Configuration Annex to the

Collaborative Protection Profile for Stateful Traffic Filter Firewalls + Errata

Annex Release 1

For collaborative Protection Profile Version 2.0e

31 July 2019

1. Purpose

This Configuration Annex to the collaborative Protection Profile (cPP) for Stateful Traffic Filter Firewall provides configuration requirements for Stateful firewalls. This Annex is consistent with [CNSSI-1253], which requires US National Security Systems to adhere to certain configuration parameters. Accordingly, configuration guidance produced according to the requirements of this Annex is suitable for use in US National Security Systems.

These configuration requirements serve the following audiences:

Audience	Purpose
IT Product Vendors	Use these guidelines to structure the creation of product-specific configuration guidance produced as part of a Common Criteria evaluation. The creation of administrative guidance is required by NIAP-approved Protection Profiles. The items specified in this document, as well as any best practices, should be provided as part of the administrative guidance. For each configuration item, the guidance must include the steps necessary to configure the setting of the product.
Test Labs	Use these guidelines to configure and test systems undergoing evaluation against a NIAP-approved Protection Profile. Using this guidance during evaluation provides assurance that the guidance is correct and implementable.
Network Owners and Assessors	Use these guidelines to assess the configuration of operational systems when product-specific guidance does not exist.

1.1 Relationship to NIST Risk Management Framework

In order to implement security controls from the NIST Risk Management Framework, each component of the information system must possess the necessary security functionality and also be properly configured to leverage that functionality.

NIAP Protection Profiles express requirements for security functionality for individual IT products within the overall information system. This includes management functions which indicate where an enterprise or end user is expected to be able to operationally configure the product. However, the Protection Profile does not indicate specific values for each configuration setting. This Annex specifies those specific requirements for operational configuration of a Stateful firewall. It also provides a mapping to each NIST control which the operational setting helps the overall system implement. This complements the control mapping provided with each Protection Profile, which is focused on security functionality.

Together, these documents support the creation of system security plans, as well as the Select, Implement, Assess, and Monitor steps of the Risk Management Framework (RMF).

2. Configuration Requirements

The table below describes configuration requirements for stateful traffic filter firewalls.

Each configuration requirement is associated with a security functional requirement (SFR) from the associated collaborative Protection Profile for Stateful Traffic Filter Firewall + Errata V2.0E. Each configuration requirement is also associated with a NIST 800-53 security control and CNSSI 1253 configuration value where applicable.

Configuration Action	NIST Control	CNSSI 1253 Value or DOD Specific Value	NIAP Reference
Ability to administer the TOE locally and remotely	AC-2(7)	*	FMT_MOF.1
Ability to configure the access banner	AC-8(a)	see text below	FMT_MOF.1
Configure the session inactivity time before session termination or locking	AC-2(5)	At the end of the users standard work period unless otherwise defined in formal organizational policy	FMT_MOF.1
Ability to update the TOE, and to verify the updates using [selection: digital signature, hash comparison] capability prior to installing those updates	SI-7(1)	*	FMT_MOF.1
Configure the Authentication Failures parameters to 3 within 15 minutes	AC-7	3 attempts in 15 mins	FMT_MOF.1
Ability to Configure firewall rules	SC-7	*	FMT_MOF.1
Ability to Configure audit behavior	AC-3	*	FMT_MOF.1
Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1	AC-14	*	FMT_MOF.1
Ability to configure the cryptographic functionality	SC-13	*	FMT_MOF.1
Ability to configure thresholds for SSH rekeying	AC-17(2)	*	FMT_MOF.1
Ability to configure the lifetime for IPsec SAs	IA-5(2)	*	FMT_MOF.1
Ability to configure the interaction between TOE components	AC-4	*	FMT_MOF.1
Ability to re-enable an Administrator account	AC-7	*	FMT_MOF.1
Ability to set the time which is used for time-stamps	AU-8	*	FMT_MOF.1
Ability to configure the reference identifier for the peer	IA-5(2)	*	FMT_MOF.1
Audit Administrative Logons (Success/Failure) and Logoff (Successful)	AU-2a.	1. Authentication events: (1) Logons (Success/Failure) (2) Logoffs (Success)	FAU_GEN.1.1c
Audit data related changes to configuration changes	AU-2a	Use of Privileged/Special Rights events: (1) Security or audit policy changes (Success/Failure) (2)Configuration changes (Success/Failure	FAU_GEN.1.1c
Audit Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).	AU-2a	*	FAU_GEN.1.1c
Audit resetting passwords (name of related user account shall be logged).	AU-2a	*	FAU_GEN.1.1c
Audit Starting and Stopping of services	AU-2a	*	FAU_GEN.1.1c

Logon Banner Text

For DoD Systems:
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:
-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.
-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 non-DoD NSS:
Organization-defined system use notification message or banner

3. References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[CNSSI-1253]	Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems, 27 March 2014