Universität Potsdam
Mathematisch-Naturwissenschaftliche Fakultät

IPv6 Firewall Protocol Tests

Oliver Eggert, Simon Kiertscher

Outline

- Motivation
- Firewall Tests
  - e.g. Overlapping IPv6 Fragments
  - PadN Covert Channel
- FT6 (Firewalltester for IPv6) - the new tool
- Test Setup & Test Results
  - Cisco ASA5510
  - IPTables
  - Juniper J2320
  - Checkpoint 2210 Appliance

Motivation

- What are current RFC requirements for firewalls?
- How can you test your firewall in an easy way?
- Can “IPv6 Ready” hardware keep its promise?

Firewall Tests

ICMPv6 filtering

- ICMPv6 is like ICMP for sharing information or error messages
- ICMPv6 also for Neighbor Discovery Protocol (NDP)
- According to RFC 4890 we made a list of packets which
  - should be dropped
  - are optional
  - must not be dropped

ICMPv6 filtering

- Non-Filtered messages according to RFC4890

ICMPv6 Type	Description
1	Destination Unreachable
2	Packet Too Big
3, Code 0	Time Exceeded*
4, Code 1 and 2	Parameter Problem
128, 129	Echo Request/Reply

*Marc Heuse recommends to drop it (c't article)

ICMPv6 filtering

- Optional Filter List

ICMPv6 Type	Description
3, Code 1	Time Exceeded
4, Code 0	Parameter Problem
144, 145, 146, 147	IPv6 Mobility
150	Seamoby Experimental
5-99, 102-126	Unallocated Error Messages
154-199, 202-254	Unallocated Informational Messages

- The rest should be filtered!

Routing Header (RH)

- Especially RH0 (deprecated since Dec 2007 according to RFC 5095)

  → treat it like an unknown RH

- Mobility Routing Header (RH 2) - RFC 3775

RH Type	Segments left field	Behavior
RH 0	≠ 0	Drop
RH 0	= 0	Forward (ignore header)
RH 2	≠ 1	Drop
RH 2	= 1	Forward
RH 200	≠ 0	Drop
RH 200	= 0	Forward (ignore header)

IPv6 Header Chain Inspection

- There are 3 basic rules (RFC2460) that govern the order and occurrence of extension headers (header chain)
  1. Destination Options (DSTOPT) header at most twice (once before a Routing header and once before the upper-layer header)
  2. All other extension headers should occur at most once
  3. The Hop-by-Hop (HBH) Options header is restricted to appear only immediately after the base IPv6 header

IPv6 Header Chain Inspection

- We test 7 different Header Chains

Header Chain	Validity
DSTOPT	Valid
DSTOPT, DSTOPT	Invalid
DSTOPT, RH, DSTOPT	Valid
HBH	Valid
HBH, HBH	Invalid
DSTOPT, HBH	Invalid
HBH, DSTOPT, RH, HBH	Invalid

Overlapping IPv6 Fragments

- Overlapping IPv6 fragments are very dangerous if processed
- RFC 5722 (Handling of Overlapping IPv6 Fragments) describes inter alia a fragmentation attack and expected node behavior

Overlapping IPv6 Fragments

Fragment appearance	Behavior
Fragmented packet without overlap	Forward
Overlapping, rewriting the upper layer protocol header	Drop
Overlapping, rewriting the payload	Drop

Overlapping IPv6 Fragments

372	25.285318	2001:2:1::b	2001:2:2::b	IPv6	IPv6 fragment (nxt=UDP (17) off=0 id=0x532fbc21)
373	25.349511	2001:2:1::b	2001:2:2::b	UDP	Source port: krb524 Destination port: ssh
374	25.428852	2001:2:1::b	2001:2:2::b	IPv6	IPv6 fragment (nxt=UDP (17) off=0 id=0x21c24a47)
375	25.490046	2001:2:1::b	2001:2:2::b	UDP	Source port: krb524 Destination port: http
376	25.523564	2001:2:1::b	2001:2:2::b	TCP	[TCP segment of a reassembled PDU]
379	25.524289	2001:2:1::b	2001:2:2::b	TCP	39296 > http [ACK] Seq=81 Ack=27037 Win=62976 Len=0 TSval=154793 TSecr=127430
381	25.525069	2001:2:1::b	2001:2:2::b	TCP	39296 > http [ACK] Seq=81 Ack=27050 Win=62976 Len=0 TSval=154793 TSecr=127430
383	26.526692	2001:2:1::b	2001:2:2::b	TCP	39296 > http [ACK] Seq=81 Ack=27122 Win=62976 Len=0 TSval=155043 TSecr=127681
385	26.527111	2001:2:1::b	2001:2:2::b	TCP	39296 > http [ACK] Seq=81 Ack=27288 Win=64512 Len=0 TSval=155043 TSecr=127681

```
⊟ Internet Protocol Version 6, Src: 2001:2:1::b (2001:2:1::b), Dst: 2001:2:2::b (2001:2:2::b)
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 160
    Next header: IPv6 fragment (44)
    Hop limit: 64
    Source: 2001:2:1::b (2001:2:1::b)
    Destination: 2001:2:2::b (2001:2:2::b)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊟ Fragmentation Header
      Next header: UDP (17)
      Reserved octet: 0x0000
      0000 0000 0000 0... = Offset: 0 (0x0000)
      .... .... .... .00. = Reserved bits: 0 (0x0000)
      .... .... .... ...1 = More Fragment: Yes
      Identification: 0x532fbc21
⊟ Data (152 bytes)
    Data: 115c005000986acd6161616161616161616161616161616161...
    [Length: 152]
```

```
0000  00 10 18 4f a9 48 18 03  73 c1 e7 3c 86 dd 60 00   ...O.H.. s..<..`.
0010  00 00 00 a0 2c 40 20 01  00 02 00 01 00 00 00 00   ....,@ . ........
0020  00 00 00 00 00 0b 20 01  00 02 00 02 00 00 00 00   ...... . ........
0030  00 00 00 00 00 0b 11 00  00 01 53 2f bc 21 11 5c   ........ ..S/.!.\
0040  00 50 00 98 6a cd 61 61  61 61 61 61 61 61 61 61   .P..j.aa aaaaaaaa
0050  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0060  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0070  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0080  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0090  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
00a0  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
00b0  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
00c0  61 61 61 61 61 61 58 58  58 58 58 58 54 65 73 74   aaaaaaXX XXXXTest
00d0  34 53 74 65 70 32                                  4Step2
```

0x50 = 80 = http

Overlapping IPv6 Fragments

```
372 25.285318 2001:2:1::b 2001:2:2::b IPv6    IPv6 fragment (nxt=UDP (17) off=0 id=0x532fbc21)
373 25.349511 2001:2:1::b 2001:2:2::b UDP     Source port: krb524  Destination port: ssh
374 25.428852 2001:2:1::b 2001:2:2::b IPv6    IPv6 fragment (nxt=UDP (17) off=0 id=0x21c24a47)
375 25.490046 2001:2:1::b 2001:2:2::b UDP     Source port: krb524  Destination port: http
376 25.523564 2001:2:1::b 2001:2:2::b TCP     [TCP segment of a reassembled PDU]
379 25.524289 2001:2:1::b 2001:2:2::b TCP     39296 > http [ACK] Seq=81 Ack=27037 Win=62976 Len=0 TSval=154793 TSecr=127430
381 25.525069 2001:2:1::b 2001:2:2::b TCP     39296 > http [ACK] Seq=81 Ack=27050 Win=62976 Len=0 TSval=154793 TSecr=127430
383 26.526692 2001:2:1::b 2001:2:2::b TCP     39296 > http [ACK] Seq=81 Ack=27122 Win=62976 Len=0 TSval=155043 TSecr=127681
385 26.527111 2001:2:1::b 2001:2:2::b TCP     39296 > http [ACK] Seq=81 Ack=27288 Win=64512 Len=0 TSval=155043 TSecr=127681
386 26.527275 2001:2:1::b 2001:2:2::b TCP     [TCP segment of a reassembled PDU]
```

```
    Next header: IPv6 fragment (44)
    Hop limit: 64
    Source: 2001:2:1::b (2001:2:1::b)
    Destination: 2001:2:2::b (2001:2:2::b)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊟ Fragmentation Header
      Next header: UDP (17)
      Reserved octet: 0x0000
      0000 0000 0000 0... = Offset: 0 (0x0000)
      .... .... .... .00. = Reserved bits: 0 (0x0000)
      .... .... .... ...0 = More Fragment: No
      Identification: 0x532fbc21
⊟ User Datagram Protocol, Src Port: krb524 (4444), Dst Port: ssh (22)
    Source port: krb524 (4444)
    Destination port: ssh (22)
    Length: 152
  ⊞ Checksum: 0x6b07 [validation disabled]
⊟ Data (144 bytes)
    Data: 6161616161616161616161616161616161616161616161616161...
    [Length: 144]
```

```
0000  00 10 18 4f a9 48 18 03  73 c1 e7 3c 86 dd 60 00   ...O.H.. s..<..`.
0010  00 00 00 a0 2c 40 20 01  00 02 00 01 00 00 00 00   ....,@ . ........
0020  00 00 00 00 00 0b 20 01  00 02 00 02 00 00 00 00   ...... . ........
0030  00 00 00 00 00 0b 11 00  00 00 53 2f bc 21 11 5c   ........ ..S/.!.\
0040  00 16 00 98 6b 07 61 61  61 61 61 61 61 61 61 61   ....k.aa aaaaaaaa
0050  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0060  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0070  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0080  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0090  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
00a0  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
00b0  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
00c0  61 61 61 61 61 61 58 58  58 58 58 58 54 65 73 74   aaaaaaXX XXXXTest
00d0  34 53 74 65 70 32                                  4Step2
```

Tiny IPv6 Fragments

- A Tiny-Fragment is a fragmented IPv6 packet where the upper-layer-header is located in the second fragment
- Firewall has to inspect the second fragment

Tiny Fragment appearance	Behavior
Upper-layer-header with allowed port number	Forward
Upper-layer-header with forbidden port number	Drop

Tiny IPv6 Fragments

- According RFC 2460 a device has to discard a packed if not all fragments have arrived within 60 seconds after the arrival of the first fragment

Tiny Fragment appearance	Behavior
Send the last fragment after 60 seconds	Forward
Send the last fragment after 61 seconds	Drop

Excessive Hop-by-Hop and Destination Option Options

- As specified in RFC 4942, every option should occur at most once, except Pad1 and PadN
- All HBH options have to be processed on every node they pass

  excessive use → denial-of-service attack

Options Profile
Jumbo Payload, PadN, Jumbo Payload
Router Alert, Pad1, Router Alert
Quick Start, Tunnel Encapsulation Limit, PadN, Quick Start
RPL Option, PadN, RPL Option

PadN Covert Channel

- PadN and Pad1 are used to align options to a multiple of 8 bytes
- Required for DSTOPT and HBH header
- Valid payload of PadN must only contains zeroes
- What if not?

  → Abuse as a covert channel

Header	PadN	Behavior
HBH	Valid	Forward
HBH	Invalid	Drop
DSTOPT	Valid	Forward
DSTOPT	Invalid	Drop

Address Scopes

- A firewall must not forward packets with a wrong scope address
- The test contains a mix of different
  - Multicast addresses
  - Link-local addresses

Scope	Address range
Multicast	ff00::/32 - ffff::/32
Link-Local	fe80::/16 - febf::/16

FT6
the new tool

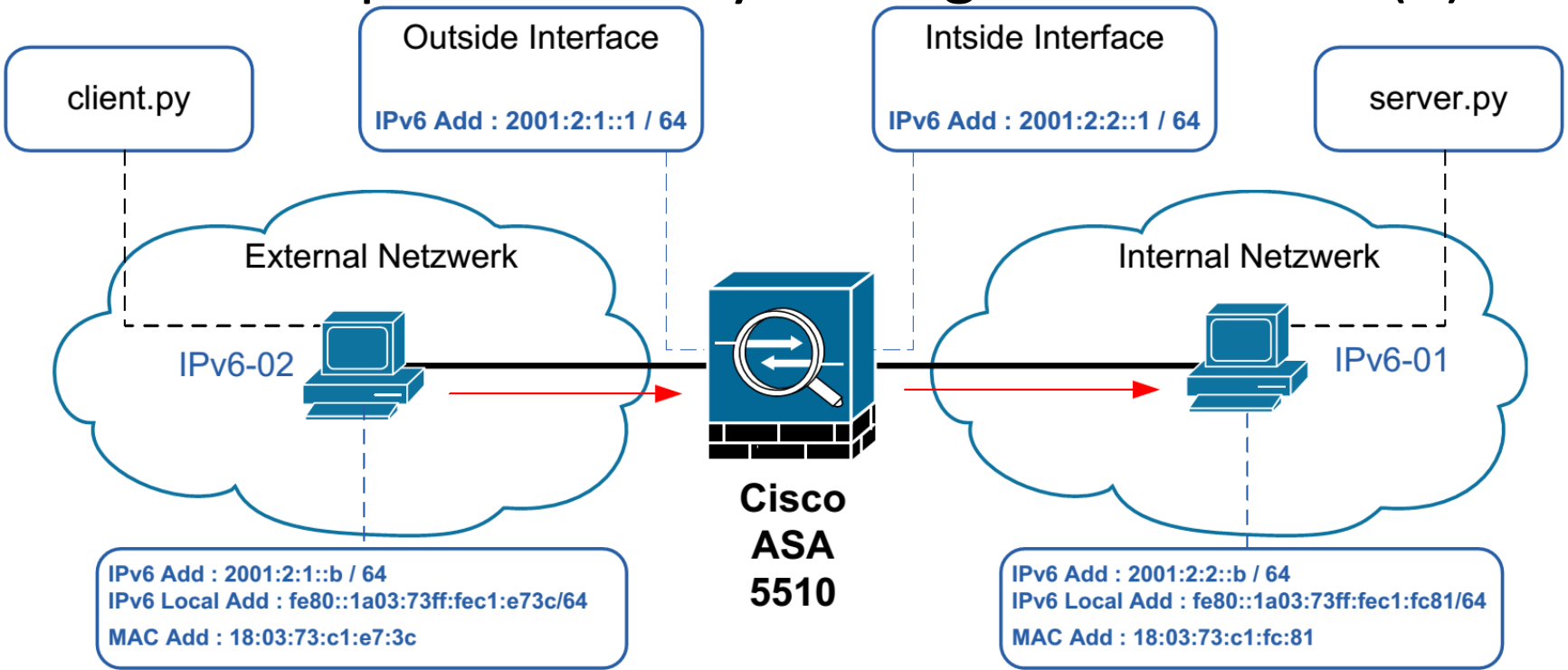
Test Setup & Test Results

Firewalls

1. Cisco ASA5510
2. IPTables
3. Juniper J2320
4. Checkpoint 2210 Appliance

Setup for Cisco ASA5510

- Linux grml 3.7.1-grml-amd64 Debian 3.7.9 + grml.1 x86_64 (uname -a)
- Cisco ASA Software Release Version 9.0(2) with Cisco Adaptive Security Manager Version 7.1(2).



Setup

- Webserver use case → only port 80 is open
- First test with basic setup (out-of-the-box)
- Second test, try to fulfill the requirements
  - Adding rules
  - Activating IPS

Test Results ASA5510

Test	Basic Rules	Advanced Rules / IPS
ICMPv6 Filtering	✗ -	✗
Routing Header	✗ -	“segments left” not filterable
Header Chain	✗	✗
Overlapping Fragments	✓	✓
Tiny IPv6 Fragments A	✓	✓
Tiny IPv6 Fragments B	✗	✗
Excessive HBH Options	✗ +	✗ +
PadN Covert Channel	✗ +	✗ +
Address Scope	✓	✓

- 100% Drop
+ 100% Forward

ICMPv6 Filtering

- Despite explicit forward rule
- Dropped:
  - Type 1, Destination Unreachable
  - Type 2, Packet Too Big
  - Type 3, Code 0, Time Exceeded
  - Type 4, Code 1 & 2, Parameter Problem

- answers to a former packed but no former package was received

Test Results ASA5510

Test	Basic Rules	Advanced Rules / IPS
ICMPv6 Filtering	✗ -	✗
Routing Header	✗ -	“segments left” not filterable
Header Chain	✗	✗
Overlapping Fragments	✓	✓
Tiny IPv6 Fragments A	✓	✓
Tiny IPv6 Fragments B	✗	✗
Excessive HBH Options	✗ +	✗ +
PadN Covert Channel	✗ +	✗ +
Address Scope	✓	✓

- 100% Drop
+ 100% Forward

Header Chain

- 2 of the 7 tests fail on default

	Header Chain	Validity	Behavior
✓	DSTOPT	Valid	Forwarded
✗	DSTOPT, DSTOPT	Invalid	Forwarded
✗	DSTOPT, RH, DSTOPT	Valid	Dropped
✓	HBH	Valid	Forwarded
✓	HBH, HBH	Invalid	Dropped
✓	DSTOPT, HBH	Invalid	Dropped
✓	HBH, DSTOPT, RH, HBH	Invalid	Dropped

Header Chain

- 1 of the 7 tests still fails after activation of an "Inspect Map"

	Header Chain	Validity	Behavior
✓	DSTOPT	Valid	Forwarded
✗	DSTOPT, DSTOPT	Invalid	Forwarded
✓	DSTOPT, RH, DSTOPT	Valid	Forwarded
✓	HBH	Valid	Forwarded
✓	HBH, HBH	Invalid	Dropped
✓	DSTOPT, HBH	Invalid	Dropped
✓	HBH, DSTOPT, RH, HBH	Invalid	Dropped

Test Results ASA5510

Test	Basic Rules	Advanced Rules / IPS
ICMPv6 Filtering	✗ -	✗
Routing Header	✗ -	“segments left” not filterable
Header Chain	✗	✗
Overlapping Fragments	✓	✓
Tiny IPv6 Fragments A	✓	✓
Tiny IPv6 Fragments B	✗	✗
Excessive HBH Options	✗ +	✗ +
PadN Covert Channel	✗ +	✗ +
Address Scope	✓	✓

- 100% Drop
+ 100% Forward

IPTables

Checkpoint

Test Results Checkpoint

- Checkpoint 2210 Appliance
- Version R75.10

Test Results Checkpoint

Test	Basic Rules	Advanced Rules / IPS
ICMPv6 Filtering	✗	✗
Routing Header	✗ -	“type” not filterable
Header Chain	✗ -	✗
Overlapping Fragments	Former bug in ft6, no fragments pass	
Tiny IPv6 Fragments A	✗ -	✗
Tiny IPv6 Fragments B	✗	✗
Excessive HBH Options	✓ -	✓
PadN Covert Channel	✗	✗
Address Scope	✓	✓

- 100% Drop
+ 100% Forward

ICMPv6 Filtering

- Forwarded only “Echo Request”
- answers to a former packed but no former package was received

Test Results Checkpoint

Test	Basic Rules	Advanced Rules / IPS
ICMPv6 Filtering	✗	✗
Routing Header	✗ -	“type” not filterable
Header Chain	✗ -	✗
Overlapping Fragments	Former bug in ft6, no fragments pass	
Tiny IPv6 Fragments A	✗ -	✗
Tiny IPv6 Fragments B	✗	✗
Excessive HBH Options	✓ -	✓
PadN Covert Channel	✗	✗
Address Scope	✓	✓

- 100% Drop
+ 100% Forward

Routing Header

- All extension headers are blocked by default
- If enabled, they will not be inspected

Test Results Checkpoint

Test	Basic Rules	Advanced Rules / IPS
ICMPv6 Filtering	✗	✗
Routing Header	✗ -	“type” not filterable
Header Chain	✗ -	✗
Overlapping Fragments	Former bug in ft6, no fragments pass	
Tiny IPv6 Fragments A	✗ -	✗
Tiny IPv6 Fragments B	✗	✗
Excessive HBH Options	✓ -	✓
PadN Covert Channel	✗	✗
Address Scope	✓	✓

- 100% Drop
+ 100% Forward

Excessive HBH

- If HBH/DSTOPT enabled, some are dropped, some are forwarded

Options Profile	HBH	DSTOPT
Jumbo Payload, PadN, Jumbo Payload	✔	✖
Router Alert, Pad1, Router Alert	✖	✖
Quick Start, Tunnel Encapsulation Limit, PadN, Quick Start	✖	✖
RPL Option, PadN, RPL Option	✔	✖

✔=Drop ✖=Forward

Test Results Checkpoint

Test	Basic Rules	Advanced Rules / IPS
ICMPv6 Filtering	✗	✗
Routing Header	✗	“type” not filterable
Header Chain	✗	✗
Overlapping Fragments	Former bug in ft6, no valid results	
Tiny IPv6 Fragments A	✗	✗
Tiny IPv6 Fragments B	✗	✗
Excessive HBH Options	✓	✓
PadN Covert Channel	✗	✗
Address Scope	✓	✓

Thank you for your attention! Questions?

Contact:

kiertscher@cs.uni-potsdam.de