

Moonv6 Test Suite
*IPv6 Firewall Functionality and
Interoperability Test Suite*

Technical Document

Revision 0.6



*IPv6 Consortium
InterOperability Laboratory
Research Computing Center
University of New Hampshire*

*121 Technology Drive, Suite 2
Durham, NH 03824-3525
Phone: (603) 862-2804
Fax: (603) 862-4181
<http://www.iol.unh.edu>*

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	4
INTRODUCTION	5
TEST ORGANIZATION.....	6
REFERENCES	7
GROUP 1: Basic Security Policy.....	8
Test FIR.1.1: Source Address Denial.....	9
Test FIR.1.2: Source Address Acceptance.....	11
Test FIR.1.3: Destination Address Denial.....	13
Test FIR.1.4: Destination Address Acceptance.....	15
Test FIR.1.5: UDP Port Numbers	17
Test FIR.1.6: TCP Port Numbers	19
Test FIR.1.7: ICMPv6 Traffic.....	21
Test FIR.1.8: Time Based Authorization	23
Test FIR.1.9: Combination Authorization.....	25
Test FIR.1.10: Firewall Screening	27
Test FIR.1.11: Address Autoconfiguration	29
Test FIR.1.12: Ordered List Policy	31
GROUP 2: IPv4 and IPv6 Authorization.....	33
Test FIR.2.1: IPv4 Authorization	34
Test FIR.2.2: IPv4 and IPv6 Functionality, Same Policy	36
Test FIR.2.3: IPv4 and IPv6 Functionality, Different Policy.....	38
GROUP 3: Logging.....	40
Test FIR.3.1: Logging with IPv6 Functionality	41
Test FIR.3.2: Logging with IPv4 and IPv6 Functionality	43
GROUP 4: Stateful Inspection.....	45
Test FIR.4.1: IPv6 TCP State.....	46
Test FIR.4.2: Mixed IPv4 and IPv6 TCP State	48
Test FIR.4.3: FTP State Inspection	50
Test FIR.4.4: ICMP State Inspection	51
Test FIR.4.5: UDP State Inspection	53
GROUP 5: Advanced Filtering.....	55
Test FIR.5.1: Multiprotocol Filtering.....	56

MODIFICATION RECORD

Draft Version Complete

Version 0.3

Version 0.5

Version 0.6

February 22, 2004

February 24, 2004: Fixed inconsistencies and typos.

Removed Part E from FIR.1.10. Added Group 5, added Part C to FIR 2.3, Added FIR.4.3, FIR.4.4.and FIR.4.5. Added part D to FIR.4.1. Added test FIR.1.12.

Added discussion on interface definition. Added Part E to FIR.1.7 and an extra set of parts to FIR.4.5 (UDP State Inspection).

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 for the base test items. Special thanks to Cisco and NetScreen for contributing additional test ideas for the base document for the first revision.

Yoni Appel	Check Point Software Technologies
Alan Bavosa	NetScreen Technologies
Paul Del Fante	Cisco Systems
Eli Ginot	Check Point Software Technologies
Vincent Le May	6Wind
Changming Liu	NetScreen Technologies
Shiva Mittal	Cisco Systems
Jeff Parker	Cisco Systems
Kari Revier	University of New Hampshire
Cathy Rhoades	University of New Hampshire
Benjamin Schultz	University of New Hampshire
Zlata Trhulj	Agilent Technologies
Dennis Vogel	Cisco Systems
Erica Williamsen	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 their Internet Protocol, version 6 firewall products. The tests do not determine if a product conforms to the IPv6 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 other IPv6 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 IPv6 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 firewall 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

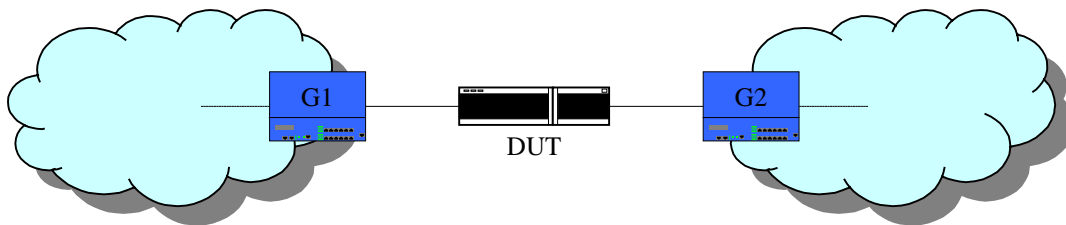
DUT: Device Under Test

TR: Testing Router

G: Traffic Generator

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.

Test Configuration



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.

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 FIR.1.2 refers to the second test of the first test group in the Firewall 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.
Resource Requirements:	The Resource Requirements section specifies the software, hardware, and test equipment that will be needed to perform the test.
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.

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

GROUP 1: Basic Security Policy

Scope:

These tests are designed to verify basic functionality and operation of IPv6-based access authorization and firewall screening.

Overview:

Firewalls are designed 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 services accessed.

Test FIR.1.1: Source Address Denial

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

References: IPv6-SPEC

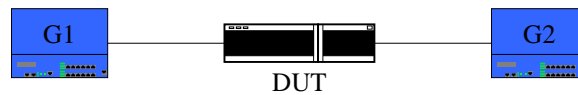
Resource Requirements:

- Monitor to capture packets

Last Modification: February 20, 2004

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 firewall properly denies traffic sourced from a specific location.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Deny all traffic originating from a global IPv6 Address

1. Configure the DUT to deny all traffic from a globally defined source IPv6 address on its interface connected to G1.
2. From G1, transmit traffic to G2 containing the source IPv6 address configured in the previous step.
3. From G1, transmit traffic to G2 containing a different global source address.
4. Observe the packets transmitted by the DUT on G2.

Part B: Deny all traffic originating from a link local IPv6 Address

5. Configure the DUT to deny all traffic from a link local defined source IPv6 address on its interface connected to G1.
6. From G1, transmit traffic to G2 containing the source IPv6 address configured in the previous step.
7. From G1, transmit traffic to G2 containing a different global source address.
8. Observe the packets transmitted by the DUT on G2.

Part C: Deny all traffic originating from a global IPv6 Network Address

9. Configure the DUT to deny all traffic from a globally defined source IPv6 network on its interface connected to G1.
10. From G1, transmit traffic to G2 containing the source IPv6 address range configured in the previous step.
11. From G1, transmit traffic to G2 containing a different global source network.
12. Observe the packets transmitted by the DUT on G2.

Part D: Deny all traffic originating from a link local IPv6 Network Address

13. Configure the DUT to deny all traffic from a link local defined source IPv6 network on its interface connected to G1.
14. From G1, transmit traffic to G2 containing the source IPv6 address range configured in the previous step.
15. From G1, transmit traffic to G2 containing a different global source network.
16. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In all Parts, the traffic transmitted from denied addresses/networks on G1 should not be forwarded by the DUT nor observed on G2. The traffic transmitted from the other address/networks at G1 should be forwarded by the DUT and observed on G2.

Possible Problems: The DUT may not allow the configuration of accept or deny function for the link-local address.

Test FIR.1.2: Source Address Acceptance

Purpose: To verify that a firewall properly accepts source IPv6 addresses based on policy.

References: IPv6-SPEC

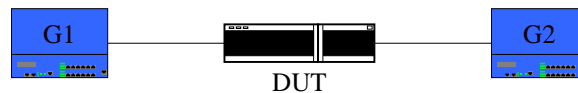
Resource Requirements:

- Monitor to capture packets

Last Modification: February 20, 2004

Discussion: The primary building deny for network access is accepting and denying application traffic based on source and destination IP addresses. The following verifies that a firewall properly forwards traffic sourced from a specific location.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Accept all traffic originating from a global IPv6 Address

1. Configure the DUT to accept all traffic from a globally defined source IPv6 address on the interface connected to G1.
2. From G1, transmit traffic to G2 containing the source IPv6 address configured in Step 1.
3. Observe the packets transmitted by the DUT on G2.

Part B: Accept all traffic originating from a link local IPv6 Address

4. Configure the DUT to accept all traffic from a link local defined source IPv6 address on the interface connected to G1.
5. From G1, transmit traffic to G2 containing the source IPv6 address configured in the previous step.
6. Observe the packets transmitted by the DUT on G2.

Part C: Accept all traffic originating from a global IPv6 Network Address

7. Configure the DUT to accept all traffic from a globally defined source IPv6 network on the interface connected to G1.
8. From G1, transmit traffic to G2 containing the source IPv6 address range configured in the previous step.
9. Observe the packets transmitted by the DUT on G2.

Part D: Accept all traffic originating from a link local IPv6 Network Address

10. Configure the DUT to accept all traffic from a link local defined source IPv6 network on the interface connected to G1.
11. From G1, transmit traffic to G2 containing the source IPv6 address range configured in the previous step.
12. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Parts A and C, the traffic transmitted from G1 should be forwarded by the DUT and observed on G2.
- In Parts B and D, the traffic transmitted from the link-local addresses/networks on G1 should not be forwarded by the DUT nor observed on G2. Link local addresses are not globally accessible.

Possible Problems: The DUT may not allow the configuration of accept or deny function for the link-local address.

Test FIR.1.3: Destination Address Denial

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

References: IPv6-SPEC

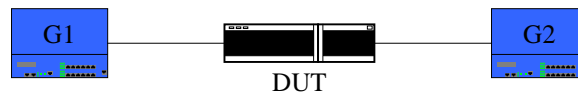
Resource Requirements:

- Monitor to capture packets

Last Modification: February 20, 2004

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 firewall properly denies traffic destined to a specific location.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Deny all traffic with a global IPv6 Address Destination

1. Configure the DUT to deny all traffic from a globally defined destination IPv6 address on the interface connected to G1.
2. From G1, transmit traffic to G2 containing the destination IPv6 address configured in the previous step.
3. From G1, transmit traffic to G2 containing a different destination address.
4. Observe the packets transmitted by the DUT on G2.

Part B: Deny all traffic with a link local IPv6 Address Destination

5. Configure the DUT to deny all traffic from a link local defined destination IPv6 address on the interface connected to G1.
6. From G1, transmit traffic to G2 containing the destination IPv6 address configured in the previous step.
7. From G1, transmit traffic to G2 containing a different destination address.
8. Observe the packets transmitted by the DUT on G2.

Part C: Deny all traffic with a global IPv6 Network Address Destination

9. Configure the DUT to deny all traffic from a globally defined destination IPv6 network on the interface connected to G1.
10. From G1, transmit traffic to G2 containing the destination IPv6 address range configured in the previous step.
11. From G1, transmit traffic to G2 containing a different destination network.
12. Observe the packets transmitted by the DUT on G2.

Part D: Deny all traffic all traffic with a global IPv6 Network Address Destination

13. Configure the DUT to deny all traffic from a link local defined destination IPv6 network on the interface connected to G1.
14. From G1, transmit traffic to G2 containing the destination IPv6 address range configured in the previous step.
15. From G1, transmit traffic to G2 containing a different destination network.
16. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In all parts, the traffic transmitted from denied addresses/networks on G1 should not be forwarded by the DUT nor observed on G2. The traffic transmitted from the other address/networks at G1 should be forwarded by the DUT and observed on G2.

Possible Problems: The DUT may not allow the configuration of accept or deny function for the link-local address.

Test FIR.1.4: Destination Address Acceptance

Purpose: To verify that a firewall properly accepts destination IPv6 addresses based on policy.

References: IPv6-SPEC

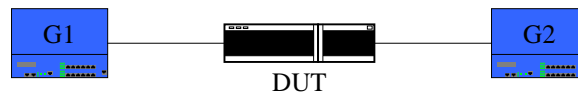
Resource Requirements:

- Monitor to capture packets

Last Modification: February 20, 2004

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 firewall properly accepts traffic based on destination address.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Accept all traffic with a global IPv6 Address Destination

1. Configure the DUT to accept all traffic from a globally defined destination IPv6 address on the interface connected to G1.
2. From G1, transmit traffic to G2 containing the source IPv6 address configured in the previous step.
3. Observe the packets transmitted by the DUT on G2.

Part B: Accept all traffic with a link local IPv6 Address Destination

4. Configure the DUT to accept all traffic from a link local defined destination IPv6 address on the interface connected to G1.
5. From G1, transmit traffic to G2 containing the destination IPv6 address configured in the previous step.
6. Observe the packets transmitted by the DUT on G2.

Part C: Accept all traffic with a global IPv6 Network Address Destination

7. Configure the DUT to accept all traffic from a globally defined destination IPv6 network on the interface connected to G1.
8. From G1, transmit traffic to G2 containing the destination IPv6 address range configured in the previous step.
9. Observe the packets transmitted by the DUT on G2.

Part D: Accept all traffic with a link local IPv6 Network Address Destination

10. Configure the DUT to accept all traffic from a link local defined destination IPv6 network on the interface connected to G1.
11. From G1, transmit traffic to G2 containing the destination IPv6 address range configured in the previous step.
12. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Parts A and C, the traffic transmitted from G1 should be forwarded by the DUT and observed on G2.
- In Parts B and D, the traffic transmitted from the link-local addresses/networks on G1 should not be forwarded by the DUT nor observed on G2.

Possible Problems: The DUT may not allow the configuration of accept or deny function for the link-local address.

Test FIR.1.5: UDP Port Numbers

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

References: UDP

Resource Requirements:

- Monitor to capture packets

Last Modification: February 20, 2004

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 firewall properly accepts traffic to and from a UDP port.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Deny all traffic with a specific UDP Port Destination

1. Configure the DUT to deny all traffic containing a destination UDP port on the interface connected to G1.
2. From G1, transmit traffic containing the destination UDP port configured in the previous step.
3. From G1, transmit traffic to G2 containing a different destination UDP port.
4. Observe the packets transmitted by the DUT on G2.

Part B: Deny all traffic with a specific UDP Port Source

5. Configure the DUT to deny all traffic containing a source UDP port on the interface connected to G1.
6. From G1, transmit traffic to G2 containing the source UDP port configured in the previous step.
7. From G1, transmit traffic to G2 containing a different source UDP port.
8. Observe the packets transmitted by the DUT on G2.

Part C: Accept all traffic with a specific UDP Port Destination

9. Configure the DUT to accept all traffic containing a destination UDP port on the interface connected to G1.
10. From G1, transmit traffic to G2 containing the destination UDP port configured in the previous step.
11. Observe the packets transmitted by the DUT on G2.

Part D: Accept all traffic with a specific UDP Port Source

12. Configure the DUT to accept all traffic containing a source UDP port on the interface connected to G1.
13. From G1, transmit traffic to G2 containing the source UDP port configured in the previous step.
14. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Parts A and B, the traffic transmitted from denied UDP port on G1 should not be forwarded by the DUT nor observed on G2. The traffic transmitted from the other UDP port at G1 should be forwarded by the DUT and observed on G2.
- In Parts C and D, the traffic transmitted from G1 should be forwarded by the DUT and observed on G2.

Possible Problems: None.

Test FIR.1.6: TCP Port Numbers

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

References: TCP

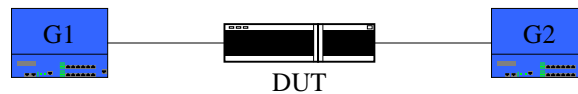
Resource Requirements:

- Monitor to capture packets

Last Modification: February 20, 2004

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 firewall properly accepts traffic to and from a TCP port.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Deny all traffic with a specific TCP Port Destination

1. Configure the DUT to deny all traffic containing a destination TCP port on the interface connected to G1.
2. From G1, transmit traffic to G2 containing the destination TCP port configured in the previous step.
3. From G1, transmit traffic to G2 containing a different destination TCP port.
4. Observe the packets transmitted by the DUT on G2.

Part B: Deny all traffic with a specific TCP Port Source

5. Configure the DUT to deny all traffic containing a source TCP port on the interface connected to G1.
6. From G1, transmit traffic to G2 containing the source TCP port configured in the previous step.
7. From G1, transmit traffic to G2 containing a different source TCP port.
8. Observe the packets transmitted by the DUT on G2.

Part C: Accept all traffic with a specific TCP Port Destination

9. Configure the DUT to accept all traffic containing a destination TCP port on the interface connected to G1.
10. From G1, transmit traffic to G2 containing the destination TCP port configured in the previous step.
11. Observe the packets transmitted by the DUT on G2.

Part D: Accept all traffic with a specific TCP Port Source

12. Configure the DUT to accept all traffic containing a source TCP port on the interface connected to G1.
13. From G1, transmit traffic to G2 containing the source TCP port configured in the previous step.
14. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Parts A and B, the traffic transmitted from denied TCP ports on G1 should not be forwarded by the DUT nor observed on G2. The traffic transmitted from the other TCP ports at G1 should be forwarded by the DUT and observed on G2.
- In Parts C and D, the traffic transmitted from G1 should be forwarded by the DUT and observed on G2.

Possible Problems: None.

Test FIR.1.7: ICMPv6 Traffic

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

References: ICMPv6

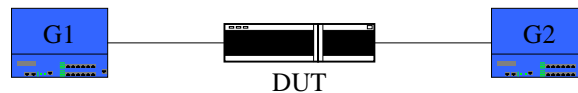
Resource Requirements:

- Monitor to capture packets

Last Modification: February 20, 2004

Discussion: IPv6 nodes report errors encountered in processing packets and to 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 and (134) Router Advertisement, (135) Neighbor Solicitation and (136) Neighbor Advertisement, (137) Redirect. Mobile IPv6 is proposing to use values 150-153. While these values are not yet approved by the IANA, they are essential to Mobile IPv6 operation.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Accept all ICMPv6 traffic

1. Configure the DUT to accept all ICMPv6 traffic on the interface connected to G1.
2. From G1, transmit traffic to G2 containing all possible ICMPv6 message types.
3. Observe the packets transmitted by the DUT on G2.

Part B: Deny all ICMPv6 traffic

4. Configure the DUT to deny all ICMPv6 traffic on the interface connected to G1.
5. From G1, transmit traffic to G2 containing all possible ICMPv6 message types.
6. Observe the packets transmitted by the DUT on G2.

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

7. Configure the DUT to deny only ICMPv6 Echo Request traffic on the interface connected to G1.
8. From G1, transmit traffic to G2 containing all possible ICMPv6 message types.
9. Observe the packets transmitted by the DUT on G2.

Part D: Deny ICMPv6 Echo Reply messages, accept all other ICMPv6 Traffic

10. Configure the DUT to deny only ICMPv6 Echo Reply traffic on the interface connected to G1.
11. From G1, transmit traffic to G2 containing all possible ICMPv6 message types.
12. Observe the packets transmitted by the DUT on G2.

Part E: Accept ICMPv6 PMTU messages

13. Configure the DUT to accept ICMPv6 Path MTU messages on the interface connected to G1.
14. From G2, transmit ICMPv6 Path MTU message to G1.
15. From G1, transmit ICMPv6 Path MTU message to G2.

16. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Part A, the ICMPv6 traffic transmitted from G1 should be forwarded by the DUT and observed on G2.
- In Part B, the ICMPv6 traffic transmitted from G1 should be not forwarded by the DUT and not observed on G2.
- In Part C, the ICMPv6 Echo Request messages transmitted from G1 should not be forwarded by the DUT and not observed on G2. All other ICMPv6 traffic transmitted from G1 should be forwarded by the DUT and observed on G2.
- In Part D, no Echo Replies should be accepted without a previous matching request. The ICMPv6 Echo Reply messages transmitted from G1 should not be forwarded by the DUT and not observed on G2. All other ICMPv6 traffic transmitted from G1 should be forwarded by the DUT and observed on G2.
- In Part E, both Path MTU messages are properly forwarded by the DUT.

Possible Problems: None.

Test FIR.1.8: Time Based Authorization

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

References: IPv6-SPEC

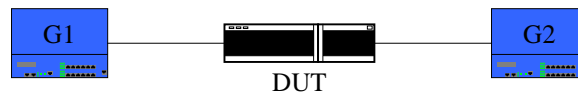
Resource Requirements:

- Monitor to capture packets

Last Modification: February 20, 2004

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

Test Setup: Connect Devices as shown.



Procedure:

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

1. Configure the DUT to deny all traffic from a globally defined source IPv6 address on the interface connected to G1 for 2 minutes from the current time.
2. From G1, transmit traffic to G2 containing the source IPv6 address configured in the previous step.
3. Observe the packets transmitted by the DUT on G2.

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

4. Configure the DUT to deny all traffic from a globally defined destination IPv6 address on the interface connected to G1 for 2 minutes from the current time.
5. From G1, transmit traffic to G2 containing the destination IPv6 address configured in the previous step.
6. Observe the packets transmitted by the DUT on G2.

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

7. Configure the DUT to deny all traffic from a globally defined source IPv6 network on the interface connected to G1 for 2 minutes from the current time.
8. From G1, transmit traffic to G2 containing the source IPv6 address configured in the previous step.
9. Observe the packets transmitted by the DUT on G2.

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

10. Configure the DUT to deny all traffic from a globally defined destination IPv6 network on the interface connected to G1 for 2 minutes from the current time.
11. From G1, transmit traffic to G2 containing the destination IPv6 address configured in the previous step.
12. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In all parts, the traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2 until the two-minute configuration time expires. At that time, traffic transmitted from G1 should be forwarded by the DUT and observed on G2.

Possible Problems: None.

Test FIR.1.9: Combination Authorization

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

References: IPv6-SPEC

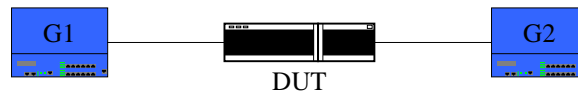
Resource Requirements:

- Monitor to capture packets

Last Modification: February 20, 2004

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

Test Setup: Connect Devices as shown.



Procedure:

Part A: Time, Source Address, Destination Address

1. Configure the DUT to deny all traffic from a globally defined source and destination IPv6 address pair on the interface connected to G1 for 2 minutes from the current time.
2. From G1, transmit traffic to G2 containing a variety of source and destination address pairs. Include packets that match the packet specifications that were configured in step 1.
3. Observe the packets transmitted by the DUT on G2.

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

4. Configure the DUT to deny all traffic from a globally defined source and destination IPv6 address pair on the interface connected to G1 for 2 minutes from the current time.
5. Configure the DUT to deny all traffic containing a source UDP port on the interface connected to G1.
6. From G1, transmit traffic to G2 containing a variety of source and destination address pairs and UDP ports. Include packets that match the packet specifications that were configured in steps 4 and 5.
7. Observe the packets transmitted by the DUT on G2.

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

8. Configure the DUT to deny all traffic from a globally defined source and destination IPv6 address pair on the interface connected to G1 for 2 minutes from the current time.
9. Configure the DUT to deny all traffic containing a source TCP port on the interface connected to G1.
10. From G1, transmit traffic to G2 containing a variety of source and destination address pairs and TCP ports. Include packets that match the packet specifications that were configured in steps 8 and 9.
11. Observe the packets transmitted by the DUT on G2.

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

12. Configure the DUT to deny all traffic from a globally defined source and destination IPv6 address pair on the interface connected to G1 for 2 minutes from the current time.
13. Configure the DUT to deny all ICMPv6 Echo Request messages on the interface connected to G1.

14. From G1, transmit traffic to G2 containing a variety of source and destination address pairs and a mix of ICMPv6 messages and non-ICMPv6 IPv6 traffic. I Include packets that match the packet specifications that were configured in steps 12 and 13.
15. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Part A, the [source, destination address pair] traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2 until the two-minute configuration time expires. At that time, the [source, destination address pair] traffic transmitted from G1 should be forwarded by the DUT and observed on G2. All background traffic transmitted from G1 should be forwarded by the DUT and observed on G2.
- In Part B, the [source, destination address pair and UDP port] traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2 until the two-minute configuration time expires. At that time, all traffic transmitted from G1 should be forwarded by the DUT and observed on G2. All background traffic transmitted from G1 should be forwarded by the DUT and observed on G2.
- In Part C, the [source, destination address pair and TCP port] traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2 until the two-minute configuration time expires. At that time, all traffic transmitted from G1 should be forwarded by the DUT and observed on G2. All background traffic transmitted from G1 should be forwarded by the DUT and observed on G2.
- In Part D, the [source, destination address pair and ICMPv6 Echo Request message] traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2 until the two-minute configuration time expires. At that time, all traffic transmitted from G1 should be forwarded by the DUT and observed on G2. All background traffic transmitted from G1 should be forwarded by the DUT and observed on G2.

Possible Problems: None.

Test FIR.1.10: Firewall Screening

Purpose: To verify that a firewall properly defends against potential Denial of Service attacks.

References: IPv6-SPEC
RFC2827
RFC3013

Resource Requirements:

- Monitor to capture packets

Last Modification: February 28, 2004

Discussion: Denial of Service attacks send disruptive traffic to hosts on a network. This traffic slows or stalls access to those hosts and/or damages the hosts by flooding their buffers and exploiting operating system security holes to gain access. Common attacks include TCP syn flood, UDP flood, ICMP flood, Spoofing, out sequence or out of state TCP packets.

Test Setup: Connect Devices as shown.



Procedure:

Part A: TCP SYN Flood

1. Configure the DUT to prevent a TCP SYN flood situation on the interface connected to G1.
2. From G1, transmit traffic to G2 a high rate of TCP traffic with the SYN bit set of variable IPv6 source addresses.
3. Observe the packets transmitted by the DUT on G2.

Part B: UDP Flood

4. Configure the DUT to prevent a UDP flood situation on the interface connected to G1.
5. From G1, transmit traffic to G2 containing a high rate of UDP traffic of variable IPv6 source addresses.
6. Observe the packets transmitted by the DUT on G2.

Part C: ICMP Flood

7. Configure the DUT to prevent an ICMPv6 flood situation on the interface connected to G1.
8. From G1, transmit traffic to G2 containing a high rate of ICMPv6 Echo Request messages of variable IPv6 source addresses.
9. Observe the packets transmitted by the DUT on G2.

Part D: Out of sequence packets

10. Configure the DUT to monitor the sequence numbers of TCP connections on the interface connected to G1.
11. From G1, transmit traffic to G2 containing the TCP packets that are out of sequence.
12. From G2 emulate a proper TCP connection.
13. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Parts A, B and C, traffic exceeding the allowed rate should be dropped, and a suitable log should be extracted.
- In Part D, the out of sequence TCP traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2.

Possible Problems: None.

Test FIR.1.11: Address Autoconfiguration

Purpose: To verify that a firewall properly implements autoconfiguration functionality.

References: ADDRCONF

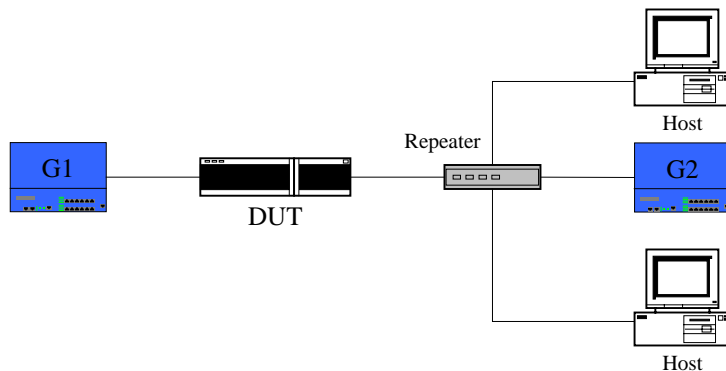
Resource Requirements:

- Monitor to capture packets
- G2 can reply to ICMPv6 Echo Requests

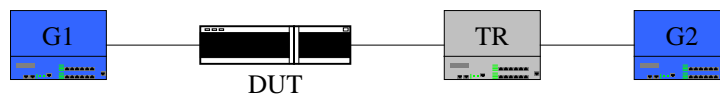
Last Modification: February 20, 2004

Discussion: When a host initializes on a given link, it performs stateless address autoconfiguration and Duplicate Address Detection. A Firewall can act like a host and a router. The objective of this test is to ensure that the DUT can both the prefix delegation router function and the autoconfiguration host function. 64 bit prefixes are used by default with the stateful management flags of the router advertisements disabled. This prefix shall be Prefix “X” and will contain a global IPv6 prefix.

Test Setup: Connect Devices as shown.



Part A: DUT as a Router



Part B: DUT as a Host

Procedure:

Part A: Address Allocation with DUT as a Router

1. Configure the DUT to send Router Advertisements for Prefix “X”.
2. Initialize the devices and allow time for all devices to perform stateless address autoconfiguration.
3. Transmit ICMP Echo Requests from G1 and G2 to the address of each host using Prefix “X”.
4. Observe the packets transmitted by the DUT on G1 and G2.

Part B: Address Allocation with the DUT as a Host

5. Configure the DUT to perform address autoconfiguration as a host.
6. TR1 transmits Router Advertisements with the prefix set to Prefix “X”.

7. Initialize the devices and allow time for all devices to perform stateless address autoconfiguration.
8. Transmit ICMP Echo Requests from G2 and the TR using Prefix “X”.
9. Observe the packets transmitted by the DUT on G1 and G2.

Observable Results:

- In Part A, the Host stations should properly obtain their global addresses and respond to pings from G1 and G2 using Prefix “X”.
- In Part B, the DUT should properly obtain its global addresses and be able to reply to the ICMPv6 Echo Requests to Prefix “X”.

Possible Problems: None.

Test FIR.1.12: Ordered List Policy

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

References: IPv6-SPEC, TCP

Resource Requirements:

- Monitor to capture packets
- G2 can reply to ICMPv6 Echo Requests

Last Modification: February 28, 2004

Discussion: Firewall 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: Connect Devices as shown.



Procedure:

Part A: Specific Deny, Generic Allow

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

Part B: Generic Allow, Specific Deny

6. As the first item on the ordered configuration list, configure the DUT to accept all TCP traffic on the interface connected to G1.
7. As the second item on the ordered configuration list, configure the DUT to deny all traffic containing a destination TCP port on the interface connected to G1.
8. From G1, transmit traffic to G2 containing the destination TCP port configured in the Step 7.
9. From G1, transmit traffic to G2 containing a different destination TCP port.
10. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Part A, the traffic transmitted from denied TCP port on G1 should not be forwarded by the DUT nor observed on G2. The traffic transmitted from other TCP ports at G1 should be forwarded by the DUT and observed on G2.
- In Part B, all traffic transmitted at G1 should be forwarded by the DUT and observed on G2, regardless of the TCP port.

Possible Problems: None.

GROUP 2: IPv4 and IPv6 Authorization

Scope:

These tests are designed to verify the functionality and operation of mixed IPv4 and IPv6 based access authorization and firewall screening.

Overview:

Firewalls are designed 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 services accessed. IPv4 and IPv6 will have a period of time where they co-exist on some networks. This will situation will require firewalls to have capabilities to handle IPv4 and IPv6 traffic.

Test FIR.2.1: IPv4 Authorization

Purpose: To verify that a firewall has basic IPv4 functionality.

References: IP

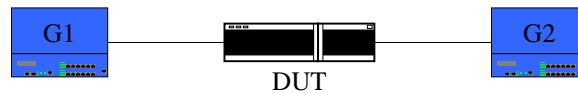
Resource Requirements:

- Monitor to capture packets

Last Modification: February 23, 2004

Discussion: Basic IPv4 functionality includes the ability to accept and deny source and destination address pairs on an IPv4 network.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Deny all traffic with an IPv4 Destination Address

1. Configure the DUT to deny all traffic from a destination IPv4 address on the interface connected to G1.
2. From G1, transmit traffic to G2 containing the destination IPv6 address configured in the previous step.
3. From G1, transmit traffic to G2 containing a different destination address.
4. Observe the packets transmitted by the DUT on G2.

Part B: Deny all traffic with an IPv4 Source Address

5. Configure the DUT to deny all traffic from a source IPv4 address on the interface connected to G1.
6. From G1, transmit traffic to G2 containing the source IPv6 address configured in the previous step.
7. From G1, transmit traffic to G2 containing a different source address.
8. Observe the packets transmitted by the DUT on G2.

Part C: Accept all traffic with an IPv4 Destination Address

9. Configure the DUT to accept all traffic from a destination IPv4 address on the interface connected to G1.
10. From G1, transmit traffic to G2 containing the destination IPv6 address configured in the previous step.
11. Observe the packets transmitted by the DUT on G2.

Part D: Accept all traffic with an IPv4 Source Address

12. Configure the DUT to accept all traffic from a source IPv4 address on the interface connected to G1.
13. From G1, transmit traffic to G2 containing the source IPv6 address configured in the previous step.
14. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Part A, the traffic transmitted from denied destination address on G1 should not be forwarded by the DUT nor observed on G2. The traffic transmitted from the other addresses at G1 should be forwarded by the DUT and observed on G2.
- In Part B, the traffic transmitted from denied source address on G1 should not be forwarded by the DUT nor observed on G2. The traffic transmitted from the other addresses at G1 should be forwarded by the DUT and observed on G2.
- In Part C, the traffic transmitted from the accepted destination address on G1 should be forwarded by the DUT and observed on G2.
- In Part D, the traffic transmitted from the accepted source address on G1 should be forwarded by the DUT and observed on G2.

Possible Problems: None.

Test FIR.2.2: IPv4 and IPv6 Functionality, Same Policy

Purpose: To verify that a firewall can block a service with IPv4 and IPv6.

References: IP
TCP
UDP

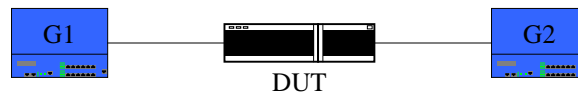
Resource Requirements:

- Monitor to capture packets

Last Modification: February 23, 2004

Discussion: Basic IPv4 functionality includes the ability to accept and deny source and destination address pairs on an IPv4 network.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Deny all traffic with a specific UDP Destination Port

1. Configure the DUT to deny all traffic containing a destination UDP port on the interface connected to G1.
2. From G1 to G2, transmit IPv6 and IPv4 traffic containing the destination UDP port configured in the previous step.
3. From G1 to G2, transmit IPv6 and IPv4 traffic containing a different destination UDP port.
4. Observe the packets transmitted by the DUT on G2.

Part B: Deny all traffic with a specific UDP Source Port

5. Configure the DUT to deny all traffic containing a source UDP port range on the interface connected to G1.
6. From G1 to G2, transmit IPv6 and IPv4 traffic containing the destination UDP port configured in the previous step.
7. From G1 to G2, transmit IPv6 and IPv4 traffic containing a different destination UDP port.
8. Observe the packets transmitted by the DUT on G2.

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

9. Configure the DUT to deny all traffic containing a destination TCP port range on the interface connected to G1.
10. From G1 to G2, transmit IPv6 and IPv4 traffic containing the destination TCP port configured in the previous step.
11. From G1 to G2, transmit IPv6 and IPv4 traffic containing a different destination TCP port.
12. Observe the packets transmitted by the DUT on G2.

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

13. Configure the DUT to deny all traffic containing a source TCP port range on the interface connected to G1.

14. From G1 to G2, transmit IPv6 and IPv4 traffic containing the destination TCP port configured in the previous step.
15. From G1 to G2, transmit IPv6 and IPv4 traffic containing a different destination TCP port.
16. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Parts A and B, the traffic transmitted from denied UDP port on G1 should not be forwarded by the DUT nor observed on G2. The traffic transmitted from the other UDP ports at G1 should be forwarded by the DUT and observed on G2.
- In Parts C and D, the traffic transmitted from denied TCP port on G1 should not be forwarded by the DUT nor observed on G2. The traffic transmitted from the other TCP ports at G1 should be forwarded by the DUT and observed on G2.

Possible Problems: None.

Test FIR.2.3: IPv4 and IPv6 Functionality, Different Policy

Purpose: To verify that a firewall can block a different services with IPv4 and IPv6.

References: IP
TCP
UDP
IPv6-SPEC

Resource Requirements:

- Monitor to capture packets

Last Modification: February 23, 2004

Discussion: Basic IPv4 functionality includes the ability to accept and deny source and destination address pairs on an IPv4 network.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Deny all traffic with a specific UDP Destination Port

1. Configure the DUT to deny all traffic containing a destination UDP port for IPv4 on the interface connected to G1.
2. Configure the DUT to deny all traffic containing a destination TCP port for IPv6 on the interface connected to G1
3. From G1 to G2, transmit IPv4 traffic containing the destination UDP port configured in Step 1.
4. From G1 to G2, transmit IPv4 traffic containing the destination TCP port configured in Step 2.
5. From G1 to G2, transmit IPv6 and IPv4 traffic containing a different destination UDP and TCP ports and addresses than described in Steps 4 and 5.
6. Observe the packets transmitted by the DUT on G2.

Part B: Deny all traffic with a specific UDP Source Port

7. Configure the DUT to deny all traffic containing a source UDP port for IPv4 on the interface connected to G1.
8. Configure the DUT to deny all traffic containing a source TCP port for IPv6 on the interface connected to G1
9. From G1 to G2, transmit IPv4 traffic containing the source UDP port configured in Step 7.
10. From G1 to G2, transmit IPv4 traffic containing the source TCP port configured in Step 8.
11. From G1 to G2, transmit IPv6 and IPv4 traffic containing a different destination UDP and TCP port ranges and addresses than described in Steps 10 and 11.
12. Observe the packets transmitted by the DUT on G2.

Part C: Deny all traffic with a specific UDP Source Port

13. Configure the DUT to accept all traffic containing source UDP port X for IPv4 on the interface connected to G1. Configure the DUT to deny all other IPv4 UDP traffic on the interface connected to G1.
14. Configure the DUT to accept all traffic containing source TCP port X for IPv4 on the interface connected to G1. Configure the DUT to deny all other IPv4 TCP traffic on the interface connected to G1.
15. Configure the DUT to accept all ICMP Echo Request messages for IPv4 on the interface connected to G1. Configure the DUT to deny all other ICMP messages for IPv4 on the interface connected to G1.
16. Configure the DUT to deny all IPv6 traffic on the interface connected to G1.
17. From G1 to G2, transmit IPv4 and IPv6 traffic containing
 - a. The source TCP port configured in Step 13.
 - b. The source TCP port configured in Step 14.
 - c. ICMP message traffic.
18. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Parts A and B, the traffic transmitted from denied TCP or UDP port on G1 should not be forwarded by the DUT nor observed on G2. The traffic transmitted from the other TCP or UDP ports at G1 should be forwarded by the DUT and observed on G2.
- In Part C, the IPv4 traffic transmitted from the accept policy (TCP or UDP ports, or ICMP messages other than Echo Request messages) from G1 should be forwarded by the DUT and observed on G2. The IPv4 traffic transmitted from the other TCP or UDP ports or ICMP Echo Request messages should not be forwarded by the DUT nor observed on G2. IPv6 traffic should not be forwarded by the DUT.

Possible Problems: None.

GROUP 3: Logging

Scope:

These tests are designed to verify the functionality of the firewall logging function

Overview:

The logging function in firewalls is essential for debugging network issues and determining sources of attacks and intrusion.

Test FIR.3.1: Logging with IPv6 Functionality

Purpose: To verify that a firewall can properly log function when enabled with an IPv6 rule.

References: IP
TCP
UDP

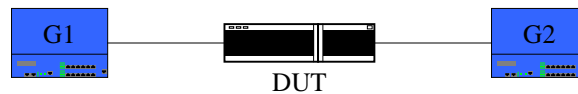
Resource Requirements:

- Monitor to capture packets

Last Modification: February 23, 2004

Discussion: Basic IPv4 functionality includes the ability to accept and deny source and destination address pairs on an IPv4 network.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Multiple Rules, Logging Enabled with TCP

1. Configure the DUT to deny all traffic on the interface connected to G1 that fits the following definition. Enable logging for this definition.
 - Globally defined source and destination IPv6 address pair “X”.
 - A specific TCP port range for source and destination ports
2. Configure the DUT to deny all traffic on the interface connected to G1 that fits the following definition. Disable logging for this definition.
 - A globally defined source and destination IPv6 address pair “Y”.
 - A specific UDP port range for source and destination ports
3. From G1 to G2, transmit a traffic profile that fits the definitions described in steps 1 and 2.
4. From G1 to G2, transmit a traffic profile that does not fit the definitions described in steps 1 and 2.
5. Observe the packets transmitted by the DUT on G2.

Part B: Multiple Rules, Logging Enabled with ICMPv6

6. Configure the DUT to deny all traffic on the interface connected to G1 that fits the following definition. Disable logging for this definition.
 - A globally defined source and destination IPv6 address pair “X”.
 - A specific TCP port range for source and destination ports
7. Configure the DUT to deny all traffic on the interface connected to G1 that fits the following definition. Enable logging for this definition.
 - A globally defined source and destination IPv6 address pair “Y”.
 - ICMPv6 Echo Request messages for source and destination ports
8. From G1 to G2, transmit a traffic profile that fits the definitions described in steps 6 and 7.

9. From G1 to G2, transmit a traffic profile that does not fit the definitions described in steps 1 and 2.
10. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Part A, logging should only report TCP traffic activity. The [source, destination address pairs “X” and “Y” and TCP/UDP ports] traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2. All background traffic transmitted from G1 should be forwarded by the DUT and observed on G2. Denials based on “X” should be logged. Denials based on “Y” should not be logged.
- In Part B, logging should only report ICMPv6 traffic activity. The [source, destination address pair “Y” and TCP or ICMPv6 Echo Request] traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2. All background traffic transmitted from G1 should be forwarded by the DUT and observed on G2. Denials based on “X” should not be logged. Denials based on “Y” should be logged.

Possible Problems: None.

Test FIR.3.2: Logging with IPv4 and IPv6 Functionality

Purpose: To verify that a firewall can properly log function when enabled with a mixed IPv4 and IPv6 rule.

References: IP
TCP
UDP

Resource Requirements:

- Monitor to capture packets

Last Modification: February 23, 2004

Discussion: Basic IPv4 functionality includes the ability to accept and deny source and destination address pairs on an IPv4 network.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Multiple Rules, Logging Enabled with IPv4 ICMP

1. Configure the DUT to deny all traffic on the interface connected to G1 that fits the following definition. Enable logging for this definition.
 - A globally defined source and destination IPv4 address pair “X”.
 - ICMP Echo Request messages
2. Configure the DUT to deny all traffic on the interface connected to G1 that fits the following definition. Disable logging for this definition.
 - A globally defined source and destination IPv6 address pair “Y”.
 - ICMPv6 Echo Request messages
3. From G1, transmit a traffic profile that fits the definitions described in steps 1 and 2.
4. From G1, transmit a traffic profile that does not fit the definitions described in steps 1 and 2.
5. Observe the packets transmitted by the DUT on G2.

Part B: Multiple Rules, Logging Enabled with ICMPv6

6. Configure the DUT to deny all traffic on the interface connected to G1 that fits the following definition. Disable logging for this definition.
 - A globally defined source and destination IPv4 address pair “X”.
 - ICMP Echo Request messages
7. Configure the DUT to deny all traffic on the interface connected to G1 that fits the following definition. Enable logging for this definition.
 - A globally defined source and destination IPv6 address pair “Y”.
 - ICMPv6 Echo Request messages
8. From G1, transmit a traffic profile that fits the definitions described in steps 1 and 2.
9. From G1, transmit a traffic profile that does not fit the definitions described in steps 1 and 2.

10. Observe the packets transmitted by the DUT on G2.

Observable Results:

- In Part A, logging should report IPv4 ICMP traffic activity. The [source, destination address pairs and ICMP/ICMPv6 Echo Request] traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2. All background traffic transmitted from G1 should be forwarded by the DUT and observed on G2.
- In Part B, logging should report ICMPv6 traffic activity. The [source, destination address pairs and ICMP/ICMPv6 Echo Request] traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2. All background traffic transmitted from G1 should be forwarded by the DUT and observed on G2.

Possible Problems: None.

GROUP 4: Stateful Inspection

Scope:

These tests are designed to verify the functionality of the firewall inspection of connection state.

Overview:

Connection tracking between nodes across the firewall boundary is essential for high resolution security operations.

Test FIR.4.1: IPv6 TCP State

Purpose: To verify that a firewall properly accepts and denies IPv6 TCP traffic based on state.

References: TCP

Resource Requirements:

- Monitor to capture packets

Last Modification: February 20, 2004

Discussion: The TCP state machine (Annex B of [TCP]) can be observed by the Firewall. The firewall can block IPv6 TCP traffic that is received out of state.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Proper Initialization Procedure

1. Configure the DUT to monitor TCP state on the interface connected to G1.
2. From G1, transmit an IPv6 TCP SYN.
3. From G2, transmit an IPv6 TCP SYN-ACK.
4. From G1, transmit an IPv6 TCP ACK.
5. From G1 and G2, transmit traffic containing the proper source and destination TCP ports.
6. Observe the packets transmitted by the DUT on G1 and G2.

Part B: Reception of SYN-ACK before SYN

7. Configure the DUT to monitor TCP state on the interface connected to G1.
8. From G1, transmit an IPv6 TCP SYN-ACK.
9. From G1 and G2, transmit traffic containing the proper source and destination TCP ports.
10. Observe the packets transmitted by the DUT on G1 and G2.

Part C: Reception of ACK before SYN or SYN-ACK

11. Configure the DUT to monitor TCP state on the interface connected to G1.
12. From G1, transmit an IPv6 TCP ACK.
13. From G1 and G2, transmit traffic containing the proper source and destination TCP ports.
14. Observe the packets transmitted by the DUT on G1 and G2.

Part D: TCP Cleanup Procedure

15. Configure the DUT to monitor TCP state on the interface connected to G1.
16. From G1, properly initialize a TCP session and emulate the client on G2.
17. From G1 and G2, transmit traffic containing the proper source and destination TCP ports.
18. From G1, properly close the TCP session.
19. From G1, transmit out of state TCP control messages (SYN-ACK, ACK, URG, PSH, FIN, FIN-ACK, RST).
20. From G1 transmit traffic containing the proper source and destination TCP ports.
21. Observe the packets transmitted by the DUT on G1 and G2.

Observable Results:

- In Part A, the traffic transmitted from G1 should be forwarded by the DUT and observed on G2.
- In Parts B and C, the traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2.
- In Part D, the TCP Connection should be opened and the traffic should be properly forwarded to G2 by the DUT. Once the TCP connection is closed the out of state control traffic and data traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2.

Possible Problems: None.

Test FIR.4.2: Mixed IPv4 and IPv6 TCP State

Purpose: To verify that a firewall properly accepts and denies TCP traffic based on state in the presence of mixed IPv4 and IPv6 traffic.

References: TCP

Resource Requirements:

- Monitor to capture packets

Last Modification: February 23, 2004

Discussion: The TCP state machine (Annex B of [TCP]) can be observed by the Firewall. The firewall can block TCP traffic that is received out of state. The firewall must maintain separate TCP state for both IPv4 and IPv6.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Proper Initialization Procedure

1. Configure the DUT to monitor TCP state on the interface connected to G1. In the exchange below, ensure to use the same TCP port numbers.
2. From G1, transmit TCP SYN packets with proper IPv4 and IPv6 headers.
3. From G2, transmit TCP SYN-ACK packets with proper IPv4 and IPv6 headers (in reply to step 2 transmissions).
4. From G1, transmit TCP ACK packets with proper IPv4 and IPv6 headers (in reply to step 3 transmissions).
5. From G1 and G2, transmit IPv4 and IPv6 traffic containing the proper source and destination TCP ports.
6. Observe the packets transmitted by the DUT on G1 and G2.

Part B: IPv6 Proper State, IPv4 Improper State

7. Configure the DUT to monitor TCP state on the interface connected to G1. In the exchange below, ensure to use the same TCP port numbers.
8. From G1, transmit an IPv6 TCP SYN.
9. From G2, transmit an IPv6 TCP SYN-ACK (in reply to step 8 transmission).
10. From G1, transmit an IPv6 TCP ACK (in reply to step 9 transmission).
11. From G1, transmit an IPv4 TCP SYN-ACK.
12. From G1 and G2, transmit IPv4 and IPv6 traffic containing the proper source and destination TCP ports.
13. Observe the packets transmitted by the DUT on G1 and G2.

Part C: IPv4 Proper State, IPv6 Improper State

14. Configure the DUT to monitor TCP state on the interface connected to G1. In the exchange below, ensure to use the same TCP port numbers.
15. From G1, transmit an IPv4 TCP SYN.
16. From G2, transmit an IPv4 TCP SYN-ACK (in reply to step 15 transmission).
17. From G1, transmit an IPv4 TCP ACK (in reply to step 16 transmission).

18. From G1, transmit an IPv6 TCP SYN-ACK.
19. From G1 and G2, transmit IPv4 and IPv6 traffic containing the proper source and destination TCP ports.
20. Observe the packets transmitted by the DUT on G1 and G2.

Observable Results:

- In Part A, the IPv4 and IPv6 traffic transmitted from G1 should be forwarded by the DUT and observed on G2.
- In Part B, the IPv6 traffic transmitted from G1 should be forwarded by the DUT and observed on G2. The IPv4 traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2.
- In Part C, the IPv4 traffic transmitted from G1 should be forwarded by the DUT and observed on G2. The IPv6 traffic transmitted from G1 should not be forwarded by the DUT nor observed on G2.

Possible Problems: None.

Test FIR.4.3: FTP State Inspection

Purpose: To verify that a firewall properly accepts and denies FTP traffic based on state in the presence of mixed IPv4 and IPv6 traffic.

References: TCP, FTP

Resource Requirements:

- Monitor to capture packets

Last Modification: February 28, 2004

Discussion: The TCP state machine (Annex B of [TCP]) can be observed by the Firewall. The firewall can block TCP traffic that is received out of state. The firewall must maintain separate TCP state for both IPv4 and IPv6.

Test Setup: Connect Devices as shown.



Procedure:

Part A: FTP connection in active mode

1. Configure the DUT to accept FTP traffic and deny all other traffic on the interface connected to G1.
2. From G1, initialize an active FTP connection to a server that is emulated on G2 and transfer a file.
3. Allow the Observe the packets transmitted by the DUT on G1 and G2.

Part B: FTP connection in passive mode

4. Configure the DUT to accept FTP traffic and deny all other traffic on the interface connected to G1.
5. From G1, initialize an active FTP connection to a server that is emulated on G2 and transfer a file.
6. Allow the Observe the packets transmitted by the DUT on G1 and G2.

Observable Results:

- In Part A, the file should properly be transferred from G1 to G2.
- In Part B, the connection in active mode should be denied. The connection in passive mode should properly transfer the file between G1 and G2.

Possible Problems: None.

Test FIR.4.4: ICMP State Inspection

Purpose: To verify that a firewall properly forwards ICMP reply messages based on state.

References: TCP, FTP

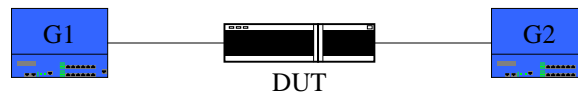
Resource Requirements:

- Monitor to capture packets

Last Modification: February 28, 2004

Discussion: ICMP alerts a host attempting to originate a connection that does not exist through a destination unreachable message. As fragmentation is done at the host in IPv6, it is necessary that hosts can receive Packet Too Big messages. Time Exceeded and Parameter Problem messages are also important error messages for a host to receive.

Test Setup: Connect Devices as shown.



Procedure:

Part A: ICMPv6 Destination Unreachable Message

1. Configure the DUT to monitor ICMPv6 traffic and deny messages that are out of state on the interface connected to G1.
2. From G1, transmit an ICMPv6 Destination Unreachable message.
3. From G2, initialize an FTP or Telnet connection to a server that is emulated on G1.
4. From G1, transmit an ICMPv6 Destination Unreachable message.
5. Allow the Observe the packets transmitted by the DUT on G1 and G2.

Part B: ICMPv6 Packet Too Big Message

6. Configure the DUT to monitor ICMPv6 traffic and deny messages that are out of state on the interface connected to G1.
7. From G1, transmit an ICMPv6 Packet Too Big message.
8. From G2, initialize an FTP or Telnet connection to a server that is emulated on G1.
9. From G1, transmit an ICMPv6 Packet Too Big message.
10. Allow the Observe the packets transmitted by the DUT on G1 and G2.

Part C: ICMPv6 Time Exceeded Message

11. Configure the DUT to monitor ICMPv6 traffic and deny messages that are out of state on the interface connected to G1.
12. From G1, transmit an ICMPv6 Time Exceeded message.
13. From G2, initialize an FTP or Telnet connection to a server that is emulated on G1.
14. From G1, transmit an ICMPv6 Time Exceeded message.
15. Allow the Observe the packets transmitted by the DUT on G1 and G2.

Part D: ICMPv6 Parameter Problem Message

16. Configure the DUT to monitor ICMPv6 traffic and deny messages that are out of state on the interface connected to G1.
17. From G1, transmit an ICMPv6 Time Exceeded message.

18. From G2, initialize an FTP or Telnet connection to a server that is emulated on G1.
19. From G1, transmit an ICMPv6 Time Exceeded message.
20. Allow the Observe the packets transmitted by the DUT on G1 and G2.

Part E: ICMPv6 Echo Reply Message

21. Configure the DUT to monitor ICMPv6 traffic and deny messages that are out of state on the interface connected to G1.
22. From G1, transmit an ICMPv6 Echo Reply message.
23. From G2, send an Echo Request to G1.
24. From G1, transmit an ICMPv6 Echo Reply message.
25. Allow the Observe the packets transmitted by the DUT on G1 and G2.

Observable Results:

- In all Parts, the first ICMP message should be denied. The second message should be forwarded by the DUT and received on G2.

Possible Problems: None.

Test FIR.4.5: UDP State Inspection

Purpose: To verify that a firewall properly forwards UDP DNS requests based on state.

References: TCP, FTP

Resource Requirements:

- Monitor to capture packets

Last Modification: February 28, 2004

Discussion: When a host makes a UDP DNS request, the DNS server must reply across the firewall. This test checks the functionality of this mechanism.

Test Setup: Connect Devices as shown.



Procedure:

Part A: DNS Query

1. Configure the DUT to monitor UDP traffic and deny messages that are out of state on the interface connected to G1.
2. From G1, transmit a UDP DNS reply message to G2.
3. From G2, transmit a UDP DNS query to a server that is emulated on G1.
4. From G1, transmit a UDP DNS reply message to G2.
5. Allow the Observe the packets transmitted by the DUT on G1 and G2.

Part B: DNS Query

6. Configure the DUT to monitor UDP traffic and deny messages that are out of state on the interface connected to G1.
7. From G1, transmit a UDP DNS reply message to G2.
8. From G2, transmit a UDP DNS query to a server that is emulated on G1.
9. From G1, transmit a UDP DNS reply message to G2.
10. Wait for a specific time to allow UDP state to expire on the firewall.
11. From G1, transmit a UDP DNS reply message to G2.
12. Allow the Observe the packets transmitted by the DUT on G1 and G2.

Part C: UDP State, destination UDP port.

13. Configure the DUT to monitor UDP state on the interface connected to G1.
14. From G1, transmit a UDP DNS request message to G2.
15. From G2, transmit a UDP DNS reply with only proper source UDP port (in reply to step 2 transmission).
16. Observe the packets transmitted by the DUT on G1 and G2.

Part D: UDP State, source UDP port.

17. Configure the DUT to monitor UDP state on the interface connected to G1.
18. From G1, transmit a UDP DNS request message to G2
19. From G2, transmit a UDP DNS reply with only proper destination UDP port (in reply to step 2 transmission).

20. Observe the packets transmitted by the DUT on G1 and G2.

Part E: UDP State, source IP address.

21. Configure the DUT to monitor UDP state on the interface connected to G1.

22. From G1, transmit a UDP DNS request message to G2.

23. From G2, transmit a UDP DNS reply with proper source and destination UDP port (in reply to step 2 transmission) to a different source IP address.

24. Observe the packets transmitted by the DUT on G1 and G2.

Part F: UDP State, destination IP address

25. Configure the DUT to monitor UDP state on the interface connected to G1.

26. From G1, transmit a UDP DNS request message to G2.

27. From G2, transmit UDP DNS reply with proper source and destination UDP port (in reply to step 2 transmission) from a different IP address.

28. Observe the packets transmitted by the DUT on G1 and G2.

Observable Results:

- In Part A, the first DNS reply should be denied. The second DNS reply message should be forwarded by the DUT and received on G2.
- In Part B, the first and third DNS replies should be denied. The second DNS reply message should be forwarded by the DUT and received on G2.
- In Parts C, D, E and F, the traffic transmitted from G2 should not be forwarded by the DUT and not observed on G1.

Possible Problems: None.

GROUP 5: Advanced Filtering

Scope:

These tests are designed to verify the functionality of the firewall in a multiprotocol environment.

Overview:

Connection tracking between nodes across the firewall boundary is essential for high resolution security. Simulating realistic operations is necessary to create a better indicator of the firewall operation.

Test FIR.5.1: Multiprotocol Filtering

Purpose: To verify that a firewall properly accepts and denies various application traffic based on state in the presence of mixed IPv4 and IPv6 traffic.

References: TCP, UDP

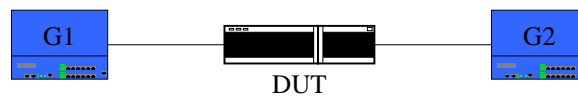
Resource Requirements:

- Monitor to capture packets

Last Modification: February 28, 2004

Discussion: To test firewall filters in a realistic setting (various UDP and TCP ports and IP addresses) application traffic is sent that “cycles” through, or randomizes, addresses/ports from address ranges. This tests the firewall's ability to block the “bad” (filtered) traffic whilst passing all the “good” traffic, using a very large range of addresses/ports, over a period of time.

Test Setup: Connect Devices as shown.



Procedure:

Part A: Filter of Application Traffic

1. Configure the DUT to accept application traffic from HTTP, ICMPv6, ICMP for IPv4 and a specific TCP ports associated with a set of (source, destination) IPv4 and IPv6 address pairs.
2. From G1, transmit IPv4 and IPv6 traffic containing the proper source and destination TCP ports, HTTP application traffic and cycling through other potential applications.
3. Observe the packets transmitted by the DUT on G1 and G2.

Part B: Dynamic Firewall Configuration

4. Configure the DUT to accept application traffic from HTTP, ICMPv6, ICMP for IPv4 and a specific TCP ports associated with a set of (source, destination) IPv4 and IPv6 address pairs.
5. From G1, transmit IPv4 and IPv6 traffic containing the proper source and destination TCP ports, HTTP application traffic and cycling through other potential applications. This transmission should be continued through Step 6.
6. While continuing to transmit (as documented in step 5), configure the DUT to accept all traffic for protocol X (FTP, for example).
7. Observe the packets transmitted by the DUT on G1 and G2.

Observable Results:

- In Part A, only the IPv4 and IPv6 traffic fitting the policy description should be forwarded by the DUT and observed on G2.
- In Part B, only the IPv4 and IPv6 traffic fitting the policy description should be forwarded by the DUT and observed on G2. When the DUT is configured in Step 6, the DUT should also forward traffic from protocol X.

Possible Problems: None.