IPv6 support in firewalls

A report from .SE

by Håkan Lindberg and Tomas Gilså

Table Of Contents

1 Introduction

1.1 The report

During September 2009 six firewalls were tested by .SE. Formally this was a workshop; the basic idea was to exchange information and to learn. .SE arranged a similar event during 2008, the main difference year 2009 was to include testing with more sessions and to include an environment with IPv4 and IPv6. The results from the tests are presented in this report.

1.2 References

[1] SSAC report 021, ICANN Security and Stability Advisory Committee Survey of IPv6 Support in Commercial Firewalls, October 2007

[2] NIST, National Institute of Standard and Technology A Profile for IPv6 in the U.S. Government, Draft from Feb 2007 and later

[3] http://www.rfc-editor.org/rfc/rfc2413.txt

1.3 About .SE

.SE (The Internet Infrastructure Foundation) is responsible for the Swedish top level domain, .se. The core business is the registration of domain names and the administration and technical operation of the national domain name registry. At the same time as .SE promotes the positive development of the Internet in Sweden.

1.4 Summary

In September 2009 IIS tested six different firewall suppliers concerning IPv6 support. All six performed well and IPv6 seems to be practically as mature as IPv4 on the basic level: it can be filtered out, checked for in the logs etc. One supplier H3C showed an early version of the IPv6-code, here we had to use the CLI (Command Line Interface). Otherwise most brands could be managed via IPv6 and IPv6 is supported in the graphical interface (the web interface).

Setting up a workshop in this way is not just a way of testing. It is also a good way of achieving hands-on experience. IPv6 is a bit different and even though the participants had many years of experience it is easy to forget that ICMPv6 is different which affects filtering.

The test of 2008 was a nice and gentle test in a pure IPv6 environment. We asked companies that sell firewalls in Sweden to participate in a small test of firewalls with support for IPv6.

Out of about 25 vendors, we ended up testing seven machines from six different vendors in 2008. Three more vendors submitted machines that were not IPv6-ready enough for our test.

In 2008 we found that firewalls are ready for implementing IPv6-networks. Even though one cannot use the same rules as in IPv4, filtering and administration worked a bit better than expected.

One reason for enabling IPv6 in your firewalls is to familiarize yourself with addresses, prefixes and new rules. The SSAC survey [1] results do suggest "that an organization that adopts IPv6 today may not be able to duplicate IPv4 security feature and policy support". Our result from the 2008 test indicates that IPv6 support is definitely good enough to start testing and for 1st phase operation.

In the test from 2008 we found that bad performance when processing IPv6-packets is a myth. Or an old truth.

1.5 Background

The Internet is running out of IPv4 addresses, by many estimates the IPv4 address space will be exhausted in 2010 or 2011. According to the same estimates it will take some years to roll out IPv6 so .SE figured it was time to begin planning for the transition. As a way to get started with IPv6, .SE decided to set up and test firewalls for IPv6 traffic.

Besides, the current use of DHCP, NAT and such is good for privacy but sometimes bad for security. With IPv6 addresses, each machine on the net can have a unique address. This makes it easier to block certain computers and open up services for others.

The transition from IPv4 to IPv6 will undoubtedly lead to a world where most of us run both protocols in parallel for the foreseeable future. There are boxes available on the market that translate between IPv4 and IPv6, transparent to the user. Several vendors have also implemented network stacks with support for both IPv4 and IPv6, so called dual stacks. RFC 4213 describes Dual Stack and also another concept for coexistence: Configured Tunneling. The latter is a method to carry IPv6 packets over an unmodified IPv4 routing infrastructure.

We will simply have to live with both IPv4 and IPv6. Nothing says we need to have just one system – as long as people can communicate, the big problem is still solved.

Several ISPs sell IPv6 connectivity. Windows Vista, Windows Server 2008, Mac OS X and all Linux distributions have good support for IPv6. Windows XP can do basically everything except DNS-queries over IPv6.

1.6 Purpose

To see the status of IPv6-readiness among the vendors, and to document what works today. .SE that runs the top level domain ".se", wanted to present this information as part of the conference Internetdagarna in Stockholm..SE also wanted to set a good example of IPv6-awareness and usage.

When selecting areas to test we mainly used two references, one document from NIST [2] which we found useful to answer the question "what is a firewall?". The SSAC report [1] was based on a survey and clearly shows that some areas should be ready for testing.

1.7 The SSAC report

One of three firewalls has IPv6 support according to the SSAC survey [1]. According to the survey there is limited support for advanced IPv6-firewall functions in the SOHO and SMB markets. Suppliers say demand for IPv6 is limited.

The SSAC survey results do suggest that "an organization that adopts IPv6 today may not be able to duplicate IPv4 security feature and policy support" The results from our tests still show that the feature set is good enough for testing and for limited operation.

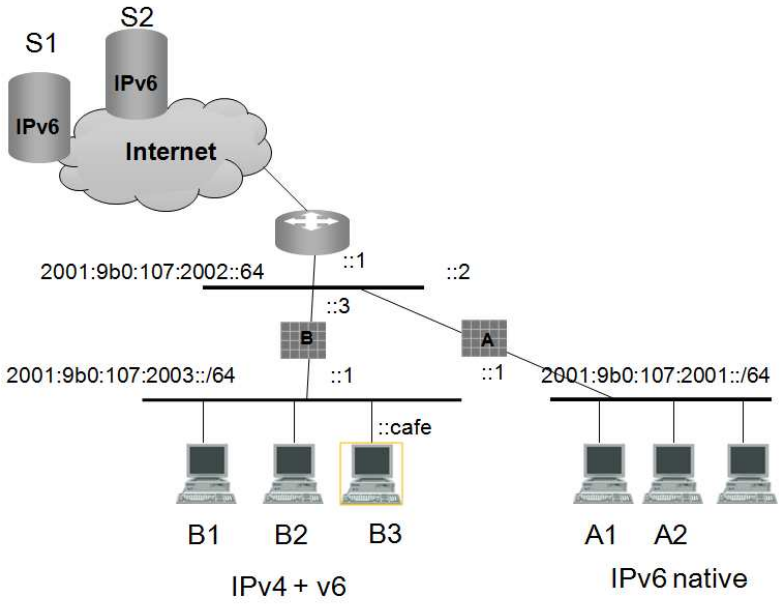
1.8 What is "IPv6 Ready"?

Some of the firewalls we planned to test 2008 were marked with an "IPv6 Ready" logo.

During 2008 we found out that IPv6 Forum has defined two levels of IPv6-readiness, called Short term period (Phase-1) and Long term period (Phase-2). The devices we tested had the Phase-1 readiness which seemingly should be translated to "Not Much". One of the vendors, D-Link, has exercised some restraint in marketing Phase 1-equipment as IPv6-ready in Sweden.

We also bought devices in 2008 that were not firewalls but rather access points with NAT-functionality, such as D-link DI-524 and DIR-615. Both products have the IPv6-logo on the IPv6-ready-logo site, but there was no IPv6 in the boxes we tested. (And D-link had not put the logo on the boxes.) So usage of the IPv6-ready-logo site is limited for the time being.

2 Method



Picture: the 2009 workshop setup

The drawing shows the principle. In reality we had to include IPv4 addresses etc. in the v6 only network for some management. We also had a local IPv6-ready HTTP server, but during the test we did use IPv6 hosts on the Internet.

Mac Minis running Ubuntu Linux were used as servers, routers and for client simulation. Windows XP, Vista and Mac machines were used as clients.

We used curl-loader to test a number of simultaneous sessions. We downloaded several objects up to 30 times from Google, Sunet and IPv6forum. Curl-loader can handle thousand of clients and much larger files then what we used in our set-up. We tested with one hundred clients and larger files than normal web pages but then we did have problems and we could not be sure if the problems were present in the Apache server, the router or in the firewall. Therefore we simulated a maximum number of 30 sessions. To compensate for the variations on the Internet performance we did several test cycles.

The test bed did not generate very high load with 30 sessions – this was not a load test. The idea was to check that firewalls can handle several connections without bad performance (meshing up tables etc.).

- Test 1: 5 clients, 3 URLs, 5 cycles
- Test 2: 10 clients, 3 URLs, 10 cycles
- Test 3: 30 sessioner,3 URLs, 10 cycles

We tested one firewall at a time. It took between 60 – 90 minutes per firewall. To speed up the test the participants could set it up beforehand at the workshop, after that we just moved the test bed. In the same manner, if one vendor had a problem with e.g. filtering we could switch them out temporarily and te[illegible]

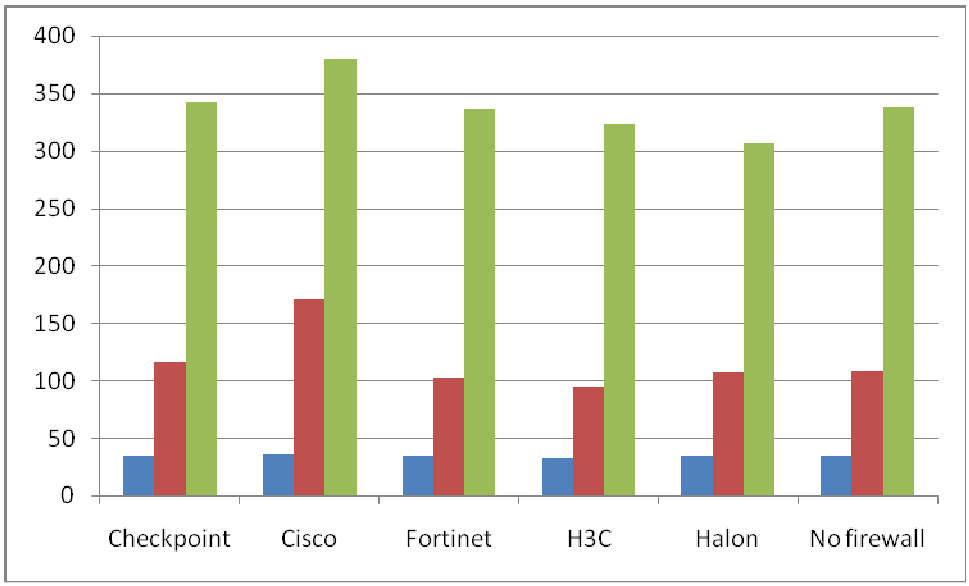
2.1 Vendors and equipment

- Checkpoint model UTM-1, model 130. Software r70.1
  - Set up by Certezza, Checkpoint declined to participate
- Cisco model ASA5505, software 8.2
- Fortinet Fortigate 111C, software v4.0MR1
- H3C, Secpath F1000E, 5.20 feature 3167
- Halon SX-150, software 1.4.0
- Juniper modelSSG320M, sw 6.1.0r2

3 Results

	IPv6 native	SPI setup ("diode")	IPv6 in log	IPv6 filter	Session test (secs)	Session Failures
Checkpoint	Ok	Ok	Ok	Ok	35 116 342	0
Cisco	Ok	Ok	Ok	Ok	36 170 380	0
Fortinet	Ok	Ok	Ok	Ok	35 102 337	0
H3C	Ok	Ok	Not verified in CLI-interface	Ok	32 95 323	0
Halon	OK	Ok	Ok	Ok	34 107 306	0
Juniper	Ok	Ok	Ok	Ok	No problems with 30 session.	0
No firewall	-	-	-	-	35 108 338	-

All firewalls performed well and could handle the number of session we tested 2009. They also scale well compared to "no firewall". The SPI set up just means that the firewall is set up as a diode, sessions that are initiated from the inside are permitted.



Graph: The session test, showing the download time in seconds (the shorter the better). Some vendors performed better than "no firewall", this is due to variations on the Internet.

Juniper is not present in the graph but had no problems with 30 sessions. We started with with Juniper and were trying to find out where the limit for the set up was. (100 sessions and 16 MB URL did not work, this could be due to hardware, the Internet connection or the internal Apache web server.)

3.1 Other comments

In 2008 we found that IPv6 was working well on most vendors in the test. This year´s workshop was a small step forward. IPv6 is now handled in the GUI on most brands, and is set up very similar to IPv4. A few comments:

Checkpoint model UTM-1, model 130. Software r70.1

- No web management via IPv6, but has SSH support for IPv6 (not tested)

Cisco model ASA5505, software 8.2

- The software now has GUI support for IPv6, last year just in the CLI

H3C, Secpath F1000E, 5.20 feature 3167

- IPv6 by CLI, no web GUI. H3C was nice and gave us an early release.

All vendors handle IPv6 in their logs and in the same way as IPv4 addresses work. This could not be verified on H3C, it could very well be because we did not understand the logging function fully.

We had no problems with DNS this year (the longer IPv6 address could be a problem because DNS packets become longer).

We did not have problems with RA, but we think the comment we made last year about this is still very applicable.

Setting up a workshop in this way is not just a way of testing. It is also a good way of achieving hands-on experience. IPv6 is a bit different and even though the participants had many years of experience it is easy to forget that ICMPv6 is different which affects filtering. We also referred to the arp-cache when we were trouble shooting (ARP does not exist in IPv6). Note that we made similar mistakes 2008. Be careful about IPv6 and ICMP.

We also found a problem with "bredbandskollen" (a site for performance testing). We were planning to use it for a small performance test, but this year it did not work in IPv6 only mode. It did work in IPv4+IPv6 mode, but then we could not be sure that IPv6 was used for the test. When testing we found that the speed was

Transmit: 71 Mbps

Receive: 94 Mbps

Not bad on a fast Ethernet connection. Compliments to the ISP!

3.2 Results 2008

The Halon had problems with filtering DNS and it was hard to filter ICMP in the test of 2008, the administrator had to know the ICMP type and code. On the other hand, the Halon machine impressed us with very good explanations of which rules had been invoked. The Snapgear could basically just translate in 2008so it was removed from the test.

Our impression is that IPv6 is as fast as IPv4 today, at least up to Fast Ethernet speed (the practical up/down speed was less than 100 Mbit/s in our test network). When checking with Sunet (Swedish University Network), they share this view.

We concluded 2008 that IPv6 support in firewalls is mature enough for test networks and 1st phase operation. By testing and using the equipment we will learn about addresses, prefixes and setting up IPv6 rules.

Equipment	C1 can reachIPv6 resources (DNS, HTTP, SMTP)	C1 could ping (ICMP) *	Filtering of addresses	Filtering of networks	Filtering ICMP	Speed up/down [Mbit/s]	Filtering and logging ”reject”, local log
Cisco ASA 5505	OK	OK	OK	OK	OK	65/80	OK
Cisco 2800 w/ IOS 12.4	OK	OK	OK	OK	OK	50/65	OK
Juniper ISG 2000	OK	OK	OK	OK	OK	75/90	OK
Monowall	OK	OK	OK	OK	OK	70/85	OK
Halon	OK	OK	Problems with filtering DNS	Same as address	Hard. Must know ICMP type and code	60/75	OK
3COM	OK	OK	OK	OK	OK	75/85	Logging? See comments

Table: Results from 2008

We also tested persistence in the simplest possible way: by pulling out the power plug. All units passed that test since they retained the IPv6 rules until power was restored.

Logging and administration worked better than expected. For example HTTP over IPv6 and SSH over IPv6 did work. We did not try to send logs to remote hosts. Initially we could not make administration over HTTP work on the Monowall using IPv6, but Håkan Carlsson later sent us a fix to correct this.

We found some issues with ICMP, DNS and RA. See below.

3.3 IPv6 test bed at IIS

The IPv6 test set up is available at .SE for test and verification even after this specific workshop. If you are interested in using it, please contact IIS.

3.4 What did we learn 2008?

- Firewalls are often routers too, and therefore send RA, Router Advertisement. This might pose a problem when firewalls advertise themselves as routers but have firewall rules that prevent them from forwarding packets. This can actually make firewalls work as small internal DoS-attacks.
- Organizations using ICMP rules for IPv4 will need to look through these rules. IPv6 nodes on the same link use Neighbor Discovery to detect each other's presence, determine each other's link-layer addresses, find routers and maintain reachability information about the paths to active neighbors. Neighbor Discovery is based on ICMPv6 and is roughly equivalent to a combination of several IPv4 protocols. The significance of this is that, while you may not handle Neighbor Discovery explicitly in your routers, ICMP rules might still affect it. If you define a rule like "accept ICMP echo reply" you might implicitly reject other ICMP packets – like the packets involved in Neighbor Discovery.
- Since DNS-packets are bigger in IPv6 than in IPv4 (over 512 bytes), you may have to adjust DNS filter rules.

3.5 Participants 2009

Johan Ivarsson - Certezza (Checkpoint distributor)

Mathias Wolkert - Certezza (Checkpoint distributor)

Håkan Nohre - Cisco

Janne Östling - Cisco

Jan Lundberg – Fortinet

Mike Blomgren – Fortinet

Rolf Börjesson – H3C/3Com

Jonas Falck – Halon

Erik Lax - Halon

Joakim Wall - Juniper

Jörgen Eriksson - .SE

Håkan Lindberg - B3IT

Patrik Wallström - .SE

4 Voices about IPv6

Vint Cerf, 30th October 2008.

Interviewer: When do you think IPv6 will receive broad adoption?

I wish I had an answer to this. I have been a strong supporter of IPv6 but it has been very slow to emerge on the Internet. IPv4 address space will be exhausted in 2010 by many estimates. Google has already begun to bring up services on IPv6 as well as IPv4. What is needed is for the ISPs of the world to implement the IPv6 protocols and to interconnect with each other in the same way they do for IPv4. We need a globally connected IPv6 network. There are alternatives being proposed, such as carrier grade NATs but I find these offerings weak compared to full IPv6 on an end to end basis. Of course, the transition period will require interim measures to allow IPv6-only devices to interact with IPv4-only servers (and peers, perhaps). Rendezvous sites that can convert between IPv4 and IPv6 will likely be common. Ultimately, I hope that the pain of trying to use interim measures will overcome the apparent inertia for the adoption of IPv6.

Magnus Kalkuhl, security expert Kaspersky Labs, 15th October 2008.

- We need IPv6, there is no alternative.

Patrik Fältström, Senior Consulting Engineer at Cisco.

- We don't even have a plan B, C or D.

5 Appendix: Extra IPsec test

We had some extra time and since Cisco and Fortinet both had IPsec we set up a VPN connection. We got it up and working after a few hours. The set up is included below. This should not be considered "best working practice", it was just the way we tested and we got it up…

5.1.1 Cisco ASA

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
!
resource policy
!
ip cef
no ip dhcp use vrf connected
!
ip dhcp pool POOL168
   network 192.168.0.0 255.255.255.0
   default-router 192.168.0.1
!
ipv6 unicast-routing
!
controller DSL 0
 line-term cpe
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 28800
crypto isakmp key gurkaipv6 address ipv6 2001:9B0:107:2002::2/128
!
crypto ipsec transform-set ESP3DESMD5 esp-3des esp-md5-hmac
!
crypto ipsec profile IPSECPROFILE
 set security-association lifetime seconds 28800
 set transform-set ESP3DESMD5
 set pfs group2
!
interface Tunnel0
 no ip address
 ipv6 address 2005::2/64
 ipv6 enable
 tunnel source FastEthernet0
 tunnel destination 2001:9B0:107:2002::2
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile IPSECPROFILE
!
interface FastEthernet0
```

```
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:9B0:107:2000::2/64
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
!
interface FastEthernet1
!
/OMITTED/
interface FastEthernet8
!
interface Vlan1
 ip address 192.168.0.1 255.255.255.0
 ipv6 address 2001:9B0:107:2001::1/64
!
no ip http server
no ip http secure-server
!
access-list 101 permit ospf any any
!
ipv6 route 2001:9B0:107:2003::/64 Tunnel0
ipv6 route ::/0 2001:9B0:107:2000::1
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end
```

5.1.2 FORTINET SETTINGS

The full configuration file for the Fortinet IPv6 setup is more than 50 pages long. Below is just a small part of the conf-file. One of the main problems we had with setting up the VPN was to set the firewalls to announce the networks over OSPF. The Fortigate needs a link local IPv6 address on the interface where OSPF information is exchanged.

```
config system interface
    edit "wan1"
        set vdom "root"
        set type physical
            config ipv6
                set ip6-address 2001:9b0:107:2002::2/64
                set ip6-allowaccess ping https ssh
            end
    next
    edit "switch"
        set vdom "root"
        set type physical
            config ipv6
```

```
                set ip6-address 2001:9b0:107:2003::1/64
                set ip6-allowaccess ping https ssh
            end
    next
    edit "v6_cisco"
        set vdom "root"
        set type tunnel
            config ipv6
                set ip6-address 2005::1/64
                set ip6-allowaccess ping
            end
        set interface "wan1"
    next
end

config firewall address6
    edit "all"
    next
    edit "2001:6b0:e:1::f:1"
        set ip6 2001:6b0:e:1::f:1/128
    next
    edit "2001:9b0:107:2001::/64"
        set ip6 2001:9b0:107:2001::/64
    next
end

config vpn ipsec phase1-interface
    edit "v6_cisco"
        set interface "wan1"
        set ip-version 6
        set local-gw6 2001:9b0:107:2002::2
        set dpd disable
        set dhgrp 2
        set proposal 3des-md5
        set remote-gw6 2001:9b0:107:2000::2
        set psksecret ENC
BAAAAJKgbMDMnQFrGSrzeidQzu/3OvVbY2kB02CGONtszU54gt3WcOQUSYGYPKzBLAMYBzohk8G
/pyrqmUSnU12XGCiw+hX/RbMC8N5YbnhI8c9b
    next
end
config vpn ipsec phase2-interface
    edit "v6_Cisco_p2"
        set dst-addr-type subnet6
        set phase1name "v6_cisco"
        set proposal 3des-md5
        set src-addr-type subnet6
        set dhgrp 2
        set keylifeseconds 28800
    next
end

config firewall policy6
    edit 1
        set srcintf switch
        set dstintf wan1
            set srcaddr "all"
            set dstaddr "all"
        set action accept
        set status disable
        set schedule "always"
            set service "ANY"
```

```
        set profile-status enable
        set logtraffic enable
        set profile "scan"
    next
    edit 2
        set srcintf wan1
        set dstintf switch
            set srcaddr "all"
            set dstaddr "all"
        set action accept
        set status disable
        set schedule "always"
            set service "ANY"
        set logtraffic enable
    next
    edit 3
        set srcintf switch
        set dstintf v6_cisco
            set srcaddr "all"
            set dstaddr "all"
        set action accept
        set schedule "always"
            set service "ANY"
        set logtraffic enable
    next
    edit 4
        set srcintf v6_cisco
        set dstintf switch
            set srcaddr "all"
            set dstaddr "all"
        set action accept
        set schedule "always"
            set service "ANY"
        set logtraffic enable
    next
end
config router static6
    edit 1
        set device "wan1"
        set gateway 2001:9b0:107:2002::1
    next
    edit 2
        set device "switch"
        set dst 2001:9b0:107:2005::/64
        set gateway 2001:9b0:107:2002::2
    next
    edit 3
        set device "v6_cisco"
        set dst 2001:9b0:107:2001::/64
    next
end

config router ospf6
        config area
            edit 0.0.0.0
            next
        end
        config ospf6-interface
            edit "to_cisco"
                set interface "v6_cisco"
            next
```

```
            edit "internal_lan"
                set interface "switch"
            next
        end
        set passive-interface "port1"
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "rip"
        end
        config redistribute "bgp"
        end
    set router-id 1.1.1.1
end
```