IPv6 Test Service

Network Protection Product

Conformance Test Plan

Version 2.2

University of New Hampshire
InterOperability Laboratory
IPv6 Test Service
https://www.iol.unh.edu

21 Madbury Road, Suite 100
Durham, NH 03824
Phone: +1-603-862-0090
Fax: +1-603-862-4181

Table of Contents

Acknowledgements

The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite.

Alan Lagace	University of New Hampshire
Christopher Brown	University of New Hampshire
Timothy Carlin	University of New Hampshire
Ben Patton	University of New Hampshire

This document includes updated versions of test cases from Network Protection Devices Test Specification, version 1.3, authored by ICSA Labs.

References

[NIST IPv6 Profile]	"NIST IPv6 Profile", NIST Special Publication (NIST SP) - 500-267Ar1, November 2020. https://doi.org/10.6028/NIST.SP.500-267Ar1
[USGv6-R1]	"USGv6 Profile", NIST Special Publication (NIST SP) - 500-267Br1, November 2020. https://doi.org/10.6028/NIST.SP.500-267Br1

Introduction

Overview

The University of New Hampshire's InterOperability Laboratory (IOL) is an institution designed to improve the interoperability of standards-based products by providing an environment where a product can be tested against other implementations of a standard. This suite of tests has been developed to help implementers evaluate the functionality of their products that support Firewall and Intrusion Detection/Prevention capabilities. This test suite has been designed to test the conformance of a device under test with the specification in NIST-500-267Ar1.

Definitions

NPP	Network Protection Product
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Messaging Protocol
TN	Test Node
ACL	Access Control List

Test Organization

This document organizes tests by group based on related test methodology or goals. Each group begins with a brief set of comments pertaining to all tests within that group. This is followed by a series of description blocks; each block describes a single test. The format of the description block is as follows:

Test Label	The **Test Label** is the first line of the test page. It will have the following form: NPP.A.B Where each component indicates the following: NPP – Test Suite Identifier A – Group Number B – Test Number Scripts implementing this test suite should follow this convention and may also append a character in the set [a-z] indicating a particular test part.
Purpose	The **Purpose** is a short statement describing what the test attempts to achieve. It is usually phrased as a simple assertion of the feature or capability to be tested.
References	The **References** section lists cross-references to the specifications and documentation that might be helpful in understanding and evaluating the test and results
Test Setup	The **Test Setup** section describes the configuration of all devices prior to the start of the test. Different parts of the procedure may involve configuration steps that deviate from what is given in the test setup. If a value is not provided for a protocol parameter, then the protocol's default is used for that parameter.
Procedure and Expected Behavior	The **Procedure and Expected Behavior** table contains the step-by-step instructions for carrying out the test. These steps include such things as enabling interfaces, unplugging devices from the network, or sending packets from a test station. The test procedure also cues the tester to make observations of expected behavior, as needed, as not all steps require observation of results. If any behavior is expected for a procedure, it is to be observed prior to continuing to the next step. Failure to observe any behavior prior to continuing constitutes a failed test. Note, that while test numbers continue between test parts, each test part is to be executed independently, and are not cascaded from the previous part.
Possible Problems	The **Possible Problems** section contains a description of known issues with the test procedure, which may affect test results in certain situations.

Common Topology

The following topologies are used for an NPP.

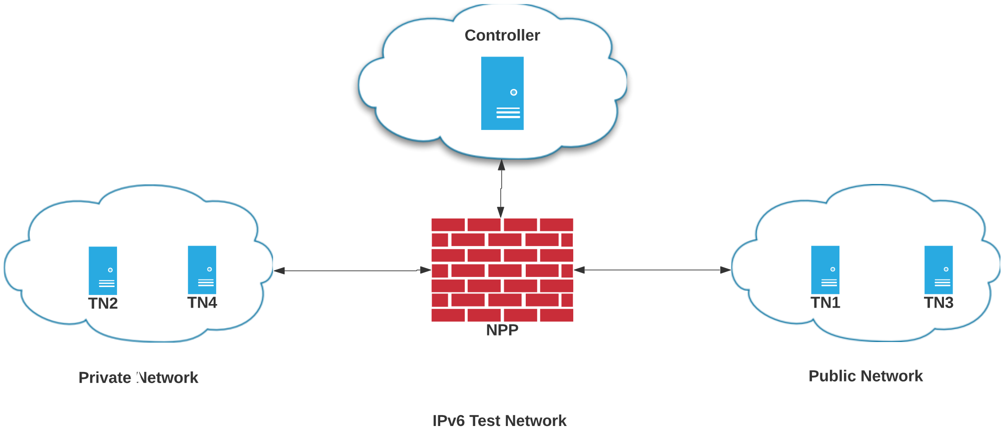

Figure 1: Layer 3 NPP Topology

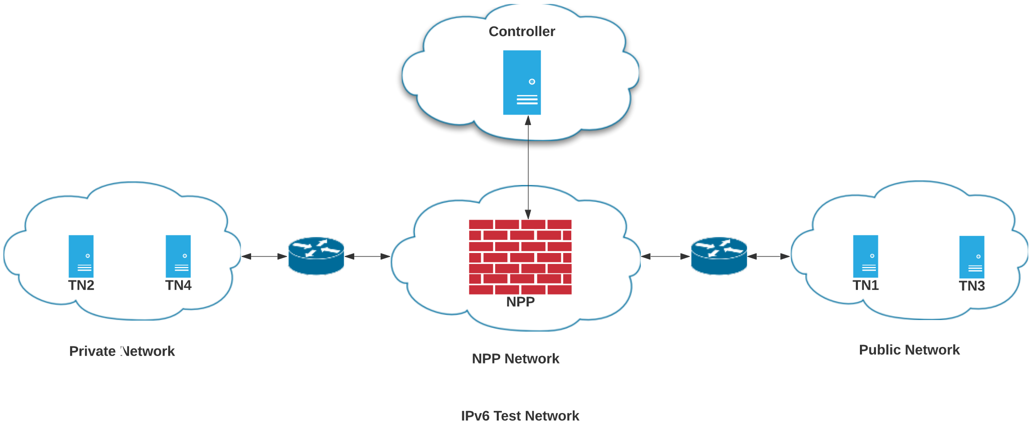

Figure 2: Layer 2 NPP Topology

- The administrative interface must be configured and accessible over IPv6-Only.
- Any test nodes not specified in these topologies are incremented by one IPv6 address.

Group 1: Common Requirements

Scope

These tests are designed to verify device functionality regarding common requirements for all Network Protection Products, unless otherwise excluded based on the product type definitions.

Overview

The tests in this group verify conformance of a device regarding common requirements for NPPs according to NIST 500-267Ar1.

Test NPP.1.1: Configuration of Protective Functionality

Purpose: To verify that an NPP's administrative interface has the ability to configure protective functionality.

Reference:

- [NIST 500-267Ar1] – Section 4.14.3.3

Test Setup: An administrative interface is made accessible. Such administrative functionality MUST be available either directly on the network protection device console or equivalent, or through remote communications using openly defined means.

Procedure:

Step	Action	Expected Behavior
1.	Add new rules to the NPP.	The new rules added must function as expected.
2.	Remove rules from the NPP.	The removed rules must no longer function.
3.	Alter rules on the NPP.	The altered rules must function as expected.

Possible Problems: None.

Test NPP.1.2: Configuration of Logging and Alert Facility Configurations

Purpose: To verify that an NPP's administrative interface has the ability to modify its logging and alert facility configurations.

Reference:

- [NIST 500-267Ar1] – Section 4.14.3.3

Test Setup: An administrative interface is made accessible, logging is enabled, and if remote logging is supported, then remote logging is also enabled. Such administrative functionality MUST be available either directly on the network protection device console or equivalent, or through remote communications using openly defined means.

Procedure:

Step	Action	Expected Behavior
1.	Enable logging and alert facilities on available items. If remote logging is supported, then it is also enabled and configured.	
2.	Trigger events to create log messages.	The NPP logging features must operate as configured.

Possible Problems: None.

Test NPP.1.3: Selectively Restricting Rights to the Administrative Interface

Purpose: To verify that an NPP's administrative controls are secure from non-authorized access and restricted to appropriately authorized users.

Reference:

- [NIST 500-267Ar1] – Section 4.14.3.4

Test Setup: An administrative interface is made accessible. Such administrative functionality MUST be available either directly on the network protection device console or equivalent, or through remote communications using openly defined means.

Procedure:

Step	Action	Expected Behavior
1.	Attempt to connect to the various administrative interfaces (e.g., GUI, serial, ssh) necessary for testing, by using credentials of a user that does not exist or was not given administrative rights.	The NPP must not allow administrative access to users without administrative access or to users who do not exist.
2.	Attempt to connect to the various administrative interfaces by using credentials with no password.	The NPP must not allow administrative access to users who attempt to use credentials with no password.
3.	Scan interfaces for applicable set of vulnerabilities.	
4.	Attempt to gain access to the administrative interfaces through any found vulnerabilities.	The NPP must not allow administrative access due to vulnerabilities.

Possible Problems: None.

Test NPP.1.4: Individual Rights

Purpose: To verify that an NPP enforces any individual rights applied to each user.

Reference:

- [NIST 500-267Ar1] – Section 4.14.3.4

Test Setup: An administrative interface is made accessible. Such administrative functionality MUST be available either directly on the network protection device console or equivalent, or through remote communications using openly defined means.

Procedure:

Step	Action	Expected Behavior
1.	Create two user accounts with different rights applied to each.	The individual rights applied to each user must operate as expected.

Possible Problems: None.

Test NPP.1.5: Administrative Communications

Purpose: To verify that an NPP properly supports at least one form of secure administrative communication.

Reference:

- [NIST 500-267Ar1] – Section 4.14.3.5

Test Setup: An administrative interface is made accessible. Such administrative functionality MUST be available either directly on the network protection device console or equivalent, or through remote communications using openly defined means. Access to the administrative interface can be local console-type access; through FIPS-approved encrypted network communication; or though network communications which are secured through other means from outside access.

Procedure:

Step	Action	Expected Behavior
1.	Configure the NPP to enable secure administrative communication using each of the secure mechanisms that the NPP supports and disable all insecure administrative communications.	
2.	Perform administrative functions, such as configuring policies or reviewing logs.	The administrative functions on the NPP must work properly via the secure mechanisms. Any supported insecure mechanisms are disabled. If using encrypted network communications, the NPP must be able to be configured to use only FIPS-approved algorithms.

Possible Problems: None.

Test NPP.1.6: Persistence of Device Settings

Purpose: To verify that device settings on an NPP persists through loss and restoration of electrical power.

Reference:

- [NIST 500-267Ar1] – Section 4.14.3.6

Test Setup: An administrative interface is made accessible. Such administrative functionality MUST be available either directly on the network protection device console or equivalent, or through remote communications using openly defined means.

Procedure:

Step	Action	Expected Behavior
1.	Configure and apply policy settings to the NPP's non-volatile storage.	
2.	Remove power from the NPP, then restore power back to the NPP.	The NPP must not lose authentication information. The NPP must have kept all policy configurations.

Possible Problems: None.

Test NPP.1.7: Logging of Configuration Change

Purpose: To verify that an NPP properly logs configuration changes applied to it.

Reference:

- [NIST 500-267Ar1] – Section 4.14.3.7

Test Setup: An administrative interface is made accessible. Such administrative functionality MUST be available either directly on the network protection device console or equivalent, or through remote communications using openly defined means.

Procedure:

Step	Action	Expected Behavior
1.	Add a new policy rule.	
2.	Delete an existing policy rule.	
3.	Change an existing policy rule.	
4.	Change a user password.	
5.	Change the system time.	The NPP must generate appropriate log messages and they are all viewable by only the authorized administrator.

Possible Problems: None.

Test NPP.1.8: Fragmented Packet

Purpose: To verify that an NPP can handle fragmented packets by provisionally reassembling and applying appropriate controls based on the reassembled packet.

Reference:

- [NIST 500-267Ar1] – Section 4.14.3.8

Test Setup: The NPP is configured with the following ACL rules:

Inbound:

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Public Net	Private Net	Any	7	UDP

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Public Net	Private Net	Any	Any	Any

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Private Net	Public Net	Any	Any	Any

Procedure:

Step	Action	Expected Behavior
1.	TN1 sends a UDP packet with destination port 53 to TN2.	The NPP must allow the UDP packet through to the Private network.
2.	TN1 sends a UDP packet with destination port 53 fragmented into three parts to TN2, with the first two parts reaching the minimum IPv6 MTU of 1280 bytes. The fragments will be sent out of order, with the last bytes of the original datagram being	The NPP must allow the fragmented packet through.

	sent first, and the first bytes being sent last.	
3.	TN1 sends a UDP packet with destination port 7 to TN2.	The NPP must drop the UDP packet.
4.	TN1 sends a UDP packet with destination port 7 fragmented into three parts to TN2, with the first two parts reaching the minimum IPv6 MTU of 1280 bytes. The fragments will be sent out of order, with the last bytes of the original datagram being sent first, and the first bytes being sent last.	The NPP must drop the fragmented packet.

Possible Problems: None.

Test NPP.1.9: Tunneled Traffic

Purpose: To verify that an NPP either blocks all tunneled packets, or that the NPP analyzes the tunneled traffic and applies appropriate controls based on the encapsulated packet header.

Reference:

- [NIST 500-267Ar1] – Section 4.14.3.9

Test Setup: The network is setup per Common Topology. The NPP is configured with the following access policies:

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	80	TCP

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	80	TCP

Procedure:

Part A: 4in6

Step	Action	Expected Behavior
1.	Through a 4in6 tunnel, TN1 sends allowed TCP traffic to TN2.	If the NPP does not support analysis of tunneled traffic, then it should drop the traffic. If the NPP supports analysis of tunneled traffic, then it must forward the traffic to TN2.
2.	Through a 4in6 tunnel, TN1 sends UDP traffic to TN2.	The NPP must drop the tunneled traffic.

Part B: 6in4

Step	Action	Expected Behavior
3.	Through a 6in4 tunnel, TN1 sends allowed TCP traffic to TN2.	If the NPP does not support analysis of tunneled traffic, then it should drop the traffic. If the NPP supports

		analysis of tunneled traffic, then it must forward the traffic to TN2.
4.	Through a 6in4 tunnel, TN1 sends UDP traffic to TN2.	The NPP must drop the tunneled traffic.

Part C: 6to4

Step	Action	Expected Behavior
5.	Through a 6to4 tunnel, TN1 sends allowed TCP traffic to TN2.	If the NPP does not support analysis of tunneled traffic, then it should drop the traffic. If the NPP supports analysis of tunneled traffic, then it must forward the traffic to TN2.
6.	Through a 6to4 tunnel, TN1 sends UDP traffic to TN2.	The NPP must drop the tunneled traffic.

Part D: Teredo

Step	Action	Expected Behavior
7.	Through a Teredo tunnel, TN1 sends allowed TCP traffic to TN2.	If the NPP does not support analysis of tunneled traffic, then it should drop the traffic. If the NPP supports analysis of tunneled traffic, then it must forward the traffic to TN2.
8.	Through a Teredo tunnel, TN1 sends UDP traffic to TN2.	The NPP must drop the tunneled traffic.

Possible Problems: None.

Group 2: Firewall

Scope

These tests are designed to verify NPP functionality as a firewall device.

Overview

The tests in this group verify conformance to NIST 500-267Ar1.

Test NPP.2.1: IPv6 Packets Sent to the Firewall

Purpose: To verify that an NPP can selectively block traffic sent directly to its interfaces based on either the source or destination address in the packet sent.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.1

Test Setup: The network is setup per Common Topology. The NPP is configured with the following ACL rules:

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN1	NPP	Any	Listening	Listening

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN3	NPP	Any	Listening	Listening

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN2	NPP	Any	Listening	Listening

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN4	NPP	Any	Listening	Listening

Procedure:

Step	Action	Expected Behavior
1.	Attempt to access an allowed port on the NPP from TN1.	The NPP must accept the traffic from TN1.
2.	Attempt to access a denied port on the NPP from TN3.	The NPP must drop the traffic.
3.	Attempt to access an allowed port on the NPP from TN2.	The NPP must accept the traffic from TN2.

4.	Attempt to access a denied port on the NPP from TN4.	The NPP must drop the traffic.

Possible Problems: If the NPP is an L2 firewall, this test may be omitted.

Test NPP.2.2: Source Addresses

Purpose: To verify that an NPP can selectively allow/block packets sent inbound or outbound through its interfaces based on the source address in the packet sent.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.1

Test Setup: The network is setup per Common Topology. The NPP is configured with the following ACL rules:

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN1	Private Net	Any	80	TCP

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN3	Private Net	Any	80	TCP

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN2	Public Net	Any	80	TCP

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN4	Public Net	Any	80	TCP

Procedure:

Part A: Global Addresses

Step	Action	Expected Behavior
1.	TN1 sends a TCP packet with destination port 80 to TN2.	The NPP must forward the packet to TN2.
2.	TN3 sends a TCP packet with destination port 80 to TN2.	The NPP must drop the packet.

3.	TN2 sends a TCP packet with destination port 80 to TN1.	The NPP must forward the packet to TN1.
4.	TN4 sends a TCP packet with destination port 80 to TN1.	The NPP must drop the packet.

Part B: IPv4-Mapped Addresses

Step	Action	Expected Behavior
5.	Configure TN1, TN2, TN3, and TN4 with IPv4-Mapped addresses, and update the rules on the NPP with these new addresses.	
6.	TN3 sends a TCP packet with destination port 80 to TN2.	The NPP must drop the packet.
7.	TN4 sends a TCP packet with destination port 80 to TN1.	The NPP must drop the packet.

Part C: IPv4-Compatible Addresses

Step	Action	Expected Behavior
8.	Configure TN1, TN2, TN3, and TN4 with IPv4-Compatible addresses, and update the rules on the NPP with these new addresses.	
9.	TN3 sends a TCP packet with destination port 80 to TN2.	The NPP must drop the packet.
10.	TN4 sends a TCP packet with destination port 80 to TN1.	The NPP must drop the packet.

Part D: RFC4193 Unique Local Addresses

Step	Action	Expected Behavior
11.	Configure TN1, TN2, TN3, and TN4 with unique local addresses, as defined in RFC4193, and update the rules on the NPP with these new addresses.	
12.	TN1 sends a TCP packet with destination port 80 to TN2.	The NPP forwards the packet to TN2.

13.	TN3 sends a TCP packet with destination port 80 to TN2.	The NPP must drop the packet.
14.	TN2 sends a TCP packet with destination port 80 to TN1.	The NPP forwards the packet to TN1.
15.	TN4 sends a TCP packet with destination port 80 to TN1.	The NPP must drop the packet.

Possible Problems: None.

Test NPP.2.3: Destination Addresses

Purpose: To verify that an NPP can selectively allow/block packets sent inbound or outbound through its interfaces based on the destination address in the packet sent.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.1

Test Setup: The network is setup per Common Topology. The NPP is configured with the following ACL rules:

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Public Net	TN2	Any	80	TCP

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Public Net	TN4	Any	80	TCP

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Private Net	TN1	Any	80	TCP

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Private Net	TN3	Any	80	TCP

Procedure:

Part A: Global Addresses

Step	Action	Expected Behavior
1.	TN1 sends a TCP packet with destination port 80 to TN2.	The NPP must forward the packet to TN2.
2.	TN1 sends a TCP packet with destination port 80 to TN4.	The NPP must drop the packet.

3.	TN2 sends a TCP packet with destination port 80 to TN1.	The NPP must forward the packet to TN1.
4.	TN2 sends a TCP packet with destination port 80 to TN3.	The NPP must drop the packet.

Part B: IPv4-Mapped Addresses

Step	Action	Expected Behavior
5.	Configure TN1, TN2, TN3, and TN4 with IPv4-Mapped addresses, and update the rules on the NPP with these new addresses.	
6.	TN1 sends a TCP packet with destination port 80 to TN4.	The NPP must drop the packet.
7.	TN2 sends a TCP packet with destination port 80 to TN3.	The NPP must drop the packet.

Part C: IPv4-Compatible Addresses

Step	Action	Expected Behavior
8.	Configure TN1, TN2, TN3, and TN4 with IPv4-Compatible addresses, and update the rules on the NPP with these new addresses.	
9.	TN1 sends a TCP packet with destination port 80 to TN4.	The NPP must drop the packet.
10.	TN2 sends a TCP packet with destination port 80 to TN3.	The NPP must drop the packet.

Part D: RFC4193 Unique Local Addresses

Step	Action	Expected Behavior
11.	Configure TN1, TN2, TN3, and TN4 with unique local addresses, as defined in RFC4193, and update the rules on the NPP with these new addresses.	
12.	TN1 sends a TCP packet with destination port 80 to TN2.	The NPP must forward the packet to TN2.

13.	TN1 sends a TCP packet with destination port 80 to TN4.	The NPP must drop the packet.
14.	TN2 sends a TCP packet with destination port 80 to TN1.	The NPP must forward the packet to TN1.
15.	TN2 sends a TCP packet with destination port 80 to TN3.	The NPP must drop the packet.

Possible Problems: None.

Test NPP.2.4: Illegal Source and Destination Addresses

Purpose: To verify that an NPP can selectively block any IPv6 packet sent inbound or outbound through its interface with an illegal source or destination address.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.1

Test Setup: The network is setup per Common Topology. The NPP is configured with the following ACL rules:

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	Any	Any

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	Any	Any

Procedure:

Part A: Unspecified Address

Step	Action	Expected Behavior
1.	Send a packet with the source address set to the unspecified address (::) from the Public Net to TN2.	The NPP must drop the packet.
2.	Send a packet with the source address set to the unspecified address (::) from the Private Net to TN1.	The NPP must drop the packet.

Part B: Interface-Local Scope

Step	Action	Expected Behavior
3.	Send a packet with the source address set to an interface-	The NPP must drop the packet.

	local multicast address from the Public Net to TN2.	
4.	Send a packet with the source address set to an interface-local multicast address from the Private Net to TN1.	The NPP must drop the packet.

Part C: Link-Local Scope

Step	Action	Expected Behavior
5.	Send a packet with the source address set to a link-local multicast address from the Public Net to TN2.	The NPP must drop the packet.
6.	Send a packet with the source address set to a link-local multicast address from the Private Net to TN1.	The NPP must drop the packet.

Part D: Admin-Local Scope

Step	Action	Expected Behavior
7.	Send a packet with the source address set to an admin-local multicast address from the Public Net to TN2.	The NPP must drop the packet.
8.	Send a packet with the source address set to an admin-local multicast address from the Private Net to TN1.	The NPP must drop the packet.

Part E: Site-Local Scope

Step	Action	Expected Behavior
9.	Send a packet with the source address set to a site-local multicast address from the Public Net to TN2.	The NPP must drop the packet.
10.	Send a packet with the source address set to a site-local multicast address from the Private Net to TN1.	The NPP must drop the packet.

Part F: Organization-Local Scope

Step	Action	Expected Behavior
11.	Send a packet with the source address set to an organization-local multicast address from the Public Net to TN2.	The NPP must drop the packet.
12.	Send a packet with the source address set to an organization-local multicast address from the Private Net to TN1.	The NPP must drop the packet.

Part G: Link-Local Source Addresses

Step	Action	Expected Behavior
13.	Send a packet from TN1's link-local address to TN2.	The NPP must drop the packet.
14.	Send a packet from TN2's link-local address to TN1.	The NPP must drop the packet.

Part H: Link-Local Destination Addresses

Step	Action	Expected Behavior
15.	Send a packet from TN1 to TN2's link-local address.	The NPP must drop the packet.
16.	Send a packet from TN2 to TN1's link-local address.	The NPP must drop the packet.

Part I: Loopback Address

Step	Action	Expected Behavior
17.	Send a packet with the source address set to the loopback address (::1) from the Public Net to TN2.	The NPP must drop the packet.
18.	Send a packet with the source address set to the loopback address (::1) from the Private Net to TN1.	The NPP must drop the packet.

Possible Problems: If the NPP is an L2 firewall, Parts G and H may be omitted.

Test NPP.2.5: Next Header Values

Purpose: To verify that an NPP can selectively block any IPv6 packet based on its Next Header (NH) value.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.1
- [NIST 500-267Ar1] – Section 4.14.4.4

Test Setup: The network is setup per Common Topology. The NPP is configured with the following access policies:

Part A: Initial Access Policy

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	Any	Any

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN15	Any	Any	Any	RSVP
TN17	Any	Any	Any	ESP
TN19	Any	Any	Any	AH
TN21	Any	Any	Any	IPv6-ICMP
TN23	Any	Any	Any	IPv6-NoNxt
TN25	Any	Any	Any	IPv6-Opts
TN27	Any	Any	Any	OSPF

Part B: Access Policy Change

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	Any	Any

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN1	Any	Any	Any	HOPOPT
TN3	Any	Any	Any	IPv4
TN5	Any	Any	Any	TCP

TN7	Any	Any	Any	UDP
TN9	Any	Any	Any	IPv6
TN11	Any	Any	Any	IPv6-Route
TN13	Any	Any	Any	IPv6-Frag

Next-Header Values:

NH Value	Protocol Abreviation	Protocol	RFC
0	HOPOPT	IPv6 Hop-by-Hop Option	8200
4	IPv4	IPv4 Encapsulation	2003
6	TCP	Transmission Control	793
17	UDP	User Datagram	768
41	IPv6	IPv6 Encapsulation	2473
43	IPv6-Route	Routing Header for IPv6	8200
44	IPv6-Frag	Fragment Header for IPv6	8200
46	RSVP	Reservation Protocol	2205
50	ESP	Encap Security Payload	4303
51	AH	Authentication Header	4302
58	IPv6-ICMP	ICMP for IPv6	8200
59	IPv6-NoNxt	No Next Header for IPv6	8200
60	IPv6-Opts	Destination Options for IPv6	8200
89	OSPF	OSPF	2328

Procedure:

Part A: Initial Access Policy

Step	Action	Expected Behavior
1.	A TN on the public network sends a packet of each Next-Header value as shown above to a TN on the private network.	The NPP must forward all packets that are allowed and must drop all packets that are explicitly denied.

Part B: Access Policy Change

Step	Action	Expected Behavior
2.	Configure the NPP to explicitly deny Next Header values that were allowed in Part A, and to	

	allow Next Header values that were denied in Part A.	
3.	A TN on the public network sends a packet of each Next-Header value as shown above to a TN on the private Network.	The NPP must forward all packets that are allowed and must drop all packets that are explicitly denied.

Possible Problems: None.

Test NPP.2.6: TCP/UDP Ports

Purpose: To verify that an NPP can selectively block any IPv6 packet based on its TCP or UDP ports.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.1

Test Setup: The network is setup per Common Topology. The NPP is configured with the following access policies:

Part A: Source Port Policies

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN1	TN2	9000	Any	TCP
TN1	TN2	9000	Any	UDP

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN1	TN2	9001	Any	TCP
TN1	TN2	9001	Any	UDP

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN4	TN3	9000	Any	TCP
TN4	TN3	9000	Any	UDP

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN4	TN3	9001	Any	TCP
TN4	TN3	9001	Any	UDP

Part B: Destination Port Policies

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN1	TN2	Any	80	TCP
TN1	TN2	Any	53	UDP

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN1	TN2	Any	81	TCP
TN1	TN2	Any	54	UDP

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN4	TN3	Any	80	TCP
TN4	TN3	Any	53	UDP

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN4	TN3	Any	81	TCP
TN4	TN3	Any	54	UDP

Procedure:

Part A: Source Port

Step	Action	Expected Behavior
1.	TN1 sends allowed TCP and UDP packets to TN2.	The NPP must forward the packets to TN2.
2.	TN1 sends TCP and UDP packets to TN2 using source port 9001.	The NPP must drop the packets.
3.	TN4 sends allowed TCP and UDP packets to TN3.	The NPP must forward the packets to TN3.
4.	TN4 sends TCP and UDP packets to TN3 using source port 9001.	The NPP must drop the packets.

Part B: Destination Port

Step	Action	Expected Behavior
5.	TN1 sends allowed TCP and UDP packets to TN2.	The NPP must forward the packets to TN2.
6.	TN1 sends TCP and UDP packets to TN2 using destination ports 81 and 54, respectively.	The NPP must drop the packets.
7.	TN4 sends allowed TCP and UDP packets to TN3.	The NPP must forward the packets to TN3.
8.	TN4 sends TCP and UDP packets to TN3 using destination ports 81 and 54, respectively.	The NPP must drop the packets.

Possible Problems: None.

Test NPP.2.7: ICMPv6

Purpose: To verify that an NPP can selectively allow/block any IPv6 packet based on its ICMPv6 type and code.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.1

Test Setup: The network is setup per Common Topology. The NPP is configured with the following access policies:

Inbound:

Allow:

Source Address	Destination Address	Type	Code	Protocol
Any	Any	1	0-6	ICMPv6
Any	Any	2	0	ICMPv6
Any	Any	3	0-1	ICMPv6
Any	Any	4	0-2	ICMPv6
Any	Any	129	0	ICMPv6

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	Any	UDP

Outbound:

Allow:

Source Address	Destination Address	Type	Code	Protocol
Any	Any	1	0-6	ICMPv6
Any	Any	2	0	ICMPv6
Any	Any	3	0-1	ICMPv6
Any	Any	4	0-2	ICMPv6
Any	Any	128	0	ICMPv6

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	Any	UDP

Procedure:

Step	Action	Expected Behavior
1.	TN2 sends a UDP packet to TN1. TN1 sends an ICMPv6 packet to TN2, with Type 1, Code 0, and specifies the preceding UDP packet as the invoking error packet.	
2.	Repeat step 1 with all allowed types and codes as specified in the table above.	The NPP must forward all packets to TN2.
3.	TN2 sends a UDP packet to TN1. TN1 sends an ICMPv6 packet to TN2, with Type 1, Code 7, and specifies the preceding UDP packet as the invoking error packet.	
4.	Repeat step 3 with all denied types and with all allowed types with denied codes as is missing in the table above.	The NPP must drop all packets to TN2.
5.	TN1 sends a UDP packet to TN2. TN2 sends an ICMPv6 packet to TN1, with Type 1, Code 0, and specifies the preceding UDP packet as the invoking error packet.	
6.	Repeat step 5 with all allowed types and codes as specified in the table above.	The NPP must forward all packets to TN1.
7.	TN1 sends a UDP packet to TN2. TN2 sends an ICMPv6 packet to TN1, with Type 1, Code 7, and specifies the preceding UDP packet as the invoking error packet.	
8.	Repeat step 7 with all denied types and with all allowed types with denied codes as is missing in the table above.	The NPP must drop all packets to TN1.

Possible Problems: None.

Test NPP.2.8: Implicit Deny Policy

Purpose: To verify that an NPP blocks all traffic that has not been explicitly allowed.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.1

Test Setup: The network is setup per Common Topology. The NPP is configured with the following access policies:

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Public Net	Private Net	Any	80	TCP

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Private Net	Public Net	Any	80	TCP

Procedure:

Step	Action	Expected Behavior
1.	TN1 sends a UDP packet to TN2.	The NPP must drop the packet.
2.	TN2 sends a UDP packet to TN1.	The NPP must drop the packet.
3.	TN1 sends a TCP packet to TN2 destination port 80.	The NPP must forward the packet to TN2.
4.	TN2 sends a TCP packet to TN1 destination port 80.	The NPP must forward the packet to TN1.

Possible Problems: None.

Test NPP.2.9: Asymmetrical Controls

Purpose: To verify that an NPP distinguishes between internal and external networks and allows asymmetrical controls of traffic between those networks.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.2

Test Setup: The network is setup per Common Topology. The NPP is configured with the following access policies:

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN1	TN2	Any	80	TCP

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN4	TN3	Any	80	TCP

Procedure:

Step	Action	Expected Behavior
1.	TN1 sends a TCP packet to TN2 destination port 80.	The NPP must forward the packet to TN2.
2.	TN4 sends a TCP packet to TN3 destination port 80.	The NPP must forward the packet to TN3.
3.	TN3 sends a TCP packet to TN4 destination port 80.	The NPP must drop the packet.
4.	TN2 sends a TCP packet to TN1 destination port 80.	The NPP must drop the packet.

Possible Problems: None.

Test NPP.2.10: Connection Oriented Protocols

Purpose: To verify that an NPP allows connection oriented protocols, such as TCP, to travel bi-directionally.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.2

Test Setup: The network is setup per Common Topology. The NPP is configured with the following access policies:

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Public Net	Private Net	Any	80	TCP

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Private Net	Public Net	Any	80	TCP

Procedure:

Step	Action	Expected Behavior
1.	TN1 establishes a TCP connection (completes the three-way handshake) with TN2, using destination port 80.	The NPP must allow TCP traffic to travel bi-directionally from TN1 and TN2, even though TN2's TCP packets don't follow the access control rules.
2.	TN4 establishes a TCP connection (completes the three-way handshake) with TN3, using destination port 80.	The NPP must allow TCP traffic to travel bi-directionally from TN4 and TN3, even though TN3s TCP packets don't follow the access control rules.
3.	TN2 sends an unsolicited SYN-ACK TCP packet to TN1 using source port 80.	The NPP must drop the packet.
4.	TN3 sends an unsolicited SYN-ACK TCP packet to TN4 using source port 80.	The NPP must drop the packet.

5.	TN1 sends a TCP RST to TN2 in order to reset the connection.	
6.	TN4 sends a TCP RST to TN3 in order to reset the connection.	

Possible Problems: None.

Test NPP.2.11: Unsolicited External Reply

Purpose: To verify that an NPP blocks all unsolicited replies from the external network.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.2

Test Setup: The network is setup per Common Topology. The NPP is configured with the following access policies:

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Public Net	Private Net	Any	Any	Any

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Private Net	Public Net	Any	Any	Any

Procedure:

Step	Action	Expected Behavior
1.	TN2 sends an ICMPv6 Echo Request to TN1 and TN1 responds with an ICMPv6 Echo Reply to TN2.	The NPP must forward the packets.
2.	TN1 sends an unsolicited ICMPv6 Echo Reply to TN2.	The NPP must drop the packet.

Possible Problems: None.

Test NPP.2.12: IPv6 Traffic Filtering

Purpose: To verify that that an NPP can filter IPv6 traffic based on reserved address space, illegal header chains and legitimate internal address ranges.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.3

Test Setup: The network is setup per Common Topology. The NPP is configured with the following access policies:

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	Any	Any

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	Any	Any

Procedure:

Part A: Source Address of Reserved IPv6 Address Space

Step	Action	Expected Behavior
1.	TN1 sends a packet to TN2 with the source address of the reserved IPv6 prefix 4000::/3.	The NPP must discard the packet.
2.	TN2 send a packet to TN1 with the source address of the reserved IPv6 prefix 4000::/3.	The NPP must discard the packet.

Part B: Destination Address of Reserved IPv6 Address Space

Step	Action	Expected Behavior
3.	TN1 sends a packet to TN2 with the destination address of the reserved IPv6 prefix 4000::/3.	The NPP must discard the packet.

4.	TN2 send a packet to TN1 with the destination address of the reserved IPv6 prefix 4000::/3.	The NPP must discard the packet.

Part C: Illegal IPv6 Header Chains

Step	Action	Expected Behavior
5.	TN1 sends a packet to TN2 that is valid in all ways except that the next-header value is set to routing option (43) and the routing option's next-header value is set to hop-by-hop (00).	The NPP must discard the packet.
6.	TN2 sends a packet to TN1 that is valid in all ways except that the next-header value is set to routing option (43) and the routing option's next-header value is set to hop-by-hop (00).	The NPP must discard the packet.

Part D: Illegitimate Internal Address

Step	Action	Expected Behavior
7.	Configure the NPP with an internal address range.	
8.	TN2 sends a packet to TN1 with the source address set to a packet outside of the internal address range.	The NPP must discard the packet.

Possible Problems: If the NPP is an L3 firewall, Part B may be omitted. If the NPP is an L2 firewall, Part D may be omitted.

Test NPP.2.13: Fail-Safe

Purpose: To verify that when an NPP is suffering performance degradation due to overuse of resources, that it fails in a manner that does not allow unauthorized access to itself or to any attached networks.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.5

Test Setup: The network is setup per Common Topology. The NPP is configured with the following access policies:

Inbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	80	TCP

Outbound:

Allow:

Source Address	Destination Address	Source Port	Destination Port	Protocol
Any	Any	Any	80	TCP

Procedure:

Step	Action	Expected Behavior
1.	Transmit TCP and UDP packets at the vendor specified maximum rated throughput. The TCP packets use destination port 80, and the UDP ports use a destination port 53.	The NPP must not allow any denied traffic to pass through.

Possible Problems: None.

Test NPP.2.14: Logging

Purpose: To verify that an NPP can log matches to filter rules that drop, deny, reject, or allow packets.

Reference:

- [NIST 500-267Ar1] – Section 4.14.4.6

Test Setup: The network is setup per Common Topology. The NPP is configured with the following access policies:

Inbound:

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN1	Private Net	Any	80	TCP
TN1	Private Net	Any	53	UDP

Outbound:

Deny:

Source Address	Destination Address	Source Port	Destination Port	Protocol
TN2	Public Net	Any	80	TCP
TN2	Public Net	Any	53	UDP

Procedure:

Part A: Deny

Step	Action	Expected Behavior
1.	TN1 sends TCP packets to TN2.	The NPP must deny the packets sending a TCP Reset to TN1. This should be logged indicating the NPP denied the packet.
2.	TN2 sends TCP packets to TN1.	The NPP must deny the packets sending a TCP Reset to TN2. This should be logged indicating the NPP denied the packet.

Part B: Drop

Step	Action	Expected Behavior

3.	Configure the NPPs action to drop.	
4.	TN1 sends TCP packets to TN2.	The NPP must silently drop the packets. This should be logged indicating the NPP dropped the packet.
5.	TN2 sends TCP packets to TN1.	The NPP must silently drop the packets. This should be logged indicating the NPP dropped the packet.

Part C: Reject

Step	Action	Expected Behavior
6.	Configure the NPPs action to reject.	
7.	TN1 sends UDP packets to TN2.	The NPP must reject the packets sending a ICMPv6 Destination Unreachable to TN1. This should be logged indicating the NPP rejected the packet.
8.	TN2 sends UDP packets to TN1.	The NPP must reject the packets sending a ICMPv6 Destination Unreachable to TN2. This should be logged indicating the NPP rejected the packet.

Part D: Allow

Step	Action	Expected Behavior
9.	Configure the NPPs action to allow.	
10.	TN1 sends UDP packets to TN2.	The NPP must allow the packets. This should be logged indicating the NPP allowed the packet.
11.	TN2 sends UDP packets to TN1.	The NPP must allow the packets. This should be logged indicating the NPP allowed the packet.

Possible Problems: The NPP vendor may have a different interpretation of the functionality of a specific action. If the NPP is an L2 firewall, Parts A and C may be omitted.

Group 3: Intrusion Detection System

Scope

These tests are designed to verify NPP functionality as an intrusion detection system. If the NPP also functions as an Intrusion Prevention System than these tests can be executed in parallel with group 4.

Overview

The tests in this group verify conformance to NIST-267-500Ar1.

Test NPP.3.1: Known Attack Detection

Purpose: To verify that an NPP can detect suspicious traffic based on known attack patterns that the USGv6 website has deemed relevant to USG organizations.

Reference:

- [NIST 500-267Ar1] – Section 4.14.6.1

Test Setup: The network is setup per Common Topology. Configure and apply a policy on the network NPP that should detect traffic indicating an attempt to exploit a vulnerability relevant to USG organizations.

Procedure:

Step	Action	Expected Behavior
1.	One at a time, generate or replay attack traffic that originates from a malicious host on the public network and targets a system on the Private network.	The NPP must detect and log 97% of the attacks.
2.	Make note of the vulnerability that was targeted, the IP addresses of the attacker and the victim, and the source or tool used to generate or replay the attack traffic.	

Possible Problems: None.

Test NPP.3.2: Fragmented Packet Attacks

Purpose: To verify that an NPP can detect fragmented packet attacks.

Reference:

- [NIST 500-267AR1] – Section 4.14.6.4

Test Setup: The network is setup per Common Topology. Configure the NPP with a policy to detect fragmented packet attacks.

Procedure:

Step	Action	Expected Behavior
1.	TN1 sends a series of three fragments to TN2 with the last fragment being valid in all ways except that the offset field is set to 0.	The NPP must detect the fragmented packet attack and log or record it.

Possible Problems: None.

Test NPP.3.3: Port-Scanning Detection

Purpose: To verify that an NPP can detect typical port and host scans.

Reference:

- [NIST 500-267Ar1] – Section 4.14.6.2

Test Setup: The network is setup per Common Topology. Configure the NPP with a policy to detect port-scanning.

Procedure:

Part A: TCP Port-Scanning

Step	Action	Expected Behavior
1.	TN1 attempts a TCP port scan of TN2 on well-known port numbers.	The NPP detects the port scan and records or logs it.

Part B: UDP Port-Scanning

Step	Action	Expected Behavior
2.	TN1 attempts a UDP port scan of TN2 on well-known port numbers.	The NPP detects the port scan and records or logs it.

Possible Problems: None.

Test NPP.3.4: Tunnel Traffic Detection

Purpose: To verify that an NPP can detect suspicious traffic based on known attack patterns, even when encapsulation is present. If encapsulation renders content inspection infeasible, the NPP must still be able to detect that encapsulation is present.

Reference:

- [NIST 500-267Ar1] – Section 4.14.6.3

Test Setup: The network is setup per Common Topology. Configure and apply a policy on the network NPP that should detect traffic indicating an attempt to exploit a vulnerability relevant to USG organizations. Also configure and set the policy to detect all forms of IPv6 to IPv4 and IPv4 to IPv6 tunneling.

Procedure:

Part A: 4in6

Step	Action	Expected Behavior
1.	Through a 4in6 tunnel, TN1 generates or replays attack traffic that targets TN2.	The NPP must detect the attack and must create a log or record of the attack.

Part B: 6in4

Step	Action	Expected Behavior
2.	Through a 6in4 tunnel, TN1 generates or replays attack traffic that targets TN2.	The NPP must detect the attack and must create a log or record of the attack.

Part C: 6to4

Step	Action	Expected Behavior
3.	Through a 6to4 tunnel, TN1 generates or replays attack traffic that targets TN2.	The NPP must detect the attack and must create a log or record of the attack.

Part D: Teredo

Step	Action	Expected Behavior
4.	Through a Teredo tunnel, TN1 generates or replays attack traffic that targets TN2.	The NPP must detect the attack and must create a log or record of the attack.

Possible Problems: None.

Test NPP.3.5: Fail-Safe

Purpose: To verify that an NPP can notify administrators when it is under severe load, when configured to do so.

Reference:

- [NIST 500-267Ar1] – Section 4.14.6.5

Test Setup: The network is setup per Common Topology. IPv6 network traffic is passed through or to the NPP by placing one or more monitoring segments of the device inline between switch ports configured as a trunk line or by connecting one or more monitoring ports on the device to a network tap or span port, respectively. How many connections are needed depends on how many monitoring segments the NPP has and what sort of throughput each segment can accommodate. Taken together, the configuration should be capable of delivering sufficient traffic to fully load the NPP. A traffic generation tool capable of filling the NPP available bandwidth is connected to the test bed network such that the traffic can be seen by the NPP.

Procedure:

Step	Action	Expected Behavior
1.	Determine the maximum throughput the NPP is expected to be capable of handling.	
2.	Configure private network TN's to send proper IPv6 network traffic with a reasonable mix of protocols to public network TN's. If multiple interfaces are required to reach maximum throughput, then use as many target nodes as needed.	
3.	Begin sending the network traffic through the NPP, starting at about 30% of the maximum throughput.	
4.	Incrementally raise the throughput until the NPP gives an indication of impending overload, or the NPP fails.	The NPP must notify an administrator of impending failure through logs, a real time event viewer, or another mechanism.

Possible Problems: None.

Group 4: Intrusion Prevention System

Scope

These tests are designed to verify NPP functionality as an intrusion prevention system.

Overview

The tests in this group verify conformance of NIST-267-500Ar1.

Test NPP.4.1: Implement Intrusion Detection Capabilities

Purpose: To verify test cases from Group 3 with the NPP as an IPS.

Reference:

- [NIST 500-267Ar1] – Section 4.14.7.1

Test Setup: The network is setup per Common Topology. Configure and apply a policy on the network NPP that should detect and prevent traffic indicating an attempt to exploit a vulnerability relevant to USG organizations.

Procedure:

Part A: Fragmented Packet Attacks

Step	Action	Expected Behavior
1.	Preform test 3.2 with the NPP as an IPS.	

Part B: Port-Scanning Prevention

Step	Action	Expected Behavior
2.	Preform test 3.3 with the NPP as an IPS.	

Part C: Tunneled Traffic Prevention

Step	Action	Expected Behavior
3.	Preform test 3.4 with the NPP as an IPS.	

Part D: Performance Under Load, Fail-Safe Prevention

Step	Action	Expected Behavior
4.	Preform test 3.5 with the NPP as an IPS.	

Possible Problems: None.

Test NPP.4.2: Stop or Attenuate Detected Attacks

Purpose: To verify that an NPP can stop or attenuate suspicious traffic based on known attack patterns that the USGv6 website has deemed relevant to USG organizations.

Reference:

- [NIST 500-267Ar1] – Section 4.14.7.1

Test Setup: The network is setup per Common Topology. Configure and apply a policy on the network NPP that should detect and prevent traffic indicating an attempt to exploit a vulnerability relevant to USG organizations.

Procedure:

Step	Action	Expected Behavior
1.	One at a time, generate or replay attack traffic that originates from a malicious host on the Public network and targets a system on the Private network.	The NPP must prevent and log 97% of the attacks.
2.	Make note of the vulnerability that was targeted, the IP addresses of the attacker and the victim, and the source or tool used to generate or replay the attack traffic.	

Possible Problems: None.

Modification Record

Version	Date	Editor	Modification
2.2	October 2022	Christopher Brown	• Modified test case 2.5 to have an "allow all" rule for the next-header values not being blocked
2.1	March 2022	Christopher Brown	• Removed Malformed Packet Detection Test Cases • Data normalization on procedural step numbering • Removed procedures for forwarding IPv4-Mapped and IPv4-Compatible addresses
2.0	August 2021	Alan Lagace & Christopher Brown	• Incorporated Tests and Updates from NPD Test Plan v.1.3 • Added test cases required by NIST 500-267Ar1
1.3	August 19, 2011		• added general configuration note to default configuration in Firewall section • removed IGMP NH value in test 2.1.2.1, and added steps to verify legitimate traffic can be passed before verifying the subset configuration • added a procedure note to test 2.1.3.2 to clarify that ICMPv6 traffic sent should be independent of firewall state information
1.2	August 30, 2010		• clarified wording for procedure and results in test 1.3.2 • remove test 1.3.3 (tested in 1.4.1 step 1) • add reference to NIST USGv6 web site for set of vulnerabilities in test 1.4.1 • removed wording "in the case of firewalls" in 1.8.1 and 1.9.1 • expanded procedure in 1.8.1 to verify proper handling of fragmented traffic

			• correct source and destination in Section 2 default firewall outbound policy table • move the tests for IPv4-mapped and IPv4-compatible addresses from test 2.1.1.3 to test 2.1.1.2 • clarify next header value requirements in test 2.1.2.1 • correct codes for ICMPv6 in test 2.1.3.2 policy tables • clarify server requirement in test 2.2.2 • clarify wording in test 2.4.1 • section 3. Application Firewalls removed • changed code type to 7 in 4.2 step m. and packet type to router solicitation (type 133) in 4.2 step p.
1.1	February 10, 2010		• added a step in test 1.6.1 instructing that settings be applied before the removal of power. • fixed a typo in test 2.2.3 in which the word “request” was used instead of “response.” • changed format of loopback address in 4.2.2a,d from “1” to the more common “::1” • added step for unspecified address testing to test 2.1.1.3 • added specifics for multicast source address test in test 2.1.1.3 • added specifics for ipv4-mapped/compatible addresses to 2.1.1.3 • removed unique local requirement in test 2.1.1.3 • clarified the requirements and tests for 1.5.2 • clarified 4.2.2l detection of MTU below minimum

			- replaced guidance for selecting relevant vulnerabilities with reference to USGv6 website - removed configuration notes referring to fully loading the IDS/IPS from all except test 4.6 - altered test 4.1.3, 4.4.3 & 5.2.3 to include replaying traffic in addition to launching attack test cases manually
1.0	November 19, 2009		- Simplified example network infrastructure for firewall testing - Altered firewall tests to represent the changed infrastructure - Added section 2.5, tunneled traffic handling for firewall testing - Generalized IDS/IPS test configuration description to focus on capabilities hardware provides and not the actual type of hardware to be used to allow for flexibility in test bed design - Limited scope of IDS/IPS protection testing from all vulnerabilities in listed vendors' products to high-severity (i.e., CVSS score of at least 8) - Merged section 4.5 (Logging and Alerts) into section 4.1 (Known Attack Detection) and modified title of latter to reflect new scope - Corrected procedure item 2b in 4.2 from "source address" to "destination address" set to 0 (unspecified address) - Added table of contents - corrected typos and minor format issues
0.90	May 15, 2009		