# Cisco Adaptive Security Appliances and ASA Virtual Version 9.6

## Security Target

**ST Version 1.0**

**March 27, 2017**

**Americas Headquarters:**

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

# Table of Contents

# List of Tables



# List of Figures

# 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 |
| ASA | Adaptive Security Appliance |
| 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 |
| IPsec | Internet Protocol Security |
| ISR | Integrated Services Router |
| 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 |
| UDP | User Datagram Protocol |
| VLAN | Virtual Local Area Network |

| Acronyms / Abbreviations | Definition |
|---|---|
| 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). 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 Adaptive Security Appliances and ASA Virtual Version 9.6 |
| ST Version | 1.0 |
| Publication Date | March 27, 2017 |
| Vendor and ST Author | Cisco Systems, Inc. |
| TOE Reference | Cisco Adaptive Security Appliances (ASA)<br>Cisco Adaptive Security Appliances Virtual (ASAv) |
| TOE Hardware Models | • ASA 5500 Series (5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X) and (5512-X, 5515-X, 5525-X, 5545-X, 5555-X)<br>• ASA 5585 Series (5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40, 5585-X SSP-60)<br>• ASA Services Module (ASA-SM)[1]<br>• ASAv running on ESXi 5.5 or 6.0 on the Unified Computing System (UCS) B22 M3, B200 M3, B200 M4, B230 M2, B260 M4, B420 M3, B420 M4, B440 M2, B460 M4, C22 M3, C24 M3, C220 M3, C220 M4, C240 M3, C240 M4, C260 M2, C420 M3, C460 M2, and C460 M4<br>• ASAv running on ESXi 5.5 or 6.0 on the E140S M1, E140S M2, E140D M1, E160D M2, E160D M1, E180D M2, E140DP M1, E160DP M1 installed on ISR[2] |
| TOE Software Version | ASA 9.6.2 and ASDM 7.6 |

[1] ASA-SM on Catalyst 6500 Series switches including 6503-E, 6504-E, 6509-E, and 6513-E in the operational environment

[2] ISR is in the operational environment. Please see table 6 in section 1.3 for UCS-E and ISR compatibility.

| | |
|---|---|
| ST Evaluation Status | In Evaluation |
| Keywords | Firewall, VPN Gateway, Router |

## 1.2 TOE Overview

The Cisco Adaptive Security Appliances TOE is a purpose-built, firewall platform with VPN capabilities. The Cisco Adaptive Security Appliances Virtual running on UCS platform (TOE) is also a firewall platform with VPN capabilities. The TOE includes the hardware models as defined in Table 2 of section 1.1. The ASAv must be the only virtual instance on the physical hardware platform providing security functionality (per TD0096). Other guest VM is allowed only if it provides networking functionality.

### 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), 5585-X Series (high-end), ASA-SM, and ASAv 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[3] VPN or remote access VPN. Other uses refer to the use of IPsec

[3] This is also known as site-to-site or peer-to-peer VPN.

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 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.

### 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 over IPsec protected channels. Any SSH client that supports SSHv2 may be used. |
| ASDM Management Platform | Yes | The ASDM 7.6 operates from any of the following operating systems:<br>• Microsoft Windows 7, 8, Server 2008, and Server 2012<br>• Apple OS X 10.4 and later<br>• Red Hat Enterprise Linux 5<br>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. |
| Audit (syslog) Server | Yes | This includes any syslog server to which the TOE would transmit syslog messages. Connections to remote audit servers must be tunneled in IPsec or TLS. |

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

## 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), ASA-SM and ASAv running on ESXi 5.5 and 6.0 on the UCS B22 M3, B200 M3, B200 M4, B230 M2, B260 M4, B420 M3, B420 M4, B440 M2, B460 M4, C22 M3, C24 M3, C220 M3, C220 M4, C240 M3, C240 M4, C260 M2, C420 M3, C460 M2, C460 M4, E140S M1, E140S M2, E140D M1, E160D M2, E160D M1, E180D M2, E140DP M1, E160DP M1 installed on ISR. The software is comprised of the Adaptive Security Appliance software image Release 9.6.2, with ASDM 7.6.

The Cisco Adaptive Security Appliances 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), GB of memory, and Intel Pentium processor.
- **5515-X** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to twelve), 8 GB of memory, and Intel Core i3 processor.
- **5525-X** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to fourteen), 8 GB of memory, and Intel Xeon 3400 Series processor.
- **5545-X** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to fourteen), 12 GB of memory, and Intel Xeon 3400 Series processor.
- **5555-X** – Two RJ-45 management Gigabit Ethernet ports, two RJ45 ports (auxiliary and console), six Gigabit Ethernet ports (expandable to fourteen), 16 GB of memory, and Intel Xeon 3400 Series processor.
- **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), 12 GB of memory, and Intel Xeon 5000 Series processor.
- **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), 24 GB of memory, and Intel Xeon 5000 Series processor.
- **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), 24 GB of memory, and Intel Xeon 5000 Series processor.
- **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), 48 GB of memory, and Intel Xeon 5000 Series processor.

- **ASA-SM** – Installs to Catalyst 6500 series switches including 6503-E, 6504-E, 6509-E, and 6513-E, with 12 GB of memory and Intel Xeon 5000 Series processor on each ASA-SM. All interfaces are logical on the ASA-SM, allowing any port on the 6500 switch to operate as a firewall/VPN port and integrating firewall and VPN gateway security inside the network infrastructure.
- The same ASA image runs on all of the model platforms identified above.

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

**Table 4: ASA 5500 Series Hardware**

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

The underlying UCS platforms 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 ASAv in terms of hardware.

**Figure 2: UCS Hardware**

**Americas Headquarters:**

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

The UCS hardware components in the TOE have the following distinct characteristics:

**Table 5: UCS Hardware**

| **Model** | **B200 M3** | **B200 M4** | **B420 M4** | **B420 M3** | **B260 M4** | **B460 M4** |
|---|---|---|---|---|---|---|
| **Number of Processors** | 2 | 2 | 2 or 4 | 2 or 4 | 2 | 4 |
| **Processor** | Intel Xeon E5-2600 processor product families | Intel Xeon E5-2600 processor product family | Intel Xeon E5-4600 processor product family | Intel Xeon E5-4600 processor product families | Intel Xeon E7 processor product family | Intel Xeon E7 processor product family |
| **Form factor** | Half-width blade | Half-width blade | Full-width blade | Full-width blade | Full-width blade | Full-width Double-high blade |
| **Maximum Memory** | 768 GB, 24 DIMMs | 768 GB, 24 x DDR4 DIMMs | 3.0 TB, 48 DIMMs | 1.5 TB, 48 DIMMs | 3.0 TB, 48 DIMMs | 6.0 TB, 96 DIMMs |
| **Disk Space** | 2.0 TB | 3.2 TB | 4.8 TB | 4.0 TB | 2.4 TB | 4.8 TB |
| **Max I/O per blade** | 80 Gbps (2 x 40 Gbps) | 80 Gbps (2 x 40 Gbps) | 160 Gbps | 160 Gbps (4 x 40 Gbps) | 160 Gbps (4 x 40 Gbps) | 160 Gbps (4 x 40 Gbps) |

| **Model** | **B22 M3** | **B230 M2** | **B440 M2** |
|---|---|---|---|
| **Number of Processors** | 2 | 2 | 2 or 4 |

| | | | |
|---|---|---|---|
| **Processor** | Intel Xeon E5-2400 product family | Intel Xeon E7-2800 or E7-8800 series processor | Intel Xeon E7-4800 or E7-8800 series processor |
| **Form factor** | Half-width blade | Half-width blade | Full-width blade |
| **Maximum Memory** | 384 GB of RAM with 12 DIMM slots | 512 GB of RAM with 32 DIMM slots | 1 TB of RAM with 32 DIMM slots |
| **Disk Space** | 1.0 TB | 400 GB | 900 GB |
| **Max I/O per blade** | 80 Gbps | 80 Gbps (2 x 40 Gbps) | 160 Gbps |

| **Model** | **C22 M3** | **C24 M3** | **C220 M3** | **C220 M4** | **C240 M3** |
|---|---|---|---|---|---|
| **Number of Processors** | 1 or 2 | 1 or 2 | 2 | 2 | 2 |
| **Processor** | Intel Xeon E5-2400 processor product family | Intel Xeon E5-2400 processor product family | Intel Xeon E5-2600 processor product families | Intel Xeon E5-2600 processor product family | Intel Xeon E5-2600 processor product families |
| **Form factor** | 1 RU | 2 RU | 1 RU | 1 RU | 2 RU |
| **Memory** | 384 GB, 12 x DDR3 DIMMs | 384 GB, 12 x DDR3 DIMMs | 512 GB, 16 x DDR3 DIMMs | 768 GB, 24 x DDR4 DIMMs | 768 GB, 24 x DDR4 DIMMs |
| **Disk Space** | SFF- 8 TB<br>LFF- 16 TB | SFF- 16 TB<br>LFF- 32 TB | SFF- 9.6 TB<br>LFF- 16 TB | SFF - 12.8 TB<br>LFF - 16 TB | SFF- 28.8 TB<br>LFF- 48 TB |
| **I/O** | 2 x 1 Gb ports | 2 x 1 Gb ports | 2 x 1 Gb ports | 2 x 1 Gb ports plus 1 x | 4 x 1 Gb ports |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Modular LOM (MLOM) | |

| **Model** | **C240 M4** | **C260 M2** | **C420 M3** | **C460 M2** | **C460 M4** |
|---|---|---|---|---|---|
| **Number of Processors** | 2 | 2 | 2 or 4 | 2 or 4 | 2 or 4 |
| **Processor** | Intel Xeon E5-2600 processor product family | Intel Xeon E7-2800 / 8800 processor product families | Intel Xeon E5-4600 processors product family | Intel Xeon E7-4800 / 8800 processor product families | Intel Xeon E7-4800 / 8800 processor product families |
| **Form factor** | 2 RU | 2 RU | 2 RU | 4 RU | 4 RU |
| **Memory** | 768 GB, 24 x DDR4 DIMMs | 1 TB, 64 x DDR3 DIMMs | 1.5 TB, 48 x DDR3 DIMMs | 2 TB, 64 x DDR3 DIMMs | Up to 3 TB |
| **Disk Space** | SFF - 38.4 TB<br>LFF - 48 TB | 16 TB | 16 TB | 12 TB | 12.8 TB |
| **I/O** | 2 x 1 Gb ports plus 1 x Modular LOM (MLOM) | 2 x 1 Gb ports<br>2 x 10 Gb SFP+ ports (optional) | 4 x 1 Gb ports | 2 x 1 Gb ports<br>2 x 10 Gb ports<br>2 x 10 Gb SFP+ ports | 2 x 1 Gb ports<br>2 x 10 Gb ports |

| **Model** | **UCS E140S M1 and M2** | **UCS E140D M1 and E160D M2 & M1 E180D M2** | **UCS E140DP M1 and E160DP M1** |
|---|---|---|---|
| **Number of Processors** | 4 | 4, 6, or 8 | 4 or 6 |

| | | | |
|---|---|---|---|
| **Processor** | Intel Xeon processor E3-1100 Series | Intel Xeon processor E5-2400 Series | Intel Xeon processor E5-2400 Series |
| **Form factor** | Single-Wide Blade | Double-Wide Blades | Double-Wide Blades with PCIe Cards |
| **Memory** | 8 GB (default) and up to 16 GB (two 8-GB DIMMs) | 8 GB (default) and up to 48 GB (three 16-GB DIMMs) | 8 GB (default) and up to 48 GB (three 16-GB DIMMs) |
| **Disk Space** | Up to two:<br>• 7200-RPM SATA: 1 TB<br>• 10,000-RPM SAS: 900 GB<br>• 10,000-RPM SAS SED: 600 GB | Up to three :<br>• 7200-RPM SATA: 1 TB<br>• 10,000-RPM SAS: 900 GB<br>• 10,000-RPM SAS SED: 600 GB | Up to two:<br>• 7200-RPM SATA: 1 TB<br>• 10,000-RPM SAS: 900 GB<br>• 10,000-RPM SAS SED: 600 GB |
| **NICs** | Two internal and one external Gigabit Ethernet ports | Two internal and two external Gigabit Ethernet ports | Two internal and two external Gigabit Ethernet ports |

**Table 6: UCS-E and ISR Compatibility**

| ISR Platform | E140S | E140D and E160D-M2 | E160D-M1 and E180D |
|---|---|---|---|
| **1921** | **NO** | **NO** | **NO** |
| **1941** | **NO** | **NO** | **NO** |
| **2901** | **NO** | **NO** | **NO** |
| **2911** | YES | **NO** | **NO** |
| **2921** | YES | YES | **NO** |
| **2951** | YES | YES | **NO** |
| **3925** | YES | YES | YES |
| **3945** | YES | YES | YES |
| **3925E** | YES | YES | YES |
| **3945E** | YES | YES | YES |
| **4321** | **NO** | **NO** | **NO** |
| **4331** | YES | **NO** | **NO** |
| **4351** | YES | YES | YES |
| **4431** | **NO** | **NO** | **NO** |
| **4451** | YES | YES | YES |

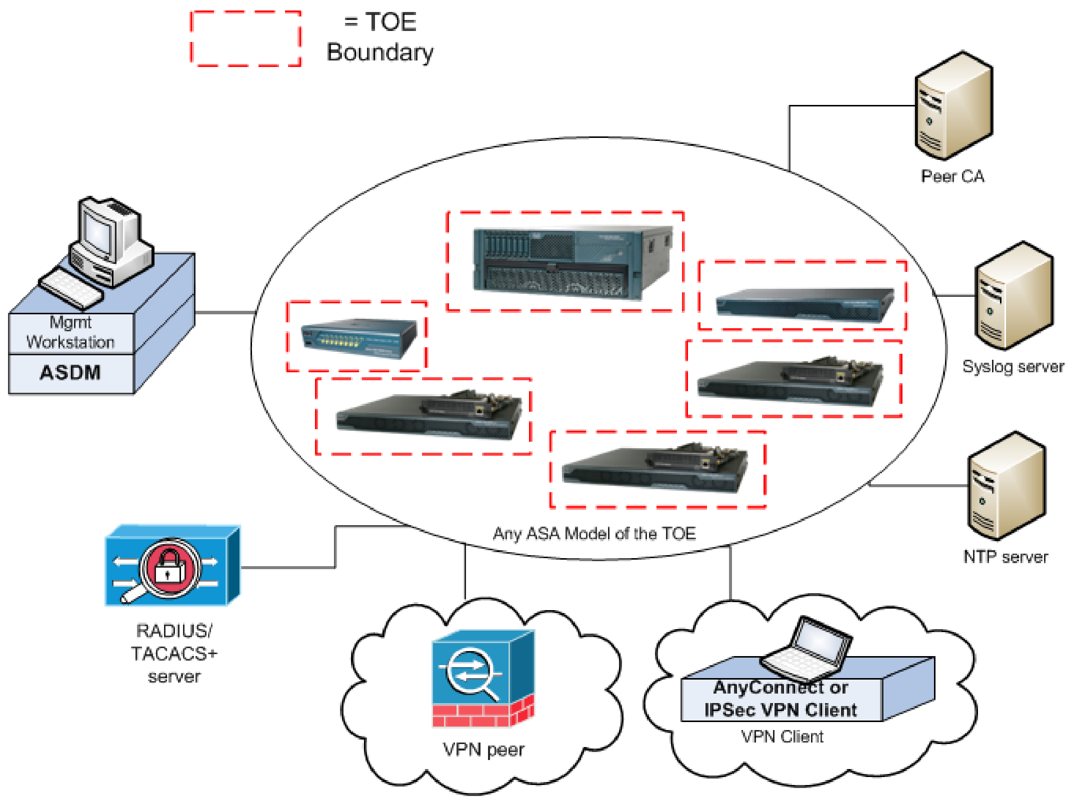
## 1.4 TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 1.5 below and includes the Cisco ASA software, which in turn includes the ASDM software and for ASAv, the UCS platforms which includes the hypervisor. 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. 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 or IPsec. The TOE is able to filter connections to/from these external using its IP traffic filtering, and can encrypt traffic where necessary using TLS and/or IPsec.

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

**Figure 3: Example TOE Deployment**




The previous figure includes the following:

- Several examples of TOE Models
- VPN Peer (Operational Environment) or another instance of the TOE

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

## 1.5 Physical Scope of the TOE

The TOE is a hardware and software solution comprised of the components described in Table 7:

**Table 7 Hardware Models and Specifications**

| TOE Configuration | Hardware Configurations | Software Version |
|---|---|---|
| **ASA 5506-X**<br>**ASA 5506H-X**<br>**ASA 5506W-X**<br>**ASA 5508-X**<br>**ASA 5516-X**<br> | The Cisco ASA 5500-X Adaptive Security Appliance provides high-performance firewall and VPN services and 4-8 Gigabit Ethernet interfaces, and support for up to 300 VPNs. | ASA release 9.6.2 |
| **ASA 5512-X**<br>**ASA 5515-X**<br>**ASA 5525-X**<br>**ASA 5545-X**<br>**ASA 5555-X**<br> | The Cisco ASA 5500-X Adaptive Security Appliance provides high-performance firewall and VPN services and 6-14 Gigabit Ethernet interfaces, and support for up to 5,000 VPNs. | ASA release 9.6.2 |
| **ASA 5585-X SSP-10**<br>**ASA 5585-X SSP-20**<br>**ASA 5585-X SSP-40**<br>**ASA 5585-X SSP-60**<br> | The Cisco ASA 5585 Adaptive Security Appliance provides high-performance firewall and VPN 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 |
| **ASA Services Module (ASA-SM)** | The Cisco Catalyst 6500 Series ASA Services Module supports up to: 20 Gbps maximum firewall throughput (max); 16 Gbps of maximum firewall throughput (multi-protocol); 300,000 connections per second; 10 million | ASA release 9.6.2 |

| | | |
|---|---|---|
|  | concurrent connections; 250 security contexts. | |
| **ASAv** | UCS B22 M3, B200 M3, B200 M4, B230 M2, B260 M4, B420 M3, B420 M4, B440 M2, B460 M4, C22 M3, C24 M3, C220 M3, C220 M4, C240 M3, C240 M4, C260 M2, C420 M3, C460 M2, C460 M4, E140S M1, E140S M2, E140D M1, E160D M2, E160D M1, E180D M2, E140DP M1, E160DP M1 including VM ESXi 5.5 and 6.0. | ASA release 9.6.2 |
| **ASDM** | Included on all ASA models with ASA 9.6.2 | Release 7.6 |

* - The main differences between the ASA and ASAv are the license options and the deployment scenarios.

## 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

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, if so configured.

### 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 over IPsec, and TLS/HTTPS. The cryptographic random bit generators (RBGs) are seeded by an entropy noise source.

### 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 and HTTPS interfaces. The TOE optionally supports use of any RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE.

### 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 over IPsec 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 a secure session is initially established, the TOE displays an administrator- configurable warning banner. This is used to provide any information deemed necessary by the administrator prior to logging in. 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 over IPsec for CLI access, and TLS/HTTPS for GUI/ASDM access. 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.

## 1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

**Table 8: 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. |

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the Protection Profiles: Network Devices collaborative Protection Profile

(NDcPP), Firewall collaborative Protection Profile[4] (FWcPP), and VPN Gateway Extended Package[5] (VPNGWcEP).

[4] Also known as the collaborative Protection Profile for Stateful Traffic Filter Firewalls.

[5] Also known as the Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway.

# 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 5.6.

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 9 below:

Table 9: Protection Profiles

| Protection Profile | Version | Date |
|---|---|---|
| collaborative Protection Profile for Network Devices | 1.0 | 27 February 2015 |
| collaborative Protection Profile for Stateful Traffic Filter Firewalls | 1.0 | 27 February 2015 |
| Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway | 2.0 | 01 December 2015 |

### 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:

- ND collaborative Protection Profile (NDcPP), Firewall collaborative Protection Profile, (FWcPP) and VPN Gateway Extended Package (VPNGWcEP)

### 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 NDcPP, 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 NDcPP, FWcPP, and VPNGWcEP 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 NDcPP and 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 will have extension [VPN] to distinguish them from the NDcPP and 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 10 TOE Assumptions**

| Assumption | Assumption Definition |
|---|---|
| **Reproduced from the NDcPP and FWcPP** | |
| 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_ADMINSTRATOR | 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 firewall. |

| Assumption | Assumption Definition |
|---|---|
| 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. |

## 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 11 Threats**

| Threat | Threat Definition |
|---|---|
| **Reproduced from the NDcPP and FWcPP** | |
| 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. |
| **Reproduced from the VPNGWcEP** | |
| T.NETWORK_DISCLOSURE[VPN] | 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 *phishing* episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information.<br><br>From an infiltration perspective, VPN gateways serve not only to limit access to only specific *destination* 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 *source* 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.<br><br>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. |

| Threat | Threat Definition |
|---|---|
| T. NETWORK_ACCESS[VPN] | 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.<br><br>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.<br><br>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. |

| Threat | Threat Definition |
| --- | --- |
| T.NETWORK_MISUSE[VPN] | Devices located outside the protected network, while permitted to access particular *public* 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.<br><br>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.<br><br>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. |
| T.DATA_INTEGRITY[VPN] | 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. |

| Threat | Threat Definition |
|---|---|
| T.REPLAY_ATTACK[VPN] | 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:<br>• 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.<br>• 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. |

## 3.3 Organizational Security Policies

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

**Table 12 Organizational Security Policies**

| Policy Name | Policy Definition |
|---|---|
| **Reproduced from the NDcPP and FWcPP** | |
| 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.

**Table 13 Security Objectives for the TOE**

| TOE Objective | TOE Security Objective Definition |
|---|---|
| **Reproduced from the VPNGWcEP** | |
| O.CRYPTOGRAPHIC_FUNCTIONS | 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 | 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 | 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. |
| O.FAIL_SECURE | 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 Objective | TOE Security Objective Definition |
|---|---|
| | 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 | 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 | 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 | 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. |

## 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 14 Security Objectives for the Environment**

| Environment Security Objective | IT Environment Security Objective Definition |
|---|---|
| **Reproduced from the NDcPP and FWcPP** | |
| 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 <u>underlined</u> text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the NDcPP, FWcPP, or VPNGWcEP itself, the formatting used in the NDcPP, 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 NDcPP and 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 15 Security Functional Requirements**

| Class Name | Component Identification | Component Name |
|---|---|---|
| **Reproduced from the NDcPP and FWcPP** | | |
| 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_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 |
| **Reproduced from the VPNGWcEP** | | |
| 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 Management | FMT_MTD.1/AdminAct [VPN] | Management of TSF Data |

| Class Name | Component Identification | Component Name |
|---|---|---|
| FPF: Packet Filtering | FPF_RUL_EXT.1[VPN] | Packet Filtering |
| FPT: Protection of the TSF | FPT_FLS.1/SelfTest [VPN] | Fail Secure |
| | FPT_TST_EXT.1.2 [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 |

## 5.3 SFRs Drawn from NDcPP and 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:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the <u>not specified</u> level of audit; and
*c) 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: [<u>no other actions</u>];*

*d) Specifically defined auditable events listed in Table 16.*

**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 16.*

**Table 16 Auditable Events**

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| **Reproduced from the NDcPP and FWcPP** | | |
| 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_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 |
| 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. |

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| | | 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.<br>Termination of the trusted channel.<br>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.<br>Termination of the trusted channel.<br>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<br>Source and destination ports<br>Transport Layer Protocol<br>TOE Interface |
| | Indication of packets dropped due to too much network traffic | TOE interface that is unable to process packets<br>Identifier of rule causing packet drop |
| FFW_RUL_EXT.2 | FTP connection | The interface where the client resides.<br>The IP address of the client.<br>The client port.<br>The interface where the server resides.<br>The IP address of the FTP server.<br>The server port.<br>The FTP username.<br>The stored or retrieved actions.<br>The file stored or retrieved. |
| **Reproduced from the VPNGWcEP** | | |
| 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<br>Source and destination ports<br>Transport Layer Protocol<br>TOE Interface |

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| | 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***

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

#### 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"***

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

#### 5.3.2.2 FCS_CKM.4 Cryptographic Key Destruction

**FCS_CKM_EXT.4.1**[6] 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 [selection:*
>
> - *○ logically addresses the storage location of the key and performs a [**single, consisting of [zeroes]**];*

*]*
that meets the following: *No Standard*.

#### 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.*

#### 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 RSASSAPKCS1v1_ 5*[7]*; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,*

---

[6] Updated per TD0130

[7] Updated per TD0116

- *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*

].

#### 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.1.3**[8] The TSF shall establish the connection only if [**the peer initiates handshake**].

#### 5.3.2.8 FCS_IPSEC_EXT.1 IPsec Procotol

*Application Note: The VPNGWcEP's FCS_IPSEC_EXT.1 takes precedent over the NDcPP.*

**FCS_IPSEC_EXT.1.1** The TSF shall implement the IPsec architecture as specified in RFC 4301.

**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 and **[tunnel mode]**.

*Application Note: The VPNGWcEP's FCS_IPSEC_EXT.1.3 version.*

[8] Updated per TD0125

**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 [*
  - *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 [*
  - *number of **kilo**bytes;*
  - *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 mod 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] Refinement:** The TSF shall ensure that all IKE protocols implement DH Groups **19 (256-bit Random ECP), 20 (384-bit Random ECP),** and [no other DH groups].

*Application Note: Updated based on the TRRT/NIT decision.*

**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 to peers with valid certificates.

#### 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)*].

**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 ASAv have different entropy sources. Both entropy sources will be described in details in the proprietary entropy design documents.*

#### 5.3.2.10 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:

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA *as defined in RFC 3268*
- [ *Optional Ciphersuites:*
  - 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_ECDSA_WITH_AES_128_GCM_SHA256 *as defined in RFC 5289*

  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 *as defined in RFC 5289*].

*Application Note: TLSv1.2 supports all the ciphersuites listed. TLSv1.1 only supports the ciphersuites with SHA.*

**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.

#### 5.3.2.11 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:

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA *as defined in RFC 3268*
- [ *Optional Ciphersuites:*
  - 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_ECDSA_WITH_AES_128_GCM_SHA256 *as defined in RFC 5289*
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 *as defined in RFC 5289*].

*Application Note: TLSv1.2 supports all the ciphersuites listed. TLSv1.1 only supports the ciphersuites with SHA.*

**FCS_TLSS_EXT.1.2**[9] The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [*none*].

**FCS_TLSS_EXT.1.3** The TSF shall generate key establishment parameters using RSA with

[9] Updated per TD0156

key size 2048 bits and [*no other size*] and *[over NIST curves [secp256r1, secp384r1] and no other curves;]*.

### 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 ), ^ (caret), _ (underscore), and ~ (tilde)];*

b) *Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater.*

#### 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.*

**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*].

#### 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 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 security functions of the TOE identified in this EP to the Administrators,*
    - *Ability to configure all security management functions identified in other sections of this EP.]*

*Application Note: Additional management functions from the VPNGWcEP have been added here.*

#### 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: TSF Testing

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

**FPT_TST_EXT.1.2[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).

*Application Note: The VPNGWcEP's FPT_TST_EXT.1.2 component has been added.*

#### 5.3.6.5 FPT_TUD_EXT.1 Trusted Update

**FPT_TUD_EXT.1.1**[10] 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**].
**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 [no other functions] prior to installing those updates.

*Application Note: The VPNGWcEP's FPT_TUD_EXT.1.3 version.*

### 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.

[10] Updated per TD0154

## 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** [*IPsec, 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 [*counting*] packets which are invalid fragments;
b) The TSF shall drop and be capable of [*counting*] 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-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,* [<u>*no other attributes*</u>].

#### 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 TOE SFR Dependencies Rationale for SFRs Found in NDcPP and FWcPP

The NDcPPv1.0 and FWcPPv1.0 contain all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PP itself has been approved.

## 5.6 Security Assurance Requirements

### 5.6.1 SAR Requirements

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

**Table 17: 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 |

### 5.6.2 Security Assurance Requirements Rationale

This Security Target claims conformance to the NDcPP and 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.

## 5.7 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 18: 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<br>ALC_CMS.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. |
| 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 19: How TOE SFRs Are Satisfied**

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Satisfied</th></tr>
<tr><td colspan="2">Security Functional Requirements Drawn from NDcPP and FWcPP</td></tr>
<tr><td>FAU_GEN.1</td><td>
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.
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:
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.
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:
Nov 21 2012 20:39:21: %ASA-3-201011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.
Nov 21 2012 20:39:21: %ASA-3-202011: Connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name
For more information on the required auditable events and the actual logs themselves, please refer to the Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration.
The following high-level events are auditable by the TOE:
<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>
</td></tr>
</table>

| 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.<br>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.<br>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. |
| FAU_GEN.2 | The TOE ensures each action performed by the administrator at the CLI or via ASDM is logged with the administrator’s identity and as a result events are traceable to a specific user. | |
| FAU_STG_EXT.1 | 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.<br>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 | |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | forwarding network traffic when it discovers it can no longer communicate with its configured syslog server(s).<br><br>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. |
| 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 | 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.<br><br>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.<br><br>Key establishment for asymmetric keys on all models of the TOE implements 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. The TOE can act as either the sender or receiver in the RSA-based key establishment scheme depending on the connection.<br><br>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 7.2. 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:<br><br>asa(config)#**crypto key zeroize rsa** [label key-pair-label] [default] [noconfirm]<br><br>asa(config)#**crypto key zeroize ec** [label key-pair-label]<br><br>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-tested 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-tested AES.<br><br>• Series: (ASA-5506-X, 5506-WH, 5508-X, 5516-X), (ASA-5512-X, 5515-X, 5525-X, 5545-X, 5555-X), (5585-X SSP10/20/40/60) FIPS #**4249**<br>• ASA-SM FIPS #**4249**<br>• ASAv software FIPS #**4344**<br><br>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, |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | the key size is configurable down to 1024, but only 2048 key size is permitted in the evaluated configuration.<br>• Series: (ASA-5506-X, 5506-WH, 5508-X, 5516-X), (ASA-5512-X, 5515-X, 5525-X, 5545-X, 5555-X), (5585-X SSP10/20/40/60) FIPS #**2298** and **989**<br>• ASA-SM FIPS #**2298** and **989**<br>• ASAv software FIPS #**2346** and **1027**<br>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:<br>• Series: (ASA-5506-X, 5506-WH, 5508-X, 5516-X), (ASA-5512-X, 5515-X, 5525-X, 5545-X, 5555-X), (5585-X SSP10/20/40/60) FIPS #**1002/1134**<br>• ASA-SM FIPS #**1002/1134**<br>• ASAv software FIPS #**1048/1135**<br>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).<br>• Series: (ASA-5506-X, 5506-WH, 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**<br>• ASA-SM FIPS #**3486** and **2787**<br>• ASAv software FIPS #**3579** and **2882**<br>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, and the ASA-SM) use an SP 800-90 Hash_DRBG with SHA-512. Random number generation in the ASAv uses hardware ring oscillators from the UCS platforms as the entropy source. More information is provided in the entropy design documentation.<br>• Series: (ASA-5506-X, 5506-WH, 5508-X, 5516-X), (ASA-5512-X, 5515-X, 5525-X, 5545-X, 5555-X), (5585-X SSP10/20/40/60) FIPS #**1328**<br>• ASA-SM FIPS # **1328**<br>• ASAv software FIPS #**1386** |
| FCS_HTTPS_EXT.1<br>FCS_TLSC_EXT.2<br>FCS_TLSS_EXT.1 | 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.<br>The TOE supports TLS v1.2 and TLSv1.1 connections with any of the following ciphersuites:<br>• TLS_RSA_WITH_AES_128_CBC_SHA |

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Satisfied</th></tr>
<tr><td></td><td>
<ul>
<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>
When the TOE acts as a TLS client, the administrators can specify the reference-identity using the following command:
asa(config)#crypto ca reference-identity reference-identity-name
follow by one or more of the values
cn-id value
dns-id value
srv-id value
uri-id value
For example,
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# cn-id syslog.cisco.com
To configure the syslog server certification[11] verification, use this syntax:
logging host interface_name syslog_ip [tcp/port | udp/port] [format emblem] [secure [reference-identity reference_identity_name]] [permit-hostdown]
For example,<br>ciscoasa(config)# logging host outside 10.86.93.123 tcp/6514 secure reference-identity syslogServer
NIST curves are supported by default but mutual authentication must be configured with the client-side X.509v3 certificate.
The TOE can be configured to specify which TLS versions are supported using
asa(config)#ssl client-version {<s>tlsv1 |</s> tlsv1.1 | tlsv1.2}
asa(config)#ssl server-version {<s>tlsv1 |</s> tlsv1.1 | tlsv1.2}
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.
</td></tr>
<tr><td>FCS_IPSEC_EXT.1</td><td>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</td></tr>
</table>

[11] Certificate pinning is not supported. In addition, IP address and wildcards are not supported in the ID.

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | 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.<br>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.<br>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 maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including:<br>• The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based),<br>• The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and<br>• 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<br>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.<br>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 |

| TOE SFRs | How the SFR is Satisfied |
| --- | --- |
| | require use of main mode by configuring the mode for each IPsec tunnel, as in the following examples:<br>asa(config)#**crypto map** *map-name seq-num* **set ikev2 phase1-mode main**<br>asa(config)# **crypto ipsec security-association lifetime {seconds** *seconds* **\|** **kilobytes** *kilobytes***}**<br>asa(config-ikev2-policy)# **lifetime seconds** *seconds*<br>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:<br>asa(config)#**crypto ipsec ikev2 ipsec-proposal** *proposal tag proposal_name*<br>asa(config-ipsec-proposal)#**protocol esp encryption** {aes \| aes-192 \| aes-256 \| aes-gcm \| aes-gcm-192 \| aes-gcm-256 ~~\| aes-gmac \| aes-gmac-192 \| aes-gmac-256~~}<br>asa(config-ipsec-proposal)#**protocol esp integrity** {sha-1 \| sha-256 \| sha-384 \| sha-512 \| null}<br>**Note:** 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.<br>The IKEv2 protocols supported by the TOE implement the following DH groups: 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:<br>asa(config)#**crypto ikev2 policy** *priority policy_index*<br>asa(config-ikev2-policy)#**encryption** [~~null \| des \| 3des \|~~ aes \| ~~aes-192~~[12] \| aes-256 \| aes-gcm \| ~~aes-gcm-192~~ \| aes-gcm-256]<br>asa(config-ikev2-policy)#**integrity [**~~md5 \|~~ sha \| sha256 \| sha384 \| sha512**]**<br>asa(config-ikev2-policy)#**group** {19 \| 20}<br>asa(config-ikev2-policy)#**prf** {sha \| sha256 \| sha512}<br>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.<br>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 **crypto ipsec ikev2 sa-strength-enforcement** command.<br>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). |

[12] 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*.

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Satisfied</th></tr>
<tr><td></td><td>To configure an IKEv2 connection to use a RSA or ECDSA signature:<br><br>asa(config)#**tunnel-group** *name* **ipsec-attributes**<br><br>asa(config-tunnel-ipsec)#**ikev2** {local-authentication | remote-authentication} **certificate** *trustpoint*<br><br>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: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “?”, 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<>, 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.<br><br>To configure an IKEv2 connection to use a pre-shared key:<br><br>asa(config)#**tunnel-group** *name* **ipsec-attributes**<br><br>asa(config-tunnel-ipsec)#**ikev2** {local-authentication | remote-authentication} **pre-shared-key hex** *key-value*<br><br>To configure the reference identifier, please use the following command:<br><br>asa(config)#**crypto ca reference-identity** *reference-identity-name*<br><br>follow by one or more of the values<br><br>cn-id *value*<br><br>dns-id *value*<br><br>srv-id *value*<br><br>uri-id *value*<br><br>Specifying the **reference-identity** keyword enables RFC 6125 (section 6.0) checks and identifies the reference identity to use by name.<br><br>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</td></tr>
</table>

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | 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. |
| FDP_RIP.2 | The TOE ensures that packets transmitted from 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. |
| FIA_PMG_EXT.1 | 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. |
| FIA_UIA_EXT.1 | 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 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.<br><br>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. |
| FIA_UAU_EXT.2 | The TOE provides a local password based authentication mechanism as well as RADIUS authentication.<br><br>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.<br><br>The TOE can invoke an external authentication server to provide a single-use authentication mechanism by forwarding the authentication requests to the external authentication server (when configured by the TOE to provide single-use authentication).<br><br>The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | 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. |
| FIA_UAU.7 | 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. |
| FIA_X509_EXT.1<br>FIA_X509_EXT.2<br>FIA_X509_EXT.3 | 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.<br><br>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.<br><br>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:<br><br>asa(config)#**crypto key generate** [rsa [general-keys \| label <name> \| modules [~~512 \| 768 \| 1024 \|~~ 2048 \| 4096] \| noconfirm \| usage-keys] \| ecdsa [label <name> \| elliptic-curve [256 \| 384 \| 521] \| noconfirm]]<br><br>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.<br><br>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), the trusted channel is not established. For more information, please refer to the Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration. |
| FMT_MOF.1(1)/<br>TrustedUpdate | 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 |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| FMT_MOF.1(1)/ AdminAct<br><br>FMT_MOF.1(2)/ AdminAct | disable service and features, and access TOE data, such as audit data, configuration data, security attributes, information flow rules, and session thresholds. |
| FMT_MTD.1 | 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. |
| FMT_SMF.1 | 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 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 ( ‘access list’ commands), information flow rules (‘access list’ commands), modify the timestamp (‘clock’ commands), specify limits for authentication failures (‘aaa local authentication lockout’), 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.<br><br>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 commends. There are specific commands for the configuration of cryptographic services. Trusted updates to the product can be verified using cryptographic digital signature.<br><br>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. |
| FMT_SMR.2 | 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. |

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Satisfied</th></tr>
<tr><td></td><td>
Through the CLI the ‘username’ command is used to maintain, create, and delete users. Through ASDM this is done on the ‘Configuration > Device Management > Users/AAA > User Accounts’ page.
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 it “admin”, allowing the username to authenticate (with valid password) to admin interfaces.
'aaa authentication ssh console LOCAL' can be used to set the TOE to authenticate SSH users against the local database. Note: The SSH must be tunneled over IPsec.
'aaa authorization exec' can be used to require re-authentication of users before they can get to EXEC mode.
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”.
When command authorization has been enabled the default sets of privileges take effect at certain levels, and the levels become customizable.
<ul>
<li>When “aaa authorization command LOCAL” has NOT been applied to the config:
<ul>
<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>
<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>
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”.
</td></tr>
<tr><td>FPT_SKP_EXT.1</td><td>The TOE stores all private keys in a secure directory (an ‘opaque’ virtual filesystem in flash memory called “system:”) that is not readily accessible to administrators. All</td></tr>
</table>

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | pre-shared and symmetric keys are stored in encrypted form, or are masked when showing the configuration via administrative interfaces (CLI or GUI). |
| FPT_APW_EXT.1 | 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. |
| FPT_STM.1 | 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.<br><br>This functionality can be set at the CLI using the 'clock' commands or in ASDM through the 'Configuration > Device Setup > System Time' page. The TOE can optionally be set to receive time from an NTP server.<br><br>The ASAv relies on a reliable software-based real-time-clock (RTC) provided by the hypervisor. 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. |
| FPT_TST_EXT.1 | The TOE run a suite of self-tests during initial start-up (power-on-self-tests or POST) to verify its correct operation. FIPS mode must be enabled in the evaluated configuration. 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. |
| FPT_TUD_EXT.1 | 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.<br><br>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 & Operational User Guide for the Common Criteria Certified Configuration. |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| FTA_SSL_EXT.1<br>FTA_SSL.3 | 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 administrator to log in again to establish a new session when needed. |
| FTA_SSL.4 | 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. |
| FTA_TAB.1 | 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). |
| FTP_ITC.1 | The TOE uses IPsec to protect communications between itself and remote entities for the following purposes:<br>• The TOE protects transmission of audit records when sending syslog message to a remote audit server by transmitting the message over IPsec and TLS.<br>• 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.<br>• 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. |
| FTP_TRP.1 | 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 ASDM connections in IPsec VPN tunnels (peer-to-peer, or remote VPN client). |
| FFW_RUL_EXT.1.1<br>FFW_RUL_EXT.1.2 | The TOE provides stateful traffic filtering of IPv4 and IPv6 network traffic. 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.<br>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.<br>The proper session establishment and termination followed by the TOE is as defined in the following RFCs: |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | • RFC 792 (ICMPv4)<br>• RFC 4443 (ICMPv6)<br>• RFC 791 (IPv4)<br>• RFC 2460 (IPv6)<br>• TCP, RFC 793, section 2.7 Connection Establishment and Clearing<br>• UDP, RFC 768 (not applicable, UDP is a "stateless" protocol)<br><br>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. |
| FFW_RUL_EXT.1.2 | 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:<br><br>• 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);<br>• 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);<br>• Port numbers, and length as defined in RFC 768 (UDP); and<br>• Session identifiers, sequence numbers, types, and codes as defined in RFC 792 (ICMPv4), and RFC 4443 (ICMPv6). |
| FFW_RUL_EXT.1.3,<br>FFW_RUL_EXT.1.4 | 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.<br><br>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.:<br><br>asa(config)# **interface** gigabitethernet0/1<br><br>asa(config-if)# **nameif** inside |

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Satisfied</th></tr>
<tr><td></td><td>The interface types that can be assigned to an access-group are:<br>• Physical interfaces<br>  o Ethernet<br>  o GigabitEthernet<br>  o TenGigabitEthernet<br>  o Management<br>• Port-channel interfaces (designated by a port-channel number)<br>• Subinterface (designated by the subinterface number)<br><br>The default state of an interface depends on the type and the context mode:<br>• For the “system” context in single mode or multiple context mode, interfaces have the following default states:<br>  o Physical interfaces = Disabled<br>  o Subinterfaces = Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.<br>• 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 been allocated.<br><br>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.<br><br>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): “nameif”, and, for routed mode, “ip address”. For subinterfaces, also configure the “vlan” command.</td></tr>
<tr><td>FFW_RUL_EXT.1.5</td><td>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.<br><br>A stateful firewall like the ASA or ASAv, however, takes into consideration the state of a packet:<br>• Is this a new connection?<br><br>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."</td></tr>
</table>

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | The session management path is responsible for the following tasks:<br>– Performing the access list checks<br>– Performing route lookups<br>– Allocating NAT translations (xlates)<br>– Establishing sessions in the "fast path"<br>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.<br>• Is this an established connection?<br>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:<br>– IP checksum verification<br>– Session lookup<br>– TCP sequence number check<br>– NAT translations based on existing sessions<br>– Layer 3 and Layer 4 header adjustments |
| FFW_RUL_EXT.1.6, FFW_RUL_EXT.1.7 | 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 count that such packets/frames were dropped.<br>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.<br>asa(config)# **ip audit name** *name* {info \| attack} [action [alarm] [drop] [reset]]<br>asa(config)# **ip audit interface** *interface_name policy_name*<br>Example:<br>asa(config)# ip audit name ccpolicy1 attack action alarm reset<br>asa(config)# ip audit name ccpolicy2 info action alarm reset<br>asa(config)# ip audit interface outside ccpolicy1<br>asa(config)# ip audit interface inside ccpolicy2<br>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:<br>%ASA-4-4000*nn*: IPS:*number string* from *IP_address* to *IP_address* on interface *interface_name* |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | The following traffic will be denied by the TOE, and audit messages will be generated as indicated:<br>1. packets which are invalid fragments, including IP fragment attack<br>%ASA-2-106020: Deny IP teardrop fragment (size = *number*, offset = *number*) from *IP_address* to *IP_address*<br>%ASA-4-209004: Invalid IP fragment, size = *bytes* exceeds maximum size= *bytes*: src = *source_address*, dest = *dest_address*, proto = *protocol*, id = *number*<br>%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*.<br>The following messages will be generated when configured as described above.<br>%ASA-4-400007: IPS:1100 IP Fragment Attack from *IP_address* to *IP_address* on interface *interface_name*<br>%ASA-4-400009: IPS:1103 IP Overlapping Fragments (Teardrop) from *IP_address* to *IP_address* on interface *interface_name*<br>%ASA-4-400023: IPS:2150 Fragmented ICMP traffic from *IP_address* to *IP_address* on interface *interface_name*<br>%ASA-4-400025: IPS:2154 Ping of Death Attack from *IP_address* to *IP_address* on interface *interface_name*<br>2. fragmented IP packets which cannot be re-assembled completely;<br>%ASA-4-209003: Fragment database limit of *number* exceeded: src = *source_address*, dest = *dest_address*, proto = *protocol*, id = *number*<br>%ASA-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.<br>%ASA-4-423005: Dropped NBDGM *pkt_type_name* fragment with *error_reason_str* from *ifc_name*:*ip_address*/*port* to *ifc_name*:*ip_address*/*port*.<br>%ASA-4-507002: Data copy in proxy-mode exceeded the buffer limit<br>%ASA-7-715060: Dropped received IKE fragment. Reason: *reason*<br>%ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.<br>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;<br>%ASA-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name.*<br>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;<br>%ASA-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name.*<br>This next message appears when Unicast RPF has been enabled with the **ip verify reverse-path** command. |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | %ASA-1-106021: Deny *protocol* reverse path check from *source_address* to *dest_address* on interface *interface_name*<br>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 **ip verify reverse-path** command is not configured.<br>%ASA-1-106022: Deny *protocol* connection spoof from *source_address* to *dest_address* on interface *interface_name*<br>*5.* packets where the source address of the network packet is defined as being on a broadcast network;<br>%ASA-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name.*<br>*6.* packets where the source address of the network packet is defined as being on a multicast network;<br>%ASA-4-106023: Deny *protocol* src [*interface_name*:*source_address/source_port*] dst i*nterface_name*:*dest_address/dest_port* [type {*string*}, code {*code*}] by access_group *acl_ID*<br>The following message will be generated when the rules listed below are configured without the "log" option.<br>%ASA-4-106100: access-list *acl_ID* denied *protocol* *interface_name*/*source_address*(*source_port*) -*interface_name*/*dest_address*(*dest_port*) hit-cnt *number* ({first hit \| *number*-secondinterval}) hash codes<br>The following message will be generated when these rules are configured with the "log" option:<br>asa(config)#**object-group network** *grp_name*<br>asa(config-network-object-group)#**network-object** 224.0.0.0 255.0.0.0 #IPv4 multicast<br>asa(config-network-object-group)#**network-object** FF00::/8 #IPv6 multicast<br>asa(config)#**access-list** *acl-name* **extended deny ip** *grp-name* **any [log]**<br>asa(config)#**access-group in interface** *int-name*<br>*7.* packets where the source address of the network packet is defined as being a loopback address;<br>%ASA-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name.*<br>The following message will be generated when no ACL has been defined to explicitly deny this traffic.<br>%ASA-4-106023: Deny *protocol* src [*interface_name*:*source_address/source_port*] dst i*nterface_name*:*dest_address/dest_port* [type {*string*}, code {*code*}] by access_group *acl_ID* |

| TOE SFRs | How the SFR is Satisfied |
| --- | --- |
| | The following message will be generated when the rules listed below are configured without the “log” option.<br><br>%ASA-4-106100: access-list *acl_ID* denied *protocol* *interface_name*/*source_address*(*source_port*) - *interface_name*/*dest_address*(*dest_port*) hit-cnt *number* ({first hit \| *number*-secondinterval}) hash codes<br>The following message will be generated when these rules are configured with the “log” option:<br>asa(config)#**object-group network** *grp_name*<br>asa(config-network-object-group)#**network-object** 127.0.0.0 255.0.0.0 #IPv4 loopback<br>asa(config-network-object-group)#**network-object** ::1/128 #IPv6 loopback<br>asa(config)#**access-list** *acl-name* **extended deny ip** *grp-name* **any [log]**<br>asa(config)#**access-group in interface** *int-name*<br><br>*8.* packets where the source address of the network packet is a multicast;<br><br>See item number 6.<br><br>*9.* packets where the source or destination address of the network packet is a link-local address;<br><br>%ASA-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name.*<br><br>The following message will be generated when no ACL has been defined to explicitly deny this traffic.<br><br>%ASA-4-106023: Deny *protocol* src [*interface_name*:*source_address/source_port*] dst i*nterface_name*:*dest_address/dest_port* [type {*string*}, code {*code*}] by access_group *acl_ID*<br>The following message will be generated when the rules listed below are configured without the “log” option.<br><br>%ASA-4-106100: access-list *acl_ID* denied *protocol* *interface_name*/*source_address*(*source_port*) - *interface_name*/*dest_address*(*dest_port*) hit-cnt *number* ({first hit \| *number*-secondinterval}) hash codes<br>The following message will be generated when these rules are configured with the “log” option:<br>asa(config)#**object-group network** *grp_name*<br>asa(config-network-object-group)#**network-object** 127.0.0.0 255.0.0.0 #IPv4 link-local<br>asa(config-network-object-group)#**network-object** FE80::/10 #IPv6 link-local<br>asa(config)#**access-list** *acl-name* **extended deny ip** *grp-name* **any [log]**<br>asa(config)#**access-list** *acl-name* **extended deny ip any** *grp-name* **[log]**<br>asa(config)#**access-group in interface** *int-name* |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | *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;<br>%ASA-4-106023: Deny *protocol* src [*interface_name*:*source_address/source_port*] dst i*nterface_name*:*dest_address/dest_port* [type {*string*}, code {*code*}] by access_group *acl_ID*<br>The following message will be generated when the rules listed below are configured without the “log” option.<br><br>%ASA-4-106100: access-list *acl_ID* denied *protocol* *interface_name*/*source_address*(*source_port*) - *interface_name*/*dest_address*(*dest_port*) hit-cnt *number* ({first hit \| *number*-secondinterval}) hash codes<br>The following message will be generated when these rules are configured with the “log” option:<br>asa(config)#**object-group network** *grp_name*<br>asa(config-network-object-group)#**network-object** 192.0.0.0 255.0.0.0 #IPv4 reserved<br>asa(config-network-object-group)#**network-object** 240.0.0.0 128.0.0.0 #IPv4 reserved<br>asa(config)#**access-list** *acl-name* **extended deny ip** *grp-name* **any [log]**<br>asa(config)#**access-list** *acl-name* **extended deny ip any** *grp-name* **[log]**<br>asa(config)#**access-group in interface** *int-name*<br>*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;<br>%ASA-4-106023: Deny *protocol* src [*interface_name*:*source_address/source_port*] dst i*nterface_name*:*dest_address/dest_port* [type {*string*}, code {*code*}] by access_group *acl_ID*<br>The following message will be generated when the rules listed below are configured without the “log” option.<br><br>%ASA-4-106100: access-list *acl_ID* denied *protocol* *interface_name*/*source_address*(*source_port*) - *interface_name*/*dest_address*(*dest_port*) hit-cnt *number* ({first hit \| *number*-secondinterval}) hash codes<br>The following message will be generated when these rules are configured with the “log” option:<br>asa(config)#**object-group network** *grp_name*<br>asa(config-network-object-group)#**network-object** :: #IPv6 unspecified<br>asa(config-network-object-group)#**network-object** 0000::/8 #IPv6 reserved<br>asa(config)#**access-list** *acl-name* **extended deny ip** *grp-name* **any [log]**<br>asa(config)#**access-list** *acl-name* **extended deny ip any** *grp-name* **[log]**<br>asa(config)#**access-group in interface** *int-name* |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | *12.* Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified;<br>%ASA-6-106012: Deny IP from *IP_address* to *IP_address*, IP options *hex*.<br>The following messages will be generated when configured as described above.<br>%ASA-4-400001: IPS:1001 IP options-Record Packet Route from *IP_address* to *IP_address* on interface *interface_name*<br>%ASA-4-400004: IPS:1004 IP options-Loose Source Route from *IP_address* to *IP_address* on interface *interface_name*<br>%ASA-4-400006: IPS:1006 IP options-Strict Source Route from *IP_address* to *IP_address* on interface *interface_name*<br>*13.* By default, TOE will also drop (and is capable of logging) a variety of other IP packets with invalid content including:<br>• Invalid source and/or destination IP address including:<br>o source or destination is the network address (e.g. 0.0.0.0)<br>o source and destination address are the same (with or without the source and destination ports being the same)<br>o first octet of the source IP is equal to zero<br>o network part of the source IP is equal to all zeros or all ones<br>o host part of the source IP is equal to all zeros or all ones<br>Invalid ICMP packets including: sequence number mismatch; invalid ICMP code, and ICMP responses unrelated to any established ICMP session |
| FFW_RUL_EXT.1.8 | 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 chances the sequence in which the entries are compared to network traffic flows. |
| FFW_RUL_EXT.1.9 | 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". |
| FFW_RUL_EXT.1.10 | 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 |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | 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. |
| FFW_RUL_EXT.2 | The TOE supports dynamic establishment of secondary network sessions (e.g., FTP). The TOE will manage establishment and teardown of the following protocols in accordance with the RFC for each protocol:<br>• FTP (File Transfer Protocol) is a TCP protocol supported in either active or passive mode:<br>o In active mode the client initiates the control session, and the server initiates the data session to a client port provided by the client;<br>o 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 permit data sessions to be initiated from the server to the client while the control session is active.<br>o 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.<br>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. |
| 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] | 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.<br>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. |
| FIA_PSK_EXT.1 [VPN] | 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- |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | 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, or HMAC-SHA-512) configured by the administrator. |
| FIA_X509_EXT.4[VPN] | See FIA_X509_EXT.x |
| FMT_MTD.1/AdminAct [VPN] | 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 and certificates used in VPN), routing tables, and session thresholds. |
| FPF_RUL_EXT.1 [VPN] | 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.<br>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.<br>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:<br>1. Presumed address of source<br>2. Presumed address of destination<br>3. Transport layer protocol (or next header in IPv6)<br>4. Service used (UDP or TCP ports, both source and destination)<br>5. Network interface on which the connection request occurs<br>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.<br>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.<br>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; |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| | 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;<br><br>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;<br><br>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;<br><br>These interfaces reject requests in which the subject specifies the route for information to flow when it is in route to its destination; and<br><br>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.<br><br>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.<br><br>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. |
| FPT_FLS.1/SelfTest [VPN] | 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.<br><br>Whenever a failure 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. |
| FPT_TST_EXT.1.2 [VPN] | See FPT_TST_EXT.1 |
| FPT_TUD_EXT.1.3 [VPN] | See FPT_TUD_EXT.1 |
| FTA_SSL.3[VPN] | 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 **vpn-idle-timeout** or **default-idle-timeout** commands in the VPN configuration. |

| TOE SFRs | How the SFR is Satisfied |
|---|---|
| FTA_TSE.1[VPN] | 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 **vpn-access-hours** command can be used to restrict access based on date and time. |
| FTA_VCM_EXT.1 [VPN] | The TOE provides the option to assign the remotely connecting VPN client an internal network IP address. The **ip-local-pool** command can be used to define the range of IP and IPv6 addresses to be available for use. |
| FTP_ITC.1.1[VPN] | See FTP_ITC.1 |

# 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**

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

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

| Keyword | Connection Type Displayed |
|---|---|
| up | Connections in the up state. |
| conn_inbound | Inbound connections. |
| ctiqbe | CTIQBE connections |
| data_in | Inbound data connections. |
| data_out | Outbound data connections. |
| finin | FIN inbound connections. |
| finout | FIN outbound connections. |
| h225 | H.225 connections |
| h323 | H.323 connections |
| http_get | HTTP get connections. |
| mgcp | 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<br>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 | Skinny 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<br>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<br>If UDP: UDP RPC2<br>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<br>For a UDP connection, the value t indicates that it will timeout after one minute. |
| T | SIP connection<br>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 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 memory (also known as flash memory).

**Table 24: TOE 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.<br>Storage: DRAM<br>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.<br>Storage: DRAM<br>Overwritten with: 0x00 |
| skeyid | Session Encryption Key and IKE Session Authentication Key. Automatically zeroized after IKE session terminated.<br>Storage: DRAM<br>Overwritten with: 0x00 |
| skeyid_d | Session Encryption Key and IKE Session Authentication Key. Automatically zeroized after IKE session terminated.<br>Storage: DRAM<br>Overwritten with: 0x00 |
| IKE Session Encryption Key | Session Encryption Key and IKE Session Authentication Key. Automatically zeroized after IKE session terminated.<br>Storage: DRAM<br>Overwritten with: 0x00 |
| IKE Session Authentication Key | Session Encryption Key and IKE Session Authentication Key. Automatically zeroized after IKE session terminated.<br>Storage: DRAM<br>Overwritten with: 0x00 |
| ISAKMP Preshared | Zeroized using the following command:<br>**# no crypto isakmp key**<br>Storage: NVRAM |

| Critical Security Parameters (CSPs) | Zeroization Cause and Effect |
|---|---|
| | Overwritten with: 0x00 |
| IKE RSA and ECDSA Private Keys | Automatically overwritten when a new key is generated or zeroized using the following commands:<br>**# crypto key zeroize rsa**<br>**# crypto key zeroize ec**<br>Storage: NVRAM<br>Overwritten with: 0x00 |
| IPsec Encryption Key | Automatically zeroized when IPsec session terminated.<br>Storage: DRAM<br>Overwritten with: 0x00 |
| IPsec Authentication Key | Automatically zeroized when IPsec session terminated.<br>Storage: DRAM<br>Overwritten with: 0x00 |
| RADIUS Secret | Zeroized using the following command:<br>**# no radius-server key**<br>Storage: NVRAM<br>Overwritten with: 0x00 |
| SSH Private Key | Automatically zeroized upon generation of a new key<br>Storage: NVRAM<br>Overwritten with: 0x00 |
| SSH Session Key | Automatically zeroized when the SSH session is terminated.<br>Storage: DRAM<br>Overwritten with: 0x00 |
| All CSPs | Zeroized on-demand on all file systems via the “erase” command.<br>Storage: NVRAM |

## 7.3 CAVP Certificate Equivalence

The TOE models and processors included in the evaluation are shown in the following table.

**Table 25: Model Processors**

| **Physical ASA Devices** | |
|---|---|
| Intel Atom C2508 | ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X,, ASA 5516-X |
| Pentium / Core i3 | ASA 5512-X, 5515-X |
| Xeon 3400 | ASA 5525-X, 5545-X, 5555-X |
| Xeon 5000 | ASA 5585-X SSP 10, 5585-X SSP-20, 5585-X SSP 40, 5585-X SSP-60 |
| **ASA Virtual (ASAv)** | |
| Xeon E5 w/ ESXi | UCS B200-M3, B200-M4, B420 M4, B420 M3, B22 M3, C22 M3, C24 M3, C220 M3, C220 M4, C240 M3, C240 M4, C420 M3, E140D M1, E160D M2 & M1, E180D M2, E140DP M1, E160DP M1 |
| Xeon E-Series w/ ESXi | B260 M4, B460 M4, B230 M2, B440 M2, C260 M2, C460 M2, C460 M4 |
| Xeon E-Series w/ ESXi | UCS E140S M1 and M2 |

ASA 55xx (physical devices in table)

- Intel Atom C25xx;
- Intel Pentium/Core i3
- Intel Xeon 34xx
- Intel Xeon 5xxx
- Intel Xeon E5-2600

ASAv

- Intel Xeon E5 w/ ESXi
- Intel Xeon E-Series w/ ESXi

**Table 26: Algorithm Numbers**

| Algorithm | SFR | ASA 55xx | ASAv Intel Xeon E5 | ASAv Intel Xeon E-Series |
|---|---|---|---|---|
| AES<br>CBC 128/256<br>GCM 128/256 | FCS_COP.1(1) | 4249 | 4344 | 4344 |
| RSA<br>At least 2048 bit<br>Signature Gen & Verify<br>Key Gen | FCS_COP.1(2)<br>FCS_CKM.1 | 2298 | 2346 | 2346 |
| ECDSA curves P-256, P-384 and P-521<br>Signature Gen & Verify<br>Key Gen | FCS_COP.1(2)<br>FCS_CKM.1 | 989 | 1027 | 1027 |
| Hashing<br>SHA-1, SHA-256, SHA-384, SHA-512 | FCS_COP.1(3) | 3486 | 3579 | 3579 |
| Keyed Hash<br>HMAC-SHA-1, HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 | FCS_COP.1(4) | 2787 | 2882 | 2882 |
| DRBG<br>Hash_DRBG(any) | FCS_RBG_EXT.1 | 1328 | 1386 | 1386 |
| CVL KAS<br>ECC | FCS_CKM.2 | 1002/1134 | 1048/1135 | 1048/1135 |

# 8 ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

**Table 27: 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 |