National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways

Version 1.1

01 July 2020

Report Number: CCEVS-VR-PP-071
Dated: 18 June 2021
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory
Base and Additional Requirements
Gossamer Security Solutions
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.1 (CFG_NDcPP-FW-VPNGW_V1.1). This PP-Configuration defines how to evaluate a TOE that claims conformance to the collaborative Protection Profile for Network Devices (CPP_ND_V2.2E) Base-PP, PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 (MOD_CPP_FW_V1.4e), and the PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1 (MOD_VPNGW_V1.1). It presents a summary of the CFG_NDcPP-FW-VPNGW_V1.1 and the evaluation results.

Gossamer Security Solutions, located in Columbia, Maryland, performed the evaluation of the CFG_NDcPP-FW-VPNGW_V1.1, MOD_CPP_FW_V1.4e, and MOD_VPNGW_V1.1 contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv (Cisco FTD).

This evaluation addressed the base security functional requirements of MOD_CPP_FW_V1.4e and MOD_VPNGW_V1.1 as part of CFG_NDcPP-FW-VPNGW_V1.1. The Module defines additional requirements, some of which the Cisco FTD evaluation claimed.

The Validation Report (VR) author independently performed an additional review of the PP-Configuration and Module as part of the completion of this VR, to confirm they met the claimed ACE requirements.

The evaluation determined the CFG_NDcPP-FW-VPNGW_V1.1 is both Common Criteria Part 2 extended and Part 3 conformant. A NIAP approved Common Criteria Testing Laboratory (CCTL) evaluated the PP-Configuration and Module identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 5). The Security Target (ST) includes material from CPP_ND_V2.2E, MOD_CPP_FW_V1.4e, and MOD_VPNGW_V1.1; completion of the ASE workunits satisfied the ACE workunits for this Module, but only for the materials defined in this Module, and only when this Module is in the defined PP-Configuration.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and Modules that have Evaluation Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 workunits specific to the technology described by the PP or Modules. Products may only be evaluated against Modules when a PP-Configuration is defined to include the Module with at least one corresponding Base-PP.

In order to promote thoroughness and efficiency, the evaluation of the CFG_NDcPP-FW-VPNGW_V1.1, MOD_CPP_FW_V1.4e, and MOD_VPNGW_V1.1 was performed concurrent with the first product evaluation to claim conformance to the PP-Configuration. In this case, the Target of Evaluation (TOE) was Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv, performed by Gossamer Security Solutions in Columbia, Maryland, United States.

This evaluation addressed the base security functional requirements of MOD_CPP_FW_V1.4e and MOD_VPNGW_V1.1 as part of CFG_NDcPP-FW-VPNGW_V1.1. The Module defined additional requirements, some of which the Cisco FTD evaluation claimed.

MOD_CPP_FW_V1.4e and MOD_VPNGW_V1.1 contain a set of base requirements that all conformant STs must include, and additionally contain optional and selection-based requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in other requirements and the capabilities of the TOE.

The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ workunits performed against the Modules. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the CFG_NDcPP-FW-VPNGW_V1.1 were evaluated.

The following identifies the Modules in the PP-Configuration evaluated by this VR. It also includes supporting information from the initial product evaluation performed against these Modules.

PP-Configuration	PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.1, 01 July 2020
Modules in PP-Configuration	PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1, 18 June 2020 PP-Module for Stateful Traffic Filter Firewall, Version 1.4e, 25 June 2020
ST (Base)	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv Security Target, Version 1.6, 24 May 2021
Assurance Activity Report (Base)	Assurance Activity Report (NDCPP22E/STFFW14E/VPNGW11) for Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCV, Version 0.3, 25 May 2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5

Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTL	Gossamer Security Solutions Columbia, Maryland 21045

3 CFG_NDcPP-FW-VPNGW_V1.1 Description

CFG_NDcPP-FW-VPNGW_V1.1 is a PP-Configuration that combines the following:

- collaborative Protection Profile for Network Devices, Version 2.2E (CPP_ND_V2.2E)
- Protection Profile Module for Stateful Traffic Filter Firewall, Version 1.4e (MOD_CPP_FW_1.4E)
- Protection Profile Module for Virtual Private Network (VPN) Gateways, Version 1.1 (MOD_VPNGW_V1.1)

The PP-Configuration defines a baseline set of security functional requirements (SFRs) for Firewall and VPN Gateway applications (defined in CPP_ND_V2.2E) that are bundled with agent applications to enforce configured policies on Firewalls (defined in MOD_CPP_FW_V1.3) and VPN Gateways (defined in MOD_VPNGW_V1.1).

A Stateful Traffic Filter Firewall and VPN Gateway are devices composed of hardware and software that are connected to two or more distinct networks and have an infrastructure role in the overall enterprise network.

Stateful traffic filtering refers to a capability of a firewall where the device tracks the state of each connection through it and have the ability to drop packets that do not appear to belong to a valid flow.

A VPN gateway establishes a secure tunnel that provides an authenticated and encrypted path to another sites and thereby decreases the risk of exposure of information transiting an untrusted network.

A TOE that conforms to CFG_NDcPP-FW-VPNGW_V1.1 is a network device that has both Stateful Traffic Filter Firewall and VPN gateway capabilities. The TOE is therefore able to allow authorized VPN peers to connect to the TOE's 'internal' network, while also examining any network traffic that transits the TOE boundary against stateful firewall rules such that unauthorized connections are discarded.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_NDcPP-FW-VPNGW_V1.1.

Note: Assumptions marked as "(applies to vNDs only)" are considered only if the TOE is a virtual network device (vND) and includes that assumption. The Cisco FTD product evaluated in the creation of this VR is not a vND and therefore does not include these assumptions.

Table 1: Assumptions

Assumption Name	Assumption Definition
From CPP_ND_V2.2E	
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or

Assumption Name	Assumption Definition
	otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES (applies to vNDs only)	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATION (applies to vNDs only)	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION (applies to vNDs only)	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.
From MOD_CPP_FW_V1.4e	
All Assumptions of the Base-PP apply also to this PP-Module. A.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module. This PP-Module extends the Base-PP threats (in section 4.1) to deal with traffic passing through the firewall, and addresses these additional threats with the TOE Security Objectives in section 5.1 and the SFRs (FDP_RIP.2, FFW_RUL_EXT.1, FFW_RUL_EXT.2, FMT_SMF.1/FFW) in section 6 and Appendix A.	

Assumption Name	Assumption Definition
From MOD_VPNGW_V1.1	
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.
All assumptions for the Operational Environment of the Base-PP also apply to this PP-Module. A.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.	

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_NDcPP-FW-VPNGW_V1.1.

Table 2: Threats

Threat Name	Threat Definition
From CPP_ND_V2.2E	
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

Threat Name	Threat Definition
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
From MOD_CPP_FW_V1.4e	
T.NETWORK_DISCLOSURE	An attacker may attempt to “map” a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported.
T.NEWORK_ACCESS	With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services.
T.NETWORK_MISUSE	An attacker may attempt to use services that are exported by machines in a way that is unintended by a site’s security policies. For example, an attacker might be able to use a service to “anonymize” the attacker’s machine as they mount attacks against others.
T.MALICIOUS_TRAFFIC	An attacker may attempt to send malformed packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash.
From MOD_VPNGW_V1.1	
T.DATA_INTEGRITY	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external

Threat Name	Threat Definition
	devices are able to communicate with devices on the protected network or if devices on the protected network can communicate with those external devices then the data contained within the communications may be susceptible to a loss of integrity.
T.NETWORK_ACCESS	Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network. From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network. From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled e-mail servers, or, that access to the mail server must be done over an encrypted link.
T.NETWORK_DISCLOSURE	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information. From an infiltration perspective, VPN gateways serve not only to limit access to only specific destination network addresses and ports within a protected network, but whether network traffic will be encrypted or transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected network thereby further limiting the potential disclosure of information. From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked

Threat Name	Threat Definition
	altogether or egress could be limited to specific addresses and/or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing.
T.NETWORK_MISUSE	Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network. From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services. From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a VPN gateway can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.
T.REPLAY_ATTACK	If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a "replay" attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions: • Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate segment of the communications to replay as well in order to cause the desired outcome. • No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured traffic and replay it to cause the desired outcome if the recipient has no means to detect these.

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_NDcPP-FW-VPNGW_V1.1.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
From CPP_ND_V2.2E	
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

OSP Name	OSP Definition
From MOD_CPP_FW_V1.4e	
No OSPs defined in MOD_CPP_FW_V1.4e.	
From MOD_VPNGW_V1.1	
No OSPs defined in MOD_VPNGW_V1.1.	

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_NDcPP-FW-VPNGW_V1.1.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From CPP_ND_V2.2E	
No security objectives for the TOE defined in CPP_ND_V2.2E.	
From MOD_CPP_FW_V1.4e	
O.RESIDUAL_INFORMATION	The TOE shall implement measures to ensure that any previous information content of network packets sent through the TOE is made unavailable either upon deallocation of the memory area containing the network packet or upon allocation of a memory area for a newly arriving network packet or both.
O.STATEFUL_TRAFFIC_FILTERING	The TOE shall perform stateful traffic filtering on network packets that it processes. For this the TOE shall support the definition of stateful traffic filtering rules that allow to permit or drop network packets. The TOE shall support assignment of the stateful traffic filtering rules to each distinct network interface. The TOE shall support the processing of the applicable stateful traffic filtering rules in an administratively defined order. The TOE shall deny the flow of network packets if no matching stateful traffic filtering rule is identified. Depending on the implementation, the TOE might support the stateful traffic filtering of Dynamic Protocols (optional).
From MOD_VPNGW_V1.1	
O.ADDRESS_FILTERING	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance, compliant TOE's will implement Packet Filtering capability. That capability will restrict the flow of network traffic between protected networks and other attached networks based on network addresses of the network nodes originating (source) and/or receiving (destination) applicable network traffic as well as on established connection information.
O.AUTHENTICATION	To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (IPSec) will allow a VPN peer to establish VPN connectivity with another VPN peer and ensure that any such connection attempt is both authenticated

TOE Security Objective	TOE Security Objective Definition
	and authorized. VPN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity.
O.CRYPTOGRAPHIC_FUNCTIONS	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption of services, and network-based reconnaissance, compliant TOE's will implement a cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE.
O.FAIL_SECURE	There may be instances where the TOE's hardware malfunctions or the integrity of the TOE's software is compromised, the latter being due to malicious or non-malicious intent. To address the concern of the TOE operating outside of its hardware or software specification, the TOE will shut down upon discovery of a problem reported via the self-test mechanism and provide signature-based validation of updates to the TSF.
O.PORT_FILTERING	To further address the issues associated with unauthorized disclosure of information, etc., a compliant TOE's port filtering capability will restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (or service) identified in the network traffic as well as on established connection information.
O.SYSTEM_MONITORING	To address the issues of administrators being able to monitor the operations of the VPN gateway, it is necessary to provide a capability to monitor system activity. Compliant TOEs will implement the ability to log the flow of network traffic. Specifically, the TOE will provide the means for administrators to configure packet filtering rules to 'log' when network traffic is found to match the configured rule. As a result, matching a rule configured to 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security associations (SAs) is auditable, not only between peer VPN gateways, but also with certification authorities (CAs).
O.TOE_ADMINISTRATION	TOEs will provide the functions necessary for an administrator to configure the packet filtering rules, as well as the cryptographic aspects of the IPsec protocol that are enforced by the TOE.

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_NDcPP-FW-VPNGW_V1.1.

Note: Security objectives for the operational environment marked as "(applies to vNDs only)" are considered only if the TOE is a virtual network device (vND) and includes that assumption. The ESR6300 product evaluated in the creation of this VR is not a vND and therefore does not include these objectives.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From CPP_ND_V2.2E	

Environmental Security Objective	Environmental Security Objective Definition
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs, the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.VM_CONFIGURATION (applies to vNDs only)	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting).

Environmental Security Objective	Environmental Security Objective Definition
	The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.
From MOD_CPP_FW_V1.4e	
All objectives for the Operational Environment of the Base-PP apply also to this PP-Module. OE.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.	
From MOD_VPNGW_V1.1	
OE.CONNECTIONS	The TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.
All objectives for the Operational Environment of the Base-PP also apply to this PP-Module. OE.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.	

5 Functional Requirements

As indicated above, CFG_NDcPP-FW-VPNGW_V1.1 includes CPP_ND_V2.2E, MOD_CPP_FW_V1.4e, and MOD_VPNGW_V1.1. The functional requirements from CPP_ND_V2.2E were evaluated separately so this section applies only to the requirements of MOD_CPP_FW_V1.4e and MOD_VPNGW_V1.1.

As indicated above, requirements in the MOD_CPP_FW_V1.4e and MOD_VPNGW_V1.1 are comprised of modified Base-PP, "base" requirements and additional requirements that are objective. The following table contains the modified "base" requirements that were validated as part of the Gossamer Security Solutions evaluation activities referenced above.

Table 6: Base-PP Modified Security Functional Requirements

Requirement Class	Requirement Component	Verified By
From MOD_CPP_FW_V1.4e		
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
From MOD_VPNGW_V1.1		
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
FCS: Cryptographic Support	FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
	FCS_IPSEC_EXT.1: IPsec Protocol	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
FIA: Identification and Authentication	FIA_X509_EXT.1/Rev: X.509 Certificate Validation	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
	FIA_X509_EXT.2: X.509 Certificate Authentication	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
	FIA_X509_EXT.3: X.509 Certificate Requests	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
FMT: Security Management	FMT_MTD.1/CryptoKeys: Management of TSF Data	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
	FMT_SMF.1: Specification of Management Functions	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv

Requirement Class	Requirement Component	Verified By
From MOD_CPP_FW_V1.4e		
FPT: Protection of the TSF	FPT_TST_EXT.1: TSF Testing	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
	FPT_TUD_EXT.1: Trusted Update	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv

The following table contains the "base" requirements specific to the TOE.

Table 7: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
From MOD_CPP_FW_V1.4e		
FDP: User Data Protection	FDP_RIP.2: Full Residual Information Protection	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
FFW: Firewall	FFW_RUL_EXT.1: Stateful Traffic Filtering	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
FMT: Security Management	FMT_SMF.1/FFW: Specification of Management Functions	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
From MOD_VPNGW_V1.1		
FCS: Cryptographic Support	FCS_CKM.1/IKE: Cryptographic Key Generation (for IKE Peer Authentication)	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
FMT: Security Management	FMT_SMF.1/VPN: Specification of Management Functions (VPN Gateway)	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
FPF: Packet Filtering	FPF_RUL_EXT.1: Rules for Packet Filtering	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
FPT: Protection of the TSF	FPT_FLS.1/SelfTest: Fail Secure (Self-Test Failures)	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
	FPT_TST_EXT.3: TSF Self-Test with Defined Methods	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
FTP: Trusted Path/Channels	FTP_ITC.1/VPN: Inter-TSF Trusted Channel (VPN Communications)	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of how those requirements were evaluated (from the list in the *Identification* section

above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant ACE workunits and has indicated its verification through "Module Evaluation."

Table 8: Optional Requirements

Requirement Class	Requirement Component	Verified By
From MOD_CPP_FW_V1.4e		
FFW: Firewall	FFW_RUL_EXT.2: Stateful Filtering of Dynamic Protocols	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
From MOD_VPNGW_V1.1		
FTA: TOE Access	FTA_SSL.3/VPN: TSF-Initiated Termination (VPN Headend)	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
	FTA_TSE.1: TOE Session Establishment	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv
	FTA_VCM_EXT.1: VPN Client Management	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant ACE workunits and has indicated its verification through "Module Evaluation."

Table 9: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
From MOD_CPP_FW_V1.4e		
No additional selection-based requirements.		
From MOD_VPNGW_V1.1		
FIA: Identification and Authentication	FIA_PSK_EXT.1: Pre-Shared Key Composition	Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv

The following table contains the "**Objective**" requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant ACE workunits and has indicated its verification through "Module Evaluation."

Table 10: Objective Requirements

Requirement Class	Requirement Component	Verified By
From MOD_CPP_FW_V1.4e		
No additional selection-based requirements.		
From MOD_VPNGW_V1.1		
No additional objective requirements.		

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by CPP_ND_V2.2E. The SARs defined in that PP are applicable to MOD_CPP_FW_V1.4e and MOD_VPNGW_V1.1, as well as CFG_NDcPP-FW-VPNGW_V1.1 as a whole.

7 Results of the Evaluation

Note that for ACE elements and workunits identical to ASE elements and workunits, the lab performed the ACE workunits concurrent to the ASE workunits.

Table 11: Evaluation Results

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module evaluation
ACE_CCL.1	Pass	Module evaluation
ACE_SPD.1	Pass	Module evaluation
ACE_OBJ.2	Pass	Module evaluation
ACE_ECD.1	Pass	Module evaluation
ACE_REQ.2	Pass	Module evaluation
ACE_MCO.1	Pass	Module evaluation
ACE_CCO.1	Pass	Module evaluation

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the MOD_VPNGW_V1.1 Evaluation Activities to determine whether the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process the CCEVS Validation Body uses that leads to the issuance of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e, 25 June 2020.

[7] PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1, 18 June 2020.

[8] collaborative Protection Profile for Network Devices, Version 2.2E, 23 March 2020.

[9] PP-Configuration for Network Devices, Stateful Traffic Filter Firewall, and Virtual Private Network (VPN) Gateways, Version 1.1, 01 July 2020.

[10] Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCv Security Target, Version 1.6, 24 May 2021

[11] Assurance Activity Report (NDCPP22E/STFFW14E/VPNGW11) for Cisco FTD (NGFW) 6.4 on Firepower 4100 and 9300 Series with FMC/FMCV, Version 0.3, 25 May 2021