DoD ANNEX
TO THE
COLLABORATIVE PROTECTION PROFILE (cPP) FOR STATEFUL TRAFFIC FILTER FIREWALLS V1.0

Version 1, Release 3

28 October 2016

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Background

This Annex to the collaborative Protection Profile (cPP) for Stateful Traffic Filter Firewalls (Version 1.0, dated 27 February 2015) delineates collaborative Protection Profile content that must be included in the Security Target (ST) for the Target of Evaluation (TOE) to be fully compliant with DoD cybersecurity policies pertaining to information systems. This content includes DoD-mandated cPP selections and assignments, and cPP security functional requirements (SFR Elements) listed as objective in the cPP but which are mandated in DoD.

Deficiencies of the TOE with respect to the DoD Annex will be reported as appropriate under the Risk Management Framework for DoD Information Technology (DoD Instruction 8510.01). DoD may determine that a TOE that does not conform to this Annex may pose an unacceptable risk to DoD. Accordingly, any vendor seeking authorization for use of its product within DoD should include the additional cPP specificity described in this Annex in its ST.

The Firewall cPP, in conjunction with this Annex, addresses the DoD-required cybersecurity controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Taken together, they supersede the DoD Firewall Security Requirements Guide.

1.2 Scope

The additional information in this document is applicable to all DoD-administered systems and all systems connected to DoD networks.

1.3 Relationship to Security Technical Implementation Guides (STIGs)

A successful Common Criteria evaluation certifies the capabilities of the TOE but does not assure its subsequent secure operation. To address security concerns with the ongoing operation of the TOE in the field, a product-specific STIG is prepared in conjunction with the Common Criteria evaluation. The STIG lists the configuration requirements for DoD implementations of the TOE and is published in eXtensible Configuration Checklist Description Format (XCCDF) to facilitate automation where feasible.

This Annex contains the required DoD configuration of features implementing the security management (FMT) class of SFR Elements listed in the Firewall cPP. For each applicable FMT SFR, the STIG will discuss the vulnerability associated with non-compliance configuration and provide step-by-step, product-specific procedures for checking for compliant configurations and fixing non-compliant configurations.

In most cases, the ST will not cover all security-relevant configurable parameters available in the TOE. However, the STIG will include these whenever they impact the security posture of DoD information systems and networks. Accordingly, the DoD Annex only addresses a subset of the controls expected to be included in a STIG.

1.4 Document Revisions

Comments or proposed revisions to this document should be sent via email to disa.stig_spt@mail.mil.

2. DOD-MANDATED SECURITY TARGET CONTENT

The following conventions are used to describe DoD-mandated ST content:

- If a cPP SFR is not listed, there is no DoD-mandated selection or assignment for that SFR.
- For cPP selections:
  - The presence of the selection indicates this is a DoD-mandated selection.
  - If a selection is not listed, then its inclusion or exclusion does not impact DoD compliance.
  - Underlined text indicates a selection.
  - *Italicized and underlined* text indicates an assignment within a selection.
  - ~~Strikethrough~~ text indicates that the ST author must exclude the selection.
- For cPP assignments:
  - The DoD-mandated assignments are listed after the assignment parameter.
  - If an assignment value appears in ~~strikethrough~~ text, this indicates that the assignment must not include this value.
  - *Italicized* text indicates an assignment.

The Annex provides the minimum text necessary to disambiguate selections and assignments. Readers will need to view both the Firewall cPP and the DoD Annex simultaneously to place the Annex information in context.

2.1 DoD-Mandated Selections and Assignments

DoD mandates the following cPP SFR selections and assignments for SFR Elements in Section 5 of the cPP:

Table 2-1: cPP SFR Selections

SFR	Selections, Assignments, and Application Notes
FMT_MTD.1.1	Application note: This includes audit data and any tools used to generate reports using audit data.
FAU_STG_EXT.1.3	*overwrite previous audit records according to the following rule: rule for overwriting previous audit records* = overwrite oldest records first Application note: The term "full" is defined as 75 percent of capacity in the context of a DoD implementation.
FFW_RUL_EXT.1.2	*IPv6 Extension header type [assignment: Next Header, Hdr Ext Len, Header Specific Data, Option Type, Opt Data Len, Option Data, Routing Type]*
FFW_RUL_EXT.1.6	Application note to a): an invalid fragment includes any improper use of fragment offsets, such as what might be used in a ping of death attack. *h) other default rules enforced by the TOE =*

SFR	Selections, Assignments, and Application Notes
	- block both inbound and outbound IPv6 Site Local Unicast addresses (FEC0::/10) - block IPv6 Jumbo Payload datagrams (Option Type 194). - drop all inbound and outbound IPv6 packets containing a Hop-by-Hop header with option type values intended for Destination Options - block RFC 6598 "Carrier Grade NAT" IP address block of 100.64.0.0/10 - drop all inbound IPv6 packets for which the layer 4 protocol and ports (undetermined transport) cannot be located. - drop all inbound IPv6 packets with a Type 0 Routing header - drop all inbound IPv6 packets with a Type 1 or Types 3 through 255 Routing Header. - drop all inbound IPv6 packets containing undefined header extensions/protocol values. - drop fragmented IPv6 packets when any fragment overlaps another. drop all inbound IPv6 packets containing more than one Fragmentation Header within an IP header chain. - drop all inbound and outbound IPv6 packets containing a Hop-by-Hop header with option type values intended for Destination Options. - block IPv6 multicast addresses (FF00::/8) as a source address.

2.2 DoD-Mandated Selection-Based and Optional

The following Security Functional Requirements (and associated selections and assignments) listed as selection-based and optional in the cPP are mandated for the DoD:

- FAU_STG.1.1
- FAU_STG.1.2
- FAU_STG_EXT.3.1
- FMT_MOF.1.1(1)/Audit
- FMT_MOF.1.1(2)/Audit
- FMT_MOF.1.1(1)/AdminAct
- FMT_MOF.1.1(2)/AdminAct
- FMT_MOF.1.1/LocSpace
- FMT_MTD.1.1/AdminAct
- FPT_FLS.1.1/LocSpace
- FCS_IPSEC_EXT.1.3
- FMT_MOF.1.1(2)/TrustedUpdate
- FIA_PMG_EXT.1.1
- FIA_X509_EXT.2.1
- FIA_X509_EXT.2.2
- FPT_TST_EXT.1.1
- FPT_TUD_EXT.1.2
- FPT_TUD_EXT.2.2

Application note: All "should" statements in the application notes to the SFR Elements listed above are required in DoD.

Table 2-2: cPP Selections and Assignments for Optional SFR Elements

SFR	Selections, Assignments, and Application Notes
FCS_IPSEC_EXT.1.3	*tunnel mode*
FMT_MOF.1.1(2)/ TrustedUpdate	*automatic checking for updates, automatic update* Application note: whatever options are supported under FPT_TUD_EXT.1.2 must be limited to the security administrator.
FIA_PMG_EXT.1.1	*"!", "@", "#","$", "%", "^", "&", "*", "(", ")"*
FIA_X509_EXT.2.1	*code signing for system software updates, code signing for integrity verification*
FIA_X509_EXT.2.2	*allow the administrator to choose whether to accept the certificate in these cases*
FPT_TST_EXT.1.1	*During initial start-up (on power on), periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-tests should occur] to demonstrate the correct operation of the TSF: [assignment: list of self-tests run by the TSF]*.
FPT_TUD_EXT.1.2	*support automatic updates*
FPT_TUD_EXT.2.2	*allow the administrator to choose whether to accept the certificate in these cases*

3. OTHER DOD MANDATES

3.1 Federal Information Processing Standard (FIPS) 140-2

Cryptographic modules supporting any SFR in the Cryptographic Support (FCS) class must be FIPS140-2 validated. While information concerning FIPS 140-2 validation should not be included in the ST, failure to obtain validation could preclude use of the TOE within DoD.

3.2 Federal Information Processing Standard (FIPS) 201-2

The firewall implementation is expected to interface with FIPS 201-2 compliant credentials (to include derived credentials as described in NIST Special Publication 800-157). The TOE may connect to a peripheral device (e.g., a smart card reader) in order to interface with PIV credentials, or natively store derived credentials (whose protections are evaluated in the Protection Profile).

3.3 Security State in Failure

Device is assumed to maintain security state or cease to forward traffic if or when it fails.

3.4 DoD-Mandated Configuration

The table below lists configuration values for product features implementing the cPP Specification of Management Functions (FMT_SMF). The ST is not expected to include this configuration information but it will be included in the product-specific STIG associated with the evaluated IT product. Non-binary configuration values are shown in *italics*.

Furthermore, the firewall implementation must not have unnecessary services and functions enabled. Only those functions and services that are necessary to support operations (mission requirements) must be enabled. This is consistent with A.LIMITED_FUNCTIONALITY (cPP Section 3.6.2). For example, if the device enables an insecure version of SNMP by default, it must be disabled.

Similarly, the firewall implementation must not enable the service or feature that automatically contacts a third party to report diagnostic or other information.

Table 3-1: Configuration Values

FMT_SMF_1.1 Function	DoD Selections and Values
Access banner	For firewalls accommodating advisory warning messages of 1300 characters: *You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.* *By using this IS (which includes any device attached to this IS), you consent to the following conditions:*

FMT_SMF_1.1 Function	DoD Selections and Values
	-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. *-At any time, the USG may inspect and seize data stored on this IS.* *-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.* *-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.* *-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.* *-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.* For firewalls with severe character limitations: *I've read & consent to terms in IS user agreem't.* **Application note**: To the extent permitted, the system should be configured to prevent further activity on the information system unless and until the user executes a positive action to manifest agreement to the advisory message.
Session inactivity time	*Security Administrator-configurable time interval of session inactivity* = 15 minutes. (implementing FTA_SSL.3.1 Refinement)
Firewall rules	*The firewall implementation must apply ingress filters entering the network to the external interface and egress filters leaving the network to the internal interface.* *The firewall implementation must manage excess bandwidth to limit the effects of packet flooding types of Denial of Service (DoS) attacks (rate limiting of traffic matching a rule).* *Specific rules:* *- block any packet with a source or destination of the IPv4 local host loopback address (127.0.0.0/8).* *- block any packet with a source or destination of the IPv6 local host loopback address (::1/128).* *- block any packet from the unspecified source address (::/128).*

FMT_SMF_1.1 Function	DoD Selections and Values
	- block IPv6 6to4 addresses for inbound and outbound traffic. (2002::/16) *- block IPv6 6bone address space on the ingress and egress filters (3FEE::/16).* *- block inbound IP packets using an RFC 1918 address space (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)* *- block inbound and outbound IPv6 Unique Local Unicast addresses (FC00::/7) (i.e., all hexadecimal addresses that begin with FC or FD).* *- block all inbound traceroutes.* *- block ICMPv6 type 134 (router advertisements)* *- block inbound packets where the destination is an IP address assigned to the management or loopback addresses of the enclave protection devices unless the packet has a source address assigned to the management network or network infrastructure.* *- block or limit IP packets destined to the control plane of the device itself.* *- block outbound IP packets that contain an illegitimate address in the source address field* *- block all ICMP responses on the external interface.* *- prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the PPSM CAL and vulnerability assessments.* *- information flow control policies set forth by the CYBERCOM J3 and the CC/S/A/FA J6.* **Application note**: The firewall implementation must only allow incoming communications from authorized sources routed to authorized destinations. The firewall implementation must be configured in accordance with the security configuration settings based on DoD security configuration or implementation guidance, including NSA configuration guides, Communications Tasking Orders (CTOs), and Directive-Type Memorandums (DTMs). Firewall rules in these documents and those specified or implied in the PPSM CAL, vulnerability assessments, and CYBERCOM J3 and the CC/S/A/FA J6 information control policies are expected to be defined in a manner consistent with FFW_RUL_EXT.1.2. Therefore, no additional TOE security functionality beyond the cPP is suggested by these statements.
Audit behavior	*- Transfer audit logs to an external IT entity on a real time basis.* *- Reveal error messages only to the Information System Security Officer (ISSO), Information System Security Manager (ISSM), or System Administrator (SA).* **Application note**: The ISSO, ISSM, and SA are personnel roles within DoD. If the TOE cannot support this requirement directly, it is acceptable to implement by assigning read permissions to the ISSO, ISSM, and SA roles on the external IT entity used to support FAU_STG_EXT.1.1.