



Cisco NGIPSv 7.0 with FMC/FMCv 7.0

Security Target

ST Version 1.0

May 16, 2023

Table of Contents

1	SECURITY TARGET INTRODUCTION	9
1.1	ST and TOE Reference	9
1.2	TOE Overview	10
1.2.1	TOE Product Type	10
1.2.2	Supported non-TOE Hardware/ Software/ Firmware	10
1.3	TOE DESCRIPTION	11
1.4	TOE Evaluated Configuration	17
1.5	Physical Scope of the TOE	18
1.6	Logical Scope of the TOE	19
1.6.1	Security Audit	19
1.6.2	Communication	19
1.6.3	Cryptographic Support	19
1.6.4	Identification and authentication	20
1.6.5	Security Management	20
1.6.6	Protection of the TSF	20
1.6.7	TOE Access	20
1.6.8	Trusted path/Channels	21
1.6.9	Intrusion Prevention System	21
1.7	Excluded Functionality	21
2	Conformance Claims	23
2.1	Common Criteria Conformance Claim	23
2.2	Protection Profile Conformance	23
2.3	Protection Profile Conformance Claim Rationale	24
2.3.1	TOE Appropriateness	24
2.3.2	TOE Security Problem Definition Consistency	25
2.3.3	Statement of Security Requirements Consistency	25
3	SECURITY PROBLEM DEFINITION	26
3.1	Assumptions	26
3.2	Threats	28

3.3	Organizational Security Policies	30
4	SECURITY OBJECTIVES	32
4.1	Security Objectives for the TOE.....	32
4.2	Security Objectives for the Environment.....	33
5	SECURITY REQUIREMENTS	35
5.1	Conventions.....	35
5.2	TOE Security Functional Requirements	35
5.3	SFRs Drawn from NDcPP	38
5.3.1	Security audit (FAU)	38
5.3.2	Communication (FCO).....	42
5.3.3	Cryptographic Support (FCS)	42
5.3.4	Identification and authentication (FIA).....	48
5.3.5	Security management (FMT).....	50
5.3.6	Protection of the TSF (FPT).....	52
5.3.7	TOE Access (FTA).....	53
5.3.8	Trusted Path/Channels (FTP).....	53
5.4	SFRs Drawn from mod_ips_v1.0	54
5.4.1	Security Audit (FAU).....	54
5.4.2	Security management (FMT).....	57
5.4.3	Intrusion Prevention (IPS)	57
5.5	TOE SFR Dependencies Rationale for SFRs Found in NDcPP	60
5.6	Security Assurance Requirements	61
5.6.1	SAR Requirements	61
5.6.2	Security Assurance Requirements Rationale	61
5.7	Assurance Measures	61
6	TOE Summary Specification.....	63
6.1	TOE Security Functional Requirement Measures.....	63
7	Supplemental TOE Summary Specification Information	91
7.1	Intrusion Rule Definition	91
7.1.1	Intrusion Rule Header	91
7.1.2	Intrusion Rule Options and Keywords	92

7.2	TOE Key Zeroization	93
7.3	CAVP Certificate Equivalence	94
8	Annex A: References	99
9	Annex B: NDcPP SFR TOE Components Mapping	101

List of Tables

TABLE 1: ACRONYMS	7
TABLE 2: ST AND TOE IDENTIFICATION	9
TABLE 3: IT ENVIRONMENT COMPONENTS	10
TABLE 4: FMC MODELS	13
TABLE 5: UCS HARDWARE	14
TABLE 6: UCS-E AND ISR COMPATIBILITY	16
TABLE 7: HARDWARE MODELS AND SPECIFICATIONS	18
TABLE 8: EXCLUDED FUNCTIONALITY	21
TABLE 9: PROTECTION PROFILES	23
TABLE 10: NIAP TECHNICAL DECISIONS	23
TABLE 11: TOE ASSUMPTIONS	26
TABLE 12: THREATS	28
TABLE 13: ORGANIZATIONAL SECURITY POLICIES	30
TABLE 14: SECURITY OBJECTIVES FOR THE TOE	32
TABLE 15: SECURITY OBJECTIVES FOR THE ENVIRONMENT	33
TABLE 16: SECURITY FUNCTIONAL REQUIREMENTS	35
TABLE 17: AUDITABLE EVENTS	39
TABLE 18: AUDITABLE EVENTS	54
TABLE 19: ASSURANCE MEASURES	61
TABLE 20: ASSURANCE MEASURES	61
TABLE 21: HOW TOE SFRS ARE SATISFIED	63
TABLE 22: TOE KEY ZEROIZATION	93
TABLE 23: PROCESSORS AND IMPLEMENTATIONS	94
TABLE 24: ALGORITHM CERTIFICATE NUMBERS	97
TABLE 25: REFERENCES	99
TABLE 26: SFR MAPPING	101

List of Figures

FIGURE 1: UCS HARDWARE	14
FIGURE 2: EXAMPLE TOE DEPLOYMENT	18
FIGURE 3: AUDIT VIEW.....	63
FIGURE 4: SYSLOG VIEW.....	64
FIGURE 5: AUTHENTICATION PROCESS.....	73

List of Acronyms

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

Table 1: Acronyms

Acronyms / Abbreviations	Definition
AMP	Advanced Malware Protection
CC	Common Criteria [for IT Security Evaluation]
CLI	Command Line Interface
CM	Configuration Management
DB	Database
FIPS	Federal Information Processing Standards
FMC	Firepower Management Center
FMCv	Virtual Firepower Management Center
FOM	FIPS Object Module
HTTP	Hypertext Transmission Protocol
HTTPS	Hypertext Transmission Protocol, Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
NDcPP	Network Device collaborative Protection Profile
NGIPSv	Virtual Next Generation Intrusion Prevention System
NIST	National Institute of Standards and Technology
PP	Protection Profile
REST	Representational State Transfer
SAR	Security Assurance Requirement
SEU	Security Enhancement Updates
SF	Security Function
SFR	Security Functional Requirement
ST	Security Target (this document)
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Security Layer
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification (section 6 of this document)
UDP	User Datagram Protocol

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 NGIPSv. 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 NGIPSv 7.0 with FMC/FMCv 7.0 Security Target
ST Version	1.0
Publication Date	May 16, 2023
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco NGIPSv 7.0 with FMC/FMCv 7.0
TOE Hardware Models	<ul style="list-style-type: none"> • Cisco Firepower Management Center (FMC) (FMC1000, FMC2500, FMC4500, FMC1600, FMC2600 and FMC4600) • FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3. <i>Note: E160S M3 and E180D M3 installed on ISR¹.</i> • NGIPSv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3. <i>Note: E160S M3 and E180D M3 installed on ISR².</i>

¹ ISR is in the operational environment. Please see the table in section 1.3 for UCS-E and ISR compatibility.

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

TOE Software Version	NGIPSv 7.0 and FMC/FMCv 7.0
Keywords	IPS/IDS

1.2 TOE Overview

The TOE is an Intrusion Detection and Prevention System, which consists of the FMC and Sensors (Distributed TOE Use Case 3). The FMC provides a centralized management console and event database for the system, and aggregates and correlates intrusion, discovery, and connection data from managed Sensors. Sensors monitor all network traffic for security events and violations and can alert and/or block malicious traffic as defined in the intrusion and access control rules. The TOE in the evaluated configuration deploys at least one FMC managing one or more Sensors. Each model of the TOE consists of a set of appliances or virtual appliances which vary primarily based on the processing power, memory performance, disk space, and port density. The virtual appliances run on hypervisor ESXi and underlying UCS hardware models which also vary based on the processing power, memory performance, disk space, and port density.

1.2.1 TOE Product Type

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

1.2.2 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Table 3: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with SSH client installed that is used by the TOE administrator to support TOE administration through SSHv2 protected channels. Any SSH client that supports SSHv2 may be used.
Management Workstation with Web Browser	Yes	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through TLS/HTTPS protected channels. Any browser identified by the administrative guidance that supports TLSv1.2 may be used.
Audit (syslog) Server	Yes	TOE can be configured to deliver audit records to an external log server over TLS.

Component	Required	Usage/Purpose Description for TOE performance
Certification Authority	Yes	The TOE can be configured to utilize digital certificates, e.g., for HTTPS connections.

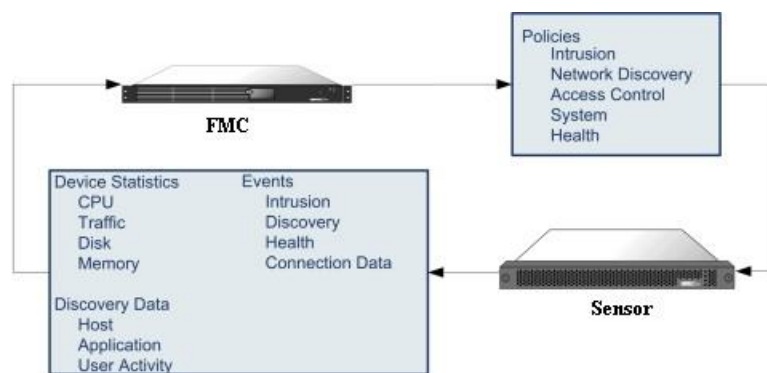
1.3 TOE DESCRIPTION

The TOE, sometimes referred to as Cisco NGIPSv, provides advanced threat protection as an intrusion prevention system that can be deployed inline (as an IPS to block suspicious or malicious traffic in real-time) or passive (as an IPS/IDS sensor) by integrating real-time inspection and logging of IPv4 and IPv6 traffic.

The Firepower Management Center (FMC) is a network appliance that provides a centralized management console and database repository for the Firepower System deployment. Administrators can also deploy 64-bit virtual Firepower Management Centers (FMCv) as ESXi hosts using the VMware vSphere Hypervisor. The FMC is a key component in the Cisco NGIPSv system. Administrators can use the FMC to manage the Cisco NGIPSv system, and to aggregate, analyze, and respond to the threats they detect on their network. By using the FMC to manage Sensors, administrators can:

- Configure policies for all Sensors from a single location, making it easier to change configurations.
- Install various types of software updates on Sensors.
- Push policies to managed Sensors and monitor their health status from the FMC.

The FMC aggregates and correlates intrusion events, anomaly, network discovery information, and Sensor performance data, allowing administrators to monitor the information the Sensors are reporting in relation to one another, and to assess the overall activity occurring on their network. The following illustration lists what is transmitted between an FMC and its managed Sensors.



The administrators can also deploy NGIPSv (a 64-bit virtual device as an ESXi host) using the VMware vSphere Hypervisor. The administrators can configure the Sensors in either a passive or inline deployment. In a passive deployment, the Sensor monitors traffic flowing across a network using a

switch SPAN or mirror port. However, when configured in a passive deployment, the TOE cannot take certain actions such as blocking or shaping traffic. In an inline IPS deployment, the Sensor operates as a bump in the wire and is transparent (i.e., no IP address) on a network segment. The Sensor can be configured to drop or alter packets, if necessary, in addition to generating alerts.

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

Table 4: FMC Models

Model	FMC1000-K9	FMC1600-K9	FMC2500-K9	FMC2600-K9	FMC4500-K9	FMC4600-K9
Processor	Intel Xeon E5-2640 v4 (Broadwell)	Intel Xeon Silver 4110 (Skylake)	Intel Xeon E5-2640 v4 (Broadwell)	Intel Xeon Silver 4110 (Skylake)	Intel Xeon E5-2620 v4 (Broadwell)	Intel Xeon Silver 4116 (Skylake)
Memory	32 GB	32 GB	64 GB	64 GB	128 GB	128 GB
Maximum Number of Sensors Managed	50	50	300	300	750	750
Maximum Number of IPS Events	60 Million	60 Million	60 Million	60 Million	300 Million	300 Million
Event Storage	900 GB	900 GB	1.8 TB	1.8 TB	3.2 TB	3.2 TB
Maximum Flow Rate	6,000 fps	6,000 fps	10,000 fps	10,000 fps	20,000 fps	20,000 fps
Maximum Network Map (hosts/users)	50,000/50,000	50,000/50,000	300,000/300,000	300,000/300,000	600,000/600,000	600,000/600,000
Network Interfaces	2 x 1Gbps	2 x 1Gbps	2 x 1Gbps	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps	2 x 1Gbps 2 x 10Gbps

The UCS hardware components, which provide the platform for the FMCv and NGIPsv, in 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 FMCv in terms of hardware.

Figure 1: UCS Hardware



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

Table 5: UCS Hardware

Model	C220 M5	C240 M5	C480-M5
Number of Processors	2	2	2-4
Processor	Intel® Xeon® Bronze 3104 (Skylake), Intel® Xeon® Silver 4110 (Skylake) Intel® Xeon® Gold 6128 (Skylake) Intel® Xeon® Platinum 8153 (Skylake)	Intel® Xeon® Bronze 3104 (Skylake), Intel® Xeon® Silver 4110 (Skylake) Intel® Xeon® Gold 6128 (Skylake) Intel® Xeon® Platinum 8153 (Skylake)	Intel® Xeon® Bronze 3104 (Skylake), Intel® Xeon® Silver 4110 (Skylake) Intel® Xeon® Gold 6128 (Skylake) Intel® Xeon® Platinum 8153 (Skylake)
Form factor	1RU rack server	2 RU	4 RU

Maximum Memory	3 TB, 24 x DDR4 DIMMs	3 TB, 24 x DDR4 DIMMs	12 TB, 256 x DDR4 DIMMs
Embedded Network Interface Cards (NICs)	Dual 10GBASE-T Intel x550 Ethernet ports	Dual 10GBASE-T Intel x550 Ethernet ports	Dual 10GBASE-T Intel x550 Ethernet ports

Model	E160S M3	E180D M3
Number of Processors	1	2
Processor	Intel® Xeon® D-1528 (Broadwell)	Intel® Xeon® D-1548 (Broadwell)
Physical dimensions (H x W x D)	1.58 x 7.44 x 7.5 in.	1.58 x 16.23 x 7.5 in.
Memory	8 – 64 GB	16 – 128 GB
Disk Space	4 TB	4 TB
I/O	<ul style="list-style-type: none"> ● 2 internal Gigabit Ethernet ports (Broadcom 5719) ● 2 external 10 Gigabit Ethernet ports (1000/10000) (Integrated within Intel CPU) 	<ul style="list-style-type: none"> ● 2 internal Gigabit Ethernet ports (Broadcom 5719) ● 2 external 10 Gigabit Ethernet ports (1000/10000) (Integrated within Intel CPU) ● 1 dedicated management Ethernet port (10/100/1000) for Cisco IMC

The Cisco UCS E-series M3 Server is available in two flavors: as singlewide (E160 M3) and as doublewide module (E180D-M3). The singlewide version occupies a single service-module slot in the Cisco 4000 Series ISR. The doublewide module occupies two service-module slots side-by-side. The table below details which of the Cisco 4000 Series ISRs are compatible with the UCS E-Series M3 servers and how many of these small form-factor blade servers can reside inside each of the ISR platforms.

Table 6: UCS-E and ISR Compatibility

ISR Platform	E160S M3	E180D M3
19xx, 29xx, 39xx	NO	NO
4221	NO	NO
4321	NO	NO
4331	1	NO
4351	2	1
4431	NO	NO
4451	2	1

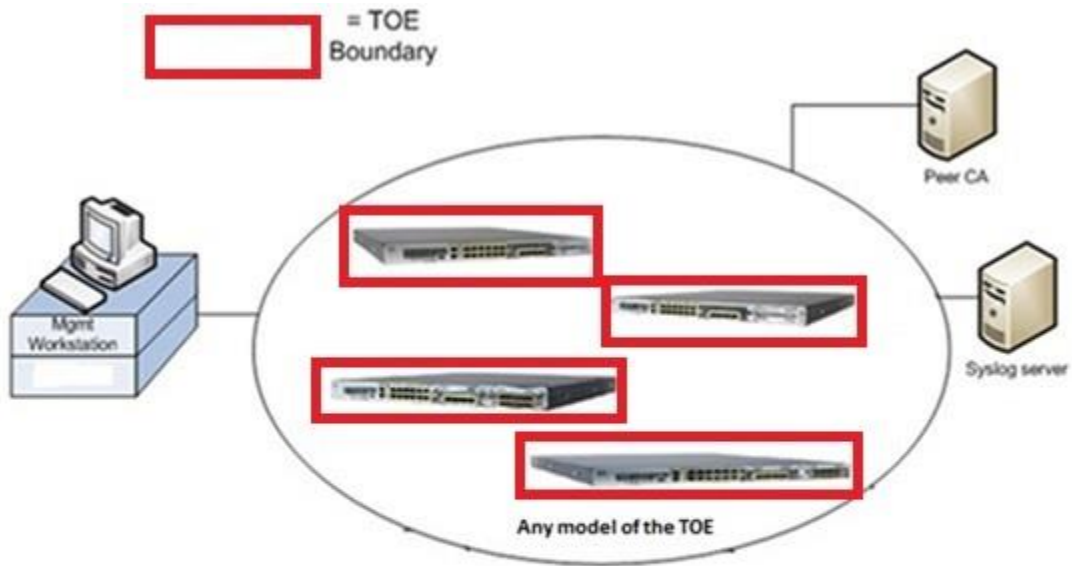
1.4 TOE Evaluated Configuration

In the evaluated configuration, the TOE consists of at least one FMC managing one or more Sensor all running version 7.0. The FMC can be a physical appliance or virtual appliance but the sensor is a virtual appliance.

The evaluated features of the TOE are listed in this paragraph and described further in section 1.6. If the TOE is to be remotely administered, the management station must connect using SSHv2 or using web browser for the UI over HTTPS. A syslog server can also be used to store audit records, and the syslog server must support syslog over TLS. The Access control policies inspect traffic for security violations and, in inline deployments, can block or alter malicious traffic using intrusion rules and other preprocessor settings provided by the TOE.

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

Figure 2: Example TOE Deployment



The previous figure includes the following:


- TOE components (at least one sensor and FMC)
- Management Workstation (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
FMC1000-K9 FMC2500-K9 FMC4500-K9 FMC1600-K9 FMC2600-K9	The Cisco FMC provides centralized management console with up to 4 management interfaces, and up to 10 Gbps speed.	Release 7.0

<p>FMC4600-K9</p> 		
<p>FMCv NGIPSv</p>	<p>UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3 including VM ESXi 6.7 or 7.0</p>	<p>Release 7.0</p>

1.6 Logical Scope of the TOE

The TOE is comprised of several security features including IPS and URL/IP filtering. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Communication
3. Cryptographic Support
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels
9. Intrusion Prevention System

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

1.6.1 Security Audit

The TOE is designed to be able to generate logs for a wide range of security relevant events such as login attempts and management functions. The complete list of auditable events and contents is in Section 5.3.1.1. The TOE can be configured to store the logs locally so they can be accessed by an administrator or alternately to send the logs to an external syslog server over a secure communication channel. The timestamp included in the audit content can be manually set on FMC/FMCv and automatically synchronized with other TOE components.

1.6.2 Communication

The TOE allows authorized administrators to control which Sensor is managed by the FMC. This is performed through a registration process over TLS. The administrator can also de-register a Sensor if he or she wish to no longer manage it through the FMC.

1.6.3 Cryptographic Support

The TOE provides FIPS-certified algorithms (Section 7.3) to provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including TLS, HTTPS, and SSH. The complete specification of algorithms, key sizes, and other attributes is in Section 5.3.3.

1.6.4 Identification and authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console as well as network accessible interfaces (SSHv2 and HTTPS) for remote interactive administrator sessions.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. All authorized TOE users must have a user account with security attributes that control the user's access to TSF data and management functions. These security attributes include username, password, and roles for TOE users. In addition, the TOE supports X.509v3 certificate authentication for the external syslog server.

1.6.5 Security Management

The TOE provides a web-based (using HTTPS) management interface for all TOE administration, including the IDS and access control rule sets, user accounts and roles, and audit functions. The ability to manage various security attributes, system parameters and all TSF data is controlled and limited to those users who have been assigned the appropriate administrative role.

The TOE also provides a command line interface (CLI) and shell access to the underlying operating system of the TOE components. The shell access must be restricted to off-line installation, pre-operational configuration, and maintenance and troubleshooting of the TOE. The CLI provides only a subset of the management functions provided by the web GUI and is only available on the Sensors. The use of the web GUI is highly recommended over the CLI.

Security management relies on a management workstation in the operational environment with a properly supported web browser or SSH client to access the management interfaces.

1.6.6 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features. It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability) or can utilize a trusted time server in the operational environment.

The TOE ensures that data transmitted between separate parts of the TOE are protected from disclosure or modification. This protection is ensured by transmission of data between the TOE components over a secure, TLS-protected tunnel.

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

1.6.7 TOE Access

The TOE can be configured to display an informative advisory banner when an administrator establishes an interactive session and subsequently enforce an administrator-defined inactivity timeout value after

which the inactive session will be terminated. The administrators can also terminate their own interactive sessions when needed.

1.6.8 Trusted path/Channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access or HTTPS for web GUI access. The TOE protects communication with network peers, such as a syslog server, using TLS connections.

1.6.9 Intrusion Prevention System

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

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

Using Security Intelligence, the administrators can customize a known-bad list (“Block List”) to deny traffic to and from specific IP addresses, URLs, and DNS domain names, before the traffic is subjected to analysis by the access control rules. Optionally, the administrators can use a “monitor-only” setting for Security Intelligence filtering.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 8: Excluded Functionality

Excluded Functionality	Exclusion Rationale
VPN Gateway with IPsec	This feature is not evaluated as part of the evaluation. The VPN Gateway Extended Package is not claimed in this evaluation.
External Authentication Servers	The NDcPP does not require external authentication servers. However, if they are used, the connection between the TOE and server must be protected by the approved security protocol.
Shell Access	The underlying shell access is only allowed for pre-operational installation, configuration, and post-operational maintenance and troubling shooting.
Timeout Exemption Option	The use of the “Exempt from Browser Session Timeout” setting is not permitted. This allows a user to be exempted from the inactivity timeout feature.

Cisco NGIPSv Security Target

REST API	This feature is not evaluated as part of the evaluation. REST API relies on HTTPS as the underlying communication protocol and can be used to build a management interface. This feature is not tested and is out of scope.
Modbus and DNP3 SCADA preprocessors	These features are not evaluated as part of the evaluation. These features are related to detection of traffic anomalies, but they are beyond the scope of testing defined in MOD_IPS_V1.0.
HTTP and Telnet for management purposes	HTTP and Telnet pass credentials in clear text and are disabled in the evaluated system.
SNMPv3 for management purposes	SNMPv3 is supported but is not permitted for management—only for sending SNMP traps for alerting.
Linux hardening	The evaluation does not directly evaluate the effectiveness of the hardening performed by Cisco on the Linux kernel included in the TOE.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017. 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
PP-Configuration for Network Device and Intrusion Prevention Systems (IPS) (CFG_NDcPP-IPS_V1.0)	1.0	18 May 2021
The PP-Configuration includes the following components:		
<ul style="list-style-type: none"> Base-PP: Collaborative Protection Profile for Network Devices, (CPP_ND_V2.2E) 	2.2e	23 March 2020
<ul style="list-style-type: none"> PP-Module: PP-Module for Intrusion Protection Systems (IPS), (MOD_IPS_V1.0) 	1.0	11 May 2021

The TOE and ST are conformant with the Protection Profiles as listed in Table 9 above. NIAP Technical Decisions (TD) have been applied as indicated in Table 10 below:

Table 10: NIAP Technical Decisions

TD #	TD Name	Protection Profiles	Applied to this TOE
TD0636	NIT Technical Decision for Clarification of Public Key User Authentication for SSH	CPP_ND_V2.2E	Not applied because this ST does not include FCS_SSHC_EXT.1
TD0635	NIT Technical Decision for TLS Server and Key Agreement Parameters	CPP_ND_V2.2E	FCS_TLSS_EXT.1.3
TD0634	NIT Technical Decision for Clarification required for testing IPv6	CPP_ND_V2.2E	FCS_TLSC_EXT.1.2
TD0633	NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	CPP_ND_V2.2E	FCS_IPSEC_EXT.1.7, FCS_IPSEC_EXT.1.8
TD0632	NIT Technical Decision for Consistency with Time Data for vNDs	CPP_ND_V2.2E	FPT_STM_EXT.1.2
TD0631	NIT Technical Decision for Clarification of public key authentication for SSH Server	CPP_ND_V2.2E	FCS_SSHS_EXT.1, FMT_SMF.1
TD0595	Administrative corrections to IPS PP-Module	MOD_IPS_V1.0	FAU_GEN.1.1/IPS
TD0592	NIT Technical Decision for Local Storage of audit records	CPP_ND_V2.2E	FAU_STG

TD0591	NIT Technical Decision for Virtual TOEs and hypervisors	CPP_ND_V2.2E	A.LIMITED_FUNCTIONALITY, ACRONYMS
TD0581	NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	CPP_ND_V2.2E	FCS_CKM.2
TD0580	NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	CPP_ND_V2.2E	FCS_CKM.1.1, FCS_CKM.2.1
TD0572	NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	CPP_ND_V2.2E	FTP_ITC.1
TD0571	NiT Technical Decision for Guidance on how to handle FIA_AFL.1	CPP_ND_V2.2E	FIA_AFL.1, FIA_UAU.1, FIA_PMG_EXT.1
TD0570	NiT Technical Decision for Clarification about FIA_AFL.1	CPP_ND_V2.2E	FIA_AFL.1
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLS_EXT.1.7	CPP_ND_V2.2E	FCS_TLSS_EXT.1.4
TD0564	NiT Technical Decision for Vulnerability Analysis Search Criteria	CPP_ND_V2.2E	AVA_VAN.1
TD0563	NiT Technical Decision for Clarification of audit date information	CPP_ND_V2.2E	FAU_GEN.1.2
TD0556	NIT Technical Decision for RFC 5077 question	CPP_ND_V2.2E	FCS_TLSS_EXT.1.4
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	CPP_ND_V2.2E	FCS_TLSS_EXT.1.4
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	CPP_ND_V2.2E	AVA_VAN.1
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	CPP_ND_V2.2E	Not applied because this ST does not include FCS_DTLS_EXT
TD0538	NIT Technical Decision for Outdated link to allowed-with list	CPP_ND_V2.2E	Section 2 of PP
TD0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	CPP_ND_V2.2E	FCS_TLSC_EXT.2
TD0536	NIT Technical Decision for Update Verification Inconsistency	CPP_ND_V2.2E	AGD_OPE.1
TD0528	NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	CPP_ND_V2.2E	Not applied because this ST does not include FCS_NTP_EXT.1
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	CPP_ND_V2.2E	FIA_X509_EXT.1/REV, FIA_X509_EXT.1/ITT

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:

- collaborative Protection Profile for Network Devices (cpp_nd_v2.2e); and
- PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0)

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 NDcPPv2.2e and mod_ips_v1.0 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 cpp_nd_v2.2e, mod_ips_v1.0 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 7 of the NDcPP.

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 MOD_IPS_V1.0 will have extension [IPS] to distinguish them from the NDcPP.

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 11: TOE Assumptions

Assumption	Assumption Definition
Reproduced from cpp_nd_v2.2e	
A.PHYSICAL_PROTECTION	The Network Device 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 device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device 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 device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the

Assumption	Assumption Definition
	device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	<p>The Security Administrator(s) for the Network Device 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 device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.</p> <p>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).</p>
A.REGULAR_UPDATES	The Network Device 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 Network Device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ADMINISTRATOR	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.

Assumption	Assumption Definition
A.VS_REGULAR_UPDATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATON	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.
Reproduced from mod_ips_v1.0	
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

3.2 Threats

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

Table 12: Threats

Threat	Threat Definition
Reproduced from cpp_nd_v2.2e	
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device 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 Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

Threat	Threat Definition
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 Network Devices that do not use standardized secure tunnelling 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 Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a 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 Network Device 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 Network Device 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 device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.

Threat	Threat Definition
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device 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	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
Reproduced from mod_ips_v1.0	
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress-or egress-based actions.
T.NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network. If malicious external devices are able to communicate with devices on the protected network via a backdoor then those devices may be susceptible to the unauthorized disclosure of information.
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to Operational Environment policies. Devices located outside the protected network may attempt to conduct inappropriate activities while communicating with allowed public services. E.g. manipulation of resident tools, SQL injection, phishing, forced resets, malicious zip files, disguised executables, privilege escalation tools and botnets.
T.NETWORK_DOS	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network. Resource exhaustion may occur in the event of co-ordinate service request flooding from a small number of sources.

3.3 Organizational Security Policies

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

Table 13: Organizational Security Policies

Policy Name	Policy Definition
Reproduced from cpp_nd_v2.2e	
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.
Reproduced from mod_ips_v1.0	
P.ANALYZE	Analytical processes and information to derive conclusions about potential intrusions must be applied to IPS data and appropriate response actions taken.

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 14: Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
Reproduced from mod_ips_v1.0	
O.SYSTEM_MONITORING	The IPS must collect and store information about all events that may indicate an IPS policy violation related to misuse, inappropriate access, or malicious activity on monitored networks.
O.IPS_ANALYZE	The IPS must apply analytical processes to network traffic data collected from monitored networks and derive conclusions about potential intrusions or network traffic policy violations.
O.IPS_REACT	The IPS must respond appropriately to its analytical conclusions about IPS policy violations.
O.TOE_ADMINISTRATION	The IPS will provide a method for authorized administrator to configure the TSF.

4.2 Security Objectives for the Environment

All of the assumptions stated in section 3.1 are covered by 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 15: Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
Reproduced from cpp_nd_v2.2e	
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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
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.
OE.COMPONENTS_RUNNING	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures

Environment Security Objective	IT Environment Security Objective Definition
	that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.VM_CONFIGURATION	<p>For vNDs, the Security Administrator ensures that the VS and VMs are configured to</p> <ul style="list-style-type: none"> • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). <p>The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualization features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.</p>
Reproduced from mod_ips_v1.0	
OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic of monitored networks.

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 5, dated: April 2017* and all international interpretations.

5.1 Conventions

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

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the `cpp_nd_v2.2e` and `mod_ips_v1.0` itself, the formatting used there 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 the module themselves. In addition, SFRs copied verbatim from SFRs `mod_ips_v1.0` will have extension [IPS] to distinguish them from the NDcPP. These SFRs that have an extension [IPS] do not exist in NDcPPv2.2e. Changes have been made to the base cPP SFRs as necessary to support the Intrusion Prevention functionality based on `mod_ips_v1.0`.

Except where noted, all aspects of SFRs are applicable to entire TOE (FMC and NGIPSv). Where specific functionality is only implemented in either FMC or NGIPSv, the applicable subcomponent is identified in an application note, or in embedded qualifiers within the text of the SFR. Application notes clarify distinctions where the TOE includes multiple implementations of a functionality, and those implementations differ in their minimum support of the functionality. Thus, the SFR is stating the combined functionality of the TOE.

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 16: Security Functional Requirements

Class Name	Component Identification	Component Name
Reproduced from <code>cpp_nd_v2.2e</code>		
FAU: Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User identity association
	FAU_GEN_EXT.1	Security Audit Generation

Class Name	Component Identification	Component Name
	FAU_STG_EXT.1	Protected Audit Event Storage
	FAU_STG_EXT.4	Protected Local Audit Event Storage for Distributed TOEs
	FAU_STG_EXT.5	Protected Remote Audit Event Storage for Distributed TOEs
FCO: Communication	FCO_CPC_EXT.1	Component Registration Channel Definition
FCS: Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_HTTPS_EXT.1	HTTPS Protocol
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_TLSC_EXT.1	TLS Client Protocol without Mutual Authentication
	FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication
	FCS_TLSS_EXT.1	TLS Server Protocol
FIA: Identification and Authentication	FIA_AFL.1	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism

Class Name	Component Identification	Component Name
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1/ITT	X.509 Certificate Validation
	FIA_X509_EXT.1/Rev	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/ManualUpdate	Management of Security Functions Behaviour
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	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 pre-shared, symmetric and private keys)
	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Trusted Update
	FPT_ITT.1	Basic internal TSF data transfer protection
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated 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/Admin	Trusted Path
Reproduced from mod_ips_v1.0		

Class Name	Component Identification	Component Name
FAU: Security Audit	FAU_GEN.1/IPS[IPS]	Audit Data Generation (IPS)
	FAU_SAR.1[IPS]	Audit Review
	FAU_SAR.2[IPS]	Restricted Audit Review
	FAU_SAR.3[IPS]	Selectable Audit Review
	FAU_STG.1/IPS[IPS]	Protected Audit Trail Storage
FMT: Security Management	FMT_SMF.1/IPS[IPS]	Specification of Management Functions (IPS)
IPS: Intrusion Prevention	IPS_ABD_EXT.1[IPS]	Anomaly-Based IPS Functionality
	IPS_IPB_EXT.1[IPS]	IP Blocking
	IPS_NTA_EXT.1[IPS]	Network Traffic Analysis
	IPS_SBD_EXT.1[IPS]	Signature-Based IPS Functionality

5.3 SFRs Drawn from NDcPP

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 not specified 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).*
 - *Changes to TSF data related to 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).*
 - *[[no other actions]];*
- d) *Specifically defined auditable events listed in Table 17.*

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 17.*

Table 17: Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
Reproduced from the NDcPP		
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_GEN_EXT.1	None.	None.
FAU_STG_EXT.1	None.	None.
FAU_STG_EXT.4	None.	None.
FAU_STG_EXT.5	None.	None.
FCO_CPC_EXT.1	<ul style="list-style-type: none"> Enabling communications between a pair of components. Disabling communications between a pair of components. 	Identities of the endpoints pairs enabled or disabled.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	Reason for failure
FCS_RBG_EXT.1	None.	None.
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_TLSC_EXT.1	Failure to establish an TLS Session	Reason for failure
FCS_TLSS_EXT.1	Failure to establish an TLS Session	Reason for failure
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	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/ITT	<p>Unsuccessful attempt to validate a certificate.</p> <p>Any addition, replacement or removal of trust anchors in the TOE's trust store</p>	<p>Reason for failure of certificate validation</p> <p>Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store</p>
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate.	Reason for failure of certificate validation

SFR	Auditable Event	Additional Audit Record Contents
	Any addition, replacement or removal of trust anchors in the TOE's trust store	Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data..	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_ITT.1	<ul style="list-style-type: none"> Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. 	Identification of the initiator and target of failed trusted channels establishment attempt
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_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None.

Application Note

Refer to Table 26 in section 9 (Annex B: NDcPP SFR TOE Components Mapping) for a mapping of which auditable events are generated by which TOE component.

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_GEN_EXT.1 Security Audit Generation

FAU_GEN_EXT.1.1 The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component.

5.3.1.4 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. In addition [

- The TOE shall be a distributed TOE that stores audit data on the following TOE components: [FMC and NGIPSv],
- The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [NGIPSv transmits its audit data to FMC].]

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.

5.3.1.5 FAU_STG_EXT.4 Protected Local Audit Event Storage for Distributed TOEs

FAU_STG_EXT.4.1 The TSF of each TOE component which stores security audit data locally shall perform the following actions when the local storage space for audit data is full:

[

overwrite previous audit records according to the following rule: [oldest records are overwritten]

]

5.3.1.6 FAU_STG_EXT.5 Protected Remote Audit Event Storage for Distributed TOEs

FAU_STG_EXT.5.1 Each TOE component which does not store security audit data locally shall be able to buffer security audit data locally until it has been transferred to another TOE component that stores or forwards it. All transfer of audit records between TOE components shall use a protected channel according to [FPT_ITT.1]

5.3.2 Communication (FCO)

5.3.2.1 FCO_CPC_EXT.1 Communication Partner Control

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses [

- A channel that meets the secure channel requirements in [FPT_ITT.1]].

for at least TSF data.

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

5.3.3 Cryptographic Support (FCS)

5.3.3.1 FCS_CKM.1 Cryptographic Key Generation

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

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4
- FFC schemes 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]].

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

5.3.3.2 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 meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,
- 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"

- FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [groups listed in RFC 3526] (TD0580 applied)] that meets the following: [assignment: list of standards].

5.3.3.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

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

]

]

that meets the following: *No Standard.*

5.3.3.4 FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption 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, 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].

5.3.3.5 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen 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 meet the following: [

- For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS2v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

- For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4

].

5.3.3.6 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash 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*] and **message digest sizes [160, 256, 384, 512] bits** that meet the following: [ISO/IEC 10118-3:2004].

5.3.3.7 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash 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, 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”.

5.3.3.8 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 If a peer certificate is presented, the TSF shall [*not require client authentication*] if the peer certificate is deemed invalid.

5.3.3.9 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 [*CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [*one platform-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.

5.3.3.10 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, [5647, 6668, 8332].

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

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [262,149] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, aes256-gcm@openssh.com].

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [rsa-sha2-256, rsa-sha2-512] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha2-256, hmac-sha2-512, implicit] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

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

FCS_SSHS_EXT.1.8 The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached a rekey needs to be performed.

5.3.3.11 FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

FCS_TLSC_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

Relevant to FPT_ITT.1:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 (TLSv1.2 only)
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 (TLSv1.2 only)
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 (TLSv1.2 only)
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 (TLSv1.2 only)
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 (TLSv1.2 only)
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2 only)

- TLS ECDHE ECDSA WITH AES 256 GCM SHA384 as defined in RFC 5289 (TLSv1.2 only)
Relevant to FTP ITC.1 (for syslog over TLS from NGIPSv and FMC/FMCv):
 - TLS RSA WITH AES 128 CBC SHA256 as defined in RFC 5246 (TLSv1.2, TLSv1.1)
 - TLS RSA WITH AES 256 CBC SHA256 as defined in RFC 5246 (TLSv1.2, TLSv1.1)
 - TLS ECDHE RSA WITH AES 128 GCM SHA256 as defined in RFC 5289 (TLSv1.2 only)
 - TLS ECDHE RSA WITH AES 256 GCM SHA384 as defined in RFC 5289 (TLSv1.2 only)
 - TLS ECDHE RSA WITH AES 256 CBC SHA384 as defined in RFC 5289 (TLSv1.2, TLSv1.1)
-].

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [

Relevant to FTP ITC.1 (for syslog over TLS from NGIPSv and FMC/FMCv): the reference identifier per RFC 6125 section 6

Relevant to FPT ITT.1: the identifier per RFC 5280 Appendix A using [id-at-title] and no other attribute types].

FCS_TLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism.

].

FCS_TLSC_EXT.1.4 The TSF shall [present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups] in the Client Hello.

Application Note

TLSv1.2 supports all the ciphersuites listed. TLSv1.1 only supports the ciphersuites with SHA.

5.3.3.12 FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

FCS_TLSC_EXT.2.1 The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

Application Note

FCS_TLSC_EXT.2 is applicable to the TLS client in FMC/FMCv that is used for transmission of syslog over TLS, and also applicable to the TLS client in NGIPSv that is used for transmission of syslog over TLS.

5.3.3.13 FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

Relevant to FPT_ITT.1:

- *TLS RSA WITH AES 128 CBC SHA as defined in RFC 3268 (TLSv1.2 only)*
- *TLS RSA WITH AES 256 CBC SHA as defined in RFC 3268 (TLSv1.2 only)*
- *TLS RSA WITH AES 128 CBC SHA256 as defined in RFC 5246 (TLSv1.2 only)*
- *TLS RSA WITH AES 256 CBC SHA256 as defined in RFC 5246 (TLSv1.2 only)*
- *TLS RSA WITH AES 128 GCM SHA256 as defined in RFC 5288(TLSv1.2 only)*
- *TLS RSA WITH AES 256 GCM SHA384 as defined in RFC 5288(TLSv1.2 only)*
- *TLS ECDHE RSA WITH AES 128 CBC SHA as defined in RFC 4492 (TLSv1.2 only)*
- *TLS ECDHE RSA WITH AES 256 CBC SHA as defined in RFC 4492 (TLSv1.2 only)*
- *TLS ECDHE RSA WITH AES 128 GCM SHA256 as defined in RFC 5289 (TLSv1.2 only)*
- *TLS ECDHE RSA WITH AES 256 GCM SHA384 as defined in RFC 5289 (TLSv1.2 only)*
- *TLS ECDHE RSA WITH AES 128 CBC SHA256 as defined in RFC 5289 (TLSv1.2 only)*
- *TLS ECDHE RSA WITH AES 256 CBC SHA384 as defined in RFC 5289 (TLSv1.2 only)*

Relevant to FTP_TRP.1 (applicable to FMC/FMCv only):

- *TLS RSA WITH AES 128 CBC SHA as defined in RFC 3268 (TLSv1.2 only)*
- *TLS RSA WITH AES 256 CBC SHA as defined in RFC 3268 (TLSv1.2 only)*
- *TLS ECDHE RSA WITH AES 128 GCM SHA256 as defined in RFC 5289 (TLSv1.2 only)*
- *TLS ECDHE RSA WITH AES 256 GCM SHA384 as defined in RFC 5289 (TLSv1.2 only)*

].

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and **[TLS 1.1]**.

FCS_TLSS_EXT.1.3 The TSF shall perform key establishment for TLS using *[RSA with key size [2048 bits], ECDHE curves [secp256r1, secp384r1, secp521r1] and no other curves]*.

FCS_TLSS_EXT.1.4 The TSF shall support [

Relevant to FPT_ITT.1:

- *no session resumption or session tickets*

Relevant to FTP_TRP.1 (applicable to FMC/FMCv only):

- *session resumption based on session tickets according to RFC 5077*

]

5.3.4 Identification and authentication (FIA)

5.3.4.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [3 to 7] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending remote Administrator from successfully establishing remote session using any authentication method that involves a password until [unlocking] is taken by an Administrator].

5.3.4.2 FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

- a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!” , “@” , “#” , “\$” , “%” , “^” , “&” , “*” , “(” , “)” , ‘ ` (double or single quote/apostrophe) , + (plus) , - (minus) , = (equal) , , (comma) , . (period) , / (forward-slash) , \ (back-slash) , | (vertical-bar or pipe) , : (colon) , ; (semi-colon) , < > (less-than, greater-than inequality signs) , [] (square-brackets) , { } (braces or curly-brackets) , ? (question-mark) , _ (underscore) , and ~ (tilde)];
- b) Minimum password length shall be configurable to [minimum of 8] and [maximum of 127].

5.3.4.3 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.

5.3.4.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local [password-based, SSH public key-based] authentication mechanism to perform local administrative user authentication.

5.3.4.5 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**.

5.3.4.6 FIA_X509_EXT.1 X.509/ITT Certificate Validation

FIA_X509_EXT.1.1/ITT The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation supporting a minimum path length of two certificates.
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [*no revocation method*].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
 - *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/ITT 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.

5.3.4.7 FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of three certificates**.
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [*a Certificate Revocation List (CRL) as specified in RFC 5759 Section 5*].
- 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/Rev 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 [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 [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 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/ManualUpdate Management of Security Functions Behaviour

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to perform manual update to Security Administrators*.

5.3.5.2 FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1.1/CoreData The TSF shall restrict the ability to *manage the TSF data to Security Administrators*.

5.3.5.3 FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to manage the *cryptographic keys to Security Administrators*.

5.3.5.4 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using **digital signature and [no other]** capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- ***Ability to manage the cryptographic keys;***
- ***Ability to configure the cryptographic functionality;***
- ***Ability to import X.509v3 certificates to the TOE's trust store;***
- [
 - *Ability to modify the behavior of the transmission of audit data to an external IT entity;*
 - *Ability to configure the interaction between TOE components;*
 - *Ability to manage the trusted public keys database;*
 - *Ability to re-enable an Administrator account;*
 - *Ability to set the time which is used for time-stamps;*
 - *Ability to configure the reference identifier for the peer;*]

5.3.5.5 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 administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

5.3.6.3 FPT_STM_EXT.1 Reliable time stamps

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [allow the Security Administrator to set the time].

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 [during initial start-up (on power on)] to demonstrate the correct operation of the TSF: *[FIPS 140-2 standard power-up self-tests and firmware integrity test]*.

5.3.6.5 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [no other TOE firmware/software version].

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 The TSF shall provide a means to authenticate firmware/software updates to the TOE using a [digital signature] prior to installing those updates.

5.3.6.6 FPT_ITT.1: Basic Internal TOE TSF data transfer

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and detect its modification when it is transmitted between separate parts of the TOE **through the use of TLS**.

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

5.3.8 Trusted Path/Channels (FTP)

5.3.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall be **capable of using [TLS]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [[no other capabilities]]** 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**.

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 TLS;*].

5.3.8.2 FTP_TRP.1/Admin Trusted Path

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

FTP_TRP.1.2/Admin The TSF shall permit remote Administrators to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

5.4 SFRs Drawn from mod_ips_v1.0

5.4.1 Security Audit (FAU)

5.4.1.1 FAU_GEN.1/IPS[IPS] Audit Data Generation (IPS)

FAU_GEN.1.1/IPS[IPS] The TSF shall be able to generate an **IPS** audit record of the following auditable **IPS** events:

- a) Start-up and shut-down of the **IPS** functions;
- b) All **IPS** auditable events for the [not specified] level of audit; and
- c) [*All dissimilar IPS events;*
- d) [*All dissimilar IPS reactions;*
- e) [*Totals of similar events occurring within a specified time period;*
- f) [*Totals of similar reactions occurring within a specified time period;*
- g) [*The events in the IPS Events table.*
- h) [no other auditable events].

FAU_GEN.1.2/IPS[IPS] The TSF shall record within each **IPS auditable event** record at least the following information:

- a) Date and time of the event, type of event **and/or reaction**, ~~subject identity, and the outcome (success or failure) of the event;~~ and;
- b) For each **IPS auditable** event type, based on the auditable event definitions of the functional components included in the PP/ST, [*Specifically defined auditable events listed in Table 18*].

Table 18: Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FMT_SMF.1/IPS[IPS]	Modification of an IPS policy element.	Identifier or name of the modified IPS policy element (e.g. which signature or known-good/known-bad list was modified).

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

5.4.1.1 FAU_SAR.1[IPS] Audit Review

FAU_SAR.1.1[IPS] The TSF shall provide [*authorized administrators*] with the capability to read [*IPS data*] from the ~~audit records~~ **IPS events**.

FAU_SAR.1.2[IPS] The TSF shall provide the ~~audit records~~ **IPS data** in a manner suitable for the ~~user administrators~~ to interpret the information.

5.4.1.2 FAU_SAR.2[IPS] Restricted Audit Review

FAU_SAR.2.1[IPS] The TSF shall prohibit all ~~users~~ **administrators** read access to the ~~audit records~~ **IPS data**, except those that have been granted explicit read-access.

5.4.1.3 FAU_SAR.3[IPS] Selectable Audit Review

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

5.4.1.4 FAU_STG.1/IPS[IPS] Protected Audit Trail Storage (IPS Data)

FAU_STG.1.1/IPS Refinement: The TSF shall protect the stored ~~audit records~~ **IPS data** from unauthorized deletion.

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

5.4.2 Security management (FMT)

5.4.2.1 FMT_SMF.1/IPS[IPS] Specification of Management Functions (IPS)

FMT_SMF.1.1/IPS[IPS] The TSF shall be capable of performing the following management functions: [

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

5.4.3 Intrusion Prevention (IPS)

5.4.3.1 IPS_ABD_EXT.1[IPS] Anomaly-Based IPS Functionality

IPS_ABD_EXT.1.1[IPS] The TSF shall support the definition of [*anomaly (“unexpected”) traffic patterns*] including the specification of [

- *frequency;*
- *[preprocessor detection rules for anomaly detected in headers and protocols]*

and the following network protocol fields:

- *[all packet header and data elements defined in IPS_SBD_EXT.1]*

Application Note

Although the term “threshold” is used in the TSS, the TOE’s definition of “threshold” matches the definition of frequency in the *mod_ips_v1.0*. Therefore, “frequency”, rather than “threshold” has been selected in the *IPS_ABD_EXT.1.1* requirement.

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

IPS_ABD_EXT.1.3[IPS] The TSF shall allow the following operations to be associated with anomaly-based IPS policies:

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

5.4.3.2 IPS_IPB_EXT.1[IPS] IP Blocking

IPS_IPB_EXT.1.1[IPS] The TSF shall support configuration and implementation of known-good and known-bad lists of [*source, destination*] IP addresses and [*no additional address types*]

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

5.4.3.1 IPS_NTA_EXT.1[IPS] Network Traffic Analysis

IPS_NTA_EXT.1.1[IPS] The TSF shall perform analysis of IP-based network traffic forwarded to the TOE’s sensor interfaces, and detect violations of administratively-defined IPS policies.

IPS_NTA_EXT.1.2[IPS] The TSF shall process (be capable of inspecting) the following network traffic protocols:

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

IPS_NTA_EXT.1.3[IPS] The TSF shall allow the signatures to be assigned to sensor interfaces configured for promiscuous mode, and to interfaces configured for inline mode, and support designation of one or more interfaces as ‘management’ for communication between the TOE and external entities without simultaneously being sensor interfaces.

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

- o no other interface types].

5.4.3.2 IPS_SBD_EXT.1[IPS] Signature-Based IPS Functionality

IPS_SBD_EXT.1.1[IPS] The TSF shall support inspection of packet header contents and be able to inspect at least the following header fields:

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

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

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

IPS_SBD_EXT.1.3[IPS] The TSF shall be able to detect the following header-based signatures (using fields identified in IPS_SBD_EXT.1.1) at IPS sensor interfaces:

a) IP Attacks

- i) *IP Fragments Overlap (Teardrop attack, Bonk attack, or Boink attack)*
- ii) *IP source address equal to the IP destination (Land attack)*

b) ICMP Attacks

- i) *Fragmented ICMP Traffic (e.g. Nuke attack)*
- ii) *Large ICMP Traffic (Ping of Death attack)*

c) TCP Attacks

- i) TCP NULL flags*
- ii) TCP SYN+FIN flags*
- iii) TCP FIN only flags*
- iv) TCP SYN+RST flags*

d) UDP Attacks

- i) UDP Bomb Attack*
- ii) UDP Chargen DDoS Attack*

IPS_SBD_EXT.1.4[IPS] The TSF shall be able to detect all the following traffic-pattern detection signatures, and to have these signatures applied to IPS sensor interfaces:

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

IPS_SBD_EXT.1.5[IPS] The TSF shall allow the following operations to be associated with signature-based IPS policies:

- In any mode, for any sensor interface: [
 - allow the traffic flow;]
- In inline mode:
 - block/drop the traffic flow;
 - and [
 - allow all traffic flow;]

IPS_SBD_EXT.1.6[IPS] The TSF shall support stream reassembly or equivalent to detect malicious payload even if it is split across multiple non-fragmented packets

5.5 TOE SFR Dependencies Rationale for SFRs Found in NDcPP

The NDcPP and PP module 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 which are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below.

Table 19: 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. 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 mod_ips_v1.0, which includes refinements to assurance measures for the SFRs defined in the two aforementioned modules 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 20: 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.

Cisco NGIPSv Security Target

Component	How requirement will be met
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s) identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ALC_CMS.1	
ATE_IND.1	Cisco provides the TOE for testing.
AVA_VAN.1	Cisco provides the TOE for testing.

6 TOE SUMMARY SPECIFICATION


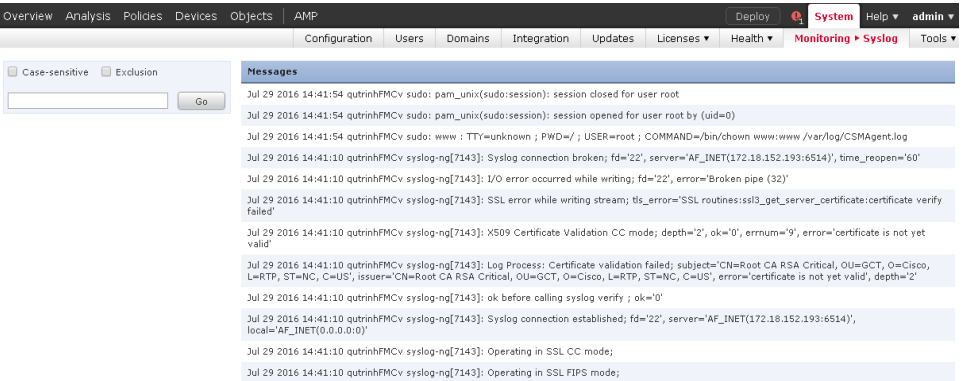
6.1 TOE Security Functional Requirement Measures

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

Table 21: How TOE SFRs Are Satisfied

TOE SFRs	How the SFR is Satisfied
Security Functional Requirements Drawn from NDcPP	
FAU_GEN.1 FAU_GEN.2 FAU_GEN_EXT.1 FAU_STG_EXT.1 FAU_STG_EXT.4 FAU_STG_EXT.5	<p>Auditing is the recording of events within the system. The TOE generates log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting the audit function³, any use of an administrator command or action via the CLI and web interfaces, and all of the required auditable events identified in Table 17. For more information about the required audit events, please refer to Table 17 and the operational user guide (also known as the CC Supplemental User guide).</p> <p>The TOE can record activity on the system in two ways. The system can generate an audit record for each user interaction with the web interface and each command in the CLI interface in the audit log and can also record system status messages in the system log (i.e., syslog). For example, when an administrator imports or deletes a certificate (with associated keys), an audit message is generated that indicates which administrator performed, the action, and includes a unique identifier for the certificate (keys cannot be imported or deleted independently of their associated certificates).</p> <p>In addition to auditing administrative activity, the TOE can generate traffic events as part of the intrusion and access control policies and these event records are stored in logs separate from the audit logs for performance and security reasons. More information about the traffic events is presented in IPS sections.</p> <p>FMC and Sensors log auditing information for all user activity in a read-only format. Modifications are not allowed by the interfaces and only authorized administrators can delete the audit logs. Audit logs are presented in a standard event view that allows administrators to view, sort, and filter audit log messages based on any item in the audit view. The audit view contains columns with information field for each audit event such as time, user, subsystem, message, and source IP. Please see the figure below for example.</p> <p style="text-align: center;">Figure 3: Audit View</p>

³ Note that the audit function cannot be disabled other than shutting down the entire system.

TOE SFRs	How the SFR is Satisfied																																																							
	 <p>Audit Log Table View of the Audit Log No Search Constraints (Edit Search)</p> <table border="1"> <thead> <tr> <th>Time</th> <th>User</th> <th>Subsystem</th> <th>Message</th> <th>Source IP</th> </tr> </thead> <tbody> <tr> <td>2016-07-29 14:39:53</td> <td>admin</td> <td>System > Users > Users</td> <td>Page View</td> <td>10.128.120.105</td> </tr> <tr> <td>2016-07-29 14:39:51</td> <td>admin</td> <td>System > Local > User Management > Users</td> <td>Added user - testuser:80</td> <td>10.128.120.105</td> </tr> <tr> <td>2016-07-29 14:39:37</td> <td>admin</td> <td>System > Users > Users > Create User</td> <td>Add</td> <td>10.128.120.105</td> </tr> <tr> <td>2016-07-29 14:39:15</td> <td>admin</td> <td>System > Users > Users > Create User</td> <td>Page View</td> <td>10.128.120.105</td> </tr> <tr> <td>2016-07-29 14:39:10</td> <td>admin</td> <td>System > Users > Users</td> <td>Page View</td> <td>10.128.120.105</td> </tr> <tr> <td>2016-07-29 14:39:02</td> <td>admin</td> <td>Devices > Device Management</td> <td>Page View</td> <td>10.128.120.105</td> </tr> <tr> <td>2016-07-29 14:38:27</td> <td>admin</td> <td>System > Monitoring > Audit</td> <td>Page View</td> <td>10.128.120.105</td> </tr> <tr> <td>2016-07-29 14:38:18</td> <td>admin</td> <td>System > Configuration > Configuration > /admin/audit_cert.cgi</td> <td>Page View</td> <td>10.128.120.105</td> </tr> <tr> <td>2016-07-29 14:38:16</td> <td>admin</td> <td>Login</td> <td>Login Success</td> <td>10.128.120.105</td> </tr> <tr> <td>2016-07-29 14:25:05</td> <td>admin</td> <td>Session Expiration</td> <td>Session expired due to inactivity (admin)</td> <td>Default User IP</td> </tr> </tbody> </table> <p>The following fields are recorded for each audit event in the audit view:</p> <ul style="list-style-type: none"> Time: The time and date that the appliance generated the audit record. User: The user name of the user that triggered the audit event. Subsystem: The menu path the user followed to generate the audit record. For example, “System > Monitoring > Audit” is the menu path to view the audit log. Message: The action the user performed. For example, “Page View” signifies that the user simply viewed the page indicated in the Subsystem, while “Save” means that the user clicked the Save button on the page. Source IP: The IP address of the host used by the user. <p style="text-align: center;">Figure 4: Syslog View</p>  <p>The user can also view the audit log using the command “show audit-log” or “show syslog” via the CLI interface. All GUI actions and CLI commands are recorded in the audit log and can only be viewed by authorized administrators. To distinguish between the two, the Subsystem field will identify “Command Line” for commands and the Message field will identify the executed command.</p> <p>In general, the logged audit records identify the date and time, the identity of the actor (e.g., user, daemon, or network host) responsible for the event, the subsystem that triggers the event, an indication of whether the event succeeded, failed or had some other outcome</p>	Time	User	Subsystem	Message	Source IP	2016-07-29 14:39:53	admin	System > Users > Users	Page View	10.128.120.105	2016-07-29 14:39:51	admin	System > Local > User Management > Users	Added user - testuser:80	10.128.120.105	2016-07-29 14:39:37	admin	System > Users > Users > Create User	Add	10.128.120.105	2016-07-29 14:39:15	admin	System > Users > Users > Create User	Page View	10.128.120.105	2016-07-29 14:39:10	admin	System > Users > Users	Page View	10.128.120.105	2016-07-29 14:39:02	admin	Devices > Device Management	Page View	10.128.120.105	2016-07-29 14:38:27	admin	System > Monitoring > Audit	Page View	10.128.120.105	2016-07-29 14:38:18	admin	System > Configuration > Configuration > /admin/audit_cert.cgi	Page View	10.128.120.105	2016-07-29 14:38:16	admin	Login	Login Success	10.128.120.105	2016-07-29 14:25:05	admin	Session Expiration	Session expired due to inactivity (admin)	Default User IP
Time	User	Subsystem	Message	Source IP																																																				
2016-07-29 14:39:53	admin	System > Users > Users	Page View	10.128.120.105																																																				
2016-07-29 14:39:51	admin	System > Local > User Management > Users	Added user - testuser:80	10.128.120.105																																																				
2016-07-29 14:39:37	admin	System > Users > Users > Create User	Add	10.128.120.105																																																				
2016-07-29 14:39:15	admin	System > Users > Users > Create User	Page View	10.128.120.105																																																				
2016-07-29 14:39:10	admin	System > Users > Users	Page View	10.128.120.105																																																				
2016-07-29 14:39:02	admin	Devices > Device Management	Page View	10.128.120.105																																																				
2016-07-29 14:38:27	admin	System > Monitoring > Audit	Page View	10.128.120.105																																																				
2016-07-29 14:38:18	admin	System > Configuration > Configuration > /admin/audit_cert.cgi	Page View	10.128.120.105																																																				
2016-07-29 14:38:16	admin	Login	Login Success	10.128.120.105																																																				
2016-07-29 14:25:05	admin	Session Expiration	Session expired due to inactivity (admin)	Default User IP																																																				

TOE SFRs	How the SFR is Satisfied																					
	<p>(if applicable), and the source IP (if applicable). The logged audit records also include event-specific content that includes at least all of the content required in table above.</p> <p>The TOE includes an internal log database implementation on FMC that can be used to store and review audit records locally on FMC. The internal audit database on FMC store a maximum of 100,000 audit records (to configure the size, go to System > Configuration > Database, and click on "Audit Event Database"). When the audit log is full, the oldest audit records are overwritten by the newest audit records. In addition, the TOE also includes a local syslog storage in /var/log/messages. Similar to the audit log, when the syslog is full, the oldest syslogs messages are overwritten by the newest one. The NGIPSv, like the FMC, stores all its audit messages locally and when the audit log is full, the oldest audit records are overwritten by the newest audit records. The NGIPSv also sends the IPS events to FMC/FMCv.</p> <p>For audit log, the events are stored in partitioned event tables. The TOE will prune (i.e., delete) the oldest partition whenever the oldest partition can be pruned without dropping the number of events count below the configured event limit. Note this limit defaults to 10,000 if you set it any lower. For example, if you set the limit to 10,000 events, the events count may need to exceed 15,000 events before the oldest partition can be deleted. For syslog, the logs are stored in /var/log/messages and are rotated daily or when the log file size exceeds 25 MB. After the maximum number of backlog files is reached, the oldest is deleted and the numbers on the other backlogs file are incremented.</p> <p>To prevent the losing of critical audit records, the administrators can configure the system to transmit all the audit events (i.e., audit log and syslog) in real-time over a secure TLS connection to an external audit server in the operational environment. When an audit event is generated, it is sent to the local storage and external audit server simultaneously. This ensures that current audit events can be viewed locally while all events, new or old, are stored off-line as required by the NDcPP.</p> <p>Note that the protection of the audit records stored at the external audit server is the responsibility of the operational environment. The TOE is only responsible for the secure communication channel. It is recommended that the audit server is physically or logically separated (e.g., VLANs) from the other networks.</p> <table border="1" data-bbox="477 1360 1430 1885"> <thead> <tr> <th data-bbox="477 1360 932 1394">SFR</th> <th data-bbox="932 1360 1182 1394">NGIPSv</th> <th data-bbox="1182 1360 1430 1394">FMC</th> </tr> </thead> <tbody> <tr> <td colspan="3" data-bbox="477 1394 1430 1428" style="text-align: center;"><i>Reproduced from the NDcPP</i></td> </tr> <tr> <td data-bbox="477 1428 932 1528">Start-up and shutdown of audit functions</td> <td data-bbox="932 1428 1182 1528">Generate. Send to syslog.</td> <td data-bbox="1182 1428 1430 1528">Generate. Store locally. Send to syslog.</td> </tr> <tr> <td data-bbox="477 1528 932 1629">Administrative login/logout</td> <td data-bbox="932 1528 1182 1629">Generate. Send to syslog.</td> <td data-bbox="1182 1528 1430 1629">Generate. Store locally. Send to syslog.</td> </tr> <tr> <td data-bbox="477 1629 932 1730">Changes to TSF data</td> <td data-bbox="932 1629 1182 1730">Generate. Send to syslog.</td> <td data-bbox="1182 1629 1430 1730">Generate. Store locally. Send to syslog.</td> </tr> <tr> <td data-bbox="477 1730 932 1831">Generating/import, changing deleting cryptographic keys</td> <td data-bbox="932 1730 1182 1831">Generate. Send to syslog.</td> <td data-bbox="1182 1730 1430 1831">Generate. Store locally. Send to syslog.</td> </tr> <tr> <td data-bbox="477 1831 932 1885">Resetting passwords</td> <td data-bbox="932 1831 1182 1885">Generate. Send to syslog.</td> <td data-bbox="1182 1831 1430 1885">Generate. Store locally.</td> </tr> </tbody> </table>	SFR	NGIPSv	FMC	<i>Reproduced from the NDcPP</i>			Start-up and shutdown of audit functions	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	Administrative login/logout	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	Changes to TSF data	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	Generating/import, changing deleting cryptographic keys	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	Resetting passwords	Generate. Send to syslog.	Generate. Store locally.
SFR	NGIPSv	FMC																				
<i>Reproduced from the NDcPP</i>																						
Start-up and shutdown of audit functions	Generate. Send to syslog.	Generate. Store locally. Send to syslog.																				
Administrative login/logout	Generate. Send to syslog.	Generate. Store locally. Send to syslog.																				
Changes to TSF data	Generate. Send to syslog.	Generate. Store locally. Send to syslog.																				
Generating/import, changing deleting cryptographic keys	Generate. Send to syslog.	Generate. Store locally. Send to syslog.																				
Resetting passwords	Generate. Send to syslog.	Generate. Store locally.																				

TOE SFRs	How the SFR is Satisfied		
			Send to syslog.
FAU_GEN.1	n/a	n/a	
FAU_GEN.2	n/a	n/a	
FAU_GEN_EXT.1	n/a	n/a	
FAU_STG_EXT.1	n/a	n/a	
FAU_STG_EXT.4	n/a	n/a	
FAU_STG_EXT.5	n/a	n/a	
FCO_CPC_EXT.1	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	
FCS_CKM.1	n/a	n/a	
FCS_CKM.2	n/a	n/a	
FCS_CKM.4	n/a	n/a	
FCS_COP.1/DataEncryption	n/a	n/a	
FCS_COP.1/SigGen	n/a	n/a	
FCS_COP.1/Hash	n/a	n/a	
FCS_COP.1/KeyedHash	n/a	n/a	
FCS_HTTPS_EXT.1	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	
FCS_RBG_EXT.1	n/a	n/a	
FCS_SSHS_EXT.1	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	
FCS_TLSC_EXT.1 and FCS_TLSC_EXT.2	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	
FCS_TLSS_EXT.1	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	
FIA_AFL.1	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	
FIA_PMG_EXT.1	n/a	n/a	
FIA_UIA_EXT.1	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	
FIA_UAU_EXT.2	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	
FIA_UAU.7	n/a	n/a	
FIA_X509_EXT.1/ITT	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	
FIA_X509_EXT.1/Rev	Generate. Send to syslog.	Generate. Store locally. Send to syslog.	

TOE SFRs	How the SFR is Satisfied		
	FIA_X509_EXT.2	n/a	n/a
	FIA_X509_EXT.3	n/a	n/a
	FMT_MOF.1/ManualUpdate	n/a	Generate. Store locally. Send to syslog.
	FMT_MTD.1/CoreData	Generate. Send to syslog.	Generate. Store locally. Send to syslog.
	FMT_MTD.1/CryptoKeys	Generate. Send to syslog.	Generate. Store locally. Send to syslog.
	FMT_SMF.1	n/a	n/a
	FMT_SMR.2	n/a	n/a
	FPT_SKP_EXT.1	n/a	n/a
	FPT_APW_EXT.1	n/a	n/a
	FPT_TST_EXT.1	n/a	n/a
	FPT_TUD_EXT.1	n/a	Generate. Store locally. Send to syslog.
	FPT_STM_EXT.1	Generate. Send to syslog.	Generate. Store locally. Send to syslog.
	FTA_SSL_EXT.1	Generate. Send to syslog.	Generate. Store locally. Send to syslog.
	FTA_SSL.3	Generate. Send to syslog.	Generate. Store locally. Send to syslog.
	FTA_SSL.4	Generate. Send to syslog.	Generate. Store locally. Send to syslog.
	FTA_TAB.1	n/a	n/a
	FTP_ITC.1	Generate. Send to syslog.	Generate. Store locally. Send to syslog.
	FTP_TRP.1/Admin	Generate. Send to syslog.	Generate. Store locally. Send to syslog.
	FPT_ITT.1	Generate. Send to syslog.	Generate. Store locally. Send to syslog.
Reproduced from the mod_ips_v1.0			
	Start-up and shut-down of the IPS functions	Generate. Send to syslog. Send to FMC.	Receive from NGIPSv. Store locally.
	All dissimilar IPS events	Generate. Send to syslog. Send to FMC.	Receive from NGIPSv. Store locally.

TOE SFRs	How the SFR is Satisfied		
	All dissimilar IPS reactions	Generate. Send to syslog. Send to FMC.	Receive from NGIPSv. Store locally.
	Totals of similar events occurring within a specified time period	Generate. Send to syslog. Send to FMC.	Receive from NGIPSv. Store locally.
	Totals of similar reactions occurring within a specified time period	Generate. Send to syslog. Send to FMC.	Receive from NGIPSv. Store locally.
	FAU_GEN.1/IPS	None.	None.
	FAU_SAR.1/IPS	None.	None.
	FAU_SAR.2/IPS	None.	None.
	FAU_SAR.3/IPS	None.	None.
	FAU_STG.1/IPS	None.	None.
	FMT_MOF.1/IPS	None.	None.
	FMT_MTD.1/IPS	None.	None.
	FMT_SMF.1/IPS	Generate. Send to syslog. Send to FMC.	Receive from NGIPSv. Store locally.
	FMT_SMR.2/IPS	n/a	n/a
	IPS_ABD_EXT.1/IPS	Generate. Send to syslog. Send to FMC.	Receive from NGIPSv. Store locally.
	IPS_IPB_EXT.1/IPS	Generate. Send to syslog. Send to FMC.	Receive from NGIPSv. Store locally.
	IPS_NTA_EXT.1/IPS	Generate. Send to syslog. Send to FMC.	Receive from NGIPSv. Store locally.
	IPS_SBD_EXT.1/IPS	Generate. Send to syslog. Send to FMC.	Receive from NGIPSv. Store locally.
	<p>The Security Audit function is designed to satisfy the following security functional requirements:</p> <ul style="list-style-type: none"> • FAU_GEN.1: The TOE can generate audit records for events to include starting the audit function, administrator commands/actions, and all other events identified in Table 15. Furthermore, each audit record identifies the date/time, responsible subject/user, event type, outcome of the event, IP source, as well as the additional event-specific content indicated in Table 15. • FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by daemon or network host) that caused the event. • FAU_STG_EXT.1: The TOE can be configured to transmit audit records to an external audit server over a secure channel. The audit records are also stored locally and when the local storage is full, the newest data will overwrite the oldest data. 		

TOE SFRs	How the SFR is Satisfied
FCO_CPC_EXT.1	<p>In order for a component to communicate with the TOE as part of a distributed TOE system, it must successfully complete a registration process. Each TOE component comes with a manufacture's TLS certificate. To start the registration process, the administrator must enable or register the TOE components. For example, on the FMC, the administrator must go to Device Management UI and click on "Add Device". At the same time, the administrator must go to the Sensor CLI or GUI, and click or enter "Configure Manager Add". The administrator must specify the peer hostname or IP address and the registration key used for the initial authentication. Because the administrator can choose the registration key and must provide a specific hostname/IP address, while initiating the registration on both TOE components, the registration action can be assured of the unique identification of the TOE components. During the registration process, the manufacturer's TLS certificates are used to setup the initial TLS channel on the internal trusted management network. If the authentication succeeded, the resident CA on the FMC will sign and issue a TLS certificate along with the private key to the Sensor which will be used for subsequent TLS channel. To disable or de-register a Sensor, the administrator must initiate a "Delete Device" on the FMC Device Management UI and then perform a "Configure Manager Delete" action on the Sensor CLI or UI. This will destroy (i.e., zeroize) the TLS certificate and private key. Once this has occurred, no further communication can happen without another registration process.</p> <p>The Communication function is designed to satisfy the following security functional requirements:</p> <ul style="list-style-type: none"> • <u>FCO_CPC_EXT.1</u>: The TOE allows authorized administrator to add or remove TOE components as part of a distributed TOE.
FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_HTTPS_EXT.1 FCS_RBG_EXT.1 FCS_SSHS_EXT.1 FCS_TLSC_EXT.1 FCS_TLSC_EXT.2 FCS_TLSS_EXT.1	<p>Each FMC and each Sensor (including the virtual appliance) "TOE" utilizes FIPS-certified cryptographic algorithms to provide supporting cryptographic functions. When the term "TOE" is used in this section, it refers to both the FMC and sensors, except where noted. The relevant algorithms have been FIPS validated as indicated in section 7.3.</p> <p>The TOE supports RSA, and ECDSA in the evaluated configuration. TLS supports both ECDSA and RSA digital signature, while SSH and trusted update only support RSA digital signature. (RSA only). Key establishment, for asymmetric keys on the TOE implements RSA-based and EllipticCurve-based key establishment schemes as specified in NIST SP 800-56A "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography". In addition, the TOE also supports FFC Schemes using "safe-prime" groups (i.e., DH group 14) key establishment scheme that meets standard RFC 3526, section 3 for interoperability.</p> <p>The TOE provides cryptographic hashing services using SHA-1 (, SHA-256, SHA-384, and SHA-512, and keyed-hash message authentication using HMAC-SHA-1 (key length and output length of 160-bits), HMAC-SHA-256 (key length and output length of 256-bit), HMAC-SHA-384 (key length and output length of 384-bit), and HMAC-SHA-512 (key length and output length of 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). [FCS_COP.1/Hash and FCS_COP.1/KeyedHash]</p> <p>The TOE uses a hardware-based random bit generator that complies with NIST 800-90A CTR_DRBG (AES-256) Deterministic Random Bit Generation (DRBG) operating in FIPS mode. In addition, the DRBG is seeded by an entropy source that is at least 256-bit value derived</p>

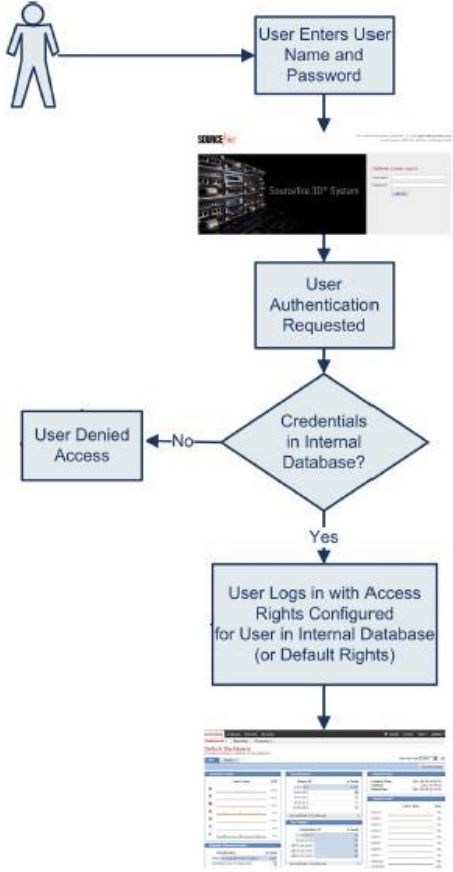
TOE SFRs	How the SFR is Satisfied
	<p>from various highly sensitive and proprietary noise sources described in the proprietary Entropy Design document.</p> <p>Additionally, the TOE is designed to zeroize secret and private keys when they are no longer required by the TOE. This zeroization mechanism is performed by overwriting the sensitive keys and data with all 0's before deleting them, followed by a read-verify. The table in section 7.2 identifies the applicable secret and private keys and summarizes, how they are generated, what are their purpose, where are they stored, and when and how are they deleted.</p> <p>The supporting cryptographic algorithms identified above are included to support the SSHv2 (RFCs 4251, 4252, 4253, 4254, 5647, 6668, and 8332) and TLSv1.2 (RFC 4346/5246)/HTTPS (RFC 2818) security communication protocols. As described in RFC 2818, HTTPS is HTTP over TLS. The HTTP client is also the TLS client, and all HTTP data is sent as TLS application data.</p> <p>When CC mode is enabled, the TOE is restricted to only support TLSv1.2 for HTTPS sessions and client/server communications between TOE components and both TLSv1.1 and TLSv1.2 for syslog communications with AES 128 or 256 bit symmetric ciphers in CBC and GCM modes, in conjunction with SHA, RSA, ECDHE (NIST curves presented in the supported curves extension in the client hello - secp256r1, secp384r1, secp521r1) and ECDSA. The following TLS cipher suites are implemented by the TOE in CC mode:</p> <ul style="list-style-type: none"> • Relevant to FTP_ITC.1, FCS_TLSC_EXT.1 and FCS_TLSC_EXT.2, for syslog over TLS (client only) from FMC/FMCv, and for syslog over TLS (client only) from NGIPSv (for transmission of IPS messages and system messages) are as listed in section 5.3.3.11 of this document. • Relevant to FPT_ITT.1, FCS_TLSC_EXT.1, and FCS_TLSS_EXT.1 (client and server) are as listed in sections 5.3.3.11 and 5.3.3.13 of this document. • Relevant to FTP_TRP.1 and FCS_TLSS_EXT.1 (server only) are as listed in section 5.3.3.13 of this document. <p>While the FOM (see section 7.3) supports additional cipher suites (for example, RSA_3DES_EDE_CBC_SHA, RSA_DES_CBC_SHA, RSA_RC4_128_MD5, RSA_RC4_128_SHA, etc.), they are all disabled while operating in CC mode. The TOE is restricted to only support TLSv1.2 for HTTPS sessions and client/server communications between TOE components and both TLSv1.1 and TLSv1.2 for syslog communications. If the TLS client does not support TLSv1.2, the TLS connection will fail and the administrators can not establish a HTTPS web-based session with the TOE. The TLS connection supporting FPT_ITT.1 supports TLSv1.2 only. Any TLS or SSL versions not supported is rejected by the TOE.</p> <p>The Key establishment parameters for each of the TLS connections in the TOE are as follows –</p> <ol style="list-style-type: none"> 1. FMC/FMCv (HTTPS/TLS)- 2048-bit RSA and ECDHE secp256r1, secp384r1 and secp521r1 2. FMC/FMCv (HTTPS/TLS)- 2048-bit RSA and ECDHE secp256r1, secp384r1 and secp521r1 <p>When in CC mode and the TOE acts as a TLS client (e.g., connection to the syslog server), the TOE will verify the server Common Name (CN) and/or Subject Alternative Name (SAN) against the reference identity (wildcard is supported as required in section 6 of RFC 6125). When TOE components are communicating with each other (as part of this distributed TOE),</p>

TOE SFRs	How the SFR is Satisfied
	<p>they verify each other using unique reference identifiers (UID) by verifying the UID in the title field of the certificates subject (wildcards are not supported for this communication, and are an optional part of the requirement). The title field (id-at-title) is used per RFC 5280 Appendix A. In either case (connection to a syslog server, or connections among TOE components), if verification fails, the TLS connection will not be established. Mutual authentication must be configured on the TOE with a client-side X.509v3 certificate. The key agreement parameters of the server key exchange message are specified in the RFC 5246 (section 7.4.3) for TLSv1.2. The TOE conforms to both RFCs supporting both RSA 2048 and NIST ECC curves secp256r1, although only RSA certificates are available to use for communication between TOE components.</p> <p>The TOE provides session resumption only for remote administration sessions. Session resumption is not supported by the NGIPSv or for Internal TOE communication (i.e., FPT_ITT.1). Only the FMC can resume a remote administration HTTPS session based upon session tickets. Session tickets are encrypted using the symmetric algorithms and key lengths associated with the negotiated ciphersuite and which are consistent with the selections from FCS_COP.1/DataEncryption. Session tickets adhere to the structural format provided in section 4 of RFC 5077.</p> <p>The TOE supports SSHv2 with AES (in CBC or GCM mode) 128 or 256 bits cipher for encryption, in conjunction with HMAC-SHA1, HMAC-SHA2-256, or HMAC-SHA2-512 for integrity and authenticity, and RSA with diffie-hellman-group14-sha1 for the key exchange method. While DES and 3DES, HMAC-MD5 and HMAC-MD5-96, and diffie-hellman-group-1 and other diffie-hellman-exchange groups are all implemented, they are disabled while the TOE is operating in CC Mode. In addition, SSHv1 is also disabled by default for security reasons. If the SSH client does not support the Approved algorithms or SSH version, the SSH connection will fail and the administrators will not establish an SSHv2 web-based session with the TOE.</p> <p>The TOE uses OpenSSH implementation version 7.6p1 to support the SSHv2 connections. The authentication timeout period is 90 seconds allowing clients to retry only 3 times. In addition, both public-key (RSA) and password-based authentication can be configured with password-based being the default method used. When an SSH client presents a public key, the TOE establishes a user identity by verifying that the SSH client's presented public key matches one that is stored within an authorized keys file. The TOE supports SSH host key implementation using rsa-sha2-256, or rsa-sha2-512 and SSH public key authentication using ssh-rsa (NGIPSv) or ecdsa-sha2-nistp256 (FMC/FMCv). The SSH packets are limited to 262,149 bytes. If OpenSSH detects packet larger than that, then it will drop the packet. Whenever the timeout period or authentication retry limit is reached, the TOE closes the applicable TCP connection and releases the SSH session resources. As SSH packets are being received, the TOE uses a buffer to build all packet information. Once complete, the packet is checked to ensure it can be appropriately decrypted. However, if it is not complete when the buffer becomes full (256 Kbytes) the packet will be dropped. Note that the TOE manages a tracking mechanism for each SSH session so that it can initiate a new key exchange when either approximately 1 hour of time or 1GB of data is reached. An audit event is generated when a successful SSH rekey occurs.</p> <p>The Cryptographic support function is designed to satisfy the following security functional requirements:</p> <ul style="list-style-type: none"> • FCS_CKM.1: The TOE generates Approved RSA public/private key pairs for key establishment to support other security protocols such as SSHv2 and TLS. The RSA

TOE SFRs	How the SFR is Satisfied																		
	<p>modulus key size is 2048 bit, which according to NIST PUB 800-57, is equivalent to a symmetric key strength of 112 bits. The FMC component of the TOE generates ECC curve P-256 remote administration via TLSv1.2. the TOE also supports FFC Schemes using “safe-prime” groups (i.e., DH group 14) key generation/establishment scheme that meets standard RFC 3526, section 3 for interoperability</p> <ul style="list-style-type: none"> <p>FCS_CKM.2: The TOE supports RSA and ECDSA algorithm as part of the TLS session establishments. RSA only for SSH session establishment.</p> <table border="1" data-bbox="571 554 1463 995"> <thead> <tr> <th>Scheme</th> <th>SFR</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td>DH-14</td> <td>FCS_SSHS_EXT.1</td> <td>Administration</td> </tr> <tr> <td rowspan="2">RSA</td> <td>FCS_TLSC_EXT.1</td> <td rowspan="2">Internal TOE Communication</td> </tr> <tr> <td>FCS_TLSS_EXT.1</td> </tr> <tr> <td rowspan="2">ECDHE</td> <td>FCS_TLSS_EXT.1</td> <td>Administration</td> </tr> <tr> <td>FCS_TLSC_EXT.1</td> <td>Syslog</td> </tr> <tr> <td></td> <td>FCS_TLSS_EXT.1</td> <td>Administration</td> </tr> </tbody> </table> <p>FCS_CKM.4: Keys are zeroized when they are no longer needed by the TOE.</p> <p>FCS_COP.1/DataEncryption: The TOE supports Approved AES symmetric algorithm for encryption and decryption of communication data, in support other security protocols such as SSHv2 and TLS.</p> <p>FCS_COP.1/SigGen: The TOE supports Approved RSA and ECDSA digital signature algorithm for signature generation and verification, in support of digital certificates. The TOE provides signature services for 2048-bit RSA keys, as well as ECDSA signatures using curves P-256, P-384 and P-521.</p> <p>FCS_COP.1/Hash: The TOE supports Approved SHA hashing algorithm for hashing of communication data, in support other security protocols such as SSHv2 and TLS.</p> <p>FCS_COP.1/KeyedHash: The TOE supports Approved HMAC-SHA message authentication algorithm for authenticating of communication data, in support other security protocols such as SSHv2 and TLS.</p> <p>FCS_HTTPS_EXT.1: The TOE (FMC only, not NGIPSv) supports HTTPS web-based secure administrator sessions.</p> <p>FCS_RBG_EXT.1: The TOE uses Approved NIST 800-90 DRBG implementation to generate random numbers for generating cryptographic keys, and seeds the DRBG with a hardware-based entropy source.</p> <p>FCS_SSHS_EXT.1: The TOE supports SSHv2 interactive CLI-based administrator sessions as described above.</p> 	Scheme	SFR	Service	DH-14	FCS_SSHS_EXT.1	Administration	RSA	FCS_TLSC_EXT.1	Internal TOE Communication	FCS_TLSS_EXT.1	ECDHE	FCS_TLSS_EXT.1	Administration	FCS_TLSC_EXT.1	Syslog		FCS_TLSS_EXT.1	Administration
Scheme	SFR	Service																	
DH-14	FCS_SSHS_EXT.1	Administration																	
RSA	FCS_TLSC_EXT.1	Internal TOE Communication																	
	FCS_TLSS_EXT.1																		
ECDHE	FCS_TLSS_EXT.1	Administration																	
	FCS_TLSC_EXT.1	Syslog																	
	FCS_TLSS_EXT.1	Administration																	

TOE SFRs	How the SFR is Satisfied
	<ul style="list-style-type: none"> • <u>FCS_TLSC_EXT.1</u> and <u>FCS_TLSS_EXT.1</u>: The TOE supports the required cipher suites and provides the secure transport protocol for the HTTPS web-based secure administrator sessions, connection to syslog server and secure connections between parts of the distributed TOE.
FIA_AFL.1 FIA_PMG_EXT.1 FIA_UIA_EXT.1 FIA_UAU_EXT.2 FIA_UAU.7	<p>The TOE is designed to successfully identify and authenticate user before allowing access to the TOE's security function. When identification and authentication data is entered (username and password), the TOE attempts to identify the applicable user account from the provided identity and if a match is found, the password provided is hashed with a salt value and compared against the stored hash⁴ with the user account information in the internal database. If a user account cannot be associated with the provided identity or the hashed password does not match that stored hash with the user account information, the process will fail. No actions are allowed, other than re-entry of identification and authentication data or viewing the login banner. Once the user has successfully logged in, the privilege level or role will control what management functions he or she has access and authorization to perform. Figure below shows the authentication process.</p> <p style="text-align: center;">Figure 5: Authentication Process</p>

⁴ The password is hashed with Approved SHA-512 and the salt value is 32-bit long.

TOE SFRs	How the SFR is Satisfied
	 <pre> graph TD User((User)) --> Step1[User Enters User Name and Password] Step1 --> Step2[User Authentication Requested] Step2 --> Decision{Credentials in Internal Database?} Decision -- No --> Step3[User Denied Access] Decision -- Yes --> Step4[User Logs in with Access Rights Configured for User in Internal Database (or Default Rights)] Step4 --> Step5[Dashboard] </pre> <p>Users can connect to the TOE via a local console (FMC or NGIPSv) or remotely using SSHv2 (FMC or NGIPSv) or HTTPS (FMC only). In each case, the user is required to log in prior to successfully establishing a session through which TOE security functions can be performed. By default, the Cisco NGIPSv System uses internal authentication to check user credentials when a user logs in.</p> <p>When logging in, the TOE will not echo passwords such that passwords are not inadvertently displayed to the user and any other users that might be able to view the login display. The TOE replaced the entered password character with a "*" character or not show any character at all. This depends on where the user is logging in from, for example, using web GUI versus the SSH client. If the authentication fails, the TOE is designed to not indicate either the username and/or password were incorrect. The error message would just state access denied or unable to authorize access. No other information about the failed login in can be ascertained from the error message. Once the number of failed attempts has exceeded the configured limit, the user will be locked out. Only administrator or user with admin privileges can unlock the user.</p> <p>Note also that should a user have their session terminated (e.g., due to inactivity), they are required to successfully re-authenticate, by re-entering their identity and authentication data, in order to gain access to their session. The authentication data is not cached by the TOE for any reason.</p>

TOE SFRs	How the SFR is Satisfied
	<p>When creating or changing passwords, the passwords must be composed of upper and lower case letters, numbers and special characters including blank space and !@#%&*() '(double or single quote/apostrophe), + (plus), - (minus), = (equal), , (comma), . (period), / (forward-slash), \ (back-slash), (vertical-bar or pipe), : (colon), ; (semi-colon), < > (less-than, greater-than inequality signs), [] (square-brackets), { } (braces or curly-brackets), ? (question-mark), (underscore), and ~ (tilde). The password must have at least one upper case, one lower case, one number, and one special character. This is configured by checking on "Check Password Strength⁵" option per each user (See CC Supplement User Guide for details). Also, the passwords have to satisfy configured minimum password length which is set in the System Policy for all users. The minimum password length can range from 8 (default) to 127 characters (maximum) long, which includes 15 characters required by the NDCPP. Note: The user password is limited to 127 characters maximum.</p> <p>The Identification and Authentication function is designed to satisfy the following security functional requirements:</p> <ul style="list-style-type: none"> • <u>FIA AFL.1</u>: The administrator can configure the maximum number of times each user can try to login after a failed login attempt before the account is locked. The default setting is five tries. The predefined admin is exempt from being locked out but with CC mode enabled, even this account can be locked out. If all admin accounts become locked for any reason, FMC can be accessed locally using password recovery procedures. • <u>FIA PMG_EXT.1</u>: The TOE implements a rich set of password composition and aging constraints as described above. • <u>FIA UIA_EXT.1</u>: The TOE requires all users to be identified and authenticated successfully before allowing access to the TOE security function. The only action allowed before is viewing the login banner. • <u>FIA UAU_EXT.2</u>: The TOE can be configured to utilize local authentication. • <u>FIA UAU.7</u>: The TOE does not echo passwords as they are entered. The character is either replaced with "*" or not shown at all.
<p>FIA_X509_EXT.1/ITT FIA_X509_EXT.1/Rev FIA_X509_EXT.2 FIA_X509_EXT.3</p>	<p>The TOE supports X.509v3 certificates as defined by RFC 5280. Public key infrastructure (PKI) credentials, such as private keys and certificates are stored securely. The identification and authentication, and authorization security functions protect an unauthorized user from gaining access to the storage.</p> <p>The validity check for the certificates takes place at session establishment and/or at time of import depending on the certificate type. For example, server certificate is checked at session establishment while CA certificate is checked at both. The TOE conforms to standard RFC 5280 for certificate and path validation (i.e., peer certificate checked for expiration, peer certificate checked if signed by a trusted CA in the trust chain, peer certificate checked for unauthorized modification, peer certificate checked for revocation).</p> <p><u>FIA_X509_EXT.1/Rev</u></p> <p>The TOE can generate a RSA key pair that can be embedded in a Certificate Signing Request (CSR) created by the TOE. The CSR can be generated at the UI. The TOE can then send the</p>

⁵ This option also prevents dictionary words or consecutive repeating characters.

TOE SFRs	How the SFR is Satisfied
	<p>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). CRL is configurable and can be used for certificate revocation check (for FTP_ITC only). NGIPSv and FMC each maintains a local cache of CRL files using an administratively configured list of CRL distribution points. NGIPSv automatically downloads new CRL files daily at a pre-set time, and FMC automatically downloads new CRL files according to an administratively configured schedule (e.g. hourly, daily, or weekly at an administrator-specified time). The extendedKeyUsage field is validated 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 and the 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.</p> <p>Checking is also done for the 'basicConstraints' extension and the 'ca' flag to determine whether they are present and set to TRUE. If they are not, the CA certificate is not accepted as a trust anchor.</p> <p>The administrators can configure a trust chain by importing the CA certificate(s) that signed and issued the server (syslog) certificate. This will tell the TOE which CA certificate(s) to use during the validation process. If the TOE does not find the trusted root CA, the TLS connection to the syslog server will fail. When the TOE is able to contact the CRL distribution point for certificate revocation checking, the TOE will reject the TLS session if the remote endpoint's (e.g. syslog server's) certificate has been revoked. When the TOE cannot establish a connection to the CRL distribution point, the TLS clients (in NGIPSv (used for transmission of system and IPS messages) and FMC/FMCv) will accept the certificate. For more information, please refer to the CC Supplemental User Guide.</p> <p><u>FIA X509 EXT.1/ITT</u></p> <p>FirePOWER Services and FMC validate each other's certificates during session establishment and validate those certificates against the locally stored root certificate. Revocation checking (e.g. CRL checking) is not performed for the TLS connection between these TOE components. The extendedKeyUsage field is validated according to the following rules - Server certificates have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field and the Client certificates have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field. Checking is done for the 'basicConstraints' extension and the 'ca' flag to determine whether they are present and set to TRUE. If they are not, the CA certificate is not accepted as a trust anchor.</p> <p>The Identification and Authentication function is designed to satisfy the following security functional requirements:</p> <ul style="list-style-type: none"> • <u>FIA X509 EXT.1/ITT</u>: The TOE supports X.509v3 certificate path validation and no CRL checking. • <u>FIA X509 EXT.1/Rev</u>: The TOE supports X.509v3 certificate path validation and CRL checking.

TOE SFRs	How the SFR is Satisfied
	<ul style="list-style-type: none"> • <u>FIA_X509_EXT.2</u>: The TOE supports X.509v3 certificate authentication for TLS connections. • <u>FIA_X509_EXT.3</u>: The TOE supports Certificate Request Message as specified by RFC 2986.
FMT_MOF.1/ ManualUpdate FMT_MTD.1/CoreData FMT_MTD.1/CryptoKeys FMT_SMF.1 FMT_SMR.2	<p>The TOE provides a web-based GUI (using HTTPS) management interface and CLI or shell (using SSH or serial connection) for all TOE administration, including the policy rule sets, user accounts and roles, and audit functions. The ability to manage various security attributes, system parameters and all TSF data is controlled and limited to those users who have been assigned the appropriate administrative role and privileges associated with those roles. Note that all users created are TOE administrators.</p> <p>Predefined User Roles</p> <p>The TOE supports the following predefined user roles:</p> <ul style="list-style-type: none"> • Administrators can set up the appliance’s network configuration, manage user accounts, and configure system policies and system settings. The Administrator Role provides access to analysis and reporting features, rule and policy configuration, system management, and all maintenance features. Users with the Administrator role have ALL access rights. <p>Note: For all non-IPS management functions, the only TOE user role is “Administrator”. This role is granted when a new user account is created and cannot be changed. The IPS Administrator will also be referred to as the “Administrator”. More details on additional IPS roles will be provided in the FMT_SMR.2/IPS section below.</p> <p>CLI and CLI Access levels</p> <p>The administrator can use the CLI to view, configure, and troubleshoot the NGIPSv systems. When administrators create a user account, they can assign it one of the following CLI access levels:</p> <ul style="list-style-type: none"> • Basic The user has read-only access and cannot run commands that impact system performance. • Configuration The user has read-write access and can run commands that impact system performance. • None The user is unable to log in. <p>Note that the CLI contains only a subset of all available functions and is only available on the Sensor. The web-based GUI is available on the FMC/FMCv only. The web-based GUI on the Sensor must be administratively removed using administrative actions outlined in the guidance during initial system configuration. The web-based GUI on the FMC is highly recommended for daily management of the FMC and its managed Sensors. Local access to the shell which allows access to the underlying operating system is allowed in the CC evaluated configuration for the initial configuration only. For normal daily operations, the web GUI is still the recommended method. Only Authorized Administrators can perform updates to all devices through the FMC.</p> <p>The Security management function is designed to satisfy the following security functional requirements:</p>

TOE SFRs	How the SFR is Satisfied
	<ul style="list-style-type: none"> • <u>FMT_MOF.1/ManualUpdate</u>: Only authorized administrators can initiate update of the TOE. • <u>FMT_MTD.1/CoreData</u>: The TOE restricts the access to manage TSF data that can affect the security functions of the TOE to Security Administrators (i.e., administrator roles). The TSF data here includes user accounts and roles, login banner, inactivity timeout values, password complexity setting, TOE updates, audit records, and audit server information. • <u>FMT_MTD.1/CryptoKeys</u>: The TOE only provides the ability for authorized administrators to access TOE data, such as audit data, configuration data, trust store, routing tables, and session thresholds. • <u>FMT_SMF.1</u>: The TOE includes the functions necessary to administer the TOE locally and remotely, to manage login banner, and to manage and verify updates of the TOE software and firmware. Please see the CC Supplemental Guide for more information. • <u>FMT_SMR.1</u>: The TOE includes one evaluated role which corresponds to the required 'Security Administrator' described above.
<p>FPT_SKP_EXT.1</p> <p>FPT_APW_EXT.1</p> <p>FPT_STM_EXT.1</p> <p>FPT_TST_EXT.1</p> <p>FPT_TUD_EXT.1</p> <p>FPT_ITT.1</p>	<p>FPT_SKP_EXT.1</p> <p>The TOE components (NGIPSv and FMC) are designed to not to disclose or store plaintext keys (e.g., pre-shared keys are never recorded in the audit records or displayed during any authentication process). Pre-shared keys are stored in plaintext and not visible via the FMC GUI or in any configuration file even by accounts that have full administrative access such as the default 'admin' account. Only the 'root' account would be able to view pre-shared keys, and use of the root account to access the Linux shell is prohibited in the evaluated configuration. The same is true for cryptographic keys such as encryption symmetric keys and private keys. The public keys can be viewed but cannot be modified without detection. Note that access to public keys is restricted to administrators.</p> <p>FPT_APW_EXT.1</p> <p>None of the administrative interfaces on these TOE components allow administrators to view administrative passwords in plaintext form. When viewing account configuration details the password field obscures with dots any existing password or any new password being entered into the field.</p> <p>FPT_STM_EXT.1</p> <p>The NGIPSv and FMC components of the TOE are hardware appliances that include a hardware-based real-time clock, while the NGIPSv and FMCv use a virtual real-time clock. The TOE's embedded OS manages the clock and the GUI exposes the clock management function to the administrators. The time source is updated frequently from the time server to ensure accuracy. The time is used for the timestamp in the audit records and events.</p> <p>FPT_TST_EXT.1</p> <p>The TOE components (NGIPSv and FMC/FMCv) include a number of built in diagnostic tests that are run during start-up to determine whether the TOE is operating properly. When CC mode is enabled, the TOE will run a HMAC-SHA512 integrity tests at power-up covering the whole kernel, all binaries and libraries, modules and boot loader of the system. If the hash verification fails, the Process Manager (PM) will not start and the system will not enter</p>

TOE SFRs	How the SFR is Satisfied
	<p>operational state. In addition, the TOE is designed to run the power-on self-tests that comply with the FIPS 140-2 requirements for self-test (e.g., known answer tests (KATs) and zeroization tests). If the TOE fails any of the FIPS power-on self-tests, the TOE will enter an error state and will not be operational. The following self-tests are executed: AES encryption/decryption KAT, RSA key generation and encryption/decryption KAT, SHA hash KATs, HMAC-SHA hash KATs, PRNG KATs, and key overwriting tests. Thus, all components of the TOE run tests (verifying the integrity of the software image prior to loading it, and verifying the correct operation of cryptographic operations prior to the TOE becoming operational) are sufficient to demonstrate that the TSF is operating correctly. Each cryptographic module includes self-tests demonstrating the correct operation of the cryptographic operations it can perform. When crypto modules are the same on different components, the cryptographic tests are the same. The approach to integrity testing is the same on the different components of the TOE, however the integrity values may differ.</p> <p>FPT_TUD_EXT.1</p> <p>The current version running on the NGIPSv and the FMC/FMCv can be queried through the FMC/FMCv WebUI. For manual update, the user will download the TOE upgrade file to FMC/FMCv and the digital signature of the downloaded file will be automatically verified as soon as the download is complete. If the digital signature verification fails the file will be automatically deleted and will not be available to be installed. This ensures TOE updates are always validated prior to installation. When an administrator attempts to initiate installation of any validated update file, the system will only allow selection of TOE components (FMC/FMCv or NGIPSv) for which the upgrade version would be appropriate (e.g., the system will not allow attempting to upgrade to an older version).</p> <p>During the update process, if the Snort engine is updated and restarted, then is a split second where the managed Sensors do not perform any traffic inspection on the network. The CC Supplemental user guide will address this situation by requiring the upgrade and maintenance actions be performed during off-peak hours where the appliance can be disconnected from the network during the upgrade process to be upgraded, restarted, and verified before re-connecting back to the network to ensure complete traffic inspection.</p> <p>FPT_ITT.1</p> <p>The TOE is designed to communicate securely with itself (i.e., TOE components) and components in the operation environment. The communication between the TOE and the administrators is either protected by physical security (e.g., local connection with serial port) or by SSHv2 or HTTPS security protocols. The communication between the TOE components is protected by TLSv1.2 security protocol. The communication between the TOE and the audit server is also protected by TLS security protocol. Protocol failures due to issues such as version mismatch (e.g., attempting to use SSHv1) or unsupported ciphersuites (e.g., using weak TLS ciphersuite) will be recorded by the TOE.</p> <p>The Protection of the TSF function is designed to satisfy the following security functional requirements:</p> <ul style="list-style-type: none"> <p>FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a cryptographic key. The protection provided by the TOE is that there is no interface available. Only 'root' user account with access to the shell can potentially view the stored keys and this is prohibited in the evaluated configuration.</p>

TOE SFRs	How the SFR is Satisfied
	<ul style="list-style-type: none"> • <u>FPT_AWP_EXT.1</u>: The TOE does not offer any functions that will disclose to any user a plaintext password. The TOE never store passwords in the plaintext. • <u>FPT_STM_EXT.1</u>: The TOE includes its own hardware clock which the administrators can manually set. Optionally, the administrator can configure the TOE components to synchronize clocks with each other (NGIPSv getting clock updates from FMC/FMCv). • <u>FPT_TST_EXT.1</u>: The TOE includes a number of power-on diagnostics and integrity test that will serve to ensure the TOE is functioning properly. The tests include ensure memory and flash can be accessed correctly as expected, and to ensure that cryptographic functions are operating normally. • <u>FPT_TUD_EXT.1</u>: The TOE provides functions to query and upgrade the versions of the TOE firmware (including installing patches/hotfixes) and SRUs. Digital signature verification is used to ensure the integrity of each upgrade prior to performing the upgrade. • <u>FPT_ITT.1</u>: The TOE protects communication between the TOE components using TLSv1.2.
FTA_SSL_EXT.1 FTA_SSL.3 FTA_SSL.4 FTA_TAB.1	<p>The TOE can be configured to display administrator-configured advisory banners that will appear when users initiate an interactive session with the TOE. The login banner can be configured in the system policy or platform settings, and can be applied to FMC itself and push out all its managed Sensors by the administrator. The login banner can be configured to display welcome information or legal in conjunction with login prompts. In each case, the banners will be displayed when accessing the TOE via the local console/serial, SSHv2, or HTTPS interfaces.</p> <p>The TOE can be configured by an administrator to set an interactive session timeout value in the system policy or platform settings, as with the login banner. The setting applies to all users and for both local and remote interactive sessions. The timeout value can be any positive integer value from 1 minute to 1,440 minutes (24 hours), with 0 disabling the timeout – the default timeout value is 60 minutes for web UI and disabled by default for CLI. The administrators can configure an exemption to the timeout feature on a per user basis. This means that the user will be exempted from the timeout. This option is not allowed in the evaluated configuration and the administrators are directed in the CC Supplement User Guide against using this option.</p> <p>A remote or local session that is inactive (i.e., no commands or actions from the remote client) for the defined timeout value will be terminated and logged by audit function. The user will be required to re-enter their username and their password to start another session. The users can also terminate their own interactive local or remote sessions, anytime they choose.</p> <p>The TOE access function is designed to satisfy the following security functional requirements:</p> <ul style="list-style-type: none"> • <u>FTA_SSL_EXT.1</u>: The TOE terminates local sessions that have been inactive for an administrator-configured period of time. Terminated sessions are disconnected from the local console input/output functions and can be reconnected only if the locked user correctly re-authenticates their username and password.

TOE SFRs	How the SFR is Satisfied
	<ul style="list-style-type: none"> • <u>FTA_SSL.3</u>: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time. • <u>FTA_SSL.4</u>: The TOE provides a logout option for users to terminate their own sessions when they choose. The ability to logout is available on the TOE Web session and CLI. • <u>FTA_TAB.1</u>: The TOE can be configured to display administrator-defined advisory banners when administrators successfully establish interactive sessions with the TOE, which include the CLI (console and SSH) access to both NGIPSv and FMC, and the WebUI (TLS) access to FMC.
<p>FTP_ITC.1 FTP_TRP.1/Admin</p>	<p>The TOE can be configured to transmit audit records to an external audit server. In order to protect exported audit records from disclosure or modification, the TOE utilizes syslog over TLS connections. The TLS provides authentication, key exchange, encryption and integrity protection of the data. For every audit event generated, the TOE stores it locally and sends it to the audit server. All the cryptographic algorithms and functions for TLS are provided by CiscoSSL.</p> <p>To support secure remote administration, the TOE includes implementations of SSHv2 (by OpenSSH) and HTTPS (HTTP over TLS, by CiscoSSL). In each case, a remote host (presumably acting on behalf of an administrator) can initiate a secure remote connection for the purpose of security management. Note that only the local console is available by default and each of these remote administration interfaces can be independently enabled by an administrator. For added security, only these security protocols and ports 22 and 443 are enabled and allowed by default. The administrators can also setup an access list to restrict only allowed IP addresses to access the TOE.</p> <p>In the cases of SSHv2 and HTTPS, the TOE offers both a secure command line interface (CLI) and a graphical user interface (GUI) interactive administrator sessions. An administrator with appropriate SSHv2 or HTTPS capable clients can establish secure remote connections with the TOE. However, to successfully establish such an interactive session, the administrator must be able to provide acceptable user credentials (e.g., user name and password), after which they will be able to issue commands or actions within their assigned authorizations.</p> <p>All of the security protocols are supported by the cryptographic operations included in the TOE implementation. Section 7.3 lists the CAVP certificates for all of the FIPS-certified algorithms.</p> <p>The Trusted Path/Channels function is designed to satisfy the following security functional requirements:</p> <ul style="list-style-type: none"> • <u>FTP_ITC.1</u>: The TOE can be configured to use TLS to ensure that any transmitted audit records are protected from tampering, and are sent only to the configured audit server so they are not subject to inappropriate disclosure or modification. • <u>FTP_TRP.1</u>: The TOE provides SSH and HTTPS, using FIPS-certified cryptographic algorithms, to support secure remote administration. In each case, the administrator can initiate the remote session, the remote session is secured (disclosure and modification) using FIPS certified cryptographic operations, and all remote security management functions require the use of one of these secure channels.

TOE SFRs	How the SFR is Satisfied
Security Functional Requirements Drawn from mod_ips_v1.0	
FAU_GEN.1[IPS] FAU_SAR.1[IPS] FAU_SAR.2[IPS] FAU_SAR.3[IPS] FAU_STG.1[IPS]	<p>The TOE will generate an event log for each intrusion event that occurs (also referred to as an intrusion event). Each event log will include a record of the date, time, type of exploit, and contextual information about the source of the attack and its target. For packet-based events, a copy of the packet or packets that triggered the event is also recorded. Managed Sensors will transmit their events to the FMC where the administrators can view the aggregated data and gain a greater understanding of the attacks against the entire network. The administrators can also deploy the managed Sensors in inline allowing them to configure the Sensors to drop or modify packets that are harmful.</p> <p>The web-based UI is the only way to view the intrusion events (Analysis > Intrusions > Events). The list below describes the intrusion event information that can be viewed, searched, filtered, and sorted by the system. In addition, basic contents such as date, time, and type can also be used to filter and sort. Note only Administrators and Intrusion Admins have access to the intrusion events.</p> <p>Access Control Policy</p> <p>The access control policy associated with the intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event is enabled.</p> <p>Access Control Rule</p> <p>The access control rule that invoked the intrusion policy that generated the event. Default Action indicates that the intrusion policy where the rule is enabled is not associated with a specific access control rule but, instead, is configured as the default action of the access control policy.</p> <p>This field is blank if intrusion inspection was associated with neither an access control rule nor the default action, for example, if the packet was examined by the default intrusion policy.</p> <p>Application Protocol</p> <p>The application protocol, if available, which represents communications between hosts detected in the traffic that triggered the intrusion event.</p> <p>Application Risk</p> <p>The risk associated with detected applications in the traffic that triggered the intrusion event: Very High, High, Medium, Low, and Very Low. Each type of application detected in a connection has an associated risk; this field displays the highest risk of those.</p> <p>Count</p> <p>The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows. This field is not searchable.</p> <p>Destination Continent</p> <p>The continent of the receiving host involved in the intrusion event.</p> <p>Destination Country</p> <p>The country of the receiving host involved in the intrusion event.</p>

TOE SFRs	How the SFR is Satisfied
	<p>Destination IP</p> <p>The IP address used by the receiving host involved in the intrusion event.</p> <p>Destination Port / ICMP Code</p> <p>The port number for the host receiving the traffic. For ICMP traffic, where there is no port number, this field displays the ICMP code.</p> <p>Destination User</p> <p>The User ID for any known user logged in to the destination host.</p> <p>Device</p> <p>The managed Sensor where the access control policy was deployed.</p> <p>Domain</p> <p>The domain of the Sensor that detected the intrusion. This field is only present if you have ever configured the Firepower Management Center for multitenancy.</p> <p>Egress Interface</p> <p>The egress interface of the packet that triggered the event. This interface column is not populated for a passive interface.</p> <p>Egress Security Zone</p> <p>The egress security zone of the packet that triggered the event. This security zone field is not populated in a passive deployment.</p> <p>Generator</p> <p>The component that generated the event.</p> <p>Ingress Interface</p> <p>The ingress interface of the packet that triggered the event. Only this interface column is populated for a passive interface.</p> <p>Ingress Security Zone</p> <p>The ingress security zone of the packet that triggered the event. Only this security zone field is populated in a passive deployment.</p> <p>Inline Result</p> <p>Actions</p> <p>Intrusion Policy</p> <p>The intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event was enabled.</p> <p>Message</p> <p>The explanatory text for the event. For rule-based intrusion events, the event message is pulled from the rule.</p> <p>Priority</p>

TOE SFRs	How the SFR is Satisfied
	<p>The event priority as determined by the Cisco Talos Security Intelligence and Research Group (Talos). The priority corresponds to either the value of the priority keyword or the value for the classtype keyword.</p> <p>For other intrusion events, the priority is determined by the decoder or preprocessor. Valid values are high, medium, and low.</p> <p>Protocol (search only)</p> <p>The name or number of the transport protocol used in the connection.</p> <p>Snort ID (search only)</p> <p>Specify the Snort ID (SID) of the rule that generated the event or, optionally, specify the combination Generator ID (GID) and SID of the rule, where the GID and SID are separated with a colon (:) in the format GID:SID.</p> <p>Source Continent</p> <p>The continent of the sending host involved in the intrusion event.</p> <p>Source Country</p> <p>The country of the sending host involved in the intrusion event.</p> <p>Source IP</p> <p>The IP address used by the sending host involved in the intrusion event.</p> <p>Source Port / ICMP Type</p> <p>The port number on the sending host. For ICMP traffic, where there is no port number, this field displays the ICMP type.</p> <p>Source User</p> <p>The User ID for any known user logged in to the source host.</p> <p>The intrusion events cannot be modified but they can be deleted by the Administrators or Intrusion Admins who have restricted access. When the intrusion events storage is full, the newest data will overwrite the oldest data.</p> <p>There is a feature called Threshold where the administrators can control the number of events that are generated per rule over time. They can limit notification to the specified number of event instances per time period or provide notification once per time period after a specified number of event instances. The administrator must specify if the event instances will be tracked by source or destination IP address, the count or the number of event instances, and the number of seconds for the time period for which event instances are tracked.</p> <p>Note the IPS function cannot be disabled unless the whole system is shutdown. The TOE also will generate all of the required auditable events identified in Table 16 (for FMT_SMF.1/IPS and IPS_NTA_EXT.1 only). All other events in Table 16 are addressed by intrusion events, not auditable events. Please see the CC Supplemental User Guide for more details.</p> <p>The Security Audit function is designed to satisfy the following security functional requirements:</p>

TOE SFRs	How the SFR is Satisfied
	<ul style="list-style-type: none"> • <u>FAU_GEN.1/IPS</u>: The TOE can be configured to generate intrusion events. In addition, all management functions are audited as well. There are certain header fields that should not be used to trigger intrusion events (in Inline mode or Passive mode). Logging events related to these fields would generate a deluge of intrusion audit records that would prevent IPS analysts from figuring out what security incidents occur in their monitored network. In addition, logging these fields will provide no benefits. Per version 2.11 of IPS EP, the following fields can be inspected and if in inline mode, dropped or modified (i.e., normalized): <ul style="list-style-type: none"> - All checksum fields - TCP Reserved field - TCP Urgent Pointer field <p>In inline mode, the TOE can count invalid checksum packets that are dropped. The TOE can also count the packets that gets normalized or dropped because of failed normalization.</p> • <u>FAU_SAR.1</u>: The TOE can allow administrators to view the intrusion events. • <u>FAU_SAR.2</u>: The TOE can restrict the viewing of intrusions events to authorized administrators. • <u>FAU_SAR.3</u>: The TOE can search and/or filter the intrusion events based on certain attributes. • <u>FAU_STG.1</u>: The TOE can protect the intrusion events from unauthorized modification and deletion.
FMT_SMF.1/IPS[IPS]	<p>The Administrators can deploy intrusion policy with intrusion rules to any interface. An interface, however, can only have one policy applied to that interface. The Administrators can also import vendor-defined signatures from Cisco, create their own intrusion rules, create rules to define which traffic is inspected and analyzed, enable anomaly rules/detections, modify thresholds and threshold duration, and configure known-good/known-bad. The Administrators or Intrusion Admins can create, modify, or delete intrusion policies but only the Administrators can deploy the policies. Here are the security roles in addition to the all-powerful “Administrator” role.</p> <ul style="list-style-type: none"> • “IPS Administrator” (or Administrator): Have all privileges and access • “IPS Analyst” (or Intrusion Admin): Have all access to intrusion policies and network analysis privileges but cannot deploy policies • Access Admin: Have all access to access control policies but cannot deploy policies • Discovery Admin: Have all access to network discovery, application detection, and correlation features but cannot deploy policies • Security Analyst: Have all access to security event analysis feature <p>The Security Management function is designed to satisfy the following security functional requirements:</p> <ul style="list-style-type: none"> • <u>FMT_SMF.1/IPS</u>: The TOE can manage the IPS functions.

TOE SFRs	How the SFR is Satisfied
	<ul style="list-style-type: none"> • <u>FMT_MOF.1/IPS</u>: The TOE can restrict the IPS functions to authorized administrators. • <u>FMT_MTD.1/IPS</u>: The TOE can restrict the IPS data including policies and rules to authorized administrators. • <u>FMT_SMR.2/IPS</u>: The TOE can provide additional IPS roles to manage the system.
<p>IPS_ABD_EXT.1[IPS] IPS_IPB_EXT.1[IPS] IPS_NTA_EXT.1[IPS] IPS_SBD_EXT.1[IPS]</p>	<p>The TOE provides network analysis and intrusion policies as part of the NGIPSv's intrusion detection and prevention system. The term "intrusion detection" generally refers to the process of passively analyzing network traffic for potential intrusions and storing attack data for security analysis. The term "intrusion prevention" includes the concept of intrusion detection, but adds the ability to block or alter malicious traffic as it travels across the network.</p> <p>In an intrusion detection/prevention deployment, the TOE examines packets as such:</p> <ul style="list-style-type: none"> • A <u>network analysis policy</u> governs how traffic is decoded and preprocessed so it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt. • An <u>intrusion policy</u> uses intrusion and preprocessor rules (sometimes referred to collectively as intrusion rules) to examine the decoded packets for attacks based on patterns or signatures. <p>Without decoding and preprocessing, the TOE could not appropriately evaluate traffic for intrusions because protocol differences would make pattern matching impossible.</p> <p>Before traffic can be inspected by intrusion policies, the TOE enforces any defined Security Intelligence (SI) policy, which consists of one or more known-good entries in a "Do-Not-Block List" and/or one or more known-bad entries in a "Block List". An IP address in a Do-Not-Block List or Block List matches a packet if the IP address in the list matches either the source address or the destination address in the packet. Entries in the Block List take precedence over entries in the Do-Not-Block List, so if the same IP address appears in both lists, the action for the Block List is applied. Matching a Do-Not-Block List entry results in skipping further IPS inspection, and is generally used to avoid false-positive IPS alerts for known-good addresses. Matching a Block List entry results in dropping the packet with no further IPS inspection, and is generally used to minimize impacts (alerts, and use of system resources) related to IPS inspection for traffic to/from known malicious entities. IPS Policy elements like URLs and domain names can also be configured like IP addresses described above.</p> <p>A network analysis policy governs packet processing in phases. First the system decodes packets through the first three TCP/IP layers, then continues with normalizing, preprocessing, and detecting protocol anomalies:</p> <ul style="list-style-type: none"> • The packet decoder converts packet headers and payloads into a format that can be easily used by the preprocessors and later, intrusion rules. Each layer of the TCP/IP stack is decoded in turn, beginning with the data link layer and continuing through the network and transport layers. The packet decoder also detects various anomalous behaviors in packet headers. • The inline normalization preprocessor reformats (i.e., normalizes) traffic to minimize the chances of attackers evading detection. It prepares packets for examination by other

TOE SFRs	How the SFR is Satisfied
	<p>preprocessors and intrusion rules, and helps ensure that the packets the system processes are the same as the packets received by the hosts on your network.</p> <ul style="list-style-type: none"> • Various network and transport layers preprocessors detect attacks that exploit IP fragmentation, perform checksum validation, and perform TCP and UDP session preprocessing. • Various application-layer protocol decoders normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the system to effectively apply the same content-related intrusion rules to packets whose data is represented differently, and to obtain meaningful results. • Several preprocessors allow administrators to detect specific threats, such as IP/TCP/UDP/ICMP portscans, ICMP/TCP flooding, DoS attacks and other rate-based attacks (“frequency”). The administrator can configure threshold that mimics normal expected frequency and configure the TOE to detect and drop events exceeding the configured thresholds. <p>Administrators can configure anomaly-based IPS functionality using two main methods:</p> <ul style="list-style-type: none"> • Enabling preprocessor inspection of specified protocols (as described in the bullets above) to ensure the traffic properly conforms to the protocol standards; • Enabling rules to allow certain types of known-good/normal/baseline traffic while also enabling rate-based attack prevention for those rules to alert and/or block the otherwise ‘normal’ traffic when the traffic exceeds specified rate limits (e.g. to permit HTTP between specified hosts/networks except when the rate of new HTTP sessions exceeds an admin-defined number of new sessions within an admin-defined period of time). Rate-based detection (i.e., Frequency) can be enabled or disabled for each rule by configuring the “Dynamic State” of any rule to define a rate limit in terms of an admin-specified count of how many times the rule is triggered within an admin-specified number of seconds at which point a new rule “state” will be applied. For example, if the normal state of the rule is to allow the traffic (with or without generating an event message), when the rate-based limit is reached the rule state could be configured to dynamically changed to drop the traffic (with or without generating an event message) until an admin-specified rate-based timeout is reached, at which point the rule state will revert to its normal setting until the rate-based limit is triggered again. <p>When the system identifies a possible intrusion, it generates an intrusion or preprocessor event (sometimes collectively called intrusion events). Managed Sensors transmit their events to the Firepower Management Center, where the administrators can view the aggregated data and gain a greater understanding of the attacks against their network assets. In an inline deployment, managed Sensors can also drop or replace packets that are known to be harmful.</p> <p>Each intrusion event in the database includes an event header and contains information about the event name and classification; the source and destination IP addresses; ports; the process that generated the event; and the date and time of the event, as well as contextual information about the source of the attack and its target. For packet-based events, the TOE also logs a copy of the decoded packet header and payload for the packet or packets that triggered the event.</p>

TOE SFRs	How the SFR is Satisfied
	<p>The packet decoder, the preprocessors, and the intrusion rules engine can all cause the TOE to generate an event. For examples,</p> <ul style="list-style-type: none"> • If the packet decoder (configured in the network analysis policy) receives an IP packet that is less than 20 bytes, which is the size of an IP datagram without any options or payload, the decoder interprets this as anomalous traffic. If, later, the accompanying decoder rule in the intrusion policy that examines the packet is enabled, the system generates a preprocessor event. • If the IP defragmentation preprocessor encounters a series of overlapping IP fragments, the preprocessor interprets this as a possible attack and, when the accompanying preprocessor rule is enabled, the system generates a preprocessor event. • Within the intrusion rules engine, most intrusion rules are written so that they generate intrusion events when triggered by packets. Please see section 7.1 for more details on Snort rule. <p>Until the administrator deploy new policies to the network interface, rules in the currently deployed intrusion policies behave as follows:</p> <ul style="list-style-type: none"> • Disabled rules remain disabled. • Rules set to Generate Events continue to generate events when triggered. • Rules set to Drop and Generate Events continue to generate events and drop offending packets when triggered. <p>The administrator can set thresholds for individual rules, per intrusion policy, to limit the number of times the system logs and displays an intrusion event based on how many times the event is generated within a specified time period. This can prevent the TOE from being overwhelmed with a large number of identical events.</p> <p>The TOE can also be configured to use intrusion rules to detect various attacks such as Teardrop, Bonk, Ping of Death, etc. The administrators can use pre-defined rule or create custom rule to detect these attacks and many more. For example, default rules can be enabled to identify common patterns of sensitive data such as credit card numbers, social security numbers, etc., and custom rules can be created to search for other patterns or specific strings or values.</p> <p>Custom IPS inspection rules (“Intrusion Rules”) can be created (under Objects > Intrusion Rules > Create Rule) with the following properties:</p> <ul style="list-style-type: none"> • Action (alert or pass) • Protocol (icmp, ip, tcp, or udp) • Direction (directional or bidirectional) • Source IP(s) • Source Port • Destination IP(s) • Destination Port • Detection Options (a drop-down list of packet fields and flags, each of which can be defined to match specific values or strings, and multiple detection options can be combined within the same rule). <p>To define string-based pattern-matching within a custom Intrusion Rule, select the “content” Detection Option, then enter the pattern in the available field using regular express (regex) syntax, and optionally indicate if the matching should be case insensitive,</p>

TOE SFRs	How the SFR is Satisfied
	<p>and/or whether the search should be performed within a specified location within the packet payload (beyond the first 4 bytes of an ICMP packet, beyond the first 20 bytes of a TCP header, or beyond the first 8 bytes of a UDP header), or on the entire payload (the default search option if no payload location is specified).</p> <p>The custom Intrusion Rules described above can be used to detect use of application protocol-specific commands, but the easier option would be to use a Network Analysis Policy (NAP), which contains application protocol-specific settings for several application protocols (e.g. for FTP, HTTP, etc.). There are default Network Analysis Policies that can be customized, or new policies can be created by copying one of the default policies as a new NAP with a new name, then assigning that new NAP to an ACP. Each NAP contains application protocol settings for:</p> <ul style="list-style-type: none"> • FTP and Telnet Configuration: Allows customizing lists of File Get Commands, File Put Commands, and Additional FTP Commands, as well as other command validity checks. • HTTP Configuration: Allows customizing a list of HTTP Methods. Matching of URLs/URIs, other strings, or web page content can be defined using custom intrusion rules, and/or URL known-good/known-bad lists. • SMTP Configuration: Allows enabling SMTP state inspection (enabled by default), and customizing lists of Custom Commands, Invalid Commands, Valid Commands, Data Commands, Binary Data Commands, Authentication Commands, etc. <p>Custom rules can be enabled or disabled within any Intrusion Policy along with other pre-defined inspection rules. For more details refer to the CC Supplemental User Guide and/or the <i>Firepower Management Center Configuration Guide</i>, chapter <i>Intrusion Detection and Prevention</i>, in either section <i>Sensitive Data Detection</i>, or section <i>The Intrusion Rules Editor</i>.</p> <p>The administrator can configure the Sensor to use its Giga Ethernet networks in either a passive or inline deployment. In a passive IPS deployment, the Sensor monitors traffic flowing across a network using a switch SPAN or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This provides the system visibility within the network without being in the flow of network traffic. When configured in a passive deployment, the system cannot take certain actions such as blocking or shaping traffic. The administrator can configure one or more physical ports on a managed Sensor as passive interfaces and deploy the intrusion policy to that interface via security zone (i.e., the interface is added to the zone). In an inline IPS deployment, the administrator configures the Sensor transparently on a network segment by binding two ports together. The administrator can configure one or more physical ports on a managed Sensor as inline interfaces then assign a pair of inline interfaces to an inline set. The intrusion policy is then deployed to that inline set via security zone.</p> <p>The management interface (typically eth0) is separate from the other data monitoring interfaces (used as passive or inline) on the Sensor. It is used to set up and register the Sensor to the FMC.</p> <p>The Intrusion Prevention function is designed to satisfy the following security functional requirements:</p> <ul style="list-style-type: none"> • <u>IPS ABD EXT.1</u>: The TOE can be configured to detect anomalies and rate-based attacks, and generate alert and/or drop the packets.

TOE SFRs	How the SFR is Satisfied
	<ul style="list-style-type: none"><li data-bbox="524 268 1455 327">• <u>IPS_IPB_EXT.1</u>: The TOE can be configured to support known-good and/or known-bad lists.<li data-bbox="524 348 1455 541">• <u>IPS_NTA_EXT.1</u>: The TOE can perform network analysis and deploy intrusion policies to any data monitoring interface as described above. The policy hierarchy order is not configurable and follows this order: Security Intelligence (the known-bad list takes precedence over the known-good list), anomaly-based rules, then signature-based rules. Conformance with protocols identified throughout the discussion of IPS is demonstrated by protocol compliance testing by the vendor.<li data-bbox="524 562 1455 684">• <u>IPS_SBD_EXT.1</u>: The TOE can support signature-based detection using intrusion rules including attributes in the headers and data payload. In addition, port/protocol scanning and flood attacks can be detected and blocked (if configured) as well.

7 SUPPLEMENTAL TOE SUMMARY SPECIFICATION INFORMATION

7.1 Intrusion Rule Definition

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

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

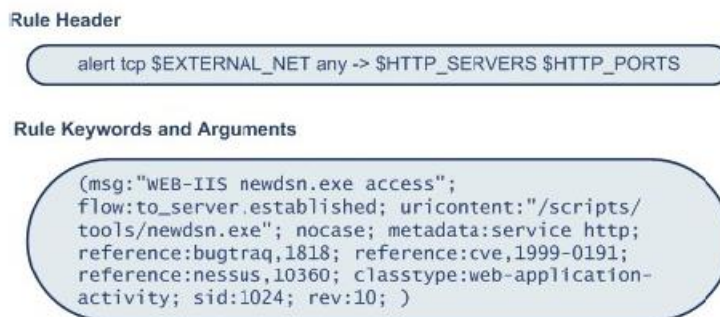
- the rule's action or type
- the protocol
- the source and destination IP addresses and netmasks
- direction indicators showing the flow of traffic from source to destination
- the source and destination ports

The rule options section contains:

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

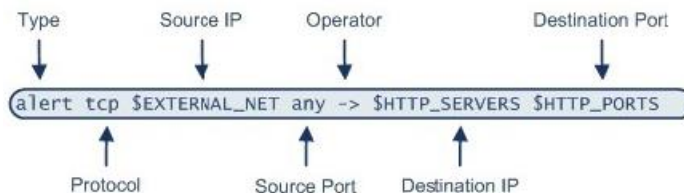
The following diagram illustrates the parts of a rule:

For example,



7.1.1 Intrusion Rule Header

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



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

Protocol (*tcp*) – Tests TCP traffic only. ICMPv4, ICMPv6, IPv4, IPv6, TCP and UDP protocols are supported.

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

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

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

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

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

7.1.2 Intrusion Rule Options and Keywords

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

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

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

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

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

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

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

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

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

The *itype* keyword: Specify the ICMP type.

The *icode* keyword: Specify the ICMP code.

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

The *ip_proto* keyword: Specify the IP protocol number.

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

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

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

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

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

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

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

7.2 TOE Key Zeroization

The following table describes the key zeroization referenced by FCS_CKM.4 provided by the TOE.

Table 22: TOE Key Zeroization

Name	Generation/ Algorithm	Purpose	Storage Location	Zeroization Summary
RSA public/private keys	DRBG	Identity certificates for the security appliance itself and also used in TLS, and SSH negotiations. The security appliance supports 2048 bit modulus key sizes or higher.	Private Key – hard disk (plaintext) and RAM (plain text) Public Key – hard disk (plaintext) and RAM (plain text)	Private Key - are zeroized then deleted from hard disk when the CA certificates are deleted by the administrators. Public Key - are deleted from hard disk when the CA certificates are deleted by the administrators.
Diffie-Hellman Key Pairs	DRBG	Key agreement for TLS, and SSH sessions.	RAM (plain text)	Keys in RAM are zeroized upon resetting (i.e., terminating all sessions) or rebooting the TOE.
RSA public/private keys	RSA	For communication between the FMC and managed Sensor.	Hard disk (plain text)/RAM (plain text)	Private Key - The private key is zeroized when the FMC and managed Sensors are de-registered.
TLS Session Keys	DH / DRBG Algorithm: AES	Used in HTTPS connections	RAM (plain text)	Keys in RAM are zeroized upon rebooting the TOE.
SSH Session Keys	DH / DRBG Algorithm: AES	SSH keys	RAM (plain text)	Keys in RAM are zeroized upon rebooting the TOE.

Name	Generation/ Algorithm	Purpose	Storage Location	Zeroization Summary
Passwords	User generated	Critical security parameters used to authenticate the administrator login.	Hard disk (Hashed with SHA-512 and salt value)	Passwords are not stored in plaintext. Only the hashed of the passwords and a 32-bit nonces are stored.
Certificates of Certificate Authorities (CAs) [FMC Only]	DRBG	Necessary to verify certificates issued by the CA. Install the CA's certificate prior to installing subordinate certificates.	Hard disk (plain text) and RAM (plain text)	CA certificates are zeroized from hard disk when the CA certificates are deleted by the administrators. CA certificates in RAM will be zeroized upon rebooting the TOE.
PRNG Seed Key	Entropy	Seed key for DRBG	RAM (plain text)	Seed keys are zeroized and overwritten with the generation of new seed

7.3 CAVP Certificate Equivalence

The TOE models, processors, and cryptographic modules included in the evaluation are shown in the following table. These cryptographic modules are commonly referred to as FOM (FIPS Object Modules). Though the name of some of the cryptographic implementations includes the word “module”, the FIPS certificates listed below are from the NIST CAVP (Cryptographic Algorithm Validation Program), not the NIST CMVP (Cryptographic Module Validation Program). The CAVP-certified cryptographic implementations of the TOE are listed in the table below (Table 23) along with the CPU for which they were certified, and the TOE component on which they’re used. The table on the following page (Table 24) lists the CAVP certificate numbers for each cryptographic implementation for each applicable SFR.

Table 23: Processors and Implementations

CPU Family	CPU Model (Microarchitecture)	FOM	Physical Appliances	CAVP Cert#
NGIPSv				
Intel Xeon Scalable w/ Linux 4 on ESXi 6.7/7.0	Intel Xeon Bronze 3104 (Skylake) w/ Linux 4 on ESXi 6.7/7.0	CiscoSSL FOM 7.3sp	UCSC-C220-M5, UCSC-C240-M5 and UCSC-C480-M5	A2952

CPU Family	CPU Model (Microarchitecture)	FOM	Physical Appliances	CAVP Cert#
	Intel Xeon Silver 4110 (Skylake) w/ Linux 4 on ESXi 6.7/7.0		UCSC-C220-M5, UCSC-C240-M5 and UCSC-C480-M5	
	Intel Xeon® Gold 6128 (Skylake) w/ Linux 4 on ESXi 6.7/7.0		UCSC-C220-M5, UCSC-C240-M5 and UCSC-C480-M5	
	Intel Xeon Platinum 8153 (Skylake) w/ Linux 4 on ESXi 6.7/7.0		UCSC-C220-M5, UCSC-C240-M5 and UCSC-C480-M5	
Intel Xeon D w/ Linux 4 on ESXi 6.7/7.0	Intel Xeon D-1528 (Broadwell) w/ Linux 4 on ESXi 6.7/7.0		UCS-E160S-M3	
	Intel Xeon D-1548 (Broadwell) w/ Linux 4 on ESXi 6.7/7.0		UCS-E180D-M3	
FMC				
Intel Xeon E5- 2600 v4	Intel Xeon E5-2620 v4 (Broadwell)	CiscoSSL FOM 7.3sp	FMC4500	A2585
	Intel Xeon E5 2640 v4 (Broadwell)		FMC1000 and FMC2500	
Intel Xeon Skylake	Intel Xeon Silver 4110 (Skylake)		FMC1600 and FMC2600	
	Intel Xeon Silver 4116 (Skylake)		FMC4600	
FMCv				

CPU Family	CPU Model (Microarchitecture)	FOM	Physical Appliances	CAVP Cert#
Intel Xeon Scalable w/ Linux 4 on ESXi 6.7/7.0	Intel Xeon Bronze 3104 (Skylake) w/ Linux 4 on ESXi 6.7/7.0	CiscoSSL FOM 7.3sp	UCSC-C220-M5, UCSC-C240-M5 and UCSC-C480-M5	A2952
	Intel Xeon Silver 4110 (Skylake) w/ Linux 4 on ESXi 6.7/7.0		UCSC-C220-M5, UCSC-C240-M5 and UCSC-C480-M5	
	Intel Xeon® Gold 6128 (Skylake) w/ Linux 4 on ESXi 6.7/7.0		UCSC-C220-M5, UCSC-C240-M5 and UCSC-C480-M5	
	Intel Xeon Platinum 8153 (Skylake) w/ Linux 4 on ESXi 6.7/7.0		UCSC-C220-M5, UCSC-C240-M5 and UCSC-C480-M5	
Intel Xeon D w/ Linux 4 on ESXi 6.7/7.0	Intel Xeon D-1528 (Broadwell) w/ Linux 4 on ESXi 6.7/7.0		UCS-E160S-M3	
	Intel Xeon D-1548 (Broadwell) w/ Linux 4 on ESXi 6.7/7.0		UCS-E180D-M3	

Table 24: Algorithm Certificate Numbers

Algorithm	SFR	CiscoSSL FOM 7.3sp (for FMC)	CiscoSSL FOM – Virtual 7.3sp (for NGIPSv/FMCv)
AES CBC 128/256 GCM 128/256	FCS_COP.1/DataEncryption	A2585	A2952
RSA 2048/3072 bits Signature Gen & Verify Key Gen	FCS_COP.1/SigGen FCS_CKM.1	A2585	A2952
DSA 2048/3072 bits	FCS_CKM.1	A2585	A2952
ECDSA curves P-256, P-384 and P-521 Key Sizes – 256, 384 and 521 bits Signature Gen & Verify Key Gen and Verify	FCS_COP.1/SigGen FCS_CKM.1	A2585	A2952
Hashing SHA-1, SHA-256, SHA-384, SHA-512	FCS_COP.1/Hash	A2585	A2952
Keyed Hash HMAC-SHA-1, HMAC-SHA-256	FCS_COP.1/KeyedHash	A2585	A2952

HMAC-SHA-384 HMAC-SHA-512			
DRBG (key size 256) CTR_DRBG(AES)	FCS_RBG_EXT.1	A2585	A2952
KAS ECC KAS FFC CVL	FCS_CKM.2	A2585	A2952

8 ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

Table 25: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, Version 3.1 Revision 5, CCMB-2017-04-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, Version 3.1 Revision 5, CCMB-2017-04-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, Version 3.1 Revision 5, CCMB-2017-04-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated April 2017, Version 3.1 Revision 5, CCMB-2017-04-004
[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

9 ANNEX B: NDcPP SFR TOE COMPONENTS MAPPING

The following mapping was provided to show which NDcPP SFRs are supported by which TOE component:

Table 26: SFR Mapping

Requirement	Description	Distributed TOE SFR Allocation
FAU_GEN.1	Audit Data Generation	All
FAU_GEN.2	User Identity Association	All
FAU_GEN_EXT.1	Security Audit Generation	All
FAU_STG_EXT.1	Protected Audit Event Storage	All
FAU_STG_EXT.4	Protected Local Audit Event Storage for Distributed TOEs	All
FAU_STG_EXT.5	Protected Remote Audit Event Storage for Distributed TOEs	All
FCO_CPC_EXT.1	Communication Partner Control	All
FCS_CKM.1	Cryptographic Key Generation	All
FCS_CKM.2	Cryptographic Key Establishment	All
FCS_CKM.4	Cryptographic Key Destruction	All
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)	All
FCS_COP.1/SigGen	Cryptographic Operation (Signature Verification)	All
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)	All
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)	All
FCS_HTTPS_EXT.1	Protocol Feature Dependent	FMC/FMCv only, not NGIPSv.
FCS_SSHS_EXT.1	SSH Server	All
FCS_TLSC_EXT.1	TLS Client Protocol without mutual authentication	All
FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication	All
FCS_TLSS_EXT.1	TLS Server	All

FCS_RBG_EXT.1	Random Bit Generation	All
FIA_AFL.1	Authentication Failure Management	All
FIA_PMG_EXT.1	Password Management	All
FIA_UIA_EXT.1	User Identification and Authentication	All
FIA_UAU_EXT.2	Password-based Authentication Mechanism	All
FIA_UAU.7	Protected Authentication Feedback	All
FIA_X509_EXT.1/ITT FIA_X509_EXT.1/Rev	X.509 Certification Validation	All
FIA_X509_EXT.2	X.509 Certificate Authentication	All
FIA_X509_EXT.3	Certificate Requests	All
FMT_MOF.1/ManualUpdate	Trusted Update - Management of Security Functions behaviour	FMC/FMCv only, not NGIPSv.
FMT_MTD.1/CoreData	Management of TSF Data	All
FMT_MTD.1/CryptoKeys	Management of TSF Data	All
FMT_SMF.1	Specification of Management Functions	FMC and FMCv (full set of management functions) and NGIPSv (subset of management functions)
FMT_SMR.2	Restrictions on Security Roles	All
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)	All
FPT_APW_EXT.1	Protection of Administrator Passwords	All
FPT_TST_EXT.1	Testing (Extended)	All
FPT_ITT.1	Basic internal TSF data transfer protection	All
FPT_STM_EXT.1	Reliable Time Stamps	All
FPT_TUD_EXT.1	Trusted Update	All
FTA_SSL_EXT.1	TSF-Initiated Session Locking	All
FTA_SSL.3	TSF-initiated Termination	All

FTA_SSL.4	User-Initiated Termination	All
FTA_TAB.1	Default TOE Access Banner	All
FTP_ITC.1	Inter-TSF Trusted Channel	All
FTP_TRP.1	Trusted Path	All