ACOS 6.0.8
Firewall Configuration Guide

December, 2025

PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at:
a10-virtual-patent-marking.

TRADEMARKS

A10 Networks, Inc. trademarks are listed at: a10-trademarks

CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting www.a10networks.com.

Table of Contents

Firewall Overview

The following topics are covered:

Overview

Firewalls offer enhanced security protection for Service Provider networks by preventing unauthorized access to the application servers, preventing users from accessing potentially malicious resources, and protecting subscribers' devices from malicious software and other threats from the internet. A firewall enables network administrators to regulate how subscribers can connect and use public internet. The firewall utilizes a stateful Layer 4 firewall to protect subscribers and service providers from DDoS attacks and data tampering. It processes the incoming traffic at Layer 1-7 and supports objects with both IPv4 and IPv6 addresses.

A10 Thunder firewall also offers the following hardware-related benefits that are specific to firewall performance:

- **High throughput** – Coupled with high density 1 GbE, 10 GbE, 40 GbE, and 100 GbE port options, Thunder appliances meet the highest networking bandwidth demands.
- **High connection performance (100+ Gbps) and high scalability** – The A10 Thunder line of appliances fits all size networks with entry-level models starting at 5 Gbps and moving up to a 153 Gbps high-performance appliance, for the most demanding data center performance requirements.
- **Large number of concurrent connections** – The A10 Thunder appliances can handle a high number of concurrent connections, with high-end models capable of offering millions of connections per second (CPS) and requests per second (RPS).
- **Low latency** – The A10 Thunder appliances are powered by ACOS software, which brings a unique combination of shared memory accuracy and efficiency, 64-bit scalability, and advanced flow processing, to provide low-latency, high throughput, thus increasing the speed and performance of the network.

Firewall Deployment

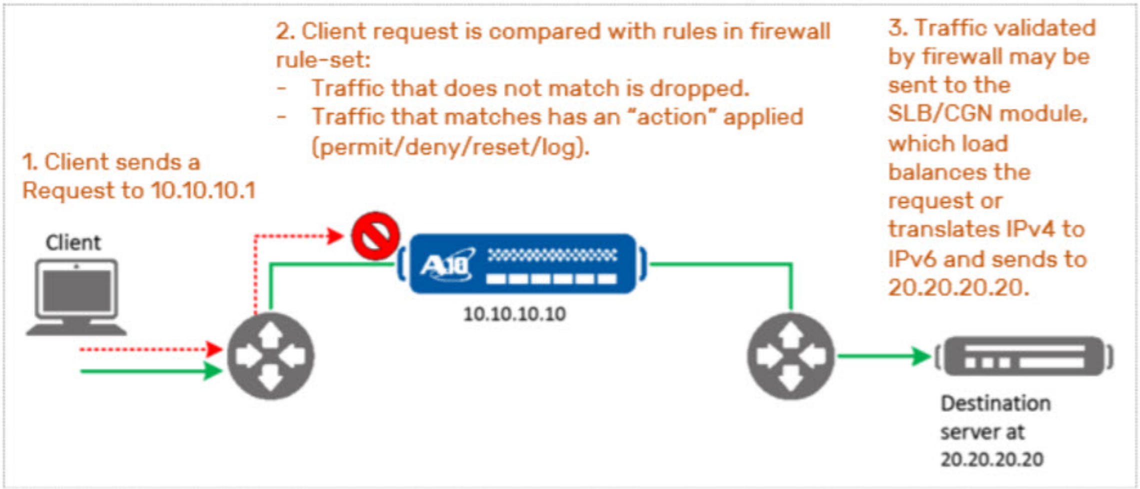
The firewall can be deployed in the following manners:

- Standalone Firewall – The firewall is deployed by itself, acting as a standalone security device.
- Data Center Firewall – The firewall can be deployed in the same partition as an Application Delivery Controller (ADC). When used with DCFW, the primary purpose of the firewall is to expose and protect the services and internal servers.
- Gi/SGi Firewall – The firewall can be deployed in the same partition as Carrier Grade NAT (CGN) that provides translation of subscriber addresses for accessing public data networks. When used with CGN, the primary purpose of the firewall is to shield residential subscribers and service providers from data tampering and attacks from the internet.

How the Firewall Works

Figure 1 illustrates basic operation of a firewall. This highly simplified example shows traffic flowing through an SLB/CGN deployment.

Figure 1 : Traffic flow through firewall


1. Client sends a Request to 10.10.10.1
2. Client request is compared with rules in firewall rule-set:
- Traffic that does not match is dropped.
- Traffic that matches has an "action" applied (permit/deny/reset/log).
3. Traffic validated by firewall may be sent to the SLB/CGN module, which load balances the request or translates IPv4 to IPv6 and sends to 20.20.20.20.
Client
A10
10.10.10.10
Destination server at 20.20.20.20

When the firewall is enabled, incoming traffic is first checked against the firewall policy (rule-set). The rules within that rule-set are used to filter traffic:

- If traffic does not match the criteria established within the rules of the firewall rule-set, then it is denied.
- If traffic matches the criteria established within the rules of the rule-set, then the pre-configured rule will act upon the traffic according to the actions. The actions can be permit, deny, reset, and log.
- Only the "permitted" traffic can establish a session with the SLB/CGN module. Traffic that does not match any rules in the rule-set is dropped before a session can be established.

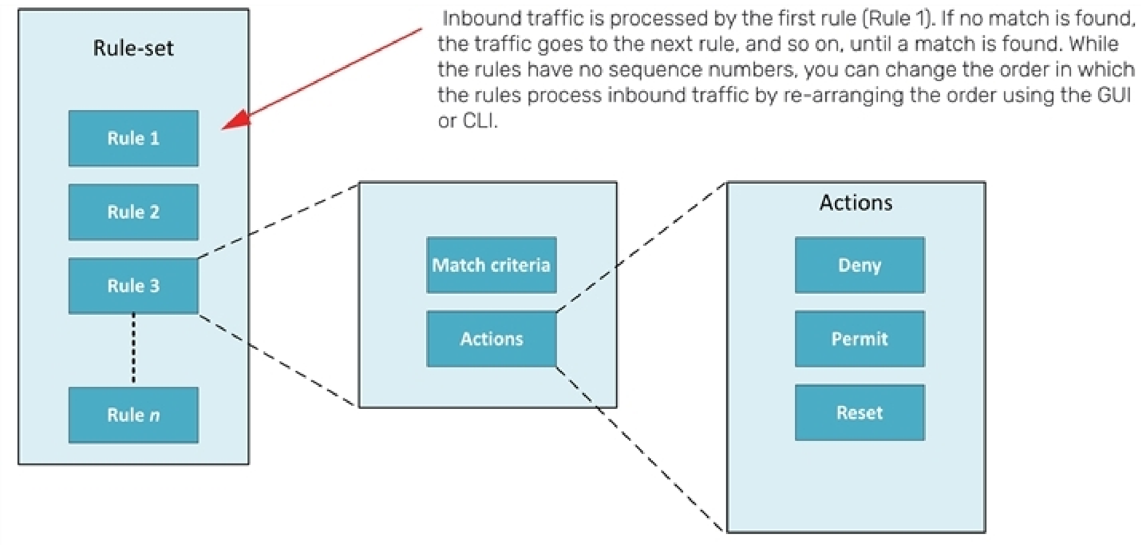
By filtering traffic before it gets to the SLB/CGN modules, the firewall can reduce security threats while simultaneously improving the performance of your network.

NOTE: In this document, the term firewall sessions refer to non-NATed traffic.

Firewall Rule-sets

Figure 2 shows the relationship between the configuration elements in a firewall rule-set.

Figure 2 : Configuration elements in a firewall rule-set



Inbound traffic is processed by the first rule (Rule 1). If no match is found, the traffic goes to the next rule, and so on, until a match is found. While the rules have no sequence numbers, you can change the order in which the rules process inbound traffic by re-arranging the order using the GUI or CLI.

NOTE:

- The firewall rule-set includes several rules.
- The Rules in a rule-set contain Match Criteria Match Criteria such as source and destination IPs, ports, object groups, and protocols.
- The rules contain one or more Actions Actions that can be applied to incoming packets.

Rule-sets

The firewall rule-sets are the top-level building blocks used to configure the firewall. The rule-sets contains one or more rules. Each rule acts like an “if/then” statement, containing match criteria and an action that will be applied to traffic if there is a match.

Based on the actions performed, the firewall allows you to configure multiple rule-set types. This enables different firewall applications such as security control, NAT, traffic control, and DDoS to classify the traffic in different ways, thereby providing flexibility and improved usability.

The following rule-set types are supported:

- Access Control: This rule-set controls the traffic by permitting or denying the packets. It also controls logging, decides how traffic is forwarded, and includes packet rewrite functions like NAT.
- Traffic Control: This rule-set applies rate limiting policies to limit the network traffic. It also supports advanced features such as hierarchical rate-limiting.

NOTE: In this document, unless mentioned otherwise, the **firewall rule-set** refers to the Access Control rule-set.

Details:

- The rule-sets must be activated before any rules can be enforced on the traffic.
- It may take approximately 10 seconds for the rule-set to become active.
- When no rule-set is active, all traffic will be allowed to pass because no firewall rules are applied to the incoming traffic.
- If an Access Control rule-set is active and no rules are defined, the default action is to **deny** the packet. Similarly, in case of Traffic Control rule-set, the default action is **no action**.

NOTE: This section offers a general description of the firewall rule-sets. For information about rule-sets specific to Gi/SGi-FW deployments, see Firewall Rule-Sets for Gi/SGi Firewall.

Using the GUI

NOTE: Currently, the GUI does not support Traffic Control rule-set configuration.

To activate the firewall rule-set using the GUI:

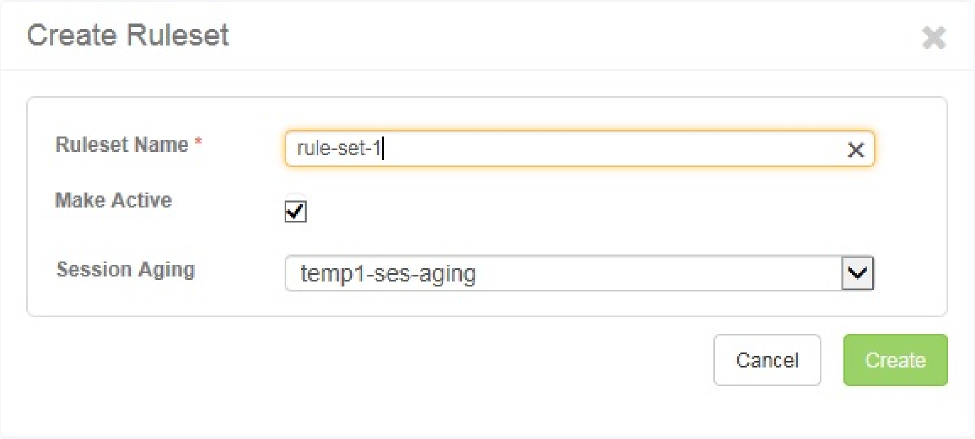
1. Navigate as follows: **Security > Firewall**.

   By default, the **Rulesets** tab is already highlighted. (If not, select the **Rulesets** tab.)

   A window appears with the configured rule-sets displayed in a table format.

2. Click **Create** at the far right. A Create Ruleset pop-up appears as shown below:

Figure 3 : Activating the firewall rule-set using the GUI



Create Ruleset

Ruleset Name *: rule-set-1

Make Active: ☑

Session Aging: temp1-ses-aging

3. In the Create Ruleset window, enter the following:
   a. Enter a name in the **Ruleset Name** field.
   b. Select the **Make Active** checkbox.

      Although multiple rule-sets can be defined, only one rule-set can be active at a time.

      It may take approximately 10 seconds for the rule-set to become active.
   c. (Optional) Click the **Session Aging** drop-down menu and select a pre-configured session aging template. The aging template allows you to define the TCP, UDP, and ICMP session timers.
4. Click **Create** to save your changes. The new firewall rule-set appears in the table.

Using the CLI

Rule-sets can be created and then globally activated using the CLI as described below:

1. Create the rule-sets using the following CLI commands. You can optionally add a rule with actions and match criteria.

   - For Access Control rule-sets:

```
rule-set rule-set-name
```

```
  rule rule-name
    action permit
     source ipv4-address address
```

- For Traffic Control rule-sets:

```
traffic-control rule-set rule-set-name
  rule rule-name
    action-group
     action limit-policy num
```

2. (Optional) Create the session-aging template. You can optionally add timeout periods for various protocols:

```
fw session-aging session-aging-template-name
  udp idle-timeout seconds
    tcp half-open-idle-timeout seconds
```

3. Activate the rule-sets with the following CLI command:

- For Access Control rule-set:

```
fw active-rule-set rule-set-name
```

- For Traffic Control rule-set:

```
traffic-control active-rule-set rule-set-name
```

Rules

Rules are the “if/then” statements inside a rule-set. For example, a possible rule could convey the following:
“if incoming traffic matches the source address 192.169.10.10, then permit the session to pass through the firewall.”

Rules are applied to traffic from the traffic initiator (client) to the responder (most likely a server). This is also known as the forward direction of traffic. Traffic in the reverse direction (i.e., from server to client) is presumed to be safe, and therefore it is not necessary to define rules to process traffic coming from the servers.

NOTE: Each rule has an administrative status (enable or disable). When the status for a rule is set to “disable,” the rule exists within the rule-set, but that rule is not acted upon.

Here is a list of criteria that can be used to filter incoming sessions:

- Match Criteria (or Match “Filters”)
- Source/Destination Zone – This can be a source zone, where a zone contains one or more physical interfaces, or VLANs.
- Source/Destination Addresses – IPv4 or IPv6 addresses (either a list or a range of addresses)
- Source/Destination Port – Either a list or a range of ports.
- Destination VIP name – The name or IP associated with a destination VIP on the ACOS device.
- Source/Destination Configuration Object – This can be a real server, virtual server, generic object, or object-group.
- Differentiated Services Code Point (DSCP)- The DSCP bits of the IP header (IPv4 and IPv6).

Match Criteria

Below are the list of match criteria that can be used to filter incoming sessions:

1. Source/destination object-groups—Network object groups can be referenced in rules to match a group of IPv4/IPv6 addresses or group of subnets, etc. For example, All subnets in Engineering or all hosts on the 2nd floor of a building, etc.
2. Source/destination subnets (both IPv4 and IPv6)
3. Source/destination zones
4. Destination VIP name—Internally this will translate to the VIP IP address. If the associated firewall action is to permit traffic that matches the VIP, then further actions will be taken by the SLB module after the traffic has passed through the firewall.
5. Service object-group—Service object groups can also be used in a rule as the match criteria to filter incoming traffic. Service object groups contain a set of TCP

or UDP services that can be grouped together. Note that if match criteria are not specified in the service object-group, all traffic will drop, since the default is “unmatched”.

6. Differentiated Services Code Point (DSCP) - The IP header (IPv4 and IPv6) DSCP bits contain packet classification information used in a rule as the match criterion. When a session matches this rule, all packets within the session are marked with the same DSCP value and are treated the same way.

   DSCP is applicable for standalone and Gi/SGi firewall.

NOTE: You can configure multiple DSCP values within the same rule using **OR** as the separator.

The DSCP values used as match filters in a rule are described in the table given below:

Binary Value	Decimal Value	DSCP Class Names
001 010	10	AF11
001 100	12	AF12
001 110	14	AF13
010 010	18	AF21
010 100	20	AF22
010 110	22	AF23
011 010	26	AF31
011 100	28	AF32
011 110	30	AF33
100 010	34	AF41
100 100	36	AF42
100 110	38	AF43
001 000	8	CS1
010 000	16	CS2
011 000	24	CS3

Binary Value	Decimal Value	DSCP Class Names
100 000	32	CS4
101 000	40	CS5
110 000	48	CS6
111 000	56	CS7
000 000	0	BE - Default
101 110	46	EF

The DSCP class names represent the following service classes:

- BE - Best Effort. There is a high probability that the routers drop these packets under congested network conditions.
- EF - Expedited Forwarding. The routers deliver assured bandwidth, low loss and low delay of packets for this service class. Voice traffic is typically marked as EF.
- AF - Assured Forwarding. The routers offer high assurance of delivering packets under prescribed conditions for this service class.
- CS - Conversational Services. The routers deliver assured (usually low) bandwidth with low delay for packets in this service class.

7. Any of the following service protocols:

   - TCP
   - UDP
   - ICMP
   - Protocol ID (followed by specific IP protocol number)

   For TCP and UDP, the ACOS device can specify the source or destination port range. Similarly, for more granular ICMP and ICMPv6 services, ACOS can specify an ICMP type and ICMP codes, as described in the tables below.

   The ICMP Types that can be used as match filters in a rule are described in Table 1.

Table 1 : Definition of ICMP Types as match criteria

Type	Element	Description
<0-254>	<0-254>	ICMP type number
any-type	any-type	Any ICMP type
Type 0	echo-reply	echo reply (used for ICMP “ping”)
Type 3	dest-unreachable	destination unreachable
Type 4	source-quench	source quench
Type 5	redirect	redirect message
Type 8	echo-request	echo request
Type 11	time-exceeded	time exceeded
Type 12	parameter-problem	parameter problem
Type 13	timestamp	timestamp
Type 14	timestamp-reply	timestamp reply
Type 15	info-request	information request
Type 16	info-reply	information reply
Type 17	mask-request	address mask request
Type 18	mask-reply	address mask reply

The ICMPv6 Types that can be used as match filters in a rule are described in Table 2.

Table 2 : Definition of ICMPv6 Types as match criteria

Element	Description
any-type	Any ICMPv6 type
Type 1	Destination-unreachable
Type 2	Packet-too-big
Type 3	Time-exceeded
Type 4	Parameter-problem
Type 128	Echo-request
Type 129	Echo-reply
Type 133	Router-solicitation

Table 2 : Definition of ICMPv6 Types as match criteria

Element	Description
Type 134	Router-advertisement
Type 135	Neighbor-solicitation
Type 136	Neighbor-advertisement
Type 137	Redirect-message

The ICMP Codes that can be used as match filters in a rule are described in Table 3.

Table 3 : Definition of ICMP Codes as match criteria

Code	Element	Description
any-code	any-code	Any ICMP code
Code 0	network-unreachable	Destination network unreachable
Code 1	host-unreachable	Destination host unreachable
Code 2	proto-unreachable	Destination protocol unreachable
Code 3	port-unreachable	Destination port unreachable
Code 4	frag-required	Fragmentation required
Code 5	route-failed	Source route failed

The ICMPv6 Codes that can be used as match filters in a rule are described in Table 4.

Table 4 : Definition of ICMPv6 Codes as match criteria

Type	Code	Description
Type 1	Code 0	No-route-to-destination
Type 1	Code 3	Address-unreachable
Type 1	Code 4	Port-unreachable
Type 4	Code 1	Unrecognized-next-header
Type 4	Code 2	Unrecognized-option

Actions

If incoming traffic matches the criteria in a rule, then the action in that rule may be applied to that traffic.

The actions that can be applied to the traffic matching criteria in the rule-set are described in Table 5.

Table 5 : Definition of actions in a rule-set

Element	Description
Deny	Silently denies the client request by dropping the packet without notifying the client.
Permit	Permits the traffic to pass through the firewall unimpeded.
Reset	Resets the TCP session, and sends an error message to notify the client. The reset option only applies to TCP traffic. Other protocol types will be silently dropped.
Log	(Optional) Logs the action applied for each connection.

For additional CGN-specific actions, see Firewall Rule-Sets for Gi/SGi Firewall.

NOTE: If an action is not specified in the configuration, then the default behavior is to deny the traffic.

For a sample firewall configuration, see Sample Firewall Configuration.

Security Zones

Security zones (or “zones”) are Layer 1 and 2 match criteria for the rules in a firewall rule-set.

Firewall rules can be configured to contain security zones. For example, you might have a source zone or a destination zone in the same rule-set.

A source zone could be set up for an interface that is facing the internal network, and a separate zone could be configured for the interface that is facing the external or public network. In this way, each security zone has a security disposition, such as being trusted, untrusted, or somewhere in between.

A zone comprises one or more physical interfaces or virtual interfaces (or “VLANs”).

Zones can be used to create logical boundaries around each interface. In the same way that multiple servers can be added to a service group for ease of configuration, a zone can be set up to include
several interfaces that could be used to handle similar types of traffic.

Details:

- A zone can include multiple interfaces, but an interface can only belong to one zone.
- The same interface cannot belong to multiple zones.
- Zones can be configured in DCFW, Gi/SGi-FW and standalone firewall deployments.

Example of Zone use

If the goal is to protect traffic from “internet to branch,” you could categorize the physical interfaces or virtual interfaces into two zones, each consisting of several interfaces/VLANs.

```
zone branchside
  interface ve 19
  network ipv4 2.2.2.0/24

zone internet
  interface ethernet 1 to 5

zone v6network
  interface ve 20
  network ipv6 2001::1/64
```

If a source or destination zone is not specified in the rule, then the zone applies as a wildcard match, meaning it will have a positive match for all traffic received from a source or destination.

Configuring the Firewall

The following topics are covered:

NOTE: For all firewall deployments, the client or inside and server or outside interfaces must be tagged using the ip client and ip server command respectively.

If there is a common partition used for NAT and transparent traffic, the same tags that are used for CGN (that is, ip nat inside or outside and ipv6 nat inside or outside) can also be used to classify the client and server interfaces.

Sample Firewall Configuration

```
ACOS(config)# rule-set test
ACOS(config-rule set:test)# rule 2
ACOS(config-rule set:test-rule:2)# action permit
ACOS(config-rule set:test-rule:2)# source ipv4-address 3.3.3.0/24
ACOS(config-rule set:test-rule:2)# source zone any
ACOS(config-rule set:test-rule:2)# dest ipv4-address any
ACOS(config-rule set:test-rule:2)# dest zone any
ACOS(config-rule set:test-rule:2)# service object-group alg
ACOS(config-rule set:test-rule:2)#dscp af23
ACOS(config-rule set:test-rule:2)#dscp cs6
ACOS(config-rule set:test-rule:2)#dscp 30 40
ACOS(config-rule set:test-rule:2)#dscp 10 20

ACOS(config-rule set:test)# rule 3
ACOS(config-rule set:test-rule:3)# action permit cgnv6
ACOS(config-rule set:test-rule:3)# source ipv4-address 3.3.3.89/32
ACOS(config-rule set:test-rule:3)# source zone any
ACOS(config-rule set:test-rule:3)# dest ipv4-address 15.15.15.90/32
ACOS(config-rule set:test-rule:3)# dest zone any
ACOS(config-rule set:test-rule:3)# service proto-id 47
ACOS(config-rule set:test)# rule 4
ACOS(config-rule set:test-rule:4)# action permit cgnv6
ACOS(config-rule set:test-rule:4)# source ipv4-address 3.3.3.89/32
ACOS(config-rule set:test-rule:4)# source zone any
ACOS(config-rule set:test-rule:4)# dest ipv4-address 15.15.15.90/32
ACOS(config-rule set:test-rule:4)# dest zone any
ACOS(config-rule set:test-rule:4)# service udp
ACOS(config-rule set:test)# rule 5
ACOS(config-rule set:test-rule:5)# action permit cgnv6
ACOS(config-rule set:test-rule:5)# source ipv4-address any
ACOS(config-rule set:test-rule:5)# source zone any
ACOS(config-rule set:test-rule:5)# dest ipv4-address any
ACOS(config-rule set:test-rule:5)# dest zone any
ACOS(config-rule set:test-rule:5)#service icmp type dest-unreachable code
port-unreachable
ACOS(config-rule set:test)# rule 6
ACOS(config-rule set:test-rule:6)# action permit cgnv6 log
ACOS(config-rule set:test-rule:6)# source ipv4-address 3.3.3.89/32
ACOS(config-rule set:test-rule:6)# source zone any
ACOS(config-rule set:test-rule:6)# dest ipv4-address 15.15.15.90/32
ACOS(config-rule set:test-rule:6)# dest zone any
ACOS(config-rule set:test-rule:6)# service icmp type echo-request

ACOS(config)# fw server syslog1 15.15.15.91
ACOS(config-real server)# port 514 udp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# fw service-group syslog1 udp
ACOS(config-fw svc group)# member syslog1 514
ACOS(config-fw svc group-member:514)# exit
ACOS(config-fw svc group)# exit

ACOS(config)# fw template logging fw_logging
ACOS(config-logging)# service-group syslog1
ACOS(config-logging)# exit
```

```
ACOS(config)# fw logging fw_logging
```

Network Address Translation with Firewall

This section describes how to configure Network Address Translation with Firewall.

The following topics are covered:

Overview of NAT with DCFW

NAT is typically used with the firewall to separate internal private network addresses from external public network addresses.

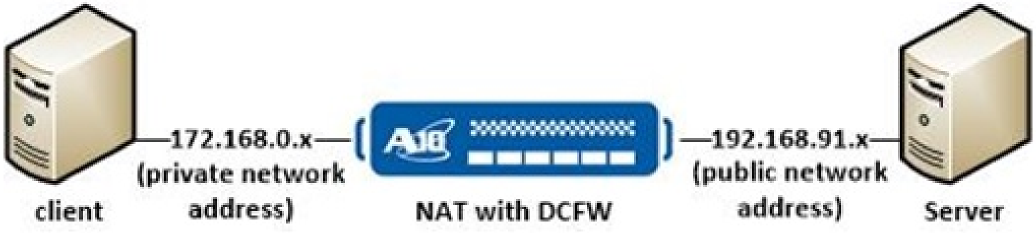
When NAT is deployed with the firewall, application protocol content may contain private IP address and port information. The application layer gateway (ALG) will translate the private information to the public information and vice versa.

When the firewall is enabled, application data sessions may be dropped if there is no matching firewall rule. Data sessions may be opened dynamically by the application, and when this happens, the ALG must work with the firewall to allow the data session through, even if no explicit rule exists.

To allow the ALG to create data sessions when no explicit rule exists, use the **`fw alg-processing override-rule-set`** command. If this option is not configured, the data session will be permitted or denied based on the explicit firewall rule configuration.

The following ALGs are supported: TFTP, FTP, PPTP, RTSP and SIP (for the full list of supported ALGs see the datasheet for the deployed platform).

Figure 4 : Network topology diagram for NAT with firewall



Sample Configuration - NAT with DCFW

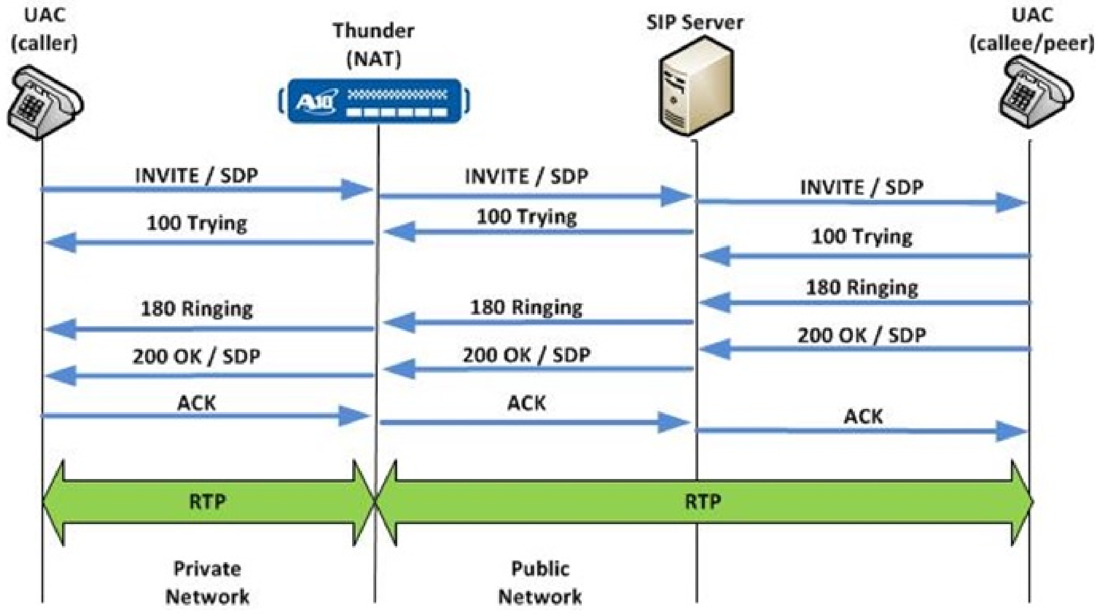
The following sample shows configuration of network address translation with firewall.

```
access-list 1 permit any
!
interface ethernet 1
  enable
  ip address 172.16.1.105 255.255.255.0
  ip nat inside
!
interface ethernet 3
  enable
  ip address 192.168.90.113 255.255.255.0
  ip nat outside
!
ip nat pool NAT-90 192.168.90.210 192.168.90.215 netmask /24 gateway
192.168.90.1
!
ip nat inside source list 1 pool NAT-90
!
ip route 0.0.0.0 /0 192.168.90.1
!
!
rule-set alg
  rule 1
    action permit
    source ipv4-address any
    source zone any
    dest ipv4-address any
    dest zone any
    service tcp dst eq 21
    service udp dst eq 69
    service udp dst eq 5060
    application any
!
fw alg-processing override-rule-set
!
fw active-rule-set alg
!
```

Configuring ALG Handling for NAT (with SIP)

The figure below shows SIP NAT ALG. The Thunder device will transform IP/port information correctly in SIP messages and prepare the RTP sessions.

Figure 5 : ALG handling for NAT with SIP

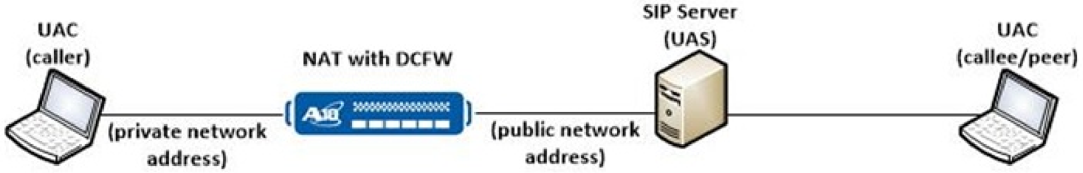


SIP and RTP protocols will work as expected.

When the firewall is enabled, RTP sessions may be denied if no explicit rule exists for the RTP session. Due to the dynamic nature of SIP, a static rule for RTP must have wider parameters, and this could result in unnecessary network exposure.

When the **`fw alg-processing override-rule-set`** option is configured, the ALG will inspect SIP messages and will automatically allow the RTP session.

Figure 6 : Network Topology diagram for NAT with firewall for SIP traffic



Application Layer Gateway

In order for various Application Layer Gateway (ALG[1]) protocols, such as FTP and SIP to function correctly through a firewall, the application must be aware of the combination of an IP address and port number that will allow incoming packets. The firewall monitors the control traffic for an FTP or SIP session, which the application will use to open up port mappings, in what is known as a “firewall pinhole”. These firewall pinholes are created dynamically, on an as-needed basis. In this way, legitimate traffic from various applications that would have otherwise been blocked can easily pass through the firewall’s security checks.

NOTE: The firewall supports ALG protocols in standalone deployments, as well as DCFW and Gi/SGi-FW deployments.

ALGs perform the following services:

- They can allow client applications to use dynamic TCP or UDP ports to establish communications with the various well-known ports that are used by the server applications. The firewall configuration might allow for a very limited number of well-known ports, but without the presence of an ALG, the ports would be blocked or perhaps the network admin would need to explicitly open up a large number of well-known ports in the firewall, which would make the network vulnerable to attacks on those ports.
- An ALG can also synchronize data for a session between two hosts. As the hosts exchange data, they could, for example, use an FTP application. This connection could use separate connections to pass traffic containing the commands used to regulate the flow and exchange of data between an end user and the distant server. If a large file is being transferred, then the control connection could remain idle for a long time. However, an ALG could prevent the control connection from being timed out by network devices before the large file transfer has completed.

[1] “ALG” may also be referred to as “Application-Level Gateway”.

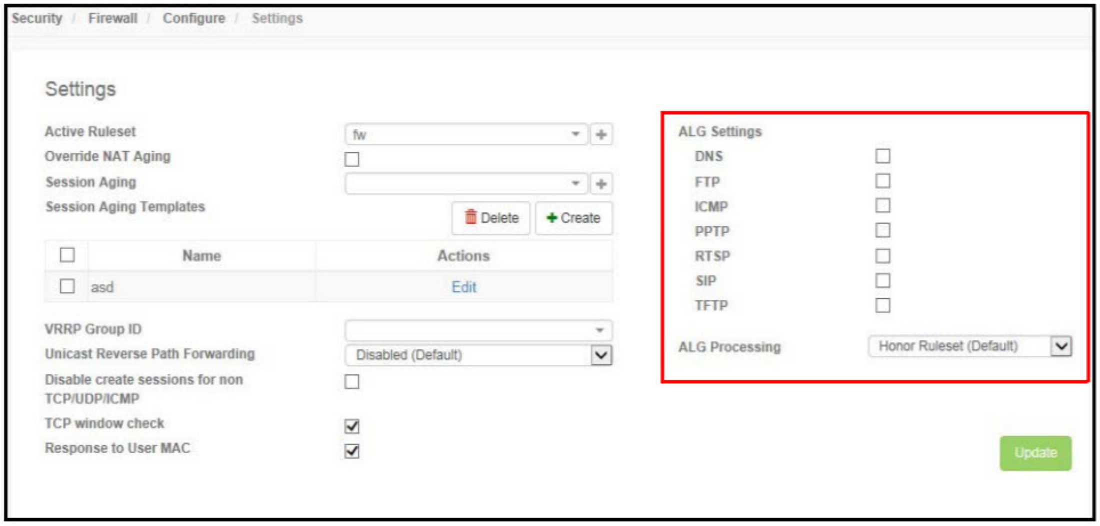
NOTE: ALGs protocols are enabled by default for traffic on well-known ports. FTP or SIP traffic may traverse the firewall, as long as the traffic is using the associated well-known port (for example, port 21 for FTP and port 5060 for SIP). The procedure below shows how to disable this default behavior so that traffic will be denied even if the ALG protocol is using its well-known port.

To configure ALG support using the GUI:

1. Navigate as follows: **Security > Firewall > Configure**.

   A window appears similar to that shown below:

   Figure 7 : Configuring ALG Support using the GUI



Security / Firewall / Configure / Settings

Settings

Active Ruleset: fw
Override NAT Aging: □
Session Aging:
Session Aging Templates

□	Name	Actions
□	asd	Edit

VRRP Group ID:
Unicast Reverse Path Forwarding: Disabled (Default)
Disable create sessions for non TCP/UDP/ICMP: □
TCP window check: ☑
Response to User MAC: ☑

ALG Settings
DNS □
FTP □
ICMP □
PPTP □
RTSP □
SIP □
TFTP □

ALG Processing: Honor Ruleset (Default)

2. Select the checkbox for the desired **ALG** protocols and port numbers to disable them. By selecting the checkbox for a protocol and its well-known port number, all ALG traffic of that type and port number will be dropped.

   You can choose to disable the following ALG protocols (on their associated well-known ports):

   - Disable DNS ALG default port 53
   - Disable FTP ALG default port 21
   - Disable ICMP ALG which allows ICMP errors to pass through the firewall

- Disable PPTP ALG default port 1723 (Not supported in DCFW deployments for 4.1.1)
- Disable RTSP ALG default port 554 (Not supported in DCFW deployments for 4.1.1)
- Disable SIP ALG default port 5060
- Disable TFTP ALG default port 69

3. Click **Update** to save your changes.

NOTE: If an application is using SIP or FTP, and the ALG is disabled on the firewall, then the application may cease to function. Clear the checkbox at a later time to re-enable ALG processing for this protocol/port combination.

To enable ALG on non-default ports using the CLI:

To (optionally) enable ALG traffic to pass through the firewall on a non-default port:

1. Use the following command to create an object-group for a service.

```
ACOS(config)# object-group service service-group-name
```

2. At the object-group service level, specify the desired protocol (for example, UDP or TCP). Since this next command allows us to specify the match criteria, you should indicate whether the match should occur on a range of port numbers, or only if the port number of the incoming traffic is equal to, greater than, or less than a designated port number.

```
ACOS(config-service:service-1)# udp eq port-num
```

3. Specify the non-default port number. (For example, you could specify the match to occur on port 1813, which is typically used for RADIUS traffic and is not the default for port DNS/UDP).

```
ACOS(config-service:service-1)# udp eq 1813
```

4. On the same line, enter the “alg” keyword, followed by the ALG protocol you want to allow to pass.

```
ACOS(config-service:service-1)# udp eq 1813 alg dns
```

CLI Example

The following example allows UDP/DNS traffic to pass through the firewall on its non-default port 1813. Typically, DNS traffic would be sent to the well-known port 53, but in our example, the traffic is only allowed to pass through if it the traffic is sent to port 1813 (which would typically be used for RADIUS):

```
ACOS(config)# object-group service SG1
ACOS(config-service:SG1)# udp eq 1813 alg dns
ACOS(config-service:SG1)# exit
ACOS(config)# exit
```

To disable ALG support using the CLI:

- Disable DNS ALG default port 53

  ```
  ACOS(config) #fw alg dns default-port-disable
  ```

- Disable FTP ALG default port 21

  ```
  ACOS(config) #fw alg ftp default-port-disable
  ```

- Disable ICMP ALG which allows ICMP errors to pass through the firewall

  ```
  ACOS(config) #fw alg icmp default-port-disable
  ```

- Disable PPTP ALG default port 1723 (Not supported in DCFW deployments for 4.1.1)

  ```
  ACOS(config) #fw alg pptp default-port-disable
  ```

- Disable RTSP ALG default port 554 (Not supported in DCFW deployments for 4.1.1)

  ```
  ACOS(config) #fw alg rtsp default-port-disable
  ```

- Disable SIP ALG default port 5060

  ```
  ACOS(config) #fw alg sip default-port-disable
  ```

- Disable TFTP ALG default port 69

  ```
  ACOS(config) #fw alg tftp default-port-disable
  ```

- Disable ESP ALG default port 500

  ```
  ACOS(config) #fw alg esp default-port-disable
  ```

Hairpinning Support

ACOS supports hairpin filtering for inside-to-inside communication (or outside-to-inside communication) of the firewall by creating a matching full-cone session.

ACOS creates a full-cone session if there is a firewall rule match that occurs with action “permit listen-on-port”. When ACOS creates the full-cone session, the corresponding hairpin session does not have to “re-match” the criteria in the firewall rule, and the session is allowed by ACOS device.

This is similar to how matching works ALG (i.e., ACOS allows free passage for the control- and data-sessions). Whenever a full-cone or hairpin session is created and freed, the ACOS device increments the counters for TCP and UDP. Full-cone sessions will increment the Outbound counter and hairpin sessions will increment the Inbound counter, as seen in the output from the `show fw full-cone-sessions` command.

NOTE: For firewall-only cases, when the `listen-on-port` option is enabled, full-cone sessions are created for IPv4 and IPv6 packets only for UDP or TCP traffic only. For each full-cone and hairpin session, counters should be displayed.

For information, see the **`rule`** and **`show counters fw global`** commands in the *Command Line Reference Guide*.

Disabling Inbound Refresh for Full-Cone and Data sessions

The session age for full-cone sessions is refreshed when new data sessions are created, and the data sessions are refreshed upon receiving inbound TCP SYN or UDP packets. This default behavior prevents the sessions from aging out, at Outbound (client to server), and Inbound (server to client) traffic. However, it also allows external attackers and misbehaving applications to keep the mapping alive indefinitely by sending packets to these sessions, thereby posing a security risk and capacity exhaustion. The firewall has the provision to disable the session refresh even upon receiving inbound packets. This allows the full-cone sessions and data sessions to age out and to be freed, thus reducing the security risk.

CLI Configuration

- To disable inbound refresh, configure the following commands at the partition level:
  - For full-cone sessions:

    ```
    ACOS(config)# fw inbound-refresh-full-cone disable
    ```

  - For data sessions:

    ```
    ACOS(config)# fw inbound-refresh disable
    ```

NOTE: The above commands do not apply to outbound packets i.e., the sessions continue to refresh if outbound packets are sent.

- To view the session statistics, use the **show fw full-cone-sessions** command as shown below:

  ```
  ACOS(config)# show fw full-cone-sessions
  ```

  Consider the following example outputs.

  Example 1:

  ```
  Firewall - Full-cone Sessions:
  Prot  Inside Address  Outbnd  Inbnd  CPU  Age
  ---------------------------------------------
  UDP   10.1.1.1:10000   1       0      1    -
  Total Full-cone Sessions: 1
  ```

  In this output, there is one active outbound session. The symbol '-' in the Age field indicates that the full-cone session is active i.e., session aging hasn't started yet.

  Example 2:

  ```
  Firewall - Full-cone Sessions:
  Prot  Inside Address  Outbnd  Inbnd  CPU  Age
  ---------------------------------------------
  UDP   10.1.1.1:10000   0       1      1    x
  Total Full-cone Sessions: 1
  ```

In this output, there is one active inbound session. The symbol **x** in the **Age** field indicates that the full-cone session is inactive and will reject any new inbound data sessions matching the full-cone session. However, the inactive full-cone session will be re-activated if a new outbound data session is created.

Processing Traffic without Matching Session

The firewall processes and forwards TCP SYN packets by creating a data session. However, it drops non-SYN TCP packets if no session is created for the connection. Additionally, in certain cases when sessions are created before the firewall becomes active or during reconfiguration/reconnection, legitimate traffic might get dropped unnecessarily.

The **fw allow-non-syn-session-create** command enables accepting and further inspection of traffic that does not match to any session. Enabling this command creates a session **on the fly** so that consequent packets are processed in the usual manner.

This command supports IPv4 and IPv6 traffic.

NOTE: Since DNS uses port 53 as a default port for transmitting DNS queries, the non-SYN TCP packets are dropped even if the **fw allow-non-syn-session-create** command is enabled. To transmit non-SYN TCP packets from port 53, you need to disable the default port by executing the **fw alg dns default-port-disable** command.

CLI Configuration

- To forward non-SYN TCP packets, configure the following command:

```
ACOS(config)# fw allow-non-syn-session-create
```

- The Non-SYN pkt forward allowed counter is incremented each time a non-SYN packet is forwarded by the firewall. To view this counter, use the following command:

```
ACOS(config)# show counters fw global
```

Known Limitations

- You cannot configure this command if the **`fw tcp syn-cookie`** command is configured globally or the TCP SYN cookie protection is enabled in the rule of the firewall rule-set.
- Rule actions for CGN and IPsec are not supported.
- If the rule matching criteria includes application/category evaluation, the classification result may not be available if beginning of the session is missed. It will be considered as no match and the configured policy action will be applied.

TCP Window Checks

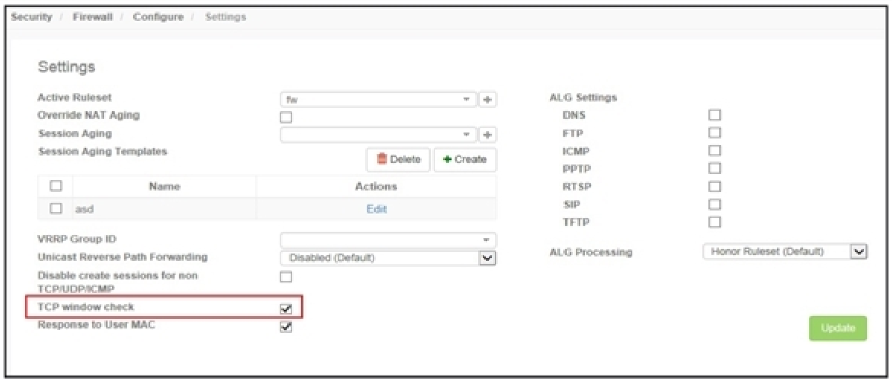
TCP Window Checks are a security function that can be used to ensure TCP packets are within the advertised window by tracking the sequence numbers and acknowledgment of traffic in both directions. Packets that are outside the advertised window will be denied.

If TCP Window Checks are not already enabled, you can do so using the GUI:

1. Navigate as follows: **Security > Firewall > Configure**.

   A window appears similar to that shown below:

   Figure 8 : Configuring TCP Window Checks using the GUI



Security / Firewall / Configure / Settings

Settings

Active Ruleset: fw
Override NAT Aging: □
Session Aging:
Session Aging Templates

□	Name	Actions
□	asd	Edit

VRRP Group ID:
Unicast Reverse Path Forwarding: Disabled (Default)
Disable create sessions for non TCP/UDP/ICMP: □
TCP window check: ☑
Response to User MAC: ☑

ALG Settings
DNS □
FTP □
ICMP □
PPTP □
RTSP □
SIP □
TFTP □

ALG Processing: Honor Ruleset (Default)

2. Select the **TCP Window Check** checkbox to enable the feature.
3. Click **Update** to save your changes.

Using the CLI

If TCP Window Checks are not already enabled, you can do so using the CLI:

1. Use the following command to enable TCP window checks:

   ```
   fw tcp-window-check enable
   ```

2. (Optional) use the following command to enable baselining and rate calculation for packets
   outside the TCP window:

   ```
   fw tcp-window-check sampling-enable outside-window
   ```

3. (Optional) use the following command to disable TCP window checks:

   ```
   fw tcp-window-check disable
   ```

(missing or bad snippet)the *Command Line Reference Guide*.

Immediate TCP Session Closure

After receiving a TCP RST packet, A10 Firewall immediately unlinks the TCP session from the active session table before adding the session to the delete queue. Since the subsequent packets do not match the session, the TCP session closes instantly, and no packets are forwarded. The **fw tcp-rst-close-immediate** command is enabled by default to support this behavior so that TCP sessions close immediately after receiving RST packets. This action proves to be useful in case of a TCP Reset attack.

However, in certain scenarios, ACOS needs to forward packets even after receiving an RST. For example, if ACOS receives an RST/ACK packet from the client immediately after receiving an RST, it needs to forward the RST/ACK packet to the server. Since the **fw tcp-rst-close-immediate** command is enabled by default, ACOS doesn't forward RST/ACK packet to the server; instead, it sends an RST to the client and closes the connection immediately. The **fw tcp-rst-close-immediate disable** command can be configured to change the above-mentioned behavior.

When this command is configured, the Firewall waits for a stipulated time (1 to 2 seconds) to unlink the TCP session from the active session table before adding it to the delete queue. If ACOS receives an RST/ACK packet from the client within this time frame, the packet is forwarded to the server.

CLI Configuration

- To disable the immediate closure of TCP sessions on receiving an RST packet:x

```
ACOS(config)# fw tcp-rst-close-immediate disable
```

- To enable immediate closure of TCP sessions on receiving an RST packet:

```
ACOS(config)# fw tcp-rst-close-immediate enable
```

Creating Full Sessions in DSR Mode

The ACOS device creates a TCP session after completing the standard 3-way TCP handshake. However, if the device is deployed in Direct Server Return (DSR) mode, the standard TCP three-way handshake cannot be completed and therefore fully established sessions cannot be created in the DSR mode.

The **fw dsr-mode-support** command is introduced to allow session creation when the device is deployed in the DSR mode. When this command is configured, a fully established session is created on receiving a single IPv4 or IPv6 TCP packet even if the standard three-way handshake is incomplete. The session is created on receiving any TCP packet except RST and FIN.

NOTE: If the **fw allow-non-syn-session-create** command is also enabled, a full session is created even on receiving a SYN TCP packet.

CLI Configuration

Configure the **fw dsr-mode-support** command to create fully established sessions in the DSR mode on receiving any TCP packet (except RST and FIN). Sessions can be created based on whether the incoming TCP packets are IPv4 or IPv6.

- To create sessions for IPv4 TCP packets:

```
ACOS(config)# fw dsr-mode-support ipv4
```

- To create sessions for IPv6 TCP packets:

```
ACOS(config)# fw dsr-mode-support ipv6
```

- To create sessions for any (IPv4 or IPv6) TCP packets:

```
ACOS(config)# fw dsr-mode-support all
```

Limitations

Following are the limitations of **`fw dsr-mode-support`** command:

- Supports session creation for TCP traffic only.
- Does not support ALG session creation.
- Firewall application classification may not work as expected.

DDoS Protection with Dynamic Blacklisting

Normally, when the platform intercepts a volumetric DDoS attack, a lot of traffic hits the deny rules, and packets are dropped based on the per-packet rule lookup. However, due to the high amount of traffic, the overhead of the per-packet rule lookup can cause CPU usage to spike. To drop these packets more efficiently i.e., with minimum processing, you can configure the **`fw ddos-protection dynamic-blacklist`** command at the partition level. When this command is enabled, if a particular deny rule is matched, the firewall creates blacklist sessions dynamically (‘on the fly’) to process such traffic efficiently. Subsequent traffic that matches the blacklist session is dropped. These sessions come out of the total session capacity in the Thunder device.

NOTE: When this DDoS protection is configured, the protective mechanism of creating blacklist sessions is triggered on a per-core basis only when the CPU utilization for that core exceeds the pre-configured threshold limit.

CLI Configuration

- To enable DDoS protection by creating blacklist sessions, configure the **`fw ddos-protection dynamic-blacklist`** command.

```
ACOS(config)# fw ddos-protection dynamic-blacklist [ enable | disable ]
[ inbound | outbound | both ] [timeout seconds ]
```

The following example demonstrates command usage:

```
ACOS(config)# fw ddos-protection dynamic-blacklist enable inbound
timeout 20
```

This configuration enables DDoS protection for inbound (downlink) traffic only. It captures all external traffic that is being initiated from the internet. Additionally, to enable DDoS protection for inbound as well as outbound traffic, configure the option **both**.

- To view the number of active blacklist sessions and the number of blacklist sessions created and freed, use the the **show session blacklist-sessions** or **show session brief** command. You can also use the **show counters system session** command to view this information.

  Example output for **show session blacklist-sessions** command:

```
ACOS(config)# show session blacklist-sessions
Traffic Type                       Total
---------------------------------------------
Total Sessions                     1
TCP Established                    0
TCP Half Open                      0
Server TCP Established             0
Server TCP Half Open               0
SCTP Established                   0
SCTP Half Open                     0
UDP                                0
Non TCP/UDP IP sessions            1
Other                              0
Reverse NAT TCP                    0
Reverse NAT UDP                    0
Curr Free Conn                     2039791
Conn Count                         2
Conn Freed                         1
TCP SYN Half Open                  0
Blacklist sessions                 1
Blacklist sessions Created         2
Blacklist sessions Freed              1
Conn SMP Alloc                        7
Conn SMP Free                         0
Conn SMP Aged                         0
Conn Type 0 Available                 3670016
Conn Type 1 Available                 1998843
Conn Type 2 Available                 933886
Conn Type 3 Available                 458752
Conn Type 4 Available                 229376
Conn SMP Type 0 Available             3670016
Conn SMP Type 1 Available             1835008
Conn SMP Type 2 Available             917504
Conn SMP Type 3 Available             466936
Conn SMP Type 4 Available             229376
Total Local Sessions                  0
Prot Forward Source              Forward Dest              Reverse Source
 Reverse Dest                 Age   Hash Flags            Type
------------------------------------------------------------------------
------------------------------------------------------------------------
Udp  172.16.25.204:1024       172.16.35.205:1024        0.0.0.0
0.0.0.0                      2     4    NFe0f0r0         FW-BLACKLIST

Total Sessions:  1
```

In the above output, the **Type** field indicates that the session is a blacklist session.

Example output for **show counters system session** command:

```
ACOS(config)# show counters system session | inc Blacklist
Blacklist Sessions                             0
Blacklist Session Created                      13
Blacklist Session Freed                        13
```

- To view the number of packets dropped, and the number of blacklist sessions created and freed, use **the show counters fw global** command.

  Example output:

```
ACOS(config)# show counters fw global | inc Blacklist
Dynamic Blacklist Session Created              23
Dynamic Blacklist Freed                        23
Dynamic Blacklist - Packet Drop                0
```

For command details, refer to the *Command Line Reference Guide*.

Limitations

- This feature is less effective if the attack traffic continuously changes the IP addresses.
- If application classification is enabled, the blacklist session is created only after the application is classified. Prior to that, a regular firewall session is created that allows packets to flow through. After classification, when a deny rule is matched, the firewall session is replaced with a blacklist session.
- The creation and deletion of blacklist sessions is not logged. Moreover, if the logging option is specified in the rule, it is ignored when this feature is active.

Support for High Availability with VRRP-A

The firewall supports VRRP-A for high availability with up to 8 devices in a VRRP-A configuration.

You can specify a VRID group in the per-partition firewall global parameters. Firewall sessions will be synchronized to the standby units.

NOTE: For DCFW to operate properly with VRRP-A, you must configure a “vrrp-a interface” for each VRRP-A peer, and each VRRP-A peer must be reachable over only one subnet. For more information about the CLI command used to add the firewall to a VRRP-A cluster, see `fw vrid` command in the *Command Line Reference Guide*. For a comprehensive discussion of VRRP-A, see the document *Configuring VRRP-A High Availability*.

Hardware Offloading Of Firewall Sessions

In general, all firewall sessions are processed and forwarded by the software. This may cause a spike in CPU usage in case of heavy network traffic. In such scenarios, you can offload some of the firewall sessions to the hardware. Hardware offloading frees up the CPU cycles, thereby enhancing the overall throughput, efficiency, and latency of the Thunder device. This feature can be enabled by configuring the **`system hardware-accelerate session-forwarding`** command.

In ACOS, hardware offloading (also known as hardware acceleration or hardware forwarding) is only supported on FPGA devices having Ternary Content-Addressable Memory (TCAM). TCAM is a specialized memory used in high-speed search applications. Thunder devices having a TCAM provide the capability to forward firewall sessions to the hardware by programming the flows in the available TCAM.

The packet processing statistics are periodically exported to the software. The statistics can be viewed using show commands (see CLI Configuration).

Hardware Offloading Features in ACOS

- Supported only on TH7655 (Lite), TH6435, and TH14045 devices.
- Only the following sessions can be offloaded to the hardware:
  - CGN LSN (NAT44) and NAT64
  - Fixed NAT
  - Firewall (Only TCP and UDP traffic)
- Up to 128K IPv4 sessions or 64K IPv6 sessions can be offloaded to the hardware.
- Only established sessions can be offloaded to hardware.
- Only active sessions can be forwarded; standby sessions cannot be forwarded.

CLI Configuration

- To enable hardware offloading of firewall sessions, configure the following command:

  ```
  ACOS(config)# system hardware-accelerate session-forwarding
  ```

- To check if a particular session is forwarded using hardware, use the **`show sessions`** command. The flags field in the show command output indicates that the session is offloaded to the hardware.
- To view the information on the hardware entries being programmed into the TCAM, use the **`show hardware-accelerate statistics`** command.

  Consider the following show command output:

```
ACOS# show hardware-accelerate statistics
Security Policy Engine Traffic statistics
-----------------------------------------
Total Hit Counts                            5
Total IPv4 hardware Hit Counts              5
Total IPv6 hardware Hit Counts              0
Total Available IPv4 SPE Entries            131072
Total Available IPv6 SPE Entries            65536
Total IPv6 hardware forwarded packets       0
Total SPE programming requests              8
Total SPE programming errors                0
Total Ageeout Drop Counts                   0
Total Flow singlebit Errors                 0
Total Tag Mismatch Errors                   0
Total Sequence Mismatch Errors              0
Total Program Invalidation drop Counts      0
Total Flow Drop Counts                      0
Total Flow Error Counts                     0
Total Flow Unalign Counts                   0
Total Flow Underflow Counts                 0
Total Flow TX Full Drop Counts              0
Total Flow QDR Full Drop Counts             0
Total Flow Phyport Mismatch Drop Counts     0
Total Flow VLAN-ID Mismatch Drop Counts     0
Total Flow VMID Mismatch Drop Counts        0
Total Flow Protocol Mismatch Drop Counts    0
```

The **`Total IPv4 hardware Hit Counts`** field indicates that five IPv4 packets are hardware forwarded. Similarly, the **`Total SPE programming requests`** field indicates that eight SPE programming requests are made to forward packets to the hardware.

- To view the hardware offloading statistics for the Firewall sessions, use the show counters fw hw-accelerate command.

Example output:

```
ACOS# show counters fw hw-accelerate
show counters fw hw-accelerate
**************************************
HW Entries Created                                 4
HW Entry Creation Failed                           0
HW Entry Creation Failed - server down             0
HW Entry Creation Failed - max entries exceeded    0
HW Entries Freed                                   4
HW Entries Freed - opposite tuple entry aged-out   2
HW Entry Freed - no HW prog                        0
HW Entry Freed - no matched conn                   0
HW Entry Freed - no software entry                 16
HW Entries Count                                   0
HW Entries Aged Out                                8
HW Entries Aged Out - idle timeout                 8
HW Entries Aged Out - TCP FIN                      0
HW Entries Aged Out - TCP RST                      0
HW Entries Aged Out - invalid dst                  0
HW Entries Force HW Invalidate                     0
HW Entries Invalidate due to server down           0
TCAM Flows Created                                 2
TCAM Flows Freed                                   2
TCAM Flow Count                                    0
```

For more information on commands, refer to the *Command Line Interface Reference* guide.

Limitations

The following are the limitations of hardware offloading:

- Hardware offloading is not supported for features that involve inspection of the payload. Therefore, the following features cannot be offloaded:
  - ALG sessions (for CGN and Firewall)
  - Tunnelled traffic (for example, DS-lite)
  - DNS64 sessions
  - SCTP, GTP traffic
  - Rate-limiting
  - Application classification

- Stateful and Generic Firewall sessions
- Firewall local connections

- Since sessions can be offloaded only after they are established, the first few packets are always forwarded to the software.
- Hardware offloaded sessions do not support Round-Robin as a load-balancing method across trunk members.
- Fat flows are not supported.

Configuring Firewall on Multi-PU Platforms

On multi-PU platforms (such as TH14045 or TH7650/TH7655S), the traffic is distributed across multiple Processing Units (multi-PUs). These platforms are built for large-scale traffic distribution, load balancing, and scalability. The multi-PU architecture has two active PUs; PU1 and PU2. User traffic is distributed between the two PUs statefully. Both PUs can process the traffic, store the data, files, and compute statistics respectively.

Configuring the firewall on multi-PU platforms is based on the firewall type. For configuration steps and other details, refer to the following topics:

- Data Center Firewall on Multi-PU Platforms
- Gi/SGi Firewall on Multi-PU Platforms

For general multi-PU implementation details, see the *Application Delivery Controller* guide.

Support for Web Filtering

ACOS supports the following types of filters that can be added to the Firewall rule.

The following topics are covered:

Geo-Location Filtering

Integration of Geo-Location lists with firewall rules allows an administrator to define firewall rules that use the geo-location list or **Geo List**, instead of using a specific IP address to identify a server or destination host. This is supported for both source and destination IP-based filters in the firewall rule.

The geo-location can be specified as a single entry or as a Geo-list and bound to an IP or geo-location filter in the firewall rule-set. The IPs can be added to the firewall rule for the source or destination match. The **Geo List** supports the IPv6 and the configuration for periodic update.

A predefined Geo-location list can be associated to a firewall rule. Firewall uses geo-location to classify traffic. Currently, you can configure the source and destination and add a list of geo-locations at the source and destination for a rule.

The geo-location list or a single geo-location name can be used in firewall rule-set as source or destination filter using the following commands:

```
ACOS(config-rule set:1-rule:1)#source geolocation name1
ACOS(config-rule set:1-rule:1)#source geolocation list list-name1

ACOS(config-rule set:1-rule:1)#dest geolocation name2
ACOS(config-rule set:1-rule:1)#dest geolocation list list-name2
```

ACOS provides predefined geo-location databases like **IANA** (default), **Geo-Lite City**, and **Geo-Lite Country** that contain mappings of IP addresses to geographic locations. These databases can also be used to create geo-location lists.

The databases can be loaded or unloaded using the following command:

```
ACOS(config)# no system geo-location load iana
ACOS(config)# system geo-location load GeoLite2_Country
```

NOTE: Geo-location databases are not fully supported on Multi-PU Platforms (like TH7650 and TH14045). The databases do not synchronize with both PUs after being loaded.

Configuration Example: Deny Services Configuration at Firewall

Deny specific countries from accessing services. For example, to deny specific services to be accessed by users in some countries the configuration procedure is as follows.

1. Configure geo-location list with countries that the services are not applicable.

```
ACOS(config)# system geoloc-list blocked-list
ACOS(config-geoloc-list:blocked-list)# include Asia.China
ACOS(config-geoloc-list:blocked-list)# include Asia.Japan
```

2. Define firewall rule-set, and use geo-location-list at source filter.

```
ACOS(config)# rule-set r1
ACOS(config-rule set:r1)# rule deny
ACOS(config-rule set:r1-rule:deny)# source geolocation list blocked-
list
```

3. Configure geo-location list at source filter. Traffic from these countries will be denied.

```
ACOS(config-rule set:r1)#rule allow
```

4. Configure a default rule to pass other traffic.

```
ACOS(config-rule set:r1-rule:allow)# action permit
ACOS(config-rule set:r1-rule:allow)# show running-config | sec rule
rule-set r1
  rule deny
    action deny
    source geolocation list blocked-list
    source ipv4-address any
    source zone any
    dest ipv4-address any
    dest zone any
    service any
  rule allow
    action permit
    source ipv4-address any
    source zone any
    dest ipv4-address any
    dest zone any
service any
```

5. Apply the rule-set.

```
ACOS(config)# fw active-rule-set r1
```

Configuration Example: Block CGN Users

Block CGN users from accessing some countries. For example, block the user from accessing the whole country of China and Japan.

1. Configure geo-location list with countries which are not allowed to access.

```
ACOS(config)# system geoloc-list blocked-list
ACOS(config-geoloc-list:blocked-list)# include Asia.China
ACOS(config-geoloc-list:blocked-list)# include Asia.Japan
```

2. Define firewall rule-set, and use geo-location-list as destination filter.

```
ACOS(config)# rule-set r1
ACOS(config-rule set:r1)# rule deny
ACOS(config-rule set:r1-rule:deny)# dest geolocation list blocked-list
```

3. Configure geolocation list as destination filter. Traffic to these countries will be denied.

```
ACOS(config-rule set:r1)# rule allow
```

4. Configure a default rule to pass other CGN traffic.

```
ACOS(config-rule set:r1-rule:allow)# action permit cgnv6
```

5. Verify the rule-setup. The deny and allow rules are setup.

```
ACOS(config-rule set:r1-rule:allow)# show running-config | sec rule
rule-set r1
  rule deny
    action deny
    source ipv4-address any
source zone any
dest geolocation list blocked-list
    dest zone any
    service any
  rule allow
    action permit cgnv6
    source ipv4-address any
    source zone any
    dest ipv4-address any
    dest zone any
service any
```

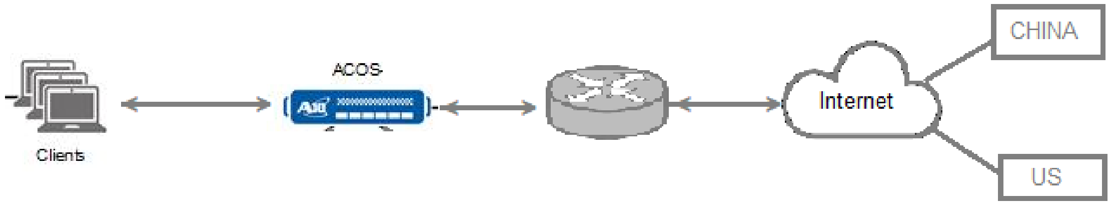
6. Apply the rule-set.

```
ACOS(config)# fw active-rule-set r1
```

CLI Implementation Example: GiFW Geo-Location Filtering

The following diagram illustrates the part of network topology for geo-location filtering setup with ACOS device.

Figure 9 : Geo-Location Filtering Configuration Topology



Base CGN configuration

Use an ACOS device pre-configured with CGN. The base CGN configuration on ACOS device can be viewed using the following command:

```
ACOS(config)# show running-config
!Current configuration: 357 bytes
!Configuration last updated at 00:24:24 GMT Wed Nov 14 2018
!Configuration last saved at 00:24:25 GMT Wed Nov 14 2018
!64-bit Advanced Core OS (ACOS) version 4.1.4-P3, build 104 (Nov-06-
2018,18:35)
!
multi-config enable
!
terminal idle-timeout 0
!
class-list ip4_all
  0.0.0.0/0 lsn-lid 1
!
```

```
hostname ACOS
!
interface management
  ip address 192.168.105.231 255.255.255.0
  ip default-gateway 192.168.105.1
!
interface ethernet 1
  enable
  ip address 60.1.1.231 255.255.255.0
  ip nat outside
!
interface ethernet 2
  enable
  ip address 61.1.1.231 255.255.255.0
  ip nat inside
!
!
ip route 0.0.0.0 /0 60.1.1.108
!
cgnv6 lsn inside source class-list ip4_all
!
cgnv6 nat pool lsn_pool 60.1.14.1 60.1.14.20 netmask /24
!
cgnv6 lsn-lid 1
  source-nat-pool lsn_pool
!
!
end
```

1. The CGN traffic can now pass though the ACOS device.

```
On Client, ping  204.79.197.200
ACOStest@C107:~$ ping 204.79.197.200
PING 204.79.197.200 (204.79.197.200) 56(84) bytes of data.
64 bytes from 204.79.197.200: icmp_seq=1 ttl=109 time=44.1 ms

ACOStest@C107:~$ ping 61.135.169.121
PING 61.135.169.121 (61.135.169.121) 56(84) bytes of data.
64 bytes from 61.135.169.121: icmp_seq=1 ttl=52 time=2.90 ms
64 bytes from 61.135.169.121: icmp_seq=2 ttl=52 time=2.81 ms
```

2. 204.79.197.200 is located in U.S. and 61.135.169.121 is located in China. The client can access both China and U.S. In this example, to block client from accessing U.S, load the geo-location database. We use built-in MAXMIND database here.

```
ACOS(config)# system geo-location load GeoLite2-Country
```

3. Check if the database is loaded, using **`show geo-location file`** command:

```
ACOS(config)# show geo-location file
                Per = Percentage of loading, Err/W = Error or Warning
                T = T(Template)/B(Built-in)

Filename                T Template               Per  Lines    Success
Err/W
-----------------------------------------------------------------------
---------
iana*                   B                        100% 73       73
0
GeoLite2-Country        B                        100% 300032   300032
0
```

4. Check the geo-location for (U.S.) 204.79.197.200 and (China) 61.135.169.121

```
ACOS(config)# show geo-location ip 204.79.197.200
                 Last = Last Matched Client, Hits = Count of Client
matched
                 T = Type, Sub = Count of Sub Geo-location
                     G(global)/P(policy), S(sub)/R(sub range)
                     M(manually config)/B(built-in)
Global
Name          From            To/Mask          Last            Hits
Sub  T
-----------------------------------------------------------------------
---------
North America 204.79.196.0    204.79.197.255                   0
68339GR
.United States

ACOS(config)# show geo-location ip 61.135.169.121
                 Last = Last Matched Client, Hits = Count of Client
matched
```

```
                 T = Type, Sub = Count of Sub Geo-location
                     G(global)/P(policy), S(sub)/R(sub range)
                     M(manually config)/B(built-in)

Global
Name          From            To/Mask         Last            Hits
Sub  T
-----------------------------------------------------------------------
---------
Asia.China    61.128.0.0      61.143.255.255                  0
6901 GR
```

5. Configure geo-location list. To block U.S, we must use geo-location list as blocked-list, containing the countries that we must block.

```
ACOS(config)# system geoloc-list blocked-list
ACOS(config-geoloc-list:blocked-list)# include "North America.United
States"
```

6. Configure firewall rule-set.

```
ACOS(config)# rule-set 1
```

   a. Configure a rule “`deny-dest-us`” to block traffic using `geolocation list blocked-list` to block traffic to U.S. North America at destination.

   ```
   ACOS(config-rule set:1)#rule deny-dest-us
   ACOS(config-rule set:1-rule:deny-dest-us)# action deny
   ACOS(config-rule set:1-rule:deny-dest-us)# dest geolocation list
   blocked-list
   ```

   b. Configure another rule to allow CGN traffic.

   ```
   ACOS(config-rule set:1)#rule allow-cgn
   ACOS(config-rule set:1-rule:allow-cgn)# action permit cgnv6
   ```

   c. Check the running configuration with rule-set.

   ```
   ACOS(config-rule set:1-rule:allow-cgn)# show running-config | sec
   rule-set
   rule-set 1
     rule deny-dest-us
       action deny
   ```

```
    source ipv4-address any
    source zone any
    dest geolocation list blocked-list
    dest ipv4-address any
    dest zone any
    service any
  rule allow-cgn
    action permit cgnv6
    source ipv4-address any
    source zone any
    dest ipv4-address any
    dest zone any
    service any
```

d. Activate the rule-set

```
ACOS(config)# fw active-rule-set 1
```

7. Check geo-location filtering function.

```
ACOStest@C107:~$ ping 61.135.169.121
PING 61.135.169.121 (61.135.169.121) 56(84) bytes of data.
64 bytes from 61.135.169.121: icmp_seq=1 ttl=52 time=11.0 ms
64 bytes from 61.135.169.121: icmp_seq=2 ttl=52 time=2.55 ms

ACOStest@C107:~$ ping 204.79.197.200
PING 204.79.197.200 (204.79.197.200) 56(84) bytes of data.

--- 204.79.197.200 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms
```

We can see that traffic to 204.79.197.200 (U.S.) are blocked for CGN users, using the
`show geoloc-list blocked-list` command.

```
ACOS(config)# show geoloc-list blocked-list
system geoloc-list blocked-list
  include North America.United States | status :Active. hit:3
  --------------------
  Total hit: 3
  Total geolocation name: 1
  Total active: 1
```

8. To check geo-location list statistics and firewall rule-set statistics, use the `show rule-set 1` command.

```
ACOS(config)# show rule-set 1
Rule-Set-Name: 1
Rule-Set-Status : active
Unmatched-Drops: 61    Action-Permit: 1919    Action-Deny: 3    Action-
Reset: 0
Total-Rule-Count: 2

Rule-Name:                      deny-dest-us
Hit-Count:                      3
Action:                         deny
Status :                         enable
Permit-bytes:                   0
Deny-bytes:                     294
Reset-bytes:                    0
Total-bytes:                    294
Permit-packets:                 0
Deny-packets:                   3
Reset-packets:                  0
Total-packets:                  3
TCP-active-session:             0
UDP-active-session:             0
ICMP-active-session:            0
SCTP-active-session:            0
OTHER-protocol-active-session:  0
Total-active-session:           0
TCP-session:                    0
UDP-session:                    0
ICMP-session:                   0
SCTP-session:                   0
OTHER-protocol-session:         0
Total-session:                  0

Rule-Name:                      allow-cgn
Hit-Count:                      1919
Action:                         permit cgnv6
```

```
Status :                         enable
Permit-bytes:                   614
Deny-bytes:                     0
Reset-bytes:                    0
Total-bytes:                    614
Permit-packets:                 7
Deny-packets:                   0
Reset-packets:                  0
Total-packets:                  7
TCP-active-session:             0
UDP-active-session:             0
ICMP-active-session:            0
SCTP-active-session:            0
OTHER-protocol-active-session:  0
Total-active-session:           0
TCP-session:                    3
UDP-session:                    0
ICMP-session:                   1
SCTP-session:                   0
OTHER-protocol-session:         0
Total-session:                  4
```

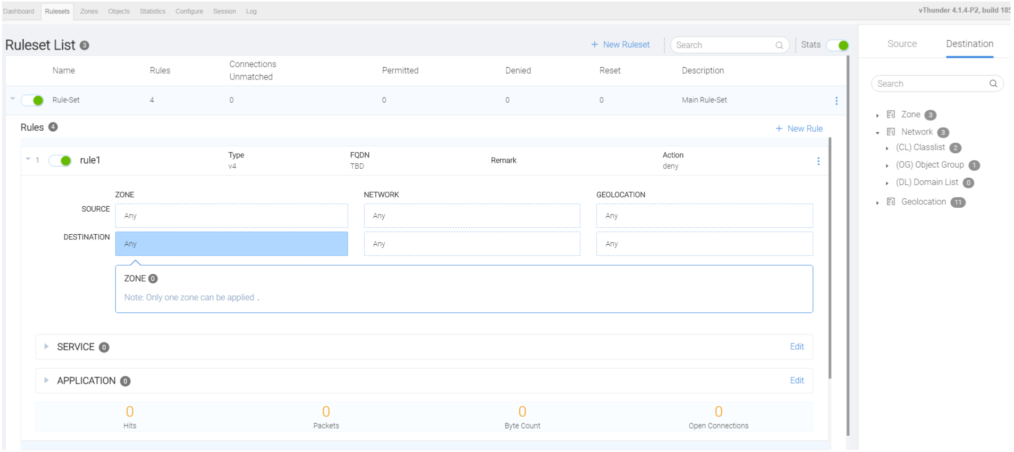
GUI Configuration: Geo-Location Filtering at Firewall

You must first create a Geo-list and then bind the Geo-list to a rule destination. To create and manage a Geo-list, see “Geo-Location Mappings” under *System Administrators Guide*.

To bind the Geo-list to rule destination, perform the following:

1. Navigate to the **Security > Firewall > Ruleset** page.
2. Click **+New Ruleset** to create new rule set or **Edit** list to add rules, set zone, destination.
3. Enter geo-list name in the **Geolocation** field to bind the geo-location to the rule destination.
4. Save the configuration.

Figure 10 : Ruleset List page



Ruleset List 3

Name	Rules	Connections Unmatched	Permitted	Denied	Reset	Description
Rule-Set	4	0	0	0	0	Main Rule-Set

Rules 4

	Type	FQDN	Remark	Action
1 rule1	v4	TBD		deny

	ZONE	NETWORK	GEOLOCATION
SOURCE	Any	Any	Any
DESTINATION	Any	Any	Any

ZONE 0

Note: Only one zone can be applied .

SERVICE 0

APPLICATION 0

Hits	Packets	Byte Count	Open Connections
0	0	0	0

FQDN-Based Filtering

FQDN integration with firewall rules allows an administrator to define firewall rules that use the domain-name instead of using a specific IP address to identify a server/destination host. This is supported only for destination IP based filter in the firewall rule and its useful for the cases where the IP address of the server keeps changing due to being hosted on AWS or similar environments.

The domain can be specified as a single entity or as a domain-list and bound as a destination IP/domain filter in the firewall rule-set. Once an FQDN is configured, a DNS lookup can be initiated to resolve the IP corresponding to it. The IPs can be added to the firewall rule for the destination match. The domain-list supports the IPv6 and the configuration for periodic update. Hit count must be activated for the particular domain list. Setup DNS cache and configure different DNS servers on different partitions. If there is no configuration of DNS server on the virtual partition use the DNS server at shared partition.

NOTE: Only the IPs that have the same IP-version (IPv4 or IPv6) with a firewall rule can be associated with the firewall rule. The other type of IPs will be ignored. When an IP address is added or deleted by the user at DNS server, the DNS cache is updated during periodic refresh. The domain list is also updated. FQDN filtering can be configured on both Gi-Firewall (CGN) and Data Center Firewall (SLB).

Implementation Example: FQDN Filtering Configuration

1. Configure the IP address of DNS Server for virtual partition to resolve the FQDN.

   ```
   !
   ip dns primary 10.1.1.3
           !
   ```

   If there is no IP address of DNS server at Layer 3 virtual partition, use the IP address of DNS server at shared partition.

2. Configure the FQDN string at domain-list:

   ```
   !
   domain-list domain1
     www.domain1.com interval 1
     www.domaintest.com
   !
   ```

   The domain-list configuration is now as follows:

   ```
   ACOS[slb](config)# show running-config domain-list
   !Section configuration: 66 bytes
   !
   domain-list domain1
       www.domain1.com interval 1
           www.domaintest.com
   ```

3. The IP DNS cache at ACOS is now layer 3 virtual partition aware. Verify the IP entries received from the DNS server:

   ```
    ACOS[slb]# show ip dns-cache
   The items of domain and IP in cache
   FQDN            IP                  TTL      query-interval
   -----------------------------------------------------------
   www.domain1.com    69.172.200.235      1348     600
   www.domaintest.com       172.16.1.3        6990        60
   www.domaintest.com       10.1.1.3          6990        60
   www.domaintest.com       2017::3          6990        60
   ```

4. The domain list and IP addresses in cache are updated during periodic refresh by the timeout of DNS TTL or query-interval; to perform this manually, please use the command
   "`clear ip dns-cache`". The DNS entries are refreshed immediately,

```
ACOS[slb]# clear ip dns-cache
```

5. Check the IP address at domain-list; the IP address is updated from the DNS-cache to domain-list

```
   ACOS[slb]# show domain-list domain1
domain-list domain1
     www.domain1.com     hitcount:0
       number of IPv4 Ips:1
        69.172.200.235
       number of IPv6 Ips:0
     www.domaintest.com     hitcount:0
       number of IPv4 Ips:2
         10.1.1.3
         172.16.1.3
       number of IPv6 Ips:1
         2017::3
```

6. Configure the domain-list to firewall rule set as destination filter. Only IPv4 addresses of the domain-list are used in this rule.

```
  !
rule-set domain1
  rule v4
    action permit
    source ipv4-address any
    source zone any
    dest ipv4-address 10.1.1.5/32
    dest domain-list domain1
dest zone any
    service any
  rule v6
    action permit
    ip-version v6
    source ipv6-address any
    source zone any
```

Only IPv6 addresses of domain-list are used in this rule

```
    dest domain-list domain1
    dest zone any
    service any
!
fw active-rule-set domain1
```

7. To check if the FQDN was matched by the traffic at firewall rule, enable the hit-count using the **`system hit-count enable`** command:

```
   !
system domain-list-hitcount-enable
!
```

8. This configuration is layer-3 virtual partition aware; and the counter is aware for a DNS domain, because the IP addresses of FQDN is dynamic. You can see the counter value through "`show domain-list`".

```
ACOS[slb]# show domain-list domain1
domain-list domain1
     www.domaintest.com     hitcount:1
       number of IPv4 Ips:1
        69.172.200.235
       number of IPv6 Ips:0
     www.domaintest.com     hitcount:5
       number of IPv4 Ips:2
         10.1.1.3
         172.16.1.3
       number of IPv6 Ips:1
         2017::3
```

9. The feature of FQDN Filtering can function both at Data center Firewall and Gi Firewall.

GUI Configuration: FQDN Filtering at Firewall

The ACOS GUI now provides the following options, which are related to FQDN filtering at the Firewall setup:

1. Create and/or manage a domain-list.
2. Add a new domain list.
3. Bind the domain-list to a rule destination.
4. Operate the DNS cache for FQDN setup.

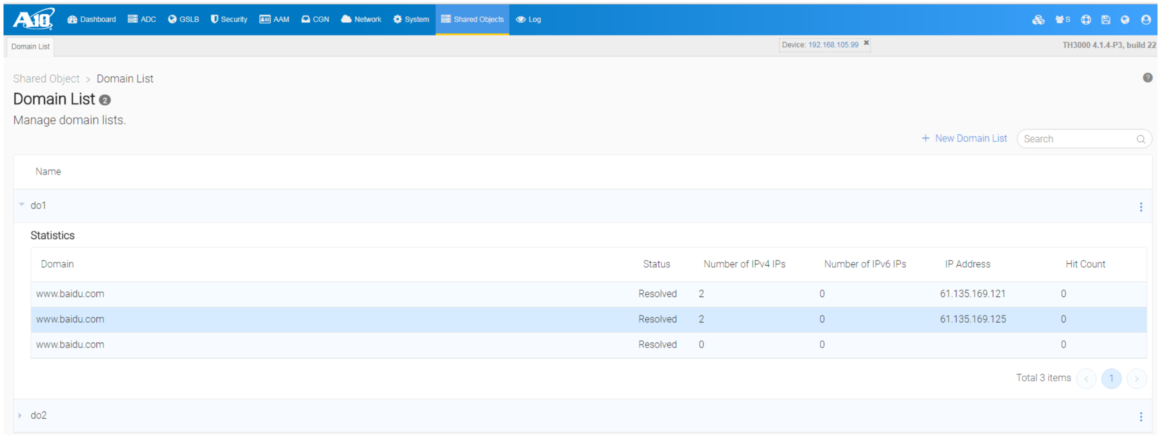
This section below provides details on the GUI screens used to configure FQDN Filtering at the firewall.

Domain List Page

The **Shared Objects > Domain List** page:

- Lists all domain-list items, and filter the items by name keywords as follows:
  - Lists the top 25 domain-list items
  - Filters the domain-list items by name keywords
  - Provides option to delete the selected domain-list items
- Provides options to create a new domain list, or edit a domain list
- Display statistics information of selected configured domain list and filter the statistics information by status.

Figure 11 : Shared Objects: Domain List



Domain	Status	Number of IPv4 IPs	Number of IPv6 IPs	IP Address	Hit Count
www.baidu.com	Resolved	2	0	61.135.169.121	0
www.baidu.com	Resolved	2	0	61.135.169.125	0
www.baidu.com	Resolved	0	0		0

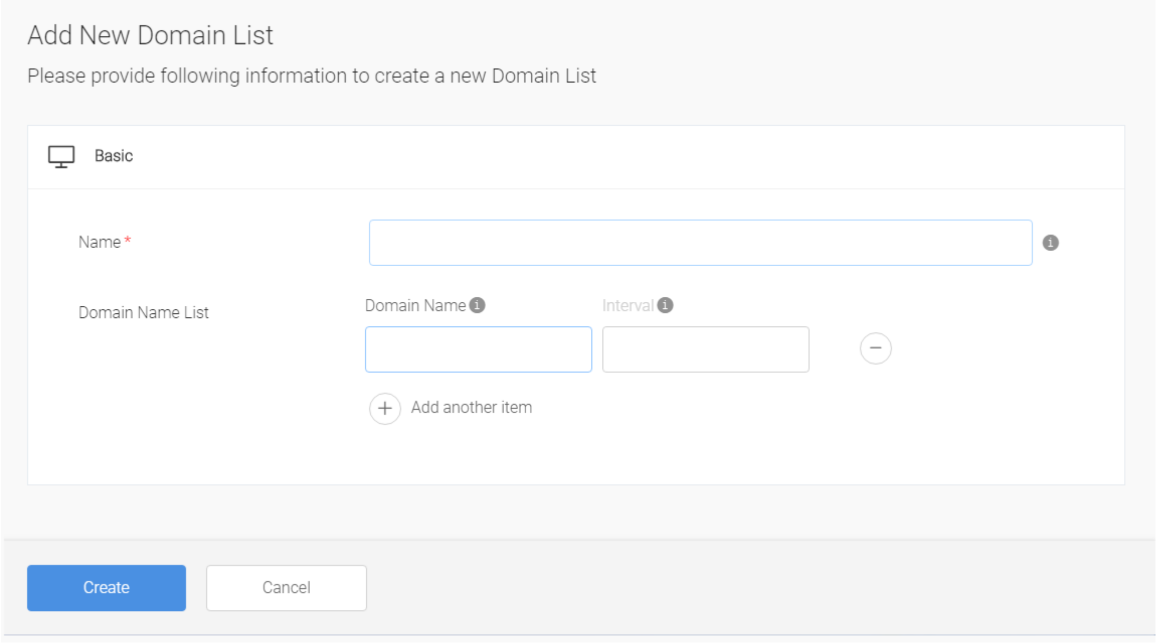
Add New Domain List

To create a new domain list:

1. Navigate to the **Shared Objects > Domain List** page.
2. Click **+New Domain List** option.
3. The **Add New Domain List** page opens up.
4. Provide a name for the new **Domain List.**

5. Add the **Domain Names** to the list and the (DNS query) **Interval.**
6. Click **Create.**

Figure 12 : Add New Domain List

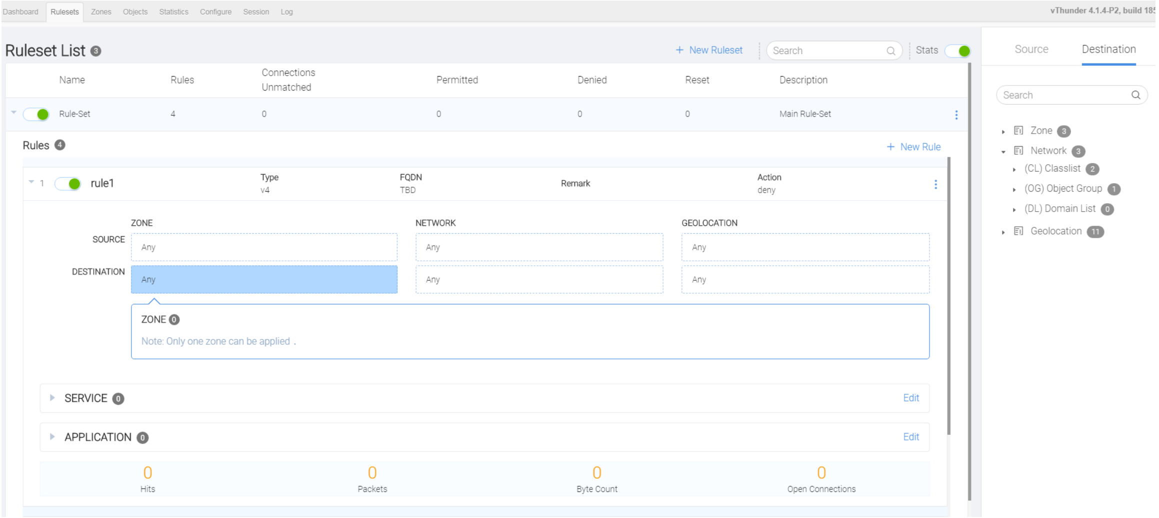


Bind Domain List to Rule Destination: Ruleset List Page

To bind the domain list to rule destination:

1. Navigate to the **Security > Firewall > Rulesets** page.
2. Click **+New Ruleset** to create new ruleset or **Edit** list to add rules, set zone, destination,
3. Enter the domain list name in the **Destination Domain List** field to bind the domain list to the rule destination.
4. Save the configuration.

Figure 13 : Ruleset List Page



Name	Rules	Connections Unmatched	Permitted	Denied	Reset	Description
Rule-Set	4	0	0	0	0	Main Rule-Set

	Type	FQDN	Remark	Action
1 rule1	v4	TBD		deny

	ZONE	NETWORK	GEOLOCATION
SOURCE	Any	Any	Any
DESTINATION	Any	Any	Any

Note: Only one zone can be applied .

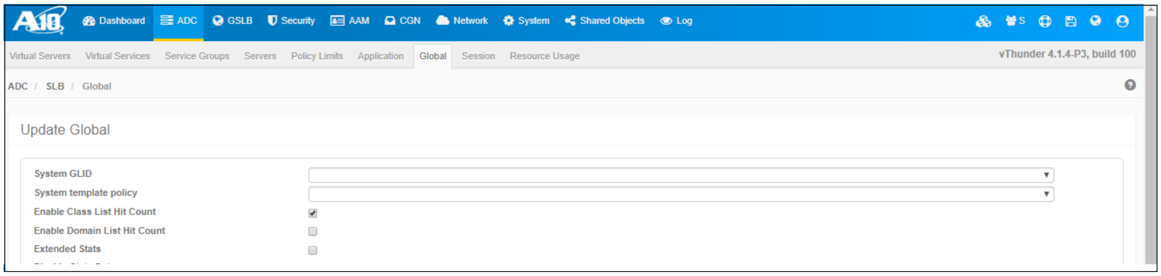
Hits	Packets	Byte Count	Open Connections
0	0	0	0

Enable or Disable Domain Hit Count: SLB Global Page

To enable Domain Hit Count for the Domain List:

1. Navigate to **ADC > SLB > Global** page.
2. Select or de-select the option **Enable Domain List Hit Count**.
3. Click **Update**.

Figure 14 : Enable/Disable Domain Hit Count: SLB Global Page



Update Global

System GLID	▾
System template policy	▾
Enable Class List Hit Count	☑
Enable Domain List Hit Count	☐
Extended Stats	☐

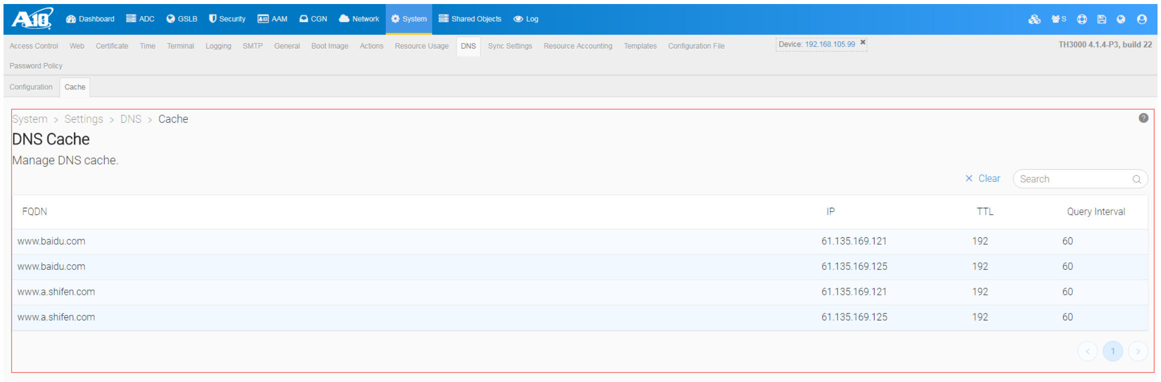
DNS Cache Page

Manage the DNS cache information through the **System > Settings > DNS > Cache** page.

This page provides the following options:

- Displays the DNS cache list.
- Filter the DNS cache list by name keywords.
- Reset the DNS cache of selected FQDN.

Figure 15 : DNS Cache Page



Device: 192.168.105.99

TH3000 4.1.4-P3, build 22

System > Settings > DNS > Cache

DNS Cache

Manage DNS cache.

FQDN	IP	TTL	Query Interval
www.baidu.com	61.135.169.121	192	60
www.baidu.com	61.135.169.125	192	60
www.a.shifen.com	61.135.169.121	192	60
www.a.shifen.com	61.135.169.125	192	60

DS-Lite Traffic Processing Support

The Firewall supports Dual-Stack Lite (DS-Lite) traffic processing. DS-Lite is a Network Address Translation (NAT) feature that enables the ACOS device to act as an endpoint for IPv4 traffic tunneled through an IPv6 link.

To process DS-Lite traffic, you must configure the firewall rule to inspect the outer IPv6 header first. After it matches the rule, the encapsulated IPv4 payload is inspected against another rule to determine the final action to be taken on the DS-Lite packet.

This decapsulated DS-Lite traffic can also go through a Threat list look-up. If the decapsulated IP address matches the IP addresses listed on the threat list, ACOS drops the traffic and prevents the subscriber from connecting to a malware IP address. However, in the case of DS-Lite traffic, the threat list must be composed of IPv4 addresses. For more information on Threat lists, refer to IP Threat List.

This section describes the configurations related to DS-Lite traffic processing.

The following topics are covered:

Configuring Firewall Rule for DS-Lite Traffic

To process the DS-Lite traffic, you must configure a firewall rule-set with specific commands. For example, in the following configuration, the rule-set **test** contains two rules, **outer-v6** and **inner-v4**.

The **outer-v6** rule is explicitly configured to inspect and match the outer IPv6 header of the DS-Lite traffic. When the rule matches, the encapsulated IPv4 payload is inspected against the **inner-v4** rule to determine the final action to be taken on the DS-Lite packet.

```
rule-set testrule inner-v4
  source ipv4-address any
  source zone any
  dest ipv4-address any
  dest zone any
  service any
  application protocol http
  action-group
    permit log
    permit limit-policy 123
rule outer-v6
  ip-version v6
  action permit cgnv6 ds-lite lsn-lid 2 inspect-payload
  source ipv6-address any
  source zone any
  dest ipv6-address any
  dest zone any
  service any
  application any
!
```

NOTE: The CGN traffic works only when the rule to inspect the IPv6 header is specifically configured to **permit** CGN in its action.

Configuring Rate Limiting for DS-Lite Traffic

Rate limiting helps to limit the incoming DS-Lite traffic from certain application protocols and categories. It is applied after the application is classified.

Rate limiting can be applied at a rule level using template policies for the encapsulated payload (IPv4) only. The following example demonstrates the same.

Consider the configuration below that contains the rule-set for DS-Lite traffic processing. The rule **inner-v4** (that inspects the encapsulated payload (IPv4)) contains the template policy (**limit 123**) to configure rate-limiting.

```
!
class-list list1
  ::/0 lsn-lid 2
!
vlan 10
  tagged ethernet 1
  router-interface ve 10
!
vlan 20
  tagged ethernet 2
  router-interface ve 20
!
interface ve 10
  ip address 10.10.10.40 255.255.0.0
  ip client
  ip nat inside
  ipv6 address 3ff3::148/64
  ipv6 nat inside
!
interface ve 20
  ip address 20.20.20.40 255.255.255.0
  ip server
  ip nat outside
!
interface ve 21
  ip address 21.21.21.40 255.255.255.0
!
cgnv6 nat pool dslite0 20.20.20.60 20.20.20.60 netmask /24
!
```

```
cgnv6 lsn-lid 2
  source-nat-pool dslite0
!
cgnv6 ds-lite inside source class-list list1
!
rule-set test
  rule inner-v4
  source ipv4-address any
  source zone any
  dest ipv4-address any
  dest zone any
  service any
  application protocol http
  action-group
    permit log
    permit limit-policy 123
rule outer-v6
  ip-version v6
  action permit cgnv6 ds-lite lsn-lid 2 inspect-payload
  source ipv6-address any
  source zone any
  dest ipv6-address any
  dest zone any
  service any
  application any
!
fw active-rule-set test
```

Rate limiting can be set by configuring the template policy for any of the following parameters:

- **Packets-Per-Second** - To configure the packets-per-second rate limit on the uplink, downlink, and the total DS-Lite traffic:

  ```
  template limit-policy 123
    limit-pps uplink 5
    limit-pps downlink 5
    limit-pps total 5
  ```

- **Throughput** - To set the throughput rate limit on the uplink, downlink, and the total DS-Lite traffic:

```
template limit-policy 123
  limit-throughput uplink 1
  limit-throughput downlink 1
  limit-throughput total 1
```

- **Connections Per Second** - To set the maximum number of connections per second limit:

```
template limit-policy 123
  limit-cps 50
```

- **Concurrent Sessions** - To configure the maximum number of connections per second allowed on a subscriber IP:

```
template limit-policy 123
  limit-concurrent-sessions 10
```

You can execute the **`show rate-limit`** command to view the **`rate-limit entries`** created, and also check if the packets are dropped when the configured rate-limit exceeds.

Configuring Logging for DS Lite Traffic

Firewall logging is an optional action. However, it can be configured to generate permit/deny for the DS-Lite traffic by applying the action to the IPv4 rule.

Follow the steps to configure firewall logging while processing DS-Lite traffic:

1. Configure the firewall rule-set to process DS-Lite traffic:

```
rule-set test
  rule inner-v4
  source ipv4-address any
  source zone any
  dest ipv4-address any
  dest zone any
  service any
  application protocol http
  action-group
    permit log
    permit limit-policy 123
rule outer-v6
  ip-version v6
  action permit cgnv6 ds-lite lsn-lid 2 inspect-payload
  source ipv6-address any
  source zone any
  dest ipv6-address any
  dest zone any
  service any
  application any
!
```

2. Configure the firewall server:

```
fw server syslog1 21.21.21.10
  port 514 udp
  health-check-disable
!
```

3. Configure the firewall service group:

```
fw service-group syslog-sg udp
  member syslog1 514
!
```

4. Configure the firewall logging template:

```
fw template logging fw-log
  log http-requests url
  include-http l4-session-info
  include-http method
  service-group syslog-sg
!
```

   By default, the messages are logged in the Common Event Format (CEF). To change the format to ASCII, use the following command:

```
fw template logging fw-log
  format ascii
!
```

5. Bind the firewall logging template globally:

```
fw logging fw-log
```

```
!
```

6. Activate the rue-set:

```
fw active-rule-set test
```

Example log in CEF format:

```
<134> Sep 24 17:58:06 vThunder-1  CEF:0|A10|CFW|5.3.0-d|FW 100|Session
opened|1|proto=TCP act=Permit rt=227759 app=google_gen c6a2=3FF3::1
src=10.10.10.10 spt=42451 c6a3=3FF3::148 dst=20.20.20.10 dpt=80
deviceInboundInterface=ve10 deviceOutboundInterface=ve20 cs1=test2 cs2=v4
cs7=web, web-ext-software cs1Label=Rule Set Name cs2Label=Rule Name
cs7Label=Application Category
```

Example log in ASCII format:

```
<134> Sep 24 18:10:49 vThunder-1 FW-TCP-G: [3ff3::1]10.10.10.10:36875<-->
[3ff3::148]20.20.20.10:80 ACT=PERMIT RT=418716 APP=google_gen IN-INTF=ve10
OUT-INTF=ve20 POLICY=test2 RULE=v4 APP-CAT=web, web-ext-software
```

Configuring NetFlow/IPFIX

An ACOS device can act as a NetFlow exporter that monitors traffic and sends the data to one or more NetFlow collectors, where the information can be stored and analysed by a network administrator.

The following section shows a NetFlow configuration example for DS-Lite traffic. Refer to the **NetFlow v9 and v10 (IPFIX)** section in the *Traffic Logging Guide* for NetFlow parameter description.

NOTE: This example only demonstrates the steps to configure the NetFlow template and monitor. The rest of the configuration is the same as described in Configuring Logging for DS Lite Traffic

Configuring the NetFlow Template

The following commands configure a NetFlow template named **ipfix-custom**:

```
netflow template ipfix-custom
```

```
  information-element application-id
  information-element cgn-flow-direction
  information-element rule-name
  information-element application-name
  template-id 2011
!
```

Configuring the NetFlow Monitor

The following commands configure the NetFlow monitor that implements the template:

```
netflow monitor nf1
  protocol v10
  record sesn-event-dslite both
  record sesn-event-fw4 both
  record sesn-event-fw6 both
  custom-record sesn-event-dslite-deletion template ipfix-custom
  destination 21.21.21.10
!
```

Threat Intelligence

This section describes how to configure threat intelligence.

The following topics are covered:

Overview

The Threat Intelligence module (or Threat Intel for short) provides data about malicious IP addresses in the internet. This information is dynamically retrieved from 3rd-party partners, and it can be used to block traffic flowing to malicious IPs.

The threat-intel module (available as a CFW add-on licensed capability) uses Webroot's IP reputation data.

About 2 million malicious IP addresses have been identified and included in Webroot's database. The list of IPs is updated multiple times throughout the day. Malicious IP addresses can change over time, so therefore this information is updated regularly in the form of Real Time Updates (RTU) and daily updates which are obtained from the Webroot servers hosted on the internet.

The IP addresses are categorized into the following threat categories:

1. Spam Sources
2. Windows Exploits
3. Web Attacks
4. BotNets
5. Scanners
6. Denial of Service
7. Reputation
8. Phishing
9. Proxy
10. Network
11. Cloud Providers
12. Mobile Threats
13. Tor Proxy

Licensing

A license needs to be installed through A10's Global License Manager (GLM) in order to use the threat-intel capability. The A10 Thunder device needs to be connected to the internet in order to periodically validate the license and obtain daily threat IP address updates.

To obtain a license, follow these steps:

1. Obtain a Webroot TI license in your GLM account or obtain from a sales representative.
2. Switch to the Activations tab on the license page, and then enter the host id of the device. The host id can be obtained using **`show license`** command.

Configure the device to retrieve the license information, as follows:

1. Configure a valid DNS server:

```
ACOS(config)# ip dns primary 192.168.1.100
```

2. Configure a route to the internet if one is not already present. The device must be able to access the internet via the management or data interface. The example below uses the data interface:

```
ip route 0.0.0.0 /0 192.168.200.1
```

3. Configure the command **`glm enable-requests`** to trigger requests to GLM to fetch license information. If the device is connected through the management interface, then run the CLI command **`glm use-mgmt-port`** first.

```
ACOS(config)# glm use-mgmt-port
ACOS(config)# glm enable-requests
WEBROOT_TI License successfully updated, please log out and log back in
to access license features
```

If communication with the GLM server is successful, then verify the license status using the command `show license-info`:

```
ACOS(config)# show license-info
Host ID          : 8530D1AA5F3FBCD965E5F910EC448E5E3A5A8F8E
USB ID           : Not Available
```

```
Billing Serials: vTh7fd3305890000, vThc5b0f1f1e0000
Token          : Not Available
Product        : CFW
Platform       : Thunder Series Advanced Traffic Manager
GLM Ping Interval in Hours: 24
-----------------------------------------------------------------------
-------------
Enabled Licenses          Expiry Date (UTC)                Notes
-----------------------------------------------------------------------
-------------
SLB                       None
CGN                       None
GSLB                      None
RC                        None
DAF                       None
WAF                       None
SSLI                      None
DCFW                      None
GIFW                      None
URLF                      None
IPSEC                     None
AAM                       None
FP                        None
WEBROOT                   N/A              Requires an additional
Webroot license.
THREATSTOP                N/A              Requires an additional
ThreatSTOP license.
QOSMOS                    N/A                 Requires an additional
Qosmos license.
WEBROOT_TI               16-July-2018
```

A Webroot TI License is associated with the Host ID highlighted above.

4. The device now has up-to-date license information and the feature is ready to use. If there is an error, run the **show log** command to obtain more information about possible causes of failure. For example:

```
ACOS(config)# show log
```

```
Feb 26 2018 11:34:21 Error       [SCM]:CURL: Error while making
requests HTTP CODE : 0 ERROR: Couldn't resolve host
'glm.a10networks.com'.
```

Resolve the issue indicated by the error log. Use the **glm send license-request** command to trigger another request to the GLM server to retrieve the license.

```
ACOS(config)# ip dns primary 192.168.1.110
ACOS(config)# glm send license-request
WEBROOT_TI License successfully updated, please log out and log back in
to access license features
```

Configuration

Configuration for this feature is controlled using the threat-intel module. Before configuring the threat-intel feature, verify that a DNS server is configured and available and verify that the ACOS device is connected to the internet.

1. Configure the threat-feed to use Webroot.

```
ACOS(config)# threat-intel
ACOS(config-threat-intel)# threat-feed webroot
```

2. If the device is connected to the internet through the management interface, configure **use-mgmt-port** before executing the **enable** command. If the device is connected to the internet through the data interface, then you can skip this step.

```
ACOS(config-threat-intel-threat-feed:webr...)# use-mgmt-port
```

3. Enable the threat-intel service feed.

```
ACOS(config-threat-intel-threat-feed:webr...)# enable
```

Other configuration options include the following:

- server-timeout: Sets a timeout for reaching Webroot servers. ACOS forfeits the connection attempt if a server is not reachable after expiry of the server-timeout time.
- update-interval: Check for any database or RTU updates based on this interval.
- rtu-update-disable: Disables RTU updates. Database updates will still occur.
- log-level: Controls the level of logs as follows:

```
ACOS(config-threat-intel-threat-feed:webr...)# log-level ?
  disable  Disable all logging
  error    Log error events
  warning  Log warning events and above
  info     Log info events and above
  debug    Log debug events and above
  trace    enable all logs
```

- server: Webroot servers (Do not change unless directed by A10 Technical Support)
- port: Port to contact Webroot servers (Do not change unless directed by A10 Technical Support)

NOTE: Users should not alter server and port values unless instructed to by A10 Technical Support.

Proxy Server Support

This section is for customers who might have strict rules for outbound traffic being inspected by a proxy server or firewall.

There could be some deployments where the customers might want all outbound traffic to be inspected by a firewall or proxy server. This could be a problem for threat-intel module because Webroot's servers are hosted on AWS which means their IP addresses are subject to change. Also, RTU updates are hosted on random AWS instances which means the hostnames are also subject to change. This makes it difficult to configure outbound rules if the servers are changing.

To counter this threat-intel module has the capability of reaching Webroot's servers through an intermediate proxy server. Proxy authentication is also supported. Currently, basic and NTLMv2 are supported.

- **proxy-host:** IP or hostname of proxy server.
- **proxy-port:** Port of proxy server. All communication is through HTTPs. So, proxy port should be configured accordingly.
- **proxy-auth-type:** If proxy authentication is desired, this setting can be changed between basic and NTLMv2. Default is NTLMv2.
- **proxy-username:** Username for proxy authentication.
- **proxy-password:** Password for proxy authentication.

Proxy server will be used if both proxy-host and proxy-port are configured.

Similarly, proxy authentication will be performed if both proxy-username and proxy-password are configured.

Delete Threat-Intel Database

This command will delete the current copy of the database.

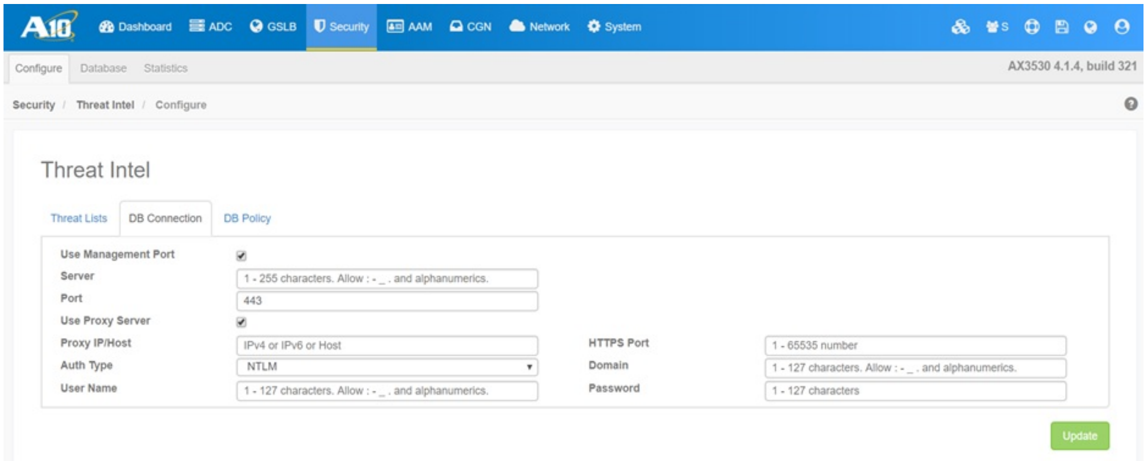
```
ACOS(config)# delete web-category database
```

NOTE: This command can only be executed if the threat-intel module is not enabled. A fresh copy of the database will be downloaded the next time the module is enabled.

Using the GUI:

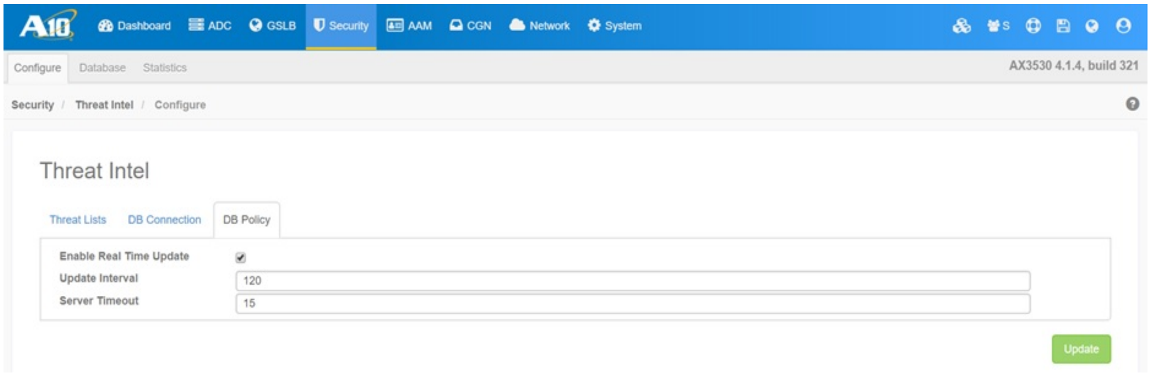
To use the GUI to configure threat-intel, navigate as follows: **Security > Threat-Intel > Configure**

Figure 16 : Security > Threat-Intel > Configure: DB Connection



Use Management Port	☑		
Server	1 - 255 characters. Allow : - _ . and alphanumerics.		
Port	443		
Use Proxy Server	☑		
Proxy IP/Host	IPv4 or IPv6 or Host	HTTPS Port	1 - 65535 number
Auth Type	NTLM ▾	Domain	1 - 127 characters. Allow : - _ . and alphanumerics.
User Name	1 - 127 characters. Allow : - _ . and alphanumerics.	Password	1 - 127 characters

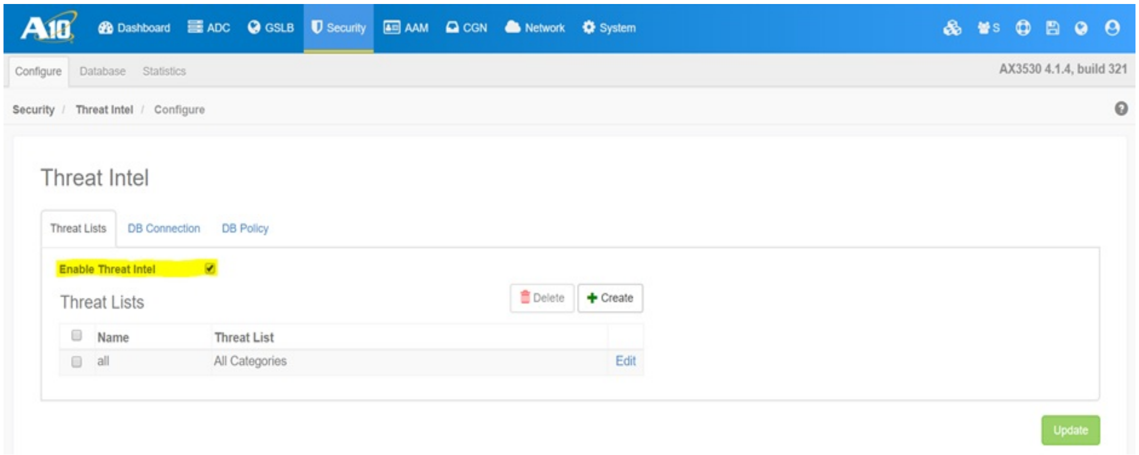
Figure 17 : Security > Threat-Intel > Configure: DB Policy



Enable Real Time Update ☑
Update Interval 120
Server Timeout 15

Select the “Enable Threat Intel” checkbox to enable this feature, and then click **Update**.

Figure 18 : Enabling threat-intel



Enable Threat Intel ☑

Threat Lists

□	Name	Threat List	
□	all	All Categories	Edit

Verifying Installation

The threat-intel module is enabled in an asynchronous manner. Once the **`enable`** command is executed, background processes are invoked to bring up the module. Even though the command returns success, it might not necessarily mean module is enabled correctly.

Various debug commands are available to verify that the threat-intel module has been enabled correctly. After the **`enable`** command has been executed, run the **`show threat-intel database webroot`** command and check the output.

```
ACOS(config)# show threat-intel database webroot
Database Name                   : wr_ip_All_1_1479.txt
Database Status                 : Active
Database Size                   : 24 MB
Database Version                : 1479
Last Update Time                : Mon Feb 26 11:28:47 2018
Next Update Time                : Mon Feb 26 13:28:42 2018
Connection Status               : GOOD
Last Successful Connection      : Mon Feb 26 11:28:53 2018

Entries loaded per threat category
spam-sources                    : 444059
windows-exploits                : 107362
web-attacks                     : 1684
botnets                         : 184306
scanners                        : 136516
dos-attacks                     : 0
reputation                      : 0
phishing                        : 78161
proxy                           : 386170
mobile-threats                  : 2019
tor-proxy                       : 925
all-categories                  : 1266571
```

The Database Status provides information about whether the module is ready to use. Possible values for this field include:

- **Inactive:** No database is loaded in memory. Threat-intel cannot be used in this state.
- **Downloading:** A database is currently being downloaded.
- **Processing:** Database file is being processed, saving to a file, checksum calculations, etc.
- **Loading into memory:** Database is being loaded into memory.
- **Active:** Database is loaded and threat-intel module is ready to process traffic.

After the **enable** command is used, if the database status is inactive, check the **show log** output for any possible reasons for failure. You can also check the threat-intel log for more details:

```
ACOS(config)# show threat-intel log webroot
```

```
2018-02-16 15:40:41 ERROR: Cannot resolve host api.bcti.brightcloud.com:
Temporary failure in name resolution
2018-02-16 15:40:41 ERROR: IpUpdateTask: OnError!
```

ACOS can change log-level for more detailed logs. By default only error logs are shown.

Once errors are resolved, execute the **no enable** and **enable** commands to trigger another attempt at enabling the module.

Using Threat-List in Firewall

The threat-intel module can be used with a firewall rule-set to block traffic to or from malicious IP addresses.

To use the threat-intel module with the firewall:

1. Configure a threat-list, or group of some or all threat-categories.

```
ACOS(config-threat-intel)# threat-list BAD_IPs webroot
ACOS(config-threat-intel-threat-list:test)#?
  all-categories    Enable all categories
  botnets           Botnet C&C channels, and infected zombie machines
controlled by
                    Bot master
  dos-attacks       IPs participating in DOS, DDOS, anomalous sync
flood, and anomalous
                    traffic detection
  mobile-threats    IPs associated with mobile threats
  phishing          IP addresses hosting phishing sites, ad click fraud
or gaming fraud
  proxy             IP addresses providing proxy services
  reputation        IP addresses currently known to be infected with
malware
  scanners          IPs associated with probes, host scan, domain scan,
and password
                    brute force attack
  spam-sources      IPs tunneling spam messages through a proxy,
anomalous SMTP
                    activities, and forum spam activities
  tor-proxy          IPs providing tor proxy services
  web-attacks        IPs associated with cross site scripting, iFrame
injection, SQL
                     injection, cross domain injection, or domain
password brute force
  windows-exploits  IPs associated with malware, shell code, rootkits,
worms or viruses
```

In the example below, botnets and phishing threat categories are added to threat-list SOME_BAD_IPs.

```
ACOS(config-threat-intel-threat-list:test)# show run threat-intel
!Section configuration: 170 bytes
threat-intel
  threat-feed webroot
    use-mgmt-port
    enable
  threat-list SOME_BAD_IPs webroot
    botnets
    phishing
```

Alternatively, users can also configure all-categories to include all threat categories.

```
ACOS(config-threat-intel-threat-list:test)# show run threat-intel
!Section configuration: 170 bytes
threat-intel
  threat-feed webroot
    use-mgmt-port
    enable
  threat-list ALL_BAD_IPs webroot
    all-categories
  threat-list BAD_IPs webroot
    botnets
    phishing
```

2. Once a threat-list is configured, it can be used in a firewall rule as shown below:

```
ACOS(config)# show run rule-set
!Section configuration: 597 bytes
!
rule-set my_fw_ruleset
```

```
  rule block_to_malicious
    action deny
    source ipv4-address any
    source zone any
    dest ipv4-address any
    dest zone any
dest threat-list ALL_BAD_IPs
    service any
    application any
  rule block_from_malicious
    action deny
    source ipv4-address any
    source zone any
    source threat-list ALL_BAD_IPs
    dest ipv4-address any
    dest zone any
    service any
    application any
  rule permit_everything_else
    action permit
    source ipv4-address any
    source zone any
    dest ipv4-address any
    dest zone any
    service any
    application any
```

```
ACOS(config)# fw active-rule-set my_fw_ruleset
```

Threat-Intel information is also added to the logs to track malicious traffic. The following fields are added to the Syslog, ACOS event log, and Application Aware Firewall local log to indicate threat-list and threat-category:

- Source Threat List: This field indicates the threat-list name configured for source criteria.
- Destination Threat List: This field indicates the threat-list name configured for destination criteria.
- Source Threat Category: This field indicates the threat-category that matches the source IP.

- Destination Threat Category: This field indicates the threat-category that matches the destination IP.

Debug and Statistics

The following section shows how to check the module status and diagnose problems.

1. Database and module status:

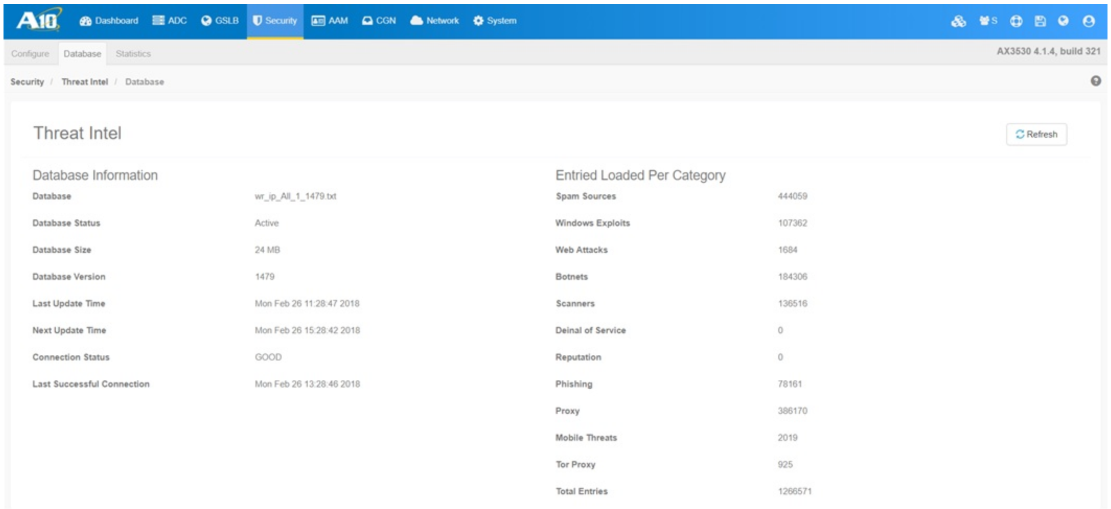
```
ACOS(config)# show threat-intel database webroot
Database Name                   : wr_ip_All_1_1479.txt
Database Status                 : Active
Database Size                   : 24 MB
Database Version                : 1479
Last Update Time                : Mon Feb 26 11:28:47 2018
Next Update Time                : Mon Feb 26 15:28:42 2018
Connection Status               : GOOD
Last Successful Connection      : Mon Feb 26 13:28:46 2018

Entries loaded per threat category
spam-sources                    : 444059
windows-exploits                : 107362
web-attacks                     : 1684
botnets                         : 184306
scanners                        : 136516
dos-attacks                     : 0
reputation                      : 0
phishing                        : 78161
proxy                           : 386170
mobile-threats                  : 2019
tor-proxy                       : 925
all-categories                  : 1266571
```

   If there's any failure, a field with the failure reason will appear (not shown in the example output). Entries loaded per threat category provide information about the number of malicious IPs categorized under each threat-category. The “all-categories” is the total number of entries loaded. This information varies based on which database is loaded.

   To configure from the GUI, navigate as follows:

Security > Threat-Intel > Database tab:

Figure 19 : Security >> Threat-Intel >> Database tab



Threat Intel

Database Information	
Database	wr_ip_All_1_1479.txt
Database Status	Active
Database Size	24 MB
Database Version	1479
Last Update Time	Mon Feb 26 11:28:47 2018
Next Update Time	Mon Feb 26 15:28:42 2018
Connection Status	GOOD
Last Successful Connection	Mon Feb 26 13:28:46 2018

Entried Loaded Per Category	
Spam Sources	444059
Windows Exploits	107362
Web Attacks	1684
Botnets	184306
Scanners	136516
Deinal of Service	0
Reputation	0
Phishing	78161
Proxy	386170
Mobile Threats	2019
Tor Proxy	925
Total Entries	1266571

2. Use the following command to determine the threat category for a particular IP:

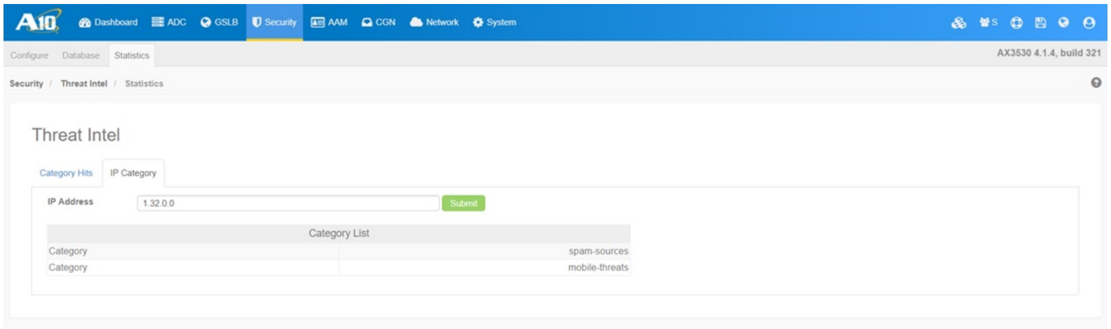
```
ACOS(config)# show threat-intel ip-category 8.8.8.8 webroot
Not a threat
ACOS(config)# show threat-intel ip-category 1.32.0.0 webroot
spam-sources
mobile-threats
```

NOTE: The command above works only if threat-intel module is enabled and the database status is active.

To configure from the GUI, navigate as follows:

Security > Threat-Intel > Statistics > IP Category:

Figure 20 : Security > Threat-Intel > Statistics > IP Category



IP Address 1.32.0.0

Category List	
Category	spam-sources
Category	mobile-threats

3. Global Counters:

To view the hit counters for each threat-category, use the following show command:

```
ACOS(config)# show threat-intel hits webroot
spam-sources                    : 1
windows-exploits                : 0
web-attacks                     : 0
botnets                         : 0
scanners                        : 0
dos-attacks                     : 0
reputation                      : 0
phishing                        : 0
proxy                           : 0
mobile-threats                  : 1
tor-proxy                       : 0
Total Lookups in Database       : 1
Total Lookups in RTU cache      : 0
Non malicious IP Lookups        : 15
```

OR

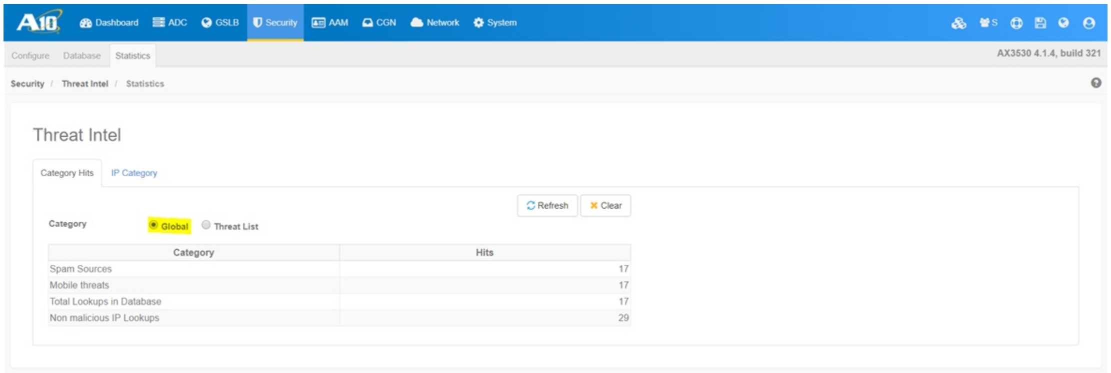
To view the global counters, use the following show command:

```
ACOS# show counters threat-intel webroot-global
Hits for spam sources                                  24
Hits for windows exploits                              0
Hits for web attacks                                   0
Hits for botnets                                       0
Hits for scanners                                      0
Hits for dos attacks                              0
Hits for reputation                               0
Hits for phishing                                 0
Hits for proxy                                    0
Hits for mobile threats                           0
Hits for tor-proxy                                0
Number of lookups in RTU cache                    0
Number of lookups in database                     24
IP's not found in database or RTU cache           7643
```

To configure from the GUI, navigate as follows:

Security > Threat-Intel > Statistics > Category Hits > Global

Figure 21 : Security > Threat-Intel > Statistics > Category Hits > Global



Threat Intel

Category ● Global ○ Threat List

Category	Hits
Spam Sources	17
Mobile threats	17
Total Lookups in Database	17
Non malicious IP Lookups	29

4. Per threat-list counters:

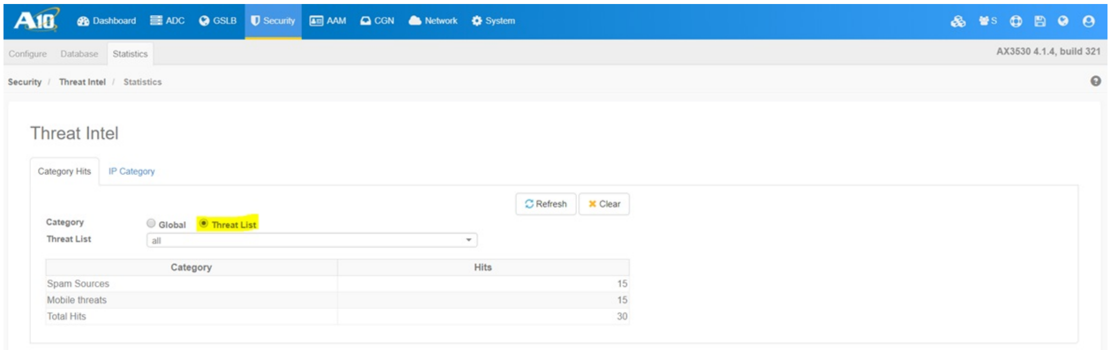
   To view the counters for a particular threat-list, use the following command:

```
ACOS# show counters threat-intel threat-list client-threats
show counters threat-intel threat-list client-threats
--------------------------------------
Hits for spam sources                              23
Hits for windows exploits                          0
Hits for web attacks                               0
Hits for botnets                                   0
Hits for scanners                                  0
Hits for dos attacks                               0
Hits for reputation                                0
Hits for phishing                                  0
Hits for proxy                                           0
Hits for mobile threats                                  0
Hits for tor-proxy                                       0
Total hits for threat-list                               23
```

To configure from the GUI, navigate as follows:

Security > Threat-Intel > Statistics > Category Hits > Threat List

Figure 22 : Security >> Threat-Intel >> Statistics >> Category Hits >> Threat List



Category ○ Global ● Threat List

Threat List: all

Category	Hits
Spam Sources	15
Mobile threats	15
Total Hits	30

5. Debug threat-intel:

   More debugging information can be obtained on a per-packet level using the following commands:

```
ACOS# debug threat-intel
ACOS# debug monitor
Wait for debug output, enter <ctrl c> to exit
[THREAT-INTEL] IP 1.32.0.0 is categorized into spam-sources
[THREAT-INTEL] IP 1.32.0.0 is categorized into mobile-threats
```

   Press control-C to exit debug.

6. Threat-intel log:

   If there are any errors with enabling the module, errors can be checked here:

```
ACOS# show threat-intel log webroot
2018-02-16 15:40:41 ERROR: Cannot resolve host
api.bcti.brightcloud.com: Temporary failure in name resolution
2018-02-16 15:40:41 ERROR: IpUpdateTask: OnError!
```

```
2018-02-16 15:59:40 ERROR: Cannot resolve host
api.bcti.brightcloud.com: Temporary failure in name resolution
2018-02-16 15:59:40 ERROR: IpUpdateTask: OnError!
2018-02-16 17:02:04 ERROR: Cannot resolve host
api.bcti.brightcloud.com: Temporary failure in name resolution
2018-02-16 17:02:04 ERROR: IpUpdateTask: OnError!
```

The default log-level is “Error”. However, if the module load fails for any reason, the log failure should have the necessary error logs. You can obtain more information about loading the module by changing the log-level under threat-feed webroot to “Info”.

Behavior on Multi-PU Platforms

On multi-PU platforms, the context of threat-intel is deployed automatically on both processing units (PUs); PU1 and PU2. After receiving traffic from both PUs, the packets comply with the same rules and perform the same actions. Therefore, the following show commands display aggregated counters from both PU1 and PU2:

- **`show threat-intel hits webroot`**
- **`show counters threat-intel threat-list`** *`<threat-list-name>`*
- **`show counters threat-intel webroot-global`**

NOTE: Viewing the threat-intel statistics is not supported in GUI for multi-PU platforms.

Similarly, on multi-PU platforms, the following **`clear`** commands clear the counters for both PU1 and PU2:

- **`clear threat-intel hits webroot`**
- **`clear counters threat-intel threat-list`** *`<threat-list-name>`*
- **`clear counters threat-intel webroot-global`**

For more information, see the *Command Line Interface Reference guide*.

IP Threat List

IP Threat List is a collection of class-lists. It contains IP addresses coming from threat actors or malicious actors launching threat activities and malware distribution.

The IP Threat List can be created using one of the following:

- Third-party database such as ThreatSTOP

  ThreatSTOP can be imported in the form of class-lists. To import the databases into a class-list, use the **import** or **import-periodic** command.

  Example commands:

```
ACOS(config)# import class-list MyClassList use-mgmt-port
scp://temp@172.33.17.89/home/classlist/threatstop_1.txt
ACOS(config)# import-periodic class-list MyClassList use-mgmt-port
scp://temp@172.33.17.89/home/classlist/threatstop_1.txt period 60
```

- A10 Threat Intel List

  This list can be imported in the form of a class-list (**a10-ip-threatList**). The A10 research team generates it by continuously monitoring live traffic, and it can be used only with a valid A10 Threat Intel license. The list can be downloaded from the GLM server using the automatic-update feature. For more information, refer to A10 Threat Intel List.

- A10 Defend Threat List

  A10 Defend offers IP Block lists (both predefined and customized), which identify malicious IP addresses originating from suspicious sources. These block lists can be imported from the A10 Defend site to the ACOS device in the form of class-lists. For more information, refer to A10 Defend Threat List.

ACOS provides an ability to configure IP Threat List. When an IP threat list is configured, ACOS matches the incoming traffic with the IP addresses listed on the threat list. If the source or the destination IP address matches the IP addresses listed on the threat list, ACOS drops the traffic and prevents the subscriber from connecting to a malware IP address. IP Threat List helps prevent subscribers and ACOS devices from DDoS attacks.

For ACOS to match the IP addresses with the IP threat list, the following criteria must match:

- The incoming packets should match the IPv4 or IPv6 protocol.
- The destination IP should not have ACOS interface IP or floating IP as the tunnel endpoint.
- The incoming packets should not have sessions already existing in the device.

NOTE: If there are sessions already existing, the IP threat list filter may not be applied to the traffic. This is to avoid performance issues. However, there are some exceptions where the IP threat list filter will be applied to Round Robin packets, fragmented packets, and ICMP or ICMPv6 packets even though they have existing sessions.

IP Threat List, which is a class-list, can be updated either periodically or manually. If there are IPs added while there are existing sessions, the traffic for those sessions may not be blocked. If there are IP addresses removed from the threat list during the update, it takes approximately a minute to remove those IP addresses from the blocked-list.

As the threat list is composed of public IPs, the IP Threat List configuration can be enabled only in Shared Partition. However, the configuration is applicable for all L3V partitions. So, the traffic in the L3V partitions go through the Threat List lookup.

The IP Threat List entries are not synchronized in the Standby mode. If the configuration is synchronized, the traffic will create the entries after the fail over.

IP Threat List is supported on all platforms. It can contain both source and destination based IP addresses.

Security Policy Engine (SPE) Support

On SPE supported platforms, SPE will drop the packets in hardware. The SPE hardware functionality will be utilized for reducing the CPU load caused due to DDoS attacks. When configured, every IP address will contain a software entry and optionally, an SPE entry.

Upon creating a software entry for the IP Threat List, as per the availability of the SPE resources, they are programmed to SPE. The SPE entries are dynamic. They have a default idle timeout of approximately a minute. However, the SW entries are removed as per the configured idle-timeout.

The SPE entries are enabled only for source-based IP addresses in the IP threat list.

NOTE: Sometimes, the IP address is not recorded as an SPE entry. This may be due to a lack of SPE resources.

Limitations

The IP Threat List capability comes with few limitations:

- If you configure or update the IP threat list while there are existing sessions for the listed IP address, that IP address may not be blocked.
- SPE can drop only IP addresses that match the TCP or UDP protocol not containing FIN and RST, that are not fragmented, and that does not contain IP options or extension headers.
- If the packets are tunneled, only the outer header information is used for matching the threat list. Only for GTP-U tunnels, the inner IP information is used for matching the threat list.

Configuring IP Threat List

You can configure the IP Threat List only in the shared partition. You can first configure an IP Threat Action template and then bind that template to the class-list or you can simply create a source, destination or internet-host IP Threat List and bind the class-list. Creating an IP Threat Action Template helps to set the idle timeout and logs. This is optional.

You can configure up to 8 IP Threat Action templates. You can bind up to 4 class-lists for each type of IP Threat List.

To configure an IP Threat Action template (optional), perform the following:

1. Configure an IP Threat Action template with a template number.

```
ACOS(config)# template ip-threat-action <1-8> [template number]
ACOS(config-ip-threat-action)#
```

2. Configure the idle timeout in minutes. By default, the timeout is set to 5 minutes.

   ```
   ACOS(config-ip-threat-action)# idle-timeout <1-1440> [idle-timeout in 
   minutes]
   ```

To enable logs for the IP Threat Action template, use the following command:

```
ACOS(config-ip-threat-action)# log enable
```

To configure an IP Threat List, use the following commands:

1. Configure an IP Threat List at the system configuration level.

   ```
   ACOS(config)# system ip-threat-list
   ```

2. Select the type of list you want to create for packet filtering. You can create any of the following Threat Lists:

   - To create an IPv4 Source List, use the following command:

     ```
     ACOS(config-ip-threat-list)#ipv4-source-list
     ACOS(config-ip-threat-list-ipv4-src)#
     ```

   - To create an IPv4 Destination List, use the following command:

     ```
     ACOS(config-ip-threat-list)#ipv4-dest-list
     ACOS(config-ip-threat-list-ipv4-dest)#
     ```

   - To create an IPv6 Source List, use the following command:

     ```
     ACOS(config-ip-threat-list)#ipv6-source-list
     ACOS(config-ip-threat-list-ipv6-src)#
     ```

   - To create an IPv6 Destination List, use the following command:

     ```
     ACOS(config-ip-threat-list)#ipv6-dest-list
     ACOS(config-ip-threat-list-ipv6-dest)#
     ```

   - To create an IPv4 Internet Host List, use the following command:

     ```
     ACOS(config-ip-threat-list)#ipv4-internet-host-list
     ACOS(config-ip-threat-list-ipv4-internet-host)#
     ```

   - To create an IPv6 Internet Host List, use the following command:

     ```
     ACOS(config-ip-threat-list)#ipv6-internet-host-list
     ACOS(config-ip-threat-list-ipv6-internet-host)#
     ```

The IPv4 and IPv6 internet host lists can track malicious internet IPs in both the directions. For example, these lists can check the destination IP for outbound new sessions as well as the source IP for inbound new sessions. Thus, a single internet host list can be used instead of two separate lists (destination list and source list).

3. To the type of threat list created in step 2, bind the class-list. For example, to bind a class-list to the `ipv4-source-list`, use the following command:

```
ACOS(config-ip-threat-list-ipv4-src)# class-list ip_threatList
```

4. To bind the IP Threat Action template, use the following command:

```
ACOS(config-ip-threat-list-ipv4-src)# class-list ip_threatList ip-
threat-action 1
```

Displaying and Clearing IP Threat Entries

- You can display the IP Threat List entries using the following command:

```
ACOS(config)#show system ip-threat-list entries <IPv4 address | IPv6
address or Prefix>
```

For example:

```
ACOS(config)#show system ip-threat-list entries 192.168.1.1
IP Address      Match Type   In-SPE    Age
---------------------------------------------
192.168.1.1     Source       0         5
```

- You can clear the IP Threat List entries using the following command:

```
ACOS(config)#clear system ip-threat-list entries <IPv4 address | IPv6
address or Prefix>
For example:
ACOS(config)#clear system ip-threat-list entries 192.168.1.1
```

It may take about approximately a minute to clear the threat list entries.

- You can view the IP Threat List counters using the following command:

```
ACOS(config)#show counters system ip-threat-list
```

Table 6 displays the `show counters system ip-threat-list` output.

Table 6 : Show Counters for IP Threat List

Counter	Description
Packet Hit Count in SW	Displays the total number of packets that hit the entries in IP Threat List
Packet Hit Count in SPE	Displays the total number of packets that hit the entries in SPE
Entries Added in SW	Displays the total number of entries added to the threat list
Entries Removed from SW	Displays the total number of entries removed from the threat list
Entries Added in SPE	Displays the total number of entries added to SPE
Entries Removed from SPE	Displays the total number of entries removed from SPE
Out of memory Error	Displays the following error: Unable to create an entry in the IP threat list due to memory exhaustion
Out of SPE Entries Error	Displays the following error: Unable to add entries to SPE due to SPE resource limit or exhaustion

NOTE: The Packet Hit Count in SPE is updated for every 4096 packets per entry or upon removal of an entry from SPE. All the SPE related counters are incremented on SPE supported platforms only.

IP Threat List Logging

Logs are disabled by default. When logging is enabled, the logs are generated locally by default when entries are added and removed from the IP Threat List. For exporting logs to the external collector, additional configuration is required. Both Syslog and CEF formats are supported.

Use the following commands to enable logs:

```
ACOS(config)# template ip-threat-action 1 ip_threatList
ACOS(config-ip-threat-action)# log enable
```

The following example shows the log displayed when an entry is added:

```
Nov 05 2019 01:26:13 Info [SYSTEM]:IP-ThreatList added entry for IP
192.168.1.1 due to packet from Source IP192.168.1.1 and Source Port 1000
to Dest IP 192.168.2.2 and Dest Port 1001 Protocol UDP
```

The following example shows the log displayed when an entry is removed:

```
Nov 05 2019 01:29:48 Info [SYSTEM]:IP-ThreatList removed for IP
192.168.1.1
```

A10 Threat Intel List

ACOS provides the ability to configure IP Threat Lists. An IP Threat List is a collection of IP address class-lists coming from malicious actors launching threat activities and malware distribution.

A10 Threat Intel list (a class-list) can also be used to create an IP Threat list. The Firewall can utilize this list to detect malicious sources and drop the traffic associated with anomalous IP addresses, thereby providing protection against DDoS attacks.

The **a10-ip-threatList** class list is generated by the A10 Research Team by continuously monitoring live traffic. It can be downloaded from the GLM server only with a valid A10 Threat Intel license. To install this license, see Installing A10 Threat Intel License.

This list must be configured at the system level using the **`system ip-threat-list`** command.

NOTE:

- The threat list is global to the system. The IPs in the threat list are common for all partitions.
- The list cannot be modified. Additionally, a white-list (exception list) or a block-list (augmented list) cannot be defined for it.

The following topics are covered:

Limitations

The A10 Threat Intel List configuration has the following limitations:

- IPv6 addresses are not supported.
- L3V level configuration is not supported.
- Only a single class-list is supported.
- Only Syslog and CEF formats are supported for logging.

Configuring A10 Threat Intel List

A10 Threat Intel list (**a10-ip-threatList** class list) can be downloaded from the GLM server by using the **automatic update** command. See Downloading and Updating A10 Threat Intel List.

This class-list must be bound to a source, destination or internet-host IP threat list by using the **system ip-threat-list** command.

CLI Configuration

- To bind **a10-ip-threatList** class-list to the IPv4 Internet Host Threat list, use the following command:

```
ACOS(config)# system ip-threat-list
ACOS(config-ip-threat-list)# ipv4-internet-host-list
ACOS(config-ip-threat-list-ipv4-src)# class-list a10-ip-threatList
```

- To view the downloaded class-list, use the following command:

```
ACOS(config)# show class-list
Name                     Type       IP       Subnet    DNS    String
Location
a10-ip-threatList        [ipv4]    78039    0          0      0          file
CL1                      [ipv4]    4        0          0      0          config
CL2                      [ipv4]    0        1          0      0          config
```

```
Total: 3
```

For more information on configuring an IP Threat list, refer Configuring IP Threat List.

Downloading and Updating A10 Threat Intel List

The A10 threat Intel List can be downloaded from the Global License Manager (GLM) server using the **automatic-update** feature. GLM is the master licensing and billing system for A10 Thunder. GLM collects information from the distributed LLPs and issues licenses for the Thunder instances upon request.

To download and update the A10 Threat Intel list, a valid A10 Threat Intel License is needed. To install this license, see Installing A10 Threat Intel License.

ACOS provides two methods to update the A10 Threat Intel List:

- Automatic Update
- Manual Update

Automatic Update

Use the **automatic-update** command to automatically download the A10 Threat Intel list from the GLM server. When the update schedule is triggered, the ACOS devices will update and install the A10 Thread Intel list.

In the case of dual blade multi-PU platform, both PU1 and PU2 will update and install bundle files when the automatic update schedule is triggered.

CLI Configuration

The **automatic-update** command is used to configure an update schedule on the ACOS device. The device will check for updates according to the update schedule (daily or weekly). The following commands demonstrate **automatic-update** usage:

- To update the A10 Threat Intel list daily:

```
ACOS(config)# automatic-update a10-threat-intel schedule daily 12:30
```

- To update the A10 Threat Intel list on a weekly basis:

```
ACOS(config)# automatic-update a10-threat-intel schedule weekly Tuesday
12:30
```

- To stop the automatic updates:

```
ACOS(config)# no automatic-update a10-threat-intel schedule daily 12:30
```

- To view the automatic update schedule:

```
ACOS (config)# show automatic-update
------------------------------------------------------------------------
--
Feature name  Version       Schedule         Time   Last Updated  Next
Check
------------------------------------------------------------------------
--
app-fw        1.360.0-23    N/A              00:00  N/A           N/A
ca-bundle     20200722      N/A              00:00  2020-09-08    N/A
a10-threat-intel     20210329090521     Daily            02:24  2021-03-24
 2021-03-24
```

Manual Update

You can manually update the A10 Threat Intel List and even revert to the previous version using the following commands.

CLI Configuration

- To manually update to the latest version:

```
ACOS (shared)# automatic-update check-now a10-threat-intel
```

- To revert to the previous version of the threat list:

```
ACOS (shared)# automatic-update revert a10-threat-intel
```

For more information on **`automatic-update`** command, refer to the *Command Line Interface Reference* guide.

Sample Configuration - A10 Threat Intel List

In this sample configuration, CGN employs A10 Threat Intel list to detect anomalous IP addresses.

- The following commands installll the A10 Threat Intel license and configures the schedule to download the A10 Threat Intel list (**`a10-ip-threatList`**) daily:

```
glm use-mgmt-port
glm enable-requests
glm token vThe38228e09

ip dns primary 8.8.8.8

automatic-update use-mgmt-port

automatic-update a10-threat-intel schedule daily 4:1
```

- The following commands configure an IP Threat Action template:

```
template ip-threat-action 2
 idle-timeout 25
 log enable
```

- The following commands bind the downloaded class-list (**`a10-ip-threatList`**) to the IPv4 Internet Host list:

```
system ip-threat-list
 ipv4-internet-host-list
   class-list a10-ip-threatList ip-threat-action 2
```

Installing A10 Threat Intel License

A10 Threat Intel license has to be installed through the Global License Manager (GLM). To install this license, you need to have the A10 Threat Intel token. This token is provided along with devices having Carrier Grade NAT (CGN) solution. You can also obtain this token using GLM GUI.

After obtaining the token, follow the steps mentioned below to activate the license. In this example, `A10d5275450e` is used as the token.

1. Log in to your ACOS device and enter the configuration mode.
2. Configure your ACOS device with a valid domain name server (DNS).

   An example configuration is provided below. Use the show run ip command to verify your configuration.

   ```
   ACOS(config)# ip dns primary 8.8.8.8
   ```

3. Configure the user management port interface.

   ```
   ACOS(config)# glm use-mgmt-port
   ```

4. Configure the license by specifying the A10 Threat Intel Token

   ```
   ACOS(config)# glm token A10d5275450e
   ```

5. Send the license request to the GLM.

   ```
   ACOS(config)# glm send license-request
   A10_TI License successfully updated, please log out and log back in to
   access license features
   ```

6. Save the configuration by executing write mem command.
7. To check if the license is updated successfully, enter the following command:

   ```
   ACOS(config)# show license-info
   Host ID  : 3BA7E826879B1BBE45D2A7AC8A0573B5DB67C041
   USB ID   : Not Available
   Billing Serials: vThf318cf56c0000, vThe38228e090000, vTh26a3096a50000
   Product  : ADC
   Platform : Thunder Series Unified Application Service Gateway
   Burst    : Disabled
   Version  : Thunder Unlimited
   GLM Ping Interval In Hours : 24
   --------------------------------------------------------------
   Enabled         Licenses Expiry Date (UTC) Notes
   --------------------------------------------------------------
   SLB              None
   CGN              None
   GSLB             None
   RC               None
   DAF              None
   WAF              None
   ```

```
SSLI             None
DCFW             None
GIFW             None
URLF            None
AAM             None
FP              None
WEBROOT         N/A Requires an additional Webroot license.
THREATSTOP   N/A Requires an additional ThreatSTOP license.
QOSMOS       N/A Requires an additional QOSMOS license.
WEBROOT_TI   N/A Requires an additional Webroot Threat Intel license.
IPSEC_VPN    N/A Requires an additional IPsec VPN license.
A10_TI  31-December-2021
```

A10 Defend Threat List

A10 Defend is a centralized threat intelligence platform that collects and analyzes data on security threats and vulnerabilities in the organization where the network security solution is implemented.

A10 Defend offers IP Block lists (both predefined and customized), which identify malicious IP addresses originating from suspicious sources. These block lists can be imported from the A10 Defend site to the ACOS device as class-lists, which can then be used to create IP Threat lists. The Firewall employs these threat lists to detect malicious sources and drop the traffic associated with such IP addresses, thereby protecting against cyberattacks.

This section provides an overview on A10 Defend IP block lists, and the steps to import the IP block lists in ACOS.

The following topics are covered:

A10 Defend IP Block Lists

A10 Defend IP Block List contain a list of malicious IP addresses across various categories including bots, reflectors, command and control (C2) servers, malware droppers, and more.

There are three types of blocklists:

- IP Block List - These are standard blocklists created by the A10 Defend team by continuously monitoring live traffic.
- Custom IP Block List - These are customized blocklists created by A10 Defend tenants (registered users).
- Aggregated IP Block List - These are customized blocklists created by aggregating IP Block Lists, Custom IP Block Lists, or both.

These IP blocklists are available in two formats: Plain IP List and STIX 2.1, both of which are supported in ACOS for importing. However, it is recommended to download the list in STIX 2.1 format, since it has a structured format with rich metadata that provides more threat intelligence information.

For more information on IP blocklists, see IP Block Lists.

Importing IP Block list in ACOS

This topic describes the steps to obtain the IP blocklist URL link from the A10 Defend site and import it into ACOS.

The following topics are covered:

Pre-requisites

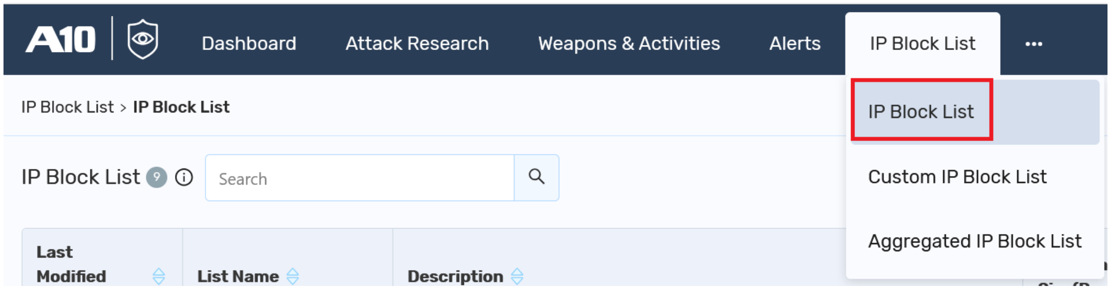
You need to register on the A10 Defend site and create an Auth User account (with a user ID and password). For more information, see Auth Users.

NOTE: While setting the password for an Auth User, ensure it does not include any of the following special characters: `(blank space) %&'/:<>?@[\]`. These characters are not supported in ACOS while entering the password after executing the **`import`** or **`import-periodic`** command.

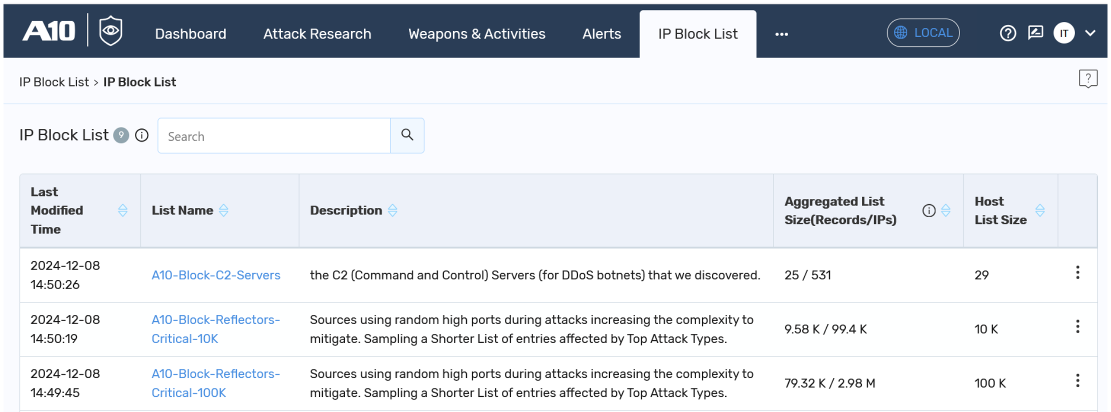
Obtaining IP Block List URL

Perform the following steps to obtain the IP Block list URL:

1. Login to the A10 Defend site using your credentials.
2. Navigate to **IP Block List** > **IP Block List**.



A list of IP Block lists is displayed.

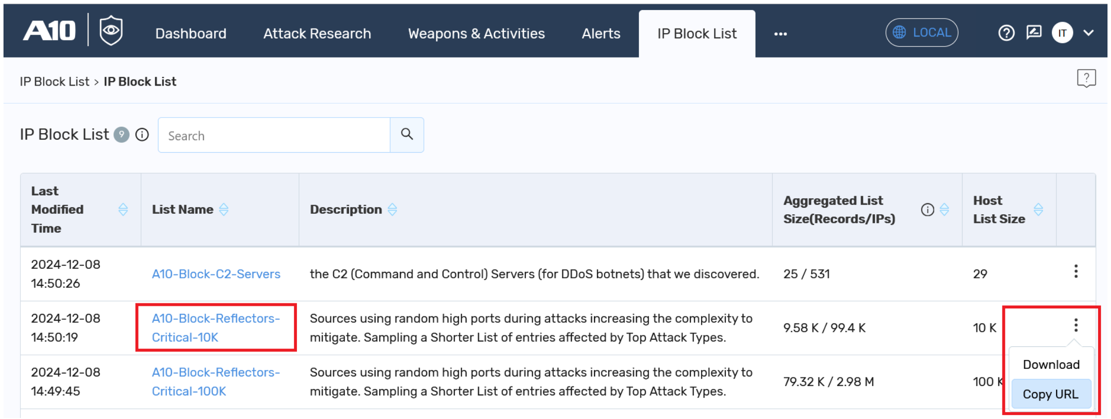


Last Modified Time	List Name	Description	Aggregated List Size(Records/IPs)	Host List Size
2024-12-08 14:50:26	A10-Block-C2-Servers	the C2 (Command and Control) Servers (for DDoS botnets) that we discovered.	25 / 531	29
2024-12-08 14:50:19	A10-Block-Reflectors-Critical-10K	Sources using random high ports during attacks increasing the complexity to mitigate. Sampling a Shorter List of entries affected by Top Attack Types.	9.58 K / 99.4 K	10 K
2024-12-08 14:49:45	A10-Block-Reflectors-Critical-100K	Sources using random high ports during attacks increasing the complexity to mitigate. Sampling a Shorter List of entries affected by Top Attack Types.	79.32 K / 2.98 M	100 K

Optionally, you can select a **Customer IP Block List** or an **Aggregated IP Block List**.

3. Select the block list to be imported (`A10-Block-Reflectors-Critical-10K` in this case) and hover over the three dots in the column to the right.

   The options **Download** and **Copy URL** are displayed.



IP Block List > **IP Block List**

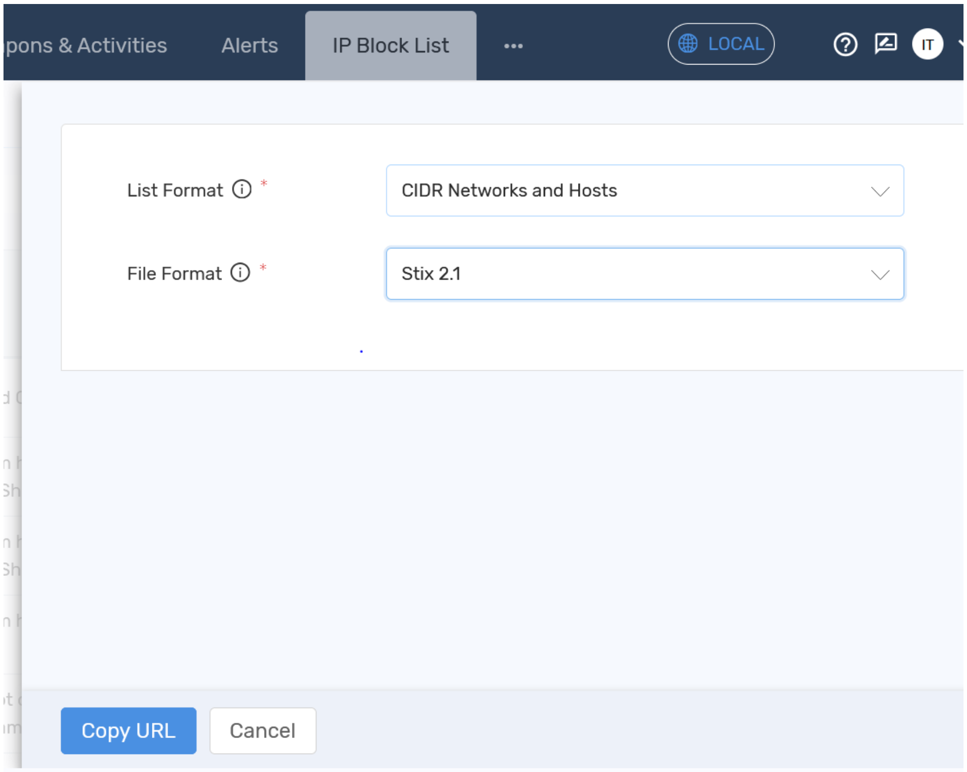
IP Block List

Search

Last Modified Time	List Name	Description	Aggregated List Size(Records/IPs)	Host List Size
2024-12-08 14:50:26	A10-Block-C2-Servers	the C2 (Command and Control) Servers (for DDoS botnets) that we discovered.	25 / 531	29
2024-12-08 14:50:19	A10-Block-Reflectors-Critical-10K	Sources using random high ports during attacks increasing the complexity to mitigate. Sampling a Shorter List of entries affected by Top Attack Types.	9.58 K / 99.4 K	10 K
2024-12-08 14:49:45	A10-Block-Reflectors-Critical-100K	Sources using random high ports during attacks increasing the complexity to mitigate. Sampling a Shorter List of entries affected by Top Attack Types.	79.32 K / 2.98 M	100 K

4. Click **Copy URL**.

The following dialog box is displayed:



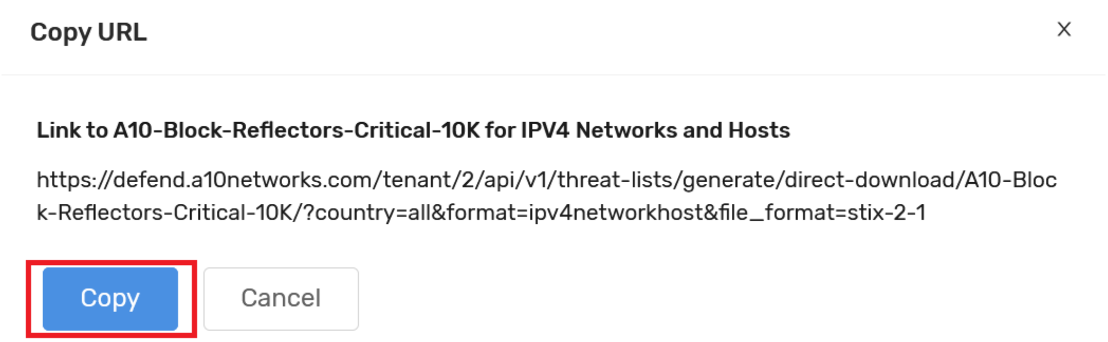
List Format * CIDR Networks and Hosts

File Format * Stix 2.1

NOTE: Optionally, you can also download the blocklist on your system (using the **Download** option). The system path can be provided while importing the blocklist file in ACOS.

5. Select the **List Format** as **CIDR Networks and Hosts**, the **File Format** as **Stix 2.1** (or **Plain IP List**), and click **Copy URL**.

   The URL to be copied is displayed.



Copy URL

Link to A10-Block-Reflectors-Critical-10K for IPV4 Networks and Hosts

https://defend.a10networks.com/tenant/2/api/v1/threat-lists/generate/direct-download/A10-Block-Reflectors-Critical-10K/?country=all&format=ipv4networkhost&file_format=stix-2-1

6. Click **Copy** to copy the URL to the clipboard.
7. Past the URL in a notepad and replace the special characters '?' and '&' with their respective URL-encoded values. Replace '?' with '%3F' and '&' with '%26'.

   Consider the following example:

   URL from A10 Defend:

```
https://defend.a10networks.com/tenant/2/api/v1/threat-
lists/generate/direct-download/A10-Block-Reflectors-Critical-
10K/?country=all&format=ipv4networkhost&file_format=stix-2-1
```

   Updated URL with special characters replaced:

```
https://defend.a10networks.com/tenant/2/api/v1/threat-
lists/generate/direct-download/A10-Block-Reflectors-Critical-
10K/%3Fcountry=all%26format=ipv4networkhost%26file_format=stix-2-1
```

Importing IP Block List

Perform the following steps to import the IP Blocklist as a class-list in ACOS:

1. After obtaining the updated URL, import the IP blocklist in ACOS using the following command:

- For STIX 2.1 format:

  ```
  ACOS(config)# import class-list <class-list-name> use-mgmt-port
  <URL>
  ```

  When prompted for username and password, enter A10 Defend Auth User credentials.

  Example command:

  ```
  ACOS(config)# import class-list A10blocklist use-mgmt-port
  https://defend.a10networks.com/tenant/2/api/v1/threat-
  lists/generate/direct-download/A10-Block-Reflectors-Critical-
  10K/%3Fcountry=all%26format=ipv4networkhost%26file_format=stix-2-1
  ```

  Optionally, to import the IP blocklist periodically, execute the **import-periodic** command.

  ```
  ACOS(config)# import-periodic class-list A10blocklist use-mgmt-port
  https://defend.a10networks.com/tenant/2/api/v1/threat-
  lists/generate/direct-download/A10-Block-Reflectors-Critical-
  10K/%3Fcountry=all%26format=ipv4networkhost%26file_format=stix-2-1
  period 60
  ```

- For Plain IP List format:

  ```
  ACOS(config)# import class-list-convert <class-list-name> class-
  list-type ipv4 use-mgmt-port <URL>
  ```

  Example command:

  ```
  ACOS(config)# import class-list-convert A10blocklist class-list-type
  ipv4 use-mgmt-port
  https://defend.a10networks.com/tenant/2/api/v1/threat-
  lists/generate/direct-download/A10-Block-Reflectors-Critical-
  10K/?country=all&format=ipv4networkhost&file_format=plain-ip-list
  ```

2. To verify successful import, execute the following show command:

   ```
   ACOS(config)# show class-list A10blocklist
   Name:               A10blocklist
   User Tag:
   Total single IP:    9367
   Total IP subnet:    307
   ```

```
Content:
    114.114.114.114/32 hitcount 0 threat-category botnets
    10.0.0.0/32 hitcount 0 threat-category botnets
    177.68.164.68/32 hitcount 0 threat-category botnets
    187.102.161.102/32 hitcount 0 threat-category botnets
    92.19.64.19/32 hitcount 0 threat-category botnets
    191.19.161.19/32 hitcount 0 threat-category botnets
    170.64.154.0/32 hitcount 0 threat-category botnets
    185.190.141.0/32 hitcount 0 threat-category botnets
    .......
    .......
```

The show command output displays the list of malicious IP addresses along with the threat categories.

NOTE: The threat categories are displayed only if the IP blocklist is in Stix 2.1 file format.

Configuring Threat List

To configure a threat-list, bind the imported blocklist to an internet-host IP threat list by using the **`system ip-threat-list`** command. The following configuration demonstrates command usage:

```
ACOS(config)# system ip-threat-list
ACOS(config-ip-threat-list)# ipv4-internet-host-list
ACOS(config-ip-threat-list-ipv4-src)# white-list mywhitelist
ACOS(config-ip-threat-list-ipv4-src)# class-list A10blocklist
```

Points to be considered while binding the blocklist:

- You can bind the blocklist to an IPv4 source list, destination list, or internet host list. However, it is recommended to bind it to an IPv4 internet host list, as this list can track malicious IPs in both directions of the data plane. For example, it can check destination IPs for outbound new sessions and source IPs for inbound new sessions, eliminating the need for separate destination and source lists.
- You can use the **`white-list`** option to bind an exception list to the IPv4 internet host list. The exception list (*`mywhitelist`*) defines IPs that are exempted from

blocking, i.e., traffic to or from these IPs is always allowed, even if they are included in the blocklist (*A10blocklist*).

Viewing IP Threat List Entries and Counters

- To view the IP Threat List entries, use the following command:

```
ACOS(config)# show system ip-threat-list entries
```

Example Output:

```
ACOS(config)# show system ip-threat-list entries
IP Address   Match Type     In-SPE    Age    Hit-count    Class-list
-----------------------------------------------------------------------
92.19.64.19  Internet host  No        5      10           botnets
```

The show command output indicates that the blocked IP address 92.19.64.19 is an 'Internet host' from the 'botnets' threat-list category, with 10 hits recorded so far.

- To view IP Threat list counters, use the following command:

```
ACOS(config)# show counters system ip-threat-list
show counters system ip-threat-list
-----------------------------------------------------
Packet Hit Count in SW           3346
Packet Hit Count in SPE          0
Entries Added in SW              14
Entries Removed from SW          12
Entries Added in SPE             0
Entries Removed from SPE         0
Out of memory Error              0
Out of SPE Entries Error         0
```

For field descriptions, see Show Counters for IP Threat List.

Limitations

- IPv6 addresses are not support, since A10 Defend does not currently support them.
- If entries overlap across different threat lists, the first matched threat list is used.

- A maximum of 16 different threat-categories are supported, with category names limited to 50 characters.
- While importing the blocklists using URLs, the characters '?' and '&' must be replaced with '%3F' and '%26' respectively.

Application Aware Firewall

Security Providers deploy network firewalls and inspect the traffic from and to their subscriber and users. The application aware firewall enforces security policies based on the recognized application and business logic applied to this type of traffic. Application recognition that is provided using various L3-L7 techniques, significantly enhances security protection as compared to traditional stateful firewalls.

The following topics are covered:

Licensing

The new license upgrade feature provides the user, option to obtain a new library package from A10 Networks and upload it to file server (FTP/SCP/SFTP/RCP and so on). Users can manually upgrade or setup automatic upgrade, to update to a new version.

For more information, contact A10 Networks Sales.

GLM Server License and Protocol Bundle Update

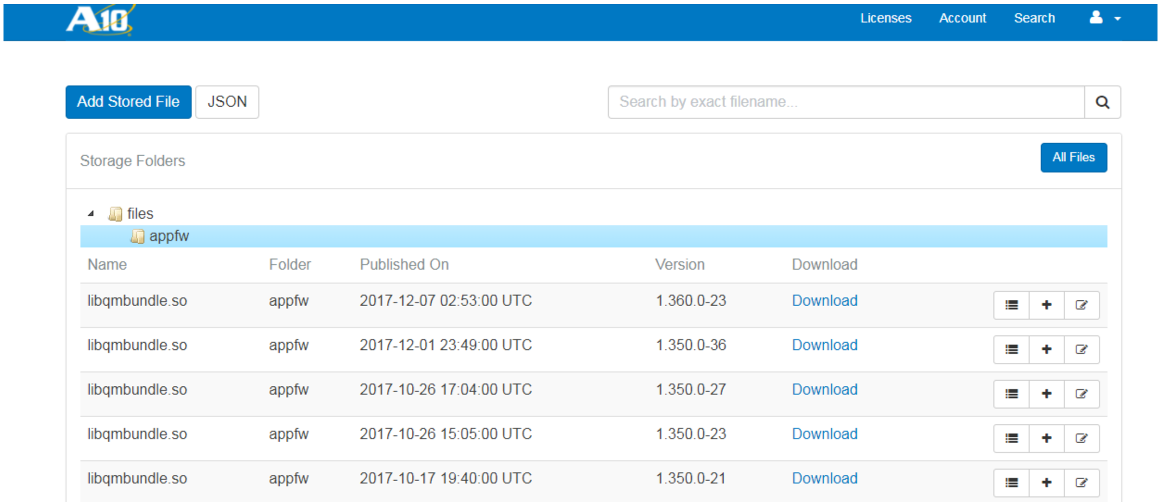
The Global License Manager (GLM) is the master licensing and billing system for A10 vThunder. GLM collects information from the distributed LLPs and issues licenses for the vThunder instances upon request.

GLM Server provides a `.json` file that contains latest software version of the application aware firewall feature. If the feature is licensed, ACOS initiates a download procedure if the automatic upgrade is activated. If automatic upgrade is not activated, then manual update must be performed.

You can download the application protocol bundles customized by A10 for your needs, from the download location on GLM Server.

The URL is as follows: https://glm.a10networks.com/stored_files/.

Figure 23 : GLM Server View



Name	Folder	Published On	Version	Download
libqmbundle.so	appfw	2017-12-07 02:53:00 UTC	1.360.0-23	Download
libqmbundle.so	appfw	2017-12-01 23:49:00 UTC	1.350.0-36	Download
libqmbundle.so	appfw	2017-10-26 17:04:00 UTC	1.350.0-27	Download
libqmbundle.so	appfw	2017-10-26 15:05:00 UTC	1.350.0-23	Download
libqmbundle.so	appfw	2017-10-17 19:40:00 UTC	1.350.0-21	Download

GLM server provides the latest protocol bundle file to ACOS. GLM server automatically pulls the latest protocol bundle files from the protocol support. The following features are provided:

- Automatic bundle updates and without service interruption.
- Two types of scheduled dynamic updates: Daily, Weekly.
- All data transmission between vThunder device and data center server goes through a secure channel. Additionally, the communication supports configuring a HTTP(s) proxy.
- The license status is checked for each feature before a feature update.
- The update can be performed through management or data port
- Software upgrade can only be configured and issued in the shared partition.

GLM License Availability

ACOS checks the license availability before it sends a request. If the license is not valid, the download request will not be sent. If a feature is not licensed, ACOS does not allow configuration of the feature.

```
ACOS(shared)# automatic-update check-now app-fw
```

The following warnings or error messages are displayed:

- If you try to configure an unlicensed feature, an error is displayed "Feature not licensed. Please contact your sales representative to license <*feature-name*>."
- If the feature license has expired, you can configure the feature with the older software version.
- Use `show license-info` to view license info.

The global configuration commands do not have a license check.

For example:

```
ACOS(shared)# automatic-update proxy-server
ACOS(shared)# automatic-update use-mgmt-port
```

Application Protocols and Categories

Application aware firewall rules are applied based on the classification result in a form of an Application-ID. The policy action is applied based on the matching criteria including the Application-ID and other conditions.

The Application aware firewall enables configuring rules matching traffic based on application protocols and categories. Currently, the ACOS application aware firewall supports more than three thousand applications belonging to 96 categories. These categories include web, file-management, gaming, web-e-commerce, and so on. An application can belong to more than one category at the same time.

Application aware Firewall also enables tracking of user activity for specific websites as defined in the rule-set. A specific protocol or category on the application aware firewall can be disabled using **`fw disable-application-protocol/category`** command.

NOTE: Application classification is also supported for DS-Lite Traffic. However, the classification happens only on the encapsulated payload (IP4) of the DS-Lite packet.

Table 7 : Example Applications, Protocols, Categories Table

Application Family-ID	Protocol-Category	Applications
1	audio-video	1 (sip)

Table 7 : Example Applications, Protocols, Categories Table

Application Family-ID	**Protocol-Category**	**Applications**
2	encrypted	2 (ssl)
3	web	3 (http) 4 (http2) 5 (skype) 6 (whatsapp)
4	instant-messaging	7 (facebook) 8 (google)
5	webmail	9 (gmail) 10 (owa)

Configuring Application Aware Firewall

The application aware firewall can be configured using one of the following approaches:

- Permissive approach
- Restrictive approach

Permissive approach, also referred to as blacklist, permits the rule at the bottom of the rule-set by default. It lists all the applications that needs to be denied permissions in the rule-set and it can deny key protocols only.

Example IPV4 Configuration

```
rule dns
  action permit
  application protocol dns

rule spotify
  action deny log
  application protocol spotify

rule dropbox
  action deny log
  application protocol dropbox
```

```
rule p2p
  remark for bittorrent
  action deny log
  application category peer-to-peer

rule im
  remark enable later to block skype,
fb-messenger and gtalk
  disable
  action deny log
  application category instant-messaging
rule skype
  action deny log
  application protocol skype

rule skype-biz
  action deny log
  application protocol lync_online

rule fb-web
  action deny log
  application protocol facebook
  application protocol fbcdn

rule fb-messenger
  action deny log
  application protocol facebook_messenger

rule fb-video
  remark fb-web needs to be permitted
  disable
  action deny log
  application protocol facebook_video
rule youtube
  action deny log
  application protocol youtube

rule gmail
  action deny log
  application protocol gmail
```

```
rule gtalk
  remark for hangouts
  action deny log
  application protocol gtalk
  application protocol gmail_chat

rule win-app-store
  action deny log
  application protocol windows_marketplace
rule xbox
  action deny log
  application protocol xbox
  application protocol xboxlive
  application protocol xboxlive_marketplace

rule default
  action permit log
```

Restrictive approach, also referred to as white-list, denies the rule at the bottom of the rule-set by default. It lists all the applications that needs to be permitted in the rule-set.

NOTE: In the restrictive approach, you must permit all the protocols that an application uses

Example IPV4 Configuration

```
rule dns
  action permit
  application protocol dns

rule spotify
  action permit log
  application protocol spotify

rule dropbox
  action permit log
  application protocol dropbox
```

```
rule p2p
  remark for bittorrent
  action permit log
  application category peer-to-peer
rule skype
  remark microsoft and windowslive are
 needed to login
  action permit log
  application protocol skype
  application protocol microsoft
  application protocol windowslive

rule msnhst
  remark skype-biz needs to access
 msnhst.microsoft.com
  action permit
  dest ipv4-address 52.112.64.0/22

rule skype-biz
  remark microsoft and office365 are needed
 to login
  action permit log
  application protocol lync_online
  application protocol office365
  application protocol microsoft
rule fb-web
  action permit log
  application protocol facebook
  application protocol fbcdn

rule fb-messenger
  action permit log
  application protocol facebook_messenger

rule fb-video
  action permit log
  application protocol facebook_video

rule youtube
  action permit log
  application protocol youtube

rule gmail
  action permit log
  application protocol gmail
rule gtalk
  remark for hangouts
  action permit log
  application protocol gtalk
  application protocol gmail_chat

rule google
  remark needed for gmail, gtalk and youtube
  action permit log
  application protocol google_gen
rule win-app-store
  remark microsoft and windowslive are needed
to login, windows_update for downloading apps
from store
  action permit log
  application protocol windows_marketplace
  application protocol windowslive
  application protocol microsoft
  application protocol windows_update

rule xbox
  remark windowslive is needed to login
  action permit log
  application protocol xbox
  application protocol xboxlive
  application protocol xboxlive_marketplace
  application protocol windowslive

rule default
  action deny log
```

Firewall rule-sets for Application Aware Firewall

The Application aware firewall provides the ability to configure the security policy using the firewall rule-set. The firewall rule-sets can be applied on any of the following:

- Category
- Protocol

Further to this, object groups can be created and the applications can be tracked.

NOTE: For more information on configuration commands, refer to the Rule-sets section.

Updating Application Protocols

Application aware firewall provides the ability to update protocol definition at higher frequency than a software upgrade. Application protocol definitions are provided as protocol bundles. The customized protocol bundles and license information for ACOS are provided on the GLM server.

ACOS provides two methods to update the application protocols and software.

- Automatic Update
- Manual Update

Automatic Update

Automatic update supports feature upgrade for Layer 7 application traffic classifications. When user upgrades the vThunder device, the associated A10 devices in the network are automatically updated when automatic upgrade is configured. The devices use default protocol bundle after the initial upgrade.

In the case of dual blade multi-PU platforms, both PU1 and PU2 will update and install bundle files when the automatic update schedule is triggered.

NOTE: The application aware firewall classifications are supported only for TCP and UDP protocols. IP protocols other than UDP and TCP are not classified.

The following topics are covered:

CLI Configuration

Configure an update schedule on the ACOS device. The device will check for updates periodically according to the update schedule.

```
ACOS (config)# automatic-update app-fw schedule ?
  daily   Every day
  weekly  Every week

ACOS (config)# automatic-update app-fw schedule daily ?
  hh:mm  Time of day to update (hh:mm) in 24 hour local time
ACOS (config)# automatic-update app-fw schedule weekly ?
  Monday     Monday
  Tuesday    Tuesday
  Wednesday  Wednesday
  Thursday   Thursday
  Friday     Friday
  Saturday   Saturday
  Sunday     Sunday
```

- To perform automatic update through management port, use the following command:

  ```
  ACOS (shared)# automatic-update use-mgmt-port
  ```

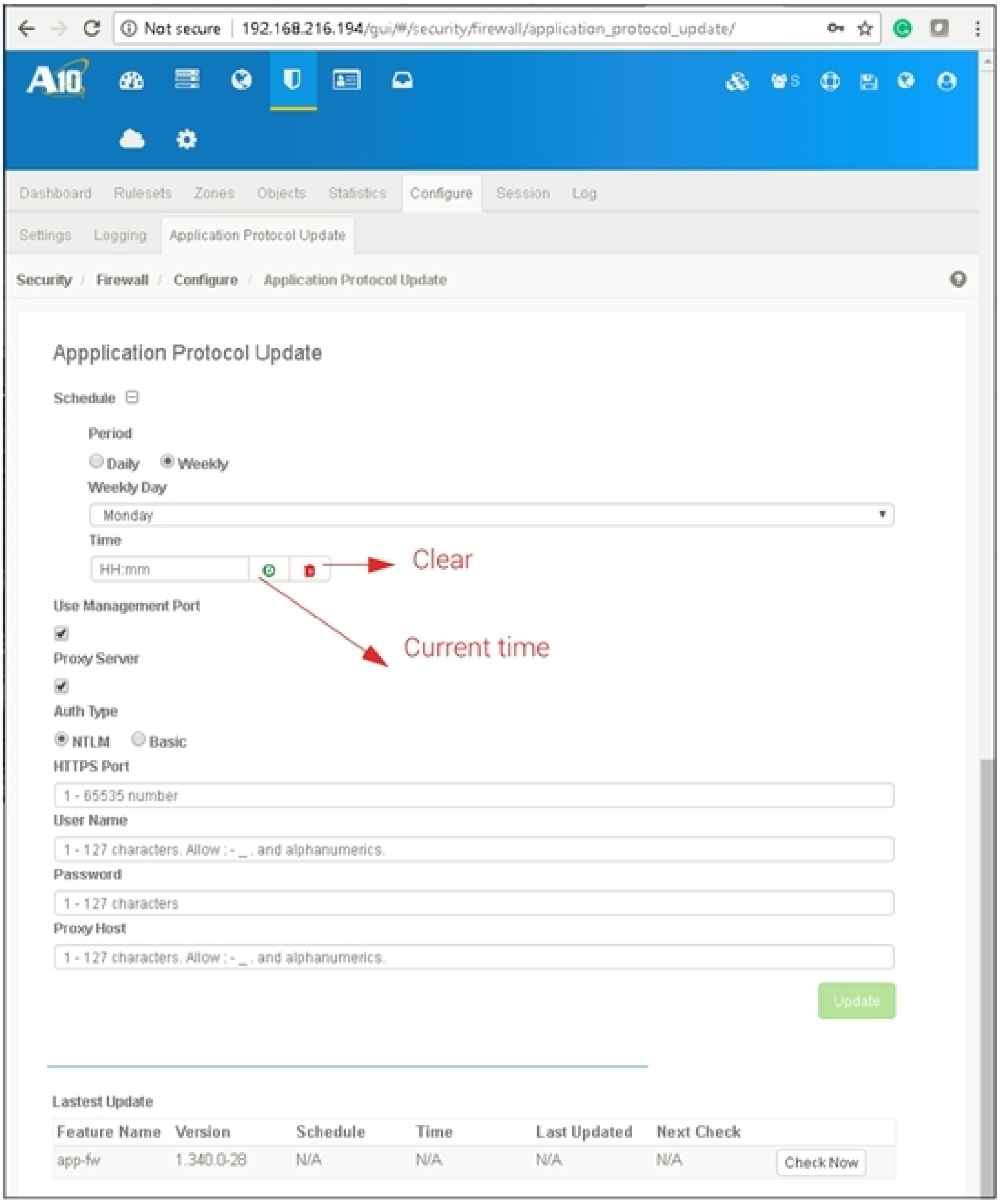
- To change back to previous protocol bundle version, use the following command:

  ```
  ACOS (shared)# automatic-update revert
  ```

GUI Configuration

1. Navigate from **Firewall** to **Configure** and then to the **Application Update** page.
2. Click the **Schedule** to open up the schedule options.
3. Select **Weekly** option, set the **Day** and **Time**. The **Current Time** and **Clear** buttons can be used if required.
4. Check the **Use Management Port** option.
5. If you select **Proxy Server** option, **NTLM** is selected by default.
6. Enter the **HTTPS Port** (value 1-65535), **User Name**, **Password** and **Proxy Host** as required.
7. Click **Update** button to update the schedule**.**
8. To check the latest update, click the **Check Now** button under **Latest Update**. QOSMOS and **History** table will be updated.

Figure 24 : Configuring Application Protocol Update


Not secure 192.168.216.194/gui/#/security/firewall/application_protocol_update/
A10
Dashboard
Rulesets
Zones
Objects
Statistics
Configure
Session
Log
Settings
Logging
Application Protocol Update
Security / Firewall / Configure / Application Protocol Update
Clear
Current time
Update
Check Now

Appplication Protocol Update

Schedule ⊟

Period

○ Daily ● Weekly

Weekly Day

Monday ▾

Time

HH:mm

Use Management Port

☑

Proxy Server

☑

Auth Type

● NTLM ○ Basic

HTTPS Port

1 - 65535 number

User Name

1 - 127 characters. Allow : - _ . and alphanumerics.

Password

1 - 127 characters

Proxy Host

1 - 127 characters. Allow : - _ . and alphanumerics.

Lastest Update

Feature Name	Version	Schedule	Time	Last Updated	Next Check	
app-fw	1.340.0-28	N/A	N/A	N/A	N/A	Check Now

Manual Update

You can manually update a feature (for example, application aware firewall) to the latest version through the ACOS CLI. Login to CLI interface and setup the manual updates for particular features using operational commands. It is possible to check for updates available for a feature, revert to a previous version, or to manually reset software to a default version.

Manual Update Configuration

- To manually upgrade software to the latest version use the following command:

```
ACOS (shared)# automatic-update check-now app-fw
```

- To manually revert software to previous successfully installed version:

```
ACOS (shared)# automatic-update revert app-fw
```

- To manually reset software to default version:

```
ACOS (shared)# automatic-update reset app-fw
```

Application Aware Firewall Logging and Reporting

Application aware firewall can identify data traffic that flows through, from the Internet. The user can view the traffic logs and analysis reports. The application aware firewall session information is stored in a database. The following logging and reporting features are provided:

- Basic log storage,
- Basic filtered log search and retrieval,
- Top N analysis based on the log content.

By default, the local log for Application Aware Firewall is disabled. Use the `fw local-logging` CLI command to enable local log.

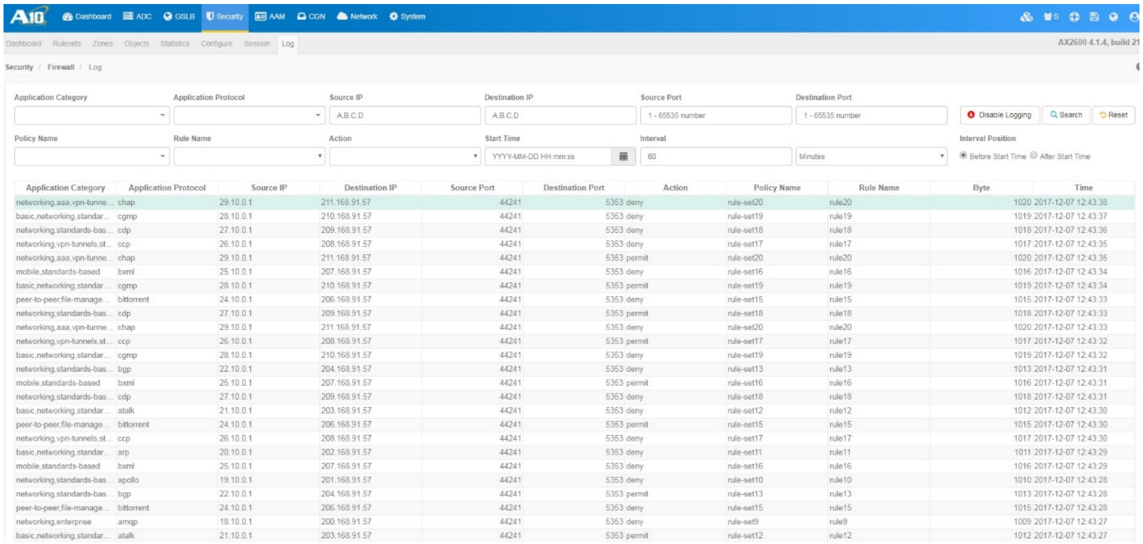
The following topics are covered:

Application Aware Firewall Report

An application aware firewall data traffic analysis report is generated from the traffic log. The following image shows the log report.

NOTE: GUI firewall logs page does not display IPv6 traffic.

Figure 25 : Application Aware Firewall Log Report



Application Category:
Application Protocol:
Source IP: A.B.C.D
Destination IP: A.B.C.D
Source Port: 1 - 65535 number
Destination Port: 1 - 65535 number
Policy Name:
Rule Name:
Action:
Start Time: YYYY-MM-DD HH:mm:ss
Interval: 60 Minutes
Interval Position: ● Before Start Time ○ After Start Time

Application Category	Application Protocol	Source IP	Destination IP	Source Port	Destination Port	Action	Policy Name	Rule Name	Byte	Time
networking,aaa,vpn-tunne...	chap	29.10.0.1	211.168.91.57	44241	5353	deny	rule-set20	rule20	1020	2017-12-07 12:43:38
basic,networking,standar...	cgmp	28.10.0.1	210.168.91.57	44241	5353	deny	rule-set19	rule19	1019	2017-12-07 12:43:37
networking,standards-bas...	cdp	27.10.0.1	209.168.91.57	44241	5353	deny	rule-set18	rule18	1018	2017-12-07 12:43:36
networking,vpn-tunnels,st...	ccp	26.10.0.1	208.168.91.57	44241	5353	deny	rule-set17	rule17	1017	2017-12-07 12:43:35
networking,aaa,vpn-tunne...	chap	29.10.0.1	211.168.91.57	44241	5353	permit	rule-set20	rule20	1020	2017-12-07 12:43:35
mobile,standards-based	bxml	25.10.0.1	207.168.91.57	44241	5353	deny	rule-set16	rule16	1016	2017-12-07 12:43:34
basic,networking,standar...	cgmp	28.10.0.1	210.168.91.57	44241	5353	permit	rule-set19	rule19	1019	2017-12-07 12:43:34
peer-to-peer,file-manage...	bittorrent	24.10.0.1	206.168.91.57	44241	5353	deny	rule-set15	rule15	1015	2017-12-07 12:43:33
networking,standards-bas...	cdp	27.10.0.1	209.168.91.57	44241	5353	permit	rule-set18	rule18	1018	2017-12-07 12:43:33
networking,aaa,vpn-tunne...	chap	29.10.0.1	211.168.91.57	44241	5353	deny	rule-set20	rule20	1020	2017-12-07 12:43:33
networking,vpn-tunnels,st...	ccp	26.10.0.1	208.168.91.57	44241	5353	permit	rule-set17	rule17	1017	2017-12-07 12:43:32
basic,networking,standar...	cgmp	28.10.0.1	210.168.91.57	44241	5353	deny	rule-set19	rule19	1019	2017-12-07 12:43:32
networking,standards-bas...	bgp	22.10.0.1	204.168.91.57	44241	5353	deny	rule-set13	rule13	1013	2017-12-07 12:43:31
mobile,standards-based	bxml	25.10.0.1	207.168.91.57	44241	5353	permit	rule-set16	rule16	1016	2017-12-07 12:43:31
networking,standards-bas...	cdp	27.10.0.1	209.168.91.57	44241	5353	deny	rule-set18	rule18	1018	2017-12-07 12:43:31
basic,networking,standar...	atalk	21.10.0.1	203.168.91.57	44241	5353	deny	rule-set12	rule12	1012	2017-12-07 12:43:30
peer-to-peer,file-manage...	bittorrent	24.10.0.1	206.168.91.57	44241	5353	permit	rule-set15	rule15	1015	2017-12-07 12:43:30
networking,vpn-tunnels,st...	ccp	26.10.0.1	208.168.91.57	44241	5353	deny	rule-set17	rule17	1017	2017-12-07 12:43:30
basic,networking,standar...	arp	20.10.0.1	202.168.91.57	44241	5353	deny	rule-set11	rule11	1011	2017-12-07 12:43:29
mobile,standards-based	bxml	25.10.0.1	207.168.91.57	44241	5353	deny	rule-set16	rule16	1016	2017-12-07 12:43:29
networking,standards-bas...	apollo	19.10.0.1	201.168.91.57	44241	5353	deny	rule-set10	rule10	1010	2017-12-07 12:43:28
networking,standards-bas...	bgp	22.10.0.1	204.168.91.57	44241	5353	permit	rule-set13	rule13	1013	2017-12-07 12:43:28
peer-to-peer,file-manage...	bittorrent	24.10.0.1	206.168.91.57	44241	5353	deny	rule-set15	rule15	1015	2017-12-07 12:43:28
networking,enterprise	amqp	18.10.0.1	200.168.91.57	44241	5353	deny	rule-set9	rule9	1009	2017-12-07 12:43:27
basic,networking,standar...	atalk	21.10.0.1	203.168.91.57	44241	5353	permit	rule-set12	rule12	1012	2017-12-07 12:43:27

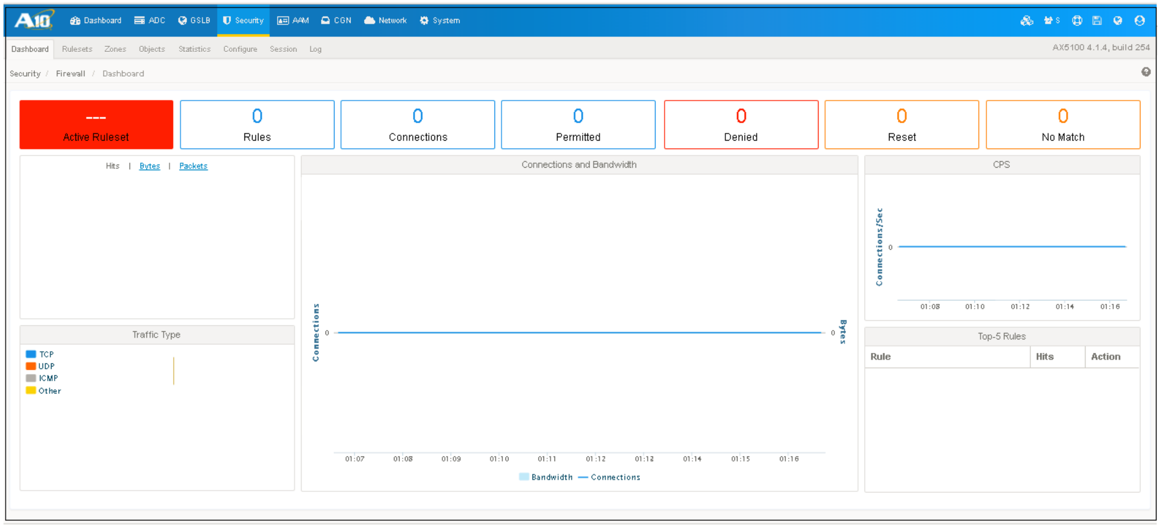
Security Firewall Dashboard

Navigate to **Security** > **Firewall** > **Dashboard**. The dashboard displays the data and analysis reports related to application aware firewall. If the related license is not activated, the dashboard is empty. If the license is active, data analysis charts are shown. You can change the time value for a bar chart and get reports for different values of time.

The following topics are covered:

The values and charts are updated every 10 seconds.

Figure 26 : Application Aware Firewall Dashboard without active License



Security and Application Aware Firewall Dashboard

Login to GUI and navigate to **Security > Firewall > Dashboard** to view data analytics and firewall statistics after application aware firewall license is enabled.

The **Firewall Dashboard** displays all the important firewall statistics and data charts.

Top N Chart on Application Aware Firewall Dashboard

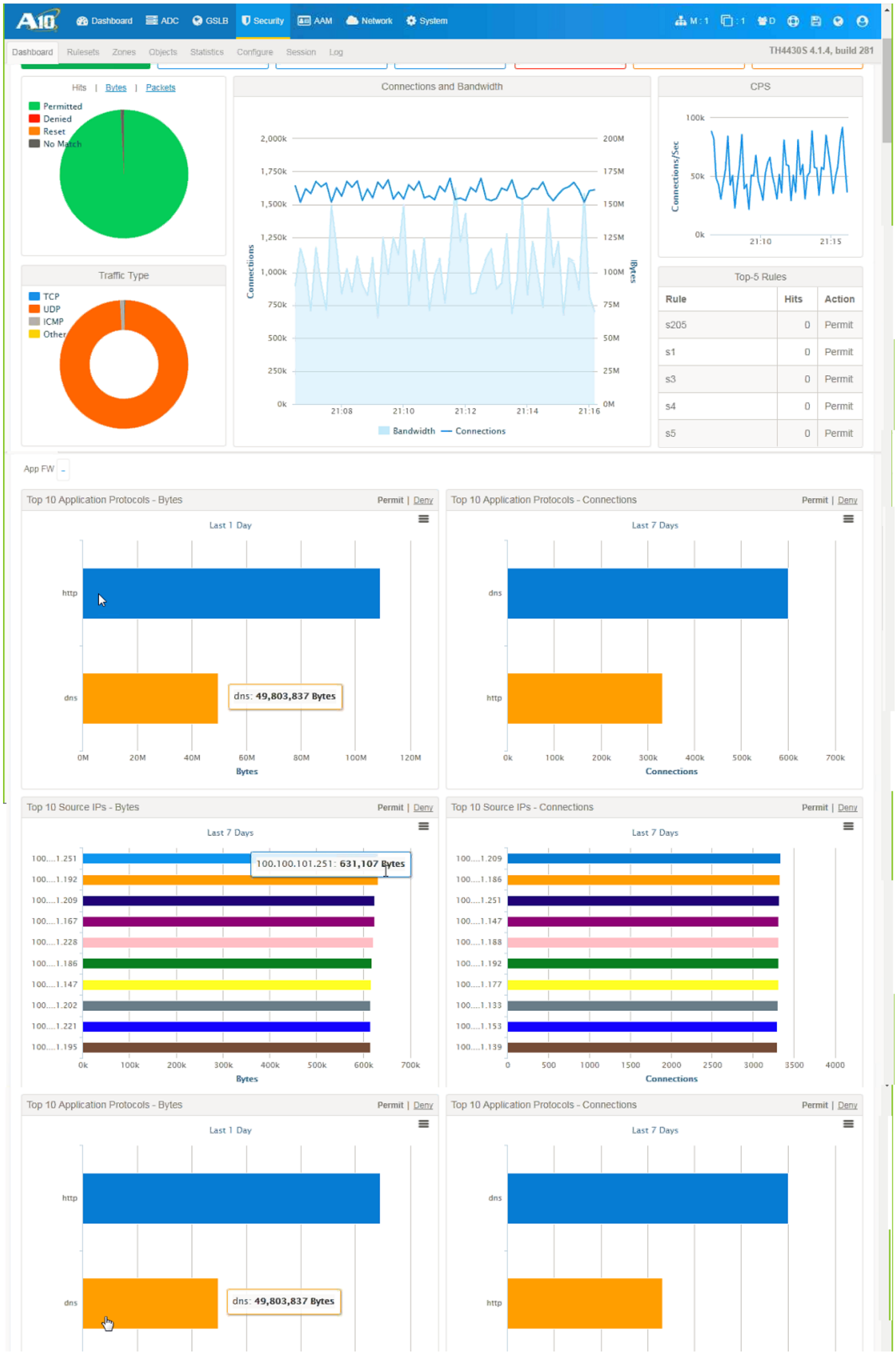
- To set the Top N bar chart to be visible on dashboard, goto the CLI prompt and configure the CLI as follows:

```
ACOS# logging.local-log.app-fw.top-n
ACOS# rba user steven
ACOS# partition shared
ACOS# logging.local-log.app-fw.top-n read
```

- Navigate to the **Application Firewall** drop down and click to open the dashboard. The **Application Firewall** dashboard displays the **Top N Charts**.

The following image illustrates the firewall dashboard with application aware firewall license activated; with all the related application statistics and Top N Charts in the **Application Firewall** dashboard.

Figure 27 : Application Firewall Dashboard



Rule	Hits	Action
s205	0	Permit
s1	0	Permit
s3	0	Permit
s4	0	Permit
s5	0	Permit

Configuration Example

The following topics are covered:

Configuring an Application Aware Firewall

1. Activate the CFW license on ACOS device.
2. Verify that the application aware firewall is activated and the protocol bundle is installed, using the `show license-info` command.
   #include o/p
3. In CLI goto **config**; the global configuration commands. Goto `appfw rule-set`
4. Use `show run | sec` to view if check the GLM server connection options.
5. Use `show cpu overall` to view data statistics through CLI.
6. Update the protocol bundle application protocols through the management port using `automatic-update` commands:

   ```
   ACOS (config)# automatic-update app-fw schedule daily 12:00
   ACOS (config)# automatic-update app-fw schedule weekly ?
   ```

   Check the automatic update settings using:

   ```
   ACOS (shared)# show run automatic-update use-mgmt-port
   ```

   Alternatively, to perform manual application protocols update, use the command :

   ```
   ACOS (shared)# automatic-update check-now app-fw
   ```

7. Configure the rule-set
8. Track the application
9. Enable local logging using the following command to log the application aware firewall statistics:

   ```
   ACOS (config)# fw local-logging
   ```

10. Use the `show rule-set application` command to view the rule-set statistics for an application, based on the protocol or category.

NOTE: On Multi-PU platforms, the statistics display aggregated counters of PU1 and PU2 (PU1 + PU2).

Configuring Rule-set and Rules

The following topics are covered:

Permissive Configuration

1. Create a rule-set called rs1.

```
ACOS(config)# rule-set rs1
```

2. Configure a rule called dns that allows dns traffic for application type protocol.

```
ACOS(config-rule set:rs1)# rule dns
ACOS(config-rule set:rs1-rule:dns)# action permit
ACOS(config-rule set:rs1-rule:dns)# application protocol dns
ACOS(config-rule set:rs1-rule:dns)# end
```

3. Similarly create the following rules.

```
ACOS(config-rule set:rs1)# rule spotify
ACOS(config-rule set:rs1-rule:spotify)# action deny log
ACOS(config-rule set:rs1-rule:spotify)# application protocol spotify
ACOS(config-rule set:rs1-rule:spotify)#end

ACOS(config-rule set:rs1)# rule im
ACOS(config-rule set:rs1-rule:im)# disable
ACOS(config-rule set:rs1-rule:im)# action deny log
ACOS(config-rule set:rs1-rule:im)# application category instant-
messaging
ACOS(config-rule set:rs1-rule:im)# end
```

NOTE: The above rule blocks all instant messaging including Skype, Facebook Mesenger, and Gtalk.

```
ACOS(config-rule set:rs1)# rule skype
ACOS(config-rule set:rs1-rule:im)# action deny log
ACOS(config-rule set:rs1-rule:im)# application protocol skype
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule skype-biz
ACOS(config-rule set:rs1-rule:im)# action deny log
ACOS(config-rule set:rs1-rule:im)# application protocol lync_online
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule fb-web
ACOS(config-rule set:rs1-rule:im)# action deny log
ACOS(config-rule set:rs1-rule:im)# application protocol facebook
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule fb-messenger
ACOS(config-rule set:rs1-rule:im)# action deny log
ACOS(config-rule set:rs1-rule:im)# application protocol facebook_
messenger
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule fb-video
ACOS(config-rule set:rs1-rule:im)# action deny log
ACOS(config-rule set:rs1-rule:im)# application protocol facebook_video
ACOS(config-rule set:rs1-rule:im)# end
```

NOTE: The fb-web rule needs to be allowed for the fb-video rule to work.

```
ACOS(config-rule set:rs1)# rule youtube
ACOS(config-rule set:rs1-rule:im)# action deny log
ACOS(config-rule set:rs1-rule:im)# application protocol youtube
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule gmail
ACOS(config-rule set:rs1-rule:im)# action deny log
ACOS(config-rule set:rs1-rule:im)# application protocol gmail
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule win-app-store
ACOS(config-rule set:rs1-rule:im)# action deny log
ACOS(config-rule set:rs1-rule:im)# application protocol windows_
marketplace
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule xbox
ACOS(config-rule set:rs1-rule:im)# action deny log
ACOS(config-rule set:rs1-rule:im)# application protocol xbox
ACOS(config-rule set:rs1-rule:im)# application protocol xboxlive
ACOS(config-rule set:rs1-rule:im)# application protocol xboxlive_
marketplace
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule default
ACOS(config-rule set:rs1-rule:im)# action permit log
```

Restrictive Configuration

1. Create a rule-set called rs1

```
ACOS(config)# rule-set rs1
```

2. Configure a rule called dns that allows dns traffic for application type protocol.

```
ACOS(config-rule set:rs1)# rule dns
ACOS(config-rule set:rs1-rule:dns)# action permit
ACOS(config-rule set:rs1-rule:dns)# application protocol dns
ACOS(config-rule set:rs1-rule:dns)# end
```

3. Similarly create the following rules.

```
ACOS(config-rule set:rs1)# rule spotify
ACOS(config-rule set:rs1-rule:spotify)# action permit log
ACOS(config-rule set:rs1-rule:spotify)# application protocol spotify
ACOS(config-rule set:rs1-rule:spotify)#end

ACOS(config-rule set:rs1)# rule dropbox
ACOS(config-rule set:rs1-rule:im)# action permit log
ACOS(config-rule set:rs1-rule:im)# application protocol dropbox
ACOS(config-rule set:rs1-rule:im)# end
```

NOTE: The following rule allows skype only if microsoft and windowslive are logged in.

```
ACOS(config-rule set:rs1)# rule skype
ACOS(config-rule set:rs1-rule:im)# action permit log
ACOS(config-rule set:rs1-rule:im)# application protocol skype
ACOS(config-rule set:rs1-rule:im)# application protocol microsoft
ACOS(config-rule set:rs1-rule:im)# application protocol windowslive
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule skype-biz
ACOS(config-rule set:rs1-rule:im)# action permit log
ACOS(config-rule set:rs1-rule:im)# application protocol lync_online
ACOS(config-rule set:rs1-rule:im)# application protocol microsoft
ACOS(config-rule set:rs1-rule:im)# application protocol office365
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule fb-web
ACOS(config-rule set:rs1-rule:im)# action permit log
ACOS(config-rule set:rs1-rule:im)# application protocol facebook
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule fb-messenger
ACOS(config-rule set:rs1-rule:im)# action permit log
ACOS(config-rule set:rs1-rule:im)# application protocol facebook_
messenger
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule fb-video
ACOS(config-rule set:rs1-rule:im)# action permit log
ACOS(config-rule set:rs1-rule:im)# application protocol facebook_video
ACOS(config-rule set:rs1-rule:im)# end
```

NOTE: The fb-web rule needs to be allowed for the fb-video rule to work.

```
ACOS(config-rule set:rs1)# rule youtube
ACOS(config-rule set:rs1-rule:im)# action permit log
ACOS(config-rule set:rs1-rule:im)# application protocol youtube
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule gmail
ACOS(config-rule set:rs1-rule:im)# action permit log
ACOS(config-rule set:rs1-rule:im)# application protocol gmail
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule win-app-store
ACOS(config-rule set:rs1-rule:im)# action permit log
ACOS(config-rule set:rs1-rule:im)# application protocol windows_
marketplace
ACOS(config-rule set:rs1-rule:im)# application protocol windowslive
ACOS(config-rule set:rs1-rule:im)# application protocol microsoft
ACOS(config-rule set:rs1-rule:im)# application protocol windows_update
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule xbox
ACOS(config-rule set:rs1-rule:im)# action permit log
ACOS(config-rule set:rs1-rule:im)# application protocol xbox
ACOS(config-rule set:rs1-rule:im)# application protocol xboxlive
ACOS(config-rule set:rs1-rule:im)# application protocol xboxlive_
marketplace
ACOS(config-rule set:rs1-rule:im)# application protocol windowslive
ACOS(config-rule set:rs1-rule:im)# end

ACOS(config-rule set:rs1)# rule default
ACOS(config-rule set:rs1-rule:im)# action deny log
```

Data Center Firewall

This section provides an example of a Data Center Firewall deployment.

The following topics are covered:

Data Center Firewall Overview

Benefits of DCFW

Data centers firewalls offer a wide range of services for a variety of applications, such as HTTP, mobile, Voice over IP (VoIP), streaming video, not to mention the needs of mobile users and social media. To meet the growing demand for such a wide array of services and applications, data centers require tremendous scalability and throughput.

To achieve this high scalability, and in order to make packet classification decisions faster and simpler, the ACOS data center firewall device offers a Layer 4 stateful DCFW.

The DCFW has a highly scalable classification algorithm which can reduce the burden placed on other backend services. The firewall provides a layer of security prior to traffic reaching the load balancer (SLB device), and it offers the benefits of consolidating functions in one device.

DCFW Features

The list below highlights the features that are specific to data center firewalls:

- The data center firewall supports SLB topologies.
- The data center firewall supports common event format (CEF) logging. When the firewall applies an action (deny/reset/permit) to a new connection request, a log is generated.
- The data center firewall can be deployed within application delivery partitions (ADP/L3V).
- The data center firewall supports up to eight devices in a VRRP-A cluster for high availability.
- The data center firewall supports rule matching based on priority.

- The data center firewall supports up to 128k rules in a rule-set, on high-end platforms.
- The data center firewall uses existing ACL configuration objects (for example, obj-group).
- The data center firewall support for Named Objects, such as SLB VIPs and real servers.
- The data center firewall supports rule-based statistics.

Known Issues for DCFW

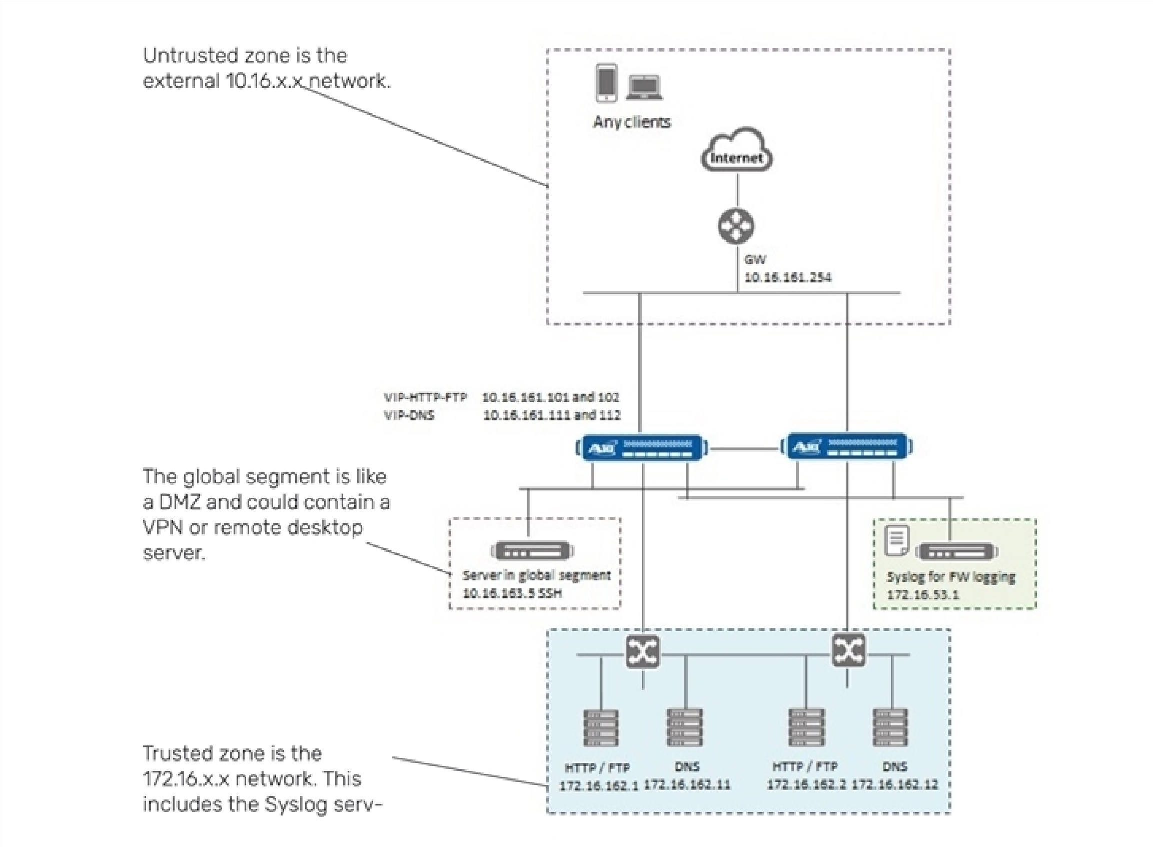
Below are limitations or known issues associated with the data center firewall feature:

- In previous releases, Firewall Logging offers support for logging additional parameters, such as:
  – RADIUS logs
  – HTTP header logs
  – Merged mode (one consolidated log for opening and closing the same session)
  – Non-merged mode (separate log messages for open session and closed session)
  These additional logging parameters are not yet supported in the new ACOS event-based logging infrastructure, so it is recommended that if your deployment requires these extra logging parameters, you should continue to use Firewall logging. (Bug 462172)
- DCFW will always takes precedence over other security configurations, such as ACL, NAT, and so on. (Bug 301153)
- Only one firewall rule-set (or “policy”) can be attached globally, or to a zone or interface.
- Destination Zone for SLB VIP traffic is always “any”.
- VLAN or Virtual Ethernet configurations in one zone cannot be re-used in another zone.
- When a DCFW rule-set is activated, it takes about 10 seconds for the rule-set to become activated.
- Layer 2 DCFW setup requires a rule to allow Link-Local address.

Sample Topology for DCFW

Figure 28 illustrates the topology for a basic sample use case of DC Firewall with an SLB deployment.

Figure 28 : Sample Data Center Firewall topology diagram for basic use case (FW + SLB)


Untrusted zone is the external 10.16.x.x network.
Any clients
Internet
GW
10.16.161.254
VIP-HTTP-FTP 10.16.161.101 and 102
VIP-DNS 10.16.161.111 and 112
A10
A10
The global segment is like a DMZ and could contain a VPN or remote desktop server.
Server in global segment
10.16.163.5 SSH
Syslog for FW logging
172.16.53.1
HTTP / FTP
172.16.162.1
DNS
172.16.162.11
HTTP / FTP
172.16.162.2
DNS
172.16.162.12
Trusted zone is the 172.16.x.x network. This includes the Syslog serv-

NOTE:

- The “untrusted zone” is the external network, near the top of the diagram, while the “trusted zone” is the internal network, near the bottom of the diagram, and includes the syslog servers.
- The middle contains a “global segment” (DMZ) with an SSH-based server (e.g., VPN or RDP) for remote access.
- See DC Firewall Configuration with SLB Deployment for the CLI commands used to configure the Data Center Firewall in this environment.

DC Firewall Configuration with SLB Deployment

The section below describes the process required to configure DCFW in a simple deployment consisting of Firewall + SLB.

Configuration Steps at a High Level

The high-level steps to setting up a basic data center firewall deployment (FW with SLB). More granular instructions can be found in the CLI sample configuration below.

1. Set up the interfaces, VLANs and ACLs configurations.
2. (Optional) Perform VRRP-A configurations if high availability is needed for multiple ACOS device(s).
3. Set up the real servers, service groups, and VIPs (for SLB deployment).
4. (Optional) Create a zone for the firewall, which may include the physical interface (s) of the ACOS device.
5. Create a network object-group for specifying match criteria using Layer 3 parameters that will be used for IPv4 firewall configurations.
6. Create a service object group for specifying matching match criteria using Layer 4 to layer 7 parameters.
7. Configure a firewall rule-set that contains a set of rules. Rules should contain the match criteria and associated action.
8. Activate the rule-set with the “fw active-rule-set” command.

Configuration Steps at a Low Level

The steps above offer a high-level list of tasks that need to be performed to set up the DC Firewall. However, the steps below provide a more granular view of the CLI commands that must be used to configure DC Firewall within an SLB deployment.

1. Configure the ACLs to allow traffic to pass from the internal DNS servers at “172.16.162.11” and “172.16.162.12” to reach the external “10.16.x.x” network. The ACL is set up to deny any other traffic from this network.

```
ACOS(config)# access-list 101 permit ip host 172.16.162.11 any
ACOS(config)# access-list 101 permit ip host 172.16.162.12 any
ACOS(config)# access-list 101 deny ip any any
```

2. Use the “multi-config” command to support several simultaneous administrative sessions. The “terminal” command sets the terminal parameters for the CLI session. In the example below, the timeout is set to “0”, meaning the session will not timeout.

```
ACOS(config)# multi-config enable
ACOS(config)# terminal idle-timeout 0
```

3. Create a virtual LAN and specify the VLAN ID number using the “vlan” command. The VLAN configuration includes the tagged and untagged ports assigned to the VLAN, as well as the virtual ethernet router, which is configured under the interface parameters.

```
ACOS(config)# vlan 21
ACOS(config-vlan:21)# tagged ethernet 16
ACOS(config-vlan:21)# router-interface ve 21
ACOS(config-vlan:21)# exit
ACOS(config)# vlan 53
ACOS(config-vlan:53)# tagged ethernet 16
ACOS(config-vlan:53)# router-interface ve 53
ACOS(config-vlan:53)# exit
ACOS(config)# vlan 99
ACOS(config-vlan:99)# untagged ethernet 1
ACOS(config-vlan:99)# router-interface ve 99
ACOS(config-vlan:99)# exit
ACOS(config)# vlan 161
ACOS(config-vlan:161)# untagged ethernet 1
ACOS(config-vlan:161)# router-interface ve 99
ACOS(config-vlan:161)# exit
ACOS(config)# vlan 161
ACOS(config-vlan:161)# tagged ethernet 15
ACOS(config-vlan:161)# router-interface ve 161
ACOS(config-vlan:161)# exit
ACOS(config)# vlan 162
ACOS(config-vlan:162)# tagged ethernet 16
ACOS(config-vlan:162)# router-interface ve 162
ACOS(config-vlan:162)# exit
ACOS(config)# vlan 163
ACOS(config-vlan:163)# tagged ethernet 16
ACOS(config-vlan:163)# router-interface ve 163
ACOS(config-vlan:163)# exit
```

4. Configure the host name for the ACOS device.

```
ACOS(config)# hostname ACOS
```

5. Configure the management interface with the desired IP and gateway.

```
ACOS(config)# interface management
ACOS(config-if:management)# ip address 192.168.229.16 255.255.255.0
ACOS(config-if:management)# ip default-gateway 192.168.229.1
ACOS(config-if:management)# exit
```

6. Use the “interface ethernet” command to configure the physical interfaces on the device. In the example below, ethernet ports 1, 15, and 16 are enabled, while the remaining interfaces are not.

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# exit
ACOS(config)# interface ethernet 15
ACOS(config-if:ethernet:15)# enable
ACOS(config-if:ethernet:15)# exit
ACOS(config)# interface ethernet 16
ACOS(config-if:ethernet:16)# enable
ACOS(config-if:ethernet:16)# exit
```

7. Assign IP addresses to the VLANs using the “Virtual Ethernet (VE)” command.

```
ACOS(config)# interface ve 21
ACOS(config-if:ve:21)# ip address 21.0.255.243 255.255.0.0
ACOS(config-if:ve:21)# exit
ACOS(config)# interface ve 53
ACOS(config-if:ve:53)# ip address 172.16.53.243 255.255.255.0
ACOS(config-if:ve:53)# exit
ACOS(config)# interface ve 99
ACOS(config-if:ve:99)# ip address 172.16.99.243 255.255.255.0
ACOS(config-if:ve:99)# exit
ACOS(config)# interface ve 161
ACOS(config-if:ve:161)# ip address 10.16.161.243 255.255.255.0
ACOS(config-if:ve:161)# exit
ACOS(config)# interface ve 162
ACOS(config-if:ve:162)# ip address 172.16.162.243 255.255.255.0
ACOS(config-if:ve:162)# exit
ACOS(config)# interface ve 163
ACOS(config-if:ve:163)# ip address 10.16.163.243 255.255.255.0
ACOS(config-if:ve:163)# exit
```

8. Enable VRRP-A for the first ACOS DC firewall device. Set the device-id to 1, and the set-id for the pair to 5. Then, enable VRRP-A on the device using the “enable” command.

```
ACOS(config)# vrrp-a common
ACOS(config-common)# device-id 1
ACOS(config-common)# set-id 5
ACOS(config-common)# enable
```

9. The commands below configure VRRP-A for high availability, which can support up to 8 redundant devices.

   In the sample configuration below, we have configured several floating IPs to allow connectivity to the ACOS devices from the external clients, the server in the global segment, the syslog for FW logging server, and the HTTP/FTP and DNS servers on the internal network. The floating IPs can help provide network stability by moving to the active device in the pair. Tracking options are used at the blade level to dynamically reduce the priority value during failover.

```
ACOS(config)# vrrp-a vrid 1
ACOS(config-vrid:1)# floating-ip 172.16.162.244  <-- for internal
HTTP/FTP/DNS servers
ACOS(config-vrid:1)# floating-ip 10.16.161.244  <-- for external
(untrusted) clients
```

```
ACOS(config-vrid:1)# floating-ip 172.16.53.244 <-- for syslog external
server
ACOS(config-vrid:1)# floating-ip 10.16.163.244 <-- for global segment
(VPN/RDP server)
ACOS(config-vrid:1)# blade-parameters
ACOS(config-vrid:1-blade-parameters)# tracking-options
ACOS(config-vrid:1-blade-parameters-track...)# interface ethernet 15 priority-cost
100
ACOS(config-vrid:1-blade-parameters-track...)# interface ethernet 16
priority-cost 100
ACOS(config-vrid:1-blade-parameters-track...)# exit
```

10. The first command below configures the NAT pool “p1” with one IP address (“10.16.161.201”), which is the IP that the internal HTTP/FTP or DNS servers will use to reach the external network. The second command binds the pool “p1” to ACL “101”.

```
ACOS(config)# ip nat pool p1 10.16.161.201 10.16.161.201 netmask /24
gateway 10.16.161.254 vrid 1
ACOS(config)# ip nat inside source list 101 pool p1
```

11. The following command configures ethernet interface 1 as the VRRP-A interface, through which the device can be reached for high availability synchronization.

```
ACOS(config)# vrrp-a interface ethernet 1
ACOS(config-ethernet:1)# exit
```

12. The command below configures a route from the internal HTTP/FTP/DNS servers to the external network.

```
ACOS(config)# ip route 0.0.0.0 /0 10.16.161.254
```

13. The following commands are used to add the VLANs created above to zones. The zones can contain an interface or a VLAN. Rather than adding all four VLANs to the same zones, an individual zone is created for each VLAN. These zones will later be added to firewall rules as match criteria.

```
ACOS(config)# zone HA
ACOS(config-zone:zone-HA)# interface ethernet 1
ACOS(config-zone:zone-HA)# interface ve 99
ACOS(config-zone:zone-HA)# exit
ACOS(config)# zone Trust_Vlan_162
ACOS(config-zone:zone-Trust_Vlan_162)# vlan 162
ACOS(config-zone:zone-Trust_Vlan_162)# exit
ACOS(config)# zone Trust_Vlan_53
ACOS(config-zone:zone-Trust_Vlan_53)# vlan 53
ACOS(config-zone:zone-Trust_Vlan_53)# exit
ACOS(config)# zone Untrust
ACOS(config-zone:zone-Untrust)# vlan 161
ACOS(config-zone:zone-Untrust)# exit
ACOS(config)# zone dmz
ACOS(config-zone:zone-dmz)# vlan 163
ACOS(config-zone:zone-dmz)# exit
```

14. The following commands configure the real server “s001” and “s002”, with TCP on ports 80 and 21 (for HTTP and FTP). The next two servers, “s011” and “s012” are configured with port 53 (for DNS).

```
ACOS(config)# slb server s001 172.16.162.1
ACOS(config-real server)# port 21 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit

ACOS(config)# slb server s002 172.16.162.2
ACOS(config-real server)# port 21 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit

ACOS(config)# slb server s011 172.16.162.11
ACOS(config-real server)# port 53 udp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit

ACOS(config)# slb server s012 172.16.162.12
ACOS(config-real server)# port 53 udp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
```

15. The following commands configure service group “sg-1” (with real server “s001”

and “s002” at port 80 for TCP/HTTP), “sg-2” (with real server “s001” and “s002” at port 21 for TCP/FTP), and “sg-3” (with real servers “s011” and “s012” at port 53 for UDP/DNS traffic).

```
ACOS(config)# slb service-group sg-1 tcp
ACOS(config-slb svc group)# member s001 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member s002 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# exit

ACOS(config)# slb service-group sg-2 tcp
ACOS(config-slb svc group)# member s001 21
ACOS(config-slb svc group-member:21)# exit
ACOS(config-slb svc group)# member s002 21
ACOS(config-slb svc group-member:21)# exit
ACOS(config-slb svc group)# exit

ACOS(config)# slb service-group sg-3 udp
ACOS(config-slb svc group)# member s011 53
ACOS(config-slb svc group-member:53)# exit
ACOS(config-slb svc group)# member s012 53
ACOS(config-slb svc group-member:53)# exit
ACOS(config-slb svc group)# exit
```

16. The following commands are used to create virtual servers “vip-161.111” and “vip-162.112” on the ACOS device. The VIPs are intended to handle DNS requests. Next, we assign “VRID 1” to both VIPs to create a logical binding for the shared VRRP-A elements. Similarly, we conifigure “vip-161.101” at (.111) and “vip-161.102” to handle HTTP and FTP traffic.

```
ACOS(config)# slb virtual-server vip-161.111_dns 10.16.161.111
ACOS(config-slb vserver)# vrid 1
ACOS(config-slb vserver)# port 53 dns-udp
ACOS(config-slb vserver-vport)# service-group sg-3
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit

ACOS(config)# slb virtual-server vip-161.112_dns 10.16.161.112
ACOS(config-slb vserver)# vrid 1
ACOS(config-slb vserver)# port 53 dns-udp
ACOS(config-slb vserver-vport)# service-group sg-3
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit

ACOS(config)# slb virtual-server vip_161.101_http_ftp 10.16.161.101
ACOS(config-slb vserver)# vrid 1
ACOS(config-slb vserver)# port 21 ftp
ACOS(config-slb vserver-vport)# ha-conn-mirror
ACOS(config-slb vserver-vport)# service-group sg-2
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# ha-conn-mirror
ACOS(config-slb vserver-vport)# service-group sg-1
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit

ACOS(config)# slb virtual-server vip_161.102_http_ftp 10.16.161.102
ACOS(config-slb vserver)# vrid 1
ACOS(config-slb vserver)# port 21 ftp
ACOS(config-slb vserver-vport)# ha-conn-mirror
ACOS(config-slb vserver-vport)# service-group sg-2
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# ha-conn-mirror
ACOS(config-slb vserver-vport)# service-group sg-1
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

17. Next, configure the syslog server at (53.1), and set the severity level for sent logs to “information” and above.

```
ACOS(config)# logging syslog information
ACOS(config)# logging host 172.16.53.1
```

18. Configure the network objects, which for use as the match criteria in the rules. As shown by the prefix in the object name (“obj_sv”), we are configuring network objects to represent the servers on the internal “172.16.x.x” network. We also configure network objects to represent the server in the DMZ and the VIPs on the

ACOS devices.

```
ACOS(config)# object network obj_sv_162.11_dns
ACOS(config-network:obj_sv_162.11_dn)# 172.16.162.11/32
ACOS(config-network:obj_sv_162.11_dn)# exit
ACOS(config)# object network obj_sv_162.12_dns
ACOS(config-network:obj_sv_162.12_dn)# 172.16.162.12/32
ACOS(config-network:obj_sv_162.12_dn)# exit

ACOS(config)# object network obj_sv_162.1_http_ftp
ACOS(config-network:obj_sv_162.1_ht)# 172.16.162.1/32
ACOS(config-network:obj_sv_162.1_ht)# exit

ACOS(config)# object network obj_sv_162.2_http_ftp
ACOS(config-network:obj_sv_162.2_ht)# 172.16.162.2/32
ACOS(config-network:obj_sv_162.2_ht)# exit

ACOS(config)# object network obj_sv_163.5_ssh
ACOS(config-network:obj_sv_163.5_ssh)# 10.16.163.5/32
ACOS(config-network:obj_sv_163.5_ssh)# exit

ACOS(config)# object network obj_sv_161.101_http_ftp
ACOS(config-network:obj_sv_161.101_ht)# 10.16.161.101/32
ACOS(config-network:obj_sv_161.101_ht)# exit

ACOS(config)# object network obj_sv_161.102_http_ftp
ACOS(config-network:obj_sv_161.102_ht)# 10.16.161.102/32
ACOS(config-network:obj_sv_161.102_ht)# exit
```

19. Next, create the network object groups for the server objects and VIP objects. Note the “firewall” keyword, designates that this object belongs to a firewall and not an ACL. Additionally, the “v4” keyword identifies this as an IPv4 object, as opposed to IPv6.

```
ACOS(config)# object-group network objg_sv_dns fw v4
ACOS(config-network:objg_sv_dns)# object obj_sv_162.11_dns
ACOS(config-network:objg_sv_dns)# object obj_sv_162.12_dns
ACOS(config-network:objg_sv_dns)# exit

ACOS(config)# object-group network objg_sv_http_ftp_tmp fw v4
ACOS(config-network:objg_sv_http_ftp)# virtual-server vip_161.101_http_
ftp
ACOS(config-network:objg_sv_http_ftp)# virtual-server vip_161.102_http_
ftp
ACOS(config-network:objg_http_ftp)# exit

ACOS(config)# object-group network objg_sv_http_ftp fw v4
ACOS(config-network:objg_sv_http_ftp)# object obj_vip_161.101_http_ftp
ACOS(config-network:objg_sv_http_ftp)# object obj_vip_161.102_http_ftp
ACOS(config-network:objg_sv_http_ftp)# exit
```

20. The following commands create an object group for services. While the “network” keyword allows you to specify match criteria based on IP addresses, zones, VIPs and ports, the “services” keyword enables you to specify match criteria for protocols. In the sample below, a match will occur for incoming traffic on TCP/HTTP port 80 or 8080.

```
ACOS(config)# object-group service obj_srv_http
ACOS(config-service:obj_srv_http)# tcp eq 80
ACOS(config-service:obj_srv_http)# tcp eq 8080
ACOS(config-service:obj_srv_http)# exit

ACOS(config)# object-group service obj_srv_ftp
ACOS(config-service:obj_srv_ftp)# tcp eq 21 alg FTP
ACOS(config-service:obj_srv_ftp)# tcp eq 20021 alg FTP
ACOS(config-service:obj_srv_ftp)# exit

ACOS(config)# object-group service obj_srv_dns
ACOS(config-service:obj_srv_dns)# udp eq 53 alg DNS
ACOS(config-service:obj_srv_dns)# tcp eq 53 alg DNS
ACOS(config-service:obj_srv_dns)# exit

ACOS(config)# object-group service obj_srv_ssh
ACOS(config-service:obj_srv_ssh)# tcp eq 22
ACOS(config-service:obj_srv_ssh)# exit
```

21. The command below creates the rule-set “r1” and adds a collections rules named “10”, “15”, “110”, and so on.

Sequence numbers in rules are hidden and non-configurable, but you can change the order in which rules appear in the rule-set using the “insert-rule” option in the CLI or “move rule” option in the GUI. At a more granular level, each rule contains match criteria and an action to be applied to traffic that matches that criterion. For example, within rule “10”, the action is to permit any traffic that matches the match criteria, which screens for traffic from source IP “172.16.99.242/32”, source zone “HA”, and destination IP “224.0.0.210/32”). Traffic will be processed according to the first rule for which there is a positive match.

```
ACOS(config)# rule-set r1
ACOS(config-rule set:r1)# rule 10
ACOS(config-rule set:r1-rule:10)# action permit
ACOS(config-rule set:r1-rule:10)# source ipv4-address 172.16.99.242/32
ACOS(config-rule set:r1-rule:10)# source zone HA
ACOS(config-rule set:r1-rule:10)# dest ipv4-address 224.0.0.210/32
ACOS(config-rule set:r1-rule:10)# exit

ACOS(config-rule set:r1)# rule 15
ACOS(config-rule set:r1-rule:15)# action permit
ACOS(config-rule set:r1-rule:15)# source ipv4-address 172.16.99.242/32
ACOS(config-rule set:r1-rule:15)# source zone HA
ACOS(config-rule set:r1-rule:15)# dest ipv4-address 172.16.99.243/32
ACOS(config-rule set:r1-rule:15)# exit

ACOS(config-rule set:r1)# rule 110
ACOS(config-rule set:r1-rule:110)# action permit log
ACOS(config-rule set:r1-rule:110)# source zone Untrust
ACOS(config-rule set:r1-rule:110)# dest object-group objg_sv_http_ftp
ACOS(config-rule set:r1-rule:110)# service object-group obj_srv_http
ACOS(config-rule set:r1-rule:110)# exit

ACOS(config-rule set:r1)# rule 111
ACOS(config-rule set:r1-rule:111)# action permit log
ACOS(config-rule set:r1-rule:111)# source zone Untrust
ACOS(config-rule set:r1-rule:111)# dest object-group objg_sv_http_ftp
ACOS(config-rule set:r1-rule:111)# service object-group obj_srv_ftp
ACOS(config-rule set:r1-rule:111)# exit

ACOS(config-rule set:r1)# rule 115
ACOS(config-rule set:r1-rule:115)# action permit log
ACOS(config-rule set:r1-rule:115)# source zone Untrust
ACOS(config-rule set:r1-rule:115)# dest virtual-server vip-161.112_dns
ACOS(config-rule set:r1-rule:115)# service object-group obj_srv_dns
ACOS(config-rule set:r1-rule:115)# exit

ACOS(config-rule set:r1)# rule 130
ACOS(config-rule set:r1-rule:130)# action permit log
ACOS(config-rule set:r1-rule:130)# source object-group objg_sv_dns
ACOS(config-rule set:r1-rule:130)# source zone Trust_Vlan_162
ACOS(config-rule set:r1-rule:130)# dest zone Untrust
ACOS(config-rule set:r1-rule:130)# service object-group obj_srv_dns
ACOS(config-rule set:r1-rule:130)# exit

ACOS(config-rule set:r1)# rule 140
ACOS(config-rule set:r1-rule:140)# action permit
ACOS(config-rule set:r1-rule:140)# source zone Trust_Vlan_162
ACOS(config-rule set:r1-rule:140)# dest zone Trust_Vlan_53
ACOS(config-rule set:r1-rule:140)# exit

ACOS(config-rule set:r1)# rule 141
ACOS(config-rule set:r1-rule:141)# action permit
ACOS(config-rule set:r1-rule:141)# source zone Trust_Vlan_53
ACOS(config-rule set:r1-rule:141)# dest zone Trust_Vlan_162
ACOS(config-rule set:r1-rule:141)# exit

ACOS(config-rule set:r1)# rule 150
ACOS(config-rule set:r1-rule:150)# action permit log
ACOS(config-rule set:r1-rule:150)# dest object obj_sv_163.5_ssh
ACOS(config-rule set:r1-rule:150)# service object-group obj_srv_ssh
ACOS(config-rule set:r1-rule:150)# exit
ACOS(config-rule set:r1)# exit
```

22. The command below associates the firewall with the VRID for high availability failover, but it is unrelated to SLB.

```
ACOS(config)# fw vrid 1
```

23. The command below is used to configure a session aging template called “a1”,

within which the idle-timeout values are set for TCP, UDP, and ICMP sessions.

```
ACOS(config)# fw session-aging a1
ACOS(config-session-aging:a1)# tcp idle-timeout 12345
ACOS(config-session-aging:a1)# udp idle-timeout 89
ACOS(config-session-aging:a1)# udp idle-timeout 9
```

24. The command below is used to activate the rule-set “r1”, and simultaneously binds the session-aging template “a1” to this rule-set.

```
ACOS(config)# fw active-rule-set r1 session-aging a1
```

Data Center Firewall on Multi-PU Platforms

On Multi-PU platforms (such as TH14045 or TH7650/TH7655S) the traffic is distributed across multiple Processing Units (multi-PUs) using the client-side IP addresses. The client-side traffic is hashed based on the client's source IP address, and the server-side traffic is hashed based on the destination IP address. This ensures that the traffic belonging to a given session always returns to the same PU.

CLI Configuration

Following are the configuration steps for deploying the Data Center (DC) Firewall on Multi-PU platforms to ensure seamless traffic distribution across PU1 and PU2:

1. Enable the odd-even IP NAT globally using the `odd-even-nat-enable` command.

```
ACOS(config)# slb common
ACOS(config-common)# odd-even-nat-enable
```

2. If you implement source NAT pool configuration, enable port splitting between PU1 and PU2 using the `system chassis-port-split` command.

```
ACOS(config)# system chassis-port-split
```

3. Configure client-side VLAN (or interface ethernet) with traffic distribution mode as **SIP** (source IP address) using the `traffic-distribution-mode` command.

```
ACOS(config)# vlan 10
ACOS(config-vlan:10)# tagged ethernet 1
ACOS(config-vlan:10)# router-interface ve 10
ACOS(config-vlan:10)# traffic-distribution-mode sip
```

4. Configure server-side VLAN (or interface ethernet) with traffic distribution mode as **DIP** (destination IP address) using the `traffic-distribution-mode` command.

```
ACOS(config)# vlan 20
ACOS(config-vlan:20)# tagged ethernet 1
ACOS(config-vlan:20)# router-interface ve 20
ACOS(config-vlan:20)# traffic-distribution-mode dip
```

5. Configure IP NAT pools using the `ip nat pool` or `ipv6 nat pool` commands. The configured NAT pools should have at least two IP addresses in range; one odd and one even IP address.

6. Configure the Threat Intel module (optional step). Configure the threat-lists (`client-threats` and `server-threats`) and later use them effectively in the firewall rules.

   The context of threat-intel is deployed automatically on PU1 and PU2. After receiving data traffic from both PUs, the packets comply with the same rules and perform the same actions. For more information, see Behavior on Multi-PU Platforms

```
ACOS(config)# threat-intel
ACOS(config-threat-intel)# threat-feed webroot
ACOS(config-threat-intel-threat-feed:webr...)# use-mgmt-port
ACOS(config-threat-intel-threat-feed:webr...)# enable

ACOS(config-threat-intel)# threat-list client-threats webroot
ACOS(config-threat-intel-threat-list:client-threats)# all-categories

ACOS(config-threat-intel)# threat-list server-threats webroot
ACOS(config-threat-intel-threat-list:server-threats)# all-categories
```

7. Configure the Firewall Rule sets. Rules should contain the match criteria and associated actions.

```
ACOS(config)# rule-set ti-test
ACOS(config-rule set: ti-test)# rule src-threats
ACOS(config-rule set: ti-test-rule:src-threats)# action deny log
ACOS(config-rule set: ti-test-rule:src-threats)# source ipv4-address
any
```

```
ACOS(config-rule set: ti-test-rule:src-threats)# source zone any
ACOS(config-rule set: ti-test-rule:src-threats)# source threat-list
client-threats
ACOS(config-rule set: ti-test-rule:src-threats)# dest ipv4-address any
ACOS(config-rule set: ti-test-rule:src-threats)# dest zone any
ACOS(config-rule set: ti-test-rule:src-threats)# service any
ACOS(config-rule set: ti-test-rule:src-threats)# application any
ACOS(config-rule set: ti-test-rule:src-threats)# exit

ACOS(config-rule set: ti-test)# rule dest-threats
ACOS(config-rule set: ti-test-rule:dest-threats)# action deny log
ACOS(config-rule set: ti-test-rule:dest-threats)# source ipv4-address
any
ACOS(config-rule set: ti-test-rule:dest-threats)# source zone any
ACOS(config-rule set: ti-test-rule:dest-threats)# dest ipv4-address any
ACOS(config-rule set: ti-test-rule:dest-threats)# dest zone any
ACOS(config-rule set: ti-test-rule:dest-threats)# dest threat-list
server-threats
ACOS(config-rule set: ti-test-rule:dest-threats)# service any
ACOS(config-rule set: ti-test-rule:dest-threats)# application any
ACOS(config-rule set: ti-test-rule:dest-threats)# exit

ACOS(config-rule set: ti-test)# rule default
ACOS(config-rule set: ti-test-rule:default)# action permit log
ACOS(config-rule set: ti-test-rule:default)# source ipv4-address any
ACOS(config-rule set: ti-test-rule:default)# source zone any
ACOS(config-rule set: ti-test-rule:default)# dest ipv4-address any
ACOS(config-rule set: ti-test-rule:default)# dest zone any
ACOS(config-rule set: ti-test-rule:default)# service any
ACOS(config-rule set: ti-test-rule:default)# application any
ACOS(config-rule set: ti-test-rule:default)# exit
```

You can verify the rule-set configuration using the following command:

```
ACOS(config)# show running-config | sec rule
rule-set ti-test
  rule src-threats
    action deny log
    source ipv4-address any
    source zone any
    source threat-list client-threats
    dest ipv4-address any
    dest zone any
    service any
    application any
   rule dest-threats
    action deny log
    source ipv4-address any
    source zone any
    dest ipv4-address any
    dest zone any
    dest threat-list server-threats
    service any
    application any
   rule default
    action permit log
    source ipv4-address any
    source zone any
    dest ipv4-address any
    dest zone any
    service any
    application any
```

8. You can enable application statistics for Application Aware Firewall using the **track-application** rule-set command (optional step). These statistics can be viewed using the **show rule-set application protocol** and **show rule-set application category** commands. On multi-PU platforms, the rule-set statistics display aggregated counters of PU1 and PU2 (PU1 + PU2).

9. You can also configure a firewall logging server, a firewall logging template, and bind the firewall logging template to the firewall.

10. Activate the firewall function using the specified rule-set.

```
ACOS(config)# fw active-rule-set ti-test
```

11. View the configuration and then use the show commands to view traffic distribution.

Show Running Config for DCFW

Output from the **show running-config** command shows the commands that must be entered for DCFW to work correctly in a simple FW + SLB deployment scenario.

```
ACOS(config)# show running-config
!Current configuration: 2822 bytes
!Configuration last updated at 01:42:08 PST Tue Nov 10 2015
!Configuration last saved at 01:56:48 PST Tue Nov 10 2015
!64-bit Advanced Core OS (ACOS) version 4.1.0, build 249 (Nov-09-
2015,05:26)
!
access-list 101 permit ip host 172.16.162.11 any
!
access-list 101 permit ip host 172.16.162.12 any
!
access-list 101 deny ip any any
!
multi-config enable
!
terminal idle-timeout 0
!
vlan 21
  tagged ethernet 16
  router-interface ve 21
!
vlan 53
  tagged ethernet 16
  router-interface ve 53
!
vlan 99
  untagged ethernet 1
  router-interface ve 99
!
vlan 161
  tagged ethernet 15
  router-interface ve 161
!
vlan 162
  tagged ethernet 16
  router-interface ve 162
!
vlan 163
  tagged ethernet 16
  router-interface ve 163
!
hostname ACOS
!
interface management
  ip address 192.168.229.16 255.255.255.0
  ip default-gateway 192.168.229.1
!
interface ethernet 1
  enable
!
interface ethernet 2
!
interface ethernet 3
!
interface ethernet 4
!
interface ethernet 5
!
interface ethernet 6
!
interface ethernet 7
!
interface ethernet 8
!
interface ethernet 9
!
interface ethernet 10
!
interface ethernet 11
!
interface ethernet 12
!
interface ethernet 13
!
interface ethernet 14
```

```
!
interface ethernet 15
  enable
!
interface ethernet 16
  enable
!
interface ethernet 17
!
interface ethernet 18
!
interface ethernet 19
!
interface ethernet 20
!
interface ve 21
  ip address 21.0.255.243 255.255.0.0
!
interface ve 53
  ip address 172.16.53.243 255.255.255.0
!
interface ve 99
  ip address 172.16.99.243 255.255.255.0
!
interface ve 161
  ip address 172.16.161.243 255.255.255.0
!
interface ve 162
  ip address 172.16.162.243 255.255.255.0
!
interface ve 163
  ip address 10.16.163.243 255.255.255.0
!
vrrp-a common
  device-id 1
  set-id 5
  enable
!
vrrp-a vrid 1
  floating-ip 172.16.162.244
  floating-ip 10.16.161.244
  floating-ip 172.16.53.244
  floating-ip 10.16.163.244
  blade-parameters
    tracking-options
      interface ethernet 15 priority-cost 100
      interface ethernet 16 priority-cost 100
!
ip nat pool p1 10.16.161.201 10.16.161.201 netmask /24 gateway
10.16.161.254 vrid 1
!
ip nat inside source list 101 pool p1
!
vrrp-a interface ethernet 1
!
ip route 0.0.0.0 /0 10.16.161.254
!
zone HA
  interface ethernet 1
  interface ve 99
!
zone Trust_Vlan_162
  vlan 162
!
zone Trust_Vlan_53
  vlan 53
!
zone Untrust
  vlan 161
!
zone dmz
  vlan 163
!
slb server s001 172.16.162.1
  port 21 tcp
  port 80 tcp
!
slb server s002 172.16.162.2
  port 21 tcp
  port 80 tcp
```

```
!
slb server s011 172.16.162.11
  port 53 udp
!
slb server s012 172.16.162.12
  port 53 udp
!
slb service-group sg-1 tcp
  member s001 80
  member s002 80
!
slb service-group sg-2 tcp
  member s001 21
  member s002 21
!
slb service-group sg-3 udp
  member s011 53
  member s012 53
!
slb virtual-server vip-161.111_dns 10.16.161.111
  vrid 1
  port 53 dns-udp
    service-group sg-3
!
slb virtual-server vip-161.112_dns 10.16.161.112
  vrid 1
  port 53 dns-udp
    service-group sg-3
!
slb virtual-server vip_161.101_http_ftp 10.16.161.101
  vrid 1
  port 21 ftp
    ha-conn-mirror
    service-group sg-2
  port 80 tcp
    ha-conn-mirror
    service-group sg-1
!
slb virtual-server vip_161.102_http_ftp 10.16.161.102
  vrid 1
  port 21 ftp
    ha-conn-mirror
    service-group sg-2
  port 80 tcp
    ha-conn-mirror
    service-group sg-1
!
logging syslog information
!
logging host 172.16.53.1
!
object network obj_sv_162.11_dns
  172.16.162.11/32
!
object network obj_sv_162.12_dns
  172.16.162.12/32
!
object network obj_sv_162.1_http_ftp
  172.16.162.1/32
!
object network obj_sv_162.2_http_ftp
  172.16.162.2/32
!
object network obj_sv_163.5_ssh
  10.16.163.5/32
!
object network obj_vip_161.101_http_ftp
  10.16.161.101/32
!
object network obj_vip_161.102_http_ftp
  10.16.161.102/32
!
object-group network objg_sv_dns fw v4
  object obj_sv_162.11_dns
  object obj_sv_162.12_dns
!
object-group network objg_sv_http_ftp_tmp fw v4
  virtual-server vip_161.101_http_ftp
  virtual-server vip_161.102_http_ftp
!
```

```
object-group network objg_sv_http_ftp fw v4
  object obj_vip_161.101_http_ftp
  object obj_vip_161.102_http_ftp
!
object-group service obj_srv_http
  tcp eq 80
  tcp eq 8080
!
object-group service obj_srv_ftp
  tcp eq 21 alg FTP
  tcp eq 20021 alg FTP
!
object-group service obj_srv_dns
  udp eq 53 alg DNS
  tcp eq 53 alg DNS
!
object-group service obj_srv_ssh
  tcp eq 22
!
rule-set r1
  rule 10
    action permit
    source ipv4-address 172.16.99.242/32
    source zone HA
    dest ipv4-address 224.0.0.210/32
  rule 15
    action permit
    source ipv4-address 172.16.99.242/32
    source zone HA
    dest ipv4-address 172.16.99.243/32
  rule 110
    action permit log
    source zone Untrust
    dest object-group objg_sv_http_ftp
    service object-group obj_srv_http
  rule 111
    action permit log
    source zone Untrust
    dest object-group objg_sv_http_ftp
    service object-group obj_srv_ftp
  rule 115
    action permit log
    source zone Untrust
    dest virtual-server vip-161.112_dns
    service object-group obj_srv_dns
  rule 130
    action permit log
    source object-group objg_sv_dns
    source zone Trust_Vlan_162
    dest zone Untrust
    service object-group obj_srv_dns
  rule 140
    action permit
    source zone Trust_Vlan_162
    dest zone Trust_Vlan_53
  rule 141
    action permit
    source zone Trust_Vlan_53
    dest zone Trust_Vlan_162
  rule 150
    action permit log
    dest object obj_sv_163.5_ssh
    service object-group obj_srv_ssh
!
fw vrid 1
!
fw session-aging a1
  tcp idle-timeout 12345
  udp idle-timeout 89
  icmp idle-timeout 9
!
fw active-rule-set r1 session-aging a1
!
end
!Current config commit point for partition 0 is 0 & config mode is
classical-mode
ACOS(config)#
```

Gi/SGi Firewall

This section describes the basic features of Gi/SGi-Firewall and explains the features and configurations in detail.

The following topics are covered:

Overview

Gi/SGi-FW utilizes a stateful firewall to protect subscribers and LTE service providers from DDoS attacks and data tampering. Gi/SGi-FW enables mobile carriers to achieve high firewall connection rates and throughput.

By leveraging the capabilities of integrated Carrier-Grade Network Address Translation (CGNAT), the lifespan of the equipment in legacy IPv4 networks is extended. In addition, this technology can help with IPv4 preservation, and the IPv6 transition technologies smooth the transition to IPv6.

The following Gi/SGi-FW features are available:

- Gi/SGi-FW leverages Carrier Grade NAT (CGNAT) that scales IPv4 networks with transparent NAT available and allows external users to initiate connections to NAT clients.
- Gi/SGi-FW supports migration to IPv6 and supports hybrid IPv4 and IPv6 networks by translating between the two technologies.
- Gi/SGi-FW offers DDoS protection for NAT pools against destructive DDoS attacks.
- Gi/SGi-FW supports IP anomaly detection that checks for over 30 IP packet anomalies or combines anomaly detections with IP addresses blocked for granular attack mitigation.
- Gi/SGi-FW supports configuring a IP threat list containing IP addresses that must be blocked in order to further reduce DDoS attacks. For more information, see IP Threat List.
- Gi/SGi-FW supports connection rate limiting by detecting and blocking attack traffic using IP-based connection rate limiting and system-wide connection limits.
- Gi/SGi-FW offers IPsec VPN in mobile networks that prevents eavesdropping, authenticate eNodeBs, and secure communications over wireless and WiFi networks.
- Gi/SGi-FW supports common event format (CEF) logging, such that when the firewall applies an action (deny/permit/reset) to a new connection request, a log is generated.

The following CGN technologies are supported with Gi/SGi-FW:

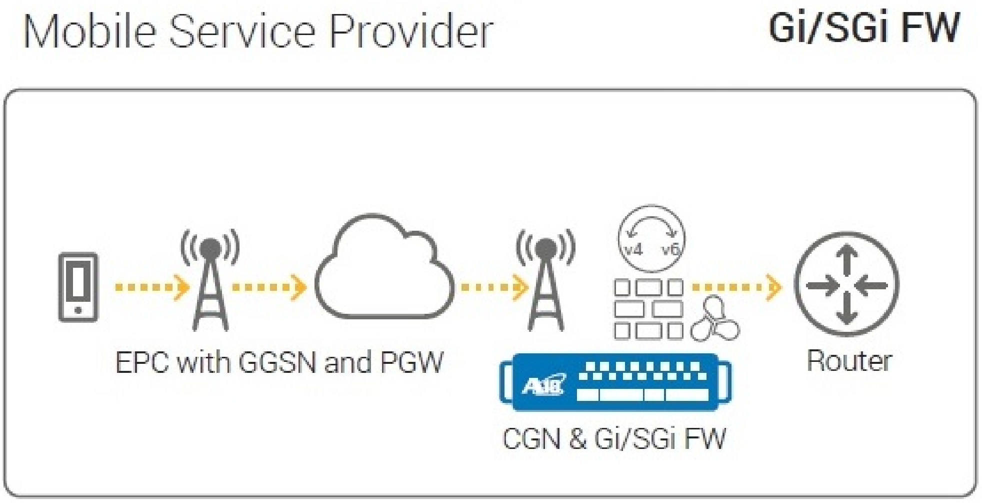
- LSN (NAT44) & NAT64
  - FTP, TFTP, RTSP, PPTP, SIP, DNS (for NAT44 only), and ICMP ALG support
- Fixed NAT - NAT44 & NAT64
  - FTP, TFTP, RTSP, PPTP, SIP, DNS (for NAT 44 only), and ICMP ALG support
- Integrated DDoS functionalities
- IP Anomaly Filtering
- Selective Filtering for CGN NAT Pools
- CGNAT Pool IP Blocked Lists
- Session rate limiting for CGN
- CEF logging format support for CGN traffic logging (HTTP logging and include-radius -attribute not supported)
- Separate logging template for Firewall logging
- A CLI **`show fw resource-usage helper-sessions`** to display helper session statistics for firewall

Gi/SGi-Firewall Deployment Topology

The firewall can be deployed with Carrier Grade NAT (CGN), which is an IP-based interface between the EPC with GGSN, PGW-U, SGW-U, or 5GC with UPF and a public data network. When used with CGN, the primary purpose of the firewall is to shield mobile subscribers and service providers from attacks and data tampering. The firewall enables mobile carriers to achieve high firewall connection rates and throughput.

Figure 29 illustrates the topology for a basic sample use case of Gi/SGi-FW with a CGN deployment.

Figure 29 : Sample Gi/SGi-FW topology diagram for basic use case (FW + CGN)



See Gi/SGi Firewall Configurations for the CLI commands used to configure the firewall in an environment similar to that shown above.

Additionally, GiFW supports the notion of interface level tags such as **`ip nat inside`**, **`ip client`**, and **`map-e inside`** to identify the interface connected to the subscriber network, thereby identifying the private IP (to be NATted to a public IP). Similarly, the tags **`ip nat outside`**, **`ip server`**, and **`map-e outside`** are used to identify the internet or destination network that the subscriber is trying to access.

The interface tags must be configured in the following scenarios:

- On Multi-PU platforms (such as TH14045 or TH7650/TH7655S) and Scaleout clusters, the traffic is distributed across multiple Processing Units (PUs) or multiple nodes. On such platforms, these interface tags are required to identify the subscriber IP as well as the packet direction for consistent hashing. This ensures the traffic belonging to a given session is always processed by the same PU or node. For more information, see Gi/SGi Firewall on Multi-PU Platforms
- In case of CGNAT deployments, these tags are used to identify the subscriber network and the IP address to be Source NATted.
- In case of Firewall deployments, most of the firewall policies require the subscriber side to be identified. These tags are used to identify if the traffic is originating from the subscriber (outbound traffic) or from the internet/server (inbound

traffic). Therefore, it is recommended to configure the appropriate interface tags for all firewall deployments.

The interface tags **`ip client`** and **`ip server`** need to be configured on interfaces carrying traffic, which is not subject to CGN (NAT), and is being forwarded through the device. The system caches the firewall connection state for efficient handling of such non-NATed traffic flows. This state is referred to as a **Firewall** session (or **transparent** session since the L3/L4 information is not modified). So, **`ip client`** and **`ip server`** tags must be configured for **Firewall** or **transparent** sessions only. Similarly, **`ip nat inside`** and **`ip nat outside`** tags must be configured for interfaces carrying CGN traffic.

NOTE: In a Gi Firewall deployment, if a common partition is used for NAT and transparent traffic, the tags **`ip-nat inside/outside`** or **`ipv6 nat inside/outside`** can coexist with **`ip client/server`** tags.

Besides the above-mentioned interface tags, ACOS also supports **`ip dmz`** interface tag to identify Demilitarized Zone (DMZ). For configuration details and other information related to DMZ, see Supporting DMZ Interfaces.

Limitations

Below are limitations associated with the Gi/SGi-Firewall feature:

- If you configure port- and protocol-based idle-timeout values that are not in multiples of 60 seconds, then ACOS will round them up or down in multiples of 60 seconds. This modification is apparent in the output in the “show session” command. For example, an idle-timeout value of 150 seconds will appear in the output as 120 seconds.
- Sending an ICMP ping packet to an Ethernet interface fails if the destination zone is “local-type” and if the source is not in the permitted list. However, if an ICMP packet is sent to a loopback address or to a VE, then it works. This is expected behavior.
- When an ICMP ping packets is sent to a VIP (and explicitly allowed by the FW rule) then the session will not be created in the session table. This behavior is by design.

- If you create a zone with the name “any”, you will not be able to later delete this zone. This limitation exists because ACOS auto-creates a zone called “any”, but the zone does not appear in the output of the “show running” CLI command. Therefore, if you manually create a zone called “any”, it will be visible in the output, but because it has the same name as the system-generated zone, you will not be able to delete it.
- When using Gi/SGi-FW with NAT64, the client denies the packets. This can occur if the client is sending packets to an IPv6 address and these v6 packets are converted to an IPv4 address. However, the route to the IPv4 destination address is not there after a v6/v4 translation. The firewall module is independent and does not know about the v6/v4 address translation, and since the route to the IPv6 destination address is not there, ACOS drops the packets.
- IPv6 packets with a destination address matching the NAT64 prefix are L3-forwarded by the ACOS device. Such packets must be handled by NAT64 or they will get dropped.
- Adding an explicit deny rule at the end of the rule-set, without specifically allowing traffic destined for the ACOS device, will cause the dynamic routing protocols, VRRP-A, and aVCS to no longer work.
- An object can be deleted while it is still being modified in another admin session.

Firewall Rule-Sets for Gi/SGi Firewall

This section provides the configuration elements of a Gi/SGi firewall rule-set.

Rule-Set

A rule-set contains firewall rules and these rules control what type of traffic is allowed to enter the firewall and which traffic will be denied. This filtering process is accomplished by configuring rules in the rule-set and each rule can be configured with an action or action-group, such as permit, reset, or deny.

For example, you could configure a rule with the action to “permit” a certain type of traffic associated with a specified application. If packets entering the firewall match the rule, they will be permitted to traverse the firewall.

Based on the actions performed, the firewall allows you to configure multiple rule-set types. This enables different firewall applications such as security control, NAT, traffic control, and DDoS to classify the traffic in different ways, thereby providing flexibility and improved usability. The following rule-set types are supported:

- Access Control: This rule-set controls the traffic by permitting or denying the packets. It also controls logging, decides how traffic is forwarded, and includes packet rewrite functions like NAT.

  Use the `rule-set` command to configure this rule-set and the `fw active-rule-set` command to activate it.

NOTE: In this document, unless mentioned otherwise, the **firewall rule-set** refers to the Access Control rule-set.

- Traffic Control: This rule-set applies rate limiting policies to limit the network traffic. Although the Access Control rule-set supports basic rate-limiting, you are recommended to configure this rule-set for improved performance.

NOTE: The Traffic Control rule-set is not a standalone rule-set; the Access Control rule-set must be configured along with it for the firewall policies to function as expected.

  Use the `traffic-control rule-set` command to configure this rule-set and the `traffic-control active-rule-set` command to activate it. For a configuration example, see Configuring Rate Limiting Using Traffic Control Rule-Set.

With multiple rule-sets configured, when a packet comes in, it is matched against the two rule-set types and the matched rule is returned for each rule-set type. Thus, the firewall returns:

- An Access Control rule that can perform one of the following actions:
  - permit/deny
  - log
  - NAT
  - listen-on-port

- ipsec
- respond-to-user-mac

- A Traffic Control rule controls the rate-limit policy to be applied to the packet.

Key Considerations

- If a configuration has template limit-policies bound to both Access Control rules and Traffic Control rules and a particular traffic stream matches a Traffic Control rule as well as an Access Control rule, the template limit-policy bound to the Traffic Control rule will come in effect to rate-limit this traffic.
- The firewall rule-sets act like firewall **access-control** policies. ACOS adds implicit rules to permit traffic associated with certain control protocols, such as BGP, OSPF, and VRRP. However if the rules that are overly broad, encompassing IPs and ports through which control traffic flows, there can be an adverse impact on the functionality of these protocols.

  It is recommended to add specific rules that are only related to the client subnet range and not add rules that allow traffic to and from all IPs (implicitly covering IP traffic from control protocols). Additionally, when used in conjunction with the Traffic Control rule-sets, you need to ensure that the Traffic Control rules are specific rather than overly permissive, as broad rules may lead to rate limiting of traffic associated with control protocols.

Rule

A rule can be configured to perform generic functions, such as “forward” or “cgnv6”. It can also be set up to perform more advanced functions such as “cgnv6 lsn-lid 2” or “cgnv6 fixed-nat”.

By default, a “permit” rule that has no specified application will be L3-forwarded and a firewall session is created. In other words, it is treated the same as a permit rule with an application specified as “forward”.

For a rule without an application associated with it, use the command **`fw permit-default-action`** `{`**`next-service-mode`** `|` **`forward`**`}` to change the default behavior of the rule. This command changes the way a packet is processed by matching a rule that contains “action permit”.

- `next-service-mode` means that the packet will be processed according to the applications configured in order.
- `forward` means that the packet will be L3 forwarded and will create a firewall session.

For detailed information about match criteria, see Match Criteria .

Action or Action-Group

Once the traffic matches a rule, the configured action is applied to the traffic. The action can be Permit, Reset, or Deny. For executing simple action behavior, you can use the "action" CLI command. For executing complex action behaviors on the matching traffic, you can use the "action-group" CLI command which provides additional options.

The following action or action-group can be applied:

- Permit—Permits the traffic to pass through the firewall unimpeded. Under Permit, the following applications are supported:
  - cgnv6—Checks the packets matching this rule against any configured CGNv6 applications. When a packet matches a cgnv6 rule, the packet will be processed according to the “cgnv6” applications configured if and only if it satisfies all the necessary conditions. A packet that is not matching any CGNv6 configurations will get dropped.
    - cgnv6 lsn-lid – Uses the specified LSN LID to perform NAT on packets matching this rule. When a packet matches a cgnv6 lsn-lid <num> rule, the packet will be processed according to the specified LSN LID. When an LSN LID is used, it is not necessary to configure an LSN class-list. However, the packet must come in on a NAT inside interface and go out through a NAT outside interface. When an LSN LID is not found, the packet will get dropped.
    - cgnv6 fixed-nat – Applies Fixed NAT on any packet matching this rule. When a packet matches a cgnv6 fixed-nat rule, the packet will be processed by Fixed NAT. The packet must come in on a NAT inside interface. A packet that is not matching the Fixed NAT configuration will get dropped.

    - cgnv6 ds-lite – Applies DS Lite on any packet matching this rule. When a packet matches a cgnv6 DS-Lite rule, the packet will be processed by DS Lite. A packet that is not matching the DS Lite configuration will get dropped.

- forward – Forwards the packets matching this rule as Firewall session. If action is selected, you can configure listen-on-port with forward. For more details, see the description specified under listen-on-port.
- ipsec - Forwards the packet matching this rule to the specified IPsec VPN tunnel. The rate-limit policy action is also supported for this action. Rate limits are applied to the outbound packets before being encrypted by IPsec. The inbound packets are first decrypted and the rate-limit is applied only if the traffic matches the rule with the configured rate-limit. For an example configuration, see Permit IPsec with Rate Limit Policy.

NOTE: The rate-limit policy is not applicable for the encrypted IPsec packets.

For configuring IPsec firewall rules, see *Configuring IPsec VPN guide*.

- log - Enables permit log to be sent to the log server. The logging template specified and bound globally applies to all rules that enable logs, or it can be explicitly specified for rules.
- listen-on-port—Creates a full-cone session for the source IP for allowing outside users to connect to this IP. This option is applicable only for transparent sessions.

The following additional actions are supported only on configuring action-group:

    - limit-policy—Applies the rules defined in the limit policy template on the packets matching the rule. This is applicable only for CGN and Firewall.

NOTE: Configuring this action under the Access Control rule-set will enable basic rate-limiting. However, for enhanced rate-limiting features and improved performance, you are recommended to configure the limit-policy under Traffic Control rule-set.

    - respond-to-user-mac—Assigns the route hop based on the MAC address inside the client’s request on the packets matching the rule.

- set-dscp - Sets the Differentiated Services Code Point (DSCP) value in the IP (IPv4 and IPv6) header for all the session packets. Hence, this is a session-based action.

  The DSCP bits contain packet classification information that signal other devices (along the path), how to treat the traffic. Refer to **`rule-set rule action-group permit`** in the Command Line Reference Guide for the list of DSCP values supported.

  For more information, see Permit Set DSCP.

  NOTE:

  - If a rule is configured with application protocol, this action is applied only after application classification.
  - If the DSCP change is applied by CGN, SLB, SSLi or IPsec modules, this action will not take effect.
  - Since this action is a session-based action, all the session packets change when this action is applied to a session. Additionally, if the DSCP configuration changes during the session life, the new DSCP value will be set for the new session only.

- tcp syn-cookie- Configures SYN cookie protection for a firewall rule. Enabling SYN cookie at this level applies protection to a specific component of the overall traffic. This configuration allows you to define a threshold for the number of TCP half-open sessions that trigger SYN cookie protection when exceeded, and a timeout for the duration the protection remains active. For configuration example, see Permit.

NOTE:

- The configuration in this command overrides the configuration in the **`fw tcp syn-cookie`** and **`cgnv6 ddos-protection syn-cookie`** commands that are enabled at the global level.
- When this command is configured at the rule-level, the 'tcp-half-open' sessions threshold considers the half-open sessions created by the rule. However, when the command is configured at the global level, it considers the total half-open sessions created system-wide.

- Deny - Silently denies the client request by dropping the packet without notifying the client. On configuring this action group, you can also bind a DDoS rate-limit policy. The rules or policies defined in the limit policy will be applied to all packets matching the rule. This allows the packets (that are being denied) to be tracked separately, thereby enabling early detection and mitigation of DDoS attacks. For more information, refer to DDoS Protection for Deny Rules.
- Reset—Resets the TCP session and sends an error message to notify the client. The reset option only applies to TCP traffic. Other protocol types will be silently dropped.

  On configuring this action-group, you can also do the following:

  - Reset the configured respond-to-user-mac action.
  - Reset the configured rate limit policy.
  - Bind a DDoS rate-limit policy. The rules or policies defined in the limit policy will be applied to all packets matching the rule. This allows the TCP sessions, that are being reset, to be tracked separately. For a configuration example, see Reset with Template Limit Policy .

For configuration information, see Configuring Firewall Rule-Sets.

TCP MSS Clamping on Gi-FW Sessions

The Maximum Transmission Unit (MTU) of an Ethernet interface is set at 1500 bytes. Out of the 1500 bytes of the IP packet, some portion is TCP/IP header information, while the rest is the actual data to be transmitted. However, not all points in the network path may support an MTU of 1500; issues such as slow performance and unexpected packet drops may occur if some parts of the network have an MTU of less than 1500 bytes.

Path MTU Discovery (PMTUD) is a process that calculates the ideal MTU in such a network path so that IP fragmentation does not occur. PMTUD works with the help of ICMP or ICMPv6 messages between various points in the network and source, so that the source and destination may converge upon an optimum MTU value. This convergence ensures packet fragmentation along the network path does not occur. However, PMTUD may not work correctly in some networks, as many security devices block the ICMP messages.

In such circumstances, a workaround is to use maximum segment size (MSS) clamping. In MSS clamping, the source and the destination are configured with a lower MTU than that of 1500 bytes. TCP MSS clamping is supported on Gi-FW sessions to prevent slow performance and data loss in the network when not all parts of the network support an MTU of 1500 bytes.

For configuration information, see Configuring MSS Clamping for Gi-FW Sessions.

MAC-based Nexthop Routing for GiFW

GiFW firewall is a stateful Layer 4 firewall that supports the ability to filter incoming traffic at Layer 1-4, where traffic is filtered based on the source and destination IP addresses, in combination with the source and destination port numbers and IP protocol.

The support of MAC-based nexthop routing for GiFW enables the ACOS device to identify the route hop based on the MAC address inside the client’s request. The ACOS device uses the MAC address instead of the routing table to select the next hop for the reply. Replies that are sent to the client use the same route hop upon which the request was received.

NOTE: This feature is only applicable to transparent sessions of which this layer-3 session passes through ACOS without any NAT.

Since a session is set up with the source MAC being learned already, the source MAC movement can occur when the packet comes on a different port. This triggers a change in the MAC table. At this point, the following scenarios can occur, depending on where the packet comes to the server:

- If the MAC address is learned on the same VLAN but a different port, then the same MAC entry is updated. When configured with the **`respond-to-user-mac`** option, the packet will return on the moved MAC.
- If the same MAC address is learned on a port on a different VLAN, then a new MAC entry is added to the MAC table and identified by the MAC address and the VLAN.

  This added entry is different from the learned MAC since the VLAN is different.
- In the case of a trunk, the lead trunk port is selected for **`respond-to-user-mac`**. The "lead" trunk port is the first port being configured.

To configure MAC-based nexthop routing support on GiFW, a two-fold configuration can be performed as follows:

- At the global level, use the **`fw respond-to-user-mac`** command to enable use of the user source MAC for the nexthop traffic instead of the routing table.
- At the firewall rule level, use the **`respond-to-user-mac`** command (under the template limit-policy) that is bound to the rule. This binding is applicable to **`action-group permit respond-to-user-mac`** and **`action-group reset respond-to-user-mac`** under the rule.

As limited by the maximum size of the MAC table as 16K, the **`fw respond-to-user-mac`** entries on the MAC table entries are limited to 16K. Thereafter, the maximum number of sessions using the **`fw respond-to-user-mac`** is based on the MAC table size.

Mac-based Nexthop Routing Synchronization

When an ACTIVE-STANDBY synchronization occurs, the MAC address, port, and VLAN information is synchronized from the Active to the Standby unit. This enables the Standby unit to set up the destination address based on the synchronized information. In the standby unit, if a physical interface is used, the MAC entry will be updated with the new physical port in the standby. The port can be different for the standby unit. In case of ports being under a VLAN, the port under the VLAN will also be the same for the standby unit, with the appropriate mac entry selected.

When an ACTIVE-STANDBY synchronization occurs, depending on the status of the existing MAC, the following scenarios might occur:

- If the MAC of an existing session has changed after the switchover from ACTIVE to STANDBY, the same MAC will be used on the reverse packet as long as the MAC address is still valid.
- If the MAC has been invalid, one of the following occurs:
  - For OUTBOUND packets, source MAC learning occurs. Once established, the configured `respond-to-user-mac` is used.
  - For INBOUND packets, the destination address is based on route lookup.
- If a packet comes in from a different source MAC after the switchover, since this MAC is different from the MAC on the ACTIVE unit, source MAC learning occurs again.

If ALG protocols such as FTP, TFTP, SIP, DNS and others are enabled on their well-known ports, the subsequent data connection still uses the reverse and forward destinations based on the `respond-to-user-mac` value. When creating a full-cone session, the reverse destination should use the `respond-to-user-mac` address. This ensures that the EIF sessions from the server matching the full-cone session use the same destination saved for the `respond-to-user-mac` address.

For configuration information, see Permit Respond to User Mac.

Multiple VRID Support

To implement redundancy and load sharing, the firewall supports multiple VRIDs. The firewall sessions can be synced with different VRRP groups (based on the VRID). The Active VRID can have multiple standby VRIDs. However, the session is synchronized only with the primary standby VRID that takes over when the active VRID fails.

The multiple VRID support depends on the following:

- Configuring multiple VRRP groups.
- Configuring the **promiscuous-mode** - The promiscuous mode must be enabled to ensure that the VRRP floating IP MAC is broadcast. This enables traffic flow detection and determines which VRRP is used to create the session.
- Upstream/downstream router – The router uses the VRRP floating IP as the next-hop to forward traffic.

Limitations

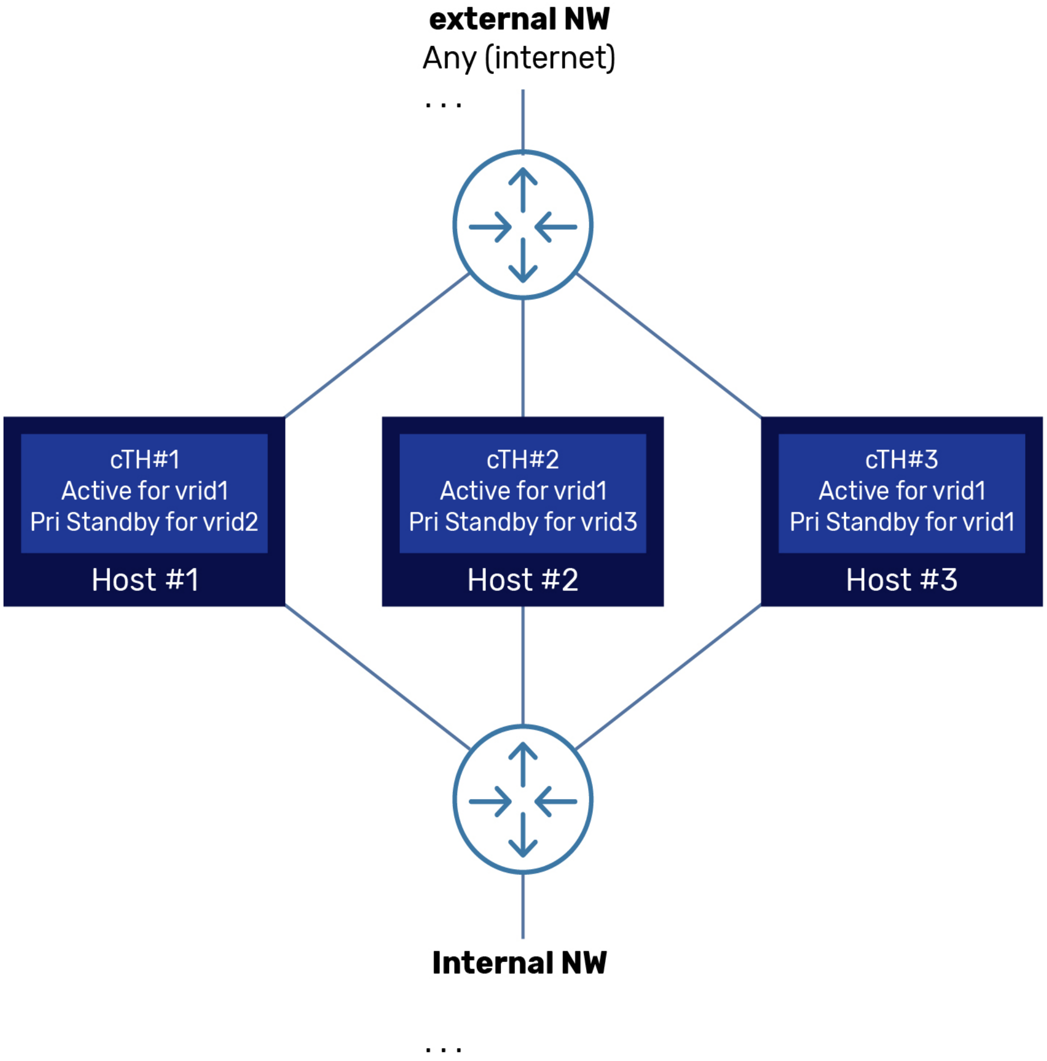
- Applies only to firewall traffic.
- Applicable only for A10 platforms that support the firewall (including application aware firewall) and VRRP-A.

  On the Thunder devices, VRRP-A is supported in the shared partition and L3V partitions. Layer 3 Virtualization allows each L3V partition to have its own VRID, independent of the VRIDs belonging to other partitions.

Deployment Example Configuration

Figure 30 demonstrates an example of multiple VRID configuration, where three VRIDs are configured on three thunder container (cThunder) devices connect to gateway routers (on the client and server side).

Figure 30 : Multiple VRID Support



In this example, when the gateway router sends traffic to cThunder, the firewall gets the VRID of the traffic based on the destination MAC. As a result, the firewall establishes sessions with different VRIDs and manages traffic based on different VRRP groups. Moreover, the firewall session syncs with the standby based on the session's VRID. However, if the firewall is unable to obtain the VRID from traffic's destination MAC, then it uses the default VRID configured using `fw vrid` command.

NOTE: The active firewall rules are shared by the traffic of all the VRRP groups. The traffic is identified by the firewall rule and the appropriate policy actions are applied.

CLI Configuration

For the topology in Figure 30, the three Thunder container (cThunder) devices need to be configured in a particular manner. Configuration steps for the first cThunder device are given below:

NOTE: Only the steps pertaining to multiple VRID configuration are listed in this topic. Refer to the Consolidated Configuration Example for detailed configuration steps.

1. Enable promiscuous mode to broadcast the VRRP floating IP MAC.

```
ACOS(config)# system promiscuous-mode
```

2. Configure the physical interfaces on the device. In this example, ethernet ports 1 to 6 are enabled.

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# name vEth-eth1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# ip address 10.10.1.2 255.255.255.0

ACOS(config)# interface ethernet 2
ACOS(config-if:ethernet:2)# name vEth-eth2
ACOS(config-if:ethernet:2)# enable
ACOS(config-if:ethernet:2)# ip address 10.10.10.2 255.255.255.0

ACOS(config)# interface ethernet 3
ACOS(config-if:ethernet:3)# name vEth-eth3
ACOS(config-if:ethernet:3)# enable
ACOS(config-if:ethernet:3)# ip address 10.10.100.2 255.255.255.0

ACOS(config)# interface ethernet 4
ACOS(config-if:ethernet:4)# name vEth-eth4
ACOS(config-if:ethernet:4)# enable
ACOS(config-if:ethernet:4)# ip address 10.10.2.1 255.255.255.0

ACOS(config)# interface ethernet 5
ACOS(config-if:ethernet:5)# name vEth-eth5
ACOS(config-if:ethernet:5)# enable
ACOS(config-if:ethernet:5)# ip address 10.10.20.1 255.255.255.0
ACOS(config)# interface ethernet 6
ACOS(config-if:ethernet:6)# name vEth-eth6
ACOS(config-if:ethernet:6)# enable
ACOS(config-if:ethernet:6)# ip address 10.10.200.1 255.255.255.0
```

3. Configure multiple VRIDs (1,2,3) by specifying the floating IPs, and setting the appropriate priorities.

   The floating IP help provide network stability since it remains reachable even if the VRRP-A failover occurs. The priority determines the role played by the VRID and what happens in case of a failover.

   ```
   ACOS(config)# vrrp-a vrid 1
   ACOS(config-vrid:1)# floating-ip 10.10.1.100
   ACOS(config-vrid:1)# floating-ip 10.10.2.100
   ACOS(config-vrid:1)# blade-parameters
   ACOS(config-vrid:1-blade-parameters)# priority 200

   ACOS(config)# vrrp-a vrid 2
   ACOS(config-vrid:2)# floating-ip 10.10.10.100
   ACOS(config-vrid:2)# floating-ip 10.10.20.100
   ACOS(config-vrid:2)# blade-parameters
   ACOS(config-vrid:2-blade-parameters)# priority 160

   ACOS(config)# vrrp-a vrid 3
   ACOS(config-vrid:3)# floating-ip 10.10.100.100
   ACOS(config-vrid:3)# floating-ip 10.10.200.100
   ACOS(config-vrid:3)# blade-parameters
   ACOS(config-vrid:3-blade-parameters)# priority 150
   ```

4. Configure VRID 1 as the default VRID.

   It is used only if the destination MAC of the packet is not the Virtual MAC i.e., if it is not possible to detect which VRID the traffic belongs to.

   ```
   ACOS(config)# fw vrid 1
   ```

5. Similarly, configure the second and the third cThunder devices. Ensure that appropriate priorities are set while configuring VRIDs 2 and 3. Refer to Consolidated Configuration Example to check the detailed steps.

Show Command

To view the multiple VRIDs and the Active/Standby status of the VRRP-A configuration, use the **show vrrp-a**command.

```
cth1# show vrrp-a
vrid 1
Unit         State      Weight     Priority
1 (Local)     Active     65534      200
became Active at: [GMT] Thu, 30-Dec-2021 13:44:40 for  4 Day,18 Hour,26
min
2 (Peer)     Standby    65534      160   *
3 (Peer)     Standby    65534      150
vrid that is running: 1
vrid 2
Unit         State      Weight     Priority
1 (Local)     Standby    65534      150
became Standby at: [GMT] Thu, 30-Dec-2021 13:44:39 for  4 Day,18 Hour,26
min
2 (Peer)     Active     65534      200
3 (Peer)     Standby    65534      160   *
vrid that is running: 2
vrid 3
Unit         State      Weight     Priority
1 (Local)     Standby    65534      160           *
became Standby at: [GMT] Fri, 31-Dec-2021 01:49:34 for  4 Day, 6 Hour,21
min
2 (Peer)     Standby    65534      150
3 (Peer)     Active     65534      200
vrid that is running: 3
```

NOTE: The * indicates the primary standby.

The above-mentioned configuration provides the following Active/Standby status for the thunder container devices:

- Thunder Container 1: Active for vrid1, Primary Standby for vrid2
- Thunder Container 2: Active for vrid2, Primary Standby for vrid3
- Thunder Container 3: Active for vrid3, Primary Standby for vrid1

The VRRP-A priority on each of the thunder container devices and the corresponding session synchronization is given in the table below:

VRRP-A VRID	Priority on each device	Session creation and synchronization
vrid1	cTh1:200, cTh2:160, cTh3:150	Session created on cTh1 and synchronized with cTh2
vrid2	cTh1:150, cTh2:200, cTh3:160	Session created on cTh2 and synchronized with cTh3
vrid3	cTh1:160, cTh2:150, cTh3:200	Session created on cTh3 and synchronized with cTh1

The following table provides the details of the traffic flow from the client, and the session created with the VRID:

Device	VRID	Tarffic Flow
Thunder Container 1	vrid1	Traffic flows from the client access server with IP 10.10.2.4, and creates a session on cTh1 with vrid1
Thunder Container 2	vrid2	Traffic flows from the client access server with IP 10.10.20.4, and creates a session on cTh2 with vrid2
Thunder Container 3	vrid3	Traffic flows from the client access server with IP 10.10.200.4, and creates a session on cTh3 with vrid3

Consolidated Configuration Example

The consolidated configuration for the three cThunder devices (cTh1, cTh2 and cTh3 in Figure 30) is given below.

```
cth1# show running-config
!Current configuration: 246 bytes
!Configuration last updated at 10:27:39 GMT Fri Dec 24 2021
!Configuration last saved at 10:30:53 GMT Fri Dec 24 2021
!64-bit Advanced Core OS (ACOS) version 5.3.0-d, build 161 (Dec-21-
2021,20:02)
!
```

```
vrrp-a common
device-id 1
set-id 1
disable-default-vrid
enable
!
system promiscuous-mode
!
hostname cth1
!
!
interface management
ip address 172.17.0.3 255.255.255.0
ip default-gateway 172.17.0.1
!
interface ethernet 1
name vEth-eth1
enable
ip address 10.10.1.2 255.255.255.0
!
interface ethernet 2
name vEth-eth2
enable
ip address 10.10.10.2 255.255.255.0
!
interface ethernet 3
name vEth-eth3
enable
ip address 10.10.100.2 255.255.255.0
!
interface ethernet 4
name vEth-eth4
enable
ip address 10.10.2.1 255.255.255.0
!
interface ethernet 5
name vEth-eth5
enable
ip address 10.10.20.1 255.255.255.0
!
```

```
interface ethernet 6
name vEth-eth6
enable
ip address 10.10.200.1 255.255.255.0
!
!
vrrp-a vrid 1
floating-ip 10.10.1.100
floating-ip 10.10.2.100
blade-parameters
priority 200
!
vrrp-a vrid 2
floating-ip 10.10.10.100
floating-ip 10.10.20.100
blade-parameters
priority 150
!
vrrp-a vrid 3
floating-ip 10.10.100.100
floating-ip 10.10.200.100
blade-parameters
priority 160
!
!
rule-set test
rule 1
action permit
source ipv4-address any
source zone any
dest ipv4-address 10.10.20.0/24
dest ipv4-address 10.10.200.0/24
dest ipv4-address 10.10.2.0/24
dest zone any
service any
rule 2
action permit
source ipv4-address any
source zone any
dest ipv4-address any
dest zone any
service any
!
fw vrid 1
!
fw active-rule-set test
!
end

cth2# show running-config
!Current configuration: 246 bytes
!Configuration last updated at 10:28:44 GMT Fri Dec 24 2021
!Configuration last saved at 10:30:42 GMT Fri Dec 24 2021
!64-bit Advanced Core OS (ACOS) version 5.3.0-d, build 161 (Dec-21-
2021,20:02)
!
vrrp-a common
device-id 2
set-id 1
disable-default-vrid
enable
!
system promiscuous-mode
!
hostname cth2
!
!
interface management
ip address 172.17.0.4 255.255.255.0
ip default-gateway 172.17.0.1
!
interface ethernet 1
name vEth-eth1
enable
ip address 10.10.1.3 255.255.255.0
!
interface ethernet 2
name vEth-eth2
enable
ip address 10.10.10.3 255.255.255.0
```

```
!
interface ethernet 3
name vEth-eth3
enable
ip address 10.10.100.3 255.255.255.0
!
interface ethernet 4
name vEth-eth4
enable
ip address 10.10.2.2 255.255.255.0
!
interface ethernet 5
name vEth-eth5
enable
ip address 10.10.20.2 255.255.255.0
!
interface ethernet 6
name vEth-eth6
enable
ip address 10.10.200.2 255.255.255.0
!
!
vrrp-a vrid 1
floating-ip 10.10.1.100
floating-ip 10.10.2.100
blade-parameters
priority 160
!
vrrp-a vrid 2
floating-ip 10.10.10.100
floating-ip 10.10.20.100
blade-parameters
priority 200
!
vrrp-a vrid 3
floating-ip 10.10.100.100
floating-ip 10.10.200.100
blade-parameters
priority 150
!
```

```
!
rule-set test
rule 1
action permit
source ipv4-address any
source zone any
dest ipv4-address 10.10.20.0/24
dest ipv4-address 10.10.200.0/24
dest ipv4-address 10.10.2.0/24
dest zone any
service any
rule 2
action permit
source ipv4-address any
source zone any
dest ipv4-address any
dest zone any
service any
!
fw vrid 1
!
fw active-rule-set test
!
end

cth3# show running-config
!Current configuration: 246 bytes
!Configuration last updated at 10:30:16 GMT Fri Dec 24 2021
!Configuration last saved at 10:30:18 GMT Fri Dec 24 2021
!64-bit Advanced Core OS (ACOS) version 5.3.0-d, build 161 (Dec-21-
2021,20:02)
!
vrrp-a common
device-id 3
set-id 1
disable-default-vrid
enable
!
system promiscuous-mode
!
```

```
hostname cth3
!
!
interface management
ip address 172.17.0.5 255.255.255.0
ip default-gateway 172.17.0.1
!
interface ethernet 1
name vEth-eth1
enable
ip address 10.10.1.4 255.255.255.0
!
interface ethernet 2
name vEth-eth2
enable
ip address 10.10.10.4 255.255.255.0
!
interface ethernet 3
name vEth-eth3
enable
ip address 10.10.100.4 255.255.255.0
!
interface ethernet 4
name vEth-eth4
enable
ip address 10.10.2.3 255.255.255.0
!
interface ethernet 5
name vEth-eth5
enable
ip address 10.10.20.3 255.255.255.0
!
interface ethernet 6
name vEth-eth6
enable
ip address 10.10.200.3 255.255.255.0
!
!
vrrp-a vrid 1
floating-ip 10.10.1.100
```

```
floating-ip 10.10.2.100
blade-parameters
priority 150
!
vrrp-a vrid 2
floating-ip 10.10.10.100
floating-ip 10.10.20.100
blade-parameters
priority 160
!
vrrp-a vrid 3
floating-ip 10.10.100.100
floating-ip 10.10.200.100
blade-parameters
priority 200
!
rule-set test
rule 1
action permit
source ipv4-address any
source zone any
dest ipv4-address 10.10.20.0/24
dest ipv4-address 10.10.200.0/24
dest ipv4-address 10.10.2.0/24
dest zone any
service any
rule 2
action permit
source ipv4-address any
source zone any
dest ipv4-address any
dest zone any
service any!
fw vrid 1
!
fw active-rule-set test
!
end
```

Rate Limiting

This section describes rate limiting for Gi/SGi-Firewall and explains the features and configurations in detail.

The following topics are covered:

Overview

ACOS provides security protection to identify and mitigate against some forms of volumetric Distributed Denial of Service (DDoS) attacks on subscriber IPs. During the DDoS attack, the subscriber may get disconnected because the traffic may not be delivered to the subscriber. Rate limiting and DDoS protection helps to ensure the firewall operation is not disrupted and the subscriber's connectivity is preserved. Some of the features such as rate limiting, and IP blocked lists limit the volume of the traffic mitigating attacks that consume resources.

Subscriber IPs (or even entire subnets) are susceptible to malicious behavior, such as port scans and DDoS attacks. High volume attacks, such as NTP reflection or DNS response spoofing, often target a single destination port that is open by a firewall rule. While ACOS identifies and drops packets from such volumetric attacks, a high rate of attack traffic may affect the service performance and resource consumption.

Rate limiting also helps to limit the traffic coming from certain application protocols and categories. It is applied after the application is classified.

Rate limiting is supported for both the Gi firewall and a transparent firewall.

To protect resources against reflection and spoofing types of volumetric attacks, ACOS offers the following rate limiting and DDoS capabilities:

- Packets-Per-Second
- Throughput
- Connections Per Second
- Concurrent Sessions

The above rate limit entries are applied for a subscriber or client IP only. It is highly recommended to configure the inside interface using the **`ip client/ip nat inside`** command and the outside interface using the **`ip server/ip nat outside`** command before configuring rate limiting. This helps to identify if the session is an inbound or outbound session.

You can apply rate limiting at a subscriber IP, subnet, rule, or for RADIUS scope using RADIUS derived attributes:

- Aggregate—The rate limiting policy is applied on the traffic at a rule level. For example, if you have configured PPS total as the rate limiting policy with limit-scope as aggregate, the PPS rate limiting is applied on the traffic matching at the rule level.
- Subscriber IP—The rate limiting policy is applied at a subscriber IP level defined in the rule. For example, if you have configured PPS total as the rate limiting policy with limit-scope as subscriber IP, the configured threshold is applied on each subscriber IP matching the rule.
- Subscriber-prefix—The rate limiting policy is applied at a prefix level. It is applied to an entire subnet, instead of a single subscriber IP address.

  A rate limiting policy with this configuration can be used with IPv4 and IPv6 traffic. However, in case of IPv4 traffic, the configured prefix-length is truncated to 32 i.e., you cannot specify a prefix-length greater than 32.
- RADIUS scope—The rate limiting policy is applied at the domain level for subscribers or user groups by using a RADIUS custom attribute. Individual rate-limits can be set for users, IPs, and aggregated rate-limits set for user groups.

For information on configuration, see Configuring Rate Limiting Scope.

Limitations

The following are the limitations:

- In case of Scaleout, the Subscriber-prefix and the aggregate level rate limiting is applied at a node level.
- When used with Firewall Scaleout Distributed Forwarding, only sessions that have the PPS uplink/downlink, throughput uplink/downlink, and CPS rate limiting metrics are subject to distributed forwarding by creating shadow sessions. Flows that need to have total throughput/PPS applied will not be subject to distributed forwarding and shadow sessions will not be created.

  Once the shadow session is created, a subsequent change in the rate-limit policy that enables or adds the total throughput/PPS metric will cause the rate-limit to not be applied correctly. It will work correctly when existing flows time out and new flows are no longer subject to distributed forwarding. This will enable a single node to check both uplink/downlink traffic and hence apply the configured total rate-limit metric correctly.
- The firewall sessions are not actively cleared out once the IP address is blocked.
- Rate limiting is not supported on one-to-one NAT sessions created by inbound traffic.

Packets-Per-Second

Packets-Per-Second (PPS) is the maximum number of packets allowed per second. When the number of packets-per-second crosses the configured threshold, the excessive traffic is dropped. The PPS threshold can range from 1 to 2147483647.

You can configure the packets-per-second for the following traffic:

- Packets-per-second uplink
- Packets-per-second downlink
- Packets-per-second total

The rate limiting can be applied at a rule level, subscriber IP level, or a prefix level.

NOTE: Packets-per-second based rate-limiting is only available via template limit-policies bound to Access Control rules.

Additionally, to manage a burst in the PPS for downlink traffic, you can configure the burst size by specifying the **burstsize** command as shown below,

```
ACOS(config-limit-policy)# limit-pps downlink 10000 burstsize 15000
```

In this example, the configured PPS rate limit for downlink traffic is set to 10000 and the burst size is set to 15000. This indicates that a sustained rate of 10000 packets-per-second is allowed in the downlink direction. However, if the downlink traffic does not use the available quota of 10000, the unused quota accumulates and allows a burst of up to 15000 packets-per-second.

For information on burst traffic, see Managing Burst Traffic and for configuration examples, see Configuring Packets-Per-Second Rate Limiting.

Throughput

Throughput is the maximum bits allowed per second (BPS). When the rate of traffic sent to a subscriber IP or a subnet exceeds the configured threshold, the excessive traffic is dropped. The throughput threshold can range from 100Kbps to 10Tbps.

You can configure the throughput rate limit for the following:

- Throughput uplink
- Throughput downlink
- Throughput total

The rate limiting can be applied at a rule level, subscriber IP level, or prefix level.

Additionally, to manage a burst in the throughput for download traffic, you can configure the burst size by specifying the **burstsize** command as shown below,

```
ACOS(config-limit-policy)# limit-throughput downlink 125000 burstsize
1875000
```

In this example, the configured throughput rate limit for downlink traffic is set to 1Mbps and the burst size is set to 1.5Mb. This indicates that a sustained rate of 1Mbps is allowed in the downlink direction. However, if the downlink traffic does not use the available quota of 1Mbps, the unused quota accumulates and allows a burst of up to 1.5Mb downlink traffic during a second.

For information on burst traffic, see Managing Burst Traffic and for configuration examples, see Configuring Throughput Rate Limiting.

Connections Per Second

Connections Per Second is the maximum number of connections that can be established per second, per subscriber IP or subnet. When the number of connections per second rate limit exceeds the configured threshold, no new connections will be allowed for the subscriber IP or the subnet. The connections per second threshold can range from 1 to 2147483647.

The rate limiting can be applied at a rule level, subscriber IP level, or a prefix level.

Additionally, to manage a burst in the CPS, you can configure the burst size by specifying the **burstsize** command as shown below,

```
ACOS(config-limit-policy)# limit-cps 1000 burstsize 1500
```

In this example, the configured rate limit for number of connections per second is set to 1000 and the burst size is set to 1500. This indicates that a sustained rate of 1000 new connections per second is allowed. However, if the traffic does not use the available quota of 1000 new connections per second, the unused quota accumulates and allows a burst of up to 1500 new connections during a second.

For information on burst traffic, see Managing Burst Traffic and for configuration examples, see Configuring Connections Per Second Rate Limiting.

Concurrent Sessions

Concurrent Sessions are the total number of simultaneous sessions allowed at any time, per subscriber IP or subnet.

When the total number of sessions exceed the configured threshold, no new sessions are allowed for the subscriber IP or subnet. The concurrent threshold can range from 1 to 2147483647.

The rate limiting can be applied at a rule level, subscriber IP level, or a prefix level.

For information on configuration, see Configuring Concurrent Sessions.

Managing Burst Traffic

High-performance rate limiting is extended by employing the standard token bucket algorithm to manage bursts in traffic. This algorithm allows a limited number of unused tokens (from the previous cycles) to be preserved for future use.

The algorithm is based on the principle of a token bucket, in which tokens are added at a steady rate. The bucket may accumulate up to a configurable number of tokens. This configurable limit is referred to as **burst size** in the command line interface. When the bucket receives a packet, it checks whether it has sufficient number of tokens, e.g., equivalent to the length of the packet in bytes for rate limiting. If yes, the packet is transmitted further, and the consumed tokens are removed from the bucket. Otherwise, the packet is considered as exceeding the configured rate limit. When the bucket is full of tokens, a burst of packets corresponding to the bucket capacity can be transmitted. This algorithm is applied to the rate limit policy so that a burst size can be configured along with the rate limit.

This algorithm is applied to the rate limit policy so that a burst size can be configured along with the rate limit.

The rate limit indicates the sustained rate at which the traffic is allowed to pass through. The burst size indicates the size of the token bucket, which is the maximum number of tokens allowed to accumulate and hence the maximum burst size of the traffic that can be allowed.

For example, a configured Connections Per Second (CPS) limit of 100 and a burst size of 150 implies that a sustained rate of 100 new connections per second is permitted. However, if the traffic does not use the available quota of 100 new connections per second, the unused quota accumulates and allows up to 150 new connections (burst) during a second.

CLI Configuration

To manage traffic bursts, you must specify the burst size while configuring the rate limit policy.

- To configure the burst size for CPS:

```
ACOS (config-limit-policy)# limit-cps limit burstsize burst_size
```

- To configure the burst size for Packets Per Second (uplink, downlink and total):

```
ACOS(config-limit-policy)# limit-pps uplink limit burstsize burst_size
ACOS(config-limit-policy)# limit-pps downlink limit burstsize burst_size
ACOS(config-limit-policy)# limit-pps total limit burstsize burst_size
```

- To configure the burst size for Throughput (uplink, downlink and total):

```
ACOS(config-limit-policy)# limit-throughput uplink limit burstsize
burst_size
ACOS(config-limit-policy)# limit-throughput downlink limit burstsize
burst_size
ACOS(config-limit-policy)# limit-throughput total limit burstsize
burst_size
```

Points to be considered while configuring burst size:

- Since rate limiting is applied over one second time intervals, ensure that the configured burst size is never less than one second worth of traffic that arrives at the configured rate limit. For example, if the configured throughput rate limit is 1 Mbps, the configured burst size must not be less than 1 Mb.
- The burst size determines the peak rate for the allowed traffic. For example, if the burst size is 5 Mb, the peak rate for the traffic will be 5 Mbps.

Hierarchical Rate Limiting

Bandwidth rate limiting helps to improve the experience of multiple users accessing the internet during periods of high demand for the throughput. It prevents overconsumption of the resources by certain users and allows a fair distribution of bandwidth among all active users.

Hierarchical rate limiting makes the process more flexible and structured by managing bandwidth on several levels. With hierarchical rate-limiting, it is possible to apply one set of limits (specified by a child template limit-policy) to the traffic belonging to an individual subscriber while applying the second set of limits (specified by a parent template limit-policy) to the aggregated traffic of all the subscribers. Furthermore, it is possible to distribute resources in a **max-min-fair** manner so that the unused portion of a subscriber’s fair-share can be distributed to other subscribers who are capable of utilizing more than their fair share.

This section covers the following topics on hierarchical rate-limiting:

Configuring Hierarchical Rate Limiting

The hierarchy among a set of template limit-policies can be defined by specifying the **parent** tag. This tag is used by a child template limit-policy to identify its parent template limit-policy. For example, in the following configuration, the **template limit-policy** *10* is the parent, whereas the **template limit-policy** *20* is the child.

```
ACOS(config)# template limit-policy 10
ACOS(config-limit-policy)# limit-throughput downlink 10240
ACOS(config-limit-policy)# limit-scope aggregate

ACOS(config-limit)# template limit-policy 20
ACOS(config-limit-policy)# limit-scope subscriber-prefix 64
ACOS(config-limit-policy)# parent 10
```

NOTE: The ID of the parent template limit-policy must be lower than that of the child template. Else, the parent configuration from the child limit-policy might be lost when the device restarts.

Points to be considered while configuring hierarchical rate-limiting:

- There is no limit on the number of hierarchies that can be present in a configuration. Each hierarchy may extend to any number of levels.
- Any configurable limits (except PPS) can be applied at any level in a hierarchy.
- Hierarchical rate-limiting functionality is only supported by Traffic Control rules. It is not possible to invoke this functionality using the Access Control rules.
- Only a leaf-level template limit policy i.e., template limit policy at the lowest level can be bound to a Traffic Control rule. Any template that serves as the parent for another template cannot be bound to a Traffic Control (or Access Control) rule. Therefore, the Traffic Control rules must be constructed to match traffic at the

lowest level of the hierarchy.

For example, in a three-level hierarchy with individual subscribers configured at the second level and the application-level traffic of individual subscribers at the third level, the traffic-control rules must be constructed to match the application-level traffic of individual subscribers and must be bound to leaf-level template limit-policies that define the rate-limit actions for such traffic.

- Template limit-policies in a hierarchy may have any scope: subscriber IP, subscriber prefix, or aggregate, as long as a parent template's scope is **NOT** more specific than that of any of its children templates.

  For example, if a child template policy has scope **`subscriber-prefix`** *`64`* associated with it, the parent template policy may have scope aggregate or **`subscriber-prefix`** *`32`* but cannot have scope **`subscriber-prefix`** *`96`* associated with it.

- A template limit policy with scope **`aggregate`** will have only one associated rate-limit entry, whereas a template with scope **`subscriber-ip`** or **`subscriber-prefix`** may have a large number (potentially millions) of associated rate-limit entries.

NOTE: Hierarchy among the template limit policies determines the hierarchy among the rate-limit entries associated with these templates.

For configuration examples, see Hierarchical Rate-Limiting Use Cases.

Enforcing Rate-limits in a Hierarchy

Rate limits for the following metrics may be specified in any template policy in the hierarchy: downlink/uplink/total throughput, connections per second. When a rate limit in a particular metric (e.g., limit-throughput downlink) is specified in a parent template, the associated parent rate-limit entries distribute tokens corresponding to the available resources in this metric to its children rate-limit entries, which further enforce rate-limits corresponding to the tokens received from their parents. This happens even when the templates associated with the children rate-limit entries do not specify any limits for this metric. For example, the following configuration has the parent template enforcing a limit on downlink throughput, but the child template does not specify any limits on this metric:

```
ACOS(config)# template limit-policy  10
ACOS(config-limit-policy)# limit-throughput downlink 10240
ACOS(config-limit-policy)# limit-scope aggregate

ACOS(config-limit)# template limit-policy  20
ACOS(config-limit-policy)# limit-scope subscriber-prefix  64
ACOS(config-limit-policy)# parent  10
```

In this case, the parent rate-limit entry corresponding to template limit-policy 10 distributes 10Gbps of downlink throughput capacity among its children rate-limit entries (each one of which rate-limit traffic belonging to a specific 64-bit subscriber). Even though template 20 associated with the child rate-limit entry does not specify a limit on downlink throughput, the child rate-limit entry limits the downlink throughput of individual subscribers to a value corresponding to the tokens received from the parent rate-limit entry.

Now, consider the following configuration:

```
ACOS(config)# template limit-policy 10
ACOS(config-limit-policy)# limit-throughput downlink 10240
ACOS(config-limit-policy)# limit-scope aggregate

ACOS(config-limit)# template limit-policy 20
ACOS(config-limit-policy)# limit-scope subscriber-prefix 64
ACOS(config-limit-policy)# parent 10
ACOS(config-limit-policy)# limit-throughput downlink 10
```

In the above configuration, template 20 specifies a limit of 10Mbps on downlink throughput. Assuming that the parent rate-limit entry (associated with template 10) assigns tokens worth 20Mbps to a child rate-limit entry (associated with template 20), this child rate-limit entry will enforce a limit of 10Mbps on the downlink throughput of the subscriber associated with it (because the limit specified in the template is less than the value corresponding to the tokens allocated by the parent). However, if the parent rate-limit entry assigns tokens worth 5Mbps to this child rate-limit entry, the child entry will enforce a limit of 5Mbps on the downlink throughput of its subscriber.

Resource Distribution Among Children by a Parent

A parent rate-limit entry distributes the resources or tokens among its children based on the rate-limit specified for the metric in the child rate-limit entry template:

- If a child template specifies a rate-limit for the metric, the parent rate-limit entry uses this rate-limit as the weight for children rate-limit entries associated with this template.
- If a child template does not specify a rate-limit for the metric, the weight for children rate-limit entries associated with this template is assumed to be the same as the highest configured rate-limit for the metric among all its sibling entries.
- If no child template specifies a rate-limit for the metric, all children rate-limit entries are assumed to have equal weight for this metric.

The number of resources or tokens calculated in this manner for allocation to a child rate-limit entry may be considered as the child's **fair-share** of the parent's resources. This resource allocation mechanism ensures that each subscriber gets a fair-share of the network resources offered by the service provider and it is not possible for a few hyperactive subscribers to consume a disproportional share of the network resources thereby causing a bad user experience for other subscribers. Allocating a fair-share to each subscriber causes the hyperactive subscribers to be sufficiently throttled so that they do not impact other subscribers.

Max-Min Fair Distribution of Resources Among Children

By default, a parent rate-limit entry determines a fair-share (in the manner described above) for each of its children rate-limit entries and allocates that many tokens to each child rate-limit entry. In case the traffic belonging to a large number of children rate-limit entries is not sufficiently high to consume the entirety of their fair-share, a significant portion of the parent's resources may go unused. It is entirely possible that many other children rate-limit entries have sufficient traffic to consume these unused resources if allocated to them. The **`max-min-fair`** tag in the configuration of the template limit-policy associated with the parent rate-limit entry allows the parent entry to track the resource usage of its children and allocate unused fair-share of some children to others who can o consume it.

CLI Configuration

To enable this feature, configure the **`max-min-fair`** command in the template limit-policy in the following manner:

```
ACOS(config)# template limit-policy  10
ACOS(config-limit-policy)# limit-throughput downlink 10240
ACOS(config-limit-policy)# limit-scope aggregate
ACOS(config-limit-policy)# max-min-fair

ACOS(config-limit)# template limit-policy  20
ACOS(config-limit-policy)# limit-scope subscriber-prefix 64
ACOS(config-limit-policy)# parent  10
```

NOTE: This command applies to all the metrics in a template limit-policy (unlike the **relaxed** command that applies only to a specific metric).

For more configuration examples, see Hierarchical Rate-Limiting Use Cases.

Relaxed Rate Limiting

With hierarchical rate-limiting configured, often a parent rate-limit entry allocates resources greater than what the child entry can consume under its configured rate limit. In these scenarios, a relaxed limit allows the child rate-limit entry to utilize more resources (when available) than the configured limit.

Consider the following configuration:

```
ACOS(config)# template limit-policy  10
ACOS(config-limit-policy)# limit-throughput downlink 10240
ACOS(config-limit-policy)# limit-scope aggregate

ACOS(config-limit)# template limit-policy  20
ACOS(config-limit-policy)# limit-scope subscriber-prefix 64
ACOS(config-limit-policy)# parent  10
ACOS(config-limit-policy)# limit-throughput downlink 10  relaxed
```

Here, the **relaxed** tag is used for the rate-limit specified in template limit-policy 20. In this case, when the tokens allocated by the parent rate-limit entry exceed the specified limit of 10Mbps, the child rate-limit entry enforces a higher limit corresponding to the tokens allocated by the parent (because the limit specified in its template is **relaxed**).

Additionally, you can configure both, strict and relaxed limits in a template limit policy. In the following example, a relaxed limit is enabled for the downlink throughput metric; however, a strict limit is set for the CPS metric:

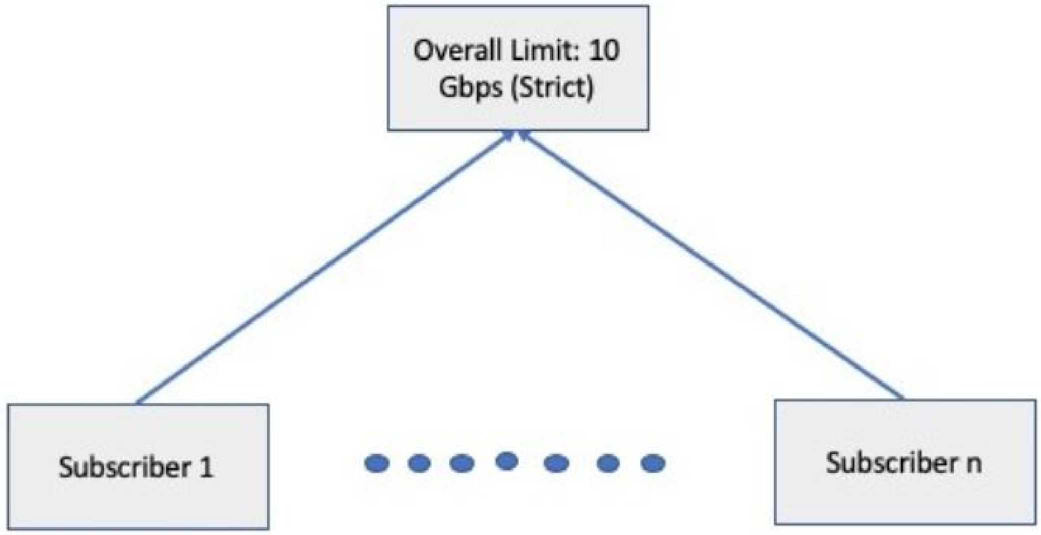
```
ACOS(config)# template limit-policy  1
ACOS(config-limit-policy)# limit-throughput downlink 100  relaxed
ACOS(config-limit-policy)# limit-cps 10
```

Hierarchical Rate-Limiting Use Cases

This topic describes the most common hierarchical rate-limiting scenarios, along with the configurations.

Use Case 1: Rate Limiting Hyperactive Subscribers

The following configuration (as shown in the figure) can be used to rate limit hyperactive subscribers.



- The aggregate rate-limit entry at the top level specifies an overall limit (e.g., for downlink throughput, 10Gbps). The traffic aggregate of all the subscribers must adhere to this limit.
- All the subscriber-level entries (at the second level) do not have specific rate limits and are children of the aggregate rate-limit entry.

CLI Configuration

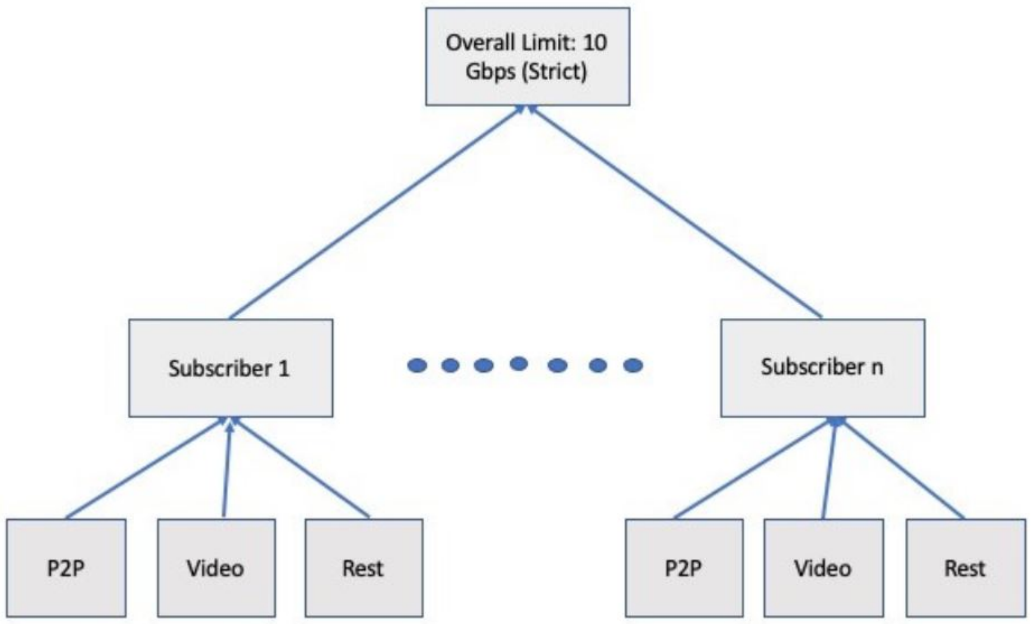
In the following configuration, template limit-policy 11 specifies the downlink throughput limit of 10Gbps and serves as the template for the parent rate-limit entry. Template limit-policy 22 is bound to the traffic-control rule identifying individual subscriber's traffic and hence serves as the template for children subscriber-level rate-limit entries.

```
template limit-policy  11
      limit-throughput downlink  10240
      limit-scope aggregate
      max-min-fair
template limit-policy  22
      limit-scope subscriber-ip
      parent  11
traffic-control rule-set hierarchical-traffic-control
      rule subscribers
            remark "rule to identify traffic for each subscriber "
            …
            action limit-policy  22
```

In this configuration, since no limits are associated with subscriber-level rate-limit entries, the parent rate-limit entry considers all children rate-limit entries as having the same weight while determining the fair-share for each subscriber. If the traffic exceeds 10Gbps, the heaviest subscribers are throttled so that the overall traffic is limited to 10Gbps. Configuring the `max-min-fair` tag in the parent template allows the parent rate-limit entry to distribute the unused fair-share of inactive subscribers among other subscribers.

Use Case 2: Application-Aware Rate Limiting at the Subscriber Level

The following configuration (as shown in the figure) provides aggregate rate-limiting at the top-level, along with **max-min-fair** support at the second (per-subscriber) level and third (application) level.



CLI Configuration

- The top-level template 1 specifies an overall limit (e.g. for downlink throughput, 10Gbps). The traffic aggregate of all the subscribers must adhere to this limit.
- The second-level template 10 specifies a relaxed downlink throughput limit of 10Mbps.
- Both templates 1 and 10 have the **max-min-fair** tag enabled.
- The third-level template 100 causes P2P traffic to be strictly limited to 1Mbps.
- The third-level template *101* allows video and “rest” traffic to use the remainder of the downlink throughput allocated to the subscriber.

```
template limit-policy 1
      limit-throughput downlink 10240
      limit-scope aggregate
      max-min-fair
template limit-policy 10
      limit-scope subscriber-prefix 64
      parent 1
      max-min-fair
      limit-throughput downlink 10 relaxed
template limit-policy 100
```

```
      limit-scope subscriber-prefix 64
      parent 10
      limit-throughput downlink 1
template limit-policy 101
      limit-scope subscriber-prefix 64
      parent 10

traffic-control rule-set hierarchical-traffic-control
      rule p2p_subscribers
            remark "rule to identify P2P  traffic for each subscriber "
            ….
            action limit-policy 100
      rule video_subscribers
            remark "rule to identify video  traffic for each subscriber "
            ….
            action limit-policy 101
      rule rest_of_the_traffic_subscribers
            remark "rule to identify rest of the traffic for each
subscriber "
            ….
            action limit-policy 101
```

As mentioned previously in Use Case 1: Rate Limiting Hyperactive Subscribers, if the traffic exceeds 10 Gbps, the heaviest subscribers are throttled so that the overall traffic is within limits. The unused fair-share of inactive subscribers is distributed among active subscribers with sufficient traffic. Additionally, the P2P traffic of each subscriber is strictly limited to 1Mbps (irrespective of the downlink throughput available to its subscriber) and the remainder of the subscriber’s allocated downlink throughput is shared among the subscriber’s video and other (non-P2P and non-video) traffic (in a **max-min-fair** manner).

Limitations

Hierarchical rate limiting has the following limitations:

- It is not supported for Packet-per-second rate-limiting.
- It is not supported for tunnelled traffic for lightweight 4 over 6, MAP-E, and GTP.
- It disallows concurrent session configuration.

- It is not possible to understand or determine the hierarchy and the rate-limits only by examining the traffic-control rules; you must check the template limit policies as well.
- A **`limit-concurrent-sessions`** configuration in a parent template limit-policy is not inherited by the children template limit-policies.
- A **`limit-scope subscriber-ip`** configuration in the parent template limit-policy is not supported for IPv6.

Rate Limiting Using RADIUS Attributes

This section describes rate limiting for domain users and user groups using RADIUS attributes and explains the features and configurations in detail.

The following topics are covered:

Overview

ACOS supports domain-based rate-limiting for subscribers by using a RADIUS custom attribute. Using this feature, users sharing the same domain can have individual rate-limits, while the domain can have an aggregated rate-limit. For example, users within the 'example' domain can be restricted to 500 Mbps per user, while the total throughput for the entire 'example' domain can be limited to 50 Gbps.

The following features are supported:

- Extraction of RADIUS derived attributes: ACOS extracts the information on domain user groups and individual users through RADIUS accounting messages.
- Granular control for dynamic rate-limiting: Rate-limiting policies can be configured for an individual subscriber, or a group of subscribers using hierarchical rate limiting.
- Supported rate-limiting types: The generic rate-limiting using RADIUS attributes supports connections per second (CPS), throughput, and concurrent sessions. However, the hierarchical rate-limiting only supports throughput and connections per second.

- Efficient traffic-control: Traffic control rules can be created to use the subscriber-related derived attributes from the RADIUS server and then be associated to configured rate-limiting policies.
- Single rule for IPv4 and IPv6: A single rule can be created to handle both IPv4 and IPv6 addresses for users and user groups by using the **ip-version** any option in the traffic-control rule-set.

Workflow

1. Individual subscribers or subscriber group from a domain can be configured as derived attributes in the system RADIUS server configuration.
2. ACOS parses the value of the derived RADIUS attributes per subscriber and stores them in the RADIUS session. The regular expression is used to extract the first matched sub-string from the value of the derived attribute.
3. Rate limit policies can be configured to limit the throughput for an associated subscriber or group.
4. Traffic control rule sets can be created to apply the specific policies. Additionally, class-lists can be configured with the string attribute and defined in the rule sets for the specific subscriber or group attributes.

Configuring Rate Limiting for Domain Users and Groups

Rate Limiting for domain users and groups considers the radius derived attributes received in RADIUS accounting messages. To configure generic rate-limits for a user group:

1. Configure the radius client.

```
ACOS(config)# ip-list radius-client1
ACOS(config-ip list)# 10.10.10.100
ACOS(config-ip list)# exit
```

2. In the RADIUS server configuration, specify the custom attributes and the derived attributes for domain user groups. The regular expression is used to extract the first matched sub-string from the value of the derived attribute. ACOS parses the value of the derived RADIUS attributes using regular expression (regex) and stores them in the RADIUS session.

```
ACOS(config)#system radius server
ACOS(config-radius-server)#remote ip-list radius-client1
ACOS(config-radius-server)#attribute custom1 username number 1
ACOS(config-radius-server)#attribute custom2 domain vendor 10101 number
20
ACOS(config-radius-server)#attribute inside-ip number 2
ACOS(config-radius-server)#attribute inside-ipv6 vendor 10101 number 29
ACOS(config-radius-server)#accounting start replace-entry
ACOS(config-radius-server)#derived-attribute usergroup attribute
custom1 regex @(\w+)
```

3. Configure a limit policy and set the total throughput limit for the user group.

```
ACOS(config)#template limit-policy 1
ACOS(config-limit-policy)#limit-throughput total 10000
ACOS(config-limit-policy)#limit-scope radius attribute usergroup
```

4. Configure Access-Control rule-sets with rules to permit traffic.

```
ACOS(config)#rule-set limit
ACOS(config-rule set:limit)#rule ipv4
ACOS(config-rule set:limit-rule:ipv4)#action permit
ACOS(config-rule set:limit-rule:ipv4)#source ipv4-address any
ACOS(config-rule set:limit-rule:ipv4)#source zone any
ACOS(config-rule set:limit-rule:ipv4)#dest ipv4-address any
ACOS(config-rule set:limit-rule:ipv4)#dest zone any
ACOS(config-rule set:limit-rule:ipv4)#service any
```

5. Activate the firewall rule-set.

```
ACOS(config)#fw active-rule-set limit
```

6. Configure traffic-control rule-sets with rules to apply traffic limits.

```
ACOS(config)#traffic-control rule-set ratelimit
ACOS(config-rule set:ratelimit)#rule ipv4
ACOS(config-rule set:ratelimit-rule:ipv4)#source ipv4-address any
ACOS(config-rule set:ratelimit-rule:ipv4)#action-group
ACOS(config-rule set:ratelimit-rule:ipv4-...)#action limit-policy 1
ACOS(config-rule set:ratelimit-rule:ipv4-...)#exit
ACOS(config-rule set:ratelimit-rule:ipv4)#rule ipv6
ACOS(config-rule set:ratelimit-rule:ipv6)#ip-version v6
ACOS(config-rule set:ratelimit-rule:ipv6)#action-group
ACOS(config-rule set:ratelimit-rule:ipv6-...)#action limit-policy 1
```

7. Activate the ratelimit traffic-control rule-set.

```
ACOS(config)#traffic-control active-rule-set ratelimit
```

When the RADIUS accounting messages are received, ACOS parses the value of the RADIUS derived attributes and gets information about domain user groups and users. As per the policy configuration, rate limits are applied to the specified user groups.

Show Commands

- To check the rate-limiting entries, use the **show fw rate-limit** command. The following example output displays the generic rate-limit entry and the hierarchical rate-limit entry:

```
ACOS(config)#show fw rate-limit
String ID IP Address  Prefix  Rule  Type  CPS-Received  CPS-Limit
Uplink-Received  Uplink-Limit  Downlink-Received  Downlink-Limit  Total-
Received  Total-Limit  Cumulative Dropped Packets
------------------------------------------------------------------------
------------------------------------------------------------------------
---------------
   10.10.10.100  32      1      2      Mbps   -             -
 -               -              -                       -
0.001               1000                -
   10.10.10.100  32      -      1      Mbps   -             -
 -               -              -                       -
0.001               10000               -
Total Rate Limit Entries Shown:2
```

- To view the value of derived attributes, use the **show system radius table** command. The following example output displays the RADIUS record with the values of the derived attributes:

```
ACOS(config-radius-server)#show system radius table
RADIUS Table Statistics:
-------------------------------------------------
Record Created                 1
Record Deleted                 0
Key Attribute          MSISDN             IMEI             IMSI
                                                           User-Name
                                                           Derived-
Attribute User Group
                                                           Derived-
Attribute User ID
------------------------------------------------------------------------
-
10.10.10.100
2001:10:10:10::240
username@domain


                                                           domain
                                                           username
Total RADIUS Records Shown: 1
```

- To filter based on a derived attribute and its value, use the **`show system radius table derived-attribute-name [usergroup | userid]`** command.

Hierarchical rate-limiting can be done for domain user groups and individual subscribers or individual IPs. For these and other configuration examples, see Rate Limiting Using RADIUS Attributes.

Limitations

Applying rate limiting for domain users and groups using RADIUS attributes has the following limitations:

- The hierarchical rate-limiting policy only supports rate-limiting throughput and connections per second (CPS).
- ACOS gets the derived attribute after it receives the RADIUS start and interim update accounting messages. If the parsing of the RADIUS derived attribute fails, rate limiting entries with new scope are not created based on the value of derived attribute. In such cases, it is necessary to resend the well-formed message to the ACOS device.
- The dynamic configuration of the derived attribute on the RADIUS server is only applied to the latest updated accounting messages. It does not affect the existing values of derived attributes per RADIUS session.
- In the dual-PU chassis and Scaleout setup, the rate-limiting per user ID is applied

only on the local node. Rate-limiting per user group is applied across the nodes.

- For dual-PU platforms and Scaleout clusters, the rate-limiting entry for the same user group or user ID does not support aggregation of traffic.

DDoS Protection

The Gi/SGi Firewall offers integrated DDoS protection to detect and mitigate DDoS attacks so that firewall operations are not disrupted, and the subscriber's connectivity is preserved. Firewall DDoS protection helps to block individual IP addresses or a subnet in case of a DDoS attack.

Attack Detection

DDoS protection can be enabled by specifying the **ddos-protection-factor** while configuring the Packet-Per-Second (PPS) threshold limit (in the template limit policy) as shown:

```
ACOS(config-limit-policy)# limit-pps downlink pps_limit <1-2147483647>
ddos-protection-factor <1-50>
```

Specifying the DDoS protection factor configures the DDoS protection threshold limit. This limit is the product of the PPS rate limiting threshold and DDoS protection factor.

The PPS threshold is checked per subscriber IP to detect a DDoS attack. When the downlink PPS exceeds the configured rate limiting threshold (specified by *pps_limit*), rate-limiting begins i.e., the excessive packets targeted towards a specific IP address are dropped. However, if the downlink PPS exceeds the DDoS protection threshold, a DDoS attack is detected.

Consider the following example command:

```
ACOS(config-limit-policy)# limit-pps downlink 100000 ddos-protection-
factor 3
```

In this case, when the downlink PPS exceeds 100000, rate-limiting begins. However, if the PPS exceeds 300000 (DDoS protection threshold), which is a value greater than the product of the PPS rate limiting threshold (100000) and the DDoS protection factor (3), a DDoS attack is detected.

The PPS threshold is configured under the template limit policy, which is bound to a firewall rule. The firewall rule can be classified as inbound or outbound based on the traffic origin.

- **Inbound Firewall rule**: A rule is considered inbound if the traffic initiates from the hosts that reside behind the **`ip server`** interfaces. If the rate limit policy is bound to an inbound rule, the downlink PPS traffic flowing from the hosts behind **`ip server`** interfaces to the hosts behind **`ip client`** interfaces is checked. In this scenario, rate-limit entries are tracked against public subscriber IPs.
- **Outbound Firewall rule**: A rule is considered outbound if the traffic initiates from the hosts that reside behind the **`ip client`** interface. If the rate limit policy is bound to an outbound rule, the downlink PPS traffic flowing from the subscribers (hosts behind **`ip client`** interfaces) to the hosts behind **`ip server`** interfaces is checked. In this scenario, rate-limit entries are tracked against client IP addresses.

Since the volumetric or DDoS attacks are initiated from the internet side (hosts that reside behind **`ip server`** interfaces), binding a rate limit policy to an outbound rule proves to be redundant and is therefore not advisable. To leverage the Firewall iDDoS functionality, it is highly recommended to bind the rate limit policy to an inbound rule.

In the following example, the rate limit policy is bound to an inbound firewall rule:

```
ACOS(config)# template limit-policy 123
ACOS(config-limit-policy)# limit-pps downlink 10000 ddos-protection-factor
3

ACOS(config)# rule-set firewall
ACOS(config-rule set:firewall)# rule rule_inbound
ACOS(config-rule set:firewall-rule:rule_inbound)# dest <public-subscriber-
ip>
ACOS(config-rule set:firewall-rule:rule_inbound)# action-group
ACOS(config-rule set:firewall-rule:rule_inbound-acti...)# permit forward
ACOS(config-rule set:firewall-rule:rule_inbound-acti...)# permit limit-
policy 123
```

NOTE: If a rate limit policy needs to be bound to an outbound rule, it should be used with transparent Firewall traffic only; usage with CGN traffic is not recommended.

Attack Mitigation

When a DDoS attack (targeted toward a specific IP address) is detected, Firewall performs the following:

- Marks the IP address unusable so that no new sessions are created for this IP address.
- Initiates the attack mitigation process by applying one of the following mitigation actions:
  - **Local Block**—Adds the IP to the local block list and drops the packets sent to the IP locally. This is the default action.

    Once the IP is added to the local block list, the firewall continues to monitor the attacks. If the attack is not detected during the `remove-wait` period, the firewall removes the IP from the local block list. The blocked list can contain up to 1024 IP addresses at any given moment. The `remove-wait` period is user configurable.
  - **Protection Based on RTBH**—Drops the packets to a specific destination using the Remotely Triggered Black Hole (RTBH) technique.

  By default, IP logging is enabled, and the event is logged for both actions. The logged event can be viewed using the `show log` command. The logs are generated by default when the firewall DDoS protection entries are added and removed. Only the Syslog format is supported.

NOTE: You can enable DDoS protection only for the Packets-Per-Second downlink traffic.

For configuration information, see Configuring DDoS Protection.

Remotely Triggered Black Hole

Remotely Triggered Black Hole (RTBH) is a routing technique that provides DDoS protection by dropping malicious traffic before it enters a protected network.

When a DDoS attack targeted towards a specific IP address is detected, the firewall marks the victim IP prefix with configured BGP community and advertises the IP prefix to the edge routers. The edge routers route all traffic coming towards the victim IP to a null route or a black hole i.e., the edge routers drop all traffic unconditionally from the network, thereby mitigating the DDoS attack.

This technique can be configured using the **redistribute-route** action under **fw ddos-protection**.

```
ACOS(config)# fw ddos-protection action redistribute-route mymap
```

Here, *mymap* is the route map that must be specified for routing or redirecting the traffic.

When the RTBH configuration comes into effect:

- All traffic is unconditionally dropped
- The victim IP is blackholed and is inaccessible
- Rate limiting is discontinued

However, in certain scenarios, it may be necessary to access the victim IP. Consider an example where the victim IP is a DNS server. If ACOS detects a DDoS attack and triggers the RTBH action, all traffic to the DNS server will be dropped unconditionally. Although the attack is mitigated, the DNS server users will be unable to access the DNS service. In such situations, you can specify the **forward** option while configuring the RTBH action.

```
ACOS(config)# fw ddos-protection action redistribute-route mymap forward
```

When this option is configured, ACOS forwards the traffic (instead of dropping it unconditionally) and continues to rate-limit the traffic directed to the victim IP. This allows subscribers to access the service even when RTBH is in effect.

Additional parameters such as **expiration**, **remove-wait-timer** and **timer-multiply-max** can also be configured.

These parameters govern the overall flow of the following events when RTBH is in effect:

1. A timer, also known as blackhole timer (configured using the **expiration** parameter), determines the duration the blackhole route must be disabled when a DDoS attack is detected. When this timer expires, ACOS removes the blackhole route remotely without enabling the blackholed IP and applies a wait period of five minutes (configured using **remove-wait** parameter).

2. During the remove-wait period, if ACOS detects an attack again, it re-initiates the blackhole entry and extends the blackhole timer by a duration that is twice the expiration time (for the first time).
3. The second time, the duration is thrice the expiration time and this duration continues to increment until it reaches the maximum limit specified by the **`timer-multiply-max`** parameter.
4. If ACOS does not detect attacks during the remove-wait period, it removes the blackhole entry completely and starts forwarding packets to the IP address.

For configuration information, see Configuring DDoS Protection.

DDoS Protection for Deny Rules

To increase the security level and infrastructure protection capabilities, the Deny rules can be bound to a DDoS rate-limiting policy template. Binding the policy to the rule allows the dropped packets to be tracked separately. When the number of packets exceeds the configured DDoS protection threshold, a DDoS attack is detected.

Once the attack is detected, the upstream router can be signalled so that the network can provide DDoS mitigation for this Border Gateway Protocol (BGP) announcement. Likewise, the router can be signalled to blackhole the traffic destined for the victim IP (see Remotely Triggered Black Hole). So, this technique enables early detection and mitigation of DDoS attacks and provides infrastructure protection to the Gi Firewall layer as well.

NOTE: The limit-policy template cannot be bound to an implicit deny rule. You must configure an explicit deny rule for this mechanism to function as expected.

Limitations:

- Only supported for Packets-Per-Second (PPS) downlink traffic.
- Only supported for the Access control rule-set i.e., the DDoS rate limit policy cannot be bound to a deny rule configured under the Traffic control rule-set.
- Only supported for an inbound rule. Therefore, it is highly recommended to

configure the inside interface and the outside interface (using the ip nat inside/outside command) before configuring rate-limiting.

CLI Configuration:

In the following configuration example, a DDoS rate limiting policy (10) is bound to a deny rule. Additionally, the inside and outside interfaces are also configured.

```
ACOS(config)# template limit-policy 10
ACOS(config-limit-policy)# limit-pps downlink 10 ddos-protection-factor 2

ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# ip address 30.1.1.11 255.255.255.0
ACOS(config-if:ethernet:1)# ip nat inside
ACOS(config-if:ethernet:1)# exit

ACOS(config)# interface ethernet 2
ACOS(config-if:ethernet:2)# enable
ACOS(config-if:ethernet:2)# ip address 20.1.1.21 255.255.255.0
ACOS(config-if:ethernet:2)# ip nat outside
ACOS(config-if:ethernet:2)# exit

ACOS(config)# rule-set firewall
ACOS(config-rule set:firewall)# rule r1
ACOS(config-rule set:firewall-rule:1)# source ipv4-address any
ACOS(config-rule set:firewall-rule:1)# source zone any
ACOS(config-rule set:firewall-rule:1)# dest ipv4-address 10.1.1.0/32
ACOS(config-rule set:firewall-rule:1)# dest zone any
ACOS(config-rule set:firewall-rule:1)# service any
ACOS(config-rule set:firewall-rule:1)# application any
ACOS(config-rule set:firewall-rule:1)# action-group
ACOS(config-rule set:firewall-rule:1-acti...)# deny limit-policy 10
```

In this example, when the downlink PPS traffic exceeds the configured limit of 10, rate-limiting begins i.e., ACOS starts dropping the excess packets. However, when the PPS exceeds 20 (the product of the PPS threshold limit and DDoS protection factor), the DDoS rate limit policy applied to the deny rule comes into effect and detects a DDoS attack.

You can execute the **`show fw rate-limit`** and **`show fw ddos-protection entries`** commands to view the rate-limit entries and DDoS entries created when the DDoS protection threshold is breached.

Example output for **`show fw rate-limit`** command:

```
ACOS(config)# show fw rate-limit
IP Address  Prefix  Rule  Template  Type  CPS-Received  CPS-Limit  Uplink-
Received  Uplink-Limit  Downlink-Received  Downlink-Limit  Total-Received
Total-Limit  Cumulative Dropped Packets
--------------------------------------------------------------------------
--------------------------------------------------------------------------
----------------------------------------
10.1.1.1    32      1     10        PPS   -             -          -
         -             20
10              -               -            189
Total Rate Limit Entries Shown: 1
```

NOTE: If **`fw ddos-protection dynamic-blacklist`** is configured, the rate-limit entries for the blacklist sessions are also displayed.

Example output for **`show fw ddos-protection`** entries command:

```
ACOS(config)# show fw ddos-protection entries
IP Address  Prefix  Rule  PPS  Expiration  Hints
------------------------------------------------
10.1.1.1    32      1     0    3589        -
```

For command details, refer to the *Command Line Reference Guide*.

Logging for DDoS Protection

Event logging for DDoS protection must be enabled in order to log and view the blocked IP addresses. Even if the configured action is to log an event when an IP is under a DDoS attack, the event will not be logged if DDoS protection logging is disabled.

When enabling the DDoS protection logging, you can choose to send the logs to the logging servers as follows:

- Local—Logs are sent to the local buffer and can be viewed using the **`show log`** command.
- Remote—Logs are sent to the remote Syslog server and IPFIX collectors.
- Both—Logs are sent to both local buffer and remote servers.

The log protocols supported are Syslog and NetFlow. For Syslog, both CEF and ASCII formats are supported.

For information about configuration, see Enabling Logging for DDoS Protection.

Gi/SGi Firewall on Multi-PU Platforms

On multi-PU platforms (such as TH14045 or TH7650/TH7655S), the GiFW traffic is distributed across multiple Processing Units (multi-PUs).

Since the traffic from the client is hashed based on the source IP and the traffic of the server is hashed based on the destination IP, it ensures that traffic belonging to a given session always returns to the same PU.

To configure IPv4 and IPv6 traffic to be distributed across PUs, under the interface configuration level, use the **`ip client`** command to turn on the interface of the client side; use the **`ip server`** command to turn on the interface of the server side.

Consider the following points while configuring:

- Do not configure both **`ip client`** and **`ip server`** under the same interface. The **`ip client`** command should be configured on the client-facing interface and **`ip server`** should be configured on the server-facing interface. Additionally, **`ip dmz`** (if required) should be configured on the DMZ-facing interface.
- Do not configure the commands **`map inside`**, **`map outside`**, **`lw4o6 inside`**, and **`lw4o6 outside`** along with **`ip client`** and **`ip server`** since the firewall does not support MAP-E, MAP-T, and LW4o6 features.

Known Limitations

- Only LSN/NAT64/Fixed-NAT44/Fixed-NAT64 are supported.
- For Firewall flows (no NAT), only ALG SIP/TFTP/FTP/PPTP/RTSP are supported.

- In a multi-PU system, traffic distribution between the PUs is based on source IP. In the case of rate-limiting configured with scope aggregate or subscriber-prefix, traffic that matches that scope is distributed across both PUs. Each PU applies the full limit.
- In case of Scaleout, the Subscriber-prefix and the aggregate level rate limiting is applied at a PU level.

For the configuration information, see Configuring Gi/SGi Firewall on Multi-PU Platform.

Rate-Limiting for Scaleout Cluster and Multi-PU Platform

Rate-limiting for multi-PU platforms (TH14045, TH7650, TH7655S) and Scaleout clusters depends on the aggregation level reflected in the **limit-scope** configuration associated with the rate-limit entries. The rate limit enforced on each or multiple nodes/PUs in the Scaleout cluster or Multi-PU configuration is based on the **limit-scope** configured in the template limit policy.

Rate Limiting for Scope Subscriber IP or Subscriber-Prefix

In a Scaleout cluster or a Multi-PU environment, if the scope associated with a rate limit entry is **subscriber-ip** or **subscriber-prefix**, all traffic belonging to a particular subscriber must be directed to a single PU or node to ensure proper rate-limiting. This can be achieved by configuring the **ipv6-prefix-length** correctly.

The **ipv6-prefix-length** command is a system-level attribute that indicates the length of the source and destination IPv6 prefix. This prefix is used to determine the user group for processing a packet. All packets with the same prefix length in the source IPv6 address will map to the same user group and hence be processed by the same node in the Scaleout cluster (or multi-PU environment). For more information about **ipv6-prefix-length**, see *Command Line Reference Guide* and *Scaleout Configuration Guide*.

Consider the following special scenarios and the corresponding prefix length to be configured:

- In a configuration with multiple subscriber prefixes being used, the **ipv6-prefix-length** should be set to the smallest prefix-length being used. This will ensure that the traffic belonging to a single subscriber always arrives at a single PU. For example, if one subscriber uses a 64-bit prefix and the other uses a 96-bit prefix, the **`ipv6-prefix-length`** should be set to 64.

- In hierarchical rate-limiting, if the subscriber prefix-length used by the parent entry is different as compared to the child entry, the **`ipv6-prefix-length`** must be set to the parent's subscriber prefix-length (smaller). For example, if the parent entry uses a subscriber prefix-length of 64 while the child uses a prefix-length of 96, the **`ipv6-prefix-length`** must be set to 64 to ensure that all the traffic belonging to a single subscriber (that matches the parent entry as well as the child entry) hits a single PU.

  Applying this principle throughout a hierarchy and across all hierarchies that exist on the cluster or a Multi-PU platform implies that the **`ipv6-prefix-length`** should be set to the smallest subscriber prefix-length configured as the scope in any template limit-policy being used in any of the hierarchies.

NOTE: A Scaleout cluster or a Multi-PU should not use the rate-limit hierarchy with a parent entry with scope **`aggregate`** and a child entry with scope **`subscriber-prefix`** or **`subscriber-ip`**.

Distributed Rate Limiting for Aggregated Scope

In a Scaleout cluster or a Multi-PU environment, if rate-limiting needs to be applied to multiple subscribers processed by multiple nodes/PUs (i.e., scope associated with a rate limit entry is **`aggregate`**), the traffic to be limited cannot be directed to a single PU (or node); the packets land on multiple PUs (or nodes) in the Multi-PU or the cluster. In such cases, distributed rate limiting is enforced to ensure a uniform division of resources across PUs.

Distributed rate limiting is applicable in the following scenarios:

- **Scaleout cluster** – Packets land on multiple nodes in the cluster

  Every node in the Scaleout cluster periodically checks the current number of active nodes (n) in the cluster and utilizes an effective rate-limit, which is 1/n times the configured rate-limit. For example: If the configured rate limit is 20 Mbps and there are five nodes currently active in the cluster, each node in the cluster will enforce a rate-limit of 4 Mbps (20/4).

- **Multi-PU Platform** - Packets land on both PUs

  Rate limit distribution depends on whether the PUs are part of a Scaleout cluster.

  - If the PUs are not part of a Scaleout cluster, each PU periodically checks the current number of PUs (m) in the node and utilizes an effective rate-limit, which is 1/m times the configured rate-limit. For example, in a Multi-PU platform, if the configured rate limit is 20 Mbps, each PU will enforce a rate-limit of 10 Mbps (20/2).
  - If the PUs are part of a Scaleout cluster, each PU periodically checks the current number of active nodes (n) in the cluster as well as the current number of PUs (m) in the node and then utilizes an effective rate-limit, which is 1/(m*n) times the configured rate-limit. For example: In a Multi-PU platform, if the configured rate limit is 20 Mbps and there are five nodes in the cluster, each PU will enforce a rate-limit of 2 Mbps (20/2*5).

NOTE: Rate-limiting accuracy depends on whether the traffic distribution is balanced between nodes or PUs. If all the nodes or PUs receive traffic (roughly) equally, the enforced rate limit will be in accordance with the above-mentioned distribution scheme.

Distributed Rate Limiting Limitations

- Only applicable for rate-limit entries with scope `aggregate`.
- Does not create a shadow session if rate-limit is configured for the flow. Shadow sessions mimic the Active node sessions and help minimize the redirection of packets.

Supporting DMZ Interfaces

This topic provides a brief overview of the DMZ network and describes the configurations required to support the DMZ network in a Firewall deployment.

The following topics are covered:

Demilitarized Zone Overview

A Demilitarized Zone (DMZ) is a physical or logical perimeter network that separates an organization's internal local-area network from untrusted networks by adding an extra layer of security. This network is typically placed between the subscriber network (protected internal network) and the untrusted network (mostly the Internet).

External-facing servers, resources, and popular services such as web, email, domain name systems, and proxy servers are usually placed in the DMZ. These servers and resources can be accessed from the internet, but the rest of the internal LAN is unreachable. Due to this extra layer of security, attackers (from the internet) cannot directly access the internal servers and sensitive data. However, since the services located in the DMZ can have access to the internal LAN and sensitive data, the connections between the DMZ-based systems and the internal LAN require additional protection against malicious content.

Firewall Deployment with DMZ

In a typical firewall deployment, as shown in Figure 31, the traffic flows within two interfaces. The orange arrows indicate the uplink traffic flowing from client network (`ip client/ip nat inside`) to the internet (`ip server/ip nat outside`) and the blue arrows indicate downlink traffic flowing from the internet (`ip server/ip nat outside`) to the subscriber network (`ip client/ip nat inside`).

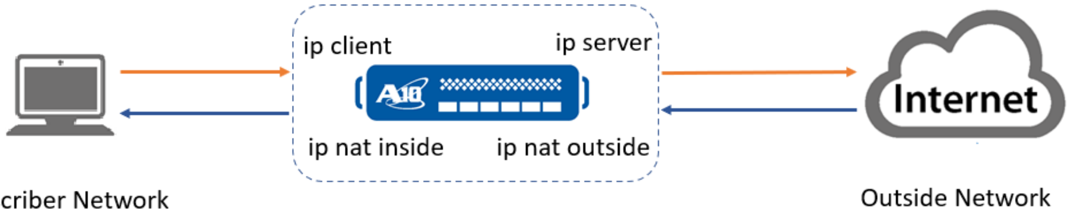


Figure 31 : Firewall Deployment shown with interface tags

ACOS uses the `ip dmz` interface tag to identify and support the DMZ-facing interfaces. With a DMZ in the network, the traffic can flow between DMZ (`ip dmz`) to the inside interface (`ip client` or `ip nat inside`) and/or DMZ (`ip dmz`) to the outside interface (`ip server` or `ip nat outside`).

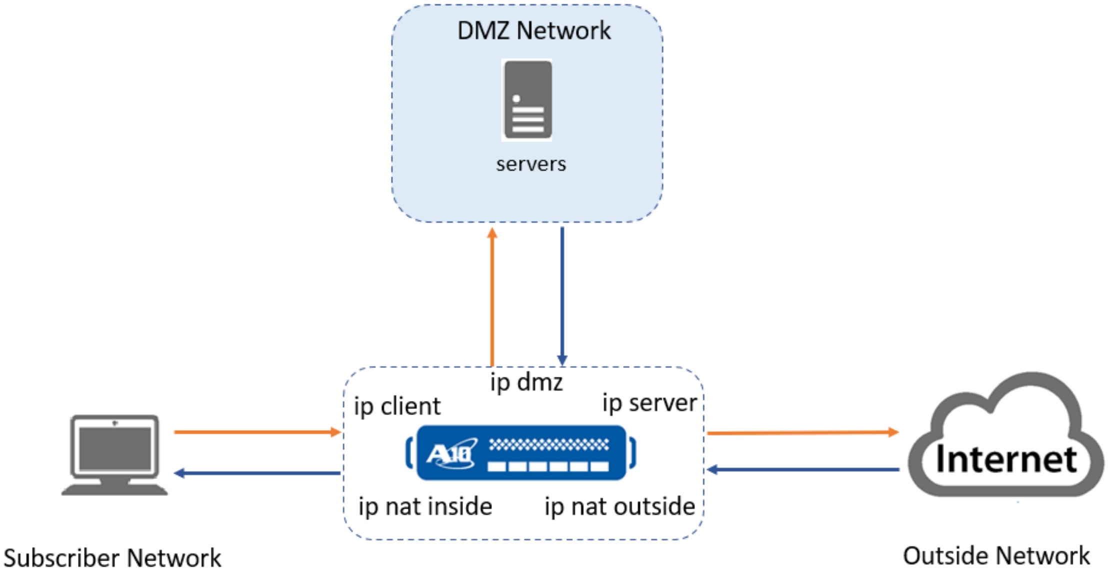


Figure 32 : Firewall Deployment with DMZ Network

The traffic flow between DMZ and other interfaces needs to be inspected to detect and block malicious content before it crosses the boundary from the Internet to the DMZ and from the DMZ to the protected internal network. The Firewall rules must be configured effectively to enforce access control as well as monitor and block malicious traffic flowing within DMZ and other interfaces.

CLI Configuration

This section describes the configurations required to support DMZ in an L3 Firewall deployment.

The overall configuration steps are similar to those required for a typical Firewall deployment (see Gi/SGi Firewall Configurations). However, to support DMZ, you need to configure the following as well:

1. Configure the interface tags for the subscriber network (**`ip client/ip nat inside`**), the internet or outside network (**`ip server/ip nat outside`**), and DMZ network (**`ip dmz`**).

   Since the behavior of many Firewall features depends on identifying the interface from which the traffic is originating (subscriber, internet, or a DMZ-based server) the interfaces need to be configured with the appropriate interface tags.

2. Configure the Firewall rules that define the action to be taken when the criteria match. The rules can set the action to forward the subscriber IP to the outside network or the DMZ network with or without being NATted (translated), etc.

Consider the following deployment example that is used to explain firewall rule configuration for different traffic flows and the action to be taken in some peculiar cases.

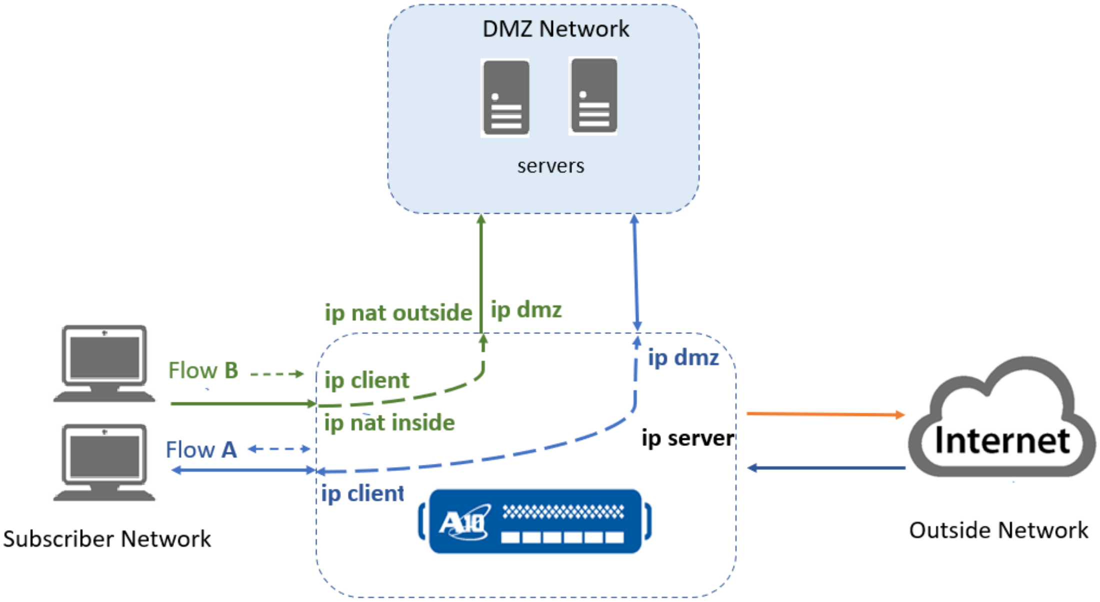


Figure 33 : Firewall deployment with DMZ network - Traffic flow example

In the above deployment (as shown in Figure 33), two subscribers need to communicate with two different servers placed in the DMZ network. However, only for one subscriber, the source IP address needs to be translated before being forwarded to the DMZ network.

The following traffic flows are possible:

- **Flow A** indicates the traffic flowing from a Subscriber to a server in the DMZ network and vice versa (without being translated). The uplink traffic consists of requests from the Subscriber to the DMZ-based server and the response from the DMZ server to the original subscriber. Since the traffic is not translated, `ip nat outside` tag is not configured on the DMZ-facing interface. The blue arrows indicate this bidirectional flow.

- **Flow B** indicates the traffic flowing from a subscriber to a server in the DMZ network after being translated (NATted). The **`ip nat outside`** tag needs to be configured for the source NAT to happen when traffic flows from the subscriber to the DMZ-based server. The green arrows indicate this traffic flow.

CLI Configuration for Flow A

1. Configure the subscriber and DMZ facing interfaces.

```
interface ve 3230 (or interface ethernet 1)
 ip address 10.0.1.18 255.255.255.0
 ip client
!
interface ve 3240 (or interface ethernet 2)
 ip address 10.0.2.18 255.255.255.0
 ip dmz
!
```

2. Configure the zones for the firewall rules.

```
zone inside
 interface ve 3230
!
zone dmz
 interface ve 3240
!
```

3. Configure the firewall rule-set with match criteria such that **`rule1`** allows the traffic to flow from the subscriber network (client) to the DMZ network (without translating it).

```
rule-set fw1
 rule rule1
  action permit
  source ipv4-address any
  source zone inside
  dest ipv4-address any
  dest zone dmz
  service any
 !
```

CLI Configuration for Flow B

1. In this case, since the subscriber address needs to be translated, configure the interface tags **ip nat inside** and **ip client** on the subscriber interface. Similarly, configure the tags **ip nat outside** and **ip dmz** on the DMZ interface.

```
interface ve 3250
 ip address 10.0.3.18 255.255.255.0
 ip client
 ip nat inside
!
interface ve 3260
 ip address 10.0.4.18 255.255.255.0
 ip dmz
 ip nat outside
!
zone inside
 interface ve 3250
!
zone dmz
 interface ve 3260
!
```

2. Configure the firewall rule for traffic flowing from the subscriber network (client) to the DMZ network with match criteria based on the source and destination IP addresses. When the traffic matches the specified source and destination IP addresses, the source IP of the subscriber gets NATted (translated) as it goes toward the host in the DMZ network.

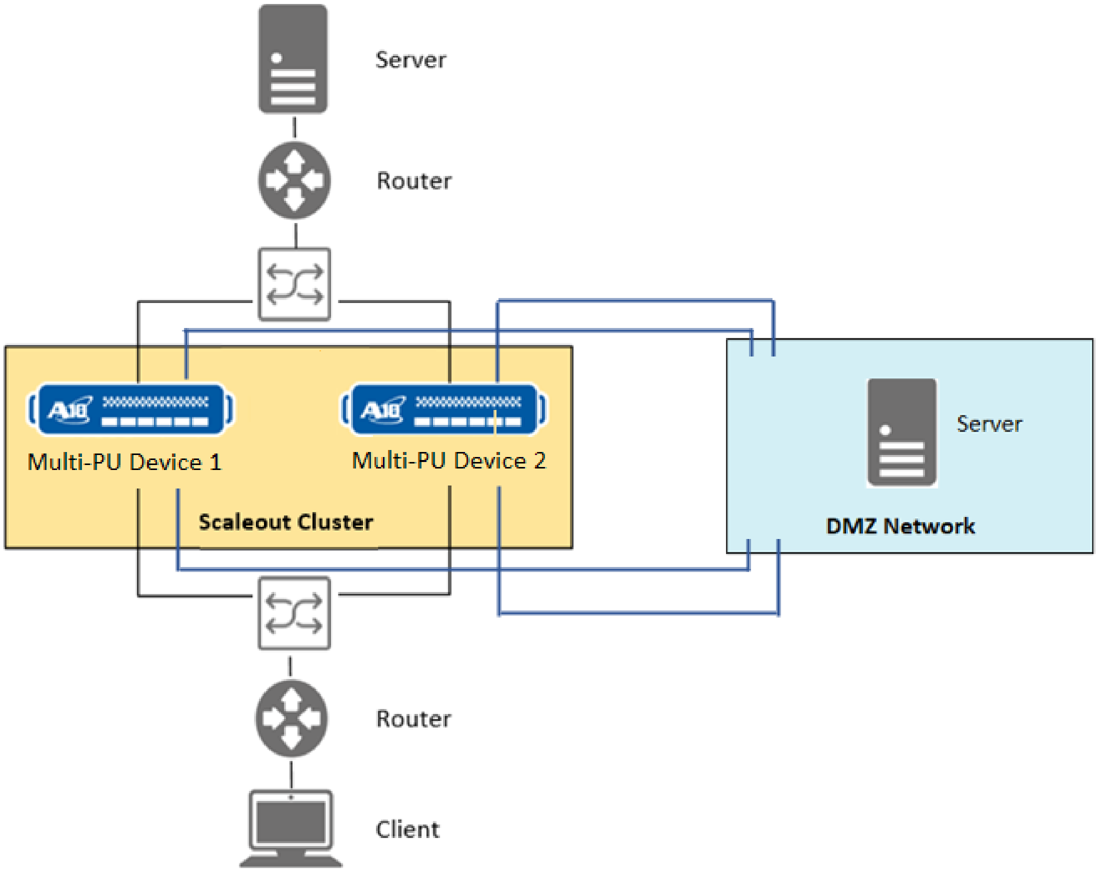
```
rule-set fw1
 rule rule1
  source ipv4-address 12.10.10.10/24
  source zone inside
  dest ipv4-address 9.9.9.173/32
  dest zone dmz
  service any
action permit cgnv6
!
```

As demonstrated above, by setting the appropriate match criteria and the action to be performed, rules can be configured for other traffic flows like DMZ to server, server to DMZ, etc.

Multi-PU Platform Support

In an architecture that consists of multiple Processing Units (PUs), ACOS needs to distribute the incoming traffic across these PUs. On such platforms, CGN and Firewall symmetrically distribute the incoming traffic so that the same PU is chosen for processing the uplink and downlink traffic within each data session.

However, the traffic flow changes when a Demilitarized Zone (DMZ) is introduced in the network. The DMZ is typically placed between the subscriber network and the internet.

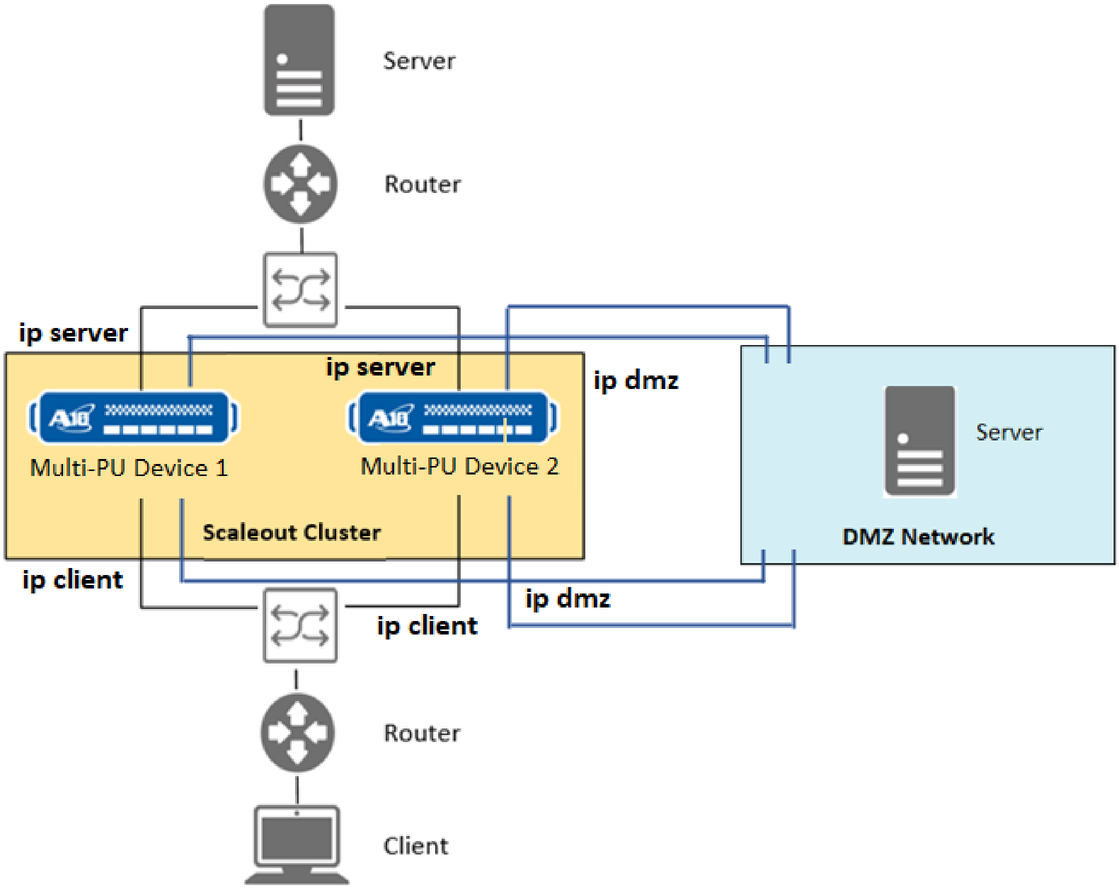


With a DMZ in the network, the traffic can flow between DMZ to the inside interface (`ip client` or `ip nat inside`) and/or DMZ to the outside interface (`ip server` or `ip nat outside`).

In such scenarios, to distribute the traffic symmetrically for both uplink and downlink traffic you need to configure the interfaces appropriately and set the traffic distribution mode. However, these configurations are deployment dependent. This section describes the configuration steps and other details to support traffic flow to a DMZ interface for the following deployments:

- Multi-PU Devices in a Scaleout Cluster
- Single-PU Devices in a Scaleout Cluster
- Standalone Multi-PU Device
- Standalone Single-PU Device

Multi-PU Devices in a Scaleout Cluster



In this deployment, multiple multi-PU devices are connected in a Scaleout cluster. Each device has two processing units, the master (PU1) and the blade (PU2). In the Scaleout cluster, each PU of the device serves as a node that processes incoming traffic and acts as a traffic classification and distribution engine.

CLI Configuration

Multi-PU platforms employ MAC-based traffic engineering and rely on Broadcom (BRCM) to distribute the traffic symmetrically across PUs. Although the basic configuration steps are similar to the ones mentioned in Configuring Gi/SGi Firewall on Multi-PU Platform, to support traffic flow across client, server, and DMZ interfaces, you need to configure the following as well:

1. Configure the interface connected to the DMZ network.

   - For **L3 mode**, use the **`ip dmz`** tag to configure the ethernet interface.

     Example configuration:

     ```
     interface ethernet 211
      enable
      ip address 211.1.1.1 255.255.255.0
      ip dmz
     ```

   - For **L2 mode**, configure the **`traffic-distribution-mode`** as **`l3-lookup`**.

     This traffic distribution mode can be configured either for the VLAN interface or the ethernet interface.

     Example configuration for VLAN interface:

     ```
     vlan 211
      tagged ethernet 13
      router-interface ve 211
      traffic-distribution-mode l3-lookup
     ```

     Example configuration for ethernet interface:

     ```
     interface ethernet 211
      enable
      ip address 211.1.1.1 255.255.255.0
      traffic-distribution-mode l3-lookup
     ```

```
ip dmz
```

NOTE: In most of the example configurations in this section, the traffic distribution mode is configured for the ethernet interface.

Example configuration for traffic initiated from Client-to-DMZ interface:

L3 mode:

```
interface ve 102
 ip address 102.1.1.1 255.255.255.0
 ip client
 ipv6 address 4011::1/64
!
interface ve 211
 ip address 211.1.1.1 255.255.255.0
 ip dmz
 ipv6 address 5012::1/64
!
```

L2 mode:

```
interface ve 102
 ip address 102.1.1.1 255.255.255.0
 traffic-distribution-mode sip
 ip client
 ipv6 address 4011::1/64
!
interface ve 211
 ip address 211.1.1.1 255.255.255.0
 traffic-distribution-mode l3-lookup
 ip dmz
 ipv6 address 5012::1/64
!
```

For configurations of traffic flowing across other interfaces (for example, DMZ-to-server, DMZ-to-client), see Interface Configurations.

2. Configure a list of client IP addresses using the `fw client class-list` command. This list is used by ACOS to identify the inside network and ensure consistent hashing of uplink and downlink traffic on multi-PU platforms.

In case of Firewall, all IP addresses/subnets identifying the inside network (behind the **ip client** interface) need to be added to this list. Similarly, in case of CGNAT, all public IPs/subnets or NATted pools must be added to this list.

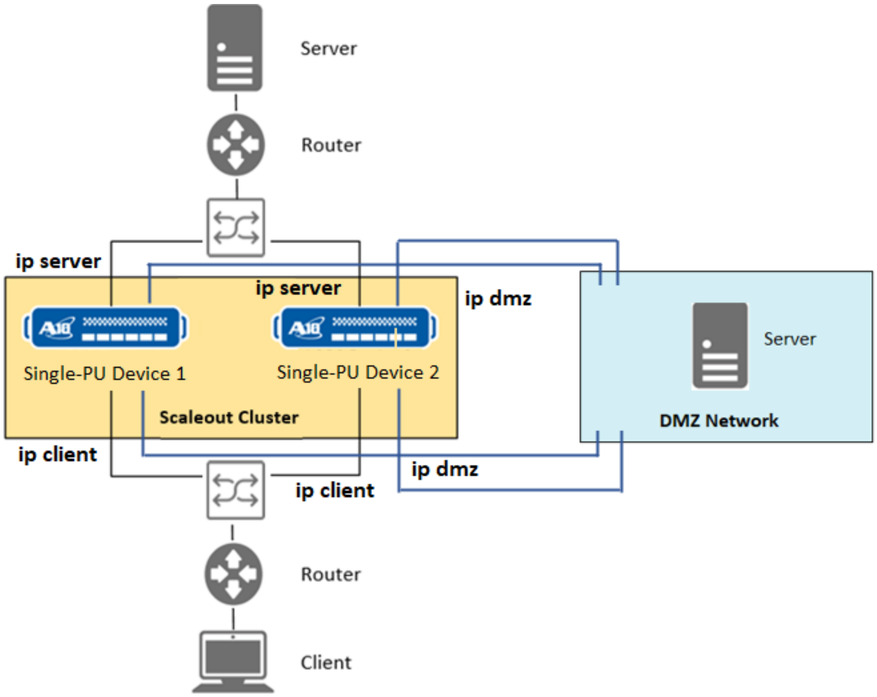
NOTE: In case of CGN, every NAT-pool change i.e., addition or removal of Subnet/IP address must reflect in the class-list entries to ensure consistent hashing on multi-PU platforms.

Example configuration:

```
class-list s2-list
11.1.1.4/32
11.1.1.1/32

fw client class-list ipv4 s2-list
```

For detailed configuration, see Consolidated Configuration Example to Support DMZ.

Single-PU Devices in a Scaleout Cluster

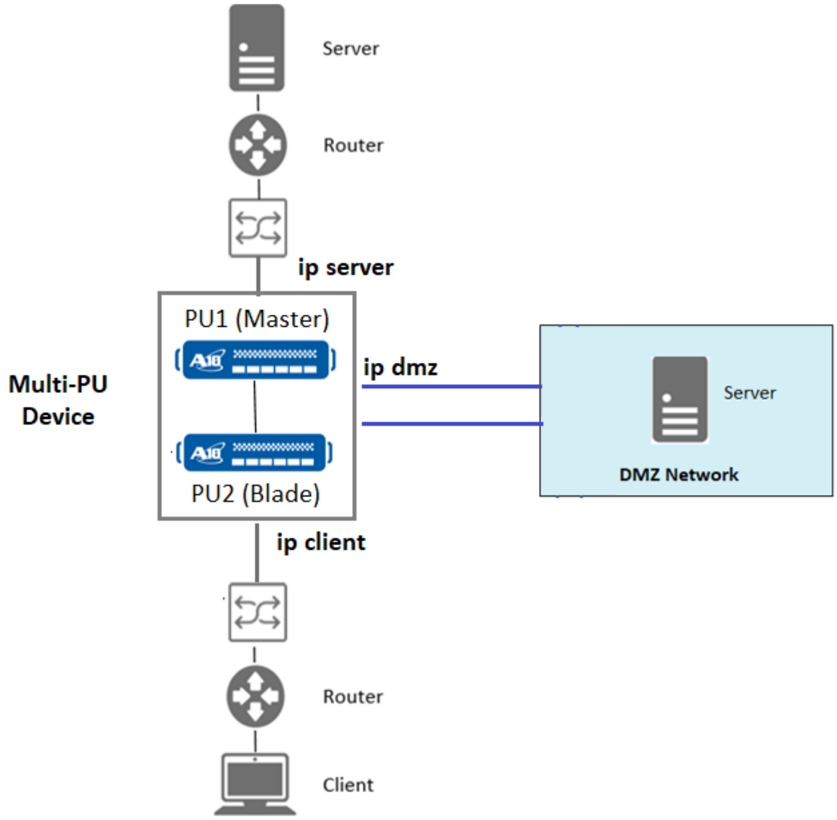


In this deployment, multiple Single-PU devices are connected in a Scaleout cluster. Each device in the cluster is a service node that processes incoming traffic and acts as a traffic classification and distribution engine. Even in this case, the uplink and downlink traffic needs to be distributed symmetrically so that the traffic lands on the same node of the Scaleout cluster.

Single-PU platforms only rely on interface tags (**`ip client`**/**`ip nat inside`**/**`ip server`**/**`ip nat outside`**/**`ip dmz`**) to understand the packet direction. Therefore, in this case, you only need to configure the client, server, and DMZ-facing interfaces using the interface tags.

For more details, refer to the Interface Configurations.

Standalone Multi-PU Device



This deployment only consists of a single multi-PU device, which is not part of a Scaleout cluster. This device has two processing units, the master (PU1) and the blade (PU2). In this case, the uplink and downlink traffic needs to land on the same

PU for processing. The configuration for this deployment is the same as that mentioned for Multi-PU Devices in a Scaleout Cluster.

Standalone Single-PU Device

This deployment only consists of one Single-PU device, which is not part of a Scaleout cluster. In this case, since there is only one node for processing the traffic, traffic distribution is not required. However, you need to configure the client, server, and DMZ-facing interfaces using the interface tags.

For more details, refer to Interface Configurations.

CLI Configuration

Consider the following points while configuring the support for DMZ interface:

- The interface tags **`ip client`**, **`ip server`**, and **`ip dmz`** are mutually exclusive; they cannot be configured on the same interface.
- The interface tags **`ip nat inside`** and **`ip dmz`** are mutually exclusive; they cannot be configured on the same interface.
- The interface tags **`ip dmz`** and **`ip nat outside`** can be configured on the same interface.

NOTE: To ensure that a network conversation is NATted, **`ip nat-inside`** and **`ip nat-outside`** tags must be configured for both uplink and downlink directions. However, conversations occurring between interfaces, such as **`ip nat-inside`** and **`ip dmz`** (only) or **`ip dmz`** and **`ip nat-outside`** do not undergo NAT. To NAT a conversation within the DMZ, you must configure the **`ip nat-outside tag`** along with the **`ip dmz`** tag.

- The **`ip client`** and **`ip server`** commands are supported in the Firewall-mode only. Similarly, **`ip nat inside`** and **`ip nat outside`** commands are only supported for CGN only.
- The commands **`traffic-distribution-mode l3-lookup`** and **`fw client class-list`** are only supported on multi-PU platforms.

Consolidated Configuration Example to Support DMZ

The following consolidated configuration is for an L3 Firewall deployed on a single node (of a multi-PU device), connected in a Scaleout cluster, facilitating traffic flow from client-to-DMZ. For other traffic flow configurations, refer to Interface Configurations.

```
!Current configuration: 1218 bytes
!Configuration last updated at 09:07:53 IST Thu Mar 30 2023
!Configuration last saved at 08:37:22 IST Thu Mar 30 2023
!64-bit Advanced Core OS (ACOS) version 5.2.1-P7, build 121 (Mar-29-
2023,13:47)
!
! multi-ctrl-cpu 2
!
no terminal auto-size
terminal length 0
terminal width 0
!
vlan 18
 tagged ethernet 1
 router-interface ve 18
!
vlan 52
 tagged ethernet 1
 router-interface ve 52
!
vlan 102
 tagged ethernet 1
 router-interface ve 102
!
vlan 212
 tagged ethernet 13
 router-interface ve 212
 traffic-distribution-mode l3-lookup
!
partition l3v id 1
!
!
interface management
 ip address 10.65.20.46 255.255.255.0
 ip default-gateway 10.65.20.1
!
interface ethernet 1
 enable
!
interface ethernet 2
!
interface ethernet 3
 enable
!
interface ethernet 4
!
interface ethernet 5
!
interface ethernet 6
!
interface ethernet 7
!
interface ethernet 8
!
interface ethernet 9
 enable
!
interface ethernet 10
!
interface ethernet 11
!
interface ethernet 12
!
interface ethernet 13
 enable
!
interface ethernet 14
!
interface ethernet 15
!
interface ethernet 16
!
interface ethernet 17
 enable
```

```
!
interface ethernet 18
!
interface ethernet 19
!
interface ethernet 20
!
interface ve 18
 ip address 18.1.1.2 255.255.255.0
!
interface ve 52
 ip address 52.1.1.1 255.255.255.0
! L3 mode: Client <---> DMZ Configuration
interface ve 102
 ip address 102.1.1.2 255.255.255.0
 ip client
 ipv6 address 4011::2/64
!
interface ve 212
 ip address 212.1.1.1 255.255.255.0
 ip dmz
 ipv6 address 5013::1/64
 ipv6 enable
!
!
ip route 11.1.1.0 /24 102.1.1.10
!
ip route 51.1.1.0 /24 52.1.1.10
!
ipv6 route 3010::/64 4011::10
!
ipv6 route 3020::/64 5013::10
!
scaleout 1
 local-device
  priority 199
  id 2
  cluster-mode layer-3
 cluster-devices
  device-id 1
```

```
   ip 51.1.1.1
  device-id 2
   ip 52.1.1.1
!
scaleout apps enable
!
class-list s1
 3010::/64
!
class-list s2
 11.1.1.1/32
 11.1.1.4/32
!
zone dmz
 interface ve 212
!
zone inside
 interface ve 102
!
router bgp 100
 bgp router-id 5.5.5.5
 neighbor 212.1.1.2 remote-as 100
 neighbor 212.1.1.2 fall-over bfd
 neighbor 212.1.1.2 route-map scaleout-event out
 neighbor 5013::10 remote-as 100
 neighbor 5013::10 route-map scaleout-event out
 redistribute ip-nat
 address-family ipv6
 neighbor 5013::10 activate
 redistribute ip-nat
!
route-map scaleout-event permit 10
 match scaleout 1 up
!
!
rule-set fw1
 rule rule1
  action permit
  source ipv4-address any
  source zone inside
  dest ipv4-address any
  dest zone dmz
  service any
 rule rule2
  action permit
  source ipv4-address any
  source zone dmz
  dest ipv4-address any
  dest zone inside
  service any
!
rule-set fwv6
 rule rule3
  ip-version v6
  action permit
  source ipv6-address any
  source zone inside
  dest ipv6-address any
  dest zone dmz
  service any
 rule rule4
  ip-version v6
  action permit
  source ipv6-address any
  source zone dmz
  dest ipv6-address any
  dest zone inside
  service any
!
fw active-rule-set fw1
!
fw client class-list ipv4 s2
!
end
!Current config commit point for partition 0 is 0 & config mode is
classical-mode
```

Interface Configurations

This topic provides configurations for various traffic flow combinations across the client, server, and DMZ interfaces.

- Client-to-Server Traffic Flow
- Client-to-DMZ Traffic Flow
- DMZ-to-Server Traffic Flow
- DMZ-to-Client Traffic Flow
- DMZ-to-DMZ Traffic Flow
- Server-to-Client Traffic Flow
- Server-to-DMZ Traffic Flow

Client-to-Server Traffic Flow

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 70.1.1.2 255.255.255.0
ACOS(config-if:ve:2)# ip client
ACOS(config-if:ve:2)# ip nat inside
ACOS(config-if:ve:2)# exit

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 181.1.1.1 255.255.255.0
ACOS(config-if:ve:3)# ip server
```

Client-to-DMZ Traffic Flow

L3 Mode:

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 70.1.1.2 255.255.255.0
ACOS(config-if:ve:2)# ip client
ACOS(config-if:ve:2)# ip nat inside

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 181.1.1.1 255.255.255.0
ACOS(config-if:ve:3)# ip dmz
```

L2 Mode:

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 70.1.1.2 255.255.255.0
ACOS(config-if:ve:2)# traffic-distribution-mode sip
ACOS(config-if:ve:2)# ip nat inside

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 181.1.1.1 255.255.255.0
ACOS(config-if:ve:3)# traffic-distribution-mode l3-lookup
ACOS(config-if:ve:3)# ip dmz
```

DMZ-to-Server Traffic Flow

L3 Mode:

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 70.1.1.2 255.255.255.0
ACOS(config-if:ve:2)# ip dmz
ACOS(config-if:ve:2)# ipv6 address 7001::2/16
ACOS(config-if:ve:2)# ipv6 enable

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 181.1.1.1 255.255.255.0
ACOS(config-if:ve:3)# ip server
ACOS(config-if:ve:3)# ipv6 enable
```

L2 Mode:

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 70.1.1.2 255.255.255.0
ACOS(config-if:ve:2)# traffic-distribution-mode l3-lookup
ACOS(config-if:ve:2)# ip dmz
ACOS(config-if:ve:2)# ipv6 address 7001::2/16
ACOS(config-if:ve:2)# ipv6 enable

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 181.1.1.1 255.255.255.0
ACOS(config-if:ve:3)# ip server
ACOS(config-if:ve:3)# traffic-distribution-mode dip
ACOS(config-if:ve:3)# ipv6 enable
```

DMZ-to-Client Traffic Flow

L3 Mode:

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 70.1.1.2 255.255.255.0
ACOS(config-if:ve:2)# ip dmz
ACOS(config-if:ve:2)# ipv6 address 7001::2/16
ACOS(config-if:ve:2)# ipv6 enable

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 181.1.1.1 255.255.255.0
ACOS(config-if:ve:3)# ip client
ACOS(config-if:ve:3)# ipv6 enable
```

L2 Mode:

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 70.1.1.2 255.255.255.0
ACOS(config-if:ve:2)# traffic-distribution-mode l3-lookup
ACOS(config-if:ve:2)# ip dmz
ACOS(config-if:ve:2)# ipv6 address 7001::2/16
ACOS(config-if:ve:2)# ipv6 enable

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 181.1.1.1 255.255.255.0
ACOS(config-if:ve:3)# traffic-distribution-mode sip
ACOS(config-if:ve:3)# ip client
ACOS(config-if:ve:3)# ipv6 enable
```

DMZ-to-DMZ Traffic Flow

L3 Mode:

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 10.0.2.18 255.255.255.0
ACOS(config-if:ve:2)# ip dmz

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 10.0.4.18 255.255.255.0
ACOS(config-if:ve:3)# ip dmz
```

L2 Mode:

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 10.0.2.18 255.255.255.0
ACOS(config-if:ve:2)# traffic-distribution-mode l3-lookup
ACOS(config-if:ve:2)# ip dmz

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 10.0.4.18 255.255.255.0
ACOS(config-if:ve:3)# traffic-distribution-mode l3-lookup
ACOS(config-if:ve:3)# ip dmz
```

Server-to-Client Traffic Flow

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 70.1.1.2 255.255.255.0
ACOS(config-if:ve:2)# ip server
ACOS(config-if:ve:2)# ipv6 address 7001::2/16
ACOS(config-if:ve:2)# ipv6 enable

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 181.1.1.1 255.255.255.0
ACOS(config-if:ve:3)# ip client
ACOS(config-if:ve:3)# ipv6 enable
```

Server-to-DMZ Traffic Flow

L3 Mode:

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 70.1.1.2 255.255.255.0
ACOS(config-if:ve:2)# ip server
ACOS(config-if:ve:2)# ipv6 address 7001::2/16
ACOS(config-if:ve:2)# ipv6 enable

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 181.1.1.1 255.255.255.0
ACOS(config-if:ve:3)# ip dmz
ACOS(config-if:ve:3)# ipv6 enable
```

L2 Mode:

```
ACOS(config)# interface ve 2
ACOS(config-if:ve:2)# ip address 70.1.1.2 255.255.255.0
ACOS(config-if:ve:2)# traffic-distribution-mode dip
ACOS(config-if:ve:2)# ip server
ACOS(config-if:ve:2)# ipv6 address 7001::2/16
ACOS(config-if:ve:2)# ipv6 enable

ACOS(config)# interface ve 3
ACOS(config-if:ve:3)# ip address 181.1.1.1 255.255.255.0
ACOS(config-if:ve:3)# traffic-distribution-mode l3-lookup
ACOS(config-if:ve:3)# ip dmz
ACOS(config-if:ve:3)# ipv6 enable
```

Gi/SGi Firewall Configurations

The following topics are covered:

Configuring Firewall Rule-Sets

This section provides the following sample configurations for configuring Gi/SGi firewall rules.

The following topics are covered:

Permit

In this configuration example, there is no application specified after the **`action permit or action-group permit`** command. The packet is processed in a L3-forward mode and a firewall session is created.

```
ACOS(config)#rule-set firewall
ACOS(config-rule set:firewall)#rule 1
ACOS(config-rule set:firewall-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:firewall-rule:1)#dest zone any
ACOS(config-rule set:firewall-rule:1)#service any
ACOS(config-rule set:firewall-rule:1)#dscp af23
ACOS(config-rule set:firewall-rule:1)#dscp range 30 40
```

Action Permit

To configure an action, use the following commands:

```
ACOS(config-rule set:firewall-rule:1)#action permit
```

Action-Group Permit

To configure an action-group, use the following commands:

```
ACOS(config-rule set:firewall-rule:1)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)# permit
ACOS(config-rule set:firewall-rule:1-acti...)# exit
```

Action-Group Permit Syn-cookie

SYN cookie protection can be enabled at the global level in Firewall and CGN, as well as per rule in a firewall. The configuration in the firewall rule overrides the global Firewall and CGN configurations.

- To configure SYN cookie protection for a firewall rule-set, use the following commands:

```
ACOS(config)#rule-set rule1
ACOS(config-rule set:rule1)#rule rl1
ACOS(config-rule set:rule1-rule:rl1)# source zone any
ACOS(config-rule set:rule1-rule:rl1)# dest zone any
ACOS(config-rule set:rule1-rule:rl1)# service any
ACOS(config-rule set:rule1-rule:rl1)# action-group
ACOS(config-rule set:rule1-rule:rl1-action-group)# permit tcp syn-cookie
enable tcp-half-open on-threshold 500 on-timeout 60
```

- To configure SYN cookie protection for the system-wide firewall as well as for a firewall rule-set, use the following commands:

```
ACOS(config)# #fw tcp syn-cookie enable tcp-half-open on-threshold 1000
on-timeout 120
!
ACOS(config)#rule-set rule1
ACOS(config-rule set:rule1)#rule rl1
ACOS(config-rule set:rule1-rule:rl1)# source zone any
ACOS(config-rule set:rule1-rule:rl1)# dest zone any
ACOS(config-rule set:rule1-rule:rl1)# service any
ACOS(config-rule set:rule1-rule:rl1)# action-group
ACOS(config-rule set:rule1-rule:rl1-action-group)# permit tcp syn-cookie
enable tcp-half-open on-threshold 500 on-timeout 60
```

- To configure SYN cookie protection for global CGN as well as for a firewall rule-set, use the following commands:

```
ACOS(config)#cgnv6 ddos-protection syn-cookie enable tcp-half-open on-
threshold 100 on-timeout 120
!
ACOS(config)#cgnv6 lsn-lid 1
!
ACOS(config)#rule-set rule1
ACOS(config-rule set:rule1)#rule rl1
ACOS(config-rule set:rule1-rule:rl1)#source zone any
ACOS(config-rule set:rule1-rule:rl1)#dest zone any
ACOS(config-rule set:rule1-rule:rl1)#service any
ACOS(config-rule set:rule1-rule:rl1)#action-group
ACOS(config-rule set:rule1-rule:rl1-action-group)#permit cgnv6 lsn-lid 1
ACOS(config-rule set:rule1-rule:rl1-action-group)#permit tcp syn-cookie
enable
```

Permit CGNv6

In this configuration example, a packet matching the rule is processed by a CGNv6 application. If the traffic does not match the CGNv6 rule, the packet will get dropped.

```
ACOS(config)#class-list lsn
ACOS(config-class list)#0.0.0.0/0 lsn-lid 1

ACOS(config)#cgnv6 lsn inside source class-list lsn
ACOS(config)#cgnv6 nat pool p3 9.9.9.50 9.9.9.50 netmask /24 vrid 31

ACOS(config)#cgnv6 lsn-lid 1
ACOS(config-lsn-lid)#source-nat-pool p3

ACOS(config)#rule-set firewall
ACOS(config-rule set:firewall)#rule 1
ACOS(config-rule set:firewall-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:firewall-rule:1)#dest zone any
ACOS(config-rule set:firewall-rule:1)#service any
```

Action Permit CGNv6

To configure an action, enter the following commands:

```
ACOS(config-rule set:firewall-rule:1)#action permit cgnv6
```

Action-Group Permit CGNv6

To configure an action-group, enter the following commands:

```
ACOS(config-rule set:firewall-rule:1)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)#permit cgnv6
```

Permit CGNv6 LSN LID

In this configuration example, a valid LSN LID is specified to perform NAT on packets matching this rule, regardless of whether an LSN class-list is configured or not. If no LSN LID is found, the packet will get dropped.

```
ACOS(config)#cgnv6 nat pool p3 9.9.9.50 9.9.9.50 netmask /24 vrid 31
ACOS(config)#cgnv6 nat pool p4 9.9.9.60 9.9.9.60 netmask /24 vrid 31
ACOS(config)#cgnv6 lsn-lid 1
ACOS(config-lsn-lid)#source-nat-pool p3

ACOS(config)#cgnv6 lsn-lid 2
ACOS(config-lsn-lid)#source-nat-pool p4

ACOS(config)#rule-set firewall
ACOS(config-rule set:firewall)#rule 1
ACOS(config-rule set:firewall-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:firewall-rule:1)#dest zone any
ACOS(config-rule set:firewall-rule:1)#service any
```

Action Permit CGNv6 LSN-LID

To configure an action, enter the following commands:

```
ACOS(config-rule set:firewall-rule:1)#action permit cgnv6 lsn-lid 2
```

Action-Group Permit CGNv6 LSN-LID

To configure an action-group, enter the following commands:

```
ACOS(config-rule set:firewall-rule:1)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)#permit cgnv6 lsn-lid 2
```

Permit CGNV6 LSN LID Conflicting Rules

In this configuration example, a firewall rule action conflicts with another rule. To resolve the conflict, a “first-come, first-served” sequence is executed to assign a NAT address to the user.

```
ACOS(config)#cgnv6 nat pool p3 9.9.9.50 9.9.9.50 netmask /24 vrid 31
ACOS(config)#cgnv6 nat pool p4 9.9.9.60 9.9.9.60 netmask /24 vrid 31
ACOS(config)#cgnv6 lsn-lid 1
ACOS(config-lsn-lid)#source-nat-pool p3
ACOS(config)#cgnv6 lsn-lid 2
ACOS(config-lsn-lid)#source-nat-pool p4

ACOS(config)#rule-set firewall
ACOS(config-rule set:firewall)#rule 1
ACOS(config-rule set:firewall-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:firewall-rule:1)#dest zone any
ACOS(config-rule set:firewall-rule:1)#service any

ACOS(config-rule set:firewall-rule:1)#action permit cgnv6 lsn-lid 2
OR
ACOS(config-rule set:firewall-rule:1)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)#permit cgnv6 lsn-lid 2

ACOS(config-rule set:firewall)#rule 4
ACOS(config-rule set:firewall-rule:4)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:4)#source zone any
ACOS(config-rule set:firewall-rule:4)#dest ipv4-address any
ACOS(config-rule set:firewall-rule:4)#dest zone any
ACOS(config-rule set:firewall-rule:4)#service any

ACOS(config-rule set:firewall-rule:4)#action permit cgnv6 lsn-lid 1
OR
ACOS(config-rule set:firewall-rule:4)#action-group
ACOS(config-rule set:firewall-rule:4-acti...)#permit cgnv6 lsn-lid 1
```

In the above example, the NAT inside source static address is problematic. Also, **lsn-lid 2** under rule 1 and **lsn-lid 1** under rule 4 are assigned to the same user. The

LSN LID to be used for the user is determined by which rule is matched by the inside user first. Only one LSN LID can be used for the same inside user.

Permit CGNv6 Fixed NAT

In this configuration example, the Fixed NAT is specified to perform NAT on packets matching this rule. If no Fixed NAT configuration is found, the packet will get dropped. An entry “Fixed NAT Conf not Found” will be displayed in the output of the **`show cgnv6 fixed-nat statistics`** command.

```
ACOS(config)#cgnv6 fixed-nat inside 12.10.10.172 12.10.10.172 netmask /24
nat 9.9.9.67 9.9.9.67 netmask /24 vrid 31

ACOS(config)#rule-set firewall
ACOS(config-rule set:firewall)#rule 1
ACOS(config-rule set:firewall-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:firewall-rule:1)#dest zone any
ACOS(config-rule set:firewall-rule:1)#service any
```

Action Permit CGNv6 Fixed NAT

To configure an action, enter the following commands:

```
ACOS(config-rule set:firewall-rule:1)#action permit cgnv6 fixed-nat
```

Action-Group Permit CGNv6 Fixed NAT

To configure an action-group, enter the following commands:

```
ACOS(config-rule set:firewall-rule:1)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)#permit cgnv6 fixed-nat
```

Permit CGNv6 Fixed NAT and LSN LID Conflict

In this configuration example, the rules for the same inside user are configured to use both Fixed NAT and LSN LID for different services.

```
ACOS(config)#class-list lsn
ACOS(config-class list)#0.0.0.0/0 lsn-lid 1

ACOS(config)#cgnv6 lsn inside source class-list lsn
ACOS(config)#cgnv6 nat pool p3 9.9.9.50 9.9.9.50 netmask /24 vrid 31
ACOS(config)#cgnv6 nat pool p4 9.9.9.60 9.9.9.60 netmask /24 vrid 31

ACOS(config)#cgnv6 fixed-nat inside 12.10.10.172 12.10.10.172 netmask /24
nat 9.9.9.67 9.9.9.67 netmask /24 vrid 31

ACOS(config)#cgnv6 lsn-lid 1
ACOS(config-lsn-lid)#source-nat-pool p3

ACOS(config)#cgnv6 lsn-lid 2
ACOS(config-lsn-lid)#source-nat-pool p4

ACOS(config)#rule-set firewall
ACOS(config-rule set:firewall)#rule 1
ACOS(config-rule set:firewall-rule:1)#source ipv4-address 12.10.10.172/32
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:firewall-rule:1)#dest zone any
ACOS(config-rule set:firewall-rule:1)#service any

ACOS(config-rule set:firewall-rule:1)#action permit cgnv6 fixed-nat
OR
ACOS(config-rule set:firewall-rule:1)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)#permit cgnv6 fixed-nat

ACOS(config-rule set:firewall)#rule 4
source ipv4-address 12.10.10.172.32
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv4-address any
ACOS(config-rule set:firewall-rule:1)# dest zone any
ACOS(config-rule set:firewall-rule:1)# service any

ACOS(config-rule set:firewall-rule:1)#action permit cgnv6 lsn-lid 1
OR
ACOS(config-rule set:firewall-rule:1-acti...)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)#permit cgnv6 lsn-lid 1
```

In the above example, **`cgnv6 fixed-nat`** under rule 1 and **`cgnv6 lsn-lid 1`** under rule 4 are assigned to the same inside user to use both Fixed NAT and LSN-LID for different services. This is a valid configuration and the same user can make use of different NAT technologies for different services.

Permit Forward

In this configuration example, the rule is configured to process the packet in a L3-forward mode and a firewall session will be created.

```
ACOS(config)#cgnv6 nat pool p3 9.9.9.50 9.9.9.50 netmask /24 vrid 31
ACOS(config)#cgnv6 nat pool p4 9.9.9.60 9.9.9.60 netmask /24 vrid 31

ACOS(config)#cgnv6 lsn-lid 1
ACOS(config-lsn-lid)#source-nat-pool p3

ACOS(config-lsn-lid)#cgnv6 lsn-lid 2
ACOS(config-lsn-lid)#source-nat-pool p4

ACOS(config)#rule-set firewall
ACOS(config-rule set:firewall)#rule 1
ACOS(config-rule set:firewall-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:firewall-rule:1)#dest zone any
ACOS(config-rule set:firewall-rule:1)#service any

ACOS(config-rule set:firewall-rule:1)#action permit forward
OR
ACOS(config-rule set:firewall-rule:1)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)#permit forward
```

Permit Forward and LSN LID Conflicting Rules

In this configuration example, the rule is configured to process the packet in a L3-forward mode and a firewall session will be created.

```
ACOS(config)#cgnv6 nat pool p3 9.9.9.50 9.9.9.50 netmask /24 vrid 31
ACOS(config)#cgnv6 nat pool p4 9.9.9.60 9.9.9.60 netmask /24 vrid 31

ACOS(config)#cgnv6 lsn-lid 1
ACOS(config-lsn-lid)#source-nat-pool p3
ACOS(config-lsn-lid)#cgnv6 lsn-lid 2
ACOS(config-lsn-lid)#source-nat-pool p4

ACOS(config)#rule-set firewall
ACOS(config-rule set:firewall)#rule 1
ACOS(config-rule set:firewall-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:firewall-rule:1)#dest zone any
ACOS(config-rule set:firewall-rule:1)#service any

ACOS(config-rule set:firewall-rule:1)#action permit forward
OR
ACOS(config-rule set:firewall-rule:1)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)#permit forward

ACOS(config-rule set:firewall)#rule 4
ACOS(config-rule set:firewall-rule:4)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:4)#source zone any
ACOS(config-rule set:firewall-rule:4)#dest ipv4-address any
ACOS(config-rule set:firewall-rule:4)#dest zone any
ACOS(config-rule set:firewall-rule:4)#service any

ACOS(config-rule set:firewall-rule:4)#action permit cgnv6 lsn-lid 1
OR
ACOS(config-rule set:firewall-rule:4)#action-group
ACOS(config-rule set:firewall-rule:4-acti...)#permit cgnv6 lsn-lid 1
```

In the above example, **`forward`** under rule 1 and **`cgnv6 lsn-lid 1`** under rule 4 are assigned to the same user. This is a valid configuration and the same inside user will either be treated as a firewall session and L3-forwarded or use LSN LID 2 for NAT, based on the destination address.

Permit Forward with Template Limit Policy

In this configuration example, a rate limit policy is bound to a rule. The rate limit policy is applied based on the rate limiting scope applied on the traffic matching the rule.

```
ACOS(config)#template limit-policy 1023
ACOS(config-limit-policy)#limit-scope subscriber-ip
ACOS(config-limit-policy)#limit-pps downlink 1000000
ACOS(config-limit-policy)#limit-pps uplink 1000000
ACOS(config-limit-policy)#limit-pps total 2000000

ACOS(config)#rule-set firewall
ACOS(config-rule set:firewall)#rule 1
ACOS(config-rule set:firewall-rule:1)#ip-version v6
ACOS(config-rule set:firewall-rule:1)#source ipv6-address any
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv6-address any
ACOS(config-rule set:firewall-rule:1)#dest zone any
ACOS(config-rule set:firewall-rule:1)#service any

ACOS(config-rule set:firewall-rule:1)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)#permit forward
ACOS(config-rule set:firewall-rule:1-acti...)#permit limit-policy 1023

ACOS(config)#fw active-rule-set firewall
```

If different protocols are used, configure separate rules for each protocol with its own per-protocol limits.

Permit IPsec with Rate Limit Policy

In this configuration example, a rate-limit policy is bound to a rule. The rate-limit policy is applied to the IPsec traffic matching the rule.

```
ACOS(config)# vpn stateful-mode

ACOS(config)# vpn ike-gateway v4
ACOS(config-vpn ike-gateway:v4)# auth-method preshare-key encrypted
/+mboU9rpJM8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
ACOS(config-vpn ike-gateway:v4)# encryption aes-192 hash sha1
ACOS(config-vpn ike-gateway:v4)# dh-group 5
ACOS(config-vpn ike-gateway:v4)# local-address ip 6.1.1.33
ACOS(config-vpn ike-gateway:v4)# remote-address ip 6.1.1.34

ACOS(config)# interface tunnel 1
ACOS(config-if:tunnel:1)# ip address 73.1.1.33 255.255.255.0

ACOS(config)# vpn ipsec v4
ACOS(config-vpn ipsec:v4)# dscp cs2
ACOS(config-vpn ipsec:v4)# dh-group 5
ACOS(config-vpn ipsec:v4)# encryption aes-256 hash sha256
ACOS(config-vpn ipsec:v4)# bind tunnel 1 73.1.1.34
ACOS(config-vpn ipsec:v4)# ike-gateway v4

ACOS(config)# template limit-policy 1
ACOS(config-limit-policy)# limit-concurrent-sessions 2
ACOS(config-limit-policy)# limit-scope subscriber-prefix 24

ACOS(config)# rule-set test
ACOS(config-rule set:test)# rule 1
ACOS(config-rule set:test-rule:1)# source ipv4-address 11.1.1.0/24
ACOS(config-rule set:test-rule:1)# source zone any
ACOS(config-rule set:test-rule:1)# dest ipv4-address any
ACOS(config-rule set:test-rule:1)# dest zone any
ACOS(config-rule set:test-rule:1)# service any
ACOS(config-rule set:test-rule:1)# application any
ACOS(config-rule set:test-rule:1)# action-group
ACOS(config-rule set:test-rule:1-acti...)# permit ipsec v4
ACOS(config-rule set:test-rule:1-acti...)# permit limit-policy 1

ACOS(config)#fw active-rule-set test
```

Permit Respond to User Mac

In this configuration example, the user's source MAC is configured as the next hop rather than the routing table:

```
ACOS(config)#rule-set fw
ACOS(config-rule set:rule-set1)# rule 1
ACOS(config-rule set:fw-rule:1)# ip-version v6
ACOS(config-rule set:fw-rule:1)# source ipv6-address any
ACOS(config-rule set:fw-rule:1)# source zone any
ACOS(config-rule set:fw-rule:1)# dest ipv6-address 2001::/64
ACOS(config-rule set:fw-rule:1)# dest zone any
ACOS(config-rule set:fw-rule:1)# service any

ACOS(config-rule set:fw-rule:1)#action-group
ACOS(config-rule set:fw-rule:1-action-gr...)#permit forward
ACOS(config-rule set:fw-rule:1-action-gr...)#permit respond-to-user-mac
```

The following command enables the use of the user's source MAC for the next hop rather than the routing table for GiFW configuration:

```
ACOS(config)# fw respond-to-user-mac
```

NOTE: This command is a global-level configuration and is applied to all active firewall rules.

Permit Listen-On-Port

In this configuration exmaple, the `listen-on-port` is configured for creating a full-cone session allowing outside users to connect with the subscriber IP. Listen-on-port cannot be configured with IPsec or Cgnv6.

```
ACOS(config)#rule-set fw
ACOS(config-rule set:rule-set1)# rule 1
ACOS(config-rule set:fw-rule:1)# ip-version v6
ACOS(config-rule set:fw-rule:1)# source ipv6-address any
ACOS(config-rule set:fw-rule:1)# source zone any
ACOS(config-rule set:fw-rule:1)# dest ipv6-address 2001::/64
ACOS(config-rule set:fw-rule:1)# dest zone any
ACOS(config-rule set:fw-rule:1)# service any
```

Action Permit Forward Listen-on-Port

To configure an action, enter the following commands:

```
ACOS(config-rule set:fw-rule:1)#action permit forward listen-on-port
OR
ACOS(config-rule set:fw-rule:1)#action permit listen-on-port
```

Action-Group Permit Forward Listen-on-Port

To configure an action-group, enter the following commands:

```
ACOS(config-rule set:fw-rule:1)#action-group
ACOS(config-rule set:fw-rule:1-action-gr...)#permit forward
ACOS(config-rule set:fw-rule:1-action-gr...)#permit listen-on-port
```

Permit Log

In this configuration example, the rate limiting logs are enabled.

```
ACOS(config)#cgnv6 nat pool p3 9.9.9.50 9.9.9.50 netmask /24 vrid 31
ACOS(config)#cgnv6 nat pool p4 9.9.9.60 9.9.9.60 netmask /24 vrid 31

ACOS(config)#cgnv6 lsn-lid 1
ACOS(config-lsn-lid)#source-nat-pool p3

ACOS(config-lsn-lid)#cgnv6 lsn-lid 2
ACOS(config-lsn-lid)#source-nat-pool p4

ACOS(config)#rule-set firewall
ACOS(config-rule set:firewall)#rule 1
ACOS(config-rule set:firewall-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:firewall-rule:1)#dest zone any
ACOS(config-rule set:firewall-rule:1)#service any

ACOS(config-rule set:firewall-rule:1)#action permit log
OR
ACOS(config-rule set:firewall-rule:1)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)#permit log
```

For more information on enabling rule-specific logging templates, see Configuring Firewall Logging.

Permit Set DSCP

In this configuration example, the set DSCP action is bound to the rule. When the session matches this rule, all packets of the session change the DSCP value in the IPv4 header.

```
ACOS(config)# rule-set test
ACOS(config-rule set:test)# rule 1
ACOS(config-rule set:test-rule:1)# source ipv4-address any
ACOS(config-rule set:test-rule:1)# source zone any
ACOS(config-rule set:test-rule:1)# dest ipv4-address any
ACOS(config-rule set:test-rule:1)# dest zone any
ACOS(config-rule set:test-rule:1)# service tcp dst eq 22
ACOS(config-rule set:test-rule:1)# service icmp
ACOS(config-rule set:test-rule:1)# application any
ACOS(config-rule set:test-rule:1)# action-group
ACOS(config-rule set:test-rule:1-acti...)#permit set-dscp cs1
ACOS(config)#fw active-rule-set test
```

Reset Respond to User Mac

In this configuration example, the respond-to-user-mac action is reset:

```
ACOS(config)#rule-set fw
ACOS(config-rule set:rule-set1)# rule 1
ACOS(config-rule set:fw-rule:1)# ip-version v6
ACOS(config-rule set:fw-rule:1)# source ipv6-address any
ACOS(config-rule set:fw-rule:1)# source zone any
ACOS(config-rule set:fw-rule:1)# dest ipv6-address 2001::/64
ACOS(config-rule set:fw-rule:1)# dest zone any
ACOS(config-rule set:fw-rule:1)# service any

ACOS(config-rule set:fw-rule:1)#action-group
ACOS(config-rule set:fw-rule:1-action-gr...)#reset respond-to-user-mac
```

Reset Log

In this configuration example, the log action is reset:

```
ACOS(config)#rule-set firewall
ACOS(config-rule set:firewall)#rule 1
ACOS(config-rule set:firewall-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:1)#source zone any
ACOS(config-rule set:firewall-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:firewall-rule:1)#dest zone any
ACOS(config-rule set:firewall-rule:1)#service any

ACOS(config-rule set:firewall-rule:1)#action reset log
OR
ACOS(config-rule set:firewall-rule:1)#action-group
ACOS(config-rule set:firewall-rule:1-acti...)#reset log
```

For more information on enabling rule-specific logging templates, see Configuring Firewall Logging.

Reset with Template Limit Policy

In this configuration example, a DDoS rate-limiting policy template is bound to a reset rule. Additionally, the inside and outside interfaces are also configured.

```
ACOS(config)# template limit-policy 10
ACOS(config-limit-policy)# limit-pps downlink 10000 ddos-protection-factor
3

ACOS(config)# interface ethernet 2
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# ip address 20.20.20.1 255.255.255.0
ACOS(config-if:ethernet:1)# ip nat inside
ACOS(config-if:ethernet:1)# exit

ACOS(config)# interface ethernet 2
ACOS(config-if:ethernet:2)# enable
ACOS(config-if:ethernet:2)# ip address 20.20.101.1 255.255.255.0
ACOS(config-if:ethernet:2)# ip nat outside
ACOS(config-if:ethernet:2)# exit

ACOS(config)# rule-set firewall
ACOS(config-rule set:firewall)# rule r1
ACOS(config-rule set:firewall-rule:1)# source ipv4-address any
ACOS(config-rule set:firewall-rule:1)# source zone any
ACOS(config-rule set:firewall-rule:1)# dest ipv4-address 20.20.20.141/32
ACOS(config-rule set:firewall-rule:1)# dest zone any
ACOS(config-rule set:firewall-rule:1)# service any
ACOS(config-rule set:firewall-rule:1)# application any
ACOS(config-rule set:firewall-rule:1)# action-group
ACOS(config-rule set:firewall-rule:1-acti...)# reset limit-policy 10
```

Deny

In this configuration example, the client request is denied by dropping the packets without notifying the client.

```
ACOS(config)# rule-set firewall
ACOS(config-rule set:firewall)# rule 1
ACOS(config-rule set:firewall-rule:1)# source ipv4-address 12.10.10.0/24
ACOS(config-rule set:firewall-rule:1)# source zone any
ACOS(config-rule set:firewall-rule:1)# dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:firewall-rule:1)# dest zone any
ACOS(config-rule set:firewall-rule:1)# service any

ACOS(config-rule set:firewall-rule:1)# action deny
OR
ACOS(config-rule set:firewall-rule:1)# action-group
ACOS(config-rule set:firewall-rule:1-acti...)# deny
```

Deny with Template Limit Policy

In this configuration example, a DDoS rate-limiting template policy is bound to a deny rule. Additionally, the inside and outside interfaces are also configured.

```
ACOS(config)# template limit-policy 10
ACOS(config-limit-policy)# limit-pps downlink 10000 ddos-protection-factor
3

ACOS(config)# interface ethernet 2
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# ip address 20.20.20.1 255.255.255.0
ACOS(config-if:ethernet:1)# ip nat inside
ACOS(config-if:ethernet:1)# exit

ACOS(config)# interface ethernet 2
ACOS(config-if:ethernet:2)# enable
ACOS(config-if:ethernet:2)# ip address 20.20.101.1 255.255.255.0
ACOS(config-if:ethernet:2)# ip nat outside
ACOS(config-if:ethernet:2)# exit

ACOS(config)# rule-set firewall
ACOS(config-rule set:firewall)# rule r1
ACOS(config-rule set:firewall-rule:1)# source ipv4-address any
ACOS(config-rule set:firewall-rule:1)# source zone any
ACOS(config-rule set:firewall-rule:1)# dest ipv4-address 20.20.20.141/32
ACOS(config-rule set:firewall-rule:1)# dest zone any
ACOS(config-rule set:firewall-rule:1)# service any
ACOS(config-rule set:firewall-rule:1)# application any
ACOS(config-rule set:firewall-rule:1)# action-group
ACOS(config-rule set:firewall-rule:1-acti...)# deny limit-policy 10
```

Configuring MSS Clamping for Gi-FW Sessions

The MTU of the network is calculated as follows:

MTU of the network = MSS + Size of TCP-IP Headers

The TCP MSS value is the maximum amount of data a host can accept in a single TCP segment. Use the ACOS CLI to set the maximum and minimum TCP MSS values, as well as the value to subtract from the configured maximum MSS value, if the configured MSS value exceeds the MTU of the network.

For the CGN sessions based on CGN rules, see the CLI command cgnv6 tcp mss-clamp to configure MSS clamping. (Refer to the *Command Line Interface Reference for CGN guide*).

Use the following command to set the maximum TCP MSS Clamping value as 500:

```
ACOS(config)#fw tcp mss-clamp fixed 500
```

Use the following command to specify a value of 100 to subtract from the maximum MSS Clamping value and also to define the minimum value for the TCP MSS Clamping as 120:

```
ACOS(config)#fw tcp mss-clamp subtract 100 min 120
```

The MSS Clamping feature is not enabled by default. The afore-mentioned configuration fixes the maximum MSS Clamping size as 500. If the network still experiences latency and packet drop issues, the maximum MSS Clamping value can be reduced by 100 each time. However, at any point of time, the MSS Clamping value does not get less than 120.

Configuring Rate Limiting

The following topics are covered:

NOTE: In this document, unless mentioned otherwise, the **firewall rule-set** refers to the Access Control rule-set.

Important Notes on Rate Limit Policy Template Changes

The following behavior is seen when you make changes to the rate limit policy template:

- If a template is bound to a rule for the first time, the change is applied to the existing sessions as well.
- If a rule has a template bound and the threshold is modified in the template, the change is applied immediately.
- If a rule has a template bound and the rate limiting scope is modified in the template, the change is applied. However, the change may not take effect immediately depending on the connection or other related factors.
- If a rule has a template bound and the template is changed to a different one, the new change will take effect immediately.

Configuring Packets-Per-Second Rate Limiting

Use the following commands to configure the packets-per-second rate limit on the uplink, downlink, and the total traffic:

```
ACOS(config)#template limit-policy 1023
ACOS(config-limit-policy)# limit-scope subscriber-prefix 24
ACOS(config-limit-policy)# limit-pps downlink 1000000
ACOS(config-limit-policy)# limit-pps uplink 1000000
ACOS(config-limit-policy)# limit-pps total 2000000
Use the following command to enable DDoS protection only for the Packets-per-second downlink traffic:
ACOS(config-limit-policy)# limit-pps downlink 1000000 ddos-protection-factor <1-50>
```

NOTE: You can either configure a PPS or a throughput under the same template limit-policy. You cannot configure both.

```
ACOS(config)# rule-set r1
ACOS(config-rule set:r1)# rule 1
ACOS(config-rule set:r1-rule:1)# source ipv4-address 12.10.10.0/24
ACOS(config-rule set:r1-rule:1)# source zone any
ACOS(config-rule set:r1-rule:1)# dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:r1-rule:1)# dest zone any
ACOS(config-rule set:r1-rule:1)# service any
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# permit forward
ACOS(config-rule set:r1-rule:1-action-group)# permit limit-policy 1023
```

Configuring Throughput Rate Limiting

Use the following commands to set the throughput rate limit on the uplink, downlink, and total traffic:

```
ACOS(config)# template limit-policy 1023
ACOS(config-limit-policy)# limit-scope subscriber-prefix 24
ACOS(config-limit-policy)# limit-throughput downlink 50000
ACOS(config-limit-policy)# limit-throughput uplink 50000
ACOS(config-limit-policy)# limit-throughput total 100000
```

NOTE: You can either configure a throughput or a PPS under the same template limit-policy. You cannot configure both.

```
ACOS(config)# rule-set r1
ACOS(config-rule set:r1)# rule 1
ACOS(config-rule set:r1-rule:1)# source ipv4-address 12.10.10.0/24
ACOS(config-rule set:r1-rule:1)# source zone any
ACOS(config-rule set:r1-rule:1)# dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:r1-rule:1)# dest zone any
ACOS(config-rule set:r1-rule:1)# service any
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# permit forward
ACOS(config-rule set:r1-rule:1-action-group)# permit limit-policy 1023
```

Configuring Connections Per Second Rate Limiting

Use the following command to set the number of connections per second rate limit:

```
ACOS(config)# template limit-policy 1023
ACOS(config-limit-policy)# limit-scope subscriber-prefix 24
ACOS(config-limit-policy)# limit-cps 10000

ACOS(config)# rule-set r1
ACOS(config-rule set:r1)# rule 1
ACOS(config-rule set:r1-rule:1)# source ipv4-address 12.10.10.0/24
ACOS(config-rule set:r1-rule:1)# source zone any
ACOS(config-rule set:r1-rule:1)# dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:r1-rule:1)# dest zone any
ACOS(config-rule set:r1-rule:1)# service any

ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# permit forward
ACOS(config-rule set:r1-rule:1-action-group)# permit limit-policy 1023
```

Configuring Concurrent Sessions

Use the following commands to configure the number of connections per second allowed on a subscriber IP:

```
ACOS(config)#template limit-policy 1023
ACOS(config-limit-policy)#limit-scope subscriber-prefix 24
ACOS(config-limit-policy)#limit-concurrent-sessions 1000000 log

ACOS(config)#rule-set r1
ACOS(config-rule set:r1)#rule 1
ACOS(config-rule set:r1-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:r1-rule:1)#source zone any
ACOS(config-rule set:r1-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:r1-rule:1)#dest zone any
ACOS(config-rule set:r1-rule:1)#service any
ACOS(config-rule set:r1-rule:1)#action-group
ACOS(config-rule set:r1-rule:1-action-group)#permit forward
ACOS(config-rule set:r1-rule:1-action-group)#permit limit-policy 1023
```

NOTE: If a concurrent session limit is configured after the sessions are established, the limit is not applied on the existing sessions. A valid QOSMOS license is needed for the application classification to work.

Configuring Application-Based Rate Limiting

Use the following commands to configure the rate limiting policy for application protocols and categories:

```
ACOS(config)#template limit-policy 1023
ACOS(config-limit-policy)#limit-scope subscriber-prefix 24
ACOS(config-limit-policy)#limit-pps downlink 1000000
ACOS(config-limit-policy)#limit-pps uplink 1000000
ACOS(config-limit-policy)#limit-pps total 2000000

ACOS(config)#template limit-policy 1022
ACOS(config-limit-policy)#limit-scope subscriber-prefix 24
ACOS(config-limit-policy)#limit-cps 1000000
```

NOTE: If connections-per-second and concurrent session limits are used with application classification, these rate limits are applied after the application is classified. It is not applied at the time of session creation.

Any Application

In this example, the **limit-policy 1023** is applied on the traffic received from any application.

```
ACOS(config)#rule-set r1
ACOS(config-rule set:r1)#rule 1
ACOS(config-rule set:r1-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:r1-rule:1)#source zone any
ACOS(config-rule set:r1-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:r1-rule:1)#dest zone any
ACOS(config-rule set:r1-rule:1)#service any
ACOS(config-rule set:r1-rule:1)#application any
ACOS(config-rule set:r1-rule:1)#track-application
ACOS(config-rule set:r1-rule:1)#action-group
ACOS(config-rule set:r1-rule:1-action-group)#permit
ACOS(config-rule set:r1-rule:1-action-group)#permit limit-policy 1023
```

Application Protocol

In this example, the **limit-policy 1023** is applied on multiple application protocols such as ftp, tftp, and dns specified in rule 1. In this case, the combined traffic received from the specified protocols is limited as per the limit-policy 1023.

```
ACOS(config)#rule-set r1
ACOS(config-rule set:r1)#rule 1
ACOS(config-rule set:r1-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:r1-rule:1)#source zone any
ACOS(config-rule set:r1-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:r1-rule:1)#dest zone any
ACOS(config-rule set:r1-rule:1)#service any
ACOS(config-rule set:r1-rule:1)#application protocol ftp
ACOS(config-rule set:r1-rule:1)#application protocol tftp
ACOS(config-rule set:r1-rule:1)#application protocol dns
ACOS(config-rule set:r1-rule:1)#track-application

ACOS(config-rule set:r1-rule:1)#action-group
ACOS(config-rule set:r1-rule:1-action-group)#permit
ACOS(config-rule set:r1-rule:1-action-group)#permit limit-policy 1023
```

Application Category

In this example, the **limit-policy 1023** is applied on the Web application category. The **limit-policy 1022** is applied on the IPv6 traffic received from any application.

```
ACOS(config)#rule-set r1
ACOS(config-rule set:r1)#rule 1
ACOS(config-rule set:r1-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:r1-rule:1)#source zone any
ACOS(config-rule set:r1-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:r1-rule:1)#dest zone any
ACOS(config-rule set:r1-rule:1)#service any
ACOS(config-rule set:r1-rule:1)#application category web
ACOS(config-rule set:r1-rule:1)#track-application
ACOS(config-rule set:r1-rule:1)#action-group
ACOS(config-rule set:r1-rule:1-action-group)#permit
ACOS(config-rule set:r1-rule:1-action-group)#permit limit-policy 1023
ACOS(config-rule set:r1-rule:1-action-group)#exit
ACOS(config-rule set:r1-rule:1)#exit

ACOS(config-rule set:r1)#rule 2
ACOS(config-rule set:r1)#ip-version v6
ACOS(config-rule set:r1-rule:2)#source ipv6-address any
ACOS(config-rule set:r1-rule:2)#source zone client_inside
ACOS(config-rule set:r1-rule:2)#dest ipv6-address 3201::172/128
ACOS(config-rule set:r1-rule:2)#dest zone server_side
ACOS(config-rule set:r1-rule:2)#service any
ACOS(config-rule set:r1-rule:2)#application any
ACOS(config-rule set:r1-rule:2)#track-application
```

NOTE: In the above example of rule 2, it is assumed that the subscriber side interface is configured as ip client and the server-side interface is configured as ip server.

```
ACOS(config-rule set:r1-rule:2)#action-group
ACOS(config-rule set:r1-rule:2-action-group)#permit
ACOS(config-rule set:r1-rule:2-action-group)#permit limit-policy 1022
```

Configuring Rate Limiting Scope

Rate limiting scope can be applied at rule level, subscriber IP level, and subscriber prefix level.

Rule Level

Use the following commands to apply the rate limiting policy at the rule level:

```
ACOS(config)#template limit-policy 1023
ACOS(config-limit-policy)#limit-scope aggregate
ACOS(config-limit-policy)#limit-pps downlink 1000000
ACOS(config-limit-policy)#limit-pps uplink 1000000
ACOS(config-limit-policy)#limit-pps total 2000000
ACOS(config)#rule-set r1
ACOS(config-rule set:r1)#rule 1
ACOS(config-rule set:r1-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:r1-rule:1)#source zone any
ACOS(config-rule set:r1-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:r1-rule:1)#dest zone any
ACOS(config-rule set:r1-rule:1)#service any
ACOS(config-rule set:r1-rule:1)#application category web
ACOS(config-rule set:r1-rule:1)#track-application

ACOS(config-rule set:r1-rule:1)#action-group
ACOS(config-rule set:r1-rule:1-action-group)#permit
ACOS(config-rule set:r1-rule:1-action-group)#permit limit-policy 1023
```

Subscriber IP Level

Use the following commands to apply the rate limiting policy at the subscriber IP level:

```
ACOS(config)#template limit-policy 1023
ACOS(config-limit-policy)#limit-scope subscriber-ip
ACOS(config-limit-policy)#limit-pps downlink 1000000
ACOS(config-limit-policy)#limit-pps uplink 1000000
ACOS(config-limit-policy)#limit-pps total 2000000

ACOS(config)#rule-set r1
ACOS(config-rule set:r1)#rule 1
ACOS(config-rule set:r1-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:r1-rule:1)#source zone any
ACOS(config-rule set:r1-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:r1-rule:1)#dest zone any
ACOS(config-rule set:r1-rule:1)#service any
ACOS(config-rule set:r1-rule:1)#application category web
ACOS(config-rule set:r1-rule:1)#track-application

ACOS(config-rule set:r1-rule:1)#action-group
ACOS(config-rule set:r1-rule:1-action-group)#permit
ACOS(config-rule set:r1-rule:1-action-group)#permit limit-policy 1023
```

Subscriber Prefix Level

Use the following commands to apply the rate limiting policy at the subscriber IP level:

```
ACOS(config)#template limit-policy 1023
ACOS(config-limit-policy)#limit-scope subscriber-prefix <128>
ACOS(config-limit-policy)#limit-pps downlink 1000000
ACOS(config-limit-policy)#limit-pps uplink 1000000
ACOS(config-limit-policy)#limit-pps total 2000000

ACOS(config)#rule-set r1
ACOS(config-rule set:r1)#rule 1
ACOS(config-rule set:r1-rule:1)#source ipv4-address 12.10.10.0/24
ACOS(config-rule set:r1-rule:1)#source zone any
ACOS(config-rule set:r1-rule:1)#dest ipv4-address 9.9.9.173/32
ACOS(config-rule set:r1-rule:1)#dest zone any
ACOS(config-rule set:r1-rule:1)#service any
ACOS(config-rule set:r1-rule:1)#application category web
ACOS(config-rule set:r1-rule:1)#track-application

ACOS(config-rule set:r1-rule:1)#action-group
ACOS(config-rule set:r1-rule:1-action-group)#permit
ACOS(config-rule set:r1-rule:1-action-group)#permit limit-policy 1023
```

Configuring Radius Logging for Rate Limiting

You can configure the radius attributes for rate limiting to be included in the logs under the firewall template logging configuration.

Use the following commands to configure the radius attributes for rate limiting:

```
ACOS(config)# fw template logging fw-log
ACOS(config-logging)# include-radius-attribute framed-ipv6-prefix prefix-length 64
ACOS(config-logging)# include-radius-attribute msisdn limit-policy
ACOS(config-logging)# include-radius-attribute imei limit-policy]
ACOS(config-logging)# include-radius-attribute imsi limit-policy
ACOS(config-logging)# include-radius-attribute custom2 limit-policy
ACOS(config-logging)# include-radius-attribute custom1 limit-policy
ACOS(config-logging)# format ascii
```

For detailed information about Radius logging, see RADIUS Logging.

Configuring Rate Limiting Using Traffic Control Rule-Set

Use the following commands to configure rate limiting using Traffic Control rule-set:

```
ACOS(config)# template limit-policy 5
ACOS(config-limit-policy)# limit-throughput uplink

ACOS(config)# traffic-control rule-set r1
ACOS(config-rule set:r1)# rule 1
ACOS(config-rule set:r1-rule:1)# source ipv4-address any
ACOS(config-rule set:r1-rule:1)# source zone any
ACOS(config-rule set:r1-rule:1)# dest ipv4-address any
ACOS(config-rule set:r1-rule:1)# dest zone any
ACOS(config-rule set:r1-rule:1)# service any
ACOS(config-rule set:r1-rule:1)# action-group
ACOS(config-rule set:r1-rule:1-action-group)# action limit-policy 5
```

Configuring Rate Limiting Using RADIUS Derived Attribute

The following examples describe the different applications for configuring rate-limiting for domain users and user groups:

Example 1: Use the following commands to configure a traffic-control rule using a source class-list filter for derived RADIUS attributes. Configure the rate limit policy for the user group.

```
ACOS(config)#template limit-policy 1
ACOS(config-limit-policy)#limit-throughput total 10000
ACOS(config-limit-policy)#limit-scope radius attribute usergroup

ACOS(config)# ip-list radius-client1
ACOS(config-ip list)# 10.10.10.100

ACOS(config)#class-list policy_cl1 string
ACOS(config-class list)#str policy_cl1

ACOS(config)#system radius server
ACOS(config-radius-server)#remote ip-list radius-client1
ACOS(config-radius-server)#attribute custom1 domain vendor 10101 number 41
ACOS(config-radius-server)#attribute inside-ip number 7
ACOS(config-radius-server)#attribute inside-ipv6 vendor 10101 number 28
ACOS(config-radius-server)#accounting start replace-entry
ACOS(config-radius-server)#derived-attribute usergroup attribute custom1
regex @(\w+)

ACOS(config)#rule-set acl
ACOS(config-rule set:acl)#rule 1
ACOS(config-rule set:acl-rule:1)#action permit
ACOS(config-rule set:acl-rule:1)#exit
ACOS(config-rule set:acl)#rule 2
ACOS(config-rule set:acl-rule:2)#ip-version v6
ACOS(config-rule set:acl-rule:2)#action permit

ACOS(config)#fw active-rule-set acl

ACOS(config)#traffic-control rule-set RateLimit-policy
ACOS(config-rule set:RateLimit-policy)#rule policy_cl1
ACOS(config-rule set:RateLimit-policy-rul...)#source class-list policy_cl1
type radius derived-attribute usergroup
ACOS(config-rule set:RateLimit-policy-rul...)#action-group
ACOS(config-rule set:RateLimit-policy-rul...)#action limit-policy 1
ACOS(config-rule set:RateLimit-policy-rul...)#exit
ACOS(config-rule set:RateLimit-policy)#rule policy_cl1_v6
ACOS(config-rule set:RateLimit-policy-rul...)#ip-version v6
ACOS(config-rule set:RateLimit-policy-rul...)#source class-list policy_cl1
type radius derived-attribute usergroup
ACOS(config-rule set:RateLimit-policy-rul...)#action-group
ACOS(config-rule set:RateLimit-policy-rul...)#action limit-policy 1

ACOS(config)#traffic-control active-rule-set RateLimit-policy
```

Example 2: Use the following commands to configure a hierarchical rate-limiting policy applying aggregated rate-limitation for a domain user group and a rate-limitation for individual subscribers.

```
ACOS(config)#template limit-policy 10
ACOS(config-limit-policy)#limit-throughput total 10000
ACOS(config-limit-policy)#limit-scope radius attribute usergroup

ACOS(config)#template limit-policy 20
ACOS(config-limit-policy)#parent 10
ACOS(config-limit-policy)limit-throughput total 1000
ACOS(config-limit-policy)#limit-scope radius attribute userid

ACOS(config)#template limit-policy 30
ACOS(config-limit-policy)#parent 10
ACOS(config-limit-policy)limit-throughput total 1000
ACOS(config-limit-policy)#limit-scope radius attribute userid

ACOS(config)# ip-list radius-client1
ACOS(config-ip list)# 10.10.10.100

ACOS(config)#class-list policy_cl1 string
ACOS(config-class list)#str policy_cl1

ACOS(config)#class-list policy_cl2 string
ACOS(config-class list)#str policy_cl2

ACOS(config)#system radius server
ACOS(config-radius-server)#remote ip-list radius-client1
ACOS(config-radius-server)#attribute custom1 user-name number 1
ACOS(config-radius-server)#attribute inside-ip number 7
ACOS(config-radius-server)#attribute inside-ipv6 vendor 10101 number 28
ACOS(config-radius-server)#accounting start replace-entry
ACOS(config-radius-server)#derived-attribute usergroup attribute custom1
regex @(\w+)
ACOS(config-radius-server)#derived-attribute userid attribute custom1
regex ([^@]+)

ACOS(config)#rule-set acl
ACOS(config-rule set:acl)#rule 1
ACOS(config-rule set:acl-rule:1)#action permit
ACOS(config-rule set:acl-rule:1)#exit
ACOS(config-rule set:acl)#rule 2
ACOS(config-rule set:acl-rule:2)#ip-version v6
ACOS(config-rule set:acl-rule:2)#action permit

ACOS(config)#fw active-rule-set acl

ACOS(config)#traffic-control rule-set RL-Hierarchy-policy
ACOS(config-rule set:RL-Hierarchy-policy)#rule policy_cl1
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#source class-list policy_
cl1 type radius derived-attribute usergroup
ACOS(config-rule set:RL-Hierarchy-policy-policy-rul...)#action-group
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#action limit-policy 20
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#exit
ACOS(config-rule set:RL-Hierarchy-policy)#rule policy_cl1_v6
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#ip-version v6
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#source class-list policy_
cl1 type radius derived-attribute usergroup
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#action-group
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#action limit-policy 20

ACOS(config-rule set:RL-Hierarchy-policy)#rule policy_cl2
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#source class-list policy_
cl2 type radius derived-attribute usergroup
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#action-group
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#action limit-policy 30
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#exit
ACOS(config-rule set:RL-Hierarchy-policy)#rule policy_cl2_v6
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#ip-version v6
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#source class-list policy_
cl2 type radius derived-attribute usergroup
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#action-group
ACOS(config-rule set:RL-Hierarchy-policy-rul...)#action limit-policy 30

ACOS(config)#traffic-control active-rule-set RL-Hierarchy-policy
```

Example 3: Use the following commands to configure a single rule for handling both IPv4 and IPv6 addresses for user group by using the **`ip-version`** `any` option in the traffic-control rule-set.

```
ACOS(config)#template limit-policy 2
ACOS(config-limit-policy)#limit-throughput total 10000
ACOS(config-limit-policy)#limit-scope radius attribute usergroup

ACOS(config)# ip-list radius-client2
ACOS(config-ip list)# 10.10.10.100

ACOS(config)#class-list policy_cl2 string
ACOS(config-class list)#str policy_cl2
ACOS(config)#system radius server
ACOS(config-radius-server)#remote ip-list radius-client2
ACOS(config-radius-server)#attribute custom1 domain vendor 10101 number 40
ACOS(config-radius-server)#attribute inside-ip number 8
ACOS(config-radius-server)#attribute inside-ipv6 vendor 10101 number 27
ACOS(config-radius-server)#accounting start replace-entry
ACOS(config-radius-server)#derived-attribute usergroup attribute custom1
regex @(\w+)

ACOS(config)#rule-set acl
ACOS(config-rule set:acl)#rule 1
ACOS(config-rule set:acl-rule:1)#action permit

ACOS(config)#fw active-rule-set acl

ACOS(config)#traffic-control rule-set RateLimit-policy1
ACOS(config-rule set:RateLimit-policy1)#rule policy_cl2
ACOS(config-rule set:RateLimit-policy1-rule:policy_cl2)#ip-version any
ACOS(config-rule set:RateLimit-policy1-rule:policy_cl2)#source class-list
policy_cl2 type radius derived-attribute usergroup
ACOS(config-rule set:RateLimit-policy1-rule:policy_cl2)#action-group
ACOS(config-rule set:RateLimit-policy1-rule:policy_cl2)#action limit-
policy 2

ACOS(config)#traffic-control active-rule-set RateLimit-policy1
```

Configuring DDoS Protection

Specify the **ddos-protection-factor** to enable DDoS protection while configuring the Packet-Per-Second (PPS) threshold limit (in the template limit policy):

```
ACOS(config-limit-policy)# limit-pps downlink pps_limit <1-2147483647>
ddos-protection-factor <1-50>
```

When the PPS exceeds the configured rate limiting threshold (specified by *pps_limit*), rate-limiting begins i.e., the excessive packets are dropped. However, if the PPS exceeds a value that is greater than the product of the PPS threshold limit and DDoS protection factor, a DDoS attack is detected, and the configured DDoS protection action is triggered.

Example:

```
ACOS(config-limit-policy)# limit-pps downlink 100000 ddos-protection-
factor 3
```

In this case, when the PPS exceeds 100000, rate-limiting begins. However, if the PPS exceeds 300000 i.e., a value greater than the product of the PPS threshold limit and DDoS protection factor, a DDoS attack is detected.

NOTE: You cannot configure **limit-scope aggregate** and **ddos-protection** in the same limit-policy template.

To configure DDoS protection actions:

- Use the following command to block the traffic locally:

```
ACOS(config)# fw ddos-protection action drop
```

- Use the following command to block the traffic using the Remotely Triggered Black Hole (RTBH) technique. The expiration time i.e., the time to determine when to revert the action, and the remove-wait period to re-initiate and extend the black-hole entry is also configured:

```
ACOS(config)# fw ddos-protection action redistribute-route map-1
expiration 5 timer-multiply-max 6 remove-wait-timer 30
```

- Use the following command to forward the traffic (instead of dropping it unconditionally) even when RTBH is in effect:

```
ACOS(config)# fw ddos-protection action redistribute-route map-1 forward
```

Enabling Logging for DDoS Protection

To enable event logging for DDoS protection, enter the following command at the global configuration level and configure one of the options:

```
ACOS(config)# fw  ddos-protection logging enable
ACOS(config)# fw  ddos-protection logging enable [local | remote | both]
```

To disable event logging for DDoS protection, enter the following command at the global configuration level:

```
ACOS(config)# fw  ddos-protection logging disable
```

The logs are generated by default when the firewall DDoS protection entries are added and removed. The log formats supported are CEF, ASCII, and IPFIX.

For more information about CEF, ASCII, and IPFIX log samples, see *Traffic Logging Guide*.

Configuring Gi/SGi Firewall with CGN Deployment

This section provides the configuration steps to set up a basic Gi/SGi-FW:

1. Configure the server(s) to which the logs will be sent.

   The following commands configure the server to which the logs are to be sent:

   ```
   ACOS(config)# cgnv6 server ls1 9.9.9.173
   ACOS(config-real server)# health-check-disable
   ACOS(config-real server)# port 514 udp
   ACOS(config-real server-node port)# health-check-disable
   ACOS(config-real server-node port)# exit
   ACOS(config-real server)# exit
   ```

2. Configure the service group for the servers.

   The following commands configure the service group of servers:

   ```
   ACOS(config)# cgnv6 service-group logging udp
   ACOS(config-cgnv6 svc group)# member ls1 514
   ACOS(config-cgnv6 svc group)# exit
   ```

3. Define a CGNv6 logging template, which NAT events to log and the format for the log messages.

   The following commands define a CGNv6 logging template. In the template, the commands also define which NAT events to log and the format for the log messages:

   ```
   ACOS(config)# cgnv6 template logging log
   ACOS(config-logging:log)# log fixed-nat port-mappings both
   ACOS(config-logging:log)# log port-mappings creation
   ACOS(config-logging:log)# format binary
   ACOS(config-logging:log)# service-group logging
   ACOS(config-logging:log)# exit
   ```

4. Set a configured LSN traffic logging template as the default template for all LSN pools.

   The following command sets a configured LSN traffic logging template as the default template for all LSN pools:

   ```
   ACOS(config)# cgnv6 lsn logging default-template log
   ```

5. Configure endpoint-independent mapping (EIM) and endpoint-independent filtering (EIF) support.
6. Configure a named set of IP addresses for use by CGN or LSN.

   The following commands configure a named set of IP addresses for use by CGN or LSN:

   ```
   ACOS(config)# cgnv6 nat pool p1 9.9.9.50 9.9.9.50 netmask/24 vrid 31
   ```

7. Configure a LID for NAT64 and add the pool to it.

   The following commands configure a LID for NAT64 and add the pool to it:

   ```
   ACOS(config)# cgnv6 lsn-lid 1
   ACOS(config-lsn-lid)# source-nat-pool p1
   ACOS(config-lsn-lid)# exit
   ```

8. Configure the NAT64 prefix to be used.

   The following command configures the NAT64 prefix:

   ```
   ACOS(config)# cgnv6 nat64 prefix 64:ff9b::/96
   ```

9. Enable Fixed NAT for Gi/SGi-FW deployment.

   The following command enables Fixed NAT:

   ```
   ACOS(config)# cgnv6 fixed-nat inside 3201::172 3201::172 netmask 96 nat
   9.9.9.45 9.9.9.45 netmask /24 vrid
   ```

10. Create a network object-group for specifying match criteria using Layer 3 parameters that will be used for IPv4 firewall configurations.

    The following commands create a network object-group for specifying match criteria using Layer 3 parameters. The following example specifically creates a network object group that will be used for IPv4 firewall configurations.

```
ACOS(config)# object-group network network1 fw v4
ACOS(config-network:network1)# 12.10.10.0/24
ACOS(config-network:network1)# exit
```

11. Create a service object group for specifying matching match criteria using Layer 4 to layer 7 parameters.

    The following commands create a service object group for specifying matching match criteria using Layer 4 to layer 7 parameters.

```
ACOS(config)# object-group service alg
ACOS(config-service:alg)# tcp eq 21 alg FTP
ACOS(config-service:alg)# icmp
ACOS(config-service:alg)# tcp range 1 65535
ACOS(config-service:alg)# udp eq 69 alg TFTP
ACOS(config-service:alg)# protocol-id 132
ACOS(config-service:alg)# udp eq 554 alg RTSP
ACOS(config-service:alg)# udp eq 53 alg DNS
ACOS(config-service:alg)# udp range 1 65535
ACOS(config-service:alg)# exit
```

12. Configure a firewall rule-set that contains a set of rules. Rules should contain the match criteria and associated action.

    The following commands configure a firewall rule-set that contains a set of rules. In this example, rule 1 specifies that any packets matching this rule must be handled by LSN configurations, whereas packets matching rule 2 must be handled by Fixed NAT configurations. Packets matching rule 3 are permitted, and no CGN configurations are applied to them.

```
ACOS(config)# rule-set firewall
ACOS(config-rule set:firewall)# rule 1
ACOS(config-rule set:firewall-rule:1)# action permit cgnv6 lsn-lid 1
ACOS(config-rule set:firewall-rule:1)# source object-group network1
ACOS(config-rule set:firewall-rule:1)# source zone inside
ACOS(config-rule set:firewall-rule:1)# dest ipv4-address any
ACOS(config-rule set:firewall-rule:1)# dest zone outside
ACOS(config-rule set:firewall-rule:1)# service object-group alg
ACOS(config-rule set:firewall-rule:1)# exit

ACOS(config)# rule-set firewall
ACOS(config-rule set:firewall)# rule 2
ACOS(config-rule set:firewall-rule:2)# action permit cgnv6 fixed-nat
ACOS(config-rule set:firewall-rule:2)# ip-version v6
ACOS(config-rule set:firewall-rule:2)# source ipv6-address
3201::172/128
ACOS(config-rule set:firewall-rule:2)# source zone inside
ACOS(config-rule set:firewall-rule:2)# dest ipv6-address any
ACOS(config-rule set:firewall-rule:2)# dest zone any
ACOS(config-rule set:firewall-rule:2)# service any
ACOS(config-rule set:firewall-rule:2)# exit

ACOS(config)# rule-set firewall
ACOS(config-rule set:firewall)# rule 3
ACOS(config-rule set:firewall-rule:3)# action permit
ACOS(config-rule set:firewall-rule:3)# source any inside
ACOS(config-rule set:firewall-rule:3)# dest any
ACOS(config-rule set:firewall-rule:3)# exit
```

13. Activate the rule-set with the “fw active-rule-set” command.

    The following command enables the firewall rule-set:

```
ACOS(config)# fw active-rule-set firewall
```

NOTE:

- The firewall rule-set must be activated with the `fw active-rule-set` command before any rules can be enforced on inbound traffic.
- When no rule-set is active, all traffic will pass, since no firewall rules are applied to the incoming traffic.
- If a firewall rule-set is active and no rules are defined, then the default action is implicit deny.
- Each rule contains one or more match criteria and associated actions that can be applied to traffic if there is a match.
- When configuring FW with NAT64 configurations, a rule must be configured to permit ICMPv4 error messages.

The output from the **show running-config** command shows the commands that must be entered for Gi/SGi-FW to work correctly in a simple FW + CGN deployment scenario.

```
ACOS(config)# show running-config
!Current configuration: 2822 bytes
!Configuration last updated at 01:42:08 PST Tue Sep 10 2016
!Configuration last saved at 01:56:48 PST Tue Sep 10 2016
!64-bit Advanced Core OS (ACOS) version 4.1.1, build 204 (Sep-14-
2016,05:26)
!
zone inside
  vlan 10
!
zone outside
  vlan 20
!
cgnv6 server ls1 9.9.9.173
  health-check-disable
  port 514 udp
    health-check-disable
!
cgnv6 service-group logging udp
  member ls1 514
!
cgnv6 template logging log
  log fixed-nat port-mappings both
  log port-mappings creation
  format binary
  service-group logging
!
cgnv6 lsn logging default-template log
!
cgnv6 nat pool p3 9.9.9.50 9.9.9.50 netmask /24 vrid 31
!
cgnv6 lsn-lid 1
  source-nat-pool p1
!
cgnv6 nat64 prefix 64:ff9b::/96
!
```

```
cgnv6 fixed-nat inside 3201::172 3201::172 netmask 96 nat 9.9.9.45
9.9.9.45 netmask /24 vrid 31
!
object-group network allowed fw v4
  12.10.10.0/24
!
object-group service alg
  tcp eq 21 alg FTP
  icmp
  tcp range 1 65535
  udp eq 69 alg TFTP
  protocol-id 132
  udp eq 554 alg RTSP
  udp eq 53 alg DNS
  udp range 1 65535
!
rule-set firewall
  rule 1
    action permit cgnv6 lsn-lid 1
    source object-group allowed
    source zone inside
    dest ipv4-address any
    dest zone outside
    service object-group alg
  rule 2
    action permit cgnv6 fixed-nat
    ip-version v6
    source ipv6-address 3201::172/128
    source zone inside
    dest ipv6-address any
    dest zone any
    service any
!
fw active-rule-set firewall
```

Configuring Gi/SGi Firewall on Multi-PU Platform

To configure firewall on Multi-PU Platforms:

1. Configure the interfaces specified as the client and the server.

```
ACOS1(config)# interface ve 81
ACOS1(config-if:ve:81)# ip address 10.1.1.47 255.255.255.0
ACOS1(config-if:ve:81)# ip client
ACOS1(config-if:ve:81)# ipv6 address 1000::47/64
ACOS1(config-if:ve:81)# exit

ACOS1(config)# interface ve 83
ACOS1(config-if:ve:83)# ip address 30.1.1.47 255.255.255.0
ACOS1(config-if:ve:83)# ip server
ACOS1(config-if:ve:83)# ipv6 address 3000::47/64
ACOS1(config-if:ve:83)# exit
```

NOTE: `ip client` and `ip server` must be configured on different interfaces. These two commands are only supported on Multi-PU platforms.

2. Configure a firewall rule-set. Rules should contain the match criteria and associated action.

```
ACOS(config)# rule-set rule2
ACOS(config-rule set: rule2)# rule r1
ACOS(config-rule set: rule2-rule:r1)# action permit
ACOS(config-rule set: rule2-rule:r1)# source ipv4-address any
ACOS(config-rule set: rule2-rule:r1)# source zone any
ACOS(config-rule set: rule2-rule:r1)# dest ipv4-address any
ACOS(config-rule set: rule2-rule:r1)# dest zone any
ACOS(config-rule set: rule2-rule:r1)# service any
ACOS(config-rule set: rule2-rule:r1)# exit

ACOS(config-rule set: rule2)# rule r2
ACOS(config-rule set: rule2-rule:r2)# action permit
ACOS(config-rule set: rule2-rule:r2)# ip-version v6
ACOS(config-rule set: rule2-rule:r2)# source ipv6-address any
ACOS(config-rule set: rule2-rule:r2)# source zone any
ACOS(config-rule set: rule2-rule:r2)# dest ipv6-address any
ACOS(config-rule set: rule2-rule:r2)# dest zone any
ACOS(config-rule set: rule2-rule:r2)# service any
ACOS(config-rule set: rule2-rule:r2)# exit
```

3. Configure a firewall logging server that specifies the IPv4 or IPv6 address, or hostname for the logging server, enables health monitoring of the server, and specifies the TCP or UDP port on which the server listens for traffic.

```
ACOS(config)# fw server s1 30.1.1.45
ACOS(config-real server)# health-check-disable
ACOS(config-real server)# port 514 udp
ACOS(config-real server-node port)# health-check-disable
ACOS(config-real server-node port)# port 514 tcp
ACOS(config-real server-node port)# health-check-disable
ACOS(config-real server-node port)# exit
```

4. Configure a service group for the firewall logging server and adds the external log server and port to the service group.

```
ACOS(config)# fw service-group fw_udp udp
ACOS(config-fw svc group)# member s1 514
ACOS(config-fw svc group)# exit
```

5. Configure a firewall logging template.

```
ACOS(config)# fw template logging log1
ACOS(config-logging)# log http-requests url
ACOS(config-logging)# rule http-requests dest-port 80
ACOS(config-logging)# service-group fw_udp
ACOS(config-logging)# exit
```

6. Bind a firewall logging template to the firewall.

```
ACOS(config)# fw logging log1
ACOS(config)# exit
```

7. Activate the firewall function using the specified rule-set.

```
ACOS(config)# fw active-rule-set rule2
```

Displaying the Rate Limiting Entries

The following show commands are displayed:

- Use the following command to display all the rate limit entries and their values:

```
ACOS(config)#show fw rate-limit
```

```
IP Address  Prefix  Rule  Type  CPS-Received  CPS-Limit  Uplink-Received
 Uplink-Limit  Downlink-Received  Downlink-Limit  Total-Received  Total-
Limit  Cumulative Dropped Packets
------------------------------------------------------------------------
------------------------------------------------------------------------
---------------
47.27.10.10  32      1     PPS   0             0             0
    0              0                       100                  0
       0                424
Total Rate Limit Entries Shown:1
```

Table 8 provides the field descriptions for the show firewall DDoS protection statistics:

Table 8 : Show Firewall Rate Limit Field Descriptions

Field	Description
IP Address	The IP address of the subscriber.
Prefix	The prefix configured for the specified subscriber IP address or subnet.
Rule	The name of the firewall rule.
Type	The type of the rate limit. It can have one of the following values: • Packets Per Second (PPS) • Bits Per Second (BPS) • Connections Per Second (CPS)
CPS	The number of Connections per second for the subscriber IP address.
CPS-Received	The number of CPS for the subscriber IP address.
CPS-Limit	The configured CPS limit.
Uplink-Received	The uplink traffic (PPS or throughput) received from a subscriber IP or a subnet.
Uplink-Limit	The configured uplink limit (for PPS or throughput).
Downlink-Received	The downlink traffic (PPS or throughput) received from a subscriber IP or a subnet.
Downlink-	The configured downlink limit (for PPS or throughput).

Table 8 : Show Firewall Rate Limit Field Descriptions

Field	Description
Limit	
Total-Received	The total number of packets received from a subscriber IP or a subnet.
Total-Limit	The configured total limit (for PPS or throughput).
Cumulative Dropped Packets	The total number of packets dropped. This count is obtained by adding the dropped packet of the current second to the dropped packets of the previous seconds.

- Use the following command to display the rate limit entries and their values for a specific IPv4 or IPv6 addresses:

```
ACOS(config)#show fw rate-limit 1.1.1.1
IP Address  Prefix Rule    Type CPS     Uplink-Rate Downlink-Rate Total-
Rate  Drop Count
---------------------------------------------------------------------
1.1.1.1      32     fw_Rule PPS  500000  1000000     1000000
2000000     10000
```

If the rate-limiting policy is applied at rule level (aggregate), the output is displayed as follows:

```
IP Address Prefix Rule    Type   CPS    Uplink-Rate Downlink-Rate Total-
Rate  Drop Count
---------------------------------------------------------------------
- -           32      fw_Rule   PPS  500000     1000000       1000000
2000000     1000
```

- In addition to the other entries, the following rate limit counters are displayed in the `show counters fw global`:

```
ACOS(config)#show counters fw global
Limit Entry Created                                      0
Limit Entry Freed                                        0
Limit Entry Creation Failure                             0
Limit Entry Found                                        0
Uplink PPS Exceeded                                      0
Downlink PPS Exceeded                                    0
```

```
Total PPS Exceeded                                       0
Uplink Throughput Limit Exceeded                         0
Downlink Throughput Limit Exceeded                       0
Total Throughput Limit Exceeded                          0
Connections Per Second Limit Exceeded                    0
```

- Use the `show rule-set` command (for Access Control rule-set) to view the number of packets dropped for the specified rule. In case of Traffic Control rule-set, use the `show traffic-control rule-set` command.

```
ACOS(config)#show rule-set rule 1
Rule-Set-Name: rule 1
Rule-Set-Status: active
Unmatched-Drops: 0    Action-Permit: 3    Action-Deny: 0    Action-
Reset: 0
Total-Rule-Count: 3
Rule-Name:                      2
Hit-Count:                      3
Action:                         permit
Status:                         enable
Permit-bytes:                   214
Deny-bytes:                     0
Reset-bytes:                    0
Total-bytes:                    214
TCP-active-session:             0
UDP-active-session:             0
ICMP-active-session:            0
SCTP-active-session:            1
OTHER-protocol-active-session:  0
Total-active-session:           1
TCP-session:                    0
UDP-session:                    0
ICMP-session:                   0
SCTP-session:                   1
OTHER-protocol-session:         0
Total-session:                  1
Rate-limit-drops:               20
```

Displaying and Clearing the DDoS Entries

The following show commands are displayed:

- Use the following command to display the IP address and the prefix that are blocked:

```
ACOS(config)#show fw ddos-protection entries
IP Address   Prefix   Rule     PPS    Expiration Hints
-------------------------------------------------------------
1.1.1.1      32       fw_IPv4  2847   48         Remove-Wait
```

Table 9 provides the field descriptions for the show firewall DDoS protection statistics:

Table 9 : Show Firewall DDoS-Protection Statistics Field Descriptions

Field	Description
IP Address	The IP address that is under attack.
Prefix	The prefix configured for the specified subscriber IP address or subnet.
Rule	The name of the firewall rule.
PPS	The number of packets-per-second sent to the subscriber IP address.
Expiration	The expiration time starts decrementing as soon as the IP is blacklisted and gets automatically renewed if the blacklisted IP continues to be under attack.
Hints	A hint that indicates whether the IP entry is in **Remove Wait** or **Time Multiplier** state.

- Use the `show counters fw ddos-protection` to display the following entries related to DDoS protection:

```
ACOS(config)#show counters fw ddos-protection
*****************************
Too many DDOS entries                                          0
DDOS entry added                                               0
DDOS entry removed                                             0
DDoS Entry added to BGP                                        0
DDoS Entry Removed from BGP                                   0
DDOS entry BGP remove failures                                0
DDOS Packet Drop                                              0
```

- Use the following command to clear the DDoS entries:

```
ACOS(config)#clear fw ddos-protection entries
```

GTP Firewall

The following topics are covered:

GTP Firewall complies with 3GPP Release 13 specifications.

GPRS Tunneling Protocol (GTP) Overview

General Packet Radio Switching (GPRS) Tunneling Protocol, commonly known as GTP, is the protocol used to carry multiprotocol packets between GPRS support nodes (GSNs) for 3G, 4G/LTE, and the recent 5G non-standalone architectures. In 4G/LTE deployments, GTP protocol is used for establishing a tunnel between a Serving Gateway (SGW) and Packet Data Network Gateway (PGW), and an SGW and Mobility Management Entity (MME). Upon receiving the packets from the user endpoints (UEs), SGW encapsulates them within a GTP tunnel and forwards them to the PGW. The PGW receives the packets and decapsulates them before forwarding them to the external host.

GPRS Tunnel Protocol (GTP) is vulnerable to attacks and malicious traffic coming through the GRX/IPX network or the Internet. The attackers often target GTP interfaces exposed to the network. They send fraudulent or spoofed messages to the interfaces to receive responses that reveal important information such as the identity, location, authentication, encryption keys for the interface, and packet data sessions of a user. This information enables them to take control of the network.

GTP firewall protects network infrastructure and the subscribers against attacks such as the following:

- **Eavesdropping**—Intercepting and snooping into GTP traffic for gaining confidential subscriber information
- **Fraud**—Utilizing services at the expense of the operator or another subscriber by using invalid or hijacked IMSI
- **Injection of Malicious GTP Messages**—Disrupting sessions and creating DDoS attacks
- **Subscriber Denial of Service**—Generating excessive volumes of malicious messages and causing service disruption
- **Message Suppression and Modification**—Preventing message delivery or allowing malicious content delivery and disrupting service
- **Network Overload or DDoS**—Sending malicious, malformed or invalid signaling packets that overwhelm network elements or cause vulnerable elements to fail.

GTP Firewall can be deployed on the S8-Gp (roaming) and S5-Gn (non-roaming) interface. It supports both Category 1 and Category 2 filtering based on GSMA FS.20 guidelines.

GTP Firewall also supports VRRP-A. For more information, see GTP VRRP-A Support .

Limitations

The following limitations apply to the GTP Firewall:

- Multi-PU platforms such as TH7650, THG7655S, and TH8655S support GTP firewall (FW) only in transparent Layer 2 (L2) mode. They do not support Layer 3 (L3) mode deployment.

Supported GTP Protocols

GTP Firewall supports the following protocols:

- GTP Control (GTP-C)
- GTP User Plane (GTP-U)

GTP-C

The GTP-C protocol is used within the network for signaling between the support nodes and the serving gateways. IPv4 and IPv6 are supported for these signaling messages. This allows the network elements to perform the following:

- Provision resources for the user
- Establish and terminate tunnels
- Control connection to the peers
- Support and adjust various quality of service requirements
- Support roaming (where users join from a different network)

GTP-C supports traffic of the following versions as defined by the 3GPP specifications:

- **GTPv2-C**—GTPv2 is part of fourth-generation (4G) LTE technology developed by 3GPP. GTPv2 is used between the SGW and PGW in an LTE architecture.

GTPv2 supports the following two main interfaces:

- **S5**—Connection between an SGW and a PGW within the same Public Land Mobile Network (PLMN).
- **S8**—Connection between two PLMNs.

GTP uses the specified protocols in the following planes:

- **Control plane**—GTP uses a tunnel control and management protocol (GTP-C) that allows the SGSN to provide packet data network access for an MS. Control plane signaling is used to create, modify, and delete tunnels.
- **User plane**—GTP uses a tunneling protocol (GTP-U) to provide a service for carrying user data packets.

GTP Firewall can be placed between the SGW and PGW to secure the following interfaces:

- **S5 interface**—Secures the GTP tunnels to protect the associated network elements.
- **S8 interface**—Secures the GTP tunnels to protect a PLMN against another PLMN.
- **GTPv1-C**—GTPv1 is part of third-generation (3G) mobile cellular network developed by 3GPP. GTPv1 is the protocol used between GPRS support nodes (GSNs) in the UMTS/GPRS backbone network. It includes both the GTP control plane (GTP-C) and data transfer (GTP-U) procedures. GTPv1 supports GTP-C control traffic to destination port 2123.

GTPv1 supports the following three main interfaces:

- **Gn**—Connection between an SGSN and a GGSN within the same Public Land Mobile Network (PLMN).
- **Gp**—Connection between two PLMNs.
- **Iu**—Connection between the SGSN and the UMTS Terrestrial Radio Access Network (UTRAN).

GTP-C and GTP-U are defined for the Gn interface (between GSNs within a PLMN), and for the Gp interface (between GSNs in different PLMNs). Only GTP-U is defined for the Iu interface between the SGSN and the UTRAN.

GTP uses the specified protocols in the following planes:

- **Control plane**—GTP uses a tunnel control and management protocol (GTP-C) that allows the SGSN to provide packet data network access for an MS. Control plane signaling is used to create, modify, and delete tunnels.
- **User plane**—GTP uses a tunneling protocol (GTP-U) to provide a service for carrying user data packets.

GTP Firewall can be placed between the SGSN and GGSN to secure the following interfaces:

- **Gn interface**—Secures the GTP tunnels to protect the associated network elements.
- **Gp interface**—Secures the GTP tunnels to protect a PLMN against another PLMN.
- **GTPv0-C**—Support for GTPv1 to GTPv0 interworking is removed from the 3GPP Rel-8 GTPv1 specification. A GTPv1 entity may or may not listen to the GTPv0 port 3386. Based on the configuration, all GTPv0 messages received on GTP Firewall are dropped unless both the peer PLMNs support GTPv0.

GTP-U

The GTP-U protocol carries IPv4 and IPv6 user data between the Radio Access Network (RAN) and the core networks, and within the core network. GTP-U exchanges this user data between SX interfaces using UDP messaging on port 2152. The associated traffic is seen on S1-U, S5, and S8 as represented in Figure 35.

GTP-U currently supports version 1 (GTPv1-U).

The GTP stack assigns a unique tunnel endpoint identifier (TEID) to each GTP control connection to the peers and to each GTP user connection (bearer) to the peers.

The GTP-U TEIDs are exchanged over the GTP-C tunnel and subsequently allow GTP-U sessions on the GTP Firewall that is linked to the GTP-C tunnel.

Simplified LTE Architecture

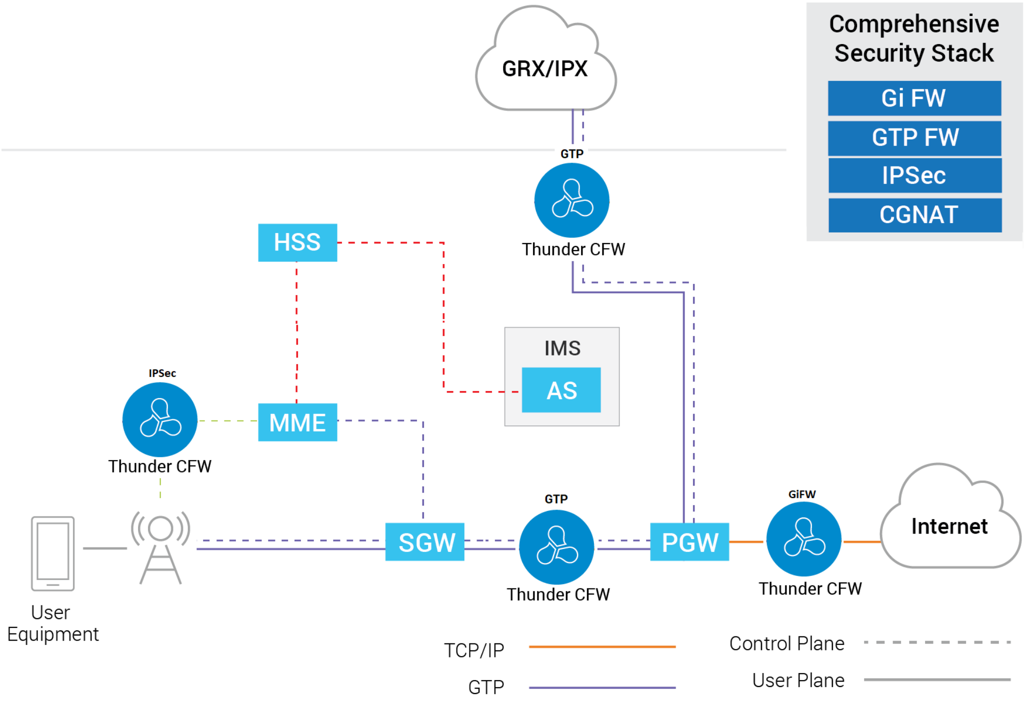
When GTP Firewall is deployed to inspect traffic, it is important to specify the connection points or 3GPP interfaces that you want GTP Firewall to secure.

The following topics are covered:

Comprehensive Security Stack (CSS)

To support 5G core, the Comprehensive Security Stack (CSS) secures the GTP traffic at three EPC interfaces. CSS provides the architectural flexibility to accommodate Network Function Virtualization (NFV), Software-Defined Networking (SDN) and Mobile Edge Computing (MEC).

Figure 34 : Firewall Deployed on Roaming



The Comprehensive Security Stack includes the following:

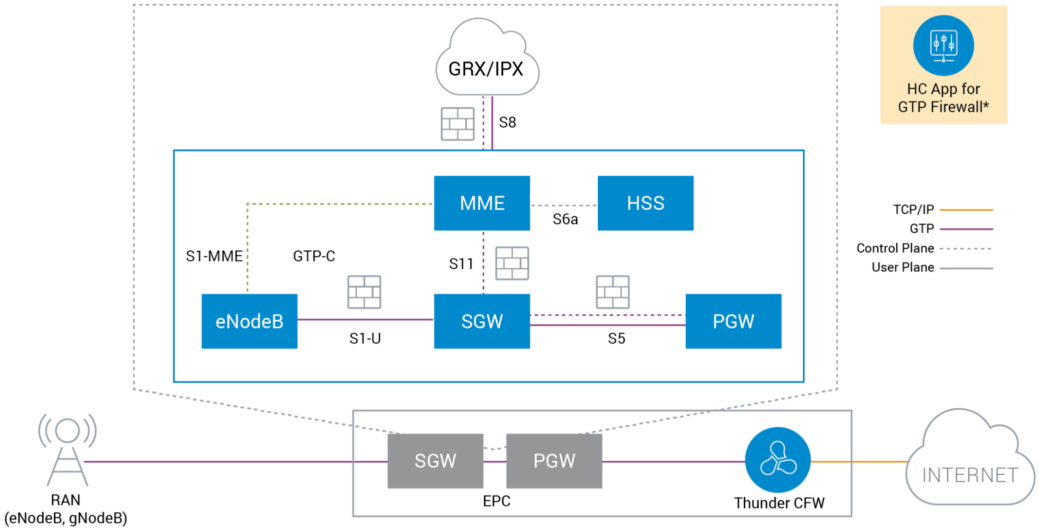
- **GiFW**—The Gi/SGi firewall defends against attacks from the Internet, public and private clouds, data center infrastructure, and other PDN gateways.

- **GTP Firewall**—The GTP (roaming) firewall with granular SCTP filtering defends the EPC against GTP-based attacks initiated from RAN or GRX/IPX networks.
- **IPSec**—IPsec provides both encryption and authentication in the mobile backhaul. The 3GPP standard requires encryption for the air interface to each eNodeB, but there is no such requirement for the S1-U interface between the eNodeBs and the SGW or the S1-MME interface between eNodeBs and MME. This protects from rogue or compromised eNodeBs or small cells.
- **DDoS Protection**—DDoS protection is required at all three interfaces - GiFW, GTP Firewall, and IPsec. The DDoS components defend against multiple classes of attack vectors, including volumetric, protocol, resource and advanced application-layer attacks, which are quickly detected and mitigated to prevent service disruption.

Radio Access Network (RAN) Security

GTP Firewall deployed for RAN security inspects the traffic flowing across the backhaul network to the EPC on the S1-U interface. Figure 35 shows how GTP control and user plane are used for the roaming (S8) interface, between eNodeB and SGW on the S1U interface, and between SGW and PGW on the S5 interface. Using GTP Firewall, you can protect the network and subscribers from GTP protocol vulnerabilities at interfaces.

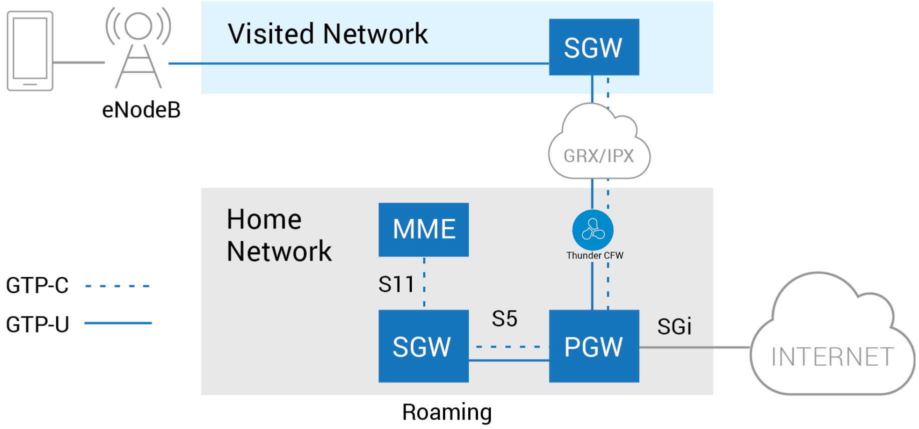
Figure 35 : GTP Firewall Deployed on EPC



Roaming Security

GTP Firewall deployed on the roaming interface inspects the traffic flowing between the EPC and the gateway that connects to the GRX/IPX on the S8 interface.

Figure 36 : GTP Firewall Deployed on Roaming



GTP Stateful Inspection

GTP Firewall performs stateful inspection of the GTP messages based on the subscriber contexts indicated by the Tunnel Endpoint Identifier (TEID). GTP stateful inspection examines the incoming and outgoing packets and provides enhanced security by denying out-of-state messages and removing stale tunnels using tunnel timeouts for GTP-C and GTP-U traffic.

GTP Tunnel Management

A GTP-C tunnel is created when a Create Session Request(v2) or a Create PDP Context (v1,v0) is received.

A GTP-U tunnel is created when the first GTP-U packet is received for any bearer. A GTP-U data tunnel is created only when the corresponding GTP-C tunnel exists. These GTP-U packets are called G-PDU.

The following events are associated with GTP-C and GTP-U tunnel creation and deletion:

- GTP-C tunnels have a configurable timeout from 5 minutes to a maximum of 1000 hours with the default value set to 24 hours (1440 minutes).
- GTP-U tunnels do not expire.
- GTP-C tunnels can be deleted by the following triggers:
  - Delete session request or response—deletes the tunnel for GTPv2
  - Delete PDP context request or response—deletes the tunnel for GTPv1 and GTPv0
  - Delete bearer request or response — deletes the default bearer for GTPv2
  - GTP-echo (keep alive) messages not received within the set time

    Once the GTP-C tunnel is deleted, no GTP-C or GTP-U packets are allowed for that tunnel.
- GTP-U tunnels can be deleted by the following triggers:
  - Delete bearer request or response—deletes the tunnel for GTPv2
  - Delete PDP context request or response—deletes the tunnel for GTPv1 and GTPv0
  - Associated GTP-C is deleted
- GTP-C tunnels reset their inactivity timer when GTP-C or GTP-U tunnels have traffic.
- GTP-C tunnels are not deleted until all GTP-U tunnels linked to it are deleted.

GTP-C tunnel timeout defines the maximum number of seconds a GTP-C tunnel remains active after it has stopped processing data (also known as idle tunnel timeout). This helps clear the state and reclaim the resources for a tunnel. For example, when a delete session response that terminates the tunnel is lost in transit, the tunnel timeout helps to clear the state and reclaim the resources.

For information about the number of tunnels created and deleted on the device, see Tunnel Counters.

GTP Message Types

GTP Firewall defines a set of messages that must be validated, and potentially filtered out between SGW/SGSN and PGW/GGSN network elements. To prevent DDOS attacks on interfaces, you can configure the maximum number of bytes allowed in GTP messages. The value can range from 64 to 1500 bytes.

For information about configuring the message length, see Configure General Policy.

The following sections covers the parsed GTP messages for GTPv2-C and GTPv1-C versions

- GTPv2-C Messages
- GTPv1-C Messages

GTPv2-C Messages

The following table describes the parsed GTPv2-C messages and their usage.

Table 10 : GTPv2-C messages

Message	Description
Create Session Request (SGW to PGW)	Creates the GTP-C tunnel and exchanges the TEID and other information for the GTP-U default bearer. It can also include bearer information for each dedicated bearer if there are more than one Bearer Context information elements (IE Type 93) in the packet.
Create Session Response (PGW to SGW)	Allows or denies GTP-C tunnel creation. The destination GTP-C Tunnel ID is notified using F-TEID IE.
Create Bearer Request (PGW to SGW)	Exchanges dedicated bearer information for adding dedicated bearers. This message is sent on the S5/S8 interface by the PGW to the SGW as part of the Dedicated Bearer Activation procedure.
Create Bearer	Allows either the creation of the Bearer Context or marks it for removal.

Table 10 : GTPv2-C messages

Message	Description
Response (SGW to PGW)	• If the Bearer Context is created, the Bearer Context IE contains the Bearer ID, the cause, the TEID, and possibly some additional optional fields. • If the Bearer Context is marked for removal, the Bearer Context IE contains the Bearer ID and the cause. The TEID is not included.
Delete Bearer Request (PGW to SGW)	Sent to delete bearers. It contains one or more EPS Bearer IDs that are used to delete dedicated bearers, or a Linked EPS Bearer ID (LBI).
Delete Bearer Response (SGW to PGW)	Contains the EPS Bearer IDs, but processes it as follows: • If it contains a Linked EPS Bearer ID (LBI), delete all GTP-U and GTP-C tunnels if the cause is not Temporarily Rejected Due to Handover/TAU/RAU Procedure in Progress. • If it contains an EPS Bearer ID within the Bearer Context, delete the dedicated GTP-U if the cause is not Temporarily Rejected Due to Handover/TAU/RAU Procedure in Progress. • If it contains an EBI, it cannot be the default bearer. Cause values are as follows: • Request Accepted • Request Accepted Partially • Context Not Found • Temporarily Rejected Due to Handover/TAU/RAU Procedure in Progress
Modify Bearer Request	Exchanges the bearer information between SGW and PGW as a part of the handover. A new GTP-C tunnel is created as the SGW changes but the PGW remains the same. This information is also sent as part of the subscriber location update or change of serving network.

Table 10 : GTPv2-C messages

Message	Description
	This message includes the bearer contexts that need to be modified or removed as part of the handover procedure.
Modify Bearer Response	Sends the message from PGW to SGW, acknowledging the receipt of Modify Bearer Request. It permits or denies the tunnel creation based on the cause value. It indicates the bearer contexts that have been modified or removed as a part of this procedure if the modify bearer request contained that information.

GTPv1-C Messages

The following table describes the GTPv1-C messages that are parsed and their usage.

Table 11 : GTPv1-C messages

Message	Description
Create PDP Context Request (SGSN to GGSN)	Used to request creation of a GTP-C tunnel and a default PDP context. After the GTP-C tunnel is established, this same message is used to add a dedicated PDP context. It also includes the following: • GTP-U tunnel ID in the Tunnel Endpoint Identifier Data information element (IE Type 16). • NSAPI information element (IE Type 20). The NSAPI information element contains an NSAPI that identifies a PDP Context in a mobility management context specified by the Tunnel Endpoint Identifier Control Plane. • Traffic class value that is part of the QoS information element (IE Type 135).
Create PDP Context Response (GGSN to SGSN)	Allows either the creation of the Bearer Context or marks it for removal.

Table 11 : GTPv1-C messages

Message	Description
Update PDP Context Request	Sends this message from SGSN to GGSN as part of the Routing Area Update procedure, modifying the PDP contexts or updating the QoS and the path. It can also be sent as part of the Secondary PDP Context Activation. This message includes the NSAPI, TEID for data, SGSN address for control and data along with the updated QoS. It can also be sent from the GGSN to SGSN to renegotiate the QoS of a PDP Context, to check if the PDP Context is active in the SGSN. This message includes IMSI and NSAPI to uniquely identify the PDP Context.
Update PDP Context Response	Sends this message from GGSN to SGSN as a response to the Update PDP Context Request with a cause value. The information elements in this message vary depending on the request sent by the SGSN. Depending on the request, the GGSN may include TEID Control Plane and TEID Data, QoS, and so on for satisfying or renegotiating the request received.
Delete PDP Context Request (SGW to PGW)	Performs one of the following actions depending on the Teardown Indicator setting: • Teardown Indicator set to 1—Deletes all GTP-U tunnels. • Teardown Indicator set to 0 or not present—Deletes only that NSAPI. • Teardown Indicator set to 0 or not present (but there is only one NSAPI)—Ignores the message.
Delete PDP Context Response (PGW to	Deletes the corresponding GTP-U tunnel and unlink the SMP. If the default bearer is deleted as part of this response, also delete GTP-C tunnel. The Delete PDP Context Response does not contain information

Table 11 : GTPv1-C messages

Message	Description
SGW)	about the associated NSAPI. This creates the expectation that there is only one NSAPI in a half-open state, which is deleted when a valid response is received (except for the case of a complete teardown, where all GTP-U tunnels are deleted).
PDU Notification Request	Sends this message if a PDP packet arrives at the GGSN. This message is sent by GGSN. If GGSN does not find an active PDP context, then GGSN/SGSN will use the PDU Notification request or response messages to activate the context or session for the Mobile Subscriber, so the PDP packets are delivered to the subscriber. GGSN may store the PDUs received for this subscriber. Create PDP Context Request may be seen after the exchange of PDU Notification Request or Response to establish a tunnel. Subscriber attributes such as IMSI, End User Address and APN, GGSN address, and TEID are included in this message.
PDU Notification Reject Request	SGSN sends this message to GGSN when a PDP Context is not established. GGSN may reject or discard the PDUs depending on the PDP type. The End User Address, APN, Cause, and TEID Control Plane are included in this message.

GTP Path Management

The GTP Path Management detects path and node failures. These include the following messages types:

- Echo messages (GTP-C and GTP-U)—A GTP echo request and response message pair intended to test network connectivity and the responsiveness of the targeted host. The echo request sends packets to the host and the host’s echo reply reports errors, lost packets, and associated statistics, including the time required to receive and respond to the request.

For information about the counters displayed for echo messages, see Echo Counters.

- Version Not Supported messages (GTP-C)—The echo request sends packets to the host and the host's echo reply reports errors, lost packets, and associated statistics, including the time required to receive and respond to the request.

GTPv1 and GTPv0 path management messages contain TEIDs as 0. GTPv2 do not have a TEID field.

The following details apply to GTP-C echo:

- GTPv1-C and GTPv2-C echo messages are health check messages that are sent to the peer by GTP sessions based on the GTP version it supports. It does not perform a firewall lookup (that is, there is no template dependency).
- Echo messages can be initiated by SGW/PGW. When an echo connection times out between the request and the response, the associated nodes are considered down and all tunnels between SGW and PGW are deleted.

For information about configuring GTP echo, see Configuring GTP Echo.

GTP Peer Restoration

GTP Firewall maintains a recovery value for each peer based on the received recovery information element (IE) the first time the node starts. When a peer restarts, it compares the stored recovery value with the recovery value received in the GTP Echo response or any other GTP-C Tunnel message for each peer entity. It processes the results as follows:

- If the stored value is 0 (zero), the value received in the message becomes the new stored value for the peer.
- If the stored value is smaller than the value received, it indicates that the peer has restarted and the nodes were restored. This results in the following:
    - All associated PDN connections (EPS bearer contexts) or PDP contexts of SGW-PGW getting deleted.

- ○ The received recovery value being stored and becoming the new value for the peer.
- If the stored value is larger than the value received, the received value is discarded. The stored value remains unchanged.

GTP Policy

A GTP policy contains rules that permit or deny packets. Multiple subpolicies are bound to a single GTP policy, which is then bound to the firewall rule.

The GTP policies and subpolicies defined within the GTP template enable the firewall to inspect GTP traffic. GTP Firewall performs the filtering by checking every single GTP packet against the policies configured on the GTP template and then forwards or drops the packet based on these policies.

Sometimes, you may want to forward packets that do not satisfy the configured (filtering and validation) policies and generate a log instead of being dropped. This behavior can be achieved by configuring some of the sub policies in the monitor mode. It helps to learn and understand the cause for the packet drops.

You can configure GTP Firewall using the command-line interface (CLI) or the aXAPI that utilizes REST web service calls.

For an example of a configured GTP Policy, see Creating a GTP Policy and Binding the Subpolicies.

GTP Subpolicies

The following are the subpolicies.

The following topics are covered:

Validation Policy

The validation policy ensures that the traffic received includes all of the required attributes to be considered a valid packet and discards any malicious packets by default. Based on the configuration, the malicious packets can also be forwarded for the purpose of learning or analyzing the traffic.

The following options ensure that the packets passing through the GTP Firewall are valid and safe:

- **Anomaly Checks**—Specifies whether to inspect the GTP header and drop the packets if there are any inconsistencies in the header. This policy is enabled by default.
- **Anti-spoofing checks**—Identifies a mismatched source IP address in a GTP-U packet from subscriber User Equipment (UE) IP address in the corresponding GTP-C message exchanged during tunnel setup. In case of downlink traffic, it identifies a mismatched destination IP address in a GTP-U packet to the subscriber User Equipment (UE) and IP address. This policy is disabled by default.

NOTE: When DHCP is used for IP address allocation, the IP address field in the GTP create message is set to 0, which prevents the identification of the UE IP spoofs.

- **Cross Layer Correlation**—Ensures that the IP addresses in the FTEID match the IP address in the IP header. The cross layer correlation can be performed only in the case of Delete Session Request. This policy is disabled by default. If the policy is enabled, the packets are dropped by default if the IP addresses mismatch.
- **Mandatory Information Element Checks**—Specifies whether the messages listed in the GTP Firewall Configuration section contain the mandatory information elements as specified by the protocol standards. If the mandatory information elements are missing, the packets are dropped by default. This policy is enabled by default.
- **MSISDN and IMSI Correlation**—Validates if the country code in MSISDN and mobile country code in IMSI match the same country code exchanged in the Create Session Request in GTPv2 and Create PDP Context Request in GTPv1 messages. In

the case of the country code mismatch, the packets are dropped by default. This policy is disabled by default.

- **Out of Order Information Element Checks—**Specifies whether GTPv1 messages are expected to have information elements in increasing order. The packets are dropped by default if this option is enabled and out of sequence information elements are received in a GTPv1 message. This policy is disabled by default.
- **Out of State Information Element Checks—**Ensures the packets in a GTP message received by the firewall include a request followed by response. GTP Firewall maintains the state for established connections and if the packets do not follow the expected sequence, they are dropped by default. This policy is disabled by default.
- **Reserved Information Element Checks—**Specifies whether information elements, defined in the 3GPP standard for future use, are permitted in a GTP message. When enabled, the packets that contain reserved information elements are dropped by default. This policy is enabled by default.
- **Sequence Number Correlation**—Ensures the sequence number value included in the request matches up with the sequence number in the response message during the exchange. If the value in the request and the response does not match, the packets are dropped by default. This policy is disabled by default.

NOTE: In some instances, the requests can get pipelined on a given tunnel. If more than 5 requests are pipelined, the packets are dropped till the responses for the pipelined requests are received.

Example Configuration:

In the following example, the policies are enabled and the invalid packets are dropped:

```
template gtp validation-policy Validate
anomaly-checks enable drop
anti-spoofing-check enable drop
crosslayer-correlation enable drop
mandatory-ie-filtering enable drop
msisdn-imsi-correlation enable drop
out-of-order-ie-filtering enable drop
out-of-state-ie-filtering enable drop
reserved-ie-check drop
```

```
sequence-num-correlation enable drop
```

In the following example, the policies are enabled and the packets are forwarded:

```
template gtp validation-policy Validate
anomaly-checks enable monitor
anti-spoofing-check enable monitor
crosslayer-correlation enable monitor
mandatory-ie-filtering enable monitor
msisdn-imsi-correlation enable monitor
out-of-order-ie-filtering enable monitor
out-of-state-ie-filtering enable monitor
reserved-ie-check monitor
sequence-num-correlation enable monitor
```

For information about configuring the Validation policy, see Configure Validation Policy.

For information about viewing the number of GTP packets that do not conform to the Validation Policy, see Validation Policy Counters.

APN IMSI Filtering Policy

GTP Firewall supports a combination of APN, IMSI, and Selection Mode filtering where the same template can be used for APN filtering, IMSI filtering, or a combination of filtering. It performs a regex match with the pattern that is received in the packet and drops or allows the packets depending on the configuration.

The supported combinations are as follows:

- APN only
- APN and IMSI
- APN, Selection Mode, and IMSI
- IMSI only (For IMSI filtering only, specify the APN as *)

The following selection modes can be configured:

- Mobile Station (MS)—Ensures the user subscription is not verified and the APN is provided by a Mobile Station.
- Network—Ensures the user subscription is not verified and the APN is provided by a Network.

- Verified—Ensures the user subscription is verified and the APN is provided by a Mobile Station or a Network.

IMSI corresponds to the subscriber’s SIM card information. It includes the following components:

- Mobile country code (MCC)
- Mobile network code (MNC)
- Mobile subscriber identification number (MSIN)

To use IMSI filtering for allowing only roaming partners, the IMSI filtering template must be bound to the ruleset as follows:

- Rule 1—Used for traffic destined to the local PGW/GGSN. This binds the template with the whitelist of local MCC.MNC.
- Rule 2—Used for traffic originating from the local SGW/SGSN. This binds the template with the whitelist of roaming partners MCC.MNC.
- Rule 3—Used for traffic originating from the local PGW/GGSN. This binds the template with the whitelist of local MCC.MNC.
- Rule 4—Used for traffic destined to the local SGW/SGSN. This binds the template with the whitelist of roaming partners MCC.MNC.

Within the 30,000 total entry length in a template, you can configure a maximum of 1000 APN IMSI entries.

Example Configuration

- APN only

```
template gtp apn-imsi-list apn
apn aaacom.com.mnc000.mcc000.gprs
apn aaacom.com.mnc000.mcc000.gprs selection mode <network |
mobilestation | verified)
imsi 3333
```

- APN and IMSI

```
template gtp apn-imsi-list apn
apn aaacom.com.mnc000.mcc000.gprs imsi 3333
```

- APN, Selection Mode, and IMSI

```
template gtp apn-imsi-list apn
apn aaacom.com.mnc000.mcc000.gprs selection mode <network |
mobilestation | verified)
imsi 3333
```

- IMSI only (For IMSI filtering only, specify the APN as *)

```
template gtp apn-imsi-list apn
apn * imsi 3333
```

For more information, see Configure APN/IMSI Filtering Policy.

MSISDN Filtering Policy

The MSISDN policy can be configured to permit or deny traffic matching the MSISDN prefix coming from specific countries. MSISDN is a unique 15-digit phone number of the subscriber. This number includes three components—a 2-digit Country Code (CC), a 3-digit National Destination Code (NDC), and a 10-digit subscriber phone number of the mobile device.

Example Configuration:

```
template gtp msisdn-list MSISDN permit
 msisdn 144799900217390
```

For more information, see Configure MSISDN Filtering Policy.

Message Filtering Policy

GTP Firewall provides the flexibility to selectively permit or deny a set of messages between SGW/SGSN and PGW/GGSN network elements on the configured interfaces. GTP Firewall can be deployed on the following interfaces:

- Roaming—The roaming interfaces include Gp and S8 interfaces.
- Non-roaming—The non-roaming interfaces include Gn and S5 interfaces.

You cannot configure both roaming and non-roaming interface types on a single policy. You must create a new message filtering policy to configure each interface type.

You can configure the GTP versions for each interface type. The supported versions are GTPv0, GTPv1, and GTPv2. By default, most of the message types under each version are enabled. You can either disable or enable the message types for allowing them on the interface.

NOTE: For GTPv0 message filtering to work, you must first enable GTPv0 in the general policy (general-policy). For information about general policy, see General Policy.

Example Configuration

- In this example, all three GTP versions are enabled on the roaming interface

```
template gtp message-filtering-policy test_1 interface-type roaming
```

where,

`message-filtering-policy test_1` specifies the name of the policy interface-type roaming specifies the interface type on which the GTP Firewall is deployed.

- In this example, only the GTPv2 is enabled

```
template gtp message-filtering-policy test_1 interface-type roaming
version-v2 enable
version-v1 disable
version-v0 disable
!
```

- In this example, only the GTPv1 is enabled and the message types Update PDP Context and PDU notification messages are disabled.

```
template gtp message-filtering-policy test_1 interface-type roaming
 version-v2 disable
 version-v1 enable
  message-type update-pdp disable
  message-type pdu-notification disable
 version-v0 disable!
!
```

For more information about configuring the Message Filtering policy, see Configure Message Filtering Policy.

Table 12 lists the GTP-v0, GTP-v1, and GTP-v2 message types that you can use to configure GTP message-type filtering on the roaming and non-roaming interface types.

For the list of GTP messages that are parsed, see GTPv2-C Messages and GTPv1-C Messages.

Table 12 : GTP Message Types

Message Type	Message Description
Version-v0	
create-aa-pdp	Create AA PDP context request and response
delete-aa-pdp	Delete AA PDP context request and response
create-pdp	Create PDP context request and response
update-pdp	Update PDP context request and response
delete-pdp	Delete PDP context request and response
gtp-pdu	Create GTP Protocol Data Unit (PDU)
pdu-notification	Create PDU Notification request and response Receive PDU Notification Reject Request Create PDU Notification Reject Response
reserved-messages	Allow or deny reserved message types
Version-v1	
create-mbms	Create MBMS context request and response
update-mbms	Update MBMS Context request and response
delete-mbms	Delete MBMS context request and response
create-pdp	Create PDP context request and response
update-pdp	Update PDP Context request and response
delete-pdp	Delete PDP context request and response
gtp-pdu	Create GTP Protocol Data Unit (PDU)
initiate-pdp	Initiate PDP context activation request and response
mbms-deregistration	MBMS Deregistration request and response
mbms-notification	MBMS Notification request and response
mbms-registration	MBMS Registration request and response
mbms-session	MBMS Session Start, Stop, and Update request and response
ms-info-change	MS Info Change Notification request and response

Table 12 : GTP Message Types

Message Type	Message Description
pdu-notification	PDU Notification request and response PDU Notification reject request and response
reserved-messages	Allow or deny reserved message types
Version-v2	
bearer-resource	Bearer Resource Command Bearer Resource Failure Indication
change-notification	Change Notification request and response
create-bearer	Create Bearer request and response
create-session	
delete-bearer	Delete Bearer request and response
delete-command	Delete Bearer Command Delete Bearer Failure Indication
delete-pdn	Delete PDN Connection request and response
delete-session	Delete Session request and response
modify-bearer	Modify Bearer request and response
modify-command	Modify Bearer Command Modify Bearer Failure Indication
pgw-downlink-trigger	PGW Downlink Trigger Notification PGW Downlink Trigger Notification acknowledge
remote-ue-report	Remote UE Report Notification Remote UE Report Acknowledge
reserved-messages	Allow or deny reserved message types
resume	Resume Notification Resume Acknowledge
suspend	Suspend Notification Suspend Acknowledge
trace-session	Trace Session Activation

Table 12 : GTP Message Types

Message Type	Message Description
	Trace Session Deactivation
update-bearer	Update Bearer request and response
update-pdn	Update PDN Connection request and response

Filtering Policy

This policy determines the filtering that is performed on a GTP message received by the firewall. The following options are available for filtering a GTP message:

- **APN IMSI Inspection:** This check allows you to choose the APN IMSI filtering policy configured in APN IMSI Filtering Policy. It performs a regex match with the pattern that is received in the packet and drops the packets that fail the APN IMSI inspection by default.
- **GTP-in-GTP Filtering**This check enables you to filter packets that have a GTP payload encapsulated in a GTP packet. This is identified by the presence of another GTP header after the first GTP header.
- **Message Filtering Policy:** This check enables you to bind the Message Filtering Policy with the Filtering Policy. If this policy is enabled, it drops the message types that should not be allowed to pass through the firewall by default. For more information, see Message Filtering Policy.
- **MSISDN Inspection:** This is similar to APN/IMSI inspection. The packet with a matching MSISDN is dropped by default if found in the packet. This check allows you to choose the MSISDN filtering policy configured in MSISDN Filtering Policy.
- **Radio Access Technology (RAT) Type Inspection:** This check allows you to control the RAT type that is being allowed to pass through the device. If a RAT type in the packet matches, the packet is dropped by default.

  The following RAT Types are supported:

  - UTRAN
  - GERAN
  - WLAN
  - GAN

- HSPA-evolution
- EUTRAN

The message inspection and filtering is category 1 and category 2 compliant.

By default, the packets that do not conform to the configured policy are dropped.

Example Configuration:

In the following example, the policies are enabled and the invalid packets are dropped:

```
template gtp filtering-policy FilteringPol
apn-imsi-filtering apn drop
gtp-in-gtp-filtering enable drop
message-filtering-policy MsgFilter drop
msisdn-filtering msisdn drop
rat-type-filtering utran drop
```

In the following example, the policies are enabled and the invalid packets are forwarded:

```
template gtp filtering-policy FilteringPol
apn-imsi-filtering apn monitor
gtp-in-gtp-filtering enable monitor
message-filtering-policy MsgFilter monitor
msisdn-filtering msisdn monitor
rat-type-filtering utran monitor
```

For more information about configuring the Filtering policy, see Configure Filtering Policy.

For information about viewing the number of GTP packets that do not conform to the policy, see Filtering Policy Counters.

Rate Limit Policy

The Rate Limit policy is designed to protect the network from volumetric attacks that attempt to exceed the network’s processing capacity. When the rate limit exceeds the configured threshold, the packets are dropped by default. The packets can also be forwarded for learning or analyzing the traffic.

This policy is used to configure rate limits for the following tunnel types:

- GTP-C tunnels—Message type rate limits.
- GTP-U tunnels—Upstream and downstream message and byte limits.

The Rate Limit policy can be reused in multiple policy templates.

Example Configuration:

In the following example, the packets exceeding the limit are dropped:

```
template gtp rate-limit-policy rate1 drop
```

```
    gtp-u-downlink-byte-rate <rate>
    gtp-u-downlink-packet-rate <rate>
    gtp-u-max-concurrent-tunnels <max-tunnels>
    gtp-u-total-byte-rate <rate>
    gtp-u-total-packet-rate <rate>
    gtp-u-tunnel-create-rate <rate>
    gtp-u-uplink-byte-rate <rate>
    gtp-u-uplink-packet-rate <rate>
    gtp-v0-c-aggregated-message-type-rate <rate>
    gtp-v1-c-aggregated-message-type-rate <rate>
    gtp-v2-c-aggregated-message-type-rate <rate>
    gtp-v1-c-create-pdp-request-rate <rate>
    gtp-v1-c-update-pdp-request-rate <rate>
    gtp-v2-c-create-session-request-rate <rate>
    gtp-v2-c-modify-bearer-request-rate <rate>
    lockout <1-1023> minutes
```

In the following example, the packets exceeding the limit are forwarded:

```
template gtp rate-limit-policy rate1 monitor
```

```
    gtp-u-downlink-byte-rate <rate>
    gtp-u-downlink-packet-rate <rate>
    gtp-u-max-concurrent-tunnels <max-tunnels>
    gtp-u-total-byte-rate <rate>
    gtp-u-total-packet-rate <rate>
    gtp-u-tunnel-create-rate <rate>
```

The previous example includes the `gtp-u-max-concurrent-tunnels` line that does not include `<rate>` but instead includes `<max-tunnels>`, which is the count of the current number of GTP-U tunnels at APN-Prefix/Network Element level.

GTP rate limiting is enforced at the peer level (SGW/PGW) by configuring a class list and binding the Rate Limit template to a single peer with either an IPv4 or IPv6 address. For example, for network elements (peers) where the last two lines activate the limit policy:

```
class-list <peer-list>
   <peer-IP-1/Subnet-1> gtp-rate-limit-policy <name1>
   <peer-IP-2/Subnet-2> gtp-rate-limit-policy <name2>
   [...]
fw gtp network element-list-v4  <v4-class-list-name>
fw gtp network element-list-v6  <v6-class-list-name>
```

GTP Rate Limit functionality is also supported at the APN Prefix level (Destination Network) by configuring a string class list and binding the Rate Limit template to an APN using the following syntax (where the last line activates the limit policy):

```
class-list <apn-list-name> ac
   starts-with <apn-prefix-1> gtp-rate-limit-policy <name-1>
   starts-with <apn-prefix-2> gtp-rate-limit-policy <name-2>
   starts-with <apn-prefix-3> gtp-rate-limit-policy <name-2>
   [...]
fw gtp apn-prefix-list  <apn-prefix-class-list>
```

For example:

```
template gtp rate-limit-policy rate1 drop

   gtp-u-downlink-packet-rate 100

   gtp-u-upstream-byte-rate 2000

   gtp-u-downstream-byte-rate 1000

template gtp rate-limit-policy rate2 drop
   gtp-u-downstream-packet-rate 200
   gtp-u-upstream-byte-rate 3000
   gtp-u-downstream-byte-rate 4000
```

```
class-list myv4list ipv4
   10.1.1.1/32  gtp-rate-limit-policy rate1
   20.1.1.1/32 gtp-rate-limit-policy rate2

class-list prefix1 string  ac
   starts-with www gtp-rate-limit-policy rate1
   starts-with www1 gtp-rate-limit-policy rate2
fw gtp network-element-list-v4  myv4list
fw gtp apn-prefix-list prefix1
```

You can enable logs to be generated when the packets are dropped due to GTP rate limiting at the APN-Prefix or Network Element (SGW/PGW) level. The logs are generated for the following message types:

- gtp-v0-c-aggregated-message-type-rate
- gtp-v1-c-aggregated-message-type-rate
- gtp-v2-c-aggregated-message-type-rate
- gtp-v1-c-create-pdp-request-rate
- gtp-v1-c-update-pdp-request-rate
- gtp-v2-c-create-session-request-rate
- gtp-v2-c-modify-bearer-request-rate

To enable logging, you must configure the log periodicity. The log periodicity can be set from 1 to 30 minutes. For example, if the periodicity is set to 2 minutes, a log is generated every 2 minutes for every message type providing the details on the Rate-Limiting Entity (APN or Network Elements key), GTP-C message type, and drop count since the last log. If there are no packet drops associated with a message type in 2 minutes, a log is not be generated for that message type.

The following example displays how to enable log periodicity for GTP rate limiting:

```
fw gtp network-element-list-v4  myv4list log-periodicity <1-30> mins
fw gtp apn-prefix-list prefix1 log-periodicity <1-30> mins
```

The `Log Event GTP Rate Limit Periodic` counter is incremented every time a log is generated for GTP rate limiting. To view the GTP firewall logging counters, use the **`show counters fw logging gtp`** command. For more information about counters, see GTP Counters and Statistics.

For more information about configuring the Rate Limit policy, see Configure Rate Limit Policy.

For information about viewing the number of GTP packets that do not conform to the policy, see Rate Limit Counters.

For more information, see GTP Counters and Statistics.

General Policy

General policies contain the following three configuration values that apply to GTP processing on GTP Firewall:

- **Tunnel Timeout—**Removes the GTP tunnel and reclaims the resources allocated for it after the specified time has passed. This value is configured in minutes ranging from 5 to a maximum of 1000 hours. The default value is 1440 (24 hours).
- **Handover Timeout—**Specifies the period for which the GTP tunnel between the previous SGW and PGW remains active after the handover request (that is, Modify Bearer Request for GTPv2 and Update PDF Context Request for GTPv1) is received from the new SGSN or SGW. After the handover timeout period, the old GTP tunnel gets deleted. This value is configured in minutes ranging from 1 to a maximum of 63 minutes. The default value is 2 minutes.
- **Maximum Message Length—**Specifies the maximum number of bytes allowed in GTP messages. This helps prevent code injection attacks and protect the network. This value is configured in bytes and range from 64 to 1500. The default value is 1500. When the maximum message length exceeds the configured value, the packets are dropped by default. The packets can also be forwarded for learning or analyzing the traffic.
- **GTP Version 0—**Specifies whether internetwork compatibility with GTPv0 is permitted. GTPv0 is disabled by default. The options are permit and deny.

Example Configuration:

In the following example, the packets exceeding the configured values are dropped by default:

```
template gtp general-policy "name"
tunnel-timeout 1440
handover-timeout 2
maximum-message-length 1500 drop
```

```
gtp-version v0 permit
```

In case of maximum-message-length, the packets are dropped by default. You can also configure the packets to be forwarded. In the following example, the packets exceeding the maximum message length are forwarded:

```
template gtp general-policy "name"
maximum-message-length 1500 monitor
```

For more information about configuring the General policy, see Configure General Policy.

For information about the number of packets dropped due to IE length exceeding the message length and the GTP header length not matching the UDP header length, see Message Length Counters.

Logging Policy

This policy defines the events that GTP Firewall logs when a packet is being dropped. Each of the policies mentioned in this section have drop events that are consolidated in one log template.

Example Configuration:

```
template gtp logging-policy <name>
log anti-spoofing-check
log apn-imsi-filtering
log crosslayer-correlation
log gtp-in-gtp-filtering
```

log invalid-header-check

```
log invalid-teid-check
log mandatory-ie-check
log max-message-length-check
log message-filtering
log msisdn-filtering
log msisdn-filtering
log msisdn-imsi-correlation
log out-of-order-ie-check
log out-of-state-ie-check
log rat-type-filtering
log reserved-ie-check
log sequence-num-correlation
```

For more information, see Configure Logging Policy.

GTP-U Inner IP Filtering

A service provider may want to prevent a subscriber from accessing some specific destinations that are forbidden due to malicious behavior or compromised equipment. Such access may expose subscribers and service provider infrastructure to security threats. Using the Threat Intel capability, the GTP firewall can block unauthorized access by dropping the packets coming from or going to such malicious destinations.

The GTP firewall leverages the Threat Intelligence module (or Threat Intel for short) that provides data about malicious IP addresses on the internet. The IP addresses of the threat actors and the forbidden destinations are collected to create a class-list. A collection of such class-lists can be used to create a Threat List. In addition, you can create a class-list with a list of malicious IPs and bind it to the threat-list.

When an IP threat list is configured, the GTP firewall matches the inner IP address of the GTP-U tunnel with the source or the destination IP addresses listed on the threat list. If the IP addresses match, the GTP firewall drops the traffic and prevents the subscriber from connecting to a malware IP address.

To configure an IP threat list, see Configuring IP Threat List.

For more information about Threat Intel, see Threat Intelligence.

GTP VRRP-A Support

GTP-FW supports the Virtual Router Redundancy Protocol (VRRP) to ensure high availability and seamless failover, providing optimal performance, session continuity, and efficient failover management.

Key Features of VRRP-A support:

- VRRP-A operates in two modes - active and standby.
- The GTP tunnel information and state are replicated across nodes used in failover scenarios.
- Traffic Handling:
  - Traffic is always directed to the active node.
  - Under normal conditions only the active device processes the packets; the standby node remains passive and does not process GTP packets if received.
  - When GTP-FW is enabled on the active node, it inspects and forwards GTP packets based on the configured or default GTP policy.
- The active node synchronizes session data with the standby node to enable a smooth transition during a failover.
- In the event of a failover, the standby node takes over, ensuring minimal disruption and continuous service.

NOTE: The GTP-FW state will be synced to the standby node only when the GTP-FW configuration is intact with the active node.

GTP Firewall Configuration

This section describes the configuration commands that are used to implement a GTP protocol. The following procedures are required.

The following topics are covered:

Refer to GTP Policy for additional details.

Creating Subpolicies

The following sections describe configuring the subpolicy templates that are later bound to the GTP Policy. At least one subpolicy must be included in the main GTP Policy.

The following topics are covered:

Configure Validation Policy

The Protocol Validation Policy contains the checks that ensure that the packets received are valid and conform to standards specified by the protocol. Refer to Validation Policy for information about template options.

The following commands use the Protocol Validation Policy configuration mode and enable specific checks for use by the firewall.

```
ACOS[GTP-test](config)# template gtp validation-policy NAME-200
ACOS[GTP-test](config-gtp-validation-policy)# anomaly-checks enable
monitor|drop
ACOS[GTP-test](config-gtp-validation-policy)# anti-spoofing-check enable
monitor | drop
ACOS[GTP-test](config-gtp-validation-policy)# crosslayer-correlation
enable monitor | drop
ACOS[GTP-test](config-gtp-validation-policy)# mandatory-ie-filtering
enable monitor | drop
ACOS[GTP-test](config-gtp-validation-policy)# msisdn-imsi-correlation
enable monitor | drop
ACOS[GTP-test](config-gtp-validation-policy)# out-of-order-ie-filtering
enable monitor | drop
```

```
ACOS[GTP-test](config-gtp-validation-policy)# out-of-state-ie-filtering
enable monitor | drop
ACOS[GTP-test](config-gtp-validation-policy)# reserved-ie-check enable
monitor | drop
ACOS[GTP-test](config-gtp-validation-policy)# sequence-num-correlation
enable monitor | drop
ACOS[GTP-test](config-gtp-validation-policy)# exit
```

NOTE: By default, the packets that do not conform to the configured policy are dropped.

Configure APN/IMSI Filtering Policy

APN/IMSI and MSISDN filter lists are referenced by Inspection Policy templates to include APN/IMSI and MSISDN items that need to be filtered. Refer to Configure Filtering Policy for information about implementing the lists after their creation.

The following commands create and configure two filter lists (`LIST-100` and `LIST-200`) for inclusion in the firewall:

```
ACOS[GTP-test](config)# template gtp apn-imsi-list LIST-100
ACOS[GTP-test](config-gtp-apn-imsi-list)# apn
aaacom.com.mnc000.mcc000.gprs selection mode <network | mobilestation |
verified) imsi 33334444333344
ACOS[GTP-test](config-gtp-apn-imsi-list)# exit
```

Configure MSISDN Filtering Policy

MSISDN filter lists are referenced by Inspection Policy templates to include MSISDN items that need to be filtered. Refer to Configure Filtering Policy for information about implementing the lists after their creation.

```
ACOS[GTP-test](config)# template gtp msisdn-list LIST-200
ACOS[GTP-test](config-gtp-msisdn-list)# msisdn 311280001001
ACOS[GTP-test](config-gtp-msisdn-list)# exit
```

Configure Message Filtering Policy

Message Filtering Policy configures messages that are exchanged between two network elements. By default, all GTP messages are dropped. This policy is required to allow GTP message processing. Refer to Message Filtering Policy for information about template options.

Use the following commands for configuring Message Filtering Policy and enable communications for specific interfaces.

```
ACOS[GTP-test](config)# template gtp message-filtering-policy NAME-300
interface-type roaming | non-roaming
ACOS[GTP-test](config-gtp-message-filtering-policy)# version-v0 enable  |
disable
ACOS[GTP-test](config-gtp-message-filtering-policy)# version-v1 enable  |
disable
ACOS[GTP-test](config-gtp-message-filtering-policy)# version-v2 enable |
disable
ACOS[GTP-test](config-gtp-message-filtering-policy)# exit
```

Configure Filtering Policy

This policy determines the filtering that is performed on a GTP message received by the firewall. Refer to Filtering Policy for information about template options.

Use the following commands for configuring Filtering Policy and enable communications for specific interfaces.

```
ACOS[GTP-test](config)# template gtp filtering-policy NAME-400
ACOS[GTP-test](config-gtp-filtering-policy)# apn-imsi-filtering APN
monitor | drop
ACOS[GTP-test](config-gtp-filtering-policy)# gtp-in-gtp-filtering enable
monitor | drop
ACOS[GTP-test](config-gtp-filtering-policy)# message-filtering-policy
NAME-300 monitor | drop
ACOS[GTP-test](config-gtp-filtering-policy)# msisdn-filtering MSISDN
monitor | drop
ACOS[GTP-test](config-gtp-filtering-policy)# rat-type-filtering
utran|geran|wlan|gan|hspa-evolution|eutran [monitor | drop]
ACOS[GTP-test](config-gtp-filtering-policy)# exit
```

NOTE: By default, the packets that do not conform to the configured policy are dropped.

Configure Rate Limit Policy

The Rate Limit policy is designed to protect the network from volumetric attacks that attempt to exceed the network's processing capacity. Refer to Rate Limit Policy for information about the options that are available for rate limiting GTP messages.

The following commands use the Rate Limit Policy configuration mode and enable specific options.

```
ACOS[GTP-test](config)# template gtp rate-limit-policy NAME-500 monitor | drop
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-u-downlink-byte-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-u-downlink-packet-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-u-max-concurrent-tunnels <max-tunnels>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-u-total-byte-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-u-total-packet-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-u-tunnel-create-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-u-uplink-byte-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-u-uplink-packet-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-v0-c-aggregated-message-type-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-v1-c-aggregated-message-type-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-v1-c-create-pdp-request-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-v1-c-update-pdp-request-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-v2-c-aggregated-message-type-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-v2-c-create-session-request-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# gtp-v2-c-modify-bearer-request-rate <rate>
ACOS[GTP-test](config-gtp-rate-limit-policy)# lockout <1-1023> minutes
```

```
ACOS[GTP-test](config-gtp-rate-limit-policy)# exit
```

NOTE: By default, the packets that do not conform to the configured policy are dropped. The packets are forwarded only if "monitor" is configured.

The following commands enforce GTP rate limiting at the peer level (SGW/PGW) by configuring a class list and binding the Rate Limit template to a single peer with either an IPv4 or IPv6 address.

```
ACOS[GTP-test](config)# class-list ClassList_1
ACOS[GTP-test](config-class list)# <peer-IP-1/Subnet-1> gtp-rate-limit-policy <name1>
ACOS[GTP-test](config-class list)# <peer-IP-2/Subnet-2> gtp-rate-limit-policy <name2>

ACOS[GTP-test](config)# fw gtp network-element-list-v4 <class-list name>
ACOS[GTP-test](config)# fw gtp network-element-list-v6 <class-list name>
```

The following commands configure a string class list and binds the Rate Limit template to an APN:

```
ACOS[GTP-test](config)# class-list ClassList_1 ac
ACOS[GTP-test](config-class list)# starts-with <apn-prefix-1> gtp-rate-limit-policy <name1>
ACOS[GTP-test](config-class list)# starts-with <apn-prefix-2> gtp-rate-limit-policy <name2>
ACOS[GTP-test](config-class list)# starts-with <apn-prefix-3> gtp-rate-limit-policy <name3>
```

```
ACOS[GTP-test](config)# fw gtp apn-prefix-list <class-list name>
```

The following command enables logging when the packets are dropped due to GTP rate limiting at the APN-Prefix or Network Element (SGW/PGW) level:

```
ACOS[GTP-test](config)# fw gtp network-element-list-v6 <class-list name> log-periodicity <1-30>
ACOS[GTP-test](config)# fw gtp apn-prefix-list <class-list name> log-periodicity <1-30>
```

Log periodicity is set in minutes.

Configure General Policy

The General Policy template includes parameters that are applicable to all GTP processing on the device. This policy is configured using the GTP General Policy configuration mode.

The command shown in the first line creates the General Policy template called **NAME-100** and enters the `config-gtp-general-policy` mode (shown in lines two through five). The **tunnel-timeout**, **maximum-message-length**, and **gtp-version** parameters (described in General Policy) are added and configured in lines two through four.

```
ACOS[GTP-test](config)# template gtp general-policy NAME-100
ACOS[GTP-test](config-gtp-general-policy)# tunnel-timeout 2000
ACOS[GTP-test](config-gtp-general-policy)# maximum-message-length 1400
monitor | drop
ACOS[GTP-test](config-gtp-general-policy)# handover-timeout 2
ACOS[GTP-test](config-gtp-general-policy)# gtp-version v0 permit
ACOS[GTP-test](config-gtp-general-policy)# exit
```

NOTE: By default, the packets that do not conform to the configured policy are dropped. For maximum message length, the packets that do not conform to the predefined General Policy are forwarded only if "monitor" is configured.

Configure Logging Policy

Logging policies specify the events that GTP Firewall logs when it drops a packet. Refer to Logging Policy for information about options that are available for inspecting GTP messages. The **log** command description lists the logging options.

The following commands use the Logging Policy configuration mode and enable logging for specific logging options.

```
ACOS[GTP-test](config)# template gtp logging-policy NAME-600
ACOS[GTP-test](config-gtp-logging-policy)# log anti-spoofing-check
ACOS[GTP-test](config-gtp-logging-policy)# log apn-imsi-filtering
ACOS[GTP-test](config-gtp-logging-policy)# log crosslayer-correlation
ACOS[GTP-test](config-gtp-logging-policy)# log gtp-in-gtp-filtering
ACOS[GTP-test](config-gtp-logging-policy)# log invalid-teid-check
ACOS[GTP-test](config-gtp-logging-policy)# log invalid-header-check
ACOS[GTP-test](config-gtp-logging-policy)# log mandatory-ie-check
ACOS[GTP-test](config-gtp-logging-policy)# log max-message-length-check
```

```
ACOS[GTP-test](config-gtp-logging-policy)# log message-filtering
ACOS[GTP-test](config-gtp-logging-policy)# log msisdn-filtering
ACOS[GTP-test](config-gtp-logging-policy)# log msisdn-filtering
ACOS[GTP-test](config-gtp-logging-policy)# log msisdn-imsi-correlation
ACOS[GTP-test](config-gtp-logging-policy)# log out-of-order-ie-check
ACOS[GTP-test](config-gtp-logging-policy)# log out-of-state-ie-check
ACOS[GTP-test](config-gtp-logging-policy)# log rat-type-filtering
ACOS[GTP-test](config-gtp-logging-policy)# log reserved-ie-check
ACOS[GTP-test](config-gtp-logging-policy)# log sequence-num-correlation
ACOS[GTP-test](config-gtp-logging-policy)# exit
```

Creating a GTP Policy and Binding the Subpolicies

The GTP-Policy template lists the subpolicies that are utilized by firewalls to which the template is bound. A subpolicy template must be configured using one of the previously described processes before it is bound to a GTP Policy.

The following commands create a GTP Policy named `GTP-000` (line one) and then binds the templates created in the previous sections to the newly-created policy (lines two through six).

```
ACOS[GTP-test](config)# template gtp-policy GTP-000
ACOS[GTP-test](config-gtp-policy)# gtp general-policy NAME-100
ACOS[GTP-test](config-gtp-policy)# gtp protocol-conformance-policy NAME-200
ACOS[GTP-test](config-gtp-policy)# gtp logging-policy NAME-500
ACOS[GTP-test](config-gtp-policy)# gtp inspection-policy NAME-400
ACOS[GTP-test](config-gtp-policy)# gtp message-filtering-policy NAME-300
ACOS[GTP-test](config-gtp-policy)# exit
```

Creating a Firewall Rule-Set and Binding the GTP Policy

GTP Firewall is implemented by including the Policy template as a rule within a firewall rule-set. The following commands configures a typical firewall:

```
ACOS[GTP-test](config)# rule-set GTP-200
ACOS[GTP-test](config-rule set:GTP-200)# rule GTP-201
ACOS[GTP-test](config-rule set:GTP-200-rule:GTP-201)# action permit log
```

```
ACOS[GTP-test](config-rule set:GTP-200-rule:GTP-201)# source ipv4-address any
ACOS[GTP-test](config-rule set:GTP-200-rule:GTP-201)# source zone any
ACOS[GTP-test](config-rule set:GTP-200-rule:GTP-201)# dest ipv4-address any
ACOS[GTP-test](config-rule set:GTP-200-rule:GTP-201)# dest zone any
ACOS[GTP-test](config-rule set:GTP-200-rule:GTP-201)# service udp dst eq 2123
ACOS[GTP-test](config-rule set:GTP-200-rule:GTP-201)# exit
```

The following commands include the GTP Policy into the rule:

```
ACOS[GTP-test](config-rule set:GTP-200-rule:GTP-201)# template gtp-policy GTP-000
ACOS[GTP-test](config-rule set:GTP-200)# exit
```

Complete the procedure described in the Enabling GTP and Activating the Firewall Rule-set section to enable the main policy and activate the firewall rule-set.

Enabling GTP and Activating the Firewall Rule-set

You can create many rule-sets, but only one can be activated at a given time. The active rule-set is the one actually processing the network traffic. Use the following command to enable GTP in the `GTP-test` L3V partition (line 1), then activate the firewall rule-set (line 2):

```
ACOS[GTP-test](config)# fw gtp enable
ACOS[GTP-test](config)# fw active-rule-set GTP-200
```

You can use the `show` command as follows to display the rule-set that is currently active:

```
ACOS[GTP-test](config)# show rule-set
```

For information about GTP session , see Show GTP Session.

For information about the counters displayed for uplink and downlink, ingress and egress, Packets and Bytes count per GTP protocol, see Packets and Bytes Counters.

For information about the counters displayed to indicate the packet drops due to routing failure, see Routing Failure Counters.

Enabling GTP Processing on a Partition

GTP Firewall can be enabled on an L3V partition. The following commands create a new partition called `GTP-test` and enables GTP Firewall processing on that partition. Creating a new partition enters the `config-partition:<name>` mode. Remember to exit the `config-partition` mode before enabling the new partition.

You can configure a total of 64 GTP templates on each partition, but only one default template may be configured per partition.

Use the following commands to enable a GTP template on an L3V partition:

```
ACOS(config)# partition GTP-test id 14
ACOS(config-partition:GTP-test)# exit
ACOS[GTP-test](config)# fw gtp enable
ACOS[GTP-test](config)#
```

Configuring GTP Firewall Deployment Mode

GTP Firewall can be deployed in two modes:

- **Tap Mode—**In this mode, the GTP firewall acts on a copy of the network traffic coming through the firewall. Tap mode allows for monitoring the traffic, evaluating policy violations, and reporting various alerts. It helps to identify the attacks happening in the network and, at the same time, ensure that no traffic is disrupted or dropped, thus preserving the subscriber connectivity.

  Use the following commands to configure GTP in the tap mode:

  ```
  ACOS(config)# fw tap-monitor
  ACOS(config-tap-monitor)# enable
  ACOS(config-tap-monitor)# ethernet 1
  ```

- **Insertion Mode**—In this mode, the GTP FW is inserted inline and you can select the following options:

  - **monitor**: Similar to the TAP Mode, the monitor mode allows for monitoring and evaluating the traffic without dropping or altering the packets. Configuring the monitor mode and generating the reports during the initial phase of GTP deployment or when there are too many packet drops helps the operator to learn and understand the type of attacks occurring in the network before activating the full-protection mode. For activating the full-protection mode, see Full-Protection Mode.

You can configure the monitor mode at the GTP firewall configuration level or the sub policy level. When configured at the GTP configuration level, it overrides the monitor mode configured at the sub-policy level.

Use the following command to deploy GTP in the insertion mode and enable the **monitor** mode:

```
ACOS(config)# fw gtp insertion-mode monitor
```

The `GTP messages forwarded via monitor mode` counter is incremented each time an invalid packet is forwarded. To view this counter, use the `show counters fw gtp` command.

- ○ **skip-state checks**—In this mode, the GTP packets without a state in an existing network are forwarded. This option is useful when a new GTP firewall is deployed in an existing network with traffic flowing through preexisting GTP tunnels and the GTP firewall does not have the necessary state to accurately track those transactions. As a result, the packets may be dropped due to the lack of state information. To prevent such drops for an existing session, you can configure **skip-state-checks** to forward packets without a state while configuring the GTP firewall for new tunnels.

  Use the following command to deploy GTP in the insertion mode and enable **skip-state-checks**:

  ```
  ACOS(config)# fw gtp insertion-mode skip-state-checks
  ```

  The `GTP Stateless Forward` counter is incremented each time a packet is forwarded without a state. This configuration must be disabled once the Stateless Forward counter reduces to a reasonable number and the GTP firewall has a state for most of the ongoing GTP tunnels.

- **Full-Protection Mode** — In this mode, the GTP firewall monitors the actual traffic, enforces the configured policies, and drops or redirects the non-conforming traffic. The logs are generated and the reports are created for various alerts.

Use the following command to change the GTP configuration from the monitor mode to the full-protection mode:

```
ACOS(config)# no fw gtp insertion-mode monitor
```

Configuring GTP Echo

The following example shows how to configure echo timeout and enable log for GTP echo:

```
ACOS# show running-config fw gtp
!Section configuration: 95 bytes
!
fw gtp state-management echo-timeout 200
fw gtp state-management Enable-Log
!
```

The echo idle timeout is configured using `Echo-timeout`. The Echo timeout value is calculated using the following formula:

```
Echo-timeout = echo interval + 2*T3_resp + 4*T3_resp... (N3request-1) times
```

where,

- echo interval—indicates the wait time before retransmitting the echo request after receiving the response
- N3 requests—represents the number of retries and T3 response, that is the wait time for echo response during retransmits

The default value for Echo timeout is 120 minutes with a range of 1 to 261 minutes.

Logging for echo messages is enabled and disabled using `Enable-Log`. Only the information events are generated with echo messages while the node restoration information events can be generated by any GTP-C message.

Configuring NetFlow/IPFIX

The following sections show a NetFlow configuration example. Refer to the “NetFlow v9 and v10 (IPFIX)” section in the *Traffic Logging Guide* for a description of NetFlow parameters.

Configuring NetFlow Templates

The following commands configure a NetFlow template named GTP-DENY that monitor deny commands.

```
ACOS(config)# netflow template GTP-DENY
ACOS(config-template:GTP-DENY)# information-element fw-deny-reset-event
ACOS(config-template:GTP-DENY)# information-element source-ipv4-address
ACOS(config-template:GTP-DENY)# information-element dest-ipv4-address
ACOS(config-template:GTP-DENY)# information-element source-port
ACOS(config-template:GTP-DENY)# information-element dest-port
ACOS(config-template:GTP-DENY)# information-element imsi
ACOS(config-template:GTP-DENY)# information-element msisdn
ACOS(config-template:GTP-DENY)# information-element gtp-apn
ACOS(config-template:GTP-DENY)# information-element gtp-deny-reason
ACOS(config-template:GTP-DENY)# information-element gtp-dteid
ACOS(config-template:GTP-DENY)# information-element gtp-selection-mode
ACOS(config-template:GTP-DENY)# information-element gtp-steid
ACOS(config-template:GTP-DENY)# information-element gtp-mcc
ACOS(config-template:GTP-DENY)# information-element gtp-mnc
ACOS(config-template:GTP-DENY)# information-element gtp-rat-type
ACOS(config-template:GTP-DENY)# information-element gtp-pdn-pdp-type
ACOS(config-template:GTP-DENY)# information-element gtp-uli
ACOS(config-template:GTP-DENY)# information-element gtp-enduser-v4-addr
ACOS(config-template:GTP-DENY)# information-element gtp-enduser-v6-addr
ACOS(config-template:GTP-DENY)# information-element gtp-bearer-id-or-nsapi
ACOS(config-template:GTP-DENY)# information-element gtp-qci
ACOS(config-template:GTP-DENY)# information-element gtp-info-event-ind
ACOS(config-template:GTP-DENY)# information-element gtp-restarted-node-ipv4
ACOS(config-template:GTP-DENY)# information-element gtp-restarted-node-ipv6
ACOS(config-template:GTP-DENY)# information-element gtp-c-tunnels-removed-with-node-restart
ACOS(config-template:GTP-DENY)# template-id 2511
ACOS(config-template:GTP-DENY)# exit

ACOS(config)# show run | sec netflow
netflow template GTP-DENY
  information-element fw-deny-reset-event
  information-element source-ipv4-address
  information-element dest-ipv4-address
  information-element source-port
  information-element dest-port
  information-element imsi
  information-element msisdn
  information-element gtp-apn
  information-element gtp-deny-reason
  information-element gtp-dteid
  information-element gtp-selection-mode
  information-element gtp-steid
  information-element gtp-mcc
  information-element gtp-mnc
  information-element gtp-rat-type
  information-element gtp-pdn-pdp-type
  information-element gtp-uli
  information-element gtp-enduser-v4-addr
  information-element gtp-enduser-v6-addr
  information-element gtp-bearer-id-or-nsapi
  information-element gtp-qci
  information-element gtp-info-event-ind
  information-element gtp-restarted-node-ipv4
  information-element gtp-restarted-node-ipv6
  information-element gtp-c-tunnels-removed-with-node-restart
template-id 2511
```

The following commands configure a NetFlow template that monitors GTP tunnels:

```
ACOS1(config)# netflow template FW-1
ACOS1(config-template:FW-1)#information-element source-ipv4-address
ACOS1(config-template:FW-1)#information-element dest-ipv4-address
ACOS1(config-template:FW-1)#information-element source-port
ACOS1(config-template:FW-1)#information-element dest-port
ACOS1(config-template:FW-1)#information-element rule-name
ACOS1(config-template:FW-1)#information-element rule-set-name
ACOS1(config-template:FW-1)#information-element imsi
ACOS1(config-template:FW-1)#information-element msisdn
ACOS1(config-template:FW-1)#information-element gtp-apn
ACOS1(config-template:FW-1)#information-element gtp-steid
ACOS1(config-template:FW-1)#information-element gtp-dteid
ACOS1(config-template:FW-1)#information-element gtp-selection-mode
```

```
ACOS1(config-template:FW-1)#information-element gtp-deny-reason
ACOS1(config-template:FW-1)#information-element gtp-mcc
ACOS1(config-template:FW-1)#information-element gtp-mnc
ACOS1(config-template:FW-1)#information-element gtp-rat-type
ACOS1(config-template:FW-1)#information-element gtp-pdn-pdp-type
ACOS1(config-template:FW-1)#information-element gtp-uli
ACOS1(config-template:FW-1)#information-element gtp-enduser-v4-addr
ACOS1(config-template:FW-1)#information-element gtp-enduser-v6-addr
ACOS1(config-template:FW-1)#information-element gtp-bearer-id-or-nsapi
ACOS1(config-template:FW-1)#information-element gtp-qci
ACOS1(config-template:FW-1)#information-element gtp-info-event-ind
ACOS1(config-template:FW-1)#information-element gtp-restarted-node-ipv4
ACOS1(config-template:FW-1)#information-element gtp-restarted-node-ipv6
ACOS1(config-template:FW-1)#information-element gtp-c-tunnels-removed-with-node-restart
ACOS1(config-template:FW-1)#template-id 2510
ACOS1(config-template:FW-1)# exit
ACOS1(config)# show run | sec FW-1
netflow template FW-1
  information-element source-ipv4-address
  information-element dest-ipv4-address
  information-element source-port
  information-element dest-port
  information-element rule-name
  information-element rule-set-name
  information-element imsi
  information-element msisdn
  information-element gtp-apn
  information-element gtp-steid
  information-element gtp-dteid
  information-element gtp-selection-mode
  information-element gtp-deny-reason
  information-element gtp-mcc
  information-element gtp-mnc
  information-element gtp-rat-type
  information-element gtp-pdn-pdp-type
  information-element gtp-uli
  information-element gtp-enduser-v4-addr
  information-element gtp-enduser-v6-addr
  information-element gtp-bearer-id-or-nsapi
  information-element gtp-qci
  information-element gtp-info-event-ind
  information-element gtp-restarted-node-ipv4
  information-element gtp-restarted-node-ipv6
  information-element gtp-c-tunnels-removed-with-node-restart
```

The following commands configure a NetFlow template that monitors GTP rate limiting:

```
ACOS1(config)# netflow template rate-limit
ACOS1(config-template:rate-limit)#information-element rate-limit-key
ACOS1(config-template:rate-limit)#information-element rate-limit-type
ACOS1(config-template:rate-limit)#information-element rate-limit-drop-
count
ACOS1(config)# show run | sec rate-limit
netflow template rate-limit
information-element rate-limit-key
information-element rate-limit-type
information-element rate-limit-drop-count
```

Configuring NetFlow Monitors

The following commands configure NetFlow monitors that implement the templates.

```
ACOS1(config)# netflow monitor s1
ACOS1(config-netflow-monitor)# protocol v10
ACOS1(config-netflow-monitor)# custom-record deny-reset-event-fw4 template
GTP-DENY
ACOS1(config-netflow-monitor)# destination 10.4.4.100
ACOS1(config-netflow-monitor)# resend-template records 1
ACOS1(config-netflow-monitor)# exit

ACOS1(config)# netflow monitor s2
ACOS1(config-netflow-monitor)# protocol v10
ACOS1(config-netflow-monitor)# custom-record sesn-event-fw4-creation
template FW-1
ACOS1(config-netflow-monitor)# custom-record sesn-event-fw4-deletion
template FW-1
ACOS1(config-netflow-monitor)# destination 10.4.4.100
ACOS1(config-netflow-monitor)# resend-template records 1
ACOS1(config-netflow-monitor)# exit
```

The following commands configure NetFlow monitors for exporting GTP rate limiting:

```
ACOS1(config)# netflow monitor s1
ACOS1(config-netflow-monitor)# protocol v10
ACOS1(config-netflow-monitor)# custom-record gtp-rate-limit-periodic
template rate-limit
ACOS1(config-netflow-monitor)# destination 10.4.4.100
ACOS1(config-netflow-monitor)# resend-template records 1
ACOS1(config-netflow-monitor)# exit
```

Logging and Visibility

GTP Firewall supports optional off-device logging to track deny and permit events in Syslog and IPFIX formats providing visibility into subscriber identity and GTP tunnel information. Additionally, a set of counters are available for state tracking and GTP drops.

GTP Firewall provides the ability to log two types of events:

- GTP Tunnel Events
- GTP Deny Events

GTP Firewall supports logging the events in the following formats:

- Syslog
  - CEF
  - ASCII
- IPFIX

This section covers the following:

- Syslog
- IPFIX
- GTP Counters and Statistics

Syslog

GTP Session Logging provides logging information in the CEF format for session creation and session deletion. Each log entry includes Source IP, Destination IP, Tunnel Endpoint Identifier, message type, packet status (permit) as shown in the following examples:

```
Syslog 708 LOCAL7.DEBUG:  Nov 27 02:08:28 2019 vThunder
CEF:0|A10|ADC|5.1.0|FW 100|Session opened|1|proto=UDP act=Permit rt=124974
c6a2=2405:200:331:3::10 c6a3=2405:200:331:9::20
deviceInboundInterface=ethernet1 deviceOutboundInterface=ethernet2 cs1=fw
cs2=gtp_c_v2_v1_ipv6 gtp-version=v2 gtp-message-id=33 suid=10001
duid=10003 dhost=a10net.mnc872.mcc405.gprs
deviceExternalId=405872000010045 selectionMode=MS or Network provided APN,
subscription verified msisdn=917011014337 imei=3576900603487001
**```mcc=405 mnc=872```** userLocation=1804257899990425780027OF10
ratType=EUTRAN pdnType=IPv4v6 cs1Label=Rule Set Name cs2Label=Rule Name
c6a2Label=Source IPv6 Address c6a3Label=Dest IPv6 Address

Syslog 819 LOCAL7.DEBUG:  Nov 27 02:09:08 2019 vThunder
CEF:0|A10|ADC|5.1.0|FW 101|Session closed|1|proto=UDP act=Permit rt=135133
c6a2=2405:200:331:3::10 c6a3=2405:200:331:9::20
deviceInboundInterface=ethernet1 deviceOutboundInterface=ethernet2 cs1=fw
cs2=gtp_c_v2_v1_ipv6 suid=10001 duid=10003 dhost=a10net.mnc872.mcc405.gprs
deviceExternalId=405872000010045 selectionMode=MS or Network provided APN,
subscription verified msisdn=917011014337 imei=3576900603487001
**```mcc=405 mnc=872```** userLocation=1804257899990425780027OF10
ratType=EUTRAN pdnType=IPv4v6 cs3=Admin initiated in=255 out=357 cn1=1
cn2=1 cn3=42 cs1Label=Rule Set Name cs2Label=Rule Name cs3Label=Reason
cn1Label=Packets TX cn2Label=Packets RX cn3Label=Session Duration Seconds
c6a2Label=Source IPv6 Address c6a3Label=Dest IPv6 Address
```

This section shows the information that is generated in the following logs:

- CEF Session Open Log
- CEF Session Close Log
- CEF Log Labels
- ASCII Session Open Log

- ASCII Session Close Log
- Deny Logs

CEF Session Open Log

Table 13 lists the information generated in the CEF Session Open log.

Table 13 : CEF Session Open Log Information

Field	Example	Comment
Severity	AUTHPRIV.WARNING	Severity of the log
Time Stamp	4/17/2019 0:46	Log generation time stamp
Device Name	ACOS DEVICE	Name of GTP Firewall
Code/Log Type	CEF:0	A10
proto	UDP	Protocol
act	Permit	Action taken by firewall
rt	808937	Receipt time of the packet
src	5.5.5.100	Source IP of the packet
spt	34273	Source Port of the packet
dst	6.6.6.100	Dest IP of the packet
dpt	2123	Dest Port of the packet
deviceInboundInterface	ve801	Interface of the incoming packet
deviceOutboundInterface	ve701	Interface of the outgoing packet
cs1	fw	Name of the rule-set
cs2	gtp	Rule Name
cs6	p1	L3V partition Name
message	Create PDP Context Request	GTP Message received
suid	854600697	Source TEID Received in the packet
cs1Label	Rule Set Name	Explanation for label cs1

Table 13 : CEF Session Open Log Information

Field	Example	Comment
cs2Label	Rule Name	Explanation for label cs2
cs6Label	Partition Name	Explanation for label cs6

CEF Session Close Log

Table 14 lists the information generated in the CEF Session Close log.

Table 14 : CEF Session Close Log Information

Field	Example	Comment
Severity	AUTHPRIV.WARNING	Severity of the log
Time Stamp	4/17/2019 0:46	Log generation time stamp
Device Name	ACOS DEVICE	Name of GTP Firewall
Code/Log Type	CEF:0	A10
proto	UDP	Protocol
act	Permit	Action taken by firewall
rt	808937	Receipt time of the packet
src	5.5.5.100	Source IP of the packet
spt	34273	Source Port of the packet
dst	6.6.6.100	Dest IP of the packet
dpt	2123	Dest Port of the packet
deviceInboundInterface	ve801	Interface of the incoming packet
deviceOutboundInterface	ve701	Interface of the outgoing packet
cs1	fw	Name of the rule-set
cs2	gtp	Rule Name

Table 14 : CEF Session Close Log Information

Field	Example	Comment
cs6	p1	L3V partition Name
message	Create PDP Context Request	GTP Message received
suid	854600697	Source TEID Received in the packet
duid	0	Dest TEID Received in the packet
dhost	eetest	APN Received in the packet
deviceExternalId	33333333333333	IMSI received in the packet
cs3	MS provided APN, subscription not verified	Selection Mode in the packet
msisdn	86152210001017	MSISDN in the packet
cs3	Admin initiated	Reason for log generation
in	0	Incoming bytes
out	187	Outgoing bytes
cn1	1	Packets transmitted
cn2	0	Packets received
cn3	11	Duration of the session
cs1Label	Rule Set Name	Explanation for label cs1
cs2Label	Rule Name	Explanation for label cs2
cs3Label	Reason	Explanation for cs3
cn1Label	Packets	TX Explanation for cn1
cn2Label	Packets	RX Explanation for cn2
cs6Label	Partition Name	Explanation for label cs6

CEF Log Labels

Table 15 lists the CEF Labels used for the GTP CEF logs.

Table 15 : CEF Log Labels

CEF Key Name	Full Name	Data Type	Length	Description
msisdn	Mobile Station International Subscriber Directory Number	String	15	Mobile phone number of the subscriber.
imei	International Mobile Equipment Identitiy	String	16	Unique ID for the device.
mcc	Mobile Country Code	String	3	Serving Node geographical code.
mnc	Mobile Network Code	String	3	Serving Node telecom network code.
ratType	Radio Access Technology	String		Subscriber Radio Access Technology type.
pdnType	Packet Data Network Type	String		Type of the network that the packet is going through.
userLocation	User Location Information	String	50	User location obtained from the packet.
bearerID	EPS Bearer ID	Number		GTP-U bearer ID from GTP-C.
QoSclassIdentifier	QoS or traffic class ID	Number		QoS specified by the bearer.

ASCII Session Open Log

Table 16 lists the information generated in the ASCII Session Open log.

Table 16 : ASCII Session Open Log Information

Field	Example	Comment
Severity	AUTHPRIV.WARNING	Severity of the log
Time Stamp	4/17/2019 0:46	Log generation time stamp
Device Name	ACOS DEVICE	Name of GTP Firewall
Log Code	FW-UDP-G	Code for the log generated
Source IP	5.5.5.100	Source IP of the packet
Dest IP	6.6.6.100	Destination IP of the packet
ACT	PERMIT	Action taken by firewall
RT	921480	Receipt time of the packet
IN-INTF	ve801	Interface of the incoming packet
OUT-INTF	ve701	Interface of the outgoing packet
POLICY	fw	Rule-Set Name
RULE	gtp	Rule Name
GTP-MSG-ID	33	ID of GTP message
S-TEID	10001	Source TEID received in the packet
D-TEID	10003	Dest TEID received in the packet
APN	a10net.mnc872.mcc405.gprs	APN received in the packet
IMSI	405872000010045	IMSI received in the packet
SEL-MOD	MS or Network provided APN	Selection Mode in the packet
MSISDN	917011014337	MSISDN in the packet
IMEI	3576900603487001	Unique ID for the device.
MCC	405	MCC received in the packet
MNC	405	Serving Node telecom network code.
User Location	18042578999904257800270F10	User location obtained from the packet.
RAT-TYPE	EUTRAN	Subscriber Radio Access Technology type.

Table 16 : ASCII Session Open Log Information

Field	Example	Comment
PDN-TYPE	IPv4v6\r\n	Type of the network that the packet is going through.

ASCII Session Close Log

Table 17 lists the information generated in the ASCII Session Open log.

Table 17 : ASCII Session Close Log Information

Field	Example	Comment
Severity	AUTHPRIV.WARNING	Severity of the log
Time Stamp	4/17/2019 0:46	Log generation time stamp
Device Name	ACOS DEVICE	Name of GTP Firewall
Log Code	FW-UDP-G	Code for the log generated
Source IP	5.5.5.100	Source IP of the packet
Dest IP	6.6.6.100	Destination IP of the packet
ACT	PERMIT	Action taken by firewall
RT	921480	Receipt time of the packet
IN-INTF	ve801	Interface of the incoming packet
OUT-INTF	ve701	Interface of the outgoing packet
POLICY	fw	Rule-Set Name
RULE	gtp	Rule Name
S-TEID	854600697	Source TEID received in the packet
D-TEID	0	Dest TEID received in the packet
APN	eetest	APN received in the packet
IMSI	333333333333333	IMSI received in the packet

Table 17 : ASCII Session Close Log Information

Field	Example	Comment
SEL-MOD	MS provided APN, subscription not verified	Selection Mode in the packet
MSISDN	86152210001017	MSISDN in the packet
FWD_ BYTES	187	Outgoing bytes
REV_BYTES	0	Incoming bytes
FWD_PKTS	1	Packets transmitted
REV_PKTS	0	Packets received
DUR	22	Duration of the session

Deny Logs

Table 18 lists the information generated in the ASCII Deny Log.

Table 18 : ASCII Deny Log Information

Field	Example	Comment
Severity	AUTHPRIV.WARNING	Severity of the log
Time Stamp	4/17/2019 0:46	Log generation time stamp
Device Name	ACOS DEVICE	Name of GTP Firewall
Log Code	FW-UDP-I	Code for the log generated
Source IP	5.5.5.100	Source IP of the packet
Source Port	34273	Source Port of the packet
Dest IP	6.6.6.100	Destination IP of the packet
Dest Port	2123	Destination Port of the packet
ACT	DENY	Action taken by firewall
RT	921480	Receipt time of the packet
IN-INTF	ve801	Interface of the incoming

Table 18 : ASCII Deny Log Information

Field	Example	Comment
		packet
POLICY	fw	Rule-Set Name
RULE	gtp	Rule Name
GTP-VER	v2	GTP Version in the packet
GTP-MSG	32	GTP Message ID
S-TEID	854600697	Source TEID received in the packet
APN	eetest	APN received in the packet
IMSI	333333333333333	IMSI received in the packet
SEL-MOD	MS provided APN, subscription not verified	Selection Mode in the packet
MSISDN	86152210001017	MSISDN in the packet

Table 19 lists the information generated in the CEF Deny Log.

Table 19 : CEF Deny Log Information

Field	Example	Comment
Severity	AUTHPRIV.WARNING	Severity of the log
Time Stamp	4/17/2019 0:46	Log generation time stamp
Device Name	ACOS DEVICE	Name of GTP Firewall
Code/Log Type	CEF:0	A10
proto	UDP	Protocol
act	Deny	Action taken by firewall
rt	808937	Receipt time of the packet
src	5.5.5.100	Source IP of the packet
spt	34273	Source Port of the packet

Table 19 : CEF Deny Log Information

Field	Example	Comment
dst	6.6.6.100	Dest IP of the packet
dpt	2123	Dest Port of the packet
deviceInboundInterface	ve801	Interface of the incoming packet
cs1	fw	Name of the rule-set
cs2	gtp	Rule Name
cs3	MS provided APN, subscription not verified	Selection Mode in the packet
c6a2	Source	Source IP address
c6a3	Destination	Destination IP address
message	Create Session Request	GTP Message received
suid	854600697	Source TEID Received in the packet
dhost	eetest	APN Received in the packet
deviceExternalId	33333333333333	IMSI received in the packet
imei	576900603487001	IMEI received in the packet
msisdn	86152210001017	MSISDN in the packet
mcc	405	MCC in the packet
mnc	287	MNC in the packet
ratType	EUTRAN	Name of the RAT type
pdnType	IPv4v6	Name of the PDN type
reason	GTP message APN filter match	Reason for GTP deny
cs1Label	Rule Set Name	Explanation for label cs1
cs2Label	Rule Name	Explanation for label

Table 19 : CEF Deny Log Information

Field	Example	Comment
		cs2
cs3Label	Reason	Explanation for cs3
cs6Label	Partition Name	Explanation for label cs6

All deny logs follow a consistent format with a different reason code to identify the trigger for the drop. The following displays the log information shown in the respective event:

- Message Filtering
- Information Element Filtering Drop
- Invalid TEID Drop
- Reserved Information Element Present Drop
- Mandatory Information Element Missing Drop
- Anomaly Drop
- MSISDN Filtering
- Out of Order Information Element Filtering
- Out of State Information Element Filtering
- Rate Limit Periodic
- End User IP Spoofed
- Cross Layer Correlation
- RAT Type Filtering
- Out of State Message
- Maximum Message Length Filtering
- Country Code Validation in IMSI and MSISDN

Message Filtering

Type of the message dropped by the firewall is logged using the following CEF format:

```
Syslog 331 LOCAL0.INFO:  Mar 24 07:57:03 2018 <ACOS Device>
CEF:0|A10|ADC|4.1.4||FW 104|GTP Message Filtering|5|proto=UDP act=Deny
rt=4305091 src=20.20.20.1 spt=2123 dst=30.30.30.1 dpt=2123
deviceInboundInterface=ve55 cs1=gtp cs2=gtpv2 message=Create Session
Request suid=0 cs1Label=Rule Set Name cs2Label=Rule Name
```

The following table describes each field in the log.

Table 20 : Message Type log field descriptions

Field	Description
Syslog 331	Protocol and size of this log.
LOCAL0.INFO: Mar 24 07:57:03 2018	Timestamp of when this log was created. It uses the month/date/time (hours:minutes:seconds)/year format.
ACOS DEVICE CEF:	Device type and version.
GTP Message Filtering |5|proto=UDP	Log type and protocol.
act=Deny	Associated GTP Firewall activity for the packet. The valid activities are Deny and Permit.
rt=4305091	Round trip time in milliseconds. This is the time it takes for a request to travel from the source to its destination, added to the time for the response to travel back to the source.
src=20.20.20.1	Source IP address.
spt=2123	Source port number.
dst=30.30.30.1	Destination IP address.
dpt=2123	Destination post number.
deviceInboundInterface=ve55	The device used to monitor inbound traffic.
cs1=gtp	Name of the cs1 field.
cs2=gtpv2	Name of the cs2 field.
message=Create Session	Message type being logged. The valid message types are: Create session Delete session

Table 20 : Message Type log field descriptions

Field	Description
Request suid=0	Unique identifier of the request.
cs1Label=Rule Set Name	Label name of the cs1 field.
cs2Label=Rule Name	Label name of the cs2 field.

Information Element Filtering Drop

The APN, IMSI, and Selection Mode information can be logged when the packet is dropped by the Information Element Filtering function. The following example log uses the CEF format:

```
Syslog 484 LOCAL0.INFO:  Mar 24 08:04:40 2018 <ACOS Device>
CEF:0|A10|ADC|4.1.4|FW 106|GTP Information Element Filtering|5|proto=UDP
act=Deny rt=4419397 src=20.20.20.1 spt=2123 dst=30.30.30.1 dpt=2123
deviceInboundInterface=ve55 cs1=gtp cs2=gtpv2 message=Create Session
Request suid=52800033 dhost=apn-1.ixiacom.com cs3=MS or Network provided
APN, subscription verified deviceExternalId=226041000000001 cs1Label=Rule
Set Name cs2Label=Rule Name cs3Label=Selection Mode
```

The following table describes each field in the log.

Table 21 : GTP IE Filtering log field descriptions

Field	Description
Syslog 484	Protocol and size of this log.
LOCAL0.INFO: Mar 24 08:04:40 2018	Timestamp of when this log was created. It uses the month/date/time (hours:minutes:seconds)/year format.
ACOS DEVICE CEF:	Device type and version.
GTP Information Element Filtering|5|proto=UDP	Log type and protocol.
act=Deny	Associated GTP Firewall activity for the packet. The valid activities are Deny and Permit.
rt=4419397	Round trip time in milliseconds. This is the time it takes for a request to travel from the source to its destination, added to the time

Table 21 : GTP IE Filtering log field descriptions

Field	Description
	for the response to travel back to the source.
src=20.20.20.1	Source IP address.
spt=2123	Source port number.
dst=30.30.30.1	Destination IP address.
dpt=2123	Destination post number.
deviceInboundInterface=ve55	The device used to monitor inbound traffic.
cs1=gtp	Name of the cs1 field.
cs2=gtpv2	Name of the cs2 field.
message=Create Session Request	Message type being logged. The valid message types are: Create session request Create session response Delete session request Delete session response
Session Request suid=0	Unique identifier of the session request.
dhost=apn-1.ixiacom.com	Destination host type and domain.
cs3=MS or Network provided APN	Selection mode or APN of the cs3 field.
subscription verified	Specifies whether the subscription is valid.
deviceExternalId=226041000000001	Identifier of the external device.
cs1Label=Rule Set Name	Label name of the cs1 field.
`cs2Label=Rule Name`	Label name of the cs2 field.
`cs3Label=Selection Mode`	Label name of the cs3 field.

The following example log uses the CEF format:

```
Syslog 484 LOCAL0.INFO:  Mar 24 08:04:40 2018 <ACOS Device>
CEF:0|A10|ADC|4.1.4|FW 106|GTP Information Element Filtering|5|proto=UDP
act=Deny rt=4419397 src=20.20.20.1 spt=2123 dst=30.30.30.1 dpt=2123
deviceInboundInterface=ve55 cs1=gtp cs2=gtpv2 message=Create Session
Request suid=52800033 dhost=apn-1.ixiacom.com cs3=MS or Network provided
APN, subscription verified deviceExternalId=226041000000001 cs1Label=Rule
Set Name cs2Label=Rule Name cs3Label=Selection Mode
```

Invalid TEID Drop

The following example log uses the CEF format:

```
Syslog 519 LOCAL0.INFO: Jun 13 19:21:59 2018 <ACOS Device>
CEF:0|A10|ADC|4.1.4-P2|FW 104|GTP Deny Log|5|proto=UDP act=Deny rt=127907
src=5.5.5.100 spt=2123 dst=6.6.6.100 dpt=2123 deviceInboundInterface=ve801
cs1=gtp cs2=1 message=Create Session Request suid=106
dhost=aaacom.com.mnc000.mcc000.gprs cs3=MS or Network provided APN,
subscription verified deviceExternalId=333333333333333
imei=999900000000010 rat-type=EUTRAN mcc=333 mnc=333 pdn-type=IPv4
reason=Invalid Tunnel Endpoint Identifier Drop cs1Label=Rule Set Name
cs2Label=Rule Name cs3Label=Selection Mode
```

The following example log uses the ASCII format:

```
Syslog 366 AUTHPRIV.WARNING: Dec 27 10:09:37.11 <ACOS Device> FW-UDP-I:
5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=14320524 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-MSG=Create Session Request SUID=106
DHOST=aaacom.com.mnc000.mcc000.gprs SEL-MOD=MS or Network provided APN,
subscription verified IMSI=333333333333333 IMEI=999900000000010  RAT-
TYPE=EUTRAN MCC=333 MNC=333 PDN-TYPE=IPv4 REASON=Invalid Tunnel Endpoint
Identifier Drop\r\n
```

Reserved Information Element Present Drop

The following example log uses the CEF format:

```
Syslog 705 LOCAL7.DEBUG:  Aug 26 21:57:20 2019 vThunder
CEF:0|A10|ADC|5.0.0-P1-GPT|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=118467 c6a2=2405:200:331:3::10 spt=2123 c6a3=2405:200:331:9::20
dpt=2123 deviceInboundInterface=ethernet1 cs1=fw cs2=gtp_c_v2_v1_ipv6
message=Create Session Request suid=10001 dhost=a10net.mnc872.mcc405.gprs
cs3=MS or Network provided APN, subscription verified msisdn=917011014337
imei=3576900603487001 mcc=405 mnc=287 ratType=EUTRAN pdnType=IPv4v6
userLocation=18042578999904257800270F10 reason=GTP message with invalid
IE, First Reserved IE found is 32 cs1Label=Rule Set Name cs2Label=Rule
Name c6a2Label=Source IPv6 Address c6a3Label=Dest IPv6 Address
```

The following example log uses the ASCII format:

```
Syslog 366 AUTHPRIV.WARNING: Dec 27 10:09:37.11 <ACOS Device> FW-UDP-I:
5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=14320524 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-MSG=Create Session Request SUID=106
DHOST=aaacom.com.mnc000.mcc000.gprs SEL-MOD=MS or Network provided APN,
subscription verified IMSI=333333333333333 IMEI=999900000000010  RAT-
TYPE=EUTRAN MCC=333 MNC=333 PDN-TYPE=IPv4 REASON=Reserved Information
Element Present\r\n
```

Mandatory Information Element Missing Drop

The following example log uses the CEF format:

```
Syslog 543 LOCAL0.INFO: Jun 13 19:21:59 2018 <ACOS Device>
CEF:0|A10|ADC|4.1.4-P2|FW 104|GTP Deny Log|5|proto=UDP act=Deny rt=127907
src=5.5.5.100 spt=2123 dst=6.6.6.100 dpt=2123 deviceInboundInterface=ve801
cs1=gtp cs2=1 message=Create Session Request suid=106
dhost=aaacom.com.mnc000.mcc000.gprs cs3=MS or Network provided APN,
subscription verified deviceExternalId=333333333333333
imei=999900000000010 rat-type=EUTRAN mcc=333 mnc=333 pdn-type=IPv4
reason=GTP message with missing mandatory IE, QoS Profile cs1Label=Rule
Set Name
```

The following example log uses the ASCII format:

```
Syslog 366 AUTHPRIV.WARNING: Dec 27 10:09:37.11 <ACOS Device> FW-UDP-I:
5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=14320524 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-MSG=Create Session Request SUID=106
DHOST=aaacom.com.mnc000.mcc000.gprs SEL-MOD=MS or Network provided APN,
subscription verified IMSI=333333333333333 IMEI=999900000000010  RAT-
TYPE=EUTRAN MCC=333 MNC=333 PDN-TYPE=IPv4 REASON= GTP message with missing
mandatory IE, QoS Profile \r\n
```

Anomaly Drop

The following example log uses the CEF format:

```
Syslog 501 AUTHPRIV.WARNING:  Jan  3 14:32:23 2019 <ACOS Device>
CEF:0|A10|ADC|4.1.4-GR1|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=2190511 src=5.5.5.100 spt=2123 dst=6.6.6.100 dpt=2123
deviceInboundInterface=ve801 cs1=fw cs2=gtp message=Create Session Request
suid=106 dhost=aaacom.com.mnc000.mcc000.gprs cs3=MS or Network provided
APN, subscription verified deviceExternalId=333333333333333
imei=999900000000010 rat-type=EUTRAN mcc=333 mnc=333 pdn-type=IPv4 reason=
GTP in GTP Filtering Drop cs1Label=Rule Set Name cs2Label=Rule Name
cs3Label=Selection Mode
```

The following example log uses the ASCII format:

```
Syslog 366 AUTHPRIV.WARNING: Dec 27 10:09:37.11 <ACOS Device> FW-UDP-I:
5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=14320524 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-MSG=Create Session Request SUID=106
DHOST=aaacom.com.mnc000.mcc000.gprs SEL-MOD=MS or Network provided APN,
subscription verified IMSI=333333333333333 imei=999900000000010 rat-
type=EUTRAN mcc=333 mnc=333 pdn-type=IPv4 REASON=GTP in GTP Filtering
Drop\r\n
```

MSISDN Filtering

The following example log uses the CEF format:

```
Syslog 532 AUTHPRIV.WARNING:  Apr  7 02:10:08 2019 <ACOS Device>
CEF:0|A10|ADC|4.1.4-GR1-P1|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=1319553 src=5.5.5.100 spt=2123 dst=6.6.6.100 dpt=2123
deviceInboundInterface=ve801 cs1=fw cs2=gtp message=Create Session Request
suid=106 dhost=aaacom.com.mnc000.mcc000.gprs cs3=MS or Network provided
APN, subscription verified deviceExternalId=333333333333333
msisdn=311280001001053 imei=999900000000010 rat-type=EUTRAN mcc=333
mnc=333 pdn-type=IPv4 reason=GTP message MSISDN filter match cs1Label=Rule
Set Name cs2Label=Rule Name cs3Label=Selection Mode
```

The following example log uses the ASCII format:

```
Syslog 366 AUTHPRIV.WARNING: Dec 27 10:09:37.11 <ACOS Device> FW-UDP-I:
5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=14320524 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-MSG=Create Session Request SUID=106
DHOST=aaacom.com.mnc000.mcc000.gprs SEL-MOD=MS or Network provided APN,
subscription verified IMSI=333333333333333 IMEI=999900000000010  RAT-
TYPE=EUTRAN MCC=333 MNC=333 PDN-TYPE=IPv4 REASON=GTP Message MSISDN filter
match\r\n
```

Out of Order Information Element Filtering

The following example log uses the CEF format:

```
Syslog 562 LOCAL7.DEBUG:  Aug 26 21:28:57 2019 vThunder
CEF:0|A10|ADC|5.0.0-P1-GPT|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=262645 src=100.100.100.10 spt=2123 dst=200.200.200.10 dpt=2123
deviceInboundInterface=ethernet1 cs1=fw cs2=gtp_c_v2_v1_ipv4
message=Create PDP Context Request suid=1 dhost=ssenoauth146 cs3=MS or
Network provided APN, subscription verified
deviceExternalId=50502410121507 msisdn=1917962480141 mcc=111 mnc=222
reason=GTP message with out of order IE, Traffic Flow Template
cs1Label=Rule Set Name cs2Label=Rule Name
```

The following example log uses the ASCII format:

```
100    Syslog 390 AUTHPRIV.WARNING:  Apr  7 02:30:05 <ACOS Device> FW-UDP-
I: 5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=921862 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-VER=v1 GTP-MSG-ID=16 S-TEID=1 DHOST=senoauth146\204
SEL-MOD=MS or Network provided APN, subscription verified IMSI=10121507
MSISDN=1796248014100 IMEI=999900000000010  RAT-TYPE=EUTRAN MCC=333 MNC=333
PDN-TYPE=IPv4 REASON=GTP message with out of order IE, NSAPI\r\n
```

Out of State Information Element Filtering

The following example log uses the CEF format:

```
Syslog 713 LOCAL7.DEBUG:  Aug 26 21:30:03 2019 vThunder
CEF:0|A10|ADC|5.0.0-P1-GPT|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=279154 c6a2=2405:200:331:3::10 spt=2123 c6a3=2405:200:331:9::20
dpt=2123 deviceInboundInterface=ethernet1 cs1=fw cs2=gtp_c_v2_v1_ipv6
message=Create Session Request suid=10001 dhost=a10net.mnc872.mcc405.gprs
cs3=MS or Network provided APN, subscription verified msisdn=917011014337
imei=3576900603487001 mcc=405 mnc=287 ratType=EUTRAN pdnType=IPv4v6
userLocation=18042578999904257800270F10 reason=GTP message with out of
state IE, First Out of State IE found is 2 cs1Label=Rule Set Name
cs2Label=Rule Name c6a2Label=Source IPv6 Address c6a3Label=Dest IPv6
Address
```

The following example log uses the ASCII format:

```
100    Syslog 390 AUTHPRIV.WARNING:  Apr  7 02:30:05 <ACOS Device> FW-UDP-
I: 5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=921862 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-VER=v1 GTP-MSG-ID=16 S-TEID=1 DHOST=senoauth146\204
SEL-MOD=MS or Network provided APN, subscription verified IMSI=10121507
MSISDN=1796248014100 IMEI=999900000000010  RAT-TYPE=EUTRAN MCC=333 MNC=333
PDN-TYPE=IPv4 REASON=GTP message with out of state IE\r\n
```

Rate Limit Periodic

The following example log uses the CEF format:

```
Syslog LOCAL0.INFO:  Dec 29 10:34:26 2020 <ACOS Device>
CEF:0|A10|CFW|5.2.1-P1-GTP|FW 134|GTP Rate Limit Periodic|5| cs1=5.5.5.100
cs1Label=Key cs2=Network-Element cs2Label=Key Type cs3=GTPv2-C Aggregated
Message Drops cs3Label=Metric cn1=948 cn1Label=Metric Value cs4=L3V
cs4Label=Partition Name
```

The following example log uses the ASCII format:

```
Syslog LOCAL0.INFO:  Dec 25 07:12:08 <ACOS Device> FW-FW 134|GTP Rate
Limit Periodic|5|:  KEY=5.5.5.100 KEY-TYPE=Network-Element METRIC=GTPv2-C
Aggregated Message Drops METRIC-VALUE=6117
```

End User IP Spoofed

The following example log uses the CEF format:

```
Syslog 532 AUTHPRIV.WARNING:  Apr  7 02:10:08 2019 <ACOS Device>
CEF:0|A10|ADC|4.1.4-GR1-P1|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=1319553 src=5.5.5.100 spt=2123 dst=6.6.6.100 dpt=2123
deviceInboundInterface=ve801 cs1=fw cs2=gtp message=Create Session Request
suid=106 dhost=aaacom.com.mnc000.mcc000.gprs cs3=MS or Network provided
APN, subscription verified deviceExternalId=333333333333333
msisdn=311280001001053 imei=999900000000010 rat-type=EUTRAN mcc=333
mnc=333 pdn-type=IPv4 reason=GTP message End User IP Address Spoofed
cs1Label=Rule Set Name cs2Label=Rule Name cs3Label=Selection Mode
```

The following example log uses the ASCII format:

```
Syslog 366 AUTHPRIV.WARNING: Dec 27 10:09:37.11 <ACOS Device> FW-UDP-I:
5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=14320524 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-MSG=Create Session Request SUID=106
DHOST=aaacom.com.mnc000.mcc000.gprs SEL-MOD=MS or Network provided APN,
subscription verified IMSI=333333333333333 IMEI=999900000000010  RAT-
TYPE=EUTRAN MCC=333 MNC=333 PDN-TYPE=IPv4 REASON= GTP message End User IP
Address Spoofed\r\n
```

Cross Layer Correlation

The following example log uses the CEF format:

IPv6 Log

```
Syslog 749 LOCAL7.DEBUG:  Aug 26 21:54:17 2019 vThunder
CEF:0|A10|ADC|5.0.0-P1-GPT|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=72828 c6a2=2405:200:331:3::10 spt=2123 c6a3=2405:200:331:9::20 dpt=2123
deviceInboundInterface=ethernet1 cs1=fw cs2=gtp_c_v2_v1_ipv6
message=Create Session Request suid=10001 dhost=a10net.mnc872.mcc405.gprs
cs3=MS or Network provided APN, subscription verified msisdn=917011014337
imei=3576900603487001 mcc=405 mnc=287 ratType=EUTRAN pdnType=IPv4v6
userLocation=18042578999904257800270F10 reason=IP Layer and GTP Layer IP
Address Mismatch, L3 IP is [2405:200:331:3::10] L5 IP is
[3405:200:331:3::10] cs1Label=Rule Set Name cs2Label=Rule Name
c6a2Label=Source IPv6 Address c6a3Label=Dest IPv6 Address
```

IPv4 Log

```
Syslog 591 LOCAL7.DEBUG:  Aug 26 21:22:48 2019 vThunder
CEF:0|A10|ADC|5.0.0-P1-GPT|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=172456 src=100.100.100.10 spt=2123 dst=200.200.200.10 dpt=2123
deviceInboundInterface=ethernet1 cs1=fw cs2=gtp_c_v2_v1_ipv4
message=Create PDP Context Request suid=1 dhost=ssenoauth146 cs3=MS or
Network provided APN, subscription verified
deviceExternalId=50502410121507 msisdn=1917962480141 mcc=111 mnc=222
reason=IP Layer and GTP Layer IP Address Mismatch, L3 IP is 100.100.100.10
L5 IP is 1.1.5.1 cs1Label=Rule Set Name cs2Label=Rule Name
```

The following example log uses the ASCII format:

```
Syslog 366 AUTHPRIV.WARNING: Dec 27 10:09:37.11 <ACOS Device> FW-UDP-I:
5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=14320524 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-MSG=Create Session Request SUID=106
DHOST=aaacom.com.mnc000.mcc000.gprs SEL-MOD=MS or Network provided APN,
subscription verified IMSI=333333333333333 IMEI=999900000000010  RAT-
TYPE=EUTRAN MCC=333 MNC=333 PDN-TYPE=IPv4 REASON= IP Layer and GTP Layer
IP Address Mismatch \r\n
```

RAT Type Filtering

The following example log uses the CEF format:

```
Syslog 543 AUTHPRIV.WARNING:  Apr  7 02:30:20 2019 <ACOS Device>
CEF:0|A10|ADC|4.1.4-GR1-P1|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=977652 src=5.5.5.100 spt=2123 dst=6.6.6.100 dpt=2123
deviceInboundInterface=ve801 cs1=fw cs2=gtp message=Create PDP Context
Request suid=1 dhost=senoauth146\204 cs3=MS or Network provided APN,
subscription verified deviceExternalId=10121507 msisdn=1796248014100
imei=999900000000010 rat-type=EUTRAN mcc=333 mnc=333 pdn-type=IPv4 reason=
GTP Message with disallowed RAT Type match cs1Label=Rule Set Name
cs2Label=Rule Name
```

The following example log uses the ASCII format:

```
100    Syslog 390 AUTHPRIV.WARNING:  Apr  7 02:30:05 <ACOS Device> FW-UDP-
I: 5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=921862 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-VER=v1 GTP-MSG-ID=16 S-TEID=1 DHOST=senoauth146\204
SEL-MOD=MS or Network provided APN, subscription verified IMSI=10121507
MSISDN=1796248014100 IMEI=999900000000010  RAT-TYPE=EUTRAN MCC=333 MNC=333
PDN-TYPE=IPv4 REASON= GTP Message with disallowed RAT Type match \r\n
```

Out of State Message

The following example log uses the CEF format:

```
Syslog 532 AUTHPRIV.WARNING:  Apr  7 02:10:08 2019 <ACOS Device>
CEF:0|A10|ADC|4.1.4-GR1-P1|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=1319553 src=5.5.5.100 spt=2123 dst=6.6.6.100 dpt=2123
deviceInboundInterface=ve801 cs1=fw cs2=gtp message=Create Session Request
suid=106 dhost=aaacom.com.mnc000.mcc000.gprs cs3=MS or Network provided
APN, subscription verified deviceExternalId=333333333333333
msisdn=311280001001053 imei=999900000000010 rat-type=EUTRAN mcc=333
mnc=333 pdn-type=IPv4 reason=GTP Out of State Message cs1Label=Rule Set
Name cs2Label=Rule Name cs3Label=Selection Mode
```

The following example log uses the ASCII format:

```
Syslog 366 AUTHPRIV.WARNING: Dec 27 10:09:37.11 <ACOS Device> FW-UDP-I:
5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=14320524 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-MSG=Create Session Request SUID=106
DHOST=aaacom.com.mnc000.mcc000.gprs SEL-MOD=MS or Network provided APN,
subscription verified IMSI=333333333333333 IMEI=999900000000010  RAT-
TYPE=EUTRAN MCC=333 MNC=333 PDN-TYPE=IPv4 REASON= GTP Out of State Message
\r\n
```

Maximum Message Length Filtering

The following example log uses the CEF format:

```
Syslog 495 LOCAL7.DEBUG:  Aug 26 21:58:25 2019 vThunder
CEF:0|A10|ADC|5.0.0-P1-GPT|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=134851 c6a2=2405:200:331:3::10 spt=2123 c6a3=2405:200:331:9::20
dpt=2123 deviceInboundInterface=ethernet1 cs1=fw cs2=gtp_c_v2_v1_ipv6
message=Create Session Request suid=0 reason=GTP Maximum Message Length
Exceeded Drop, Length of message is 291 cs1Label=Rule Set Name
cs2Label=Rule Name c6a2Label=Source IPv6 Address c6a3Label=Dest IPv6
Address
```

The following example log uses the ASCII format:

```
Syslog 366 AUTHPRIV.WARNING: Dec 27 10:09:37.11 <ACOS Device> FW-UDP-I:
5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=14320524 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-MSG=Create Session Request SUID=106
DHOST=aaacom.com.mnc000.mcc000.gprs SEL-MOD=MS or Network provided APN,
subscription verified IMSI=333333333333333 imei=999900000000010 rat-
type=EUTRAN mcc=333 mnc=333 pdn-type=IPv4 REASON= GTP message maximum
length exceeded \r\n
```

Country Code Validation in IMSI and MSISDN

The following example log uses the CEF format:

```
Syslog 532 AUTHPRIV.WARNING:  Apr  7 02:10:08 2019 <ACOS Device>
CEF:0|A10|ADC|4.1.4-GR1-P1|FW 104|GTP Deny Log|5|proto=UDP act=Deny
rt=1319553 src=5.5.5.100 spt=2123 dst=6.6.6.100 dpt=2123
deviceInboundInterface=ve801 cs1=fw cs2=gtp message=Create Session Request
suid=106 dhost=aaacom.com.mnc000.mcc000.gprs cs3=MS or Network provided
APN, subscription verified deviceExternalId=333333333333333
msisdn=311280001001053 imei=9999000000000010 rat-type=EUTRAN mcc=333
mnc=333 pdn-type=IPv4 reason= GTP message with mismatched Country Codes in
MSISDN and IMSI cs1Label=Rule Set Name cs2Label=Rule Name
cs3Label=Selection Mode
```

The following example log uses the ASCII format:

```
Syslog 366 AUTHPRIV.WARNING: Dec 27 10:09:37.11 <ACOS Device> FW-UDP-I:
5.5.5.100:2123<-->6.6.6.100:2123 ACT=DENY RT=14320524 IN-INTF=ve801
POLICY=fw RULE=gtp GTP-MSG=Create Session Request SUID=106
DHOST=aaacom.com.mnc000.mcc000.gprs SEL-MOD=MS or Network provided APN,
subscription verified IMSI=333333333333333 IMEI=9999000000000010  RAT-
TYPE=EUTRAN MCC=333 MNC=333 PDN-TYPE=IPv4 REASON=GTP message with
mismatched Country Codes in MSISDN and IMSI\r\n
```

IPFIX

Table 22 lists the following supported IPFIX events:

Table 22 : Supported IPFIX Events

Field	Description
GTP-C Tunnel Event	A log sent when a GTP-C tunnel is created or deleted
GTP-U Tunnel Event	A log sent when a GTP-U tunnel is created or deleted.
GTP Deny Event	A log sent when the packet is denied by GTP Firewall.
GTP Info Event	A log sent when a node restart message occurs. This requires that the records pertaining to that node be cleared.

Table 23 lists the following supported IPFIX information elements:

Table 23 : Supported IPFIX Information Elements

Field	Description
flow-end-reason	Number that indicates the reason for closing the connection and clearing it. Maximum size is 1 byte. The following A10 flow end reasons are displayed for CEF and IPFIX: 0x0 - Unknown 0x01 - TCP FIN send by FWD side 0x02 - DNS Response 0x03 - Radius Stop Message 0x04 - TCP FIN send by rev side 0x05 - TCP RST send by FWD side 0x06 - TCP RST send by REV side 0x07 - TCP RST send by Thunder 0x11 - Idle Timeout 0x12 - Fast Aging 0x21 - Admin Issued Clear Session 0x22 - Config Change 0x31 - DDoS 0x41 - GTP Delete Request Received 0x42 - GTP Handover Request Received 0x43 - GTP Path or Node Failure Detected 0x44 - GTP Control Session Deleted 0x45 - GTP Create Session Retransmitted
gtp-deny-reason	String that is used when GTP FW denies a certain packet.

Table 23 : Supported IPFIX Information Elements

Field	Description
	Maximum size is 100 bytes.
gtp-apn	String that specifies the APN retrieved from the GTP-C packet. Maximum size is 100 bytes.
gtp-steid	Number that indicates the source tunnel ID of a GTP Tunnel. Size is 4 bytes.
gtp-dteid	Number that indicates the destination tunnel ID of a GTP Tunnel. Size is 4 bytes.
gtp-selection-mode	String that indicates the selection-mode found in the GTP-C packet. Maximum size is 50 bytes.
gtp-mcc	Mobile Country Code derived from the Serving Network IE in the GTP-C packet. Size is 3 bytes.
gtp-mnc	Mobile Network Code derived from the Serving Network IE in the GTP-C packet. Size is 3 bytes.
gtp-rat-type	Radio Access Type string found in the GTP-C packet. Size is 6 bytes.
gtp-pdn-pdp-type	PDN/PDP type that gets extracted from the GTP-C packet. Size is 6 bytes.
gtp-uli	User Location Information found from the GTP-C packet. Maximum size is 50 bytes.
gtp-enduser-v4-addr	IPV4 Address allocated by the PGW in the response packet. Size is 4 bytes.
gtp-enduser-v6-addr	IPV6 Address allocated by the PGW in the response packet. Size is 4 bytes.
gtp-bearer-id-or-nsapi	IPV6 Address allocated by the PGW in the response packet. Size is 16 bytes.
gtp-qci	Bearer ID found in the bearer context IE of GTP-V2 packet and NSAPI of GTP-V1 packet. Size is 1 byte.
gtp-info-event-ind	Qos Profile IE in GTP-V1 and QCI in bearer context IE in GTP-V2. Size is 1 byte.
gtp-restarted-node-ipv4	IPV4 address of the restarted node. Size is 4 bytes.

Table 23 : Supported IPFIX Information Elements

Field	Description
gtp-restarted-node-ipv6	IPV6 address of the restarted node. Size is 16 bytes.
gtp-c-tunnels-removed-with-node-restart	Indicates the number of tunnels removed when a node restart event occurs. Size is 4 bytes.

For IPFIX configuration example, see Configuring NetFlow/IPFIX.

GTP Counters and Statistics

Counters provide information about the tunnel creation and deletion and where the packets are dropped. Counters are maintained at a policy level. Because only one policy is active at a time, the same counters are used for all supported GTP versions.

The show command output is grouped into different categories based on the information the counters display.

The GTP firewall counters can be accessed using the `show counters` command from the command-line interface as described in each of the following sections:

- Use the `show counters fw gtp` command to display the GTP firewall counters:

```
ACOS(config)#show counters fw gtp
Out of Resource Counters
---------------------------------------------
Out of Tunnel Memory
GTP Tunnel Level Rate Limit Entry Create Failure
GTP Rate Limit SMP Create Failure
GTP Rate Limit Dynamic Counters Create Failure
GTP Rate Limit Entry Create Failure

Routing Failure Drop Counters
---------------------------------------------
No Forward Route
No Reverse Route

Echo Counters
```

```
---------------------------------------------
GTP Node Restoration due to Recovery IE in Echo
GTP-C Path Failure due to Echo
GTP Echo Out of State Drop

Retransmit Counters
---------------------------------------------
GTP-C Retransmitted Delete Bearer Request
GTP-C Retransmitted Add Bearer Response


Packet and Byte Counters
---------------------------------------------
GTP-U Out of state Drop
GTP-C Handover Request Out of state Drop
GTPv1-C NSAPI Not Found in GTP Request
GTPv2-C Bearer Not Found in GTP Request
GTPv2-C Bearer Not Found in GTP Response
GTP Message Dropped in RR Mode
GTP Fragmented or JUMBO packet Drop
GTPv0-C Uplink Ingress Packets
GTPv0-C Uplink Egress Packets
GTPv0-C Downlink Ingress Packets
GTPv0-C Downlink Egress Packets
GTPv0-C Uplink Ingress Bytes
GTPv0-C Uplink Egress Bytes
GTPv0-C Downlink Ingress Bytes
GTPv0-C Downlink Egress Bytes
GTPv1-C Uplink Ingress Packets
GTPv1-C Uplink Egress Packets
GTPv1-C Downlink Ingress Packets
GTPv1-C Downlink Egress Packets
GTPv1-C Uplink Ingress Bytes
GTPv1-C Uplink Egress Bytes
GTPv1-C Downlink Ingress Bytes
GTPv1-C Downlink Egress Bytes
GTPv2-C Uplink Ingress Packets
GTPv2-C Uplink Egress Packets
GTPv2-C Downlink Ingress Packets
```

```
GTPv2-C Downlink Egress Packets
GTPv2-C Uplink Ingress Bytes
GTPv2-C Uplink Egress Bytes
GTPv2-C Downlink Ingress Bytes
GTPv2-C Downlink Egress Bytes
GTP-U Uplink Ingress Packets
GTP-U Uplink Egress Packets
GTP-U Downlink Ingress Packets
GTP-U Downlink Egress Packets
GTP-U Uplink Ingress Bytes
GTP-U Uplink Egress Bytes
GTP-U Downlink Ingress Bytes
GTP-U Downlink Egress Bytes
```

Drop Counters

```
---------------------------------------------
GTP-U Message Length Mismatch Across Layers
GTP-Path Message Length Mismatch Across Layers
Missing conditional IE in bearer context Drop
GTP Bearer not found in response
GTP-U Out of state Drop
GTP-C Handover Request Out of state Drop
GTPv1-C NSAPI Not Found in GTP Request
GTPv2-C Bearer Not Found in GTP Request
GTPv2-C Bearer Not Found in GTP Response
GTP Message Dropped in RR Mode
GTP Fragmented or JUMBO packet Drop
```

Inline Deployment Mode Counters

```
---------------------------------------------
GTP Stateless Forward
GTP messages forwarded via monitor mode
```

- Use the `show counters template gtp-policy <policy-name>` command to display the counters at the policy level.

```
ACOS (config)#show counters template gtp-policy <policy-name>
```

Tunnel Counters

```
---------------------------------------------
GTPv0-C Tunnel Created
GTPv0-C Half open tunnel created
GTPv0-C Tunnel Delete Request
GTPv0-C Tunnel Marked Deleted
GTPv0-C Tunnel Deleted
GTPv0-C Half open tunnel closed
GTPv1-C Tunnel Created
GTPv1-C Half open tunnel created
GTPv1-C Tunnel Delete Request
GTPv1-C Tunnel Marked Deleted
GTPv1-C Tunnel Deleted
GTPv1-C Half open tunnel closed
GTPv2-C Tunnel Created
GTPv2-C Half open tunnel created
GTPv2-C Tunnel Delete Request
GTPv2-C Tunnel Marked Deleted
GTPv2-C Tunnel Deleted
GTPv2-C Half open tunnel closed
GTP-U Tunnel Created
GTP-U Tunnel Deleted
GTPv0-C Tunnel Deleted with Restart/failure
GTPv1-C Tunnel Deleted with Restart/failure
GTPv2-C Tunnel Deleted with Restart/failure
```

Information Counters

```
---------------------------------------------
GTPv0-C Update PDP Context Response Unsuccessful
GTPv1-C Update PDP Context Response Unsuccessful
GTPv2-C Modify Bearer Response Unsuccessful
GTPv0-C Create PDP Context Response Unsuccessful
GTPv1-C Create PDP Context Response Unsuccessful
GTPv2-C Create Session Response Unsuccessful
GTPv2-C Piggyback Message
GTP Path Management Messages Received
Permit GTPv0-C Reserved Messages
Permit GTPv1-C Reserved Messages
Permit GTPv2-C Reserved Messages
GTPv2-C Load Control Info IEs in message exceeded 2
```

```
GTPv1-C PDU Notification Request Forward
GTPv1-C PDU Notification Reject Request Forward
GTPv0-C PDU Notification Request Forward
GTPv0-C PDU Notification Reject Request Forward
GTPv0-C APN/IMSI Filtering Skipped (No IMSI)
GTPv1-C APN/IMSI Filtering Skipped (No IMSI)
GTPv2-C APN/IMSI Filtering Skipped (No IMSI)
GTPv0-C MSISDN Filtering Skipped (No MSISDN)
GTPv1-C MSISDN Filtering Skipped (No MSISDN)
GTPv2-C MSISDN Filtering Skipped (No MSISDN)
GTPv0-C Packet With Dummy MSISDN Forwarded
GTPv1-C Packet With Dummy MSISDN Forwarded
GTPv2-C Packet With Dummy MSISDN Forwarded
```

Validation Policy Drop Counters

```
---------------------------------------------
Validation Drop: GTPv2-C Create Session Request with TEID
Validation Drop: GTPv1-C PDU Notification Request with TEID
Validation Drop: GTPv0-C PDU Notification Request with TEID
Validation Drop: GTP repeated IE count exceeded
Validation Drop: Reserved Header Field Set
Validation Drop: Tunnel Header Flag Not Set
Validation Drop: Invalid Flow Label in GTPv0-C Header
Validation Drop: Invalid TEID Value
Validation Drop: Out Of State GTP Message
Validation Drop: Mandatory IE Not Present
Validation Drop: Mandatory IE in Grouped IE Not Present
Validation Drop: GTPv1-C Message Out of Order IE
Validation Drop: Unexpected IE Present in Message
Validation Drop: Reserved IE Field Present
Validation Drop: Invalid GTP version
Validation Drop: Message Length Exceeded
Validation Drop: Cross Layer IP Address Mismatch
Validation Drop: Country Code Mismatch in IMSI and MSISDN
Validation Drop: GTP-U IP Address Spoofed
Validation Drop: GTP Bearer count exceeded max (11)
Validation Drop: GTPV2-C Wrong LBI in Create Bearer Request
Validation Drop: GTP-C Drop Since Handover In Progress
Validation Drop: GTPv0-C Reserved Message Drop
Validation Drop: GTPv1-C Reserved Message Drop
Validation Drop: GTPv2-C Reserved Message Drop
Validation Drop: Piggyback message invalid packet length
Validation Drop: piggyback message anomaly failed
Validation Drop: GTP-C Sequence number Mismatch
Validation Drop: GTPV0 -C conn Sequence number Buffer Full
Validation Drop: GTPV1-C conn Sequence number Buffer Full
Validation Drop: GTPV2-C conn Sequence number Buffer Full
Validation Drop: GTP-C Invalid IMSI Length Drop
Validation Drop: GTP-C Invalid APN Length Drop
Validation Drop: Protocol flag in Header Field not Set
Validation Drop: GTPV0-c Subscriber Attributes Missing
Validation Drop: GTPV1-c Subscriber Attributes Missing
Validation Drop: GTPV2-c Subscriber Attributes Missing
Validation Drop: GTPv0-C APN/IMSI Filtering Dropped (No APN)
Validation Drop: GTPv1-C APN/IMSI Filtering Dropped (No APN)
Validation Drop: GTPv2-C APN/IMSI Filtering Dropped (No APN)
```

Filtering Policy Drop Counters

```
---------------------------------------------
Filtering Drop: Message Type Not Permitted on Interface
Filtering Drop: APN IMSI Filtering
Filtering Drop: MSISDN Filtering
Filtering Drop: RAT Type Filtering
Filtering Drop: GTP in GTP Tunnel Present
```

Rate-limit Policy Drop Counters

```
---------------------------------------------
Rate-limit Drop: Maximum GTPv0-C Message rate
Rate-limit Drop: Maximum GTPv1-C Message rate
Rate-limit Drop: Maximum GTPv2-C Message rate
Rate-limit Drop: GTPv1-C Create PDP Request rate
Rate-limit Drop: GTPv2-C Create Session Request rate
Rate-limit Drop: GTPv1-C Update PDP Request rate
Rate-limit Drop: GTPv2-C Modify Bearer Request rate
Rate-limit Drop: GTP-U Tunnel Creation rate
Rate-limit Drop: GTP-U Uplink byte rate
Rate-limit Drop: GTP-U Uplink packet rate
Rate-limit Drop: GTP-U Downlink byte rate
```

```
Rate-limit Drop: GTP-U Downlink packet rate
Rate-limit Drop: GTP-U Total byte rate
Rate-limit Drop: GTP-U Total packet rate
Rate-limit Drop: GTP-U Concurrent Tunnels

Message Length Drop Counters
---------------------------------------------
GTPv0-C IE Length Exceeds Message Length
GTPv1-C IE Length Exceeds Message Length
GTPv2-C IE Length Exceeds Message Length
GTPv0-C Message Length Mismatch Across Layers
GTPv1-C Message Length Mismatch Across Layers
GTPv2-C Message Length Mismatch Across Layers
```

- Use the `show counters fw logging` command to display the counters for GTP firewall logging.

```
ACOS(config)#show counters fw logging

show counters fw logging
**************************************
Log Packet Sent                                                  0
Log Event Type Reset                                             0
Log Event Type Deny                                              0
Log Event Type Session Close                                     0
Log Event Type Session Open                                      0
Firewall Rule Not Logged                                         0
Log Packets Dropped                                              0
TCP Session Created                                              0
TCP Session Deleted                                              0
UDP Session Created                                              0
UDP Session Deleted                                              0
ICMP Session Deleted                                             0
ICMP Session Created                                             0
ICMPV6 Session Deleted                                           0
ICMPV6 Session Created                                           0
Other Session Deleted                                            0
Other Session Created                                            0
```

```
HTTP Request Logged                                              0
HTTP Logging Invalid Format Error                                0
SCTP Session Created                                             0
SCTP Session Deleted                                             0
Log Event Type SCTP Inner Proto Filter                           0
iDDoS IP Entry Created                                           0
iDDoS IP Entry Deleted                                           0
Session Limit Exceeded                                           0
```

- Use the `show session gtp` command to display the GTP session information.

```
ACOS(config)#show session gtp
Traffic Type                       Total
---------------------------------------------
GTP-C Established                  0
GTP-C Half Open                    0
GTP-U Count                        0
GTP-Echo Count                     0
GTP Current Available Conn         203979
GTP Conn Created(cumulative)       0
GTP Conn Freed(cumulative)         0
```

You can use `show session gtp rev-dest-teid <tied number>` to display the GTP session matching rev tuple dest-teid.

Table 24 : Show Session GTP Field Description

Field	**Description**
GTP-C Established	Indicates the number GTP-C sessions established.
GTP-C Half Open	Indicates the number of GTP-C sessions half-open.
GTP-U Count	Indicates the total number of GTP-U sessions.
GTP-Echo Count	Indicates the total number of GTP Echo sessions.
GTP Current Available Conn	Indicates the number of GTP sessions that can be created. **Note:** The number of GTP connections displayed is an approximate value.
GTP Conn Created (cumulative)	Indicates the cumulative number of GTP connections created including GTP-C, GTP-U and GTP Echo
GTP Conn Freed	Indicates the cumulative number of GTP connections freed

Table 24 : Show Session GTP Field Description

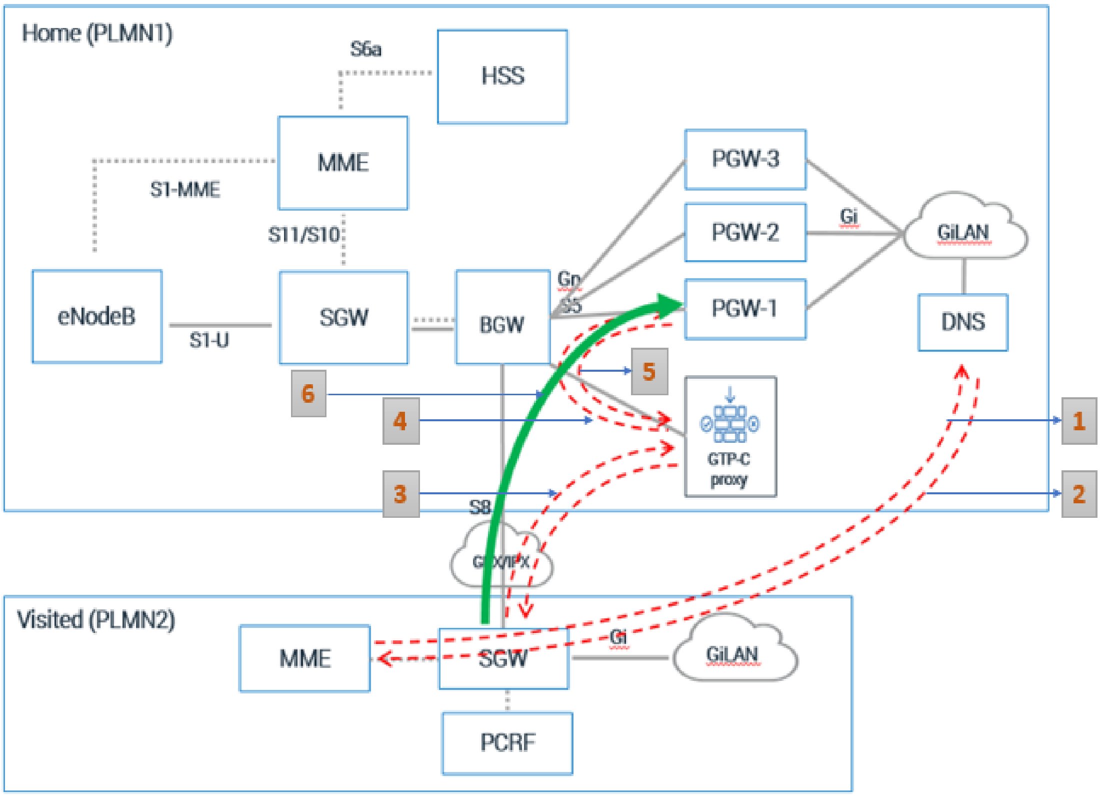
Field	Description
(cumulative)	

GTP Director

GTP Director directs the traffic from an SGW in the visited PLMN to a PGW in the home PLMN based on certain information elements in the GTP payload. For example, the selection criteria could include IMSI and APN (among other fields) from the GTP payload.

Figure 37 illustrates the flow of establishing a GTP tunnel between the visitor and the home network using GTP Director.

Figure 37 : GTP Director



In Figure 37, a Public Land Mobile Network (PLMN) is a network run by an operator. When subscribers use their operator’s network, it is called Home PLMN. In this case, it is named as **Home (PLMN1)**. When another user uses the resources from the other operator’s network, the other network is called Visited PLMN. In this case, it is named as **Visited (PLMN2)**.

GTP Director is deployed in one-arm mode. A representative flow used for establishing a GTP tunnel between Visited (PLMN2) and Home (PLMN2) is as follows:

1. The visitor Mobility Management Entity (MME) sends a request to home DNS.
2. Home DNS responds with the GTP-C Director IP.
3. Visitor SGW sends the request to GTP-C Director IP.
4. GTP Director directs the traffic to a specific Home PGW based on the IMSI and APN information available in the GTP payload and changes the source IP (SNAT).
5. Home PGW responds to GTP Director based on SNAT and forwards the packets to visitor SGW.
6. Visitor SGW sets up a GTP-U tunnel to a specific Home PGW based on the Fully Qualified Tunnel End Point Identifier (F-TEID) defined in the GTP response payload.

GTP Director directs the traffic to a specific Home PGW based on the configuration rules set on the ACOS devices for the fields in the GTP payload. For example, let’s assume the following IMSI and APN information exists in the sample packets:

- IMSI—466924000003930
- APN—internet.mnc092.mcc466.gprs

Using aFlex, you can manually configure rules as follows:

- Rule 1: If IMSI starts with "466924" and APN starts with "internet" then direct the traffic to PGW-1
- Rule 2: If IMSI starts with "466777" and APN starts with "internet" then direct the traffic to PGW-2
- Rule 3: If IMSI starts with "355000" and APN starts with "xxxpan" then direct the traffic to PGW-3

Based on the above rule, the sample packets are directed to PGW-1.

For configuring rules using aFlex, see *aFleX Scripting Language Reference*.

The GTP Director functionality also supports load balancing. Using the A10's SLB feature, you can define a virtual server and configure a virtual IP for the ports that are going to be used to direct the GTP traffic. You can configure a service group defining all the PGWs that are going to part of the load balancing group.

For performing load balancing on GTP-C connections, see the following example configuration:

```
ACOS(config)# slb virtual-server vip1 192.168.1.99
ACOS(config-slb vserver)# port 2123 udp
ACOS(config-slb vserver-vport)# service-group SG_1
ACOS(config-slb vserver-vport)# gtp-session-lb
```

The **`gtp-session-lb`** CLI command enables the stateful parsing of GTP payload to ensure that multiple requests on the same 5-tuple can be correctly load balanced to different servers.

In addition, aFlex can also select the server for each of the match criteria from within the aFlex policy and then default to the service-group configured under the VIP if no match occurs for the default selection.

For information on GTP load balancing, see *Application Delivery Controller Guide* and *Command Line Interface Reference for ADC.*

SCTP Firewall

The following topics are covered:

SCTP Firewall Overview

Stream Control Transmission Protocol (SCTP) is a transport-layer protocol that offers reliable transport of messages for end-to-end communications. Being a message-oriented transport protocol, SCTP preserves message boundaries. If a 100-byte message is sent from the sending application, the peer application will receive all 100 bytes in a single read.

Upon one single connection, SCTP can handle multiple simultaneous streams and multiplexed streams. Data is delivered in multiple and independent streams to prevent the possibility of data loss over one single stream. This ensures concurrent data streams (messages) can be successfully transmitted between connected endpoints.

SCTP multi-homing provides redundant paths to increase reliability and enables each of the two endpoints during an SCTP association setup to specify multiple points of attachment. This allows data to be automatically sent to alternate addresses when failures occur. Having multiple interfaces allows data to be automatically sent to alternate addresses when failures occur. With a 32-bit end-to-end checksum calculation, SCTP provides stronger verifications of messages passing end-to-end without bit errors going undetected.

In addition to ordered message service, SCTP also offers the reliable delivery of messages with no order constraints. Out-of-order packet delivery is supported in which packets are delivered in a different order from which they were sent.

SCTP uses a four-way handshake with a syn cookie to prevent flooding attack and to defer commitment of resources at the responding SCTP node until the handshake is completed after the initiator proves it is at the IP address from which it claims to be setting up the association. A Verification Tag is also used to prevent insertion of extraneous packets into the flow of an established association.The verification tag is used by SCTP to validate the sender. During the connection setup, the end-points exchange internally chosen Verification Tags which are used by the other endpoint to validate every packet they send.

SCTP Configuration

This section provides high-level configuration steps to set up a basic SCTP firewall. More granular CLI commands are described in the next section.

1. Configure a SCTP template.
2. Configure a firewall rule-set that contains a set of rules. Rules should contain the match criteria and associated action.
3. Optionally, bind the SCTP template to a rule. If no SCTP template is bound to a rule, the default template is used.
4. Activate the rule-set with the **`fw active-rule-set`** command.

SCTP Configuration Notes

- Firewall rule-sets include the option of configuring SCTP as a service under a firewall rule by configuring SCTP source and destination ports with IPv4 and IPv6 addresses under the rule-set.
- Specify all IPs to be allowed to create sessions as source ipv4- or source ipv6-address on separate prompts or as part of the object, then bind it as part of the rule-set.
- Out-of-state packets and packets that fail packet anomaly checks per RFC 4960 are dropped.
- To enable SCTP to work with Static NAT, configure the **`action permit cgnv6 static-nat`** option under the rule-set. Static NAT should be configured for each source address for Multi-homing purpose. SCTP does not work under LSN or Fixed-NAT.
- Use a SCTP template to configure SCTP-specific options. Bind this template to SCTP service in the rule. If no SCTP template is attached, then the default template is

used.

The following options are available for SCTP template configuration:

  - Use the **checksum-check** option to enable the verification of checksum.
  - Half-open and idle timeouts can be configured using the **half-open-idle-timeout** and **idle-timeout** options under the template. If this template is bound to a firewall rule, then half-open and idle timeout is handled based on the rule. Otherwise, if there is no SCTP template bound to the rule, then the default values for half-open and idle timeouts are used.
  - To filter packets based on the inner payload identifiers in the data chunk, use the **permit-payload-protocol** option under the SCTP template. By default, all payload protocols are allowed.
  - When this option is selected, payload protocol identifier values are set to 0xFFFF and the user data field is not modified. If all chunks in a packet are to be filtered, then the packet is dropped.
  - To log the protocol IDs that are filtered, use the **log payload-proto-filtering** option under the SCTP template.

- To configure SCTP session logging, use the **action permit log** option while configuring a rule.

SCTP Limitations

- A maximum of 8 IPv4/IPv6 addresses is supported for SCTP multi-homing purpose.
- There is no Multi-PU support for SCTP sessions.

SCTP Configuration Example (CLI)

The following commands configure a SCTP template:

```
ACOS(config)# template sctp test
ACOS(config-sctp template)# half-open-idle-timeout 5
ACOS(config-sctp template)# idle-timeout 10
ACOS(config-sctp template)# checksum-check enable
ACOS(config-sctp template)# permit-payload-protocol iua
ACOS(config-sctp template)# log payload-proto-filtering
```

The following commands configure a firewall rule-set that contains a set of rules and bind the SCTP template to a service destination port under the rule.

```
ACOS(config)# rule-set fw
ACOS(config-rule set:fw)# rule 1
ACOS(config-rule set:fw-rule:1)# action permit log
ACOS(config-rule set:fw-rule:1)# source ipv4-address any
ACOS(config-rule set:fw-rule:1)# source zone src
ACOS(config-rule set:fw-rule:1)# dest ipv4-address any
ACOS(config-rule set:fw-rule:1)# dest zone b
ACOS(config-rule set:fw-rule:1)# service sctp template default
ACOS(config-rule set:fw)# rule 2
ACOS(config-rule set:fw-rule:2)# action permit log
ACOS(config-rule set:fw-rule:2)# ip-version v6
ACOS(config-rule set:fw-rule:2)# source ipv6-address any
ACOS(config-rule set:fw-rule:2)# source zone src
ACOS(config-rule set:fw-rule:1)# dest ipv6-address any
ACOS(config-rule set:fw-rule:1)# dest zone b
ACOS(config-rule set:fw-rule:1)# service sctp template test
ACOS(config-rule set:fw)# rule 3
ACOS(config-rule set:fw-rule:2)# action permit cgnv6
ACOS(config-rule set:fw-rule:2)# ip-version v6
ACOS(config-rule set:fw-rule:2)# source ipv6-address any
ACOS(config-rule set:fw-rule:2)# source zone src
ACOS(config-rule set:fw-rule:1)# dest ipv6-address any
ACOS(config-rule set:fw-rule:1)# dest zone b
ACOS(config-rule set:fw-rule:1)# service sctp template test
```

The following command enables the firewall rule-set:

```
ACOS(config)# fw active-rule-set fw
```

Firewall Logging

This section describes how to create firewall logging templates.

The following topics are covered:

Firewall Logging Overview

Firewall logging action can be applied to any rule. When the logging action is enabled, log messages are generated when a session is created, terminated, or denied.

DC firewall, Gi firewall (GiFW), and Application aware firewall do not store log messages locally but send them to an external collector using a configured protocol and format.

The following topics are covered:

Firewall Event Types

Firewall log messages consist of the following basic event types:

- Configuration events – These messages indicate that a configuration change has occurred.
  Typically, this type of firewall event is generated when you configure a firewall rule or other setting. Firewall configuration logs are sent following successful configuration of system logging. Firewall configuration logs are included as part of the system logs, and these configuration logs are only sent out after using the **`logging host`** command. See the **`logging host`** command in the CLI Reference for details on setting up basic system logging. When the firewall configuration log is sent to the remote log server, it will also appear in the log buffer. By default, only configuration events are logged to the local logging buffer on ACOS.
- Session events – These event types indicate that a firewall session has been created or terminated. Session logs for data events can be sent using either of two logging commands (**`logging host`** or **`fw logging`**).

  - Session events are not logged by default. Due to the potentially high volume of session event messages, these are only accessible using external logging servers. You can configure the firewall to use a single logging server or a group of logging servers.
  - To set up firewall logging for session events, use the **`fw logging`** command. (See the **`fw logging`** command for details.)

NOTE: If an external logging server is not set up, then firewall configuration events are stored locally, and session events will not be logged.

Configuring the External Logging Server

The firewall may create a high volume of log messages. These messages are directed to an external logging server. Because all firewall logs are verbose and occur at high frequency, the ACOS device can separate log messages associated with firewall activity from log messages related to general device configuration.

The firewall uses system logging host configuration to obtain the syslog server information. This approach may be limiting, because the system logging host configuration is used for device system logging. This host must also have a custom logging template configured and must be bound to the firewall (GiFW, CFW) rule-set. The logging host must be configured to accept syslog messages, and it must be reachable from within the partition's routing domain.

NOTE: When configuring multiple logging hosts, requests are sent to the destination using round-robin load balancing. The logging host must not be on the management network.

Firewall logging is available in the following partitions:

- Firewall partition
- CGN-Firewall partition

The key building blocks of a firewall logging configuration are:

- firewall logging servers
- firewall service groups

- firewall logging templates

Firewall Logging Template

Firewall logging templates can be configured globally or in specific rules. After configuring a template, you will need to bind it before it can be used. The only available server selection method in the firewall logging template is the source IP hash-based method. You can configure Firewall, CGNv6, or NetFlow monitor logging templates in Firewall only partition or a CGN-Firewall partition.

Globally configured logging templates help you collect and export logs from all rules to external servers in an efficient way. However, in some cases you may want to configure templates specific to rules that allow precise logging. While configuring a selective logging template under a specific rule, consider the following points:

- Firewall, CGNv6, and NetFlow monitor templates are supported.
- The rule-specific logging template action must be inside an action group.
- Up to four logging templates can be configured for each rule.
- You must use two commands to enable and bind the template. For example, in the action group, use `permit log` to enable logs and then `permit log <log-template-type> <template-name>` to bind and activate the template. The following are the template types:
    - fw-logging-template
    - cgnv6-logging-template
    - netflow-monitor

Firewall logs are sent out using multiple protocols and formats. For more information, see Configuring Logging Format. For sample configuration of logging templates, see Configuring Firewall Logging.

NOTE: A firewall service group or a CGNv6 service group can be bound to a firewall logging template. UDP and TCP are the firewall service-group types that can be bound to a firewall logging template.

Limitations:

- Any change in the logging template after session creation may result in creating and deletion logs being logged on to different log servers.
- Within any given partition, configuring an SLB template with the same name as a firewall template is not permitted.

Binding Firewall Logging Template Globally

For firewall logs to be sent using the firewall logging template, the firewall logging template must be bound globally. The following command binds the template irrespective of whether it is used for specific rules.

```
ACOS(config)# fw logging <template name>
```

NOTE: Logging templates that are configured inside rules can be bound and activated for those rules as well as at the global level.

HTTP Logging Support

HTTP logging provides the ability to send logging information for CGN-based events such as the following:

- log http-request url
- include-http l4-session-info
- rule http-requests dest-port 80

For a full list of options supported by HTTP logging, see the **`include-http`**, **`log http-requests`**, and **`rule http-requests`** options under the **`fw template logging`** command.

How HTTP Logging Works

Upon receiving a TCP packet ACOS first matches against the configured rule-set to check if it is permitted. ACOS then does a destination port lookup to decide if HTTP logging is required for the session.

Configuration

HTTP logging is enabled on a destination port basis and is configured in the firewall logging template.

The following sample configuration shows how to enable HTTP logging on ports 80 and 880:

```
ACOS(config)# fw template logging log1
ACOS(config-logging)# log http-request url
ACOS(config-logging)# rule http-requests dest-port 80
ACOS(config-logging)# rule http-requests dest-port 880
```

NOTE: HTTP Logging requires that log messages be sent in ASCII format. Therefore, you must change the log message format from CEF to ASCII for HTTP Logging to work. For more information, see Configuring Logging Format.

NOTE: For a comprehensive discussion of HTTP logging, see “Logging HTTP Headers” section in the 2.8.2-P6 Traffic Logging Guide for IPv6 Migration.

Configuring Firewall Logging

Firewall logging can be configured in Firewall-only partition or a CGN-Firewall partition. The key building blocks of a firewall logging configuration are firewall logging servers, firewall service groups, firewall logging templates.

The following process summarizes the key tasks:

1. Create a server configuration for each log server.

   Depending on whether ACOS is configured with a single syslog server for both CGN and Firewall configurations, the same IP for CGN and FW logging can be shared in a single CGN or Firewall server.

2. Configure a TCP or UDP service group and add the log servers to the group. The service group can contain a maximum of 32 members for external logging.

3. Configure a logging template. Within the template, specify the service group and the types of events to log.

   If ACOS is configured with both CGN and any Firewall configurations, CGN service group can be configured in a firewall template for an existing CGN deployment upgraded with GiFW or Application aware firewall. Conversely, a firewall service group can be configured in the CGN template for an existing firewall deployment.

4. Activate the template.

NOTE: The service group (slb or cgnv6) cannot share the same name as a firewall service group.

Configuring Firewall Logging for Firewall Deployment Only

The following commands configure the firewall servers:

```
ACOS(config)# fw server syslog 15.15.15.91
ACOS(config-real server)# port 514 udp (or tcp)
ACOS(config-real server-node port)# exit
ACOS(config)# fw server syslog2 15.15.15.92
ACOS(config-real server)# port 514 udp (or tcp)
ACOS(config-real server-node port)# exit
```

The following commands configure the firewall service groups:

```
ACOS(config)# fw service-group syslog1 udp (or tcp)
ACOS(config-fw svc group)# member syslog 514
ACOS(config-fw svc group)# exit
ACOS(config)# fw service-group syslog2 udp (or tcp)
ACOS(config-fw svc group)# member syslog2 514
ACOS(config-fw svc group)# exit
```

The following commands configure the firewall logging templates:

```
ACOS(config)# fw template logging fw_logging
ACOS(config-logging)# service-group syslog1
ACOS(config-logging)# exit
ACOS(config)# fw template logging fw_logging2
ACOS(config-logging)# service-group syslog2
```

The following command binds the firewall logging template globally:

```
ACOS(config)# fw logging fw_logging
```

In the following sample, the **rule-set** *test* has two rules.

- **rule 1**: The command **permit log** enables logs for the rule. This rule uses the global logging template *fw_logging* configured and bound earlier.
- **rule 2**: The command **permit log** enables logs and the command **permit log fw-logging-template fw_logging2** binds and activates the template for the rule.

```
ACOS(config)# rule-set test
ACOS(config-rule set:test)# rule 1
ACOS(config-rule set:test-rule:1)# source ipv4-address 3.3.3.0/24
ACOS(config-rule set:test-rule:1)# source zone any
ACOS(config-rule set:test-rule:1)# dest ipv4-address any
ACOS(config-rule set:test-rule:1)# dest zone any
ACOS(config-rule set:test-rule:1)# action-group
ACOS(config-rule set:test-rule:1-acti...)# permit log
ACOS(config-rule set:test)# rule 2
ACOS(config-rule set:test-rule:2)# source ipv4-address 3.3.3.89/32
ACOS(config-rule set:test-rule:2)# source zone any
ACOS(config-rule set:test-rule:2)# dest ipv4-address 15.15.15.90/32
ACOS(config-rule set:test-rule:2)# dest zone any
ACOS(config-rule set:test-rule:2)# action-group
ACOS(config-rule set:test-rule:2-acti...)# permit log
ACOS(config-rule set:test-rule:2-acti...)# permit log fw-logging-template
fw_logging2
```

Disabling Undetermined Rule Logs

When the Firewall is configured, some logs having undetermined rules are generated in the Syslog (cs2 field for CEF format and RULE field for ASCII format). To reduce excessive logging and improve syslog readability, you can disable these logs by enabling the **fw disable-undetermined-rule-logs** command as shown below.

```
ACOS(config)# fw disable-undetermined-rule-logs
```

When this command is enabled, the undetermined rule logs are not sent to the syslog server.

NOTE: This command does not affect the firewall logs sent to the Harmony Controller and IPFIX collectors.

Additionally, whenever logs with undetermined rules are generated, the **`Undetermined rule detected`** counter is incremented. To view this counter, use the **`show counters fw global`** command.

Disabling CEF Labels in the Syslog

When Firewall logging is configured to use the CEF format, the resulting logs contain numerous labels. Although these labels provide context and metadata about each event, they increase the packet size, consequently raising logging costs. To optimize log management processes, and enhance efficiency and readability, you can suppress these labels by configuring the **`fw logging cef-label`** command, as shown below:

```
ACOS(config)# fw logging cef-label disable
```

By default, all CEF labels are included in the Syslog. When this command is configured, all CEF labels are suppressed in the Syslog.

CEF Log Message Examples

- With **`fw logging cef-label enable`** configured (default):

```
 Feb 26 22:24:06 vThunder CEF:0|A10|CFW|6.0.3-P1|FW 101|Session
closed|1|proto=ICMP flexNumber1=8 flexNumber2=0 act=Permit rt=89126806
src=10.0.0.6 dst=20.0.0.4 deviceInboundInterface=ve2
deviceOutboundInterface=ve3 cs1=rs1 cs2=1 cs3=Idle timeout in=392
out=392 cn1=4 cn2=4 cn3=5 cn4=0 cn5=0 cn6=0 cn7=0 cs1Label=Rule Set Name
cs2Label=Rule Name cs3Label=Reason cn1Label=Forward packets
cn2Label=Reverse packets cn3Label=Session Duration Seconds
cn4Label=Forward drop packets cn5Label=Forward drop bytes
cn6Label=Reverse drop packets cn7Label=Reverse drop bytes
flexNumber1Label=ICMP Type flexNumber2Label=ICMP Code
```

- With **`fw logging cef-label disable`** configured:

```
Feb 26 22:27:28 vThunder CEF:0|A10|CFW|6.0.3-P1|FW 101|Session
closed|1|proto=ICMP flexNumber1=3 flexNumber2=3 act=Permit rt=89177307
src=20.0.0.4 dst=20.0.0.3 deviceInboundInterface=ve3
deviceOutboundInterface=ve3 cs1=rs1 cs2=1 cs3=Idle timeout in=0 out=686
cn1=2 cn2=0 cn3=4 cn4=0 cn5=0 cn6=0 cn7=0
```

The highlighted CEF labels are suppressed when **`fw logging cef-label disable`** is configured.

Configuring Logging Format

Log messages are sent to external logging servers in various formats that comply with respective protocols such as syslog protocol or IPFIX protocol. The following table lists the formats supported for Firewall, CGNv6, and NetFlow (IPFIX) templates:

Template	Supported Protocols	Supported Log Formats	Default Format
Firewall	Syslog	• CEF • ASCII • Custom	CEF
	IPFIX (Binary)	IPFIX (Binary)	
CGN	Syslog	• Binary • compact • custom • ASCII • rfc5424 • CEF	ASCII
	IPFIX (Binary)	IPFIX (Binary)	

Use with the following commands to specify the logging format:

```
ACOS(config)# fw template logging name
ACOS(config-logging)# format {ascii | cef | custom }

ACOS(config)# fw template logging appfw
ACOS(config-logging)# format ascii
```

For more information, see the **fw template logging** command in the ***Command Line Reference Guide***. For more information on the logging formats for CGN, see ***Traffic Logging Guide***.

CEF Logging Format

Firewall log messages that use CEF format contain the following fields:

CEF Source message:

```
Timestamp | host| CEF:version|device-vendor|device-product|
device-version|Signature ID (or “module”)|Name (or “event-
type”)|Severity|CEF-extension
100.100.100.12.59109 > localhost.localdomain.syslog: SYSLOG, length: 502
        Facility local0 (16), Severity info (6)
        Msg:  Apr  4 13:17:01 2018 Dj4430SAX1 CEF:0|A10|CFW|4.1.4-P1|FW
100|Session opened|1|proto=TCP act=Permit rt=109752862 app=google_
analytics src=20.20.20.216 spt=47559 dst=172.217.6.78 dpt=443
deviceInboundInterface=ethernet15 cs4=ztrunksrc
deviceOutboundInterface=ethernet13 cs5=appfwdst cs1=hairpinscale
cs2=google_play cs6=dcfwalg cs7=web, analytics-and-statistics
cs1Label=Rule Set Name cs2Label=Rule Name cs4Label=Source Zone
cs5Label=Dest Zone cs6Label=Partition Name cs7Label=Application Category
```

CEF Destination Message

```
100.100.100.12.63532 > localhost.localdomain.syslog: SYSLOG, length: 617
        Facility local0 (16), Severity info (6)
        Msg:  Apr  4 13:17:01 2018 Dj4430SAX1 CEF:0|A10|CFW|4.1.4-P1|FW
101|Session closed|1|proto=UDP act=Permit rt=109752727 app=dns
src=20.20.20.216 spt=36096 dst=192.168.1.50 dpt=53
deviceInboundInterface=ethernet15 cs4=ztrunksrc
deviceOutboundInterface=ethernet13 cs5=appfwdst cs1=hairpinscale
cs2=twitterdns cs6=dcfwalg cs7=networking, standards-based cs3=Normal in=0
out=130 cn1=1 cn2=0 cn3=1 cs1Label=Rule Set Name cs2Label=Rule Name
cs3Label=Reason cn1Label=Packets TX cn2Label=Packets RX cn3Label=Session
Duration Seconds cs4Label=Source Zone cs5Label=Dest Zone
cs6Label=Partition Name cs7Label=Application Category
```

Table 25 describes the fields that may appear in the firewall logs of CEF-formatted messages

Table 25 : Firewall log fields in CEF-formatted messages

Field	Description
Timestamp	Date and time the log was generated, in the following format: Mon Day hh:mm:ss Year
Host	Name (or IP) of the firewall device.
CEF version	CEF version.
device-vendor	Vendor name, “A10”.
device-product	CFW
device-version	For example, “4.1.4”
signature-id (a.k.a., “module”)	The signature-id is a unique identifier for each of the different event types. This can be a string or an integer, and it is used to identify the type of event that is being reported. The signature-id field has prefix “FW” before a numbered code, such as “FW 100”.
name (a.k.a., “event-type”)	The name field is a description of the FW event-type. For example: Session opened Session closed
Severity	The Severity field indicates the severity of the event in the range of 0 to 10. 0 is the lowest and 10 is the highest.
CEF-extension (an extension is a collection of key-value pairs)	The CEF extension for FW uses the following elements: • **proto** – TCP, UDP, ICMP, ICMPv6, IP, GRE, RTSP and OTHER • **act** – Action taken by the firewall device: ○ Permit ○ Deny ○ Reset • **rt** – “rt” or “receiptTime” is a timestamp representing the time at

Table 25 : Firewall log fields in CEF-formatted messages

Field	Description
	which the event related to the activity was received. The format is MMM dd yyyy HH:mm:ss (e.g., Jan 21 1980), or "rt" can also be expressed as the number of milliseconds since the epoch. • **app** -- Application • **src** – Source IP of the request or response. • **spt** – Source protocol port of the request or response. • **dst** – Destination IP of the request or response. • **dpt** – Destination protocol port of the request or response. • **deviceInboundInterface** – Interface upon which the data or packet entered the device. • **deviceOutboundInterface** – Interface upon which the data or packet exited the device. • **cs1** and **cs1Label** – The name of the rule-set. • **cs2** and **cs2Label** – The name of the rule within the rule-set. • **cs4** and **cs4Label** – The name of the source zone. • **cs5** and **cs5Label** – The name of the destination zone. • **cs6** and **cs6Label** – The name of the partition. (Note: This field is N/A if the event is invoked in the shared partition) • **cs7** and **cs7Label -** The application protocol and category. • **cs8 and cs8Label** – The name of the source threat list. • **cs9 and cs9Label** – The name of the destination threat list. • **cs10 and cs10Label** – The source threat category. • **cs11 and cs11Label** – The destination threat category • **cn1** and **cn1Label** – Packets transferred from source to destination. Appears in close event only. • **cn2** and **cn2Label** – Packets transferred from destination to source. Appears in close event only.

Table 25 : Firewall log fields in CEF-formatted messages

Field	Description
	• **cn3** and **cn3Label** – Session duration (in seconds) since open event. Appears in close event only. • **c6a2** and **c6a2Label** – IPv6 source address. • **c6a3** and **c6a3Label** – IPv6 destination address. • **flexNumber1** and **flexNumber1Label** – ICMP/ICMPv6 type. • **flexNumber2** and **flexNumber2Label** – ICMP/ICMPv6 code.

The following section shows a sample FW log message in CEF format for a UDP session that is being opened.

```
100.100.100.12.59109 > localhost.localdomain.syslog: SYSLOG, length: 502

Facility local0 (16), Severity info (6)

Msg: Apr 4 13:17:01 2018 Dj4430SAX1 CEF:0|A10|CFW|4.1.4-P1|FW 100|Session
opened|1|proto=TCP act=Permit rt=109752862 app=google_analytics
src=20.20.20.216 spt=47559 dst=172.217.6.78 dpt=443
deviceInboundInterface=ethernet15 cs4=ztrunksrc
deviceOutboundInterface=ethernet13 cs5=appfwdst cs1=hairpinscale cs2=google_
play cs6=dcfwalg cs7=web, analytics-and-statistics cs1Label=Rule Set Name
cs2Label=Rule Name cs4Label=Source Zone cs5Label=Dest Zone cs6Label=Partition
Name cs7Label=Application Category
```

```
100.100.100.12.63532 > localhost.localdomain.syslog: SYSLOG, length: 617

Facility local0 (16), Severity info (6)

Msg: Apr 4 13:17:01 2018 Dj4430SAX1 CEF:0|A10|CFW|4.1.4-P1|FW 101|Session
closed|1|proto=UDP act=Permit rt=109752727 app=dns src=20.20.20.216 spt=36096
dst=192.168.1.50 dpt=53 deviceInboundInterface=ethernet15 cs4=ztrunksrc
deviceOutboundInterface=ethernet13 cs5=appfwdst cs1=hairpinscale cs2=twitterdns
cs6=dcfwalg cs7=networking, standards-based cs3=Normal in=0 out=130 cn1=1 cn2=0
cn3=1 cs1Label=Rule Set Name cs2Label=Rule Name cs3Label=Reason
cn1Label=Packets TX cn2Label=Packets RX cn3Label=Session Duration Seconds
```

cs4Label=Source Zone cs5Label=Dest Zone cs6Label=Partition Name cs7Label=Application Category

Table 26 labels each field that appears in the above log message.

Table 26 : FW log example (CEF) opening session

Field	Value
Timestamp	Sep 30 15:21:39 2016
Host	vThunder
CEF version	0
device-vendor	A10 NETWORKS
device-product	Thunder Series Unified Application Service Gateway
device-version	4.1.4
signature-id (module)	FW 100
name (event-type)	Session opened
Common Event Format	1
Protocol	TCP

CEF-extension (i.e., key-value pairs)	act=Permit
	rt=4299774764
	src=192.168.101.50
	spt=59298
	dst=192.168.201.51
	dpt=80
	deviceInboundInterface =ethernet1
	deviceOutboundInterface =ethernet2
	cs1=fw-policy

Table 26 : FW log example (CEF) opening session

Field	Value
	cs2=any **cs6**=p1 **cs1Label**=Rule Set Name **cs2Label**=Rule Name **cs6Label**=Partition Name

ASCII Logging Format

ASCII formatted log messages can include additional information that cannot be conveyed using standard CEF log messages. For example, the following CGN logging options are supported when using ASCII formatted log messages:

- Inclusion of RADIUS attributes in log messages
- Support for HTTP logging
- Inclusion of timestamp resolution
- Inclusion of the byte count in log messages
- Ability to set the firewall logging facility, for example, to CFW or Application Aware Firewall

Sample ASCII-formatted Log Messages

This sample firewall ASCII-formatted log message shows an IPv4 or IPv6 UDP session:

```
100.100.100.12.45786 > localhost.localdomain.syslog: SYSLOG, length: 825
        Facility local0 (16), Severity info (6)
        Msg:  Apr  4 13:22:35 Dj4430SAX1 FW-UDP-G: 20.20.20.216:47128<--
>192.168.1.50:53 ACT=PERMIT RT=109836533 APP=dns IN-INTF=ethernet15 IN-
ZN=ztrunksrc OUT-INTF=ethernet13 OUT-ZN=appfwdst POLICY=hairpinscale
RULE=twitterdns APP-CAT=networking, standards-based\0x0d\0x0a<134> Apr  4
13:22:36 Dj4430SAX1 FW-UDP-H: 20.20.20.216:47128<-->192.168.1.50:53
ACT=PERMIT RT=109836771 APP=dns IN-INTF=ethernet15 IN-ZN=ztrunksrc OUT-
INTF=ethernet13 OUT-ZN=appfwdst POLICY=hairpinscale RULE=twitterdns APP-
CAT=networking, standards-based FWD_BYTES=316 REV_BYTES=0 FWD_PKTS=1 REV_
PKTS=0 DUR=1\0x0d\0x0a<134> Apr  4 13:22:38 Dj4430SAX1 FW-UDP-G:
20.20.20.216:46855<-->192.168.1.50:53 ACT=PERMIT RT=109837113 APP=dns IN-
INTF=ethernet15 IN-ZN=ztrunksrc OUT-INTF=ethernet13 OUT-ZN=appfwdst
POLICY=hairpinscale RULE=twitterdns APP-CAT=networking, standards-
based\0x0d\0x0a

    100.100.100.12.46849 > localhost.localdomain.syslog: SYSLOG, length:
879
        Facility local0 (16), Severity info (6)
        Msg:  Apr  4 13:22:38 Dj4430SAX1 FW-UDP-H: 20.20.20.216:48382<--
>192.168.1.50:53 ACT=PERMIT RT=109837271 APP=dns IN-INTF=ethernet15 IN-
ZN=ztrunksrc OUT-INTF=ethernet13 OUT-ZN=appfwdst POLICY=hairpinscale
RULE=twitterdns APP-CAT=networking, standards-based FWD_BYTES=150 REV_
BYTES=0 FWD_PKTS=1 REV_PKTS=0 DUR=1\0x0d\0x0a<134> Apr  4 13:22:39
Dj4430SAX1 FW-UDP-G: 20.20.20.216:46450<-->192.168.1.50:53 ACT=PERMIT
RT=109837341 APP=dns IN-INTF=ethernet15 IN-ZN=ztrunksrc OUT-
INTF=ethernet13 OUT-ZN=appfwdst POLICY=hairpinscale RULE=twitterdns APP-
CAT=networking, standards-based\0x0d\0x0a<134> Apr  4 13:22:40 Dj4430SAX1
FW-UDP-H: 20.20.20.216:46450<-->192.168.1.50:53 ACT=PERMIT RT=109837591
APP=dns IN-INTF=ethernet15 IN-ZN=ztrunksrc OUT-INTF=ethernet13 OUT-
ZN=appfwdst POLICY=hairpinscale RULE=twitterdns APP-CAT=networking,
standards-based FWD_BYTES=208 REV_BYTES=0 FWD_PKTS=1 REV_PKTS=0
DUR=1\0x0d\0x0a
```

Table 27 : FW log example (ASCII format) IPv4 or IPv6 UDP session

Field	**Value**
Host	LOCAL0.INFO:
Timestamp	Jan 2 17:04:18
device-product	ACOS DEVICE

Table 27 : FW log example (ASCII format) IPv4 or IPv6 UDP session

Field	Value
Application-Protocol-EventType	FW-UDP-H For firewall logs, event type can be: G – session OPEN H – session CLOSE I – session DENY J – session RESET
Src IP/port	3.3.3.89:58219
Dst IP/port	15.15.15.90:14000

ASCII-extension (i.e., key-value pairs)	ACT= PERMIT
	RT= 4295164466
	IN-INTF=ve301
	OUT-INTF=ve401
	POLICY=fw-only
	RULE=2
	FWD_BYTES=180
	REV_BYTES=0
	FWD_PKTS=3
	REV_PKTS=0
	DUR=10\r\n

Custom Logging Format

The standard logging formats such as CEF and ASCII provide a strong logging framework. However, they often contain excessive data that may not always be relevant. This additional data increases the packet size, which results in higher logging expenses. To optimize log management, and improve efficiency and readability, you can use the custom logging format for Firewall Session Open and Delete logs.

This compact format allows you to create an arbitrary log format by including only specific events and fields in the Firewall logs. It provides the flexibility to:

- Log session creation and session deletion events (currently, only these events are supported).
- Include event-specific details such as session start time, session duration, and more by using certain predefined keywords. For the keyword list, see Keywords for Custom Logging Format.
- Insert text string (plain text) without any keywords.

This flexibility allows you to adjust and reduce the log size, thereby lowering logging costs.

Set the **format custom** and **custom message** commands in the Firewall logging template to configure a custom logging format for the Firewall.

NOTE: In case of traffic routed through CGN and firewall, it is recommended to use the NAT logging template instead of the Firewall logging template.

CLI Configuration

To configure a custom log format, enable the **format custom** command and set the message string using the **custom message** command in the Firewall logging template:

```
ACOS(config)# fw template logging template_name
ACOS(config-logging)# format custom
ACOS(config-logging)# custom message {session-created | session-deleted}
custom_string
```

The **custom message** command allows you to set an arbitrary log message by including specific events, text strings, and predefined keywords. For the keyword list, see Keywords for Custom Logging Format.

The following configuration example demonstrates command usage:

1. Configure the Firewall logging template.

   a. Set the **format** as **custom** to enable custom logging:

   ```
   ACOS(config)# fw template logging custom_template
   ACOS(config-logging)# format custom
   ```

   b. Set the custom message string, using the **custom message** command:

   ```
   ACOS(config-logging)# custom message session-created FW_SESSION_
   CREATED,$src-ip$,$src-port$,$proto-name$,$dst-ip$,$dst-port$,$sesn-
   start-time$,$rule-set-name$,$rule-name$,$in-interface$,$out-
   interface$,$sesn-start-time-epoch$,$src-zone$,$dest-zone$,$radius-
   imei$,$radius-ctm1$

   ACOS(config-logging)# custom message session-deleted FW_SESSION_
   DELETED,$src-ip$,$src-port$,$proto-name$,$dst-ip$,$sesn-start-
   time$,$rule-set-name$,$rule-name$,$in-bytes$,$out-bytes$,$pkts-
   rx$,$sesn-start-time-epoch$,$sesn-end-time$,$dest-zone$,$app-
   id$,$radius-msisdn$,$radius-imei$,$radius-ctm4$
   ```

   NOTE: The **format custom** command must be configured to enable custom logging. If the **custom message** command is configured without enabling this command, logs will be generated in the default CEF format. . A maximum of only 20 attributes can be configured at a time.

2. Bind the logging template globally, using the following command:

   ```
   ACOS(config)# fw logging custom_template
   ```

3. Bind the logging template to a rule within a Firewall rule-set:

   ```
   ACOS(config)# rule-set test
   ACOS(config-rule set:test)# rule 1
   ACOS(config-rule set:test-rule:1)# source ipv4-address any
   ACOS(config-rule set:test-rule:1)# source zone any
   ACOS(config-rule set:test-rule:1)# dest ipv4-address any
   ACOS(config-rule set:test-rule:1)# dest zone any
   ACOS(config-rule set:test-rule:1)# service any
   ACOS(config-rule set:test-rule:1)# application any
   ```

```
ACOS(config-rule set:test-rule:1)# action-group
ACOS(config-rule set:test-rule:1-acti...)# permit log fw-logging-
template custom_template
```

4. Activate the Firewall rule-set:

```
ACOS(config)# fw active-rule-set test
```

Sample custom logs generated:

```
FW_SESSION_
CREATED,10.0.0.6,1769,UDP,20.0.0.4,0,20240425223523,rs1,rule1,ve2,ve3,1726
081258,outside,inside,5,999,a222,b222,c222
FW_SESSION_
DELETED,10.0.0.6,1768,UDP,20.0.0.4,0,20240425223543,14559,rs1,rule1,0,42,1
,0,42,1,0,1726081258,20190520062200,1726081272,outside,inside,5,999,a222,b
222,c2222
```

Keywords for Custom Logging Format

Certain predefined keywords can be included in the custom log format to add event-specific details such as session start time, session duration, and more to the firewall logs.

NOTE: The keywords must be enclosed in dollar signs ($).

The following tables list the keywords that can be included in the custom logging format:

Table 28 : Keywords for **session-create** event

Keyword	Description	Example Output in logs
$proto-name$	Protocol used in the session.	UDP/TCP
$src-ip$	Source IP address of the session.	5.5.5.100
$src-port$	Source Port number of the session.	34273
$dst-ip$	Destination IP address of the session.	6.6.6.100
$dst-port$	Destination Port number of the session.	2123

Keyword	Description	Example Output in logs
`$in-interface$`	Incoming network interface of the session.	ve801
`$out-interface$`	Outgoing network interface of the session.	ve701
`$rule-set-name$`	Specific rule set applied to the session.	rule-set1
`$rule-name$`	Specific rule name within the rule set that matched the session.	rule1
`$partition-name$`	Partition within the Firewall where the session exists.	p1
`$sesn-start-time$`	Start time of the session.	20190520062105
`$sesn-start-time-epoch$`	Epoch start time of the session.	1726081258
`$time-stamp$`	Log generation time stamp	20200510062005
`$src-zone$`	Source Zone	outside
`$dest-zone$`	Destination Zone	inside
`$app-id$`	App Id	5
`$radius-msisdn$`	RADIUS attribute: MSISDN	999
`$radius-imei$`	RADIUS attribute: IMEI	999
`$radius-imsi$`	RADIUS attribute: IMSI	999
`$radius-ctm1`	RADIUS attribute: Custom1	a222
`$radius-ctm2$`	RADIUS attribute: Custom2	b222
`$radius-ctm3$`	RADIUS attribute: Custom3	c222
`$radius-ctm4`	RADIUS attribute: Custom4	d222
`$radius-ctm5`	RADIUS attribute: Custom5	e222
`$radius-ctm6`	RADIUS attribute: Custom6	f222

Table 29 : Keywords for **`session-delete`** event

Keyword	Description	Example Output in logs
`$proto-name$`	Protocol used in the session.	UDP/TCP
`$src-ip$`	Source IP address of the session.	5.5.5.100
`$src-port$`	Source Port number of the session.	34273
`$dst-ip$`	Destination IP address of the session.	6.6.6.100
`$dst-port$`	Destination Port number of the session.	2123
`$in-interface$`	Incoming network interface of the session.	ve801
`$out-interface$`	Outgoing network interface of the session.	ve701
`$rule-set-name$`	Specific rule set applied to the session.	rule-set1
`$rule-name$`	Specific rule name within the rule set that matched the session.	rule1
`$partition-name$`	Partition within the Firewall where the session exists.	p1
`$sesn-start-time$`	Start time of the session.	20190520062105
`$sesn-start-time-epoch$`	Epoch start time of the session.	1726081258
`$sesn-dur$`	Total time the session was active.	12
`$in-bytes$`	Total number of bytes received during the session.	0
`$out-bytes$`	Total number of bytes sent during the session.	187
`$pkts-rx$`	Total number of packets received by the session.	0
`$pkts-tx$`	Total number of packets transmitted (sent) from the session.	1

Keyword	Description	Example Output in logs
$sesn-end-time$	Session end time	20190520062200
$sesn-end-time-epoch$	Epoch end time of the session.	1726081272
$time-stamp$	Log generation time stamp	20200510062005
$src-zone$	Source Zone	outside
$dest-zone$	Destination Zone	inside
$app-id$	App Id	5
$radius-msisdn$	RADIUS attribute: MSISDN	999
$radius-imei$	RADIUS attribute: IMEI	999
$radius-imsi$	RADIUS attribute: IMSI	999
$radius-ctm1	RADIUS attribute: Custom1	a222
$radius-ctm2$	RADIUS attribute: Custom2	b222
$radius-ctm3$	RADIUS attribute: Custom3	c222
$radius-ctm4	RADIUS attribute: Custom4	d222
$radius-ctm5	RADIUS attribute: Custom5	e222
$radius-ctm6	RADIUS attribute: Custom6	f222

Sample Log Messages

Following are some examples of custom message strings and corresponding logs generated:

- For session creation event with IPv6 traffic using ICMP protocol:

Custom Message String:

```
custom message session-created FW_SESSION_CREATED,$proto-name$,$src-ip$,$src-port$,$dst-ip$,$dst-port$,$in-interface$,$out-interface$,$rule-set-name$,$rule-name$,$partition-name$,$sesn-start-time$,$radius-msisdn$
```

Log Generated:

```
FW_SESSION_CREATED,ICMP,2020::100,0,2020::1,0,ethernet2,ethernet2,fw-rule-set,r2,Shared,20240508161759,999
```

- For session deletion event with IPv4 traffic using UDP protocol:

  Custom Message String:

  ```
  custom message session-deleted,FW_SESSION_DELETED,$proto-name$,$src-
  ip$,$src-port$,$dst-ip$,$dst-port$,$in-interface$,$out-interface$,$rule-
  set-name$,$rule-name,$pkts-tx$,$pkts-rx$,$sesn-dur$,$sesn-end-
  time$,$sesn-end-time-epoch$,$src-zone$,$dest-zone$,$radius-ctm1
  ```

  Log Generated:

  ```
  FW_SESSION_
  DELETED,UDP,10.1.1.1,1752,20.1.0.100,0,ethernet1,ethernet2,fw-rule-
  set,r1, 1,0,11070,20240508144205,1726081272,outside,inside,a222
  ```

Configuring Same Syslog Server for CGN and Firewall

A single syslog server configuration (CGNv6 or Firewall server) can be used for both FW and CGN logging.

Configuration Example 1

Create Server Configurations for the CGN Traffic Log Servers

To create a server configuration for a traffic log server and specify the port on which the server listens for log traffic, use the following commands:

```
ACOS(config)# cgnv6 server cgns 15.15.15.90
ACOS(config-real-server)# port 514 udp
ACOS(config-real server-node port)# exit
```

Configure a CGN Service Group and Its Member

To create a CGN service group (server pool) for the traffic log servers and to add a traffic log server and its UDP port to the service group, use the following commands.

```
ACOS(config)# cgnv6 service-group cgnsg udp
ACOS(config-cgnv6 svc group)# member cgns 514
ACOS(config-cgnv6 svc group)# exit
```

Enable CGN Logging

Configuring an External CGN Logging Template

To configure an external CGN logging template and to add the service group of external log servers to the template, use the following commands:

```
ACOS(config)# cgnv6 template logging lsn_log
ACOS(config-logging:lsn_logging)# log sessions
ACOS(config-logging:lsn_logging)# service-group cgnsg
ACOS(config-logging:lsn_logging)# exit
```

The service group is the only required configuration item in external logging templates.

Activate the External CGN Logging Template

To activate the external logging template, use the following command at the global configuration level of the CLI:

```
ACOS(config)# cgnv6 lsn logging default-template lsn_log
```

External traffic logging does not take effect until you use this command.

Although this command and the following command contain the “lsn” keyword, the commands also apply to NAT64/DNS64 and DS-Lite.

Enable Firewall Logging

Binding CGN Service Group to Firewall Template

To bind a CGN service group to a firewall logging template, use the following commands:

```
ACOS(config)# fw template logging fw-log
ACOS(config-logging)# include-radius-attribute imei sessions
ACOS(config-logging)# include-http cookie max-length 110
ACOS(config-logging)# format ascii
ACOS(config-logging)# service-group cgnsg
```

Bind Firewall Logging Template to Firewall

To bind a firewall logging template to the firewall, use the following command:

```
ACOS(config)# fw logging fw-log
```

Configuration Example 2

Create Server Configurations for the Firewall Traffic Log Servers

To create a server configuration for the traffic log server and specify the port on which the server
listens for log traffic, use the following commands:

```
ACOS(config)# fw server fws 15.15.15.90
ACOS((config-real-server)# port 514 udp
ACOS(config-real server-node port)# exit
```

Configure a Firewall Service Group and Its Member

To create a service group for the traffic log servers and to add a traffic log server and its UDP port to the service group, use the following commands.

```
ACOS(config)# fw service-group fwsg udp
ACOS(config-cgnv6 svc group)# member fws 514
ACOS(config-cgnv6 svc group)# exit
```

Enable CGN Logging

Binding Firewall Service Group to CGN Template

To bind a firewall service group to a CGNv6 template, use the following commands:

```
ACOS(config)# cgnv6 template logging lsn_log
ACOS(config-logging:lsn_logging)# log sessions
ACOS(config-logging:lsn_logging)# service-group fwsg
ACOS(config-logging:lsn_logging)# exit
```

The service group is the only required configuration item in external logging templates.

Activate the External CGN Logging Template

To activate the external logging template, use the following command at the global configuration level of the CLI:

```
ACOS(config)# cgnv6 lsn logging default-template lsn_log
```

Enable Firewall Logging

Binding Firewall Service Group to Firewall Template

To bind a CGNv6 service group to a firewall logging template, use the following commands:

```
ACOS(config)# fw template logging fw-log
ACOS(config-logging)# include-radius-attribute imei sessions
ACOS(config-logging)# include-http cookie max-length 110
ACOS(config-logging)# format ascii
ACOS(config-logging)# service-group fwsg
```

Bind Firewall Logging Template to Firewall

To bind a firewall logging template to the firewall, use the following command:

```
ACOS(config)# fw logging fw-log
```

Sample Rule-Set Configuration

```
ACOS(config)# rule-set test
ACOS(config-rule set:test)# rule 2
ACOS(config-rule set:test-rule:2)# action permit cgnv6
ACOS(config-rule set:test-rule:2)# source ipv4-address 3.3.3.0/24
ACOS(config-rule set:test-rule:2)# source zone any
ACOS(config-rule set:test-rule:2)# dest ipv4-address any
ACOS(config-rule set:test-rule:2)# dest zone any
ACOS(config-rule set:test-rule:2)# service object-group alg
ACOS(config-rule set:test)# rule 3
ACOS(config-rule set:test-rule:3)# source ipv4-address 3.3.3.89/32
ACOS(config-rule set:test-rule:3)# source zone any
ACOS(config-rule set:test-rule:3)# dest ipv4-address 15.15.15.90/32
ACOS(config-rule set:test-rule:3)# dest zone any
ACOS(config-rule set:test-rule:3)# service proto-id 47
ACOS(config-rule set:test-rule:3)# action-group
ACOS(config-rule set:test-rule:3-acti...)# permit log cgnv6-logging-
template lsn_log
ACOS(config-rule set:test-rule:3-acti...)# permit log
ACOS(config-rule set:test-rule:3-acti...)# permit cgnv6
ACOS(config-rule set:test)# rule 4
ACOS(config-rule set:test-rule:4)# source ipv4-address 4.4.4.1/32
ACOS(config-rule set:test-rule:4)# source zone any
ACOS(config-rule set:test-rule:4)# dest ipv4-address 25.25.10.1/32
ACOS(config-rule set:test-rule:4)# dest zone any
ACOS(config-rule set:test-rule:4)# action-group
ACOS(config-rule set:test-rule:4-acti...)# deny log fw-logging-template
fw_logging2
ACOS(config-rule set:test)# rule 5
ACOS(config-rule set:test-rule:5)# action permit cgnv6
ACOS(config-rule set:test-rule:5)# source ipv4-address any
ACOS(config-rule set:test-rule:5)# source zone any
ACOS(config-rule set:test-rule:5)# dest ipv4-address any
ACOS(config-rule set:test-rule:5)# dest zone any
ACOS(config-rule set:test-rule:5)#service icmp type dest-unreachable code
port-unreachable
ACOS(config-rule set:test)# rule 6
ACOS(config-rule set:test-rule:6)# source ipv4-address 4.4.4.1/32
ACOS(config-rule set:test-rule:6)# source zone any
ACOS(config-rule set:test-rule:6)# dest ipv4-address 25.25.10.1/32
ACOS(config-rule set:test-rule:6)# dest zone any
ACOS(config-rule set:test-rule:6)# action-group
ACOS(config-rule set:test-rule:6-acti...)# permit log fw-logging-template
fw_logging2
ACOS(config-rule set:test-rule:6-acti...)# permit log fw-logging-template
fw_logging3
ACOS(config-rule set:test)# rule 7
ACOS(config-rule set:test-rule:7)# source ipv4-address any
ACOS(config-rule set:test-rule:7)# source zone any
ACOS(config-rule set:test-rule:7)# dest ipv4-address any
ACOS(config-rule set:test-rule:7)# dest zone any
ACOS(config-rule set:test-rule:7)# action-group
ACOS(config-rule set:test-rule:7-acti...)# permit log
ACOS(config-rule set:test-rule:7-acti...)# permit log netflow-monitor nf1
ACOS(config)# fw active-rule-set test
```

Note:

• In rule 6, two templates are configured and bound. You can configure up to four templates in a rule.

• In rule 7, NetFlow monitor template nf1 is configured and activated. Note that NetFlow monitor templates have global scope by default. You must use scope firewall-rule configuration in the template that is being used in a specific rule.

Sample Firewall Log Messages

Session Open Log

```
May  1 18:06:04 2020 ACOS_Device  CEF:0|A10|ADC|5.2.0-d|FW 100|Session
opened|1|proto=ICMP flexNumber1=8 flexNumber2=0 act=Permit rt=15148529
src=1.0.7.1 dst=192.168.148.106 deviceInboundInterface=ve148
deviceOutboundInterface=ve148 cs1=ti-test cs2=src-threats cs8=client-
threats cs10=mobile-threats cs1Label=Rule Set Name cs2Label=Rule Name
flexNumber1Label=ICMP Type flexNumber2Label=ICMP Code cs8Label=Source
Threat List cs10Label=Source Threat Category
```

Session Close Log

```
May  1 18:11:22 2020 ACOS_Device CEF:0|A10|ADC|5.2.0-d|FW 101|Session
closed|1|proto=ICMP flexNumber1=8 flexNumber2=0 act=Permit rt=15227963
src=1.0.221.131 dst=192.168.148.106 deviceInboundInterface=ve148
deviceOutboundInterface=ve148 cs1=ti-test cs2=src-threats cs8=client-
threats cs10=spam-sources, windows-exploits, scanners cs3=Idle timeout
in=0 out=240 cn1=4 cn2=0 cn3=5 cs1Label=Rule Set Name cs2Label=Rule Name
cs3Label=Reason cn1Label=Packets TX cn2Label=Packets RX cn3Label=Session
Duration Seconds flexNumber1Label=ICMP Type flexNumber2Label=ICMP Code
cs8Label=Source Threat List cs10Label=Source Threat Category
```

Deny Log

```
May  2 01:44:46 2020 ACOS_Device  CEF:0|A10|ADC|5.2.0-d|FW 102|Session
denied|5|proto=ICMP flexNumber1=8 flexNumber2=0 act=Deny rt=22028896
src=1.0.221.131 dst=192.168.148.106 deviceInboundInterface=ve148 cs1=ti-
test cs2=src-threats cs8=client-threats cs10=spam-sources, windows-
exploits, scanners cs1Label=Rule Set Name cs2Label=Rule Name
flexNumber1Label=ICMP Type flexNumber2Label=ICMP Code cs8Label=Source
Threat List cs10Label=Source Threat Category
```

Reset Log

```
May  2 01:50:33 2020 ACOS_Device  CEF:0|A10|ADC|5.2.0-d|FW 103|Session
reset|5|proto=ICMP flexNumber1=8 flexNumber2=0 act=Reset rt=22115649
src=192.168.48.68 dst=1.4.1.110 deviceInboundInterface=ve148 cs1=ti-test
cs2=dst-threats cs9=server-threats cs11=spam-sources cs1Label=Rule Set
Name cs2Label=Rule Name flexNumber1Label=ICMP Type flexNumber2Label=ICMP
Code cs9Label=Dest Threat List cs11Label=Dest Threat Category
```

DDoS Entry Created Log

ASCII Format

```
Syslog message: LOCAL0.INFO:  Nov 12 07:03:27 TH3040-A FW-DDOS-L3-A:
IP=100.1.1.10 PREFIX_LEN=32 RULE=v4 cs6=SHARED MSISDN=999 IMEI=999
IMSI=999
```

CEF Format

```
Syslog message: LOCAL0.INFO:  Nov 12 06:55:39 TH3040-A
CEF:0|A10|CFW|5.2.1-d|FW 131|iDDoS IP entry create|5|src=100.1.1.10
cs12=32 cs2=v4 cs6=SHARED MSISDN=999 IMEI=999 IMSI=999
```

DDoS Entry Deleted Log

ASCII Format

```
Syslog message: LOCAL0.INFO:  Nov 12 07:00:06 TH3040-A FW-DDOS-L3-D:
IP=100.1.1.10 PREFIX_LEN=32 RULE=v4 cs6=SHARED MSISDN=999 IMEI=999
IMSI=999
```

CEF Format

```
Syslog message: LOCAL0.INFO:  Nov 12 06:57:05 TH3040-A
CEF:0|A10|CFW|5.2.1-d|FW 132|iDDoS IP entry delete|5|src=100.1.1.10
cs12=32 cs2=v4 cs6=SHARED MSISDN=999 IMEI=999 IMSI=999
```

Session Limit Exceeded Log

ASCII Format

```
Syslog message: LOCAL0.INFO:  Nov 12 07:09:45 TH3040-A FW-: Concurrent
Session Limit Exceeded  IP=100.1.1.10/32 RULE=v4 LIMIT_EXCEEDED_COUNT=6
PARTITION_NAME=SHARED MSISDN=999 IMEI=999 IMSI=999
```

CEF Format

```
Syslog message: LOCAL0.INFO:  Nov 12 07:07:32 TH3040-A
CEF:0|A10|CFW|5.2.1-d|FW 133|Session Limit Exceeded|5|src=100.1.1.10
cs12=32 cs2=v4 cs13=5 cs6=SHARED MSISDN=999 IMEI=999 IMSI=999
```

Session Periodic Log with Drop Log

CEF format

```
<134> Jul 25 12:35:50 vth  CEF:0|A10|CFW|5.2.1-p5|FW 106|Session periodic
log|5|proto=UDP act=Permit rt=223110 src=20.20.20.141 spt=45678
dst=20.20.101.142 dpt=23456 deviceInboundInterface=ethernet1
deviceOutboundInterface=ethernet2 cs1=rs1 cs2=r1 in=0 out=2040 cn1=34
cn2=0 cn3=70 cn4=15 cn5=900 cn6=0 cn7=0 cs1Label=Rule Set Name
cs2Label=Rule Name cs3Label=Reason cn1Label=Forward packets
cn2Label=Reverse packets cn3Label=Session Duration Seconds
cn4Label=Forward drop packets cn5Label=Forward drop bytes cn6Label=Reverse
drop packets cn7Label=Reverse drop bytes
```

ASCII format

```
<134> Jul 25 12:31:47 vth FW-UDP-P: 20.20.20.141:45678<--
>20.20.101.142:23456 ACT=PERMIT RT=162518 IN-INTF=ethernet1 OUT-
INTF=ethernet2 POLICY=rs1 RULE=r1 FWD_BYTES=4080 REV_BYTES=0 FWD_PKTS=68
REV_PKTS=0 FWD_DROP_BYTES=1920 REV_DROP_BYTES=0 FWD_DROP_PKTS=32 REV_DROP_
PKTS=0 DUR=140
```

Session Created Log with Custom Message

The following CGNv6 syslog shows custom message or notice with fields such as proto and rule name.

```
21:50:25.954058 IP 1.0.4.1.syslog > 1.0.4.147.syslog: [|syslog]
E..c....@..d.............OW.Notice: Creating session proto=UDP rule
name=r1 [- 1.0.3.148 1.0.4.147]
21:50:25.970014 IP 1.0.4.1.syslog > 1.0.4.147.syslog: [|syslog]
E..cV...@..e.............OW.Notice: Creating session proto=UDP rule
name=r1 [- 1.0.3.148 1.0.4.147]
21:51:41.970107 IP 1.0.4.1.syslog > 1.0.4.147.syslog: [|syslog]
E.......@................|)MNotice: Deleting session which started at
20220825144642: client IP=1.0.3.148, session duration=313967, rule name=r1
21:51:44.822327 IP 1.0.4.1.afrog > 1.0.4.147.syslog: [|syslog]
E.. .e@.@.T..............}.A10.
21:51:50.030944 IP 1.0.4.1.afrog > 1.0.4.147.syslog: [|syslog]
E.. .
@.@.Q/..............}.A10.
21:51:54.950903 IP 1.0.4.1.afrog > 1.0.4.147.syslog: [|syslog]
E.. ..@.@.P..............}.A10.
21:51:59.958828 IP 1.0.4.1.afrog > 1.0.4.147.syslog: [|syslog]
E.. .I@.@.O..............}.A10.
21:52:04.883109 IP 1.0.4.1.boinc-client > 1.0.4.147.syslog: [|syslog]
E.. ..@.@.O].............}.A10.
21:52:10.082892 IP 1.0.4.1.boinc-client > 1.0.4.147.syslog: [|syslog]
E.. .f@.@.J..............}.A10.
21:52:13.954081 IP 1.0.4.1.syslog > 1.0.4.147.syslog: [|syslog]
E.......@.^..............|)ZNotice: Deleting session which started at
20220825144641: client IP=1.0.3.148, session duration=348011, rule name=r1
```

RADIUS Logging

When a firewall rule-set configured with firewall logging is being applied to a rule, log messages are generated whenever a session is created, destroyed, or denied. This rule controls what type of traffic is allowed to enter the firewall, and which traffic will be denied. While sending firewall logs, RADIUS attributes can be added to the firewall log messages.

ACOS is configured to act as a RADIUS server so that it can receive RADIUS accounting requests that include the client RADIUS attributes.

When client’s AAA server sends out RADIUS accounting packet that has the Framed IP and (/or) Framed IPv6 Prefix to ACOS, ACOS intercepts the packet, creates a RADIUS table entry based on the IP and IPv6 Prefix. When the inside user creates a data connection either from the IP or from IPv6 address (from the prefix), ACOS then includes the RADIUS attributes while sending the log messages.

The ACOS device acts as a RADIUS server. ACOS acts as a RADIUS server intercepting RADIUS accounting request messages sent to the Interface / Floating IPs configured on ACOS. To create a RADIUS server configuration for Firewall deployment, use the **`fw radius server`** command.

When configuring the Firewall RADIUS server or CGNV6 RADIUS server, use the **`framed-ipv6-prefix`** command to specify the Framed IPv6 Prefix as a RADIUS attribute for RADIUS accounting requests. The following combination are possible in a RADIUS packet:

- Framed IPv4 address and Framed IPv6 prefix — ACOS accepts the packet and creates the RADIUS entries based on the IPv4 address and the IPv6 prefix.
- Framed IPv4 address and Framed IPv6 address — ACOS accepts the packet and create the RADIUS entries based on the IPv4 address and the IPv6 address.
- Framed IPv6 address and Framed IPv6 prefix — ACOS accepts the packet and creates 1 record with ipv6 address.
- Framed IPv6 address and Framed IPv6 prefix are present.

The Framed IPv6 prefix attribute in the RADIUS packet contains the prefix with the configured prefix length. When the configured prefix length on the RADIUS server does not match with the incoming prefix length, then the packet will be dropped.

When the prefix length is changed in the RADIUS server, the existing RADIUS table must be explicitly cleared.

NOTE: The value of the Framed IPv6 Prefix is configurable. If the configured prefix is changed, the RADIUS table must be explicitly cleared to remove the previously learned RADIUS table entries.

NOTE: ACOS accepts the RADIUS accounting packets only when the packet is destined to the ACOS Interface IP or Floating IP.

RADIUS support is available with the following topologies:

- FW only scenarios
- CGN and Firewall scenarios
- L3Vs

Firewall Only Partition

The following commands configure the RADIUS attributes in FW only partition:

1. These command creates an ip-list to be used by other FW commands. The IPs associated to the ip-list are the ones of which RADIUS packets will be accepted.

```
ACOS(config)# ip-list client
ACOS(config-ip-list)# 5.5.5.100
ACOS(config-ip-list)# exit
```

2. These commands create a RADIUS server configuration and specify the RADIUS attributes for ACOS to receive from external RADIUS servers in response to RADIUS Accounting requests:

```
ACOS(config)# fw radius server
ACOS(config-radius-server)# remote ip-list client
ACOS(config-radius-server)# secret a10
ACOS(config-radius-server)# attribute inside-ip number 8
ACOS(config-radius-server)# attribute msisdn number 31
ACOS(config-radius-server)# attribute imei vendor 10415 number 20
ACOS(config-radius-server)# attribute imsi vendor 10415 number 1
ACOS(config-radius-server)# attribute custom1 NAS-IP-Address value hexadecimal number 4
ACOS(config-radius-server)# attribute custom2 Connection_PVC vendor 22610 number 43
ACOS(config-radius-server)# attribute custom3 xDSL_number vendor 22610 number 44
ACOS(config-radius-server)# attribute inside-ipv6-prefix prefix-length 64 number 97
ACOS(config-radius-server)# attribute inside-ipv6 vendor 22610 number
29
ACOS(config-radius-server)# accounting start replace-entry
ACOS(config-radius-server)# accounting stop delete-entry-and-sessions
ACOS(config-radius-server)# accounting interim-update replace-entry
```

3. These commands configure a firewall logging template:

```
ACOS(config)# fw template logging fw-log
ACOS(config-logging)# include-radius-attribute framed-ipv6-prefix
prefix-length 64
ACOS(config-logging)# include-radius-attribute msisdn [http-
requests|sessions|limit-policy]
ACOS(config-logging)# include-radius-attribute imei [http-
requests|sessions|limit-policy]
ACOS(config-logging)# include-radius-attribute imsi [http-
requests|sessions|limit-policy]
ACOS(config-logging)# include-radius-attribute custom2 [http-
requests|sessions|limit-policy]
ACOS(config-logging)# include-radius-attribute custom1 [http-
requests|sessions|limit-policy]
ACOS(config-logging)# format ascii
```

4. These commands configure a firewall rule-set:

```
ACOS(config)# rule-set 1
ACOS(config-rule set:1)# rule 1
ACOS(config-rule set:1-rule:1)# action permit log
ACOS(config-rule set:1-rule:1)# source ipv4-address 5.5.5.100/32
ACOS(config-rule set:1-rule:1)# source zone any
ACOS(config-rule set:1-rule:1)# dest ipv4-address 6.6.6.100/32
ACOS(config-rule set:1-rule:1)# dest ipv4-address 6.6.6.101/32
ACOS(config-rule set:1-rule:1)# service any
```

5. This command activates the firewall function using the specified rule-set:

```
ACOS(config)# fw active-rule-set 1
```

CGN and Firewall Partition

The following commands configure the RADIUS attributes in CGN and FW partition.

1. Enter the following command to create an IP list for client RADIUS servers:

```
ACOS(config)# ip-list RADIUS_IP_LIST
ACOS(config-ip list)# 40.40.40.1 to 40.40.40.2
ACOS(config-ip list)# exit
```

2. The following commands configure RADIUS server parameters for ACOS:

```
ACOS(config)# cgnv6 lsn radius server
ACOS(config-lsn radius)# remote ip-list RADIUS_IP_LIST
ACOS(config-lsn radius)# listen-port 1813
ACOS(config-lsn radius)# attribute inside-ip number 8
ACOS(config-lsn radius)# secret a10
ACOS(config-radius-server)# attribute inside-ip number 8
ACOS(config-radius-server)# attribute msisdn number 31
ACOS(config-radius-server)# attribute imei vendor 10415 number 20
ACOS(config-radius-server)# attribute imsi vendor 10415 number 1
ACOS(config-radius-server)# attribute custom1 NAS-IP-Address value
hexadecimal number 4
ACOS(config-radius-server)# attribute custom2 Connection_PVC vendor
22610 number 43
ACOS(config-radius-server)# attribute custom3 xDSL_number vendor 22610
number 44
ACOS(config-radius-server)# attribute inside-ipv6-prefix prefix-length
64 number 97
ACOS(config-radius-server)# attribute inside-ipv6 vendor 22610 number
29
ACOS(config-radius-server)# accounting start replace-entry
ACOS(config-radius-server)# accounting stop delete-entry-and-sessions
ACOS(config-radius-server)# accounting interim-update replace-entry
```

3. The following commands configure a logging template:

```
ACOS(config)# cgnv6 template logging log
ACOS(config-logging:log)# log http-requests url
ACOS(config-logging:log)# log sessions
ACOS(config-logging:log)# include-radius-attribute msisdn [http-
requests|sessions|limit-policy]
ACOS(config-logging:log)# include-radius-attribute imei [http-
requests|sessions|limit-policy]
```

```
ACOS(config-logging:log)# include-radius-attribute imsi [http-
requests|sessions|limit-policy]
ACOS(config-logging:log)# include-radius-attribute custom1 [http-
requests|sessions|limit-policy]
ACOS(config-logging:log)# include-radius-attribute custom2 [http-
requests|sessions|limit-policy]
ACOS(config-logging:log)# include-radius-attribute custom3 [http-
requests|sessions|limit-policy]
ACOS(config-logging:log)# include-radius-attribute framed-ipv6-prefix
prefix-length 64
ACOS(config-logging:log)# include-http referer
ACOS(config-logging:log)# include-http user-agent
ACOS(config-logging:log)# include-http header1 GET
ACOS(config-logging:log)# include-http l4-session-info
ACOS(config-logging:log)# include-http method
ACOS(config-logging:log)# include-http request-number
ACOS(config-logging:log)# include-http file-extension
ACOS(config-logging:log)# rule http-requests dest-port 80
ACOS(config-logging:log)# rule http-requests log-every-http-request
ACOS(config-logging:log)# rule http-requests max-url-len 200
ACOS(config-logging:log)# rule http-requests include-all-headers
ACOS(config-logging:log)# rule http-requests disable-sequence-check
ACOS(config-logging:log)# batched-logging-disable
ACOS(config-logging:log)# service-group cgn-log-group
```

ACOS Event-based Logging

This section describes how to configure event-based logging.

The following topics are covered:

NOTE: For a general discussion of firewall logging, see Firewall Logging.

Overview

ACOS provides the support for firewall event logs to be sent over the ACOS event-based logging infrastructure. This provides a centralized logging infrastructure that allows applications to generate and send logs through a common interface.

As with prior releases, the ACOS firewall will continue to send logs to an external Syslog server in both CEF and ASCII format. However, the format of the new log messages under the new ACOS event logging infrastructure will be slightly different from the format of the log messages in prior releases.

Changes to the format of CEF logs

- No year appears in the timestamp.
- Signature is followed by event.
- The order of extension fields is different.
- Custom fields are always followed by their label fields.

Changes to the format of ASCII logs

- “a10logd: [ACOS]” is followed by the header field.
- The order of the fields is different.

Despite these changes, the new firewall logs will convey information that is equivalent to the old firewall logs.

Event Log Triggers

If firewall traffic matches a rule and that rule has the “log” option enabled under actions, then certain events will trigger the firewall to send an event log through the new ACOS event logging infrastructure. The following events can trigger an event log to be sent:

- **Open event:** When traffic matches a permit rule and a session is created.
- **Close event:** When a session is closed or deleted.
- **Deny event:** When traffic matches a deny rule.
- **Reset event:** When traffic matches a reset rule.

Messages can also be filtered based on their severity. By specifying the "message-id" one can determine which types of logs (session-opened, closed, denied, or reset) will be sent to the remote server.

The syntax below can be used for filtering messages based on their severity.

```
ACOS(config)# acos-events message-selector FW
ACOS(config-msg-selector:FW)#rule 4
ACOS(config-msg-selector:FW-rule:4)#message-id fw all severity equal ?
  emergency      System unusable log messages (Most Important)
  alert          Action must be taken immediately
  critical       Critical conditions
  error          Error conditions
  warning        Warning conditions
  notification   Normal but significant conditions
  information    Informational messages
  debugging      Debug level messages (Least Important)
```

Details:

- To select open/close messages, select **`information`**
- To select deny/reset messages, select **`critical`**

If the severity level is equal and higher, then all messages equal to that severity level (and higher) would be logged. For example, selecting `information` would include all messages with a severity level equal to or greater than this level, and only `debugging` messages would not be excluded.

Differences Between the Firewall Logging and Event-based Logging

Many of the old names, extensions, and events available in Firewall Logging are preserved in the migration to ACOS Event Logging. Some fields have been moved, appear in a different order in the log message, or have been renamed.

- CEF Logging Under ACOS Event Logging
- ASCII Logging Under ACOS Event Logging

NOTE: Labels for custom fields such as `cn1Label` and `cs1Label` will appear in the log only if relevant custom fields are present.

CEF Logging Under ACOS Event Logging

The following table shows the ACOS Event Logging extension fields in CEF format log messages.

Table 30 : : CEF extension fields in new ACOS Event Logging

Name	Events	Description
proto	All	Protocol
act	All	Firewall action
rt	All	Timestamp
app	All	Application protocol (if available)
src	All	Source IPv4 address
dst	All	Destination IPv4 address
c6a2	All	Source IPv6 address
c6a3	All	Destination IPv6 address
spt	All	Source port (if proto is either “TCP” or “UDP”)
dpt	All	Destination port (if proto is either “TCP” or “UDP”)
flexNumber1	All	ICMP type (if proto is either “ICMP” or “ICMPv6”)

Table 30 : : CEF extension fields in new ACOS Event Logging

flexNumber2	All	ICMP code (if proto is either “ICMP” or “ICMPv6”)
deviceInboundInterface	All	Inbound interface (if available)
deviceOutboundInterface	All	Outbound interface (if available)
cs1	All	Rule-set name
cs2	All	Rule name
cs3	Close	Reason
cs4	All	Source zone (if available)
cs5	All	Destination zone (if available)0
cs6	All	Partition name (if logged by L3V partition)
cs7	All	Application category (if available)
cs8	All	Source Threat List
cs9	All	Destination Threat List
cs10	All	Source Threat Category
cs11	All	Destination Threat Category
out	Close	Forward bytes
in	Close	Reverse bytes
cn1	Close	Forward packets
cn2	Close	Reverse packets
cn3	Close	Session duration in seconds

Differences from Existing External CEF Logs

Compared to existing external CEF logs, some of log fields are different. An example is provided below for a close event.

CEF Log with Firewall Logging (old)

```
Aug  5 10:52:50 2018 ACOS_Device CEF:0|A10|CFW|4.1.4-P2|FW 101|Session
closed|1|proto=UDP act=Permit rt=1828472 app=dns src=40.40.40.213
spt=37242 dst=20.20.20.104 dpt=53 deviceInboundInterface=ethernet7
cs4=client deviceOutboundInterface=ethernet8 cs5=server cs1=fw cs2=dns
cs7=networking, standards-based cs3=Normal in=86 out=70 cn1=1 cn2=1 cn3=2
cs1Label=Rule Set Name cs2Label=Rule Name cs3Label=Reason cn1Label=Packets
TX cn2Label=Packets RX cn3Label=Session Duration Seconds cs4Label=Source
Zone cs5Label=Dest Zone cs7Label=Application Category
```

CEF Log with ACOS Event (new)

```
Aug  5 10:52:50 ACOS_Device CEF: 0|A10|CFW|4.1.4-P2|FW 101
6260003482044989551|Session closed|2|proto=UDP act=Permit rt=1828472
app=dns src=40.40.40.213 spt=37242 dst=20.20.20.104 dpt=53
deviceInboundInterface=ethernet7 deviceOutboundInterface=ethernet8 in=86
out=140174847639622 cn1=1 cn1Label=Packets TX cn2=1 cn2Label=Packets RX
cn3=2 cn3Label=Session Duration Seconds cs1=fw cs1Label=Rule Set Name
cs2=dns cs2Label=Rule Name cs3=Normal cs3Label=Reason cs4=client
cs4Label=Source Zone cs5=server cs5Label=Dest Zone cs7=networking,
standards-based cs7Label=Application Category
```

ASCII Logging Under ACOS Event Logging

The following table shows the ACOS Event Logging extension fields in ASCII format log messages.

Table 31 : : ASCII extension fields in new ACOS Event Logging

Key	Events	Description
ACT	All	Firewall action in upper case
RT	All	Timestamp
POLICY	All	Rule-set name
RULE	All	Rule name
IN-INTF	All	Inbound interface (if available)
OUT-INTF	All	Outbound interface (if available)
IN-ZN	All	Source zone (if available)
OUT-ZN	All	Destination zone (if available)
APP	All	Application protocol (if available)

Table 31 : : ASCII extension fields in new ACOS Event Logging

APP-CAT	All	Application category (if available)
FWD_BYTES	Close	Forward bytes
REV_BYTES	Close	Reverse bytes
FWD_PKTS	Close	Forward packets
REV_PKTS	Close	Reverse packets
DUR	Close	Session duration in seconds
SRC-THR-LST	All	Source Threat List
DST-THR-LST	All	Destination Threat List
SRC-THR-CAT	All	Source Threat Category
DST-THR-CAT	All	Destination Threat Category

Differences from Existing External ASCII Logs

Compared to existing external ASCII logs, some of log fields are different. An example is provided below for a close event.

ASCII Log with Firewall Logging (old)

```
Aug  5 11:00:41 ACOS_Device FW-UDP-H: 40.40.40.213:41147<--
>20.20.20.104:53 ACT=PERMIT RT=1946243 APP=dns IN-INTF=ethernet7 IN-
ZN=client OUT-INTF=ethernet8 OUT-ZN=server POLICY=fw RULE=dns APP-
CAT=networking, standards-based FWD_BYTES=70 REV_BYTES=86 FWD_PKTS=1 REV_
PKTS=1 DUR=2#015
```

ASCII Log with ACOS Event (new)

```
Aug  5 11:00:41 ACOS_Device a10logd: [ACOS]<6> FW-UDP-H:
40.40.40.213:41147<-->20.20.20.104:53 ACT=PERMIT RT=1946243 POLICY=fw
RULE=dns IN-INTF=ethernet7 OUT-INTF=ethernet8 IN-ZN=client OUT-ZN=server
APP=dns APP-CAT=networking, standards-based FWD_BYTES=70 REV_BYTES=86 FWD_
PKTS=1 REV_PKTS=1 DUR=2
```

Details:

- CEF format is the default for FW logging.
- ASCII format is the default for the new “ACOS Event-based Logging”. However, in the CLI, this option is called “syslog” and does not appear as “ascii”.

Configuring ACOS Event-based Logging

Migrating from “Firewall Logging” to “ACOS Event-based Logging” does not happen automatically upon upgrading. The following configurations are necessary:

1. Configure the acos-events message-selector and add a message-id under the rule configuration:

   ```
   ACOS(config)# acos-events message-selector MS1
   ACOS(config-msg-selector:MS1)# rule 1
   ACOS(config-msg-selector:MS1-rule:1)# message-id fw all
   ACOS(config-msg-selector:MS1-rule:1)# exit
   ```

2. Configure the acos-events log server and bind it to UDP port 514:

   ```
   ACOS(config)# acos-events log-server SYSLOG1 20.20.20.20
   ACOS(config-log-server)# port 514 udp
   ACOS(config-log-server-logging port)# exit
   ```

3. Configure the acos-events collector-group for CEF format and for ASCII format. The collector-group is similar to a service group. Add the log server to both collector groups:

   ```
   ACOS(config)# acos-events collector-group CG-ASC udp
   ACOS(config-collector-group:CG-ASC)# log-server SYSLOG1 514
   ACOS(config-collector-group:CG-ASC)# exit
   ACOS(config)# acos-events collector-group CG-CEF udp
   ACOS(config-collector-group:CG-CEF)# format cef
   ACOS(config-collector-group:CG-CEF)# log-server SYSLOG1 514
   ACOS(config-collector-group:CG-CEF)# exit
   ```

4. Create an acos-events template and bind the message-selector to the ASCII collector group:

   ```
   ACOS(config)# acos-events template FWLOG-ASC
   ACOS(config-template:FWLOG-ASC)# message-selector MS1 collector-group
   CG-ASC
   ACOS(config-template:FWLOG-ASC)# exit
   ```

5. Create an acos-events template and bind the message-selector to the CEF collector group:

   ```
   ACOS(config)#acos-events template FWLOG-CEF
   ```

```
ACOS(config-template:FWLOG-CEF)#message-selector MS1 collector-group
CG-CEF
ACOS(config-template:FWLOG-CEF)#exit
```

6. Activate the acos-events template:

```
ACOS(config)#active-template FWLOG-ASC
ACOS(config)#active-template FWLOG-CEF
```

For more information, see the **`acos-events`** command in the *Command Line Reference Guide*.

Firewall Statistics

The ACOS firewall tracks the number of hits for each rule, as well as the number of requests that are implicitly denied, due to not matching the criteria in any of the rules within a rule-set.

You can display this information using the **`show rule-set`** command (for Access Control rule-set) or **`show traffic-control rule-set`** command (for Traffic Control rule-set). For information about using this command, see the **Firewall clear and show commands** in the *Command Line Reference Guide*.

Harmony Controller Configuration for Firewall

Firewall per connection system logs are sent to the Harmony Controller.

Per connection logs are generated upon session open or closed events for permit rule and deny or reset events. If data traffic matches a rule with action permit log, per connection logs are sent out when the session is opened and closed. This is sent out to Harmony Controller for visibility.

NOTE: If Application Aware Firewall is enabled:
– Sending PC logs will be delayed until application classification is done.
– Fields for application protocol and category can be empty if a session is closed before application classification is done.

The HC configuration mode on ACOS configures the option to collect ACOS data metrics to HarmonyTM Controller through ACOS CLI.

For further information on CLI and HC configuration on ACOS, refer to *Harmony^{TM} Controller Integration Guide*.

Troubleshooting Firewall Deployment

This section covers the following troubleshooting scenarios.

The following topics are covered:

IPv4 packets are getting dropped

If this issue occurs, use the following approaches to diagnose and correct:

- Enable “debug fw” and search the output for DENY or UNMATCHED DENY, as shown in the samples below:

```
@134537 [DCFW] TCP 2.2.2.1:56275->3.3.3.1:80 fw_policy_action_fast_path
policy match my-rule-set rule-port80-drop rule ID=1 action=DENY
TCP 3.3.3.8:60803->3.3.3.1:80 fw_policy_action_fast_path UNMATCHED DENY
```

- For traffic on non-default ALG ports, check to see if the ALG flag has been configured for that rule. For example:

```
service tcp src eq 2121 dst eq 2121 alg FTP
```

- For TCP, check if the session still exists, using the “show sessions” command.

  TCP sessions may get deleted because of “force-delete-timeout” configuration in the firewall session aging-template.

TCP window check issues

- If the packet is getting dropped after being permitted, use the **show counters** command shown below to check if the packet was dropped due to TCP Window checks. For example:

```
firewall-Active(config)# show counters fw tcp-window-check
packet dropped for outside of tcp window          327719254
```

- Enable “debug fw” and check for any logs indicating that the drops were due to firewall TCP window checks. For example:

```
“DROP REV nseq=453D86F, wsize=7D78, plen=1B, seq=434A97D”
```

IPv6 packets are getting dropped

- If IPv6 packets are being dropped, check that “ip-version v6” is configured under the rule that is intended to match.

- IPv6 neighbor discovery packets are dropped by the firewall, unless there is a rule to permit such traffic:
    - Since neighbor discovery does not happen, end-to-end traffic never flows.
    - One method of permitting such traffic to flow is to add a rule explicitly permitting ICMPv6 types/codes pertaining to neighbor discovery/router solicitation messages. For example:

```
rule permit-v6-neigh-disc
  action permit
  ip-version v6
  source ipv6-address any
  source zone any
  dest ipv6-address any
  dest zone any
  service object-group ipv6-neigh-disc
  object-group service ipv6-neigh-disc
  icmpv6 type 133
  icmpv6 type 134
  icmpv6 type 135
  icmpv6 type 136
  icmpv6 type 137
```

Rule-set changes were not applied

- It takes up to10 seconds for rule-set changes to take effect.
    - Use the **`fw apply-changes`** command to make rule-set changes take effect immediately.
- New rule-set changes do not apply to already existing sessions.

  Use the **`clear sessions`** command to clear out any existing sessions.
- Firewall rule-set compilation might have failed.

  Use the **`show fw status`** command to check for rule-set compilation status.
- A rule might be disabled or the rule-set may not be active.

  - Check the rule-set configuration to see if the rule is disabled, and make sure that rule-set is active.

VRRP-A does not work with firewall enabled

- A rule in active rule-set might be denying VRRP-A packets
  - Enable **`debug fw`** and look for DENY in the logs.
- Firewall internal rule-set compilation may have failed.
  - Use the **`show fw status internal`** command to check for internal rule-set compilation status.
- Check if the firewall is part of the correct vrid.
- Check if internal rules are installed using the “devcall dump_fw_rules(0, 1)”. For example:

```
Total rules 2
Rule vrrpa_ipv4_hello_mcast idx 0 id 1 permit udp (proto-id 17) dst
224.0.0.210 /32 src_port 65244 - 65244 dst_port 65244 - 65244 hits 0
Rule vrrpa_ipv6_hello_mcast idx 0 id 2 permit udp (proto-id 17) dst
ff02::d2/128 src_port 65244 - 65244 dst_port 65244 - 65244 hits 0
```

ALG does not work

- ALG data sessions are not getting created
  - Check if any rules in the rule-set are getting applied.
  - Enable **`debug fw`** and look for DENY in the logs.
  - You can bypass the rule-set lookup for data sessions by configuring **`fw alg-processing override-rule-set`**.
- ALGs are not supported in Layer 2 setups.
  - If clients and servers are in same subnet and the firewall is switching packets (as opposed to routing), ALG data sessions will not be created.

Other miscellaneous issues

- Firewall CLI commands are absent or have disappeared.
  - DCFW is part of CFW product.
  - Check the output from the **`show license-info`** command for a valid CFW license.
- The syslog server is not displaying any logs:
  - Ensure that the **`action`** under a rule has the “log” keyword.
  - Ensure that the syslog server is reachable through the data ports.
- Firewall CLI commands are rejected with an error: “Periodic compilation in progress, please try after some time.”
  - When rule-set compilation is in progress in a given partition, any further firewall CLI commands that change rules are blocked.
  - Wait for the rule-set compilation to finish. Then, check the output of **`show log`** for the following message:

    ```
    [Firewall]:Rule-set “my-rule-set" in partition "shared" successfully
    compiled at 2016-05-17 20:59:17.
    ```

Contact Us