ACOS Security Hardening Guide

v2.0.0

June, 2025

Information in this document is subject to change without notice.

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

Introduction

This document contains information and recommendations to help you harden and secure your A10 ACOS systems, which will improve security in your networks and ACOS deployments. This information describes recommended security practices for hardening your ACOS systems that should be considered and applied in accordance with your organization's security policy.

NOTE: This document is not intended to be a tutorial on the general use and configuration of ACOS systems or how to best utilize and take advantage of security-related features and services of these systems. For information on features and services, see the ACOS product documentation

Networking System Planes

ACOS hardening is addressed for three different planes inherent in contemporary networking systems.

1. Management Plane – Supports functions used to control and administer the ACOS system with applications such as Command Line Interface (CLI), web-based management GUI (Web/GUI), logging, and Authentication/Authorization/Accounting (AAA). These functions use commonly known protocols such as Secure Shell (SSH), SNMP, HTTP/HTTPS, Syslog, RADIUS, TACACS+, LDAPS, and others.
2. Control Plane – Supports functions used between networking devices such as the Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Intermediate System to Intermediate System (IS-IS), Bidirectional Forwarding Protocol (BFD), and others.
3. Data Plane – Supports functions that operate on data passing through the ACOS systems and between the ACOS system and interior managed service systems. These include functions such as:

- Application Delivery services (e.g. load balancing, server health monitoring, packet inspection/transformation, white/black lists, etc.)
- Application Acceleration services (e.g. HTTP Acceleration/Caching, SSL/TLS Offloading, SSL/TLS Proxy, etc.)
- Application Security services (e.g. SSL/TLS Intercept (SSLi), Web-Application Firewall (WAF), Application Access Management (AAM), Single Sign-On (SSO), bandwidth limiting, connection/rate limiting, etc.)
- Distributed Denial of Service (DDOS) services (e.g. Detection, Mitigation, & Cloud Protection)
- IPv6 Migration/IPv4 preservation (e.g. Carrier Grade NAT (CGN/CGNAT), NAT64/DNS64, DS-Lite, 6rd, LW4o6, etc.)

Hardening considerations are presented, in turn, for each of the planes in the subsequent chapters of this document.

Scope

This document addresses hardening factors for Thunder ACOS releases 6.0.5 and later.

Configuration examples presented in this document are provided for the ACOS CLI. Corresponding ACOS Web/GUI and aXAPI operations are available and described in the ACOS product documentation.

Configuration examples presented are provided for IPv4 addressing only. For IPv6 equivalents, see the ACOS product documentation.

On occasions where the contents of this document conflicts or are inconsistent with the ACOS product documentation, the ACOS documentation should be considered as the defining reference.

Conventions

The following conventions are used in the content and prose of discussions for this document:

- Underline indicates emphasis.
- *Italics* indicates references to specific documents in the ACOS product documentation.
- *Blue Italics Underline* indicates a click-able link to another location in this document.
- Blue Normal Underline indicates a click-able hyperlink to an internet accessible web page.
- `Courier font` indicates ACOS CLI command or parameter.

CLI Examples

ACOS CLI examples presented in this document shown as `single-indented, Courier New font`, for input commands and parameter, as well as displayed output content. For example:

```
// HTTPS, gmt.. port already enabled
// Create Mgmt I/F ACL 100 for ACOS gmt.. port (incl HTTPS, gmt.. port
rules).
//    - ACL 10 will be an overall ACL for the ACOS gmt.. port
//
ACOS-TH####(config)#access-list 100 1 remark "ACL – gmt. port @ HTTPS"
ACOS-TH####(config)#access-list 100 2 permit tcp 10.10.10.0 /24 any eq 443

ACOS-TH####(config)#enable-management service acl-v4 100
ACOS-TH####(config-enable-management acl-v4)#management
```

Additional conventions used in CLI examples include:

- Lines starting with `ACOS-TH####` indicate CLI command inputs.
- **`Bold`** indicates ACOS CLI commands and their parameters.
- `Text` indicates CLI command options that the user must enter or select.
- **`exit`** command to complete input at a given configuration level are not indicated, for readability.
- Lines starting with `//` are comments included in the example for the purpose of

this document. If entered at CLI prompt, an ACOS error message will be displayed.

- Command contents between <<< and >>> indicate references to earlier examples.

Notes

The following conventions are used for notation call outs in this document:

NOTE: Notes are represented like this and contain technical information the reader should take note of, providing important additional information to the prior discussion or example content.

CAUTION: Notes are represented like this and contain information the reader should take note of regarding scope and presentation in the remainder of the document.

SECURITY NOTE: Even though this document is focused on hardening and security overall, notes like this contain information and perspective that is particularly important for the reader to take note of.

Documentation

ACOS product documentation can be found in the *SOFTWARE AND DOCUMENTATION* section of the A10 Support Portal.

Download the Latest ACOS Software

To ensure systems are protected against the latest security vulnerabilities, download the most recent ACOS software update images from the A10 Support Portal. Regular updates include critical remediations and corrections addressing security risks.

For information on vulnerability exposures and resolved ACOS releases see the Security Advisories on the A10 Product Security Incident Response Team (PSIRT) webpage, accessible through A10 Networks website.

SECURITY NOTE: A majority of vulnerabilities in networked systems are due to the outdated software, even when updates are readily available. Exposures to vulnerabilities grow significantly the longer systems remain unpatched or outdated. ACOS software updates play a key role in mitigating these risks by addressing sources of compromise in A10 systems.

It is strongly recommended that ACOS administrators put programs in place to maintain and keep the ACOS systems up to date, especially for deployed and production configurations. For information on available versions and updates, contact an A10 Sales Engineer or the A10 Technical Assistance Center (TAC)

Hardening the ACOS Management Plane

This chapter addresses hardening considerations of the ACOS management plane whose functions support management and device administration of the ACOS System. These functions include:

- Interactive management and administration of the system.
- Connections to management services (e.g. NTP, Syslog, external authentication services).
- Support for management data gathering services (e.g. SNMP, NetFlow).
- Programmatic management services (e.g. RESTful aXAPI, External Health Monitor, aFlex).

It is critical that the ACOS management plane is protected and is used within the boundaries of acceptable practices by trusted administrators with access from trusted management systems to ensure the availability and stability of the ACOS system. It is recommended to isolate the management network from data and control networks.

Password and User Management

Passwords control administrative access to the ACOS systems as well as configuration resources and key services of ACOS. More secure environments will manage passwords and users through RADIUS, TACACS+, or LDAPS external authentication servers. Certainly, users and their passwords can also be configured locally in ACOS for conditions when external services are not available or have failed.

It is important to consider that when external authentication configurations become unavailable that access to the ACOS device is not ultimately blocked or unavailable. To this end it can be important for availability of the ACOS system to have locally configured users, beyond just the ACOS root admin, that can manage the ACOS system on these occasions.

The following subsections share hardening recommendations for configuring passwords, locally configured administrators, and assigning access privileges.

Default Password Policy

ACOS cannot control or enforce your policy for passwords when they are managed by RADIUS, TACACS+, or LDAPS services external to ACOS. Various password practices are outlined below. A10 recommends using strict password policy rather than the default policy for passwords locally configured on the ACOS system. ACOS provides the ability to customize password policies to your organization's needs; however, the default password policy is intended to provide acceptable security for most. If default password policy is used, A10 recommends setting a password age and history to enforce password change. For external authentication services, A10 recommends applying a consistent password policy as with local authentication.

The default password policy has the following criteria:

- The password should be at least nine characters in length.
- The password should contain at least one number, an uppercase letter (English), a lowercase letter (English), and a special character.
- The password should not contain its corresponding username with the same capitalization of letters.
- The password should not have consecutive repeated letter or number.
- The password should not contain the sequential row keyboard input of four letters or numbers with the same capitalization of letters.
- The password should have at least one letter or number different from the previous password.

Examples:

- asdf$98ujkY (This password contains 4 consecutive characters on keyboard)
- admin@A10Pw (This password contains username)
- a10$Password (This password contains repeat letters "ss")
- a10$PasSword (This password is accepted)

ACOS versions prior to 6.0.0 do not have this default password policy. When older ACOS versions are upgraded to ACOS 6.0.0, the default password policies must be enabled manually, or a system reset must be executed to enable the default password policy to take effect.

To enable the enhanced password policy when upgrading from a ACOS version prior to 6.0.0 without issuing a system reset, use the following commands:

```
system password-policy complexity Default username-check enable
system password-policy complexity Default forbid-consecutive-character 4
system password-policy complexity Default repeat-character-check enable
```

A10 recommends applying these configurations after upgrading from an ACOS version prior to 6.0.0.

For more information, see ACOS Management Access and Security Guide.

Password Policy for Privileged Mode

Privileged mode is used to configure the device. This mode is entered by typing ‘enable’ after logging in via the command line. The password to enter privileged mode is referred to as ‘enable password.’ By default, the configured password policy doesn’t apply to the ‘enable password.’

To enable password policy, execute the following command:

```
system enable-password follow-password-policy
```

A10 recommends applying these configurations after upgrading from an ACOS version prior to 6.0.0.

Change the ACOS Default Admin Password

By default, ACOS is provisioned with one administrator account named “admin” and one partition named “shared.” This default admin account, also referred to as the root admin account, is the master administrator of the ACOS system and has root access to ACOS. Root access means that “admin” has read-write privileges to all ACOS objects across all partitions.

Upon first login, the root admin is required to change the default “a10” password to a strong user-defined password defined by a predefined default password policy mentioned above. For ACOS versions prior to 6.0.0 that upgrade to 6.0.0, the admin is not required to change the default password if enhanced password policy is not enabled, and system reset is not performed but is strongly recommended to change the admin password. For example:

```
ACOS-TH####(config)#admin admin password
Password: <type your password>
Retype password: <type your password again>
```

In addition, it is recommended to periodically change the enable password based on the password age policy.

Change the ACOS Default Enable Password

When users log into the CLI, the initial User EXEC level of access provides a very limited set of management operations. These include showing (viewing) the status or configuration information of the system, initiating SSH or Telnet terminal sessions to remote systems, performing management connectivity operations (e.g. ping, traceroute, test a device’s health status), and entering the Privileged EXEC level.

The Privileged EXEC level of the CLI allows users to change or modify the ACOS system configuration and can be entered via the global password-protected enable command. By default, this password that is empty (e.g. just press Enter at the password prompt).

It is strongly recommended to change this default to a strong user-defined password. For example:

```
ACOS-TH####(config)#enable-password
Password: <type your password>
Retype password: <type your password again>
```

In addition, it is recommended to periodically change the enable password based on the password age policy.

Common Password Security Practices

The following security practices are commonplace in the industry and should be considered for any passwords configured in the ACOS system:

- Contain uppercase, lowercase, numeric, and special characters depending on the password-policy complexity configured.
- Are not the same values as passwords included in this document or any other ACOS product document.
- Are not based on words in any language, jargon, slang or dialect and are not words or based on words found in any dictionary.
- Are not based on personal or familiar names, such as the name of a family member, pet, or friend.
- Are not based personal information, such as PINs, telephone numbers, addresses, or birthdays.
- Are not based on predictable patterns, such as ‘12345678’, ‘qwerty’, ‘aaaabbbb’, or ‘123123’.
- Are not based on commonly known default passwords for networking or other products, such as ‘password’, ‘admin’, ‘user’, ‘sysadm’, ‘root’, ‘123456’, ‘admin123’, ‘qwerty’, etc.
- Are not any of the above spelled backwards.
- Are not any of the above prefixed or post fixed by a number, such as ;jambalaya1; or ;1jambalaya;.

Especially for networking devices, the following are additional common practices to consider:

- Periodically change static passwords, though this is recognizably tedious in even modest networks and potentially unmanageable in larger networks without automation capabilities.
- Avoid using passwords commonly known as default passwords in networking products, including Internet of Things (IoT) devices.
- The Privileged EXEC level of the CLI allows users to change or modify the ACOS system configuration and can be entered via the global password-protected enable

command. By default, this password that is empty (e.g. just press Enter at the password prompt).

NOTE: Passwords, shared secrets, secret keys, etc. for various networking protocols, their implementation in ACOS, or ACOS implementation features may be limited in the ranges of characters allowed. Typically, these conditions will occur for the range of special characters supported.

Local Password Practices

ACOS cannot control or enforce your policy for passwords when they are managed by RADIUS, TACACS+, or LDAPS services external to ACOS. However, A10 can recommend various password practices and can provide some services to enforce policy for passwords locally configured on the ACOS system.

The user can now manage the passwords for local authentication in the ACOS device. The password policy management is designed with a key focus on the following parameters:

- Password Complexity
- Password Aging
- Password History
- Password Checks

For more information on the above parameters, see *Configuring Password Policy for Local Authentication* topic in the Management Access and Security Guide.

Failed Authentication Lockout

ACOS cannot control or enforce your policy for handling multiple failed authentications detected through RADIUS, TACACS+, or LDAPS services. ACOS does, however, support an administrator lockout capability for failed authentications on locally configured, ACOS user accounts. The `admin-lockout` feature is enabled by default with the following settings:

- 5 # of failed attempts before the account is locked out
- 10 minutes Duration the account is locked out and any further attempts will be summarily failed
- 10 minutes Duration after which prior failed attempts will be forgotten

A10 recommends that administrators do not disable this feature and update it by using the admin-lockout command to settings consistent with the organization's security policy. The following example changes the threshold to 5 failed attempts over a period of 30 minutes with a lockout of the account for 1 hour if the threshold is reached.

```
ACOS-TH####(config)#admin-lockout threshold 5
ACOS-TH####(config)#admin-lockout duration 60
ACOS-TH####(config)#admin-lockout reset-time 30
```

NOTE: Setting the `duration` value to zero (0) will permanently lockout an account if the number of failed attempts reach the threshold. On these occasions, the root administrator of the ACOS system will need to manually unlock the account to reenable access for the ACOS user. The root administrator has read-write privileges to all ACOS objects across all partitions.

Authentication, Authorization, and Accounting (AAA)

Authentication, Authorization, and Accounting (AAA) is a framework fundamental to securing user access to ACOS systems. ACOS provides a number of methods for authenticating users and preventing unauthorized access to management services of the system, ranging from local authentication services on the system to Role-Based Authentication (RBA) using external servers. Accounting is not provided by ACOS and must be handled via an external service such as RADIUS.

The following subsections discuss key aspects of this framework in ACOS, including:

- Authentication methods supported
- Foundation model for User Access and Privileges
- Role-Based Access (RBA) with external servers

ACOS Authentication Methods

Authentication permits or denies access to the ACOS based on the administrator username and password credentials provided when ACOS is being access from the:

- System's Web/GUI
- Command Language Interface (CLI) via the system console or remotely via SSH
- aXAPI for external management applications

By default, when an admin user or management application attempts to login to the ACOS system, the device determines whether the username and password exist in a local database. Without additional configuration, the authentication process stops at this point. If the username and password exist in the local database, the user is permitted access; otherwise, access is denied.

Authorized users can configure the ACOS system to also use external RADIUS, TACACS+ or LDAP servers for authentication. ACOS can be configured to use one or more of these methods, along with the local database using the authentication type CLI command. Precedence of authentication method is indicated by the order specified and ACOS will query them in order as it attempts to successfully authenticate access.

NOTE: The local database method must always be included in this configuration as it is an ever-present fallback in the event that all external authentication servers are not available. Authentication using only remote servers is not supported by ACOS.

For example, to configure the ACOS system to use external RADIUS authentication and the local database, with RADIUS preferred:

```
ACOS-TH####(config)#authentication type radius local
```

Alternately, to configure the ACOS for multi-tier authentication mode multiple where TACACS+ is queried first, a RADIUS backup authentication service is tried next, a secondary backup LDAP server after that, and lastly the local database as a last resort. These backup mechanisms are tried in priority order when the ones with higher priority methods fail for reasons such as service being down or user not found.

```
ACOS-TH####(config)#authentication mode multiple
ACOS-TH####(config)#authentication type tacacs radius ldap local
```

NOTE: A10 recommends that the local database option (local) should be included as one of the authentication sources, regardless of the order is which the sources are used. When local database option isn't included, the default "admin" user will use the local database unless "admin" user is disabled.

ACOS User Access and Privilege Assignment

ACOS users (administrators) can be assigned a range of access types and privileges when their accounts are created; either through locally configured accounts or through external authentication services such as RADIUS, TACACS+, or LDAPS. It is important to be diligent when making access and privilege assignments for ACOS users and their relative roles in administering the ACOS system.

See ACOS Management Access and Security Guide for details on configuring users (administrators) for the ACOS system.

User Access Types

ACOS supports three (3) fundamental access methods for administrators.

- cli Access to the ACOS CLI via physical console or remote terminal session. This is the most intimate level of access for configuring the ACOS system.
- web Access to the ACOS GUI via web browser. This method provides a rich graphical interface to configure the ACOS system, though some granular configuration options may be only available via the CLI.
- axapi Real-time access to XML-based programs via HTTP/HTTPS. This method supports programmatic access to ACOS configuration and extended services for external management applications.

When assigning access types for a given user (admin) account, ACOS administration should consider the following:

- Not all ACOS admins need to have CLI access. For many admins, Web/GUI access will be enough.
- In general, more seasoned administrators should be permitted to access the ACOS CLI, given the CLI's notable complexity and extended capabilities compared to the Web/GUI interface.

- Administrators without the need to develop or run applications using the aXAPI web/cli access should not be enabled for aXAPI access.

Read, Write, Partition Privileges

ACOS supports three (3) fundamental privileges for administrators.

- Read: Allows the administrator to view and display ACOS configuration elements.
- Write: Allows the administrator to create, modify, or delete ACOS configuration elements - with the exception of selected External Health Monitor objects.
- Partition: Constrains the administrator other privileges (read, write) to the scope of a given ACOS Layer 3 Virtual (L3V) partition.

These privileges are assigned in combinations to enable a range of abilities for administrators to configure and observe status/statistics in the overall ACOS system or in the scope of a given L3V partition.

When assigning privileges for a given user (admin) account, the ACOS administration should consider the following:

- ACOS admins responsible for monitoring status and notifying others to resolve downed links, excessive CPU use, etc. should only be assigned “read” privilege.
- Only admins trusted to make changes in the ACOS system’s configuration should be assigned “write” privilege.
- Partition-based admin accounts should consider the points described above relative to the respective L3V partitions defined for the ACOS system.
- Shared partition admin accounts can affect the overall ACOS system, including any L3V partitions that it supports. Accordingly, this level of privilege should be assigned for more seasoned and trusted members of the organization.
- Always be diligent and cautious when assigning privileges to ACOS admin accounts.

ACOS also supports an optional Role-Based Access (RBA) mechanism, discussed below, which builds on top of this base-set of privileges for finer-grained control of permissions and privileges of ACOS administrator accounts.

HM Privilege

There is a fourth privilege for ACOS administrator accounts, the External Health

Monitor (hm) privilege, that is noteworthy of separate mention and consideration.

This privilege allows the ACOS admin to import, create, edit, and delete scripts intended for the purpose of monitoring health and status of external server applications by the ACOS system. Though a very useful and practical capability, this ACOS feature (by its very nature) represents an avenue for programs/code unsanctioned by A10 to enter the otherwise closed ACOS system.

SECURITY NOTE: The `hm` privilege is only supported for configured ACOS admins with both **read** and **write** privileges for the ACOS shared partition. It is not supported for partition ACOS admins since External Health Monitors execute on a system-wide basis in the ACOS device.
The hm privilege is disabled by default for provisioned admin users.

With this privilege a malicious or compromised administrator or an administrator whose system is unknowingly compromised could introduce programs/code into the ACOS system that could leverage a variety of vulnerabilities and attacks, negatively impacting the ACOS system or the connected network and systems.

Accordingly, the hm privilege should be assigned only to administrators who are significantly trusted in the organization. Only these administrators should be allowed to develop and maintain External Health Monitor scripts on the ACOS system or, more importantly, to establish them on production ACOS system deployments

For more information on configuring administrative users, refer to the ACOS Management Access and Security Guide. See the *External Health Monitor Practices* discussion below for additional discussion on securing this feature.

SECURITY NOTE: The hm privilege could allow an administrator to use the ACOS External Health Monitor feature for potentially malicious purposes. Only assign this privilege to administrators sufficiently trusted in your organization

Role-Based Access (RBA)

RBA allows finer grained controls of ACOS management privileges, described above, with predefined roles mapped to standardized privilege levels (for RADIUS and TACACS+) and predefined roles with additional parameters (for LDAP). This affords

much more efficient scaling of privilege and access management for larger user communities.

To support these roles and additional access factors, ACOS defines extensions to the data model (e.g. schema, dictionary, etc.) for these protocol that can be configured into the external authentication servers, as described in the ACOS Management Access and Security Guide of the ACOS product documentation.

ACOS RBA with TACACS+ or RADIUS

For ACOS systems enabling TACACS+ or RADIUS for external authentication, ACOS supports a number of predefined roles which map to privilege levels of these protocols as shown in the table below:

Access Role	RADIUS Privilege	TACACS+ Privilege	Partition Role
ReadWriteAdmin	2	15	N
SystemAdmin	3	14	N
NetworkAdmin	4	13	N
NetworkOperator	5	12	N
SlbServiceAdmin	6	11	N
SlbServiceOperator	7	10	N
ReadOnlyAdmin	1	0	N
PartitionReadWrite	8	9	Y
PartitionNetworkOperator	9	8	Y
PartitionSlbServiceAdmin	10	7	Y
PartitionSlbServiceOperator	11	6	Y
PartitionReadOnly	12	5	Y

SECURITY NOTE: The ReadWriteAdmin role includes the ACOS hm privilege, allowing access to External Health Monitor files as described in the HM Privilege discussion above. See the External Health Monitor Practices discussion for more information on potential security risks involving these monitors.

ACOS RBA with LDAP

For ACOS systems enabling LDAP for external authentication, ACOS supports a number of predefined roles that may be indicated for the A10AdminRole parameter of the LDAP schema extensions for ACOS. These roles include:

- ReadOnlyAdmin
- ReadWriteAdmin
- PartitionSlbServiceOperator
- PartitionReadOnly
- PartitionReadWrite

Another element of the LDAP schema extension is the A10AccessType parameter. It consists of a list of access privileges corresponding to the User Access Types and HM Privilege discussed earlier; namely:

- cli
- axapi
- web
- hm

SECURITY NOTE: Including the hm attribute for a ReadWriteAdmin role will allow access to External Health Monitor files as described in the HM Privilege discussion above. See the External Health Monitor Practices discussion for more information on potential security risks involving these monitors.

See the *Securing Other Management Protocols* section below for discussions on securely configuring LDAP and servers in ACOS.

Custom Role Based Access

ACOS provides custom role based access by allowing admins to fine-tune the permissions and privileges of individual accounts or groups of accounts. Custom roles may be defined limiting privileges of each configuration object by specifying the object's class lineage followed by the permitted privilege level (no access, read, write).

For more information on how to configure custom role based access and apply them to users or groups, refer to the *Management Access and Security guide*, section *Configuring Role-Based Access (RBA)* and *Fine Tuning Privileges*.

Restrict User Access based on Source Network

In addition to securing access to an ACOS system by identity and configured privilege (as described above), constraining access to the ACOS system and its services provides a further layer of confidence by ensuring that access is only from trusted network segments or even individually trusted client systems.

Two ways to limit access based on where users are accessing ACOS from include:

- Access relative to user (administrator) network address
- Access relative to ACOS interface and service

A10 recommends that administrators do not disable this feature and update it by using the admin-lockout command to settings consistent with the organization's security policy. The following example changes the threshold to 5 failed attempts over a period of 30 minutes with a lockout of the account for 1 hour if the threshold is reached.

```
ACOS-TH####(config)#admin-lockout threshold 5
ACOS-TH####(config)#admin-lockout duration 60
ACOS-TH####(config)#admin-lockout reset-time 30
```

NOTE: Setting the `duration` value to zero (0) will permanently lockout an account if the number of failed attempts reach the threshold. On these occasions, the root administrator of the ACOS system will need to manually unlock the account to reenable access for the ACOS user. The root administrator has read-write privileges to all ACOS objects across all partitions.

User Identity Access Controls

ACOS cannot control or enforce where RADIUS, TACACS+, or LDAPS configured ACOS users can access ACOS from. In these cases, network administrators are responsible for managing identity-based access to ACOS systems in their authentication service infrastructure.

ACOS does, however, support network identity-based access controls for locally configured ACOS user accounts. By default, locally configured ACOS users are permitted to login from any source address, without restriction. The trusted-host command allows individual users to be restricted from logging in based on their IP subnet or host address or through an Access Control List (ACL) for more complex criteria.

For example, to restrict logins for “bob” from any DHCP-assigned, address on the 10.10.10.x subnet, though not from when connected in on any other subnet, and “ted” from the hardened and monitored management access server at 10.10.7.42:

```
ACOS-TH####(config)#admin bob
ACOS-TH####(config-admin:bob)#trusted-host 10.10.10.0/24
ACOS-TH####(config)#admin ted
ACOS-TH####(config-admin:ted)#trusted-host 10.10.7.42/32
```

NOTE: IPv6 is not supported for the address information parameter to the trusted-host command. However, the IPv6 addresses are supported for the access-list variant below.

As an alternate example, an ACL can be used to restrict logins for “carol” from any DHCP-assigned, client address on the 10.10.10.x subnet or the 10.10.7.42 access server:

```
ACOS-TH####(config)#access-list 7 1 remark "ACL – Net Admin segment +
Restricted Server"
ACOS-TH####(config)#access-list 7 2 permit ip 10.10.10.0/24
ACOS-TH####(config)#access-list 7 3 permit ip 10.10.7.42/32
ACOS-TH####(config)#admin carol
ACOS-TH####(config-admin:carol)#trusted-host access-list 7
```

NOTE: User level ACLs are not able to constrain the ACOS devices interfaces being used for permitted client addresses. The services themselves being used for such access (e.g. SSH, HTTPS, etc.) do, however, provide interface level access control.

Interface and Service Level Controls

Every ACOS system supports interfaces for a management port, real data ports (e.g. eth1, eth2, etc.), and virtual ethernets ports (e.g. ve1, ve2, etc.) based on VLAN

configuration. By default, as shown in the table below, selected management services are only enabled on the management port, except for “ping” and “ntp” which is also enabled on real and virtual ethernet ports.

Management Service	Management I/F	Data Interfaces
PING	Enabled	Enabled
SSH	Enabled	Disabled
Telnet	Disabled	Disabled
HTTP	Enabled, w/ Redirect to HTTPS	Disabled
HTTPS	Enabled	Disabled
SNMP	Enabled	Disabled
NTP	Enabled	Enabled

ACOS also supports management functions where the ACOS system initiates to trusted servers for various management services; including NTP, TACACS+, Radius, and LDAP/LDAPS. These functions are enabled only when configured into the ACOS system.

By default, these enabled services and functions have no access restrictions. ACOS supports a range of ACLs to support limiting access to management services by users in selected networks segments or from specific network addresses. ACLs can also be used to constrain access by the ACOS system to specific, trusted management servers.

NOTE: For clarity of purpose, this document will use the management interface ACL method for access control examples of management services and functions. This method uses the `enable-management service acl-v4` form of the `enable-management service` command to apply ACL rules on supported interfaces of the ACOS system.

Though certainly viable, other ACL methods are beyond scope for the remainder of this document. Administrators are referred to ACOS product documentation for insights into other ACL methods that may be more convenient for their deployments of like and equivalent access rules.

ACOS supports two basic, underlying forms of ACLs; standard and extended. Standard ACLs (acl-id values 1 -99) support source IP address host and segment constraints. Extended ACLs (acl-id values 100 – 199) support a variety of additional controls; including IP destination addressing, TCP/UDP source/destination ports, and others.

NOTE: For simplicity and to avoid ACOS management-related ACL nuances, this document will use the extended ACL form for access control examples.

It is commonplace for ACOS deployments to seek management access via data ports, in addition to the system's management port. ACOS allows various management services to be:

- enabled or disabled per interface, and
- configured with per-interface ACLs for finer grained access controls.

The following is an example of using ACLs for broader community access to for selected services for:

- HTTPS access only via management and eth1 data ports from the 10.10.10.0/24 network segment.
- SSH access via data port eth1, though just from the 192.10.7.42 shared access server.

```
// HTTPS, mgmt. port already enabled
// Create Mgmt I/F ACL 100 for ACOS mgmt. port (incl HTTPS, mgmt. port
rules).
//    - ACL 100 will be an overall ACL for the ACOS mgmt. port
//
ACOS-TH####(config)#access-list 100 1 remark "ACL – mgmt port @ HTTPS"
ACOS-TH####(config)#access-list 100 2 permit tcp 10.10.10.0 /24 any eq 443
ACOS-TH####(config)#enable-management service acl-v4 100
ACOS-TH####(config-enable-management acl-v4)#management
// Enable HTTPS on ethernet 1
// Create Mgmt I/F ACL 101 for ACOS eth1 port (incl HTTPS, eth1 port
rules).
//    - ACL 101 will be an overall ACL for the ACOS eth1 port
```

```
//
ACOS-TH####(config)#enable-management service https
ACOS-TH####(config-enable-management https)#ethernet 1

ACOS-TH####(config)#access-list 101 1 remark "ACL - eth1 port @ HTTPS"
ACOS-TH####(config)#access-list 101 2 permit tcp 10.10.10.0 /24 any eq 443

ACOS-TH####(config)#enable-management service acl-v4 101
ACOS-TH####(config-enable-management acl-v4)#ethernet 1
// Enable SSH on ethernet 1
// Add SSH, eth1 port rules to eth1 ACL 101
//

ACOS-TH####(config)#enable-management service ssh
ACOS-TH####(config-enable-management-ssh)#ethernet 1

ACOS-TH####(config)#access-list 101 5 remark "ACL - eth1 port @ SSH from
hardened server"
ACOS-TH####(config)#access-list 101 6 permit tcp host 192.10.7.42 any eq
22
ACOS-TH####(config)#show management
PING    SSH         Telnet      HTTP         HTTPS     SNMP     NTP        ACL
-------------------------------------------------------------------------------
----
mgmt    ACL 100     ACL 100     ACL 100     ACL 100     ACL 100  ACL 100    100
eth1    ACL 101     ACL 101     ACL 101     ACL 101     ACL 101  ACL 101    101
eth2     on         off         off         off         off      off        -
eth3     on         off         off         off         off      off        -
eth4     on         off         off         off         off      off        -
```

NOTE: The extended ACLs 100 and 101 created here will be used throughout the remainder of this document in examples of provisioning access controls to harden and secure ACOS management plane protocols. ACL 100 will build up rules for management access on the mgmt interface. ACL 101 will do the same for the eth1 interface.

Unsecure Management Access Protocols

ACOS supports the following general management services and protocols for access from management clients and to external servers.

- CLI/Terminal Access : SSH, Telnet
- Web-GUI and aXAPI Access : HTTPS, HTTP
- Network Management Access : SNMPv1/v2c, SNMPv3
- Remote File Transfer : HTTPS, HTTP, SFTP, SCP, FTP, TFTP
- Network Time : NTP

Of these, the following are considered unsecured as they exchange information in clear text, without encryption.

- Access Protocols : Telnet, HTTP, SNMPv1/v2
- File Transfer Protocols : FTP, TFTP, HTTP

Administrators can view which general management services are enabled, on which interfaces, and if there are any interface ACLs enabled with the show management command. For example:

```
ACOS-TH####(config)#show management
PING    SSH         Telnet      HTTP         HTTPS     SNMP      NTP       ACL
-------------------------------------------------------------------------------
----
mgmt    on          on          off          on        on        on        -
eth1    on          off         off          off       off       on        -
eth2    on          off         off          off       off       on        -
eth3    on          off         off          off       off       on        -
eth4    on          off         off          off       off       on        -
```

Telnet, HTTP, SNMPv1/v2

By default, Telnet protocol disabled on all interfaces but the service is enabled for localhost. SNMP protocol is enabled on management interface and disabled for all data interface. SNMP service is disabled by default and must be explicitly enabled.

Secure practices recommend that Telnet and SNMPv1/v2 protocols remain disabled in the ACOS system.

NOTE: Secure configuration of SNMPv3 is discussed separately, later in this document.

By default, HTTP access on the ACOS management plane will automatically redirect HTTP (TCP port 80) connections to the HTTPS service (TCP port 443). Though not recommended, full access to the ACOS Web-GUI and aXAPI services via HTTP can be enabled as follows:

```
ACOS-TH####(config)#web-service auto-redirt disable
```

For organizations with strict security policies that prohibit any HTTP traffic in their device management networks, this method of access to the ACOS system can be fully disabled, while leaving HTTPS access enabled, as follows:

```
ACOS-TH####(config)#web-service server disable
```

NOTE: Attempting to disable HTTP with the no enable-management service http management command will not disable HTTP redirects when the auto-redirt feature is enabled.

Avoid Using FTP, TFTP, or HTTP File Transfer Mechanisms

The following management operations support the transfer of files into and from the ACOS system:

- Import, Export commands
- Log Exports
- Periodic Import commands
- Restoring Start-up Configuration
- Backup of Log Files
- Loading an SSH Key
- Backup of System Configuration
- Importing an SSH Public Key

- Periodic Backups
- Upgrading ACOS to a new version
- Backup of System Information
- Exporting System Information for troubleshooting
- Copying Running Configuration
- Periodic Importing of Geo-Location Lists
- Loading ACOS Web/GUI service certificate or private-key
- Enabling the loopback interface to source such management traffic (ACOS TPS Only)
- Power On Auto Provisioning

A10 recommends that ACOS administration define and implement a policy for their ACOS admins to not use FTP, TFTP, or HTTP options for these and any other ACOS operations not listed above.

Instead, the following secure transfer protocols options should be used.

- scp: Remote file path of SCP file , Format: scp://[user@]host/file
- sftp: Remote file path of SFTP file , Format: sftp://[user@]host/file
- https: Remote file path of HTTP file, Format: https://[user@]host/file

Securing Interactive Management Sessions

Interactive management methods available in of ACOS include:

- CLI via system console of the ACOS device
- CLI via remote terminal connections
- Web/GUI from web browsers
- Programmatic aXAPI from RESTful management applications.

The following subsections share hardening recommendations for configuring these services and their underlying SSH and HTTPS access protocols.

Configuring the Management Interface as Source for Automated Management Traffic

Best practice says to use an isolated management network for management protocols. By default, use of the management interface as the source interface for automated management traffic is disabled. To enable it, use the ip control-apps-use-mgmt-port command at the configuration level for the management interface:

```
ACOS-TH####(config)#interface management
ACOS-TH####(config-if:management)#ip control-apps-use-mgmt-port
```

This defaults the control traffic (ntpd, ntpdc, ntpdate, snmpd, syslogd, a10timer, mailx, ssh, telnet, a10logd, a10scmd, TACACS+, LDAP and RADIUS) to use the management interface by default.

Session Timeouts

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of an unattended, management session enabled on the console, a remote terminal, browser, or an aXAPI application that has been left unattended.

ACOS supports management access session timeouts for the following services:

- ACOS CLI via the system console or remote terminal connections (e.g. SSH)
- ACOS Web/GUI
- ACOS aXAPI programmatic API

CLI Session Timeout

ACOS CLI sessions can be configured to timeout after a period of inactivity resulting in the following behaviors:

- Console port - login session will be terminated, returning terminal session to ACOS login prompt.
- Remote terminal - TCP connection to remote terminal (e.g. SSH) client will be terminated by ACOS.

By default, ACOS CLI sessions will time-out after 15 minutes of inactivity. Use the terminal idle-timeout command to change this duration in accordance with the organization's security policy. For example, to set the idle-timeout to 10 minutes:

```
ACOS-TH####(config)#terminal idle-timeout 10
```

Web/GUI Session and aXAPI Timeouts

ACOS Web/GUI and aXAPI applications sessions can be configured to timeout after a period of inactivity with ACOS terminating their underlying TCP connections.

By default, these sessions will time-out after 10 minutes of inactivity. Use the `web-service gui-timeout-policy` and `web-service axapi-timeout-policy` commands to change these durations in accordance with the organization's security policy. For example, to set the idle-timeout to 15 and 20 minutes; respectively:

```
ACOS-TH####(config)#web-service gui-timeout-policy idle 15
ACOS-TH####(config)#web-service axapi-timeout-policy idle 20
```

Login Banners

Legal notification requirements can be very complex and vary by jurisdiction, company policies, department policies, and other guidelines. Failure to display a login banner prior to a logon attempt or displaying a banner with insufficient content can compromise an organization's ability to prosecute malicious users. It may also put the organization at legal risk by monitoring users' activities without consideration in such notifications.

Login banners are recommended on all external, interactive interfaces for the ACOS system. The content of these banners should be consistent with the organization's policies and reviewed by legal counsel, if needed. From a security perspective, they should not contain any of the following information:

- Purpose, location, logical network name, or owner of the device.
- Make, model, or manufacturer of the device.
- Software or version on the device.

It is recommended that login banners should be displayed before access authentication (e.g. username and/or password entry) is completed.

CLI Login Banner

A login banner can be configured for the ACOS CLI using the banner login command. This will display the banner's content after the ACOS admin user name is entered and before the password is prompted. For example:

```
ACOS-TH####(config)#banner login multi-line
Input a string to mark the end of banner text, up to 2 characters:
bb
Enter text message, end with string 'bb'.
 *** WARNING ***

This system is private and may be accessed only by authorized users for
official purposes.  The system owner reserves the right to monitor any and
all activity taking place on this system and any attempts to connect to
it. Individuals using this computer system are subject to having all of
their activities monitored and recorded by system personnel.  Use of this
system evidences an express consent to such monitoring and agreement that
if such monitoring reveals evidence of possible abuse or criminal
activity, system personnel may provide the results of such monitoring to
appropriate officials. Unauthorized users or users who exceed (or attempt
to exceed) their authorized level of access are subject to prosecution
under any local or international laws that apply as well as Company
initiated proceedings.

bb
ACOS-TH####(config)#
```

NOTE: Be careful not to confuse this with the banner exec command which configures a banner to be displayed after successful login.

The above banner is only provided as an example. You should consult the organization's policies and/or legal counsel for the actual content.

Web/GUI Login Banner

A login banner can be configured for the ACOS Web/GUI's login page using the web-service login-message command, with the message in double-quotes (""). For example:

```
ACOS-TH####(config)#web-service login-message

 *** WARNING ***
***\n\nThis system is private and may be accessed only by authorized users
for official purposes.  The system owner reserves the right to monitor any
and all activity taking place on this system and any attempts to connect
to it. Individuals using this computer system are subject to having all of
their activities monitored and recorded by system personnel.  Use of this
system evidences an express consent to such monitoring and agreement that
if such monitoring reveals evidence of possible abuse or criminal
activity, system personnel may provide the results of such monitoring to
appropriate officials. Unauthorized users or users who exceed (or attempt
to exceed) their authorized level of access are subject to prosecution
under any local or international laws that apply as well as Company
initiated proceedings.\n\n"
ACOS-TH####(config)#
```

NOTE: This banner is displayed after a successful login via the ACOS Web/GUI. The ACOS Web/GUI does not presently support a pre-login banner.

NOTE: The web-service command above supports a single string, terminated by entering the CLI command. Line breaks and blank lines can be included using **\n** and **\n\n** characters; respectively.

NOTE: The above banner is only provided as an example. You should consult the organization's policies and/or legal counsel for the actual content.

Securing SSH and HTTPS Services

Updating cryptographic keys and certificates is a common requirement of an organizations security policy, both when installing a new networking device and periodically. The following describe procedures to update keys and certificates in ACOS for SSH and HTTPS.

Update SSHD Keys

A common security practice is to update the network device's SSH Server key to ensure appropriate key size and uniqueness, thus avoiding potentially duplicate or undersized keys instantiated by the manufacturer. Though this should not be necessary with new installations of contemporary ACOS devices and releases, ACOS devices with a history of upgrades from legacy releases could still have issues on this front.

Accordingly, it is recommended to re-generate or replace the SSH Server keys by using the `sshd key regenerate` or `sshd key load` ACOS commands, followed by a restart of the SSH server with the `sshd restart` command. Note that the `sshd restart` command will cause existing SSH sessions to be terminated.

NOTE: Replacement of the key is the preferred approach as it consistent with the FIPS-compatible mode of operation for ACOS.

The following example generates the SSH server's 2048 bit RSA key and ECDSA 256 bit key using P-256 curve.

```
ACOS-TH####(config)#sshd key regenerate size 2048
ACOS-TH####(config)#sshd restart
```

NOTE: A 4096-bit key size would be even stronger and is also supported by specifying 4096 for the size. NIST recommends using a 2048 bit RSA key until 2030. After 2030, NIST recommends using at least a 3072 bit RSA key. NIST recommends using a minimum of 256 bit ECDSA key.

ECDSA Keys for SSHD

ACOS device supports encryption based on the Elliptic Curve Digital Signature Algorithm (ECDSA) used by ssh clients to enhance security and align with FIPS compliance. ECDSA offers strong security with shorter key lengths than RSA and provides improved performance. By default a 256-bit ECDSA key is generated using a P-256 curve in ACOS. To use a different ECDSA key size and curve, you may generate the ECDSA key outside of ACOS using various 3rd party tools and import the ECDSA key into ACOS. The following describes the process of manually generating an ECDSA key outside of ACOS, and importing the key material into ACOS.

The process of generating ECDSA keys involves using the 'ssh-keygen' tool outside of the ACOS device then importing the private key into the ACOS device. The tool allows you to create an authentication key pair using the ECDSA algorithm with SHA-256, SHA-382, or SHA-512 digest-type. By default, SHA-256 is used. Once generated, these keys can be loaded and imported into the ACOS device, and they can also be regenerated if needed.

```
# ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_ecdsa): ecdsa_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_ecdsa
Your public key has been saved in /home/user/.ssh/id_ecdsa.pub
The key fingerprint is: SHA256:E9KhaAfXIAtNrifKE09+uF4qNP9IF+3KDdfb4AvG0jI
user@VirtualBox
The key's randomart image is:
+---[ECDSA 256]---+ | .o+ oo. | | o.* o.. | | = + o | | o ... . | | .o...
.S | |.+=o. = .. | |ooo= E B o | | .o.O X o + | | o=.+ . +.. | +----
[SHA256]-----+
```

To import the ECDSA private key into ACOS, use the following example:

```
ACOS-TH####(config)#sshd key load use-mgmt-port
scp://user@172.20.20.20/home/user/.ssh/id_ecdsa
```

Attempt to login from an external host to the ACOS device using ECDSA

```
ssh -o "HostKeyAlgorithms ecdsa-sha2-nistp256" admin@10.10.10.1
The authenticity of host '10.10.10.1 (10.10.10.1)' can't be established.
ECDSA key fingerprint is
SHA256:OMhF6LOYt5laawn7t4wBYPMdTCOivLZOZvOK232KQoY.
ECDSA key fingerprint is
MD5:00:0b:ac:78:1b:51:2b:47:d8:13:7c:e2:c9:58:a4:e2.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.1' (ECDSA) to the list of known
hosts.
Password:
Last login: Mon Jul 3 17:40:23 2023 from 172.20.20.20
System is ready now.
```

```
[type ? for help]
ACOS-TH####>
```

For more information about generating ECDSA key and importing them into ACOS, refer to the *System Configuration and Administrator* guide section *Key Configuration*.

Enable TLS 1.3

TLS 1.3 is faster and more secure than TLS 1.2. While insecure protocols from TLS 1.2 were removed at the time of this publication, A10 recommends enabling TLS 1.3 for HTTPS. To enable TLS 1.3, use the following command:

```
ACOS-TH####(config)#system tls-1-3-mgmt enable
```

While TLS 1.3 is enabled, TLS 1.2 is also enabled.

The following cipher suites are supported for TLS 1.2:

Elliptic Curves

- secp256r1
- secp521r1
- secp384r1
- secp256k1

Ciphers

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

In ACOS 6.0.5, the following ciphers are enabled by default:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA3840
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

```
ACOS-TH####(config)#sshd key load use-mgmt-port
scp://user@172.20.20.20/home/user/.ssh/id_ecdsa
```

Attempt to login from an external host to the ACOS device using ECDSA

```
ssh -o "HostKeyAlgorithms ecdsa-sha2-nistp256" admin@10.10.10.1
The authenticity of host '10.10.10.1 (10.10.10.1)' can't be established.
ECDSA key fingerprint is
SHA256:OMhF6LOYt5laawn7t4wBYPMdTCOivLZOZvOK232KQoY.
ECDSA key fingerprint is
MD5:00:0b:ac:78:1b:51:2b:47:d8:13:7c:e2:c9:58:a4:e2.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.1' (ECDSA) to the list of known
hosts.
Password:
Last login: Mon Jul 3 17:40:23 2023 from 172.20.20.20
System is ready now.
[type ? for help]
ACOS-TH####>
```

For more information about generating ECDSA key and importing them into ACOS, refer to the *System Configuration and Administrator* guide section *Key Configuration*.

Update HTTPS Cert-Key Pair

A common security practice is to update the network device's HTTPS certificate and key (cert-key) pair to ensure appropriate key size and cert-key pair uniqueness, thus avoiding potentially duplicate or undersized cert-keys instantiated by the manufacturer. Though this should not be necessary with new installations of contemporary ACOS devices and releases, ACOS devices with a history of upgrades from legacy releases could still have issues on this front.

Accordingly, it is recommended to re-generate or replace the using HTTPS cert-key pair by using the `web-service secure regenerate` or `web-service secure load` ACOS commands, followed by a restart of the HTTPS server with the `web-service restart` command. Note that the `web-service restart` command will cause existing HTTPS sessions to be terminated.

NOTE: Replacement of the key-pair is the preferred approach as it consistent with the FIPS-compatible mode of operation for ACOS.

The following example shows how to regenerate the HTTPS cert-key pair with a self-signed certificate, based on a 2048-bit RSA key with SHA-2 signature and valid for 2 years.

```
ACOS-TH####(config)#web-service secure regenerate domain my-domain country
my-country-code state my-state-code
ACOS-TH####(config)#web-service restart
```

NOTE: HTTPS certificates used with ACOS systems are often self-signed since device management networks are commonly isolated within an organization's internal, private network environment, are not permitted access to the Internet, and/or have no otherwise available Certificate Authority (CA).

Administrators seeking to generate their own HTTPS cert-key pair for the ACOS system should ensure the following:

- For RSA pair: Public Key >= 1024-bit, Private Key >= 2048-bit, Signature Alg = SHA-2
- For ECDSA pair: Public Key >= 224-bit, Private Key >= 224-bit, Signature Alg = SHA-2

NIST recommends using a 2048 bit RSA key until 2030. After 2030, NIST recommends using at least a 3072 bit RSA key. NIST recommends using a 256 bit ECDSA key.

Once generated, the cert-key pair can be loaded for use by the ACOS HTTPS service. For example, to load a newly generated cert-key pair (new) from a local administration system (10.1.2.20):

```
ACOS-TH####(config)#web-service secure wipe
ACOS-TH####(config)#web-service secure certificate load
scp://u1@10.1.2.20/home/u1/new-cert.pem
ACOS-TH####(config)#web-service secure private-key load
scp://u1@10.1.2.20/home/u1/new-key.pem
...
ACOS-TH####(config)#web-service restart
```

External Health Monitor Practices

The External Health Monitors (Ext-HMs) feature of ACOS extends the native ACOS monitoring of server and service availability for custom applications. It also can modify the behavior of ACOS based on external conditions. This feature allows ACOS deployments to import scripts and code into the ACOS system written in shell, python, and other languages and to be scheduled to be periodically executed to determine health and availability of the underlying servers and their services.

Though Ext-HMs can provide a tremendously valuable service and capability, they also represent an avenue for programs/code, not sanctioned or warranted by A10, to be included into the ACOS system. Inherent in the Ext-HM feature is the addition of programmatic code, in the form of scripts, by administrators into the closed, system-level, run-time environment within ACOS. Running at elevated processing privilege, this code will have intimate access throughout the ACOS system and broad connectivity to its deployed networking environment as scripts may use axAPIs to modify running configuration.

Well behaved scripts contain trusted code solely for performing functions to monitor the health of real servers and applications in the organization's network. It is the organization's responsibility to ensure the integrity and content of these scripts; namely, that the code is trusted and that the scripts are free of code that can compromise the security of the ACOS system or systems in connected networks.

Malicious code in External Health Monitor scripts, whether intentional by disaffected ACOS admins or unintentional by compromised ACOS admins or their systems, can

expose the ACOS system and connected environment to a range of exploits, such as, but not limited to, the following:

- Denial of Service (DoS)
- Exfiltration of Sensitive Information
- Distributed Denial of Service (DDoS)
- Side-Channel Vulnerabilities
- Remote Code Execution (RCE)
- Brute Force Attacks
- Buffer Overflow
- Man-in-the-Middle Attacks
- Trojan Horses
- Spyware
- Network Worms
- Ransomware

To secure Ext-HMs and keep them secure, ACOS administration can restrict access to these services, monitor access activity, and review the content of these scripts. The recommendation is to limit or avoid use of external health monitor scripts.

Restricting Extended Health Monitor Access

All ACOS admins, except for the ACOS root admin, are not permitted to import, create, edit/modify, or delete Ext-HM scripts as a default. Selected ACOS admins sufficiently trusted to access these scripts can be allowed to perform these operations by provisioning with the health monitor (hm) privilege. For more information on configuring administrative users, refer the User Access and Privilege Assignment discussion above.

Only ACOS, system-level admins with Read-Write (R/W) privilege and specifically assigned this privilege will be permitted to perform these operations for External Health Monitor scripts. As these monitoring scripts have access throughout the ACOS system, this privilege is not available to partition constrained ACOS admins.

SECURITY NOTE: To minimize the threat surface of this feature, provision this privilege for the fewest users necessary.

Monitor External Health Monitor Activities

Administrator and aXAPI application activities to configure external health monitors in the ACOS system can be monitored through the ACOS Audit Log (see Audit Logging Practices below). These configuration operations can be monitored more effectively when audit logging to an external Syslog server is configured and enabled. As such, real-time filters and alerts can be configured to detect the following CLI commands, as well as their aXAPI and Web/GUI equivalent operations.

- import health-monitor
- no audit enable
- create health-monitor
- no audit enable privilege
- edit health-monitor
- no logging auditlog host

These operations can be detected by matching rules on the Syslog server for the following strings in ACOS log records.

- import health-monitor
- no audit enable
- health external create
- no logging auditlog host
- health external edit

Import, create, and edit operations on external health monitor scripts represent potential threat events when administrators are establishing or are trying to instantiate programs (code) on the ACOS system which could contain malicious content. The audit log operations can be indicators that someone may be disabling logging in the system to avoid its recording or reporting their subsequent activities, which could include external health monitor script access operations.

Especially for ACOS production deployments, it is strongly recommended that these events raise alerts in the organization which promote their inspection and review, in accordance with the organization's security policy.

Review Extended Health Monitor Scripts

External health monitor scripts should be reviewed and audited, especially when alerts described above are raised, to ensure the scripts' integrity and intended use in the ACOS system. Instantiated scripts can be:

- Listed with the show health external command.
- Inspected individually using the show health external <script-name.ext> command, where <script-name.ext> is the filename of a listed script.
- Exported for offline inspection and review with the export health external <script-name.ext> command, where <script-name.ext> is the filename of a listed script.

Securing Other Management Protocols

ACOS supports a variety of other protocols for various management services when they are configured and enabled. These protocols typically have two aspects for security; namely, enabling security features of the protocols and using ACOS ACLs to limit external access to these protocols. These protocols include:

- NTP
- Radius
- SNMP
- TACACS+
- LDAP/LDAPS

NTP

Maintaining accurate time is a critical function in providing accurate and secure network services. The Network Time Protocol (NTP) is a UDP-based protocol which accurately maintains and synchronizes time across devices in the network. For

instance, NTP ensures that timestamps in network device log messages are coherently recorded by logging servers shared among the devices.

The NTP client service in ACOS is disabled by default.

NTP Authentication

It is important to enable NTP authentication for any NTP time source configured in an ACOS system. This will ensure that the contents of NTP messages are not modified and are only exchanged with trusted NTP peers. Administrators can configure NTP authentication with the `ntp auth-key` ACOS command.

This command is used to specify the key ID, algorithm, and shared secret password for authentication to be used with one or more NTP servers. These authentication values must match corresponding values configured on the remote NTP servers. Alternatives for the choice of algorithm include:

- md5 Uses Message Digest Algorithm 5 (MD5) encryption, 128-bits
- sha Uses Security Hash Algorithm (SHA-0) encryption, 160 bits
- sha1 Uses Security Hash Algorithm (SHA-1) encryption, 160 bits (recommended, most secure)

NOTE: SHA-0 was the original version of the SHA. It was found to be flawed due ease of producing hash collisions and was revised as the SHA-1 to strengthen its cryptographic strength.

It is a good practice to include multiple NTP peers on different interfaces to maximize time continuity if one of the NTP peers goes offline or the interface's link goes down.

The following example configures two NTP local network peers with authentication and where the first peer is set as preferred.

```
// Create two authentication keys (29748, 13579) w/ SHA-1.
// Add them to ACOS's list of trusted keys.

ACOS-TH####(config)#ntp auth-key 29748 SHA1 ascii Zn17yf37x
ACOS-TH####(config)#ntp auth-key 13579 SHA1 ascii XxEnc192

ACOS-TH####(config)#ntp trusted-key 29748
ACOS-TH####(config)#ntp trusted-key 13579
```

```
// Configure two NTP servers with their corresponding trusted keys and
enable time
// synchronization with them.
ACOS-TH####(config)#ntp server 10.171.124.36
ACOS-TH####(config-ntpsvr:10.171.124.36)#prefer
ACOS-TH####(config-ntpsvr:10.171.124.36)#key 29748
ACOS-TH####(config-ntpsvr:10.171.124.36)#enable

ACOS-TH####(config)#ntp server 192.69.131.204
ACOS-TH####(config-ntpsvr:192.69.131.204)#key 13579
ACOS-TH####(config-ntpsvr:192.69.131.204)#enable
```

Alternatively, for vThunder/Cloud or SOHO environments where there is no local NTP peer available, a remote NTP peer from NIST can be configured as follows:

```
// Create two authentication keys (12345, 54321) w/ SHA-1.
// Add them to ACOS's list of trusted keys.

ACOS-TH####(config)#ntp auth-key 12345 SHA1 ascii Ugx17hF9yF
ACOS-TH####(config)#ntp auth-key 54321 SHA1 ascii Wny9y6fZX7

ACOS-TH####(config)#ntp trusted-key 12345
ACOS-TH####(config)#ntp trusted-key 54321

// Configure two NTP servers with their corresponding trusted keys and
enable time
// synchronization with them.

ACOS-TH####(config)#ntp server time-a-g.nist.gov
ACOS-TH####(config-ntpsvr:time-a-g.nist.gov)#prefer

ACOS-TH####(config-ntpsvr:time-a-g.nist.gov)#key 12345

ACOS-TH####(config-ntpsvr:time-a-g.nist.gov)#enable
ACOS-TH####(config)#ntp server time-a-b.nist.gov

ACOS-TH####(config-ntpsvr:time-b-g.nist.gov)#key 54321
ACOS-TH####(config-ntpsvr:time-b-g.nist.gov)#enable
```

NOTE: Authentication keys are assigned at the time of registration with the NIST service, as described in https://www.nist.gov/pml/time-and-frequency-division/time-services/nist-authenticated-ntp-service.

NOTE: For a list of NIST NTP time servers, see https://tf.nist.gov/tf-cgi/servers.cgi.

NTP Interfaces and ACLs

To limit NTP exchanges with selected, trusted servers on their desired ACOS interfaces, ACLs can be applied. The following example builds on those with ACLs above in order to enable NTP exchanges with the 10.171.124.36 server on the `mgmt` port and the 192.69.131.204 server on the `eth1` data port using the standard NTP port 123.

```
// Add NTP 10.171.124.36:123, mgmt port rule to mgmt ACL 100
ACOS-TH####(config)#access-list 100 10 remark "ACL – NTP mgmt. port, UDP
Src Port 123"
ACOS-TH####(config)#access-list 100 11 permit udp host 10.171.124.36 eq
123 any

// Add NTP 192.69.131.204:123, eth1 port rule to eth1 ACL 101
ACOS-TH####(config)#access-list 101 10 remark "ACL – NTP eth1 port, UDP
Src Port 123"
ACOS-TH####(config)#access-list 101 11 permit udp host 192.69.131.204 eq
123 any
```

Disable Access to NTP Server on ACOS

To prevent ACOS from acting as an NTP server and responding to the requests received from NTP clients, you can use the `disable-management service ntp` CLI command. Configuring the `disable-management service ntp` CLI command at the configuration level disables access to the NTP service and stops ACOS from responding to the NTP client requests.

An Access Control List (ACL) permits or denies management access through the interface by specific hosts or subnets. You can use `the enable-management service acl-v4` command to apply ACL on incoming NTP requests on any or all interfaces OR apply ACL on all interfaces. Configuring the `enable-management service acl-v4`

command at the management level stops the services from responding to the incoming NTP client requests.

The following example shows how to stop ACOS from responding to the incoming NTP client requests on the specified port ethernet 3 using the disable-management service:

```
ACOS-TH####(config)#disable-management service ntp
You may lose connection by disabling the ntp service.
Continue? [yes or no]: yes
ACOS-TH####(config-disable-management ntp)#ethernet 3
```

A10 recommends disabling NTP service on all interfaces from which you don't expect NTP to be used.

The following example shows how to configure an ACL for incoming NTP request on any or all interfaces using the enable-management service:

```
ACOS-TH####(config)#enable-management service ntp
ACOS-TH####(config-enable-management ntp)#acl-v4 1
ACOS-TH####(config-enable-management ntp-acl-v4)#ethernet 1
```

To view where NTP service is enabled, use the following show command:

```
ACOS#show management
```

SNMP

Simple Network Management Protocol (SNMP) is an Internet Standard protocol widely used in network management for network monitoring with three versions of significance. SNMPv1 is the original version of the protocol. SNMPv2c and SNMPv3 bring feature improvements in performance, flexibility and security.

SNMPv2c uses community names for read and write access, much like passwords are used for authentication, to distinguish privilege. SNMPv2c passes these community names in clear-text on the wire, so it is still considered weak from a security perspective. Malicious users could capture these community names and use them in SNMP SET commands to perform unauthorized and damaging changes to the ACOS system or use SNMP GET commands to access unauthorized or sensitive information from the system.

SNMPv3 adds a higher degree of security to SNMPv2c by authenticating and encrypting packets over the network.

The following subsections share recommendations for securely configuring SNMP in ACOS systems.

For Security Policies that Prohibit SNMP

SNMP support in ACOS is disabled by default and is accordingly compliant with organization security policies that mandate SNMP be summarily disabled in all networking systems. If an ACOS system's configuration has enabled SNMP, this service can be summarily disabled with the no form of the `snmp-server enable service` ACOS command. For example:

```
ACOS-TH####(config)#no snmp-server enable service
```

Alternatively, for device management networks that allow and require SNMP, review and consider the following subsections.

SNMPv3 Configuration

For organizations allowing SNMP in their security policy, SNMPv3 should be used and configured in the ACOS system using the following steps.

Enable SNMP and Configure SNMPv3 Engine ID

In SNMPv3, SNMP user authentication and privacy digests are derived from an engine ID and user passwords. As such, this identifier must be configured before adding SNMPv3 user accounts.

NOTE: If the SNMPv3 engine ID is changed, all SNMPv3 user accounts will need to be reconfigured.

If the SNMP service is enabled in ACOS, the engine ID can be configured using the snmp-server engineID command. For example, to do both operations:

```
ACOS-TH####(config)#snmp-server enable service
ACOS-TH####(config)#snmp-server engineID 1234567890

ACOS-TH####(config)#show snmp-server engineID
EngineID: 80001f8804313233343536373839 30
```

Configure SNMP Views

Beyond overall access to SNMP services in ACOS, SNMP views grant or restrict user groups access to specific portions of the MIB. As such, they can be used to allow certain SNMP users access to sensitive information in the MIB, while denying access for the same information to less trusted users. In ACOS, SNMPv3 group definitions include specific views to control MIB access for their SNMP users.

For example, to define a view called “mibs-wo-ifs-access” that permits access to all of MIB-2 (1.3.6.1.2.1) and A10 MIB (1.3.6.1.4.1.22610), while excluding access to the Interfaces branch (1.3.6.1.2.1.2) under MIB-2 and the axInterfaces branch (1.3.6.1.4.1.22610.2.1.7.1) under the A10 MIB:

```
ACOS-TH####(config)#snmp-server view mibs-wo-ifs-access 1.3.6.1.2.1
included
ACOS-TH####(config)#snmp-server view mibs-wo-ifs-access 1.3.6.1.4.1.22610
included
```

```
ACOS-TH####(config)#snmp-server view mibs-wo-ifs-access 1.3.6.1.2.1.2
excluded
ACOS-TH####(config)#snmp-server view mibs-wo-ifs-access
1.3.6.1.4.1.22610.2.4.1.7.1 excluded
```

Configure SNMPv3 Groups

SNMPv3 supports three basic security methods which can be specified for various SNMPv3 user groups along with the respective SNMP views they will have read access to:

- noauth - Does not use any authentication of packets, aka `noAuthNoPriv`.
- auth - Uses packet authentication but does not encrypt the packets, aka `authNoPriv`.
- priv - Uses packet authentication and encryption, aka `authPriv`. (recommended)

Users added to these groups will include the appropriate and corresponding selections for security algorithms. For example, to define a group called “users-group1” that enables both packet authentication and encryption for read access to the view in the example above:

```
ACOS-TH####(config)#snmp-server group users-group1 v3 priv read mibs-wo-ifs-access
```

Configure SNMPv3 Users

Having completed the previous steps, SNMPv3 user accounts can now be defined. ACOS administrators will be able to select the authentication and encryption algorithms to be used on an individual user basis, including the following options.

- auth Specifies the encryption method for user authentication.
  - md5 Use Message Digest Algorithm 5 (MD5) encryption, 128-bits
  - sha Use Security Hash Algorithm (SHA) encryption, 160 bits (recommended, most secure)
- priv Specifies the encryption method to use for user privacy.
  - aes Use Advanced Encryption Standard (AES) algorithm. This uses a fixed block size of 128 bits, and has a key size of 128, 192, or 256 bits. (recommended, most secure)
  - sha Use Data Encryption Standard (DES) algorithm to apply a 56-bit key to each 64-bit block of data. This is considered strong encryption.

For example, to add an SNMPv3 user called “user-5” for the group in the example above and passwords for both authentication and encryption using the stronger of SNMPv3 cryptographic algorithms:

```
ACOS-TH####(config)#snmp-server SNMPv3 user user-5 group users-group1 v3 auth sha
```

NOTE: SNMPv3 passwords in ACOS can be 8-31 printable ASCII characters long and may only contain -.()special characters.

Configure SNMPv3 Traps

SNMP traps are alert messages sent from a monitored SNMP-enabled device to a central collector, colloquially referred to as an SNMP trap receiver, SNMP Manager, or a Network Management System (NMS) device. In SNMPv3 managed networks, the identity and security settings need to be configured for this class of messages, as

they do not have the benefit of a user or manager application to enter or select them.

For this purpose, ACOS supports a modest SNMPv3-related extension to the snmp-server host command normally used to configure SNMPv1/2c for a given trap receiver. This command extension, user <name>, identifies a configured SNMP user account and associated security setting to use when generating SNMPv3-compatible traps. Furthermore, since these messages will only involve SNMP notifications rather than read/write accessible objects, it is a good practice to limit the associated view-scope to NOTIFICATION-TYPE MIB items or the related MIB branches.

The following example first defines an SNMP view that includes all ACOS-specific SNMP traps (axNotification - 1.3.6.1.4.1.22610.2.4.3.12) and then defines an SNMPv3 group for the view, along with recommended security method. Next, an SNMPv3 user account is defined using this groups. Lastly, SNMPv3 hosts are defined to be the receivers of traps (10.10.10.12 and 192.10.10.12) generated within the scope of the view; including the associated cryptographic selections and passwords.

```
ACOS-TH####(config)#snmp-server view acos-mib-trap
1.3.6.1.4.1.22610.2.4.3.12 included
ACOS-TH####(config)#snmp-server group users-group1 v3 priv read acos-mib-
traps
ACOS-TH####(config)#snmp-server SNMPv3 user user-acos-traps group users-
group1 v3 auth sha *XynC2MQD< priv aes ^6"}{WBN9]
ACOS-TH####(config)#snmp-server host 10.10.10.12 version v3 user user-
acos-traps
ACOS-TH####(config)#snmp-server host 192.10.10.12 version v3 user user-
acos-traps
ACOS-TH####(config)#snmp-server enable traps all
```

Configure SNMP Interfaces and ACLs

With the ACOS SNMP service configured, the next step is to provision it for access with external SNMP clients. This includes enabling the service for access from selected interfaces of the ACOS device and optionally restricting access to selected, secured SNMP Networks Management Systems (NMSs) via ACLs.

NOTE: There are a couple of different ways to do ACL for ACOS management services as indicated in the examples that follow.

SNMP is enabled for access using the enable management ACOS command. For example, to enable SNMP access on the management and eth1 interfaces of the ACOS device:

```
ACOS-TH####(config)#enable-management service snmp
ACOS-TH####(config-enable-management snmp)#management
ACOS-TH####(config-enable-management snmp)#ethernet 1
```

Additionally, to generally restrict access on clients allowed to access these SNMP services on 10.10.10.120 and 192.10.10.120 to clients from specific management and eth1 subnetworks; respectively:

```
// SNMP, mgmt. port already enabled
// Allow SNMP access from 10.10.10.0/24 subnet, SNMP port rule to mgmt ACL
100

ACOS-TH####(config)#access-list 100 15 remark "ACL – mgmt port @ SNMP"
ACOS-TH####(config)#access-list 100 16 permit udp 10.10.10.0 /24 any eq
161

// SNMP, eth1 port already enabled
// Allow SNMP access from 192.10.10.0/24 subnet, SNMP port rule to eth1
ACL 101

ACOS-TH####(config)#access-list 101 15 remark "ACL – eth1 port @ SNMP"
ACOS-TH####(config)#access-list 101 16 permit udp 192.10.10.0 /24 any eq
161
```

Alternately, to restrict access from specific client, SNMP NMS systems at 10.10.10.12 for access to ACOS via the system's management interface only:

```
// SNMP, mgmt. port already enabled
// Allow SNMP access from 10.10.10.12 host, SNMP port rule to mgmt ACL 100

ACOS-TH####(config)#access-list 100 15 remark "ACL – mgmt port @ SNMP,
from 10.10.10.12"
ACOS-TH####(config)#access-list 100 16 permit udp 10.10.10.12 any eq 161

// SNMP, eth1 port already enabled
// Leave blocked SNMP access on eth1 - ACL 101 comment to document
```

```
ACOS-TH####(config)#access-list 101 15 remark "ACL – eth1 port @ SNMP, no rule to permit"
```

When SNMPv3 Is Not an Option

Real-world deployments can still encounter environments with legacy SNMP management resources where SNMPv3 is not a viable option. When this is the case, review the following considerations to better secure SNMP services:

- At least seek to support SNMPv2c.
  - Modest security is still better than no security.
- Never (never, ever) use “public” for a community string.
  - This is the 1st community string in even most simple-minded hacker’s playbook
- Treat community strings like device/system passwords. Namely, with strong password strength.
  - This may be more cumbersome to manage, but it will be much more secure.
- If possible, do not define or configure a read-write (rw) community
  - Write-access via this community to SNMP objects can allow potentially malicious users (and hackers) to modify the state of the SNMP-enabled device and adversely impact the normal operation of the system to affect a Denial-Of-Service (DOS) of the system and/or its connected network environment.
- Apply strict access controls (ACLs) for Read-only (ro) community SNMP managers as a best means to control access to sensitive information that could be exposed from the device’s MIB.
  - There are few, if any, alternatives to contain sensitive information leakage for this access vector.

NOTE: SNMPv1/v2c in ACOS does not support read-write (rw) communities or SNMP SET operations, to avoid such potential security exposures.

RADIUS

Remote Access Dial-In User Service (RADIUS) is an IETF standard for Authentication, Authorization and Accounting (AAA). Like TACACS+ and LDAP the RADIUS protocol

can be used to externally authenticate users (administrators) of the ACOS system in addition to its use authorization and accounting services as discussed separately and later in this chapter. Compared to TACACS+ the Radius protocol is faster yet less reliable, owing to its use of UDP rather than TCP. RADIUS is also the less secure of the two as it only encrypts the password fields rather than the entire message payloads.

The following subsections share recommendations for securely configuring RADIUS in ACOS systems.

RADIUS Authentication

RADIUS servers configured in an ACOS system must specify the common, shared secret values used to encrypt the message password during session initialization. These shared secret values should be strong passwords and consistent with the organization's security policies.

NOTE: ACOS only supports RADIUS servers that include a secret key or secret server value in their installed configurations.

It is a good practice to configure multiple RADIUS servers on different interfaces, for redundancy and improved availability. ACOS supports a maximum of two (2) configured RADIUS servers with preference being in the order they are configured.

The following example configures two RADIUS servers, with authentication preference to the first server (10.171.124.37). It then shows how to enable both RADIUS and local user authentication methods for the system, with preference to the RADIUS mechanism.

```
ACOS-TH####(config)#radius-server host 10.171.124.37 secret Zn17yf37x
ACOS-TH####(config)#radius-server host 192.69.131.205 secret Vke1324as
ACOS-TH####(config)#radius-server message-authenticator-verify-enable

ACOS-TH####(config)#authentication type radius local
```

NOTE: Radius secret values in ACOS can be up to 128 printable ASCII characters long and may only contain -.() special characters.
The `message-authenticator-verify-enable` option is available from ACOS version 6.0.6 onwards.

RADIUS Interfaces and ACLs

To limit RADIUS connections with selected, trusted servers on their desired ACOS interfaces, ACLs can be applied. The following example builds on those with ACLs above in order to enable RADIUS authentication and accounting exchanges with the 10.171.124.37 server on the `gmt` port and the 192.69.131.205 server on the `eth1` data port.

```
// Add RADIUS 10.171.124.37:1812/1813, gmt. port rule to gmt. ACL 100
ACOS-TH####(config)#access-list 100 25 remark "ACL – RADIUS gmt.. port,
UDP Src Port 1812/13"
ACOS-TH####(config)#access-list 100 26 permit udp host 10.171.124.37 eq
1812 any
ACOS-TH####(config)#access-list 100 27 permit udp host 10.171.124.37 eq
1813 any

// Add RADIUS 192.69.131.205:1812/1813, eth1 port rule to eth1 ACL 101
ACOS-TH####(config)#access-list 101 25 remark "ACL – RADIUS eth1 port, UDP
Src Port 1812/13"
ACOS-TH####(config)#access-list 101 26 permit udp host 192.69.131.205 eq
1812 any
ACOS-TH####(config)#access-list 101 27 permit udp host 192.69.131.205 eq
1813 any
```

NOTE: Prior to IANA's assignment of ports 1812 and 1813, ports 1645 and 1646 (authentication and accounting, respectively) were the de facto standard ports used for RADIUS. The use of ports 1645 and 1646 continues to be common practice for many RADIUS server configurations.

TACACS+

TACACS+ is a Cisco protocol that can be used to externally authenticate users (administrators) of the ACOS system, as well as provide authorization and accounting services discussed later in this chapter. Compared to Radius the TACACS+ protocol is more reliable yet slower, owing to its use of TCP rather than UDP. TACACS+ is also the more secure of the two as it encrypts its message payloads rather than just the password field.

The following subsections share recommendations for securely configuring TACACS+ in ACOS systems.

TACACS+ Authentication

TACACS+ servers configured in an ACOS system must specify the common, shared secret values used to encrypt message payloads. These shared secret values should be strong passwords and consistent with the organization's security policies.

NOTE: ACOS only supports TACACS+ servers that include a secret key or secret server value in their installed configurations.

It is a good practice to configure multiple TACACS+ servers on different interfaces for redundancy and improved availability. ACOS supports a maximum of two (2) configured TACACS+ servers with preference being in the order they are configured.

The following example configures two TACACS+ servers, with authentication preference to the first server (10.171.124.37). It then enables both TACACS+ and local user authentication methods for the system, with preference to the TACACS+ mechanism.

```
ACOS-TH####(config)#tacacs-server host 10.171.124.37 secret Zn17yf37x
ACOS-TH####(config)#tacacs-server host 192.69.131.205 secret Vke1324as

ACOS-TH####(config)#authentication type tacplus local
```

NOTE: TACACS+ secret values in ACOS can be up to 127 printable ASCII characters long and may only contain -.()special characters.

TACACS+ Interfaces and ACLs

To limit TACACS+ connections with selected, trusted servers on their desired ACOS interfaces, ACLs can be applied. The following example builds on those with ACLs above in order to enable TACACS+ connections with the 10.171.124.37 server on the `gmt`. port and the 192.69.131.205 server on the `eth1` data port using the standard TACACS+ port 49.

```
// Add TACACS+ 10.171.124.37:49, gmt. port rule to gmt. ACL 100
ACOS-TH####(config)#access-list 100 20 remark "ACL – TACACS+ gmt.. port,
TCP Src Port 49"
ACOS-TH####(config)#access-list 100 21 permit tcp host 10.171.124.37 eq 49
```

```
any

// Add TACACS+ 192.69.131.205:49, eth1 port rule to eth1 ACL 101
ACOS-TH####(config)#access-list 101 20 remark "ACL – TACACS+ eth1 port,
TCP Src Port 49"
ACOS-TH####(config)#access-list 101 21 permit tcp host 192.69.131.205 eq
49 any
```

LDAP/LDAPS

Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard commonly used in network infrastructures for administrative user identity and capabilities management. LDAP's scope focuses singularly on user identification, hierarchy, capabilities, and authentication. LDAP has no provisions for authorization or accounting services.

LDAP has no inherent security considerations for secure communications and messaging. For security, LDAP relies upon encapsulating exchanges under TLS called LDAPS (LDAP over SSL). Compared to TACACS+ and RADIUS, LDAPS is the most secure approach for external authentication services access. It is commonplace to combine LDAP with TACACS+ and/or RADIUS for authorization and accounting AAA services.

LDAPS is commonly used in Microsoft Active Directory environments.

The following subsections share recommendations for securely configuring LDAPS in ACOS systems.

LDAP Security

A10 recommends that LDAP servers configured in an ACOS system enable operation over TLS by including the ssl parameter to ensure the secure exchange of LDAP protocol messages.

It is a good practice to configure multiple LDAPS servers on different interfaces, for redundancy and improved availability. ACOS supports a maximum of two (2) configured LDAPS servers with preference being in the order they are configured.

The following example configures two LDAPS servers, with preference to the first server (10.171.124.37). It then enables both LDAP and local user authentication methods for the system, with preference to the LDAP mechanism.

```
ACOS-TH####(config)#ldap-server host 10.171.124.37 cn LDAPServer-1 dn
ou=StaffAccounts,ou=ServiceAccounts,dc=ad,dc=example,dc=org ssl

ACOS-TH####(config)#ldap-server host 192.69.131.205 cn LDAPServer-2 dn
ou=StaffAccounts,ou=ServiceAccounts,dc=ad,dc=example,dc=edu ssl

ACOS-TH####(config)#authentication type ldap local
```

LDAPS Interfaces and ACLs

To limit LDAPS connections with selected, trusted servers on their desired ACOS interfaces, ACLs can be applied. The following example builds on those with ACLs above in order to enable LDAPS connections with the 10.171.124.37 server on the `gmt`. port and the 192.69.131.205 server on the eth1 data port using the standard LDAPS port 636.

```
// Add LDAPS 10.171.124.37:636, gmt. port rule to gmt. ACL 100
ACOS-TH####(config)#access-list 100 30 remark "ACL – LDAPS gmt.. port, TCP
Src Port 636"
ACOS-TH####(config)#access-list 100 31 permit tcp host 10.171.124.37 eq
636 any

// Add LDAPS 192.69.131.205:636, eth1 port rule to eth1 ACL 101
ACOS-TH####(config)#access-list 101 30 remark "ACL – LDAPS eth1 port, TCP
Src Port 636"
ACOS-TH####(config)#access-list 101 31 permit tcp host 192.69.131.205 eq
636 any
```

Logging Practices

Event logging provides visibility into the operation of an ACOS system as well as the underlying networks connected to the system. Logging is critical to the security of ACOS systems as it provides an ability to review and audit the history of activities on the system. This knowledge gained from logging can be used:

- To alert the organization on occasions of activities warranting timely review.
- In forensic investigations of security events – such as breaches, intrusions, service

denials, scan attempts, probes, etc.

- To troubleshoot network and service issues impacting service availability.

Logs can be stored locally on the ACOS system or in more secure configurations can be sent to remote, centralized servers via the industry-standard Syslog protocol. Best practice is to separate system and audit logging using an isolated management network, rather than mix logging with data or control networks. To configure logging to use the management interface, use ip-control-apps-use-mgmt-port command. Typically, severity levels of the reported events are used to determine the volume, extent, and targets of reported events.

The following subsections share recommendations for securely configuring event logging in ACOS systems.

Logging Levels

ACOS supports following severities:

emergency	Level 0	emergency events – system unusable
alert	Level 1	alert events – take action immediately
critical	Level 2	system is in critical condition
error	Level 3	system has an error condition
warning	Level 4	system has warning conditions
notifications	Level 5	normal but significant conditions
information	Level 6	informational messages
debugging	Level 7	debug level messages

As a general guideline, it is a good practice to enable level 6 (information) and level 7 (debugging) messages for local file logging only as these events are typically used for troubleshooting. With these levels, remote logs can be easily overrun or the bandwidth of the management ACOS CPU(s) may be outstripped, resulting in dropped or missed events.

Logging higher level events (emergency (0) – warning notifications (5)) to remote servers for alerts, forensic, and monitoring purposes is recommended. These levels

should include the information needed for these activities, consistent with the organization's security policy.

NOTE: On some ACOS systems, notably CGN-based systems, warning event volume at these levels may overrun the capacity of the ACOS management plane, the logging servers, or both.

When configuring the logging level in ACOS, the indicated level will be the lowest logging level and will enable all higher level. For example, to enable remote logging to Syslog for only error, critical, alert and emergency events:

```
ACOS-TH####(config)#logging syslog error
```

Console and Monitor Logging

By default, ACOS will not display real time logging events as they occur to the ACOS system's console or to remote CLI sessions in the EXEC mode (entered via the `enable` ACOS CLI command). For organizations with security policies that seek higher agility and real-time awareness for their administrator community, ACOS allows these logging events to be configured for these displays at the discretion of the organization via the `logging console` and `logging monitor` CLI commands.

For example, to configure ACOS to only display only emergency and alert events on the ACOS system's console and display only emergency on the remote, CLI sessions in EXEC mode:

```
ACOS-TH####(config)#logging console alert
ACOS-TH####(config)#logging monitor emergency
```

Securing Syslog Servers

It is a good practice to configure multiple Syslog servers on different interfaces for redundancy and improved availability. When multiple Syslog servers are configured, ACOS will replicate logging event messages to all the servers indicated. ACOS supports a maximum of ten (10) configured Syslog servers.

Syslog servers can be configured in ACOS using the logging host command. By default, the ACOS device can reach remote log servers only if they are reachable

through the ACOS device's data ports, not the management port. To enable the ACOS device to reach remote log servers through the management port, include the use-mgmt parameter.

The default protocol for syslog is UDP and is insecure. A10 recommends using syslog TCP over TLS to secure the logs sent to the syslog server. Enabling TLS requires more processing to encrypt log messages thus the control CPU utilization will be higher when TLS is enabled.

When using syslog TCP over TLS, a CA certificate must be imported and used to validate the syslog server's cert. This is needed before the configuration can succeed. Before setting a CA, first import the CA cert, by using the command:

```
ACOS-TH####(config)#import ca-cert syslog-ca.cert use-mgmt-port
scp://your_user_name@host:/path_to_file/syslog-ca.cert
ACOS-TH####(config:)#show pki ca-cert

Name                Type                          Expiration  Status

-------------------------------------------------------------------------
----
syslog-tls-ca       certificate  Oct 22 00:02:09 2029 GMT  [Unexpired,
Unbound]
default_ca_bundle   certificate  Jan 28 12:00:00 2028 GMT  [Unexpired,
Unbound]

ACOS-TH####(config)#template syslog-over-tls
ACOS-TH####(config)#ca-cert syslog-tls-ca.cert
```

After importing the ca cert, and associating it with the syslog template, you may configure the logging hosts. The following example configures two Syslog servers, with one constrained for access on the `mgmt` port.

```
ACOS-TH####(config)#logging host 10.171.124.37 use-mgmt tcp over-tls
ACOS-TH####(config)#logging host 192.69.131.205 use-mgmt tcp over-tls
```

NOTE: For Syslog logging configured using the logging host command, log events from the ACOS management and control planes will be replicated across the configured servers. Log events from the ACOS data plane, however, will not be replicated. To support data plane logging replication, see the Advance Logging Services discussion below.

Syslog Interfaces and ACLs

To limit Syslog connections with selected, trusted servers on their desired ACOS interfaces, ACLs can be applied. The following example builds on those with ACLs above in order to enable Syslog connections with the 10.171.124.37 server on the `mgmt` port and the 192.69.131.205 server on the `eth1` data port using the standard Syslog port 514.

```
// Add Syslog 10.171.124.37:514, gmt. port rule to gmt. ACL 100
//
ACOS-TH####(config)#access-list 100 35 remark "ACL – Syslog gmt.. port,
TCP Src Port 514"
ACOS-TH####(config)#access-list 100 36 permit tcp host 10.171.124.37 eq
514 any

// Add Syslog 192.69.131.205:514, eth1 port rule to eth1 ACL 101
//
ACOS-TH####(config)#access-list 101 35 remark "ACL – Syslog eth1 port, TCP
Src Port 514"
ACOS-TH####(config)#access-list 101 36 permit tcp host 192.69.131.205 eq
514 any
```

Advanced Logging Service

ACOS supports an event logging service, called ACOS Events, that can be used as an alternative to the traditional logging hosts service. The ACOS Events service is configurable through the acos-events CLI command and supports advanced logging features available for groups of log servers; such as:

- Replication Across Servers
- Syslog, CEF, and LEEF log formats
- Data Plane Event Replication
- Integrated Logging Server Health Check
- Round-Robin Event Reporting
- Major Module Events Include/Exclude
- Rate Limiting
- Rules to Include/Exclude Event Groups

The same principles described above can be applied to ACOS Events. For more information on this service, see the ACOS product documentation.

Audit Logging Practices

The ability to monitor and review a history of activities performed on the ACOS system by administrators and administrative applications is essential to an organizations security awareness and change management. It also provides agility in detecting intentioned or mis-intentioned mal-behavior. Auditing logging in ACOS provides this capability by logging the date and time for the following types of system management events.

- Administrator logins and log outs for CLI, GUI, and aXAPI sessions
- Unsuccessful administrator login attempts
- Configuration changes. All attempts to change the configuration are logged, even if they are unsuccessful
- CLI commands at the Privileged EXEC level (if audit logging is enabled for this level)

Audit logging is configured and administered separately from general Syslog logging, described earlier. The following subsections share hardening recommendations and practices for this service.

Audit Logging Enabled by Default

In ACOS, audit logging is enabled by default. Moreover, and very importantly, configuration activities to disable audit logging are not saved in the running configuration which means that turning off this service, with the no audit enable command, will not persist across ACOS system reload and reboot operations.

Configuring Audit Logging

ACOS systems, especially in production deployments, should configure this service to log privileged mode CLI commands, in addition to EXEC mode commands supported by default. Privileged mode command logging can be enabled as follows.

```
ACOS-TH####(config)#audit enable privilege
```

Typically, the number of entries recorded in the audit log would be considered next, especially for logs maintained on the ACOS system. Since it is a bad practice to rely on logs not centrally stored, this is a moot point.

Audit Logging to Remote Syslog

Audit logging should always be sent to centralized remote syslog servers where they are free from manipulation by malicious activities in the network device. This service can be configured and restricted to selected ACOS system interfaces, as described below.

Audit Logging to Syslog

ACOS audit logging can and should be configured to report log events to Syslog, rather than a local log file, with the logging auditlog host command. For example:

```
ACOS-TH####(config)#logging auditlog host 10.171.124.38
```

NOTE: ACOS currently supports only one (1) configured Syslog server for audit logging.

Audit Logging Interfaces and ACLs

To limit Syslog connections for audit logging with the selected, trusted servers on the desired ACOS interfaces, ACLs can be applied. The following example builds on those with ACLs above in order to enable this service with the 10.171.124.38 server on the `mgmt` port using the standard Syslog port 514.

```
// Add Syslog of Audit Log for 10.171.124.38:514, mgmt port rule to mgmt
ACL 100
//
ACOS-TH####(config)#access-list 100 40 remark "ACL – Syslog of Audit Log,
TCP Src Port 514"
ACOS-TH####(config)#access-list 100 41 permit tcp host 10.171.124.38 eq
514 any
```

NOTE: Audit logging activity to the Syslog server will be very modest in both transaction rate and bandwidth, so using the limited bandwidth mgmt port should not pose performance impact to the ACOS system.

Monitoring Audit Logging Activities

Administrator and aXAPI application activities to configure audit logs in the ACOS system can be monitored and trigger alerts. Very importantly, activities to disable this logging, especially in a deployed production system, can be an indicator of mal-intent and attempts to compromise the integrity of the ACOS system.

As such, real-time filters and alerts can be configured to detect the following CLI commands, as well as their aXAPI and Web/GUI equivalent operations:

- no audit enable
- no logging auditlog host
- no audit enable privilege

These audit log operations can be indicators that someone may be disabling logging in the system to avoid its recording or reporting their subsequent activities, potentially with malicious intent. It is strongly recommended that these events raise alerts in the organization which promote their inspection and review, in accordance with the organization's security policy.

Hardening the ACOS Control Plane

This chapter addresses hardening considerations for the ACOS control plane consisting of protocols supporting routing, link-state, neighbor-discovery, signaling and other protocols that define and maintain the topology and state of the network. Namely, protocols that support and coordinate the movement of data through the ACOS data plane.

Hardening of the ACOS control plane is critical to ensure that the services of the ACOS data plane are available and secure. This includes the following protocols:

- Internet Control Message Protocol (ICMP)
- Dynamic Host Configuration Protocol (DHCP)
- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)
- Intermediate System – Intermediate System (IS-IS)
- Routing Information Protocol (RIP)
- Bi-Directional Forwarding Detection (BFD)

Other control plane protocols supported by ACOS are limited in their ability and scope to be secured. These include the following.

- ACOS High Availability Protocol (VRRP-A)
- ACOS Virtual Chassis System (aVCS) control protocol
- Link Aggregation Control Protocol (LACP)
- Link Layer Discovery Protocol (LLDP)
- Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP)

General Control Plane Hardening

To protect the ACOS control plane from potential threats and ensure optimal performance, the following configurations are recommended.

ICMP Redirect and Destination Unreachable

A malicious user can adversely impact the CPU usage, and hence performance, of routing services in ACOS by continually sending packets to an ACOS device which forces it to respond with ICMP redirect or ICMP unreachable messages. To avoid such exploits, configure ACOS to not send ICMP redirect or ICMP unreachable messages for both Ipv4. For example:

```
ACOS-TH####(config)#ip icmp disable redirect
ACOS-TH####(config)#ip icmp disable unreachable
```

DHCP Relay

A DHCP relay is an agent that forwards DHCP packets between clients and servers. ACOS systems can be configured for this service to relay DHCP traffic between DHCP clients and DHCP servers located in different VLANs or subnets. When enabled, the ACOS device intercepts broadcast DHCP packets sent by clients on interfaces configured with the helper address. It then places the receiving interface's IP address (not the helper address) in the relay gateway address field and forwards the DHCP packet to the server. When the DHCP server replies, the ACOS device forwards the response to the client.

The DHCP relay service in ACOS is disabled by default. If this service is not needed in the target network topology, it is recommended to leave the service disabled.

Routing Protocol Hardening

There are many advised and recommended practices for routing in the industry. From a security point of view, it is important to consider practices that ensure the integrity of routing updates exchanged with trusted neighbors. Malicious individuals or groups that can instantiate unauthorized routers in the network can send phony

route advertisements that may alter or disrupt the intended flow of traffic, allowing them to observe sensitive information, exfiltrate data, or deny service in the network.

To avoid these compromises, enable authentication features supported by the underlying routing protocols to ensure that only trusted routers are participating in routing exchanges for the deployed network.

BGP

Border Gateway Protocol (BGP) is often called the routing protocol of the Internet. It is the protocol that manages how packets are routed across the internet by exchanging routing and reachability information between edge routers. BGP is a popular target of attackers. To increase security of the BGP configuration for ACOS consider enabling security factors for BGP.

NOTE: In addition to the following discussions, the ANSSI BGP Configuration Best Practices is a good resource for general and security best practice recommendations for BGP.

EBGP-Multihop

When external BGP (EBGP) peers are not directly connected to each other, they must cross one or more non-BGP routers to reach each other. Configuring EBGP multihop enables the peers to pass through the other routers to form peer relationships and exchange update messages. EBGP multihop uses the 1-byte Time-To-Live (TTL) packet value to limit the number intermediate devices the BGP packets can traverse.

Starting values for the TTL are commonly 64 to 255. However, for more restricted topologies the TTL can be initiated with a smaller value. The following example sets a maximum of two intermediate devices that can be traversed by setting the `ebgp-multihop` parameter to 2.

```
ACOS-TH####(config)#router bgp 123
ACOS-TH####(config-bgp:123)# bgp router-id 10.10.10.1

ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 remote-as 123
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 ebgp-multihop 2
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 enforce-multihop
```

BGP MD5 Authentication

BGP supports a Message Digest 5 (MD5) authentication mechanism. When enabled for BGP peers, any Transmission Control Protocol (TCP) segment belonging to BGP exchanged between the peers is verified and accepted only if authentication is successful. To enable and configure this mechanism use the password setting, as follows:

```
ACOS-TH####(config)#router bgp 123
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 password
MNQHsKkg4oC70A2D
```

NOTE: BGP passwords in ACOS can be up to 80 printable ASCII characters long and cannot contain‘”"<>&\/? special characters.

BGP Prefix Limits

To avoid memory exhaustion and the ACOS BGP service from being interrupted, especially in configurations where portions of all Internet prefixes may need to be stored, configure a maximum number of prefixes for each BGP peer using the maximum-prefix setting. The following example configures 2 BGP peers with 256 and 2048 prefix maximums. The second will generate a warning when 85% of the limit is reached, rather than the default 75%:

```
ACOS-TH####(config)#router bgp 123
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 maximum-prefix 256

ACOS-TH####(config)#router bgp 321
ACOS-TH####(config-bgp:321)#neighbor 10.10.10.220 maximum-prefix 2048 85
```

BGP Prefix Filters

ACOS prefix lists can be used to permit or deny specific prefixes that are sent or received by the ACOS BGP service. They should be used to ensure network traffic is sent over intended paths and should be applied to BGP peers for both inbound and outbound prefixes. ACOS supports prefix filtering by BGP autonomous system (AS) path access lists where by the ACOS device can filter incoming received and outgoing advertised prefixes based on the AS-path attribute of a prefix.

In the example below, inbound prefixes are restricted to those originated by the indicated remote AS and outbound prefixes advertised to those originated by the local AS (e.g. the ACOS device).

```
ACOS-TH####(config)#ip as-path AS-PLIST-IN  ^321$ permit
ACOS-TH####(config)#ip as-path AS-PLIST-OUT ^

ACOS-TH####(config)#router bgp 123
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 remote-as 321
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 filter-list AS-PLIST-IN
in
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 filter-list AS-PLIST-OUT
out
```

For the example below, prefix lists are defined such that 192.168.1.0/24 and 192.168.9.0/24 are the only prefixes accepted inbound from the BGP peer and the prefix 172.122.1.0/24 is the only route allowed to be advertised to the BGP peer

```
ACOS-TH####(config)#ip prefix-list LIST-IN seq 5 permit 192.168.1.0/24
ACOS-TH####(config)#ip prefix-list LIST-IN seq 10 permit 192.168.9.0/24
ACOS-TH####(config)#ip prefix-list LIST-IN seq 15 deny 0.0.0.0/0 le 32

ACOS-TH####(config)#ip prefix-list LIST-OUT seq 5 permit 172.122.1.0/24

ACOS-TH####(config)#router bgp 123
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 remote-as 321
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 filter-list LIST-IN in
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 filter-list LIST-OUT out
```

OSPF

Open Shortest Path First (OSPF) is a routing protocol for IP networks and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS). As an IGP, OSPF is also a popular target of interior attackers to disrupt or compromise network integrity. ACOS supports OSPFv2 for iPv4 and OSPFv3 for IPv6.

To increase security of the OSPF configuration for ACOS consider enabling the OSPF security features described below.

OSPF MD5 Authentication

OSPFv3 uses IPSec to secure communications between neighbors and does not require separate hardening considerations.

OSPFv2 supports an MD5 authentication mechanism which should be enabled along with a password for configured OSPF instances. The following iPv4 example defines an OSPF instance and shows how to enable it for MD5 password authentication.

```
ACOS-TH####(config)#router ospf 1
ACOS-TH####(config-ospf:1)#router-id 10.10.10.1
ACOS-TH####(config-ospf:1)#area 0 authentication message-digest

ACOS-TH####(config)#interface ethernet 3
ACOS-TH####(config-if:ethernet:3)#ip address 10.10.10.1 255.255.255.0
ACOS-TH####(config-if:ethernet:3)#ip ospf authentication message-digest
ACOS-TH####(config-if:ethernet:3)#ip ospf message-digest-key 42 md5
Bh^grZz3mT&iPw6M
```

NOTE: OSPF passwords in ACOS can be up to 16 printable ASCII characters long and cannot contain‘”"<>&\/? special characters.

OSPF Passive Interfaces

Sending or processing OSPF Link-State Advertisements (LSAs) can be disabled to avoid advertising information on networks outside the OSPF router’s administrative control. This practice mitigates information leaks and potential false information into the OSPF IGP.

The `passive-interface` command is available for this purpose for both OSPFv2 and OSPFv3. The following example shows how to configure a passive interface under OSPFv2 on the Virtual Ethernet (VE) interface on the `eth2` data port and OSPFv3 on eth3:

```
ACOS-TH####(config)#router ospf 1
ACOS-TH####(config-ospf:1)#passive-interface ethernet 2

ACOS-TH####(config)#router ipv6 ospf 2
ACOS-TH####(config-ospf:2)#passive-interface ethernet 3
```

OSPF Route Filters

When the passive-interface configuration can't be used, filtering summary routes advertised or processed by a configured OSPF router for the network helps to reduce the probability of introducing false routes. In this configuration, routing occurs when route filtering is enabled for an interface with information advertised (out) or processed (in), limited by the filters.

The `area filter-list` OSPFv2 command is available for this purpose when the router is acting as an Area Border Router (ABR). For example:

```
ACOS-TH####(config)#ip prefix-list LIST-IN seq 5 permit 192.168.1.0/24
ACOS-TH####(config)#ip prefix-list LIST-IN seq 10 permit 192.168.9.0/24
ACOS-TH####(config)#ip prefix-list LIST-IN seq 15 deny 0.0.0.0/0 le 32

ACOS-TH####(config)#router ospf 1
ACOS-TH####(config-ospf:1)#area 0 filter-list prefix-list LIST-IN in
```

NOTE: Filter lists are not available for OSPFv3 configurations.

OSPF Prefix Limits

To avoid memory exhaustion and the ACOS OSPF service from being interrupted, configure OSPF to limit resource consumption using the `overflow database` command for OSPFv2. Limits may be defined for LSA or AS-external-LSA volumes.For example:

```
ACOS-TH####(config)#router ospf 1
ACOS-TH####(config-ospf:1)#overflow database 4194304

ACOS-TH####(config)#router ospf 2
ACOS-TH####(config-ospf:1)#overflow database external 2097152
```

NOTE: OSPF database limits are not available for OSPFv3 configurations.

IS-IS

Integrated Intermediate System-to-Intermediate System (IS-IS) is a link-state Interior Gateway Protocol (IGP) developed in the late 1980s and standardized by the International Standards Organization (ISO) in ISO/IEC 10589 for the ISO protocol

suite. RFC 1195 defined IS-IS support for iPv4, and additional IETF extensions have defined IS-IS support for IPv6 (RFC 2373). As an IGP, IS-IS is also another target of interior attackers to disrupt or compromise network integrity.

To increase security of the IS-IS configuration for ACOS consider enabling IS-IS security features described below.

IS-IS MD5 Authentication

By default, IS-IS supports a plaintext authentication mechanism which provides nominal security, if any, against unauthorized parties. IS-IS can, however, be configured to support an HMAC-MD5 mechanism where the password is never sent on the wire. Instead, it is used to calculate a data-integrity checksum for subsequent exchanges on the connection.

Enabling MD5 authentication is recommended, if the stronger IS-IS keychain authentication is not supported in the target network.

For example, for level 1 IS-IS:

```
ACOS-TH####(config)#router isis
ACOS-TH####(config-isis)#net 47.0000.0000.0000.0001.00
ACOS-TH####(config-isis)#is-type level-1
ACOS-TH####(config-isis)#authentication mode md5 level-1

ACOS-TH####(config)#interface ethernet 3
ACOS-TH####(config-if:ethernet:3)#ip address 10.10.10.1 255.255.255.0
ACOS-TH####(config-if:ethernet:3)#ip router isis
ACOS-TH####(config-if:ethernet:3)#isis password Zz!%hHt7aR$L@95@ level-1
```

NOTE: ISIS passwords in ACOS can be up to 16 printable ASCII characters long and cannot contain‘”"<>&\/? special characters.

IS-IS MD5 Keychain Authentication

The more secure form of authentication is available for IS-IS which extends the MD5 authentication mechanism to operate over a group of keys, called a “key chain”. For example, first set up a key chain of three (3) MD5 passwords/key-strings:

```
ACOS-TH####(config)#key chain my-isis-key-chain-#1
ACOS-TH####(config-keychain)#key 1
ACOS-TH####(config-keychain-key)#key-string y*OckB!Yi%bKo6gv
```

```
ACOS-TH####(config-keychain)#key 2
ACOS-TH####(config-keychain-key)#key-string m*x!q!@ac!YhVjmK

ACOS-TH####(config-keychain)#key 3
ACOS-TH####(config-keychain-key)#key-string %CA4T%OptNW3HfNJ
```

NOTE: Keychain authentication strings in ACOS can be up to 16 printable ASCII characters long and cannot contain‘”"<>&\/? special characters.

Next, enable both MD5 and key chain authentication:

```
ACOS-TH####(config)#router isis
ACOS-TH####(config-isis)#net 47.0000.0000.0000.0001.00
ACOS-TH####(config-isis)#is-type level-1
ACOS-TH####(config-isis)#isis authentication mode md5
ACOS-TH####(config-isis)#isis authentication mode key-chain my-isis-key-
chain-#1 level-1
```

IS-IS Passive Interfaces

Sending or processing IS-IS routing updates can be disabled to avoid advertising information on networks outside the IS-IS router’s administrative control. This practice mitigates information leaks and potentially false information into the IS-IS IGP.

The **passive-interface** command is available for this purpose for IS-IS. For example, to configure a passive interface under IS-IS on Ethernet port 7:

```
ACOS-TH####(config)#router isis
ACOS-TH####(config-isis)#passive-interface ethernet 7
```

Routing Information Protocol

The Routing Information Protocol (RIP) is a historic distance-vector routing protocols that uses hop count as a routing metric. It prevents routing loops by limiting the number of hops allowed from source to destination and support various mechanisms to prevent incorrect routing information from being propagated. ACOS supports RIP Version 1 (RIPv1) and Version 2 (RIPv2).

To increase security of the RIP configuration for ACOS consider enabling RIP security features described below.

Do Not Enable RIPv1

RIPv1 has no support for router authentication. RIPv2 made up for this shortcoming by including MD5 and key chain authentication mechanisms. As such, use of RIPv1 should be avoided for network environments requiring RIP services.

ACOS supports RIPv2, by default, for configured RIP routers.

RIP MD5 Authentication

By default, RIPv2 supports a plaintext authentication mechanism which provides nominal, if any security against unauthorized parties. RIPv2 can, however, be configured to support an MD5 mechanism for improved security.

Enabling MD5 authentication is recommended, if the stronger MD5 keychain authentication is not supported in the target network.

The following example defines a RIPv2 instance on eth3 and shows how to enable it for MD5 password authentication:

```
ACOS-TH####(config)#router rip
ACOS-TH####(config-rip)#network 10.10.10.0/24
ACOS-TH####(config-rip)#network ethernet 3

ACOS-TH####(config)#interface ethernet 3
ACOS-TH####(config-if:ethernet:3)#ip address 10.10.10.1 255.255.255.0
ACOS-TH####(config-if:ethernet:3)#ip rip authentication mode md5
ACOS-TH####(config-if:ethernet:3)#ip rip authentication string
DgUwTtzc34F8rEO2
```

NOTE: RIPv2 passwords in ACOS can be up to 16 printable ASCII characters long and cannot contain‘”"<>&\/? special characters.

RIPv2 MD5 Keychain Authentication

A more secure form of authentication is available for RIPv2 which extends the MD5 authentication mechanism to operate over a group of keys called a “key chain”. For example, first set up a key chain of three (3) MD5 passwords/key-strings:

```
ACOS-TH####(config)#key chain my-ripv2-key-chain-#1
ACOS-TH####(config-keychain)#key 1
ACOS-TH####(config-keychain-key)#key-string hIz2%2ovr1j*dT%d

ACOS-TH####(config-keychain)#key 2
ACOS-TH####(config-keychain-key)#key-string jx^#dpQ!j63vDeE*

ACOS-TH####(config-keychain)#key 3
ACOS-TH####(config-keychain-key)#key-string !tpkTWHHg^YD&x@d
```

NOTE: Keychain authentication strings can be up to 16 printable ASCII characters long and cannot contain‘”"<>&\/? special characters.

Next, enable both MD5 and key chain authentication, as follows.

```
ACOS-TH####(config)#interface ethernet 3
ACOS-TH####(config-if:ethernet:3)#ip address 10.10.10.1 255.255.255.0
ACOS-TH####(config-if:ethernet:3)#ip rip authentication mode md5
ACOS-TH####(config-if:ethernet:3)#ip rip authentication key-chain my-
ripv2-key-chain-#1
```

Bidirectional Forwarding Detection (BFD)

Bidirectional Forwarding Detection (BFD) is a network protocol used to detect faults between forwarding engines. BFD does not have its own discovery mechanism and relies on sessions explicitly configured between endpoints or use of other protocols to determine adjacency (e.g. BGP, OSPF, IS-IS) and bootstrap BFD sessions.

Bidirectional Forwarding Detection (BFD) provides very fast failure detection for routing protocols. When BFD is enabled, the ACOS device periodically sends BFD control packets to the neighboring devices that are also running BFD. If a neighbor stops sending BFD control packets, the ACOS device quickly brings down the BFD session(s) with the neighbor and recalculates paths for routes affected by the down neighbor.

To increase security of the BFD configuration for ACOS consider enabling the BFD security features described below:

BFD Authentication

BFD can be configured for individual ACOS interfaces or specific neighbors, in conjunction with other routing protocols (OSPF, IS-IS, BGP) enabled. It is a good practice to enable BFD authentication when instantiating this service with the routing configuration using one of the following schemes for shared secret values configured on BFD endpoints:

- Simple password
- Keyed MD5
- Meticulous Keyed MD5
- Keyed SHA1 (recommended)
- Meticulous Keyed SHA1 (recommended)

The simple password and MD5 schemes provide nominal to weak security protection from attacks. Use of these schemes for BFD authentication is strongly discouraged and should be applied only when compatibility with legacy implementations not supporting SHA1 is needed.

NOTE: Though meticulous keyed BFD authentication schemes are more secure than their keyed alternatives, they may not be available in commercial routers when proprietary high-availability features are enabled and may take additional time to authenticate.

The following configuration examples apply BFD for ISIS configured routers in ACOS. Like and similar configuration operations are supported for BGP, OSPF, and RIP. See the ACOS product documentation for information on configuring BFD with these other routing protocols.

Per Instance BFD Authentication

The following example sets up an ISIS router, configures the interface for BFD authentication with meticulous keyed SHA1 (with the bfd authentication command), and enables BFD on the ISIS router (with the `isis bfd` command):

```
// Set-up ISIS Router on eth3
ACOS-TH####(config)#interface ethernet 3
ACOS-TH####(config-if:ethernet:3)#ip address 10.10.10.1 255.255.255.0
ACOS-TH####(config-if:ethernet:3)#ip router isis
```

```
ACOS-TH####(config-if:ethernet:3)#isis password Zz!%hHt7aR$L@95@ level-1

// Enable BFD with authentication for all peers on eth3
// Enable BFD for ISIS router on eth3 port
ACOS-TH####(config-if:ethernet:3)#bfd authentication 1 meticulous-sha1
T@ZqIkA4*l6FN#9p
ACOS-TH####(config-if:ethernet:3)#isis bfd
```

NOTE: BFD shared, secret keys in ACOS can be up to 16 printable ASCII characters long and cannot contain‘”"<>&\/? special characters.

NOTE: Per interface configuration for BFD shared secret key values is supported in this fashion for the BGP, OSPF, ISIS, and RIP routing protocols

BFD Authentication – Per BGP Neighbor

Alternatively, BFD authentication can be configured for individual neighbors using the fall-over bfd variant of the neighbor ACOS command, as shown in the following example:

```
ACOS-TH####(config)#router bgp 123
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 remote-as 123
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 password
MNQHsKkg4oC70A2D
ACOS-TH####(config-bgp:123)#neighbor 10.10.10.197 fall-over bfd
authentication 1 meticulous-sha1 0oSZB%@QV5FHSI@W
```

NOTE:

- BFD shared, secret keys in ACOS can be up to 16 printable ASCII characters long and cannot contain‘”"<>&\/? special characters.
- Per neighbor configuration for BFD shared secret key values is supported in ACOS only for the BGP routing protocols.

Other Control Plane Protocol Hardening

ACOS supports other control plane protocols, notably for Link-Layer and High Availability functions. The scope of these protocols, which include the following, does not include provisions for authentication or encryption:

- Link Aggregation Control Protocol (LACP)
- ACOS High Availability Protocol (VRRP-A)
- ACOS Virtual Chassis System Protocol (aVCS)
- Link Layer Discovery Protocol (LLDP)
- Spanning Tree Protocols (STP, MSTP, RSTP)

The following sub-sections discuss approaches to containing potential exposures for these otherwise unsecure-able protocols.

Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (LACP) is a standard link-layer protocol that supports the bundling of several physical (virtual) ports together to form a single logical channel, commonly referred to as a port channel. It allows a network device to negotiate the bundling of links by sending LACP packets to directly-connected peers that also support LACP.

LACP is disabled by default in ACOS. If LACP is not supported for devices on networks directly connected to the ACOS system, it is recommended to leave the service disabled. Otherwise, a good practice is to ensure LACP is only configured and enabled for ACOS system interfaces connected to immediate networks supporting LACP-enabled devices.

For example, to create an LCAP trunk and assign the `eth3` data port, with a system priority of 32768:

```
// Assign eth3 to the LACP trunk
ACOS-TH####(config)#interface ethernet 3
ACOS-TH####(config-if:ethernet:3)#trunk-group 4 lacp

ACOS-TH####(config)#lacp system-priority 32768
```

Permitting the following for only ACOS systems and other LACP-enabled devices on interconnecting switches can constrain most, if not all, exposures to compromises or attacks on LACP:

- EtherType : 0x8809
- Ethernet Slow Protocols Subtype : 0x01
- LACP Version : 0x01

Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol (LLDP) is a standard link-layer protocol for advertising their identity, capabilities, and neighbors on IEEE 802 networks. It allows ACOS systems to discover directly-connected LAN neighbors and these neighbors to discover the ACOS system devices.

LLDP is disabled by default in ACOS. If LLDP is not supported for devices on networks directly connected to the ACOS system, it is recommended to leave the service disabled. Otherwise, a good practice is to ensure LLDP is only configured and enabled for ACOS system interfaces connected to immediate networks supporting LLDP-enabled devices. If ACOS system is connected to a public network, ensure LLDP is disabled for the interfaces connected to the public network.

For example, to enable LLDP on `eth2` data port for both discovery (rx) and announcement (tx):

```
// Enable LLDP on eth3
ACOS-TH####(config)#interface ethernet 2
ACOS-TH####(config-if:ethernet:2)#lldp enable rx tx
```

Permitting the following for only ACOS systems and other LLDP-enabled devices on interconnecting switches can constrain most, if not all, exposures to compromises or attacks on LLDP:

- EtherType := 0x88cc

Spanning Tree Protocols (STP/MSTP/RSTP)

Spanning tree protocols detect and prevent loops in a layer 2 network topology. By sending Bridge Protocol Data Units (BPDUs), the protocol can detect bridge loops

and activate a blocking mode on interfaces thereby to prevent redundant paths in the network.

Spanning tree protocols are disabled by default and should only be enabled when required. If spanning tree is required, best practice is only to enable spanning tree on interfaces that will participate in the protocol and if enabled, configure the port to be an edge port if connected to an endpoint so the port does not participate in STP.

To configure an edge port, select the interface and apply the following:

```
ACOS(config-if:ethernet:1)#spanning-tree admin-edge
```

ACOS High Availability Protocol (VRRP-A)

VRRP-A is an A10 proprietary protocol that provides the High Availability (HA) feature for ACOS systems. Though it does borrow concepts from the Virtual Router Redundancy Protocol (VRRP), this A10 HA protocol is completely different from the industry standard, specified in IETF RFC-5798.

Whereas the standard VRRP is meant for redundancy amongst routers, VRRP-A supports HA for ACOS ADC, CFW, CGN, and SSLi systems; providing redundancy for:

- Virtual server IP addresses (VIPs)
- Floating IP addresses used as default gateways by downstream devices
- IPv6 NAT pools
- IPv4 NAT pools
- IPv4 static range lists and individual mappings for inside source NAT

The VRRP-A service in ACOS is disabled by default. If the ACOS system is not deployed in a HA configuration, it is recommended to leave the service disabled. Alternatively, and as is very commonly the case when deployments seek high availability, it is a good practice to ensure that VRRP-A is carefully configured and only enabled for interfaces connecting ACOS systems.

Permitting the following for only ACOS systems on interconnecting switches can constrain most, if not all, exposures to compromises or attacks on VRRP-A:

- Multicast IPv4 := 224.0.0.210
- Multicast IPv6 := FF02::D2
- Multicast UDP Source Port := 0xFEDC (65244)
- Multicast UDP Destination Port:= 0xFEDC (65244)
- Unicast IPv4 and IPv6 := VRRP-A interface IP addresses
- Unicast UDP Destination Port := 0x5700 (22272)

NOTE: VRRP-A 'configure sync' command uses the SSH protocol to exchange configuration data between ACOS devices. Specify the target IP address in the command to synchronize the configuration to. It is important to ensure that the SSH protocol is enabled on the dedicated interfaces (real or virtual) of the target ACOS devices, using the `enable-management service ssh` command.

ACOS Virtual Chassis System (aVCS)

ACOS Virtual Chassis System (aVCS) enables you to manage a cluster of ACOS devices like a single, virtual chassis. One ACOS device in the virtual chassis is the virtual master (vMaster). The other ACOS devices are virtual blades (vBlades) within the virtual chassis, and are managed by the vMaster. As a controller for the vBlades, the vMaster provides centralized storage of the entire ACOS device configuration. Any configuration changes from the vMaster are automatically propagated to the vBlades. aVCS, as a management tool, provides high availability functionality on the ACOS device with the help of VRRP-A across multiple ACOS devices.

aVCS protocols uses IP multicast and IP unicast. All ACOS devices in an aVCS virtual chassis must be in the same Layer 2 broadcast domain.

By default, the following multicast IP and port are used for discovery.

Multicast IP: 224.0.1.210 (ACOS 6.0.6 and higher uses 224.0.0.211)

Multicast Port: 41217 (0xA101)

If there are concerns about using multi-cast for discovery, enable unicast mode for added security.

aVCS can operate in unicast only mode but member discovery is not available, and members must be explicitly defined in each member of the cluster. For more information about configuring aVCS in unicast mode, refer to “Scaleout Configuration Guide” section “Configure aVCS on Each Device for Unicast Mode.”

The following config enables unicast mode:

```
ACOS-TH####(config:1)#vcs unicast-election
ACOS-TH####(config:1-unicast-election)#members
ACOS-TH####(config:1-unicast-election-members)#ip-address 2.2.2.115
ACOS-TH####(config:1-unicast-election-members)#ip-address 2.2.2.116
ACOS-TH####(config:1-unicast-election-members)#ip-address 2.2.2.117
ACOS-TH####(config:1-unicast-election-members)#exit
ACOS-TH####(config:1)#vcs discovery-mode unicast
```

Unicast Election port: 41473 (0xA201)

aVCS uses a TCP unicast channel for synchronization of configuration between peers.

TCP Unicast Port: 41216 (0xa100)

A10 strongly recommends enabling aVCS only on management interfaces and securing and isolating the management network physically. In addition, enable SSL in VCS to secure the control traffic between aVCS peers.

```
ACOS-TH####(config)#vcs ssl-enable
ACOS-TH####(config)#vcs reload
```

Hardening the ACOS Data Plane

This section addresses hardening considerations for the ACOS data plane.

Data planes are often considered less critical to harden compared to the management and control planes, under the assumption that secure practices for those planes will inherently secure the data plane. While this is true for the overall strength and integrity of the ACOS system, there are still many features and configuration options that promote secure data plane traffic.

ACOS aims to provide a highly-secured data plane service while maintaining excellent performance. However, it faces the notable challenge of supporting the legacy servers that use services considered insecure and antiquated by contemporary standards and industry expectations. This is especially true for cryptographic ACOS features like SSL/TLS, IPsec, OpenSSH, offloading, proxy, and inspection.

Additionally, hardening the data plane involves securing services accessed through the ACOS data plane, such as web servers located behind the ACOS system. To help protect legacy, under-provisioned, or misconfigured web servers, several security considerations are outlined below.

General Data Plane Hardening

There are some areas to consider in hardened ACOS deployments that don't fit into another category, such as ICMP Redirects (anti-DoS) and Anomalous Packet Handling (anti-DoS).

Anomalous Packets Handling

Anomalous packet encodings can be used by malicious parties attempting to disrupt or surveil the ACOS system, or to subvert the data-stream it is processing. Traffic of this nature is generally more commonplace on ACOS interfaces at the network edge where DoS and precursor surveillance are seen more and more often in the industry.

Internal networks will typically see significantly less malformed traffic but are still not immune to activities of bad actors.

ACOS supports the detection of a variety of packet anomalies, with no impact to performance in ACOS systems that include A10 Flexible Traffic Accelerators (FTAs) and nominal impact in other ACOS hardware-based and virtual platforms. By default, ACOS drops some of these malformed packets and passes others packets by default, thus A10 recommends to configure ACOS with the following configuration to drop anomalous packets.

Drop Anomalous L3/L4 Packets

ACOS is configured to drop anomalous packets through the `ip anomaly-drop` command with several anomaly groups to choose from as shown in the example below. Additional options are supported for compatibility with legacy anomaly controls in ACOS.

```
ACOS-TH####(config)#ip anomaly-drop packet-deformity layer-3
ACOS-TH####(config)#ip anomaly-drop packet-deformity layer-4
ACOS-TH####(config)#ip anomaly-drop security-attack  layer-3
ACOS-TH####(config)#ip anomaly-drop security-attack  layer-4
```

The complete list of anomalies and their statistics can be seen with the `show ip anomaly-drop statistics` command. They are associated with the anomaly groups above as follows:

Deformities – Layer 3

- Runt IP Header
- Bad IP Header Length
- Bad IP Flags
- Bad IP TTL
- Bad IP Checksum
- Bad IP Payload Length
- Oversize IP Payload
- Bad IP Fragment Offset
- IP-over-IP Tunnel Mismatch

- IP-over-IP Tunnel Error
- VXLAN Tunnel Error
- GRE Tunnel Error
- GRE PPTP Error

Attacks – Layer 3

- Land Attack (2)
- ICMP Ping of Death (2)
- No IP Payload
- Empty Fragment
- Micro Fragment

Deformities – Layer 4

- Runt TCP/UDP Header
- TCP Short Header
- TCP Bad IP Length
- TCP Fragmented Header (1)
- TCP Bad Checksum
- TCP Option Error
- TCP Bad Urgent Offset
- TCP SYN and FIN (1) (2)
- TCP SYN Fragment (1) (2)
- TCP Null Flags (1) (2)
- TCP Null Scan (1)
- TCP XMAS Flags (1)
- TCP XMAS Scan (1)
- UDP Short Header
- UDP Bad Length

- UDP Bad Checksum
- UDP Port Loopback (1)

Attacks – Layer 4

- *** Incl. Layer 4 Deformities above with note (1)
- UDP Kerberos Fragment

(1) Anomaly is included in both deformities and attacks.

(2) Anomaly also has a separate, legacy control under the `ip anomaly-drop` command.

Drop IP Option Packets

IP options in packets are generally considered to be a security risk as they can be used to leak address and topology information about interior networks to the outside world or bypass network security controls. It is a common practice to filter out (drop) packets with IP Options, especially for networked devices deployed at the network edge.

ACOS systems are often deployed at or near the network edge. For such ACOS systems it is recommended that packets with IP Options be summarily dropped. This behavior is enabled with the `ip anomaly-drop` command. For example:

```
ACOS-TH####(config)#ip anomaly-drop ip-option
```

Drop IPv4 Source Routing

IPv4 source routing options were originally intended to aid in network diagnostics and troubleshooting, allowing the sender of a packet to specify an exact path or sequence of gateways that the packet must traverse on its way to the destination. Malicious users long ago figured out how to use these options to target network segments while bypassing configured and learned routing topology information, allowing them to determine the path packets take; potentially subverting security policies and management of the target network. Accordingly, it has become a common practice to drop IPv4 packets attempting to specify routing paths within interior networks.

ACOS does not support configurations to selectively drop source routing options, while allowing other options to pass. To drop IPv4 packets with source routing

options, ACOS deployments will need to enable dropping of packets with any IPv4 options, as described above.

Monitor Anomalous L3/L4 Packets Statistics

Anomalous packets can be a bellwether of malicious activity, more so for some malformed packets than others. For example, bad checksums can happen from time to time. However, spikes or elevations in these events can be good indicators of DoS attacks and/or surveillance attempts.

Administrative users are advised to monitor ACOS anomaly volume through the `acosIpAnomalyDropS` statistics array (1.3.6.1.4.1.22610.2.4.10.55.5.1) via SNMP and take appropriate actions on occasions of increased anomalous activity.

Disable ICMP Redirects

ICMP redirects let one network device inform another of a better path to a given IP destination. By default, ACOS sends an ICMP redirect if it receives a packet that needs to be routed through the interface it was received. Attackers can leverage this common default behavior, using the CPU overhead it entails to deny service (DoS) in the ACOS system's data plane.

To avoid such exploits in the ACOS data, control, and management planes it is recommended to configure ACOS to not send ICMP redirects. For example:

```
ACOS-TH####(config)#ip icmp disable redirect
```

SSL/TLS Configuration Hardening

The ACOS data plane in A10 ADC and SSL Insight (SSLi) products supports a robust set of SSL/TLS-based features; such as cryptographic acceleration/off-loading, forward/reverse proxies, and interception/inspection. Underlying these features is the SSL/TLS data plane that provides common cryptographic services.

The SSL/TLS data plane can be a challenging area for many organizations that need to support legacy environments with old browser or web servers, historic applications that still need to function, and the like. To support these environments, SSL/TLS in the ACOS data plane continues to make older SSL/TLS protocol versions and ciphers

available. For example, ACOS continues to support the SSL Version 3 (SSLv3) protocol since some ACOS deployments still need to communicate to antiquated production servers and applications that only support SSLv3.

NOTE: Transport Layer Security (TLS) is the successor to the Secure Socket Layer (SSL) protocols. The reader will see that ACOS ubiquitously use the term SSL (or ssl) for ACOS SSL/TLS object names and configuration keywords. These references should be effectively considered to refer to TLS, the successor protocol to SSL, unless otherwise noted.

ACOS abstracts two basic configuration objects for provisioning the SSL/TLS service instances. One is the client SSL (client-ssl) template used to configure ACOS for SSL/TLS connections initiated by clients external to ACOS, such as browsers and RESTful client applications. The other is the server SSL (server-ssl) template used to configure ACOS for SSL/TLS connections to servers or resources being requested, such as HTTPS web servers and SMTPS mail servers. These templates can be further provisioned with additional options and settings before associating them with ACOS Virtual IPs (VIPs). They are created and configured using the `slb template client-ssl` and `slb template server-ssl` commands.

In the subsections below, we share common practices and alternatives for securely configuring ACOS's SSL/TLS underlying services.

SSL/TLS Ciphers

When an SSL client or server template is created a default set of ciphers are enabled which includes many of the ciphers that ACOS supports. This default set of ciphers can be overridden by creating an SSL cipher template with the `slb template cipher` ACOS command, specifically enabling select ciphers in the template. The cipher template can then be bound to the client or server SSL template using the `template cipher` command.

In general, A10 recommends that ACOS administrators always define SSL cipher templates for their deployments instead of simply relying on ACOS defaults.

Maximum Security, HTTP2 Compatibility

Deployments that seek to maximize security will enable only PFS ciphers that use ChaCha20-Poly1305 or AES-GCM encryption algorithms. These ciphers are generally

considered some of the strongest, commonly supported ciphers in the industry. They are also fully compatible with cipher requirements for the HTTP/2 (aka HTTP/2.0) protocol.

An SSL cipher template supporting this most secure scope would look like the following:

```
ACOS-TH####(config)#slb template cipher MaxSec_HTTP2_0-Ciphers
ACOS-TH####(config-cipher)#tls1_3 TLS_CHACHA20_POLY1305_SHA256 priority 96
ACOS-TH####(config-cipher)#tls1_3 TLS_AES_256_GCM_SHA384 priority 94
ACOS-TH####(config-cipher)#tls1_3 TLS_AES_128_GCM_SHA256 priority 92
ACOS-TH####(config-cipher)#TLS1_ECDHE_ECDSA_CHACHA20_POLY1305_SHA256
priority 88
ACOS-TH####(config-cipher)#TLS1_ECDHE_RSA_CHACHA20_POLY1305_SHA256
priority 86
ACOS-TH####(config-cipher)#TLS1_ECDHE_ECDSA_AES_256_GCM_SHA384 priority 78
ACOS-TH####(config-cipher)#TLS1_ECDHE_RSA_AES_256_GCM_SHA384 priority 76
ACOS-TH####(config-cipher)#TLS1_ECDHE_ECDSA_AES_128_GCM_SHA256 priority 68
ACOS-TH####(config-cipher)#TLS1_ECDHE_RSA_AES_128_GCM_SHA256 priority 66

ACOS-TH####(config)#slb template client-ssl sample-client-ssl-template
ACOS-TH####(config-client ssl)#template cipher MaxSec_HTTP2_0-Ciphers

ACOS-TH####(config)#slb template server-ssl sample-server-ssl-template
ACOS-TH####(config-server ssl)#template cipher MaxSec_HTTP2_0-Ciphers
```

Cipher priority values can be 1 - 100 with the highest (most favored) priority being 100. When ciphers are assigned the same priority the strongest (most secure) ciphers will be more favored for incoming SSL/TLS connections processed against the client SSL template. If the optional priority value is not indicated, a default value of 1 (least favored) will be applied.

NOTE: Priority values are ignored by ACOS for server SSL templates since it is the external SSL/TLS responder that chooses the cipher for a session from the preferred cipher list configured on the server SSL template. Cipher templates for server SSL templates serve only to control which ciphers are proposed in connections to SSL/TLS responders.

Default Ciphers

When the client and server SSL templates are created, default ciphers are selected and they are generally selected for maximum compatibility.

The following cryptographic algorithms have known vulnerabilities and A10 recommends you avoid using them. If required due to legacy compatibility reasons, care should be taken when using them in production environments.

- DES, 3DES
- RC4
- AES CBC
- RSA key exchange
- DHE key exchange
- MD5
- SHA-1
- Static DH or ECDH

SSL/TLS Protocol Versions

ACOS supports the following SSL/TLS protocol versions with controls in the client and server SSL templates to override the enabled or disabled defaults.

Because SSL v3, TLS v1.0 and v1.1 are deprecated, and have known vulnerabilities, A10 recommends disabling them and only enable TLS 1.2 and TLS 1.3. The following lists the default SSL and TLS versions enabled for client and server SSL templates:

- TLS Version 1.3 (TLSv1.3) -default enabled (select models)
- TLS Version 1.2 (TLSv1.2) - default enabled (select models)
- TLS Version 1.1 (TLSv1.1) - default enabled
- TLS Version 1.0 (TLSv1.0) - default enabled
- SSL Version 3 (SSLv3) - default disabled

TLSv1.2 and v1.3 are broadly supported throughout the industry today and is supported by ACOS. All major web browsers support TLS 1.3 but some sites may still not support it. ACOS supports TLS 1.3 and can help add support to existing web

services. Not all Thunder platforms support hardware acceleration for TLS v1.3. Hardware acceleration for TLS v1.3 is supported on Thunder hardware platforms with Intel's Quick Assist Technology (QAT) to offload encryption and decryption operations. All Thunder software platforms such as vThunder, cThunder, support TLS 1.3 using a software cryptographic module. Thunder hardware models which do not have QAT hardware offload, may configure the software cryptographic module; however, this configuration will disable other cryptographic operations from using hardware offload and that will impact overall SSL/TLS performance. A10 does not recommend enabling software cryptographic module on A10 hardware appliances.

To check if TLS v1.3 hardware acceleration is available on your Thunder platform issue the "show hardware" command and look at the SSL Cards field below. If the field contains QAT devices, hardware SSL offload with TLS v1.3 is supported.

```
ACOS-TH####(config)#show hardware
Thunder Series Unified Application Service Gateway TH6655S
Serial No  : TH660E5524040009
CPU        : Intel(R) Xeon(R) Gold 6258R CPU @ 2.70GHz
56 cores
7 stepping
Storage    : Single 931G drive, Free storage is 713G
Memory     : Total System Memory 786233 Mbytes, Free Memory 711376 Mbytes
SSL Cards  : 9 device(s) present
9 QAT SSL device(s)

L2/3 ASIC  : 1 device(s) present
IPMI       : IPMI Present
SP Engine  : Present

Ports      : 19
Flags      : CF
SMBIOS     : Build  5.14
03/04/2024
FPGA       : 4 instance(s) present
Date: 01/09/2024
MCPLD Type : 4
Date: 05/05/2020
```

If you have a software Thunder platform, and do not see any SSL cards, TLS v1.3 is supported.

```
ACOS-TH####(config)#show hardware
Thunder Series Unified Application Service Gateway vThunder
Serial No   : 0000-0009-1634-453
CPU         : Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz
4 cores
7 stepping
Storage     : Dual 30G drive, Free storage is 16G
Memory      : Total System Memory 16382 Mbytes, Free Memory 6889 Mbytes


L2/3 ASIC   : 0 device(s) present

Ports       : 0
Flags       : No CF
SMBIOS      : Build  090008
12/07/2018
```

Issue “show slb ssl stats” command, and observed the field “SSL module:” The text should indicate TLS v1.3 is supported. The below is an example for a vThunder.

```
ACOS-TH####(config)#show slb ssl stats
SSL module: Software with TLS13

Current clientside SSL connections: 0
Total clientside SSL connections: 0
Current serverside SSL connections: 0
Total serverside SSL connections: 0
Total Non SSL Bypass connections: 0
Total times of stateful session reuse in client ssl: 0
Total times of stateful session reuse in server ssl: 0
Total times of stateless session reuse in client ssl: 0
Total times of stateless session reuse in server ssl: 0
Total clientside early data connections: 0
Total serverside early data connections: 0
Total clientside failed early data connections: 0
Total serverside failed early data connections: 0
Failed SSL handshakes: 0
Failed crypto operations: 0
SSL memory usage: 13485 bytes
SSL server certificate errors: 0
SSL client certificate authorization failed: 0
```

```
SSL fail CA verification 0
HW Context Memory alloc failed 0
HW ring full 0
Record too big 0
Total client ssl context malloc failures: 0
```

The following example is the output of a hardware model with QAT.

```
ACOS-TH####(config)#show slb ssl stats
SSL module: QAT
Config module: Hardware
Number of SSL modules: 9
```

Even though systems supporting only TLSv1.1 and/or TLSv1.0 have been phasing out over the last number of years, it is still not uncommon to encounter them both in legacy SSL/TLS applications, client browsers, and servers. SSLv3-based systems continue to become more and more of a rarity, but still are encountered. Accordingly, the ACOS SSL/TLS data-plane continues to support them.

The following discusses common practices for configuring SSL/TLS protocol versions in SSL templates.

Enable TLS v1.3 and TLS v1.2

Depending on the Thunder ACOS model, TLS v1.3 or TLS v1.2 may be enabled by default. The recommendation is to enable both TLS versions if supported by your model. Issue the version command in the client and server ssl template context.

```
ACOS-TH####(config)#slb template client-ssl client-ssl-template-1
ACOS-TH####(config-client ssl)#version 34 33
ACOS-TH####(config)#slb template server-ssl server-ssl-template-1
ACOS-TH####(config-client ssl)#version 34 33
```

Hardware acceleration for TLS 1.3 is not supported on all Thunder ACOS platforms. If you receive an error “Operation not supported by SSL module,” the TLS 1.3 is not supported. Simply enable TLS 1.2.

```
ACOS-TH####(config)#slb template client-ssl client-ssl-template-1
ACOS-TH####(config-client ssl)#version 33 33
ACOS-TH####(config)#slb template server-ssl server-ssl-template-1
ACOS-TH####(config-client ssl)#version 34 33
```

Disable TLSv1.0 and TLSv1.1

TLSv1.0 is also considered unsafe to use, especially with the 2012 advent of the CRIME (Compression Ratio Info-leak Made Easy) security exploit against secret web cookies over HTTPS and SPDY connections. Additionally, TLSv1.0 does not support contemporary ciphers with strong security and will no longer pass compliance testing for PCI (Payment Card Industry) DSS (Data Security Standard) certifications.

TLSv1.0 and TLS v1.1 are disabled by default in client and server SSL templates. It is a good security practice to disable TLSv1.0 using the version command in SSL templates, unless there is a specific need to support this version. For example, to configure two client SSL templates with one supporting TLSv1.2 only and the other supporting TLSv1.2 and TLSv1.3:

```
ACOS-TH####(config)#slb template client-ssl client-ssl-template-1
ACOS-TH####(config-client ssl)#version 33 33

ACOS-TH####(config)#slb template client-ssl client-ssl-template-2
ACOS-TH####(config-client ssl)#version 34 33

ACOS-TH####(config-client ssl)#version ?
<30-33>  TLS/SSL version: 30-SSLv3.0, 31-TLSv1.0, 32-TLSv1.1, 33-TLSv1.2
and 34-TLSv1.3
```

For reasons like and akin SSLv3, described above, organizations may need to enable TLSv1.0 to support legacy TLS clients and servers. Similarly, it is a good practice to isolate the legacy systems through their own ACOS VIPs and client/server SSL templates where TLSv1.0 can be selectively enabled, using the version command, without security impacts to other VIPs and services.

There are known vulnerabilities with TLSv1.1 and the protocol is deprecated. It is disabled by default, and it is recommended not to enable it.

Disable SSLv3

Notably due to the POODLE (Padding Oracle On Downgraded Legacy Encryption) vulnerability, SSLv3 is considered unsafe to use and can allow plaintext of secure connections to be retrieved an attacker. Furthermore, several other security issues affect SSLv3 and many contemporary ciphers supporting strong security cannot be used with SSLv3. It follows that ensuring SSLv3 is disabled is an important consideration for securing ACOS system deployments, as described below:

Disable SSLv3 – Non-FIPS Mode

Most ACOS systems are not FIPS-certified models where SSLv3 is disabled by default. It is highly recommended for security of these systems that ACOS administrators disable SSLv3, unless there is specific need to support it.

Requirements in ACOS deployments to provide services for legacy client/server applications, web servers, and web applications that only work with old browsers (e.g. such as Internet Explorer 6) can be motivating needs to leave SSLv3 support enabled. In these circumstances, seek to isolate the legacy systems through their own ACOS VIPs and client/server SSL templates where SSLv3 can be selectively left enabled without security impacts to other VIPs and services.

SSLv3 is disabled for a client SSL template with the `disable-sslv3` command and for a server SSL template by excluding `30` in the `version` command.

Non-FIPS mode models can be configured to operate in FIPS mode with the `system fips enable` CLI command. For ACOS systems configured in this fashion, see the discussion below.

Disable SSLv3 – FIPS Mode

SSLv3 is disabled by default in client and server SSL templates when FIPS-mode is enabled. It is highly recommended for security that ACOS administrators avoid enabling SSLv3 without specific need.

Requirements in ACOS deployments as described above can be motivating needs to enable support for SSLv3. In these circumstances, seek to isolate the legacy systems through their own ACOS VIPs and client/server SSL templates where SSLv3 can be selectively enabled without security impacts to other VIPs and services.

SSLv3 is disabled for a client SSL template with the `no disable-sslv3` command and for a server SSL template by excluding `30` in the `version` command.

2K dh-param

ACOS client SSL templates support a default size for the DH Parameter of 2048-bits. Though 2048-bits is commonly supported throughout the industry for this setting, legacy SSL/TLS clients require a lesser size.

In these circumstances, it is recommended to isolate legacy systems by dedicating ACOS VIPs and SSL client templates just for these systems where a smaller DH

Parameter can be selectively configured without security impacts to other VIPs and services. The DH Parameter can be set for an SSL client template with the `dh-param` command.

Configure OCSP Stapling

Major browsers support OCSP stapled responses to validate server certificates. All browsers will warn the user if the server's certificate can't be validated as trusted. OCSP stapled responses improve the TLS connection time by 30% not requiring the browser to fetch the OCSP status from the OCSP server. This results in your service being more responsive.

To configure OCSP stapling:

```
ACOS-TH####(config)#aam authentication server ocsp a1
ACOS-TH####(config-auth server ocsp)#url http://[OCSP server IP
addr]:7878/
ACOS-TH####(config-auth server ocsp)#responder-ca RootCA.crt
ACOS-TH####(config)#slb template client-ssl c1
ACOS-TH####(config-client ssl)#cert server.crt key server.key
ACOS-TH####(config-client ssl)#ocsp-stapling ca-cert RootCA.crt ocsp a1
period minutes 1 timeout 1
```

Enable Automated Certificate Management

Maintaining valid SSL/TLS certificates for your sites is important for security and is an ongoing, repetitive task because certificates expire and need to be renewed. Most policies require certificates to be renewed yearly. Leaving certificate renewal to alerts or reminders which require user intervention and actions can result in your sites using expired certificates. Using expired certificates opens the door to multiple vulnerabilities where the clients using the service can no longer verify the authenticity of the site thus making it more prone to potential threats which bad actors can take advantage of. Using automated certificate enrollment and renewal is strongly recommended. ACOS provides multiple options for automating certificate lifecycle management. The following options are available depending on your needs:

- Automatic Certificate Management Environment (ACME) Procotol
- Certificate Management Protocol (CMP)
- Simple Certificate Enrollment Protocol (SCEP)

A10 recommends using ACME as the preferred choice for certificate lifecycle automation but your choice may depend on what your public key infrastructure (PKI) supports. For more details how to use and configure these protocols, please refer to *the Application Delivery Controller Guide* section *CA and CSR Management*.

Web VIP Configuration Hardening

With almost 50% of today's vulnerabilities being web-related, secure practices for ACOS Web VIPs is clearly an important area to consider in hardening ACOS system deployments. Notable practices in this pursuit include configuring Web VIPs to reduce exposure to Denial-of-Service (DoS) attacks, ensure web content transferred is encrypted, supporting HTTP security headers, and optionally deploying a Next Generation Web Application Firewall.

Several HTTP security headers have been introduced in recent years that help protect against exploits from various attacks; such as cross-site scripting (XSS), man-in-the-middle (MitM) attacks, clickjacking, cross-site request forgery and other threat vectors. It is important to make sure HTTP security headers are present in outgoing HTTP responses from the Web VIP, even if the underlying HTTP servers are misconfigured or simply do not support them.

These practices are also helpful in reducing warnings and alerts from web application and vulnerability scanners that are becoming more available and used to test security and compliance for web services.

Enable TCP SYN-Cookies

A TCP SYN-flooding attack is a type of Denial-of-Service (DoS) attack and is all too commonly used to target web-based services. The TCP SYN-Cookie is a mechanism that helps protect the ACOS system as well as the services it provides. Enabling SYN-Cookies is always a recommended practice; especially for services facing the network edge.

FTA Models: To enable hardware-based SYN cookies on ACOS models that feature FTAs, use the syn-cookie enable command at the global configuration level.

```
ACOS-TH####(config)#syn-cookie enable
```

Non-FTA Models: To enable software-based SYN cookies, use the syn-cookie command at the virtualport level. For example:

```
ACOS-TH####(config)#slb virtual-server vip1
ACOS-TH####(config-slb vserver)#port 80 tcp
ACOS-TH####(config-slb vserver-vport)#syn-cookie
```

NOTE: If hardware-based SYN-cookies are configured and enabled for the ACOS system, the software based SYN-cookie mechanism for virtual ports is not used, even if it is configured for the virtual port as described above. Hardware based SYN-cookies are only supported on ACOS systems with FTA hardware and are enabled globally for the ACOS system using the `syn-cookie enable` command. See the *DDoS Mitigation for ADC Guide* for more information on this hardware-based feature and its configuration.

Enable HTTPS

The following example begins with a basic Web VIP configuration in ACOS with TCP SYN-Cookies enabled. This configuration, which will be further built upon in later discussions, defines a Web VIP for a web-site with the following characteristics:

- Outside IP: 1.1.1.1
- Outside Services: HTTP (80), HTTPS (443)
- Inside IPs: 192.168.1.11, 192.168.1.12
- Inside Services: HTTP (80), HTTPS (443), load balanced

We start by configuring ACOS for two internal web servers and two service groups to load balance across the servers, one group to serve HTTP and the other HTTPS.

```
ACOS-TH####(config)#slb server Inside-Server-1 192.168.1.11
ACOS-TH####(config-real server)#port 80 tcp
ACOS-TH####(config-real server)#port 443 tcp
```

```
ACOS-TH####(config)#slb server Inside-Server-2 192.168.1.12
ACOS-TH####(config-real server)#port 80 tcp
ACOS-TH####(config-real server)#port 443 tcp

ACOS-TH####(config)#slb service-group Inside-Group-HTTP tcp
ACOS-TH####(config-slb svc group)#member Inside-Server-1 80
ACOS-TH####(config-slb svc group)#member Inside-Server-2 80

ACOS-TH####(config)#slb service-group Inside-Group-HTTPS tcp
ACOS-TH####(config-slb svc group)#member Inside-Server-1 443
ACOS-TH####(config-slb svc group)#member Inside-Server-2 443
```

Next, we create a client and server SSL templates. For the internet facing client SSL template we choose a set of strong ciphers compatible with modern web browsers and servers and bind a suitable SSL/TLS certificate and key.

```
ACOS-TH####(config)#slb template client-ssl HTTPS_Client_Template
ACOS-TH####(config-client ssl)#cert My-Webs-VIP-certificate
ACOS-TH####(config-client ssl)#key My-Webs-VIP-key
ACOS-TH####(config-client ssl)#template cipher MaxSec_HTTP2_0-Ciphers

ACOS-TH####(config)#slb template server-ssl HTTPS_Server_Template
ACOS-TH####(config-server ssl)#template cipher MaxSec_HTTP2_0-Ciphers
```

NOTE: Instead of the default ciphers for connections to the internal HTTPS servers, ACOS administrators can define a cipher template consistent with the organization's security policy for communications with these servers.

Next, we create a Web VIP that serves both HTTP and HTTPS to outside users. SYN-cookies are enabled with the syn-cookie command.

```
ACOS-TH####(config)#slb virtual-server My-Webs-VIP-1 1.1.1.1
ACOS-TH####(config-slb vserver)#port 80 http
ACOS-TH####(config-slb vserver-vport)#syn-cookie
ACOS-TH####(config-slb vserver-vport)#service-group Inside-Group-HTTP

ACOS-TH####(config-slb vserver)#port 443 https
ACOS-TH####(config-slb vserver-vport)#syn-cookie
ACOS-TH####(config-slb vserver-vport)#service-group Inside-Group-HTTPS
```

```
ACOS-TH####(config-slb vserver-vport)#template client-ssl HTTPS_Client_
Template
ACOS-TH####(config-slb vserver-vport)#template server-ssl HTTPS_Server_
Template
```

Redirect unencrypted HTTP traffic to HTTPS

Unencrypted HTTP connections expose web services to man-in-the-middle (MITM) attacks and risks the interception of user data, passwords, and other sensitive information. It is highly recommended to provide the content of services via HTTPS, redirecting any HTTP request to the HTTPS service.

ACOS can be configured to immediately redirect new HTTP connections to the HTTPS port of the VIP, rather than relying on internal web servers to perform this operation. This method eliminates the possibility of misconfigured servers that could unintentionally leave HTTP access available.

To continue the example above we restrict the Web VIP for HTTPS by doing the following:

- Create an ACOS HTTP template for use in redirecting traffic to HTTPS (443)
- Remove the HTTP service group from the VIP
- Add the redirection HTTP template to the VIP's HTTP service to redirect connections to HTTPS by adding the redirect HTTP template for the service.

```
ACOS-TH####(config)#slb virtual-server My-Webs-VIP-1 1.1.1.1
ACOS-TH####(config-slb vserver)#port 80 http
ACOS-TH####(config-slb vserver-vport)#redirect-to-https
ACOS-TH####(config-slb vserver-vport)#service-group Inside-Group-HTTP
```

When allowed by the organization's security policy, ACOS can be configured to serve HTTPS and redirected HTTP connections using just the internal HTTP servers. This is called SSL offloading and is often used to reduce CPU load on web servers by not having them decrypt SSL/TLS traffic.

To continue the example, we restrict the Web VIP to just the internal HTTP servers as follows:

- Replace the HTTPS service group with the HTTP service group under the HTTPS (443) virtual port (simply declaring it replaces the existing service-group).
- Remove the server SSL template since there will no longer be any SSL/TLS connections to servers on the internal network.

```
ACOS-TH####(config)#slb virtual-server My-Webs-VIP-1 1.1.1.1
ACOS-TH####(config-slb vserver)#port 443 https
ACOS-TH####(config-slb vserver-vport)#service-group Inside-Group-HTTP
ACOS-TH####(config-slb vserver-vport)#no template server-ssl MaxSec_HTTP2
```

HTTP Strict Transport Security (HSTS)

The Strict-Transport-Security header is a security enhancement that restricts web browsers accessing web servers solely over HTTPS. It ensures the connection cannot be established through an insecure HTTP connection which could be susceptible to attacks. Web servers are commonly under-configured by not enabling support for this security header. In more rare circumstances the servers support legacy web implementations that don't support HSTS.

For deployments where administrators are not fully confident of their server settings (present or on-going) or know that legacy servers are in play, ACOS Web VIPs can be configured to include this HTTP header if it does not exist in HTTP responses from the internal servers.

Continuing the example, we define an HTTP template to insert an HSTS header if the real server did not include one in its HTTP responses and then enable this capability for both services on the VIP.

NOTE: Of the considered security headers, HSTS is one that MUST also be included in the 301/302 redirects from HTTP. Accordingly, it is enabled for the VIP's HTTP port as well.

```
ACOS-TH####(config)#slb template http add-HSTS
ACOS-TH####(config-http)#response-header-insert "Strict-Transport-
Security: max-age=31536000; includeSubDomains; preload" insert-if-not-
exist

ACOS-TH####(config)#slb virtual-server My-Webs-VIP-1 1.1.1.1
ACOS-TH####(config-slb vserver)#port 80 http
```

```
ACOS-TH####(config-slb vserver-vport)#template http add-HSTS

ACOS-TH####(config-slb vserver)#port 443 https
ACOS-TH####(config-slb vserver-vport)#template http add-HSTS
```

Administrators should review the parameter selections for this HSTS header and update values for it according to their security policy. Also, see the ACOS product documentation for alternately replacing or adding HSTS headers when the real servers do indeed include them.

X-XSS-Protection

The `X-XSS-Protection` header is a security enhancement designed to enable the cross-site scripting (XSS) filter built into modern web browsers that prevents them from loading pages when cross-site scripting (XSS) attacks are detected. Valid settings for the header will do one of the following:

- disable protection
- enable protection and attempt to sanitize the response to stop a detected attack
- enable protection and block the response for a detected attack (most secure)

For deployments where administrators are not fully confident of their server settings (present or on-going), or know that legacy servers are in play, ACOS Web VIPs can be configured to include this HTTP header if it does not exist in HTTP responses from the internal servers.

Continuing the example, we define an HTTP template to insert an X-XSS-Protection header if the real server did not include one in its HTTP responses and enable this capability for the HTTPS service on the VIP.

```
ACOS-TH####(config)#slb template http add-X-XSS-Protection
ACOS-TH####(config-http)#response-header-insert "X-XSS-Protection: 1;
mode=block" insert-if-not-exist

ACOS-TH####(config)#slb virtual-server My-Webs-VIP-1 1.1.1.1
ACOS-TH####(config-slb vserver)#port 443 https
ACOS-TH####(config-slb vserver-vport)#template http add-X-XSS-Protection
```

The enable and block option is considered the optimal and most secure setting for this header. See the ACOS product documentation for alternately replacing or adding X-XSS-Protection headers when the real servers do indeed include them.

X-Frame-Options

The `X-Frame-Options` header indicates whether a browser can render a page in an HTML frame, iframe or object tag. Web sites and applications find this header useful to avoid clickjacking attacks as it helps ensure that their content cannot be embedded in other sites. For hardening, it is a common practice to set this header for one of the following:

In general, A10 recommends that ACOS administrators always define SSL cipher templates for their deployments instead of simply relying on ACOS defaults:

- only allow resources that are part of the same origin policy to frame the resource of the HTTP response (SAMEORIGIN)
- deny any resource (local or remote) attempting to frame the resource of the HTTP response (DENY)

For deployments where administrators are not fully confident of their server settings (present or on-going), or know that legacy servers are in play, ACOS Web VIPs can be configured to include this HTTP header if it does not exist in HTTP responses from the internal servers.

Continuing the example, we define an HTTP template to insert an X-Frame-Options header if the real server did not include one in its HTTP responses and enable this capability for the HTTPS service on VIP.

```
ACOS-TH####(config)#slb template http add-X-Frame-Options
ACOS-TH####(config-http)#response-header-insert "X-Frame-Options:
SAMEORIGIN" insert-if-not-exist

ACOS-TH####(config)#slb virtual-server My-Webs-VIP-1 1.1.1.1
ACOS-TH####(config-slb vserver)#port 443 https
ACOS-TH####(config-slb vserver-vport)#template http add-X-Frame-Options
```

Administrators should review the parameter selections for this X-Frame-Options header and update values for it according to their security policy. See the ACOS

product documentation for alternately replacing or adding X-Frame-Options headers when the real servers do indeed include them.

X-Content-Type-Options

The `X-Content-Type-Options` header indicates that the MIME types listed in the Content-Type headers should not be changed and must be followed, effectively disabling MIME type sniffing in the browsers. With MIME sniffing, browsers guess what content type is, rather than trusting Content-Type header's value. Based on that guess, browsers can mistakenly interpret the response content (e.g. thinking text content is Javascript) or tricked into executing malicious code. There is only one valid setting for this header.

For deployments where administrators are not fully confident of their server settings (present or on-going), or know that legacy servers are in play, ACOS Web VIPs can be configured to include this HTTP header if it does not exist in HTTP responses from the internal servers.

Continuing the example above, we define an HTTP template to insert an X-XSS-Protection header if the real server did not include one in its HTTP responses and enable this capability for the HTTPS service on the VIP.

```
ACOS-TH####(config)#slb template http add-X-Content-Type-Options
ACOS-TH####(config-http)#response-header-insert "X-Content-Type-Options:
nosniff" insert-if-not-exist

ACOS-TH####(config)#slb virtual-server My-Webs-VIP-1 1.1.1.1
ACOS-TH####(config-slb vserver)#port 443 https
ACOS-TH####(config-slb vserver-vport)#template http add-X-Content-Type-
Options
```

With only one real encoding, there is no real need to consider replacing or adding this header when the real servers include them.

Block HTTP Methods

Some of the HTTP methods such as TRACE, HEAD, CONNECT and so on can be used for malicious purposes and pose security risk for the web application. Hence, to

protect your web applications you can disallow the HTTP methods which are not used frequently.

Best practice is to block the HTTP methods not used. ACOS sends a 400 response to the client before dropping the request. HTTP protocol versions HTTP 1.1, HTTP/2, and HTTP/3 are supported.

The methods that can be disallowed are: GET, BIND, CONNECT, COPY, DELETE, HEAD, LABEL, LOCK, MERGE, MKCOL, MOVE, OPTIONS, PATCH, POST, PRI, PROPFIND, PROPPATCH, PUT, REBIND, TRACE, UNBIND, UNLINK, UNLOCK, UPDATE, PURGE, TRACK.

To block the HTTP methods, use the **disallowed-methods** command in the SLB template HTTP:

```
ACOS-TH####(config)#slb template http HTTP-Blocked-Methods
ACOS-TH####(config-http)#disallowed-methods "TRACE CONNECT" action drop
```

HTTP Connection Idle Timeout

Holding connections can cause denial of service attacks by depleting the connection resource. By detecting and disconnecting idle connections, ACOS prevents unused or stalled connections from consuming server resources indefinitely. Set the maximum time an HTTP client connection can remain idle such that if no data is sent or received after the idle time expires, the connection is closed.

To configure the connection idle timeout, use option 'client-idle-timeout' under SLB Template HTTP.

```
ACOS-TH####(config)#slb template http http-template
ACOS-TH####(config-http)#client-idle-timeout <seconds>
```

The idle timeout value depends on the application. Typical web applications set the idle timeout to 5 seconds.

HTTP Request Header Timeout

Some attacks such as Slowloris attempts to split the HTTP request across multiple packets very slowly. Setting the HTTP request header timeout is one preventative measure. Preventing Slowloris involves implementing other measures such as

limiting the number of connections per IP. It is recommended to set the HTTP request header timeout to 10 seconds and apply the template to the VIP.

```
ACOS-TH####(config)#slb template http http-template
ACOS-TH####(config-http)#req-hdr-wait-time 10
```

IP Limits

Another prevention measure to be used with other measure against denial of service attacks is the IP limits feature. IP limits enforces the following limits if defined for each source IP:

- Concurrent connections
- Connection rate
- Concurrent Layer 7 requests
- Layer 7 request rate

IP limits may be configured globally, per virtual server, or per virtual server port.

A10 recommends applying IP limits on your services to limit exposure to high connection and request attacks from unique sources.

A simple configuration is provided below but you must customize the limit policy based on your needs. For more details, refer to the *DDoS Mitigation for ADC Guide*. Below is an example of setting the 4 limit types. Rate limits are specified in rate per 100 ms units. 10 units of 100 ms is 1000ms or 1 s. The rates in the example below are 2 per second.

```
ACOS-TH####(config)#glid 1
ACOS-TH####(config-glid:1)#request-limit 10
ACOS-TH####(config-glid:1)#request-rate-limit 2 per 10
ACOS-TH####(config-glid:1)#connection-limit 20

ACOS-TH####(config-glid:1)#connection-rate-limit 2 per 10
ACOS-TH####(config-glid:1)#over-limit-action reset log
ACOS-TH####(config-glid:1)#exit
ACOS-TH####(config)#class-list 2
ACOS-TH####(config-class list)#0.0.0.0/0 glid 1
ACOS-TH####(config)#slb template policy global_policy
ACOS-TH####(config-policy)#class-list 2
```

```
ACOS-TH####(config)#slb virtual-server vip 10.10.10.10
ACOS-TH####(config-slb vserver-vport)#template policy global_policy
```

HTTP/2 Frame Limits

ACOS provide built in mechanisms to protect against HTTP/2 rapid reset DDoS attacks. To further limit the attack, A10 recommends changing the frame limit in http template from the default of 10,000 to 50 and apply the http template to the VIP. The frame-limit configuration limits the number of CONTINUATION, PING, PRIORITY, RESET, SETTINGS and empty frames in one HTTP2 connection. The default limit is 10,000.

```
ACOS-TH####(config)#slb template http frame-limit
ACOS-TH####(config-http)#frame-limit 50
```

HTTP/3 over QUIC

ACOS can load balance HTTP version 3 (HTTP/3) protocol traffic. HTTP/3 uses QUIC, a UDP based transport protocol that provides a reliable and secure connection for multiplexing several requests and a faster response time. While QUIC is a secure protocol similar to TLS 1.3, support for QUIC in other network security and inspection devices is limited or non-existent. Most network security best practices recommend blocking QUIC at the firewall or at the web browser. A10 recommends avoid using HTTP/3 over QUIC and recommends HTTP/2 over TLS v1.3.

Rate Limit ICMP

ICMP is useful for troubleshooting and essential for the network to operate properly. Blocking ICMP completely isn't recommended. ICMP floods can cause denial of service attacks by consuming resources. To minimize the risk of denial of service, apply ICMP rate limits. You may rate limit ICMP globally, at the interface, or on the VIP. Rates are defined in units ICMP packets per second.

To limit ICMP rate globally:

```
ACOS-TH####(config)#icmp-rate-limit 2000
ACOS-TH####(config)#icmpv6-rate-limit 2000
```

To limit ICMP rate on an interface:

```
ACOS-TH####(config)#interface ethernet 1
ACOS-TH####(config:ethernet:1)#icmp-rate-limit 2000
ACOS-TH####(config:ethernet:1)#icmpv6-rate-limit 2000
```

To limit ICMP rate on a VIP:

```
ACOS-TH####(config)#slb template virtual-server vs-template
ACOS-TH####(config-vserver)#icmp-rate-limit
ACOS-TH####(config-vserver)#icmpv6-rate-limit
ACOS-TH####(config)#slb virtual-server My-Webs-VIP-1 1.1.1.1
ACOS-TH####(config-slb vserver)#template virtual-server vs-template
```

You may also set lock out periods where all ICMP is dropped for a specified time period if exceeding the defined lockout rate. For more information, refer to the *DDoS Mitigation for ADC Guide*.

Access Control based on Allow or Deny Lists

Whether you are providing public or private services, limiting exposure to known bad actors or threats and minimizing access to trusted IP subnets, IP hosts, port and protocol is important.

By default, all IP subnets and hosts are allowed access to the virtual server provisioned. It is recommended that you apply a control to limit access services being provided by using one of the following methods available in ACOS.

- Access control lists (ACL)
- Firewall rules (available only on Convergent Firewall CFW)
- Class-lists

A10 recommends using the Firewall for controlling access based to the VIP on Layer 1 through Layer 4 parameters. The Firewall is available only in the Thunder Convergent Firewall (CFW) product.

Configuring the Firewall

The basic steps to configure the firewall are to define the outside and inside zones, typically these are grouped by interfaces, where the outside can be considered the network between the client and the virtual server hosted by ACOS device, and the inside is between the virtual server (hosted by ACOS device) and the real backend

server. Once the zones are defined, assuming you have already configured and validated the virtual servers, create firewall rules using the virtual servers created.

The following is a simple example of how to configure the firewall for a HTTPS virtual service:

```
zone Inside
  interface ethernet 3
!
zone Outside
  interface ethernet 2
```

```
slb virtual-server Web-Portal 10.10.10.10
  <virtual server config>

object-group network Client-Network fw v4
  192.168.1.0/24
!
object-group service HTTPS-Service
  tcp eq 443
!
rule-set rs1
  rule portal
    source object-group Client-Network
    source zone Outside
    dest virtual-server Web-Portal
    dest zone Inside
    service object-group HTTPS-Service
    action permit log
!
fw active-rule-set rs1
```

The Firewall may provide additional security checks and features such as unicast reverse path forwarding (URPF), tcp window, rate limiting, logging, and dynamic blacklisting. For more details and options to figure the firewall, refer to the *Firewall Configuration Guide*.

Configuring Access Control Lists

Access control lists is available in all Thunder products and can be used to filter out unwanted traffic when the firewall feature is not present. Aside from basic Layer 4 packet filtering, access lists do not provide the additional security checks provided by the Firewall. Controlling network access to the VIP can be achieved by creating an access list and applying it to the vport or the VIP. Recommend limit network access to only those hosts and network which should be allowed access.

The following example allows only subnet 192.168.1.0/24 to access the VIP:

```
object-group network Client-Subnet
 192.168.1.0 0.0.0.255

access-list 120 4 permit ip object-group Client-Subnet any log
```

Apply the access-list to the vport

```
slb virtual-server vs-hosted 2.2.2.2
  port 443 http
    access-list 120
```

For transparent proxy deployments (where the Thunder doesn't host the VIP IP), the ACL may be applied to the virtual server object like such.

```
slb virtual-server vs-transparent 3.3.3.3 acl 120
```

Threat IPs

A10 provides IP threat lists via the A10 Defend Threat Control and recommends using the IP threat list to block bad actors from using known malicious sources when providing services exposed to the internet. IP threat lists are dynamic and need to be updated frequently. Dynamic and up-to-date threat lists requires Thunder CFW and additional subscription of A10 Defend Threat Control. The following example updates the threat-list every 8 hours. Traffic matching the threat-list is dropped.

```
ACOS-TH####(config)#import-periodic class-list threat-list
<https://a10defend-threat-list-url> period 28800
system ip-threat-list
ipv4-internet-threat-list
class-list threat-list
```

Controlling Access Based on Geolocation

Geo-location-based access controls uses client's location to determine access privileges. Using black-white lists, ACOS can perform one of the following actions to traffic from a client based on the client's geographic location. ACOS comes preinstalled with several geolocation databases from IANA, AFRINIC, APNIC, ARIN, LACNIC, and RIPE.

- Drop the traffic
- Reset the connection
- Send the traffic to a service group

The following command imports black/white list "geolist" onto the ACOS device.

```
ACOS-TH####(config)#import bw-list geolist scp://192.168.1.20/root/geolist
```

The file geolist must be a text file that contains entries (rows) in the following format:

```
L "geo-location" group-id #conn-limit
```

The following commands configure a policy template named "geoloc" and add the black/white list to it. The template is configured to drop traffic from clients in the geo-location mapped to group 1 in the list. The geo-location code can be found by show gslb geo-location.

```
ACOS-TH####(config)#slb template policy geoloc
ACOS-TH####(config-policy)#bw-list name geolist
ACOS-TH####(config-policy)#bw-list id 1 drop
ACOS-TH####(config-policy)#exit
```

The following commands apply the policy template to port 443 on virtual server "vip1":

```
ACOS-TH####(config)#slb virtual-server vip1
ACOS-TH####(config-slb vserver)#port 80 http
ACOS-TH####(config-slb vserver-vport)#template policy geoloc
```

A10 recommends using a commercial source such as MaxMind or DB-IP to provide the latest geo-location data for improved accuracy.

For more information on how to configure access by geolocation, refer to *DDoS Mitigation Guide For ADC* section “Location based VIP Access.”

Next Generation Web Application Firewall (NGWAF)

A10 Next-Gen WAF (NGWAF) is a supplemental add-on to an existing ADC or CFW deployment that monitors suspicious and anomalous web traffic and protects against attacks directed at applications and origin servers. It provides superior protection for applications and APIs provides protection against the following attacks:

- OWASP Top 10
- Advanced Web attacks
- Malicious bots
- DDoS attacks
- Volumetric attacks
- Account Takeover (ATO) and Credential Stuffing - Prevents attackers from using known lists of compromised credentials and breach data dumps for illegal access.

API and microservice protection

- API Brute Forcing Protection - Identifies and blocks brute forcing sensitive IDs or tokens in APIs attacks such as Unique Identifier Enumeration.
- Unauthorized API Access Prevention - Protects fraud gift card and credit card validations, attempts to obtain patient healthcare records, and more.
- API Abuse Mitigation - Mitigates potential attacks aiming to abuse sign-up systems, emails, and other sensitive actions.

A10 recommends using NGWAF to protect your web and API based services. A10’s NGWAF requires an additional license to enable as well as an account on the partner Cloud Portal. To configure NGWAF, please refer to the *Next Generation Web Application Firewall Guide.*

Authentication, Authorization, and Audit

Most websites have protected content such that portions of their site require authentication and authorization. Authorization or access to specific portions of a site may be restricted based on a user's role or group membership. Thunder ACOS Application Access Module (AAM) provides both authentication, authorization, and audit capabilities which you may use for your website. ACOS does not provide the identity store for your users but can integrate with major identity providers by supporting the most commonly used protocols: OpenID Connect (OIDC), OAuth, and Security Assertion Markup Language (SAML). A10 recommends integrating your website's login with your identity provider to control access to the protected resources. To configure OIDC and OAuth, refer to section "OAuth 2.0 and Open ID Connect" of the "Application Access Management Guide." To configure SAML, refer to section "Security Assertion Markup Language" of the "Application Access Management Guide."

ACOS provides a centralized authorization policy which allows you to control access to different locations within your site based on attributes in the user's authorization token. To configure authorization policy, refer to the "Application Access Management Guide" section "AAA and AAA Policies."

ACOS generates authentication and access logs which can be used for auditing purposes. ACOS standard syslog and acos-event logging may be configured to send these logs to external syslog servers. To configure the logs, refer to the *Application Access Management Guide* section *Authentication Logs*.

```
ACOS-TH####(config)#aam authentication oauth authorization-server <NAME>
ACOS-TH####(config)#aam authentication oauth client <NAME>
ACOS-TH####(config)#aam authentication relay oauth <NAME>
ACOS-TH####(config)#aam authentication template <NAME>
ACOS-TH####(config-auth template:<NAME>)#type oauth
ACOS-TH####(config-auth template:<NAME>)#oauth-authorization-server
<oauth_authz_svr>
ACOS-TH####(config-auth template:<NAME>)#oauth-client <oauth_client>
```

reCAPTCHA Challenge Authentication

Any website that has a login page to authenticate users is subject to hackers and malicious software bots trying to gain access or disable accounts of users. To prevent and deter these types of attacks, ACOS integrates with the reCAPTCHA challenge service from Google to improve security and protect against brute force password hacks. It also supports Google's reCAPTCHA web service and using AAM flexible advanced customization to add challenges in the form-based logon.

The reCAPTCHA challenge blocks the automated password guessing attacks, followed by temporary account lockout after several authentication failures.

```
ACOS-TH####(config)#aam authentication portal default-portal
ACOS-TH####(config-portal:default-portal)#logon
ACOS-TH####(config-portal:default-portal-logon)#enable-CAPTCHA type
reCAPTCHAv2-checkbox site-key <key>
ACOS-TH####(config)#aam authentication logon form-based <NAME>
ACOS-TH####(config-form-based auth logon:<NAME>)#portal default-portal
ACOS-TH####(config)#aam authentication captcha <NAME>
ACOS-TH####(config)#aam authentication template <NAME>
ACOS-TH####(config-auth template:<NAME>)#captcha <captcha_profile>
```

When managing your own login pages, A10 recommends adding the reCAPTCHA service. For more information about configuring reCAPTCHA, refer to the "Application Access Management Guide" section "reCAPTCHA Challenge for Authentication."

Contact Us