Network Device Protection Profile (NDPP) Extended Package
Stateful Traffic Filter Firewall

Information Assurance Directorate

19 December 2011

Version 1.0

Table of Contents

1 Introduction

This Extended Package (EP) describes security requirements for a Stateful Traffic Filter Firewall (defined to be a device that filters layers 3 and 4 (IP and TCP/UDP) network traffic optimized through the use of stateful packet inspection) is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats. However, this EP is not complete in itself, but rather extends the *Security Requirements for Network Devices* protection profile (NDPP). This introduction will describe the features of a compliant Target of Evaluation (TOE), and will also discuss how this EP is to be used in conjunction with the NDPP.

1.1 Conformance Claims

The *Security Requirements for Network Devices* Protection Profile (NDPP) defines the baseline Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for network infrastructure devices in general. This EP serves to extend the NDPP baseline with additional SFRs and associated 'Assurance Activities' specific to Stateful Traffic Filter Firewall network infrastructure devices. Assurance Activities are the actions that the evaluator performs in order to determine a TOE's compliance to the SFRs.

This EP conforms to *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 3. It is CC Part 2 extended and CC Part 3 conformant.

1.2 How To Use This Extended Package

As an EP of the NDPP, it is expected that the content of both this EP and the NDPP be appropriately combined in the context of each product-specific Security Target. This EP has been specifically defined such that there should be no difficulty or ambiguity in so doing. An ST must identify the applicable versions of the NDPP (see http://www.niap-ccevs.org/pp/ for the current version) and this EP in its conformance claims.

1.3 Compliant Targets of Evaluation

This EP is one of a series of related EPs that define requirements for the evaluation of network devices implementing firewall-related security features. Such products are generally boundary protection devices or sets of devices, such as dedicated firewalls, routers, or perhaps even switches designed to control the flow of information between attached networks. While in some cases network devices implementing firewall-related security features serve to segregate two distinct networks – a trusted or protected enclave and an untrusted external network such as the Internet – that is only one of many possible applications. It is common for firewalls to have multiple physical and logical network connections enabling a wide range of possible configurations and network information flow policies.

This EP specifically addresses network devices that perform network layer 3 and 4 stateful traffic filtering. A Stateful Traffic Filter Firewall is a device composed of hardware and software that is

connected to two or more distinct networks and has an infrastructure role in the overall enterprise network.

Since this EP builds on the NDPP, conformant TOEs are obligated to implement the functionality required in the NDPP along with the additional functionality defined in this EP in response to the threat environment discussed subsequently herein. Briefly, compliant TOEs will control the flow of information (i.e., packets) between attached networks based on configured rules based on network layer 3 and 4 traffic attributes (i.e., addresses and ports) and derived session state information potentially up to network layer 7.

It is intended that the set of requirements in this EP is limited in scope in order to promote quicker, less costly evaluations that provide some value to end users. Future drafts of this EP are envisioned, which will include optional functionality (e.g., transparent mode) in an appendix. Future Firewall EPs will be used to specify sets of additional functionality (e.g., Application Filtering), which can then be used by ST writers looking to specify additional functionality. In the context of this EP, additional features such as these are simply ignored for the purpose of evaluation except where they may have some effect of the security requirements defined herein. Another example of this is network address translation (NAT) or port address translation (PAT). While many devices that will be evaluated against this EP will have the capability to perform NAT or PAT, there are no requirements that specify this capability. This decision was made based on the premise that NAT and PAT are not primarily security mechanisms, but rather were created as a network addressing convenience; although some installations may believe it is a means to hide their network topology.

2 Security Problem Description

Stateful Traffic Filter Firewalls address a range of security threats related to infiltration into a protected network and exfiltration from a protected network. The term *protected network* is used here to represent an attached network for which rules are defined to control access. As such, a given Stateful Traffic Filter Firewall could potentially have a variety of attached protected and unprotected networks simultaneously depending on its specific configuration. Also, it should be clear that all attached networks are presumed to be *protectable* at the discretion of an authorized administrator.

The term ingress traffic is used below to represent traffic from threat agents that exist outside a protected network and the term egress traffic is used below to represent traffic from threat agents that exist inside a protected network. Applicable threats include unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance. However, relative to the data, it does not matter where the threat agent is located. Example: data exfiltration means that data was removed without proper authorization to remove it. That can be a pull or a push. It can result from intrusion from the outside or by the actions of the insider. A site is responsible for developing its security policy and configuring a ruleset that the firewall will enforce to meet their needs.

Note that this EP does not repeat the threats identified in the NDPP, though they all apply given the conformance and hence dependence of this EP on the NDPP. Note also that while the NDPP contains only threats to the ability of the TOE to provide its security functions, this EP addresses only business threats to resources in the operational environment. Together the threats of the NDPP and those defined in this EP define the comprehensive set of security threats addressed by a Stateful Traffic Filter Firewall TOE.

2.1 Unauthorized Disclosure of Information

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, Stateful Traffic Filter Firewalls serve to limit access to only specific *destination* network addresses and ports within a protected network. 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, Stateful Traffic Filter Firewalls 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 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 routed through authorized proxies or filters to further mitigate inappropriate disclosure of data through extrusion.

(T.NETWORK_DISCLOSURE)

2.2 Inappropriate Access to Services

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. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network.

From an ingress perspective, Stateful Traffic Filter Firewalls can be configured so that only those network servers intended for external consumption 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, Stateful Traffic Filter Firewalls can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled e-mail servers. Note that the effectiveness of a Stateful Traffic Filter Firewall is rather limited in this regard since external servers can offer their services on alternate ports – this is where an Application Filter Firewall offers more reliable protection, for example.

(T. NETWORK_ACCESS)

2.3 Misuse of Services

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, Stateful Traffic Filter Firewalls can log policy violations that might indicate violation of publicized usage statements for publicly available services.

From an egress perspective, Stateful Traffic Filter Firewalls can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a Stateful Traffic Filter Firewall 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, Stateful Traffic Filter Firewalls 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.NETWORK_MISUSE)

2.4 Disruption or Denial of Services

Stateful Traffic Filter Firewalls may be vulnerable to denial of services (DOS) attacks related to resource exhaustion in the event of coordinated service request flooding originating from outside of the protected network.

From an ingress perspective, Stateful Traffic Filter Firewalls can be configured so that only those network servers intended for external consumption are accessible and only via the intended ports and as a result potential attacks can be limited to select servers and services that have been configured (e.g., 'hardened') for that purpose. This serves to reduce available attack surface and mitigate the potential for external network attacks against internal servers. Attacks against even those servers that are externally accessible would be limited to the configured ports reducing the possible attack vectors.

From an egress perspective, Stateful Traffic Filter Firewalls can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network. For example, access to external mail servers can be blocked to reduce the chance of e-mail based attacks that might serve to introduce viruses, malware, etc. ultimately resulting in disruption of services on a protected network. Note that the effectiveness of a Stateful Traffic Filter Firewall is rather limited in this regard since external servers can offer their services on alternate ports – this is where an Application Filter Firewall offers more reliable protection, for example. However, logging can serve to help identify service disruptions that have not been prevented (e.g., by detecting the spread of viruses or 'botnet' activity patterns).

(T.NETWORK_DOS)

3 Security Objectives

The Security Problem described in Section 2 will be addressed primarily via Stateful Traffic Filtering capabilities. Compliant TOEs will provide security functionality that addresses threats to the TOE and enforces policies that are imposed by law or regulation. The following subsections provide a description of the security objectives required to meet the threats/policies previously discussed. The description of that security objectives are in addition to that described in [NDPP].

Note: in each subsection below particular security objectives are identified (highlighted by *O.*) and they are matched with the associated security functional requirements (SFRs) that provide the mechanisms to satisfy the objectives.

3.1 Address-Based 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 a Stateful Traffic 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.ADDRESS_FILTERING → FFW_RUL_EXT.1)

3.2 Port Based 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.PORT_FILTERING → FFW_RUL_EXT.1)

3.3 Stateful Inspection

Stateful packet inspection is used to aid in the performance of packet flow through the TOE. Rather than apply the ruleset against each packet that is processed at a TOE interface, the TOE will determine whether a packet belongs to an "approved" established connection. The minimum set of attributes that are used to determine whether a packet is part of an established session are mandated for TCP and UDP, and the ST author is allowed to expand the attributes considered for TCP sessions, and add the ICMP protocol if they desire.

(O.STATEFUL_INSPECTION → FFW_RUL_EXT.1)

3.4 Related Connection Filtering

This objective addresses the concept of "dynamic rule" creation, where due to the expected behavior of an application layer protocol, a new connection or path is created due to the creation of a connection that is allowed by the ruleset. The File Transfer Protocol is an example of such a protocol, where a data connection is created in response to an allowed command connection.

(O.RELATED_CONNECTION_FILTERING → FFW_RUL_EXT.1)

3.5 System Monitoring

To address the issues of System Administrators being able to monitor the operations of the Stateful Traffic Filtering capability this security objective, which originated in the NDPP, is extended as follows.

Compliant TOEs will implement the ability to log the flow of network traffic. Specifically, the TOE will provide the means for administrators to configure firewall specific firewall rules to 'log' when network traffic is found to match the configured rule. As a result, matching a firewall rule configured to 'log' will result in informative event logs whenever a match occurs.

(O.SYSTEM_MONITORING → FAU_GEN.1, FFW_RUL_EXT.1)

3.6 TOE Administration

To address the issues involved with a trusted means of administration of the Stateful Traffic Filtering capability this security objective, which originated in the NDPP, is extended as follows. *Note that it is*

assumed that use of the functions indicated below is protected in accordance with the requirements in the NDPP.

Compliant TOEs will provide the functions necessary for an administrator to configure the firewall rules that are enforced by the TOE.

(O.TOE_ADMINISTRATION → FMT_SMF.1)

4 Security Requirements

This section specifies a Security Functional Requirement for the TOE, as well as specifying the assurance activities the evaluator performs.

4.1 Conventions

While the SFR in this EP is extended, it is defined in a flexible manner for use in this and other EPs, or PPs, and as such operations are performed in the context of this EP.

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

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

4.2 TOE Security Functional Requirements

There is one SFR component with ten elements contained within this EP. In addition to the Stateful Traffic Filter SFR, there are two additions to the SFRs specified in the NDPP – FAU_Gen.1 (two audit events are added), and FMT_SMF.1 (management capability to configure the firewall rules).

4.2.1 FFW_RUL_EXT.1 Stateful Traffic Filtering

FFW_RUL_EXT.1.1 The TSF shall perform Stateful Traffic Filtering on network packets processed by the TOE.

Application Note: This element is identifies the policy (Stateful Traffic Filtering) that is applied to the network packets that are processed at the TOE's interfaces. Every packet that is received at a TOE's interface either has the ruleset that expresses this policy applied, or it is determined that the packet belongs to an established connection. The remaining elements in this component provide the details of the policy.

It is important to note that the TOE, which also includes the underlying platform, cannot permit network packets to flow unless the ruleset contains a rule that permits the flow, or the packet is deemed to belong to an established connection that has been permitted to flow. This is principle must hold true during TOE startup, and upon failures the TOE may encounter.

FFW_RUL_EXT.1.2 The TSF shall process the following network traffic protocols:

- Internet Control Message Protocol version 4 (ICMPv4)
- Internet Control Message Protocol version 6 (ICMPv6)
- Internet Protocol (IPv4)
- Internet Protocol version 6 (IPv6)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

and be capable of inspecting network packet header fields defined by the following RFCs to the extent mandated in the other elements of this SFR

- RFC 792 (ICMPv4)

- RFC 4443 (ICMPv6)
- RFC 791 (IPv4)
- RFC 2460 (IPv6)
- RFC 793 (TCP)
- RFC 768 (UDP).

Application Note: This element identifies the protocols and references the protocol definitions that serve to define to what extent the network traffic can be interpreted by the TOE when importing (receiving network traffic or ingress) and exporting (sending – or forming to be sent - network traffic or egress).

While the protocol formatting specified in the RFCs is still used, many RFCs define behaviors which are no longer considered safe to follow. For example, RFC792 defined the "Redirect" ICMP type, which is not considered safe to honor when it might come from an adversary; the "source quench" message, which is insecure because its source cannot be validated.

FFW_RUL_EXT.1.3 The TSF shall allow the definition of Stateful Traffic Filtering rules using the following network protocol fields:

- ICMPv4
    - Type
    - Code
- ICMPv6
    - Type
    - Code
- IPv4
    - Source address
    - Destination Address
    - Transport Layer Protocol
- IPv6
    - Source address
    - Destination Address
    - Transport Layer Protocol
- TCP
    - Source Port
    - Destination Port
- UDP
    - Source Port
    - Destination Port

and distinct interface.

Application Note: This element identifies the various attributes that are applicable when constructing rules to be enforced by this requirement – the applicable interface is a property of the TOE and the rest of the identified attributes are defined in the associated RFCs. Note that the 'Transport Layer Protocol' is the IPv4/IPv6 field that identifies the applicable protocol, such as TCP, UDP, ICMP, or GRE. Also, 'Interface' identified above is the external port where the applicable network traffic was received or alternately will be sent.

FFW_RUL_EXT.1.4 The TSF shall allow the following operations to be associated with Stateful Traffic Filtering rules: permit, deny, and log.

Application Note: This element defines the operations that can be associated with rules used to match network traffic. Note that the data to be logged is identified in the Security Audit requirements, Section 4.2.2.

FFW_RUL_EXT.1.5 The TSF shall allow the Stateful Traffic Filtering rules to be assigned to each distinct network interface.

Application Note: This element identifies where rules can be assigned. Specifically, a conforming TOE must be able to assign filtering rules specific to each of its available and identifiable distinct network interfaces that handle layer 3 and 4 network traffic. Identifiable means the interface is unique and identifiable within the TOE, and does not necessarily require the interface to be visible from the network perspective (e.g., does not need to have an IP address assigned to it). A distinct network interface is one or more physical connections that share a common logical path into the TOE. For example, the TOE might have a small form-factor pluggable (SFP) port supporting SFP modules that expose a number of physical network ports, but since a common driver is used for all external ports they can be treated as a single distinct network interface.

Note that there could be a separate ruleset for each interface or alternately a shared ruleset that somehow associates rules with specific interfaces.

FFW_RUL_EXT.1.6 The TSF shall:

a) accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols: TCP, UDP, [selection: ICMP, no other protocols] based on the following network packet attributes:

    1. TCP: source and destination addresses, source and destination ports, sequence number, Flags;

    2. UDP: source and destination addresses, source and destination ports;

    3. [selection: 'ICMP: source and destination addresses, [selection: type, code, *[assignment: list of matching attributes]*]', no other protocols].

b) Remove existing traffic flows from the set of established traffic flows based on the following: [selection: session inactivity timeout, completion of the expected information flow].

Application Note: This element requires that the protocols be identified for which the TOE can determine and manage the state such that sessions can be established and are used to make traffic flow decisions as opposed to fully processing the configured rules. This element also requires that applicable attributes used to determine whether a network packet matches and established session are identified.

If ICMP is selected as a protocol the source and destination addresses are required to be considered when determining if a packet belongs to an established "connection". The type and code attributes may be used to provide a more robust capability in determining whether an ICMP packet is what is expected in an established connection flow. For example, one would not expect echo replies to be part of a flow if an echo request had not been received. The open assignment in the selection for ICMP attributes is left for implementations that may use IPv6 attributes.

Item b) in this element requires specification of how the firewall can determine that established information flows should be removed from the set of established information flows by observing events such as the termination of a TCP session initiated by either endpoint with FIN flags in the TCP packet. If protocols are handled differently, it is expected that the ST would identify those differences.

FFW_RUL_EXT.1.7 The TSF shall be able to process the following network protocols:

1. FTP,
2. [selection: H.323: *[assignment: other supported protocols]*, no other protocols],

to dynamically define rules or establish sessions allowing network traffic of the following types:

- FTP: TCP data sessions in accordance with the FTP protocol as specified in RFC 959,
- [selection: *[assignment: list of additionally supported protocols and the types of network traffic to be allowed based on those protocols]*, none].

Application Note: This element requires the specification of more complex protocols that require the firewall to allow network traffic flow even though an existing rule does not explicitly allow the flow. For example, the FTP protocol requires both a control connection and a data connection if a user is to transfer files. While there are well-known ports involved, port 21 (control port on FTP server) and port 20 (data port on server in active mode), there are random ports > 1023 used on the client side. In passive mode, the FTP server may use a random port >1023 instead of port 20. The data connection is initiated by the client in passive mode, and imitated by the FTP server in active mode.

For these types of protocols, the establishment of a "new" connection is allowed, even though the ruleset may appear to deny it (e.g., since a rule cannot predict which random port will be used by the client or potentially the server, the default rule to deny may appear to apply). The TSF could create a dynamic rule that governs the traffic flow, or the TSF could implicitly allow the new connection to be established based on expectations of the protocol implementation as specified in the RFC.

It is important to note that there is no expectation that any network packets be inspected beyond layer 4 (TCP/UDP). This requirement simply requires that the ST author specify the conditions in which a "hole

is punched" into the firewall to allow expected connections with unpredictable UDP/TCP ports to correctly be established.

If the ST Author includes additional protocols they must identify the RFC that specifies the behavior of the protocol, as was done for FTP in item 2 above.

FFW_RUL_EXT.1.8 The TSF shall enforce the following default Stateful Traffic Filtering rules on all network traffic:

1. *The TSF shall reject and be capable of logging packets which are invalid fragments;*
2. *The TSF shall reject and be capable of logging fragmented IP packets which cannot be re-assembled completely;*
3. *The TSF shall reject and be capable of logging network packets where the source address of the network packet is equal to the address of the network interface where the network packet was received;*
4. *The TSF shall reject and be capable of logging network packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received;*
5. *The TSF shall reject and be capable of logging network packets where the source address of the network packet is defined as being on a broadcast network;*
6. *The TSF shall reject and be capable of logging network packets where the source address of the network packet is defined as being on a multicast network;*
7. *The TSF shall reject and be capable of logging network packets where the source address of the network packet is defined as being a loopback address;*
8. *The TSF shall reject and be capable of logging network packets where the source address of the network packet is a multicast;*
9. *The TSF shall reject and be capable of logging network packets where the source or destination address of the network packet is a link-local address;*
10. *The TSF shall reject and be capable of logging network packets where the source or destination address of the network packet is defined as being an address "reserved for future use" as specified in RFC 5735 for IPv4;*
11. *The TSF shall reject and be capable of logging network packets where the source or destination address of the network packet is defined as an "unspecified address" or an address "reserved for future definition and use" as specified in RFC 3513 for IPv6;*
12. *The TSF shall reject and be capable of logging network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified*; and

13. [selection: *[assignment: other default rules enforced by the TOE]*, no other rules].

Application Note: This element defines the minimum default rules that are always applied. Note that when packets might be rejected based on the rules identified above, the TOE also needs to be capable of logging so that related attacks might be detectable. Note that the data to be logged is identified in the Security Audit requirements.

Item 1 and item 2 above express how the TOE processes fragmented packets. Item 1, introduces the notion of invalid fragments, and allows the ST author to define what constitutes an invalid fragment. An acceptable implementation could consider any fragmented packet as invalid. Another acceptable implementation could consider a fragmented packet that partially overlaps a previously received fragment as invalid. Item 2 ensures that the ruleset is only applied when a packet is reassembled to address the threat of fragmented packet attacks. Note that in item 1, the logging of an invalid fragment may not be able to include all the fields that are expected in a packet header due to pieces missing in the invalid fragment.

In item 4, the intent is that the "networks associated" with the network interface may be beyond the immediate subnet associated with the interface. For example, the network topology could include a router and a subsequent subnet "behind" the firewall interface. Strict Reverse Path Forwarding would be an acceptable implementation to determine if this is the case, where Loose RPF would not be acceptable. The use of Access Control Lists may be another example of an acceptable implementation that allows this default to be overridden.

Item 13, provides the ST author the ability to specify additional rules that are enforced (either with or without specification in the administrator defined ruleset). The type of rules specified here could include things such as filtering of Christmas tree packets, filtering of non-SYN packets not related to an existing connection, and filtering of split handshake connections. This element could also be used to express behavior that *allows* packet flow, such as an ICMP response due to a host being unreachable.

FFW_RUL_EXT.1.9 When FFW_RUL_EXT.1.6 or FFW_RUL_EXT.1.7 do not apply, the TSF shall process the applicable Stateful Traffic Filtering rules (as determined in accordance with FFW_RUL_EXT.1.5) in the following order: administrator-defined.

Application Note: This element requires that an administrator is able to define the order in which configured filtering rules are processed for matches.

FFW_RUL_EXT.1.10 When FFW_RUL_EXT.1.6 or FFW_RUL_EXT.1.7 do not apply, the TSF shall deny packet flow if a matching rule is not identified.

Application Note: This element requires that, except when a packet is part of an established session, the behavior is always to deny network traffic when no rules apply and no other operations are required, though they are not necessarily prohibited.

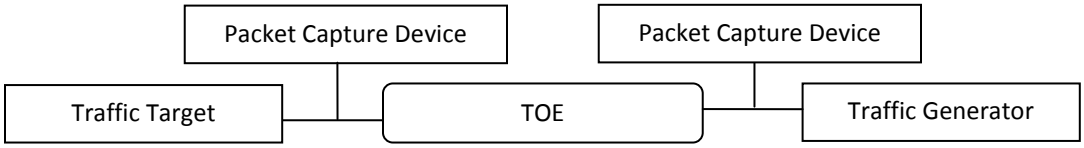
4.2.1.1 Assurance Activities

The following table defines the assurance activities to be performed by the evaluators in order to ensure conformance with FFW_RUL_EXT.1. The assurance activities are intended to address the required content of the TOE Summary Specification (TSS) of the ST, the required content of the TOE's operational guidance, and required test activities to be independently performed by the evaluators.

It is assumed the evaluator will have tools suitable to establish sessions, modify or create session packets, and perceive whether packets are getting through the TOE as well as to examine the content of those packets. In general, it is expected that traffic filter firewall rule configuration and logging capabilities of the TOE can be used to reach appropriate determinations where applicable.

The tests specified below need to be repeated for each distinct network interface type. Given the definition of interface type (all packets are processed through the same logical path within the TOE) tests are necessary to ensure all logical paths that a packet may take through the TOE adhere to the security policy specified by this EP.

The evaluators shall minimally create a test environment equivalent to the test environment illustrated below. The evaluators must provide Justification for any differences in the test environment.



4-1 FFW_RUL_EXT.1 Assurance Activities

SFR	Activity	Assurance Activity
FFW_RUL_EXT.1.1	**TSS**	The evaluator shall verify that the TSS provide a description of the TOE's initialization/startup process, which clearly indicates where processing of network packets begins to take place, and provides a discussion that supports the assertion that packets cannot flow during this process. The evaluator shall verify that the TSS also include a narrative that identifies the components (e.g., active entity such as a process or task) involved in processing the network packets and describe the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. This could include the failure of a component, such as a process being terminated, or a failure within a component, such as memory buffers full and cannot process packets.
	Guidance	The operational guidance associated with this requirement is assessed in the subsequent test assurance activities.
	Tests	Test 1: The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be directed at the TOE's interfaces, with packet sniffers listening to see if any network traffic is allowed through. Note: The remaining testing associated with application of the ruleset is addressed in the subsequent test assurance activities.
FFW	**TSS**	The evaluator shall verify that the TSS indicates that the following protocols are supported:

SFR	Activity	Assurance Activity
		• RFC 792 (ICMPv4) • RFC 4443 (ICMPv6) • RFC 791 (IPv4) • RFC 2460 (IPv6) • RFC 793 (TCP) • RFC 768 (UDP) The evaluator shall verify that the TSS describes how conformance with the identified RFCs has been determined by the TOE developer (e.g., third party interoperability testing, protocol compliance testing).
	Guidance	The evaluator shall verify that the operational guidance indicates that the following protocols are supported: • RFC 792 (ICMPv4) • RFC 4443 (ICMPv6) • RFC 791 (IPv4) • RFC 2460 (IPv6) • RFC 793 (TCP) • RFC 768 (UDP) If the guidance describes other protocols that are processed by the TOE, it should be made clear that those protocols were not considered as part of the TOE evaluation.
	Tests	The testing associated with this requirement is addressed in the subsequent test assurance activities.

FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4/FFW_RUL_EXT.1.5	**TSS**	The evaluator shall verify that the TSS describes a stateful packet filtering policy and the following attributes are identified as being configurable within stateful traffic filtering rules for the associated protocols:
		
		• ICMPv4
		  ○ Type
		  ○ Code
		• ICMPv6
		  ○ Type
		  ○ Code
		• IPv4
		  ○ Source address
		  ○ Destination Address
		  ○ Transport Layer Protocol
		• IPv6
		  ○ Source address
		  ○ Destination Address
		  ○ Transport Layer Protocol
		• TCP
		  ○ Source Port
		  ○ Destination Port
		• UDP
		  ○ Source Port
		  ○ Destination Port
		
		The evaluator shall verify that each rule can identify the following actions: permit, deny, and log.
		
		The evaluator shall verify that the TSS identifies all interface types subject to the stateful packet

SFR	Activity	Assurance Activity
		filtering policy and explains how rules are associated with distinct network interfaces. Where interfaces can be grouped into a common interface type (e.g., where the same internal logical path is used, perhaps where a common device driver is used) they can be treated collectively as a distinct network interface.

	Guidance	The evaluators shall verify that the operational guidance identifies the following attributes as being configurable within stateful traffic filtering rules for the associated protocols:
		• ICMPv4
		  ○ Type
		  ○ Code
		• ICMPv6
		  ○ Type
		  ○ Code
		• IPv4
		  ○ Source address
		  ○ Destination Address
		  ○ Transport Layer Protocol
		• IPv6
		  ○ Source address
		  ○ Destination Address
		  ○ Transport Layer Protocol
		• TCP
		  ○ Source Port
		  ○ Destination Port
		• UDP
		  ○ Source Port
		  ○ Destination Port
		The evaluator shall verify that the operational guidance indicates that each rule can identify the following actions: permit, deny, and log.
		The evaluator shall verify that the operational guidance explains how rules are associated with distinct network interfaces.
		The evaluator shall verify that the operational guidance explains how to determine the interface type of a distinct network interface (e.g., how to determine the device driver for a distinct network interface).

	Tests	Test 1: The evaluator shall use the instructions in the operational guidance to test that stateful packet filter firewall rules can be created that permit, deny, and log packets for each of the following attributes:
		• ICMPv4
		  ○ Type
		  ○ Code
		• ICMPv6
		  ○ Type
		  ○ Code
		• IPv4
		  ○ Source address
		  ○ Destination Address
		  ○ Transport Layer Protocol
		• IPv6

SFR	Activity	Assurance Activity
		○ Source address ○ Destination Address ○ Transport Layer Protocol • TCP ○ Source Port ○ Destination Port • UDP ○ Source Port ○ Destination Port Test 2: Repeat the test assurance activity above to ensure that stateful traffic filtering rules can be defined for each distinct network interface type supported by the TOE. Note that these test activities should be performed in conjunction with those of FFW_RUL_EXT.1.10 where the effectiveness of the rules is tested. The test activities for FFW_RUL_EXT.1.10 define the protocol/attribute combinations required to be tested. If those combinations are configured manually, that will fulfill the objective of these test activities, but if those combinations are configured otherwise (e.g., using automation), these test activities may be necessary in order to ensure the guidance is correct and the full range of configurations can be achieved by a TOE administrator.
FFW_RUL_EXT.1.6	**TSS**	The evaluator shall verify that the TSS identifies the protocols that support stateful session handling. The TSS shall identify TCP, UDP, and ICMP if selected by the ST author. The evaluator shall verify that the TSS describes how stateful sessions are established (including handshake processing) and maintained. The evaluator shall verify that for TCP, the TSS identifies and describes the use of the following attributes in session determination: source and destination addresses, source and destination ports, sequence number, and individual flags. The evaluator shall verify that for UDP, the TSS identifies and describes the following attributes in session determination: source and destination addresses, source and destination ports. The evaluator shall verify that for ICMP (if selected), the TSS identifies and describes the following attributes in session determination: source and destination addresses, other attributes chosen in FFW_RUL_EXT.1.6. The evaluator shall verify that the TSS describes how established stateful sessions are removed. The TSS shall describe how connections are removed for each protocol based on normal completion and/or timeout conditions. The TSS shall also indicate when session removal becomes effective (e.g., before the next packet that might match the session is processed).
	Guidance	The evaluator shall verify that the operational guidance describes stateful session behaviors. For example, a TOE might not log packets that are permitted as part of an existing session.
	Tests	Test 1: The evaluator shall configure the TOE to permit and log TCP traffic. The evaluator shall initiate a TCP session. While the TCP session is being established, the evaluator shall introduce session establishment packets with incorrect flags to determine that the altered traffic is not accepted as part of the session (i.e., a log event is generated to show the ruleset was applied). After a TCP session is successfully established, the evaluator shall alter each of the session determining attributes (source and destination addresses, source and destination ports, sequence number, flags) one at a time in order to verify that the altered packets are not accepted as part of the established session. Test 2: The evaluator shall terminate the TCP session established per Test 1 as described in the

SFR	Activity	Assurance Activity
		TSS. The evaluator shall then immediately send a packet matching the former session definition in order to ensure it is not forwarded through the TOE without being subject to the ruleset. Test 3: The evaluator shall expire (i.e., reach timeout) the TCP session established per Test 1 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset. Test 4: The evaluator shall configure the TOE to permit and log UDP traffic. The evaluator shall establish a UDP session. Once a UDP session is established, the evaluator shall alter each of the session determining attributes (source and destination addresses, source and destination ports) one at a time in order to verify that the altered packets are not accepted as part of the established session. Test 5: The evaluator shall expire (i.e., reach timeout) the UDP session established per Test 4 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset. Test 6: If ICMP is selected, the evaluator shall configure the TOE to permit and log ICMP traffic. The evaluator shall establish a session for ICMP as defined in the TSS. Once an ICMP session is established, the evaluator shall alter each of the session determining attributes (source and destination addresses, other attributes chosen in FFW_RUL_EXT.1.6) one at a time in order to verify that the altered packets are not accepted as part of the established session. Test 7: If applicable, the evaluator shall terminate the ICMP session established per Test 6 as described in the TSS. The evaluator shall then immediately send a packet matching the former session definition in order to ensure it is not forwarded through the TOE without being subject to the ruleset. Test 8: The evaluator shall expire (i.e., reach timeout) the ICMP session established per Test 6 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset.
FFW_RUL_EXT.1.7	**TSS**	The evaluator shall verify that the TSS identifies the protocols that can cause the automatic creation of dynamic packet filtering rules. In some cases rather than creating dynamic rules, the TOE might establish stateful sessions to support some identified protocol behaviors. The TSS shall identify FTP and optionally other protocols. The evaluator shall verify that the TSS explains the dynamic nature of session establishment and removal. The TSS also shall explain any logging ramifications. The evaluator shall verify that for FTP, the TSS explains how FTP data sessions will be allowed through the TOE in response to FTP control sessions. The evaluator shall verify that for each of the other protocols selected, the TSS explains the dynamic nature of session establishment and removal specific to the protocol.
	Guidance	The evaluator shall verify that the operational guidance describes dynamic session establishment capabilities. The evaluator shall verify that the operational guidance describes the logging of dynamic sessions consistent with the TSS.
	Tests	Test 1: The evaluator shall define stateful traffic filtering rules to permit and log an FTP session and deny and log TCP ports above 1024. Subsequently, the evaluator shall establish an FTP session in order to ensure that it succeeds. The evaluator shall examine the generated logs to verify they are consistent with the operational guidance. Test 2: Continuing from Test 1, the evaluator shall determine (e.g., using a packet sniffer) which

SFR	Activity	Assurance Activity
		port above 1024 is being used by the FTP data session, terminate the FTP session, and then verify that TCP packets cannot be sent through the TOE using the same source and destination addresses and ports. Test 3: For each additionally supported protocol, the evaluator shall repeat the procedure above for the protocol. In each case the evaluator must use the applicable RFC or standard in order to determine what range of ports to block in order to ensure the dynamic rules are created and effective.
FFW_RUL_EXT.1.8	**TSS**	The evaluator shall verify that the TSS identifies the following as packets that will be automatically rejected and are capable of being logged: 1. Packets which are invalid fragments, including a description of what constitutes an invalid fragment 2. Fragments that cannot be completely re-assembled 3. Packets where the source address is equal to the address of the network interface where the network packet was received 4. Packets where the source address does not belong to the networks associated with the network interface where the network packet was received, including a description of how the TOE determines whether a source address belongs to a network associated with a given network interface 5. Packets where the source address is defined as being on a broadcast network 6. Packets where the source address is defined as being on a multicast network 7. Packets where the source address is defined as being a loopback address 8. Packets where the source address is defined as being a reserved address as specified in RFC 1918 for IPv4, and RFC 3513 for IPv6 9. Packets where the source or destination address of the network packet is a link-local address 10. Packets where the source or destination address of the network packet is defined as being an address “reserved for future use” as specified in RFC 5735 for IPv4 11. Packets where the source or destination address of the network packet is defined as an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6 12. Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified 13. Other packets defined in FFW_RUL_EXT.1.8.
	Guidance	The evaluator shall verify that the operational guidance describes packets that are discarded and potentially logged by default. If applicable protocols are identified, their descriptions need to be consistent with the TSS. If logging is configurable, the evaluator shall verify that applicable instructions are provided to configure auditing of automatically rejected packets.
	Tests	Test 1: The evaluator shall test each of the conditions for automatic packet rejection in turn. In each case, the TOE should be configured to allow all network traffic and the evaluator shall generate a packet or packet fragment that is to be rejected. The evaluator shall use packet captures to ensure that the unallowable packet or packet fragment is not passed through the TOE. Test 2: For each of the cases above, the evaluator shall use any applicable guidance to enable rejected packet logging. In each case above, the evaluator shall ensure that the rejected packet or packet fragment was appropriately logged.
FFW_	**TSS**	The evaluator shall verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an

SFR	Activity	Assurance Activity
		established session, and application of administrator defined and ordered ruleset.
	Guidance	The evaluator shall verify that the operational guidance describes how the order of stateful traffic filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing.
	Tests	Test 1: The evaluator shall devise two equal stateful traffic filtering rules with alternate operations – permit and deny. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation. Test 2: The evaluator shall repeat the procedure above, except that the two rules should be devised where one is a subset of the other (e.g., a specific address vs. a network segment). Again, the evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule.
FFW_RUL_EXT.1.10	**TSS**	The evaluator shall verify that the TSS describes the process for applying stateful traffic filtering rules and also that the behavior (either by default, or as configured by the administrator) is to deny packets when there is no rule match unless another required conditions allows the network traffic (i.e., FFW_RUL_EXT.1.6 or FFW_RUL_EXT.1.7).
	Guidance	The evaluator shall verify that the operational guidance describes the behavior if no rules or special conditions apply to the network traffic. If the behavior is configurable, the evaluator shall verify that the operational guidance provides the appropriate instructions to configure the behavior to deny packets with no matching rules.
	Tests	Test 1: The evaluator shall configure the TOE to permit and log each defined ICMPv4 Type and Code (see table 4-2 Defined Protocol-specific Attributes). The evaluator will generate packets matching each defined ICMPv4 Type and Code in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Test 2: The evaluator shall configure the TOE to deny and log each defined ICMPv4 Type and Code (see table 4-2 Defined Protocol-specific Attributes). The evaluator will generate packets matching each defined ICMPv4 Type and Code in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Test 3: The evaluator shall configure the TOE with no ICMPv4 rules. The evaluator will generate packets matching each defined ICMPv4 Type and Code in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE). Test 4: The evaluator shall configure the TOE to permit and log each defined ICMPv6 Type and Code (see table 4-2 Defined Protocol-specific Attributes). The evaluator will generate packets matching each defined ICMPv6 Type and Code in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Test 5: The evaluator shall configure the TOE to deny and log each defined ICMPv6 Type and Code (see table 4-2 Defined Protocol-specific Attributes). The evaluator will generate packets matching each defined ICMPv6 Type and Code in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Test 6: The evaluator shall configure the TOE with no ICMPv6 rules. The evaluator will generate packets matching each defined ICMPv6 Type and Code in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE). Test 7: The evaluator shall configure the TOE to permit and log each defined IPv4 Transport Layer Protocol (see table 4-2 Defined Protocol-specific Attributes) in conjunction with a specific

SFR	Activity	Assurance Activity
		source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv4 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Test 8: The evaluator shall configure the TOE to permit all traffic except to deny and log each defined IPv4 Transport Layer Protocol (see table 4-2 Defined Protocol-specific Attributes) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv4 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Test 9: The evaluator shall configure the TOE to permit and log each defined IPv4 Transport Layer Protocol (see table 4-2 Defined Protocol-specific Attributes) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. Additionally, the evaluator shall configure the TOE to deny and log each defined IPv4 Transport Layer Protocol (see table 4-2 Defined Protocol-specific Attributes) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv4 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE). Test 10: The evaluator shall configure the TOE to permit and log each defined IPv6 Transport Layer Protocol (see table 4-2 Defined Protocol-specific Attributes) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Test 11: The evaluator shall configure the TOE to permit all traffic except to deny and log each defined IPv6 Transport Layer Protocol (see table 4-2 Defined Protocol-specific Attributes) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Test 12: The evaluator shall configure the TOE to permit and log each defined IPv6 Transport Layer Protocol (see table 4-2 Defined Protocol-specific Attributes) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address

SFR	Activity	Assurance Activity
		and wildcard destination address. Additionally, the evaluator shall configure the TOE to deny and log each defined IPv6 Transport Layer Protocol (see table 4-2 Defined Protocol-specific Attributes) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE). Test 13: The evaluator shall configure the TOE to permit and log TCP using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Test 14: The evaluator shall configure the TOE to deny and log TCP using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Test 15: The evaluator shall configure the TOE to permit and log UDP using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Test 16: The evaluator shall configure the TOE to deny and log UDP using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged.

The following table identifies the RFC defined type, code, and transport layer attributes for the applicable protocols to be used in configuring and otherwise testing stateful traffic filter firewall rule definition and enforcement. Note that TCP and UDP are not included in the table since the only required attributes defined for those protocols are network addresses and ports all of which are potentially usable within a given TOE operational environment.

4-2 Defined Protocol-specific Attributes

Protocol	Defined Attributes
ICMPv4	Type 0 (Echo Reply) Type 3 (Destination Unreachable) Type 3 code 0 (Net Unreachable) Type 3 code 1 (Host Unreachable) Type 3 code 2 (Protocol Unreachable) Type 3 code 3 (Port Unreachable) Type 3 code 4 (Fragmentation Needed and Don't Fragment was set) Type 3 code 5 (Source Route Failure) Type 3 code 6 (Destination Network Unknown) Type 3 code 7 (Destination Host Unknown)

Protocol	Defined Attributes
	Type 3 code 8 (Source Host Isolated) Type 3 code 9 (Communication with Destination Network is Administratively Prohibited) Type 3 code 10 (Communication with Destination Host is Administratively Prohibited) Type 3 code 11 (Destination Network Unreachable for Type of Service) Type 3 code 12 (Destination Host Unreachable for Type of Service) Type 3 code 13 (Communication Administratively Prohibited) Type 4 (Source Quench) Type 5 (Redirect) Type 5 code 0 (Redirect Datagram for the Network (or subnet)) Type 5 code 1 (Redirect Datagram for the Host) Type 5 code 2 (Redirect Datagram for the Type of Service and Network) Type 5 code 3 (Redirect Datagram for the Type of Service and Host) Type 6 (Alternative Address for Host) Type 6 code 0 (Alternate Address for Host) Type 8 (Echo) Type 9 (Router Advertisement) Type 10 (Router Selection) Type 11 (Time Exceeded) Type 11 code 0 (Time to Live exceeded in Transit) Type 11 code 1 (Fragment Reassembly Time Exceeded) Type 12 (Parameter Problem) Type 12 code 0 (Pointer indicates the error) Type 12 code 1 (Missing a Required Option) Type 12 code 2 (Bad Length) Type 13 (Timestamp) Type 14 (Timestamp Reply) Type 15 (Information Request) Type 16 (Information Reply) Type 17 (Address Mask Request) Type 18 (Address Mask Reply) Type 30 (Traceroute) Type 31 (Datagram Conversion Error) Type 32 (Mobile Host Redirect) Type 35 (Mobile Registration Request) Type 36 (Mobile Registration Reply)
ICMPv6	Type 1 (Destination Unreachable) Type 1 code 0 (no route to destination) Type 1 code 1 (communication with destination administratively prohibited) Type 1 code 2 (beyond scope of source address) Type 1 code 3 (address unreachable) Type 1 code 4 (port unreachable) Type 1 code 5 (source address failed ingress/egress policy) Type 1 code 6 (reject route to destination) Type 1 code 7 (Error in Source Routing Header) Type 2 (Packet Too Big) Type 3 (Time Exceeded) Type 3 code 0 (hop limit exceeded in transit) Type 3 code 1 (fragment reassembly time exceeded) Type 4 (Parameter Problem) Type 4 code 0 (erroneous header field encountered) Type 4 code 1 (unrecognized Next Header type encountered) Type 4 code 2 (unrecognized IPv6 option encountered) Type 100 (Private Experimentation) Type 101 (Private Experimentation) Type 128 (Echo Request) Type 129 (Echo Reply) Type 130 (Multicast Listener Query) Type 131 (Multicast Listener Report) Type 132 (Multicast Listener Done) Type 133 (Router Solicitation) Type 134 (Router Advertisement) Type 135 (Neighbor Solicitation) Type 136 (Neighbor Advertisement) Type 137 (Redirect Message)

Protocol	Defined Attributes
	Type 138 (Router Renumbering) Type 138 code 0 (Router Renumbering Command) Type 138 code 1 (Router Renumbering Result) Type 138 code 225 (Sequence Number Reset) Type 139 (ICMP Node Information Query) Type 139 code 0 (The data field contains an IPv6 address which is the subject of this query) Type 139 code 1 (The data field contains a name which is the subject of this query or is empty, as in the case of a NOOP) Type 139 code 2 (The Data field contains an IPv4 address which is the Subject of this Query.) Type 140 (ICMP Node Information Response) Type 140 code 0 (A successful reply. The Reply Data field may or may not be empty) Type 140 code 1 (The Responder refuses to supply the answer. The Reply Data field will be empty) Type 140 code 2 (Qtype of the Query is unknown to the Responder. The Reply Data field will be empty) Type 141 (Inverse Neighbor Discovery Solicitation Message) Type 142 (Inverse Neighbor Discovery Advertisement Message) Type 143 (Version 2 Multicast Listener Report) Type 144 (Home Agent Address Discovery Request Message) Type 145 (Home Agent Address Discovery Reply Message) Type 146 (Mobile Prefix Solicitation) Type 147 (Mobile Prefix Advertisement) Type 148 (Certification Path Solicitation Message) Type 149 (Certification Path Advertisement Message) Type 150 (ICMP messages utilized by experimental mobility protocols such as Seamoby) Type 151 (Multicast Router Advertisement) Type 152 (Multicast Router Solicitation) Type 153 (Multicast Router Termination) Type 154 (FMIPv6 Messages) Type 155 (RPL Control Message)
IPv4	Transport Layer Protocol 1 - Internet Control Message Transport Layer Protocol 2 - Internet Group Management Transport Layer Protocol 3 - Gateway-to-Gateway Transport Layer Protocol 4 - IP in IP (encapsulation) Transport Layer Protocol 5 - Stream Transport Layer Protocol 6 - Transmission Control Transport Layer Protocol 7 - UCL Transport Layer Protocol 8 - Exterior Gateway Protocol Transport Layer Protocol 9 - any private interior gateway Transport Layer Protocol 10 - BBN RCC Monitoring Transport Layer Protocol 11 - Network Voice Protocol Transport Layer Protocol 12 - PUP Transport Layer Protocol 13 - ARGUS Transport Layer Protocol 14 - EMCON Transport Layer Protocol 15 - Cross Net Debugger Transport Layer Protocol 16 - Chaos Transport Layer Protocol 17 - User Datagram Transport Layer Protocol 18 - Multiplexing Transport Layer Protocol 19 - DCN Measurement Subsystems Transport Layer Protocol 20 - Host Monitoring Transport Layer Protocol 21 - Packet Radio Measurement Transport Layer Protocol 22 - XEROX NS IDP Transport Layer Protocol 23 - Trunk-1 Transport Layer Protocol 24 - Trunk-2 Transport Layer Protocol 25 - Leaf-1 Transport Layer Protocol 26 - Leaf-2 Transport Layer Protocol 27 - Reliable Data Protocol Transport Layer Protocol 28 - Internet Reliable Transaction Transport Layer Protocol 29 - ISO Transport Protocol Class 4 Transport Layer Protocol 30 - Bulk Data Transfer Protocol Transport Layer Protocol 31 - MFE Network Services Protocol Transport Layer Protocol 32 - MERIT Internodal Protocol Transport Layer Protocol 33 - Sequential Exchange Protocol Transport Layer Protocol 34 - Third Party Connect Protocol Transport Layer Protocol 35 - Inter-Domain Policy Routing Protocol Transport Layer Protocol 36 - XTP Transport Layer Protocol 37 - Datagram Delivery Protocol

Protocol	Defined Attributes
	Transport Layer Protocol 38 - IDPR Control Message Transport Protocol Transport Layer Protocol 39 - TP++ Transport Protocol Transport Layer Protocol 40 - IL Transport Protocol Transport Layer Protocol 41 - Simple Internet Protocol Transport Layer Protocol 42 - Source Demand Routing Protocol Transport Layer Protocol 43 - SIP Source Route Transport Layer Protocol 44 - SIP Fragment Transport Layer Protocol 45 - Inter-Domain Routing Protocol Transport Layer Protocol 46 - Reservation Protocol Transport Layer Protocol 47 - General Routing Encapsulation Transport Layer Protocol 48 - Mobile Host Routing Protocol Transport Layer Protocol 49 - BNA Transport Layer Protocol 50 - SIPP Encap Security Payload Transport Layer Protocol 51 - SIPP Authentication Header Transport Layer Protocol 52 - Integrated Net Layer Security TUBA Transport Layer Protocol 53 - IP with Encryption Transport Layer Protocol 54 - NBMA Next Hop Resolution Protocol Transport Layer Protocol 61 - any host internal protocol Transport Layer Protocol 62 - CFTP Transport Layer Protocol 63 - any local network Transport Layer Protocol 64 - SATNET and Backroom EXPAK Transport Layer Protocol 65 - Kryptolan Transport Layer Protocol 66 - MIT Remote Virtual Disk Protocol Transport Layer Protocol 67 - Internet Pluribus Packet Core Transport Layer Protocol 68 - any distributed file system Transport Layer Protocol 69 - SATNET Monitoring Transport Layer Protocol 70 - VISA Protocol Transport Layer Protocol 71 - Internet Packet Core Utility Transport Layer Protocol 72 - Computer Protocol Network Executive Transport Layer Protocol 73 - Computer Protocol Heart Beat Transport Layer Protocol 74 - Wang Span Network Transport Layer Protocol 75 - Packet Video Protocol Transport Layer Protocol 76 - Backroom SATNET Monitoring Transport Layer Protocol 77 - SUN ND PROTOCOL-Temporary Transport Layer Protocol 78 - WIDEBAND Monitoring Transport Layer Protocol 79 - WIDEBAND EXPAK Transport Layer Protocol 80 - ISO Internet Protocol Transport Layer Protocol 81 - VMTP Transport Layer Protocol 82 - SECURE-VMTP Transport Layer Protocol 83 - VINES Transport Layer Protocol 84 - TTP Transport Layer Protocol 85 - NSFNET-IGP Transport Layer Protocol 86 - Dissimilar Gateway Protocol Transport Layer Protocol 87 - TCF Transport Layer Protocol 88 - IGRP Transport Layer Protocol 89 - OSPFIGP Transport Layer Protocol 90 - Sprite RPC Protocol Transport Layer Protocol 91 - Locus Address Resolution Protocol Transport Layer Protocol 92 - Multicast Transport Protocol Transport Layer Protocol 93 - AX.25 Frames Transport Layer Protocol 94 - IP-within-IP Encapsulation Protocol Transport Layer Protocol 95 - Mobile Internetworking Control Protocol Transport Layer Protocol 96 - Semaphore Communications Security Protocol Transport Layer Protocol 97 - Ethernet-within-IP Encapsulation Transport Layer Protocol 98 - Encapsulation Header Transport Layer Protocol 99 - any private encryption scheme Transport Layer Protocol 100 - GMTP
IPv6	Transport Layer Protocol 0 - IPv6 Hop-by-Hop Option Transport Layer Protocol 1 - Internet Control Message Transport Layer Protocol 2 - Internet Group Management Transport Layer Protocol 3 - Gateway-to-Gateway Transport Layer Protocol 4 - IPv4 encapsulation Transport Layer Protocol 5 - Stream Transport Layer Protocol 6 - Transmission Control

Protocol	Defined Attributes
	Transport Layer Protocol 7 - CBT Transport Layer Protocol 8 - Exterior Gateway Protocol Transport Layer Protocol 9 - any private interior gateway Transport Layer Protocol 10 - BBN RCC Monitoring Transport Layer Protocol 11 - Network Voice Protocol Transport Layer Protocol 12 - PUP Transport Layer Protocol 13 - ARGUS Transport Layer Protocol 14 - EMCON Transport Layer Protocol 15 - Cross Net Debugger Transport Layer Protocol 16 - Chaos Transport Layer Protocol 17 - User Datagram Transport Layer Protocol 18 - Multiplexing Transport Layer Protocol 19 - DCN Measurement Subsystems Transport Layer Protocol 20 - Host Monitoring Transport Layer Protocol 21 - Packet Radio Measurement Transport Layer Protocol 22 - XEROX NS IDP Transport Layer Protocol 23 - Trunk-1 Transport Layer Protocol 24 - Trunk-2 Transport Layer Protocol 25 - Leaf-1 Transport Layer Protocol 26 - Leaf-2 Transport Layer Protocol 27 - Reliable Data Protocol Transport Layer Protocol 28 - Internet Reliable Transaction Transport Layer Protocol 29 - Transport Protocol Class 4 Transport Layer Protocol 30 - Bulk Data Transfer Protocol Transport Layer Protocol 31 - MFE Network Services Protocol Transport Layer Protocol 32 - MERIT Internodal Protocol Transport Layer Protocol 33 - Datagram Congestion Control Protocol Transport Layer Protocol 34 - Third Party Connect Protocol Transport Layer Protocol 35 - Inter-Domain Policy Routing Protocol Transport Layer Protocol 36 - XTP Transport Layer Protocol 37 - Datagram Delivery Protocol Transport Layer Protocol 38 - IDPR Control Message Transport Proto Transport Layer Protocol 39 - TP++ Transport Protocol Transport Layer Protocol 40 - IL Transport Protocol Transport Layer Protocol 41 - IPv6 encapsulation Transport Layer Protocol 42 - Source Demand Routing Protocol Transport Layer Protocol 43 – Routing Header for IPv6 Transport Layer Protocol 44 – Fragment Header for IPv6 Transport Layer Protocol 45 - Inter-Domain Routing Protocol Transport Layer Protocol 46 - Reservation Protocol Transport Layer Protocol 47 - General Routing Encapsulation Transport Layer Protocol 48 - Dynamic Source Routing Protocol Transport Layer Protocol 49 - BNA Transport Layer Protocol 50 - Encap Security Payload Transport Layer Protocol 51 - Authentication Header Transport Layer Protocol 52 - Integrated Net Layer Security Transport Layer Protocol 53 - IP with Encryption Transport Layer Protocol 54 - NBMA Address Resolution Protocol Transport Layer Protocol 55 - Mobility Transport Layer Protocol 56 - Transport Layer Security Protocol using Kryptonet key management Transport Layer Protocol 57 - SKIP Transport Layer Protocol 58 – ICMP for IPv6 Transport Layer Protocol 59 – No Next Header for IPv6 Transport Layer Protocol 60 – Destination Options for IPv6 Transport Layer Protocol 61 - any host internal protocol Transport Layer Protocol 62 - CFTP Transport Layer Protocol 63 - any local network Transport Layer Protocol 64 - SATNET and Backroom EXPAK Transport Layer Protocol 65 - Kryptolan Transport Layer Protocol 66 - MIT Remote Virtual Disk Protocol Transport Layer Protocol 67 - Internet Pluribus Packet Core Transport Layer Protocol 68 - any distributed file system Transport Layer Protocol 69 - SATNET Monitoring Transport Layer Protocol 70 - VISA Protocol

Protocol	Defined Attributes
	Transport Layer Protocol 71 - Internet Packet Core Utility Transport Layer Protocol 72 - Computer Protocol Network Executive Transport Layer Protocol 73 - Computer Protocol Heart Beat Transport Layer Protocol 74 - Wang Span Network Transport Layer Protocol 75 - Packet Video Protocol Transport Layer Protocol 76 - Backroom SATNET Monitoring Transport Layer Protocol 77 - SUN ND PROTOCOL-Temporary Transport Layer Protocol 78 - WIDEBAND Monitoring Transport Layer Protocol 79 - WIDEBAND EXPAK Transport Layer Protocol 80 - ISO Internet Protocol Transport Layer Protocol 81 - VMTP Transport Layer Protocol 82 - SECURE-VMTP Transport Layer Protocol 83 - VINES Transport Layer Protocol 84 - TTP Transport Layer Protocol 84 - Internet Protocol Traffic Manager Transport Layer Protocol 85 - NSFNET-IGP Transport Layer Protocol 86 - Dissimilar Gateway Protocol Transport Layer Protocol 87 - TCF Transport Layer Protocol 88 - EIGRP Transport Layer Protocol 89 - OSPFIGP Transport Layer Protocol 90 - Sprite RPC Protocol Transport Layer Protocol 91 - Locus Address Resolution Protocol Transport Layer Protocol 92 - Multicast Transport Protocol Transport Layer Protocol 93 - AX.25 Frames Transport Layer Protocol 94 - IP-within-IP Encapsulation Protocol Transport Layer Protocol 95 - Mobile Internetworking Control Pro. Transport Layer Protocol 96 - Semaphore Communications Sec. Pro. Transport Layer Protocol 97 - Ethernet-within-IP Encapsulation Transport Layer Protocol 98 - Encapsulation Header Transport Layer Protocol 100 - GMTP Transport Layer Protocol 101 - Ipsilon Flow Management Protocol Transport Layer Protocol 102 - PNNI over IP Transport Layer Protocol 103 - Protocol Independent Multicast Transport Layer Protocol 104 - ARIS Transport Layer Protocol 105 - SCPS Transport Layer Protocol 106 - QNX Transport Layer Protocol 107 - Active Networks Transport Layer Protocol 108 - Payload Compression Protocol Transport Layer Protocol 109 - Sitara Networks Protocol Transport Layer Protocol 110 - Compaq Peer Protocol Transport Layer Protocol 111 - IPX in IP Transport Layer Protocol 112 - Virtual Router Redundancy Protocol Transport Layer Protocol 113 - PGM Reliable Transport Protocol Transport Layer Protocol 114 - any 0-hop protocol Transport Layer Protocol 115 - Layer Two Tunneling Protocol Transport Layer Protocol 116 - D-II Data Exchange (DDX) Transport Layer Protocol 117 - Interactive Agent Transfer Protocol Transport Layer Protocol 118 - Schedule Transfer Protocol Transport Layer Protocol 119 - SpectraLink Radio Protocol Transport Layer Protocol 120 - UTI Transport Layer Protocol 121 - Simple Message Protocol Transport Layer Protocol 122 - SM Transport Layer Protocol 123 - Performance Transparency Protocol Transport Layer Protocol 124 - ISIS over IPv4 Transport Layer Protocol 125 - FIRE Transport Layer Protocol 126 - Combat Radio Transport Protocol Transport Layer Protocol 127 - Combat Radio User Datagram Transport Layer Protocol 128 - SSCOPMCE Transport Layer Protocol 129 - IPLT Transport Layer Protocol 130 - Secure Packet Shield Transport Layer Protocol 131 - Private IP Encapsulation within IP Transport Layer Protocol 132 - Stream Control Transmission Protocol Transport Layer Protocol 133 - Fibre Channel Transport Layer Protocol 134 - RSVP-E2E-IGNORE

Protocol	Defined Attributes
	Transport Layer Protocol 135 - Mobility Header Transport Layer Protocol 136 - UDPLite Transport Layer Protocol 137 - MPLS-in-IP Transport Layer Protocol 138 - MANET Protocols Transport Layer Protocol 139 - Host Identity Protocol Transport Layer Protocol 140 - Shim6 Protocol Transport Layer Protocol 141 - Wrapped Encapsulating Security Payload Transport Layer Protocol 142 - Robust Header Compression

4.2.2 Security Audit

There are no additional SFRs for security audit. However, there are additional auditable events that serve to extend the FAU_GEN.1 SFR found in the NDPP. As such, the following events should be combined with those of the NDPP in the context of a conforming Security Target.

The following audit events are applicable when the Firewall SFRs are claimed.

4-3 FAU_GEN.1 Audit Event and Details

SFR	Audit Event	Additional Details
FFW_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets

4.2.2.1 Assurance Activities

The following table defines the assurance activities to be performed by the evaluators in order to ensure conformance with FAU_GEN.1.

4-4 FAU_GEN.1 Assurance Activities

SFR	Activity	Assurance Activity
FAU_GEN.1.1/FAU_GEN.1.2	**TSS**	The evaluator shall verify that the TSS describes how the stateful traffic filter firewall rules can be configured to log network traffic associated with applicable rules. Note that this activity should have been addressed with a combination of the TSS assurance activities for FFW_RUL_EXT.1. The evaluator shall verify that the TSS describes how the TOE behaves when one of its interfaces is overwhelmed by network traffic. It is acceptable for the TOE to drop packets that it cannot process, but under no circumstances is the TOE allowed to pass packets that do not satisfy a rule that allows the permit operation or belong to an allowed established session. It may not always be possible for the TOE to audit dropped packets due to implementation limitations. These limitations and circumstances in which the event of dropped packets is not audited shall be described in the TSS.

SFR	Activity	Assurance Activity
	Guidance	The evaluator shall verify that the operational guidance describes how to configure the stateful traffic filter firewall rules to result in applicable network traffic logging. Note that this activity should have been addressed with a combination of the guidance assurance activities for FFW_RUL_EXT.1.
	Tests	Test 1: The evaluator shall test that the interfaces used to configure the stateful traffic filter firewall rules for logging yield expected network traffic logs in association with the applicable rules. A number of rule combination and ordering scenarios need to be configured and tested by attempting to pass both valid and invalid network traffic matching rules design to permit, deny and log matching network traffic. Note that this activity should have been addressed with a combination of the Test assurance activities for FFW_RUL_EXT.1. Test 2: The evaluator shall attempt to flood the TOE with network packets such that the TOE will be unable to process all the packets. This may require the evaluator to configure the TOE to limit the bandwidth the TOE is capable to handling (e.g., use of a 10 MB interface).

4.2.3 Security Management

There are no additional SFRs for security management. As indicated in the NDPP, access to the rules, defaults, etc. that serve to define the firewall behaviors are restricted to the Security Administrator. No additional role is specifically required for those security management functions.

The NDPP includes FMT_SMF.1 requiring the existence of specific security management functions. The following security management functions are applicable when Firewall SFRs are claimed. As such, the following security management functions should be combined with those of the NDPP in the context of a conforming Security Target.

4-5 FMT_SMF.1 Security Management Functions

SFR	Security Management Functions
FFW_RUL_EXT.1	Configure Firewall rules

4.2.3.1 Assurance Activities

The following table defines the assurance activities to be performed by the evaluators in order to ensure conformance with FMT_SMF.1.

4-6 FMT_SMF.1 Assurance Activities

SFR	Activity	Assurance Activity
FMT_SMF.1.1	**TSS**	The evaluator shall verify that the TSS describes how the stateful traffic filter firewall rules can be configured. Note that this activity should have been addressed with the TSS assurance activities for FFW_RUL_EXT.1.

SFR	Activity	Assurance Activity
	Guidance	The evaluator shall verify that the operational guidance describes how to configure the stateful traffic filter firewall rules, including how to set any configurable defaults and how to configure each of the applicable rule attributes, actions, and associated interfaces. The evaluator must ensure that the operational guidance also provides instruction that would allow an administrator to ensure that configured rules are properly ordered. Note that this activity should have been addressed with the Guidance assurance activities for FFW_RUL_EXT.1.
	Tests	Test 1: The evaluator shall devise tests that demonstrate that the functions used to configure the stateful traffic filter firewall rules yield expected changes in the rules that they are correctly enforced. A number of rule combination and ordering scenarios need to be configured and tested by attempting to pass both valid and invalid network traffic through the TOE. Note that this activity should have been addressed with a combination of the Test assurance activities for FFW_RUL_EXT.1.

4.3 Security Assurance Requirements

It is important to note that a TOE that is evaluated against this EP is inherently evaluated against the NDPP as well. The NDPP includes a number of Assurance Activities associated with both Security Functional Requirements (SFRs) and SARs. Additionally, this EP includes a number of SFR-based Assurance Activities that similarly refine the SARs associated with the EAL identified in the NDPP. The assurance activities associated with SARs that are prescribed by the NDPP are performed against the entire TOE, with the addition of the specific vulnerability testing described here.

4.3.1 AVA_VAN.1 Vulnerability survey

Assurance Activity:

The evaluator shall generate network packets that cycle through all of the values for attributes, Type, Code, and Transport Layer Protocol, that are undefined by the RFC for each of the protocols, ICMPv4, ICMPv6, IPv4, and IPv6. For example, ICMPv4 has an eight-byte field for Type and an eight-byte field for the Code. Only 21 Types are defined in the RFC (see table 4-2), but there are 256 possible value. Each Type has a Code associated with it, the number of RFC defined Codes varies based on the Type. The evaluator is required to construct packets that exercise each possible value not defined in the RFC (the defined values are already tested in FFW_RUL_EXT.1.10) of Type and Code (including all possible combinations) and target each distinct interface type to determine that the TOE handles these packets appropriately. Since none of these packets will match a rule, or belong to an allowed session the packets should be dropped. Since there are no requirements that the firewall audit a packet being dropped under these circumstances, the evaluator shall ensure the firewall does not allow these packets to flow through the TOE.

In addition to the undefined attribute testing required above, the evaluator shall perform intelligent fuzz testing of the remaining fields in the required protocol headers (excluding FTP). The intent of intelligent fuzzing is that a packet that is otherwise correctly constructed, such that it will be denied when the ruleset is applied, has random values inserted into each of the protocol header fields. The evaluator

ensures a statistically significant sample size, which will vary depending on the protocol field length, is used and is justified in their report.

The evaluator should consult whatever diagnostics (e.g., logging, process status, interface errors) the TOE offers to determine if the TOE was adversely impacted by the processing of such packets.

5 Rationale

In this EP, the focus in the initial sections of the document is to use a narrative presentation in an attempt to increase the overall understandability of the threats addressed by Stateful Traffic Filter Firewalls; the methods used to mitigate those threats; and the extent of the mitigation achieved by compliant TOEs. This presentation style does not readily lend itself to a formalized evaluation activity, so this section contains the tabular artifacts that can be used for the evaluation activities associated with this document.

5.1 Security Problem Definition

5.1.1 Assumptions

The specific conditions listed below are assumed to exist in the TOE's Operational Environment. These assumptions are in addition to those defined in the NDPP and include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

5-1 TOE Assumptions

Assumption Name	Assumption Definition
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.

5.1.2 Threats

The threats listed below are addressed by Stateful Traffic Filter Firewalls. Note that these threats are in addition to those defined in the NDPP, all of which apply to Stateful Traffic Filter Firewalls.

5-2 Threats

Threat Name	Threat Definition
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T. NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network.
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to Operational Environment policies.
T.NETWORK_DOS	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network.

5.1.3 Organizational Security Policies

No organizational policies have been identified that are specific to Stateful Traffic Filter Firewalls. However, all the organizational security policies in the NDPP apply to Stateful Traffic Filter Firewalls.

5.1.4 Security Problem Definition Correspondence

The following table serves to map the threats and assumptions defined in this EP to the security objectives also defined or identified in this EP.

5-3 Security Problem Definition Correspondence

Threat or Assumption	Security Objectives
A.CONNECTIONS	OE.CONNECTIONS
T.NETWORK_DISCLOSURE	O.ADDRESS_FILTERING and O.PORT_FILTERING
T. NETWORK_ACCESS	O.ADDRESS_FILTERING, O.RELATED_CONNECTION_FILTERING and O.PORT_FILTERING
T.NETWORK_MISUSE	O.ADDRESS_FILTERING, O.PORT_FILTERING and O.SYSTEM_MONITORING
T.NETWORK_DOS	O.ADDRESS_FILTERING, O.STATEFUL_INSPECTION and O.PORT_FILTERING

5.2 Security Objectives

5.2.1 Security Objectives for the TOE

The following table contains security objectives specific to Stateful Traffic Filter Firewalls. These security objectives are in addition to those defined in the NDPP, all of which apply to Stateful Traffic Filter Firewalls. Note that while two of the NDPP security objectives (O.SYSTEM_MONITORING and O.TOE_ADMINISTRATION) have been extended in this EP, that does not affect the corresponding security objective definitions.

5-4 Security Objectives for the TOE

Security Objective Name	Security Objective Definition
O.ADDRESS_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination addresses.
O.PORT_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination transport layer ports.
O.STATEFUL_INSPECTION	The TOE will determine if a network packet belongs to an allowed established connection before applying the ruleset.
O.RELATED_CONNECTION_FILTERING	For specific protocols, the TOE will dynamically permit a network packet flow in response to a connection permitted by the ruleset.

5.2.2 Security Objectives for the Operational Environment

The following table contains security objectives specific to the operational environments for Stateful Traffic Filter Firewalls. These security objectives are in addition to those defined in the NDPP, all of which apply to the operational environments for Stateful Traffic Filter Firewalls.

5-5 Security Objectives for the Operational Environment

Security Objective Name	Security Objective Definition
OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic

	flowing among attached networks.

5.2.3 Security Objective Correspondence

The correspondence between the Security Functional Requirements (SFRs) and Security Objectives identified or defined in this EP is provided in section 3.