Cisco ASA 9.20 on Firepower 4100 and 9300 Security Appliances

Preparative Procedures & Operational User Guide

for the Common Criteria Certified Configuration

Version 1.0

January 7, 2024

Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

Introduction 5

Distinctions between ASA and FXOS on Firepower 4100 and 9300 5

ASA Version 9.20(3) Documentation Set 6

Audience 6

Supported Hardware & Software Versions 6

Overview of the Cisco ASA Firewall & VPN Platforms 7

Operational Environment Component & Usage 7

Example Deployment 8

Security Information 9

Organizational Security Policy 9

Securing the Operational Environment 9

Certified Configuration 11

Physical Security 11

Administrative Access 11

Monitoring & Maintenance 12

Systems Logs 12

Administration 12

Saving the Configuration 14

Backup and Restoration 14

Device Failover 14

Authentication to the ASA 14

Local and Remote Access 14

Login Banners 16

Usernames, Privileges, and Administrative Roles 17

Usernames and Privileges 17

Authorized Administrator 17

Passwords 18

Password Complexity, Length, and Uniqueness 18

Password Policies 19

Setting the Clock 20

Account Lockout after Failed Login Attempts 21

Secure Communications 22
Evaluated Cryptography........ 22
Enable FIPS Mode 22
Configuring SSH [Optional] 23
ECDSA Key Generation........ 23
Restrict SSH Connections 24
Enable SSHv2 and Disable SSHv1 24
Encryption Algorithms 24
Hashing Algorithms........ 25
Key-Exchange 25
SSH Session Rekey Limits 25
Authentication 26
Idle Timeouts 26
SCopy (disabled by default) 27
Configuring TLS 27
Specify the TLS Version........ 27
Specify the TLS Ciphersuites (optional)........ 27
Specify the TLS Server and Client Certificates 28
Configuring IPsec........ 28
Managing Public Key Infrastructure (PKI) Keys........ 29
Enable IKEv2........ 29
Post Quantum Preshared Key (PPK) Configuration 29
IKEv2 Parameters for IKE Phase 1 (the IKE SA) 30
IKEv2 Parameters for IKE Phase 2 (the IPsec SA) 30
Create an Access-List and Assigning to Crypto Map........ 31
Select Tunnel or Transport mode 32
Certificate Map Subject DN........ 32
Viewing an IPsec Configuration 33
Clearing Security Associations 33
IPsec Authentication........ 34
VPN Client Access Restriction 38
Configure an IP Address Assignment Policy........ 38
Specifying a VPN Session Idle Timeout 39

Firewall Functionality 39
Routed Mode and Transparent Mode 39
Routed Mode 39
Transparent Mode 39
Setting Transparent or Routed Firewall Mode at the CLI 39
Audit Trail Full Mode 39
Enabling Syslog Host Status Monitoring 40
Recovering from Syslog Host Down 40
Traffic Flow Overview 41
Trusted & Untrusted Networks 41
Stateful Inspection Overview 41
Application Layer Protocol Inspection 42
Same-Security-Traffic 42
Access Lists 42
Configure Extended ACLs 43
Using the ‘Established’ Keyword 44
Time-to-Live 44
VLAN Interfaces 44
Interface Types 44
Servers and Proxies 45
Protect from SYN Flood DoS Attack (TCP Intercept) 45
Configure Global Timeouts 47
Default Traffic Flow (without ACLs) 47
Optional Traffic Inspection 49
Unicast RPF 49
STP & Transparent Mode 49
Inspect ICMP 50
Inspect ARP 50
Prohibit IPv6 Extension Header 0 50
Optional Authentication of Throughput Traffic 50
Mandatory Traffic Flow Controls 51
Set “ip audit” Actions 51
Do not disable certain signatures 52

Define “ip audit” Policies 52
Apply “ip audit” Policies to Interfaces 52
Overview of Traffic to Be Dropped, and the Related Syslog Messages 52
Logging and Log Messages 63
Timestamps in Audit Messages 63
Usernames in Audit Messages 63
Using TCP Syslog to Detect Syslog Host Down 63
Timely Notification/Transmission of ACL Logging 64
Secure Transmission of Audit Messages 64
Configure Reference Identifier: 64
Securing Syslog with TLS: 66
Securing Syslog with IPsec 67
Securing RADIUS Accounting Messages with IPsec 67
Auditable Events Certified Under Common Criteria 67
ASA Installation 77
Verification of Image and Hardware 78
Adaptive Security Device Manager (ASDM) 79
Enabling HTTPS Access 79
Configure DN matching for ASDM 80
Enable Idle-Timeouts of ASDM Sessions 80
Accessing ASDM from Your Workstation 80
Running ASDM 81
Network Services and Protocols 82
Modes of Operation 86
Appendix: 89
Acronyms & Abbreviations 89
Obtaining Documentation 91
Obtaining Technical Assistance 91
Cisco Technical Support & Documentation Website 91
Submitting a Service Request 91
Definitions of Service Request Severity 92
Obtaining Additional Publications and Information 92

Introduction

This document describes how to install and configure the Cisco ASA Adaptive Security Appliance (ASA) running software version 9.20(3) on Firepower 4100 and 9300 certified under Common Criteria as conformant with the Protection Profiles as listed in the table below.

Protection Profile	Version	Date
PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways (CFG_NDcPP-FW-VPNGW_V1.3)	1.3	18 August 2023
The PP-Configuration includes the following components:		
• Base-PP: Collaborative Protection Profile for Network Devices, (CPP_ND_V2.2E)	2.2e	23 March 2020
• PP-Module for Stateful Traffic Filter Firewalls, (MOD_CPP_FW_1.4E)	1.4 + Errata 20200625	25 June 2020
• PP-Module for Virtual Private Network (VPN) Gateways, (MOD_VPNGW_V1.3)	1.3	16 August 2023

In this guide, “security appliance” and “adaptive security appliance” apply to all Firepower 4100 and 9300 models running version 9.20, unless specifically noted otherwise. Version 9.20 will be referred to as 9.20 or 9.20.x hereinafter.

Note: Failure to follow the information provided in this document will result in the adaptive security appliance not being compliant with the evaluation and may make it insecure.

This document is an addendum to other documentation available for installation and configuration of the Cisco ASA with version 9.20, and this document should be read in its entirely before configuring the security appliance. The Firepower 4100 and 9300 Series appliances running ASA are also running FXOS (Firepower eXtensible Operating System) version 2.14. To configure the FXOS portion of this system, refer to “Cisco FXOS 2.14 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration.”

Distinctions between ASA and FXOS on Firepower 4100 and 9300

Except where specified, details described in this document apply only to ASA. For corresponding details about FXOS, refer to, *“Cisco FXOS 2.14 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration.”*

All firewall and VPN gateway functionality is enforced by ASA. FXOS is used to manage the Firepower 4100 and 9300 chassis. Use the FXOS interfaces to install and upgrade ASA devices onto these platforms. On the Firepower 4100 and 9300 platforms, ASA and FXOS generate separate syslog messages and each transmit their messages separately to remote syslog servers over their own secure channels, which do not interfere with each other. FXOS will always secure syslog in IPsec, while ASA can be configured to transmit syslog via TLS, or IPsec or both (TLS over IPsec).

ASA Version 9.20(3) Documentation Set

- *Release Notes for the Cisco Secure Firewall ASA, 9.20(x), August 14, 2024*
- **ASA Quick Start Guides:**
  - ***Cisco Firepower 4100 Getting Started Guide***
  - ***Cisco Firepower 9300 Getting Started Guide***
- **CLI Configuration:**
  - *General Operations CLI Configuration*
  - *Firewall CLI Configuration*
  - *VPN CLI Configuration*
  - ***FXOS Configuration:*** *To configure the FXOS portion of this system, refer to Cisco FXOS 2.14 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration, October 14, 2024*
- **Cisco AnyConnect:**
  - *Cisco AnyConnect Secure Mobility Client Administrator Guide*
- **Syslog Messages**:
  - *Cisco ASA Series Syslog Messages, 9.20*
- **Regulatory Compliance and Safety Information:**
  - Regulatory Compliance and Safety Information - Cisco Firepower 4100 Series, March 15, 2017 *https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/4100/hw/regulatory/compliance/RCSI-0285-book.pdf*
  - Regulatory Compliance and Safety Information - Cisco Firepower 9300, July 21, 2017 *https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/9300/hw/regulatory/compliance/RCSI-0203-book.pdf*

To find an HTML or PDF version of many Cisco titles go to *www.cisco.com*. Type the title in the 'Search' field and click **Go**.

Audience

This document is written for administrators configuring the Cisco ASA version 9.20(3). This document assumes you are familiar with networks and network terminology, that you are a trusted individual, and that you are trained to use the Internet and its associated terms and applications.

Supported Hardware & Software Versions

Only the following hardware and software listed in Table 1 and Table 2 is compliant with the security appliance 9.20(3) Common Criteria evaluation. Using hardware not specified invalidates the secure configuration. Likewise, using any software version other than the Cisco ASA with 9.20(3) will invalidate the secure configuration.

Table 1: Supported Hardware

Hardware Models	• ASA Firepower 4100 Series (4112, 4115, 4125 and 4145) • ASA Firepower 9300 (including chassis, supervisor blade, security module)

Table 2: Supported Software

Software	**Version**
Cisco Adaptive Security Appliance 'image'	9.20(3)

Firepower eXtensible Operating System (FXOS)	2.14
Cisco AnyConnect Client (in operational environment)	4.10 or later
Cisco Adaptive Security Device Manager (ASDM)	7.22

Overview of the Cisco ASA Firewall & VPN Platforms

The configuration consists of the following configuration:

- Firepower Appliance: One or more Firepower 4100 Series appliances (4112, 4115, 4125 and 4145), and/or one or more Firepower 9300 appliance with one or more security modules (SM-40, SM-48 or SM-56), running FXOS version 2.14.
- ASA software: ASA 9.20 installed to the Firepower hardware listed above.
- ASDM software: The ASDM software is installed on each ASA. Only the Cisco ASDM Launcher is installed locally on the management platform.

Operational Environment Component & Usage

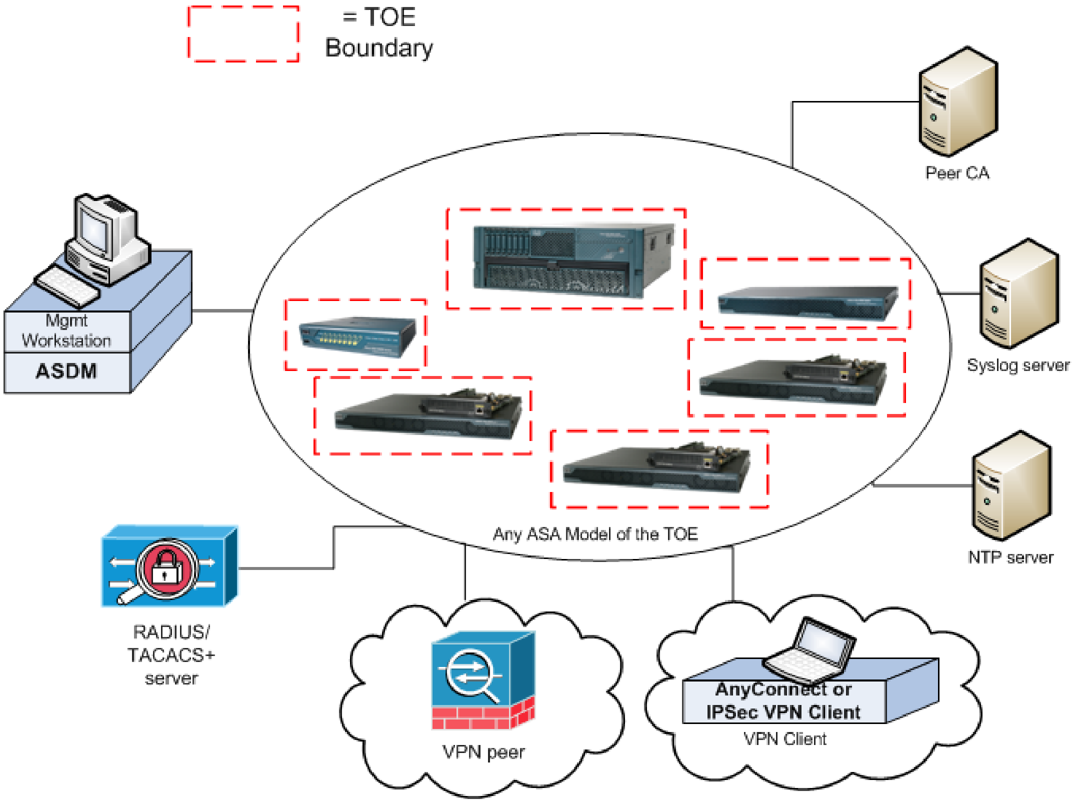
The following are components of the environment of the evaluated product.

Table 3: Components of the Operational Environment

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with SSH client installed that is used by the TOE administrator to support TOE administration through SSHv2 protected channels. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	The Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
ASDM Management Platform	Yes	The ASDM operates from any of the following operating systems: Microsoft Windows 7, 8, 10, 11, Server 2008, Server 2012, Server 2012 R2, Server 2016, Server 2019 and Server 2022 Apple OS X 10.4 and later ASDM runs on the management platform (workstation) and is used to connect to the TOE over TLS using a web browser.
Web browser	Yes	The following web browsers are supported for access to the ASDM; • Internet Explorer • Firefox • Safari • Chrome Note: Using the latest supported web browser version is recommended.

Component	Required	Usage/Purpose Description for TOE performance
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Connections to remote audit servers must be tunneled in IPsec or TLS.
AAA Server	No	This includes any IT environment AAA server that provides single-use authentication mechanisms. The TOE correctly leverages the services provided by this AAA server to provide single-use authentication to administrators. Connections to remote AAA servers must be tunneled in IPsec.
Certification Authority	Yes	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
Remote Tunnel Endpoint	Yes	This includes any peer with which the TOE participates in tunneled communications. Remote tunnel endpoints may be any device or software client (e.g., Cisco AnyConnect) that supports IPsec tunneling. Both VPN clients and VPN gateways can be considered to be remote tunnel endpoints.
NTP Server	No	The TOE supports communications with an NTP server. Connections to remote NTP servers can be tunneled in IPsec.

Example Deployment



The previous figure includes the following:

- Several examples of TOE Models
- VPN Peer (Operational Environment) or another instance of the TOE
- VPN Peer (Operational Environment) with Cisco VPN Client or AnyConnect Client
- Management Workstation (Operational Environment) with ASDM and SSH client
- Remote Authentication Server (Operational Environment)
- NTP Server (Operational Environment)
- Peer CA (Operational Environment)
- Syslog server (Operational Environment)

Security Information

In addition to the *Regulatory Compliance and Safety Information* documentation (see document links above), the following sections provide additional security information for use with a Common Criteria Certified adaptive security appliance.

Organizational Security Policy

Ensure that your security appliance is delivered, installed, managed, and operated in a manner that maintains an organizational security policy.

Securing the Operational Environment

Proper operation of the ASA it is Common Criteria certified configuration, i.e., the Target of Evaluation (TOE), requires that some security objectives be satisfied by the operational environment. It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions and adheres to the environment security objectives listed below. The environmental security objective identifiers map to the environmental security objectives as defined in the certified Security Target document.

Table 4: Operational Environment Security Measures

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	Administrators must ensure the ASA is installed and maintained within a secure physical location. This can include a secured building with key card access or within the physical control of an authorized administrator in a mobile environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	Administrators must not add any general-purpose computing capabilities (e.g., compilers or user applications) to the ASA.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.	Administrators must ensure that there is no unauthorized access and the operational environment is set up as described
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	Administrators must be properly trained in the usage and proper operation of the ASA and all the enabled functionality. These administrators must follow the provided guidance.

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must regularly update the ASA to address any known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators must protect their access credentials where ever they may be.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on firewall equipment when the equipment is discarded or removed from its operational environment.	Administrators must ensure that there is no unauthorized access to sensitive information on firewall equipment.

Certified Configuration

Use only the security appliance software version 9.20(3). Only the hardware versions listed in Table 1 and software version in Table 2 can be used to implement one of the certified configurations. Changing the software to a different version invalidates the evaluated status of a particular hardware platform.

Features Prohibited from Use

In its Common Criteria certified configuration the following are prohibited:

- Use of the TTL Decrement feature
- Use of telnet for administrative access
- Use of the SNMP server on the ASA
- Use of Security Policy Manager
- Use of ASA Clustering

Physical Security

The security appliance must be located in a physically secure environment to which only a trusted administrator has access. The secure configuration of the security appliance can be compromised if an intruder gains physical access to the security appliance. Similarly, the audit server used to store and manage the security appliance system log messages must be protected physically, and with appropriate logical security protections.

Administrative Access

There are only three methods by which the administrator can manage the security appliance:

- Local serial console port access to the command line interface (CLI)
- SSH (SSHv2) for remote access to the command line interface (CLI)

- ASDM (TLS) for remote access to the graphical user interface (GUI)

Note: Telnet is not permitted for management on the certified security appliance. It is disabled by default, and must remain disabled. If telnet is accidentally enabled, use the “no” version of the command to disable it.

```
hostname(config)# no telnet [IP address] [subnet mask] [interface]
```

Note: The CLI is the preferred method for VPN management configuration.

Monitoring & Maintenance

The security appliance software provides several ways to monitor the security appliance, from logs to messages.

- Ensure you know how you will monitor the security appliance, both for performance and for possible security issues.
- Plan your backups. If a hardware or software problem occurs, you may need to restore the security appliance configuration.
- The configuration of the security appliance should be reviewed regularly to ensure that the configuration meets the security objectives of the organization in the face of the following:
    - Changes in the security appliance configuration
    - Changes in the security objectives
    - Changes in the threats presented by the external network

Systems Logs

Cisco ASA Series Syslog Messages provides details on the security appliance system logs. The following sections are not supported in the certified configuration:

- Security Appliance System Log
    - Receiving SNMP requests
    - Sending SNMP Traps
- Other Remote Management and Monitoring Tools
    - Cisco Secure Policy Manager
    - SNMP Traps

Administration

Note: The details described in this section apply only to ASA. For corresponding details about FXOS, refer to, “Cisco FXOS 2.14 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration.”

The Security Management Function provides a command line interface (CLI) that allows an authorized administrator to configure security functionality on the ASA either locally via the console port, remotely via ASDM (TLS), or remotely using SSH, and optionally tunneling SSH and ASDM sessions over IPsec, to perform the following actions:

1. Enable or disable the operation of the product;
2. Configure the access banner for CLI (console and SSH) and GUI (ASDM);
3. Configure the session inactivity time before session termination;
4. Update/replace ASA software, and verify the integrity of new software using digital signature prior to installing the updates. **Note:** ASA running on Firepower 4100 and 9300 is not updated via ASA CLI or ASDM as with ASA running on other platforms. On these platforms all ASA installations and upgrades are managed via the FXOS (via CLI or Firepower Chassis Manager). For further information, refer to “Image

Management" section of the *Cisco FXOS 2.14 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration*.;

5. Specify the limits for the number of authentication failures;
6. Configure firewall rules;
7. Configure cryptographic functionality;
8. Configure IPsec functionality;
9. Import X.509v3 certificates;
10. Generate, import, change and delete cryptographic keys;
11. Enable or disable the multiple authentication functions including;
    a. Single-use authentication
    b. Reusable password authentication
    c. Certificate-based authentication of tunnel endpoints
12. Enable, disable, determine and modify the behavior of the audit trail management;
13. Enable, disable, determine and modify the behavior of the functionality to backup and restore data including information flow rules, and audit trail data;
14. Enable, disable, determine and modify the behavior of communication of authorized external IT entities;
15. Query, modify, delete, and assign the administrator attributes including;
    a. username
    b. privilege level
    c. password
16. Set the time and date used to form the timestamps.

Upon successful identification and authentication, the administrator has access to the CLI that enables an administrator to manage and monitor the ASA. The CLI is divided into different command modes. Each command mode has its own set of commands available for the configuration, maintenance, and monitoring of the ASA. The commands available depend on the current active mode. The use of specific commands allows navigation from one command mode to another.

The command modes are grouped into two categories based on the Authorized Administrator role; "unprivileged" is where an administrator can view configuration information but cannot change it, which is the initial login state when logging into the CLI when privilege level is set to 1 and the command prompt is a ">". The other mode is "privileged" mode which provides the ability to change configuration information, and the command prompt is a hash, "#".

The ASA supports multiple privilege levels for administrative sessions, the highest of which is a privilege 15. Within the single local database, users can each be assigned a privilege level (0-14) and service-type set to "admin". (NOTE: In the Common Criteria certified configuration, usernames in the local user database must not have privilege level 15 so that the ASA is able to enforce lockout of all local accounts, given that privilege level 15 is exempt from lockout.)

The following applies when authentication and "exec" authorization are enabled: In order to be authorized for "enabled" access, i.e, access to the privileged prompt, the user must have the their service-type set to "admin". Note that users in the local user database are automatically given "admin" service-tag if the service-type attribute is not otherwise configured.

- 'aaa authentication ssh console LOCAL' sets the ASA to authenticate SSH users against the local database.
- 'aaa authorization exec' requires authorization of users before they can get to the exec console.

Upon successful login, by default, the administrator can access the unprivileged CLI commands. When the administrator authenticates with the enable or login command, the administrator has access to privileged modes and commands. Though the administrator could also use the unprivileged mode, all ASA relevant administrative operations are performed in a privileged mode. The above listed management functions can only be performed by the authorized administrator in a privileged mode.

The Security Management Function ensures that validated security attributes are entered by an authenticated administrator

Saving the Configuration

The **write memory** command should be used frequently when making changes to the configuration of the security appliance. If the security appliance reboots and resumes operation when uncommitted changes were made, these changes will be lost and the security appliance will revert to the last configuration saved.

The security appliance loads the saved startup configuration and automatically copies this configuration into the running configuration. As a user configures the running configuration to his specific needs he either saves the running configuration or saves the updated configuration to the startup configuration. The running configuration is held in volatile memory so if the security appliance is reloaded due to either operational reasons or operational error and any changes have not been saved these changes will be lost.

Backup and Restoration

Note: Use of backup and restoration is optional in the certified configuration, but if backup and restoration are performed over a network connection, encrypted connections must be used as described in this section.

The ASA provide the capability to backup and restore configuration information. This can be accomplished by accessing the ASA through either the ASA CLI or the ASDM. Information regarding ASA Backup and Restoration can be found in the "Back Up and Restore Configurations or Other Files" section of the *CLI Book 1* or *ASDM Book 1,* the "General Operations" guides.

To securely copy configuration files, log files, or software images to or from the ASA, use the copy command from the ASA CLI:

```
copy http[s]://[user[:password]@]server[:port]/[path/]filename]”
```

Note: There is a "copy http" command, but be sure to use "copy https" (with the 's').

Note: When using "copy https", the encrypted channel is established before the password is transmitted, so the password is not transmitted in plaintext.

Device Failover

Configuration of failover is optional in the certified configuration, and evaluation of the encryption method used for the failover connection was beyond the scope of the evaluation. However, if failover is enabled, the recommended configuration is to enable encryption as described here.

When using failover, configure an authentication password to be used between the two firewall units, and ensure the password used for the key complies with the "Password Complexity" guidance within this document. The command is:

```
failover key {secret | hex key}
```

For more information see the "High Availability and Scalability" section of the *CLI Book 1* or *ASDM Book 1*, the "General Operations" guides.

Authentication to the ASA

Local and Remote Access

Administrative access to any administrative interface (console, SSH, and/or ASDM) can be configured to use remote AAA (RADIUS) authentication, and/or local authentication. For example, the following authentication mechanisms would be viable configurations for each interface:

- SSH: Authenticate first to a remote AAA server, and fallback to local user database authentication if the remote AAA server is unavailable.
    - Note: Configuring fall-back to local authentication is optional. If no fallback to local is configured, access via SSH is not possible when the remote AAA server is unavailable.
    - Accounts defined on the remote AAA server can be defined as privilege level 15, or any other level 1 or higher (level 1 is the minimum level required for access via SSH).
- ASDM: Authenticate only to the remote AAA server, and never fallback to the local user database when the remote AAA server is unavailable.
    - Note: Not configuring fall-back to local authentication is optional, and would result in no access via ASDM when the remote AAA server is unavailable.
    - Accounts defined on the remote AAA server can be defined as privilege level 15, or any other level 2 or higher (level 2 is the minimum level required for access via ASDM).
- ASDM or SSH from AnyConnect or Cisco VPN Client: Authenticate
    -

Note: When administrators are authenticated to a remote AAA server, any account lockout functions of the local user database will not be applied, so the remote AAA server would need to provide account lockout after failed authentication attempts.

Before any of the following steps to configure the ASA to use a remote AAA server, first choose a RADIUS solution and install it. To create a server group, add AAA servers to it, configure the protocol, add authentication to SSH, and perform the following steps:

Step 1: Identify the server group name and the protocol. To do so, enter the following command:

```
hostname(config)# aaa-server server_group protocol {radius | tacacs+}
```

For example, to use RADIUS to authenticate network access and TACACS+ to authenticate CLI access, you need to create at least two server groups, one for RADIUS servers and one for TACACS+ servers.

You can have up to 15 single-mode server groups or 4 multi-mode server groups. Each server group can have up to 16 servers in single mode or up to 4 servers in multi-mode.

When you enter a **aaa-server protocol** command, you enter group mode.

Step 2: For each AAA server on your network, follow these steps:

Identify the server, including the AAA server group it belongs to. To do so, enter the following command:

```
hostname(config)# aaa-server server_group (interface_name) host server_ip password
```

When you enter a **aaa-server host** command, you enter host mode.

After the aaa-server and group are configured, use the following commands to configure authentication at each administrative interface (serial, ASDM (http over TLS), and SSH), and require administrators to re-enter their own password when accessing a higher privilege level (up to their highest authorized privilege level).

```
hostname(config)# aaa authentication enable console {LOCAL | server_group [LOCAL]}
```

Require use of individual username and password to log into the serial console:

```
hostname(config)# aaa authentication serial console {LOCAL | server_group [LOCAL]}
```

By default, it would be possible to log into ASDM with a blank username and the enable password set by the **enable password** command. The secure configuration requires initial authentication using a username and password. Configure HTTP authentication, so no one can use ASDM with a blank username and the enable password.

```
hostname(config)# aaa authentication http console {LOCAL | server_group [LOCAL]}
```

The security appliance allows SSH connections to the security appliance for management purposes. The security appliance allows a maximum of 5 concurrent SSH connections per context, if available, with a maximum of 100 connections divided between all contexts. SSH sessions in the certified configuration must be authenticated using a single use password solution, and not the local password database.

```
hostname(config)# aaa authentication ssh console {LOCAL | server_group [LOCAL]}
```

Note: Enable authentication can use either the local user database or remote AAA server. Reusable passwords are permitted. SSH authentication must use remote AAA server configured for single use authentication. Use of the authentication method "none" is not permitted.

For information on configuring SSH, see the "Management Access" chapter of the *CLI Book 1* or *ASDM Book 1*, the "General Operations" guides.

Note: By default, SSH allows both version 1 and version 2; always select version 2. To specify the version number, enter the command **ssh version** version_number.

```
hostname(config)# ssh version 2
```

Note: For each address or subnet, identifies the IP addresses from which the ASA accepts connections, and the interface on which you can SSH.

```
hostname(config)# ssh source_IP_address mask source_interface
```

Note: Instead of entering the **enable** command at the ">" prompt after establishing the SSH session, the administrator shall enter "login" and then log in with a local database account and password. This results in all audit events being attributed to that local user.

Once it has been configured, logging in with remote access over SSH is done via a CLI command.

```
root@host:~# ssh username@device_ip
```

The user will then be prompted to enter the password to authenticate. A login over serial console connection will require similar credentials, but will not require a CLI command to be prompted.

Login via ASDM will first present a banner page, and then an authentication page. The user will be prompted for a username and password; once these credentials have been authenticated, the user will be allowed to access the device's GUI.

Login Banners

There are several configurable login banners on the ASA. The Common Criteria certified configuration requires that an advisory notice and consent warning message be displayed prior to establishment of the administrative user session.

During the CLI (console or SSH) login process, the "banner login" will be displayed prior to the end-user providing their password[1], so the "login banner" can provide the warning that entering a password indicates consent.

```
asa(config)# banner login This is the login banner.
asa(config)# banner login NOTICE:  If you do not consent to the xyz policies for this system,
asa(config)# banner login … do not enter a password in the command line interface (CLI).
asa(config)# banner login NOTICE: If you do not consent to the xyz policies for this system,
asa(config)# banner login … do not enter a password at the next ASDM login prompt.
asa(config)# banner login CLI Behavior: When connecting via CLI, this banner is displayed…
asa(config)# banner login … after a username is provided, but before the password is entered.
asa(config)# banner login ASDM Behavior… When connecting via ASDM, this banner is displayed
asa(config)# banner login … after the ASDM launcher prompts (but does not require) the end-user
```

[1] All login banners appear directly after the user logs in with their SSH private key via the CLI.

asa(config)# **banner login** … to enter a username and password, but before sending them to the ASA.

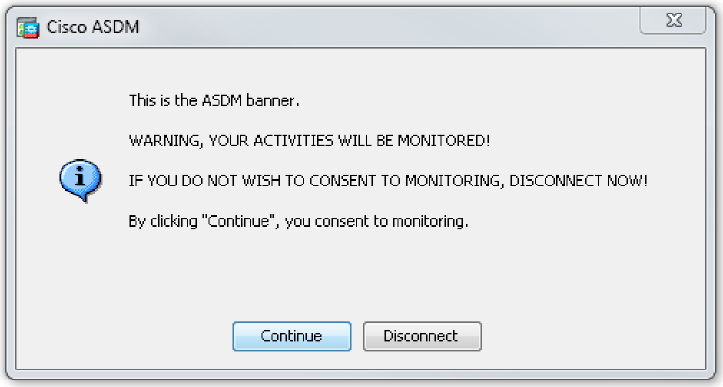
During the ASDM login and after the username and password have been provided, the authentication credentials are passed to the ASA. If the credentials are wrong, the user is prompted again for a username and password. If the credentials are validated, the ASDM banner is displayed, but the administrator user session has not been started. The administrative user session will not be established until the user clicks the "Continue" button. The ASDM banner window has a "Continue" button that can be used to express consent, and a "Disconnect" button to discontinue loading of ASDM and avoid establishing the interactive administrative user session. Here's an example of how to create an ASDM banner via the CLI:

asa(config)# **banner asdm** This is the ASDM banner.

asa(config)# **banner asdm** WARNING, YOUR ACTIVITIES WILL BE MONITORED!

asa(config)# **banner asdm** IF YOU DO NOT WISH TO CONSENT TO MONITORING, DISCONNECT NOW!

asa(config)# **banner asdm** By clicking "Continue", you consent to monitoring.



This is the ASDM banner.

WARNING, YOUR ACTIVITIES WILL BE MONITORED!

IF YOU DO NOT WISH TO CONSENT TO MONITORING, DISCONNECT NOW!

By clicking "Continue", you consent to monitoring.

Usernames, Privileges, and Administrative Roles

Usernames and Privileges

Usernames are defined on the certified configuration and are used to separate the defined roles into separate individuals. Use the **username** command to assign a password and a privilege level for a user. Privilege levels range from 0 (the lowest) through 15. System administrators generally have the highest privilege level.

username *name* {**nopassword** | **password** *password* [**encrypted**]} [**privilege** *priv_level*]}

In the following example, the username is testuser:

username testuser **password** 12RsxXQnphyr/I9Z **encrypted privilege** 15

When the certified configuration is operating in multiple context mode, usernames are constrained to the individual context where they were created.

For a complete description of the command syntax, see the "Management Access" chapter of the *CLI Book 1,* the "General Operations" guide.

Application Note: The administrator is also advised to never use the value "none" by itself for any authentication option. Use of the value "none" by itself removes the requirement for entering a password.

Authorized Administrator

An "authorized administrator" is any account with a privilege level of 1 or higher and with their service-type attribute set to "admin" (the default setting) is considered an "authorized administrator". When command authorization has been enabled the default sets of privileges take effect at certain levels, and the levels become customizable.

- When "aaa authorization command LOCAL" has NOT been applied to the config:
    - All usernames with level 2 and higher have the same full read-write access as if they had level 15 once their interactive session (CLI or ASDM) is effectively at level 2 or higher.
    - Usernames with privilege levels 1 and higher can login to the CLI, and "enable" to their max privilege level (the level assigned to their username).
    - Usernames with privilege levels 2-14 can login to ASDM, and have full read-write access.
    - Privilege levels cannot be customized.
- When "aaa authorization command LOCAL" has been applied to the config:
    - Default command authorizations for privilege levels 3 and 5 take effect, where level 3 provides "Monitor Only" privileges, levels 4 and higher inherit privileges from level 3, level 5 provides "Read Only" privileges (a superset of Monitor Only privileges), and levels 6-14 inherit privileges from level 5.
    - Privilege levels (including levels 3 and 5) can be customized from the default to add/remove specific privileges.
    - To display the set of privileges assigned to levels 3 or 5 (or any other privilege level), use "show running-config all privilege all", which shows all the default configuration settings that are not shown in the output of "show running-config all".

When creating a new user (such as via CLI with the "username" command), the privilege can be specified for the new account. If a privilege is not specified, the default privilege level (level 2) is applied to the new account. Privilege level 2 allows access via serial console, SSH, and ASDM. If command authorization is enabled, level 2 would not allow any additional command access above the defaults for level 1 unless specific commands had been explicitly authorized for level 2 using the following commands:

privilege [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **configure**}] **command** *command*

aaa authorization command LOCAL

Example:

```
hostname(config)# privilege level 2 command config

hostname(config)# privilege level 2 command logging

command filterhostname(config)# aaa authorization command LOCAL
```

Administrators who authenticate to the CLI (serial or SSH) have the 'current' privilege of their interactive session set to level 1, and can "enable" a higher privilege level (up to the privilege level set for their username) but entering the "enable" command and re-typing their individual password.

Passwords

The ASA is configured to authenticate the administrator for both unprivileged and privileged access to the CLI using a username and password. A RADIUS server or internal authentication server can be used to authenticate administrators. The ASA by default is configured to perform local authentication and stores user names and passwords in an internal user authentication database which is only accessible by the administrator via privileged commands.

Password Complexity, Length, and Uniqueness

In the certified configuration, the minimum password length must be set by an administrator to 8 characters or longer, and have some complexity requirements enforced. To set the minimum password length, refer to the guidance in the next section of this document.

The following is a list of characters can be used within passwords:

- 26 Upper case letters (A - Z)

- 26 Lower case letter (a – z)
- 10 Numbers (0 – 9)
- !"#$%&'()*+,-./:;<@[\`{|=>]^_}~

These are a total of 93 characters that may be used to construct a password. The use of the space character is prohibited.

The password guidance included in this section applies to creation and management of administrator passwords. Administrators must ensure that when creating or changing a password, the following requirements are met:

1. Passwords must:
   - be settable and can support 15 characters long (NOTE: no lower than 8 minimum!)
   - include mixed-case alphabetic characters
   - include at least 1 numeric character
   - include at least 1 special character
2. Passwords must not include:
   - birthdays
   - names (parents, family, spouse, pets, favorite sports player)
   - sports teams
   - towns, cities or countries

Password Policies

In order to set password policy for the current context, the "password-policy" command must be used. Note that the [no] form of each command shown below sets the corresponding password policy attribute to its default value.

```
[no] password-policy lifetime <0-65535>
[no] password-policy minimum-changes <0-127> ##  Recommended to be set to 4 or greater.
[no] password-policy minimum-length <3-127> ## Recommended to be set to 8 or greater.
[no] password-policy minimum-lowercase <0-127> ##  Recommended to be set to 1 or greater.
[no] password-policy minimum-numeric <0-127>  ##  Recommended to be set to 1 or greater.
[no] password-policy minimum-special <0-127>##  Recommended to be set to 1 or greater.
[no] password-policy minimum-uppercase <0-127>##  Recommended to be set to 1 or greater.
```

Lifetime sets the interval in days when passwords expire. The default lifetime is 0 and specifies that local user passwords never expire. Note that passwords expire at 12:00 AM of the day following lifetime exhaustion.

Minimum-changes sets the minimum number of characters that must be changed between new and old passwords. The system default for minimum-changes is 0, but the value should be set to 4 or greater to be consistent with the Common Criteria certified configuration.

Minimum-length sets the minimum length of passwords. The system default minimum-length is 3. If minimum-length is less than any of the other minimums (changes, lowercase, uppercase, numeric and special), an error message is displayed and minimum-length will not be changed.

Minimum-lowercase sets the minimum number of lowercase characters that passwords must contain. The default 0 means there is no minimum.

Minimum-numeric sets the minimum number of numeric characters that passwords must contain. The default 0 means there is no minimum.

Minimum-special sets the minimum number of special characters that password must contain. The default 0 means there is no minimum.

Minimum-uppercase sets the minimum number of uppercase characters that passwords must contain. The default 0 means there is no minimum.

Note: Password complexity settings, minimum password length, and requiring a minimum number of character changes from previous password are not enforced by the "username" command, nor by the ASDM equivalent (whenever an authenticated administrator is creating a new account or modifying the password for an existing administrator account). These password requirements are only enforced:

1. When an admin is forced to change his/her own password at login, such as when the password lifetime has expired.
2. When an admin initiates a change to his/her own password using the "change-password" command.

Note: When an administrator attempts to login remotely (via ASDM, SSH) after his/her password has expired (or the management session quota has been reached), an error message is displayed, an error syslog message is generated, and system access is denied. When a remote admin logs in to the system within 7 days of user password expiration, a warning message is displayed and system access is granted. Note that passwords expire at 12:00 AM of the day following lifetime exhaustion.

Warning: If an administrator's password expires, his/her account will not be able to login remotely (via SSH or ASDM). S/he will still be able to login via the local serial console to reset his/her own password, or another administrator can reset their password for them, or another administrator can reset their password expiration using the command syntax, **username** *<username>* **password-date** *<mmm dd yyyy>*.

Note: The console session is never blocked by password expiration in order to prevent system lock-out.

Note: For ASA, some account management commands have been added or modified.

- A **change-password** command has been added to enable the user to change his password after authenticating.
- The **clear config username** command no longer allows users delete their own account.
- The **username** command no longer allows users to change their own password or delete their own account.
- The **username** command syntax has been augmented to accommodate password creation date. When running config is saved, two username commands are written to the configuration file for each user. The first is exactly like the username command in previous releases, specifying the username, password, password-type and privilege level. The second contains just the username and password creation date.
    - The format of this username command is:
        - username <username> password-date <mmm dd yyyy>
    - where:

<username>	user's name
<mmm>	abbreviated month name (Jan, Feb, Mar,…)
<dd>	day of month
<yyyy>	year in range 1993-2035

Setting the Clock

The ASA clock cannot be updated directly through any of the ASA interfaces. This is different functionality than other ASA platforms. To update the ASA clock, update the FXOS clock using the "set clock" command at the FXOS CLI console, or configure FXOS to synchronize its clock with an external NTP source. The ASA clock will be automatically updated via NTP across an internal network that exists only between the FXOS and ASA, and is not externally accessible.

The ASA clock is automatically synchronized to the FXOS clock. The ASA clock cannot be set directly on ASA, and the ASA clock update interval is not configurable. For instructions to configure the FXOS clock, refer to, "*Cisco FXOS 2.14 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration*."

When the ASA clock is synchronized with the FXOS clock, an audit message will be generated by ASA. The log message shows the old and new times, and indicates that the clock was updated by FXOS (source: Chassis), with the source IP address being an internal IP address on an isolated internal subnet that only exists within backplane of the Firepower chassis. Example:

```
%ASA-5-771002: CLOCK: System clock set, source: Chassis SSPXRU, IP: 127.128.254.1, before: 04:05:36.499 EDT Sun May 20
2018, after: 04:05:36.000 EDT Sun May 20 2018
```

Account Lockout after Failed Login Attempts

To be in the certified configuration, the ASA must be configured to lock local accounts after a configurable non-zero number of consecutive failed login attempts. The ASA can be configured to enforce that requirement on all interfaces (including the local serial console) by using the methods described below, but caution should be used when applying these configurations to the local serial console interface to avoid a situation in which all local admin accounts become locked.

Tip: The number of failed attempts resets to zero and the lockout status resets to 0 when the user successfully authenticates or when the ASA reboots.

To limit the number of consecutive failed local login attempts that the ASA allows any given user account (with the exception of users with a privilege level of 15; this feature does not affect level 15 users), use the "**aaa local authentication attempts max-fail"** command in global configuration mode. To enforce the ability to lockout any local account after consecutive failed logins, ensure that no privilege level 15 accounts exist in the local user database. By enabling local command authorization, commands that are normally reserved for level 15 users can be associated with lower privilege levels.

In a configuration where no privilege level 15 accounts exist in the local user database, it's still possible to login to any admin interface (serial, SSH, or ASDM) using an account that has privilege level 15 if that account is authenticated to a remote AAA server. In such cases, it would be expected that the remote AAA server would enforce locking of accounts after successive failed login attempts.

If the serial console authentication is configured to authenticate first to the LOCAL user database, then to a remote AAA server an administrator could login to the CLI using a local user account, then access privilege level 15 commands. Using the "login" command when already logged in allows an authenticated administrator to login using another username in the local user database, or a level 15 account that does not exist in the local user database but does exist on the remote AAA server.

Tip: By using the "login" command instead of the "enable" command to access privilege level 15, audit records will continue to identify the administrator by their individual username instead of as "enable_15."

Tip: To allow access to level 15 commands when the remote AAA server is unavailable, create an enable password that is only shared with essential personnel, and only used in maintenance periods when it's understood that the ASA will not be logging the administrator's username to the audit messages.

Note: Using the "service-type" attribute on a local user account is not sufficient to protect against repeated failed login attempts to a local account with privilege level 15. Setting the service-type attribute for any account to "remote-access" will restrict the account so it's only able to login via VPN (remote-access), or the serial console, but the account would not be able to authenticate using SSH or ASDM.

The "**aaa local authentication attempts max-fail**" command only affects authentication with the local user database. To disable this feature and allow an unlimited number of consecutive failed local login attempts, use the **no** form of this command.

```
aaa local authentication attempts max-fail number
```

number = The maximum number of times a user can enter a wrong password before being locked out. This number can be in the range 1-16.

Related Commands:

- **clear aaa local user lockout:** Clears the lockout status of the specified users and set their failed-attempts counter to 0.
- **clear aaa local user fail-attempts:** Resets the number of failed user authentication attempts to zero without modifying the user locked-out status.
- **show aaa local user:** Shows the list of usernames that are currently locked.

Secure Communications

Evaluated Cryptography

The Common Criteria certification evaluated the following cryptographic functionality, all of which must be configured as described in this guide:

- The TOE should be operating in FIPS mode.
  - When in FIPS mode, the TOE does not require explicit configuration to allow use of cryptographic signature services, nor explicit configuration for use of RNG functionality. Cryptographic capabilities will be limited to those which are FIPS compliant.
- SSHv2 must be used instead of SSHv1 with ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521 as the only public key algorithms used for authentication implementation. All other algorithms need to be rejected.
- CiscoSSH needs to be disabled, so the TOE can use the native ASA SSH stack.
- TLS must be used instead of SSL, with certain ciphersuites enabled as described in this document.
- IPsec must be used to secure connections to AAA servers and may be used to secure other traffic that originates from the ASA, or terminates at the ASA, but the certified configuration is not approved for using IPsec to secure traffic flows through the ASA.
  - IKEv2 must be used instead of IKEv1 and must be configured as described in this document.
  - ESP must be used as described in this document.

The Common Criteria certification did not evaluate any of the cryptographic functionality:

- MD5 may be used, such as in authentication of routing protocols, and NTP.
- RADIUS or TACACS+ may be used, but only when tunneled in IPsec.
- AH may be used in IPsec, but use of ESP is mandatory.
- Any other cryptographic functions not listed above as evaluated.

Enable FIPS Mode

To enable, use the "fips enable" command, then reload the ASA.

```
hostname# configuration terminal
```

```
hostname(config)# fips enable
hostname(config)# end
hostname# write memory
hostname# reload
```

Configuring SSH [Optional]

All inbound SSH sessions for remote administration of the ASA may be tunneled through IPsec. To ensure all inbound SSH is tunneled, ensure the ACL that's associated with the crypto map includes the range(s) of IP addresses listed in the "**ssh** *ip-address netmask interface*" command, which might be:

```
hostname(config)# ssh 192.168.1.0 255.255.255.0 management
```

For example, if the local ASA interface to which SSH should be allowed is the management interface, and the IP address on the management interface is 192.168.1.1, include this entry in the access-list that's mapped to crypto map that's applied to the management interface:

```
hostname(config)# access-list access-list-name extended permit tcp 192.168.1.0 255.255.255.0 host 192.168.1.1
```

If desired, that access-list entry can be limited to inbound SSH traffic (on TCP port 22):

```
hostname(config)# access-list access-list-name extended permit tcp 192.168.1.0 255.255.255.0 host 192.168.1.1 eq ssh
```

Associate that access-list with the appropriate crypto map:

```
hostname(config)# crypto map map-name seq-num match address access-list-name
```

Apply that crypto map to the management interface:

```
hostname(config)# crypto map map-name interface interface-name
```

ECDSA Key Generation

Generate an ECDSA key pair using the "crypto key generate" command. ASA supports ECDSA curves of 256, 384 and 521 bits.

Syntax: crypto key generate ecdsa ***ecdsa [label name | elliptic-curve [256 | 384 | 521]***

Example:

```
asa(config)# crypto key generate ecdsa elliptic-curve ?

configure mode commands/options:
256 256 bits
384 384 bits
521 521 bits
asa(config)# crypto key generate ecdsa elliptic-curve 384 ?

configure mode commands/options:
noconfirm Specify this keyword to suppress all interactive prompting.
<cr>
asa(config)# crypto key generate ecdsa elliptic-curve 384

ECDSA keypair generation process begin. Please wait...
The ECDSA keypairs were successfully generated.
```

To zeroize the key set, use the following command:

```
crypto key zeroize [rsa | ecdsa] [default | label <name> | noconfirm]
```

Note (relevant to Common Criteria certification): There are no configurations or circumstances that do not strictly conform to the key destruction requirement (FCS_CKM.4) as described in the Security Target.

CSfC Alignment

To operate the TOE in alignment with the CSfC selections for the IPsec VPN Gateways, only NIST curve 384 needs to be used for the TOE operation in CC mode.

Restrict SSH Connections

For each address or subnet, identifies the IP addresses from which the ASA accepts connections, and the interface on which you can SSH.

Syntax: **ssh** *source_IP_address mask source_interface*

Enable SSHv2 and Disable SSHv1

Using the “ssh version” command will enable one version and disable the other. By default, both versions are enabled (“no ssh version”).

Syntax: **ssh version** {~~1 |~~ **2**}

Example: hostname(config)# **ssh version 2**

When SSH version 2 and FIPS mode (‘fips enable’) are enabled, the following security algorithms and ciphers are supported on the ASA though some of these must be restricted in CC-certified configuration by following the guidance in the subsequent sections:

- AES ciphers for data encryption
- HMAC-SHA1 and HMAC-SHA2-256 algorithms for packet integrity
- Diffie-Hellman Group 14 algorithms for key exchange.
- RSA public key algorithm for host authentication

When FIPS mode is enabled, the number of supported algorithms will be reduced to only the FIPS and CC Approved algorithms (AES128-CBC, AES256-CBC, HMAC-SHA1, HMAC-SHA2-256).

The following SSH Version 2 features are not supported on the ASA:

- X11 forwarding
- Port forwarding
- SFTP support
- Kerberos and AFS ticket passing
- Data compression

Encryption Algorithms

When SSH version 2 is enabled the ASA will support AES-CBC-128, and AES-CBC-256, both of which are permitted in the certified configuration when FIPS mode is enabled. The ASA will disconnect any attempt to open a SSH session with 3DES-CBC.

To ensure only approved ciphers are used, add the following command to the ASA configuration:

```
hostname(config)# ssh cipher encryption fips
```

To verify the proper encryption algorithms are used for established connections, use the “show ssh sessions” command:

```
hostname# show ssh sessions
SID Client IP     Version Mode Encryption Hmac State          Username
0   172.69.39.39  1.99    IN   aes128-cbc sha1  SessionStarted pat
```

```
            OUT  aes128-cbc sha1  SessionStarted pat
```

Hashing Algorithms

When SSH version 2 is enabled the hashing algorithms supported by the ASA for data integrity are hmac-sha1, hmac-sha1-96, hmac-md5, and hmac-md5-96. When FIPS mode is enabled, only hmac-sha1 and hmac-sha1-256 are enabled, after adding the following command to the configuration:

Syntax:

ssh cipher integrity [~~all | custom |~~ fips ~~| high | low | medium~~**]**

Example:

hostname(config)# **ssh cipher integrity fips**

Key-Exchange

Require SSH key-exchange to use Diffie-Hellman Group 14, and not allow DH Group 1.

Syntax: **ssh key-exchange group** {~~*dh-group1-sha1* |~~ *dh-group14-sha1*}

Example:

hostname(config)# **ssh key-exchange group dh-group14-sha1**

Note: When the ASA is in FIPS mode (when the running-config contains “FIPS enable”), dh-group14-sha1 will remain enabled and cannot be disabled, and attempting to disable Group 14 will display a warning:

```
hostname(config)# no ssh key-exchange
warning: fips is enabled.
    Cannot change ssh key-exchange group to dh-group1-sha1
hostname(config)#
```

CSfC Alignment

To operate the TOE in alignment with the CSfC selections for the IPsec VPN Gateways, only ecdh-sha2-nistp256 and ecdh-sha2-nistp384 need to be used as the key exchange methods for the TOE operation in CC mode.

SSH Session Rekey Limits

The SSH session rekey limits are not configurable. SSH sessions will renew their keys within 60 minutes and 1GB of traffic, whichever limit is reached first. To display the counters for active SSH sessions, use “show ssh sessions detail”:

```
asa# show ssh sessions detail
SSH Session ID         : 0
 Client IP             : 192.0.0.192
 Username              : admin123
 SSH Version           : 2.0
 State                 : SessionStarted
 Inbound Statistics
  Encryption           : aes256-cbc
  HMAC                 : sha1
  Bytes Received       : 13068
 Outbound Statistics
  Encryption           : aes256-cbc
  HMAC                 : sha1
  Bytes Transmitted    : 14216
```

```
Rekey Information
 Time Remaining (sec)  : 2449
 Data Remaining (bytes): 996132984
 Last Rekey           : 15:40:42.224 EST Fri Feb 2 2018
 Data-Based Rekeys     : 0
 Time-Based Rekeys     : 0
```

Authentication

Password-Based Authentication

To configure password-based authentication for a username, specify the password with the username command.

hostname(config)# **username** {*username*} **password** {password}

Key-Based Authentication

To enable public key authentication on a per-user basis, use the "**ssh authentication**" command in username attributes mode. To disable public key authentication on a per-user basis, use the **no** form of this command.

hostname(config)# **username** {*username*} **attributes**

hostname(config-username)# **ssh authentication** {**pkf** | **publickey** [**nointeractive**] *key* [**hashed**]}

Example:

```
hostname(config-username)# ssh authenticate pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
hostname(config-username)#
```

You can specify a public key file formatted key (**pkf** keyword) or a Based64-encoded key (**publickey** keyword). For a **publickey**, you can generate the key using any SSH key generation software (such as ssh keygen) that can generate ecdsa-sha2-nistp keys.

The public key algorithms used in the Common Criteria evaluated configuration are - ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521.

Idle Timeouts

Configure an idle timeout for SSH connections to specify the duration in minutes that an SSH session can remain inactive before being disconnected.

Syntax: **ssh timeout** *minutes*

Syntax: **console timeout** *minutes*

Valid values are from 0 to 60 minutes, with a value of 0 minutes meaning the session will not time out.
For the CC-certified configuration, these timeouts must be set to non-zero values.
Example: **ssh timeout** *10*

SCopy (disabled by default)

The ASA contains a server implementation of SCopy (secure copy over SSH) to allow inbound connection using SCP to upload/download files from the local file system.

This SCP server implementation does not support login banners, and therefore must remain disabled in the certified configuration. If it is enabled by accident, use this command to disable it.

Example: hostname(config)# **no ssh scopy enable**

Configuring TLS

By default, only TLSv1.1 and 1.2 are enabled. The “ssl client-version” command specifies the TLS protocol version the ASA uses when acting as a client. The “ssl server-version” command specifies the minimum protocol version for which the ASA will negotiate a TLS connection. In the CC evaluated configuration, these commands are used to enable only TLSv1.2.

The syntax is: ssl client-version [~~*tlsv1 | tlsv1.1*~~ | *tlsv1.2*]

ssl server-version [~~*tlsv1 | tlsv1.1*~~ | *tlsv1.2*]

In addition, only Diffie-Hellman Group 14 (2048 bits) and Diffie-Hellman Group 15 (3072 bits) should be supported for TLS when FIPS mode is enabled.

The syntax is: ssl dh-group [*group14 | group15*]

The key agreement parameters of the server key exchange message are specified in the RFC 5246 (section 7.4.3) for TLSv1.2. The TOE conforms to both RFCs supporting DH 2048 bits, DH 3072 bits and NIST ECC curves secp256r1, secp384r1, secp521r1.

CSfC Alignment

To operate the TOE in alignment with the CSfC selections for the IPsec VPN Gateways, only TLS 1.2 needs to be enabled for the TOE operation in CC mode.

```
ssl server-version tlsv1.2

ssl client-version tlsv1.2
```

Specify the TLS Version

The configuration must be TLSv1.2:

hostname(config)# [no] **ssl server-max-version [tlsv1.2 |** tlsv1.3**]**

hostname(config)# [no] **ssl client-max-version [tlsv1.2 |** tlsv1.3**]**

Specify the TLS Ciphersuites (optional)

The ASA can be configured to restrict which TLS ciphersuites will be used by its TLS server (and client). In the certified configuration, the list of negotiated ciphersuites should be limited using the ssl cipher command and selecting one or more of these ciphersuites:

- DHE-RSA-AES128-SHA (TLS_DHE_RSA_WITH_AES_128_CBC_SHA)
- DHE-RSA-AES256-SHA (TLS_DHE_RSA_WITH_AES_256_CBC_SHA)

- DHE-RSA-AES128-SHA256 (TLS_DHE_RSA_WITH_AES_128_CBC_SHA256)
- DHE-RSA-AES256-SHA256 (TLS_DHE_RSA_WITH_AES_256_CBC_SHA256)
- ECDHE-ECDSA-AES128-GCM-SHA256 (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256)
- ECDHE-ECDSA-AES256-GCM-SHA384 (TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384)

Note: TLSv1.2 supports all the ciphersuites listed.

The “ssl cipher” command can be used to define the set of encryption algorithms that the ASA will allow to be negotiated for TLS sessions. This command defines the algorithms that will be allowed for both the ASA’s TLS client and the ASA’s TLS server:

Syntax: **ssl cipher** *version* [*level* | **custom** *“string”*]

The v*ersion* must be “tlsv1.2”.

The *level* must be “high” (for tlsv1.2). The “high” includes only AES-256 with SHA-2 ciphers.

The **custom** *“string”* keyword-argument pair allows you to have full control of the cipher suite using OpenSSL cipher definition strings. This is the recommended setting to select only the ciphersuites you want to support for TLS.

Example:

```
hostname(config)# ssl cipher tlsv1.2 custom "ECDHE-ECDSA-AES256-GCM-SHA384"
```

CSfC Alignment

To operate the TOE in alignment with the CSfC selections for the IPsec VPN Gateways, restrict the TLS ciphers to only the ECDHE-ECDSA-AES256-GCM-SHA384 (TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384) ciphersuite.

Specify the TLS Server and Client Certificates

The certificate is configured by the “ssl trust-point” command specifying the certificate and interface. If the server requests a client certificate from the ASA for authentication, the ASA will send whatever client identity certificate is configured for that interface. Follow the instructions in this document in section *Create Trustpoint and Generate Certificate Signing Request (CSR)* to create a trustpoint and import a device/client certificate into that trustpoint. Then use the command below to map the TLS connection to that trustpoint and interface

Example:

```
hostname(config)# ssl trust-point myCA inside
```

Configuring IPsec

IPsec peer-to-peer tunnels or IPsec VPN client tunnels can be used between the ASA and a remote host for transmission of any of the following:

- Syslog (UDP or TCP) from the ASA to an audit server
- RADIUS from the ASA to a remote authentication server
- VPN Client connections to the ASA for remote administration (using SSH or ASDM) or remote network access.

Tunnel mode is the usual way to implement IPsec between two ASAs that are connected over an untrusted network, such as the public Internet. Tunnel mode is the default and requires no configuration.

The following commands show which options are allowed to be used in the certified configuration, and the options that have strikethrough (~~strikethrough~~) are prohibited from use.

Note: IKEv1 is not approved for use in the Common Criteria certified configuration because it doesn't support Diffie-Hellman Group 14.

Managing Public Key Infrastructure (PKI) Keys

The key generation is invoked via the **crypto key generate** command below. You can specify the type of key (RSA vs. ECDSA) and key sizes. Public and private keys are stored in proprietary format at specific location, such as NVRAM and flash memory. If configuring a cryptography map to use RSA or ECDSA trustpoint for authentication, the administrator must first generate the key set. To generate the key set, use the following command:

crypto key generate [rsa [general-keys | label <name> | modules [~~512 | 768 | 1024 |~~ 2048] | noconfirm | usage-keys] | ecdsa [label <name> | elliptic-curve [256 | 384 | 521] | noconfirm]]

To display the key output set, use the following command:

show crypto key mypubkey [rsa | ecdsa]

To zeroize the key set, use the following command:

crypto key zeroize [rsa | ecdsa] [default | label <name> | noconfirm]

Note (relevant to Common Criteria certification): There are no configurations or circumstances that do not strictly conform to the key destruction requirement (FCS_CKM.4) as described in the Security Target.

Enable IKEv2

Enable IKEv2, though enabling "client services" is irrelevant since that enables services for VPN clients. Client services include enhanced AnyConnect Secure Mobility client features including software updates, client profiles, GUI localization (translation) and customization, Cisco Secure Desktop, and SCEP proxy.

hostname(config)# **crypto ikev2 enable** *interface-name* [~~client-services~~ [**port** *port*]]

NAT traversal for ESP packets to pass through one or more NAT devices, is enabled by default.

Only main mode can be used for IKEv2 Phase 1 (SA) when initiating a connection.

Specify the ISAKMP identity method. Select "auto" to automatically determine based on connection type: IP address for preshared key and Cert DN for certificate-based connections.

Syntax: crypto isakmp identity auto

Post Quantum Preshared Key (PPK) Configuration

Post Quantum Preshared Keys (PPKs) are included in the IKEv2 key material to make the exchange secure from quantum attacks. The following commands are used to configure Post Quantum Preshared Key (PPK) in compliance with RFC 8784.

```
tunnel-group 1.1.1.1 type ipsec-l2l
tunnel-group 1.1.1.1 general-attributes
  default-group-policy  GroupPolicy5
tunnel-group 1.1.1.1 ipsec-attributes
  ikev2 remote-authentication post-quantum-key ********** identity myPPK2 mandatory
```

remote-authentication: specifies the PPK that will be used with the tunnel-group peer *post-quantum-key*: specifies a PPK is to follow instead of a pre-shared-key

<key>: The 256 bit PPK as a 64 character hex string

Identity <identifier>: specifies the PPK_ID to be associated with the PPK<id>: The PPK_ID to use as a string

Mandatory Flag: Configures the PPK as mandatory for the connection. This can be added after the *identifier*. Adding this flag marks adding the PPK as mandatory.

IKEv2 Parameters for IKE Phase 1 (the IKE SA)

IKEv2 Policies

The Security Policy Database and Security Association Database (SAD) are internal databases consisting of policies created in "IKEv2 Parameters for IKE Phase 1 (the IKE SA)" and "IKEv2 Parameters for IKE Phase 2 (the IPsec SA)", respectively. The policy entries in SPD are ordered by priority, and the first matched policy will be used to process the traffic.

The following commands show which options are allowed to be used in the certified configuration, and the options that have strikethrough (~~strikethrough~~) are prohibited from use.

hostname(config)# **crypto ikev2 policy** *priority*

hostname(config-ikev2-policy)# **encryption** [~~null | des | 3des |~~ **aes |** **~~aes-192~~**[2] **| aes-256 | aes-gcm |** **~~aes-gcm-192~~** **| aes-gcm-256**]

hostname(config-ikev2-policy)# **integrity [**~~md5 |~~ **sha | sha256 | sha384 | sha512]**

hostname(config-ikev2-policy)# **group** [~~1 | 2 | 5~~ **| 14 | 19 | 20** ~~| 21~~ **| ~~24~~**]

hostname(config-ikev2-policy)# **prf [**~~md5 |~~ **sha | sha256 |** ~~sha384 |~~ **sha512]**

IKE SA Lifetime Limits

Configuring lifetime limits is optional but recommended. Lifetime limits for IKE Phase 1 SAs can be configured in seconds. The valid range is from 120 to 2,147,483,647 seconds. The default is 86,400 seconds (24 hours). It is recommended to choose a lifetime value below 86100 seconds since the actual rekey time may be 1-3 minutes longer than the configured time.

hostname(config-ikev2-policy)# **lifetime seconds** *seconds*

IKEv2 Parameters for IKE Phase 2 (the IPsec SA)

IPsec Proposals

To create an IKEv2 proposal, use the **crypto ipsec ikev2 ipsec-proposal** command in global configuration mode. To remove the proposal, use the **no** form of this command.

hostname(config)# crypto ipsec ikev2 ipsec-proposal *proposal_name*

hostname(config-ipsec-proposal)# **protocol esp encryption [~~3des |~~ aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 ~~| aes-gmac | aes-gmac-192 | aes-gmac-256 | des | null~~]**

hostname(config-ipsec-proposal)# **protocol esp integrity [~~md5 |~~ sha-1 | sha-256 | sha-384 | sha-512 | null]**

[2] ASA supports AES-192 CBC and GCM but AES-192* was not an option in the VPN Gateway Extended Package. Therefore, the use of AES-128* or AES-256* is recommended over AES-192*.

Note: When AES-GCM is specified as the encryption algorithm, an administrator can choose null as the IKEv2 integrity algorithm.

Note: The ASA has a configuration option to deny tunnel if the phase 1 SA is weaker than the phase 2. The crypto strength check is configured via the crypto ipsec ikev2 sa-strength-enforcement command.

To associate one or more ipsec-proposals with a crypto map, use the "**crypto map … set ikev2 ipsec-proposal**" command.

Syntax: hostname(config)# **crypto map** *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1* [… *proposal-name11*]

Example: hostname(config)# **crypto map** map2 10 **set ikev2 ipsec-proposal** 128aes-sha 256aes-sha

IPsec SA Lifetime Limits

Setting lifetime limits for IKE and IPsec security associations (SAs) is optional in the certified configuration. If setting lifetime in seconds and in kilobytes, enter both values with the same command, otherwise the second command will overwrite the first command.

The valid range in seconds is 120-2147483647 (2 min to 68 years)

The valid range in kilobytes is 10-2147483647 (10KB to 2TB)

To set the values globally, use the "crypto ipsec" form of the command:

hostname(config)# **crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

To override global values for a specific crypto map, use the "crypto map" form of the command:

hostname(config)# **crypto map** *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

Create an Access-List and Assigning to Crypto Map

Create an access-list to define the traffic to be encrypted/decrypted, and create a crypto map that references that access-list, and defines the rest of the IPsec SA parameters. If the traffic matches any of the permit ACLs, the traffic will be protected using IPsec. If the traffic matches any of the deny ACLs, the traffic will be bypassed and be subjected to the interface ACLs. If the traffic matches none of the interface ACLs, it will be dropped.

Assign an ACL[3] to a crypto map:

hostname(config)# **access-list** *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask log*

Example:
hostname(config)# **access-list Protect permit ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 log**
hostname(config)# **access-list Bypass deny ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 log**

hostname(config)# **crypto map** *map-name seq-num* **match address** *access-list-name*[4]

Specify the peer to which the IPsec-protected traffic can be forwarded:

hostname(config)# **crypto map** *map-name seq-num* **set peer** *ip-address/hostname*

Specify which SA proposal and lifetime that will be used for the connection, if not done already.

hostname(config)# **crypto map** *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1* [… *proposal-name11*]

[3] If this is a permit ACL, the traffic matching this ACL will be protected (i.e., encrypted with IPsec or PROTECT). If this is a deny ACL, the traffic matching this ACL will be bypassed and subject to the interface ACLs (no encryption or BYPASS). If there are no interface ACL matching the traffic, it will be dropped (i.e., DISCARD).

[4] By default, the ASA lets IPsec packets bypass interface ACLs. To apply interface ACLs to IPsec traffic, use: `no sysopt connection permit-vpn` command.

```
hostname(config)# crypto map map-name seq-num set security-association lifetime {seconds seconds | kilobytes kilobytes}
```

To specify the trustpoint that identifies the certificate to send for authentication during Phase 1 negotiations for the crypto map entry, use the **crypto map set trustpoint** command in global configuration mode. To remove a trustpoint from a crypto map entry, use the **no** form of this command.

```
hostname(config)# crypto map map-name seq-num set trustpoint trustpoint-name [chain]
```

Apply a Crypto Map set to an interface for evaluating IPsec traffic:

```
hostname(config)# crypto map map-name interface interface-name
```

Select Tunnel or Transport mode

To select mode for the IPsec channel using the following command:

```
hostname(config)# crypto map map_name sequence_number set ikev2 mode [tunnel | transport | transport-require]
```

tunnel Encapsulation mode will be tunnel mode

transport Encapsulation mode will be transport mode with option to fallback on tunnel mode, if the peer does not support it

transport-require Encapsulation mode will be transport mode only

Default will be tunnel mode.

Certificate Map Subject DN

Note: Use **crypto ca certificate map** to define certificate matching rules for IPsec tunnels. Use **crypto ca reference-identity** to define certificate matching rules for TLS connections.

To indicate that rule entry is applied to the subject DN of the IPsec peer certificate, use the **subject-name** command in **crypto ca certificate map** configuration mode. To remove a subject-name, use the **no** form of the command.

```
subject-name [ attr tag eq | ne |co | nc string ]
```

```
no subject-name [ attr tag eq | ne |co | nc string ]
```

attr *tag*	Indicates that only the specified attribute value from the certificate DN will be compared to the rule entry string. The tag values are as follows:
	DNQ = DN qualifier
	GENQ = Generational qualifier
	I = Initials
	GN = Given name
	N = Name
	SN = Surname
	IP = IP address
	SER = Serial number
	UNAME = Unstructured name
	EA = Email address
	T = Title
	O = Organization Name
	L = Locality
	SP = State/Province
	C = Country
	OU = Organizational unit
	CN = Common name

co	Specifies that the rule entry string must be a substring in the DN string or indicated attribute.
eq	Specifies that the DN string or indicated attribute must match the entire rule string.
nc	Specifies that the rule entry string must not be a substring in theDN string or indicated attribute.
ne	Specifies that the DN string or indicated attribute must not match the entire rule string.
string	Specifies the value to be matched.

For example:

```
hostname(config)# crypto ca certificate map test-map 1
hostname(config-ca-cert-map)# subject-name attr cn eq mycert
```

Once a certificate map has been created, associate the certificate map with an IPsec tunnel-group using the “tunnel-group-map” command, for example:

```
hostname(config)# tunnel-group-map test-map 10 tunnel-group-name
```

Viewing an IPsec Configuration

The following commands can be used to view information about IPsec connections:

Command	**Purpose**
show running-configuration crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.
show running-config crypto ipsec	Displays the complete IPsec configuration.
show running-config crypto isakmp	Displays the complete ISAKMP configuration.
show running-config crypto map	Displays the complete crypto map configuration.
show crypto ikev2 sa detail	Shows the Suite B algorithm support in the Encryption statistics.
show crypto ipsec sa	Shows the Suite B algorithm support and the ESP IPsec output.

Clearing Security Associations

Certain configuration changes take effect only during the negotiation of subsequent SAs. If you want the new settings to take effect immediately, clear the existing SAs to reestablish them with the changed configuration. The following commands can be used to clear and reinitialize IPsec SAs:

Command	**Purpose**
clear configure crypto	Removes an entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.
clear configure crypto ca trustpoint	Removes all trustpoints.

clear configure crypto map	Removes all crypto maps. Includes keywords that let you remove specific crypto maps.
clear configure crypto isakmp	Removes the entire ISAKMP configuration.
clear configure crypto isakmp policy	Removes all ISAKMP policies or a specific policy.
clear crypto isakmp sa	Removes the entire ISAKMP SA database.

If the IPsec connection is broken, the user will need to perform the following steps for recovery:

- Check the networking cables and settings.
- Make sure the network cards are in good status.
- Re-establish the connection for the IPsec connection.

IPsec Authentication

Authentication can be performed using pre-shared keys, or X.509v3 certificates.

Using Pre-Shared Keys

Authentication for IPsec tunnels can use pre-shared keys or certificates. If using preshared keys, enter a key that is complex/strong, using characters from all available character sets (lower-case, upper-case, numeric, and special/punctuation), and at least 22 characters long (lengths up to 128 characters are supported). The pre-shared keys must be entered by an administrator, and it is the administrator's responsibility to ensure the keys are sufficiently complex; the ASA does not generate pre-shared keys.

The administrator needs to configure the default connection profile (tunnel group), DefaultL2Lgroup, to specify the pre-shared key authentication method.

Example:

```
hostname(config)# tunnel-group DefaultL2Lgroup[5] type ipsec-l2l
hostname(config)# tunnel-group DefaultL2Lgroup ipsec-attributes
hostname(config-tunnel-ipsec)#

tunnel-group-ipsec mode commands/options:
 certificate    Allow certificate authentication from remote peer
 pre-shared-key  Allow pre-shared-key authentication from remote peer
hostname(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key ?

tunnel-group-ipsec mode commands/options:
 0          Specifies an UNENCRYPTED password will follow
 8          Specifies an ENCRYPTED password will follow
 WORD < 129 char  Enter an alphanumeric string between 1-128 characters
 hex         Configure a hex pre-shared-key
```

[5] To streamline the configuration task, the security appliance provides a default LAN-to-LAN tunnel group (DefaultL2Lgroup), a default remote access tunnel group (DefaultRAgroup), and a default group policy (DfltGrpPolicy). Otherwise, the IP address of the peer should be used.

```
hostname(config-tunnel-ipsec)# $ ikev2 remote-authentication pre-shared-key hex ?

tunnel-group-ipsec mode commands/options:
  Hex-string  Enter a hex pre-shared-key between 2-256 even number of
              characters
```

Note: The pre-shared-key type indicates what format of the pre-shared key is being entered at the CLI. Type 8 indicates the key being entered is in encrypted format. Type 8 cannot be combined with the ‘hex’ keyword as the two options are mutually exclusive. Type 0 is the default and means that the pre-shared-key being entered at the CLI is in plaintext format. The text-based pre-shared key will be processed by the "prf” or pseudo-random function configured by the administrator.

Using X.509v3 Digital Certificates

ASA supports X.509v3 certificates as defined by RFC 5280 for use in authentication of a network peer using IPsec and TLS. Public key infrastructure (PKI) credentials, such as private keys and certificates are stored in a specific location, such as NVRAM and flash memory. The identification and authentication, and authorization security functions protect an unauthorized user from gaining access to the storage. The TOE supports RSA and ECDSA certificates. The ECDSA certificates use NIST curve sizes P-256, P-384, and P-521.

Digital certificates provide digital identification for authentication. A digital certificate includes information that identifies a device or user, such as the common name, serial number, company, department, state, country, or IP address. CAs are trusted authorities that “sign” certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs issue digital certificates in the context of a PKI, which uses public-key or private-key encryption to ensure security.

For authentication using digital certificates, at least one identity certificate and its issuing CA certificate must exist on an ASA. This configuration allows multiple identities, roots, and certificate hierarchies. The ASA evaluates third-party certificates against CRLs, also called authority revocation lists, all the way from the identity certificate up the chain of subordinate certificate authorities.

Descriptions of several different types of available digital certificates follow:

- A CA certificate is used to sign other certificates. It is self-signed and called a root certificate. A certificate that is issued by another CA certificate is called a subordinate certificate.
- CAs also issue identity certificates, which are certificates for specific systems or hosts.

An identity certificate also contains information indicating the intended use of the certificate. That is, an identity certificate intended to authenticate a TLS server or TLS client will contain a “ServerAuth” or “ClientAuth” Extended key Usage (EKU), while one intended for use by peers in an IPsec VPN would contain an “IPsec Tunnel” EKU. The identity certificate presented by an OCSP responder when returning revocation status for a certificate must contain the OCSPsigning EKU. The The identity certificate presented by CRL provider when returning a CRL must contain the CRLsign Key Usage (KU). ASA does not enforce any other EKU.

Network peers in the operational environment to which the ASA will connect using TLS or IPsec, must be configured to present a valid x509v3 identity certificate issued by a PKI trusted by the ASA. For example, if audit transfer is protected by TLS, then the TLS connection offered by the audit server must provide a valid x509v3 identity certificate.

The ASA CA integrates an independent certificate authority feature on the ASA, deploys certificates, and provides secure revocation checking of issued certificates. The ASA CA provides a secure, configurable, in-house authority for certificate authentication with user enrollment through a website login page.

When a certificate is issued, it is valid for a fixed period of time. Sometimes a CA revokes a certificate before this time period expires; for example, because of security concerns or a change of name or association. CAs periodically issue a signed list of revoked certificates. Enabling revocation checking forces the ASA to check that the CA has not revoked a certificate each time that it uses the certificate for authentication.

When the administrator enables revocation checking, the ASA checks certificate revocation status during the PKI certificate validation process[6], which can use either CRL checking, OCSP, or both. OCSP is only used when the first method returns an error (for example, indicating that the server is unavailable).

With CRL checking, the ASA retrieves, parses, and caches CRLs, which provide a complete list of revoked (and unrevoked) certificates with their certificate serial numbers. The ASA evaluates certificates according to CRLs, also called authority revocation lists, from the identity certificate up the chain of subordinate certificate authorities.

OCSP offers a more scalable method of checking revocation status in that it localizes certificate status through a validation authority, which it queries for status of a specific certificate.

When the TOE cannot establish a connection for the validity check using CRL or the OCSP responder for verification, the TOE will not accept the certificate and the trusted channel will not be established. If a TLS or IPSec session fails due to inability to contact the CRL server or OCSP server, the connectivity to the CRL or OCSP server should be restored before reattempting to establish the session.

CRLs

CRLs provide the ASA with one way of determining whether a certificate that is within its valid time range has been revoked by the issuing CA. CRL configuration is part of configuration of a trustpoint.

The administrator can configure the ASA to make CRL checks mandatory when authenticating a certificate by using the revocation-check crl command. This configuration is required to be in a Common Criteria certified configuration.

The ASA can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for each trustpoint are cached for a configurable amount of time for each trustpoint.

OCSP

OCSP provides the ASA with a way of determining whether a certificate that is within its valid time range has been revoked by the issuing CA. OCSP configuration is part of trustpoint configuration.

OCSP localizes certificate status on a validation authority (an OCSP server, also called the responder) which the ASA queries for the status of a specific certificate. This method provides better scalability and more up-to-date revocation status than does CRL checking, and helps organizations with large PKI installations deploy and expand secure networks.

Note: The ASA allows a five-second time skew for OCSP responses.

You can configure the ASA to make OCSP checks mandatory when authenticating a certificate by using the revocation-check ocsp command. This configuration is required to be in a Common Criteria certified configuration.

Create Trustpoint and Generate Certificate Signing Request (CSR)

Generate a RSA or ECDSA key pair. See “Managing Public Key Infrastructure (PKI) Keys” section.

Example:

```
hostname(config)# crypto key generate rsa label RSA-key modulus 2048
```

Create and configure a CA trustpoint.

[6] Certificate revocation checking occurs on all certificates except self-signed Root Certificate Authorities when either CRL or OCSP revocation-check has been defined for a trustpoint.

Example:

```
hostname(config)# crypto ca trustpoint myCA

hostname(config-ca-trustpoint)# enrollment terminal

hostname(config-ca-trustpoint)# subject-name CN=<name>,OU=<unit>,O=<company>,C=<country>

hostname(config-ca-trustpoint)# keypair RSA-key

hostname(config-ca-trustpoint)# revocation-check crl

hostname(config-ca-trustpoint)# write memory

hostname(config-ca-trustpoint)# exit
```

To import the CA certificate for the configured trustpoint.

```
ciscoasa(config)#crypto ca authenticate myCA

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

<Copy and Paste the CA Certificate Here>

quit

INFO: Certificate has the following attributes:

Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34

Do you accept this certificate? [yes/no]:

y

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

Enforcement of the basic constraints CA flag	Certificates without the CA flag cannot be installed on the ASA as CA certificates by default. The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. You can configure the ASA to allow installation of these certificates if desired. ASA introduced the following command: **ca-check**

Generate the CSR.

```
hostname(config)#crypto ca enroll myCA

% Start certificate enrollment ..
% The subject name in the certificate will be: subject-name CN=<name>,OU=<unit>,O=<company>,C=<country>
% The fully-qualified domain name in the certificate will be: <FQDN>

% Include the device serial number in the subject name? [yes/no]: no

Display Certificate Request to terminal? [yes/no]: yes

Certificate Request follows:
<Certificate Request will be pasted here>


---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
hostname(config)#
```

The CSR is base64 encoded PEM format. This string is then sent to the CA, which then signs and issues the public certificate. To import this certificate, use the following command:

```
hostname(config)# crypto ca import myCA certificate

% The fully-qualified domain name in the certificate will be:

<FQDN>

Enter the base 64 encoded certificate.

End with a blank line or the word "quit" on a line by itself

<Copy and Paste the Certificate Here>

quit

INFO: Certificate successfully imported
```

Verify that the enrollment process was successful by displaying certificate details issued for the ASA and the CA certificate for the trustpoint.

```
hostname(config)# show crypto ca server certificate
```

To specify the trustpoint that identifies the certificate to send for authentication during Phase 1 negotiations for the crypto map entry, use the **crypto map set trustpoint** command in global configuration mode.

hostname(config)# **crypto map** *map-name seq-num* **set trustpoint** *trustpoint-name* [**chain**]

VPN Client Access Restriction

The administrators can restrict which remote VPN client access based on IP address or time range (also known as access hours). To restrict access based on IP address(s), define ACL to deny such connection from those addresses. To restrict access based on the access hours, the administrator can use the following command:

```
vpn-access-hours value {time-range-name | none}
```

This can be applied on per-user-basis (username username attributes) or as part of a group policy which applies it to all the users in the group.

Configure an IP Address Assignment Policy

The ASA can use one or more of the following methods for assigning IP addresses to remote access clients. If you configure more than one address assignment method, the ASA searches each of the options until it finds an IP address. By default, all methods are enabled.

- aaa — Retrieves addresses from an external authentication, authorization, and accounting server on a per-user basis.

- dhcp — Obtains IP addresses from a DHCP server. If you want to use DHCP, you must configure a DHCP server. You must also define the range of IP addresses that the DHCP server can use.

- local — Internally configured address pools are the easiest method of address pool assignment to configure. If you choose local, you must also use the **ip-local-pool** command to define the range of IP addresses to use. This method is available for IPv4 and IPv6 assignment policies.

Specifying a VPN Session Idle Timeout

Configure the user timeout period using the following command in group-policy configuration mode or in username configuration mode:

```
hostname(config-group-policy)#vpn-idle-timeout {minutes | none}
```

```
hostname(config-username)#vpn-idle-timeout {minutes | none}
```

AnyConnect:

```
hostname(config-webvpn)# default-idle-timeout seconds
```

The range for this value is 60-86400 seconds; the default idle timeout in seconds is 1800 seconds (30 min).

Note: A non-zero idle timeout value is required by ASA for all AnyConnect connections.

Firewall Functionality

The firewall component of the product has three modes of operation: routed, transparent and audit trail full modes. The authorized administrator can configure the security appliance to run in routed or transparent mode. In either of these modes the security appliance can be configured to run as a single context or as multiple contexts. If multiple contexts is chosen, all the contexts must run as either routed or transparent, a mixture of both is not allowed. For more information, see the “Security Context Overview” section of the *CLI Book 1* or *ASDM Book 1*, the “General Operations” guides.

Routed Mode and Transparent Mode

Routed Mode

This is the default mode set on the security appliance. The IP address of the security appliance can be seen on the outside network. The product allows for Network Address Translation to be configured in this mode.

Transparent Mode

In transparent mode the IP address of the security appliance is not visible to the outside network. Traffic being sent must be addressed to its end destination. Network Address Translation cannot be configured in this mode. When modes are changed the security appliance clears the previously configured mode as some commands are not usable in both modes. In either routed or transparent mode access lists have to be configured to allow traffic to flow.

Setting Transparent or Routed Firewall Mode at the CLI

By default, the security appliance runs in routed firewall mode. If you want to run in transparent firewall mode, you must set the mode using the Command Line Interface (CLI) before you configure anything else on the security appliance. (When you change modes, the adaptive security appliance clears the configuration, because many commands are not supported in both modes.)

To set the mode at the CLI, see the “Transparent or Routed Firewall Mode” chapter of the *CLI Book 1* or *ASDM Book 1*, the “General Operations” guides.

Audit Trail Full Mode

Note: Enabling this feature is optional in the certified configuration.

The ASA can be configured to prohibit traffic flow across the ASA when syslog messages cannot be sent to the syslog server. In order to support this functionality, the ASA must be configured to use TCP syslog instead of the default UDP syslog. Using the connection-oriented TCP protocol instead of connectionless UDP allows the ASA to track the replies from the syslog server for each message sent to the server.

Enabling Syslog Host Status Monitoring

When this functionality is enabled, and the audit server appears full, unavailable, or otherwise unresponsive, any traffic arriving at a network interface will not be allowed to pass through the security appliance.

The security appliance tries to reconnect to the syslog server five times, and while retrying the connection it stops all **new** connections through the security appliance.

To enable this feature, use the **no logging permit-hostdown** command. By default, if logging has been configured to use TCP syslog, the ASA does not allow new network access sessions when the syslog server is unavailable for any reason.

Applicable syslog error messages:

- Message ID: 414003
    - Explanation: This message indicates that the TCP syslog server for remote host logging is successful, is connected to the server, and that new connections are permitted or denied based on the logging permit-hostdown policy. If logging permit-hostdown is configured, a new connection is permitted. If not configured, a new connection is denied.
    - Recommended Action: Check whether or not the configured TCP syslog server is up. To permit new connections through the ASA, use “logging permit-hostdown”. To deny new connections, use “no logging permit-hostdown”.
    - Syntax: %ASA-3-414003: TCP Syslog Server *intf*: *IP_Address*/*port* not responding. New connections are [permitted|denied] based on logging permit-hostdown policy.
    - Variables:
        - *intf*—Interface of the adaptive security appliance to which the server is connected
        - *IP_Address*—IP address of the remote TCP syslog server
        - *port*—Port of the remote TCP syslog server
- Message ID: 414004
    - Explanation: A retry to the TCP syslog server has been successful, and the connection has been established. This message is the first to reach the syslog server after a successful connection.
    - Recommended Action None required.
    - Syntax: %ASA-6-414004: TCP Syslog Server *intf*: *IP_Address*/*port* - Connection restored
    - Variables:
        - *intf*—Interface of the adaptive security appliance to which the server is connected
        - *IP_Address*—IP address of the remote TCP syslog server
        - *port*—Port of the remote TCP syslog server

Recovering from Syslog Host Down

To recover from the disk-full condition, perform the following steps:

Step 1 Resolve the connectivity issues with the syslog server and/or the log storage issues on the syslog server.

Step 2 On the ASA check that syslog is disabled with the **show logging** command. If the syslog server has disabled the connection, the display contains the “disable” keyword.

Step 3 Disable logging to the syslog server with the **no logging host** command:

```
no logging host dmz1 10.0.0.2
```

Step 4 Restart logging with the **logging host** command:

```
logging host dmz1 10.0.0.2 tcp/1468
```

Step 5 Check that the server is now enabled with the **show logging** command. The “disabled” keyword should no longer be visible.

Traffic Flow Overview

Trusted & Untrusted Networks

The security appliance can be used to isolate your network from the Internet or from another network. A trusted network is usually your internal network and an untrusted network may be the Internet or any other network. Therefore, the security appliance must be configured so that it acts as the only network connection between your internal network and any external networks. The security appliance will deny any information flows for which no rule is defined. Your security implementation is based on the control of traffic from one network to the other, and should support the security policy of your organization/agency/enterprise.

The security appliance supports the following protocols: ICMP, ICMPv6, IPv4, IPv6, TCP and UDP[7]. For TCP and UDP traffic, service policies operate on traffic flows, and not just individual packets. If traffic is part of an existing connection that matches a feature in a policy on one interface, that traffic flow cannot also match the same feature in a policy on another interface; only the first policy is used.

Stateful Inspection Overview

All traffic that goes through the ASA is inspected using the Adaptive Security Algorithm and either allowed through or dropped. A simple packet filter can check for the correct source address, destination address, and ports, but it does not check that the packet sequence or flags are correct. A filter also checks every packet against the filter, which can be a slow process.

A stateful firewall like the ASA, however, takes into consideration the state of a packet:

- Is this a new connection?

  If it is a new connection, the ASA has to check the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the "session management path," and depending on the type of traffic, it might also pass through the "control plane path."

  The session management path is responsible for the following tasks:

  – Performing the access list checks

  – Performing route lookups

  – Allocating NAT translations (xlates)

  – Establishing sessions in the "fast path"

  The ASA creates forward and reverse flows in the fast path for TCP traffic; the ASA also creates connection state information for connectionless protocols like UDP, ICMP (when you enable ICMP inspection), so that they can also use the fast path.

- Is this an established connection?

  If the connection is already established, the ASA does not need to re-check packets; most matching packets can go through the "fast" path in both directions. The fast path is responsible for the following tasks:

  – IP checksum verification

  – Session lookup

[7] These protocols are the only ones that were evaluated.

- TCP sequence number check
- NAT translations based on existing sessions
- Layer 3 and Layer 4 header adjustments

Application Layer Protocol Inspection

Inspection engines are required for services that embed IP addressing in formation in the user data packet or that open secondary channels on dynamically assigned ports (i.e., dynamic protocol). Many protocols open secondary TCP or UDP ports. The initial session on a well-known port is used to negotiate dynamically assigned port numbers. When you enable application inspection for a service that uses dynamically assigned ports, the ASA monitors sessions to identify the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session. For example, to inspect FTP

Create an FTP inspection policy map:

```
hostname(config)# policy-map type inspect ftp policy_map_name
```

```
hostname(config-pmap)#
```

If you created an FTP class map, specify it by entering the following command:

```
hostname(config-pmap)# class class_map_name
```

```
hostname(config-pmap-c)#
```

Specify the action you want to perform on the matching traffic by entering the following command:

```
hostname(config-pmap-c)# reset [log]
```

The reset keyword drops the packet, closes the connection, and sends a TCP reset to the server or client. Add the log keyword to send a system log message.

When a user establishes a connection, the ASA checks the packet against ACLs, creates an address translation, and creates an entry for the session in the fast path, so that further packets can bypass time-consuming checks. However, the fast path relies on predictable port numbers and does not perform address translations inside a packet.

Many protocols open secondary TCP or UDP ports. The initial session on a well-known port is used to negotiate dynamically assigned port numbers. If you use applications like these, then you need to enable application inspection

When you enable application inspection for a service that uses dynamically assigned ports, the ASA monitors sessions to identify the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session.

Same-Security-Traffic

The **same-security-traffic** command is not allowed in the certified configuration. When this command is enabled traffic is allowed to pass between interfaces with the same security level, regardless of current security policy. When **same-security-traffic** is enabled, any AAA statements configured using “include” are bypassed.

Access Lists

The **access-list** command operates on a first-match basis. Therefore, the last rule added to the access list is the last rule checked. Administrators must take note of this when entering the initial rules during the configuration, as it may impact the remainder of the rule parsing.

Configure Extended ACLs

An extended ACL is composed of all ACEs with the same ACL ID or name. Extended ACLs are the most complex and feature-rich type of ACL. For a full explanation of creation, modification, and deletion of ACLs, refer to the “Access Control Lists” chapter in Book 2: Cisco ASA Series Firewall Configuration Guide, 9.20.

access-list *access_list_name* [**line** *line_number*] **extended** {**deny | permit**} {**tcp | udp | ip | icmp | icmp6**} *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] **| disable | default**] [**time-range** *time-range-name*] [**inactive**]

Within the access-list command:

- The protocol (after the ‘deny’ or ‘permit’ keyword) can be entered as number (0-255) instead of a keyword. If protocol is entered as a number and that number matches a keyword, the keyword will appear in the configuration instead of the number. The keywords ‘tcp’, ‘udp’, and ‘ip’ are used for IPv4 or IPv6 traffic.
- The address (source or destination) can be an IPv4 address (network or host), or can be an IPv6 address (network or host), or keywords can be used for ‘any’ address, where ‘any4’ specifies IPv4 traffic only, ‘any6’ specified IPv6 traffic only, and ‘any’ means any IPv4 or IPv6 traffic.
- The ‘port-argument’ (after the source or destination address) can also be entered as a number or a keyword, use the ‘?’ to display the list of available keywords for the argument.

To specify IP (IPv4 or IPv6) protocol or ICMP type and code, you can define a named object service.

- service protocol—The name or number (0-255) of an IP protocol. Specify ip to apply to all protocols.
- service {icmp | icmp6} [icmp-type [icmp_code]]—For ICMP or ICMP version 6 messages. You can optionally specify the ICMP type by name or number (0-255) to limit the object to that message type. If you specify a type, you can optionally specify an ICMP code for that type (1-255). If you do not specify the code, then all codes are used.

For example,

```
object service ICMP_unreachable

 service icmp unreachable 13

access-list <name> extended permit object ICMP_unreachable host <IP1> host <IP2> log

…

object service IPv6-134

 service 134

access-list <name> extended deny object IPv6-134 host <IP1> host <IP2> log
```

The TOE supports all IPv4 protocols excluding Protocol 2 (IGMP) which is not routable and thus will not be forwarded by the TOE.

The TOE supports the following 16 IPv6 protocols:

- Transport Layer Protocol 4 - IPv4 encapsulation
- Transport Layer Protocol 6 - Transmission Control
- Transport Layer Protocol 8 - Exterior Gateway Protocol
- Transport Layer Protocol 9 - any private interior gateway
- Transport Layer Protocol 17 - User Datagram
- Transport Layer Protocol 41 - IPv6 encapsulation
- Transport Layer Protocol 46 - Reservation Protocol
- Transport Layer Protocol 47 - General Routing Encapsulation
- Transport Layer Protocol 49 - BNA
- Transport Layer Protocol 58 - ICMP for IPv6
- Transport Layer Protocol 59 - No Next Header for IPv6

- Transport Layer Protocol 88 - TCF
- Transport Layer Protocol 89 – EIGRP
- Transport Layer Protocol 105 - SCPS Transport Layer Protocol
- Transport Layer Protocol 112 - Virtual Router Redundancy Protocol
- Transport Layer Protocol 132 - Stream Control Transmission Protocol

IPv6 Protocol 2 (IGMP) and Protocol 103 (PIM) are excluded as they are not routable and thus not forwarded by the TOE despite the TOE recognizing the protocol.

All other IPv6 protocols from the RFC Values for IPv4 and IPv6 table in the MOD VPNGW Supporting Document (SD) v1.1 are dropped by default by the TOE.

Using the 'Established' Keyword

Administrators are advised not to use the **established** command on the certified security appliance. Incorrect use of this command may give external entities greater access to inside systems than is intended, and for this reason its use is not recommended.

Time-to-Live

The Time-to-Live (TTL) decrement feature was introduced in version 7.2.4, and it is disabled by default. The TTL decrement feature is not to be enabled in the certified configuration as it can result in an insecure configuration.

VLAN Interfaces

The ASA supports VLAN interfaces for separation of communications received on an interface. On the ASA is accomplished using the **interface vlan** command or though the ASDM web interface. Information regarding configuring VLAN interfaces can be found in the "VLAN Interfaces" chapter of the *CLI Book 1* or *ASDM Book 1*, the "General Operations" guides.

Interface Types

ASA interfaces capable of enforcing traffic filtering (via the **access-group** command), or terminating tunnels (e.g. via the **crypto-map** command) are interfaces that have been "named" (via the **nameif** command). The interface name is used in all configuration commands on the ASA instead of the interface type and ID (such as gigabitethernet0/1), and is therefore required before traffic can pass through the interface. For subinterfaces, a VLAN must be assigned to the subinterface (via the **vlan** command) before the subinterface can be named.

Interfaces that can be "named" are those that can be referenced using a 'physical' interface type (e.g. Ethernet, GigabitEthernet, etc), plus the interface identifier (slot/port.subinterface), e.g.: Ethernet0/1, GigabitEthernet0/1, GigabitEthernet0/1.2, TenGigabitEthernet0/1, or Management0/0, etc.

Example of named interfaces:

```
hostname(config)# access-group <name of access-list> in interface ?

configure mode commands/options:

Current available interface(s):

  inside      Name of interface GigabitEthernet0/0

  outside     Name of interface GigabitEthernet0/1

  management  Name of interface Management0/0
```

Servers and Proxies

To ensure complete security when the security appliance is shipped, inbound access to all proxies and servers is initially disabled. After the installation, you must explicitly permit each service and enable the services necessary for your security policy. Use the **show logging** command or the external syslog server to view log file messages. For more details see the *CLI Book 1* or *ASDM Book 1*, the "General Operations" guides. Certification requires a completely controlled environment in which specified services are allowed and all others denied. Doing this allows the administrator to configure the TOE to filter traffic appropriately. Any service may be configured on the network, as long as, the TOE administrator has considered the services impact on the operational environment and configured the TOE to appropriately handle the traffic.

Protect from SYN Flood DoS Attack (TCP Intercept)

A SYN-flooding denial of service (DoS) attack occurs when an attacker sends a series of SYN packets to a host. These packets usually originate from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests from legitimate users.

The administrators can limit the number of embryonic connections to help prevent SYN flooding attacks. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.

When the embryonic connection threshold of a connection is crossed, the ASA acts as a proxy for the server and generates a SYN-ACK response to the client SYN request using the SYN cookie method (see Wikipedia for details on SYN cookies). When the ASA receives an ACK back from the client, it can then authenticate that the client is real and allow the connection to the server. The component that performs the proxy is called TCP Intercept.

The end-to-end process for protecting a server from a SYN flood attack involves setting connection limits, enabling TCP Intercept statistics, and then monitoring the results.

Note: Ensure that you set the embryonic connection limit lower than the TCP SYN backlog queue on the server that you want to protect.

Step 1 Create an L3/L4 class map to identify the servers you are protecting. Use an access-list match.

Example:

```
hostname(config)# access-list servers extended permit tcp any host 10.1.1.5 eq http
hostname(config)# access-list servers extended permit tcp any host 10.1.1.6 eq http
hostname(config)# class-map protected-servers
hostname(config-cmap)# match access-list servers
```

Step 2 Add or edit a policy map that sets the actions to take with the class map traffic, and identify the class map.

Example:

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class protected-servers
```

Step 3 Set the embryonic connection limits.

- **set connection embryonic-conn-max** n—The maximum number of simultaneous embryonic connections allowed, between 0 and 2000000. The default is 0, which allows unlimited connections.

- **set connection per-client-embryonic-max** n—The maximum number of simultaneous embryonic connections allowed per client, between 0 and 2000000. The default is 0, which allows unlimited connections.

Example:

```
hostname(config-pmap-c)# set connection embryonic-conn-max 1000
hostname(config-pmap-c)# set connection per-client-embryonic-max 50
```

Step 4 If you are editing an existing service policy (such as the default global policy called global_policy), you can skip this step. Otherwise, activate the policy map on one or more interfaces.

service-policy *policymap_name* {**global | interface** *interface_name*}

Example:

```
hostname(config)# service-policy global_policy global
```

Step 5 Configure threat detection statistics for attacks intercepted by TCP Intercept.

threat-detection statistics tcp-intercept [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]

Where:

- rate-interval minutes sets the size of the history monitoring window, between 1 and 1440 minutes. The default is 30 minutes. During this interval, the ASA samples the number of attacks 30 times.
- burst-rate attacks_per_sec sets the threshold for syslog message generation, between 25 and 2147483647. The default is 400 per second. When the burst rate is exceeded, syslog message 733104 is generated.
- average-rate attacks_per_sec sets the average rate threshold for syslog message generation, between 25 and 2147483647. The default is 200 per second. When the average rate is exceeded, syslog message 733105 is generated.

Example:

```
hostname(config)# threat-detection statistics tcp-intercept
```

Step 6 Monitor the results with the following commands:

- **show threat-detection statistics top tcp-intercept** [all | detail]—View the top 10 protected servers under attack. The all keyword shows the history data of all the traced servers. The detail keyword shows history sampling data. The ASA samples the number of attacks 30 times during the rate interval, so for the default 30 minute period, statistics are collected every 60 seconds.
- **clear threat-detection statistics tcp-intercept**—Erases TCP Intercept statistics.

Example:

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack Time)>
----------------------------------------------------------------------------------
```

```
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

Configure Global Timeouts

The administrators can set the global idle timeout durations for the connections using the timeout command.

The administrators can configure the following global timeouts.

- **timeout conn** *hh*:*mm*:*ss*—The idle time after which a connection closes, between 0:5:0 and 1193:0:0. The default is 1 hour (1:0:0).
- **timeout half-closed** *hh*:*mm*:*ss*—The idle time until a TCP half-closed connection closes. The minimum is 30 seconds. The default is 10 minutes.
- **timeout udp** *hh*:*mm*:*ss*—The idle time until a UDP connection closes. This duration must be at least 1 minute. The default is 2 minutes.
- **timeout icmp** *hh*:*mm*:*ss*—The idle time for ICMP, between 0:0:2 and 1193:0:0. The default is 2 seconds (0:0:2).
- **timeout tcp-proxy-reassembly** *hh*:*mm*:*ss*—The idle timeout after which buffered packets waiting for reassembly are dropped, between 0:0:10 and 1193:0:0. The default is 1 minute (0:1:0).

Default Traffic Flow (without ACLs)

The ASA, by default, is configured with a default DHCP address pool. The outbound interface disallows all external to internal data flows. The administrator needs to be aware of this, and ensure that the correct policy for the organization is installed and committed before users are permitted to use the security appliance. Access Lists are required to be set up to enable traffic to flow through the security appliance. Specific permit or deny rules are required to be applied to a protocol, a source and destination IP address or Network and optionally, the source and destination ports.

Table 5 and Table 6 list the default/implicit traffic flow policy applied between the “outside” and “inside” networks when no ACLs have been applied to outside or inside interfaces of the ASA.

Table 5: Default Configuration: Traffic Types Showing Inside to Outside Traffic

Traffic Type	**Single Routed Mode**	**Multiple Routed Mode**	**Single Transparent Mode**	**Multiple Transparent Mode**
Spoofed Traffic	No (RPF enabled)	No (RPF enabled)	No (ARP inspection enabled)	No (ARP inspection enabled)
Ethernet	Yes	Yes	Yes	Yes
ARP	No (Router hop)	No (Router hop)	Yes	Yes
DNS	Yes	Yes	Yes	Yes
Echo	Yes	Yes	Yes	Yes
Finger	Yes	Yes	Yes	Yes
H.323	Yes	Yes	Yes	Yes

IP	Yes	Yes	Yes	Yes
ICMP	Yes	Yes	Yes	Yes
TCP	Yes	Yes	Yes	Yes
UDP	Yes	Yes	Yes	Yes
FTP*	Yes	Yes	Yes	Yes
GTP	Yes	Yes	Yes	Yes
HTTP	Yes	Yes	Yes	Yes
ILS	Yes	Yes	Yes	Yes
MGCP	Yes	Yes	Yes	Yes
POP3	Yes	Yes	Yes	Yes
RSH	Yes	Yes	Yes	Yes
RTSP	Yes	Yes	Yes	Yes
Skinny	Yes	Yes	Yes	Yes
SIP	Yes	Yes	Yes	Yes
ESMTP	Yes	Yes	Yes	Yes
SunRPC	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes
TFTP	Yes	Yes	Yes	Yes
Traceroute	Yes	Yes	Yes	Yes
STP	No	No	Yes	Yes
All other Traffic	Yes	Yes	Yes	Yes

Table 6: Default Configuration: Traffic Types Showing Outside to Inside Traffic

Traffic Type	**Single Routed Mode**	**Multiple Routed Mode**	**Single Transparent Mode**	**Multiple Transparent Mode**
Spoofed Traffic	No (RPF enabled)	No (RPF enabled)	No (ARP inspection enabled)	No (ARP inspection enabled)
Ethernet	No	No	Yes	Yes
ARP	No (Router hop)	No (Router hop)	No	No
DNS	No	No	No	No
Echo	No	No	No	No
Finger	No	No	No	No
H.323	No	No	No	No

IP	No	No	No	No
ICMP	No	No	No	No
TCP	No	No	No	No
UDP	No	No	No	No
FTP	No	No	No	No
GTP	No	No	No	No
HTTP	No	No	No	No
ILS	No	No	No	No
MGCP	No	No	No	No
POP3	No	No	No	No
RSH	No	No	No	No
RTSP	No	No	No	No
Skinny	No	No	No	No
SIP	No	No	No	No
ESMTP	No	No	No	No
SunRPC	No	No	No	No
Telnet*	No	No	No	No
TFTP	No	No	No	No
Traceroute	No	No	No	No
STP	No	No	Yes (Can be denied by ACL)	Yes (Can be denied by ACL)
All other Traffic	No	No	No	No

Optional Traffic Inspection

Unicast RPF

Note: Configuring this feature is optional in the certified configuration.

To enable Unicast RPF, use the **ip verify reverse-path** command in global configuration mode. Unicast RPF guards against IP spoofing (a packet uses an incorrect source IP address to obscure its true source) by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table. Unicast RPF is only applicable when a context is operating in routing mode.

```
hostname(config)# ip verify reverse-path interface outside
```

```
hostname(config)# ip verify reverse-path interface inside
```

STP & Transparent Mode

Note: Configuring this feature is optional in the certified configuration.

Spanning Tree Protocol (STP) is passed through the firewall by default in transparent mode. This default operation of the product can be mitigated by creating an access list to block the traffic.

```
hostname(config)# access-list layer2 ethertype deny bpdu
```

Inspect ICMP

Note: Configuring this feature is optional in the certified configuration.

To configure the ICMP inspection engine, use the **inspect icmp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. The inspect icmp command is required to prevent ICMP traffic from passing through the firewall in the event the remote syslog server should fail.

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

Inspect ARP

Note: Configuring this feature is optional in the certified configuration.

To configure the ARP inspection engine, use the **arp-inspection** command in global configuration mode. ARP inspection is required when a firewall context is operating in transparent mode, to prevent IP spoofing of traffic.

To complete the configuration of ARP inspection the administrator must create static ARP entries for each host protected by the firewall context.

```
hostname(config)# arp inside 192.0.2.0 0050.abcd.1234
hostname(config)# arp-inspection outside enable
hostname(config)# arp-inspection inside enable
```

Prohibit IPv6 Extension Header 0

Warning: Do not permit IPv6 Extension Header 0 packets using these commands. For example,

```
object service IPv6-0
service 0
access-list acl_name extended permit object IPv6-0 host IPv6_address1 host IPv6_address2 log log_number interval interval_number
```

Optional Authentication of Throughput Traffic

Note: Configuring this feature is optional in the certified configuration.

Warning: Authentication of Telnet and FTP flows through the ASA can be configured in more than one way: through use of “aaa authentication match”, or “aaa authentication include”. ASDM will always use “aaa authentication match” with a matching named access -list. If the CLI is used to configure this function using the “aaa authentication include” command, the ASDM cannot be used to subsequently modify function, and the CLI must be used instead. For best results, use one of either GUI or CLI to configure and reconfigure this function.

To configure AAA for Telnet and FTP using cut-through proxies, you must first configure the AAA server group and authentication settings (via CLI or GUI). The following procedures and examples show how to configure this function via the CLI after the AAA server settings are in effect.

Enable authentication of Telnet and FTP using the **aaa authentication include** {telnet, ftp} command.

Note: Running FTP and TELNET servers on non-standard ports will result in those flows not requiring RADIUS or authentication and is therefore not to be allowed in the certified configuration.

```
Hostname (config)# aaa-server aaasrvgrp protocol radius

hostname (config-aaa-server-group)# exit

hostname (config)# aaa-server aaasrvgrp host 10.0.0.2

hostname (config-aaa-server-host)# authentication-port 1645

hostname (config-aaa-server-host)# timeout 10

hostname (config-aaa-server-host)# retry-interval 2

hostname (config-aaa-server-host)# exit

hostname (config)# aaa authentication include telnet outside 0 0 0 0 aaasrvgrp

hostname (config)# aaa authentication include ftp outside 0 0 0 0 aaasrvgrp

hostname (config)# aaa authentication include telnet inside 0 0 0 0 aaasrvgrp

hostname (config)# aaa authentication include ftp inside 0 0 0 0 aaasrvgrp
```

To ensure that separate sessions from a multi-user machine are not able to piggy-back on an existing authentication request, ensure that the timeout for authentication is set to 0, for no caching of authentication data.

```
hostname (config)# timeout uauth 0:00:00
```

Mandatory Traffic Flow Controls

In its Common Criteria certified configuration, the ASA must be drop certain traffic at all enabled interfaces at all times. Some of the traffic that must be dropped will be dropped at all times, regardless of configuration, other traffic will be dropped by ACLs, and still other traffic will be dropped by the “ip audit” feature.

The “ip audit” feature is configured with the following commands:

ip audit attack Sets the default actions for packets that match an attack signature.

ip audit info Sets the default actions for packets that match an informational signature.

ip audit name Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.

ip audit interface Assigns an audit policy to an interface.

show running-config ip audit signature Shows the configuration for the **ip audit signature** command.

Set “ip audit” Actions

Set the actions to be taken when packets match “info” signatures and “attack” signatures. The default action for “ip audit info” and “ip audit attack” is to audit only. The certified configuration requires the action to include “drop”, and optionally allows the action to include “audit” and/or “reset”.

Syntax for “info” signatures: **ip audit info** [**action** [**alarm**] [**drop**] [**reset**]]

Allowed settings:

```
ip audit info action drop
```

ip audit info action alarm drop

ip audit info action drop reset

ip audit info action alarm drop reset

Syntax for "attack" signatures: **ip audit attack** [**action** [**alarm**] [**drop**] [**reset**]]

Allowed settings:

ip audit attack action drop

ip audit attack action alarm drop

ip audit attack action drop reset

ip audit attack action alarm drop reset

Do not disable certain signatures

When "ip audit" has been enabled for either "info" or "attack" signatures, the full set of "info" or "attack" signatures defined in syslog message range 4000xx (400000-400099), will be enabled. Individual signatures can be disabled with the "ip audit signature" command, but the following signatures must remain enabled in the Common Criteria certified configuration:

- 4000001, IP options-Bad Option List
- 4000004, IP options-Loose Source Route
- 4000006, IP options-Strict Source Route
- 4000007, IP Fragment Attack
- 4000009, IP Fragments Overlap
- 4000023, Fragmented ICMP Traffic
- 4000025, Ping of Death Attack

Define "ip audit" Policies

Define two "ip audit" policies, one for "info" events, and one for "attack" events, and set the "action" to "drop":

Syntax: **ip audit name** *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

Example:

hostname(config)# **ip audit name** *infopolicy* **info action drop**

hostname(config)# **ip audit name** *attackpolicy* **attack action drop**

Apply "ip audit" Policies to Interfaces

Apply both "ip audit" policies to each enabled interface.

Syntax: **ip audit interface** *interface_name policy_name*

Examples:

hostname(config)# **ip audit interface** inside infopolicy

hostname(config)# **ip audit interface** inside attackpolicy

hostname(config)# **ip audit interface** outside infopolicy

hostname(config)# **ip audit interface** outside attackpolicy

Overview of Traffic to Be Dropped, and the Related Syslog Messages

To ensure that the ASA is operating in the CC-certified configuration, such that it will drop all traffic as required by the collaborative Protection Profile for Stateful Traffic Filter Firewalls, the ASA administrator must ensure that all non-default “configuration” steps listed below have been added to the ASA’s configuration.

1) Packets which are invalid fragments
   a) Fragments are considered invalid by the ASA when they violate fragmentation rules, such as with a “teardrop” attack.
   b) Syslog messages related to invalid fragments
      i) Syslog messages generated regardless of the “ip audit name”settings
         (1) IP Overlapping Fragments (Teardrop)
            (a) Condition: The ASA discarded an IP packet with a teardrop signature containing either a small offset or fragment overlapping. This is a hostile event that circumvents the ASA or an Intrusion Detection System.
            (b) %ASA-2-**106020**: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
         (2) Malformed IP fragments
            (a) Condition: An IP fragment is malformed, for example: the total size of the reassembled IP packet exceeds the maximum possible size of 65,535 bytes.
            (b) %ASA-4-**209004**: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source_address, dest = dest_address, proto = protocol, id = number
         (3) Fragmented decapsulated IPsec packets
            (a) Condition: A decapsulatd IPsec packet included an IP fragment with an offset less than or equal to 128 bytes. The latest version of the security architecture for IP RFC recommends 128 bytes as the minimum IP fragment offset to prevent reassembly attacks. This may be part of an attack. This message is rate limited to no more than one message every five seconds.
            (b) %ASA-4-**402118**: IPSEC: Received an protocol packet (SPI=spi, sequence number seq_num) from remote_IP (username) to local_IP containing an illegal IP fragment of length frag_len with offset frag_offset.
         (4) Malformed NetBIOS Datagram (NBDGM) fragments
            (a) The NBDGM fragment format is incorrect.
            (b) %ASA-4-**423005**: {Allowed | Dropped} NBDGM pkt_type_name fragment with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port.
      i) Additional syslog messages generated by “ip audit name <name> **info** action **audit** drop”
         - None.
      ii) Additional syslog messages generated by “ip audit name <name> **attack** action **audit** drop”
         - IP Fragment Attack, message number **400007** (see table below)
         - IP Overlapping Fragments (Teardrop), message number **400009** (see table below)
         - Fragmented ICMP Traffic, message number **400023** (see table below)
         - Ping of Death Attack, message number **400025** (see table below).
2) Fragmented IP packets which cannot be re-assembled completely
   a) Fragmented IP packets cannot be re-assembled completely if they exceed the configurable allowed parameters for reassembly
   b) Configuration of fragmentation rules:
      i) To show the current fragmentation limits:
         - hostname# **show fragment**
         - hostname# **show running-config fragment**
      ii) To adjust the fragmentation settings:
         - **fragment reassembly** {**full** | **virtual**} {**size** | **chain** | **timeout** *limit*} [*interface*]
            - **reassembly full** | **virtual** Specifies the full or virtual reassembly for IP fragments that are routed through the ASA. IP fragments that terminate at the ASA are always fully reassembled.
            - **size** *limit* Sets the maximum number of fragments that can be in the IP reassembly database waiting for reassembly.

            - ➢ **Note** The ASA does not accept any fragments that are not part of an existing fabric chain after the queue size reaches 2/3 full. The remaining 1/3 of the queue is used to accept fragments where the source/destination IP addresses and IP identification number are the same as an incomplete fragment chain that is already partially queued. This limit is a DoS protection mechanism to help legitimate fragment chains be reassembled when there is a fragment flooding attack.
        - o **chain** *limit* Specifies the maximum number of fragments into which a full IP packet can be fragmented.
        - o **timeout** *limit* Specifies the maximum number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded.
        - o *interface* (Optional) Specifies the ASA interface. If an interface is not specified, the command applies to all interfaces.
    - iii) The default values are:
        - Virtual reassembly is enabled.
        - **size** is 200 fragments
        - **chain** is 24 packets
        - **timeout** is 5 seconds
        - *interface* is all interfaces
- c) Syslog messages related to packets which cannot be re-assembled
    - i) Fragmentation exceeded limits
        - (1) %ASA-4-**209003**: Fragment database limit of number exceeded: src = source_address, dest = dest_address, proto = protocol, id = number
        - (2) %ASA-4-**209005**: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.
    - ii) IKE fragments not re-assembled
        - (1) %ASA-7-**715060**: Dropped received IKE fragment. Reason: reason
    - iii) Packet fragments re-sent, i.e. a resend of the same packet occurred, but fragmented to a different MTU, or another packet altogether.
        - (1) %ASA-7-**715061**: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.
    - iv) Non-contiguous fragment numbers
        - (1) %ASA-7-**715062**: Error assembling fragments! Fragment numbers are non-continuous.

3) <u>Network packets where the source address of the network packet is equal to the address of the network interface where the network packet was received</u>
    - a) Configuration:
        - i) To drop this traffic, include within the inbound ACL applied to each enabled interface an entry that explicitly denies traffic where the source address is equal to the address of the network interface where the packet was received.
        - ii) Tip: To avoid adding unnecessary entries to each ACL, this rule can be configured using object groups, for example:
            - hostname(config)# object-group network local-interfaces
            - hostname(config-network-object-group)# network-object host inside
            - hostname(config-network-object-group)# network-object host outside
            - hostname(config-network-object-group)# network-object host <other-interfaces>
            - hostname(config-network-object-group)# exit
            - hostname(config)# **access-list** inbound-inside **extended deny ip** local-interfaces **any** [log]
            - hostname(config)# **access-list** inbound-outside **extended deny ip** local-interfaces **any** [log]
            - hostname(config)# access-group inbound-inside in interface inside
            - hostname(config)# access-group inbound-outside in interface outside
    - b) Syslog messages:
        - i) %ASA-4-**106023**: Deny protocol src [interface_name:source_address/source_port] [([idfw_user|FQDN_string], sg_info)] dst interface_name:dest_address/dest_port

[([idfw_user|FQDN_string], sg_info)] [type {string}, code {code}] by access_group acl_ID [0x8ed66b60, 0xf8852875]

ii) %ASA-4-**106100**: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name/source_address(source_port) (idfw_user, sg_info) interface_name/dest_address(dest_port) (idfw_user, sg_info) hit-cnt number ({first hit | number-second interval}) hash codes

4) <u>Network packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received</u>

a) Configuration: Enable "ip verity reverse-path" on each enabled interface, e.g:

i) **ip verify reverse-path interface** *interface_name*

b) Syslog message: %ASA-1-**106021**: Deny protocol reverse path check from source_address to dest_address on interface interface_name

5) <u>Network packets where the source address of the network packet is defined as being on a broadcast network</u>

a) Configuration: Default.

b) Syslog message: %ASA-2-**106016**: Deny IP spoof from (IP_address) to IP_address on interface interface_name.

6) <u>Network packets where the source address of the network packet is defined as being on a multicast network</u>

a) Condition:

i) IPv4 multicast addresses are in the range 224.0.0.0/4 (224.0.0.0 through 239.255.255.255)

ii) IPv6 multicast addresses have the prefix ff00::/8

b) Configuration:

i) To drop this traffic, include within the inbound ACL applied to each enabled interface an entry that explicitly denies traffic where the source address is a multicast address.

ii) Tip: To avoid adding unnecessary entries to each ACL, this rule can be configured using object groups. The example below shows creation of an object-group named "ipmulticast" which contains IPv4 network objects and IPv6 network objects. That object-list is then referenced in separate ACL entries in two separate ACLs, one IPv6 ACL (named "inbound-inside"), and one IPv4 ACL (named "inbound-outside"). Both sample ACL entries show the object-group being used to match traffic by the source address (where "ipmulticast" defines the source, listed first in the rule, and "any" defines the destination, listed second in the rule). The example also shows the "access-group" command that would be used to apply the two ACLs to interfaces (in this case, the "inbound-inside" ACL is applied to the "inside" interface, and the other ACL is applied to the "outside" interface, to control traffic being received inbound (defined by use of the keyword "in") to each interface:

- hostname(config)# **object-group network** ipmulticast
- hostname(config-network-object-group)# **network-object** 224.0.0.0 240.0.0.0
- hostname(config-network-object-group)# **network-object** ff00::/8
- hostname(config-network-object-group)# **exit**
- hostname(config)# **access-list** in-inside **deny** ip **object-group** ipmulticast **any** log
- hostname(config)# **access-list** in-outside **deny** ip **object-group** ipmulticast **any** log
- hostname(config)# **access-group** in-inside in **interface** inside
- hostname(config)# **access-group** in-outside in **interface** outside

c) Syslog messages: Same as for item 3 (**106023**, and **106100**)

7) <u>Network packets where the source address of the network packet is defined as being a loopback address</u>

a) Condition:

i) IPv4 loopback addresses are in the range 127.0.0.0/8

ii) IPv6 loopback address is 0:0:0:0:0:0:0:1, or written as ::1

b) Configuration: Default, no ACL required.

c) Syslog messages: %ASA-2-**106016**: Deny IP spoof from (IP_address) to IP_address on interface interface_name.

8) <u>Network packets where the source address of the network packet is a multicast</u>

    a) Redundant to item 6 of this list.
    b) Note: The numbering of this list mirrors the numbering of items in the Common Criteria requirements document, “Traffic Filter Firewall Extended Package for the Network Device Protection Profile”

9) <u>Network packets where the source or destination address of the network packet is a link-local address</u>
    a) Condition:
        i) IPv4 link-local addresses are defined in the address block 169.254.0.0/16.
        ii) IPv6 link-local addresses are assigned with the fe80::/64 prefix.
    b) Configuration:
        i) To drop this traffic, include within the inbound ACL applied to each enabled interface an entry that explicitly denies traffic where the source address or the destination address is a link-local address.
        ii) Tip: To avoid adding unnecessary entries to each ACL, this rule can be configured using object groups, for example:

- hostname(config)# **object-group network** linklocal
- hostname(config-network-object-group)# **network-object** 169.254.0.0 255.255.0.0
- hostname(config-network-object-group)# **network-object** fe80::/64
- hostname(config-network-object-group)# **exit**
- hostname(config)# **access-list** in-inside **deny ip object-group** linklocal **any** log
- hostname(config)# **access-list** in-inside **deny ip any object-group** linklocal log
- hostname(config)# **access-list** in-outside **deny ip object-group** linklocal **any** log
- hostname(config)# **access-list** in-outside **deny ip any object-group** linklocal log
- hostname(config)# **access-group** in-inside in **interface** inside
- hostname(config)# **access-group** in-outside in **interface** outside

    c) Syslog messages: Same as for item 3 (**106023**, and **106100**)

10) <u>Network packets where the source or destination address of the network packet is defined as being an address “reserved for future use” as specified in RFC 5735 for IPv4</u>
    a) Condition: IPv4 addresses reserved for future use are in the range 240.0.0.0/4.
    b) Configuration:
        i) To drop this traffic, include within the inbound ACL applied to each enabled interface an entry that explicitly denies traffic where the source address or the destination address is a link-local address.
        ii) Tip: To avoid adding unnecessary entries to each ACL, this rule can be configured using object groups, for example:

- hostname(config)# **object-group network** reserved
- hostname(config-network-object-group)# **network-object** 240.0.0.0 240.0.0.0
- hostname(config-network-object-group)# **exit**
- hostname(config)# **access-list** in-outside **deny ip object-group** reserved **any** log
- hostname(config)# **access-list** in-outside **deny ip any object-group** reserved log
- hostname(config)# **access-group** in-outside in **interface** outside

    c) Syslog messages: Same as for item 3 (**106023**, and **106100**)

11) <u>Network packets where the source or destination address of the network packet is defined as an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6</u>

    a) Condition:

        i) “reserved for future definition and use” = addresses that DO NOT start with binary value 001.
        ii) “unspecified addresses” = 0:0:0:0:0:0:0:0 = :: = ::/128
    b) Configuration:
        i) To drop this traffic, include within the inbound ACL applied to each enabled interface an entry that explicitly denies traffic where the source address or the destination address is reserved or unspecified.
        ii) Tip: To avoid adding unnecessary entries to each ACL, ALC rules can be configured using object groups. The example below shows creation of an object-group named “reserved.” That object-list is then referenced in two entries within an IPv6 ACL, named “inbound-inside,” to cover traffic that would match any of the network-objects defined within the object-group. Examples of two ACL

entries are shown to illustrate how the object-group can be used to match traffic by the source address (where “reserved” is the source, listed first in the rule, and “any” is the destination, listed second in the rule), or would match the object-group in the destination address (where “any” is the source and “reserved” is the destination). The example also shows the “access-group” command that would be used to apply that ACL to an interface (in this case, the “inside” interface), to control traffic being sent “in” to “out” from that interface (in this case, “in”):

- hostname(config)# **object-group network** reserved
- hostname(config-network-object-group)# **network-object** ::/128
- hostname(config-network-object-group)# **network-object** ::/8
- hostname(config-network-object-group)# **network-object** 0100::/8
- hostname(config-network-object-group)# **network-object** 0400::/6
- hostname(config-network-object-group)# **network-object** 0800::/5
- hostname(config-network-object-group)# **network-object** 1000::/4
- hostname(config-network-object-group)# **network-object** 4000::/3
- hostname(config-network-object-group)# **network-object** 6000::/3
- hostname(config-network-object-group)# **network-object** 8000::/3
- hostname(config-network-object-group)# **network-object** a000::/3
- hostname(config-network-object-group)# **network-object** c000::/3
- hostname(config-network-object-group)# **network-object** e000::/4
- hostname(config-network-object-group)# **network-object** f000::/5
- hostname(config-network-object-group)# **network-object** f800::/6
- hostname(config-network-object-group)# **network-object** fc00::/7
- hostname(config-network-object-group)# **network-object** fe00::/9
- hostname(config-network-object-group)# **exit**
- hostname(config)# **access-list** in-inside **deny ip object-group** reserved **any** log
- hostname(config)# **access-list** in-inside **deny ip any object-group** reserved log
- hostname(config)# **access-group** in-inside in **interface** inside

c) Syslog messages: Same as for item 3 (**106023**, and **106100**)

12) Network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified

a) Configuration: Default.

b) Syslog messages:

i) Syslog messages generated regardless of the “ip audit name”settings

(1) %ASA-6-**106012**: Deny IP from IP_address to IP_address, IP options hex.

ii) Additional syslog messages generated by “ip audit name <name> **info** action **audit** drop”

(1) IP options-Record Packet Route, message number **400001** (see table below)

(2) IP options-Loose Source Route, message number **400004** (see table below)

(3) IP options-Strict Source Route, message number **400006** (see table below)

iii) Additional syslog messages generated by “ip audit name <name> **attack** action **audit** drop”

(1) None.

13) Additional packets dropped by default

a) Slowpath security checks failed:

i) Conditions:

(1) In routed mode when the ASA receives a through-the-box:

(a) IPv4 packet with destination IP address equal to 0.0.0.0

(b) IPv4 packet with source IP address equal to 0.0.0.0

(2) In routed or transparent mode when the ASA receives a through-the-box IPv4 packet matching any of the conditions listed below where the "network part" and "host part" are determined by the size of the local subnet of the ingress interface (when the ASA is in routed mode), or the subnet size of the management interface (when the ASA is in transparent mode):

(a) first octet of the source IP address equal to zero

(b) network part of the source IP address equal to all 0's

(c) network part of the source IP address equal to all 1's

(d) source IP address host part equal to all 0's or all 1's

  - ii) Syslog message: %ASA-2-**106016**: Deny IP spoof from (IP_address) to IP_address on interface interface_name.
- b) "Land" attack:
  - i) Condition: Received IP packets with the IP source address equal to the IP destination, and the destination port equal to the source port.
  - ii) Syslog message: %ASA-2-**106017**: Deny IP due to Land Attack from IP_address to IP_address
- c) Non-IP packet received in routed mode:
  - i) Condition: The appliance receives a packet which is not IPv4, IPv6 or ARP and the appliance/context is configured for routed mode.
  - ii) Syslog messages:
    - (1) %ASA-6-**106026**: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol
    - (2) %ASA-4-**106027**:Failed to determine the security context for the packet:vlansource Vlan#:ethertype src sourceMAC dst destMAC
- d) ICMP Inspect seq num not matched:
  - i) Condition: The sequence number in the ICMP echo reply message does not match any ICMP echo message that passed across the appliance earlier on the same connection.
  - ii) Syslog message: %ASA-4-**313004**:Denied ICMP type=icmp_type, from source_address on interface interface_name to dest_address:no matching session
- e) ICMP Error Inspect and ICMPv6 Error Inspect
  - i) ICMP condition: ICMP error packets were dropped by the ASA because the ICMP error messages are not related to any session already established in the ASA.
  - ii) ICMPv6 condition: The appliance is not able to find any established connection related to the frame embedded in the ICMPv6 error message.
  - iii) Syslog message: %ASA-4-**313005**: No matching connection for ICMP error message: icmp_msg_info on interface_name interface. Original IP payload: embedded_frame_info icmp_msg_info = icmp src src_interface_name:src_address [([idfw_user | FQDN_string], sg_info)] dst dest_interface_name:dest_address [([idfw_user | FQDN_string], sg_info)] (type icmp_type, code icmp_code) embedded_frame_info = prot src source_address/source_port [([idfw_user | FQDN_string], sg_info)] dst dest_address/dest_port [(idfw_user|FQDN_string), sg_info]
- f) ICMP Inspect bad icmp code:
  - i) Condition: An ICMP echo request/reply packet was received with a malformed code(non-zero).
  - ii) Syslog message: %ASA-4-**313009**: Denied invalid ICMP code icmp-code, for src-ifc:src-address/src-port (mapped-src-address/mapped-src-port) to dest-ifc:dest-address/dest-port (mapped-dest-address/mapped-dest-port) [user], ICMP id icmp-id, ICMP type icmp-type
- g) Invalid TCP header length
  - i) Condition: A header length in TCP was incorrect. Some operating systems do not handle TCP resets (RSTs) correctly when responding to a connection request to a disabled socket.
  - ii) syslog message: %ASA-5-**500003**: Bad TCP hdr length (hdrlen=bytes, pktlen=bytes) from source_address/source_port to dest_address/dest_port, flags: tcp_flags, on interface interface_name

Table 7: Messages Enabled by "ip audit" Alarms

Number	**Title**	**Type**	**Description**
400000	IP options-Bad Option List	Informational	Triggers on receipt of an IP datagram where the list of IP options in the IP datagram header is incomplete or malformed. The IP options list contains one or more options

			that perform various network management or debugging tasks.
400001	**IP options-Record Packet Route**	**Informational**	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 7 (Record Packet Route).
400002	IP options-Timestamp	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 4 (Timestamp).
400003	IP options-Security	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 2 (Security options).
400004	**IP options-Loose Source Route**	**Informational**	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 3 (Loose Source Route).
400005	IP options-SATNET ID	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 8 (SATNET stream identifier).
400006	**IP options-Strict Source Route**	**Informational**	Triggers on receipt of an IP datagram in which the IP option list for the datagram includes option 2 (Strict Source Routing).
400007	**IP Fragment Attack**	**Attack**	Triggers when any IP datagram is received with an offset value less than 5 but greater than 0 indicated in the offset field.
400008	IP Impossible Packet	Attack	Triggers when an IP packet arrives with source equal to destination address. This signature will catch the so-called Land Attack.
400009	**IP Overlapping Fragments (Teardrop)**	**Attack**	Triggers when two fragments contained within the same IP datagram have offsets that indicate that they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments, which is how the Teardrop attack works to create a DoS.
400010	ICMP Echo Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 0 (Echo Reply).
400011	ICMP Host Unreachable	Informational	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable).

400012	ICMP Source Quench	Informational	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench).
400013	ICMP Redirect	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect).
400014	ICMP Echo Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request).
400015	ICMP Time Exceeded for a Datagram	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 11(Time Exceeded for a Datagram).
400016	ICMP Parameter Problem on Datagram	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 (Parameter Problem on Datagram).
400017	ICMP Timestamp Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13 (Timestamp Request).
400018	ICMP Timestamp Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 14 (Timestamp Reply).
400019	ICMP Information Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 15 (Information Request).
400020	ICMP Information Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 16 (ICMP Information Reply).
400021	ICMP Address Mask Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17 (Address Mask Request).
400022	ICMP Address Mask Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18 (Address Mask Reply).
400023	**Fragmented ICMP Traffic**	**Attack**	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and either the more fragments flag is set to 1 (ICMP) or there is an offset indicated in the offset field.

400024	Large ICMP Traffic	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP) and the IP length > 1024.
400025	**Ping of Death Attack**	**Attack**	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP), the Last Fragment bit is set, and (IP offset * 8) + (IP data length) > 65535 that is to say, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8 byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
400026	TCP NULL flags	Attack	Triggers when a single TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host.
400027	TCP SYN+FIN flags	Attack	Triggers when a single TCP packet with the SYN and FIN flags are set and is sent to a specific host.
400028	TCP FIN only flags	Attack	Triggers when a single orphaned TCP FIN packet is sent to a privileged port (having port number less than 1024) on a specific host.
400029	FTP Improper Address Specified	Informational	Triggers if a port command is issued with an address that is not the same as the requesting host.
400030	FTP Improper Port Specified	Informational	Triggers if a port command is issued with a data port specified that is <1024 or >65535.
400031	UDP Bomb attack	Attack	Triggers when the UDP length specified is less than the IP length specified. This malformed packet type is associated with a denial of service attempt.
400032	UDP Snork attack	Attack	Triggers when a UDP packet with a source port of either 135, 7, or 19 and a destination port of 135 is detected.
400033	UDP Chargen DoS attack	Attack	This signature triggers when a UDP packet is detected with a source port of 7 and a destination port of 19.
400034	DNS HINFO Request	Informational	Triggers on an attempt to access HINFO records from a DNS server.
400035	DNS Zone Transfer	Informational	Triggers on normal DNS zone transfers, in which the source port is 53.
400036	DNS Zone Transfer from High Port	Informational	Triggers on an illegitimate DNS zone transfer, in which the source port is not equal to 53.
400037	DNS Request for All Records	Informational	Triggers on a DNS request for all records.

400038	RPC Port Registration	Informational	Triggers when attempts are made to register new RPC services on a target host.
400039	RPC Port Unregistration	Informational	Triggers when attempts are made to unregister existing RPC services on a target host.
400040	RPC Dump	Informational	Triggers when an RPC dump request is issued to a target host.
400041	Proxied RPC Request	Attack	Triggers when a proxied RPC request is sent to the portmapper of a target host.
400042	ypserv (YP server daemon) Portmap Request	Informational	Triggers when a request is made to theportmapper for the YP server daemon (ypserv) port.
400043	ypbind (YP bind daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP bind daemon (ypbind) port.
400044	yppasswdd (YP password daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP password daemon (yppasswdd) port.
400045	ypupdated (YP update daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP update daemon (ypupdated) port.
400046	ypxfrd (YP transfer daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP transfer daemon (ypxfrd) port.
400047	mountd (mount daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the mount daemon (mountd) port.
400048	rexd (remote execution daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the remote execution daemon (rexd) port.
400049	rexd (remote execution daemon) Attempt	Informational	Triggers when a call to the rexd program is made. The remote execution daemon is the server responsible for remote program execution. This may be indicative of an attempt to gain unauthorized access to system resources.
400050	statd Buffer Overflow	Attack	Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources.

Logging and Log Messages

Monitoring activity in the log files is an important aspect of your network security and should be conducted regularly. Monitoring the log files lets you take appropriate and timely action when you detect security breaches or events that are likely to lead to a security breach in the future. Logging messages generated by the ASA can output to various destinations including the 'console' (which will include any connected CLI session, including SSH sessions), the local logging 'buffer' (which is a local circular log file with default size of 4KB that overwrites oldest messages when the log is full), and a logging 'host' (which is a remote syslog server). Logging to each of those destinations can be enabled or disabled independently, and each destination can be configured to receive a different set of log messages based on syslog severity level, or a 'logging list" if one has been configured. Thus, the local logging buffer will not necessarily contain the same messages that are sent to a remote syslog server.

Use the **show logging** command to view messages in the local logging buffer, or use an external syslog server to view log messages. See online document *Cisco ASA Series Syslog Messages* for information on sending messages, and archiving. For more information, refer to the "Logging" chapter of the *CLI Book 1* or *ASDM Book 1*, the "General Operations" guides.

Timestamps in Audit Messages

By default, all audit records are not stamped with the time and date, which are generated from the system clock when an event occurs. The certified security appliance requires that the timestamp option is enabled. To enable the timestamp of audit events, use the **logging timestamp** command. To ensure that the timestamp option remains the default, use the **write memory** command to save the option to the startup configuration.

```
hostname(config)# logging timestamp
```

Note: The ASA can be configured to use NTP to synchronize its clock with a reliable time source. NTP is transmitted in clear text (unencrypted) with limited (MD5) authentication functionality. The certified configuration does **not** require NTP to be transmitted through an encrypted channel, but the ASA does support that option by allowing NTP to be transmitted/received through an IPSec tunnel.

Usernames in Audit Messages

When configuring the ASA to audit commands entered by administrators, ensure that actual usernames are written into audit messages instead of generic usernames (such as "enable_15") by following the following procedures.

Require use of usernames (and passwords) to authentication to all administrative interfaces (serial, ssh, and ASDM) by configuring "aaa authentication" for each type of interface. For more detail, refer to section, "Configure Authentication on the ASA" elsewhere in this document.

```
hostname(config)# aaa authentication serial console {LOCAL | server_group [LOCAL]}

hostname(config)# aaa authentication ssh console {LOCAL | server_group [LOCAL]}

hostname(config)# aaa authentication http console {LOCAL | server_group [LOCAL]}
```

Instead of creating an "enable password" for any privilege level, require administrators to re-enter their own password to access the higher privilege level (up to their highest authorized privilege level) using the following command.

```
hostname(config)# aaa authentication enable console {LOCAL | server_group [LOCAL]}
```

Using TCP Syslog to Detect Syslog Host Down

By default, auditing events are transported to the remote syslog server over UDP. The certified security appliance requires auditing events to be transported over TCP. The TCP option is configured using the **logging host** interface *ip_address* **tcp**/*port_number* command. With TCP logging configured, new sessions through the certified security appliance will be disallowed if log messages cannot be forwarded to the remote host.

If using the “no-logging-permit-hostdown” feature to stop the flow of traffic across the ASA when the connection to syslog server(s) is down, the use of TCP syslog is required. By default, auditing events are transported to remote syslog servers over UDP. To ensure that audit events are reliably delivered to the remote syslog server the TCP option should be employed. The **logging host** <ip-address> tcp/<port-number> command is used to achieve this.

If the network cable is accidently disconnected, for TLS connection, just reconnect the cable and the reliable nature of TCP will restore the connection.

Timely Notification/Transmission of ACL Logging

When using the “log” keyword at the end of ACL entries to log denied packets, there’s a default delay between the time the packet is denied and when the resulting syslog message is generated. The default interval for generation of syslog messages for packets denied by ACLs is 300 seconds (five minutes). Valid values are from 1 to 3600 seconds. To modify the time interval between these messages, use the “**access-list alert-interval**” command in global configuration mode. To return to the default settings, use the **no** form of this command.

hostname(config)# **access-list alert-interval** *secs*

Secure Transmission of Audit Messages

To ensure audit messages are transmitted securely from the ASA to the remote syslog server, configure the connection to each syslog host to use IPsec or TLS to encrypt syslog messages as the messages leave the ASA.

Note: On the Firepower 4100 and 9300 platforms, ASA and FXOS generate separate syslog messages and each transmit their messages separately to remote syslog servers over their own secure channels, which do not interfere with each other. FXOS will always secure syslog in IPsec, while ASA can be configured to transmit syslog via TLS, or IPsec or both (TLS over IPsec).

Configure Reference Identifier:

Note: Use **crypto ca certificate map** to define certificate matching rules for IPsec tunnels. Use **crypto ca reference-identity** to define certificate matching rules for TLS connections.

To configure a reference-identity object, use the **crypto ca reference-identity** command in configuration mode. To delete a reference-identity object, use the **no** form of this command.

crypto ca reference-identity *reference_identity_name*

no crypto ca reference-identity *reference_identity_name*

Enter the **crypto ca reference-identity** command in global configuration mode to place the ASA in ca-reference-identity mode. Enter the following reference-ids while in ca-reference-identity mode. Multiple reference-ids of any type may be added. Use the no form of each command to remove reference-ids.

[**no**] **cn-id** *value*

[**no**] **dns-id** *value*

[**no**] **srv-id** *value*

[**no**] **uri-id** *value*

Syntax Description

reference-identity-name	Name of the reference-identity object.
value	Value of each reference-id.

cn-id	Common Name (CN), where the value matches the overall form of a domain name. The CN value cannot be free text. A CN-ID reference identifier does not identify an application service.
dns-id	A subjectAltName entry of type dNSName. This is a DNS domain name. A DNS-ID reference identifier does not identify an application service.
srv-id	A subjectAltName entry of type otherName whose name form is SRVName as defined in RFC 4985. A SRV-ID identifier may contain both a domain name and an application service type. For example, a SRV-ID of "_imaps.example.net" would be split into a DNS domain name portion of "example.net" and an application service type portion of "imaps."
uri-id	A subjectAltName entry of type uniformResourceIdentifier whose value includes both (i) a "scheme" and (ii) a "host" component (or its equivalent) that matches the "reg-name" rule specified in RFC 3986. A URI-ID identifier must contain the DNS domain name, not the IP address, and not just the hostname. For example, a URI-ID of "sip:voice.example.edu" would be split into a DNS domain name portion of "voice.example.edu" and an application service type of "sip."

Reference identities and objects have no default behavior or values.

A reference identity is created when configuring one with a previously unused name. Once a reference identity has been created, the four identifier types and their associated values can be added or deleted from the reference identity.

When multiple entries are used, the following behavior is expected if the certificate contains at least one instance of srv-id, uri-id, or dns-id:

- If any instance of uri-id in the certificate matches any instance of uri-id on the named reference id, then the certificate matches the reference identity.
- If any instance of srv-id in the certificate matches any instance of srv-id on the named reference id, then the certificate matches the reference identity.
- If any instance of dns-id in the certificate matches any instance of dns-id on the named reference id, then the certificate matches the reference identity.
- If none of these scenarios exist, the certificate does not match the reference identity.

When multiple entries are used, the following behavior is expected if the certificate does not contain at least one instance of srv-id, uri-id, or dns-id but does contain at least one cn-id:

- If any instance of cn-id in the certificate matches any instance of cn-id on the named reference id, then the certificate matches the reference identity. Otherwise, the certificate does not match the reference identity.
- If the certificate does not contain at least one instance of srv-id, uri-id, dns-id, or cn-id, then the certificate does not match the reference identity.

When the ASA is acting as a TLS client, it supports rules for verification of an application server's identity as defined in RFC 6125. Reference identities are configured on the ASA, to be compared to the identity presented in a server certificate during connection establishment. These identifiers are specific instances of the four identifier types also specified in RFC 6125.

The reference identifiers **cn-id** and **dns-id** MAY NOT contain information identifying the application service and MUST contain information identifying the DNS domain name.

The following example creates a reference-identity for a syslog server:

```
hostname(config)# crypto ca reference-identity syslogServer
hostname(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
hostname(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

Securing Syslog with TLS:

To transmit the messages using TLS, add the "secure" keyword to the "logging host" command, e.g.:

```
hostname(config)# logging host interface_name syslog_ip [tcp/port | udp/port] [format emblem] [secure  [reference-identity
reference_identity_name]] [permit-hostdown]
```

Specifying the reference-identity keyword enables RFC 6125 checks and identifies the reference identity to use by name. The reference identity must already existIssuing this command without the reference-identity keyword disables RFC 6125 server certificate validation for this syslog server and is the default.

An example of the use of this command for enabling RFC 6125 checks with an existing reference identity for a syslog server:

```
hostname(config)# logging host outside 10.86.93.123 tcp/6514 secure reference-identity syslogServer
```

Configure TLS on the ASA as described in the "*Secure Communications*" section of this document.

This outbound TLS connection from the ASA to the syslog server is not related to any TLS VPN configuration, but instead uses TLS functionality similar to what's used for ASDM – though the outbound connection to the syslog server uses the TLS client on ASA whereas the inbound connection from ASDM uses the TLS server of the ASA.

Verifying the Syslog Server's Certificate

When syslog over TCP is enabled on the ASA the ASA can verify the syslog server's identity using the server's public certificate, though the syslog server may not attempt to validate the ASA's (TLS client's) certificate.

To view the installed CA and server certificates:

```
hostname# show crypto ca trustpool
```

To import CA or server certificates, do one or more of the following:

a) Install the default set of root CA certificates to the ASA:

```
hostname(config)# crypto ca trustpool import default
```

a) Install the certificate of a non-default CA server to the ASA: Example…

```
hostname# copy https://some-CA.com/some-CA-cert.p7b disk0:
hostname(config)# crypto ca trustpool import url disk0:/some-CA-cert.p7b
```

a) Install the syslog server's public certificate to the ASA: Example…

```
hostname# copy https://some-SERVER.com/some-SERVER-cert.p7b disk0:
hostname(config)# crypto ca trustpool import url disk0:/some-SERVER-cert.p7b
```

Configuring the Syslog Server

Configure TLS on the remote syslog server in a manner consistent with the TLS configuration on the ASA, including ensuring the remote TLS server supports at least one of the TLS ciphersuites listed in the "*Secure Communications*" section of this document.

Known compatible syslog servers include Kiwi Syslog Server release 9.2 or later; or syslog-ng release 2.0 or later. Only one syslog server is required.

- Kiwi Syslog Server software, installation instructions and guidance can be obtained from: http://www.kiwisyslog.com/
- Syslog-ng software, installation instructions and guidance can be obtained from: http://www.balabit.com/network-security/syslog-ng

Install the syslog server per installation instructions provided with the syslog server software. Configure the host operating system to restrict access to syslog data to authorized personnel only. Configure the system to accept inbound syslog over TLS from the IP address of the ASA using the IP address of the ASA's interface that would be used to transmit packets to the server (refer to the ASA's routing table using "**show route**").

To install a server certificate on syslog server (necessary when the syslog server is running on separate host from the CA server), follow below steps:

1. Request certificate from Certification Authority (CA), specifying "Server Authentication Certificate" as certificate purpose.
2. Copy the certificate to host where the syslog server is installed.
3. Install the certificate on syslog server host. For example, if the syslog server is running on Microsoft Windows, use the Microsoft Management Console (MMC):
    a. Start > Run > [type] mmc [Enter] > [Inside MMC Console] File > Add/Remove Snap-in > Add > Certificate > Add > Computer account > Next > Local computer > Finish > Close > OK
    b. Expand Certificates > Personal folder > Certificates (Local Computer) right click > All tasks > Import > Specify path to browse for file and import it to Personal folder.
4. In the syslog server software select that certificate as the one to use for the secure TCP connection.

Securing Syslog with IPsec

To transmit the messages using IPsec, configure a crypto map to encrypt outbound syslog traffic (UDP syslog or TCP syslog) with IPsec.

Configure IPsec on the ASA as described in the "Secure Communications" section of this document.

Configure IPsec on the remote IPsec peer by following guidance for that remote system, and configuring the IPsec parameters to be consistent with those configured on the ASA for connection to that peer.

Securing RADIUS Accounting Messages with IPsec

To transmit the RADIUS messages using IPsec, configure a crypto map to encrypt outbound RADIUS traffic with IPsec.

Configure IPsec as described in the "*Secure Communications*" section of this document.

Configure IPsec on the remote IPsec peer by following guidance for that remote system, and configuring the IPsec parameters to be consistent with those configured on the ASA for connection to that peer.

Auditable Events Certified Under Common Criteria

The following list shows how to enable logging of the auditable event types required during the Common Criteria evaluation, though it's not required to enable any auditing in the certified configuration.

When auditing is configured as described above with "**logging timestamp**" enabled, all audit messages will include at least the following details: Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Some of the audit events in the table below will include additional detail consistent with the Common Criteria certification requirements, such as an IP address or username.

To enable logging for all configured output locations, use the **logging enable** command in global configuration mode. To disable logging, use the **no** form of this command.

Syntax: hostname(config)# **logging enable**

To define a list of events as a logging list, use the logging list command.

Syntax: hostname(config)# **logging list** *name* {**level** *level* [**class** *event_class*] | **message** *start_id*[-*end_id*]}

To send any these log messages to a syslog server, use the "logging host" command as described above to configure the connection to the syslog server, and use the "logging trap" to set a syslog severity level or define a list of messages to be send to logging hosts.

Syntax: hostname(config)# **logging trap** [*logging_list* | *level*]

To store messages in the local logging buffer, use the "logging buffer" command. When used with the external audit server configuration, generated audit event is simultaneously sent to the external server and the local logging buffer.

Syntax: hostname(config)# **logging buffered** [*logging_list* | *level*]

To change the local logging buffer size, use the "logging buffer-size" command. The default buffer size is 4 KB.

Syntax: hostname(config)# **logging buffer-size** *bytes*

1) Miscellaneous Events

a) Auditable Event: Start-up and shutdown of the audit functions

i) Additional message details: *No additional information.*

ii) Configuration required for generating the syslog messages:

(1) Enable logging with severity level 5 (includes the "logging enable" and "no logging enable" commands), or with a logging list including the message ID(s) below.

iii) Syslog messages:

(1) At startup:

(a) %ASA-5-111008: User '*username*' executed the 'logging enable' command.

(2) At shutdown:

(a) %ASA-5-111008: User '*username*' executed the 'no logging enable' command.

b) Auditable Event: Changes to TSF configuration.

i) Additional message details: *No additional information.*

ii) Configuration required for generating the syslog messages:

(1) Enable logging with severity level 5 (includes the "logging enable" and "no logging enable" commands), or with a logging list including the message ID(s) below.

iii) Syslog messages:

(a) %ASA-5-111008: User user executed the command string

(i) The string will show the commands that address any configuration change (e.g., adding and removing trusted root certificates, adding firewall rules)

(b) %ASA-7-111009:User *user* executed cmd:*string*

(i) This audit applies to any command that does not modify configuration (i.e., show commands).

c) Auditable Event: Changes to the login banner.

i) Additional message details:

(1) The username

ii) Configuration required for generating the syslog messages:

(1) Enable logging with severity level 5

iii) Syslog messages:

(a) %ASA-5-111008: User '*username*' executed the 'banner login *string*' command.

(b) %ASA-5-111008: User '*username*' executed the 'banner asdm *string*' command.

Note: All commands entered and executed will be logged with %ASA-5-111008. This covers all administrative actions as noted below.

d) Auditable Event: Discontinuous changes to time
   i) Additional message details: *No additional information.*
   ii) Configuration required for generating the syslog messages:
      (1) Enable logging with severity level 5 (includes the "logging enable" and "no logging enable" commands), or with a logging list including the message ID(s) below.
   iii) Syslog messages:

%ASA-5-771001: CLOCK: System clock set, source: Manual, before: 14:37:17.992 EDT Tue May 14 2024, after: 11:11:11.000 EST Sat Nov 11 2000

e) Auditable Event: Initiation of software updates

Note: ASA running on Firepower 4100 and 9300 is not updated via ASA CLI or ASDM as with ASA running on other platforms. On these platforms all ASA installations and upgrades are managed via the FXOS (via CLI or Firepower Chassis Manager). For further information, refer to "Image Management" section of the *Cisco FXOS 2.14 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration*.

2) Identification, Authentication, and Authorization

a) Auditable Event: All administrative actions
   i) Additional message details: Login IDs (usernames).
   ii) Configuration required for generating the syslog messages:
      (1) Use the "**aaa authentication**" commands as described in the "Usernames in Audit Messages" section of this guide.
      (2) Enable logging with severity level 5 (for non-show commands) or 7 (for show commands), or with a logging list including the message ID(s) below.
   iii) Syslog messages:
      (1) %ASA-5-111008: User '*username*' executed the '*string*' command.
      (2) %ASA-7-111009: User '*username*' executed cmd:'*string*'
      (3) %ASA-5-111010: User '*username*', running '*CLI*' from IP *ip-address*, executed '*string*'

b) Auditable Event: All use of the identification and authentication mechanism.
   i) Additional message details: Provided user identity, origin of the attempt (e.g., IP address).
   ii) Configuration required for generating the syslog messages:
      (1) Enable logging with severity level 4, 5, or 6, or with a logging list including the message ID(s) below.
   iii) Syslog messages:
      (1) %ASA-5-502103: User priv level changed: Uname: user From: privilege_level To: privilege_level
      (2) %ASA-6-605004: Login denied from source-address/source-port to interface:destination/service for user "username[8]"
      (3) %ASA-6-605005: Login permitted from source-address/source-port to interface:destination/service for user "username"
      (4) %ASA-6-605005: Login permitted from serial to console for user "admin"
      (5) %ASA-6-611101: User authentication succeeded: IP, IP address: Uname: user
      (6) %ASA-6-611102: User authentication failed: IP, IP address: Uname: user

c) Auditable Event: Any attempts at unlocking of an interactive session.
   i) Additional message details: *No additional information.*
   ii) Configuration required for generating the syslog messages:
      (1) Not applicable. The administrative sessions do not support session locking.
   iii) Syslog messages:

[8] In a failed login attempt, the presumed username will be shown as "*****". This is intended to prevent user from accidentally entering their password in the username field and having it logged.

(1) None.

d) Auditable Event: The termination of a remote SSH session due to inactivity.

i) Additional message details: *No additional information.*

ii) Configuration required for generating the syslog messages:

(1) Enable logging with severity level 4, or with a logging list including the message ID(s) below.

iii) Syslog messages:

(1) %ASA-6-315011:: Group = group, Username = username, IP = peer_address, Session disconnected. Session Type: type, Duration: duration, Reason: reason

(a) Where 'reason' = "Time-out activated"

e) Auditable Event: The termination of a remote ASDM session (cookie) due to inactivity.

i) Additional message details: *No additional information.*

ii) Configuration required for generating the syslog messages:

(1) ASDM uses a series of short-lived HTTPS sessions for each active ASDM client. These temporary HTTPS sessions process session TLS negotiation parameters, as well as reading and updating the ASA configuration. Following initial TLS session negotiation and password-based authentication, a cookie is used to authenticate the subsequent actions initiated from the ASDM client. The cookie expires when either http server timeout expires, "http server idle-timeout" or "http server session-timeout". Thus, the most specific messages to use to track termination of an authenticated ASDM 'session' are those that show expiration of the cookie, and those are debug messages.

(2) Warnings about performance impact:

(a) Generating the audit messages to indicate when cookies expire requires enabling debug messages, which can have an impact on performance.

(b) Enabling "debug http" can generate a large number of debug messages, which can quickly fill the local buffer. To avoid filling the local logging buffer with debug messages do not configure "logging buffered debug", or increase the size of the local logging buffer using the "logging buffer-size" command.

(c) Transmitting debug messages to a syslog server can generate a relatively large amount of syslog messages

(d) Due to the impact on performance, the "debug http" is not persistent in the configuration so the CLI session must remain open for the 711001 messages to be generated.

(3) To generate the correct debug message, enable "debug http" at least to level 16, for example:

(a) hostname# debug http 16

(4) To redirect debugging messages to logs as syslog message 711001 issued at severity level 7, use the "logging debug-trace" command in global configuration mode. Example:

(a) hostname(config)# logging debug-trace [persistent]

(5) Prior to entering enabling "logging debug-trace" all debug messages that were enabled with the "debug" command would be output to the active CLI sessions. Once the "logging debug-trace" command has been added to the running configuration, the following informational message will be output to the active CLI session:

(a) INFO: 'logging debug-trace' is enabled. All debug messages are currently being redirected to syslog:711001 and will not appear in any monitor session.

iii) Syslog messages:

(1) %ASA-7-711001: HTTP: Session: <ID> (user) is expired. Deleted.

f) Auditable Event: The termination of an interactive session.

i) Additional message details: *No additional information.*

ii) Configuration required for generating the syslog messages:

(1) Enable logging with severity level 5, or with a logging list including the message ID(s) below.

iii) Syslog messages:

(1) %ASA-5-611103: User logged out: Uname: user

(2) %ASA-5-611104: Serial console idle timeout exceeded

g) Auditable Event: Unsuccessful login attempts limit is met or exceeded.

i) Additional message details: Origin of the attempt (e.g., IP address).

ii) Configuration required for generating the syslog messages:

(1) Set the login failure limit using: aaa local authentication attempts max-fail [limit]

iii) Syslog messages (two messages would be seen together, providing all the required audit details, where message 113006 indicates the failed number of login attempts has been reached, and 605004 includes the origin of the login attempt:

(1) %ASA-6-611102:User authentication failed from *source-address*, user *username*

(2) %ASA-6-605004: Login denied from source-address/source-port to interface:destination/service for user “username[9]”

h) <u>Auditable Event: All use of the identification and authentication mechanism.</u>

i) Successful login via console (“ttyS0” = console):

```
%FPRM-6-AUDIT: [session][internal][creation][internal][126610][sys/user-ext/sh-login-
USERNAME-ttyS0_1_12542][id:ttyS0_1_12542, name:USERNAME, policyOwner:local][] Fabric A:
local user USERNAME logged in from console
```

ii) Failed login via console (“null” = console):

```
%AUTHPRIV-5-SYSTEM_MSG: FAILED LOGIN 1 FROM (null) FOR USERNAME, Authentication
failure - login
```

iii) Successful login via SSH (“pts” = SSH):

```
%FPRM-6-AUDIT: [session][internal][creation][internal][126614][sys/user-ext/sh-login-
USERNAME-pts_0_1_13390][id:pts_0_1_13390, name:USERNAME, policyOwner:local][] Fabric A:
local user USERNAME logged in from IP-ADDRESS
```

iv) Failed login via SSH:

```
%DAEMON-6-SYSTEM_MSG: Failed none for USERNAME from IP-ADDRESS port 49224 ssh2 -
sshd[13284]
```

v) Successful login via WebUI (“web” = WebUI):

```
%FPRM-6-AUDIT: [session][internal][creation][internal][126605][sys/user-ext/web-login-
USERNAME-web_55167_A][id:web_55167_A, name: USERNAME, policyOwner:local][] Web A:
local user USERNAME logged in from IP-ADDRESS
```

vi) Failed login via WebUI:

```
%USER-6-SYSTEM_MSG: [ssl:info] [pid 31244:tid 1892854672] [client IP-ADDRESS:58079]
AH01964: Connection to child 58 established (server IP-ADDRESS:443) - httpd[31244]
```

(1) %USER-6-SYSTEM_MSG: authentication failed for USERNAME - httpd[31244]

3) <u>SSH inbound for remote administration</u>

a) <u>Auditable Event: Initiation and establishment of an SSH session.</u>

i) Additional message details:

(1) Identification of the initiator and target of failed trusted channels establishment attempt.

ii) Configuration required for generating the syslog messages:

(1) Enable logging with severity level 7, or with a logging list including the message ID(s) below.

iii) Syslog messages:

(1) %ASA-6-302013: Built inbound TCP connection <num> for mgmt: source_address/source_port to identity: dest_address/service

(2) %ASA-6-605005: Login permitted from *source-address* /*source-port* to *interface:destination* /*service* for user “*username* ”

b) <u>Auditable Event: Termination of an SSH session</u>

[9] In a failed login attempt, the presumed username will be shown as “*****”. This is intended to prevent user from accidentally entering their password in the username field and having it logged.

i) Additional message details:
(1) Remote endpoint of connection (IP address).
ii) Configuration required for generating the syslog messages:
(1) Enable logging with severity level 6, or with a logging list including the message ID(s) below.
iii) Syslog messages:
(1) %ASA-6-315011: SSH session from *IP_address* on interface mgmt. for user *user* terminated normally

c) Auditable Event: Failure to establish an SSH session
i) Additional message details:
(1) Remote endpoint of connection (IP address).
(2) Reason for failure to establish.
ii) Configuration required for generating the syslog messages:
(1) Enable logging with severity level 6, or with a logging list including the message ID(s) below.
iii) Syslog messages:
(1) %ASA-6-315011: SSH session from IP_address on interface interface_name for user user disconnected by SSH server, reason: reason

4) TLS/HTTPS inbound for remote administration

a) Auditable Event: Initiation and establishment of a TLS/HTTPS session.
i) Additional message details:
(1) Identification of the initiator and target of failed trusted channels establishment attempt.
(2) Identification of the claimed user identity.
ii) Configuration required for generating the syslog messages:
(1) Enable logging with severity level 6 or 7, or with a logging list including the message ID(s) below.
iii) Syslog messages:
(1) %ASA-7-710001: TCP access requested from source_address/source_port to interface_name:dest_address/service
(2) %ASA-7-710002: {TCP|UDP} access permitted from source_address/source_port to interface_name:dest_address/service%ASA-6-725001 Starting SSL handshake with remote_device interface_name: IP_address/port for SSL_version session.
(3)
(4) %ASA-6-725002 Device completed SSL handshake with remote_device interface_name: IP_address/port
(5) %ASA-6-725003 SSL client interface_name: IP_address/port request to resume previous session.

b) Auditable Event: Termination of a TLS/HTTPS session.
i) Additional message details:
(1) Remote endpoint of connection (IP address).
ii) Configuration required for generating the syslog messages:
(1) Enable logging with severity level 6, or with a logging list including the message ID(s) below.
iii) Syslog messages:
(1) %ASA-6-725007 SSL session with remote_device interface_name: IP_address/port terminated.

c) Auditable Event: Failure to establish a TLS/HTTPS session.
i) Additional message details:
(1) Remote endpoint of connection (IP address).
(2) Reason for failure to establish.
ii) Configuration required for generating the syslog messages:
(1) Enable logging with severity level 7, or with a logging list including the message ID(s) below.
(2) To redirect debugging messages to logs as syslog message, use the "logging debug-trace" command in global configuration mode.
iii) Syslog messages:
(1) %ASA-6-725001: Starting SSL handshake with peer-type interface: src-ip/src-port to dst-ip/dst-port for protocol session

Follow by 725011, 725014, and 711001

(2) %ASA-7-725011: Cipher[order number]: cipher_name

(3) %ASA-7-725014: SSL lib error. Function: routine_name Reason: reason_string

The following is a specific example of this general audit:

(a) %ASA-7-725014: SSL lib error. Function: SSL3_GET_CLIENT_HELLO Reason: no shared cipher

(4) %ASA-7-711001: error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher@s3_srvr.c:2023

Follow by 302014 and 609002 both of which include "duration 0:00:00"

(5) %ASA-6-302014: Teardown TCP connection id for interface: real-address/real-port [(idfw_user)] to real-address/real-port [(idfw_user)] duration 0:00:00 bytes bytes [reaon] [(user)]

(7) %ASA-7-609002: Teardown local-host zone-name/*:ip-address duration time

5) IPsec for secure transmission of Syslog, RADIUS, or other protocols

a) Auditable Event: Initiation and establishment of an IPsec SA.

i) Additional message details:

(1) Identification of the initiator and target of failed trusted channels establishment attempt.

ii) Configuration required for generating the syslog messages:

(1) Enable logging with severity level 5, 6, or 7, or with a logging list including the message ID(s) below.

(2) To capture the contents of packet during IPsec establishment, enter the following commands:

(a) debug crypto ikev2 protocol 255

(b) logging debug-trace [persistent]

iii) Syslog messages:

(1) %ASA-6-302015: Built inbound UDP connection 198 for outside:192.168.144.254/4500 (192.168.144.254/4500) to identity:192.168.144.208/4500 (192.168.144.208/4500)

(2) %ASA-5-750006: Local:192.168.144.208:4500 Remote:192.168.144.254:4500 Username:192.168.144.254 IKEv2 SA UP. Reason: New Connection Established

(3) %ASA-6-602303: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been created.

b) Auditable Event: Termination of an IPsec SA.

i) Additional message details:

(1) Remote endpoint of connection (IP address)

ii) Configuration required for generating the syslog messages:

(1) Enable logging with severity level 3, 5, or 6, or with a logging list including the message ID(s) below.

iii) Syslog messages:

(1) %ASA-6-602304: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been deleted.

(2) %ASA-5-713050: Connection terminated for peer IP_address. Reason: termination reason Remote Proxy IP_address, Local Proxy IP_address

(a) Where reasons include: IPsec SA Idle Timeout ; IPsec SA Max Time Exceeded ; Administrator Reset ; Administrator Reboot ; Administrator Shutdown ; Session Disconnected ; Session Error Terminated ; Peer Terminate

(3) %ASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive_type)

c) Auditable Event: Failure to establish an IPsec SA.

i) Additional message details:

(1) Remote endpoint of connection (IP address).

(2) Reason for failure to establish.

ii) Configuration required for generating the syslog messages:

(1) Enable logging with severity level 3, 4, or 6, or with a logging list including the message ID(s) below.

iii) Syslog messages:

(1) *%ASA-5-750002: Local:local IP :local port Remote: remote IP : remote port Username: username Received a IKE_INIT_SA request*

(2) *%ASA-4-750003: Local: local IP:local port Remote: remote IP:remote port Username: username Negotiation aborted due to ERROR: error*

(3) %ASA-7-711001: debug_trace_msg

(a) Note: The debug trace message is only generated when the “logging debug-trace” command is enabled.

(b) Where message details can include:

(i) IKEv2-PROTO-1: … Failed to find a matching policy

(ii) IKEv2-PROTO-2: … Verification of peer's authentication data FAILED

d) VPN Audit Flooding –**Error Message %ASA-4-733100: *Object* drop rate *rate_ID* exceeded. Current burst rate is *rate_val* per second, max configured rate is *rate_val* ; Current average rate is *rate_val* per second, max configured rate is *rate_val* ; Cumulative total count is *total_cnt***. The specified object in the message has exceeded the specified burst threshold rate or average threshold rate. The object can be a drop activity of a host, TCP/UDP port, IP protocol, or various drops caused by potential attacks. The TOE may be under attack.

- *Object* —The general or particular source of a drop rate count, which might include the following:

  - Firewall
  - Bad pkts
  - Rate limit
  - DoS attck
  - ACL drop
  - Conn limit
  - ICMP attk
  - Scanning
  - SYN attck
  - Inspect
  - Interface

(A citation of a particular interface object might take a number of forms. For example, you might see 80/HTTP, which would signify port 80, with the well-known protocol HTTP.)

- *rate_ID* —The configured rate that is being exceeded. Most objects can be configured with up to three different rates for different intervals.
- *rate_val* —A particular rate value.
- *total_cnt* —The total count since the object was created or cleared.

The following three examples show how these variables occur:

- For an interface drop caused by a CPU or bus limitation:

%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per second, max configured rate is 8000; Current average rate is 2030 per second, max configured rate is 2000; Cumulative total count is 3930654.”

- For a scanning drop caused by potential attacks:

%ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per second_max configured rate is 10; Current average rate is 245 per second_max configured rate is 5; Cumulative total count is 147409 (35 instances received)

- For bad packets caused by potential attacks:

%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per second, max configured rate is 400; Current average rate is 760 per second, max configured rate is 100; Cumulative total count is 1938933

- Because of the scanning rate configured and the threat-detection rate scanning-rate 3600 average-rate 15 command:

%ASA-4-733100: [144.60.88.2] drop rate-2 exceeded. Current burst rate is 0 per second, max configured rate is 8; Current average rate is 5 per second, max configured rate is 4; Cumulative total count is 38086

e) **SYN Flood attacks** - burst-rate attacks_per_sec sets the threshold for syslog message generation, between 25 and 2147483647. The default is 400 per second. When the burst rate is exceeded, syslog message 733104 is generated. E.g.: **Error Message %ASA-4-733104: TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED**. The TOE is protected by the TCP intercept mechanism when it is under Syn flood attack. If the average rate for intercepted attacks exceeds the configured threshold, this message is produced. The example above is showing which server is under attack and where the attacks are coming from.

(7) average-rate attacks_per_sec sets the average rate threshold for syslog message generation, between 25 and 2147483647. The default is 200 per second. When the average rate is exceeded, syslog message 733105 is generated. E.g.: **Error Message %ASA-4-733105: TD_SYSLOG_TCP_INTERCEPT_BURST_RATE_EXCEED**. The TOE is protected by the TCP intercept mechanism when it is under Syn flood attack. If the burst rate for intercepted attacks exceeds the configured threshold, this message is produced. The message is showing which server is under attack and where the attacks are coming from.

6) X.509v3 Certificate Validation

i) Auditable Event: Unsuccessful attempt to validate a certificate

(1) Additional message details: Reason for failure

(2) Configuration required for generating the syslog messages: None.

(3) Syslog messages:

(a) %ASA-7-717029: Identified client certificate within certificate chain. serial number: *serial_number* , subject name: *subject_name* .

(b) %ASA-3-717027: Certificate chain failed validation. *reason_string*.

(c) %ASA-3-717009: Certificate validation failed. Reason: reason_string.

Additional Supporting audits include

(d) %ASA-6-717022: Certificate was successfully validated. *certificate_identifiers*

(e) %ASA-7-717025: Validating certificate chain containing *number* of certs certificate(s).

(f) %ASA-7-717030: Found a suitable trustpoint *trustpoint name* to validate certificate.

(g) %ASA-3-717032: OCSP status check failed. Reason: Failed to verify OCSP response.

(h) %ASA-3-717032: OCSP status check failed. Reason: Certificate is revoked.

(i) %ASA-6-717033: OCSP response status - Successful.

(j) %ASA-4-717035: OCSP status is being checked for certificate. *certificate_identifier*.

(k) %ASA-6-717056: Attempting *type* revocation check from *Src Interface* :*Src IP /Src Port* to *Dst IP /Dst Port* using *protocol*

7) CA Establishment

i) %ASA-6-717056: Attempting type revocation check from Src Interface:Src IP/Src Port to Dst IP/Dst Port using protocol[10]

ii) ASA’s PKI module makes various different connections to the CA servers like revocation checking using HTTP, LDAP and OCSP etc. To be common criteria certified, all of these exchanges will be logged as debug traces under “debug crypto ca message 5”

It will have HTTP headers and hex dump of the context along with the ASCII.

For LDAP and OCSP, it will dump the hex data of the request

```
CRYPTO_PKI: HTTP response header:
 HTTP/1.1 404 Not Found
Date: Wed, 30 Sep 2015 15:58:29 GMT
Server: Apache/2.2.15 (Red Hat)
Content-Length: 282
Connection: close
Content-Type: text/html; charset=iso-8859-1

3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50    |  <!DOCTYPE HTML P
55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f    |  UBLIC "-//IETF//
44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e    |  DTD HTML 2.0//EN
22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a    |  ">.<html><head>.
3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46    |  <title>404 Not F
6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68    |  ound</title>.</h
65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e    |  ead><body>.<h1>N
6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70    |  ot Found</h1>.<p
3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55    |  >The requested U
52 4c 20 2f 63 72 2e 20 77 61 73 20 6e 6f 74 20    |  RL /cr. was not
66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65    |  found on this se
72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c    |  rver.</p>.<hr>.<
61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32    |  address>Apache/2
2e 32 2e 31 35 20 28 52 65 64 20 48 61 74 29 20    |  .2.15 (Red Hat)
53 65 72 76 65 72 20 61 74 20 31 37 32 2e 31 38    |  Server at 172.18
2e 31 33 36 2e 32 31 37 20 50 6f 72 74 20 38 30    |  .136.217 Port 80
3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64    |  </address>.</bod
79 3e 3c 2f 68 74 6d 6c 3e 0a                      |  y></html>.
```

8) <u>Traffic Filtering</u>

a) <u>Auditable Event: Application of rules configured with the ‘log’ operation</u>

i) Additional message details:

(1) Source and destination addresses
(2) Source and destination ports
(3) Transport Layer Protocol
(4) Local interface

ii) Configuration required for generating the syslog messages:

(1) Enable logging with severity level 3, or with a logging list including the message ID(s) below.

[10] For more details, please review the Cisco ASA Series Syslog Messages Guide

iii) Syslog messages:
   (1) %ASA-3-710003: {TCP|UDP} access denied by ACL from source_IP/source_port to interface_name:dest_IP/service

b) <u>Auditable Event: Indication of packets dropped due to too much network traffic</u>
   i) Additional message details:
      (1) Local interface that is unable to process packets
   ii) Configuration required for generating the syslog messages:
      (1) Enable logging with severity level 3, or with a logging list including the message ID(s) below.
   iii) Syslog messages:
      (1) TCP and UDP connections:
         (a) %ASA-3-201002: Too many TCP connections on {static|xlate} global_address! econns nconns
         (b) %ASA-3-201004: Too many UDP connections on {static|xlate} global_address!udp connections limit
         (c) %ASA-3-201005: FTP data connection failed for IP_address IP_address
         (d) %ASA-3-201010: Embryonic connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name
         (e) %ASA-3-202011: Connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name
      (2) IP connections and address translations
         (a) %ASA-2-201003: Embryonic limit exceeded nconns/elimit for outside_address/outside_port (global_address) inside_address/inside_port on interface interface_name
         (b) %ASA-3-201011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.
         (c) %ASA-3-202010: [NAT | PAT] pool exhausted for pool-name, port range [1-511 | 512-1023 | 1024-65535]. Unable to create protocol connection from in-interface:src-ip/src-port to out-interface:dst-ip/dst-port

c) <u>Auditable Event: FTP Connection</u>
   i) Additional message details:
      (1) *src_ifc* —The interface where the client resides.
      (2) *src_ip* —The IP address of the client.
      (3) *src_port* —The client port.
      (4) *dst_ifc* —The interface where the server resides.
      (5) *dst_ip* —The IP address of the FTP server.
      (6) *dst_port* —The server port.
      (7) *username* —The FTP username.
      (8) *action* —The stored or retrieved actions.
      (9) *filename* —The file stored or retrieved.
   ii) Syslog messages:
      (1) <u>%ASA-6-303002: FTP connection from *src_ifc* : *src_ip* / *src_port* to *dst_ifc* : *dst_ip* / *dst_port*, user *username action* file *filename*</u>

ASA Installation

Before installing ASA on the 4100 and 9300 platforms, read the Quick Start Guide (*Cisco ASA for Firepower 4100 Quick Start Guide*, or *Cisco ASA for Firepower 9300 Quick Start Guide*).

Note: The ASA software image running on the ASA hardware cannot be updated/patched, it can only be replaced, requiring reboot to a different software image. There are no means to support self-updating of ASA software.

Note: ASA running on Firepower 4100 and 9300 is not updated via ASA CLI or ASDM as with ASA running on other platforms. On these platforms all ASA installations and upgrades are managed via the FXOS (via CLI or Firepower

Chassis Manager). For further information, refer to “Image Management” section of the *Cisco FXOS 2.14 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration*.

Verification of Image and Hardware

To verify that the security appliance software and hardware was not tampered with during delivery, perform the following steps:

Step 1: Before unpacking the security appliance, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment, Cisco Systems or an authorized Cisco distributor/partner.

Step 2: Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3: Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems barcoded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4: Note the serial number of the security appliance on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the security appliance. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5: Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6: Once the security appliance is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. Also, verify the hardware received is the correct TOE model. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 7: Download a Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. To access this site, you must be a registered user and you must be logged in. Software images are available from Cisco.com at: https://software.cisco.com/

Step 8: Download the ***cisco-asa.9.20.3.SPA.csp*** file from Cisco Connection Online (CCO) to a local server or workstation. https://software.cisco.com/download/navigator.html

Optional: Once the file is downloaded, verify that it was not tampered with by using an MD5 or SHA512 utility to compute an MD5 or SHA512 checksum for the downloaded file and compare this with the checksum for the image as listed on https://software.cisco.com/. If the checksums do not match, contact Cisco TAC.

Note: This hash is intended as a verification of the download accuracy. The image verification that occurs in step 8 was not evaluated and authenticates the image as being provided by Cisco.

Step 9: To copy the image that was downloaded from the web to the Firepower 4100 or 9300, follow instructions in the “Image Management” section of the *Cisco FXOS 2.14 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration*. Once the ASA image has been loaded to the Firepower 4100 or 9300, follow instructions in the “Deploy the ASA” section of the Quick Start Guide (*Cisco ASA for Firepower 4100 Quick Start Guide*, or *Cisco ASA for Firepower 9300 Quick Start Guide*).

Step 10: After loading the ASA image to the Firepower appliance the ASA image is automatically verified. The integrity can be optionally re-verified by FXOS prior to deploying the ASA by using via the Firepower Chassis Manager WebUI by navigating to System, then Updates, then clicking "Check Image Integrity" button next to the ASA image. After the ASA has been deployed and started, the ASA can optionally re-verify the integrity of the ASA binary image, that's part of the CCO image downloaded from Cisco.com, use the "verify" command in order to verify the digital signature. The digital signature uses 2048-bit RSA with SHA-512. Note that the *.csp image that's deployed by FXOS (e.g. via Firepower Chassis Manager) is extracted to multiple files during ASA deployment, thus the *.csp file does not appear in the ASA filesystem. To verify the binary ASA image, verify the "asa-restapi", or to verify the ASDM image, verify the asdm*.bin file, both of which are stored in the "disk0:" filesystem, for example:

```
verify disk0:/asa-restapi
or
verify disk0:/asdm-7202.bin
```

If the image verification fails, the system will not boot into operational mode. If the update succeeds, the system will boot to the new image.

Step 11: To display the version number via the ASA CLI, use the **show version** command as follows. Verify that the version is 9.20(3). If the security appliance image fails to load, or if the security appliance version is not 9.20(3), contact Cisco TAC.

The following is sample output from the **show version** command output, displaying the security appliance version:

```
hostname# show version

Cisco Adaptive Security Appliance Software Version 9.20(3)

Firepower Extensible Operating System Version 2.14(1.167)

Device Manager Version 7.20(2)

<truncated output>
```

Note: If the ASA module is being updated from the FXOS CLI, the command to display the ASA version number will be 'show app-instance'. Additionally, to view the loaded image versions on the TOE from the FXOS CLI, the 'show app' command can be used. This will also query which image version is currently the default boot option and running.

Once the ASA image has been copied onto the Firepower chassis, the installation will NOT occur without administrator initiation. The 'show version' or 'show app-instance' commands will not display the new image version at this step; this must be viewed using the 'verify' command specified previously.

Adaptive Security Device Manager (ASDM)

To use ASDM, you need to enable the HTTPS server, and allow HTTPS connections to the adaptive security appliance. All of these tasks are completed if you use the setup command. This section describes how to manually configure ASDM access and how to login to ASDM.

The security appliance allows a maximum of 5 concurrent ASDM instances per context, if available, with a maximum of 32 ASDM instances between all contexts.

Enabling HTTPS Access

To configure ASDM access, follow these steps:

Step 1: To identify the IP addresses from which the adaptive security appliance accepts HTTPS connections, enter the following command for each address or subnet:

```
hostname(config)# http source_IP_address mask source_interface
```

Step 2: To enable the HTTPS server, enter the following command:

```
hostname(config)# http server enable [port]
```

By default, the port is 443. If you change the port number, be sure to include the new port in the ASDM access URL. For example, if you change it to port 444, that port number would be specified in the browser with the following syntax:

https://10.1.1.1:444

Step 3: To specify the location of the ASDM image, enter the following command:

```
hostname(config)# asdm image disk0:/asdmfile
```

For example, to enable the HTTPS server and let a host on the inside interface with an address of 192.168.1.2 access ASDM, enter the following commands:

```
hostname(config)# crypto key generate rsa modulus 2048 # use modulus size 2048 or greater

hostname(config)# write mem

hostname(config)# http server enable

hostname(config)# http 192.168.1.2 255.255.255.255 inside
```

To allow all users on the 192.168.3.0 network to access ASDM on the inside interface, enter the following command:

```
hostname(config)# http 192.168.3.0 255.255.255.0 inside
```

Configure DN matching for ASDM

To configure a certificate map that will be evaluated for the certificate received, the certificate map will be referenced by the name. The map will match if any of the entries in it match. Within each entry, there may be multiple attributes and they all have to match for that entry to pass. This feature is optional.

Syntax: **http authentication-certificate** *interface_name* [**match** *certificate_map_name*]

Example:

```
hostname(config)# http authentication-certificate inside match ?

configure mode commands/options:

 WORD  < 65 char           Certificate map label
```

Enable Idle-Timeouts of ASDM Sessions

Enable automatic session locking for ASDM sessions after a period of inactivity using the following commands:

```
hostname(config)# http server idle-timeout {minutes 1-1440}

hostname(config)# aaa authentication http console
```

Accessing ASDM from Your Workstation

From a supported web browser on the adaptive security appliance network, enter the following URL:

https://*interface_ip_address[:port]*

With the factory default configuration, clients on the 192.168.1.0/24 inside network can access ASDM. To allow other clients to access ASDM see the “Configuring Device Access for ASDM, Telnet, or SSH" section below.

For more information, see *ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, 7.16*.

Running ASDM

The web page that loads when connecting to https://interface_ip_address[:port] displays buttons to:

- Run ASDM
- Install ASDM Launcher
- Run Startup Wizard

To maintain the ASA in its certified configuration, do not use “Install ASDM Launcher” and if a copy of ASDM Launcher has already been installed to your workstation, do not use it. Always use the “Run ASDM” option, which will load the ASDM software directly from the ASA.

Note: If you are using the Factory Default Configuration, you do not need a username or password. Leave these fields blank to login to ASDM.

Network Services and Protocols

The table below lists the network services/protocols available on the ASA as a client (initiated outbound) and/or server (listening for inbound connections), all of which run as system-level processes. The table indicates whether each service or protocol is allowed to be used in the certified configuration.

For more detail about each service, including whether the service is limited by firewall mode (routed or transparent), or by context (single, multiple, system), refer to *Firewall CLI* guide, or the *Firewall ASDM* guide *(CLI Book 2)*.

Table 8: Network Services and Protocols

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
AH	Authentication Header (part of IPsec)	Yes	Yes	Yes	Yes	No restrictions. ESP must be used in all IPsec connections. Use of AH in addition to ESP is optional.
DHCP	Dynamic Host Configuration Protocol	Yes	Yes	Yes	Yes	No restrictions.
DNS	Domain Name Service	Yes	Yes	No	**n/a**	No restrictions.
ESP	Encapsulating Security Payload (part of IPsec)	Yes	Yes	Yes	Yes	Configure ESP as described in the "*Secure Communications*" section of this document.
FTP	File Transfer Protocol	Yes	**No**	No	n/a	Use SCP or HTTPS instead.
HTTP	Hypertext Transfer Protocol	Yes	For OCSP or copy	Yes	**No**	Used implicitly for OCSP. For other HTTP functions, such as "copy", recommend using HTTPS instead, or tunneling through IPsec.
HTTPS	Hypertext Transfer Protocol Secure	Yes	Yes	Yes	Yes	No restrictions.
ICMP	Internet Control Message Protocol	Yes	Yes	Yes	Yes	No restrictions.

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
IKE	Internet Key Exchange	Yes	Yes	Yes	Yes	As described in the "*Secure Communications*" section of this document.
IMAP4S	Internet Message Access Protocol Secure version 4	Yes	Over TLS	No	n/a	No restrictions.
IPsec	Internet Protocol Security (suite of protocols including IKE, ESP and AH)	Yes	Yes	Yes	Yes	Only use for securing traffic to/from the ASA itself, not for "VPN Gateway" (securing traffic through the ASA). See IKE and ESP for other usage restrictions.
Kerberos	A ticket-based authentication protocol	Yes	Over IPsec	No	n/a	If used for authentication of ASA administrators, tunnel this authentication protocol secure with TLS or IPsec.
LDAP	Lightweight Directory Access Protocol	Yes	**No**	No	n/a	No, ASA's support for LDAP-over-IPsec was not evaluated for use in the Common Criteria certified configuration.
LDAP-over-SSL	LDAP over Secure Sockets Layer	Yes	**No**	No	n/a	No, ASA's support for LDAP-over-TLS was not evaluated for use in the Common Criteria certified configuration.
NT	NT domain authentication	Yes	Over IPsec	No	n/a	If used for authentication of ASA administrators, secure through TLS or IPsec.
NTP	Network Time Protocol	Yes	Yes	No	n/a	Any configuration. Use of key-based authentication is recommended.
POP3S	Post Office Protocol version 3 over TLS	Yes	Over TLS	No	n/a	Configure TLS as described in section "*Secure Communications*" of this document.
RADIUS	Remote Authentication Dial In User Service	Yes	Yes	No	n/a	If used for authentication of ASA administrators, secure through TLS or IPsec.
SCP	Secure Copy (over SSH)	No	n/a	Yes	**No**	Must remain disabled as describe in section "*Secure Communications*".
SDI (RSA SecureID)	RSA SecurID authentication	Yes	Over IPsec	No	n/a	If used for authentication of ASA administrators, secure through TLS or IPsec.

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
SMTP	Simple Mail Transfer Protocol	Yes	Yes	No	n/a	Recommended to use SMTPS instead.
SMTPS	SMTP over TLS	Yes	Over TLS	No	n/a	Configure TLS as described in section "*Secure Communications*" of this document.
SNMP	Simple Network Management Protocol	Yes (snmp-trap)	Yes	Yes	**No**	Outbound (traps) only. Recommended to tunnel through IPsec.
SSH	Secure Shell	Yes	Yes	Yes	Yes	As described in the "*Secure Communications*" section of this document.
SSL (not TLS)	Secure Sockets Layer	Yes	**No**	Yes	**No**	Use TLS instead.
TACACS+	Terminal Access Controller Access-Control System Plus	Yes	Yes	No	n/a	If used for authentication of ASA administrators, secure through TLS or IPsec.
Telnet	A protocol used for terminal emulation	Yes	**No**	Yes	**No**	Use SSH instead.
TLS	Transport Layer Security	Yes	Yes	Yes	Yes	As described in the "*Secure Communications*" section of this document.
TFTP	Trivial File Transfer Protocol	Yes	Yes	No	n/a	Recommend using SCP or HTTPS instead, or tunneling through IPsec.

The table above does not include the types of protocols and services listed here:

- OSI Layer 2 protocols such as CDP, VLAN protocols like 802.11q, Ethernet encapsulation protocols like PPPoE, etc. The certified configuration places no restrictions on the use of these protocols; however evaluation of these protocols was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.
- Routing protocols such as EIGRP, OSPF, and RIP. The certified configuration places no restrictions on the use of these protocols; however evaluation of these protocols was beyond the scope of the Common Criteria product evaluation, so follow best practices for the secure usage of these protocols.
- Protocol inspection engines that can be enabled with "inspect" commands because inspection engines are used for filtering traffic, not for initiating or terminating sessions, so they're not considered network 'services' or 'processes' in the context of this table. The certified configuration places no restrictions on the use protocol inspection functionality; however evaluation of this functionality was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.
- Network protocols that can be proxied through/by the ASA. Proxying of services by the ASA does not result in running said service on the ASA in any way that would allow the ASA itself to be remotely accessible via that service, nor does it allow the ASA to initiate a connection to a remote server

independent of the remote client that has initiated the connection. The certified configuration places no restrictions on enabling of proxy functionality; however the evaluation of this functionality was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.

Modes of Operation

The ASA has the following modes of operation:

Booting – While booting, the ASA does not support authentication via any CLI, (console or SSH), nor GUI (e.g. ASDM), but the ASA does display a running list of status updates to the serial console port so a locally connected user can view the boot process activity. While in this mode, the ASA is starting processes and applications and running Power-On Self-Tests (POST) including testing of cryptographic modules and software integrity to ensure proper operation of the ASA before it progresses to a normal mode of operation. This boot process automatically progresses to the Normal mode of operation as long as no errors are detected during POST. If errors are detected, the ASA will halt, and depending on the error may automatically re-initiate the booting process.

Normal – In this mode the ASA processes, applications, and network services are fully operational such that the ASA implements the previously stored configuration to support (as configured) authentication though CLI and GUI, traffic forwarding and blocking, auditing of events, etc.

Shutdown – This mode is triggered through use of the "**reload**" command with optional command parameters.

By default, the **reload** command is interactive. The ASA first checks whether the configuration has been modified but not saved. If so, the ASA prompts the administrator to save the configuration. In multiple context mode, the ASA prompts for each context with an unsaved configuration. If the **save-config** parameter was specified, the configuration is saved without prompting. The ASA then prompts for confirmation before reloading the system. Only a response of **y** or pressing the **Enter** key causes a reload. Upon confirmation, the ASA starts or schedules the reload process, depending upon whether a delay parameter (**in** or **at**) was specified.

By default, the reload process operates in "graceful" (also known as "nice") mode. All registered subsystems are notified when a reboot is about to occur, allowing these subsystems to shut down properly before the reboot. To avoid waiting until for such a shutdown to occur, specify the **max-hold-time** parameter to specify a maximum time to wait. Alternatively, use the **quick** parameter to force the reload process to begin abruptly, without notifying the affected subsystems or waiting for a graceful shutdown.

To force the **reload** command to operate non-interactively, specify the **noconfirm** parameter. In this case, the ASA does not check for an unsaved configuration unless you have specified the **save-config** parameter. The ASA does not prompt for confirmation before rebooting the system. It starts or schedules the reload process immediately, unless a delay parameter has been specified, an in accordance with any **max-hold-time** or **quick** parameters specified.

Using **reload cancel** will cancel a scheduled reload, but a reload that is already in progress cannot be cancelled.

Note Configuration changes that are not written to the flash partition are lost after a reload. Before rebooting, enter the **write memory** command to store the current configuration in the flash partition.

Self-Testing:

Following operational error, the ASA reboots (once power supply is available) and enters booting mode. The only exception to this is if there is an error during the Power on Startup Test (POST) during bootup, then the ASA will shut down. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen, and saved in the crashinfo file, which can be viewed via the CLI with the "**show crashinfo console**" command unless the "**crashinfo console disable**" command has been applied. Within the POST, self-tests for the cryptographic operations are performed. The same cryptographic POSTs can also be run on-demand using the "**fips self-test poweron**" command. Entering this command causes the device to run all self-tests required for FIPS 140-2 compliance. Tests include the cryptographic algorithm test, software integrity test, and critical functions test.
If the self-tests fail, for example the software was tampered with or the FIPS known answer tests (KATs) did not produce the expected results, the following actions should be taken:

- If possible, review the crashinfo file. This will provide additional information on the cause of the crash

- Restart the ASA to perform POST and determine if normal operation can be resumed
- If the problem persists, contact Cisco Technical Assistance via http://www.cisco.com/techsupport or 1 800 553-2447
- If necessary, return the ASA to Cisco under guidance of Cisco Technical Assistance.

To ensure the DRNG functions with a high degree of reliability and robustness, validation features have been included that operate in an ongoing manner and at system startup. These include the DRNG Online Health Tests (OHTs) that are run in an ongoing manner (continuously), and Built-In Self Tests (BISTs) that are run at startup.

Online Health Tests (OHTs) are designed to measure the quality of entropy generated by the ES using both per sample and sliding window statistical tests in hardware. Per sample tests compare bit patterns against expected pattern arrival distributions as specified by a mathematical model of the ES. An ES sample that fails this test is marked "unhealthy." Using this distinction, the conditioner can ensure that at least two healthy samples are mixed into each seed. This defends against hardware attacks that might seek to reduce the entropic content of the ES output. Sliding window tests look at sample health across many samples to verify they remain above a required threshold. The sliding window size is large (65536 bits) and mechanisms ensure that the ES is operating correctly overall before it issues random numbers. In the rare event that the DRNG fails during runtime, it would cease to issue random numbers rather than issue poor quality random numbers. The entropy source and extraction algorithms are designed to comply with SP800-90B.

Built-In Self Tests (BISTs) are designed to verify the health of the ES prior to making the DRNG available to software. These include Entropy Source Tests (ES-BIST) that are statistical in nature and comprehensive test coverage of all the DRNG’s deterministic downstream logic through BIST Known Answer Tests (KAT-BIST).

When ASA is booting, the output to the console indicates when FIPS self-tests are being run, and the result of self-testing. Output to the console during boot will include:

```
INFO: Power-On Self-Test in process.

.....................................

INFO: Power-On Self-Test complete.
```

Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Appendix:

Acronyms & Abbreviations

Table 9: Acronyms and Abbreviations

Acronyms or Abbreviation	**Meaning**
AAA	Authentication, Authorization, Auditing
ACL	Access Control List
AIP	Advanced Inspection and Prevention
AIC	Alarm Interface Controller
ARP	Address Resolution Protocol
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
CA	Certificate Authority
CLI	Command Line Interface
DHCP	Dynamic Host Control Protocol
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GHz	Gigahertz
ICMP	Internet Control Message Protocol
IP	Internet Protocol
MD	Message Digest
MHz	Megahertz
NTP	Network Time Protocol
OS	Operating System
RADIUS	Remote Authentication Dial-In User Service
RPF	Reverse Path Forwarding
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
syslog	system log
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transport Control Protocol

TTL	Time-to-Live
UDP	User Datagram Protocol
VPN	Virtual Private Network

Obtaining Documentation

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at: *http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html*

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

To find an HTML or PDF version of many Cisco titles go to *www.cisco.com*. Type the title in the 'Search' field and click **Go**.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL: *http://www.cisco.com/techsupport*

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL: *http://tools.cisco.com/RPF/register/register.do*

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the Tools & Resources link under Documentation & Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL: *http://www.cisco.com/techsupport/servicerequest*

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227) EMEA: +32 2 704 55 55USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1) – Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2) – Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3) – Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4) – You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html