IPv6 CONSORTIUM TEST SUITE

Access Policy

Functionality Test Suite

Technical Document

Revision 1.0

IPv6 Consortium
InterOperability Laboratory
Research Computing Center
University of New Hampshire

121 Technology Drive, Suite 2
Durham NH, 03824
Phone: +1-603-862-2804
Fax: +1-603-862-0898
Web: www.iol.unh.edu

TABLE OF CONTENTS

MODIFICATION RECORD

Draft Version	**August 11, 2004**	**Completed Draft Version**
Version 0.3	**August 15, 2004**	
Version 0.5	**September 9, 2004**	**Created a new set of test plans including Policy, Base Firewall and Firewall Interoperability.**
Version 0.7	**October 31, 2004**	**Scanned for errors and finished discussions and references.**
Version 0.8	**January 3, 2005**	**Removed table and misc errors/corrections**
Version 0.9	**January 17, 2005**	**Finalized and submitted for release.**
Version 1.0	**January 19, 2005**	**Approved for release.**

ACKNOWLEDGEMENTS

The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite. This test suite belongs to the University of New Hampshire InterOperability Lab and is a collaborative effort of those listed below and the participants of Moonv6. Special thanks to Check Point, Cisco and NetScreen for contributing test ideas for the base document of the Moonv6 Firewall Functionality test plan, from which this document is based.

Yoni Appel	Check Point Software Technologies
Eric Barrett	University of New Hampshire
Ankur Chadda	University of New Hampshire
Eli Ginot	Check Point Software Technologies
Paul Meyer	Secure Computing
Jeff Pomeroy	Secure Computing
Kari Revier	University of New Hampshire
Benjamin Schultz	University of New Hampshire
Shinsuke Suzuki	Hitachi Ltd.
L. Brad Upson	University of New Hampshire
Erica Williamsen	University of New Hampshire
Timothy Winters	University of New Hampshire

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 functioning of the policy functionality of Router products. The tests do not determine if a product conforms to any specifications, nor are they purely interoperability tests. Rather, they provide one method to isolate problems within a device. Successful completion of all tests contained in this suite does not guarantee that the tested device will interoperate with any other devices. However, combined with satisfactory operation in the IOL's semi-production environment, these tests provide a reasonable level of confidence that the Device Under Test will function well in most multi-vendor environments.

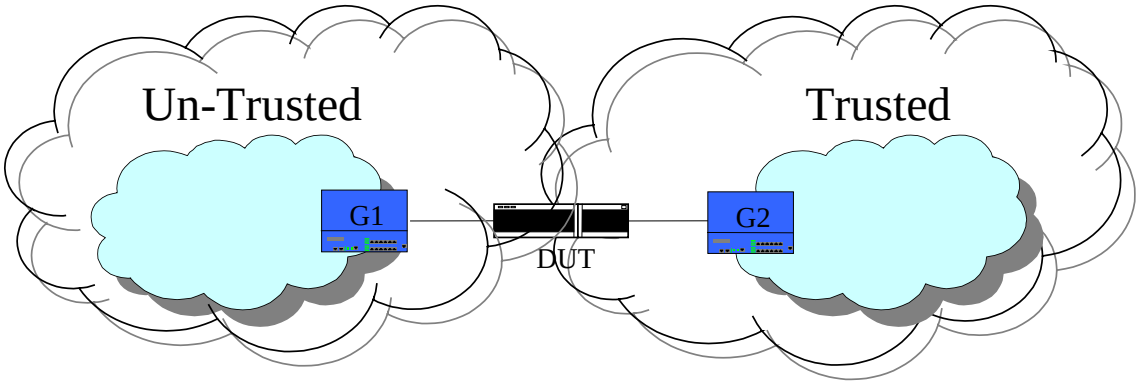
In this test suite, when using interface oriented terms such as "accept...on the interface" or "configure ... on its interface", it is up to the equipment vendor to supply the desired functionality according to the implementation of the DUT. The term "interface" only describes the externally observable behavior, not the specifics of an internal configuration.

Acronyms

DUT: Device **U**nder **T**est
G: Traffic **G**enerator
Trusted: The network or network segments considered internal and therefore "trusted".
Un-Trusted: The network or network segments considered public and therefore "un-trusted"

When several entities of the same type are present in a test configuration, a number is appended to the acronym to yield a label for each entity. For example, if there were three traffic generators in the test configuration, they would be labeled G1, G2 and G3.

Common Test Setup



Basic Test Configuration

Traffic is passed from G1 to G2 via the DUT. The DUT may be configured as a Router for some of the tests below which contain destination traffic to more than one network. When the term "Network Address" is used in the procedures below, it means that there is a range of IP addresses transmitted to a certain prefix that represents the destination subnet.

Common Test Setup

Summary: Clear configuration from the DUT.

1. Remove any existing access policy configurations on the DUT.

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 and title comprise the first line of the test block. The test label is composed by concatenating the short test suite name, the group number, and the test number within the group, separated by periods. The Test Number is the group and test number, also separated by a period. So, test label AP.1.2 refers to the second test of the first test group in the AP test suite. The test number is 1.2.
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.
Discussion:	The Discussion is a general discussion of the test and relevant section of the specification, including any assumptions made in the design or implementation of the test as well as known limitations.
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:	This section of the test description 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 packet from a test station. The test procedure also cues the tester to make observations, which are interpreted in accordance with the observable results given for that test part.
Observable Results:	This section lists observable results that can be examined by the tester to verify that the DUT is operating properly. When multiple observable results are possible, this section provides a short discussion on how to interpret them. The determination of a pass or fail for each test is usually based on how the DUT's behavior compares to the results described in this section.
Possible Problems:	This section contains a description of known issues with the test procedure, which may affect test results in certain situations.

REFERENCES

The following documents are referenced in this text:

[ADDRCONF] Thomson, S., T. Narten, IPv6 Stateless Address Autoconfiguration, RFC 2462, December 1998.

[ICMPv6] Conta, A., S. Deering, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC 2463, December 1998.

[IPv6-SPEC] Hinden, R., S. Deering, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998.

[ND] Narten, T., Nordmark, E., and W. Simpson, Neighbor Discovery for IP Version 6 (IPv6), RFC 2461, December 1998.

[PMTU] McCann, J., S. Deering, and J. Mogul, Path MTU Discovery for IPv6, RFC 1981, August 1996.

[ADDR] Hinden, R., S. Deering, IP Version 6 Addressing Architecture, RFC 2373, July 1998.

[IP] Jon Postel, Editor. Internet Protocol: DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, RFC 791, September 1981.

[TCP] Jon Postel, Editor. Internet Protocol: DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, RFC 793, September 1981.

[UDP] Jon Postel. User Datagram Protocol, RFC 768, August 1980.

[RFC2827] P. Ferguson and D. Senie, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827, May 2000.

[RFC3013] T. Killalea, Recommended Internet Service Provider Security Services and Procedures. RFC 3013, November 2000.

[RFC3775] D. Johnson, C. Perkins and J. Arkko, Mobility Support in IPv6. RFC 3775, June, 2004.

[FTP] Jon Postel. File Transfer Protocol (FTP), RFC 768, October 1985.

[RFC1858] G. Ziemba, D. Reed and P. Traina. Security Considerations for IP Fragment Filtering, RFC 1858, October 1995.

[IEEE802] IEEE Std 802-1990. IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture. December, 1990.

REFERENCES (continued)

[IPSec] RFC 1825 - IPSec Architecture
RFC 1826 – AH
RFC 1827 – ESP
RFC 1828 - AH-MD5
RFC 1829 - ESP-DES
RFC 1851 - ESP-3DES
RFC 1852 - AH-SHA-1
RFC 1853 - IP-in-IP
RFC 2085 - AH HMAC-MD5

GROUP 1: Basic Access Policy

Scope:

The following tests are designed to verify basic functionality and operation of IPv6-based access policy.

Overview:

IPv6 Routers are designed to forward traffic between IPv6 networks. Access Policies (APs) are static accept and deny features that some IPv6 Routers have to limit access between networks. This reduces the ability to attack insecure hosts and the information on them. Acceptance and rejection policy can be based upon IPv6 address, time and/or TCP/UDP ports.

Test AP.1.1: Source Address Denial

Purpose: To verify that a device properly denies source IPv6 addresses based on policy.

References: IPv6-SPEC

Discussion: The primary building block for network access is accepting and denying application traffic based on source and destination IP addresses. The following test verifies that a Router properly denies trafficfrom a specific location.

Test Setup: Common Test Setup is performed. The Common Test Cleanup procedure is performed after each part.

Procedure:

Part A: Deny all IPv6 traffic

1. Configure the DUT to deny all IPv6 traffic.
2. From G1, transmit IPv6 traffic to G2 containing a source address of 4000::1.
3. Observe the packets transmitted by the DUT.
4. From G1, transmit IPv6 traffic to G2 containing a source address of 4000::5.
5. Observe the packets transmitted by the DUT.
6. From G1, transmit IPv6 traffic to G2 containing a source address of 5000::1.
7. Observe the packets transmitted by the DUT.

Part B: Allow all IPv6 traffic

8. Configure the DUT to allow all IPv6 traffic.
9. From G1, transmit IPv6 traffic to G2 containing a source address of 4000::1.
10. Observe the packets transmitted by the DUT.
11. From G1, transmit IPv6 traffic to G2 containing a source address of 4000::5.
12. Observe the packets transmitted by the DUT.
13. From G1, transmit IPv6 traffic to G2 containing a source address of 5000::1.
14. Observe the packets transmitted by the DUT.

Part C: Deny IPv6 traffic originating from a global IPv6 Source Address

15. Configure the DUT to deny IPv6 traffic from the source address of 4000::1.
16. From G1, transmit IPv6 traffic to G2 containing a source address of 4000::1.
17. Observe the packets transmitted by the DUT.
18. From G1, transmit IPv6 traffic to G2 containing a source address of 4000::5.
19. Observe the packets transmitted by the DUT.
20. From G1, transmit IPv6 traffic to G2 containing a source address of 5000::1.
21. Observe the packets transmitted by the DUT.

Part D: Deny IPv6 traffic originating from a global IPv6 Prefix

22. Configure the DUT to deny IPv6 traffic from the source address of 4000::/64.
23. From G1, transmit IPv6 traffic to G2 containing a source address of 4000::1.
24. Observe the packets transmitted by the DUT.
25. From G1, transmit IPv6 traffic to G2 containing a source address of 4000::5.
26. Observe the packets transmitted by the DUT.
27. From G1, transmit IPv6 traffic to G2 containing a source address of 5000::1.
28. Observe the packets transmitted by the DUT.

Observable Results:

- *In Part A,*
  Step 3: The DUT must not forward the IPv6 traffic with a source address of 4000::1 to G2.
  Step 5: The DUT must not forward the IPv6 traffic with a source address of 4000::5 to G2.
  Step 7: The DUT must not forward the IPv6 traffic with a source address of 5000::1 to G2.
- *In Part B,*
  Step 10: The DUT must forward the IPv6 UDP traffic with a source address of 4000::1to G2.
  Step 12: The DUT must forward the IPv6 UDP traffic with a source address of 4000::5 to G2.
  Step 14: The DUT must forward the IPv6 UDP traffic with a source address of 5000::1 to G2.
- *In Part C,*
  Step 17: The DUT must not forward the IPv6 traffic with a source address of 4000::1 to G2.
  Step 19: The DUT must forward the IPv6 traffic with a source address of 4000::5 to G2.
  Step 21: The DUT must forward the IPv6 traffic with a source address of 5000::1 to G2.
- *In Part D,*
  Step 24: The DUT must not forward the IPv6 traffic with a source address of 4000::1
  Step 26: The DUT must not forward the IPv6 traffic with a source address of 4000::5 to G2.
  Step 28: The DUT must forward the IPv6 traffic with a source address of 5000::1 to G2.

Possible Problems:

- None.

Test AP.1.2: Destination Address Denial

Purpose: To verify that a device properly denies destination IPv6 addresses based on policy.

References: IPv6-SPEC

Discussion: The primary building block for network access is accepting and denying application traffic based on source and destination IP addresses. The following verifies that a Router properly denies traffic to a specific location.

Test Setup: Common Test Setup is performed. The Common Test Cleanup procedure is performed after each part.

Procedure:

Part A: Deny all IPv6 traffic

1. Configure the DUT to deny all IPv6 traffic.
2. From G1, transmit IPv6 traffic to G2 containing a destination address of 4000::1.
3. Observe the packets transmitted by the DUT.
4. From G1, transmit IPv6 traffic to G2 containing a destination address of 4000::5.
5. Observe the packets transmitted by the DUT.
6. From G1, transmit IPv6 traffic to G2 containing a destination address of 5000::1.
7. Observe the packets transmitted by the DUT.

Part B: Allow all IPv6 traffic

8. Configure the DUT to allow all IPv6 traffic.
9. From G1, transmit IPv6 traffic to G2 containing a destination address of 4000::1.
10. Observe the packets transmitted by the DUT.
11. From G1, transmit IPv6 traffic to G2 containing a destination address of 4000::5.
12. Observe the packets transmitted by the DUT.
13. From G1, transmit IPv6 traffic to G2 containing a destination address of 5000::1.
14. Observe the packets transmitted by the DUT.

Part C: Deny IPv6 traffic with a global IPv6 destination Address

15. Configure the DUT to deny IPv6 traffic from the destination address of 4000::1.
16. From G1, transmit IPv6 traffic to G2 containing a destination address of 4000::1.
17. Observe the packets transmitted by the DUT.
18. From G1, transmit IPv6 traffic to G2 containing a destination address of 4000::5.
19. Observe the packets transmitted by the DUT.
20. From G1, transmit IPv6 traffic to G2 containing a destination address of 5000::1.
21. Observe the packets transmitted by the DUT.

Part D: Deny IPv6 traffic with a global IPv6 Prefix

22. Configure the DUT to deny IPv6 traffic from the destination address of 4000::/64.
23. From G1, transmit IPv6 traffic to G2 containing a destination address of 4000::1.
24. Observe the packets transmitted by the DUT.
25. From G1, transmit IPv6 traffic to G2 containing a destination address of 4000::5.
26. Observe the packets transmitted by the DUT.
27. From G1, transmit IPv6 traffic to G2 containing a destination address of 5000::1.
28. Observe the packets transmitted by the DUT.

Observable Results:

- *In Part A,*
  Step 3: The DUT must not forward the IPv6 traffic with a destination address of 4000::1 to G2.
  Step 5: The DUT must not forward the IPv6 traffic with a destination address of 4000::5 to G2.
  Step 7: The DUT must not forward the IPV6 traffic with a destination address of 5000::1 to G2.
- *In Part B,*
  Step 10: The DUT must forward the IPv6 traffic with a destination address of 4000::1 to G2.
  Step 12: The DUT must forward the IPv6 traffic with a destination address of 4000::5 to G2.
  Step 14: The DUT must forward the IPv6 traffic with a destination address of 5000::1 to G2.
- *In Part C,*
  Step 17: The DUT must not forward the IPv6 traffic with a destination address of 4000::1.
  Step 19: The DUT must forward the IPv6 traffic with a destination address of 4000::5.
  Step 21: The DUT must forward the IPv6 traffic with a destination address of 5000::1.
- *In Part D,*
  Step 24: The DUT must not forward the IPv6 traffic with a destination address of 4000::1.
  Step 26: The DUT must not forward the IPv6 traffic with a destination address of 4000::5.
  Step 28: The DUT must forward the IPv6 traffic with a destination address of 5000::1.

Possible Problems:

- None.

Test AP.1.3: UDP Port Numbers

Purpose: To verify that a device properly accepts and denies UDP port numbers based on policy.

References: UDP

Discussion: An extended building block for network access is accepting and denying application traffic based on source and destination UDP ports. The following verifies that a Router properly accepts traffic to and from a UDP port.

Test Setup: Common Test Setup is performed. The Common Test Cleanup procedure is performed after each part.

Procedure:

Part A: Deny all UDP traffic

1. Configure the DUT to deny all IPv6 traffic.
2. From G1, transmit IPv6 UDP traffic to G2 containing a destination port of 20.
3. Observe the packets transmitted by the DUT.
4. From G1, transmit IPv6 UDP traffic to G2 containing a destination port of 25.
5. Observe the packets transmitted by the DUT.

Part B: Allow all UDP traffic

6. Configure the DUT to allow all IPv6 traffic.
7. From G1, transmit IPv6 UDP traffic to G2 containing a destination port of 20.
8. Observe the packets transmitted by the DUT.
9. From G1, transmit IPv6 UDP traffic to G2 containing a destination port of 25.
10. Observe the packets transmitted by the DUT.

Part C: Deny IPv6 traffic with a specific UDP Port Destination

11. Configure the DUT to only deny IPv6 UDP traffic from the destination port of 20.
12. From G1, transmit IPv6 UDP traffic to G2 containing a destination port of 20.
13. Observe the packets transmitted by the DUT.
14. From G1, transmit IPv6 UDP traffic to G2 containing a destination port of 25.
15. Observe the packets transmitted by the DUT.

Part D: Deny IPv6 traffic with a specific UDP Port Source

16. Configure the DUT to only deny IPv6 UDP traffic from the source port of 20.
17. From G1, transmit IPv6 UDP traffic to G2 containing a source port of 20.
18. Observe the packets transmitted by the DUT.
19. From G1, transmit IPv6 UDP traffic to G2 containing a source port of 25.
20. Observe the packets transmitted by the DUT.

Part E: Accept traffic with a specific UDP Port Destination

21. Configure the DUT to only accept IPv6 UDP traffic from the destination port of 20.
22. From G1, transmit IPv6 UDP traffic to G2 containing a destination port of 20.
23. Observe the packets transmitted by the DUT.
24. From G1, transmit IPv6 UDP traffic to G2 containing a destination port of 25.
25. Observe the packets transmitted by the DUT.

Part F: Accept traffic with a specific UDP Port Source

26. Configure the DUT to accept IPv6 UDP traffic from the source port of 20.

27. From G1, transmit IPv6 UDP traffic to G2 containing a source port of 20.
28. Observe the packets transmitted by the DUT.
29. From G1, transmit IPv6 UDP traffic to G2 containing a source port of 25.
30. Observe the packets transmitted by the DUT.

Observable Results:

- *In Part A,*
  Step 3: The DUT must not forward the IPv6 UDP traffic with a destination port of 20 to G2.
  Step 5: The DUT must not forward the IPv6 UDP traffic with a destination port of 25 to G2.
- *In Part B,*
  Step 8: The DUT must forward the IPv6 UDP traffic with a destination port of 20 to G2.
  Step 10: The DUT must forward the IPv6 UDP traffic with a destination port of 25 to G2.
- *In Part C,*
  Step 13: The DUT must not forward the IPv6 UDP traffic with a destination port of 20 to G2.
  Step 15: The DUT must forward the IPv6 UDP traffic with a destination port of 25 to G2.
- *In Part D,*
  Step 18: The DUT must not forward the IPv6 UDP traffic with a source port of 20 to G2.
  Step 20: The DUT must forward the IPv6 UDP traffic with a source port of 25 to G2.
- *In Part E,*
  Step 23: The DUT must forward the IPv6 UDP traffic with a destination port of 20 to G2.
  Step 25: The DUT must not forward the IPv6 UDP traffic with a destination port of 25 to G2.
- *In Part F,*
  Step 28: The DUT must forward the IPv6 UDP traffic with a source port of 20 to G2.
  Step 30: The DUT must not forward the IPv6 UDP traffic with a source port of 25 to G2.

Possible Problems:

- None.

Test AP.1.4: TCP Port Numbers

Purpose: To verify that a device properly accepts and denies TCP port numbers based on policy.

References: TCP

Discussion: An extended building block for network access is accepting and denying application traffic based on source and destination TCP ports. The following verifies that a Router properly accepts traffic to and from a TCP port.

Test Setup: Common Test Setup is performed. The Common Test Cleanup procedure is performed after each part.

Procedure:

Part A: Deny TCP traffic

1. Configure the DUT to deny all IPv6 traffic.
2. From G1, transmit IPv6 TCP traffic to G2 containing a destination port of 23.
3. Observe the packets transmitted by the DUT.
4. From G1, transmit IPv6 TCP traffic to G2 containing a destination port of 80.
5. Observe the packets transmitted by the DUT.

Part B: Allow all TCP traffic

6. Configure the DUT to allow all IPv6 traffic.
7. From G1, transmit IPv6 TCP traffic to G2 containing a destination port of 23.
8. Observe the packets transmitted by the DUT.
9. From G1, transmit IPv6 TCP traffic to G2 containing a destination port of 80.
10. Observe the packets transmitted by the DUT.

Part C: Deny IPv6 traffic with a specific TCP Port Destination

11. Configure the DUT to only deny IPv6 TCP traffic from the destination port of 23.
12. From G1, transmit IPv6 TCP traffic to G2 containing a destination port of 23.
13. Observe the packets transmitted by the DUT.
14. From G1, transmit IPv6 TCP traffic to G2 containing a destination port of 80.
15. Observe the packets transmitted by the DUT.

Part D: Deny IPv6 traffic with a specific TCP Port Source

16. Configure the DUT to only deny IPv6 TCP traffic from the source port of 23.
17. From G1, transmit IPv6 TCP traffic to G2 containing a source port of 23.
18. Observe the packets transmitted by the DUT.
19. From G1, transmit IPv6 TCP traffic to G2 containing a source port of 80.
20. Observe the packets transmitted by the DUT.

Part E: Accept traffic with a specific TCP Port Destination

21. Configure the DUT to only accept IPv6 TCP traffic from the destination port of 23.
22. From G1, transmit IPv6 TCP traffic to G2 containing a destination port of 23.
23. Observe the packets transmitted by the DUT.
24. From G1, transmit IPv6 TCP traffic to G2 containing a destination port of 80.
25. Observe the packets transmitted by the DUT.

Part F: Accept traffic with a specific TCP Port Source

26. Configure the DUT to only accept IPv6 TCP traffic from the source port of 23.

27. From G1, transmit IPv6 TCP traffic to G2 containing a source port of 23.
28. Observe the packets transmitted by the DUT.
29. From G1, transmit IPv6 TCP traffic to G2 containing a source port of 80.
30. Observe the packets transmitted by the DUT.

Observable Results:

- *In Part A,*
  Step 3: The DUT must not forward the IPv6 TCP traffic with a destination port of 23 to G2.
  Step 5: The DUT must not forward the IPv6 TCP traffic with a destination port of 80 to G2.
- *In Part B,*
  Step 8: The DUT must forward the IPv6 TCP traffic with a destination port of 23 to G2.
  Step 10: The DUT must forward the IPv6 TCP traffic with a destination port of 80 to G2.
- *In Part C,*
  Step 13: The DUT must not forward the IPv6 TCP traffic with a destination port of 23 to G2.
  Step 15: The DUT must forward the IPv6 TCP traffic with a destination port of 80 to G2.
- *In Part D,*
  Step 18: The DUT must not forward the IPv6 TCP traffic with a source port of 23 to G2.
  Step 20: The DUT must forward the IPv6 TCP traffic with a source port of 80 to G2.
- *In Part E,*
  Step 23: The DUT must forward the IPv6 TCP traffic with a destination port of 23 to G2.
  Step 25: The DUT must not forward the IPv6 TCP traffic with a destination port of 80 to G2.
- *In Part F,*
  Step 28: The DUT must forward the IPv6 TCP traffic with a source port of 23 to G2.
  Step 30: The DUT must not forward the IPv6 TCP traffic with a source port of 80 to G2.

Possible Problems:

- None.

Test AP.1.5: ICMPv6 Traffic

Purpose: To verify that a device properly accepts and denies ICMPv6 traffic based on policy.

References: ICMPv6

Discussion: IPv6 nodes report errors encountered in processing packets and perform other internet-layer functions through the use of Internet Control Message Protocol for IPv6 (ICMPv6). These functions specifically include: (1) Destination Unreachable, (2) Packet Too Big, (3) Time Exceeded, (4) Parameter Problem, (128) Echo Request, (129) Echo Reply. The ICMPv6 functionality has been extended to have local meanings (133) Router Solicitation, (134) Router Advertisement, (135) Neighbor Solicitation, (136) Neighbor Advertisement and (137) Redirect.

Test Setup: Common Test Setup is performed. The Common Test Cleanup procedure is performed after each part.

Procedure:

Part A: Deny all ICMPv6 traffic

1. Configure the DUT to deny all ICMPv6 traffic on the interface connected to G1.
2. From G1, transmit an ICMPv6 Echo Request to G2.
3. Observe the packets transmitted by the DUT.

4. From G1, transmit an ICMPv6 Echo Reply to G2.
5. Observe the packets transmitted by the DUT.

Part B: Allow all ICMPv6 traffic

6. Configure the DUT to allow all ICMPv6 traffic on the interface connected to G1.
7. From G1, transmit an ICMPv6 Echo Request to G2.
8. Observe the packets transmitted by the DUT.

9. From G1, transmit an ICMPv6 Echo Reply to G2.
10. Observe the packets transmitted by the DUT.

Part C: Deny ICMPv6 Echo Request messages, accept all other ICMPv6 Traffic

11. Configure the DUT to deny ICMPv6 Echo Request messages on the interface connected to G1.
12. From G1, transmit an ICMPv6 Echo Request to G2.
13. Observe the packets transmitted by the DUT.
14. From G1, transmit an ICMPv6 Echo Reply to G2.

15. Observe the packets transmitted by the DUT.
16.

Part D: Accept ICMPv6 Echo Request messages, deny all other ICMPv6

17. Configure the DUT to allow only ICMPv6 Echo Request messages on the interface connected to G1.
18. From G1, transmit an ICMPv6 Echo Request to G2.
19. Observe the packets transmitted by the DUT.

20. From G1, transmit an ICMPv6 Echo Reply to G2.
21. Observe the packets transmitted by the DUT.

Observable Results:

- *In Part A,*
  Step 3: The DUT must not forward the ICMPv6 Echo Request to G2.
  Step 5: The DUT must not forward the ICMPv6 Echo Reply to G2.
- *In Part B,*
  Step 8: The DUT must forward the ICMPv6 Echo Request to G2.
  Step 10: The DUT must forward the ICMPv6 Echo Reply to G2.
- *In Part C,*
  Step 13: The DUT must not forward the ICMPv6 Echo Request to G2.
  Step 15: The DUT must forward the ICMPv6 Echo Reply to G2.

- *In Part D,*
  Step 23: The DUT must forward the ICMPv6 Echo Request to G2.

  Step 28: The DUT must not forward the ICMPv6 Echo Reply to G2.

Possible Problems:

- None.

Test AP.1.6: Time Based Authorization

Purpose: To verify that a device properly denies source and IPv6 addresses based on time.

References: IPv6-SPEC

Discussion: The primary building block for network access is accepting and denying application traffic based on source and destination IPv6 addresses. Functionality can be increased if this can be extended to a specific access time.

Test Setup: Common Test Setup is performed. The Common Test Cleanup procedure is performed after each part.

Procedure:

Part A: Deny all IPv6 traffic for specific time

1. Configure the DUT to deny all IPv6 traffic on the interface connected to G1 for 2 minutes.
2. From G1, transmit HTTPv6 traffic to G2.
3. Observe the packets transmitted by the DUT.
4. After 2 minutes has expired, from G1 transmit HTTPv6 traffic to G2.
5. Observe the packets transmitted by the DUT.

Part B: Allow all IPv6 traffic for specific time

6. Configure the DUT to allow all IPv6 traffic on the interface connected to G1 for 2 minutes, after which the DUT should deny all IPv6 traffic.
7. From G1, transmit HTTPv6 traffic to G2.
8. Observe the packets transmitted by the DUT.
9. After 2 minutes has expired, from G1 transmit HTTPv6 traffic to G2.
10. Observe the packets transmitted by the DUT.

Part C: Deny all traffic with a global IPv6 Source Address for a specific time

11. Configure the DUT to deny all IPv6 traffic from a source address of 4000::1 on the interface connected to G1 for 2 minutes.
12. From G1, transmit HTTPv6 traffic with a source address of 4000::1 to G2.
13. Observe the packets transmitted by the DUT.
14. After 2 minutes has expired, from G1 transmit HTTPv6 traffic with a source address of 4000::1 to G2.
15. Observe the packets transmitted by the DUT on G2.

Part D: Deny all traffic with a global IPv6 Destination Address for a specific time

16. Configure the DUT to deny all IPv6 traffic from a destination address of 4000::1 on the interface connected to G1 for 2 minutes.
17. From G1, transmit HTTPv6 traffic with a destination address of 4000::1 to G2.
18. Observe the packets transmitted by the DUT.
19. After 2 minutes has expired, from G1 transmit HTTPv6 traffic with a destination address of 4000::1 to G2.
20. Observe the packets transmitted by the DUT on G2.

Part E: Deny all traffic with a global IPv6 Source Network Address for a specific time

21. Configure the DUT to deny all IPv6 traffic from a source address of 4000::/64 on the interface connected to G1 for 2 minutes.
22. From G1, transmit HTTPv6 traffic with a source address of 4000::5, 4000::1 and 5000::1 to G2.
23. Observe the packets transmitted by the DUT.
24. After 2 minutes has expired, from G1 transmit HTTPv6 traffic with a source address of 4000::5, 4000::1 and 5000::1 to G2.
25. Observe the packets transmitted by the DUT.

Part F: Deny all traffic with a global IPv6 Destination Network Address for a specific time

26. Configure the DUT to deny all IPv6 traffic from a destination address of 4000::/64 on the interface connected to G1 for 2 minutes.
27. From G1, transmit HTTPv6 traffic with a destination address of 4000::5, 4000::1 and 5000::1 to G2.
28. Observe the packets transmitted by the DUT.
29. After 2 minutes has expired, from G1 transmit HTTPv6 traffic with a destination address of 4000::5, 4000::1 and 5000::1 to G2.
30. Observe the packets transmitted by the DUT.

Observable Results:

- *In Part A,*
  Step 3: The DUT must not forward the HTTPv6 traffic to G2.
  Step 5: The DUT must forward the HTTPv6 traffic to G2.
- *In Part B,*
  Step 8: The DUT must forward the HTTPv6 traffic to G2.
  Step 10: The DUT must not forward the HTTPv6 traffic to G2.
- *In Part C,*
  Step 13: The DUT must not forward the HTTPv6 traffic with a source address of 4000::1 to G2.
  Step 15: The DUT must forward the HTTPv6 traffic with a source address of 4000::1 to G2.
- *In Part D,*
  Step 18: The DUT must not forward the HTTPv6 traffic with a destination address of 4000::1 to G2.
  Step 20: The DUT must forward the HTTPv6 traffic with a destination address of 4000::1 to G2.
- *In Part E,*
  Step 23: The DUT must not forward the HTTPv6 traffic with a source address of 4000::1 or 4000::5 to G2. The DUT must forward the HTTPv6 traffic with a source address of 5000::1 to G2.
  Step 25: The DUT must forward the HTTPv6 traffic with a source address of 4000::1, 4000::5 and 5000::1 to G2.
- *In Part F,*
  Step 28: The DUT must not forward the HTTPv6 traffic with a destination address of 4000::1 or 4000::5 to G2. The DUT must forward the HTTPv6 traffic with a destination address of 5000::1 to G2.

Step 30: The DUT must forward the HTTPv6 traffic with a destination address of 4000::1, 4000::5 and 5000::1 to G2.

Possible Problems:

- The DUT might not allow setting Deny/Accept lists to expire, they might be static.

Test AP.1.7: IPSec Forwarding

Purpose: To verify that a device will properly forward IPSec traffic.

References: IPSec

Discussion: IPSec traffic should be setup to be forwarded end-to-end. A device should have the configuration flexibility to support a rule that allows or denies traffic with a next header of 50.

Test Setup: Common Test Setup is performed. The Common Test Cleanup procedure is performed after each part.

Procedure:

Part A: Deny IPv6 traffic with a next header of 50 (IPSec)

1. Configure the DUT to deny only IPv6 traffic with a next header of 50 on the interface connected to G1.
2. From G1, transmit IPv6 traffic to G2 containing a next header of 50.
3. Observe the packets transmitted by the DUT.
4. From G1, transmit IPv6 traffic to G2 containing a next header of 6.
5. Observe the packets transmitted by the DUT.

Part B: Accept IPv6 traffic with a next header of 50 (IPSec)

6. Configure the DUT to accept only IPv6 traffic with a next header of 50 on the interface connected to G1.
7. From G1, transmit IPv6 traffic to G2 containing a next header of 50.
8. Observe the packets transmitted by the DUT.
9. From G1, transmit IPv6 traffic to G2 containing a next header of 6.
10. Observe the packets transmitted by the DUT.

Observable Results:

- *In Part A,*
  Step 3: The DUT must not forward the IPpv6 traffic with a next header of 50 to G2.
  Step 5: The DUT must forward the IPv6 traffic with a next header of 6 to G2.
- *In Part B,*
  Step 8: The DUT must forward the IPv6 traffic with a next header of 50 to G2.
  Step 10: The DUT must not forward the IPv6 traffic with a next header of 6 to G2.

Possible Problems:

- None.

GROUP 2: Advanced AP Functionality

Scope:

The following tests are designed to verify the functionality and operation of IPv6 based access authorization and other advanced features.

Overview:

Access Policies (APs) are static accept and deny features that some IP Routers have to limit access between networks. This reduces the ability to attack insecure hosts and the information on them. Acceptance and rejection policy can be based upon IP address, time and/or TCP/UDP fields.

Test AP.2.1: Combination Authorization

Purpose: To verify that a device properly accepts and denies traffic based on multiple rules.

References: IPv6-SPEC

Discussion: Multiple rules for traffic acceptance and denial allow a device to accept and deny traffic for a complex authorization policy.

Test Setup: Common Test Setup is performed. The Common Test Cleanup procedure is performed after each part.

Procedure:

Part A: Time, Source Address, Destination Address

1. Configure the DUT to deny IPv6 traffic from a source address of 4000::1 or destination address of 5000::1 on the interface connected to G1 for 2 minutes.
2. From G1, transmit HTTPv6 traffic to G2 with a source address of 4000:1 and a destination address 6000::1.
3. Observe the packets transmitted by the DUT.
4. From G1, transmit HTTPv6 traffic to G2 with a source address of 7000::1 and a destination address of 5000::1.
5. Observe the packets transmitted by the DUT.
6. From G1, transmit HTTPv6 traffic to G2 with a source address of 7000::1 and a destination address of 6000::1.
7. Observe the packets transmitted by the DUT.
8. After 2 minutes repeat steps 2 through 6.
9. Observe the packets transmitted by the DUT.

Part B: Time, UDP, Source Address, Destination Address

10. Configure the DUT to deny IPv6 traffic containing a UDP source port of 21 from a source address of 4000::1 or destination address of 5000::1 on the interface connected to G1 for 2 minutes.
11. From G1, transmit IPv6 UDP traffic to G2 containing a source port of 69 with a source address of 4000:1 and a destination address 6000::1.
12. Observe the packets transmitted by the DUT.
13. From G1, transmit IPv6 UDP traffic to G2 containing a source port of 69 with a source address of 7000::1 and a destination address of 5000::1.
14. Observe the packets transmitted by the DUT.
15. From G1, transmit IPv6 UDP traffic to G2 containing a source port of 21 with a source address of 7000::1 and a destination address of 6000::1.
16. Observe the packets transmitted by the DUT.
17. From G1, transmit IPv6 UDP traffic to G2 containing a source port of 69 with a source address of 7000::1 and a destination address of 6000::1.
18. Observe the packets transmitted by the DUT.
19. After 2 minutes repeat steps 11 through 17.
20. Observe the packets transmitted by the DUT.

Part C: Time, TCP, Source Address, Destination Address

21. Configure the DUT to deny IPv6 traffic containing a TCP source port of 23 from a source address of 4000::1 or destination address of 5000::1 on the interface connected to G1 for 2 minutes.
22. From G1, transmit IPv6 TCP traffic to G2 containing a source port of 22 with a source address of 4000:1 and a destination address 6000::1.
23. Observe the packets transmitted by the DUT.
24. From G1, transmit IPv6 TCP traffic to G2 containing a source port of 22 with a source address of 7000::1 and a destination address of 5000::1.
25. Observe the packets transmitted by the DUT.
26. From G1, transmit IPv6 TCP traffic to G2 containing a source port of 23 with a source address of 7000::1 and a destination address of 6000::1.
27. Observe the packets transmitted by the DUT.
28. From G1, transmit IPv6 TCP traffic to G2 containing a source port of 22 with a source address of 7000::1 and a destination address of 6000::1.
29. Observe the packets transmitted by the DUT.
30. After 2 minutes repeat steps 22 through 28.
31. Observe the packets transmitted by the DUT.

Part D: Time, ICMPv6, Source Address, Destination Address

32. Configure the DUT to deny ICMPv6 Echo Requests and IPv6 traffic from a source address of 4000::1 or destination address of 5000::1 on the interface connected to G1 for 2 minutes.
33. From G1, transmit an ICMPv6 Echo Reply to G2 with a source address of 4000:1 and a destination address 6000::1.
34. Observe the packets transmitted by the DUT.
35. From G1, transmit an ICMPv6 Echo Reply to G2 with a source address of 7000::1 and a destination address of 5000::1.
36. Observe the packets transmitted by the DUT.
37. From G1, transmit an ICMPv6 Echo Request to G2 with a source address of 7000::1 and a destination address of 6000::1.
38. Observe the packets transmitted by the DUT.
39. From G1, transmit an ICMPv6 Reply to G2 with a source address of 7000::1 and a destination address of 6000::1.
40. Observe the packets transmitted by the DUT.
41. After 2 minutes repeat steps 33 through 39.
42. Observe the packets transmitted by the DUT.

Observable Results:

- *In Part A,*
  Step 3: The DUT must not forward the HTTPv6 traffic with a source address of 4000:1 and a destination address 6000::1 to G2.
  Step 5: The DUT must not forward the HTTPv6 traffic with a source address of 7000::1 and a destination address of 5000::1 to G2.
  Step 7: The DUT must forward the HTTPv6 traffic with a source address of 6000::1 and a destination address of 6000::1 to G2.
  Step 9: The DUT must forward the HTTPv6 traffic to G2.
- *In Part B,*

Step 12: The DUT must not forward the IPv6 UDP traffic containing a source port of 69 with a source address of 4000:1 and a destination address 6000::1 to G2.
Step 14: The DUT must not forward the IPv6 UDP traffic containing a source port of 69 with a source address of 7000::1 and a destination address of 5000::1 to G2.
Step 16: The DUT must not forward the IPv6 UDP traffic containing a source port of 21 with a source address of 7000::1 and a destination address of 6000::1 to G2.
Step 18: The DUT must forward the IPv6 UDP traffic containing a source port of 69 with a source address of 7000::1 and a destination address of 6000::1 to G2.
Step 20: The DUT must forward the IPv6 UDP traffic to G2.

- *In Part C,*
  Step 23: The DUT must not forward the IPv6 TCP traffic containing a source port of 22 with a source address of 4000::1 and a destination address of 5000::1 to G2.
  Step 25: The DUT must not forward the IPv6 TCP traffic containing a source port of 22 with a source address of 7000::1 and a destination address of 5000::1 to G2.
  Step 27: The DUT must not forward the IPv6 TCP traffic containing a source port of 23 with a source address of 7000::1 and a destination address of 6000::1 to G2.
  Step 29: The DUT must forward the IPv6 TCP traffic containing a source port of 22 with a source address of 7000::1 and a destination address of 6000::1.
  Step 31: The DUT must forward the IPv6 TCP traffic to G2.
- *In Part D,*
  Step 34: The DUT must not forward the ICMPv6 Echo Reply with a source address of 4000::1 and a destination address of 6000::1 to G2.
  Step 36: The DUT must not forward the ICMPv6 Echo Reply with a source address of 7000::1 and a destination address of 5000::1 to G2.
  Step 38: The DUT must not forward the ICMPv6 Echo Request with a source address of 7000::1 and a destination address of 6000::1 to G2.
  Step 40: The DUT must forward the ICMPv6 Echo Reply with a source address of 7000::1 and a destination address of 6000::1 to G2.
  Step 42: The DUT must forward the ICMPv6 traffic to G2.

Possible Problems:

- The DUT might not allow setting Deny/Accept lists to expire, they might be static.

Test AP.2.2: Ordered List Policy

Purpose: To verify that a device properly implements an ordered list policy procedure.

References: IPv6-SPEC, TCP

Discussion: Access policies usually are in an ordered list and first match rule applies. To test this, a more specific deny rule is defined first and a more generic permit rule is defined second. It is ensured that the traffic matched the specific rules is dropped. The opposite scenario will ensure the traffic is permitted.

Test Setup: Common Test Setup is performed. The Common Test Cleanup procedure is performed after each part.

Procedure:

Part A: Specific Deny, Generic Allow

1. As the first item on the ordered configuration list, configure the DUT to deny IPv6 traffic containing a TCP port of 23 on the interface connected to G1.
2. As the second item on the ordered configuration list, configure the DUT to accept all IPv6 TCP traffic on the interface connected to G1.
3. From G1, transmit IPv6 traffic to G2 containing a TCP destination port of 23.
4. Observe the packets transmitted by the DUT.
5. From G1, transmit IPv6 traffic to G2 containing a TCP destination port of 22.
6. Observe the packets transmitted by the DUT.

Part B: Generic Allow, Specific Deny

7. As the first item on the ordered configuration list, configure the DUT to accept all IPv6 TCP traffic on the interface connected to G1.
8. As the second item on the ordered configuration list, configure the DUT to deny IPv6 traffic containing a TCP destination port of 23 on the interface connected to G1.
9. From G1, transmit IPv6 traffic to G2 containing a TCP destination port of 23.
10. Observe the packets transmitted by the DUT.
11. From G1, transmit IPv6 traffic to G2 containing a TCP destination port of 22.
12. Observe the packets transmitted by the DUT.

Part C: Specific Allow, Generic Deny

13. As the first item on the ordered configuration list, configure the DUT to allow IPv6 traffic containing a TCP port of 23 on the interface connected to G1.
14. As the second item on the ordered configuration list, configure the DUT to deny all IPv6 TCP traffic on the interface connected to G1.
15. From G1, transmit IPv6 traffic to G2 containing a TCP destination port of 23.
16. Observe the packets transmitted by the DUT.
17. From G1, transmit IPv6 traffic to G2 containing a TCP destination port of 22.
18. Observe the packets transmitted by the DUT.

Part D: Generic Deny, Specific Allow

19. As the first item on the ordered configuration list, configure the DUT to deny all IPv6 TCP traffic on the interface connected to G1.

20. As the second item on the ordered configuration list, configure the DUT to allow IPv6 traffic containing a TCP port of 23 on the interface connected to G1.
21. From G1, transmit IPv6 traffic to G2 containing a TCP destination port of 23.
22. Observe the packets transmitted by the DUT.
23. From G1, transmit IPv6 traffic to G2 containing a TCP destination port of 22.
24. Observe the packets transmitted by the DUT.

Observable Results:

- *In Part A,*
  Step 4: The DUT must not forward the IPv6 traffic containing a TCP destination port of 23 to G2.
  Step 6: The DUT must forward the IPv6 traffic containing a TCP destination port of 22 to G2.
- *In Part B,*
  Step 10: The DUT must forward the IPv6 traffic containing a TCP destination port of 23 to G2.
  Step 12: The DUT must forward the IPv6 traffic containing a TCP destination port of 22 to G2.
- *In Part C,*
  Step 16: The DUT must forward the IPv6 traffic containing a TCP destination port of 23 to G2.
  Step 18: The DUT must not forward the IPv6 traffic containing a TCP destination port of 22 to G2.
- *In Part D,*
  Step: The DUT must not forward the IPv6 traffic containing a TCP destination port of 23 to G2.
  Step 24: The DUT must not forward the IPv6 traffic containing a TCP destination port of 22 to G2.

Possible Problems:

- None.