ERNW
providing security.

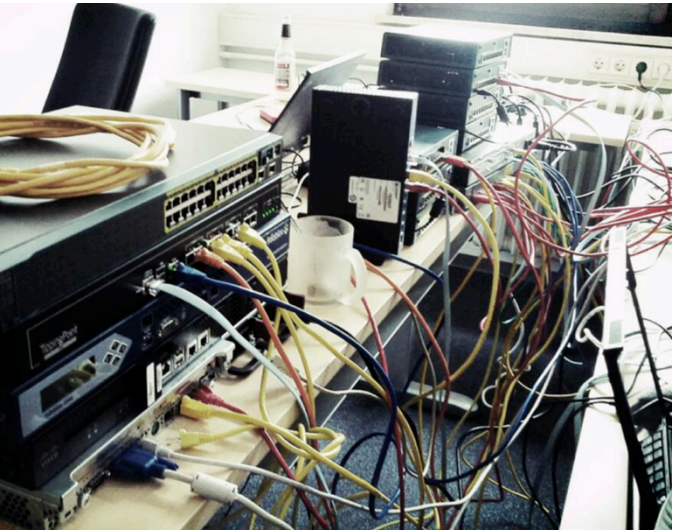
IPv6 Capabilities of Commercial Security Components

Enno Rey, erey@ernw.de
Christopher Werny, cwerny@ernw.de
Stefan Schwalb, sschwalb@ernw.de

Preliminary Notes

- We (as ERNW) do not sell any devices. We don't have any vendor affiliations.
  - We don't have any interest in promoting (or bashing) any vendor.
- We just want to contribute to an understanding "what works & what doesn't" as of _today_ (Jul2013).
  - "Contribute" means: this is by no means comprehensive as for vendor space or testing approaches.

Disclaimer II



- All this is *work in progress*.
  - Noted the v0_9 in the filename?
- We have a lab.
- At least one ERNW student continuously works on this stuff
  - Currently, that's Stefan ;-)
- Still, we're not where we would like to be.
- You can join us ;-)
  - "Open lab day" on Nov 07, together with Antonios Atlasis.

ERNW
providing security.

Disclaimer III

We love to share.

- We're hosting the beautiful **TROOPERS.de** Conference & Workshop series!
  - Next: March 17-21. 2014, Heidelberg, DE
  - More info: See last slide.

Electronic name badge of TROOPERS13.

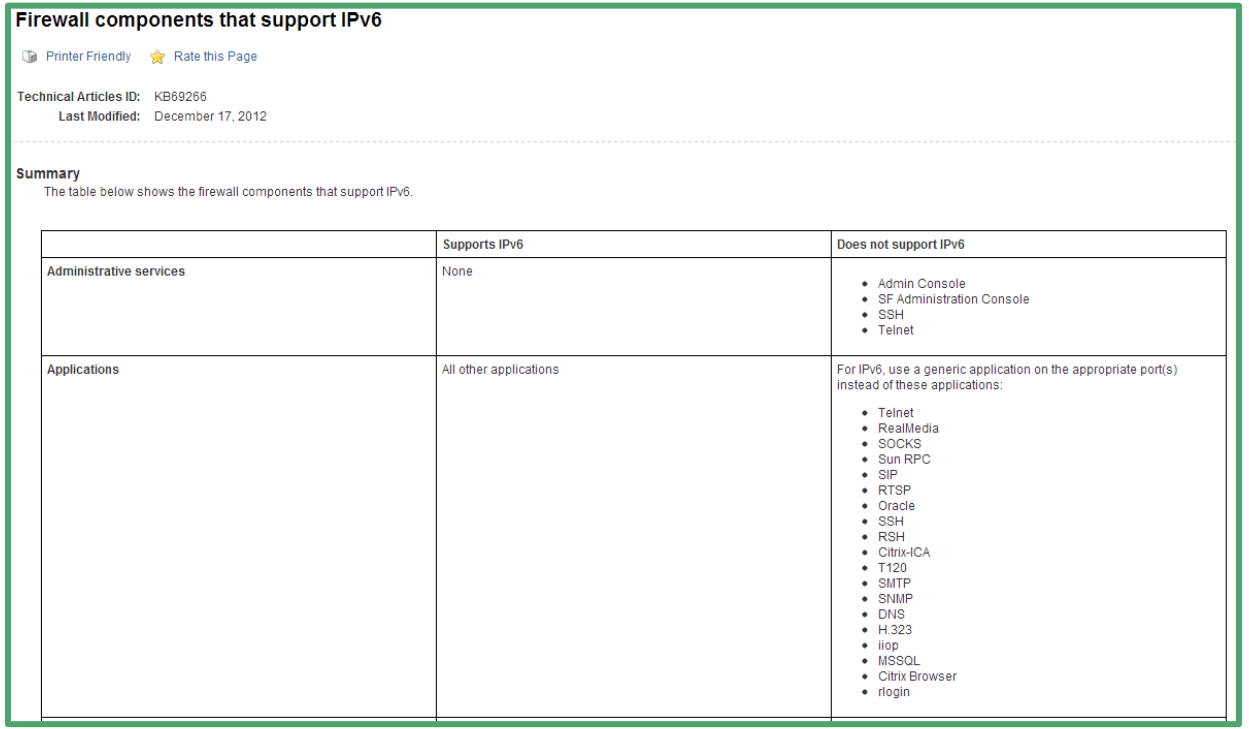
This could be your badge ;-)

- Visit our blog **INSINUATOR.NET** & join the discussion!

Related Work

- What Marc did for German c't magazine recently and subsequently discussed at the *IPv6 Kongress*, together w/ Fernando
  - http://www.si6networks.com/presentations/ipv6kongress/mhfg-ipv6-kongress-ipv6-security-assessment.pdf
- Johannes' great master thesis.
  - http://blog.webernetz.net/2013/05/06/ipv6-security-master-thesis/
  - Covered
    - Cisco ASA, Juniper SSG, Palo Alto PA
  - Strong focus on various attacks.

Problem Statement



Firewall components that support IPv6

Printer Friendly Rate this Page

Technical Articles ID: KB69266
Last Modified: December 17, 2012

Summary

The table below shows the firewall components that support IPv6.

	Supports IPv6	Does not support IPv6
Administrative services	None	• Admin Console • SF Administration Console • SSH • Telnet
Applications	All other applications	For IPv6, use a generic application on the appropriate port(s) instead of these applications: • Telnet • RealMedia • SOCKS • Sun RPC • SIP • RTSP • Oracle • SSH • RSH • Citrix-ICA • T120 • SMTP • SNMP • DNS • H.323 • iiop • MSSQL • Citrix Browser • rlogin

What You Might Be Interested In

Relevant Capabilities

- (Security) Feature Parity
- Robustness & Performance of IPv6 stack/general processing
- Support of IPv6 specific capabilities
  - Security related
    - Filtering of extension headers
    - Handling of fragments
  - Other
- “Compliance” w/ some “standard”

(Security) Feature Parity

Simply said:

- Does $COMPONENT provide the same security functions – and hence, ideally, the same security benefit – for IPv6 (network traffic) as for IPv4? e.g.
  - Simple filtering (stateless/stateful, L3+4)
  - Advanced filtering (OSI layer 4 & above)
  - High availability
  - VPN is a whole own story, we didn't look at that.
    - Isn't IPSec part of the IPv6 stack anyway? ;-)))

Robustness & Performance

- Does $COMPONENT provide the same processing/throughput for IPv6 (network traffic) as for IPv4?

Support of IPv6 Specific Capabilities

- Filtering of/based on
  - Extension headers
  - Extension headers + fragmentation
- Handling of fragmentation
  - In particular in the IPS space.
- “Support” of PMTUD on stateful devices
  - Can they associate ICMP too big with some TCP flow already in state table?

“Compliance” with $SOME_STANDARD

- Where $SOME_STANDARD could be
  - RIPE 554, sect. on “network security equipment”
  - DoD Profile for IPv6 Capable Products
    - http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_product_profile_v3.pdf
    - Is obsolete, was replaced by *UC APL*
    - https://aplits.disa.mil/processAPList.do?group=Security

To Answer these Questions You Could

- Look for publicly available sources & testing reports
  - Pay close attention to dates then!
  - Often not very detailed information available (see next slides)
- Ask the vendor
  - With a grain of salt, of course.
- Ask industry peers
  - We might help you with finding somebody who already has $COMPONENT in (IPv6) use.
- Mailing lists

Types of Tests Performed in Lab

Firewalls

- General capabilities
  - Can IPv6 be configured on $DEVICE?
- Throughput
  - In particular compared with IPv4.
  - Some application layer filtering testing (focus performance), e.g. FTP
- Some general “IPv6 attack resistance” testing
  - RA/NS flooding et.al.
- Management
  - Vendor specific (Check Point!)
  - Syslog, SNMP, NTP etc.

We Did Not

- Any of those semi-formal test methodologies
  - http://jitc.fhu.disa.mil/adv_ip/register/docs/ipv6v4_may09.pdf

Tests Performed

IPS

- General capabilities / function
- Some performance testing

Firewall Testbed

- Cisco ASA 5505
  - Running 8.4(5) Image
- CP Gaia R76 on HP DL360 G4
  - Released in February 2013 and claims to have extended IPv6 support ;)
- Juniper SSG-5
  - Running 6.3r13 Image

Throughput Testing

Some Details

- Step 1:
  - Generate rule set for IPv4 and IPv6 with approx. 1000 Rules each (to simulate production environments)
    - Fortunately, this could be realized with a short custom written script ;)
- Step 2:
  - IPv4 throughput testing (using Iperf 2.0.5) to establish a baseline
  - Place permitting rule on line 1, 500 and 1000 in the rule set
  - Run each test five times and calculate the average throughput

Throughput Testing

Some Details

- Step 3:
  - Repeat Step 2 with IPv6
    - Fortunately Iperf supports IPv6 since 2010 ;)
- Step 4:
  - Throughput test with FTP and application inspection enabled.
    - Copying a 1.5 Gigabyte file to the FTP Server
  - Both for IPv4 and IPv6

“IPv6 attack resistance”

- For these tests we used the THC-IPv6 tool suite (v2.1) and the IPv6 Toolkit from SI6 Networks
  - flood_router26 module to see how the firewalls coped with an excessive amount of RA’s
  - scan6 module to see how the firewalls behave when sending out a lot of neighbor solicitations for address resolution of non-existing addresses

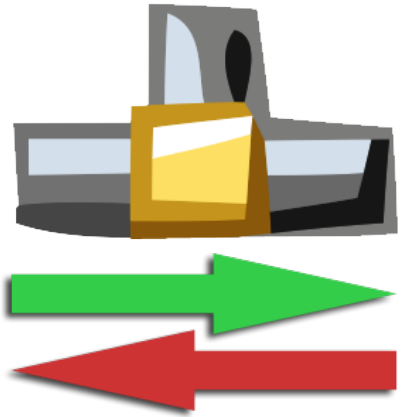
ASA-Results


cisco
Power
Status
Active
VPN
SSC
CISCO ASA 5505 SERIES
Adaptive Security Appliance

General Capabilities

- Well, the ASA supports filtering of IPv6 traffic for quite some time now.
- Alas, in regards to feature parity to IPv4, there are still some gaps to close ;)
  - (Most?) *inspects*.
  - Management stuff (NTP, SNMP, syslog)

IPv4 Throughput ASA



- According to Cisco
  - The ASA should be able to push 150Mbit traffic (bi-directional)
- We were able to push approx. 93 Mbit in one direction
  - Which is nearly the theoretical maximum for the Fast Ethernet interface the ASA has built-in.

```
C:\Program Files (x86)\iperf>iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[ ID] Interval       Transfer     Bandwidth
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53689
[  4]  0.0-60.0 sec   668 MBytes  93.4 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53690
[  4]  0.0-60.0 sec   668 MBytes  93.4 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53691
[  4]  0.0-60.0 sec   669 MBytes  93.4 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53692
[  4]  0.0-60.0 sec   668 MBytes  93.4 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53693
[  4]  0.0-60.0 sec   669 MBytes  93.5 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53694
[  4]  0.0-60.0 sec   669 MBytes  93.5 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53696
[  4]  0.0-60.0 sec   668 MBytes  93.3 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53697
[  4]  0.0-60.0 sec   669 MBytes  93.5 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53698
[  4]  0.0-60.0 sec   668 MBytes  93.4 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53699
[  4]  0.0-60.0 sec   669 MBytes  93.5 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53700
[  4]  0.0-60.0 sec   669 MBytes  93.4 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53701
[  4]  0.0-60.0 sec   669 MBytes  93.4 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53702
[  4]  0.0-60.0 sec   669 MBytes  93.5 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53703
[  4]  0.0-60.0 sec   669 MBytes  93.5 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 53704
[  4]  0.0-60.0 sec   669 MBytes  93.4 Mbits/sec

CPU utilization for 5 seconds = 45%; 1 minute: 41%; 5 minutes: 34%
```

ERNW
providing security.

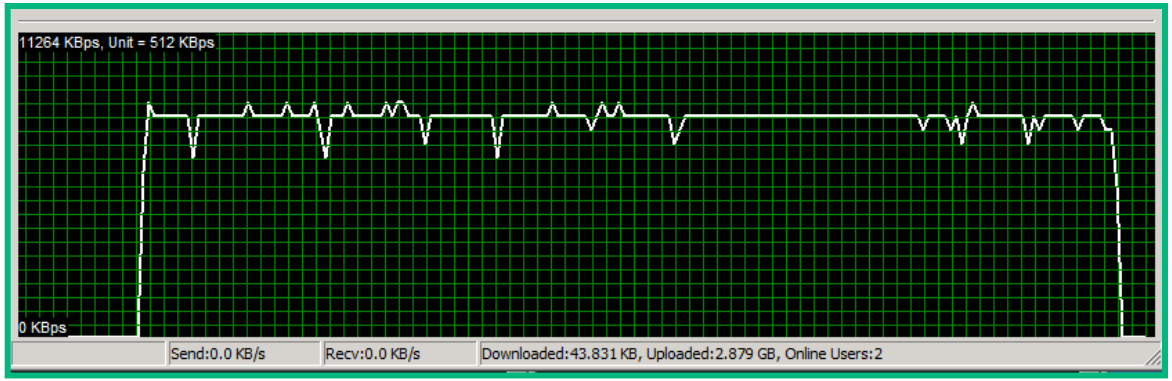
IPv4 Throughput ASA

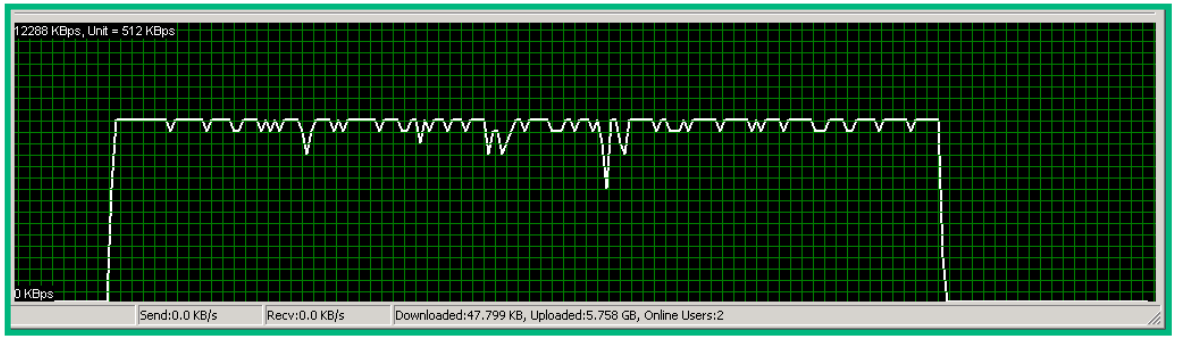
No worries, at the end you will see a comprehensive (graphical) summary/comparison ;)

```
C:\Program Files (x86)\iperf>iperf -s -V
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[ ID] Interval       Transfer     Bandwidth

[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59322
[  4]  0.0-60.0 sec   630 MBytes  88.0 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59324
[  4]  0.0-60.0 sec   660 MBytes  92.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59325
[  4]  0.0-60.0 sec   659 MBytes  92.1 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59326
[  4]  0.0-60.0 sec   660 MBytes  92.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59327
[  4]  0.0-60.0 sec   660 MBytes  92.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59328
[  4]  0.0-60.0 sec   659 MBytes  92.1 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59329
[  4]  0.0-60.0 sec   660 MBytes  92.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59330
[  4]  0.0-60.0 sec   660 MBytes  92.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59331
[  4]  0.0-60.0 sec   660 MBytes  92.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59332
[  4]  0.0-60.0 sec   660 MBytes  92.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59333
[  4]  0.0-60.0 sec   660 MBytes  92.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59334
[  4]  0.0-60.0 sec   659 MBytes  92.1 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59335
[  4]  0.0-60.0 sec   660 MBytes  92.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59336
[  4]  0.0-60.0 sec   659 MBytes  92.1 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:4dcc:67d3:5c1c:41dd port 59337
[  4]  0.0-60.0 sec   657 MBytes  91.8 Mbits/sec

CPU utilization for 5 seconds = 48%; 1 minute: 42%; 5 minutes: 38%
```

ERNW
providing security.

IPv6 Throughput ASA

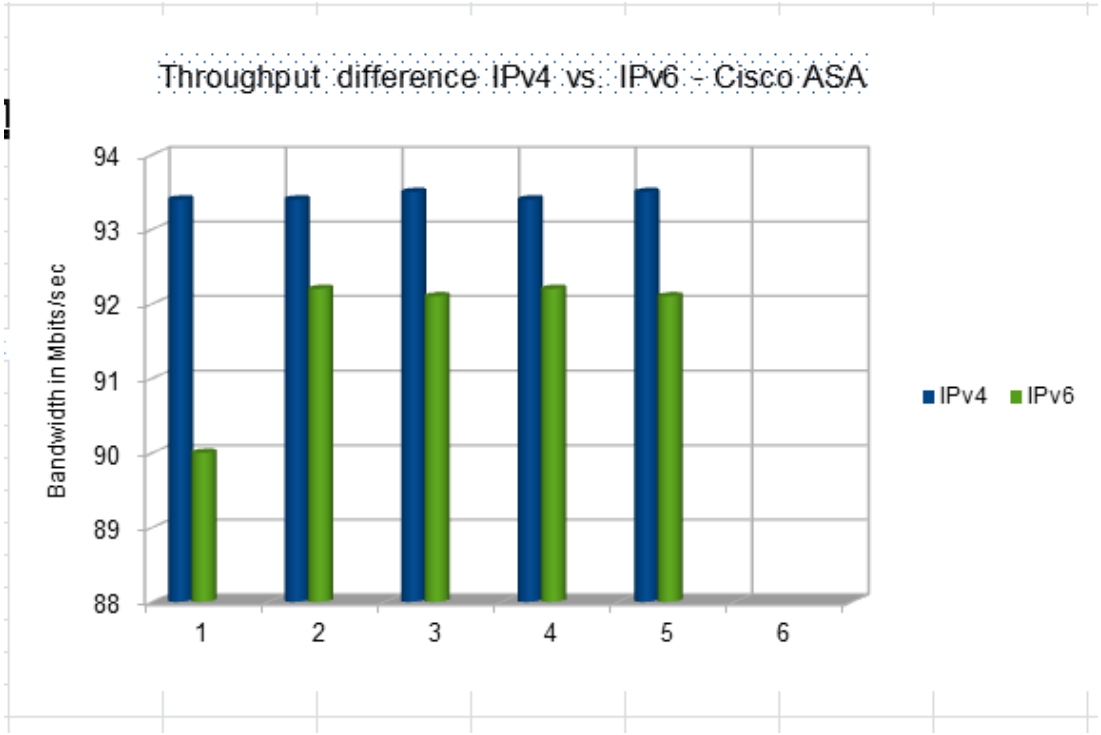




FTP Throughput with Application Inspection

IPv4 in the top

IPv6 in the bottom


Throughput difference IPv4 vs. IPv6 - Cisco ASA
Bandwidth in Mbits/sec
94
93
92
91
90
89
88
1
2
3
4
5
6
IPv4
IPv6

Summary

Conclusion

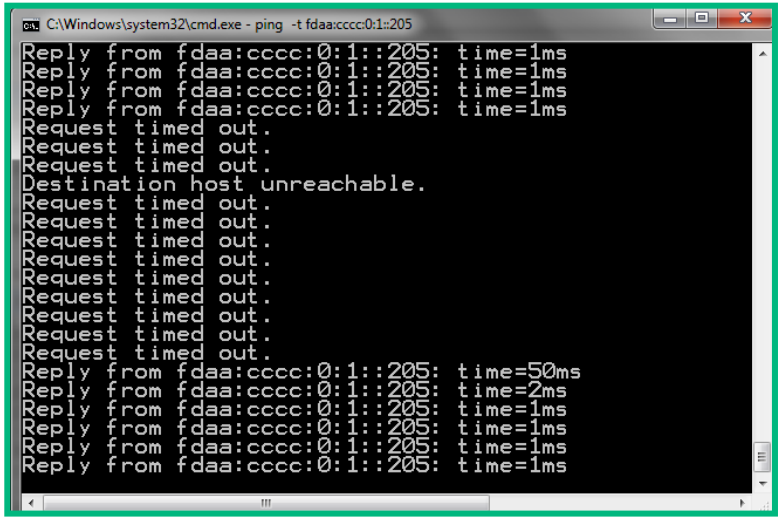
- Throughput of IPv4 and IPv6 is nearly equivalent.
- Application Layer Inspection for IPv6 does not reduce the throughput of the ASA.

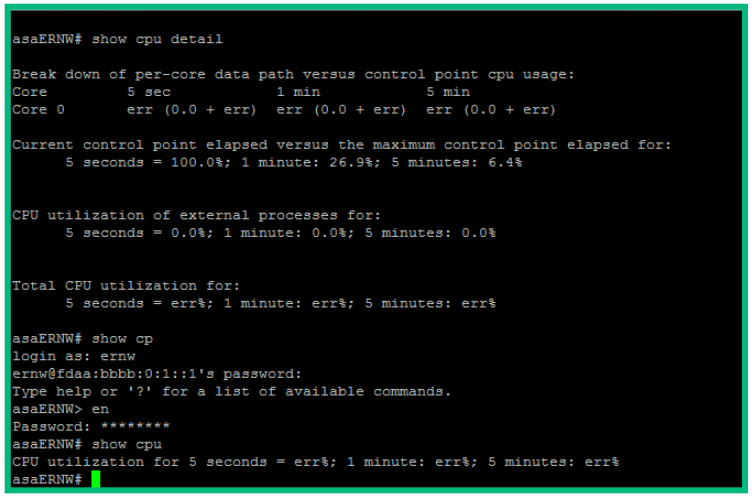
IPv6 – RA flooding

- There were quite some interesting results when we did the testing with the ASA.
- First test was to flood the segment with RAs to see how the ASA behaves.

Results

- CPU Utilization jumps to 100%
- SSH session gets terminated and could be barely reestablished.
- Traffic flowing _through_ the ASA stops completely.
- According to Marc this was/is fully to be expected ;-)





Some Screenshots

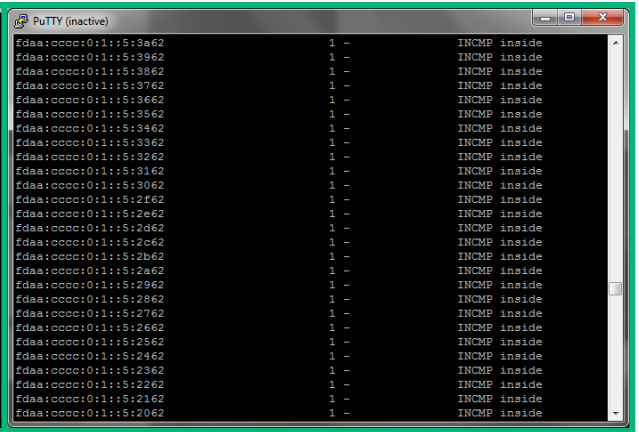
Address Scanning

- The second test consisted of sending packets to non-existing destinations in the DMZ to force the ASA to perform Neighbor Discovery.
- Performed with the scan6 tool with the following command:
  - ./scan6 -i eth0 -d fdaa:cccc:0:1::1-ffff:1-ffff

Results

- CPU Utilization jumps to 100%
- SSH Session was not terminated
- Traffic flowing through the ASA was not affected
  - Well, the latency increased a little, but traffic was not dropped

```
Reply from fdaa:cccc:0:1::205: time=5ms
Reply from fdaa:cccc:0:1::205: time=3ms
Reply from fdaa:cccc:0:1::205: time=5ms
Reply from fdaa:cccc:0:1::205: time=3ms
Reply from fdaa:cccc:0:1::205: time=8ms
Reply from fdaa:cccc:0:1::205: time=6ms
Reply from fdaa:cccc:0:1::205: time=6ms
Reply from fdaa:cccc:0:1::205: time=4ms
Reply from fdaa:cccc:0:1::205: time=5ms
Reply from fdaa:cccc:0:1::205: time=3ms
Reply from fdaa:cccc:0:1::205: time=7ms
Reply from fdaa:cccc:0:1::205: time=3ms
Reply from fdaa:cccc:0:1::205: time=4ms
Reply from fdaa:cccc:0:1::205: time=3ms
Reply from fdaa:cccc:0:1::205: time=7ms
Reply from fdaa:cccc:0:1::205: time=4ms
Reply from fdaa:cccc:0:1::205: time=4ms
Reply from fdaa:cccc:0:1::205: time=4ms
Reply from fdaa:cccc:0:1::205: time=7ms
Reply from fdaa:cccc:0:1::205: time=3ms
```




```
asaERNW# show cpu detailed

Break down of per-core data path versus control point cpu usage:
Core          5 sec             1 min             5 min
Core 0        err (0.0 + err)   err (0.0 + err)   err (0.0 + err)

Current control point elapsed versus the maximum control point elapsed for:
      5 seconds = 100.0%; 1 minute: 38.2%; 5 minutes: 22.6%


CPU utilization of external processes for:
      5 seconds = 0.0%; 1 minute: 0.0%; 5 minutes: 0.0%


Total CPU utilization for:
      5 seconds = err%; 1 minute: err%; 5 minutes: err%

asaERNW#
```

Various Screenshots

Management Protocols

- SSH/HTTPS access works like a charm.
- Syslog not supported over IPv6
  - Even in the next Major Release Version (9.0) still not supported
- SNMP not supported over IPv6
  - See above

Management Protocols

- Failover is supported over IPv6 and in the meantime “matured”.
  - Initial support was introduced in 8.2.2 but there were some “teething problems” in the beginning.
- OSPFv3 support was introduced in 9.0.1
  - But we haven’t tested it yet

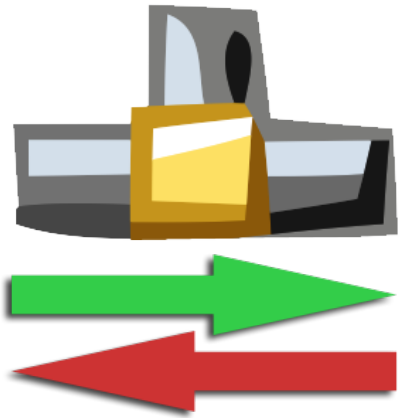
Checkpoint-Results

Check Point®
SOFTWARE TECHNOLOGIES LTD.

General Capabilities

- Well, the Checkpoint supports filtering of IPv6 traffic for some releases
  - But in the early versions there were huge limitations (installation of additional packages etc.)
- R76 added quite a bit of IPv6 enhancements in regards to management and policy rule base.
- Of course, in regards to feature parity to IPv4, there are still some gaps to close ;)

IPv4 Throughput CP



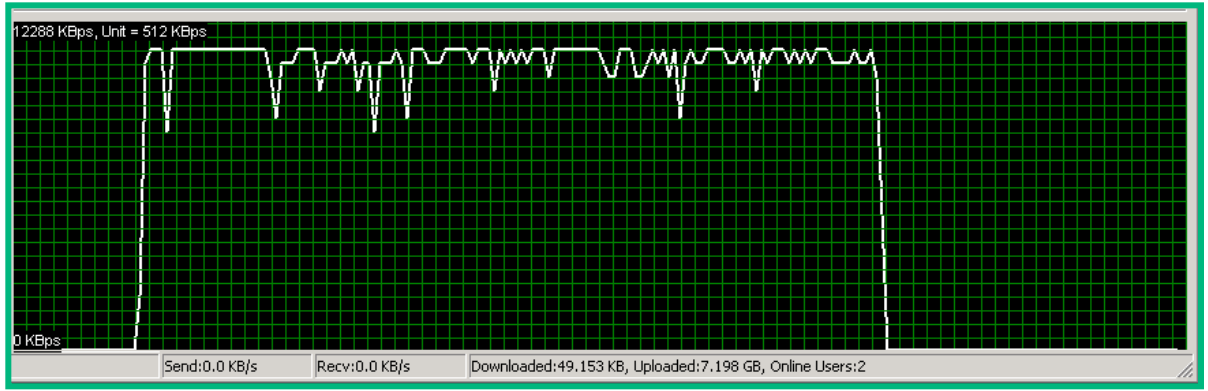
- As we were using commodity hardware, there were no official specs from Checkpoint
- We were able to push approx. 94 Mbit in one direction
  - Which is nearly the theoretical maximum as the Checkpoint was connected to an Fast Ethernet Switch.

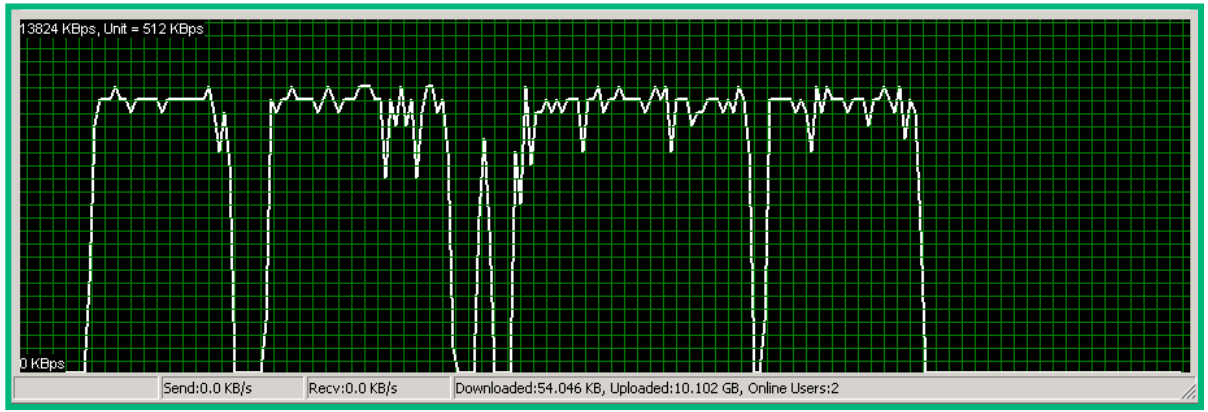
```
C:\Program Files (x86)\iperf>iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56049
[ ID] Interval       Transfer     Bandwidth

[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56054
[  4]  0.0-60.0 sec   672 MBytes  93.8 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56055
[  4]  0.0-60.0 sec   672 MBytes  93.8 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56056
[  4]  0.0-60.0 sec   672 MBytes  93.9 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56057
[  4]  0.0-60.0 sec   672 MBytes  93.9 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56058
[  4]  0.0-60.0 sec   672 MBytes  93.9 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56059
[  4]  0.0-60.0 sec   671 MBytes  93.7 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56060
[  4]  0.0-60.0 sec   672 MBytes  93.9 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56061
[  4]  0.0-60.0 sec   672 MBytes  93.9 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56062
[  4]  0.0-60.0 sec   671 MBytes  93.8 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56063
[  4]  0.0-60.0 sec   672 MBytes  93.8 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56064
[  4]  0.0-60.0 sec   672 MBytes  93.8 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56065
[  4]  0.0-60.0 sec   672 MBytes  93.9 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56066
[  4]  0.0-60.0 sec   672 MBytes  93.9 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56067
[  4]  0.0-60.0 sec   672 MBytes  93.9 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 56068
[  4]  0.0-60.0 sec   672 MBytes  93.9 Mbits/sec
```

IPv4 Throughput CP

```
C:\Program Files (x86)\iperf>iperf -s -V
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44924
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-60.0 sec   606 MBytes  84.6 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44925
[  4]  0.0-60.0 sec   496 MBytes  68.4 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44926
[  4]  0.0-60.0 sec   538 MBytes  75.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44927
[  4]  0.0-60.0 sec   583 MBytes  81.5 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44928
[  4]  0.0-60.0 sec   527 MBytes  73.7 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44929
[  4]  0.0-60.0 sec   557 MBytes  77.9 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44930
[  4]  0.0-60.0 sec   504 MBytes  70.4 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44931
[  4]  0.0-59.9 sec   614 MBytes  86.0 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44932
[  4]  0.0-60.0 sec   536 MBytes  75.0 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44933
[  4]  0.0-60.0 sec   530 MBytes  74.1 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44934
[  4]  0.0-60.1 sec   612 MBytes  85.5 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44935
[  4]  0.0-60.0 sec   532 MBytes  74.3 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44936
[  4]  0.0-61.4 sec   566 MBytes  77.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44937
[  4]  0.0-60.0 sec   604 MBytes  84.4 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 44938
[  4]  0.0-60.0 sec   536 MBytes  75.0 Mbits/sec
```

IPv6 Throughput CP

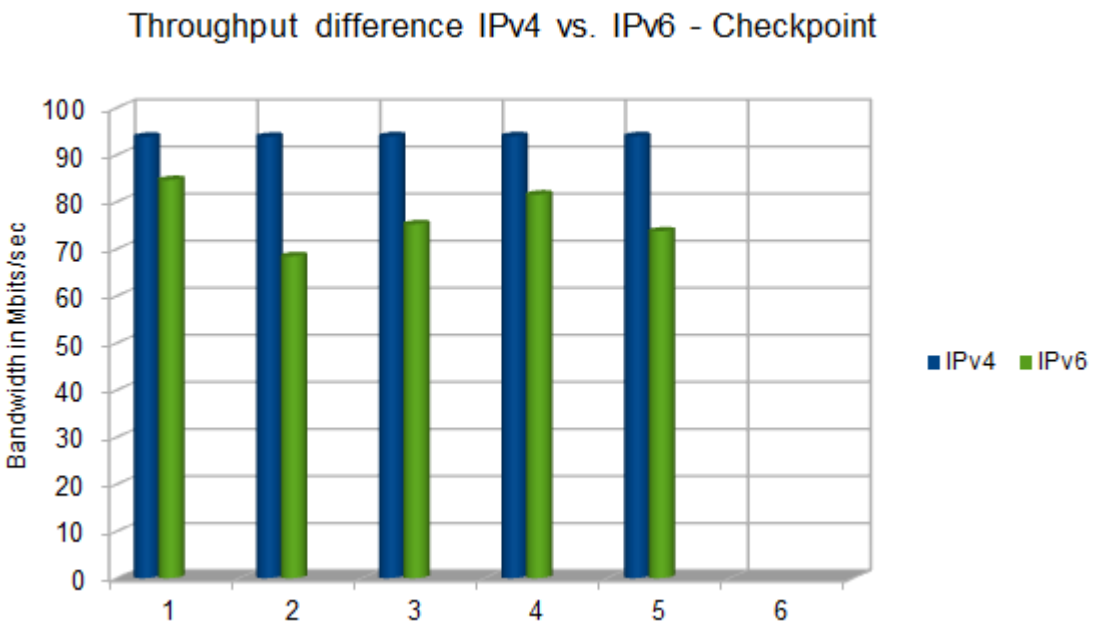




FTP Throughput with Application Inspection

IPv4 in the top

IPv6 in the bottom


Throughput difference IPv4 vs. IPv6 - Checkpoint
Bandwidth in Mbits/sec
100
90
80
70
60
50
40
30
20
10
0
1
2
3
4
5
6
IPv4
IPv6

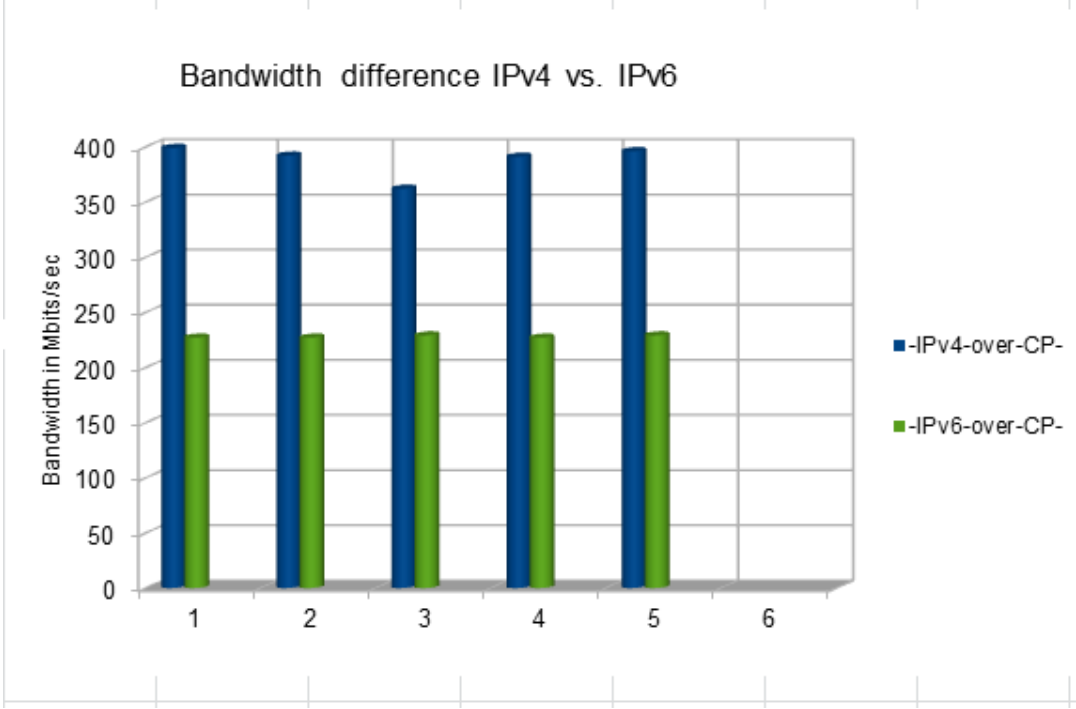
Summary

Interim Conclusion

- Even with the tested (quite new) release, there are some performance differences between IPv4 und IPv6.
- There seems to be a problem with Checkpoint and FTP traffic over IPv6
  - We couldn't find a plausible explanation
  - But some of our customers reported similar problems.

Further Throughput Tests

- As the HP Server has a Gigabit Ethernet card we did the throughput tests again with a Gigabit Switch between “them”.
  - Cisco 4948E (to avoid potential interface buffer issues)



Summary – Gigabit Connection

Final Conclusion

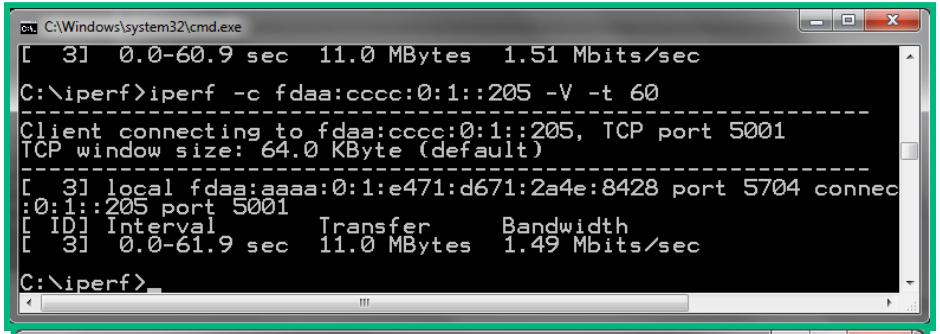
- It seems that the Checkpoint has some problems with FTP and IPv6.
- The difference in throughput can be quite huge.
  - Up to 40%
- There needs some work to be done.

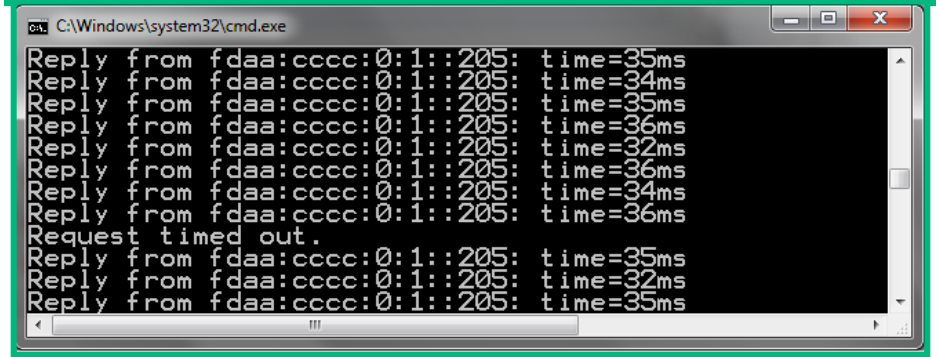
IPv6 – RA flooding

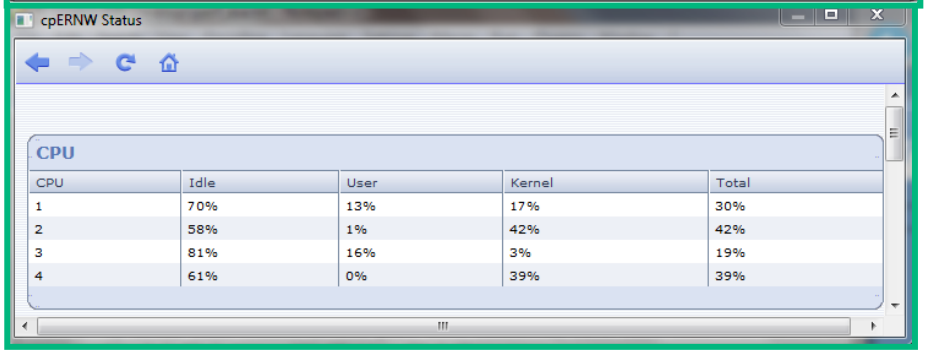
- As with the ASA, the first test was to flood the segment with RAs to see how the CP behaves.

Results

- The results looked kind of better than on the ASA ;)
  - But this could be because the Checkpoint has more CPU Power than the ASA
- CPU Utilization went to ~50%
- All Management Sessions were kept alive.
- Throughput of traffic flowing _through_ the Checkpoint dropped quite heavily.







Some Screenshots ;)

Address Scanning

- The second test consisted of sending packets to non-existing destinations in the DMZ to force the CP to perform Neighbor Discovery
- Performed with the scan6 tool with the following command:
  - ./scan6 -i eth0 -d fdaa:cccc:0:1::1-ffff:1-ffff

Results

- We made some weird observation:
- Even though we sent out a lot of ICMPv6 Echo Requests to non existing IPv6 addresses
- No incomplete entries could be found on the Check Point
- We assume that the checkpoint only insert an entry if ND is successful

Management Protocols

- SSH/HTTPS access works like a charm
- Communication between the *SmartConsole* and the Security Gateway works reliably over IPv6.
- Syslog not supported over IPv6.
- SNMP not supported over IPv6.
- NTP not supported over IPv6.

Management Protocols

- ClusterXL is supported over IPv6
- VRRPv3 and OSPFv3 are supported since R76
  - But we haven't fully tested them.
  - At least the OSPFv3 adjacency between Cisco Router and the Checkpoint came up.

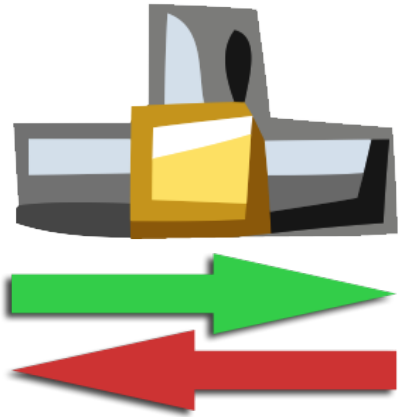
ERNW
providing security.

Juniper-SSG Results

General Capabilities

- ScreenOS 6.3r13 supports the filtering the of IPv6 traffic
- With regard to feature parity to IPv4, there are still some gaps to close ;)

IPv4 Throughput Juniper



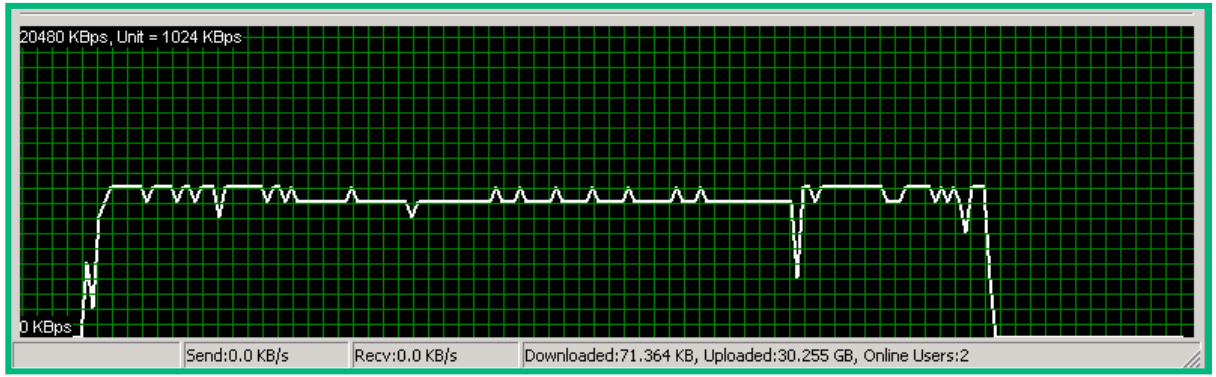
- According to Juniper, the SSG5 can push up to 160 Mbit of traffic
- We were able to push approx. 90 Mbit in one direction
  - Which is nearly the theoretical maximum as the Juniper has only a Fast Ethernet interface.

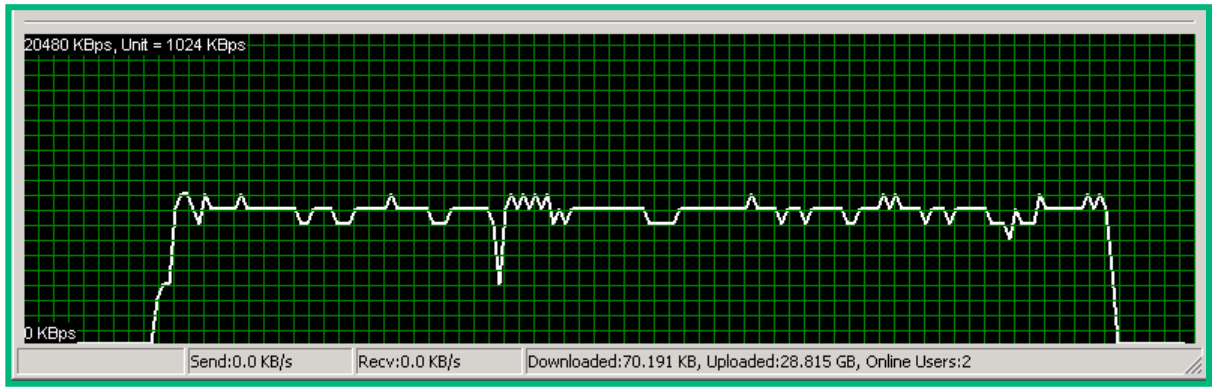
```
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57224
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-60.0 sec   627 MBytes  87.6 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57227
[  4]  0.0-60.0 sec   659 MBytes  92.1 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57228
[  4]  0.0-60.0 sec   664 MBytes  92.7 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57229
[  4]  0.0-60.0 sec   667 MBytes  93.2 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57230
[  4]  0.0-60.0 sec   663 MBytes  92.6 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57244
[  4]  0.0-60.1 sec   614 MBytes  85.7 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57245
[  4]  0.0-60.0 sec   664 MBytes  92.7 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57246
[  4]  0.0-60.0 sec   639 MBytes  89.3 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57247
[  4]  0.0-60.0 sec   633 MBytes  88.4 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57248
[  4]  0.0-60.0 sec   645 MBytes  90.2 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57264
[  4]  0.0-60.0 sec   668 MBytes  93.3 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57265
[  4]  0.0-60.0 sec   646 MBytes  90.3 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57266
[  4]  0.0-60.1 sec   630 MBytes  87.9 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57267
[  4]  0.0-60.0 sec   614 MBytes  85.8 Mbits/sec
[  4] local 192.168.3.205 port 5001 connected with 192.168.1.2 port 57268
[  4]  0.0-60.0 sec   661 MBytes  92.4 Mbits/sec
```

IPv4 Throughput SSG

```
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45956
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-60.0 sec   636 MBytes  88.8 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45961
[  4]  0.0-60.0 sec   637 MBytes  89.0 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45962
[  4]  0.0-60.0 sec   634 MBytes  88.6 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45963
[  4]  0.0-60.0 sec   632 MBytes  88.4 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45964
[  4]  0.0-60.0 sec   633 MBytes  88.4 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45978
[  4]  0.0-60.0 sec   637 MBytes  89.0 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45979
[  4]  0.0-60.0 sec   635 MBytes  88.7 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45980
[  4]  0.0-60.0 sec   636 MBytes  88.9 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45981
[  4]  0.0-60.0 sec   634 MBytes  88.7 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45982
[  4]  0.0-60.0 sec   632 MBytes  88.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45989
[  4]  0.0-60.0 sec   632 MBytes  88.3 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45990
[  4]  0.0-60.0 sec   638 MBytes  89.2 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45991
[  4]  0.0-60.0 sec   632 MBytes  88.3 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45992
[  4]  0.0-60.0 sec   636 MBytes  88.9 Mbits/sec
[  4] local fdaa:cccc:0:1::205 port 5001 connected with fdaa:aaaa:0:1:51e9:6968:1025:7e71 port 45993
[  4]  0.0-60.0 sec   631 MBytes  88.2 Mbits/sec
```

IPv6 Throughput SSG

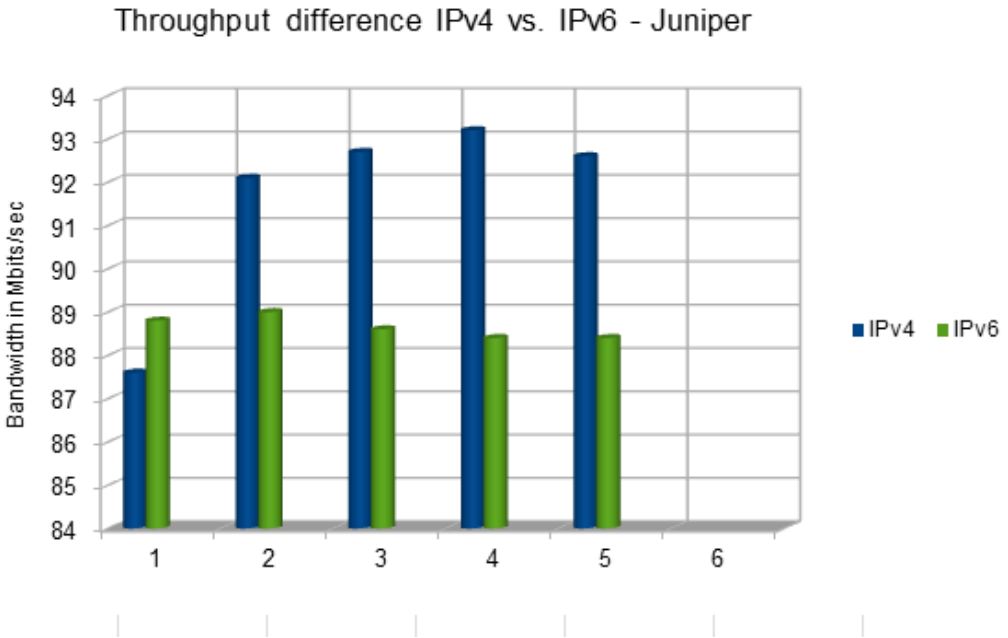




FTP Throughput with Application Inspection

IPv4 in the top

IPv6 in the bottom


Throughput difference IPv4 vs. IPv6 - Juniper
Bandwidth in Mbits/sec
94
93
92
91
90
89
88
87
86
85
84
1
2
3
4
5
6
IPv4
IPv6

Summary

Conclusion

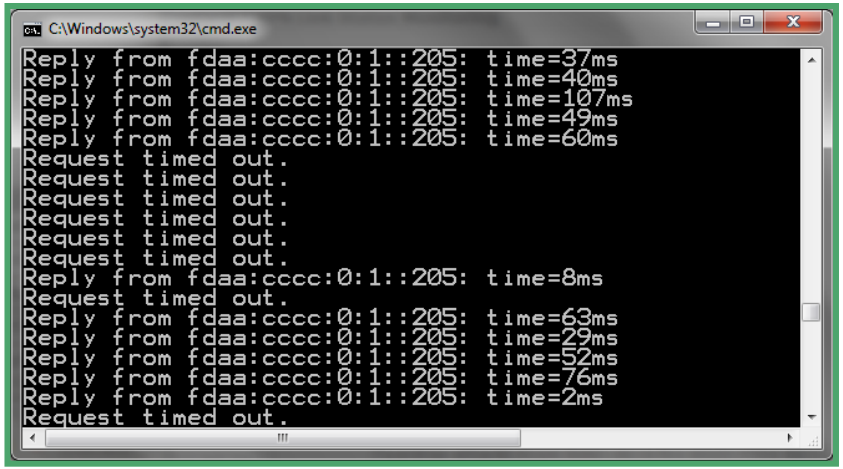
- Throughput of IPv4 and IPv6 is nearly equivalent.
- Application Layer Inspection for IPv6 does not reduce the throughput of the Juniper.

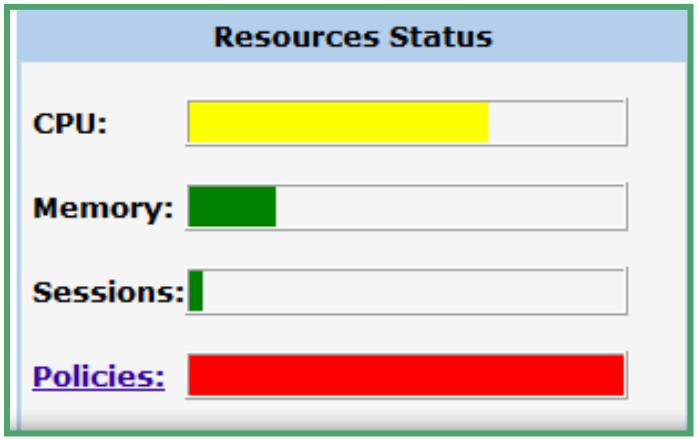
IPv6 – RA flooding

- As with the ASA and Check Point, the first test was to flood the segment with RAs to see how the Juniper behaves.

Results

- The results looked kind of better than on the ASA ;)
- CPU Utilization went “only” to ~70%
  - Which is way better for a such a small device than 50% on 4 Core Xeon ;)
- All Management Sessions were kept alive.
- Throughput of traffic flowing _through_ the Juniper dropped quite heavily.



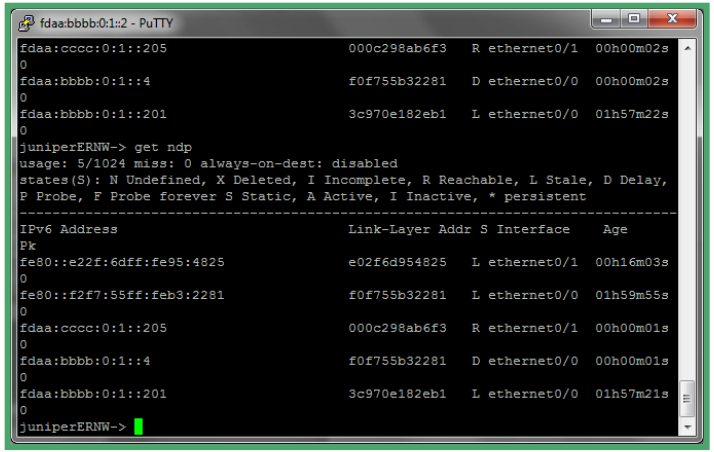


Some Screenshots ;)

Address Scanning

- The second test consisted of sending packets to non-exisiting destinations in the DMZ to force the Juniper to perform Neighbor Discovery
- Performed with the scan6 tool with the following command:
  - ./scan6 -i eth0 -d fdaa:cccc:0:1::1-ffff:1-ffff

Results



- We made some weird observation:
- Even though we sent out a lot of ICMPv6 Echo Requests to non existing IPv6 addresses.
- No incomplete entries could be found in the Juniper.
- We assume that the Juniper only insert an entry if ND is successful.

Management Protocols

- SSH/HTTPS access works like a charm.
- Syslog not supported over IPv6.
- SNMP not supported over IPv6.
- NTP not supported over IPv6.

What We Have Observed in Customer Environments

- MEF
  - See above at *Problem Statement* ;)
- Cisco CSM does not support IPv6 ACLs for Routers.
  - Still the case in July 2013?
    to be verified.

Student Work

Recent Student Work

- Stefan will take over here.

- He's a student with ERNW and had some time to play in the lab.
- He starts writing his bachelor thesis on "this stuff" on 08/01/13 ;-)

Theme

- First Test (practical work for university)
  - Build up a laboratory
  - Perform three evaluation Methods
    - Check against RIPE554
    - Security Tests (THC IPv6-Suite)
    - Performance Test
- Second Test (Bachelor Thesis)
  - Taking a closer look of the extension header implementation
  - Fuzzing $Sec-Device with Dizzy
  - Build own Scapy Scripts

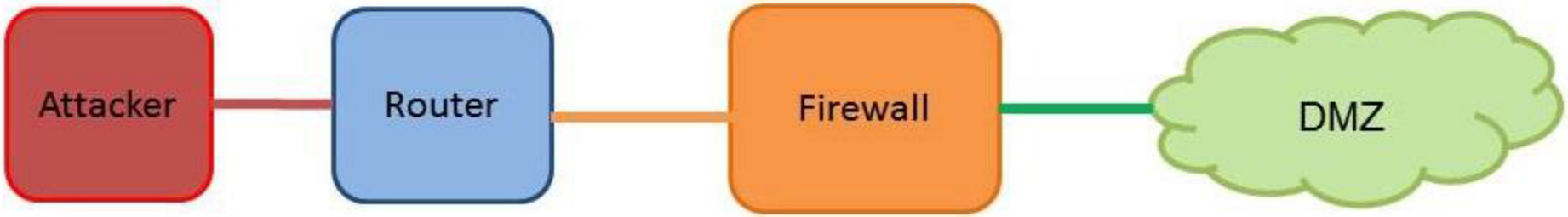
Laboratory & First Tests

Laboratory

VLAN10
IPv4: 192.168.1.0/24
IPv6: 2001:db8:0:1::/64

VLAN20
IPv4: 192.168.2.0/24
IPv6: 2001:db8:0:2::/64

VLAN30
IPv4: 192.168.3.0/24
IPv6: 2001:db8:0:3::/64



Tested devices

- Juniper SSG 5

- Cisco ASA 5505

RIPE 554

- Published in June 2012
- Overview about the specific requirements of IPv6 Environments
- -> ensure that the devices are able to support the IPv6 basic functionalities

Security tests

- THC-IPv6 Security Toolkit
- Marc Heuse
- Selected remote attacks:
  - firewall6
  - implementation6
  - thcping6
  - toobig6
  - ndpexhaust26
  - thcsyn6

Performance test

- Iperf – bandwidth measuring tool
  - IPv4 and IPv6 on each $sec-device
  - Start iperf server in DMZ
    - Iperf –s (-V)
  - Start iperf client at attacker vlan
    - Iperf –c 2001:db8:0:3::2008 –V

Test Results

RIPE 554

performed test	Cisco ASA 5505	Juniper SSG 5
check against RIPE 554		
IPv6 Basic specification	☺	☺
IPv6 Addressing Architecture	☺	☺
Default Address Selection	☺	☺
ICMPv6	☺	☺
SLAAC	☺	☺
Router-Alert option	☺	
Path MTU Discovery	☺	☺
Neighbor Discovery	☺	☺
Basic Transition Mechanisms	☺	☺

Test results – Security Tests

performed test	Cisco ASA 5505	Juniper SSG 5
check against RIPE 554		
./firewall6 eth0 2001:db8:0:3::2008 22	😐	😐
./firewall6 eth0 2001:db8:0:3::2008	😐	😐
./implementation6 –p eth0 2001:db8:0:3:2008	☺	😐
./thcping6 eth0 2001:db8:0:1::1 2001:db8:0:3::2008	☹	☹
./toobig6 eth0 2001:db8:0:1::1 2001:db8:0:3::2008 1280	☺	☺
./toobig6 eth0 2001:db8:0:1::1 2001:db8:0:3::2008 48	☹	☹
./toobig6 eth0 2001:db8:0:1::1 2001:db8:0:3::2008 100000	☹	☹

Test results – Security Tests

performed test	Cisco ASA 5505	Juniper SSG 5
check against RIPE 554		
./ndpexhaust26 –c –r eth0	☹	☺
./ndpexhaust26 –c –r –p eth0 2001:db8:0:3::	☹	☹
./thcsyn6 eth0 2001:db8:0:3::2008 80	😐	😐
./thcsyn6 –A eth0 2001:db8:0:3::2008 80	😐	😐
./thcsyn6 eth0 2001:db8:0:3::2008 x	😐	😐
./thcsyn6 –S eth0 2001:db8:0:3::2008 x	😐	😐

Performance test

- Cisco ASA
  - IPv4 93.9 Mbit/sec
  - IPv6 76.76 Mbit/sec
- Juniper SSG 5
  - IPv4 97.44 Mbit/sec
  - IPv6 88.6 Mbit/sec

Second Part (Bachelor Thesis)

Future work

- Taking a closer look of the extension header implementation
- Fuzzing the IPv6 Header
  - All Extension Headers in different combinations
- Crafting own Packets with scapy
  - Different kinds of extension header chains
- More Vendors!

Fuzzing with Dizzy

- ERNW made fuzzing framework
  - Python based
  - Fast!
  - Can send on L2 and upper Layers (TCP/UDP/SCTP)
  - Very easy protocol definition syntax

- See also: http://www.insinuator.net/2012/05/releasing-dizzy-version-0-6/

Fuzzing with Dizzy

```
#IPv6-Template
name = "ipv6 template"

objects = [
    field("eth_dst", 48, "\xff\xff\xff\xff\xff\xff", "none"),
    field("eth_src", 48, "\x00\x14\xe2\xab\xe0\x69", "none"),
    #rand("eth_src", 48),
    field("eth_type", 16, "\x08\x00", "none"),

    field("ip_ver", 4, "\x06", none),
    field("tra_cla", 8, "\x00", none),
    field("flo_lab", 20, "\x00\x00\x00", none),
    field("pay_len", 16, "\x00\x00", full),
    field("nex_hea", 8, "\x00", none),
    field("hop_lim", 8, "\x00", none),
    field("ip_src", 128, "\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00", none),
    field("ip_dst", 128, "\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff", none),

    field("udp_src", 16, "\x00\x44", none),
    field("udp_dst", 16, "\x00\x43", none),
    field("udp_len", 16, "\x00\x00", none),
    field("udp_csum", 16, "\x00\x00", none),
    ]

functions = []
```

Scapy

- Python-based
- Build packets
- Decodes, but cant interpret packets
- Using in Scripts / Interactive
- Predefined header templates

Scapy example

```
#!/usr/bin/env python
from scapy.all import sr1,IPv6

packet= IPv6(src=srcip, dst=dstip)\
   /IPv6ExtHdrFragment(offset=0,m=1)\
   /IPv6ExtHdrDestOpt(nh=60)\
  /IPv6ExtHdrDestOpt(nh=60)\
  /IPv6ExtHdrDestOpt(nh=60)\
  /IPv6ExtHdrDestOpt(nh=58)
packet2 = IPv6(src=srcip, dst=dstip)\
  /IPv6ExtHdrFragment(offset=5,m=0,nh=58)\
  /ICMPv6EchoRequest(cksum=csum, data=payload)
send (packet)
send (packet2)
```

Testing approaches, tools or any aspects?

sschwalb@ernw.de

Appendix: IDP and SIEM Solutions

Overview of the Real-World Capabilities of Major Commercial Security Products.

IDP/SIEM

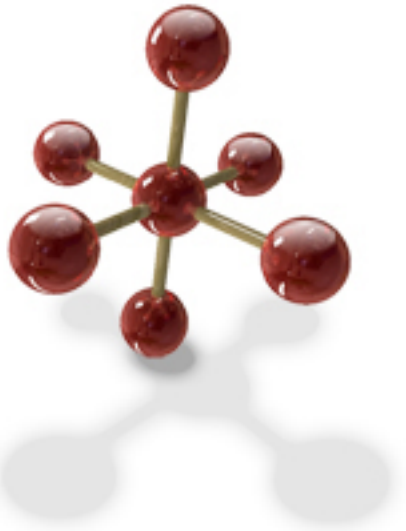
- Almost all vendors are „IPv6 proofed“, but still are working on feature set like in IPv4
- The need of IPv6 has not yet arrived!
- Different kind of IPv6 support
  - Management Interfaces
  - Engine Support
  - Ruleset
  - Event Sources

Evaluated Equipment

- Intrusion Detection and Prevention Systems
  - HP Tipping Point
  - McAfee Network Security Platform
  - Juniper IDP
  - Cisco ASA SSC Module
- Security Incident Event Monitoring
  - HP ArcSight
  - IBM QRadar
  - Nitro
  - Splunk

Event Sources

IPv6 Support on Cisco Network Devices



- Netflow over IPv6
  - Recording IPv6 records
  - No transport over IPv6
    - Sending flow records over IPv4 exporter
  - Limited kpoint only uses IPv4
  - Flexible Netflow supports it since IOS 15.2
- IPv6 support for Syslog and SNMP depends on device
  - IOS 12.2 – Cisco 3560
  - IOS 15.0 – Cisco 1921/2951
  - Whats about Cisco 2950/3550?

Event Sources

Windows Management Instrumentation (WMI)

- WMI is supporting connections via IPv4 and IPv6
- Limitation within IP related classes, e.g. network adapter and routing information
  - *E.g. Win32_ActiveRoute and Win32_NetworkAdapter*

> *"Starting with Windows Vista, WMI also provides limited support for IPv6 network capabilities."*
> *-> msdn.microsoft.com, 03-2013*

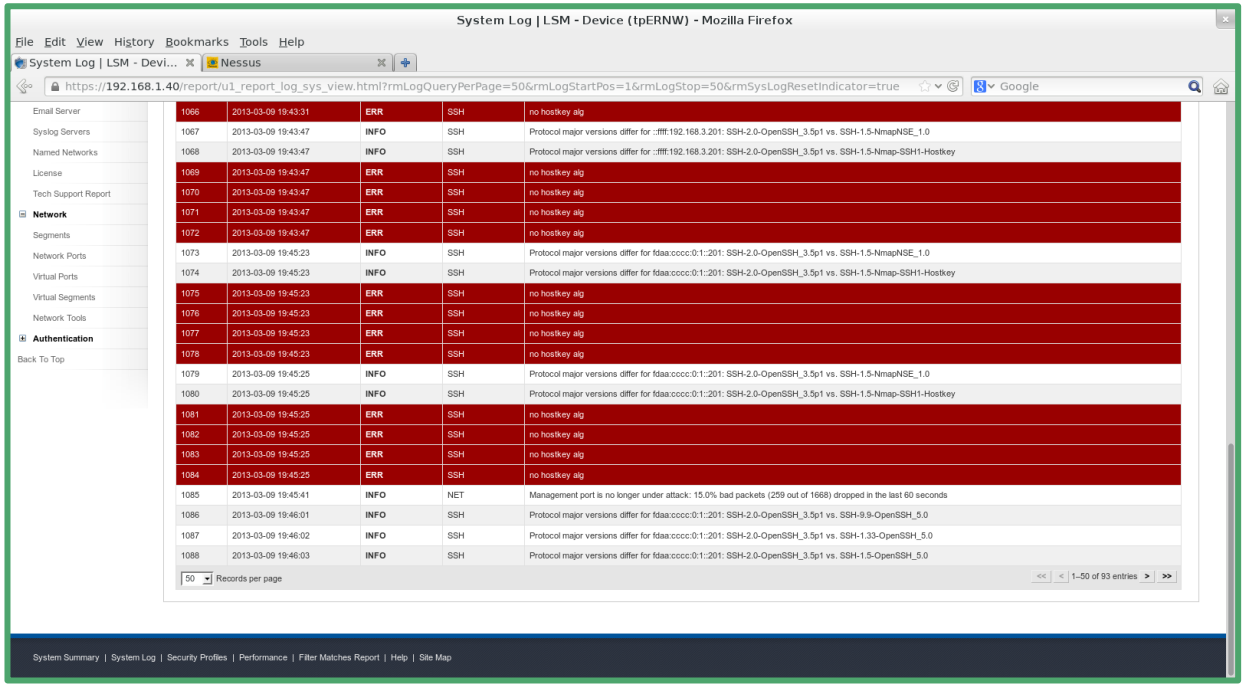
Management Interfaces

- Usually, one of the latest features, supported by the appliance.
  - E.g. Cisco ASA currently is working on it
- Trouble with management interfaces
  - Kind of „new feature“ – in 2012/2013
  - e.g. firefox is not able to handle [2001:db8::1] with HTTPS, in 2013
    - Ever tried [::1] in IE?

HP Tipping Point

Overview

- Supporting IPv6 since TOS v3.1
  - Management interface available through IPv4 and IPv6
  - Inspection of IPv6 Traffic
- IPv6 ruleset is enabled by default.
- In our tests, TP showed up an equal behavior between IPv4 and IPv6 in both, performance and intrusion detection.



HP Tipping Point

Nessus IPv6 Scan

ERNW
providing security.

HP Tipping Point

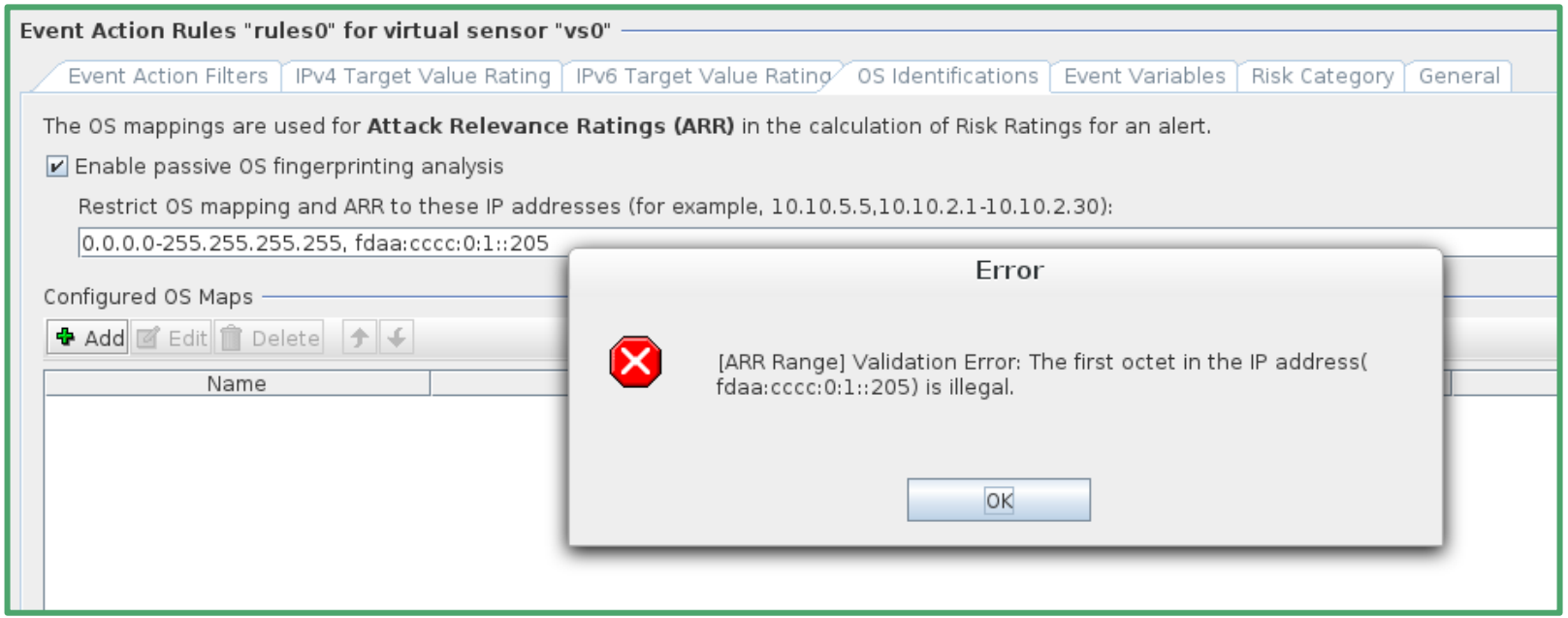
Cisco ASA and SSC-5

Overview

- IPv6 requirements
  - At least ASA Software Release 8.2
  - IPS Sensor Software Release 6.2
- But no support for management interface via IPv6.
- Limited IPv6 rule and feature set.

Cisco ASA and SSC-5

Limited IPv6 Features



Cisco ASA and SSC-5

IPv6 Support Documentation?

Cisco ASA IPS

Q. Can the Cisco ASA 5500 Series IPS solution support hybrid IPv6 and IPv4 deployments?

A. Yes. The Cisco ASA 5500 Series IPS solution provides protection for pure IPv6 deployments, pure IPv4 deployments, and hybrid IPv6 and IPv4 deployments with a single appliance, for maximum deployment flexibility and investment protection.

Q. Which versions of Cisco ASA Software are required to support IPv6 for IPS?

A. In order to support IPv6 for IPS, Cisco ASA devices must be running a minimum of Cisco ASA Software Release 8.2 and a minimum of Cisco IPS Sensor Software Release 6.2 and E3 engine on the IPS module.

Q. Are the IPv6 for IPS capabilities on Cisco IPS Sensor Software Release 6.2 National Security Agency (NSA) approved?

A. Yes. The IPv6 for IPS capabilities on Cisco IPS Sensor Software Release 6.2 are NSA approved.

Q. What management applications can be used to configure the Cisco ASA AIP SSMs to protect my IPv6 network?

A. The Cisco Adaptive Security Device Manager (ASDM), Cisco IPS Device Manager (IDM), or Cisco IPS Manager Express (IME) can be used to configure the IPv6 and IPv4 IPS capabilities on the Cisco ASA AIP SSMs.

McAfee NSP

NSP Versions: 6.0, 6.1, and 7.0
„Full IPv6 support“

2. Features that do not support IPv6

IPv6 is not supported for the following features in Network Security Platform:

- Access Control Lists/ Firewall policies [classic (ACLs) and advanced policies]: works when not using IPv6 addresses
- IP spoofing
- Virtualization (VIDS) based on CIDR interfaces
- TACACS+
- DoS/DDoS detection
- Threat Analyzer launch using IPv6 addresses
- Network Access Control [NAC]
- Network Threat Behavior Analysis [NTBA]
- Integration with:
  - McAfee ePolicy Orchestrator [ePO]
  - McAfee Host Intrusion Prevention
  - McAfee Vulnerability Manager
  - McAfee Global Threat Intelligence [GTI] for IP Reputation

Reference: McAfee® Application Note, Network Security Platform: IPv6 Support, 04-Jun-2012

PROBLEM OR GOAL:

By default, IPv6 traffic is dropped on IDP stand-alone platforms.

CAUSE:

SOLUTION:

The 4.x, 5.0rx, and 5.1rx IDP software version handle IPv6 traffic as non-IP protocol and by default, drop it. **Layer 2 bypass** must be enabled to forward IPv6 traffic, as well as other non-IP protocols.

To enable this option:

1. Logon to the IDP ACM via a web browser (**https://IDP_IP_ADDRESS**).
2. Click ACM; from the **ACM** menu, select **Configure Virtual Routers**.
3. In the web page, select the **Enable layer2 bypass** check box.
4. Then, adhere to the rest of the wizard instructions and confirm the configuration at the end. This will restart the IDP processes.

To verify if the ACM setting is in effect:

1. Edit the **/usr/idp/device/cfg/idp.cfg** file.
2. Verify the **idp.layer2_bypass** line; the value must be set to 1 (enabled).
3. IDP processes must be restarted to apply the change.

Currently, IPv6 traffic inspection is not available for stand-alone IDP platforms.

Juniper IDP

[KB14828]

SIEM

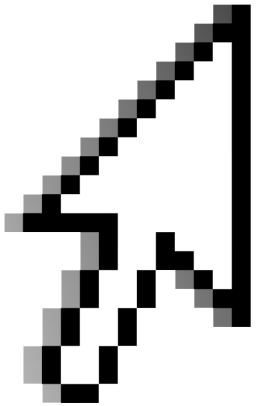
- Security Information and Event Management
  - Data aggregation
  - Log and event correlation
  - Monitoring, alerting and dashboard functionalities
- Real-time analysis of security alerts generated by network hardware and applications.
- Therefor as central component must deal with IPv6, or?

HP ArcSight

- „IPv6 is fully supported“
- But more means a kind of limited IPv6 support
- ESM is supporting IPv6, enabled by default
  - Known problems in viewing address space (using text fields)
  - No standard rules based on IPv6

IBM QRadar

- Engine is IPv6 ready, but yet there exist not much IPv6 rules.



McAfee ESM & Splunk

- McAfee ESM
  - „Supporting IPv6“ with 8.4.x
  - Event delivery supported since 9.0
- Splunk
  - Full IPv6 support on base system, including indexing services.
  - Event management relates on used app

Conclusion

- There is no need of IPv6 rules yet, therefore vendors have no focus on creating them.
  - Customers must apply pressure!
- Almost all appliances are IPv6 ready, within limitations.
  - E.g. within additional feature sets
- Differences in rulesets are necessary, e.g. related to IPv6 specific attacks!

ERNW providing security.

Stay in touch

The legendary TROOPERS 10k run

- Visit our blog and join the discussion: INSINUATOR.NET
- Join us at **TROOPERS.de** conference!
  - Details: See next slide.
- Ping us at Twitter: @WEareTROOPERS @Insinuator
- Drop us a mail.

There are few things to know about TROOPERS:

DATE: March, 17-21. 2014
PLACE: Heidelberg, Germany
MISSION: Make the world a safer place.

REGISTRATION OPEN: www.troopers.de

ERNW providing security.

The Archive

Jeff Gough at TROOPERS13

- Feel the spirit – TROOPERS13 Teaser: https://www.youtube.com/watch?v=lfBo48r-Qho
- TROOPERS13 Talks:
  - Videos: http://www.youtube.com/playlist?list=PL1eoQr97VfJl1LdMzyQPz71uR6bwiUGog
  - Slides: https://www.troopers.de/archives/index.html
- We hope to see you in 2014!