



# Cisco ASA with FirePOWER Services

## Security Target

---

**ST Version 1.0**

**January 8, 2018**



**Americas Headquarters:**

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

© 2018 Cisco Systems, Inc. This document can be reproduced in full without any modifications.

## Table of Contents

1	SECURITY TARGET INTRODUCTION .....	9
1.1	ST and TOE Reference .....	9
1.2	TOE Overview .....	9
1.2.1	TOE Product Type .....	10
1.2.2	Supported non-TOE Hardware/ Software/ Firmware .....	11
1.3	TOE DESCRIPTION .....	12
1.4	TOE Evaluated Configuration .....	16
1.5	Physical Scope of the TOE .....	17
1.6	Logical Scope of the TOE .....	18
1.6.1	Security Audit .....	19
1.6.2	Cryptographic Support .....	19
1.6.3	Full Residual Information Protection .....	19
1.6.4	Identification and authentication .....	19
1.6.5	Security Management .....	20
1.6.6	Protection of the TSF .....	20
1.6.7	TOE Access .....	20
1.6.8	Trusted path/Channels .....	21
1.6.9	Filtering .....	21
1.6.10	Intrusion Prevention System .....	22
1.7	Excluded Functionality .....	22
2	Conformance Claims .....	24
2.1	Common Criteria Conformance Claim .....	24
2.2	Protection Profile Conformance .....	24
2.2.1	Protection Profile Additions or Modifications .....	25
2.3	Protection Profile Conformance Claim Rationale .....	25
2.3.1	TOE Appropriateness .....	25
2.3.2	TOE Security Problem Definition Consistency .....	25
2.3.3	Statement of Security Requirements Consistency .....	25
3	SECURITY PROBLEM DEFINITION .....	26

3.1	Assumptions.....	26
3.2	Threats.....	27
3.3	Organizational Security Policies.....	33
4	SECURITY OBJECTIVES.....	34
4.1	Security Objectives for the TOE.....	34
4.2	Security Objectives for the Environment.....	37
5	SECURITY REQUIREMENTS .....	38
5.1	Conventions .....	38
5.2	TOE Security Functional Requirements .....	38
5.3	SFRs Drawn from FWcPP .....	40
5.3.1	Security audit (FAU).....	40
5.3.2	Cryptographic Support (FCS).....	43
5.3.3	User data protection (FDP) .....	50
5.3.4	Identification and authentication (FIA) .....	51
5.3.5	Security management (FMT).....	53
5.3.6	Protection of the TSF (FPT) .....	54
5.3.7	TOE Access (FTA) .....	55
5.3.8	Trusted Path/Channels (FTP).....	56
5.3.9	Stateful Traffic Filtering (FFW) .....	56
5.4	SFRs from the VPNGWcEP .....	59
5.4.1	Cryptographic Support (FCS).....	59
5.4.2	Identification and authentication (FIA) .....	60
5.4.3	Security management (FMT).....	61
5.4.4	Packeting Filtering (FPF).....	61
5.4.5	Protection of the TSF (FPT) .....	62
5.4.6	TOE Access (FTA) .....	62
5.5	SFRs from the IPScEP .....	63
5.5.1	Security Audit (FAU) .....	63
5.5.2	Security management (FMT).....	65
5.5.3	Intrusion Prevention (IPS) .....	66
5.5.4	Protection of the TSF (FPT) .....	70
5.6	TOE SFR Dependencies Rationale for SFRs Found in FWcPP .....	70

5.7	Security Assurance Requirements .....	70
5.7.1	SAR Requirements.....	70
5.7.2	Security Assurance Requirements Rationale .....	70
5.8	Assurance Measures.....	71
6	TOE Summary Specification .....	72
6.1	TOE Security Functional Requirement Measures .....	72
7	Supplemental TOE Summary Specification Information.....	120
7.1	Tracking of Stateful Firewall Connections .....	120
7.1.1	Establishment and Maintenance of Stateful Connections.....	120
7.1.2	Viewing Connections and Connection States .....	120
7.1.3	Examples .....	124
7.2	Intrusion Rule Definition .....	126
7.2.1	Intrusion Rule Header .....	126
7.2.2	Intrusion Rule Options and Keywords.....	127
7.3	Key Zeroization .....	128
8	Annex A: References .....	133

## List of Tables

TABLE 1 ACRONYMS.....	6
TABLE 2: ST AND TOE IDENTIFICATION .....	9
TABLE 3: IT ENVIRONMENT COMPONENTS.....	11
TABLE 4: ASA 5500 SERIES AND FMC HARDWARE .....	14
TABLE 5 HARDWARE MODELS AND SPECIFICATIONS .....	17
TABLE 6: EXCLUDED FUNCTIONALITY .....	22
TABLE 7: PROTECTION PROFILES.....	24
TABLE 8 TOE ASSUMPTIONS .....	26
TABLE 9 THREATS.....	27
TABLE 10 ORGANIZATIONAL SECURITY POLICIES.....	33
TABLE 11 SECURITY OBJECTIVES FOR THE TOE .....	34
TABLE 12 SECURITY OBJECTIVES FOR THE ENVIRONMENT.....	37
TABLE 13 SECURITY FUNCTIONAL REQUIREMENTS.....	38
TABLE 14 AUDITABLE EVENTS.....	41
TABLE 15 AUDITABLE EVENTS.....	63
TABLE 16: ASSURANCE MEASURES.....	70
TABLE 17: ASSURANCE MEASURES.....	71
TABLE 18: HOW TOE SFRs ARE SATISFIED .....	72
TABLE 19: CAVP ALGORITHMS .....	79
TABLE 20: SYNTAX DESCRIPTION .....	120
TABLE 21: CONNECTION STATE TYPES.....	121
TABLE 22: CONNECTION STATE FLAGS.....	122
TABLE 23: TCP CONNECTION DIRECTIONALITY FLAGS .....	124
TABLE 24: ASA KEY ZEROIZATION .....	128
TABLE 25: FP SERVICES KEY ZEROIZATION .....	130
TABLE 26: REFERENCES .....	133

## List of Figures

FIGURE 1: ASA 5500 SERIES HARDWARE.....	12
FIGURE 2: EXAMPLE TOE DEPLOYMENT .....	16
FIGURE 3: ASA AND FIREPOWER TRAFFIC FLOW.....	17
FIGURE 4: AUDIT VIEW .....	75

FIGURE 5: SYSLOG VIEW .....	75
FIGURE 6: AUTHENTICATION PROCESS .....	88

## List of Acronyms

The following acronyms and abbreviations are common and may be used in this Security Target:

**Table 1 Acronyms**

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
ASDM	Adaptive Security Device Manager
CC	Common Criteria
CEM	Common Evaluation Methodology
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WAN Interface Card
ESP	Encapsulating Security Payload
Gbps	Gigabits per second
GE	Gigabit Ethernet port
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IT	Information Technology
NDcPP	Network Device Collaborative Protection Profile
OS	Operating System
PoE	Power over Ethernet
POP3	Post Office Protocol
PP	Protection Profile
SA	Security Association
SFP	Small-form-factor pluggable port
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SSHv2	Secure Shell (version 2)
SSM	Security Services Module
SSP	Security Services Processor
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

Acronyms / Abbreviations	Definition
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WIC	WAN Interface Card

## DOCUMENT INTRODUCTION

Prepared By:

Cisco Systems, Inc.  
170 West Tasman Dr.  
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Adaptive Security Appliances (ASA) with FirePOWER Services. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, authorized administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.



# 1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- ◆ Security Target Introduction [Section 1]
- ◆ Conformance Claims [Section 2]
- ◆ Security Problem Definition [Section 3]
- ◆ Security Objectives [Section 4]
- ◆ IT Security Requirements [Section 5]
- ◆ TOE Summary Specification [Section 6]
- ◆ Supplemental TOE Summary Specification Information [Section 7]
- ◆ References [Section 8]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 2.

## 1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

**Table 2: ST and TOE Identification**

Name	Description
ST Title	Cisco ASA with FirePOWER Services
ST Version	1.0
Publication Date	January 8, 2018
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco ASA with FirePOWER Services Cisco FirePOWER Services on ASA
TOE Hardware Models	<ul style="list-style-type: none"> <li>• Cisco ASA 5500 Series (5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X) and (5512-X, 5515-X, 5525-X, 5545-X, 5555-X)</li> <li>• Cisco ASA 5585 Series (5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40, 5585-X SSP-60)</li> <li>• Cisco FireSIGHT<sup>1</sup> (FS750, FS1500, FS2000, FS3500, and FS4000)</li> </ul>
TOE Software Version	ASA 9.6.2 and ASDM 7.6 with FirePOWER Services 6.1
Keywords	Firewall, VPN Gateway, Router, Intrusion Prevention System

## 1.2 TOE Overview

The Cisco Adaptive Security Appliances with FirePOWER (FP) Services is a purpose-built, firewall platform with VPN and IPS capabilities. The FMC appliances provide a centralized management console and event database for the FirePOWER Services, and aggregates and correlates intrusion, discovery, and connection data from the FirePOWER Services. In this deployment, the ASA provides VPN, firewall filtering, and passes traffic to the FirePOWER

---

<sup>1</sup> Also known as the FirePOWER Management Center (FMC)

Services for discovery, intrusion detection, and access control. The TOE includes the hardware models as defined in Table 2 of section 1.1.

### 1.2.1 TOE Product Type

The TOE consists of hardware and software that provide connectivity and security services onto a single, secure device.

For firewall services, the ASA 5500-X Series (low-end to mid-range) and 5585-X Series (high-end), all provide application-aware stateful packet filtering firewalls. A stateful packet filtering firewall controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorized administrator for firewalls. This header information includes source and destination host (IP) addresses, source and destination port numbers, and the transport service application protocol (TSAP) held within the data field of the IP packet. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The stateful firewall remembers the state of the connection from information gleaned from prior packets flowing on the connection and uses it to regulate current packets. The packet will be denied if the security policy is violated.

In addition to IP header information, the TOE mediates information flows on the basis of other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface. For connection-oriented transport services, the firewall either permits connections and subsequent packets for the connection or denies the connection and subsequent packets associated with the connection.

The application-inspection capabilities automate the network to treat traffic according to detailed policies based not only on port, state, and addressing information, but also on application information buried deep within the packet header. By comparing this deep-packet inspection information with corporate policies, the firewall will allow or block certain traffic. For example, it will automatically drop application traffic attempting to gain entry to the network through an open port-even if it appears to be legitimate at the user and connection levels-if a business's corporate policy prohibits that application type from being on the network.

The TOE also provides IPsec connection capabilities. All references within this ST to “VPN” connectivity refer to the use of IPsec tunnels to secure connectivity to and/or from the TOE, for example, gateway-to-gateway<sup>2</sup> VPN or remote access VPN. Other uses refer to the use of IPsec connections to tunnel traffic that originates from or terminates at the TOE itself, such as for transmissions from the TOE to remote audit/syslog servers, or AAA servers, or for an additional layer of security for remote administration connections to the TOE, such as SSH or TLS connections tunneled in IPsec.

The TOE can operate in a number of modes: as a single standalone device, or in high-availability (HA) failover-pairs; with a single-context, or with multiple-contexts within each single/pair; as a

---

<sup>2</sup> This is also known as site-to-site or peer-to-peer VPN.

transparent firewall when deployed in single-context, or with one or more contexts connected to two or many IP subnets when configured in router mode.

For management purposes, the ASDM is included. ASDM allows the TOE to be managed from a graphical user interface. Its features include:

- TLS/HTTPS encrypted sessions.
- Rapid Configuration: in-line and drag-and-drop policy editing, auto complete, configuration wizards, appliance software upgrades, and online help;
- Powerful Diagnostics: Packet Tracer, log-policy correlation, packet capture, regular expression tester, and embedded log reference;
- Real-Time Monitoring: device, firewall, content security, real-time graphing; and tabulated metrics;
- Management Flexibility: A lightweight and secure design enables remote management of multiple security appliances.

For the Next Generation IPS (NGIPS) functionality, the FirePOWER Services (part of the TOE) provides access control, malware protection, and URL/IP filtering known as Security Intelligence. The FirePOWER Services monitors incoming and outgoing network traffic and performs real-time traffic analysis and logging using the industry-leading Snort® engine. All packets on the monitored network are scanned, decoded, preprocessed and compared against a set of rules to determine whether inappropriate traffic, such as system attacks, is being sent over the network. The system generates alerts or blocks the traffic when deviations of the expected network behavior are detected or when there is a match to a known attack pattern.

### 1.2.2 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

**Table 3: IT Environment Components**

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.
ASDM Management Platform	Yes	<p>The ASDM 7.6 operates from any of the following operating systems:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows 7, 8, Server 2008, and Server 2012</li> <li>• Apple OS X 10.4 and later</li> <li>• Red Hat Enterprise Linux 5</li> </ul> <p>Note that that ASDM software is part of the TOE and the management platform is used to connect to the TOE and run the ASDM. The only software installed on the management platform is a Cisco ASDM Launcher. ASA only.</p>
Audit (syslog)	Yes	This includes any syslog server to which the TOE would transmit syslog

Component	Required	Usage/Purpose Description for TOE performance
Server		messages. Connections to remote audit servers must be tunneled in IPsec (ASA only) or TLS.
AAA Server	No	This includes any IT environment AAA server that provides single-use authentication mechanisms. This can be any AAA server that provides single-use authentication. 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 (ASA only).
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, Cisco VPN client) that supports IPsec tunneling. Both VPN clients and VPN gateways can be considered to be remote tunnel endpoints. ASA only.
NTP Server	No	The TOE supports communications with an NTP server. Connections to remote NTP servers can optionally be tunneled in IPsec (ASA Only).

### 1.3 TOE DESCRIPTION

This section provides an overview and description of the TOE. The TOE is comprised of both software and hardware. The model is comprised of the following: ASA 5500 Series (5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X), (5512-X, 5515-X, 5525-X, 5545-X, 5555-X), (5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40, 5585-X SSP-60), and FireSIGHT (FS750, FS1500, FS2000, FS3500, and FS4000). The software is comprised of the Adaptive Security Appliance software image version 9.6.2, with ASDM 7.6 and FirePOWER Service version 6.1 (two separate binaries).

The models that comprise the TOE have common hardware characteristics. These differing characteristics affect only non-TSF relevant functionality (such as throughput, processing speed, number and type of network connections supported, number of concurrent connections supported, and amount of storage) and therefore support security equivalency of the ASAs in terms of hardware.

**Figure 1: ASA 5500 Series Hardware**





The ASA mid-range to high-end hardware components in the TOE have the following distinct characteristics:

- **5512-X** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to twelve), and 4 GB of memory.
- **5515-X** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to twelve), and 8 GB of memory.
- **5525-X** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to fourteen), and 8 GB of memory.
- **5545-X** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to fourteen), and 12 GB of memory.
- **5555-X** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to fourteen), and 16 GB of memory.
- **5585-X SSP-10** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), eight Gigabit Ethernet ports (expandable to sixteen), two 10 Gigabit Ethernet SFP+ fiber ports (expandable to four), and 12 GB of memory.
- **5585-X SSP-20** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), eight Gigabit Ethernet ports (expandable to sixteen), a two 10 Gigabit Ethernet SFP+ fiber ports (expandable to four), and 24 GB of memory.
- **5585-X SSP-40** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to twelve), a four 10 Gigabit Ethernet SFP+ fiber ports (expandable to eight), and 24 GB of memory.
- **5585-X SSP-60** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to twelve), a four 10 Gigabit Ethernet SFP+ fiber ports (expandable to eight), and 48 GB of memory.
- The same ASA image runs on all of the model platforms identified above. The same FP image runs on all the ASA platforms.

The ASA low-end hardware components in the TOE have the following distinct characteristics:

**Table 4: ASA 5500 Series and FMC Hardware**

Model	ASA 5506-X	ASA 5506W-X	ASA 5506H-X	ASA 5508-X	ASA 5516-X
<b>Number of Processors</b>	1	1	1	1	1
<b>Processor</b>	Intel Atom C2508	Intel Atom C2508	Intel Atom C2508	Intel Atom C2508	Intel Atom C2508
<b>Memory</b>	4 GB	4 GB	4 GB	8 GB	8 GB
<b>Integrated I/O</b>	8 x 1 Gigabit Ethernet (GE)	8 x 1 GE	4 x 1 GE	8 x 1 GE	8 x 1 GE
<b>Stateful inspection throughput (max)</b>	750 Mbps	750 Mbps	750 Mbps	1 Gbps	1.8 Gbps
<b>Maximum concurrent sessions</b>	20,000/50,000	20,000/50,000	50,000	100,000	250,000
<b>VLANs</b>	5 / 30	5 / 30	30	50	100
<b>Maximum Cisco AnyConnect IKEv2 remote access VPN or clientless VPN user sessions</b>	2 / 50	2 / 50	50	100	300
The same ASA image runs on all of the model platforms identified in this table.					

<b>Model</b>	<b>FS750</b>	<b>FS1500</b>	<b>FS2000</b>	<b>FS3500</b>	<b>FS4000</b>
<b>Processor</b>	Intel Xeon E3 1200 Series	Intel Xeon E5 5600 Series	Intel Xeon E5 2600 Series	Intel Xeon E5 5600 Series	Intel Xeon E5 2600 Series
<b>Maximum Number of Sensors Managed</b>	10	35	70	150	300
<b>Maximum Number of IPS Events</b>	20 Million	30 Million	60 Million	150 Million	300 Million
<b>Event Storage</b>	100 GB	125 GB	1.8 TB	400 GB	4.8 TB
<b>Maximum Flow Rate</b>	2,000 fps	6,000 fps	12,000 fps	10,000 fps	20,000 fps
<b>Maximum Network Map (hosts/users)</b>	2,000/2,000	50,000/50,000	150,000/150,000	300,000/300,000	600,000/600,000
<b>Network Interfaces</b>	2 x 1Gbps	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps
The same FirePOWER image runs on all of the model platforms identified in this table.					



**Americas Headquarters:**

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

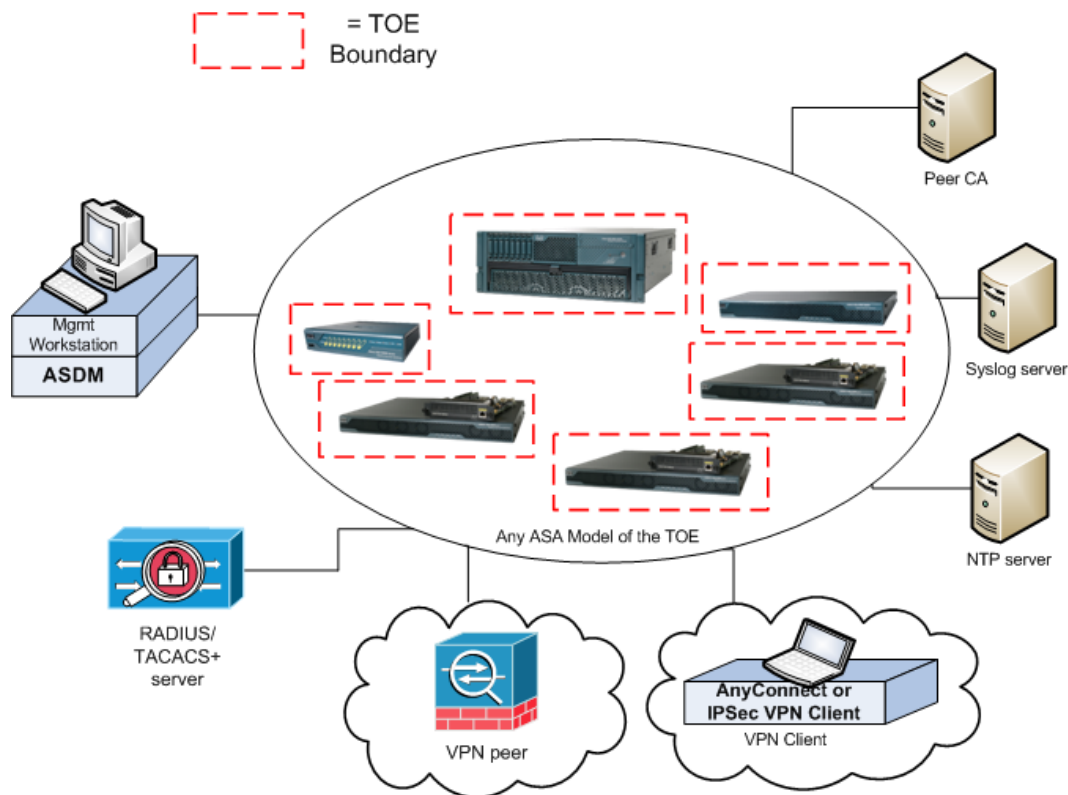
## 1.4 TOE Evaluated Configuration

The TOE consists of one or more ASA physical devices which include the Cisco ASA software, which in turn includes the ASDM software, and the FirePOWER Services software that is managed by one FMC physical device. Each instantiation of the TOE has two or more network interfaces, and is able to filter IP traffic to and through those interfaces.

The TOE can optionally connect to an NTP server for clock updates. If the TOE is to be remotely administered, the management station must connect using SSHv2 over IPsec (ASA Only). When ASDM is used a remote workstation with a TLS-enabled browser must be available. A syslog server can also be used to store audit records, and the syslog server must support syslog over TLS (ASA and FP) or IPsec (ASA only). The TOE is able to filter connections to/from these external using its IP traffic filtering, and can encrypt traffic where necessary using TLS, SSH, and/or IPsec (ASA only).

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.

**Figure 2: Example TOE Deployment**



The previous figure includes the following:

- Several examples of TOE Models



Americas Headquarters:

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

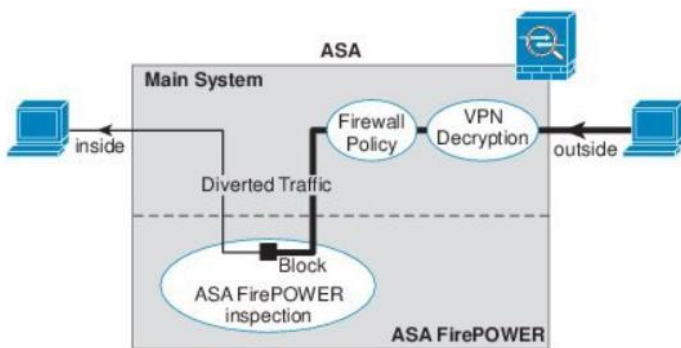


- VPN Peer (Operational Environment) or another instance of the TOE
- VPN Peer (Operational Environment) with Cisco VPN Client or AnyConnect Client
- Management Workstation (Operational Environment) with ASDM
- Remote Authentication Server (Operational Environment)
- NTP Server (Operational Environment)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

The administrator can configure the FirePOWER Services on ASA either inline or monitor-only (passive) mode. In inline mode, traffic goes through the ASA firewall checks before being forwarded to the FirePOWER Services. When the administrators identify traffic for the FirePOWER Services to inspect, traffic flows through the ASA and FP Services as follows:

1. Traffic enters the ASA.
2. Incoming VPN traffic is decrypted.
3. Firewall policies are applied.
4. Permitted traffic is sent to the FirePOWER.
5. The FirePOWER applies its security policy to the traffic, and takes appropriate actions.
6. Valid traffic is sent back to the ASA; the FirePOWER might block some traffic according to its security policy, and that traffic is not passed on.
7. Outgoing VPN traffic is encrypted.
8. Traffic exits the ASA.

**Figure 3: ASA and FirePOWER traffic Flow**







The TOE can be managed by the CLI, on-box ASDM UI and FMC appliance web UI.

## 1.5 Physical Scope of the TOE

The TOE is a hardware and software solution comprised of the components described in Table 5:

**Table 5 Hardware Models and Specifications**

TOE Configuration	Hardware Configurations	Software Version
ASA 5506-X	The Cisco ASA 5500-X Adaptive Security Appliance provides high-	ASA release 9.6.2 with FirePOWER release 6.1

<b>ASA 5506H-X</b> <b>ASA 5506W-X</b> <b>ASA 5508-X</b> <b>ASA 5516-X</b> 	performance firewall, VPN, and IPS services and 4-8 Gigabit Ethernet interfaces, and support for up to 300 VPNs.	
<b>ASA 5512-X</b> <b>ASA 5515-X</b> <b>ASA 5525-X</b> <b>ASA 5545-X</b> <b>ASA 5555-X</b> 	The Cisco ASA 5500-X Adaptive Security Appliance provides high-performance firewall, VPN, and IPS services and 6-14 Gigabit Ethernet interfaces, and support for up to 5,000 VPNs.	ASA release 9.6.2 with FirePOWER release 6.1
<b>ASA 5585-X SSP-10</b> <b>ASA 5585-X SSP-20</b> <b>ASA 5585-X SSP-40</b> <b>ASA 5585-X SSP-60</b> 	The Cisco ASA 5585 Adaptive Security Appliance provides high-performance firewall, VPN, and IPS services and 6-16 Gigabit Ethernet interfaces, 2-10 10Gigabit Ethernet interfaces, and support for up to 10,000 VPNs.	ASA release 9.6.2 with FirePOWER release 6.1
<b>FS750</b> <b>FS1500</b> <b>FS2000</b> <b>FS3500</b> <b>FS4000</b> 	The Cisco FireSIGHT Series provides centralized management console with up to 4 management interfaces, and up to 10 Gbps speed.	FirePOWER release 6.1
<b>ASDM</b>	Included on all ASA models with ASA 9.6.2	Release 7.6

## 1.6 Logical Scope of the TOE

The TOE is comprised of several security features including stateful traffic firewall and VPN gateway. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Cryptographic Support
3. Full Residual Information Protection
4. Identification and Authentication

5. Security Management
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels
9. Filtering
10. Intrusion Prevention System

These features are described in more detail in the subsections below.

### **1.6.1 Security Audit**

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are backed up over an encrypted channel to an external audit server.

### **1.6.2 Cryptographic Support**

The TOE provides cryptography in support of other TOE security functionality. The TOE provides cryptography in support of secure connections using IPsec and TLS, and remote administrative management via SSHv2 (FP Service), SSHv2 over IPsec (ASA), and TLS/HTTPS. The cryptographic random bit generators (RBGs) are seeded by an entropy noise source. Note IPsec is only supported on the ASA software, not FP Service.

### **1.6.3 Full Residual Information Protection**

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

### **1.6.4 Identification and authentication**

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the authorized administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec X509v3 certificate based authentication or pre-shared key methods.

The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI and GUI administrator interfaces. The TOE requires authorized administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE also implements a lockout mechanism if the number of configured unsuccessful threshold has been exceeded.

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH and HTTPS interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE optionally supports use of any AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE. Note SSH traffic to the ASA must be tunneled over IPsec in the evaluated configuration.

### **1.6.5 Security Management**

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 (FP Service), SSHv2 over IPsec (ASA), or TLS/HTTPS session, or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users; all identification and authentication; all audit functionality of the TOE; all TOE cryptographic functionality; the timestamps maintained by the TOE; TOE configuration file storage and retrieval, and the information flow control policies enforced by the TOE including encryption/decryption of information flows for VPNs. The TOE supports an “authorized administrator” role, which equates to any account authenticated to an administrative interface (CLI or GUI, but not VPN), and possessing sufficient privileges to perform security-relevant administrative actions.

When an administrative session is initially established, the TOE displays an administrator-configurable warning banner. This is used to provide any information deemed necessary by the administrator. After a configurable period of inactivity, administrative sessions will be terminated, requiring administrators to re-authenticate.

### **1.6.6 Protection of the TSF**

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to authorized administrators. The TOE prevents reading of cryptographic keys and passwords.

Additionally TOE is not a general-purpose operating system and access to the TOE memory space is restricted to only TOE functions.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE’s clock manually, or can configure the TOE to use NTP to synchronize the TOE’s clock with an external time source. Additionally, the TOE performs testing to verify correct operation of the appliance itself and that of the cryptographic module. Whenever any system failures occur within the TOE the TOE will cease operation.

### **1.6.7 TOE Access**

When an administrative session is initially established, the TOE displays an administrator-configurable warning banner. This is used to provide any information deemed necessary by the administrator. After a configurable period of inactivity, administrator and VPN client sessions will be terminated, requiring re-authentication. The TOE also supports direct connections from

VPN clients, and protects against threats related to those client connections. The TOE disconnects sessions that have been idle too long, and can be configured to deny sessions based on IP, time, and day, and to NAT external IPs of connecting VPN clients to internal network addresses.

### 1.6.8 Trusted path/Channels

The TOE supports establishing trusted paths between itself and remote administrators using SSHv2 for CLI access (FP Service), SSHv2 over IPsec for CLI access (ASA), and TLS/HTTPS for GUI/ASDM and web UI access on the FMC. The TOE supports use of TLS and/or IPsec for connections with remote syslog servers. The TOE can use IPsec to encrypt connections with remote authentication servers (e.g. RADIUS). The TOE can establish trusted paths of peer-to-peer VPN tunnels using IPsec, and VPN client tunnels using IPsec or TLS. Note that the VPN client is in the operational environment.

### 1.6.9 Filtering

The TOE provides stateful traffic firewall functionality including IP address-based filtering (for IPv4 and IPv6) to address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance. Address filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on source and/or destination IP addresses. Port filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (service). Stateful packet inspection is used to aid in the performance of packet flow through the TOE and to ensure that only packets are only forwarded when they're part of a properly established session. The TOE supports protocols that can spawn additional sessions in accordance with the protocol RFCs where a new connection will be implicitly permitted when properly initiated by an explicitly permitted session. The File Transfer Protocol is an example of such a protocol, where a data connection is created as needed in response to an explicitly allowed command connection. System monitoring functionality includes the ability to generate audit messages for any explicitly defined (permitted or denied) traffic flow. TOE administrators have the ability to configure permitted and denied traffic flows, including adjusting the sequence in which flow control rules will be applied, and to apply rules to any network interface of the TOE.

The TOE also provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers as well as between remote VPN clients and the TOE. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map set.

### 1.6.10 Intrusion Prevention System

The TOE provides intrusion policies consisting of rules and configurations invoked by the access control policy. The intrusion policies are the last line of defense before the traffic is allowed to its destination. All traffic permitted by the access control policy is then inspected by the designated intrusion policy. Using intrusion rules and other preprocessor settings, these policies inspect traffic for security violations and, in inline deployments, can block or alter malicious traffic.

If the vendor-provided intrusion policies do not fully address the security needs of the organization, custom policies can improve the performance of the system in the environment and can provide a focused view of the malicious traffic and policy violations occurring on the network. By creating and tuning custom policies the administrators can configure, at a very granular level, how the system processes and inspects the traffic on the network for intrusions.

Using Security Intelligence, the administrators can blacklist—deny traffic to and from—specific IP addresses, URLs, and DNS domain names, before the traffic is subjected to analysis by the access control rules. Optionally, the administrators can use a “monitor-only” setting for Security Intelligence filtering.

## 1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

**Table 6: Excluded Functionality**

Excluded Functionality	Exclusion Rationale
Telnet for management purposes	Telnet passes authentication credentials in clear text and is disabled by default.
Secure Policy Manager is excluded from the evaluated configuration	Use of Security Policy Manager is beyond the scope of this Common Criteria evaluation.
Filtering of non-IP traffic provided by the EtherType option when configuring information flow policies is excluded from the evaluated configuration	Use of non-IP traffic filtering is beyond the scope of this Common Criteria evaluation.
Smart Call Home. The Smart Call Home feature provides personalized, e-mail-based and web-based notification to customers about critical events involving their individual systems.	Use of Smart Call Home is beyond the scope of this Common Criteria evaluation.
Shell Access on FirePOWER	The shell access is only allowed for pre-operational installation, configuration, and post-operational maintenance and troubleshooting.
Timeout Exemption Option on FirePOWER	The use of the “Exempt from Browser Session Timeout” setting is not permitted. This allows a user to be exempted from the inactivity timeout feature.
REST API on FirePOWER	This feature is not evaluated as part of the

	evaluation. REST API relies on HTTPS as the underlying communication protocol and can be used to build a management interface. This feature is not tested and is out of scope.
--	--

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the Protection Profiles: Firewall collaborative Protection Profile<sup>3</sup> (FWcPP), VPN Gateway Extended Package<sup>4</sup> (VPNGWcEP), and IPS Extended Package<sup>5</sup> (IPScEP).

---

<sup>3</sup> Also known as the collaborative Protection Profile for Stateful Traffic Filter Firewalls.

<sup>4</sup> Also known as the Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway.

<sup>5</sup> Also known as the collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS).

## 2 CONFORMANCE CLAIMS

### 2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: September 2012. For a listing of Assurance Requirements claimed see section 5.7.

The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

### 2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 7 below:

Table 7: Protection Profiles

Protection Profile	Version	Date
collaborative Protection Profile for Stateful Traffic Filter Firewalls	1.0	27 February 2015
Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway	2.1	08 March 2017
collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS)	2.11	15 June 2017

The TOE and ST are conformant with the Protection Profiles as listed in Table above. The following NIAP Technical Decisions (TD) have also been applied:

- TD0125
- TD0130
- TD0143
- TD0150
- TD0151
- TD0154
- TD1055
- TD0156
- TD0165
- TD0167
- TD0179
- TD0187
- TD0189
- TD0199
- TD0209
- TD0223
- TD0226
- TD0235



### 2.2.1 Protection Profile Additions or Modifications

The following requirement was modified:

- FAU\_GEN.1 – Additional auditable events were added from the VPNGWcEP.
- FMT\_SMF.1 – Additional management functions were added to configure VPN settings from the VPNGWcEP.

## 2.3 Protection Profile Conformance Claim Rationale

### 2.3.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the:

- Firewall collaborative Protection Profile (FWcPP), VPN Gateway Extended Package (VPNGWcEP), and IPS Extended Package (IPScEP)

### 2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the FWcPP and VPNGWcEP for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in the U.S. Government Protection Profile for Security Requirements for Network Devices for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

### 2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the FWcPP, VPNGWcEP, and IPScEP for which conformance is claimed verbatim and several additional Security Functional Requirements are included as a result. All concepts covered the Protection Profile's Statement of Security Requirements are included in the Security Target. Additionally, the Security Assurance Requirements included in the Security Target are identical to the Security Assurance Requirements included in section 4.3 of the FWcPP.

### 3 SECURITY PROBLEM DEFINITION

This chapter identifies the following:

- ◆ Significant assumptions about the TOE's operational environment.
- ◆ IT related threats to the organization countered by the TOE.
- ◆ Environmental threats requiring controls to provide sufficient protection.
- ◆ Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with “assumption” specifying a unique name. Threats are identified as T.threat with “threat” specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with “osp” specifying a unique name. In addition, threats copied verbatim from the VPNGWcEP and IPScEP will have extension [VPN] and [IPS] to distinguish them from the FWcPP.

#### 3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

**Table 8 TOE Assumptions**

Assumption	Assumption Definition
<b>Reproduced from the FWcPP</b>	
A.PHYSICAL_PROTECTION	The firewall is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the firewall's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the firewall and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the firewall that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the firewall.
A.LIMITED_FUNCTIONALITY	The firewall is assumed to provide networking and filtering functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the firewall should not provide computing platform for general purpose applications (unrelated to networking/filtering functionality).
A.TRUSTED_ADMINISTRATOR	The authorized administrator(s) for the firewall are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the firewall. The firewall is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the

Assumption	Assumption Definition
	firewall.
A.REGULAR_UPDATES	The firewall firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the firewall are protected by the host platform on which they reside.
<b>Reproduced from the VPNGWcEP</b>	
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

## 3.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

**Table 9 Threats**

Threat	Threat Definition
<b>Reproduced from the FWcPP</b>	
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the firewall by nefarious means such as masquerading as an administrator to the firewall, masquerading as the firewall to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between the firewall and a network device. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the firewall and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATIONS_CHANNELS	Threat agents may attempt to target firewalls that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the firewall itself.

Threat	Threat Definition
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the firewall itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the firewall without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and firewall data enabling continued access to the firewall and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or firewall credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the firewall. Having privileged access to the firewall provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the firewall may fail during start-up or during operations causing a compromise or failure in the security functionality of the firewall, leaving the firewall susceptible to attackers.
T.NETWORK_DISCLOSURE	An attacker may attempt to “map” a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported.
T.NETWORK_ACCESS	With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services.

Threat	Threat Definition
T.NETWORK_MISUSE	An attacker may attempt to use services that are exported by machines in a way that is unintended by a site's security policies. For example, an attacker might be able to use a service to "anonymize" the attacker's machine as they mount attacks against others.
T.MALICIOUS_TRAFFIC	An attacker may attempt to send malformed packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash.
<b>Reproduced from the VPNGWcEP</b>	
T.NETWORK_DISCLOSURE[VPN]	<p>Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a <i>phishing</i> episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information.</p> <p>From an infiltration perspective, VPN gateways serve not only to limit access to only specific <i>destination</i> network addresses and ports within a protected network, but whether network traffic will be encrypted or transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific <i>source</i> addresses and ports so that specific networks or network nodes can be blocked from accessing a protected network thereby further limiting the potential disclosure of information.</p> <p>From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses and/or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing.</p>

Threat	Threat Definition
T. NETWORK_ACCESS[VPN]	<p>Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network.</p> <p>From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network.</p> <p>From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled e-mail servers, or, that access to the mail server must be done over an encrypted link.</p>

Threat	Threat Definition
T.NETWORK_MISUSE[VPN]	<p>Devices located outside the protected network, while permitted to access particular <i>public</i> services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network.</p> <p>From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services.</p> <p>From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a VPN gateway can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.</p>
T.DATA_INTEGRITY[VPN]	<p>Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can establish communications with those external devices then the data contained within the communications may be susceptible to a loss of integrity.</p>

Threat	Threat Definition
T.REPLAY_ATTACK[VPN]	<p>If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a “replay” attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions:</p> <ul style="list-style-type: none"> <li>• Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate segment of the communications to replay as well in order to cause the desired outcome.</li> <li>• No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured traffic and replay it to cause the desired outcome if the recipient has no means to detect these modifications.</li> </ul>
T.HIJACKED_SESSION[VPN]	There may be an instance where a remote client’s session is hijacked due to session activity. This could be accomplished because a user has walked away from the machine that was used to establish the session
T.UNAUTHORIZED_CONNECTION[VPN]	While a VPN client may have the necessary credentials (e.g., certificate, pre-shared key) to connect to a VPN gateway, there may be instances where the remote client, or the machine the client is operating on, has been compromised and attempts to make unauthorized connections.
T.UNPROTECTED_TRAFFIC[VPN]	A remote machine’s network traffic may be exposed to a hostile network. A user may be required to use a hostile (or unknown) network to send network traffic without being able to route the traffic appropriately.
<b>Reproduced from the IPSecP</b>	
T.NETWORK_DISCLOSURE[IPS]	Sensitive information on a protected network might be disclosed resulting from disclosure/transmitted information in violation of policy, such as sending unencrypted credit card numbers. The IPS TOE will be capable of inspecting packet payloads for data strings and patterns of characters.
T.NETWORK_ACCESS[IPS]	An attacker may attempt to gain inappropriate access to one or more networks, endpoints, or services, such as through brute force password guessing attacks, or by transmitting malicious executable code, scripts, or commands. If malicious external devices are able to communicate with devices on the protected network, then those devices may be susceptible to the unauthorized disclosure of information.



Threat	Threat Definition
T.NETWORK_MISUSE[IPS]	Access to services made available by a protected network might be used counter to Operational Environment policies. Devices located outside the protected network may attempt to conduct inappropriate activities while communicating with allowed public services, (e.g. manipulation of resident tools, SQL injection, phishing, forced resets, malicious zip files, disguised executables, privilege escalation tools, and botnets).
T.NETWORK_DOS[IPS]	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network. Resource exhaustion may occur in the event of co-ordinate service request flooding from a small number of sources. Though most IPS will provide some protection from DDoS (distributed denial of service) attacks, providing protection against DDoS attacks is not a requirement for conformant TOEs, as this is best counteracted by firewalls, cloud computing and design. Note however that DoS protection is required.

### 3.3 Organizational Security Policies

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

**Table 10 Organizational Security Policies**

Policy Name	Policy Definition
<b>Reproduced from the FWcPP</b>	
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

## 4 SECURITY OBJECTIVES

This section identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

- ◆ This document identifies objectives of the TOE as O.objective with objective specifying a unique name. Objectives that apply to the IT environment are designated as OE.objective with objective specifying a unique name.

### 4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document. . In addition, security objectives copied verbatim from the VPNGWcEP and IPScEP will have extension [VPN] and [IPS] to distinguish them from each other.

**Table 11 Security Objectives for the TOE**

TOE Objective	TOE Security Objective Definition
<b>Reproduced from the VPNGWcEP</b>	
O.CRYPTOGRAPHIC_FUNCTIONS[VPN]	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption of services, and network-based reconnaissance, compliant TOE's will implement a cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE.
O.AUTHENTICATION[VPN]	To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (IPSec) will allow a VPN peer to establish VPN connectivity with another VPN peer. VPN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity.
O.ADDRESS_FILTERING[VPN]	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance, compliant TOE's will implement Packet Filtering capability. That capability will restrict the flow of network traffic between protected networks and other attached networks based on network addresses of the network nodes originating (source) and/or receiving (destination) applicable network traffic as well as on established connection information.

TOE Objective	TOE Security Objective Definition
O.FAIL_SECURE[VPN]	There may be instances where the TOE's hardware malfunctions or the integrity of the TOE's software is compromised, the latter being due to malicious or non-malicious intent. To address the concern of the TOE operating outside of its hardware or software specification, the TOE will shut down upon discovery of a problem reported via the self-test mechanism and provide signature-based validation of updates to the TSF.
O.PORT_FILTERING[VPN]	To further address the issues associated with unauthorized disclosure of information, etc., a compliant TOE's port filtering capability will restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (or service) identified in the network traffic as well as on established connection information.
O.SYSTEM_MONITORING[VPN]	To address the issues of administrators being able to monitor the operations of the VPN gateway, it is necessary to provide a capability to monitor system activity. Compliant TOEs will implement the ability to log the flow of network traffic. Specifically, the TOE will provide the means for administrators to configure packet filtering rules to 'log' when network traffic is found to match the configured rule. As a result, matching a rule configured to 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security associations (SAs) is auditable, not only between peer VPN gateways, but also with certification authorities (CAs).
O.TOE_ADMINISTRATION[VPN]	Compliant TOEs will provide the functions necessary for an administrator to configure the packet filtering rules, as well as the cryptographic aspects of the IPsec protocol that are enforced by the TOE.
O. ASSIGNED_PRIVATE_ADDRESS	There are instances where a remote client desires secure communication with a gateway that is trusted. While a user may be connected via an untrusted network, it should still be possible to ensure that it can communicate with a known entity that controls the routing of the client's network packets. This can be accomplished by the VPN headend assigning an IP address that the gateway controls, as well as providing a routing point for the client's network traffic.
O. CLIENT_ESTABLISHMENT_CONSTRAINTS	To address the concern that a remote client may be compromised and attempt to establish connections with the headend VPN gateway outside of "normal" operations, this objective specifies conditions under

TOE Objective	TOE Security Objective Definition
	which a remote client may establish connections. The administrator may configure the headend VPN gateway to accept a client's request for a connection based on attributes the administrator feels are appropriate.
O.PORT_FILTERING	To further address the issues associated with unauthorized disclosure of information, etc., a compliant TOE's port filtering capability will restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (or service) identified in the network traffic as well as on established connection information.
<b>Reproduced from the IPSecP</b>	
O.SYSTEM_MONITORING[IPS]	To be able to analyze and react to potential network policy violations, the IPS must be able to collect and store essential data elements of network traffic on monitored networks.
O.IPS_ANALYZE[IPS]	Entities that reside on or communicate across monitored networks must have network activity effectively analyzed for potential violations of approved network usage. The TOE must be able to effectively analyze data collected from monitored networks to reduce the risk of unauthorized disclosure of information, inappropriate access to services, and misuse of network resources.
O.IPS_REACT[IPS]	The TOE must be able to react in real-time as configured by the IPS administrators to terminate and/or block traffic flows that have been determined to violate administrator-defined IPS policies.
O.TOE_ADMINISTRATION[IPS]	To address the threat of unauthorized administrator access that is defined in the base PP, conformant TOEs will provide the functions necessary for an administrator to configure the IPS capabilities of the TOE.
O.TRUSTED_COMMUNICATIONS[IPS]	To further address the threat of untrusted communications channels that is defined in the base PP, conformant TOEs will provide trusted communications between distributed components if any exist.

## 4.2 Security Objectives for the Environment

All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

**Table 12 Security Objectives for the Environment**

<b>Environment Security Objective</b>	<b>IT Environment Security Objective Definition</b>
<b>Reproduced from the FWcPP</b>	
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the 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.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
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.
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.

## 5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012* and all international interpretations.

### 5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the FWcPP or VPNGWcEP itself, the formatting used in the FWcPP or VPNGWcEP has been retained.

Extended SFRs are identified by having a label ‘EXT’ after the requirement name for TOE SFRs. Formatting conventions outside of operations and iterations matches the formatting specified within the PP and EP themselves. In addition, SFRs copied verbatim from the VPNGWcEP will have extension [VPN] to distinguish them from the FWcPP.

### 5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

**Table 13 Security Functional Requirements**

Class Name	Component Identification	Component Name
<b>Reproduced from the FWcPP</b>		
FAU: Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	Protected Audit Event Storage
FCS: Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1(1)	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1(2)	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1(3)	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1(4)	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_HTTPS_EXT.1	HTTPS Protocol
	FCS_IPSEC_EXT.1	IPsec Protocol

Class Name	Component Identification	Component Name
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_TLSC_EXT.2	TLS Client Protocol with Authentication
	FCS_TLSS_EXT.1	TLS Server Protocol
FDP: User Data Protection	FDP_RIP.2	Full Residual Information Protection
FIA: Identification and Authentication	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
FMT: Security Management	FMT_MOF.1(1)/TrustedUpdate	Management of Security Functions Behaviour
	FMT_MOF.1(1)/AdminAct	Management of Security Functions Behaviour
	FMT_MOF.1(2)/AdminAct	Management of Security Functions Behaviour
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_SKP_EXT.1	Protection of TSF Data (for Reading of All Symmetric Keys)
	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_STM.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Trusted Update
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Session Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path
FFW: Stateful Traffic Filtering	FFW_RUL_EXT.1	Stateful Traffic Filtering
	FFW_RUL_EXT.2	Stateful Filtering of Dynamic Protocols
<b>Reproduced from the VPNGWcEP</b>		
FCS: Cryptographic Support	FCS_CKM.1/IKE[VPN]	Cryptographic Key Generation (for IKE Peer Authentication)
	FCS_COP.1(1)[VPN]	Cryptographic Operation (for Data Encryption/Decryption)
	FCS_IPSEC_EXT.1[VPN]	Extended: IPsec
FIA: Identification and Authentication	FIA_AFL.1[VPN]	Authentication Failure Handling
	FIA_PSK_EXT.1[VPN]	Pre-Shared Key Composition
	FIA_X509_EXT.4[VPN]	X.509 Certificate Identity
FMT: Security	FMT_MTD.1/AdminAct	Management of TSF Data

Class Name	Component Identification	Component Name
Management	[VPN]	
FPP: Packet Filtering	FPP_RUL_EXT.1[VPN]	Packet Filtering
FPT: Protection of the TSF	FPT_FLS.1/SelfTest [VPN]	Fail Secure
	FPT_TST_EXT.2.1 [VPN]	Extended: TSF Testing
	FPT_TUD_EXT.1.3 [VPN]	Extended: Trusted Update
FTA: TOE Access	FTA_SSL.3[VPN]	TSF-initiated Termination
	FTA_TSE.1[VPN]	TOE Session Establishment
	FTA_VCM_EXT.1[VPN]	VPN Client Management
FTP: Trusted path/channels	FTP_ITC.1.1[VPN]	Inter-TSF Trusted Channel
<b>Reproduced from the IPSecP</b>		
FAU: Security Audit	FAU_GEN.1/IPS	Audit Data Generation (IPS)
	<i>FAU_SAR.1*</i>	<i>Audit Review (IPS Data)</i>
	<i>FAU_SAR.2*</i>	<i>Restricted Audit Review (IPS Data)</i>
	<i>FAU_SAR.3*</i>	<i>Selectable Audit Review (IPS Data)</i>
	<i>FAU_STG.1*</i>	<i>Protected Audit Trail Storage (IPS Data)</i>
FMT: Security Management	FMT_SMF.1/IPS	Specification of Management Functions (IPS)
	<i>FMT_MOF.1/IPS*</i>	<i>Management of Security Functions Behavior</i>
	<i>FMT_MTD.1/IPS*</i>	<i>Management of IPS Data</i>
	<i>FMT_SMR.2/IPS*</i>	<i>Security Roles (IPS)</i>
IPS: Intrusion Prevention	IPS_ABD_EXT.1	Anomaly-Based IPS Functionality
	IPS_IPB_EXT.1	IP Blocking
	IPS_NTA_EXT.1	Network Traffic Analysis
	IPS_SBD_EXT.1	Signature-Based IPS Functionality
	<i>IPS_SBD_EXT.2*</i>	<i>Traffic Normalization</i>
FPT: Protection of the TSF	<i>FPT_ITT.1*</i>	<i>Basic Internal TSF Data Transfer Protection</i>
* - Optional SFRs		

## 5.3 SFRs Drawn from FWcPP

### 5.3.1 Security audit (FAU)

#### 5.3.1.1 FAU\_GEN.1 Audit Data Generation

**FAU\_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the not specified level of audit; and
- All administrative actions comprising:
  - Administrative login and logout (name of user account shall be logged if



*individual user accounts are required for administrators).*

- *Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*
- *Starting and stopping services (if applicable)*
- *Selection: [no other actions];*

d) *Specifically defined auditable events listed in Table 14.*

**FAU\_GEN.1.2** The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *information specified in column three of Table 14.*

**Table 14 Auditable Events**

SFR	Auditable Event	Additional Audit Record Contents
<b>Reproduced from the FWcPP</b>		
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1(1)	None.	None.
FCS_COP.1(2)	None.	None.
FCS_COP.1(3)	None.	None.
FCS_COP.1(4)	None.	None.
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	Reason for failure
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure
FCS_RBG_EXT.1	None.	
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
	Successful SSH rekey	Non-TOE endpoint of connection (IP address)
FCS_TLSC_EXT.2	Failure to establish an TLS Session	Reason for failure
FCS_TLSS_EXT.1	Failure to establish an TLS Session	Reason for failure
FDP_RIP.2	None.	None.
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1	Unsuccessful attempt to validate a certificate	Reason for failure

SFR	Auditable Event	Additional Audit Record Contents
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1(1)/TrustedUpdate	Any attempt to initiate a manual update	None.
FMT_MOF.1(1)/AdminAct	Modification of the behaviour of the TSF.	None.
FMT_MOF.1(2)/AdminAct	Starting and stopping of services.	None.
FMT_MTD.1	All management activities of TSF data.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	No additional information.
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.
FFW_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets Identifier of rule causing packet drop
FFW_RUL_EXT.2	FTP connection	The interface where the client resides. The IP address of the client. The client port. The interface where the server resides.

SFR	Auditable Event	Additional Audit Record Contents
		The IP address of the FTP server. The server port. The FTP username. The stored or retrieved actions. The file stored or retrieved.
<b>Reproduced from the VPNGWcEP</b>		
FCS_IPSEC_EXT.1 [VPN]	Session Establishment with peer	Entire packet contents of packets transmitted/received during session establishment
FIA_X509_EXT.1	Session Establishment with CA	Entire packet contents of packets transmitted/received during session establishment
FPF_RUL_EXT.1 [VPN]	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets

### 5.3.1.2 FAU\_GEN.2 User Identity Association

**FAU\_GEN.2.1** For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

### 5.3.1.3 FAU\_STG\_EXT.1 Protected Audit Event Storage

**FAU\_STG\_EXT.1.1** The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP\_ITC.1.

**FAU\_STG\_EXT.1.2** The TSF shall be able to store generated audit data on the TOE itself.

**FAU\_STG\_EXT.1.3** The TSF shall [overwrite previous audit records according to the following rule: [the newest audit record will overwrite the oldest audit record]] when the local storage space for audit data is full.

## 5.3.2 Cryptographic Support (FCS)

### 5.3.2.1 FCS\_CKM.1 Cryptographic Key Generation

**FCS\_CKM.1.1** The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- ***RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;***

- ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1

] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

*Application Note: FFC is supported by FP Service only.*

### 5.3.2.1 FCS\_CKM.2 Cryptographic Key Establishment

**FCS\_CKM.2.1** The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”;
- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”
- Finite field-based key establishment schemes that meets the following: NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”
- Key establishment scheme using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3

] that meets the following: [assignment: *list of standards*].

*Application Note: Updated per TD0235.*

### 5.3.2.2 FCS\_CKM.4 Cryptographic Key Destruction

**FCS\_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

- For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes]];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [
  - o logically addresses the storage location of the key and performs a [single, [one]-pass] overwrite consisting of [zeroes];

]

]

that meets the following: *No Standard*.

*Application Note: Updated per TD0130.*

### 5.3.2.3 FCS\_COP.1(1) Cryptographic Operation (AES Data Encryption/Decryption)

**FCS\_COP.1.1(1)** The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in [CBC, GCM] mode* and cryptographic key sizes [*128 bits, 192 bits, 256 bits*] that meet the following: *AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, GCM as specified in ISO 19772]*.

*Application Note: The VPNGWcEP requires that IKE/IPsec used for VPN IPsec tunnel can support AES in either CBC or GCM mode. SSH only supports AES in CBC mode and with key sizes 128 and 256 bits.*

### 5.3.2.4 FCS\_COP.1(2) Cryptographic Operation (Signature Generation and Verification)

**FCS\_COP.1.1(2)** The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm [

- *RSA Digital Signature Algorithm and cryptographic key sizes (**modulus**) [2048 bits]*
- *Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256, 384, and 521 bits]*

]

that meets the following: [

- *For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS2v1 5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,*
- *For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [P-256, P-384, and P-521]; ISO/IEC 14888-3, Section 6.4*

].

*Application Note: IKE/IPsec supports both ECDSA and RSA digital signature. SSH and trusted update only support RSA digital signature.*

*Application Note: Only ASA supports ECDSA and RSA algorithms. FP supports RSA algorithm only.*

*Application Note: Updated per TD0199.*

### 5.3.2.5 FCS\_COP.1(3) Cryptographic Operation (Hash Algorithm)

**FCS\_COP.1.1(3)** The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [*SHA-1, SHA-256, SHA-384, SHA-512*] and cryptographic key sizes [~~assignment: cryptographic key sizes~~] that meet the following: *ISO/IEC 10118-3:2004.*

### 5.3.2.6 FCS\_COP.1(4) Cryptographic Operation (Keyed Hash Algorithm)

**FCS\_COP.1.1(4)** The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [*HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512*] and cryptographic key sizes [*160, 256, 384, and 512 bits*] and **message digest sizes** [*160, 256, 384, 512*] *bits* that meet the following: *ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”*.

### 5.3.2.7 FCS\_HTTPS\_EXT.1 HTTPS Protocol

**FCS\_HTTPS\_EXT.1.1** The TSF shall implement the HTTPS protocol that complies with RFC 2818.

**FCS\_HTTPS\_EXT.1.2** The TSF shall implement HTTPS using TLS.

**FCS\_HTTPS\_EXT.1.2** The TSF shall establish the connection only if [*the peer initiates handshake*].

*Application Note: FCS\_HTTPS\_EXT.1.3 updated per TD0125.*

### 5.3.2.8 FCS\_IPSEC\_EXT.1 IPsec Protocol

*Application Note: The VPNGWcEP's FCS\_IPSEC\_EXT.1 takes precedent over the FWcPP.*

**FCS\_IPSEC\_EXT.1.1** The TSF shall implement the IPsec architecture as specified in RFC 4301.

*Application Note: Only ASA supports the IPsec and VPN functionality.*

**FCS\_IPSEC\_EXT.1.2** The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

**FCS\_IPSEC\_EXT.1.3[VPN] Refinement:** The TSF shall implement [**transport mode, tunnel mode**].

*Application Note: The VPNGWcEP's FCS\_IPSEC\_EXT.1.3 version.*

**FCS\_IPSEC\_EXT.1.4[VPN] Refinement:** The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602) and **AES-GCM-128 (specified in RFC 4106), AES-GCM-256 (specified in RFC 4106)** together with a Secure Hash Algorithm (SHA)-based HMAC.

*Application Note: The VPNGWcEP's FCS\_IPSEC\_EXT.1.4 version.*

**FCS\_IPSEC\_EXT.1.5** The TSF shall implement the protocol: [

- *IKEv2 as defined in RFC 5996 and [with mandatory support for NAT traversal as specified in RFC 5996, section 2.23], and [RFC 4868 for hash functions]*

].

**FCS\_IPSEC\_EXT.1.6** The TSF shall ensure the encrypted payload in the [IKEv2] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [AES-GCM-128, AES-GCM-256 as specified in RFC 5282].

**FCS\_IPSEC\_EXT.1.7** The TSF shall ensure that [

- *IKEv2 SA lifetimes can be configured by an Security Administrator based on*  
[  
  - o length of time, where the time values can configured within [120 to 2,147,483,647 seconds. The default is 86,400 seconds or 24] hours

].

*Application Note: IKEv2 SA can be limited by time only. IKEv2 Child SA can be limited by time or number of kilobytes. The time is in number of seconds.*

**FCS\_IPSEC\_EXT.1.8** The TSF shall ensure that [

- *IKEv2 Child SA lifetimes can be configured by a Security Administrator based on*  
[  
  - o number of kilobytes;
  - o length of time, where the time values can be configured within [120-2,147,483,647 seconds including 28,800 seconds which is 8] hours;

].

*Application Note: The valid range in kilobytes is 10-2,147,483,647 (10KB to 2TB).*

**FCS\_IPSEC\_EXT.1.9** The TSF shall generate the secret value  $x$  used in the IKE Diffie-Hellman key exchange (" $x$ " in  $g^x \bmod p$ ) using the random bit generator specified in FCS\_RBG\_EXT.1, and having a length of at least [512] bits.

**FCS\_IPSEC\_EXT.1.10** The TSF shall generate nonces used in [IKEv2] exchanges of length [

- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash

].

**FCS\_IPSEC\_EXT.1.11[VPN]** The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), 19 (256-bit Random ECP), 20 (384-bit Random ECP), and [no other DH groups].

*Application Note: FCS\_IPSEC\_EXT.1.11 updated per TD0209.*

**FCS\_IPSEC\_EXT.1.12** The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv2 IKE SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv2 CHILD\_SA] connection.

**FCS\_IPSEC\_EXT.1.13** The TSF shall ensure that all IKE protocols perform peer authentication using [*RSA, ECDSA*] that use X.509v3 certificates that conform to RFC 4945 and [*Pre-shared Keys*].

**FCS\_IPSEC\_EXT.1.14** The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following types: [*Fully Qualified Domain Name (FQDN)*, *Distinguished Name (DN)*] and [*no other reference identifier type*].

*Application Note: FCS\_IPSEC\_EXT.1.14 updated per TD0223.*

### 5.3.2.9 FCS\_RBG\_EXT.1 Random Bit Generation

**FCS\_RBG\_EXT.1.1** The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [*Hash DRBG (any)*, *CTR DRBG (AES)*].

**FCS\_RBG\_EXT.1.2** The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [ *[one] software-based noise source*, *[one] hardware-based noise source*] with a minimum of [*256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

*Application Note: The ASA and FP Services have different entropy sources. ASA uses Hash\_DRBG (SHA-512) and FP Service uses CTR\_DRBG(AES-256). Both entropy sources will be described in details in the proprietary entropy design documents.*

### 5.3.2.1 FCS\_SSHS\_EXT.1 SSH Server Protocol

**FCS\_SSHS\_EXT.1.1** The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254, and [*no other RFCs*].

**FCS\_SSHS\_EXT.1.2** The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

**FCS\_SSHS\_EXT.1.3** The TSF shall ensure that, as described in RFC 4253, packets greater than [*65,535 bytes*] bytes in an SSH transport connection are dropped.

**FCS\_SSHS\_EXT.1.4** The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [*aes128-cbc*, *aes256-cbc*, *AEAD AES 128 GCM*, *AEAD AES 256 GCM*].

*Application Note: FCS\_SSHS\_EXT.1.4 updated per TD0189.*

**FCS\_SSHS\_EXT.1.5** The TSF shall ensure that the SSH transport implementation uses [*ssh-rsa*] and [*no other public key algorithms*] as its public key algorithm(s) and rejects all other public key algorithms.



**FCS\_SSHS\_EXT.1.6** The TSF shall ensure that the SSH transport implementation uses [*hmac-sha1, hmac-sha2-256, hmac-sha2-512*] and [*AEAD\_AES\_128\_GCM, AEAD\_AES\_256\_GCM*] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

**FCS\_SSHS\_EXT.1.7** The TSF shall ensure that [*diffie-hellman-group14-sha1*] and [*no other methods*] are the only allowed key exchange methods used for the SSH protocol.

**FCS\_SSHS\_EXT.1.8** The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

*Application Note: Only FP Service supports SSH. ASA must tunnel SSH over IPsec.*

*Application Note: FCS\_SSHS\_EXT.1.8 has been updated per TD0167.*

### 5.3.2.2 FCS\_TLSC\_EXT.2 TLS Client Protocol with Authentication

**FCS\_TLSC\_EXT.2.1** The TSF shall implement [*TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] supporting the following ciphersuites:

- [
  - TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268
  - TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268
  - TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246
  - TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246
  - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289
  - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289
  - TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 4492
  - TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5289
  - TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 as defined in RFC 5289].

*Application Note: Updated per TD0226.*

**FCS\_TLSC\_EXT.2.2** The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125.

**FCS\_TLSC\_EXT.2.3** The TSF shall only establish a trusted channel if the peer certificate is valid.

**FCS\_TLSC\_EXT.2.4** The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [*secp256r1, secp384r1, secp521r1*] and no other curves.

**FCS\_TLSC\_EXT.2.5** The TSF shall support mutual authentication using X.509v3 certificates.

### 5.3.2.3 FCS\_TLSS\_EXT.1 TLS Server Protocol

**FCS\_TLSS\_EXT.1.1** The TSF shall implement [*TLS 1.2 (RFC 5246)*, *TLS 1.1 (RFC 4346)*] supporting the following ciphersuites:

- [
  - TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268
  - TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268
  - TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246
  - TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246
  - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289
  - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289
  - TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5289
  - TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 as defined in RFC 5289].

*Application Note: Updated per TD0226.*

**FCS\_TLSS\_EXT.1.2** The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [*none*].

*Application Note: Updated per TD0156.*

**FCS\_TLSS\_EXT.1.3** The TSF shall [*perform RSA key establishment with key size [2048 bits]; generate EC Diffie-Hellman parameters over NIST curves [secp256r1, secp384r1, secp521r1] and no other curves; generate Diffie-Hellman parameters of size [selection: 2048]*].

*Application Note: Updated per TD0226.*

## 5.3.3 User data protection (FDP)

### 5.3.3.1 FDP\_RIP.2 Full Residual Information Protection

**FDP\_RIP.2.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*allocation of the resource to*] all objects.

### 5.3.4 Identification and authentication (FIA)

#### 5.3.4.1 FIA\_PMG\_EXT.1 Password Management

**FIA\_PMG\_EXT.1.1** The TSF shall provide the following password management capabilities for administrative passwords:

- a) *Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “\*”, “(“, “)”, “ ”, “` (double or single quote/apostrophe), + (plus), - (minus), = (equal), , (comma), . (period), / (forward-slash), \ (back-slash), | (vertical-bar or pipe), : (colon), ; (semi-colon), < > (less-than, greater-than inequality signs), [ ] (square-brackets), { } (braces or curly-brackets), ? (question-mark), ^ (caret), \_ (underscore), and ~ (tilde)];*
- b) *Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater.*

*Application Note: Only FP Service supports the “?” special character in the password.*

#### 5.3.4.2 FIA\_UIA\_EXT.1 User Identification and Authentication

**FIA\_UIA\_EXT.1.1** The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA\_TAB.1;
- [*no other actions*]

**FIA\_UIA\_EXT.1.2** The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated action on behalf of that administrative user.

#### 5.3.4.3 FIA\_UAU\_EXT.2 Password-based Authentication Mechanism

**FIA\_UAU\_EXT.2.1** The TSF shall provide a local password-based authentication mechanism, [*support for RADIUS*] to perform administrative user authentication.

#### 5.3.4.4 FIA\_UAU.7 Protected Authentication Feedback

**FIA\_UAU.7.1** The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress at the local console.

#### 5.3.4.5 FIA\_X509\_EXT.1 X.509 Certificate Validation

**FIA\_X509\_EXT.1.1** The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
  - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
  - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
  - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

*Application Note: ASA supports both CRL and OCSP for certificate revocation check. FP Services only supports CRL.*

**FIA\_X509\_EXT.1.2** The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

#### **5.3.4.1 FIA\_X509\_EXT.2 X.509 Certificate Authentication**

**FIA\_X509\_EXT.2.1** The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [IPsec, TLS], and [no additional uses].

**FIA\_X509\_EXT.2.2** When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate, accept the certificate].

*Application Note: ASA supports not accepting the certificate while FP Services supports accepting the certificate.*

#### **5.3.4.1 FIA\_X509\_EXT.3 X.509 Certificate Requests**

**FIA\_X509\_EXT.3.1** The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

**FIA\_X509\_EXT.3.2** The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

### 5.3.5 Security management (FMT)

#### 5.3.5.1 FMT\_MOF.1(1)/TrustedUpdate Management of Security Functions Behaviour

**FMT\_MOF.1.1(1)/TrustedUpdate** The TSF shall restrict the ability to enable the functions *perform manual update* to *Security Administrators*.

#### 5.3.5.1 FMT\_MOF.1(1)/AdminAct Management of Security Functions Behaviour

**FMT\_MOF.1.1(1)/AdminAct** The TSF shall restrict the ability to *modify the behaviour* of the functions *TOE Security Functions* to *Security Administrators*.

#### 5.3.5.1 FMT\_MOF.1(2)/AdminAct Management of Security Functions Behaviour

**FMT\_MOF.1.1(2)/AdminAct** The TSF shall restrict the ability to enable, disable the functions *services* to *Security Administrators*.

#### 5.3.5.2 FMT\_MTD.1 Management of TSF Data

**FMT\_MTD.1.1** The TSF shall restrict the ability to manage the *TSF data* to the *Security Administrators*.

#### 5.3.5.3 FMT\_SMF.1 Specification of Management Functions

**FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using **digital signature and [hash comparison]** capability prior to installing those updates;*
- *Ability to configure firewall rules;*
- *Ability to configure the cryptographic functionality;*
- *Ability to configure the IPsec functionality;*
- *Ability to import X.509v3 certificates;*
- *Ability to enable, disable, determine and modify the behavior of all the security functions of the TOE identified in this EP to the Administrator;*
- *Ability to configure all security management functions identified in other sections of this EP;*
- [
  - *No other capabilities.*]]

*Application Note: Updated per TD0179.*

#### 5.3.5.4 FMT\_SMR.2 Restrictions on Security Roles

**FMT\_SMR.2.1** The TSF shall maintain the roles:

- *Security Administrator.*

**FMT\_SMR.2.2** The TSF shall be able to associate users with roles.

**FMT\_SMR.2.3** The TSF shall ensure that the conditions

- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely;*

are satisfied.

#### 5.3.6 Protection of the TSF (FPT)

##### 5.3.6.1 FPT\_SKP\_EXT.1 Protection of TSF Data (for Reading of All Symmetric Keys)

**FPT\_SKP\_EXT.1.1** The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

##### 5.3.6.2 FPT\_APW\_EXT.1 Protection of Administrator Passwords

**FPT\_APW\_EXT.1.1** The TSF shall store passwords in non-plaintext form.

**FPT\_APW\_EXT.1.2** The TSF shall prevent the reading of plaintext passwords.

##### 5.3.6.3 FPT\_STM.1 Reliable time stamps

**FPT\_STM.1.1** The TSF shall be able to provide reliable time stamps.

##### 5.3.6.4 FPT\_TST\_EXT.1 and FPT\_TST\_EXT.2: TSF Testing

**FPT\_TST\_EXT.1.1** The TSF shall run a suite of the following self-tests [*during initial start-up (on power on)*] to demonstrate the correct operation of the TSF: [*FIPS 140-2 standard power-up self-tests and firmware integrity test*].

**FPT\_TST\_EXT.2.1[VPN]** The TSF shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic service specified in FCS\_COP.1(2).

##### 5.3.6.5 FPT\_TUD\_EXT.1 Trusted Update

**FPT\_TUD\_EXT.1.1** The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [*the most recently installed version of the TOE firmware/software, no other TOE firmware/software version*].

*Application Note: FPT\_TUD\_EXT.1.1 updated per TD0154.*

*Application Note: The first selection is made for ASA. The second selection is made for FP Service.*

**FPT\_TUD\_EXT.1.2** The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [*no other update mechanism*].

**FPT\_TUD\_EXT.1.3[VPN]** The TSF shall provide a means to authenticate firmware/software updates to the TOE using a digital signature mechanism and [published hash] prior to installing those updates.

*Application Note: The VPNGWcEP's FPT\_TUD\_EXT.1.3 version.*

*Application Note: The ASA image is verified using digital signature mechanism. Only the ASA software is claiming the VPN requirements. FP Services is claiming the IPS requirements.*

### 5.3.7 TOE Access (FTA)

#### 5.3.7.1 FTA\_SSL\_EXT.1 TSF-initiated Session Locking

**FTA\_SSL\_EXT.1.1** The TSF shall, for local interactive sessions, [

- terminate the session]

after a Security Administrator-specified time period of inactivity.

#### 5.3.7.2 FTA\_SSL.3 TSF-initiated Termination

**FTA\_SSL.3.1(1) Refinement:** The TSF shall terminate a **remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

#### 5.3.7.3 FTA\_SSL.4 User-initiated Termination

**FTA\_SSL.4.1 Refinement:** The TSF shall allow **Administrator**-initiated termination of the **Administrator's** own interactive session.

#### 5.3.7.4 FTA\_TAB.1 Default TOE Access Banners

**FTA\_TAB.1.1 Refinement:** Before establishing an **administrative user** session the TSF shall display a **Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

### 5.3.8 Trusted Path/Channels (FTP)

#### 5.3.8.1 FTP\_ITC.1 Inter-TSF Trusted Channel

**FTP\_ITC.1.1[VPN]** The TSF shall **use IPsec, and [TLS]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, VPN communications, [authentication server]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

*Application Note: The VPNGWcEP's FTP\_ITC.1.1 version.*

**FTP\_ITC.1.2** The TSF shall permit **the TSF, or the authorized IT entities** to initiate communication via the trusted channel.

**FTP\_ITC.1.3** The TSF shall initiate communication via the trusted channel for [

- *Audit server: transmit audit data via syslog over IPsec or TLS;*
- *Authentication server: authentication of TOE administrators using AAA servers including RADIUS over IPsec;*
- *Remote VPN peer using IPsec;].*

#### 5.3.8.2 FTP\_TRP.1 Trusted Path

**FTP\_TRP.1.1** The TSF shall **be capable of using [SSH, HTTPS]** to provide a communication path between itself and **authorized remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *disclosure and detection of modification of the communicated data*.

**FTP\_TRP.1.2** The TSF shall permit **remote administrators** to initiate communication via the trusted path.

**FTP\_TRP.1.3** The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions**.

### 5.3.9 Stateful Traffic Filtering (FFW)

#### 5.3.9.1 FFW\_RUL\_EXT.1 Stateful Traffic Filtering

**FFW\_RUL\_EXT.1.1** The TSF shall perform Stateful Traffic Filtering on network packets processed by the TOE.

**FFW\_RUL\_EXT.1.2** The TSF shall allow the definition of Stateful Traffic Filtering rules using the following network protocol fields:

- ICMPv4
  - Type
  - Code



- ICMPv6
  - Type
  - Code
- IPv4
  - Source address
  - Destination Address
  - Transport Layer Protocol
- IPv6
  - Source address
  - Destination Address
  - Transport Layer Protocol
  - [no other field]
- TCP
  - Source Port
  - Destination Port
- UDP
  - Source Port
  - Destination Port
- and distinct interface.

**FFW\_RUL\_EXT.1.3** The TSF shall allow the following operations to be associated with Stateful Traffic Filtering rules: permit or drop with the capability to log the operation.

**FFW\_RUL\_EXT.1.4** The TSF shall allow the Stateful Traffic Filtering rules to be assigned to each distinct network interface.

**FFW\_RUL\_EXT.1.5** The TSF shall:

a) accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols: TCP, UDP, [no other protocols] based on the following network packet attributes:

1. TCP: source and destination addresses, source and destination ports, sequence number, Flags;
2. UDP: source and destination addresses, source and destination ports;
3. [no other protocols].

b) Remove existing traffic flows from the set of established traffic flows based on the following: [session inactivity timeout, completion of the expected information flow].

**FFW\_RUL\_EXT.1.6** The TSF shall enforce the following default Stateful Traffic Filtering rules on all network traffic:

- a) The TSF shall drop and be capable of [logging] packets which are invalid fragments;
- b) The TSF shall drop and be capable of [logging] fragmented packets which cannot be re-assembled completely;

- c) The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a broadcast network;
- d) The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a multicast network; The TSF shall drop and be capable of logging network packets where the source address of the network packet is defined as being a loopback address;
- e) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address “reserved for future use” (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4;
- f) The TSF shall drop and be capable of logging 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” (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6;
- g) The TSF shall drop and be capable of logging network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified; and
- [[Other traffic dropped by default and able to be logged:
  - i. Slowpath Security Checks – The TSF shall reject and be capable of logging the detection of the following network packets:
    - 1. In routed mode when the TOE receives a through-the-box:
      - a. L2 broadcast packet (MAC address FF:FF:FF:FF:FF:FF)
      - b. IPv4 packet with destination IP address equal to 0.0.0.0
      - c. IPv4 packet with source IP address equal to 0.0.0.0
    - 2. In routed or transparent mode when the TOE receives a through-the-box IPv4 packet with any of:
      - 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
      - e. source IP address and destination IP address are the same (“land.c” attack)
    - 3. IPv6 through-the-box packet with identical source and destination address.
  - ii. LAND Attack: The TSF shall reject and be capable of logging network packets with the IP source address equal to the IP destination, and the destination port equal to the source port.
  - iii. ICMP Error Inspect and ICMPv6 Error Inspect - The TSF shall reject and be capable of logging ICMP error packets when the ICMP error messages are not related to any session already established in the TOE.
  - iv. ICMPv6 condition - The TSF shall reject and be capable of logging network packets when the appliance is not able to find any established connection related to the frame embedded in the ICMPv6 error message.
  - v. ICMP Inspect bad icmp code - The TSF shall reject and be capable of logging network packets when an ICMP echo request/reply packet was received with a malformed code(non-zero)]].

**FFW\_RUL\_EXT.1.7** The TSF shall be capable of dropping and logging according to the following rules:

- a) The TSF shall drop and be capable of logging 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;
- b) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is a link-local address;
- c) The TSF shall drop and be capable of logging 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.

**FFW\_RUL\_EXT.1.8** , The TSF shall process the applicable Stateful Traffic Filtering rules in an administratively defined order.

**FFW\_RUL\_EXT.1.9** The TSF shall deny packet flow if a matching rule is not identified.

**FFW\_RUL\_EXT.1.10** The TSF shall be capable of limiting an administratively defined number of *half-open TCP connections*. *In the event that the configured limit is reached, new connection attempts shall be dropped and the drop event shall be [counted]*.

### 5.3.9.1 FFW\_RUL\_EXT.2 Stateful Filtering of Dynamic Protocols

**FFW\_RUL\_EXT.2.1** The TSF shall dynamically define rules or establish sessions allowing network traffic to flow for the following network protocols [*FTP*].

## 5.4 SFRs from the VPNGWcEP

### 5.4.1 Cryptographic Support (FCS)

#### 5.4.1.1 FCS\_CKM.1/IKE[VPN] Cryptographic Key Generation (for IKE Peer Authentication)

**FCS\_CKM.1.1/IKE[VPN] Refinement:** The TSF shall generate **asymmetric** cryptographic keys **used for IKE peer authentication** in accordance with a: [

- FIPS PUB 186-4, “Digital Signature Standard (DSS)”; Appendix B.3 for RSA schemes;
- FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4 for ECDSA schemes and implementing “NIST curves” P-256, P-384 and [P-521]

]

and specified cryptographic key sizes *equivalent to, or greater than, a symmetric key strength of 112 bits*.

#### 5.4.1.2 FCS\_COP.1(1)[VPN] Cryptographic Operation (for Data Encryption/Decryption)

**FCS\_COP.1.1(1)[VPN] Refinement:** The TSF shall perform *encryption/ decryption* in accordance with a specified cryptographic algorithm *AES operating in GCM, CBC* and

cryptographic key sizes **128 bits, 256 bits, and [192 bits]** that meet the following: *AES as specified in ISO 18033-3, CBC as specified in ISO 10116, GCM as specified in ISO 19772.*

## 5.4.2 Identification and authentication (FIA)

### 5.4.2.1 FIA\_AFL.1[VPN] Authentication Failure Handling

**FIA\_AFL.1.1[VPN] Refinement:** The TSF shall detect when **an Administrator configurable positive integer of successive** unsuccessful authentication attempts occur related to **administrators attempting to authenticate remotely**.

**FIA\_AFL.1.2[VPN] Refinement:** When the defined number of unsuccessful authentication attempts has been met, the TSF shall **prevent the offending remote administrator from successfully authenticating until [an authorized administrator unlocks the locked user account] is taken by a local Administrator**.

### 5.4.2.2 FIA\_PSK\_EXT.1[VPN] Extended: Pre-Shared Key Composition

**FIA\_PSK\_EXT.1.1[VPN]** The TSF shall be able to use pre-shared keys for IPsec and [no other protocols].

**FIA\_PSK\_EXT.1.2[VPN]** The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and [up to 128 characters];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “\*”, “(”, and “”).

**FIA\_PSK\_EXT.1.3[VPN]** The TSF shall condition the text-based pre-shared keys by using [HMAC-SHA1, HMAC-SHA-256, HMAC-SHA384, HMAC-SHA-512].

**FIA\_PSK\_EXT.1.4[VPN]** The TSF shall be able to [accept] bit-based pre-shared keys.

### 5.4.2.3 FIA\_X509\_EXT.4[VPN] X.509 Certificate Identity

**FIA\_X509\_EXT.4.1[VPN]** The TSF shall not establish an SA if the distinguished name (DN) contained in a certificate does not match the expected DN for the entity attempting to establish a connection.

### 5.4.3 Security management (FMT)

#### 5.4.3.1 FMT\_MTD.1/AdminAct[VPN] Management of TSF Data

**FMT\_MTD.1.1/AdminAct[VPN] Refinement:** The TSF shall restrict the ability to *modify, delete, generate/import* the *cryptographic keys and certificates used for VPN operation* to *Security Administrators*.

### 5.4.4 Packeting Filtering (FPF)

#### 5.4.4.1 FPF\_RUL\_EXT.1 Packet Filtering

**FPF\_RUL\_EXT.1.1** The TSF shall perform Packet Filtering on network packets processed by the TOE.

**FPF\_RUL\_EXT.1.2** The TSF shall process the following network traffic protocols:

- Internet Protocol (IPv4)
- Internet Protocol version 6 (IPv6)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

and be capable of inspecting network packet header fields defined by the following RFCs to the extent mandated in the other elements of this SFR

- RFC 791 (IPv4)
- RFC 2460 (IPv6)
- RFC 793 (TCP)
- RFC 768 (UDP).

**FPF\_RUL\_EXT.1.3** The TSF shall allow the definition of Packet Filtering rules using the following network protocol fields:

- IPv4
  - o Source address
  - o Destination Address
  - o Protocol
- IPv6
  - o Source address
  - o Destination Address
  - o Next Header (Protocol)
- TCP
  - o Source Port

- o Destination Port
- UDP
  - o Source Port
  - o Destination Port

and distinct interface.

**FPF\_RUL\_EXT.1.4** The TSF shall allow the following operations to be associated with Packet Traffic Filtering rules: permit, ~~deny~~, **discard**, and log.

**FPF\_RUL\_EXT.1.5** The TSF shall allow the Packet Traffic Filtering rules to be assigned to each distinct network interface.

**FPF\_RUL\_EXT.1.6** The TSF shall process the applicable Packet Filtering rules (as determined in accordance with FPF\_RUL\_EXT.1.5) in the following order: Administrator-defined.

**FPF\_RUL\_EXT.1.7** The TSF shall deny packet flow if a matching rule is not identified.

#### 5.4.5 Protection of the TSF (FPT)

##### 5.4.5.1 FPT\_FLS.1/SelfTest[VPN] Fail Secure

**FPT\_FLS.1.1/SelfTest[VPN] Refinement:** The TSF shall **shutdown** when the following types of failures occur: failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests.

#### 5.4.6 TOE Access (FTA)

##### 5.4.6.1 FTA\_SSL.3[VPN] TSF-initiated Termination

**FTA\_SSL.3.1[VPN] Refinement:** The TSF shall terminate a **remote VPN client** session after an *Administrator-configurable time interval of session inactivity*.

##### 5.4.6.2 FTA\_TSE.1[VPN] TOE Session Establishment

**FTA\_TSE.1.1[VPN] Refinement:** The TSF shall be able to deny establishment of a **remote VPN client** session based on *location, time, day, [no other attributes]*.

##### 5.4.6.3 FTA\_VCM\_EXT.1[VPN] VPN Client Management

**FTA\_VCM\_EXT.1.1[VPN]** The TSF shall assign a private IP address to a VPN client upon successful establishment of a security session.

## 5.5 SFRs from the IPScEP

### 5.5.1 Security Audit (FAU)

#### 5.5.1.1 FAU\_GEN.1/IPS Audit Data Generation (IPS)

**FAU\_GEN.1.1/IPS Refinement:** The TSF shall be able to generate an **IPS** audit record of the following auditable **IPS** events:

- a) Start-up and shut-down of the **IPS** functions;
- b) All **IPS** auditable events for the [not specified] level of audit; and
- ~~c) All administrative actions;~~
- d) *[All dissimilar IPS events;*
- e) All dissimilar IPS reactions;*
- f) *Totals of similar events occurring within a specified time period; and*
- g) *Totals of similar reactions occurring within a specified time period.*

**FAU\_GEN.1.2/IPS Refinement:** The TSF shall record within each **IPS auditable event** record at least the following information:

- a) Date and time of the event, type of event **and/or reaction**, ~~subject identity, and the outcome (success or failure) of the event;~~ and;
- b) For each **IPS auditable** event type, based on the auditable event definitions of the functional components included in the PP/ST, *[Specifically defined auditable events listed in Table 16]*.

**Table 15 Auditable Events**

SFR	Auditable Event	Additional Audit Record Contents
<b>Reproduced from the IPScEP</b>		
FMT_SMF.1/IPS	Modification of an IPS policy element.	Identifier or name of the modified IPS policy element (e.g. which signature, baseline, or known-good/known-bad list was modified).
IPS_ABD_EXT.1	Inspected traffic matches an anomaly-based IPS policy.	Source and destination IP addresses.
		The content of the header fields that were determined to match the policy.
		TOE interface that received the packet.
		Aspect of the anomaly-based IPS policy rule that triggered the event (e.g. throughput, time of day, frequency, etc.).
		Network-based action by the TOE (e.g. allowed, blocked, sent reset to source IP, sent blocking notification to firewall).
IPS_IPB_EXT.1	Inspected traffic matches a list of known-good or known-bad	Source and destination IP addresses (and, if applicable, indication of whether the source

SFR	Auditable Event	Additional Audit Record Contents
	addresses applied to an IPS policy.	and/or destination address matched the list).
		TOE interface that received the packet.
		Network-based action by the TOE (e.g. allowed, blocked, sent reset).
IPS_NTA_EXT.1	Modification of which IPS policies are active on a TOE interface.	Identification of the TOE interface.
	Enabling/disabling a TOE interface with IPS policies applied.	The IPS policy and interface mode (if applicable).
	Modification of which mode(s) is/are active on a TOE interface.	
IPS_SBD_EXT.1	Inspected traffic matches a signature-based IPS rule with logging enabled.	Name or identifier of the matched signature.
		Source and destination IP addresses.
		The content of the header fields that were determined to match the signature.
		TOE interface that received the packet.
		Network-based action by the TOE (e.g. allowed, blocked, sent reset).

#### 5.5.1.2 FAU\_SAR.1 Audit Review (IPS)\*

**FAU\_SAR.1.1 Refinement:** The TSF shall provide [*authorized administrators*] with the capability to read [*IPS data*] from the ~~audit records~~ IPS events.

**FAU\_SAR.1.2 Refinement:** The TSF shall provide the ~~audit records~~ **IPS data** in a manner suitable for the ~~user~~ **administrators** to interpret the information.

#### 5.5.1.3 FAU\_SAR.2 Restricted Audit Review (IPS)\*

**FAU\_SAR.2.1 Refinement:** The TSF shall prohibit all ~~users~~ **administrators** read access to the ~~audit records~~ **IPS data**, except those that have been granted explicit read-access.

#### 5.5.1.4 FAU\_SAR.3 Selectable Audit Review (IPS)\*

**FAU\_SAR.3.1 Refinement:** The TSF shall provide the ability to apply [*filtering and sorting*] of ~~audit~~ **IPS data** based on [*filtering parameters: risk rating, time period, source IP address, destination IP address and [other filtering parameters described in the TSS]*]; and sorting parameters: event ID, event type, time, signature ID, IPS actions performed, and [*other sorting parameters described in the TSS*]].

#### 5.5.1.5 FAU\_STG.1 Protected Audit Trail Storage (IPS Data)\*

**FAU\_STG.1.1 Refinement:** The TSF shall protect the stored ~~audit records~~ **IPS data** from unauthorized deletion.



**FAU\_STG.1.2 Refinement:** The TSF shall be able to *[prevent]* unauthorized modifications to the stored ~~audit records~~ **IPS data in the audit trail**.

## 5.5.2 Security management (FMT)

### 5.5.2.1 FMT\_SMF.1/IPS Specification of Management Functions (IPS)

**FMT\_SMF.1.1/IPS** The TSF shall be capable of performing the following management functions: [

- *Enable, disable signatures applied to sensor interfaces, and determine the behavior of IPS functionality*
- *Modify these parameters that define the network traffic to be collected and analyzed:*
  - *Source IP addresses (host address and network address)*
  - *Destination IP addresses (host address and network address)*
  - *Source port (TCP and UDP)*
  - *Destination port (TCP and UDP)*
  - *Protocol (IPv4 and IPv6)*
  - *ICMP type and code*
- *Update (import) signatures*
- *Create custom signatures*
- *Configure anomaly detection*
- *Enable and disable actions to be taken when signature or anomaly matches are detected*
- *Modify thresholds that trigger IPS reactions*
- *Modify the duration of traffic blocking actions*
- *Modify the known-good and known-bad lists (of IP addresses or address ranges)*
- *Configure the known-good and known-bad lists to override signature-based IPS policies]*

### 5.5.2.2 FMT\_MOF.1/IPS Management of Security Functions Behavior\*

**FMT\_MOF.1.1/IPS** The TSF shall restrict the ability to modify the behavior of the functions [*IPS data collection, analysis, and reaction*] to [*authorized IPS Administrators*].

### 5.5.2.3 FMT\_MTD.1/IPS Management of IPS Data\*

**FMT\_MTD.1.1/IPS Refinement:** The TSF shall restrict the ability to [change default, query, modify, delete, clear] the [*all IPS data*] to [*the IPS Administrator, IPS Analyst and other IPS-specific roles identified in FMT\_SMR.2/IPS*].

### 5.5.2.4 FMT\_SMR.2/IPS Security Roles (IPS)\*

**FMT\_SMR.2.1/IPS Refinement:** The TSF shall maintain the roles: [*IPS Administrator, IPS Analyst, and [[Access Admin, Discovery Admin, Security Analyst]]*].

**FMT\_SMR.2.2/IPS** The TSF shall be able to associate users with roles.

**FMT\_SMR.2.3/IPS** The TSF shall ensure that [

- *IPS Administrator (or Administrator): Have all privileges and access*
- *IPS Analyst (or Intrusion Admin): Have all access to intrusion policies and network analysis privileges but cannot deploy policies*
- *Access Admin: Have all access to access control policies but cannot deploy policies*
- *Discovery Admin: Have all access to network discovery, application detection, and correlation features but cannot deploy policies*
- *Security Analyst: Have all access to security event analysis feature*

] are satisfied.

## 5.5.3 Intrusion Prevention (IPS)

### 5.5.3.1 IPS\_ABD\_EXT.1 Anomaly-Based IPS Functionality

**IPS\_ABD\_EXT.1.1** The TSF shall support the definition of [baselines ('expected and approved'), anomaly ('unexpected') traffic patterns] including the specification of [

- Throughput ([packets matching a configured signature in the specified time period])
- [preprocessor detection rules for anomaly detected in headers and protocols]

and the following network protocol fields:

- [all packet header and data elements defined in IPS\_SBD\_EXT.1]

**IPS\_ABD\_EXT.1.2** The TSF shall support the definition of anomaly activity through [manual configuration by administrators].

**IPS\_ABD\_EXT.1.3** The TSF shall allow the following operations to be associated with anomaly-based IPS policies:

- In any mode, for any sensor interface: [ o allow the traffic flow ]
- In inline mode:
  - o allow the traffic flow
  - o block/drop the traffic flow
  - o and [no other actions]

### 5.5.3.2 IPS\_IPB\_EXT.1 IP Blocking

**IPS\_IPB\_EXT.1.1** The TSF shall support configuration and implementation of known-good and known-bad lists of [source, destination] IP addresses.

**IPS\_IPB\_EXT.1.2:** The TSF shall allow IPS Administrators and [Access Admin] to configure the following IPS policy elements: [known-good list rules, known-bad list rules, IP addresses, Domain names and URLs].

### 5.5.3.3 IPS\_NTA\_EXT.1 Network Traffic Analysis

**IPS\_NTA\_EXT.1.1** The TSF shall perform analysis of IP-based network traffic forwarded to the TOE's sensor interfaces, and detect violations of administratively-defined IPS policies.

**IPS\_NTA\_EXT.1.2:** The TSF shall process (be capable of inspecting) the following network traffic protocols:

- Internet Protocol (IPv4), RFC 791
- Internet Protocol version 6 (IPv6), RFC 2460
- Internet control message protocol version 4 (ICMPv4), RFC 792
- Internet control message protocol version 6 (ICMPv6), RFC 2463
- Transmission Control Protocol (TCP), RFC 793
- User Data Protocol (UDP), RFC 768

**IPS\_NTA\_EXT.1.3** The TSF shall allow the signatures to be assigned to sensor interfaces configured for promiscuous mode, and to interfaces configured for inline mode, and support designation of one or more interfaces as 'management' for communication between the TOE and external entities without simultaneously being sensor interfaces.

- Promiscuous (listen-only) mode: *[Giga Ethernet]*;
- Inline (data pass-through) mode: *[Giga Ethernet]*;
- Management mode: *[Giga Ethernet]*;

- [
  - o no other interface types].

#### 5.5.3.4 IPS\_SBD\_EXT.1 Signature-Based IPS Functionality

**IPS\_SBD\_EXT.1.1** The TSF shall support inspection of packet header contents and be able to inspect at least the following header fields:

- IPv4: Version; Header Length; Packet Length; ID; IP Flags; Fragment Offset; Time to Live (TTL); Protocol; Header Checksum; Source Address; Destination Address; and IP Options and [no other field].
- IPv6: Version; payload length; next header; hop limit; source address; destination address; routing header; and [no other field].
- ICMP: Type; Code; Header Checksum; and [ID, sequence number, *[no other field]*].
- ICMPv6: Type; Code; and Header Checksum.
- TCP: Source port; destination port; sequence number; acknowledgement number; offset; reserved; TCP flags; window; checksum; urgent pointer; and TCP options.
- UDP: Source port; destination port; length; and UDP checksum.

**IPS\_SBD\_EXT.1.2** The TSF shall support inspection of packet payload data and be able to inspect at least the following data elements to perform string-based pattern-matching:

- ICMPv4 data: characters beyond the first 4 bytes of the ICMP header.
- ICMPv6 data: characters beyond the first 4 bytes of the ICMP header.
- TCP data (characters beyond the 20 byte TCP header), with support for detection of:
  - i) FTP (file transfer) commands: help, noop, stat, syst, user, abort, acct, allo, appe, cdup, cwd, dele, list, mkd, mode, nlst, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru, and type.
  - ii) HTTP (web) commands and content: commands including GET and POST, and administrator-defined strings to match URLs/URIs, and web page content.
  - iii) SMTP (email) states: start state, SMTP commands state, mail header state, mail body state, abort state.
  - iv) [no other types of TCP payload inspection];
- UDP data: characters beyond the first 8 bytes of the UDP header;
- [no other types of packet payload inspection]

In addition, the TSF shall support stream reassembly or equivalent to detect malicious payload even if it is split across multiple non-fragmented packets.

**IPS\_SBD\_EXT.1.3:** The TSF shall be able to detect the following header-based signatures (using fields identified in IPS\_SBD\_EXT.1.1) at IPS sensor interfaces:

- a) IP Attacks
  - i) IP Fragments Overlap (Teardrop attack, Bonk attack, or Boink attack)
  - ii) IP source address equal to the IP destination (Land attack)
- b) ICMP Attacks
  - i) Fragmented ICMP Traffic (e.g. Nuke attack)
  - ii) Large ICMP Traffic (Ping of Death attack)
- c) TCP Attacks
  - i) TCP NULL flags
  - ii) TCP SYN+FIN flags
  - iii) TCP FIN only flags
  - iv) TCP SYN+RST flags
- d) UDP Attacks
  - i) UDP Bomb Attack
  - ii) UDP Chargen DoS Attack

**IPS\_SBD\_EXT.1.4:** The TSF shall be able to detect all the following traffic-pattern detection signatures, and to have these signatures applied to IPS sensor interfaces:

- a) Flooding a host (DoS attack)
  - i) ICMP flooding (Smurf attack, and ping flood)
  - ii) TCP flooding (e.g. SYN flood)
- b) Flooding a network (DoS attack)
- c) Protocol and port scanning
  - i) IP protocol scanning
  - ii) TCP port scanning
  - iii) UDP port scanning
  - iv) ICMP scanning

**IPS\_SBD\_EXT.1.5** The TSF shall allow the following operations to be associated with signature-based IPS policies:

- In any mode, for any sensor interface: [
  - o allow the traffic flow; ]
- In inline mode:
  - o allow the traffic flow;
  - o block/drop the traffic flow;
  - o and [no other actions]

## 5.5.4 Protection of the TSF (FPT)

### 5.5.4.1 FPT\_ITT.1 Basic Internal TSF Data Transfer Protection\*

**FPT\_ITT.1.1 Refinement:** The TSF shall protect TSF data from [disclosure, modification] using [TLS] when it is transmitted between [the FMC and Sensor] ~~separate parts of the TOE.~~

## 5.6 TOE SFR Dependencies Rationale for SFRs Found in FWcPP

The FWcPPv1.0 contains all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PP itself has been approved.

## 5.7 Security Assurance Requirements

### 5.7.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the FWcPP which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

**Table 16: Assurance Measures**

Assurance Class	Components	Components Description
DEVELOPMENT	ADV_FSP.1	Basic Functional Specification
GUIDANCE DOCUMENTS	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
LIFE CYCLE SUPPORT	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Coverage
TESTS	ATE_IND.1	Independent Testing - Conformance
VULNERABILITY ASSESSMENT	AVA_VAN.1	Vulnerability Analysis

### 5.7.2 Security Assurance Requirements Rationale

This Security Target claims conformance to the FWcPP. This target was chosen to ensure that the TOE has a basic to moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks. The ST also claims conformance to the VPNGWcEP, which includes refinements to assurance measures for the SFRs defined in the VPNGWcEP, including augmenting the vulnerability analysis (AVA\_VAN.1) with specific vulnerability testing.

## 5.8 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. The table below lists the details.

**Table 17: Assurance Measures**

Component	How requirement will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ALC_CMS.1	
ATE_IND.1	Cisco provides the TOE for testing.
AVA_VAN.1	Cisco provides the TOE for testing.

## 6 TOE SUMMARY SPECIFICATION

### 6.1 TOE Security Functional Requirement Measures

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

**Table 18: How TOE SFRs Are Satisfied**

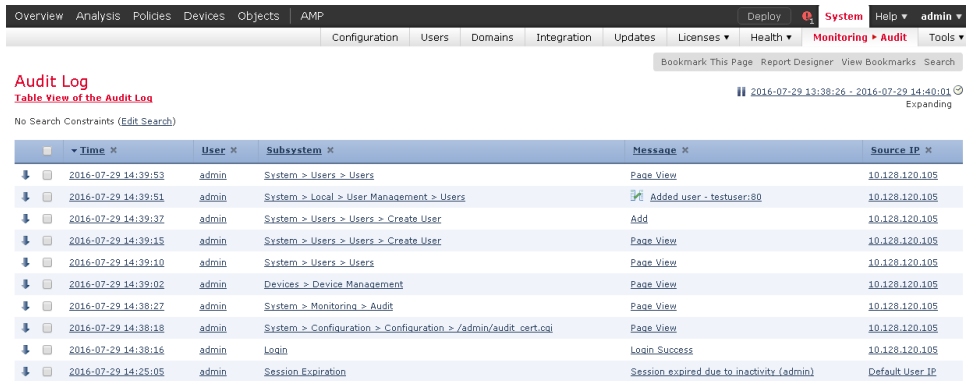
TOE SFRs	How the SFR is Satisfied				
<b>Security Functional Requirements Drawn from FWcPP</b>					
FAU_GEN.1	<p><b>ASA</b></p> <p>Shutdown and start-up of the audit functions are logged by events for reloading the TOE, and the events when the TOE comes back up. When audit is enabled, it is on whenever the TOE is on. Also, if logging is ever disabled, it is displayed in the ASDM Real-Time Log Viewer as a syslog disconnection and then a reconnection once it is re-established followed by an event that shows that the "logging enable" command was executed. See the table within this cell for other required events and rationale.</p> <p>The TOE generates events in the following format, with fields for date and time, type of event (the ASA-x-xxxxxx identifier code), subject identities, and outcome of the event:</p> <p>Nov 21 2012 20:39:21: %ASA-3-713194: Group = 192.168.22.1, IP = 192.168.22.1, Sending IKE Delete With Reason message: Disconnected by Administrator.</p> <p>Network interfaces have bandwidth limitations, and other traffic flow limitations that are configurable. When an interface has exceeded a limit for processing traffic, traffic will be dropped, and audit messages can be generated, such as:</p> <p>Nov 21 2012 20:39:21: %ASA-3-201011: Connection limit exceeded <i>cnt/limit</i> for <i>dir</i> packet from <i>sip/sport</i> to <i>dip/dport</i> on interface <i>if_name</i>.</p> <p>Nov 21 2012 20:39:21: %ASA-3-202011: Connection limit exceeded <i>econns/limit</i> for <i>dir</i> packet from <i>source_address/source_port</i> to <i>dest_address/dest_port</i> on interface <i>interface_name</i></p> <p>For more information on the required auditable events and the actual logs themselves, please refer to the Preparative Procedures &amp; Operational User Guide for the Common Criteria Certified Configuration.</p> <p>The following high-level events are auditable by the TOE:</p> <table> <tr> <th>Auditable Event</th><th>Rationale</th></tr> <tr> <td>Modifications to the group of users that are part of the authorized administrator role.</td><td>All changes to the configuration (and hence all security relevant administrator actions) are logged when the logging level is set to at least the 'notifications' level. These changes would fall into the category of configuration changes such as enabling or disabling features and services. The identity of the administrator taking the action and the user being affected (assigned to</td></tr> </table>	Auditable Event	Rationale	Modifications to the group of users that are part of the authorized administrator role.	All changes to the configuration (and hence all security relevant administrator actions) are logged when the logging level is set to at least the 'notifications' level. These changes would fall into the category of configuration changes such as enabling or disabling features and services. The identity of the administrator taking the action and the user being affected (assigned to
Auditable Event	Rationale				
Modifications to the group of users that are part of the authorized administrator role.	All changes to the configuration (and hence all security relevant administrator actions) are logged when the logging level is set to at least the 'notifications' level. These changes would fall into the category of configuration changes such as enabling or disabling features and services. The identity of the administrator taking the action and the user being affected (assigned to				

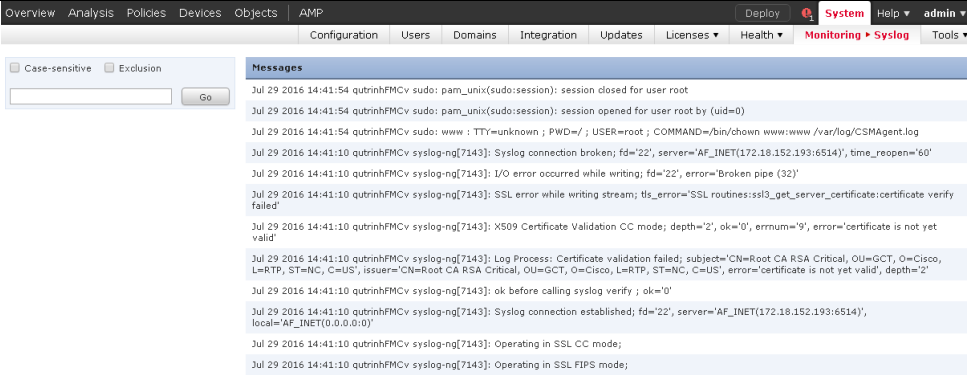


TOE SFRs	How the SFR is Satisfied	
		the authorized administrator role) are both included within the event.
	All use of the user identification mechanism.	Events will be generated for attempted identification/ authentication, and the username attempting to authenticate will be recorded in the event.
	Any use of the authentication mechanism.	Events will be generated for attempted identification/ authentication, and the username attempting to authenticate will be recorded in the event along with the origin or source of the attempt.
	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the user's capability to authenticate.	Failed attempts for authentication will be logged, and when the threshold is reached, it will also be logged. All changes to the configuration are logged when the logging level is set to at least the 'notifications' level. Changes to restore a locked account would fall into the category of configuration changes.
	All decisions on requests for information flow.	In order for events to be logged for information flow requests, the 'log' keyword may need to be in each line of an access control list. The presumed addresses of the source and destination subjects are included in the event.
	Success and failure, and the type of cryptographic operation	Attempts for VPN connections are logged (whether successful or failed). Requests for encrypted session negotiation are logged (whether successful or failed). The identity of the user performing the cryptographic operation is included in the event.
	Failure to establish and/or establishment/termination of an IPsec session	Attempts to establish an IPsec tunnel or the failure of an established IPsec tunnel is logged as well as successfully established and terminated IPsec sessions with peer.
	Establishing session with CA and IPsec peer	The connection to CA's or any other entity (e.g., CDP) for the purpose of certificate verification or revocation check is logged. In addition, the TOE can be configured to capture the packets' contents during the session establishment.
	Changes to the time.	Changes to the time are logged with old and new time values.

TOE SFRs	How the SFR is Satisfied	
	Use of the functions listed in this requirement pertaining to audit.	All changes to the configuration are logged when the logging level is set to at least the 'notifications' level. These changes would fall into the category of configuration changes.
	Loss of connectivity with an external syslog server.	Loss of connectivity with an external syslog server is logged as a terminated or failed cryptographic channel.
	Initiation of an update to the TOE.	TOE updates are logged as configuration changes.
	Termination of local and remote sessions. Note that the TOE does not support session locking, so there is no corresponding audit.	Termination of a local and remote session is logged. This also includes termination of remote VPN session as well. The user may initiate or the system may terminate the session based idle timeout setting.
	Initiation, termination and failures in trusted channels and paths.	Requests for encrypted session negotiation are logged (whether successful or failed). Similarly, when an established cryptographic channel or path is terminated or fails a log record is generated. This applies to HTTPS, TLS, and IPsec.
	Application of rules configured with the 'log' operation	Logs are generated when traffic matches ACLs that are configured with the log operation.
	Indication of packets dropped due to too much network traffic	Logs are generated when traffic that exceeds the settings allowed on an interface is received.
	FTP Connection	Logs are generated for all FTP connections.
<b><u>FP Services</u></b> Auditing is the recording of events within the system. The TOE generates log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting the audit function <sup>6</sup> , any use of an administrator command or action via the CLI and web interfaces, and all of the required auditable events identified in table above. For more		

<sup>6</sup> Note that the audit function cannot be disabled other than shutting down the entire system.

TOE SFRs	How the SFR is Satisfied
	<p>information about the required audit events, please refer to table above and the operational user guide (also known as the CC Supplemental User guide).</p> <p>The TOE can record activity on the system in two ways. The system can generate an audit record for each user interaction with the web interface and each command in the CLI interface in the audit log, and can also record system status messages in the system log (i.e., syslog). In addition, the TOE can generate traffic events as part of the intrusion and access control policies and these event records are stored in logs separate from the audit logs for performance and security reasons. More information about the traffic events is presented in IPS sections.</p> <p>FMC and Sensors log auditing information for all user activity in a read-only format. Modifications are not allowed by the interfaces and only authorized administrators can delete the audit logs. Audit logs are presented in a standard event view that allows administrators to view, sort, and filter audit log messages based on any item in the audit view. The audit view contains columns with information field for each audit event such as time, user, subsystem, message, and source IP. Please see the figure below for example.</p> <p style="text-align: center;">Figure 4: Audit View</p>  <p>The following fields are recorded for each audit event in the audit view:</p> <ul style="list-style-type: none"> <li><b>Time:</b> The time and date that the appliance generated the audit record.</li> <li><b>User:</b> The user name of the user that triggered the audit event.</li> <li><b>Subsystem:</b> The menu path the user followed to generate the audit record. For example, “System &gt; Monitoring &gt; Audit” is the menu path to view the audit log.</li> <li><b>Message:</b> The action the user performed. For example, “Page View” signifies that the user simply viewed the page indicated in the Subsystem, while “Save” means that the user clicked the Save button on the page.</li> <li><b>Source IP:</b> The IP address of the host used by the user.</li> </ul> <p style="text-align: center;">Figure 5: Syslog View</p>

TOE SFRs	How the SFR is Satisfied
	 <p>The user can also view the audit log using the command “show audit-log” or “show syslog” via the CLI interface. All GUI actions and CLI commands are recorded in the audit log and can only be viewed by authorized administrators. To distinguish between the two, the Subsystem field will identify “Command Line” for commands and the Message field will identify the executed command.</p> <p>In general, the logged audit records identify the date and time, the identity of the actor (e.g., user, daemon, or network host) responsible for the event, the subsystem that triggers the event, an indication of whether the event succeeded, failed or had some other outcome (if applicable), and the source IP (if applicable). The logged audit records also include event-specific content that includes at least all of the content required in table above.</p> <p>The TOE includes an internal log database implementation that can be used to store and review audit records locally. However, the internal log only stores a default of 100,000 entries in the local database (to configure the size, go to System &gt; Configuration &gt; Database, and click on “Audit Event Database”). When the audit log is full, the oldest audit records are overwritten by the newest audit records. In addition, the TOE also includes a local syslog storage in /var/log/messages. Similar to the audit log, when the syslog is full, the oldest syslogs messages are overwritten by the newest one.</p> <p>For audit log, the events are stored in partitioned event tables. The TOE will prune (i.e., delete) the oldest partition whenever the oldest partition can be pruned without dropping the number of events count below the configured event limit. Note this limit defaults to 10,000 if you set it any lower. For example, if you set the limit to 10,000 events, the events count may need to exceed 15,000 events before the oldest partition can be deleted. For syslog, the logs are stored in /var/log/messages and are rotated daily or when the log file size exceeds 25 MB. After the maximum number of backlog files is reached, the oldest is deleted and the numbers on the other backlogs file are incremented.</p> <p>To prevent the losing of critical audit records, the administrators can configure the system to transmit all the audit events (i.e., audit log and syslog) in real-time over a secure TLS connection to an external audit server in the operational environment. When an audit event is generated, it is sent to the local storage and external audit server simultaneously. This ensures that current audit events can be viewed locally while all events, new or old, are stored off-line as required by the FWcPP.</p>

TOE SFRs	How the SFR is Satisfied
	Note that the protection of the audit records stored at the external audit server is the responsibility of the operational environment. The TOE is only responsible for the secure communication channel. It is recommended that the audit server is physically or logically separated (e.g., VLANs) from the other networks.
FAU_GEN.2	<p><b><u>ASA and FP Services</u></b></p> <p>The TOE ensures each action performed by the administrator at the CLI, or via ASDM and FMC web UI is logged with the administrator's identity and as a result events are traceable to a specific user.</p>
FAU_STG_EXT.1	<p><b><u>ASA</u></b></p> <p>The TOE can be configured to export syslog records to an administrator-specified, external syslog server. The TOE can be configured to encrypt the communications with an external syslog server using IPsec or TLS.</p> <p>If using syslog through an IPsec tunnel, the TOE can be configured to block any new 'permit' actions that might occur. In other words, it can be configured to stop forwarding network traffic when it discovers it can no longer communicate with its configured syslog server(s).</p> <p>The TOE will buffer syslog messages locally, but the local buffer will be cleared when the TOE is rebooted. The default size of the buffer is 4KB, and can be increased to 16KB. When the local buffer is full, the oldest message will be overwritten with new messages. Only authorized administrators can configure the local buffer size, reboot the TOE, and configure the external syslog server.</p> <p><b><u>FP Services</u></b></p> <p>The TOE includes an internal log database implementation that can be used to store and review audit records locally. However, the internal log only stores a maximum of 100,000 entries in the local database. When the audit log is full, the oldest audit records are overwritten by the newest audit records (i.e., log rotation). To prevent the losing of critical audit records, the administrators can configure the system to transmit all the audit event logs in real-time over a secure TLS connection to an external audit server in the operational environment. When an audit event is generated, it is sent to the local database and external audit server simultaneously. This ensures that current audit events can be viewed locally while all events, new or old, are stored off-line as required by the FWcPP.</p>
FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), and FCS_RBG_EXT.1	<p><b><u>ASA</u></b></p> <p>In the TOE cryptographic functions are used to establish TLS, HTTPS, and IPsec sessions, for IPsec traffic and authentication keys, and for IKE authentication and encryption keys.</p> <p>Key generation for asymmetric keys on all models of the TOE implements ECDSA with NIST curve sizes P-256, P-384, and P-521 according to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 and RSA with key size 2048 bits according to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3.</p> <p>Key establishment for asymmetric keys on all models of the TOE implements</p>

TOE SFRs	How the SFR is Satisfied
	<p>ECDSA-based key establishment scheme as specified in NIST SP 800-56A “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and RSA-based key establishment schemes as specified in NIST SP 800-56B “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography” with key sizes greater than 112 bit key strength. In addition, ASA supports RFC 3526 section 3 domain parameters. Note that IPsec and TLS protocols can use either ECDSA or RSA. The TOE can act as either the sender or receiver in the RSA-based key establishment scheme depending on the connection.</p> <p>The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) with the added feature of read-verify. Additional key zeroization detail is provided in section 7.3. An example of manually triggering zeroization is: existing RSA and ECDSA keys will be zeroized when new RSA and ECDSA keys are generated, and zeroization of RSA and ECDSA keys can be triggered manually through use of the commands:</p> <pre>asa(config)#crypto key zeroize rsa [label key-pair-label] [default] [noconfirm] asa(config)#crypto key zeroize ec [label key-pair-label]</pre> <p>The TOE supports AES-CBC and AES-GCM, each with 128, 192, or 256-bit (as described in ISO 10116 and ISO 19772). The TOE uses a CAVP-validated implementation of AES with 128, 192, and 256 bit keys. Configuring the TOE software in or out of FIPS mode does not modify the TOE’s use of the CAVP-validated AES.</p> <ul style="list-style-type: none"> <li>Series: (ASA-5506-X, 5506-W, 5506-H, 5508-X, 5516-X), (ASA-5512-X, 5515-X, 5525-X, 5545-X, 5555-X), (5585-X SSP10/20/40/60) FIPS #<b>4249</b></li> </ul> <p>The TOE provides cryptographic signature services using RSA and ECDSA with key sizes (modulus) of 2048 bits, and 256, 384, and 521 bits, respectively. For RSA, the key size is configurable down to 1024, but only 2048 key size is permitted in the evaluated configuration.</p> <ul style="list-style-type: none"> <li>Series: (ASA-5506-X, 5506-W, 5506-H, 5508-X, 5516-X), (ASA-5512-X, 5515-X, 5525-X, 5545-X, 5555-X), (5585-X SSP10/20/40/60) FIPS #<b>2298</b> and <b>989</b></li> </ul> <p>The TOE supports key establishment including ECDSA-based scheme and RSA-based schemes. The RSA-based implementation is vendor affirmation and the ECC KAS CVL algorithm testing is provided below:</p> <ul style="list-style-type: none"> <li>Series: (ASA-5506-X, 5506-W, 5506-H, 5508-X, 5516-X), (ASA-5512-X, 5515-X, 5525-X, 5545-X, 5555-X), (5585-X SSP10/20/40/60) FIPS #<b>1002/1134</b></li> </ul> <p>The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512, and keyed-hash message authentication using HMAC-SHA-1 (160-bit), HMAC-SHA-256 (256-bit), HMAC-SHA-384 (384-bit), and HMAC-SHA-512 (512-bit) with block size of 64 bytes (HMAC-SHA-1 and HMAC-SHA-256) and 128 bytes (HMAC-SHA-384 and HMAC-SHA-512).</p>

TOE SFRs	How the SFR is Satisfied																					
	<ul style="list-style-type: none"><li>Series: (ASA-5506-X, 5506-W, 5506-H, 5508-X, 5516-X), (ASA-5512-X, 5515-X, 5525-X, 5545-X, 5555-X), (5585-X SSP10/20/40/60) FIPS #3486 and 2787</li></ul> <p>Random number generation in the TOE uses different methods depending on the underlying hardware. The ASA 5500 Series single-core platforms (5506, 5508, and 5516) and multi-core platforms (5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X) use an SP 800-90 Hash_DRBG with SHA-512. Random number generation in the ASA uses hardware ring oscillators from the third-party chip as the entropy source. More information is provided in the entropy design documentation.</p> <ul style="list-style-type: none"><li>Series: (ASA-5506-X, 5506-W, 5506-H, 5508-X, 5516-X), (ASA-5512-X, 5515-X, 5525-X, 5545-X, 5555-X), (5585-X SSP10/20/40/60) FIPS #1328</li></ul> <p><b>FP Services</b></p> <p>Each FMC and each sensor “TOE” utilizes a cryptographic module (i.e., Cisco FIPS Object Module) providing supporting cryptographic functions. When the term “TOE” is used in this section, it refers to each appliance. The algorithm implementations have been tested in accordance to validation suites set by the Cryptographic Algorithm Validation Program (CAVP). The following algorithms have been CAVP tested in accordance with the identified standards:</p> <p>Table 19: CAVP Algorithms</p> <table><tr><th>Algorithms</th><th>Standards</th><th>Certificate Numbers</th></tr><tr><td colspan="3"><b>Asymmetric Key Generation</b></td></tr><tr><td><ul style="list-style-type: none"><li>Domain parameter generation</li></ul></td><td>FIPS PUB 186-4 Appendix B.1, B.3, and B.4.</td><td>#2297 (RSA) #1197 (ECDSA) #1183 (ECC and FFC)</td></tr><tr><td colspan="3"><b>Encryption/Decryption</b></td></tr><tr><td><ul style="list-style-type: none"><li>AES (128 and 256 bits) in CBC and GCM mode</li></ul></td><td>FIPS PUB 197 NIST SP 800-38A NIST SP 800-38D</td><td>#4266</td></tr><tr><td colspan="3"><b>Cryptographic Signature Services</b></td></tr><tr><td><ul style="list-style-type: none"><li>RSA Digital Signature Algorithm (rDSA) (modulus 2048)</li></ul></td><td>FIPS PUB 186-4</td><td>#2297 (RSA) #1197 (ECDSA)</td></tr></table>	Algorithms	Standards	Certificate Numbers	<b>Asymmetric Key Generation</b>			<ul style="list-style-type: none"><li>Domain parameter generation</li></ul>	FIPS PUB 186-4 Appendix B.1, B.3, and B.4.	#2297 (RSA) #1197 (ECDSA) #1183 (ECC and FFC)	<b>Encryption/Decryption</b>			<ul style="list-style-type: none"><li>AES (128 and 256 bits) in CBC and GCM mode</li></ul>	FIPS PUB 197 NIST SP 800-38A NIST SP 800-38D	#4266	<b>Cryptographic Signature Services</b>			<ul style="list-style-type: none"><li>RSA Digital Signature Algorithm (rDSA) (modulus 2048)</li></ul>	FIPS PUB 186-4	#2297 (RSA) #1197 (ECDSA)
Algorithms	Standards	Certificate Numbers																				
<b>Asymmetric Key Generation</b>																						
<ul style="list-style-type: none"><li>Domain parameter generation</li></ul>	FIPS PUB 186-4 Appendix B.1, B.3, and B.4.	#2297 (RSA) #1197 (ECDSA) #1183 (ECC and FFC)																				
<b>Encryption/Decryption</b>																						
<ul style="list-style-type: none"><li>AES (128 and 256 bits) in CBC and GCM mode</li></ul>	FIPS PUB 197 NIST SP 800-38A NIST SP 800-38D	#4266																				
<b>Cryptographic Signature Services</b>																						
<ul style="list-style-type: none"><li>RSA Digital Signature Algorithm (rDSA) (modulus 2048)</li></ul>	FIPS PUB 186-4	#2297 (RSA) #1197 (ECDSA)																				

TOE SFRs	How the SFR is Satisfied		
	<b>Cryptographic Hashing</b>		
	<ul style="list-style-type: none"> <li>SHA-1, SHA-256, SHA-384, and SHA-512 (digest sizes 160, 256, 384 and 512 bits)</li> </ul>	FIPS PUB 180-4	#3512
	<b>Keyed-hash Message Authentication</b>		
	<ul style="list-style-type: none"> <li>HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 (message digest sizes 160, 256, 384, and 512 bits)</li> </ul>	FIPS PUB 198-1 FIPS PUB 180-4	#2811
	<b>Deterministic Random Bit Generation (DRBG)</b>		
	<ul style="list-style-type: none"> <li>DRBG</li> </ul>	NIST 800-90A	#1337
	<b>Key Establishment</b>		
	<ul style="list-style-type: none"> <li>RSA</li> <li>FFC (DH and DHE) and ECC (ECDSA and ECDHE)</li> </ul>	NIST 800-56A NIST 800-56B	Vendor assertion #1008 (CVL: SSH, TLS) #1196 (DSA) #1183 (ECC and FFC)
<p>The TOE supports RSA, FFC, and ECDSA in the evaluated configuration. RSA and ECDSA digital signature are used in TLS connections and SSH connections (RSA only). Key establishment for asymmetric keys on the TOE implements ECDSA-based and DH-based key establishment schemes as specified in NIST SP 800-56A “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”. In addition, the TOE also supports DH group 14 key establishment scheme that meets standard RFC 3526, section 3 for interoperability.</p> <p>The TOE uses a software-based random bit generator that complies with NIST 800-90A CTR_DRBG (AES-256) Deterministic Random Bit Generation (DRBG) operating in FIPS mode. In addition, the DRBG is seeded by an entropy source that is at least 256-bit value derived from various highly sensitive and proprietary noise sources described in the proprietary Entropy Design document.</p>			



TOE SFRs	How the SFR is Satisfied
	<p>Additionally, the TOE is designed to zeroize secret and private keys when they are no longer required by the TOE. This zeroization mechanism is performed by overwriting the sensitive keys and data with all 0's before deleting them, followed by a read-verify. The table in section 7.3 identifies the applicable secret and private keys and summarizes, how they are generated, what are their purpose, where are they stored, and when and how are they deleted.</p>
<p>FCS_HTTPS_EXT.1 FCS_TLSC_EXT.2 FCS_TLSS_EXT.1</p>	<p><b><u>ASA</u></b></p> <p>The TOE implements HTTP over TLS (or HTTPS) to support remote administration using ASDM, and TLS to support secure syslog connection. A remote administrator can connect over HTTPS to the TOE with their web browser and load the ASDM software from the ASDM.</p> <p>The TOE supports TLS v1.2 and TLSv1.1 connections with any of the following ciphersuites:</p> <ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_128_CBC_SHA256</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA256</li> <li>• TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</li> <li>• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</li> </ul> <p>When the TOE acts as a TLS client, the administrators can specify the reference-identity using the following command:</p> <pre>asa(config)#crypto ca reference-identity <i>reference-identity-name</i></pre> <p>follow by one or more of the values</p> <p>cn-id <i>value</i></p> <p>dns-id <i>value</i></p> <p>srv-id <i>value</i></p> <p>uri-id <i>value</i></p> <p>For example,</p> <pre>ciscoasa(config)# crypto ca reference-identity syslogServer ciscoasa(config-ca-ref-identity)# cn-id syslog.cisco.com</pre> <p>To configure the syslog server certification<sup>7</sup> verification, use this syntax:</p> <pre>logging host <i>interface_name</i> <i>syslog_ip</i> [tcp/port / udp/port] [format emblem] [secure</pre>

<sup>7</sup> Certificate pinning is not supported. In addition, IP address and wildcards are not supported in the ID.

TOE SFRs	How the SFR is Satisfied
	<p>[reference-identity <i>reference_identity_name</i>]] [permit-hostdown]</p> <p>For example,  ciscoasa(config)# logging host outside 10.86.93.123 tcp/6514 secure <b>reference-identity</b> syslogServer</p> <p>NIST “secp” curves are supported for all TLS connections by default but mutual authentication must be configured with the client-side X.509v3 certificate.</p> <p>The TOE can be configured to specify which TLS versions are supported using  asa(config)#ssl <b>client-version</b> {<del>tlsv1</del> / tlsv1.1 / tlsv1.2}  asa(config)#ssl <b>server-version</b> {<del>tlsv1</del> / tlsv1.1 / tlsv1.2}</p> <p>The key agreement parameters of the server key exchange message are specified in the RFC 5246 (section 7.4.3) for TLSv1.2 and RFC 4346 (section 7.4.3) for TLSv1.1. The TOE conforms to both RFCs supporting both RSA 2048 bits and NIST curves <u>secp256r1</u>, <u>secp384r1</u>, <u>secp521r1</u>.</p> <p><b><u>FP Services</u></b></p> <p>The supporting cryptographic algorithms identified in the FCS SFRs are included to support the SSHv2 (RFCs 4251, 4252, 4253, and 4254) and TLSv1.1/TLSv1.2 (RFC 4346/5246)/HTTPS (RFC 2818) security communication protocols. Note that IPsec communication protocol is not supported for FP Services.</p> <p>When CC mode is enabled, the TOE is restricted to only support TLSv1.1 and TLSv1.2 with AES 128 or 256 bit symmetric ciphers in CBC and GCM modes, in conjunction with SHA and RSA. The following TLS cipher suites are implemented by the TOE in CC mode:</p> <ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA (client and server)</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA (client and server)</li> <li>• TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (client only)</li> <li>• TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (client only)</li> <li>• TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (client only)</li> <li>• TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (client only)</li> <li>• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (client only)</li> <li>• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (client and server)</li> <li>• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (server only)</li> </ul> <p>While CiscoSSL supports additional cipher suites (for example, RSA_3DES_EDE_CBC_SHA, RSA_DES_CBC_SHA, RSA_RC4_128_MD5, RSA_RC4_128_SHA, etc.), they are all disabled while operating in CC mode. If the TLS client does not support TLSv1.1 or TLSv1.2, the TLS connection will fail and the administrators will not establish a HTTPS web-based session with the TOE.</p>

TOE SFRs	How the SFR is Satisfied
	<p>Optionally, the TOE can be configured with “client-verify enable” in which case the client will be required to provide a certificate suitable for authentication via the TLS protocol (i.e., mutual authentication). If that certificate-based authentication fails, no session will be established and the client user cannot further attempt to log in. If that succeeds, the user is still required to provide a username and password in order to log in to obtain access to security management functions. By default, the TLS protocol only uses server-side authentication whereby the server must provide a trusted server certificate for authentication.</p> <p>When in CC mode and the TOE acts as a TLS client (e.g., connection to the syslog server), the TOE will verify the server Common Name (CN) and/or Subject Alternative Name (SAN) against the reference identity (wildcard is supported as required in section 6 of RFC 6125). If verification fails, the TLS connection will not be established. Mutual authentication must be configured with the client-side X.509v3 certificate with RSA 2048-bits (or higher) and SHA-256 (or higher). The key agreement parameters of the server key exchange message are specified in the RFC 5246 (section 7.4.3) for TLSv1.2 and RFC 4346 (section 7.4.3) for TLSv1.1. The TOE conforms to both RFCs.</p>
FCS_IPSEC_EXT.1	<p><b><u>ASA Only</u></b></p> <p>The IPsec implementation provides both VPN peer-to-peer (i.e., site-to-site) and VPN client to TOE (i.e., remote access) capabilities. The VPN peer-to-peer tunnel allows for example the TOE and another TOE to establish an IPsec tunnel to secure the passing of user data. Another configuration in the peer-to-peer configuration is to have the TOE be set up with an IPsec tunnel with a VPN peer to secure the session between the TOE and syslog server. The VPN client to TOE configuration would be where a remote VPN client connects into the TOE in order to gain access to an authorized private network. Authenticating with the TOE would give the VPN client a secure IPsec tunnel to connect over the internet into their private network.</p> <p>The TOE implements IPsec to provide both certificates and pre-shared key-based authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE implementation of the IPsec standard (in accordance with the RFCs noted in the SFR) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services. In addition, the TOE supports both transport and tunnel modes. Transport mode is only supported for peer-to-peer IPsec connection while tunnel mode is supported for all VPN connections including remote access.</p> <p>IPsec Internet Key Exchange, also called IKE, is the negotiation protocol that lets two peers agree on how to build an IPsec Security Association (SA). In the evaluated configuration, only IKEv2 is supported. The IKEv2 protocols implement Peer Authentication using the RSA, ECDSA algorithm with X.509v3 certificates, or pre-shared keys. IKEv2 separates negotiation into two phases: SA and Child SA. IKE SA creates the first tunnel, which protects later IKE negotiation messages. The key negotiated in IKE SA enables IKE peers to communicate securely in IKE Child SA. During Child SA IKE establishes the IPsec SA. IKE</p>

TOE SFRs	How the SFR is Satisfied
	<p>maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including:</p> <ul style="list-style-type: none"> <li>• The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based),</li> <li>• The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and</li> <li>• The agreement of secure bulk data encryption AES keys for use with ESP. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation</li> </ul> <p>The TOE implements IPsec using the ESP protocol as defined by RFC 4303, using the cryptographic algorithms AES-CBC-128, AES-CBC-256, AES-GCM-128 and AES-GCM-256 (both specified by RFCs 3602 and 4106) along with SHA-based HMAC algorithms, and using IKEv2, as specified for FCS_IPSEC_EXT.1.5, to establish security associations. NAT traversal is supported in IKEv2 by default.</p> <p>The IKE SA exchanges use only main mode and the IKE SA lifetimes are able to be limited to 24 hours for Phase 1 (SAs) and 8 hours for Phase 2 (Child SAs). Furthermore, the IKE SA lifetime limits can be configured so that no more than 200 MB of traffic can be exchanged for IKE Child SAs. Administrators can require use of main mode by configuring the mode for each IPsec tunnel, as in the following examples:</p> <pre>asa(config)#crypto map map-name seq-num set ikev2 phase1-mode main asa(config)# crypto ipsec security-association lifetime {seconds seconds / kilobytes kilobytes} asa(config-ikev2-policy)# lifetime seconds seconds</pre> <p>In the evaluated configuration, use of “confidentiality only” (i.e. using ESP without authentication) for IPsec connections is prohibited. The TOE allows the administrator to define the IPsec proposal for any IPsec connection to use specific encryption methods and authentication methods as in the following examples:</p> <pre>asa(config)#crypto ipsec ikev2 ipsec-proposal proposal tag proposal_name asa(config-ipsec-proposal)#protocol esp encryption {aes   aes-192   aes-256   aes-gcm   aes-gcm-192   aes-gcm-256   <del>aes-gmac   aes-gmac-192   aes-gmac-256</del>} asa(config-ipsec-proposal)#protocol esp integrity {sha-1   sha-256   sha-384   sha-512   null}</pre> <p><b>Note:</b> When AES-GCM is used for encryption, the ESP integrity selection will be “null” because GCM mode provides integrity. AES-GMAC is not allowed in the evaluated configuration.</p> <p>In the evaluated configuration, the IKEv2 protocols supported by the TOE implement the following DH groups: 14 (2048-bit MODP), 19 (256-bit Random ECP), 20 (384-bit Random EC), and use the RSA and ECDSA algorithms for Peer Authentication. The following command is used to specify the DH Group used for SAs:</p> <pre>asa(config)#crypto ikev2 policy priority policy_index</pre>

TOE SFRs	How the SFR is Satisfied
	<pre>asa(config-ikev2-policy)#<b>encryption</b> [<del>null</del>   <del>des</del>   <del>3des</del>   aes   <del>aes-192</del><sup>8</sup>   aes-256   aes-gcm   <del>aes-gcm-192</del>   aes-gcm-256]</pre> <pre>asa(config-ikev2-policy)#<b>integrity</b> [<del>md5</del>   sha   sha256   sha384   sha512]</pre> <pre>asa(config-ikev2-policy)#<b>group</b> { 14   19   20   <del>24</del>}</pre> <pre>asa(config-ikev2-policy)#<b>prf</b> { sha   sha256   sha384   sha512 }</pre> <p>The secret ‘x’ generated is 64 bytes long (or 512 bits), is the same across all the DH groups, and is generated with the DRBG specified in FCS_RBG_EXT.1. This is almost double the size of the highest comparable strength value which is 384 bits.</p> <p>The TOE has a configuration option to deny tunnel if the phase 2 SA is weaker than the phase 1. The crypto strength check is enabled via the <b>crypto ipsec ikev2 sa-strength-enforcement</b> command.</p> <p>The TOE can be configured to authenticate IPsec connections using RSA and ECDSA signatures. When using RSA and ECDSA signatures for authentication, the TOE and its peer must be configured to obtain certificates from the same certification authority (CA).</p> <p>To configure an IKEv2 connection to use a RSA or ECDSA signature:</p> <pre>asa(config)#<b>tunnel-group</b> <i>name</i> <b>ipsec-attributes</b></pre> <pre>asa(config-tunnel-ipsec)#<b>ikev2</b> { local-authentication   remote-authentication } <b>certificate</b> <i>trustpoint</i></pre> <p>Pre-shared keys can be configured in TOE for IPsec connection authentication. However, pre-shared keys are only supported when using IKEv2 for peer-to-peer VPNs. The text-based pre-shared keys can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, “)”, “?”, space “ ”, tilde~, hyphen-, underscore_, plus+, equal=, curly-brackets{ }, square-brackets[, vertical-bar(pipe) , forward-slash/, back-slash\, colon:, semi-colon;, double-quote“, single-quote‘, angle-brackets&lt;&gt;, comma,, and period.. The text-based pre-shared keys can be 1-128 characters in length and is conditioned by a “prf” (pseudo-random function) configurable by the administrator. The bit-based pre-shared keys can be entered as HEX value as well. When using pre-shared keys for authentication, the IPsec endpoints must both be configured to use the same key.</p> <p>To configure an IKEv2 connection to use a pre-shared key:</p> <pre>asa(config)#<b>tunnel-group</b> <i>name</i> <b>ipsec-attributes</b></pre> <pre>asa(config-tunnel-ipsec)#<b>ikev2</b> { local-authentication   remote-authentication } <b>pre-shared-key</b> <i>hex key-value</i></pre> <p>To configure the reference identifier, please use the following command:</p>

<sup>8</sup> 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\*.

TOE SFRs	How the SFR is Satisfied
	<p>asa(config)#<b>crypto ca reference-identity</b> <i>reference-identity-name</i></p> <p>follow by one or more of the values</p> <p>cn-id <i>value</i></p> <p>dns-id <i>value</i></p> <p>srv-id <i>value</i></p> <p>uri-id <i>value</i></p> <p>Specifying the <b>reference-identity</b> keyword enables RFC 6125 (section 6.0) checks and identifies the reference identity to use by name.</p> <p>A crypto map (the Security Policy Definition) set can contain multiple entries, each with a different access list. The crypto map entries are searched in a top-down sequence - the TOE attempts to match the packet to the crypto access control list (ACL) specified in that entry. The crypto ACL can specify a single address or a range of address and the crypto map can be applied to an inbound interface or an outbound interface. When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map of that interface is applied. If the crypto map entry is tagged as ipsecisakmp, IPsec is triggered. The traffic matching the permit crypto ACLs would then flow through the IPSec tunnel and be classified as PROTECTED. Traffic that does not match a permit crypto ACL or match a deny crypto ACL in the crypto map, but is permitted by other ACLs on the interface is allowed to BYPASS the tunnel. Traffic that does not match a permit crypto ACL or match a deny crypto ACL in the crypto map, and is also blocked by other non-crypto ACLs on the interface would be DISCARDED.</p>
FCS_SSHS_EXT.1	<p><b><u>FP Services</u></b></p> <p>The TOE supports SSHv2 with AES (in CBC or GCM mode) 128 or 256 bits cipher for encryption, in conjunction with HMAC-SHA1, HMAC-SHA-256, or HMAC-SHA-512 for integrity and authenticity, and RSA with diffie-hellman-group14-sha1 for the key exchange method. While DES and 3DES, HMAC-MD5 and HMAC-MD5-96, and diffie-hellman-group-1 and other diffie-hellman-exchange groups are all implemented, they are disabled while the TOE is operating in CC Mode. In addition, SSHv1 is also disabled by default for security reasons. If the SSH client (in the operational environment) does not support the Approved algorithms or SSH version, the SSH connection will be rejected by the TOE (SSH server) and the administrators will not establish an SSHv2 web-based session with the TOE.</p> <p>The TOE uses OpenSSH implementation version 7.2p2 to support the SSHv2 connections. The authentication timeout period is 90 seconds allowing clients to retry only 3 times. In addition, both public-key (RSA) and password-based authentication can be configured with password-based being the default method used. The SSH packets are limited to 256 Kbytes. If OpenSSH detects packet larger than maximum (#define PACKET_MAX_SIZE (256 * 1024)), then it will drop the packet. Whenever the timeout period or authentication retry limit is reached, the TOE closes the applicable TCP connection and releases the SSH session resources. As SSH packets are being received, the TOE uses a buffer to build all packet information. Once complete, the packet is checked to ensure it can be appropriately</p>

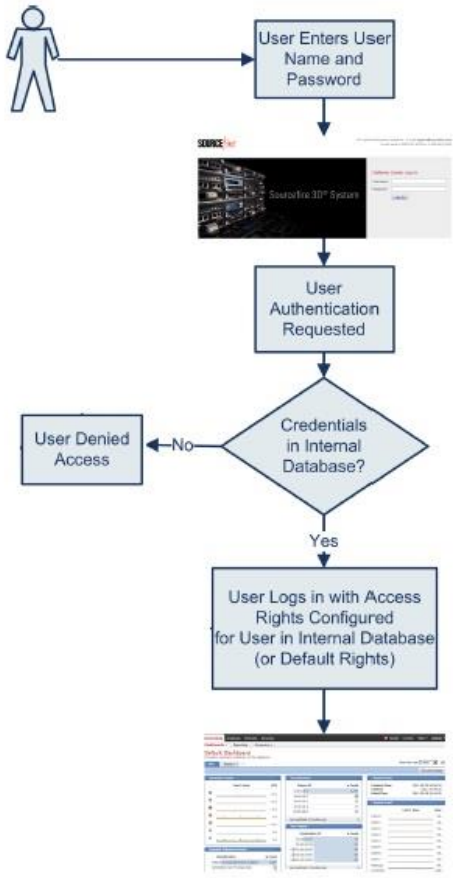
TOE SFRs	How the SFR is Satisfied
	decrypted. However, if it is not complete when the buffer becomes full (256 Kbytes) the packet will be dropped. Note that the TOE manages a tracking mechanism for each SSH session so that it can initiate a new key exchange when either approximately 1 hour of time or 1GB of data is reached. An audit event is generated when a successful SSH rekey occurs.
FDP_RIP.2	<p><b><u>ASA Only</u></b></p> <p>The TOE ensures that packets transmitted through the TOE do not contain residual information from previous packets. Packets that are not the required length use zeros for padding. Residual data is never transmitted from the TOE. Packet handling within memory buffers ensures new packets cannot contain portions of previous packets. This applies to data plane traffic and even administrative session traffic.</p>
FIA_PMG_EXT.1	<p><b><u>ASA</u></b></p> <p>The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters as listed in the SFR. Minimum password length is settable by the Authorized Administrator, and support passwords of 8 to 127 characters. Password composition rules specifying the types and number of required characters that comprise the password are settable by the Authorized Administrator. Passwords can be configured with a maximum lifetime, configurable by the Authorized Administrator. New passwords can be required to contain a minimum of 4 character changes from the previous password.</p> <p><b><u>FP Services</u></b></p> <p>When creating or changing passwords, the passwords must be composed of upper and lower case letters, numbers and special characters including blank space and ~!@#\$%^&amp;*()_+={ } []\:'&gt;,&lt;./?. The password must have at least one upper case, one lower case, one number, and one special character. This is configured by checking on “Check Password Strength<sup>9</sup>” option per each user (See CC Supplement User Guide for details). Also, the passwords have to satisfy configured minimum password length which is set in the System Policy for all users. The minimum password length can range from 8 (default) to 32 characters (maximum) long, which includes 15 characters required by the NDcPP. Note: The user password is limited to 32 characters maximum.</p>
FIA_UIA_EXT.1	<p><b><u>ASA</u></b></p> <p>The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Administrative access to the TOE is facilitated through the TOE’s CLI (SSH over IPsec or console), and through the GUI (ASDM). The TOE mediates all administrative actions through the CLI and GUI. Once a potential administrative user attempts to access an administrative</p>

<sup>9</sup> This option also prevents dictionary words or consecutive repeating characters.

TOE SFRs	How the SFR is Satisfied
	<p>interface either locally or remotely, the TOE prompts the user for a user name and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated.</p> <p>The TOE provides an automatic lockout when a user attempts to authenticate and enters invalid credentials. After a defined number of authentication attempts fail exceeding the configured allowable attempts, the user is locked out until an authorized administrator can unlock the user account.</p> <p><b><u>FP Services</u></b></p> <p>The TOE is designed to successfully identify and authenticate user before allowing access to the TOE's security function. When identification and authentication data is entered (username and password), the TOE attempts to identify the applicable user account from the provided identity and if a match is found, the password provided is hashed with a salt value and compared against the stored hash<sup>10</sup> with the user account information in the internal database. If a user account cannot be associated with the provided identity or the hashed password does not match that stored hash with the user account information, the process will fail. No actions are allowed, other than re-entry of identification and authentication data or viewing the login banner. Once the user has successfully log in, the privilege level or role will control what management functions he or she has access and authorization to. Figure below shows the authentication process.</p> <p style="text-align: center;">Figure 6: Authentication Process</p>

<sup>10</sup> The password is hashed with Approved SHA-512 and the salt value is 32-bit long.



TOE SFRs	How the SFR is Satisfied
	 <pre> graph TD     User((User)) --&gt; Step1[User Enters User Name and Password]     Step1 --&gt; Step2[User Authentication Requested]     Step2 --&gt; Decision{Credentials in Internal Database?}     Decision -- No --&gt; Step3[User Denied Access]     Decision -- Yes --&gt; Step4[User Logs in with Access Rights Configured for User in Internal Database (or Default Rights)]     Step4 --&gt; Step5[Dashboard]   </pre> <p>Users can connect to the TOE via a local console or remotely using SSHv2 or HTTPS. In each case, the user is required to log in prior to successfully establishing a session through which TOE security functions can be performed. By default, the Cisco NGIPS System uses internal authentication to check user credentials when a user logs in. Alternately, the TOE can be configured to use an external authentication server for user identification and authentication. For FP and in the evaluated configuration, the use of an external authentication server such as RADIUS or LDAP is not allowed.</p>
FIA_UAU_EXT.2	<p><b><u>ASA</u></b></p> <p>The TOE provides a local password based authentication mechanism as well as RADIUS authentication.</p> <p>The administrator authentication policies include authentication to the local user database or redirection to a remote authentication server. Interfaces can be configured to try one or more remote authentication servers, and then fall back to the local user database if the remote authentication servers are inaccessible.</p> <p>The TOE can invoke an external authentication server to provide a single-use authentication mechanism by forwarding the authentication requests to the external</p>

TOE SFRs	How the SFR is Satisfied
	<p>authentication server (when configured by the TOE to provide single-use authentication).</p> <p>The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via SSHv2 over IPsec or TLS. At initial login in the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access (if the combination of username and password is correct) or indicates that the login was unsuccessful. The TOE does not provide indication of whether the username or password was the reason for an authentication failure.</p> <p><b><u>FP Services</u></b></p> <p>See previous section.</p>
FIA_UAU.7	<p><b><u>ASA</u></b></p> <p>When a user enters their password at the local console, the TOE displays only ‘*’ characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.</p> <p><b><u>FP Services</u></b></p> <p>When logging in, the TOE will not echo passwords such that passwords are not inadvertently displayed to the user and any other users that might be able to view the login display. The TOE replaced the entered password character with a “*” character or not show any character at all. This depends on where the user is logging in from, for example, using web GUI versus the SSH client. If the authentication fails, the TOE is designed to not indicate either the username and/or password were incorrect. The error message would just state access denied or unable to authorize access. No other information about the failed login in can be ascertained from the error message.</p> <p>Note also that should a user have their session terminated (e.g., due to inactivity), they are required to successfully re-authenticate, by re-entering their identity and authentication data, in order to gain access to their session. The authentication data is not cached by the TOE for any reason.</p>
FIA_X509_EXT.1 FIA_X509_EXT.2 FIA_X509_EXT.3	<p><b><u>ASA</u></b></p> <p>The TOE support X.509v3 certificates as defined by RFC 5280. 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.</p> <p>The validity check for the certificates takes place at session establishment and/or at time of import depending on the certificate type. For example, server certificate is checked at session establishment while CA certificate is checked at both. The TOE conforms to standard RFC 5280 for certificate and path validation (i.e., peer certificate checked for expiration, peer certificate checked if signed by a trusted CA</p>

TOE SFRs	How the SFR is Satisfied
	<p>in the trust chain, peer certificate checked for unauthorized modification, peer certificate checked for revocation).</p> <p>The TOE can generate a RSA or ECDSA key pair that can be embedded in a Certificate Signing Request (CSR) created by the TOE. The key pair can be generated with the following command:</p> <pre>asa(config)#crypto key generate [rsa [general-keys   label &lt;name&gt;   modules [512+768+1024+2048   4096]   noconfirm   usage-keys]   ecdsa [label &lt;name&gt;   elliptic-curve [256   384   521]   noconfirm]]</pre> <p>The TOE can then send the CSR manually to a Certificate Authority (CA) for the CA to sign and issue a certificate. Once the certificate has been issued, the administrator can import the X.509v3 certificate into the TOE. Integrity of the CSR and certificate during transit are assured through the use of digital signature (signing the hash of the TOE's public key contained in the CSR and certificate). Both OCSP and CRL are configurable and may be used for certificate revocation check. Checking is also done for the basicConstraints extension and the cA flag to determine whether they are present and set to TRUE. If they are not, the CA certificate is not accepted as a trustpoint.</p> <p>The administrators can configure a trustpoint and associate it with a crypto map. This will tell the TOE which certificate(s) to use during the validation process. When the TOE cannot establish a connection for the validity check (e.g., CRL checking) or if the peer certificate is invalid (see above), the trusted channel is not established. The TOE can configure the expected domain name/hostname (i.e., reference identifier) and compare the TLS server's certificate Common Name (CN) and/or Subject Alternative Name (SAN) to the reference identifier based on section 6 of RFC 6125. If there is no match, the trust channel is not established. For more information, please refer to the Preparative Procedures &amp; Operational User Guide for the Common Criteria Certified Configuration.</p> <p><b><u>FP Services</u></b></p> <p>The TOE support X.509v3 certificates as defined by RFC 5280. Public key infrastructure (PKI) credentials, such as private keys and certificates are stored securely. The identification and authentication, and authorization security functions protect an unauthorized user from gaining access to the storage.</p> <p>The validity check for the certificates takes place at session establishment and/or at time of import depending on the certificate type. For example, server certificate is checked at session establishment while CA certificate is checked at both. The TOE conforms to standard RFC 5280 for certificate and path validation (i.e., peer certificate checked for expiration, peer certificate checked if signed by a trusted CA in the trust chain, peer certificate checked for unauthorized modification, peer certificate checked for revocation).</p> <p>The TOE can generate a RSA key pair that can be embedded in a Certificate Signing Request (CSR) created by the TOE. The CSR can be generated at the UI. The TOE can then send the CSR manually to a Certificate Authority (CA) for the CA to sign and issue a certificate. Once the certificate has been issued, the administrator can import the X.509v3 certificate into the TOE. Integrity of the CSR and certificate</p>

TOE SFRs	How the SFR is Satisfied
	<p>during transit are assured through the use of digital signature (signing the hash of the TOE's public key contained in the CSR and certificate). CRL is configurable and can be used for certificate revocation check. Checking is also done for the 'basicConstraints' extension and the 'cA' flag to determine whether they are present and set to TRUE. If they are not, the CA certificate is not accepted as a trust anchor.</p> <p>The administrators can configure a trust chain by importing the CA certificate(s) that signed and issued the server (syslog) certificate. This will tell the TOE which CA certificate(s) to use during the validation process. If the TOE does not find the trusted root CA, the TLS connection to the syslog server will fail. When the TOE cannot establish a connection for the validity check (e.g., CRL checking), the trusted channel is not established. For more information, please refer to the CC Supplemental User Guide.</p>
FMT_MOF.1(1)/ TrustedUpdate  FMT_MOF.1(1)/ AdminAct  FMT_MOF.1(2)/ AdminAct	<p><b><u>ASA and FP Services</u></b></p> <p>The TOE restricts the ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE to an authorized administrator. The TOE provides the ability for authorized administrators to initiate TOE update, enable or disable service and features, and access TOE data, such as audit data, configuration data, security attributes, information flow rules, and session thresholds.</p>
FMT_MTD.1	<p><b><u>ASA</u></b></p> <p>The TOE provides the ability for authorized administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds. The TOE also restricts access to TSF data so that no manipulation can be performed by non-administrators. Each of the predefined and administratively configured privilege level has default set of permissions that will grant them access to the TOE data, though with some privilege levels, the access is limited. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged levels. For the purposes of this evaluation, the privileged level is equivalent to full administrative access to the CLI or GUI, and equivalent to privilege level 15. The term "authorized administrator" or "Security Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action.</p> <p><b><u>FP Services</u></b></p> <p>The TOE provides a web-based GUI (using HTTPS) management interface and CLI or shell (using SSH or serial connection) for all TOE administration, including the policy rule sets, user accounts and roles, and audit functions. The ability to manage various security attributes, system parameters and all TSF data is controlled and limited to those users who have been assigned the appropriate administrative role and privileges associated with those roles. Note that all users created are TOE administrators.</p>
FMT_SMF.1	<p><b><u>ASA</u></b></p> <p>The TOE is configured to restrict the ability to enter privileged configuration mode to level 15 users (the authorized administrator) once AAA authorizations has been</p>

TOE SFRs	How the SFR is Satisfied
	<p>enabled. Privileged configuration (EXEC) mode is where the commands are available to modify user attributes ('username' and 'password' commands), operation of the TOE ('reload'), authentication functions ('aaa' commands), audit trail management ('logging' commands), backup and restore of TSF data ('copy' commands), communication with authorized external IT entities ('ssh' and 'access list' commands), information flow rules ('access list' commands), modify the timestamp ('clock' commands), specify limits for authentication failures ('aaa local authentication logout'), etc. These commands are not available outside of this mode. Communications with external IT entities, include the host machine for ASDM. This is configured through the use of 'https' commands that enable communication with the host and limit the IP addresses from which communication is accepted.</p> <p>Note that the TOE does not provide services (other than connecting using HTTPS, and establishment of VPNs) prior to authentication so there are no applicable commands. There are specific commands for the configuration of cryptographic services. Trusted updates to the product can be verified using cryptographic digital signature.</p> <p>The ASDM uses the same privileges that the user would have at the CLI to determine access to administrative functions in the ASDM GUI. All administrative configurations are done through the 'Configuration' page.</p> <p><b><u>FP Services</u></b></p> <p>See previous section.</p>
FMT_SMR.2	<p><b><u>ASA</u></b></p> <p>The TOE supports multiple levels of administrators, the highest of which is a privilege 15. In this evaluation, privilege 15 would be the equivalent of the authorized administrator with full read-write access. Multiple level 15 administrators with individual usernames can be created.</p> <p>Through the CLI the 'username' command is used to maintain, create, and delete users. Through ASDM this is done on the 'Configuration &gt; Device Management &gt; Users/AAA &gt; User Accounts' page.</p> <p>Usernames defined within the local user database are distinguished based on their privilege level (0-15) and the service-type attribute assigned to the username, which by default is "admin", allowing the username to authenticate (with valid password) to admin interfaces.</p> <p>'aaa authentication ssh console LOCAL' can be used to set the TOE to authenticate SSH users against the local database.</p> <p>'aaa authorization exec' can be used to require re-authentication of users before they can get to EXEC mode.</p> <p>The TOE also supports creating of VPN User accounts, which cannot login locally to the TOE, but can only authenticate VPN sessions initiated from VPN Clients. VPN users are accounts with privilege level 0, and/or with their service-type attribute set to "remote-access".</p>

TOE SFRs	How the SFR is Satisfied
	<p>When command authorization has been enabled the default sets of privileges take effect at certain levels, and the levels become customizable.</p> <ul style="list-style-type: none"> <li>When “aaa authorization command LOCAL” has NOT been applied to the config: <ul style="list-style-type: none"> <li>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.</li> <li>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).</li> <li>Usernames with privilege levels 2-14 can login to ASDM, and have full read-write access.</li> <li>Privilege levels cannot be customized.</li> </ul> </li> <li>When “aaa authorization command LOCAL” has been applied to the config: <ul style="list-style-type: none"> <li>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.</li> <li>Privilege levels (including levels 3 and 5) can be customized from the default to add/remove specific privileges.</li> </ul> </li> </ul> <p>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”.</p> <p><b><u>FP Services</u></b></p> <p><b>Predefined User Roles</b></p> <p>The TOE supports the following predefined user roles:</p> <ul style="list-style-type: none"> <li><b>Administrators</b> can set up the appliance’s network configuration, manage user accounts, and configure system policies and system settings. The Administrator Role provides access to analysis and reporting features, rule and policy configuration, system management, and all maintenance features. Users with the Administrator role have ALL access rights.</li> </ul> <p>Note: For all non-IPS management functions, the only TOE user role is “Administrator”. This role is granted when a new user account is created and cannot be changed. The IPS Administrator will also be referred to as the “Administrator”. More details on additional IPS roles will be provided in the FMT_SMR.2/IPS section below.</p> <p><b>CLI and CLI Access levels</b></p> <p>The administrator can use the CLI to view, configure, and troubleshoot the NGIPS systems. When administrators create a user account, they can assign it one of the following CLI access levels:</p>

TOE SFRs	How the SFR is Satisfied
	<ul style="list-style-type: none"> <li>• <b>Basic</b> The user has read-only access and cannot run commands that impact system performance.</li> <li>• <b>Configuration</b> The user has read-write access and can run commands that impact system performance.</li> <li>• <b>None</b> The user is unable to log in.</li> </ul> <p>Note that the CLI contains only a subset of all available functions and is only available on the Sensor. The web GUI is available on both the FMC and Sensor. The web GUI on the FMC is highly recommended for daily management of the FMC and its managed Sensors. Local access to the shell which allows access to the underlying operating system is allowed in the CC evaluated configuration for the initial configuration only. For normal daily operations, the web GUI is still the recommended method.</p>
FPT_SKP_EXT.1	<p><b><u>ASA</u></b></p> <p>The TOE stores all private keys in a secure directory (an ‘opaque’ virtual filesystem in RAM called “system:”) that is not readily accessible to administrators. All pre-shared and symmetric keys are stored in encrypted form, or are masked when showing the configuration via administrative interfaces (CLI or GUI).</p> <p><b><u>FP Services</u></b></p> <p>The TOE is designed to not to disclose or store plaintext passwords (e.g., passwords are never recorded in the audit records or display during authentication process). The passwords are stored hashed using Approved SHA-512 with a 32-bit salt value. Only ‘root’ user account with access to the shell can view the hashed passwords and this is prohibited in the evaluated configuration. The same is true for cryptographic keys such as encryption symmetric keys and private keys. The public keys can be viewed but cannot be modified without detection. Note that access to public keys is restricted to administrators.</p>
FPT_APW_EXT.1	<p><b><u>ASA</u></b></p> <p>The TOE includes a Master Passphrase features that can be used to configure the TOE to encrypt all locally defined user passwords. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators.</p> <p><b><u>FP Services</u></b></p> <p>See previous section.</p>
FPT_STM.1	<p><b><u>ASA</u></b></p> <p>The ASA provides a source of date and time information for the firewall, used in audit timestamps, in validating service requests, and for tracking time-based actions related to session management including timeouts for inactive administrative sessions (FTA_SSL_EXT.*), and renegotiating SAs for IPsec tunnels (FCS_IPSEC_EXT.1). This function can only be accessed from within the configuration exec mode via the privileged mode of operation of the firewall. The clock function is reliant on the system clock provided by the underlying hardware.</p>

TOE SFRs	How the SFR is Satisfied
	<p>This functionality can be set at the CLI using the ‘clock’ commands or in ASDM through the ‘Configuration &gt; Device Setup &gt; System Time’ page. The TOE can optionally be set to receive time from an NTP server.</p> <p>The clock’s date and time can be adjusted by authorized administrators, and authorized administrators can configure the TOE to use clock updates from NTP servers. The TOE supports use of NTP version 3, which supports use of hashing to authenticate clock updates, but use of any hashing method in NTPv3 is outside the scope of this Common Criteria evaluation.</p> <p><b><u>FP Services</u></b></p> <p>The TOE is a hardware appliance that includes a hardware-based real-time clock. The TOE’s embedded OS manages the clock and the GUI exposes the clock management function to the administrators. Optionally, the TOE can be configured to use a NTP server in the operational environment. The time source is updated frequently from the time server to ensure accuracy. The time is used for the timestamp in the audit records and events.</p>
FPT_TST_EXT.1	<p><b><u>ASA</u></b></p> <p>The TOE run a suite of self-tests during initial start-up (power-on-self-tests or POST) to verify its correct operation. When FIPS mode is enabled on the TOE, additional cryptographic tests and software integrity test will be run during start-up. The self-testing includes cryptographic algorithm tests (known-answer tests) that feed pre-defined data to cryptographic modules and confirm the resulting output from the modules match expected values, and firmware integrity tests that verify the digital signature of the code image using RSA-2048 with SHA-512. The cryptographic algorithm testing verifies proper operation of encryption functions, decryption functions, signature padding functions, signature hashing functions, and random number generation. The firmware integrity testing verifies the image has not been tampered with or corrupted. If any of these self-tests fails, the TOE will cease operation. For more details, please see FPT_FLS.1.</p> <p><b><u>FP Services</u></b></p> <p>The TOE includes a number of built in diagnostic tests that are run during start-up to determine whether the TOE is operating properly. The built-in BIOS self tests include basic read-write memory, flash read, software checksum tests, and device detection tests. When CC mode is enabled, the TOE will run a HMAC-SHA512 integrity tests at power-up covering the whole kernel, all binaries and libraries, modules and boot loader of the system. If the hash verification fails, the Process Manager (PM) will not start and the system will not enter operational state. In addition, the TOE is designed to run the power-on self-tests that comply with the FIPS 140-2 requirements for self-test (e.g., known answer tests (KATs) and zeroization tests). If the TOE fails any of the FIPS power-on self-tests, the TOE will enter an error state and will not be operational. The following self-tests are executed: AES encryption/decryption KAT, RSA key generation and encryption/decryption KAT, SHA hash KATs, HMAC-SHA hash KATs, PRNG KATs, and key overwriting tests.</p>



TOE SFRs	How the SFR is Satisfied
FPT_TUD_EXT.1	<p><b><u>ASA</u></b></p> <p>The TOE (and other TOE components) have specific versions that can be queried by an administrator. When updates are made available by Cisco, an administrator can obtain and manually install those updates.</p> <p>Digital signatures are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to update the applicable TOE components. The update process will fail if the digital signature verification process fails. Instructions on how to perform verification and update are provided in the Preparative Procedures &amp; Operational User Guide for the Common Criteria Certified Configuration.</p> <p><b><u>FP Services</u></b></p> <p>The TOE can be updated manually or automatically<sup>11</sup>. For manual update, the user will download the TOE upgrade file, compute the hash of the upgrade file, and verify the computed hash matches the hash published on the secure website. Each upgrade file will have a corresponding published SHA-512 hash value with it. Note that the published hash value is also embedded with the TOE upgrade file in case the users choose not to use the manual update method. The TOE also includes a validity checking function that is always run when upgrading the TOE firmware (including patches) and Rule Updates. This ensures TOE updates are always validated prior to installation. In either case, manual or automatic, the upgrade version will be checked to ensure it is appropriate (e.g., not upgrading to an older version) and the upgrade file will be verified using an embedded SHA-512 hashed value verified against the value computed during upgrade. If the version is incorrect or the SHA-512 hashed value cannot be verified, the upgrade will not proceed in order to protect the integrity of the TOE. More specifically, each update includes a header and metadata with the version and hashed value. In order to verify the data, the TOE generates its own SHA-512 secure has of the update data, compares it with the embedded hash in the update header to ensure they match.</p> <p>During the update process, if the Snort engine is updated and restarted, then is a split second where the managed Sensors do not perform any traffic inspection on the network. The CC Supplemental user guide will address this situation by requiring the upgrade and maintenance actions be performed during off-peak hours where the appliance can be disconnected from the network during the upgrade process to be upgraded, restarted, and verified before re-connecting back to the network to ensure complete traffic inspection.</p>
FTA_SSL_EXT.1	<p><b><u>ASA</u></b></p> <p>An administrator can configure maximum inactivity times for both local and remote administrative sessions. When a session is inactive (i.e., no session input) for the configured period of time the TOE will terminate the session, requiring the</p>
FTA_SSL.3	

<sup>11</sup> This process requires constant access to the Internet and is out of scope of the evaluation.

TOE SFRs	How the SFR is Satisfied
	<p>administrator to log in again to establish a new session when needed.</p> <p><b><u>FP Services</u></b></p> <p>The TOE can be configured by an administrator to set an interactive session timeout value in the system policy or platform settings, as with the login banner. The setting applies to all users and for both local and remote interactive sessions. The timeout value can be any positive integer value from 1 minute to 1,440 minutes (24 hours), with 0 disabling the timeout – the default timeout value is 60 minutes for web UI and disabled by default for CLI. The administrators can configure an exemption to the timeout feature on a per user basis. This means that the user will be exempted from the being timeout. This option is not allowed in the evaluated configuration and the administrators are advised in the CC Supplement User Guide against using this option.</p> <p>A remote or local session that is inactive (i.e., no commands or actions from the remote client) for the defined timeout value will be terminated and logged by audit function. The user will be required to re-enter their username and their password to start another session. The users can also terminate their own interactive local or remote sessions, anytime they choose.</p>
FTA_SSL.4	<p><b><u>ASA</u></b></p> <p>An administrator is able to exit out of both local and remote administrative sessions, effectively terminating the session so it cannot be re-used and will require authentication to establish a new session.</p> <p><b><u>FP Services</u></b></p> <p>See previous section.</p>
FTA_TAB.1	<p><b><u>ASA</u></b></p> <p>The TOE provides administrators with the capability to configure advisory banner or warning message(s) that will be displayed prior to completion of the logon process at the local console or via any remote connection (e.g., SSH over IPsec or HTTPS).</p> <p><b><u>FP Services</u></b></p> <p>The TOE can be configured to display administrator-configured advisory banners that will appear when users initiate an interactive session with the TOE. The login banner can be configured in the system policy or platform settings, and can be applied to FMC itself and push out all its managed Sensors by the administrator. The login banner can be configured to display welcome information or legal in conjunction with login prompts. In each case, the banners will be displayed when accessing the TOE via the local console/serial, SSHv2, or HTTPS interfaces.</p>
FTP_ITC.1	<p><b><u>ASA</u></b></p> <p>The TOE uses IPsec to protect communications between itself and remote entities for the following purposes:</p> <ul style="list-style-type: none"> <li>• The TOE protects transmission of audit records when sending syslog message</li> </ul>

TOE SFRs	How the SFR is Satisfied
	<p>to a remote audit server by transmitting the message over IPsec and TLS.</p> <ul style="list-style-type: none"> <li>• Connections to authentication servers (AAA servers) can be protected via IPsec tunnels. Connections with AAA servers (via RADIUS) can be configured for authentication of TOE administrators.</li> <li>• Connections to VPN peers can be initiated from the TOE using IPsec. In addition the TOE can establish secure VPN tunnels with IPsec VPN clients. Note that the remote VPN client is in the operational environment.</li> </ul> <p><b><u>FP Services</u></b></p> <p>The TOE can be configured to transmit audit records to an external audit server. In order to protect exported audit records from disclosure or modification, the TOE utilizes syslog over TLS connections. The TLS provides authentication, key exchange, encryption and integrity protection of the data. For every audit event generated, the TOE stores it locally and sends it to the audit server. All the cryptographic algorithms and functions are provided by CiscoSSL.</p>
FTP_TRP.1	<p><b><u>ASA</u></b></p> <p>The TOE uses SSHv2 over IPsec or HTTPS (for ASDM) to provide the trusted path (with protection from disclosure and modification) for all remote administration sessions. Optionally, the TOE also supports tunneling the SSH and ASDM connections in IPsec VPN tunnels (peer-to-peer, or remote VPN client). All protocols (i.e., SSH, HTTPS, IPsec) can be applied to any interface including management interface.</p> <p><b><u>FP Services</u></b></p> <p>To support secure remote administration, the TOE includes implementations of SSHv2 (by OpenSSH) and HTTPS (HTTP over TLS). In each case, a remote host (presumably acting on behalf of an administrator) can initiate a secure remote connection for the purpose of security management. Note that only the local console is available by default and each of these remote administration services can be independently enabled by an administrator. For added security, only these security protocols and ports 22 and 443 are enabled and allowed by default. The administrators can also setup an access list to restrict only allowed IP addresses to access the TOE.</p> <p>In the cases of SSHv2 and HTTPS, the TOE offers both a secure command line interface (CLI) and a graphical user interface (GUI) interactive administrator sessions. An administrator with appropriate SSHv2 or HTTPS capable clients can establish secure remote connections with the TOE. However, to successfully establish such an interactive session, the administrator must be able to provide acceptable user credentials (e.g., user name and password), after which they will be able to issue commands or actions within their assigned authorizations.</p> <p>All of the security protocols are supported by the cryptographic operations provided by the crypto module included in the TOE implementation.</p>
FFW_RUL_EXT.1.1	<p><b><u>ASA Only</u></b></p> <p>The TOE provides stateful traffic filtering of IPv4 and IPv6 network traffic.</p>

TOE SFRs	How the SFR is Satisfied
FFW_RUL_EXT.1.2	<p>Administratively-defined traffic filter rules (access-lists) can be applied to any interface to filter traffic based on IP parameters including source and destination address, transport layer protocol, type and code, TCP and UDP port numbers. The TOE allows establishment of communications between remote endpoints, and tracks the state of each session (e.g. initiating, established, and tear-down), and will clear established sessions after proper tear-down is completed as defined by each protocol, or when session timeouts are reached.</p> <p>To track the statefulness of sessions to/from and through the firewall, the TOE maintains a table of connections in various connection states and connection flags. The TOE updates the table (adding, and removing connections, and modifying states as appropriate) based on configurable connection timeout limits, and by inspecting fields within the packet headers. For further explanation of connection states, see section 7.1.</p> <p>The proper session establishment and termination followed by the TOE is as defined in the following RFCs:</p> <ul style="list-style-type: none"> <li>• RFC 792 (ICMPv4)</li> <li>• RFC 4443 (ICMPv6)</li> <li>• RFC 791 (IPv4)</li> <li>• RFC 2460 (IPv6)</li> <li>• TCP, RFC 793, section 2.7 Connection Establishment and Clearing</li> <li>• UDP, RFC 768 (not applicable, UDP is a “stateless” protocol)</li> </ul> <p>During initialization/startup (while the TOE is booting) the configuration has yet to be loaded, and no traffic can flow through any of its interfaces. No traffic can flow through the TOE interfaces until the POST has completed, and the configuration has been loaded. If any aspect of the POST fails during boot, the TOE will reload without forwarding traffic. If a critical component of the TOE, such as the clock or cryptographic modules, fails while the TOE is in an operational state, the TOE will reload, which stops the flow of traffic. If a component such as a network interface, which is not critical to the operation of the TOE, but may be critical to one or more traffic flows, fails while the TOE is operational, the TOE will continue to function, though all traffic flows through the failed network interface(s) will be dropped.</p>
FFW_RUL_EXT.1.2	<p><b><u>ASA Only</u></b></p> <p>The TOE supports filtering of the following protocols and enforces proper session establishment, management, and termination as defined in each protocol’s RFC including proper use of:</p> <ul style="list-style-type: none"> <li>• Addresses, type of service, fragmentation data, size and padding, and IP options including loose source routing, strict source routing, and record route as defined in RFC 791 (IPv4), and RFC 2460 (IPv6);</li> <li>• Port numbers, sequence and acknowledgement numbers, size and padding, and control bits such as SYN, ACK, FIN, and RST as defined in RFC 793 (TCP);</li> <li>• Port numbers, and length as defined in RFC 768 (UDP); and</li> <li>• Session identifiers, sequence numbers, types, and codes as defined in RFC 792 (ICMPv4), and RFC 4443 (ICMPv6).</li> </ul>

TOE SFRs	How the SFR is Satisfied
	<p>Cisco confirms proper implementation of the RFCs through interoperability testing with Cisco and 3<sup>rd</sup> party products and through protocol compliant testing.</p> <p>The TOE can also support deeper packet inspection and enforce additional RFC compliance beyond session management, but such traffic inspection functionality is not defined within the FWcPP and is therefore beyond the scope of this CC certification.</p>
FFW_RUL_EXT.1.3, FFW_RUL_EXT.1.4	<p><b><u>ASA Only</u></b></p> <p>Each traffic flow control rule on the TOE is defined as either a “permit” rule, or a “deny” rule, and any rule can also contain the keyword “log” which will cause a log message to be generated when a new session is established because it matched the rule. The TOE can be configured to generate a log message for the session establishment of any permitted or denied traffic (in this case, attempt to establish a session). When a rule is created to explicitly allow a protocol which is implicitly allowed to spawn additional sessions, the establishment of spawned sessions is logged as well.</p> <p>Access Control Lists (ACLs) are only enforced after they’ve been applied to a network interface. Any network interface can have an ACL applied to it with the “access-group” command, e.g. “access-group sample-acl in interface outside”. Interfaces can be referred to by their identifier (e.g. GigabitEthernet 0/1), or by a name if named using the “nameif” command e.g.:</p> <pre>asa(config)# <b>interface</b> gigabitethernet0/1 asa(config-if)# <b>nameif</b> inside</pre> <p>The interface types that can be assigned to an access-group are:</p> <ul style="list-style-type: none"> <li>• Physical interfaces             <ul style="list-style-type: none"> <li>○ Ethernet</li> <li>○ GigabitEthernet</li> <li>○ TenGigabitEthernet</li> <li>○ Management</li> </ul> </li> <li>• Port-channel interfaces (designated by a port-channel number)</li> <li>• Subinterface (designated by the subinterface number)</li> </ul> <p>The default state of an interface depends on the type and the context mode:</p> <ul style="list-style-type: none"> <li>• For the “system” context in single mode or multiple context mode, interfaces have the following default states:             <ul style="list-style-type: none"> <li>○ Physical interfaces = Disabled</li> <li>○ Subinterfaces = Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.</li> </ul> </li> <li>• For any non-system context (in multiple context mode): All allocated interfaces (allocated to the context by the system context) are enabled by default, no matter what the state of the interface is in the system context. However, for traffic to pass through the interface, the interface also has to be enabled in the system context. If you shut down an interface in the system context, then that interface is down in all contexts to which that interface has</li> </ul>

TOE SFRs	How the SFR is Satisfied
	<p>been allocated.</p> <p>In interface configuration mode, the administrator can configure hardware settings (for physical interfaces), assign a name, assign a VLAN, assign an IP address, and configure many other settings, depending on the type of interface and the security context mode.</p> <p>For an enabled interface to pass traffic, the following interface configuration mode commands must be used (in addition to explicitly permitting traffic flow by applying and access-group to the interface): “<b>nameif</b>”, and, for routed mode, “<b>ip address</b>”. For subinterfaces, also configure the “<b>vlan</b>” command.</p>
FFW_RUL_EXT.1.5	<p><b><u>ASA Only</u></b></p> <p>All traffic that goes through the TOE is inspected using the Adaptive Security Algorithm and either is 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.</p> <p>A stateful firewall like the ASA, however, takes into consideration the state of a packet:</p> <ul style="list-style-type: none"> <li>• Is this a new connection?</li> </ul> <p>If it is a new connection, the TOE has to check the packet against access control 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."</p> <p>The session management path is responsible for the following tasks:</p> <ul style="list-style-type: none"> <li>– Performing the access list checks</li> <li>– Performing route lookups</li> <li>– Allocating NAT translations (xlates)</li> <li>– Establishing sessions in the "fast path"</li> </ul> <p>The TOE creates forward and reverse flows in the fast path for TCP traffic; the TOE 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.</p> <ul style="list-style-type: none"> <li>• Is this an established connection?</li> </ul> <p>If the connection is already established, the TOE does not need to re-check packets against the ACL; matching packets can go through the "fast" path based on attributes identified in FFW_RUL_EXT.1.5. The fast path is responsible for the following tasks:</p> <ul style="list-style-type: none"> <li>– IP checksum verification</li> <li>– Session lookup</li> </ul>

TOE SFRs	How the SFR is Satisfied
	<ul style="list-style-type: none"> <li>– TCP sequence number check</li> <li>– NAT translations based on existing sessions</li> <li>– Layer 3 and Layer 4 header adjustments</li> </ul>
FFW_RUL_EXT.1.6, FFW_RUL_EXT.1.7	<p><b><u>ASA Only</u></b></p> <p>The TOE can be configured to implement default denial of various mal-formed packets/fragments, and other illegitimate network traffic, and can be configured to log that such packets/frames were dropped.</p> <p>The TOE's can be used to deny and log traffic by defining policies with the "ip audit name" command, specifying the "drop" action, and applying the policy or policies to each enabled interface. Each signature has been classified as either "informational", or "attack". Using the "info" and "attack" keywords in the "ip audit name" command defines the action the TOE will take for each signature classification.</p> <pre>asa(config)# ip audit name name {info   attack} [action [alarm] [drop] [reset]] asa(config)# ip audit interface interface_name policy_name</pre> <p>Example:</p> <pre>asa(config)# ip audit name ccpolicy1 attack action alarm reset asa(config)# ip audit name ccpolicy2 info action alarm reset asa(config)# ip audit interface outside ccpolicy1 asa(config)# ip audit interface inside ccpolicy2</pre> <p>Specifying the "alarm" action in addition to the "drop" action will result in generating an audit message when the signature is detected. Messages 400000 through 400051 are Cisco Intrusion Prevention Service signature messages, and have this format:</p> <pre>%ASA-4-4000nn: IPS:number string from IP_address to IP_address on interface interface_name</pre> <p>The following traffic will be denied by the TOE, and audit messages will be generated as indicated:</p> <ol style="list-style-type: none"> <li>1. packets which are invalid fragments, including IP fragment attack</li> </ol> <pre>%ASA-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address</pre> <pre>%ASA-4-209004: Invalid IP fragment, size = bytes exceeds maximum size= bytes: src = source_address, dest = dest_address, proto = protocol, id = number</pre> <pre>%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.</pre> <p>The following messages will be generated when configured as described above.</p> <pre>%ASA-4-400007: IPS:1100 IP Fragment Attack from IP_address to IP_address on interface interface_name</pre> <pre>%ASA-4-400009: IPS:1103 IP Overlapping Fragments (Teardrop) from IP_address to IP_address on interface interface_name</pre> <pre>%ASA-4-400023: IPS:2150 Fragmented ICMP traffic from IP_address to IP_address on</pre>

TOE SFRs	How the SFR is Satisfied
	<p>interface <i>interface_name</i></p> <p>%ASA-4-400025: IPS:2154 Ping of Death Attack from <i>IP_address</i> to <i>IP_address</i> on interface <i>interface_name</i></p> <p>2. fragmented IP packets which cannot be re-assembled completely;</p> <p>%ASA-4-209003: Fragment database limit of <i>number</i> exceeded: src = <i>source_address</i>, dest = <i>dest_address</i>, proto = <i>protocol</i>, id = <i>number</i></p> <p>%ASA-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.</p> <p>%ASA-4-423005: Dropped NBDGM <i>pkt_type_name</i> fragment with <i>error_reason_str</i> from <i>ifc_name:ip_address/port</i> to <i>ifc_name:ip_address/port</i>.</p> <p>%ASA-4-507002: Data copy in proxy-mode exceeded the buffer limit</p> <p>%ASA-7-715060: Dropped received IKE fragment. Reason: <i>reason</i></p> <p>%ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.</p> <p>3. packets where the source address of the network packet is equal to the address of the network interface where the network packet was received;</p> <p>%ASA-2-106016: Deny IP spoof from (<i>IP_address</i>) to <i>IP_address</i> on interface <i>interface_name</i>.</p> <p>4. 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;</p> <p>%ASA-2-106016: Deny IP spoof from (<i>IP_address</i>) to <i>IP_address</i> on interface <i>interface_name</i>.</p> <p>This next message appears when Unicast RPF has been enabled with the <b>ip verify reverse-path</b> command.</p> <p>%ASA-1-106021: Deny <i>protocol</i> reverse path check from <i>source_address</i> to <i>dest_address</i> on interface <i>interface_name</i></p> <p>This next message appears when a packet matching a connection arrived on a different interface from the interface on which the connection began, and the <b>ip verify reverse-path</b> command is not configured.</p> <p>%ASA-1-106022: Deny <i>protocol</i> connection spoof from <i>source_address</i> to <i>dest_address</i> on interface <i>interface_name</i></p> <p>5. packets where the source address of the network packet is defined as being on a broadcast network;</p> <p>%ASA-2-106016: Deny IP spoof from (<i>IP_address</i>) to <i>IP_address</i> on interface <i>interface_name</i>.</p> <p>6. packets where the source address of the network packet is defined as being on a multicast network;</p> <p>%ASA-4-106023: Deny <i>protocol</i> src [<i>interface_name:source_address/source_port</i>] dst <i>interface_name:dest_address/dest_port</i> [type {<i>string</i>}, code {<i>code</i>}] by access_group <i>acl ID</i></p>



TOE SFRs	How the SFR is Satisfied
	<p>The following message will be generated when the rules listed below are configured without the “log” option.</p> <pre>%ASA-4-106100: access-list <i>acl_ID</i> denied <i>protocol</i> <i>interface_name</i>/<i>source_address</i>(<i>source_port</i>)- <i>interface_name</i>/<i>dest_address</i>(<i>dest_port</i>) hit-cnt <i>number</i> ({first hit   <i>number</i>- secondinterval})) hash codes</pre> <p>The following message will be generated when these rules are configured with the “log” option:</p> <pre>asa(config)#<b>object-group network</b> <i>grp_name</i> asa(config-network-object-group)#<b>network-object</b> 224.0.0.0 255.0.0.0 #IPv4 multicast asa(config-network-object-group)#<b>network-object</b> FF00::/8 #IPv6 multicast asa(config)#<b>access-list</b> <i>acl-name</i> <b>extended deny ip</b> <i>grp-name</i> <b>any</b> [log] asa(config)#<b>access-group</b> <b>in</b> <i>interface</i> <i>int-name</i></pre> <p>7. packets where the source address of the network packet is defined as being a loopback address;</p> <pre>%ASA-2-106016: Deny IP spoof from (<i>IP_address</i>) to <i>IP_address</i> on interface <i>interface_name</i>.</pre> <p>The following message will be generated when no ACL has been defined to explicitly deny this traffic.</p> <pre>%ASA-4-106023: Deny <i>protocol</i> src [<i>interface_name</i>:<i>source_address</i>/<i>source_port</i>] dst <i>interface_name</i>:<i>dest_address</i>/<i>dest_port</i> [type {<i>string</i>}, code {<i>code</i>}] by access_group <i>acl_ID</i></pre> <p>The following message will be generated when the rules listed below are configured without the “log” option.</p> <pre>%ASA-4-106100: access-list <i>acl_ID</i> denied <i>protocol</i> <i>interface_name</i>/<i>source_address</i>(<i>source_port</i>)- <i>interface_name</i>/<i>dest_address</i>(<i>dest_port</i>) hit-cnt <i>number</i> ({first hit   <i>number</i>- secondinterval})) hash codes</pre> <p>The following message will be generated when these rules are configured with the “log” option:</p> <pre>asa(config)#<b>object-group network</b> <i>grp_name</i> asa(config-network-object-group)#<b>network-object</b> 127.0.0.0 255.0.0.0 #IPv4 loopback asa(config-network-object-group)#<b>network-object</b> ::1/128 #IPv6 loopback asa(config)#<b>access-list</b> <i>acl-name</i> <b>extended deny ip</b> <i>grp-name</i> <b>any</b> [log] asa(config)#<b>access-group</b> <b>in</b> <i>interface</i> <i>int-name</i></pre> <p>8. packets where the source address of the network packet is a multicast;</p> <p>See item number 6.</p> <p>9. packets where the source or destination address of the network packet is a link-</p>

TOE SFRs	How the SFR is Satisfied
	<p>local address;</p> <p>%ASA-2-106016: Deny IP spoof from (<i>IP_address</i>) to <i>IP_address</i> on interface <i>interface_name</i>.</p> <p>The following message will be generated when no ACL has been defined to explicitly deny this traffic.</p> <p>%ASA-4-106023: Deny <i>protocol</i> src [<i>interface_name</i>:<i>source_address</i>/<i>source_port</i>] dst <i>interface_name</i>:<i>dest_address</i>/<i>dest_port</i> [type {<i>string</i>}, code {<i>code</i>}] by access_group <i>acl_ID</i></p> <p>The following message will be generated when the rules listed below are configured without the “log” option.</p> <p>%ASA-4-106100: access-list <i>acl_ID</i> denied <i>protocol</i> <i>interface_name</i>/<i>source_address</i>(<i>source_port</i>) - <i>interface_name</i>/<i>dest_address</i>(<i>dest_port</i>) hit-cnt <i>number</i> ({first hit   <i>number</i>-secondinterval}) hash codes</p> <p>The following message will be generated when these rules are configured with the “log” option:</p> <pre>asa(config)#object-group network <i>grp_name</i> asa(config-network-object-group)#network-object 127.0.0.0 255.0.0.0 #IPv4 link-local asa(config-network-object-group)#network-object FE80::/10 #IPv6 link-local asa(config)#access-list <i>acl-name</i> extended deny ip <i>grp-name</i> any [log] asa(config)#access-list <i>acl-name</i> extended deny ip any <i>grp-name</i> [log] asa(config)#access-group in interface <i>int-name</i></pre> <p>10. 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;</p> <p>%ASA-4-106023: Deny <i>protocol</i> src [<i>interface_name</i>:<i>source_address</i>/<i>source_port</i>] dst <i>interface_name</i>:<i>dest_address</i>/<i>dest_port</i> [type {<i>string</i>}, code {<i>code</i>}] by access_group <i>acl_ID</i></p> <p>The following message will be generated when the rules listed below are configured without the “log” option.</p> <p>%ASA-4-106100: access-list <i>acl_ID</i> denied <i>protocol</i> <i>interface_name</i>/<i>source_address</i>(<i>source_port</i>) - <i>interface_name</i>/<i>dest_address</i>(<i>dest_port</i>) hit-cnt <i>number</i> ({first hit   <i>number</i>-secondinterval}) hash codes</p> <p>The following message will be generated when these rules are configured with the “log” option:</p> <pre>asa(config)#object-group network <i>grp_name</i> asa(config-network-object-group)#network-object 192.0.0.0 255.0.0.0 #IPv4 reserved asa(config-network-object-group)#network-object 240.0.0.0 128.0.0.0 #IPv4 reserved asa(config)#access-list <i>acl-name</i> extended deny ip <i>grp-name</i> any [log] asa(config)#access-list <i>acl-name</i> extended deny ip any <i>grp-name</i> [log]</pre>

TOE SFRs	How the SFR is Satisfied
	<p>asa(config)#<b>access-group</b> in interface <i>int-name</i></p> <p>11. 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;</p> <p>%ASA-4-106023: Deny <i>protocol</i> src [<i>interface_name</i>:<i>source_address</i>/<i>source_port</i>] dst <i>interface_name</i>:<i>dest_address</i>/<i>dest_port</i> [<i>type</i> {<i>string</i>}, code {<i>code</i>}] by access_group <i>acl_ID</i></p> <p>The following message will be generated when the rules listed below are configured without the “log” option.</p> <p>%ASA-4-106100: access-list <i>acl_ID</i> denied <i>protocol</i> <i>interface_name</i>/<i>source_address</i>(<i>source_port</i>)- <i>interface_name</i>/<i>dest_address</i>(<i>dest_port</i>) hit-cnt <i>number</i> ({first hit   <i>number</i>-<i>second</i>interval}) hash codes</p> <p>The following message will be generated when these rules are configured with the “log” option:</p> <p>asa(config)#<b>object-group network</b> <i>grp_name</i> asa(config-network-object-group)#<b>network-object</b> :: #IPv6 unspecified asa(config-network-object-group)#<b>network-object</b> 0000::/8 #IPv6 reserved asa(config)#<b>access-list</b> <i>acl-name</i> <b>extended deny ip</b> <i>grp_name</i> <b>any</b> [log] asa(config)#<b>access-list</b> <i>acl-name</i> <b>extended deny ip</b> <i>any</i> <i>grp_name</i> [log] asa(config)#<b>access-group</b> in interface <i>int-name</i></p> <p>12. Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified;</p> <p>%ASA-6-106012: Deny IP from <i>IP_address</i> to <i>IP_address</i>, IP options <i>hex</i>.</p> <p>The following messages will be generated when configured as described above.</p> <p>%ASA-4-400001: IPS:1001 IP options-Record Packet Route from <i>IP_address</i> to <i>IP_address</i> on interface <i>interface_name</i></p> <p>%ASA-4-400004: IPS:1004 IP options-Loose Source Route from <i>IP_address</i> to <i>IP_address</i> on interface <i>interface_name</i></p> <p>%ASA-4-400006: IPS:1006 IP options-Strict Source Route from <i>IP_address</i> to <i>IP_address</i> on interface <i>interface_name</i></p> <p>13. By default, TOE will also drop (and is capable of logging) a variety of other IP packets with invalid content including:</p> <ul style="list-style-type: none"> <li>• Invalid source and/or destination IP address including: <ul style="list-style-type: none"> <li>○ source or destination is the network address (e.g. 0.0.0.0)</li> <li>○ source and destination address are the same (with or without the source and destination ports being the same)</li> <li>○ first octet of the source IP is equal to zero</li> <li>○ network part of the source IP is equal to all zeros or all ones</li> <li>○ host part of the source IP is equal to all zeros or all ones</li> </ul> </li> </ul>

TOE SFRs	How the SFR is Satisfied
	Invalid ICMP packets including: sequence number mismatch; invalid ICMP code, and ICMP responses unrelated to any established ICMP session
FFW_RUL_EXT.1.8	<p><b><u>ASA Only</u></b></p> <p>TOE administrators have control over the sequencing of access control entries (ACEs) within an access control list (ACL) to be able to set the sequence in which ACEs are applied within any ACL. The entries within an ACL are always applied in a top-down sequence, and the first entry that matches the traffic is the one that's applied, regardless of whether there may be a more precise match for the traffic further down in the ACL. By changing the ordering/numbering of entries within an ACL, the administrator changes the sequence in which the entries are compared to network traffic flows.</p>
FFW_RUL_EXT.1.9	<p><b><u>ASA Only</u></b></p> <p>An implicit "deny-all" rule is applied to all interfaces to which any traffic filtering rule has been applied. The implicit deny-all rule is executed after all admin-defined rules have been executed, and will result in dropping all traffic that has not been explicitly permitted, or explicitly denied. If an administrator wants to log all denied traffic, a rule entry should be added that denies all traffic and logs it, e.g. "access-list sample-acl deny ip any any log".</p>
FFW_RUL_EXT.1.10	<p><b><u>ASA Only</u></b></p> <p>TOE administrators can configure the maximum number of half-open TCP connections allowed using the "set connection embryonic-conn-max 0-65535" in the service-policy command. After the configured limit is reached, the TOE will act as a proxy for the server and generates a SYN-ACK response to new client SYN request. 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. If an ACK is not received in the configurable time frame, the session is closed, resource is returned to the free pool, and it will be counted. The default idle time until a TCP half-open connection closes is 10 minutes.</p>
FFW_RUL_EXT.2	<p><b><u>ASA Only</u></b></p> <p>The TOE supports numerous TCP and UDP protocols that require dynamic establishment of secondary network sessions including FTP. The TOE will manage establishment and teardown of the following protocols in accordance with the RFC for each protocol:</p> <ul style="list-style-type: none"> <li>• FTP (File Transfer Protocol) is a TCP protocol supported in either active or passive mode: <ul style="list-style-type: none"> <li>○ In active mode the client initiates the control session, and the server initiates the data session to a client port provided by the client;</li> <li>○ For active FTP to be allowed through the TOE, the firewall rules must explicitly permit the control session from the client to the server, and "inspect ftp" must be enabled. The TOE will then explicitly permit a control session to be initiated from the client to the server, and implicitly</li> </ul> </li> </ul>

TOE SFRs	How the SFR is Satisfied
	<p>permit data sessions to be initiated from the server to the client while the control session is active.</p> <ul style="list-style-type: none"> <li>○ In passive (PASV) mode, the client initiates the control session, and the client also initiates the data session to a secondary port provided to the client by the server.</li> </ul> <p>For passive FTP to be permitted through the TOE, the firewall rules must explicitly permit the control session from the client to the server, and “inspect ftp” must be enabled with the “match passive-ftp” option enabled. That feature will cause the TOE to look for the PASV or EPSV commands in the FTP control traffic and for the server’s destination port, and dynamically permit the data session.</p>
Reproduced from the VPNGWcEP	
FCS_CKM.1/IKE [VPN]	See FCS_CKM.1
FCS_COP.1(1)[VPN]	See FCS_COP.1(1)
FCS_IPSEC_EXT.1 [VPN]	See FCS_IPSEC_EXT.1
FIA_AFL.1[VPN]	<p><b><u>ASA Only</u></b></p> <p>The TOE provides the privileged administrator the ability to specify the maximum number of unsuccessful authentication attempts (between 1 and 16) before privileged administrator or non-privileged administrator is locked out.</p> <p>When a privileged administrator or non-privileged administrator attempting to login reaches the administratively set maximum number of failed authentication attempts, the user will not be granted access to the administrative functionality of the TOE until a privileged administrator resets the user's number of failed login attempts (i.e., unlocks) through the administrative CLI. This applies to both password-based and public key authentication methods.</p>
FIA_PSK_EXT.1 [VPN]	<p><b><u>ASA Only</u></b></p> <p>The TOE supports use of IKEv2 pre-shared keys for authentication of IPsec tunnels. Pre-shared keys can be entered as ASCII character strings, or HEX values. The text-based pre-shared keys can be composed of any combination of upper and lower case letters, numbers, and special characters. The TOE supports keys that are from 1 character in length up to 128 in length. The text-based pre-shared key is conditioned by one of the prf functions (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, or HMAC-SHA-512) configured by the administrator.</p>
FIA_X509_EXT.4[VPN]	See FIA_X509_EXT.x
FMT_MTD.1/AdminAct [VPN]	<p><b><u>ASA Only</u></b></p> <p>The TOE only provides the ability for authorized administrators to access TOE data, such as audit data, configuration data, security attributes (such as cryptographic keys</p>

TOE SFRs	How the SFR is Satisfied
	and certificates used in VPN), routing tables, and session thresholds.
FPF_RUL_EXT.1 [VPN]	<p><b><u>ASA Only</u></b></p> <p>An authorized administrator can define the traffic that needs to be protected by configuring access lists (permit, deny, log) and applying these access lists to interfaces using access and crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port.</p> <p>The TOE enforces information flow policies on network packets that are received by TOE interfaces and leave the TOE through other TOE interfaces. When network packets are received on a TOE interface, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, pass/not pass information, as well as optional logging.</p> <p>The TOE implements rules that define the permitted flow of traffic between interfaces of the TOE for unauthenticated traffic. These rules control whether a packet is transferred from one interface to another based on:</p> <ol style="list-style-type: none"> <li>1. Presumed address of source</li> <li>2. Presumed address of destination</li> <li>3. Transport layer protocol (or next header in IPv6)</li> <li>4. Service used (UDP or TCP ports, both source and destination)</li> <li>5. Network interface on which the connection request occurs</li> </ol> <p>These rules are supported for the following protocols: RFC 791(IPv4); RFC 2460 (IPv6); RFC 793 (TCP); RFC 768 (UDP). TOE compliance with these protocols is verified via regular quality assurance, regression, and interoperability testing.</p> <p>Packets will be dropped unless a specific rule has been set up to allow the packet to pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to pass traffic). Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied.</p> <p>These rules are entered in the form of access lists at the CLI (via ‘access list’ and ‘access group’ commands). These interfaces reject traffic when the traffic arrives on an external TOE interface, and the source address is an external IT entity on an internal network;</p> <p>These interfaces reject traffic when the traffic arrives on an internal TOE interface, and the source address is an external IT entity on the external network;</p> <p>These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on a broadcast network;</p> <p>These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on the loopback network;</p>

TOE SFRs	How the SFR is Satisfied
	<p>These interfaces reject requests in which the subject specifies the route for information to flow when it is in route to its destination; and</p> <p>For application protocols supported by the TOE (e.g., DNS, HTTP, SMTP, and POP3), these interfaces deny any access or service requests that do not conform to its associated published protocol specification (e.g., RFC). This is accomplished through protocol filtering proxies that are designed for that purpose.</p> <p>Otherwise, these interfaces pass traffic only when its source address matches the network interface originating the traffic to the network interface corresponding to the traffic's destination address.</p> <p>During the boot cycle, the TOE first powers on hardware, loads the image, and executes the power on self-tests. Until the power on self tests successfully complete, the interfaces to the TOE are deactivated. Once the tests complete, the interfaces become active and the rules associated with the interface become immediately operational. There is no state during initialization/ startup that the access lists are not enforced on an interface.</p> <p>During initialization/startup (while the ASA is booting) the configuration has yet to be loaded, and no traffic can flow through any of its interfaces. No traffic can flow through the ASA interfaces until the POST has completed, and the configuration has been loaded. If any aspect of the POST fails during boot, the ASA will reload without forwarding traffic. If a critical component of the ASA, such as the clock or cryptographic modules, fails while the ASA is in an operational state, the ASA will reload, which stops the flow of traffic. If a component such as a network interface, which is not critical to the operation of the ASA, but may be critical to one or more traffic flows, fails while the ASA is operational, the ASA will continue to function, though all traffic flows through the failed network interface(s) will be dropped.</p>
FPT_FLS.1/SelfTest [VPN]	<p><b><u>ASA Only</u></b></p> <p>Noise source health tests are run both periodically and at start-up to determine the functional health of the noise source. These tests are specifically designed to catch catastrophic losses in the overall entropy associated with the noise source. Tests are run on the raw noise output, before the application of any conditioners. If a noise source fails the health test either at start-up or after the device is operational, the platform will be shut down.</p> <p>Whenever a failure (e.g., POST or integrity test fails) occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads. So long as the failures persist, the TOE will continue to reload. This functionally prevents any failure from causing an unauthorized information flow. There are no failures that circumvent this protection.</p>
FPT_TST_EXT.2.1 [VPN]	See FPT_TST_EXT.1
FPT_TUD_EXT.1.3 [VPN]	See FPT_TUD_EXT.1

TOE SFRs	How the SFR is Satisfied
FTA_SSL.3[VPN]	<p><b><u>ASA Only</u></b></p> <p>When a remote VPN client session reaches a period of inactivity, its connection is terminated and it must re-establish the connection with new authentication to resume operation. This period of inactivity is set by the administrator using <b>vpn-idle-timeout</b> or <b>default-idle-timeout</b> commands in the VPN configuration.</p>
FTA_TSE.1[VPN]	<p><b><u>ASA Only</u></b></p> <p>The TOE allows for creation of acls that restrict VPN connectivity based client's IP address (location). These acls allow customization of all of these properties to allow or deny access. In addition, the <b>vpn-access-hours</b> command can be used to restrict access based on date and time.</p>
FTA_VCM_EXT.1 [VPN]	<p><b><u>ASA Only</u></b></p> <p>The TOE provides the option to assign the remotely connecting VPN client an internal network IP address. The <b>ip-local-pool</b> command can be used to define the range of IP and IPv6 addresses to be available for use.</p>
FTP_ITC.1.1[VPN]	See FTP_ITC.1
Reproduced from the IPScEP	
FAU_GEN.1/IPS FAU_SAR.1* FAU_SAR.2* FAU_SAR.3* FAU_STG.1*	<p><b><u>FP Services Only</u></b></p> <p>The TOE will generate an event log for each intrusion event that occurs. Each event log will include a record of the date, time, type of exploit, and contextual information about the source of the attack and its target. For packet-based events, a copy of the packet or packets that triggered the event is also recorded. Managed Sensors will transmit their events to the FMC where the administrators can view the aggregated data and gain a greater understanding of the attacks against the entire network. The administrators can also deploy the managed Sensors in inline allowing them to configure the Sensors to drop or modify packets that are harmful.</p> <p>The web-based UI is the only way to view the intrusion events (Analysis &gt; Intrusions &gt; Events). The list below describes the intrusion event information that can be viewed, searched, filtered, and sorted by the system. In addition, basic contents such as date, time, and type can also be used to filter and sort. Note only Administrators and Intrusion Admins have access to the intrusion events.</p> <p><b>Access Control Policy</b></p> <p>The access control policy associated with the intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event is enabled.</p> <p><b>Access Control Rule</b></p> <p>The access control rule that invoked the intrusion policy that generated the event. Default Action indicates that the intrusion policy where the rule is enabled is not associated with a specific access control rule but, instead, is configured as the default action of the access control policy.</p>



TOE SFRs	How the SFR is Satisfied
	<p>This field is blank if intrusion inspection was associated with neither an access control rule nor the default action, for example, if the packet was examined by the default intrusion policy.</p> <p><b>Application Protocol</b></p> <p>The application protocol, if available, which represents communications between hosts detected in the traffic that triggered the intrusion event.</p> <p><b>Application Risk</b></p> <p>The risk associated with detected applications in the traffic that triggered the intrusion event: Very High, High, Medium, Low, and Very Low. Each type of application detected in a connection has an associated risk; this field displays the highest risk of those.</p> <p><b>Count</b></p> <p>The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows. This field is not searchable.</p> <p><b>Destination Continent</b></p> <p>The continent of the receiving host involved in the intrusion event.</p> <p><b>Destination Country</b></p> <p>The country of the receiving host involved in the intrusion event.</p> <p><b>Destination IP</b></p> <p>The IP address used by the receiving host involved in the intrusion event.</p> <p><b>Destination Port / ICMP Code</b></p> <p>The port number for the host receiving the traffic. For ICMP traffic, where there is no port number, this field displays the ICMP code.</p> <p><b>Destination User</b></p> <p>The User ID for any known user logged in to the destination host.</p> <p><b>Device</b></p> <p>The managed Sensor where the access control policy was deployed.</p> <p><b>Domain</b></p> <p>The domain of the Sensor that detected the intrusion. This field is only present if you have ever configured the Firepower Management Center for multitenancy.</p> <p><b>Egress Interface</b></p> <p>The egress interface of the packet that triggered the event. This interface column is not populated for a passive interface.</p> <p><b>Egress Security Zone</b></p> <p>The egress security zone of the packet that triggered the event. This security zone</p>

TOE SFRs	How the SFR is Satisfied
	<p>field is not populated in a passive deployment.</p> <p><b>Generator</b></p> <p>The component that generated the event.</p> <p><b>Ingress Interface</b></p> <p>The ingress interface of the packet that triggered the event. Only this interface column is populated for a passive interface.</p> <p><b>Ingress Security Zone</b></p> <p>The ingress security zone of the packet that triggered the event. Only this security zone field is populated in a passive deployment.</p> <p><b>Inline Result</b></p> <p>Actions</p> <p><b>Intrusion Policy</b></p> <p>The intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event was enabled.</p> <p><b>Message</b></p> <p>The explanatory text for the event. For rule-based intrusion events, the event message is pulled from the rule.</p> <p><b>Priority</b></p> <p>The event priority as determined by the Cisco Talos Security Intelligence and Research Group (Talos). The priority corresponds to either the value of the priority keyword or the value for the classtype keyword.</p> <p>For other intrusion events, the priority is determined by the decoder or preprocessor. Valid values are high, medium, and low.</p> <p><b>Protocol (search only)</b></p> <p>The name or number of the transport protocol used in the connection.</p> <p><b>Snort ID (search only)</b></p> <p>Specify the Snort ID (SID) of the rule that generated the event or, optionally, specify the combination Generator ID (GID) and SID of the rule, where the GID and SID are separated with a colon (:) in the format GID:SID.</p> <p><b>Source Continent</b></p> <p>The continent of the sending host involved in the intrusion event.</p> <p><b>Source Country</b></p> <p>The country of the sending host involved in the intrusion event.</p> <p><b>Source IP</b></p> <p>The IP address used by the sending host involved in the intrusion event.</p>

TOE SFRs	How the SFR is Satisfied
	<p><b>Source Port / ICMP Type</b></p> <p>The port number on the sending host. For ICMP traffic, where there is no port number, this field displays the ICMP type.</p> <p><b>Source User</b></p> <p>The User ID for any known user logged in to the source host.</p> <p>The intrusion events cannot be modified but they can be deleted by the Administrators or Intrusion Admins who have restricted access. When the intrusion events storage is full, the newest data will overwrite the oldest data.</p> <p>There is a feature called Threshold where the administrators can control the number of events that are generated per rule over time. They can limit notification to the specified number of event instances per time period or provide notification once per time period after a specified number of event instances. The administrator must specify if the event instances will be tracked by source or destination IP address, the count or the number of event instances, and the number of seconds for the time period for which event instances are tracked.</p> <p>The TOE can overwrite the oldest data with the newest data when the local IPS events storage is full. The intrusion events are generated by the “log” operation in the rule. The events are restricted to 100,000 entries size. However, the internal log only stores a maximum of 100,000 entries in the local database (to configure the size, go to System &gt; Configuration &gt; Database, and click on “Intrusion Event Database” or “Connection Database”). When the events log is full, the oldest events are overwritten by the newest events.</p> <p>Note the IPS function cannot be disabled unless the whole system is shutdown. The TOE also will generate all of the required auditable events identified in Table 16 (for FMT_SMF.1/IPS and IPS_NTA_EXT.1 only). All other events in Table 16 are addressed by intrusion events, not auditable events.</p> <p>The TOE can be configured to generate intrusion events. In addition, all management functions are audited as well. There are certain header fields that should not be used to trigger intrusion events (in Inline mode or Passive mode). Logging events related to these fields would generate a deluge of intrusion audit records that would prevent IPS analysts from figuring out what security incidents occur in their monitored network. In addition, logging these fields will provide no benefits. The following fields can be inspected and if in inline mode, dropped or modified (i.e., normalized):</p> <ul style="list-style-type: none"> <li>• All checksum fields</li> <li>• TCP Reserved field</li> <li>• TCP Urgent Pointer field</li> </ul> <p>In inline mode, the TOE can count invalid checksum packets that are dropped. The TOE can also count the packets that gets normalized or dropped because of failed normalization.</p>
FMT_SMF.1/IPS	<p><b><u>FP Services Only</u></b></p> <p>The Administrators can deploy intrusion policy with intrusion rules to any interface.</p>

TOE SFRs	How the SFR is Satisfied
FMT_MOF.1/IPS* FMT_MTD.1/IPS* FMT_SMR.2/IPS*	<p>An interface, however, can only have one policy applied to that interface. The Administrators can also import vendor-defined signatures from Cisco, create their own intrusion rules, create rules to define which traffic is inspected and analyzed, enable anomaly rules/detections, modify thresholds and threshold duration, and configure white-list/black-list. The Administrators or Intrusion Admins can create, modify, or delete intrusion policies but only the Administrators can deploy the policies. Here are the security roles in addition to the all-powerful “Administrator” role.</p> <ul style="list-style-type: none"> <li>• “IPS Administrator” (or Authorized Administrator): Have all privileges and access. This is the same role as identified in FMT_SMR.2 above.</li> <li>• “IPS Analyst” (or Intrusion Admin): Have all access to intrusion policies and network analysis privileges but cannot deploy policies</li> <li>• Access Admin: Have all access to access control policies but cannot deploy policies</li> <li>• Discovery Admin: Have all access to network discovery, application detection, and correlation features but cannot deploy policies</li> <li>• Security Analyst: Have all access to security event analysis feature</li> </ul>
IPS_ABD_EXT.1 IPS_IPB_EXT.1 IPS_NTA_EXT.1 IPS_SBD_EXT.1	<p>The TOE provides network analysis and intrusion policies as part of the NGIPS’s intrusion detection and prevention system. The term “intrusion detection” generally refers to the process of passively analyzing network traffic for potential intrusions and storing attack data for security analysis. The term “intrusion prevention” includes the concept of intrusion detection, but adds the ability to block or alter malicious traffic as it travels across the network.</p> <p>In an intrusion detection/prevention deployment, the TOE examines packets as such:</p> <ul style="list-style-type: none"> <li>• A <u>network analysis policy</u> governs how traffic is decoded and preprocessed so it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt.</li> <li>• An <u>intrusion policy</u> uses intrusion and preprocessor rules (sometimes referred to collectively as intrusion rules) to examine the decoded packets for attacks based on patterns or signatures.</li> </ul> <p>Without decoding and preprocessing, the TOE could not appropriately evaluate traffic for intrusions because protocol differences would make pattern matching impossible. Network analysis policies govern these traffic-handling tasks:</p> <ol style="list-style-type: none"> <li>1. After traffic is filtered by Security Intelligence (i.e., Whitelist/Blacklist). The filtering can be based on IP address, domain name, or URL.</li> <li>2. Before traffic can be inspected by intrusion policies</li> </ol> <p>A network analysis policy governs packet processing in phases. First the system decodes packets through the first three TCP/IP layers, then continues with normalizing, preprocessing, and detecting protocol anomalies:</p>

TOE SFRs	How the SFR is Satisfied
	<ul style="list-style-type: none"> <li>• The packet decoder converts packet headers and payloads into a format that can be easily used by the preprocessors and later, intrusion rules. Each layer of the TCP/IP stack is decoded in turn, beginning with the data link layer and continuing through the network and transport layers. The packet decoder also detects various anomalous behaviors in packet headers.</li> <li>• The inline normalization preprocessor reformats (i.e., normalizes) traffic to minimize the chances of attackers evading detection. It prepares packets for examination by other preprocessors and intrusion rules, and helps ensure that the packets the system processes are the same as the packets received by the hosts on your network.</li> <li>• Various network and transport layers preprocessors detect attacks that exploit IP fragmentation, perform checksum validation, and perform TCP and UDP session preprocessing.</li> <li>• Various application-layer protocol decoders normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the system to effectively apply the same content-related intrusion rules to packets whose data is represented differently, and to obtain meaningful results.</li> <li>• The Modbus and DNP3 SCADA preprocessors detect traffic anomalies and provide data to intrusion rules. The baselines are provided by the preprocessors and detection of anomalies through rules configured by the administrator.</li> <li>• Several preprocessors allow administrators to detect specific threats, such as IP/TCP/UDP/ICMP portscans, ICMP/TCP flooding, DoS attacks and other rate-based attacks (“frequency”). The administrator can configure threshold that mimics normal expected frequency and configure the TOE to detect and drop events exceeding the configured thresholds.</li> </ul> <p>When the system identifies a possible intrusion, it generates an intrusion or preprocessor event (sometimes collectively called intrusion events). Managed Sensors transmit their events to the Firepower Management Center, where the administrators can view the aggregated data and gain a greater understanding of the attacks against their network assets. In an inline deployment, managed Sensors can also drop or replace packets that are known to be harmful.</p> <p>Each intrusion event in the database includes an event header and contains information about the event name and classification; the source and destination IP addresses; ports; the process that generated the event; and the date and time of the event, as well as contextual information about the source of the attack and its target. For packet-based events, the TOE also logs a copy of the decoded packet header and payload for the packet or packets that triggered the event.</p> <p>The packet decoder, the preprocessors, and the intrusion rules engine can all cause the TOE to generate an event. For examples,</p> <ul style="list-style-type: none"> <li>• If the packet decoder (configured in the network analysis policy) receives an IP packet that is less than 20 bytes, which is the size of an IP datagram without any options or payload, the decoder interprets this as anomalous traffic. If, later, the accompanying decoder rule in the intrusion policy that examines the packet is</li> </ul>

TOE SFRs	How the SFR is Satisfied
	<p>enabled, the system generates a preprocessor event.</p> <ul style="list-style-type: none"> <li>• If the IP defragmentation preprocessor encounters a series of overlapping IP fragments, the preprocessor interprets this as a possible attack and, when the accompanying preprocessor rule is enabled, the system generates a preprocessor event.</li> <li>• Within the intrusion rules engine, most intrusion rules are written so that they generate intrusion events when triggered by packets. Please see section 7.1 for more details on Snort rule.</li> </ul> <p>Until the administrator deploy new policies to the network interface, rules in the currently deployed intrusion policies behave as follows:</p> <ul style="list-style-type: none"> <li>• Disabled rules remain disabled.</li> <li>• Rules set to <b>Generate Events</b> continue to generate events when triggered.</li> <li>• Rules set to <b>Drop and Generate Events</b> continue to generate events and drop offending packets when triggered.</li> </ul> <p>The administrator can set thresholds for individual rules, per intrusion policy, to limit the number of times the system logs and displays an intrusion event based on how many times the event is generated within a specified time period. This can prevent the TOE from being overwhelmed with a large number of identical events.</p> <p>The TOE can also be configured to use intrusion rules to detect various attacks such as Teardrop, Bonk, Ping of Death, etc. The administrators can use pre-defined rule or create custom rule to detect these attacks and many more. Please reference the CC Supplemental User Guide for more details.</p> <p>The administrator can configure the Sensor in either a passive or inline deployment. In a passive IPS deployment, the Sensor monitors traffic flowing across a network using a switch SPAN or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This provides the system visibility within the network without being in the flow of network traffic. When configured in a passive deployment, the system cannot take certain actions such as blocking or shaping traffic. The administrator can configure one or more physical ports on a managed Sensor as passive interfaces and deploy the intrusion policy to that interface via security zone (i.e., the interface is added to the zone). In an inline IPS deployment, the administrator configures the Sensor transparently on a network segment by binding two ports together. The administrator can configure one or more physical ports on a managed Sensor as inline interfaces then assign a pair of inline interfaces to an inline set. The intrusion policy is then deployed to that inline set via security zone.</p> <p>The management interface (typically eth0) is separate from the other data monitoring interfaces (used as passive or inline) on the Sensor. It is used to set up and register the Sensor to the FMC. The TOE can perform network analysis and deploy intrusion policies to any data monitoring interface as described above. The policy hierarchy order is not configurable and follows this order: Security Intelligence (whitelist takes precedence over blacklist), anomaly-based rules, then signature-based rules.</p>



TOE SFRs	How the SFR is Satisfied
FPT_ITT.1	The communication between the FMC and Sensor is protected by TLS. TLS provides authentication, key exchange, encryption and integrity protection of all data transmitted between the TOE components.

## 7 SUPPLEMENTAL TOE SUMMARY SPECIFICATION INFORMATION

### 7.1 Tracking of Stateful Firewall Connections

#### 7.1.1 Establishment and Maintenance of Stateful Connections

As network traffic enters an interface of the TOE, the TOE inspects the packet header information to determine whether the packet is allowed by access control lists, and whether an established connection already exists for that specific traffic flow. The TOE maintains and continuously updates connection state tables to keep tracked of establishment, teardown, and open sessions. To help determine whether a packet can be part of a new session or an established session, the TOE uses information in the packet header and protocol header fields to determine the session state to which the packet applies as defined by the RFC for each protocol.

#### 7.1.2 Viewing Connections and Connection States

To display the connection state for the designated connection type, use the **show conn** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses. The syntax is:

```
show conn [count | [all] [detail] [long] [state state_type] [protocol {tcp | udp}] [scansafe] [address src_ip[-src_ip] [netmask mask]] [port src_port[-src_port]] [address dest_ip[-dest_ip] [netmask mask]] [port dest_port[-dest_port]] [user-identity | user [domain_nickname\user_name | user-group [domain_nickname\\user_group_name] | security-group]
```

The **show conn** command displays the number of active TCP and UDP connections, and provides information about connections of various types. By default, the output of “**show conn**” shows only the through-the-TOE connections. To include connections to/from the TOE itself in the command output, add the **all** keyword, “**show conn all**”.

**Table 20: Syntax Description**

<b>address</b>	(Optional) Displays connections with the specified source or destination IP address.
<b>all</b>	(Optional) Displays connections that are to the device or from the device, in addition to through-traffic connections.
<b>count</b>	(Optional) Displays the number of active connections.
<i>dest_ip</i>	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: 10.1.1.1-10.1.1.5
<i>dest_port</i>	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-). For example: 1000-2000
<b>detail</b>	(Optional) Displays connections in detail, including translation type and interface information.



<b>long</b>	(Optional) Displays connections in long format.
<b>netmask</b> <i>mask</i>	(Optional) Specifies a subnet mask for use with the given IP address.
<b>port</b>	(Optional) Displays connections with the specified source or destination port.
<b>protocol</b> { <b>tcp</b>   <b>udp</b> }	(Optional) Specifies the connection protocol, which can be <b>tcp</b> or <b>udp</b> .
<b>scansafe</b>	(Optional) Shows connections being forwarded to the Cloud Web Security server.
<b>security-group</b>	(Optional) Specifies that all connections displayed belong to the specified security group.
<b>src_ip</b>	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: 10.1.1.1-10.1.1.5
<b>src_port</b>	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-). For example: 1000-2000
<b>state</b> <i>state_type</i>	(Optional) Specifies the connection state type.
<b>user</b> [ <i>domain_nickname\</i> ] <i>user_name</i>	(Optional) Specifies that all connections displayed belong to the specified user. When you do not include the <i>domain_nickname</i> argument, the TOE displays information for the user in the default domain.
<b>user-group</b> [ <i>domain_nickname\</i> ] <i>user_group_name</i>	(Optional) Specifies that all connections displayed belong to the specified user group. When you do not include the <i>domain_nickname</i> argument, the TOE displays information for the user group in the default domain.
<b>user-identity</b>	(Optional) Specifies that the TOE display all connections for the Identity Firewall feature. When displaying the connections, the TOE displays the user name and IP address when it identifies a matching user. Similarly, the TOE displays the host name and an IP address when it identifies a matching host.

The connection types that you can specify using the **show conn state** command are defined in the table below. When specifying multiple connection types, use commas without spaces to separate the keywords.

**Table 21: Connection State Types**

<b>Keyword</b>	<b>Connection Type Displayed</b>
<b>up</b>	Connections in the up state.
<b>conn_inbound</b>	Inbound connections.
<b>ctiqbe</b>	CTIQBE connections
<b>data_in</b>	Inbound data connections.
<b>data_out</b>	Outbound data connections.
<b>finin</b>	FIN inbound connections.
<b>finout</b>	FIN outbound connections.
<b>h225</b>	H.225 connections
<b>h323</b>	H.323 connections
<b>http_get</b>	HTTP get connections.
<b>mgcp</b>	MGCP connections.

nojava	Connections that deny access to Java applets.
rpc	RPC connections.
service_module	Connections being scanned by an SSM.
sip	SIP connections.
skinny	SCCP connections.
smtp_data	SMTP mail data connections.
sqlnet_fixup_data	SQL*Net data inspection engine connections.
tcp_embryonic	TCP embryonic connections.
vpn_orphan	Orphaned VPN tunneled flows.

When using the **detail** option, the TOE displays information about the translation type and interface information using the connection flags defined in the table below.

**Table 22: Connection State Flags**

Flag	Description
a	awaiting outside ACK to SYN
A	awaiting inside ACK to SYN
b	TCP state bypass. By default, all traffic that passes through the Cisco Adaptive Security Appliance (ASA) is inspected using the Adaptive Security Algorithm and is either allowed through or dropped based on the security policy. In order to maximize the firewall performance, the ASA checks the state of each packet (for example, is this a new connection or an established connection?) and assigns it to either the session management path (a new connection SYN packet), the fast path (an established connection), or the control plane path (advanced inspection). TCP packets that match existing connections in the fast path can pass through the adaptive security appliance without rechecking every aspect of the security policy. This feature maximizes performance.
B	initial SYN from outside
C	Computer Telephony Interface Quick Buffer Encoding (CTIQBE) media connection
d	dump
D	DNS
E	outside back connection. This is a secondary data connection that must be initiated from the inside host. For example, using FTP, after the inside client issues the PASV command and the outside server accepts, the ASA preallocates an outside back connection with this flag set. If the inside client attempts to connect back to the server, then the ASA denies this connection attempt. Only the outside server can use the preallocated secondary connection.
f	inside FIN
F	outside FIN
g	Media Gateway Control Protocol (MGCP) connection
G	connection is part of a group The G flag indicates the connection is part of a group. It is set by the GRE and FTP Strict fixups to designate the control connection and all its associated secondary connections. If the control connection terminates, then all associated secondary connections are also terminated.
h	H.225
H	H.323
i	incomplete TCP or UDP connection

I	inbound data
k	Skinnny Client Control Protocol (SCCP) media connection
K	GTP t3-response
m	SIP media connection
M	SMTP data
O	outbound data
p	replicated (unused)
P	inside back connection This is a secondary data connection that must be initiated from the inside host. For example, using FTP, after the inside client issues the PORT command and the outside server accepts, the ASA preallocates an inside back connection with this flag set. If the outside server attempts to connect back to the client, then the ASA denies this connection attempt. Only the inside client can use the preallocated secondary connection.
q	SQL*Net data
r	inside acknowledged FIN
R	If TCP: outside acknowledged FIN for TCP connection If UDP: UDP RPC2 Because each row of “show conn” command output represents one connection (TCP or UDP), there will be only one R flag per row.
s	awaiting outside SYN
S	awaiting inside SYN
t	SIP transient connection For a UDP connection, the value t indicates that it will timeout after one minute.
T	SIP connection For UDP connections, the value T indicates that the connection will timeout according to the value specified using the “timeout sip” command.
U	up
V	VPN orphan
W	WAAS
X	Inspected by the service module, such as a CSC SSM.
y	For clustering, identifies a backup owner flow.
Y	For clustering, identifies a director flow.
z	For clustering, identifies a forwarder flow.
Z	Cloud Web Security

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by *app\_id*, and the idle timer for each *app\_id* runs independently. Because the *app\_id* expires independently, a legitimate DNS response can only pass through the TOE within a limited period of time and there is no resource build-up. However, when the **show conn** command is entered, you will see the idle timer of a

DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

When the TOE creates a pinhole to allow secondary connections, this is shown as an incomplete conn by the **show conn** command. Incomplete connections will be cleared from the connections table when they reach their timeout limit, and can be cleared manually by using the “**clear conn**” command. When there is no TCP traffic for the period of inactivity defined by the **timeout conn** command (by default, 1:00:00), the connection is closed and the corresponding conn flag entries are no longer displayed.

If a LAN-to-LAN/Network-Extension Mode tunnel drops and does not come back, there might be a number of orphaned tunnel flows. These flows are not torn down as a result of the tunnel going down, but all the data attempting to flow through them is dropped. The **show conn** command output shows these orphaned flows with the **V** flag.

**Table 23: TCP connection directionality flags**

Flag	Description
B	Initial SYN from outside
a	Awaiting outside ACK to SYN
A	Awaiting inside ACK to SYN
f	Inside FIN
F	Outside FIN
s	Awaiting outside SYN
S	Awaiting inside SYN

### 7.1.3 Examples

The following is sample output from the **show conn** command. This example shows a TCP session connection from inside host 10.1.1.15 to the outside Telnet server at 10.10.49.10. Because there is no B flag, the connection is initiated from the inside. The "U", "I", and "O" flags denote that the connection is active and has received inbound and outbound data.

hostname# **show conn**

54 in use, 123 most used

TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO

UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-

TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags UTIOB

TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags UTIOB

TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB

TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB

TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti

TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0, flags Ti

TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti

TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0, flags Ti

TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti

TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0, flags Ti

TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti

TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0, flags Ti

TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti

TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0, flags Ti

The following is sample output from the **show conn detail** command. This example shows a UDP connection from outside host 10.10.49.10 to inside host 10.1.1.15. The D flag denotes that this is a DNS connection. The number 1028 is the DNS ID over the connection.

### hostname# show conn detail

54 in use, 123 most used

Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,

B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,

D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,

G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,

i - incomplete, J - GTP, j - GTP data, K - GTP t3-response

k - Skinny media, M - SMTP data, m - SIP media, n - GUP

O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,

q - SQL\*Net data, R - outside acknowledged FIN,

R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,

s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,

V - VPN orphan, W - WAAS,

X - inspected by service module

TCP outside:10.10.49.10/23 inside:10.1.1.15/1026, flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435

UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028, flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435

TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060, flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435

TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060, flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346

TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000, flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464

TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000, flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156

TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000, flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405

TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060, flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129

TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060, flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529

TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000, flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718

TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000, flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694

TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000, flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742

TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000, flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582

TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000, flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617

## 7.2 Intrusion Rule Definition

An intrusion rule is a set of keywords and arguments that the system uses to detect attempts to exploit vulnerabilities on your network. As the system analyzes network traffic, it compares packets against the conditions specified in each rule. If the packet data matches all the conditions specified in a rule, the rule triggers. If a rule is an alert rule, it generates an intrusion event. If it is a pass rule, it ignores the traffic. For a drop rule in an inline deployment, the system drops the packet and generates an event. The administrator can view and evaluate intrusion events from the FMC web interface.

All rules contain two logical sections: the rule header and the rule options. The rule header contains:

- the rule's action or type
- the protocol
- the source and destination IP addresses and netmasks
- direction indicators showing the flow of traffic from source to destination
- the source and destination ports

The rule options section contains:

- event messages
- keywords and their parameters and arguments
- patterns that a packet's payload must match to trigger the rule
- specifications of which parts of the packet the rules engine should inspect

The following diagram illustrates the parts of a rule:

For example,

### Rule Header

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
```

### Rule Keywords and Arguments

```
(msg:"WEB-IIS newdsn.exe access";
flow:to_server,established; uricontent:"/scripts/
tools/newdsn.exe"; nocase; metadata:service http;
reference:bugtraq,1818; reference:cve,1999-0191;
reference:nessus,10360; classtype:web-application-
activity; sid:1024; rev:10; )
```

### 7.2.1 Intrusion Rule Header

Every rule has a rule header containing parameters and arguments. The following illustrates parts of a rule header:



Action (*alert*) – generates an intrusion event when triggered.

Protocol (*tcp*) – Tests TCP traffic only. ICMP, IP, TCP, and UDP protocols are supported.

Source IP (*\$EXTERNAL NET*) – Tests traffic coming from any host that is not on your internal network.

Source Port (*any*) – Tests traffic coming from any port on the originating host.

Operate (*->*) – Tests external traffic destined for the web servers on your network.

Destination IP (*\$HTTP SERVERS*) - Tests traffic to be delivered to any host specified as a web server on your internal network. Both IP and IPv6 addresses and ranges are supported.

Destination Port (*\$HTTP PORTS*) - Tests traffic delivered to an HTTP port on your internal network.

## 7.2.2 Intrusion Rule Options and Keywords

Rule options follow the rule header and are enclosed inside a pair of parentheses. There may be one option or many and the options are separated with a semicolon. If you use multiple options, these options form a logical AND. The action in the rule header is invoked only when all criteria in the options are true. In general, an option may have two parts: a keyword and an argument.

The *message* keyword: Specify meaningful text that appears as a message when the rule triggers.

The *ack* keyword: Specify the acknowledgement value. For example, (*flags: A; ack: 0; msg: "TCP ping detected";*) means receive a TCP packet with the A flag set and the acknowledgement contains a value of 0.

The *content* keyword: Specify data pattern inside a packet. The pattern may be presented in the form of an ASCII string or as binary data in the form of hexadecimal characters.

The *offset* keyword: Specify a certain offset from the start of the data part of the packet to search.

The *dsize* keyword: Specify the length of the data part of a packet.

The *flags* keyword: Find out which flag bits are set inside the TCP header of a packet.

The *fragbits* keyword: Find out which three frag bits (Reserved, Don't Frag, More Frag) in the IP headers.

The *fragoffset* keyword: Tests the offset of a fragmented packet.

The *itype* keyword: Specify the ICMP type.

The *icode* keyword: Specify the ICMP code.

The *ipopts* keyword: Specify the IP Options. Record Route, Loose Source Routing, Strict Source Routing.

The *ip\_proto* keyword: Specify the IP protocol number.

The *id* keyword: Specify the IP header fragment identification field

The *nocase* keyword: Its only purpose is to make a case insensitive search of a pattern within the data part of a packet. It is used in conjunction with the *content* keyword.

The *seq* keyword: Specify the sequence number of a TCP packet.

The *window* keyword: Specify the TCP window size.

The *flow* keyword: Apply a rule on TCP sessions to packets flowing in a particular direction.

The *tos* keyword: Detect a specific value in the Type of Service (TOS) field of the IP header.

The *ttl* keyword: Detect Time to Live value in the IP header of the packet.

### 7.3 Key Zeroization

The following table describes the key zeroization referenced by FCS\_CKM.4 provided by the TOE. DRAM (dynamic random access memory) is volatile memory and NVRAM (non-volatile random access memory) is non-volatile “flash” memory.

**Table 24: ASA Key Zeroization**

Critical Security Parameters (CSPs)	Zeroization Cause and Effect
Diffie-Hellman Shared Secret	Automatically zeroized after completion of DH exchange, by calling a specific API within the two crypto modules, when module is shutdown, or reinitialized. Storage: DRAM Overwritten with: 0x00
Diffie Hellman Private Exponent	Automatically zeroized upon completion of DH exchange, by calling a specific API within the two crypto modules, and when module is shutdown, or reinitialized. Storage: DRAM Overwritten with: 0x00
skeyid	Session Encryption Key and IKE Session Authentication Key. Automatically zeroized after IKE session terminated. Storage: DRAM Overwritten with: 0x00
skeyid_d	Session Encryption Key and IKE Session Authentication Key. Automatically zeroized after IKE session terminated.



Critical Security Parameters (CSPs)	Zeroization Cause and Effect
	Storage: DRAM Overwritten with: 0x00
IKE Session Encryption Key	Session Encryption Key and IKE Session Authentication Key. Automatically zeroized after IKE session terminated. Storage: DRAM Overwritten with: 0x00
IKE Session Authentication Key	Session Encryption Key and IKE Session Authentication Key. Automatically zeroized after IKE session terminated. Storage: DRAM Overwritten with: 0x00
ISAKMP Preshared	Zeroized using the following command: <b># no crypto isakmp key</b> Storage: NVRAM Overwritten with: 0x00
IKE RSA and ECDSA Private Keys	Automatically overwritten when a new key is generated or zeroized using the following commands: <b># crypto key zeroize rsa</b> <b># crypto key zeroize ec</b> Storage: NVRAM Overwritten with: 0x00
IPsec Encryption Key	Automatically zeroized when IPsec session terminated. Storage: DRAM Overwritten with: 0x00
IPsec Authentication Key	Automatically zeroized when IPsec session terminated. Storage: DRAM Overwritten with: 0x00
RADIUS Secret	Zeroized using the following command: <b># no radius-server key</b>

Critical Security Parameters (CSPs)	Zeroization Cause and Effect
	Storage: NVRAM Overwritten with: 0x00
SSH Private Key	Automatically zeroized upon generation of a new key Storage: NVRAM Overwritten with: 0x00
SSH Session Key	Automatically zeroized when the SSH session is terminated. Storage: DRAM Overwritten with: 0x00
All CSPs	Zeroized on-demand on all file systems via the “erase” command. Storage: NVRAM

Table 25: FP Services Key Zeroization

Name	Generation / Algorithm	Purpose	Storage Location	Zeroization Summary
RSA public/private keys	DRBG	Identity certificates for the security appliance itself and also used in TLS, and SSH negotiations. The security appliance supports 2048 bit modulus key sizes or higher.	Private Key – Nonvolatile flash memory and DRAM Public Key – Nonvolatile flash memory and DRAM	Private Key - are zeroized then deleted from hard disk when the CA certificates are deleted by the administrators.  Public Key - are deleted from hard disk when the CA certificates are deleted by the administrators.

Name	Generation / Algorithm	Purpose	Storage Location	Zeroization Summary
Diffie-Hellman Key Pairs	DRBG	Key agreement for TLS, and SSH sessions.	DRAM	Keys in RAM are zeroized upon resetting (i.e., terminating all sessions) or rebooting the TOE.
RSA public/private keys	RSA	For communication between the FMC and managed Sensor.	Nonvolatile flash memory/DRAM	Private Key - The private key is zeroized when the FMC and managed Sensors are de-registered.
TLS Session Keys	DH / DRBG Algorithm: AES	Used in HTTPS connections	DRAM	Keys in RAM are zeroized upon rebooting the TOE.
SSH Session Keys	DH / DRBG Algorithm: AES	SSH keys	DRAM	Keys in RAM are zeroized upon rebooting the TOE.
Passwords	User generated	Critical security parameters used to authenticate the administrator login.	Nonvolatile flash memory (Hashed with SHA-512 and salt value)	Passwords are not stored in plaintext. Only the hashed of the passwords and a 32-bit nonces are stored.
Certificates of Certificate Authorities (CAs) [FMC Only]	DRBG	Necessary to verify certificates issued by the CA. Install the CA's certificate prior to installing subordinate certificates.	Nonvolatile flash memory and DRAM	CA certificates are zeroized from hard disk when the CA certificates are deleted by the administrators.  CA certificates in RAM will be zeroized upon rebooting the TOE.

Name	Generation / Algorithm	Purpose	Storage Location	Zeroization Summary
PRNG Seed Key	Entropy	Seed key for DRBG	DRAM	Seed keys are zeroized and overwritten with the generation of new seed

## 8 ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

**Table 26: References**

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-4]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) July 2013
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-4]	FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS) March 2012