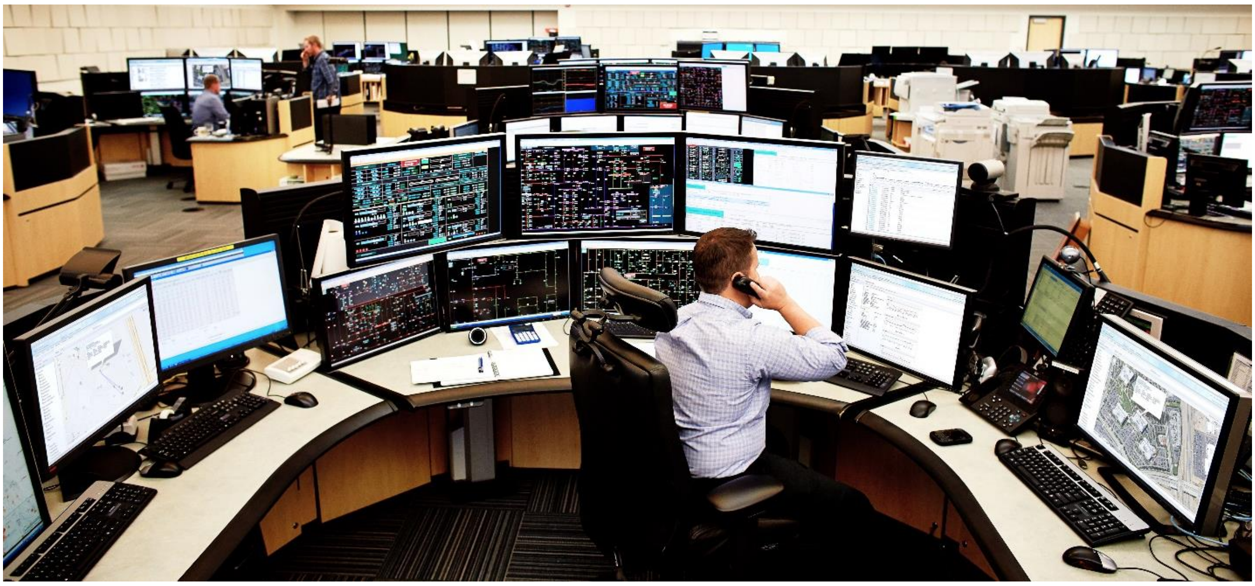


Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect

Security Target

ST Version 1.0

August 05, 2022

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

Table of Contents

List of Tables

List of Figures

DOCUMENT INTRODUCTION

Prepared By:

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Firepower Threat Defense (FTD). 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 and TOE Description [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]
- Rationale [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 3, Chapter 4.

1.1 ST and TOE Reference

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

Table 1: ST and TOE Identification

Name	Description
ST Title	Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect
ST Version	1.0
Publication Date	August 5, 2022
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect
TOE Software Version(s)	• FTD 6.4 • FXOS 2.6 • FMC 6.4 • AnyConnect 4.10
Keywords	Firewall, VPN Gateway, VPN Client

1.2 TOE Overview

The TOE is a distributed system of multiple components, which together provide firewall and VPN capabilities and centralized management. The TOE is comprised of Cisco Firepower Threat Defense (FTD) software running on Cisco Firepower security appliances that provide the firewall and VPN gateway functionality, and Firepower Management Center (FMC) software running on Cisco Firepower appliances that provide centralized management, and the AnyConnect Secure Mobility Client providing remote-access VPN functionality.

The TOE is comprised of software only, and includes the FMC 6.4, FTD 6.4, FXOS 2.6 and AnyConnect 4.10. The FMC, FTD, and FXOS software includes Cisco operating systems and Cisco applications that run on dedicated Cisco hardware appliances, which are outside the TOE boundary. The AnyConnect client is a software application that runs on a non-Cisco platform that is outside the TOE boundary.

The FMC provides a centralized management console and database repository for the Firepower devices which it manages (i.e., FTD). The FMC is a key component in the Cisco Firepower system. Administrators can use the FMC to manage multiple FTD appliances, and to aggregate, analyze, and respond to the threats they detect on their network. The FTD component of the TOE performs all traffic filtering (firewall) functionality by implementing access control policies (ACP) and VPN policies, which are all configured on the FMC and pushed to the FTD from the FMC. The AnyConnect component of the TOE is installed on remote workstations and allows remote VPN users to connect securely to one or more instances of FTD.

By using the FMC to manage multiple access control policies and VPN policies, FMC administrators can:

- Configure policies for all FTD appliances from a single location, making it easier to change configurations.
- Install software updates to the FMC itself and to FTD appliances.
- Push policies to FTD appliances and monitor their health status from the FMC.
- Define VPN policies for all peer-to-peer (e.g. FTD to FTD) and remote access (i.e. AnyConnect to FTD) connections.

1.2.1 TOE Product Type

The TOE consists of a number of software components which provide connectivity and security services on purpose-built appliances. The appliances running FTD include an instance of the Firepower eXtensible Operating System (FXOS), which loads the FTD applications that provide the Firewall and VPN Gateway functionality within the TOE. The appliance running FMC provides management functionality and centralized audit log collection for all managed FTD instances. The AnyConnect component of the TOE is software installed to a remote workstation to support remote access VPN client connections to FTD.

The FTD provides stateful packet filtering to control the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorized administrator for firewalls. This header information includes source and destination IP addresses, and the source and destination port numbers. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The stateful firewall remembers the state of the connection from information gleaned from prior packets flowing on the connection and uses it to regulate current packets. The packet will be denied if the security policy is violated.

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

The TOE also provides IPsec connection capabilities. All references within this ST to “VPN” connectivity refer to the use of IPsec tunnels to secure connectivity to and/or from the TOE, for example, site-to-site VPN or remote access VPN.

1.2.2 Supported non-TOE Hardware / Software / Firmware

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

Table 2: IT Environment Components

Component	Required	Usage/Purpose Description
Firepower Appliance	Yes	Firepower appliances supporting FTD 6.4: • Firepower 1000 Series (the same installation and patch files are used for all models in this series: 1010, 1120, and 1140) • Firepower 2100 Series (the same installation and patch files are used for all models in this series: 2110, 2120, 2130, and 2140) • Firepower 4100 Series and Firepower 9300 (the same installation and patch files are used for all models in the 4100 series (4110, 4120, 4140, 4150, 4115, 4125, and 4145) as well as for the 9300 and all its supported security modules (SM-24, SM-36, SM-44, SM-40, SM-48, and SM-56)).
FMC Appliance	Yes	FMC appliances that support FMC 6.4 (the same installation and patch files are used for all hardware models listed here): • FMC 1600, 2600, 4600 • FMC 1000, 2500, 4500 • FMC 2000, 4000 • FMC 750, 1500, 3500
VPN Peer	No	This includes any peer with which the TOE participates in VPN communications. VPN peers may be any device that supports IPsec communications. Both VPN clients and VPN gateways are considered VPN peers by the TOE. Note that one VPN client, AnyConnect, is considered part of the TOE, and multiple instances of FTD can act as VPN peers with each other.
VPN Client Platform	Yes	This includes the platform and OS (Windows 10) on which the AnyConnect software is installed. The CC evaluated configuration includes the AnyConnect client running on Microsoft Windows 10 x64 (64-bit).
Remote workstation including Web browser and SSH client	Yes	The following web browsers are supported for remote administrative access to the FMC and FCM (Firepower Chassis Manager running on MIO): Google Chrome; Mozilla Firefox; Microsoft Internet Explorer 11 (MS-Windows only) SSH clients must support SSHv2.
Remote Authentication Server	No	The TOE supports RADIUS.
NTP Server	No	The TOE supports communications with an NTP server, with support for NTPv3 recommended.
Peer Certificate Authority (CA)	Yes	The TOE relies on external CA servers to sign identity certificates for TOE components, and the TOE supports X.509v3 certificate revocation checking using external OCSP Responders and CRL distribution points.

Component	Required	Usage/Purpose Description
Syslog Server	No	The TOE supports UDP syslog (FMC, FTD, and MIO), TCP syslog (FTD), syslog over TLS (FTD).

1.3 TOE Description

1.3.1 TOE Evaluated Configuration

The TOE consists of software images (including operating systems and applications) and a software client application as specified in section 1.3.2 below. The TOE includes the Cisco FMC, FTD[1], MIO[2], and the Cisco AnyConnect VPN client.

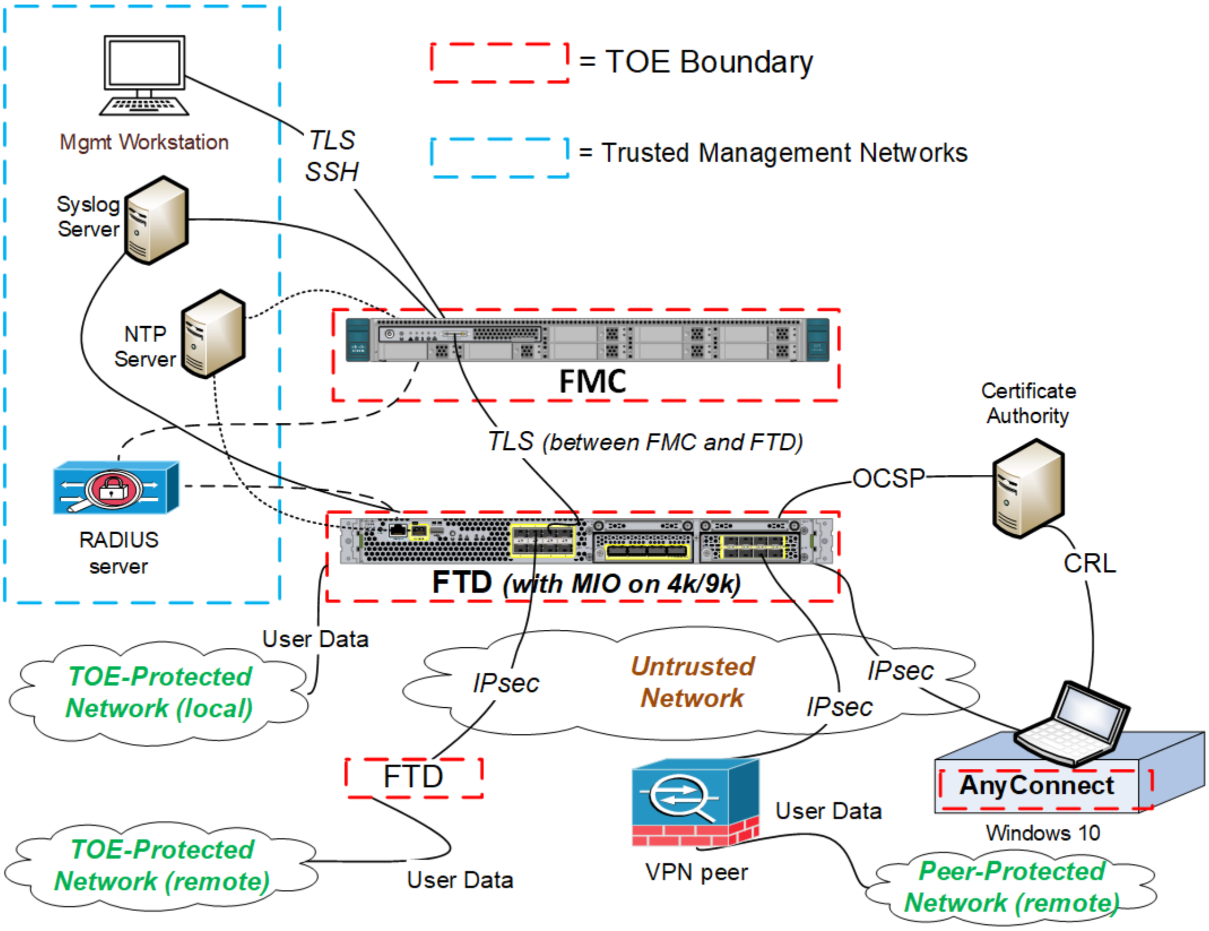
Administration of the TOE is performed by connecting to the WebUI on the FMC from a remote workstation with a TLS-enabled browser. The FMC allows management of multiple instances of FTD and provides centralized management of firewall and VPN policies and distribution of those policies to FTDs, and also provides centralized collection of firewall and VPN audit records from FTDs. The FMC, FTD, and MIO can also be configured to transmit their audit records to remote syslog servers and can use UDP syslog (FMC, FTD, and MIO), TCP syslog (FTD), or can be configured to secure syslog in either TLS (FMC and FTD) or IPsec (MIO). The FTD component of the TOE provides firewall functionality to filter network traffic to/from external entities using its IP traffic filtering and provides VPN functionality to encrypt traffic between itself and other IPsec gateways as well as the AnyConnect VPN client.

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line. The FMC can use a single network interface for all communications or can be configured to use multiple interfaces. Each instantiation of FTD has multiple network interfaces and is able to filter IP traffic to and through those interfaces. The AnyConnect client uses a single network interface from its underlying host.

[1] Depending on which underlying hardware platforms are used for FTD in the deployed TOE configuration, the deployed TOE will include one or more builds of FXOS. A minimally-featured build of FXOS runs the FTD applications on all platforms (1k, 2k, and on the SM in 4k/9k). A more fully-featured build of FXOS is only present on the 4k/9k platforms and runs in the chassis Supervisor Engine that is not present on the 1k/2k platforms.

[2] To help distinguish between the FXOS builds this document will refer to the FXOS build on the supervisor engine as “MIO” (Management Input/Output), and “FTD” will refer to the FXOS build that loads the FTD applications and also to the FTD applications themselves.

Figure 1: Example TOE deployment



The figure shown directly above includes the following:

- TOE components: FMC, FTD, MIO, and AnyConnect
- VPN Peer: Another instance of FTD, or a non-TOE peer (Operational Environment)
- Management Workstation (Operational Environment)
- AAA (RADIUS) server (Operational Environment)
- Certificate Authority CA / OCSP Responder (Operational Environment)
- Syslog server (Operational Environment)
- NTP server (Operational Environment)

1.3.2 Physical Scope of the TOE

The TOE is a software solution comprised of the components and documentation listed in Table 3. All software is downloadable from https://software.cisco.com. All documentation is downloadable from https://www.cisco.com:

Table 3: Models and Specifications

TOE Component
Firepower Management Center (FMC) 6.4 *Requires installation of initial FMC 6.4 release, 6.4.0-113, either as new installation (using *Restore.iso, or upgrade from an earlier release using the *Upgrade*.tar), plus installation of the latest *Patch*.tar).* *For all FMC hardware platforms:* • Cisco_Firepower_Mgmt_Center-6.4.0-113-Restore.iso

TOE Component
• Cisco_Firepower_Mgmt_Center_Upgrade-6.4.0-113.sh.REL.tar • Cisco_Firepower_Mgmt_Center_Patch-6.4.0.15-26.sh.REL.tar
Firepower Threat Defense (FTD) 6.4 *Requires installation of initial FTD 6.4 release (6.4.0-102) either as new installation (using *.SPA binary or *.csp binary), or upgrade from an earlier release (using the *Upgrade*.tar), and subsequent installation of the latest patch (using the *Patch*.tar).* *1000/1100 series (no upgrade available from previous FTD releases):* • cisco-ftd-fp1k.6.4.0-102.SPA • Cisco_FTD_SSP_FP1K_Patch-6.4.0.15-26.sh.REL.tar *2100 series:* • cisco-ftd-fp2k.6.4.0-102.SPA • Cisco_FTD_SSP_FP2K_Upgrade-6.4.0-102.sh.REL.tar • Cisco_FTD_SSP_FP2K_Patch-6.4.0.15-26.sh.REL.tar *4100/9300 series (no upgrade available from previous FTD releases):* • cisco-ftd.6.4.0.102.SPA.csp • Cisco_FTD_SSP_Patch-6.4.0.15-26.sh.REL.tar
Firepower eXtensible Operating System (FXOS) 2.6 *For the supervisor engine (MIO) on 4k/9k:* • fxos-k9.2.6.1.254.SPA
AnyConnect Secure Mobility Client 4.10 *AnyConnect can be installed using a “predeploy” package, or a “webdeploy” package. The “predeploy” package is downloaded from Cisco.com as a *.zip, and extracted on the Windows workstation as *.msi and *.exe files that are installed locally. The “webdeploy” package is downloaded from Cisco.com as a *.pkg (a compressed zip file), and uploaded by a TOE administrator to FMC, which copies it to FTD, from where it can be downloaded directly to a Windows workstation, and extracted on the Windows workstation as *.msi and *.exe files that are installed locally.* anyconnect-win-4.10.05111-predeploy-k9.zip **Preparative and Operational Guidance** *The CC guide is available as a PDF, downloadable from Cisco.com, and contains links to additional guidance documentation, also downloadable from Cisco.com.* • Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect Common Criteria Operational User Guidance and Preparative Procedures, version 1.0, Date August 5, 2022

1.3.3 Logical Scope of the TOE

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

1. Security Audit
2. Traffic Flow Control
3. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. TOE Access
7. Trusted Path/Channels

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

1.3.3.1 Security Audit

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. The administrator configures audit functionality and manages audit data storage. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail, and the TOE provides interfaces to review the audit trail.

1.3.3.2 Traffic Flow Control

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

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

1.3.3.3 Identification and Authentication

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

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

The TOE provides administrator authentication against a local user database using password-based authentication. Password-based authentication can be performed on the serial console or SSH and HTTPS interfaces. The SSHv2 interface on MIO also supports authentication using SSH keys. The TOE also supports use of single-use authentication by supporting use of AAA (RADIUS) servers (outside the TOE boundary), where RADIUS supports use of password-based, single-use, or multi-factor authentication.

1.3.3.4 Security Management

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

1.3.3.5 Protection of the TSF

The TOE is not a general-purpose operating system and access to the TOE memory space is restricted to only TOE functions. The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to authorized administrators. The TOE prevents reading of cryptographic keys and passwords by: not providing any administrative interface that allows viewing of stored keys or passwords; masking (e.g. with asterisks) any passwords entered by an administrator via administrative interfaces including authentication prompts; and protecting data in transit during inter-TSF communication (between FMC and FTD, and between AnyConnect and FTD), and during remote administration.

The TOE (FMC, FTD, and MIO) internally maintains the date and time, and uses internal clocks as the source for timestamps applied to audit records generated by the FMC, FTD, and MIO (AnyConnect does not generate audit messages relevant to this CC evaluation). Administrators can update the TOE’s clocks manually via FMC or MIO or can configure the TOE to update its clocks automatically via NTP.

The TOE supports IPsec VPN connections between TOE components, as peer-to-peer VPN tunnels between multiple instances of FTD, and remote access IPsec VPN tunnels from the AnyConnect component of the TOE to the FTD component of the TOE.

1.3.3.6 TOE Access

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

When an administrative session is initially established, the TOE displays an administrator-configurable warning banner. Display of login banners is also supported for VPN client (AnyConnect) sessions. These banners are used to provide any information deemed necessary by the administrator. After a configurable period of inactivity, administrative sessions and VPN client sessions will be terminated, requiring administrators to re-authenticate.

1.3.3.7 Trusted Path/Channels

The TOE supports establishing trusted paths between itself and remote administrators using SSHv2 for CLI access, and TLS/HTTPS for GUI access. The TOE supports use of TLS for connections with remote syslog servers (FTD supports syslog over TLS). The TOE (FTD) can establish trusted paths between itself and VPN gateways (either non-TOE gateways, or between instances of FTD) to establish peer-to-peer VPN tunnels using IPsec, and can establish remote-access IPsec VPN connections between AnyConnect and FTD. Where the TOE supports certificate-based authentication (including IPsec VPN communications, and authentication of syslog servers using TLS), the TOE components also support communications with certificate authorities (OCSP responders) via OCSP.

1.3.4 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 4: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Telnet for management purposes	Telnet passes authentication credentials in clear text and is disabled by default.
Firepower Device Manager (FDM)	Firepower Device Manager is a web-based local manager for FTD. FDM is automatically disabled on FTD when FTD is managed by FMC, as is the case with all Common Criteria evaluated TOE configurations.
Filtering of non-IP traffic provided by the EtherType option when configuring information flow policies is excluded from the evaluated configuration.	Use of non-IP traffic filtering is beyond the scope of this Common Criteria evaluation.
Smart Call Home. The Smart Call Home feature provides personalized, e-mail-based and web-based notification to customers about critical events involving their individual systems.	Use of Smart Call Home is beyond the scope of this Common Criteria evaluation.
FXOS REST API (on MIO only)	Allows users to programmatically configure and manage their chassis. Use of REST API is beyond the scope of this Common Criteria evaluation.
FMC REST API	Allows users to programmatically configure and manage their chassis. Use of REST API is beyond the scope of this Common Criteria evaluation.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The ST and the TOE it describes are conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017
  - Part 3 Conformant

The claimed assurance package is EAL4+ augmented with ALC_FLR.2.

2.2 Protection Profile Conformance

This ST claims no compliance to any Protection Profiles.

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. Policies are identified as P.policy with "policy" specifying a unique name.

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 5: TOE Assumptions

Assumption Name	Assumption Definition
A.NOEVIL	Authorized administrators are non-hostile, trained, and follow all administrator guidance.
A.PHYSEC	The hardware components on which the TOE's Firepower components are installed are kept physically secure.
A.PROTRA	The remote access VPN workstations on which the TOE's AnyConnect component is installed are issued and managed by the same organization that manages the other TOE components and are protected by physical and/or cryptographic means (e.g. disk/drive encryption).
A.PROTENV	The operational environment servers on which the TOE relies, including NTP, syslog, CA/OCSP/CRL, and RADIUS servers remain physically and logically protected from malicious activity.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

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 6: Threats

Threat Name	Threat Definition
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

Threat Name	Threat Definition
T.ASPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T.VPN	A malicious user or process may intercept traffic and cause TSF data to be inappropriately accessed (viewed, modified, or deleted) during transfer with a remote VPN endpoint (client or gateway).
T.UNAUTHORIZED	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNDETECTED	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following table, Organizational Security Policies, identifies the organizational security policies.

Table 7: Organizational Security Policies

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

4 SECURITY OBJECTIVES

This Chapter identifies the security objectives of the TOE and the operational environment. The security objectives identify the responsibilities of the TOE and the TOE's operational 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 operational 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 8: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
O.ACCOUNTABLE	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.AUDIT	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times.
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
O.MEDIATE	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.
O.PROCOM	The TOE will provide properly protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions and must ensure that only authorized administrators are able to access such functionality.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions or data.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.

TOE Security Objective	TOE Security Objective Definition
O.VPN	The TOE will provide a means to ensure VPN users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity. The TOE must be able to protect the integrity and confidentiality of VPN data.

4.2 Security Objectives for the Environment

The assumptions identified previously are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. The following table, Security Objectives for the Environment, identifies the security objectives for the environment.

Table 9: Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.NOEVIL	Authorized administrators are non-hostile, trained, and follow all administrator guidance.
OE.PHYSEC	The hardware components on which the TOE's Firepower components are installed are kept physically secure.
OE.PROTRA	The remote access VPN workstations on which the TOE's AnyConnect component is installed are issued and managed by the same organization that manages the other TOE components and are protected by physical and/or cryptographic means (e.g. disk/drive encryption).
OE.PROTENV	The operational environment servers on which the TOE relies, including NTP, syslog, CA/OCSP/CRL, and RADIUS servers remain physically and logically protected from malicious activity. The NTP, syslog, and RADIUS servers will be located on a trusted management network accessible from FMC, FTD, and MIO.
OE.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived verbatim from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated: April 2017 and all National Information Assurance Partnership (NIAP) and 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:

- Refinement: Indicated with **bold** text and strikethroughs (~~**bold**~~), if necessary;
- Selection: Indicated with [underlined] text in brackets;
- Assignment: Indicated with [*italicized*] text in brackets;
- Assignment within a Selection: Indicated with [*underlined and italicized*] text in brackets;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

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 10: Security Functional Requirements

SFR Component ID	Component Name
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FDP_IFC.1(1)	Subset information flow control
FDP_IFC.1(2)	Subset information flow control
FDP_IFF.1(1)	Simple security attributes
FDP_IFF.1(2)	Simple security attributes
FIA_AFL.1	Authentication failure handling
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1(1)	Management of security attributes

SFR Component ID	Component Name
FMT_MSA.1(2)	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic Internal TSF Data Transfer Protection
FPT_STM.1	Reliable time stamps
FTA_SSL.3	TSF-initiated Termination
FTA_TAB.1	Default TOE Access Banners
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1	Trusted Path

5.2.1 Security audit (FAU)

5.2.1.1 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) [*the events listed in Table 11*].

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, 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 11*].

Table 11: Auditable Events

SFR	Auditable Event	Additional Audit Record Content
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_SAR.1	None.	
FAU_STG.1	None.	
FAU_STG.4	None.	
FDP_IFC.1(*)	None.	
FDP_IFF.1(*)	All decisions on requests for information flow.	The presumed addresses of the source and destination subject. Application-specific attributes leading to a denial of flow.
FDP_IFF.1(2)	Errors during IPSec processing	The presumed addresses of the source and destination subject.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the	The identity of the offending user and the authorized administrator

SFR	Auditable Event	Additional Audit Record Content
	authorized administrator of the users' capability to authenticate.	
FIA_SOS.1	None.	
FIA_UAU.1	None.	
FIA_UAU.5	Any use of the authentication mechanism.	The user identities provided to the TOE
FIA_UAU.7	None.	
FIA_UID.2	All use of the user identification mechanism.	
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation
FMT_MSA.1(*)	None.	
FMT_MSA.3	None.	
FMT_SMF.1	All administrator actions.	
FMT_SMR.1	Modifications to the group of users that are part of the authorized administrator role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FPT_ITT.1	None.	
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation. The old and new values for the time. Origin of the attempt (e.g., IP address)
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_TAB.1	None.	
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	Identification of the claimed user identity.

5.2.1.2 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.

5.2.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [*authorized administrators*] with the capability to read [*all FMC audit trail data*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.1.4 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

5.2.1.5 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_IFC.1(1) Subset information flow control

FDP_IFC.1.1(1) The TSF shall enforce the [*FIREWALL SFP*] on: [

a) subjects: unauthenticated external IT entities that send and receive information through the TOE;

b) information: traffic sent through the TOE's data interfaces;

c) operations: forward or drop information].

5.2.2.2 FDP_IFC.1(2) Subset information flow control

FDP_IFC.1.1(2) The TSF shall enforce the [*VPN SFP*] on: [

a) subjects: IPsec VPN endpoints;

b) information: IP traffic associated with an IPsec security policy;

c) operations: encrypt, decrypt, or drop information].

5.2.2.3 FDP_IFF.1(1) Simple security attributes

FDP_IFF.1.1(1) The TSF shall enforce the [*FIREWALL SFP*] based on **at least** the following types of subject and information security attributes: [

a) subject security attributes:

- *presumed source address;*

b) information security attributes:

- *security zone associated with the TOE's ingress interface*
- *source IP address;*
- *destination IP address;*
- *transport layer protocol;*
- *TCP or UDP port number*].

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and **another** controlled ~~**information**~~ **subject** via a controlled operation if the following rules hold: [

- *An administratively-defined rule within an active policy (the Access Control Policy, including its associated Prefilter Policy) explicitly allows traffic matching any combination of information security attribute values.*]

FDP_IFF.1.3(1) The TSF shall enforce the [*none*].

FDP_IFF.1.4(1) The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow **if any of** the following rules **is met**: [

a) An administratively-defined rule within an active policy (the Access Control Policy, including its associated Prefilter Policy) that explicitly blocks traffic matching any combination of the information security attribute values is a higher priority rule within the policy than any rule that would explicitly allow the information flow;

b) The information received via the ingress interface contains a presumed address of the source subject that is known by the TOE's routing table to not be reachable via the ingress interface;

c) The presumed address of the source subject is a broadcast address;

d) The presumed address of the source subject is on a loopback network.]

5.2.2.4 FDP_IFF.1(2) Simple security attributes

FDP_IFF.1.1(2) The TSF shall enforce the [*VPN SFP*] based on the following types of subject and information security attributes: [

a) subject security attributes:

- *VPN endpoint identity;*
- *VPN endpoint authentication credentials;*

b) information security attributes:

- *source IP address;*
- *destination IP address;*
- *transport layer protocol;*
- *TCP or UDP port number*].

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and **another** controlled **~~information~~ subject** via a controlled operation if the following rules hold: [

a) The remote VPN endpoint (peer-to-peer gateway, or remote access client) must be successfully authenticated to the TOE before the TOE will permit information flow across the VPN;

b) The information security attribute values must match the administratively-defined information attribute values allowed in an active VPN policy].

FDP_IFF.1.3(2) The TSF shall enforce the [*following additional rules:*

a) Incoming encrypted VPN traffic shall be decrypted by the TOE prior to inspection of information security attributes;

b) Outgoing traffic that matches an active VPN policy shall be encrypted prior to transmission from the TOE to the remote VPN endpoint].

FDP_IFF.1.4(2) The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow **if any of** the following rules **is met**: [

a) The information flow would violate anti-spoofing controls, such that the information received via the ingress interface contains a presumed address of the source subject that is known by the TOE's routing table to not be reachable via the ingress interface;

b) The presumed address of the source subject is a broadcast address;

c) The presumed address of the source subject is on a loopback network.]

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [*FMC: 1-999; MIO and FTD: 1-10*]] unsuccessful authentication attempts occur related to [*administrators attempting to remotely access the TOE using password-based authentication and a locally-defined administrative account*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met (on FTD) or surpassed (on FMC)], the TSF shall [*prevent the offending account from successfully authenticating until the administratively-configurable lockout period has expired, or an authorized administrator unlocks the locked account*].

5.2.3.2 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

a) a minimum length of:

- *FMC WebUI: administratively configurable from 15-32 characters*
- *FMC CLI: 8 characters*
- *FTD: administratively configurable from 8-127 characters*
- *MIO: administratively configurable from 8-80 characters*

b) optionally, a minimum complexity that must include:

- *FMC WebUI: at least one uppercase alphabetic character, at least one lowercase alphabetic character, at least one numeric digit, and at least one special character.*
- *FMC CLI: at least one uppercase alphabetic character, at least one lowercase alphabetic character, at least one numeric digit, and at least one special character.*
- *FTD: at least one uppercase alphabetic character, at least one lowercase alphabetic character, at least one numeric digit, and at least one special character.*
- *MIO: at least one uppercase alphabetic character, at least one lowercase alphabetic character, and at least one special character*].

5.2.3.3 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [*initiation of TLS/HTTPS sessions, initiation of SSH sessions, initiation of console sessions, and initiation of IPsec sessions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.3.4 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [*password, RADIUS, and certificate-based authentication mechanisms*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*following multiple authentication mechanism rules:*

a) reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal or via remote administrative interfaces such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator;

b) if configured, RADIUS authentication mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal or remote administrative interfaces such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator;

c) if configured, reusable password mechanism shall be used for VPN users to access the TOE to establish a VPN session such that successful authentication must be achieved before allowing any other TSF-mediated actions;

d) if configured, certificate-based authentication mechanism shall be used for VPN users accessing the TOE to establish remote access VPN sessions such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that VPN user].

5.2.3.5 FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only *[obscured feedback]* to the user while the authentication is in progress at the local console.

5.2.3.6 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [<u>determine the behaviour of, disable, enable, modify the behaviour of</u>] the functions [*all functions listed in FMT_SMF.1*] to [*authorized administrators*].

5.2.4.2 FMT_MSA.1(1) Management of security attributes

FMT_MSA.1.1(1) The TSF shall enforce the [*FIREWALL SFP*] to restrict the ability to [<u>change_default, query, modify, delete</u>] the security attributes [*listed in section FDP_IFF1.1(1)*] to [*authorized administrators*].

5.2.4.3 FMT_MSA.1(2) Management of security attributes

FMT_MSA.1.1(2) The TSF shall enforce the [*VPN SFP*] to restrict the ability to [<u>change_default, query, modify, delete</u>] the security attributes [*listed in section FDP_IFF1.1(2)*] to [*authorized administrators*].

5.2.4.4 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [*FIREWALL SFP and VPN SFP*] to provide [restrictive] default values for **information flow** security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow [*the authorized administrator*] to specify alternative initial values to override the default values when an object or information is created.

5.2.4.5 FMT_SMF.1 Specification of Management Functions

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

a) start-up and shutdown the TOE;
b) create, delete, modify, and view information flow SFPs defined in FDP_IFF.1(1) and FDP_IFF.1(2);
c) create, delete, modify, local accounts and their credentials;
d) enable and disable remote (AAA) authentication mechanisms;
e) modify and set the threshold for the number of permitted authentication attempt failures;
f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures;
g) configure clock settings, including setting the time and date and configuring NTP;
h) configure local audit storage limits;
i) configure remote audit transmission;
j) enable and disable remote administration and restrict addresses from which remote administration can be performed;
k) install software updates to the TOE;
l) management of PKI attributes;
m) Configure the advisory warning message displayed prior to establishing an administrative or VPN client session;
n) Configure idle time limits for administrative sessions.
].

5.2.4.6 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [*authorized administrator, and VPN user*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

5.2.5.2 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.6 TOE Access (FTA)

5.2.6.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate **local and remote** interactive sessions after a [*authorized administrator-configurable time interval of session inactivity of up to 1440 minutes (24 hours) for FMC and FTD, up to 3600 seconds (1 hour) for MIO, and up to 1440 minutes (24 hours) for VPN clients*].

5.2.6.2 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing **~~a user~~ an administrative or VPN client** session the TSF shall display **an authorized administrator-configurable** advisory warning message regarding unauthorized use of the TOE.

5.2.7 Trusted Path/ Channels (FTP)

5.2.7.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF, another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [

a) *VPN connections with external peers via IPsec; and*
b) *exporting audit records to external servers via TLS (FTD)].*

5.2.7.2 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] **~~users~~ administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote ~~users~~ **administrators**] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial ~~user~~ **administrator** authentication, [*all remote administrative actions*]].

5.2.8 TOE SFR Dependencies

This section of the Security Target demonstrates that the identified TOE and IT Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. The following table lists the TOE Security Functional Components and the Security Functional Components each are dependent upon and any necessary rationale.

'N/A' in the Rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required.

Table 12: Security Functional Requirement

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Met by FAU_GEN. Met by FIA_UID.2
FAU_SAR.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_STG.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_STG.4	FAU_STG.1	Met by FAU_STG.1
FDP_IFC.1(1)	FDP_IFF.1	Met by FDP_IFF.1(1)
FDP_IFC.1(2)	FDP_IFF.1	Met by FDP_IFF.1(2)
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(1) Met by FMT_MSA.3
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(2) Met by FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	Met by FIA_UAU.1
FIA_UAU.1	FIA_UID.1	Met by FIA_UID.2
FIA_UAU.5	No dependencies	N/A
FIA_UAU.7	FIA_UAU.1	Met by FIA_UID.2
FIA_UID.2	No dependencies	N/A
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1(1) Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by FDP_IFC.1(2) Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Met by FMT_MSA.1 Met by FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	Met by FIA_UID.2
FPT_ITT.1	No dependencies	N/A
FPT_STM.1	No dependencies	N/A
FTA_SSL.3	No dependencies	N/A
FTA_TAB.1	No dependencies	N/A
FTP_ITC.1	No dependencies	N/A
FTP_TRP.1	No dependencies	N/A

5.3 TOE Security Assurance Requirements

The TOE assurance requirements for this ST are EAL4 Augmented with ALC_FLR.2 derived from Common Criteria Version 3.1, Revision 5. The Security Target Claims conformance to EAL4 Augmented with ALC_FLR.2. The assurance requirements are summarized in the table below.

Table 13: SAR Requirements

Assurance Class	Components	Components Description
Development	ADV_ARC.1	Architectural Design with domain separation and non-bypassability
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC _LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
	ALC_FLR.2	Flaw Reporting Procedures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

5.3.1 Security Assurance Requirements Rationale

This Security Target claims conformance to EAL4 Augmented with ALC_FLR.2. This target was chosen to ensure that the TOE has a 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. Augmentation was chosen to address having flaw remediation procedures and correcting security flaws as they are reported.

The level of security assurance exceeds that which was claimed in the PPs, basic robustness. This level of robustness was chosen for an international applicability. The chosen assurance level is consistent with the postulated threat environment. Specifically, the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low, and the product will have undergone a search for obvious flaws. This is supported by the inclusion of the AVA_VAN.3 requirement.

5.4 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 14: Assurance Measures

Component	How requirement will be met
ADV_ARC.1	The architecture of the TOE that is used to protect the TSF documented by Cisco in their development evidence.

Component	How requirement will be met
ADV_FSP.4	The externally visible interfaces of the TOE used by the users of the TOE along with the description of the security functions and a correspondence between the interfaces and the security functions from the ST are documented by Cisco in their development evidence. The development evidence also contains a tracing to the SFRs described in this ST.
ADV_IMP.1	Cisco provides access to the TSF implementation to the evaluation lab.
ADV_TDS.3	The design of the TOE will be described in the development evidence. This evidence will also contain a tracing to the TSFI defined in the FSP.
AGD_OPE.1	The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance.
AGD_PRE.1	Cisco documents 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.4	Cisco performs configuration management on configuration items of the TOE. Configuration management is performed on the TOE and the implementation representation of the TOE.
ALC_CMS.4	Cisco uniquely identifies configuration items and each release of the TOE has a unique reference. The Configuration Management documentation contains a configuration item list.
ALC_DEL.1	Cisco documents the delivery procedure for the TOE to include the procedure on how to download certain components of the TOE from the Cisco website and how certain components of the TOE are delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained. Further, the delivery documentation describes how to acquire the proper license keys to use the TOE components.
ALC_DVS.1	Cisco implements security controls over the development environment. Cisco meets these requirements by documenting the security controls.
ALC_FLR.2	Cisco documents the flaw remediation and reporting procedures so that security flaw reports from TOE users can be appropriately acted upon, and TOE users can understand how to submit security flaw reports to the developer.
ALC_LCD.1	Cisco documents the TOE development life-cycle to meet these requirements.
ALC_TAT.1	Cisco uses well-defined development tools for creating the TOE.
ATE_COV.2	Cisco demonstrates the interfaces tested during functional testing using a coverage analysis.
ATE_DPT.2	Cisco demonstrates the TSF subsystems tested during functional testing using a depth analysis.
ATE_FUN.1	Cisco functional testing documentation contains a test plan, a description of the tests, along with the expected and actual results of the test conducted against the functions specified in the ST.
ATE_IND.2	Cisco will help meet the independent testing by providing the TOE to the evaluation facility.
AVA_VAN.3	Cisco will provide 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 15: TOE SFR Measures

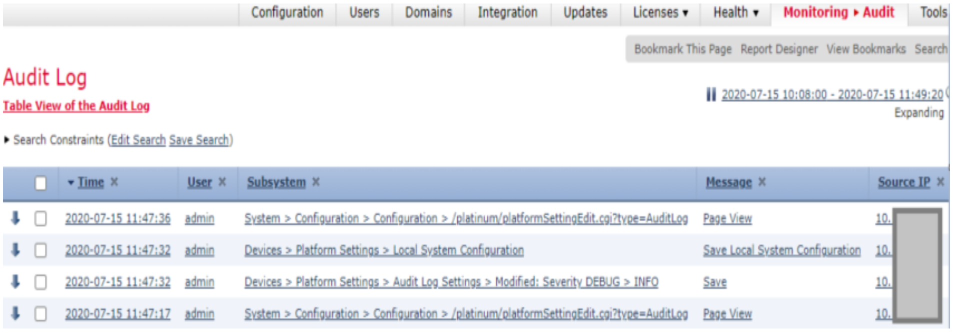
SFRs	How the SFRs are Satisfied
FAU_GEN.1 Audit data generation FAU_GEN.2 User identity association FAU_SAR.1 Audit review	Auditing is the recording of events within the system. The TOE generates log records for a wide range of security-relevant and other events as they occur. The events that can cause an audit record to be logged include starting the audit function[3], any all of the auditable events identified in Table 11: Auditable Events. All audit messages include at least a minimum set of details that includes a date/timestamp, the type of event, identification of what or who triggered the event, and the outcome (success or failure, which is often implicit in the message details). The TOE is comprised of multiple distributed components, most of which generate audit messages relevant to the events listed in FAU_GEN.1. The FMC, FTD, and MIO each generate audit messages. The AnyConnect TOE component does not generate audit messages though messages related to VPN client activity are logged by the FTD to which the AnyConnect component is communicating. Some TOE components have multiple audit generation mechanisms. • FMC has multiple audit generation mechanisms: o One generates messages related to use of the WebUI. o One generates messages related to system-level events. o One generates messages related to use of the CLI. • FTD has multiple audit generation mechanisms: o One generates system-level events, including use of the CLI. o One generates messages related to firewall events (relevant to the Firewall SFP). o One generates messages related to VPN events (relevant to the VPN SFP). • MIO has one generation mechanism: o Generates messages related to system-level events. The TOE components that provide administrative interfaces (FMC, FTD, and MIO, but not AnyConnect) generate audit messages to indicate when administrators have modified the TOE configuration, and those audit messages include the username of the administrator who made the change (relevant to FAU_GEN.2). The FMC component of the TOE allows review of locally stored audit records (relevant to FAU_SAR.1). Audit logs are presented via the WebUI of FMC in in two separate views, depending on what type of messages are being reviewed, and both views present messages in a format with sufficient detail and clarity that allows administrators to interpret the messages.

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

The FMC provides separate methods for viewing Audit Log messages (those stored in the internal database) vs Syslog messages (those stored in local flat files).

- Messages regarding administrative actions performed via the WebUI and CLI can be viewed in the **Audit Log** (under System > Monitoring > **Audit**).
- System-level messages, including administrative logins via CLI can be viewed in the **System Log** (under System > Monitoring > **Syslog)**, which allows viewing of the contents of /var/log/messages.

Figure 2: Sample contents of the Audit Log (System > Monitoring > Audit)



Audit Log

Table View of the Audit Log

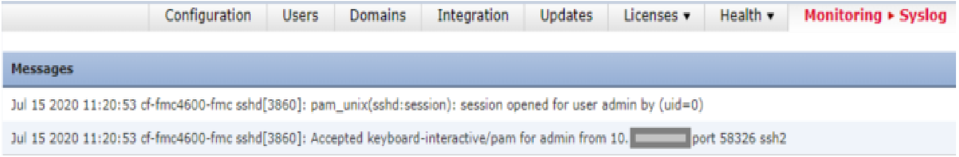
2020-07-15 10:08:00 - 2020-07-15 11:49:20

Expanding

▸ Search Constraints (Edit Search Save Search)

	□	Time	User	Subsystem	Message	Source IP
⬇	□	2020-07-15 11:47:36	admin	System > Configuration > Configuration > /platinum/platformSettingEdit.cgi?type=AuditLog	Page View	10.[redacted]
⬇	□	2020-07-15 11:47:32	admin	Devices > Platform Settings > Local System Configuration	Save Local System Configuration	10.[redacted]
⬇	□	2020-07-15 11:47:32	admin	Devices > Platform Settings > Audit Log Settings > Modified: Severity DEBUG > INFO	Save	10.[redacted]
⬇	□	2020-07-15 11:47:17	admin	System > Configuration > Configuration > /platinum/platformSettingEdit.cgi?type=AuditLog	Page View	10.[redacted]

Figure 3: Sample contents of the System Log (System > Monitoring > Syslog)



Messages

```
Jul 15 2020 11:20:53 cf-fmc4600-fmc sshd[3860]: pam_unix(sshd:session): session opened for user admin by (uid=0)
Jul 15 2020 11:20:53 cf-fmc4600-fmc sshd[3860]: Accepted keyboard-interactive/pam for admin from 10.[redacted] port 58326 ssh2
```

The following fields are displayed for each audit event in the **Audit Log** view:

- **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.

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.

FAU_STG.1 Protected audit trail storage

FAU_STG.4 Prevention of audit data loss

The TOE that have multiple audit generation components also have multiple audit storage mechanisms.

- FMC has two audit storage mechanisms:
  - Messages related to use of the WebUI and CLI are stored in a local database (locally reviewable via the WebUI under System > Monitoring > Audit).

  - Messages related to other system events are stored by syslog in local files (locally reviewable via the WebUI under System > Monitoring > Syslog).
- FTD has two audit storage mechanisms:
  - Messages related to firewall and VPN actions (relevant to the Firewall SFP and VPN SFP) are stored in a local log buffer.
  - Messages related to IPS events (some of which can provide additional detail related to Firewall SFP events, but those details are beyond what is defined in Table 11: Auditable Events), are not stored locally on FTD, and are transmitted directly to FMC for storage in a database on FMC.
- MIO has one audit storage mechanism:
  - Messages related to system-level events are stored in local files.

All the audit storage mechanisms protect the locally stored audit messages from unauthorized deletion, and from modification of audit records (relevant to FAU_STG.1). The FMC Audit Log interface allows authorized administrators to select and delete audit log messages from the Audit Log, no messages can be selectively deleted from any other local storage mechanism, and locally stored messages can be modified.

All storage mechanisms automatically overwrite the oldest stored audit records with new messages once the storage limit is reached (relevant to FAU_STG.4). Each audit storage mechanism implements its own limits, most of which are administratively configurable. Local audit storage limits:

- FMC Audit Log storage limits are configurable via the WebUI under System > Configuration > Database. There are multiple databases that store different types of messages, most of which are outside the scope of the TSF (e.g. those related to IPS events, including an Intrusion Event Database, and a Malware Event Database). Databases relevant to the TSF include: the Audit Event Database (default limit is 100,000 records); and the Connection Database (default limit is 1,000,000 records).
- FMC System Log is rotated daily whenever the log size has reached 25MB.
- MIO logging buffer: The audit storage on MIO has configurable size from 4096 to 4194304 bytes.
- FTD logging buffer has a default limit of 4096 bytes, and is configurable from 4096 to 52,428,800 bytes.
- FTD IPS events (outside the scope of this evaluation): Are not stored locally on FTD, but are transmitted from FTD to FMC (stored in a database, and viewable via the FMC Audit Log), and optionally also transmitted directly from the FTD to a remote syslog server.

The table below shows which messages are generated on each TOE component, and whether they're stored locally, and/or transmitted to another TOE component for storage, and/or transmitted to a remote syslog server.

SFR	FMC	FTD	MIO
Start-up and shutdown of audit functions	Generate. Store locally. Send to syslog.	Generate. Send to syslog.	Generate. Send to syslog.
FAU_GEN.1	n/a	n/a	n/a
FAU_GEN.2	n/a	n/a	n/a
FAU_SAR.1	n/a	n/a	n/a

FAU_STG.1	n/a	n/a	n/a
FAU_STG.4	n/a	n/a	n/a
FDP_IFC.1(*)	n/a	n/a	n/a
FDP_IFF.1(*)	n/a	Generate. Send to syslog	n/a
FDP_IFF.1(2)	n/a	Generate. Send to syslog	n/a
FIA_AFL.1	Generate. Store locally. Send to syslog.	Generate. Send to syslog.	Generate. Send to syslog.
FIA_SOS.1	n/a	n/a	n/a
FIA_UAU.1	n/a	n/a	n/a
FIA_UAU.5	Generate. Store locally. Send to syslog.	Generate. Send to syslog.	Generate. Send to syslog.
FIA_UAU.7	n/a	n/a	n/a
FIA_UID.2	Generate. Store locally. Send to syslog.	Generate. Send to syslog.	Generate. Send to syslog.
FMT_MOF.1	Generate. Store locally. Send to syslog.	Generate. Send to syslog.	Generate. Send to syslog.
FMT_MSA.1(*)	n/a	n/a	n/a
FMT_MSA.3	n/a	n/a	n/a
FMT_SMF.1	Generate. Store locally. Send to syslog.	Generate. Send to syslog.	Generate. Send to syslog.
FMT_SMR.1	Generate. Store locally. Send to syslog.	Generate. Send to syslog.	Generate. Send to syslog.
FPT_ITT.1	n/a	n/a	n/a
FPT_STM.1	Generate. Store locally. Send to syslog.	Generate. Send to syslog.	Generate. Send to syslog.
FTA_SSL.3	Generate. Store locally. Send to syslog.	Generate. Send to syslog.	Generate. Send to syslog.
FTA_TAB.1	n/a	n/a	n/a
FTP_ITC.1	n/a	Generate. Send to syslog.	n/a
FTP_TRP.1	Generate. Store locally. Send to syslog.	Generate. Send to syslog.	Generate. Send to syslog.

FDP_IFC.1(1) Subset information flow control FDP_IFF.1(1) Simple security attributes (Applicable only to FTD)	**FTD Only** All traffic that goes through the TOE is inspected using an Access Control Policy (defined on FMC, and 'deployed' to FTD) and is either allowed or blocked (dropped) by the FTD. The FTD provides stateful traffic filtering of IPv4 and IPv6 network traffic. To track the statefulness of sessions to/from and through the firewall, the FTD maintains a table of connections in various connection states and connection flags. The TOE updates the table (adding, and removing connections, and modifying states as appropriate) based on configurable connection timeout limits, and by inspecting fields within the packet headers. During initialization/startup (while the FTD is booting) the configuration has yet to be loaded, and no traffic can flow through any of its interfaces. No traffic can

	flow through the FTD interfaces until the POST has completed, and the configuration has been loaded. If any aspect of the POST fails during boot, the FTD will reload without forwarding traffic. If a critical component of the TOE, such as the clock or cryptographic modules, fails while the FTD is in an operational state, the FTD will reload, which stops the flow of traffic. If a component such as a network interface, which is not critical to the operation of the FTD, but may be critical to one or more traffic flows, fails while the FTD is operational, the FTD will continue to function, though all traffic flows through the failed network interface(s) will be dropped. A stateful firewall like the FTD takes into consideration the state of the traffic flow for each packet, to consider whether the packet is part of a new connection, or an established connection. **If the packet is part of a new traffic flow,** the FTD has to check the packet against access control lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the "session management path," and depending on the type of traffic, it might also pass through the "control plane path." The session management path is responsible for the following tasks: – Performing the access list checks – Performing route lookups – Allocating NAT translations (xlates) – Establishing sessions in the "fast path" The FTD creates forward and reverse flows in the fast path for TCP traffic; the TOE also creates connection state information for connectionless protocols like UDP, ICMP (when you enable ICMP inspection), so that they can also use the fast path. **If the packet is part of an established traffic flow,** the FTD does not need to re-check packets against the ACL; matching packets can go through the "fast" path based on attributes identified in FFW_RUL_EXT.1.5. The fast path is responsible for the following tasks: – IP checksum verification – Session lookup – TCP sequence number check – NAT translations based on existing sessions – Layer 3 and Layer 4 header adjustments **For all traffic flows,** the TOE supports filtering of the following protocols and enforces proper session establishment, management, and termination as defined in each protocol's RFC , using the following filtering options configured via FMC: <u>To filter ICMPv4 or ICMPv6 Type and Code:</u> • Policies > Access Control > Access Control > Add Rule > a. Zones (mapped to interfaces) > Available Zones > click either “Add to Source” or “Add to Destination” b. Networks > select IPv4 networks> add to source and/or destination

	c. Ports > Selected Destination Ports > Protocol > ICMP > select type and code To filter ICMPv6 Type and Code: As explained above for ICMPv4, but under “Networks” select IPv6 addresses. To filter IPv4 Source address, Destination Address, and Transport Layer Protocol: - Policies > Access Control > Access Control > Add Rule > a. Zones (mapped to interfaces) > Available Zones > click either “Add to Source” or “Add to Destination” b. Networks > select IPv4 networks > add to source and/or destination c. Ports > select a pre-named port, or create a new named protocol+port > add to source and/or destination To filter IPv6 Source Address, Destination Address, and Transport Layer Protocol: As explained above for IPv4, but under “Networks” select IPv6 addresses. To filter TCP Source Port and/or Destination Port: As explained above for IPv4 or IPv6, and under “Ports” select “TCP” and a port under either or both of “Selected Source Ports” and/or “Selected Destination Ports.” To filter UDP Source Port and/or Destination Port: As explained above for IPv4 or IPv6, and under “Ports” select “UDP” and a port under either or both of “Selected Source Ports” and/or “Selected Destination Ports.” Applicable RFCs: - Addresses, type of service, fragmentation data, size and padding, and IP options including loose source routing, strict source routing, and record route as defined in RFC 791 (IPv4), and RFC 2460 (IPv6); - Port numbers, sequence and acknowledgement numbers, size and padding, and control bits such as SYN, ACK, FIN, and RST as defined in RFC 793 (TCP); - Port numbers, and length as defined in RFC 768 (UDP); and - Session identifiers, sequence numbers, types, and codes as defined in RFC 792 (ICMPv4), and RFC 4443 (ICMPv6). Cisco confirms proper implementation of the RFCs through interoperability testing with Cisco and 3rd party products and through protocol compliant testing. The TOE can also support deeper packet inspection and enforce additional RFC compliance beyond session management, but such traffic inspection functionality is not defined within this Security Target and is therefore beyond the scope of this CC certification. Note: Rules of an Access Control Policies (ACP) are only enforced after the ACP has been deployed via the FMC to the FTD, which will automatically apply the ACP to all network interfaces defined within the ACP. The FMC will warn the administrator if they attempt to define parameters within an ACP that would not be applicable to any FTD to which the ACP has been assigned. For example, if a rule specifies an interface name or security ‘zone’ that has not been defined on any FTD that has been assigned to the ACP. The FMC will ensure that each FTD is only assigned to one ACP at a time.
FDP_IFC.1(2) Subset	**FTD**

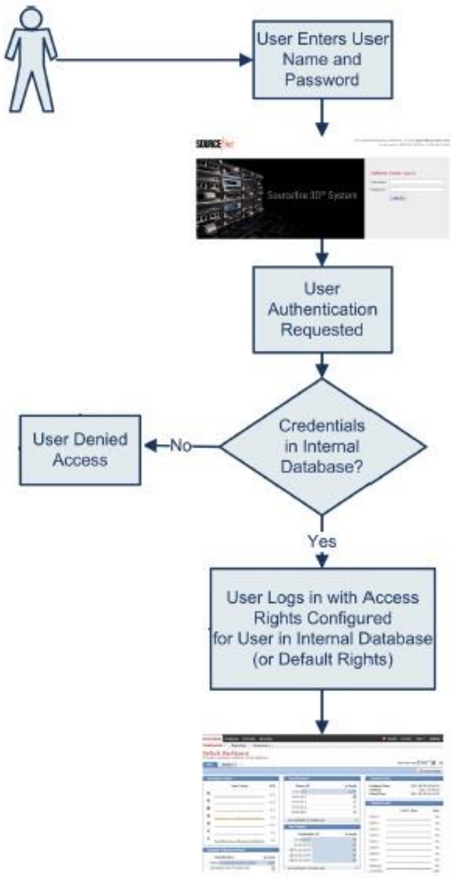
information flow control FDP_IFF.1(2) Simple security attributes (Applicable only to FTD and AnyConnect)	The TOE provides site-to-site VPN (e.g. FTD to FTD), and remote access VPN (AnyConnect to FTD) capabilities. The VPN site-to-site tunnel allows the FTD to act as a VPN gateway for connections with another VPN gateway (e.g. another FTD) to establish an IPsec tunnel to secure the passing of user data. The remote access VPN configuration allows a remote VPN client (AnyConnect) to connects to the TOE (FTD) to gain access to an authorized private network. Authenticating to the FTD would provide the AnyConnect client a secure IPsec tunnel to connect over the internet into their private network. Administratively-defined traffic filter rules (access-lists or **Objects > Object Management > Access Control Lists > Extended**) can be applied to any site-to-site or remote access VPN policy to filter traffic based on IP parameters including source and destination address, transport layer protocol, type and code, TCP and UDP port numbers. The TOE allows establishment of communications between remote endpoints, and tracks the state of each session (e.g. initiating, established, and tear-down), and will clear established sessions after proper tear-down is completed as defined by each protocol, or when session timeouts are reached. An authorized administrator can define the traffic that needs to be protected by configuring access lists (permit, deny, log) and applying these access lists to VPN policies, which are assigned to FTD instances. The TOE enforces information flow policies on network packets that are received by TOE interfaces and leave the TOE through other TOE interfaces. When network packets are received on a TOE interface, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, pass/not pass information, as well as optional logging. The TOE implements rules that define whether traffic will be encrypted, decrypted, and forwarded based on: 1. The identity of the remote IPsec endpoint. 2. The authentication status of the remote IPsec endpoint. 3. Whether the traffic traversing the TOE is associated with an IPsec security policy, where traffic can match the security policy based on: a. source IP address b. destination IP address c. transport layer protocol d. TCP or UDP port number These rules are supported for the following protocols: RFC 791(IPv4); RFC 2460 (IPv6); RFC 793 (TCP); RFC 768 (UDP). TOE compliance with these protocols is verified via regular quality assurance, regression, and interoperability testing. Packets will bypass IPsec tunnels (and potentially be dropped the Firewall SFP) unless rule exists within the IPsec security policy to allow (encrypt and/or decrypt) the traffic. Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied. **AnyConnect** After successful client authentication to the FTD, a virtual IP address is assigned by the FTD (from its administratively-defined address pool) to the AnyConnect client. The AnyConnect client then uses its assigned virtual IP address for the duration of the established tunnel to route all network traffic between the AnyConnect's underlying host and the FTD to which AnyConnect has established the IPsec tunnel.

	When all traffic is tunneled (when split-tunneling is not explicitly permitted), a new default route is added to the host OS platform with a lower metric directing all traffic to be protected with IPsec by AnyConnect. AnyConnect uses active SA settings or creates new SAs for initial connections with the FTD. All client-side ESP processing to authenticate, encrypt, and tunnel the traffic is performed by AnyConnect itself, not by the underlying host. If the remote access policy (defined on FMC, then deployed to FTD) explicitly permits use of split-tunneling, a remote access policy on the FTD allows the administrator to define IPsec protection for the organization's network(s) but bypass protection for other traffic. When a portion of traffic is tunneled, a route is added to the host OS platform corresponding to the network segment requiring IPsec protection by the TOE. Network(s) not subjected to the remote access policy, but reachable from the platform, such as Internet traffic, travels without being protected with IPsec by the TOE. Within the scope of this CC evaluation, SPD rules to discard/block/drop traffic are performed exclusively by the FTD platform, not AnyConnect. IPsec Internet Key Exchange (IKE) is the negotiation protocol that lets AnyConnect and FTD agree on how to build an IPsec Security Association (SA). IKE separates negotiation into two phases: phase 1 and phase 2. During IKE Phase 1, the TOE authenticates the remote VPN Gateway using device-level authentication with ECDSA or RSA X.509v3 certificates provided by the TOE platform. AnyConnect implements IKEv2, use of IKEv1 is not allowed in the CC-evaluated configuration.
FIA_AFL.1 Authentication failure handling	**FMC** FMC provides the administrator the ability to specify the maximum number (can be set differently per account on FMC) of unsuccessful remote authentication attempts via WebUI (disabled by default, configurable from 1-999) before the offending account is locked. Only an authorized administrator (with the 'administrator' role) can unlock a locked account. By default, the predefined 'admin' account is exempt from becoming locked, but that default is overridden if CC mode is enabled on FMC. If all admin accounts become locked for any reason, FMC can be accessed locally using password recovery procedures. **FTD** FTD on Firepower 1k and 2k platforms allows a maximum number of consecutive failed login attempts via CLI (SSH and local serial console) before the offending account becomes locked ('lock-status' set to 'locked'). When an account is locked the user must wait for the account to be unlocked by another administrator who has the 'config' role (the 'basic' role is not sufficient). If all admin accounts become locked for any reason, FTD can be accessed locally using password recovery procedures. All types of user accounts (including account type 'admin') are locked out of the system after exceeding the maximum number of login attempts. The default maximum number of unsuccessful login attempts is '3' (configurable from 1-10). The default amount of time the user is locked out of the system after exceeding the maximum number of login attempts is 30 minutes (1800 seconds), configurable from 10 minutes (600 seconds) to 10 hours (36000 seconds). **MIO**

	MIO will allow a maximum number (same value applies to all MIO accounts) of consecutive failed login attempts via SSH or WebUI before the offending account becomes locked (‘lock-status’ set to ‘locked’) for a specified period of time. When an account is locked the user must wait the specified amount of time before attempting to log in, or the account can be unlocked by another administrator who has the ‘admin’ role (not just ‘read-only’). If all admin accounts become locked for any reason, MIO can be accessed locally using password recovery procedures. • All types of user accounts (including account type 'admin') are locked out of the system after exceeding the maximum number of login attempts. • The default maximum number of unsuccessful login attempts is '3' (configurable from 1-10). The default amount of time the user is locked out of the system after exceeding the maximum number of login attempts is 30 minutes (1800 seconds), configurable from 10 minutes (600 seconds) to 10 hours (36000 seconds).
FIA_SOS.1 Verification of secrets	***Note:*** *The password constraints (minimum length, and minimum complexity) described below apply to locally-defined accounts (with locally-stored reusable passwords). Where AAA (RADIUS) is used for authentication, the RADIUS server (outside the TOE boundary) would enforce password constraints.* **FMC** FMC has two local authentication mechanisms, one for the WebUI, and one for the CLI. • FMC WebUI accounts can be configured to require a minimum password length of 15-32 characters. If the optional Check Password Strength setting is enabled on any account, the FMC WebUI will require new passwords for that account to contain at least one upper case, one lower case, one number, and one special character. The minimum password length and the Check Password Strength option are set individually for each account. By default, the minimum password length is eight, and Check Password Strength is disabled. • FMC CLI account requires a minimum password length of eight characters, and requires new passwords to contain at least one upper case, one lower case, one number, and one special character. Those settings are not configurable. Note: In addition to requiring *inclusion* of certain character sets the Check Password Strength option of the FMC WebUI also enforces *exclusion* of certain patterns (such as dictionary words, etc.), but testing of the exclusions is beyond the scope of this CC evaluation. **FTD** FTD has a single local authentication mechanism for administrative access that allows administrative accounts to be configured to require a minimum password length of 8-127 characters. If the optional password strength check setting is enabled on any account, the FTD will require new passwords for that account to contain at least one upper case, one lower case, one number, and one special character. The minimum password length and the password strength check option are set individually for each account via the commands “configure user minpasswdlen <username>” and “configure user strengthcheck <username>”. By default, the minimum password length is eight, and strengthcheck is disabled.

	In addition to the local authentication mechanism for administrative access, FTD has a separate mechanism for authenticating of remote access VPN connections, which are authenticated either using AAA (RADIUS) or using X.509v3 certificates, neither of which is applicable to FIA_SOS.1. **MIO** MIO has a single local authentication mechanism, which applies the same administratively configurable password strength requirements to all accounts. The minimum password length is configurable from 8-80 characters, and is configurable via the CLI using the "set min-password-length" command. If the optional Password Strength Check setting is enabled (via CLI or WebUI), MIO will require new passwords to include: at least one uppercase alphabetic character, at least one lowercase alphabetic character, and at least one non-alphanumeric (special) character ($ (dollar sign), ? (question mark), and = (equals sign) are prohibited). By default, the minimum password length is eight, and Password Strength Check is disabled. Note: In addition to requiring *inclusion* of certain character sets the Password Strength Check on MIO also enforces *exclusion* of certain patterns (such as repeated characters, etc.), but testing of the exclusions is beyond the scope of this CC evaluation.
FIA_UAU.1 Timing of authentication FIA_UID.2 User identification before any action	**FMC, FTD, and MIO** The TOE is designed to successfully identify and authenticate a user before allowing access to the TOE's security function. When identification and authentication data (credentials, i.e. username and password) are entered, the TOE attempts to identify the applicable user account from the provided identity and if a match is found, the password provided is hashed with a salt value and compared against the stored hash[4] with the user account information in the internal database. If a user account cannot be associated with the provided identity or the hashed password does not match that stored hash with the user account information, the process will fail. No actions are allowed, other than re-entry of identification and authentication data or viewing the login banner. Once the user has successfully log in, the privilege level or role will control what management functions he or she has access and authorization to. Figure below shows the authentication process. Figure 4: Authentication Process

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

	 User Enters User Name and Password User Authentication Requested Credentials in Internal Database? No User Denied Access Yes User Logs in with Access Rights Configured for User in Internal Database (or Default Rights) Users can connect to the TOE via a local console or remotely using SSHv2 or HTTPS. In each case, the user is required to log in prior to successfully establishing a session through which TOE security functions can be performed. **AnyConnect** The AnyConnect component of the TOE does not contain a mechanism for identification and authentication (I&A). AnyConnect relies on its underlying operating system to control access to AnyConnect. AnyConnect supports authentication of VPN client users by providing a login interface, but authentication is enforced by FTD.
FIA_UAU.5 Multiple authentication mechanisms	**FMC** FMC has two administrative interfaces, each of which uses a separate authentication mechanism. The FMC CLI only supports local password-based authentication. The FMC WebUI supports local password-based authentication, and also supports remote AAA (RADIUS) authentication. The RADIUS server is outside the scope of the TOE. **FTD** FTD has one administrative interface (the CLI is accessible via local serial console, or SSH), which only supports local password-based authentication. FTD supports use of X.509v3 certificates and/or AAA (RADIUS) for authentication of remote-access VPN clients connecting to FTD from AnyConnect. **MIO**

	MIO includes a local password-based authentication mechanism, and also supports use of remote AAA (RADIUS) authentication. MIO provides two administrative interfaces (WebUI and CLI), both of which share the same authentication mechanisms, but administrators can set a preferred authentication mechanism (local or RADIUS) separately for WebUI login vs console login. The RADIUS server is outside the scope of the TOE. **AnyConnect** The AnyConnect component of the TOE does not contain a mechanism for identification and authentication (I&A). AnyConnect relies on its underlying operating system to control access to AnyConnect. AnyConnect supports authentication of VPN client users by providing an interactive (password-based) login interface, and supporting use of X.509v3 certificates for authentication, but authentication is enforced by FTD.
FIA_UAU.7 Protected Authentication Feedback	**FMC, FTD, and MIO** When logging in, all interfaces of 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. 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. **AnyConnect** AnyConnect supports authentication of VPN client users to FTD by providing a login interface, which does not echo the VPN user's password as it's typed.
FMT_MOF.1 Management of security functions behavior FMT_SMF.1 Specification of Management Functions	**FMC, FTD, and MIO** The TOE restricts the ability to perform of all of the security functions of the TOE to authorized administrators. The TOE provides the ability for authorized administrators to start up and shutdown the TOE, manage firewall rules, manage accounts, configure authentication mechanisms and settings including failure thresholds and accounts that have become locked out, manage NTP settings and clock settings via MIO, make changes to the amount of space dedicated to audit storage, configure the connection and protocols for transmitting audit messages to syslog servers, configure the interfaces and protocols that can be used for administration, and initiate TOE updates. **FMC** Only accounts with 'administrator' privilege can upload patches to FMC and initiate installation of patches to FMC or FTD devices (the FMC WebUI is used to configure FMD and FTD). Only accounts with 'administrator' privilege can update system configuration settings related to: • local logging and remote logging • clock settings

	• account management including account lockout settings and unlocking accounts • login banners • cryptographic functionality including SSH (FMC), TLS (FMC), and IPsec (FTD) • generation of CSRs, and import or delete X.509v3 certificates • firewall functionality • VPN functionality **FTD** Most configuration for FTD is performed via FMC, through configuration of "Platform Settings". Configurations that can be performed directly via the FTD CLI are: • configuring, enabling, disabling transmission of system-level audit messages to a remote syslog server. **MIO** Only accounts with 'admin' role can upload software updates to MIO and initiate updates of MIO and configure: • local logging and remote logging • clock settings • account management including account lockout settings and unlocking accounts • login banners • cryptographic functionality including SSH, TLS, and IPsec **AnyConnect** AnyConnect does not perform any security management functions as an administrator. Those functions are provided by the host OS. All VPN traffic flow control policies are configured on FMC and enforced by FTD.
FMT_MSA.1(1) Management of security attributes	**FMC Only** The TOE allows for creation of Access Control Policies (ACPs) to either "allow" or "block" traffic to/from an FTD, and any rule can optionally also be configured to log when the rule is matched. The ACPs can only be created, deleted, modified, enabled, or disabled by authorized administrators via the FMC WebUI.
FMT_MSA.1(2) Management of security attributes	**FMC Only** The TOE allows for creation of access control lists (ACLs) to restrict what traffic is allowed to flow through IPsec tunnels. The ACLs can only be created, deleted, modified, enabled, or disabled by authorized administrators via the FMC WebUI. The ACLs allow customization of all of these properties to allow or deny access (**Objects > Object Management > Group Policy > Traffic Filter Fields > Access List Filter)**. In addition, the administrator can create Group Policy tied to Connection Profile (**Objects > Object Management > Group Policy > Session Settings > Access Hours)** can be used to restrict access based on date and time.

FMT_MSA.3 Static attribute initialization	**FMC Only** By default, no traffic flow control policies are assigned to any FTD, and none exist by default on FMC. When policies are created on FMC, the administrator can choose which other policy to use as an initial "base policy" definition, then further customize the new policy after its been created. As each policy is created, the administrator must select a "default action" that will be applied to all traffic that does not explicitly match an administratively-defined rule within the policy. Default actions include: block all traffic (which is the default selection); intrusion prevention (to enable default IPS policies); and network discover (a permissive policy that can be used to monitor networks). In addition, each FTD interface is disabled by default, and no traffic flow policies exist by default on an FTD, thus no traffic can flow through an FTD prior to a policy being deployed to FTD from FMC. This is true for firewall functionality (implemented as Access Control Policies, ACPs), and VPN functionality (implemented as Site To Site policies or Remote Access policies).
FMT_SMR.1 Security roles	**FMC** The FMC provides a web-based GUI (using HTTPS) management interface and CLI or shell (using SSH or serial connection). On FMC, both the GUI and CLI have a default "admin" account, but the accounts are defined and maintained separately within FMC. Once the FMC has been configured into its CC-evaluated configuration, the actions that can be performed via the CLI will be greatly limited, and will be a very small subset of what can be performed via the GUI, through which all administrative actions can be performed. 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 in the context of this CC evaluation, all users created on FMC are TOE administrators. • Administrators of the FMC WebUI can configure all aspects of the FMC itself, add/remove managed FTD instances, define policies for all managed FTD instances, manage FMC user accounts, and configure auditing, and review locally stored audit messages. • Administrators of the FMC CLI can change its own password, and shutdown or restart the FMC. **FTD** The FTD has one default administrative account, and two privilege levels, 'config' and 'basic'. The default account, which always has the 'config' privilege, can perform all administrative functions that are allowed via the FTD CLI. The FTD CLI provides only a small subset of all available functions that could be performed via the FMC WebUI. **MIO** The 'admin' account is a default user account and cannot be modified or deleted. This account is the system administrator or superuser account and has full privileges. The term "authorized administrator" or "Security Administrator" applies to this account and other accounts assigned to the Administrator role. Additional named accounts can be created, and all would be considered to be authorized administrators for the purposes of the CC evaluation. MIO (the FXOS in the supervisor engine, which is only present on 4100 series and 9300 platforms) has two administrative interfaces, the WebUI (FCM), and

	CLI. Both administrative interfaces on these platforms use the same local authentication mechanisms (the 'admin' account that logs in via CLI is the same 'admin' account that logs in via the WebUI). By contrast, the FXOS in FTD on 1000/1100 series and 2100 series platforms, and on any SM within 4k/9k platforms does not support the WebUI (FCM) in the CC-evaluated configuration (when FTD is 'managed' by FMC), so the only administrative interfaces is the CLI (accessible via local serial console or SSH), but the 'admin' account on these platforms has the same role as on other platforms. **AnyConnect** There is one non-TOE role, and one TOE role relevant to installation and operation of the AnyConnect TOE component: 1) the Windows administrator/user who installs the AnyConnect software; and 2) the VPN user who uses the AnyConnect software to authenticate to the FTD. The Windows accounts (administrator and user) are not TOE roles, and their Windows credentials are not used to authenticate to the TOE. The VPN user role is a TOE role though that account is not uniquely defined within the TOE. The TOE does not maintain a list of individual authorized VPN user accounts, instead the TOE is configured (via FMC) by the TOE's authorized administrator to authenticate VPN users using credentials provided via AnyConnect to FTD and referred by FTD to an external authentication source (either a Certificate Authority, or RADIUS server). Regardless of the authentication method (X.509 certificate, and/or username/password) the TOE limits the permissions of the VPN user role such that an authenticated VPN user can only transmit/receive IPsec traffic to/from an FTD, the VPN user role has no access to any administrative interfaces on FMC, FTD, or MIO.
FPT_ITT.1 Basic Internal TSF Data Transfer Protection	**FMC and FTD** The communication between the FMC and FTD is protected by TLSv1.2. TLS provides authentication, key exchange, encryption and integrity protection of all data transmitted between the TOE components. **FTD and AnyConnect** The communication between the FTD and AnyConnect is protected by IPSec. IPSec provides authentication, key exchange, encryption and integrity protection of all data transmitted between the TOE components.
FPT_STM.1 Reliable time stamps	**FMC** The FMC maintains its own internal software clock, which is used for generating timestamps for audit messages. Administrators can manually set the clock, or configure it to be updated automatically via NTP with the NTP server located on a trusted management network. **FTD** On 1000/1100 series and 2100 series: The clock can be configured to be automatically synchronized to the FMC clock, or to use an NTP server. On 4100 series and 9300: The clock (including manually setting the time and enabling/disabling/configuring NTP) can only be configured via MIO. The TOE automatically synchronizes its clock with the MIO clock. **MIO** The MIO maintains its own internal software clock, which is used for generating timestamps for audit messages. Administrators can manually set the clock, or

	configure it to be updated automatically via NTP with the NTP server located on a trusted management network.
FTA_SSL.3 TSF-initiated Termination	**FMC, FTD, and MIO** The TOE can be configured by an administrator to set an interactive session idle timeout value in the system policy or platform settings, which will terminate sessions after the configured limit of inactivity. The setting applies to all users and for both local and remote interactive sessions. For FMC and FTD, the timeout value can be any positive integer value from 1 minute to 1,440 minutes (24 hours), and the default timeout value is 60 minutes for WebUI and is disabled by default for CLI. For MIO, the timeout limit can be any positive integer value from 1 minute to 3600 seconds (1 hour). Note: FMC supports the ability to exempt individual accounts from having the Browser Session Timeout enforced for their WebUI sessions, but that exemption cannot be enabled for any account with the 'Administrator' role, and the AGD prohibits exempting any account from the session timeout limit regardless of the role(s) assigned to the account. 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.
FTA_TAB.1 Default TOE Access Banners	**FMC, FTD, MIO, and AnyConnect** The TOE provides administrators with the capability to configure advisory banner or warning message(s) that will be displayed prior to completion of the logon process at the local console or via any remote connection (e.g., SSH or HTTPS). The TOE displays an advisory notice and a consent warning message for each administrative and VPN Client method of access: • FMC: Console, SSH, and WebUI • FTD: SSH on all platforms, and console on 1k/2k platforms (the console banner on 4k/9k is provided by MIO) • MIO: Console, SSH, and WebUI (FCM) • AnyConnect: VPN Client User Interface (displayed during VPN session establishment, not during Windows login)
FTP_ITC.1 Inter-TSF Trusted Channel	**FTD, and AnyConnect** The TOE uses IPsec (in FTD on all platforms) and TLS (FTD) to protect communications between itself and remote entities for the following purposes: • The TOE (FTD only) protects transmission of audit records when sending syslog message to a remote audit server by transmitting the messages: • From FTD (for transmission of firewall messages and VPN messages) as a TLS client, using X.509v3 certificates for assured identification of the syslog server. • **Note:** The remote audit (syslog) server is located on a trusted management network.. • The TOE (FTD only) protects peer-to-peer VPN connections between itself and VPN peers (connections can be initiated by the TOE or by the

	peer) using IPsec, using X.509v3 certificates for assured identification of the peer. • The TOE (FTD and AnyConnect) protects remote access VPN connections between AnyConnect and FTD using IPsec, authenticated with username/password, or X.509v3 certificates for assured identification of the VPN client. **Note:** The TOE (FTD, and AnyConnect) validates the identification of remote endpoints using OCSP for validation of certificates.
FTP_TRP.1 Trusted Path	**FMC, FTD, and MIO** To support secure remote administration of FMC, FTD and MIO, the TOE includes implementations of HTTPS (HTTP over TLS, based on OpenSSL). FTD and MIO also include implementations of SSH (based on OpenSSH). FTD, and MIO use only SSHv2, not SSHv1. FMC allows only TLSv1.2, while MIO allows both TLSv1.1 and TLSv1.2. Note that in the CC evaluated configuration, where FTD is managed by FMC, FTD doesn't have its own HTTPS interface for remote management. 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 each of these remote administration services can be independently enabled by an administrator. For added security, only these security protocols and ports 22 and 443 are enabled and allowed by default. The administrators can also setup an access list to restrict only allowed IP addresses to access the TOE. Note, no TLS versions other than those listed above are supported on any TOE administrative interface, thus there's no risk of a remote client triggering a 'downgrade' to an older SSL/TLS version. In the cases of SSH 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 SSH 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 valid user credentials (user name and password), after which they will be able to issue commands or actions within their assigned authorizations.

6.2 TOE Bypass and Interference/Logical Tampering Protection Measures

The TOE consists of multiple software solutions. All TSP enforcement functions must be invoked and succeed prior to functions within the TSC proceeding.

The TOE has been designed so that all locally maintained TSF data can only be manipulated via the secured management interface, a CLI, a GUI (FMC) interface. There are no undocumented interfaces for managing the product.

In order to access any portion of these TOE components, the Identification & Authentication mechanisms of the TOE must be invoked and succeed.

No processes outside of the TOE are allowed direct access to any TOE memory. The TOE only accepts traffic through legitimate TOE interfaces. None of these interfaces provide any access to internal TOE resources.

The software running on each underlying Cisco appliance provide a secure domain for each context to operate within. Each context has its own resources that other contexts within the same TOE platform are not able to affect.

Finally, the FTD and AnyConnect components of the TOE enforce information flow control and VPN policies and apply network traffic security on its interfaces before traffic passes into or out of the TOE. The TOE controls every ingress and egress traffic flow. Policies are applied to each traffic flow. Traffic flows characterized as unauthorized are discarded and not permitted to circumvent the TOE.

There are no unmediated traffic flows into or out of the TOE. The information flow policies identified in the SFRs are applied to all traffic received and sent by the TOE. Each communication is mediated by the TOE. There is no opportunity for unaccounted traffic flows to flow into or out of the TOE.

The Cisco AnyConnect Secure Mobility Client, as a software implementation, is dependent upon its operational environment for protection. This software component runs on the operating systems identified in Table 2. This component uses its own crypto libraries (not those of the host operating system) for all IPsec connections to the FTD.

This design, combined with the fact that only an administrative user with the appropriate role may access the TOE security functions, provides a distinct protected domain for the TOE that is logically protected from interference and which cannot be bypassed.

7 Rationale

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined within this Security Target. The table below illustrates the mapping from Security Objectives to Threats and Policies.

7.1 Rationale for the TOE Security Objectives

Table 16: Tracing of IT Security Objectives

	T.NOAUTH	T.ASPOOF	T.MEDIAT	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL	T.VPN	T.UNAUTHORIZED	T.UNDETECTED	P.ACCESS_BANNER
O.IDAUTH	X										
O.MEDIATE		X	X								
O.SECSTA	X					X					
O.SELPRO	X					X	X				
O.AUDIT					X						
O.ACCOUNTABLE					X						
O.SECFUN	X						X				
O.LIMEXT	X										
O.VPN								X			
O.BANNER											X
O.PROCOM				X					X		
O.SESSION_LOCK									X		
O.MONITORING									X	X	
O.ADMINISTRATION									X		

O.IDAUTH This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.

O.MEDIATE This security objective is necessary to counter the threats: T.ASPOOF, and T.MEDIAT which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE.

O.SECSTA This security objective ensures that no information is compromised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

O.SELPRO This security objective is necessary to counter the threats: T.SELPRO, T.AUDFUL and T.NOAUTH because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

O.AUDIT This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail.

O.ACCOUNTABLE This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

O.LIMEXT This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.

O.VPN This security objective is necessary to counter the threat: T.VPN because it ensures that a trusted communication path exists between the TOE and remote VPN endpoints (clients and gateways). This objective ensures all tunneled VPN data sent/received to/from remote VPN endpoints (clients or gateways) is properly encrypted/decrypted data integrity is assured/verified.

O.BANNER This security objective is necessary to address the policy P.ACCESS_BANNER because it ensures an advisory banner is displayed when users log in to establish interactive sessions.

O.PROCOM This security objective is necessary to counter the threats T.PROCOM, and T.UNAUTHORIZED because it ensures the TOE will properly encrypt its communication channels to protect them.

O.SESSION_LOCK This security objective is necessary to counter the threat T.UNAUTHORIZED because it ensures the TOE will lock inactive, and hence perhaps unattended, interactive sessions.

O.MONITORING This security objective is necessary to counter the threats T.UNAUTHORIZED, and T.UNDETECTED because it ensures the TOE will log administrator commands that might serve to help identify previous errors and the TOE will log security relevant events that might be indicative of inappropriate access or access that requires accountability.

O.ADMINISTRATION This security objective is necessary to counter the threat T.UNAUTHORIZED because it ensures the TOE is designed to ensure that only administrators can access security management functions and only after they have been properly identified and authenticated.

7.2 Rationale for the Security Objectives for the Environment

Table 17: Tracing of Security Objectives for the Environment

	A.NOEVIL	A.PHYSEC	A.PROTRA	A.PROTENV	A.REMACC	A.SINGEN
OE.NOEVIL	X					
OE.PHYSEC		X				
OE.PROTRA			X			
OE.PROTENV				X		
OE.REMACC					X	

	A.NOEVIL	A.PHYSEC	A.PROTRA	A.PROTENV	A.REMACC	A.SINGEN
OE.SINGEN						X

OE.NOEVIL Authorized administrators are non-hostile, trained, and follow all administrator guidance. This OE is necessary to uphold A.NOEVIL.

OE.PHYSEC The hardware components on which the TOE's Firepower components are installed are kept physically secure. This OE is necessary to uphold A.PHYSEC.

OE.PROTRA The workstations on which the TOE's AnyConnect component is installed are issued and managed by the same organization that manages the other TOE components and are kept secure through physical and/or cryptographic means (e.g. disk/drive encryption). This OE is necessary to uphold A.PROTRA.

OE.PROTENV The operational environment servers on which the TOE relies, including NTP, syslog, CA/OCSP/CRL, and RADIUS servers remain physically and logically protected from malicious activity. The NTP, syslog, and RADIUS servers will be located on a trusted management network accessible from FMC, FTD, and MIO. This OE is necessary to uphold A.PROTENV.

OE.REMACC Authorized administrators may access the TOE remotely from the internal and external networks. This OE is necessary to uphold A.REMACC.

OE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE. This OE is necessary to uphold A.SINGEN.

7.3 Rationale for SFRs-SARs/TOE Objectives

This section provides rationale for the Security Functional Requirements/Security Assurance Requirements demonstrating that the Security Functional Requirements/Security Assurance Requirements are suitable to address the security objectives. The table below illustrates the mapping from SFRs to Security Objectives.

Table 18: Summary of Mappings Between IT Security Objectives and SFRs

	O.IDAUTH	O.MEDIATE	O.SECSTA	O.SELPRO	O.AUDIT	O.ACCOUNTABLE	O.SECFUN	O.LIMEXT	O.VPN	O.BANNER	O.PROCOM	O.SESSION_LOCK	O.MONITORING	O.ADMINISTRATION
FAU_GEN.1					X	X							X	
FAU_GEN.2													X	
FAU_SAR.1					X									
FAU_STG.1			X	X			X							
FAU_STG.4			X	X			X							
FDP_IFC.1(1)		X												

	O.IDAUTH	O.MEDIATE	O.SECSTA	O.SELPRO	O.AUDIT	O.ACCOUNTABLE	O.SECFUN	O.LIMEXT	O.VPN	O.BANNER	O.PROCOM	O.SESSION_LOCK	O.MONITORING	O.ADMINISTRATION
FDP_IFC.1(2)									X					
FDP_IFF.1(1)		X												
FDP_IFF.1(2)									X					
FIA_AFL.1				X										
FIA_SOS.1														X
FIA_UAU.1	X													
FIA_UAU.5	X													
FIA_UAU.7														X
FIA_UID.2	X					X								
FMT_MOF.1			X				X	X						
FMT_MSA.1(1)		X	X				X							
FMT_MSA.1(2)		X	X				X		X					
FMT_MSA.3		X	X											
FMT_SMF.1							X							X
FMT_SMR.1							X							X
FPT_ITT.1											X			
FPT_STM.1					X								X	
FTA_SSL.3												X		X
FTA_TAB.1										X				
FTP_ITC.1	X			X							X			
FTP_TRP.1											X			

FAU_GEN.1 Audit data generation

This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDIT, O.ACCOUNTABLE, and O.MONITORING.

FAU_GEN.2 User identity association

This component ensures that the TSF traces audit records to the user that caused them. This component traces back to and aids in meeting the following objective: O.MONITORING.

FAU_SAR.1 Audit review

This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDIT.

FAU_STG.1 Protected audit trail storage

This component is chosen to ensure that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator and that start-up and recovery does not compromise the audit records. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN and O.SECSTA.

FAU_STG.4 Prevention of audit data loss

This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO, O.SECFUN, and O.SECSTA.

FDP_IFC.1 Subset information flow control (1)

This component identifies the entities involved in the FIREWALL information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIATE.

FDP_IFC.1 Subset information flow control (2)

This component identifies the entities involved in the VPN information flow control SFP, which ensures all IPsec encrypted data received from a peer TOE is properly decrypted and authentication verified. This component traces back to and aids in meeting the following objective: O.VPN.

FDP_IFF.1 Simple security attributes (1)

This component identifies the attributes of the users sending and receiving the information in the FIREWALL_SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIATE.

FDP_IFF.1 Simple security attributes (2)

This component satisfies the VPN_SFP by ensuring that all IPsec encrypted data received from a peer TOE is properly decrypted and authentication verified. This component traces back to and aids in meeting the following objective: O.VPN.

FIA_AFL.1 Authentication failure handling

This component ensures that human users who are not authorized administrators cannot endlessly attempt to authenticate. After some number of failures that the authorized administrator decides, that must not be zero, the user becomes unable from that point on in attempts to authenticate. This goes on until an authorized administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.

FIA_UAU.1 Timing of authentication

This component ensures that before anything occurs on behalf of a user, the user's identity is authenticated to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUNTABLE.

FIA_UAU.5 Multiple authentication mechanisms

This component was chosen to ensure that multiple authentication mechanism are used appropriately in all attempts to authenticate at the TOE from an internal or external network. A SOF metric for this requirement is defined in section 5.1.1 to ensure that the mechanisms are of adequate probabilistic strength to protect against authentication data compromise. This component traces back to and aids in meeting the following objective: O.IDAUTH.

FIA_UAU.7 Protected Authentication Feedback

This component ensures that the TSF will not echo passwords when being entered to mitigate the chance of an accidental password disclosure s. This traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FIA_UID.2 User identification before any action

This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUNTABLE.

FMT_MOF.1 Management of security functions behavior

This component was to ensure the TSF restricts the ability to modify the behavior of functions such as audit trail management, start up and shut down operation, and multiple authentication function to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

FMT_MSA.1 Management of security attributes (1)

This component ensures the TSF enforces the FIREWALL_SFP to restrict the ability to delete, modify, and add within a rule those security attributes that are listed in section FDP_IFF1.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIATE, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (2)

This component ensures the TSF enforces the VPN_SFP to restrict the ability to delete, modify, and add within a rule those specified security attributes that are listed in section FDP_IFF1.1(2). This component traces back to and aids in meeting the following objectives: O.VPN, O.SECSTA, and O.SECFUN.

FMT_MSA.3 Static attribute initialization

This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIATE and O.SECSTA.

FMT_SMF.1 Specification of Management Functions

This component ensures that the TSF restrict the set of management functions to the authorized administrator. It also ensures that the TSF will provide a minimum set of security functions to ensure the TOE security features can be properly managed. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.ADMINISTRATION.

FMT_SMR.1 Security roles

Each of the CC class FMT components in this Protection Profile depends on this component. It requires the PP/ST writer to choose a role(s). It also ensures that the TSF will provide a minimum set of a Administrator roles and can implement additional roles where necessary. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.ADMINISTRATION.

FPT_ITT.1 Basic internal TSF data transfer protection

This component ensures that the TSF requires protection of the administrative traffic between the FMC component and the FTD, and the VPN client and the FTD for certificate delivery. This traces back to and aids in meeting the following objective: O.PROCOM.

FPT_STM.1 Reliable time stamps
FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objectives: O.AUDIT and O.MONITORING.

FTA_SSL.3 TSF-initiated Termination
This component ensures that the TSF will terminate local and remote sessions after an administrator defined period of inactivity indicating the user may not be in attendance. This traces back to and aids in meeting the following objectives: O.SESSION_LOCK and O.ADMINISTRATION.

FTA_TAB.1 Default TOE Access Banners
This component ensures that the TSF will display a configured advisory banner whenever a user/administrator connects to the TOE. This traces back to and aids in meeting the following objective: O.BANNER.

FTP_ITC.1 Basic internal TSF data transfer protection
These components ensure that the TSF requires protection of the audit data transmitted from the TOE (FTD only) to remote syslog servers and secure IPsec tunneling. between two trusted VPN peers as well as between remote VPN clients and the FTD. This traces back to and aids in meeting the following objectives: O.IDAUTH, O.SELPRO, and O.PROCOM.

FTP_TRP.1 Trusted Path
This component ensures that the TSF will protect communication between itself and its administrators from disclosure and modification. These trace back to and aids in meeting the following objective: O.PROCOM.

FIA_SOS.1 Verification of secrets
This component ensures that the TSF will implement mechanisms allowing an administrator to constrain the construction of passwords to encourage more secure (or harder to guess) passwords. This traces back to and aids in meeting the following objective: O.ADMINISTRATION

8 Glossary: Acronyms and Abbreviations

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

Table 19: Acronyms and Abbreviations

Acronym or Abbreviation	Definition
1k	Cisco Firepower 1000 series appliances (1010, 1120, and 1140)
2k	Cisco Firepower 2100 series appliances (2110, 2120, 2130, and 2140)
4k	Cisco Firepower 4100 series appliances (4110, 4120, 4140, 4150, 4115, 4125, and 4145)
9k	Cisco Firepower 9300 appliance (including security modules: SM-24, SM-36, SM-44, SM-40, SM-48, and SM-56)
AAA	Authentication, Authorization, and Accounting
ACP	Access Control Policy
AES	Advanced Encryption Standard
CA	Certificate Authority
CC	Common Criteria
DES	Data Encryption Standard
DH	Diffie Hellman (DH) - Key Technique used to exchange private encryption keys.
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
FCM	Firepower Chassis Manager (the WebUI of MIO)
FMC	Firepower Management Center
FTD	Firepower Threat Defense
FXOS	Firepower eXtensible Operating System
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP tunneling protocol that manages encryption between multiple hosts using secure communication
LAN	Local Area Network
MIO	Management Input/Output (FXOS running on the supervisor engine on 4k/9k platforms)
MS	Microsoft
PP	Protection Profile
rDSA	RSA Digital Signature Algorithm
RSA	Asymmetric cryptographic algorithm developed by Rivest, Shamir, and Adleman
SA	Security Association
SAR	Security Assurance Requirements
SM	Security Module (server blades running FTD within 4k/9k platforms)
SMB	Small and Medium-sized Business
SFP	Security Function Policy

Acronym or Abbreviation	Definition
SFR	Security Functional Requirements
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
VPN	Virtual Private Network

9 References and Related Documents

The following documentation was used to prepare this ST:

[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

10 Obtaining Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html