Status of Open Source and commercial IPv6 firewall implementations

Dr. Peter Bieringer
AERAsec Network Services & Security GmbH
info@aerasec.de
http://www.aerasec.de/

European Conference on Applied IPv6 (ECAI6)
Cologne, Germany
September 6 - 7, 2007

Abstract

IPv6, the successor of IPv4, has been ready for production for quite some time. For security reason, firewalling in IPv6 is also an important requirement. This paper presents an overview of the status of Open Source and commercial implementations.

Introduction

With IPv4 nowadays, many client-to-server and most client-to-client communications are intercepted by gateways with address and port masquerading abilities, usually named Network (and Port) Address Translation (NAT, NAPT). This prohibits native client-to-client communication, if both peers are located behind such gateways. In this case, only special tunnelling techniques, like STUN (Simple traversal of UDP over NATs), which requires special servers located at the Internet, or other "firewall-piercing" methods can help to establish native and bidirectional client-to-client communication.

One of the goals of IPv6 is the re-introduction of bidirectional, native end-to-end communication without playing any tricks on gateways in between. Also, IPv6 has a large enough address space which should suffice for the next decades. Therefore NAT was left out by design, too.

Jumping back to IPv4, the initial intention of introducing NAT was the lack of IPv4 addresses for use in internal networks, while still allowing clients to open connections to the Internet via a hiding mechanism. It turned out to also protect internal networks against threats from the Internet, because under normal circumstances (bug-free stateful hiding-NAT implementation on the gateway) it's not possible for an outside node to connect to an internal host without any dedicated rule on the gateway. Therefore NAT results in some kind of automatic firewalling for IPv4. Today, this still holds, but attackers have learnt and moved on to the use of trojan horses or spyware, which open connections from the inside to the Internet ("phone home") and wait for instructions, e.g. attacking other internal hosts. Thus even with IPv4, gateway protection by itself no longer fulfils the real need, an additional host protection is necessary.

In addition, the required protection level for nodes is independent of the use of IPv4 or IPv6, because attackers could simply switch to IPv6, if it became public that the protection level is not as high as with IPv4. Also because of the re-establishment of end-to-end communication, the attacks would no longer need to employ trojan horses or spyware. The only positive aspect seems to be that scanning for active IPv6 addresses would become much more difficult because of the huge amount.

And finally, think about Microsoft Windows Vista, which enables IPv6 by default and tries to get native IPv6 connectivity using the TEREDO tunnel mechanism - out of the box! Henceforth, the need for IPv6 firewalling is real.

Status of implementations of IPv6 firewalls

Given the need for IPv6 capable firewalls, the status of available implementations is an important consideration in planning and during implementation of IPv6 networks. The rest of this paper presents the state of implementation of IPv6 support of the most popular firewall software.

Open Source based firewall frameworks

All important Open Source based firewall frameworks nowadays already support IPv6.

Linux netfilter

URL: http://www.netfilter.org/

Running on: Linux

The *netfilter* framework is located in the Linux kernel and controlled by user space binaries for maintaining the filter tables. Their names are “iptables” (IPv4) and “ip6tables” (IPv6). Stateless IPv6 support first occurs in stable kernel series 2.4.x (since January, 2001). Stateful IPv6 support was integrated into kernel 2.6.20 (released February, 2007) by switching from protocol depended connection tracking modules to protocol independent ones (also known as “xtables”), which can be used by IPv4 and IPv6 helper modules.

Further information regarding a useful IPv6 filter setup can be found in the Linux+IPv6-HOWTO (chapter firewalling/security).

IPFilter (IPF)

URL: http://coombs.anu.edu.au/~avalon/ip-filter.html

Current version: 4.1.24 (release Jul 8, 2007)

Running on: FreeBSD, OpenBSD, NetBSD, Apple Mac OS X, Sun Solaris and other BSD based OS, Linux

IPFilter supports stateful IPv6 packet filtering.

pf

URL: http://www.benzedrine.cx/pf.html

Running on: OpenBSD, FreeBSD, NetBSD

The development of *pf* was started in June, 2001 after licensing problems were identified with “IPFilter” in OpenBSD. It supports stateful IPv6 packet filtering.

ipfw

URL: http://www.freebsd.org/cgi/man.cgi?query=ipfw

Running on: FreeBSD, Apple Mac OS X

ipfw supports stateful IPv6 packet filtering.

Selection of Open Source based firewall products

Based on the above projects several Open Source firewall products exist. Some can be used out-of-the-box, some on-top of existing Open Source systems.

IPcop

URL: http://ipcop.org/

Current version: 1.4.15 (released Mar 10, 2007)

IPcop is a ready-to-use out-of-the-box Open Source firewall delivered as CD image. It's based on Linux kernel 2.4.x series and uses the built-in *netfilter* framework. Currently, it features no IPv6 support, nor does the roadmap mention any plans to include support.

firestarter

URL: http://www.fs-security.com/

Current version: 1.0.3 (released Jan 29, 2007)

firestarter is a personal client firewall for Linux systems using the built-in *netfilter* framework. Currently, it has no IPv6 support. Additionally, no information was found about future plans.

m0n0wall

URL: http://m0n0.ch/wall/

Current version: 1.231 (Apr 4, 2007)

m0n0wall is similar to IPcop a ready-to-use out-of-the-box Open Source firewall delivered as CD image. It's based on FreeBSD and uses the *IPFilter* framework. Currently it has no IPv6 support, also nothing related was found on the TODO.

pfSense

URL: http://pfsense.com/

Current version: 1.2-BETA-2 (Jul 4, 2007)

pfSense was derived from *m0n0wall* but based on OpenBSD and uses the *pf* filter framework. According to the CVS Trac Timeline support of IPv6 is under development.

Selection of Open Source and commercial UNIX operating systems with built-in firewall capabilities

To protect a node itself or a network behind a gateway, at least self-made firewall policies can be used. It is thus useful to know, which capabilities are available on Open Source operating systems.

Red Hat Enterprise Linux

URL: http://www.redhat.com/

Red Hat Enterprise Linux uses the kernel built-in *netfilter* framework for firewalling. The capability of IPv6 firewalling strongly depends on the used kernel version. Red Hat publishes major releases of Enterprise Linux usually after approx. 1.5 to 2 years, with updated kernel versions. Red Hat wants to keep the ABI and API stable in one major release, so during minor release updates, at least the kernel version would not be changed, instead only fixes and sometimes hardware drivers were backported.

Release	Publish in	Kernel version	Current package
RHEL 3	October 2003	2.4.21	2.4.21-50.EL
RHEL 4	February 2005	2.6.9	2.6.9-55.0.2.EL

RHEL 5	March 2007	2.6.18	2.6.18-8.1.8.el5

As already described in the *netfilter* section, stateful IPv6 firewalling was introduced in kernel 2.6.20. Therefore all current available versions of Red Hat Enterprise Linux only support stateless IPv6 firewalling. When release 6 will be published (expected end of 2008), stateful firewalling will be finally available for IPv6.

Note that RHEL3 has a bug regarding to IPv6 address representation in “ip6tables” (BZ#184359), which will not be fixed.

Fedora Linux

URL: http://fedoraproject.org/

Fedora (Core) Linux uses the kernel built-in *netfilter* framework for firewalling. The capability of IPv6 firewalling strongly depends on the used kernel version. Fedora releases updates for supported versions in short intervals, even kernel updates. Therefore users are more or less near the leading edge of kernel developing.

Release	Published in	Initial released kernel version	Current kernel version (at time of writing)
Fedora Core 6	October 2006	2.6.18-1.2798.fc6	2.6.20-1.2962.fc6
Fedora 7	May 2007	2.6.21-1.3194.fc7	2.6.22.1-41.fc7

Fedora Core Linux 6 started with a kernel which supports only stateless IPv6 firewalling. Meanwhile during updates this has changed to stateful. Fedora Linux 7 already started with a newer kernel version and got stateful IPv6 firewalling support since beginning (but not enabled, see *system-config-securitylevel* below).

Debian GNU/Linux

URL: http://debian.org/

The Debian project's GNU/Linux operating system builds on the kernel's *netfilter* framework for firewalling. The currently stable release, Debian 4.0 “etch” comes with the Linux kernel version 2.6.18 and thus only supports stateless IPv6 firewalling. The forthcoming Debian 4.1 “lenny” release will include stateful IPv6 firewalling, and a kernel update to “etch” is planned in early 2008 with “etch r3”.

Ubuntu Linux

URL: http://ubuntu.com/

The current Ubuntu release 7.04 “feisty” ships with the 2.6.20 kernel and thus supports stateful IPv6 firewalling.

Other Linux distributions

Stateful IPv6 firewalling depends on the kernel version used. Thus it is relatively easy to determine whether a given Linux distribution supports it.

BSD based Open Source operating systems

As already shown, all three filter frameworks for BSD based operating systems have stateful IPv6 support. At least one can be used on FreeBSD, NetBSD, OpenBSD or Mac OS X.

Sun Solaris

URL: http://www.sun.com/software/solaris/

Sun Solaris has supported IPv6 since version 8. Usually the *IPFilter* framework from BSD is used here. Currently, no release supports IPv6 packet filtering, but it is planned for Solaris 10 U4.

Open Source tools for filter generation

It's more or less hard to create a well-working and secure filter rule set for Open Source based firewall frameworks. Some tools were developed to put an abstraction layer in between. Objects, services and rules can be defined in a policy, and the tool converts it afterwards to a working filter setup. The layout and quality, which can be sometimes discussable, strongly depends on the used tool.

system-config-securitylevel

URL: http://fedoraproject.org/wiki/SystemConfig/securitylevel

Version: 1.7.0-5.fc7 (released Aug, 2 2007)

Supports: *netfilter* on Red Hat Enterprise Linux / Fedora (Core) Linux

system-config-securitylevel is a simple tool for creating a lightweight filter setup. It supports some built-in services. IPv6 support is included, but *lokkit* (the underlying rule generator) creates only stateless rule in older releases (BZ#244729) and uses still wrong ICMPv6 messages for rejects (BZ#214117). The tool can't create a complex ruleset, but for a node protection, it's mostly well enough.

fwbuilder

URL: http://www.fwbuilder.org/

Supports: *netfilter*, *IPFilter*, *pf*, Cisco PIX, Cisco router ACL

Version: 2.1.12 (released Jun 5, 2007)

fwbuilder is a graphical tool with an object and policy database. It can create a filter setup for several frameworks and also commercial firewall and router products. It still has no IPv6 support, also nothing was found about plans for support it in the future.

ip-firewalling

URL: ftp://ftp.aerasec.de/pub/linux/ip-firewalling/

Supports: *netfilter* on at least Red Hat Enterprise Linux / Fedora (Core) Linux and OpenWRT

Version: 0.2.1 (released Jul 5, 2007)

ip-firewalling is a script framework (initscript, shell written library, configuration file) for creation of a filter setup, developed by the author. It is in productive use on his private systems as well as on systems of AERAsec Network Services and Security GmbH and part of their customers. It supports IPv6 depending on the used kernel version stateless or stateful. In addition, it can create an equal filter setup for IPv4 and IPv6 in an abstract manner (ICMP type/code mapping included), keeping the IPv6 overhead small.

Commercial firewall products for gateways

Beyond Open Source based frameworks, tools and products, also commercial firewall products are available with IPv6 support.

Check Point FW-1

URL: http://www.checkpoint.com/

Check Point began to support IPv6 in FW-1 NG R54, first on Sun Solaris and Nokia IPSO only, nowadays also on their “SecurePlatform” (a stripped and slicely modified Red Hat Enterprise Linux 3 using kernel 2.4.21). Unfortunately, there are still bugs and caveats around.

Evaluated version: FW-1 NGX R65 on “SecurePlatform” (“SPlat”)

Status:

System configuration	“SPlat” still misses support of persistent IPv6 configuration via “sysconfig” IPv6 interface, routing and perhaps tunneling configuration must be done by storing related commands into /etc/rc.d/rc.local.user
Firewalling	Support of IPv6 firewalling (at least active & passive FTP is stateful) exists
Policy Editor (SmartDashboard)	Support of dedicated IPv6 host and network objects exists Only firewall objects can have IPv4 & IPv6 addresses, other objects need to be defined independently (one for IPv4, one for IPv6) Using mixed objects (IPv4 and IPv6) in one rule requires this for source and destination - otherwise the policy compiler throws an error (workaround: [adding a dummy IPv6 host object] to related rules)
Logging (SmartTracker)	Logging of IPv6 traffic exists, but also independently, means IPv4 and IPv6 source/destination appear in different columns Description of unknown services is currently improper
Intrusion prevention system (SmartDefense)	Supports IPv6 Currently logs strange IPv4 instead of IPv6 addresses on IPv6 events

Outlook:

- Known bugs will be fixed in R65 IPv6Pack, but at this time, no release date is known

Fortinet FortiGate

URL: http://www.fortinet.com/

Fortinet began to support IPv6 on FortiGate in FortiOS 2.8, a major step was made in FortiOS 3.0 (released in 2006)

Evaluated version: 3.00 MR5 build 0601 (inofficial build from June, 2007) on a FGT-100

Status:

System configuration	Configuration is currently only supported via CLI only and missing in WebUI Supports dedicated IPv6 interface, routing and tunneling configuration IPv6 interface can be enabled for sending router advertisements Supports IPv6 IPsec (according to documentation, IPv4-in-IPv6 and IPv6-in-IPv4 is possible)
Firewalling	Support of basic IPv6 firewalling (at least active & passive FTP is stateful) exists Unlike to IPv4, transparent content filtering (URL, AV for HTTP) is currently not supported
Policy Editor	Dedicated policy for IPv6 is required, only supported via CLI only
Diagnose	“diag debug flow” currently does not support IPv6

Outlook:

- FortiOS v4, planned for Q2/Q3 2008 will support full content inspection for IPv6 (URL, AV filtering etc.)

Interesting documents:

- FortiGate IPv6 Support

Juniper SSG

URL: http://www.juniper.net/

Juniper acquired NetScreen in 2004, taking over the since 2003 existing IPv6 support. Improvements were made in ScreenOS 6.0.0 (release in 2007), available on SSG5, SSG20 and NS-5000.

Evaluated version: ScreenOS 6.0.0r1.0 on a SSG20

Status:

General	After activation of IPv6, configuration is supported via CLI and WebUI
System configuration	Supports dedicated IPv6 interface, routing and tunnelling configuration IPv6 interface can be enabled for sending router advertisements Supports DHCPv6, NAT-PT and IPsec
Firewalling	Support of basic IPv6 firewalling (at least active & passive FTP is stateful) exists Unlike to IPv4, transparent content filtering (URL, AV for HTTP) is currently not supported
Policy Editor	Supports IPv4 and IPv6, but a rule can contain only IPv4 or IPv6 objects
Intrusion prevention system (Screening)	Ping Size Limiter currently does not detect large IPv6 ping

Outlook:

- The next release of ScreenOS (6.0r2) will support IPv6 on the ISG 1000 device

Interesting documents:

- Concepts & Examples ScreenOS Reference Guide: Vol 14, Dual-Stack Architecture with IPv6
- ScreenOS 6.0 IPv6 CLI Reference Guide: Command Descriptions

Cisco Adaptive Security Appliance (ASA)

URL: http://www.cisco.com/

Cisco starts with support of IPv6 on ASA (the successor of PIX firewall) in version 7.0 (release in May, 2005)

Evaluated version: ASA 8.0(2) (released Jul, 2007)

Status:

General	After activation of IPv6, configuration is supported via CLI only, WebUI and other GUI tools are still not IPv6 capable
System configuration	Supports dedicated IPv6 interface and routing configuration IPv6 interface can be enabled for sending router advertisements
Firewalling	Support of basic IPv6 firewalling (at least active & passive FTP is stateful) exists ICMP is stateful, if added as “inspect icmp” to “policy-map global_policy/class inspection_default” - very recommended to allow PTMU discovery, which is mandatory in IPv6
Policy Editor	Dedicated access lists are required for IPv6 “access-group” can be used to bind one IPv6 and one IPv4 access list per interface
Intrusion prevention system („inspect“)	Current inspection engines with IPv6 support: FTP, HTTP, ICMP, SIP, SMTP, TCP, UDP

Interesting documents:

- Cisco ASA - Configuring IPv6

Phion Netfence

URL: http://www.phion.com/

Phion Netfence is a Linux based firewall with their own programmed firewall filter engine (unrelated to *netfilter*

framework). It's currently based on 2.4.x kernel series and does not support IPv6 at the moment. However, a major update is planned for mid of 2008, changing to 2.6.x kernel series and supporting IPv6 then.

Commercial products for endpoint security

As already stated in the introduction, IPv6 re-establishes native end-to-end communication. Therefore, a local firewall would be required on each hosts to prevent unwanted connections from the Internet.

While on Open Source based systems the same filter framework can be used on gateways and hosts, on commercial systems mostly commercial products are required. On Microsoft Windows XP, IPv6 must be still manually enabled, but on Microsoft Windows Vista is IPv6-enabled by default. This finally triggered software vendors to support IPv6 in their personal firewall software to keep the protection level up. Following tests were done on Microsoft Windows XP, with following pre-requirements: incoming “echo-requests” are allowed in Microsoft Windows built-in firewall:

- IPv6 ping from host to Internet
- IPv6 ping from Internet to host
- Internet Explorer browsing to http://ipv6.aerasec.de/ (check IPv6 connectivity)
- Internet Explorer browsing to http://www.eicar.org/download/eicar_com.zip (check for IPv4 transparent HTTP-AV)
- Internet Explorer browsing to http://www.ipv6.bieringer.de/eicar/eicar_com.zip (check for IPv6 transparent HTTP-AV)
- Restrict IPv6 access via rule

Just for interest, the built-in Anti-Virus engine for transparent HTTP scanning was tested with IPv6, if available.

Microsoft Windows XP built-in firewall

URL: http://www.microsoft.com/

Microsoft Windows XP has a built-in firewall with some filter capabilities for incoming connection requests and ICMP traffic.

Tested filter ruleset: default, note that the built-in firewall has no transparent HTTP-AV included.

Test results:

„IPv6 echo request“ from host to Internet	works
„IPv6 echo request“ from Internet to host	works (can be controlled by dedicated config option)
Internet Explorer browsing to http://ipv6.aerasec.de/	works via IPv6
Restriction of IPv6 access via rule	IPv6 addresses not supported in Windows Firewall exceptions

Summary:

- IPv6 support available
- Dedicated ICMP type/code filter matches at least IPv4 and IPv6 “echo-requests”
- Restrictions of source addresses for local running services currently misses IPv6 support

Kaspersky Internet Security 7.0

URL: http://www.kaspersky.com/

Kaspersky Internet Security is a combination of a personal firewall and Anti-Virus solution including transparent HTTP traffic analysis.

Evaluated version: 7.0.0.124 (released Jun 27, 2007)

Filter ruleset: default

Test results:

IPv6 ping from host to Internet	works
IPv6 ping from Internet to host	works, also, if „block all“ of Kaspersky Internet Security in enabled (instead of IPv4)
Internet Explorer browsing to http://ipv6.aerasec.de/	works via IPv6
Internet Explorer browsing to http://www.eicar.org/download/eicar_com.zip	works, virus detected by Web-Anti-Virus
Internet Explorer browsing to http://www.ipv6.bieringer.de/eicar/eicar_com.zip	works, but virus detected by File-Anti-Virus
Restriction of IPv6 access via rule	Not supported

Summary:

- Firewall: does not support IPv6 (traffic passes by)
- Web-Anti-Virus does not support IPv6

Outlook:

- Vendor statement (Jul 7, 2007): IPv6 support is planned for “Maintenance Pack 1” for version 7, probably released in 2 months.

F-Secure Client Security 7

URL: http://www.f-secure.com/

F-Secure Client Security is a combination of a personal firewall and Anti-Virus solution including transparent HTTP traffic analysis.

Evaluated version: 7.10beta build 169 (released Jul 2, 2007)

Test results:

IPv6 ping from host to Internet	works if „allow all“ is enabled or IPv6 is explicitly allowed by policy
IPv6 ping from Internet to host	works until „block all“ of F-Secure Client Security is enabled
Internet Explorer browsing to http://ipv6.aerasec.de/	works via IPv6
Internet Explorer browsing to http://www.eicar.org/download/eicar_com.zip	works, virus detected by real-time web anti-virus engine
Internet Explorer browsing to http://www.ipv6.bieringer.de/eicar/eicar_com.zip	works, but virus detected by file anti-virus engine
Restriction of IPv6 access via rule	Not supported for custom rules

Summary:

- Firewall: supports IPv6, IPv6 can be completely blocked
  - No support of IPv6 addresses in custom rules
- Web Anti-Virus engine does not support IPv6

Outlook:

- Vendor statement (26.07.2007): IPv6 support for custom rules will be supported in final version, release planned for September/October 2007.

Other personal firewalls

A short test of following versions of products do not show any IPv6 support, traffic passes by:

- Sunbelt Kerio firewall, Version: 4.5.916.0, http://www.sunbelt-software.com/
- ZoneLabs ZoneAlarm, Version: 7.0.362.000, http://www.zonealarm.com/

Conclusion

IPv6 was defined in 1996, implementation started soon afterwards in some operating systems and was improved and updated to changed standards over time. Support of IPv6 firewalling is a lot behind, e.g. *netfilter* framework in Linux kernel needed 6 years from stateless to stateful IPv6 support. Commercial vendors of firewall solutions also need a long time for implementation, mostly because of missing market driven development. This has caused a major delay in global IPv6 use by pushing the henn-egg-problem forward on time scale.

Today, there is a speed-up caused by the roll-out of Microsoft Windows Vista at least on commercial software for client security. But they still lack behind at the moment, features are missing in comparison to IPv4 support.

In the domain of gateway security, all tested implementations currently support IPv4 and IPv6 using separate objects and mostly separate rules. This makes no real sense for the future, because object and policy maintenance would become harder. So there is still some work to do for firewall vendors and for sure for Open Source tools to keep IPv4 and IPv6 filter setup generation more abstract from defined objects and policy.

Credits

Credits to Benedikt Stockebrand for invitation to this conference and to Martin F. Krafft for reviewing this paper and for supplying information about Debian related distributions. Major credits to the author's current employer AERAsec Network Services and Security GmbH for let him spend time on creating this paper and supplying with hard- and software. Also a thankyou must be given to distributor ComputerLinks and vendors Juniper & Cisco for supplying with appliances.

About the author

Dr. Peter Bieringer, born in 1968, had studied Physics at the TU Munich/Germany (finished 1994) and append a PhD on the University of Federal Army Forces in Munich in semiconductor analysis (finished 1999). During this time, the author got in contact with the Internet by administration of the institute's Local Area Network. A request for designing a course on IPv6 in 1996 was the trigger for his IPv6-related work. After a 15 month job position covering system administration and network consulting, he joined AERAsec Network Services and Security GmbH in September 2000 as security consultant and trainer for several courses including one about IPv6. Network services offered by AERAsec are IPv6-enabled since a usable and stable implementation exists. The author is also publisher of several IPv6 related documents on the World Wide Web like the 'IPv6 & Linux - HowTo' and its successor 'Linux IPv6 HOWTO', 'IPv6 & Linux - Current Status' and as co-maintainer its successor 'Current Status of IPv6 Support for Networking Applications'. Also he programs the tool 'ipv6calc' and developed the IPv6 support in 'initscripts', which is used in Red Hat (Enterprise) Linux / Fedora (Core) and clones. In addition he is co-founder and core member of the 'Deep Space 6' project and a member of the 'German IPv6 Task Force'.

The author can be also contacted by private e-mail address pb@bieringer.de, for more information take also a look on his homepage http://www.bieringer.de/pb/.