IPv6 support in firewalls

A report from .SE

by Håkan Lindberg and Tomas Gilså

Table Of Contents

1 Introduction

1.1 The report

During August and September 2008 seven firewalls were tested by .SE. This test was a part of the conference "Internetdagarna". The results from the tests are presented in this report.

1.2 Terms

DHCP, Dynamic Host Configuration Protocol
Technology to make many clients time-share a pool of IP addresses.

NAT, Network Address Translation
Technology to make many clients and even subnets share a single IP-address through internal address translation. NAT works on the Network layer, Layer 3, in the IP-stack by rewriting the address information in the IP packets.

1.3 References

**[1] SSAC report 021, ICANN Security and Stability Advisory Committe
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/rfc2461.txt

[4] http://www.rfc-editor.org/rfc/rfc5006.txt

1.4 About .SE

.SE (The Internet Infrastructure Foundation) is responsible for the top-level Swedish Internets 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.

2 Summary

This 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. Three more vendors submitted machines that were not IPv6-ready enough for our test.

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 one 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 tests indicates that IPv6 support is definitely good enough to start testing and for 1st phase operation.

We found that bad performance when processing IPv6-packets is a myth. Or an old truth.

2.1 Background

The Internet is running out of IPv4 addresses, by many estimates the IPv4 address space will be exhausted in 2010. 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.

2.2 Purpose

To see the status of IPv6-readiness among the vendors, and to document what works today. .SE (The Internet Infrastructure Foundation), that runs the top level domain .se, wanted to present this information as part of the conference Internetdagarna in Stockholm October 20-22, 2008. .SE also wanted to set a good example of IPv6-awareness and usage.

Throughout our work, the intention has been to do a gentle test. 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.

2.3 Who paid for this?

The vendors and some ISP's volunteered machines and time. Tele2 supplied us with IPv6 Internet connectivity. .SE paid for the setup, project management and documentation. The testing personnel volunteered.

2.4 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.

2.5 What is "IPv6 Ready"?

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

We later 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 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.

3 Testing

Figure 1: The test was set up at Tele2 in Stockholm. The testing personnel volunteered.

A Mac Mini running Ubuntu Linux was used as server and router. Macintoshes and Vista machines were used as clients. Since a Mac Mini has only one Ethernet interface, the LAN interfaces were connected over USB-2. This should work up to 100 Mbit/s, thus matching the connection to the ISP router.

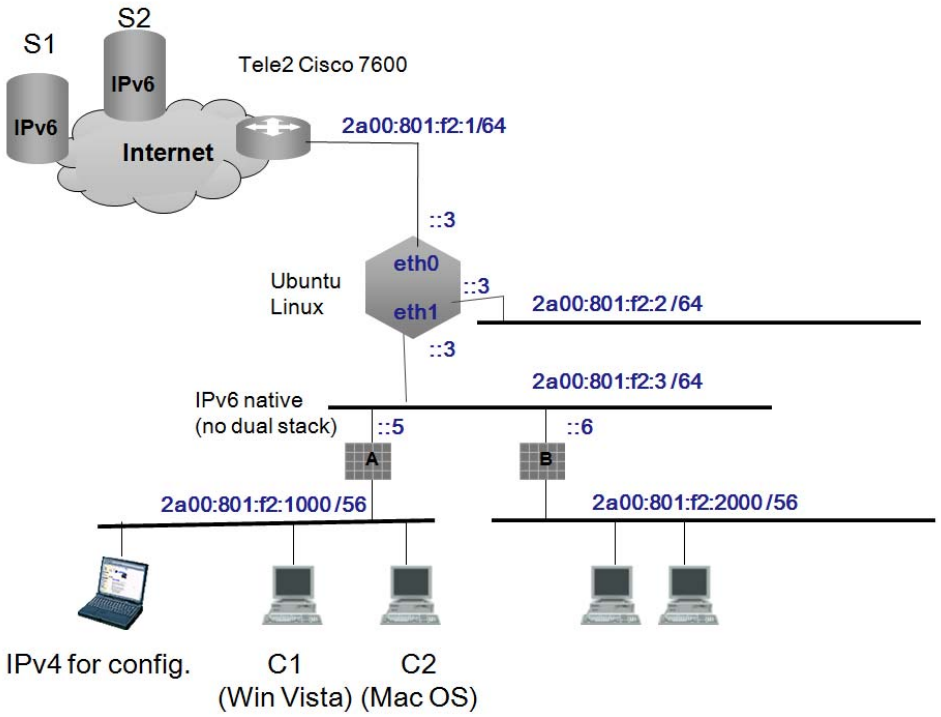

Figure 2: The test setup

The first test was to see if the machines supported an IPv6 interface and if different clients could ping each other and reach IPv6 resources via DNS, HTTP, SMTP and Ping (ICMP).

Next we tested to set firewall rules to filter addresses, networks and ICMP. Then we used the site ipv6.bredbandskollen.se to measure the speed up- and downstream. Finally we checked the filtering and logging of rejects.

3.1 Equipment

These machines were tested:

- 3Com MSR 50-40
- Cisco ASA 5505 (the machine that replaces the Pix)
- Cisco 2800 with IOS 12.4
- Halon SX 101
- Juniper ISG 2000
- Monowall 1.3b14 on Soekris hardware
- SnapGear SG650

We excluded a Linksys machine on the grounds that it could not edit access lists. Since it is built around Linux, you can probably make it work using IP-tables if you are enough of a Linux expert.

We also received a D-link switch with IPv6-support that we couldn't deploy because of the management software, so it was not tested. (The software needed Microsoft Access in a version we could not run on Windows Vista.)

3.1.1 POSITIVE FROM THE BEGINNING BUT ...

Some vendors were positive from the beginning but later declined to participate:

- Checkpoint / FW-1
- Extreme Networks
- Fortinet

Some other vendors declined from the very beginning, some for the obvious reason that they still had not implemented IPv6 in their equipment.

4 Results

All machines got an OK in all aspects, except Halon and Snapgear. The Halon had problems with filtering DNS and it was hard to filter ICMP, 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 so 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.

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

We conclude 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.

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.

4.1 What did we learn?

Each machine took one to two hours to set up and test. About half of the time was spent trouble-shooting. There are significant differences between IPv4 and IPv6 in setting up a local network. Once we got things to work, however, it worked fine.

During the tests we also realized the truth in the Internet Layers Robustness Principle as described in RFC 1122: Be liberal in what you accept, and conservative in what you send. It is easy for one misconfigured host to deny service to many users.

- 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.

4.2 Comments and some thoughts

There are still many things to discover about firewalls and IPv6, but compared to the situation in 1991 when the first commercial IPv4 services were sold to the public, we have much more general knowledge about networks now. Hopefully, adoption might therefore be quicker this time.

Is end-to-end communication a good idea? One expectation on IPv6 is that it will allow us to return to end-to-end communication, where all clients have unique and stable IP addresses.

What happens with viruses? Worms that scan the network for new hosts to infect will have to update their search algorithms significantly. And hackers might have problems to scan the vast address spaces that IPv6 provides.

4.3 Various problems

Some of the problems we encountered on different machines:

- ICMP was not enabled, preventing us from getting correct error messages and Neighbor Discovery packets.
- We had problem with Panda Antivirus and IPv6 on a few machines.
- When downloading a new boot image, the network flapped up and down for 40 minutes. We believe the firewall tried repeatedly to reach a new DHCP-server upgrade through the gateway.

- We made several typos inputting IPv6 addresses. In IPv6 the addresses should be handled by machines, they are much too complicated to be entered by humans. Sure, it is doable, but the error rate goes up. Or we need to skip the idea of using EUI-64 addresses.

- One of the devices under test probably had some load balancing function, making blocking of ipv6.sunet.se difficult when the IP-address moved.

- When stateful inspection was activated in one firewall, the service ipv6.bredbandskollen.se (online speed-checker operated by .SE) did not work properly.

- Windows Vista surprised us by advertising a different temporary IP address than the static address we had fed it.

5 Suggestions for further testing

Dual stack and practical migration from IPv4 to IPv6.

How to reach IPv6 services if your environment is IPv4? Including NAT-PT and TOTD.

How to migrate from one ISP to another while keeping your addresses and prefixes.

How should firewalls handle header extensions that are not standardized today?

Fragmentation and how it confuses firewalls

Strict or loose source routing

Tunneling

Checking for SPI functionality

How does IPSec (which is built into IPv6) affect performance? How does the number of sessions affect performance?

Masquerading

Port mapping

RFC 4193 Unique Local IPv6 Unicast Addresses

Delegated subnetting

Dividing addresses into PI and PA addresses, as in IPv4.

Home user equipment in the price range 1000 SEK (about 100 Euro), preferably with 802.11n functionality.

From the conference

Questions from the audience at the conference Internetdagarna were mainly about how to migrate, how to handle the technical stuff and some questions about which machines work with IPv6. One attendee also brought up the question of how to set up IPv6 in a SOHO environment.

6 Participants

Mikael Abrahamasson - Tele2

Tobias Andersson - Romab

Mikael Björn - SNUS

Rolf Börjesson - 3Com

Håkan Carlsson - Daemon Software

Jörgen Eriksson - .SE

Tomas Gilså - secretary

Mats Karlsson - SNUS, 3Com

Håkan Lindberg - B3IT

Mohammad Mahloujian - .SE

Håkan Nohre - Cisco

Joachim Orrblad - IP Solutions

Joakim Wall - Juniper

Patrik Wallström - .SE

7 Comments from the suppliers

7.1 3COM

3Com's mission is to provide customers worldwide with high quality, low-cost networking infrastructure solutions that enable the convergence of applications and emerging technologies into the network. 3Com is committed to IPv6 and has delivered several IPv6-based solutions the last years, particularly in China and Japan, through H3C Technologies Co. Limited (H3C), a company 100 percent owned by 3Com.

The MSR 50-40 is a powerful and advanced product with Gbit/s capacity. The firewall forwarding capacity is 1,5 Gbit/s. The product is Gold certified IPv6 Ready. The product supports the Network Address Translator-Protocol Translator (NAT-PT), the IPv6 Provider Edge router (6PE), the trans-IPv4 tunneling technology of IPv6, IS-IS Ipv6, BGP4+, MLDv1 and MLDv2.

Background from the test team: we could see that MSR 50-40 accepted log commands but we did not actually find the log. 3COM has later e-mailed us information about how the log could be checked. For more information about this matter, check with 3COM.

7.2 Cisco

Cisco is committed to IPv6. We have a long experience of supporting IPv6 in Cisco switches, routers and firewalls. We chose to participate with affordable firewall products for small business and remote offices (ASA5505 and Cisco 1800). This shows that an IPv6 firewall does not have to be expensive or complicated.

The test was done on a Cisco 2800, but the same software (version 12.4) run on e.g. Cisco 1803. Cisco 1803 was tested during the conference.

For more information on IPv6, see http://www.cisco.com/go/ipv6

7.3 Juniper

This test clearly shows Juniper Networks' commitment to new technologies and the ease of use of it. We have a reputation for predictable performance, excellent customer experience as well as standards-based open platforms that customers can implement smoothly in their network. Support for IPv6 is no exception. In the latest release of ScreenOS (6.2) we have added several enhancements and IPv6 features such as BGP for IPv6, Transparent Mode for IPv6, NSRP high-availability (HA) clusters using IPv6 (Active/Passive and Active/Active), DHCPv6 Relay and Multicast Listener Discovery (IPv6) - MLDv1. We will continue to develop this as it will be an important function in the future for high-performance businesses and organizations.

7.4 Halon

In accordance with this report it is known that filtering DNS can be a problem with the current firmware release, also it is hard to filter ICMP since it requires quite a bit more experience from the firewall administrator. Improvements and easier administration will be deployed in an upcoming firmware release.

Support for IPv6 is also available in our other products, SPG (Spam Prevention Gateway) and VSP (Virtual Spam Prevention). SPG and VSP prevents spammers and zombie networks from sending spam, virus and malicious attacks on ip connections level, providing customers clean, safe and business network usage. By providing IPv6 support it opens up

for a future safe networking without having to re-invest in new technology once IPv6 is more adopted.

Halon Security offers IT security products in network security and spam prevention since 2002. The products are developed on the market's most secure operating system, BSD, and have received multiple top ratings in media due to outstanding performance, dynamics, and innovative functionalities. Halon Security products are sold throughout Europe, Asia and North America. Halon Security is based in Gothenburg, Sweden.

For more information, visit http://www.halonsecurity.com.

8 Appendix

8.1 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.