Status of Open Source and commercial IPv6 firewall implementations

Dr. Peter Bieringer

AERAsec Network Services & Security GmbH
info@aerasec.de

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

Contents

- Reasons for firewalling in IPv6
- Open Source based firewall frameworks
- Open Source based firewall products
- Open Source and commercial UNIX operating systems with built-in firewall capabilities
- Open Source tools for filter generation
- Commercial firewall products for gateways
- Commercial products for endpoint security
- Summary & Outlook

About me

- **Living in Munich (Germany)**
- **Employee of *AERAsec Network Services and Security GmbH* (since 2000)**
  - Focussing on IT security and network consulting
  - Trainer for IPv6, TCP/IP and others
- **Co-founder and core member of *Deep Space 6***
- **Member of the German IPv6 Task Force**
- **Author of the Linux IPv6 HowTo and others**

Reasons for firewalling in IPv6

Reasons for firewalling in IPv6

- **In IPv4 today, NAT no longer really protects a node**
  - STUN used as “firewall piercing” method for bidirectional native end-to-end communication
  - Everything (else) is tunneled over HTTP(S)
    - SSL-VPN
    - Trojans and other software will “phone home” all the time
- **In IPv6, NAT was left-out by design**
  - Re-introduction of bidirectional native end-to-end communication defined as a goal of IPv6

Reasons for firewalling in IPv6

- **IPv6 enabled client gets a global IPv6 address**
  - Automatically by
    - Receiving a router advertisement
  - Pseudo-automatically by
    - TEREDO tunneling (Microsoft Windows Vista or XP SP2)
    - 6to4, ISATAP or other tunneling methods

  ➔ Easier to attack, but harder to discover
- **Anyway, protection level for IPv6 must be equal to the established one in IPv4**
  - Security policy must be fulfilled!

  ➔ IPv6 firewalling on each node is required!

Status of IPv6 support
in
Open Source based firewall frameworks

Open Source base firewall frameworks

- **Linux netfilter** **http://www.netfilter.org/**
  - 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)
    - Switching from protocol depended connection tracking modules to independent ones (also known as “xtables”)
      - Can be used by IPv4 and IPv6 helper modules
  - Information about a useful IPv6 filter setup can be found in the Linux+IPv6-HOWTO (chapter firewalling/security)

Open Source base firewall frameworks

- **IPFilter (IPF)** **http://coombs.anu.edu.au/~avalon/ip-filter.html**
  - Running on: FreeBSD, OpenBSD, NetBSD, Apple Mac OS X, Sun Solaris and other BSD based OS, Linux
  - Current version: 4.1.24 (release Jul 8, 2007)
    - Supports stateful IPv6 packet filtering
- **pf** **http://www.benzedrine.cx/pf.html**
  - Running on: OpenBSD, FreeBSD, NetBSD
  - Supports stateful IPv6 packet filtering
- **ipfw** **http://www.freebsd.org/cgi/man.cgi?query=ipfw**
  - Running on: FreeBSD, Apple Mac OS X
  - Supports stateful IPv6 packet filtering

Status of IPv6 support

in

Open Source based firewall products

Open Source based firewall products

- **IPcop** **http://ipcop.org/**
  - Ready-to-use out-of-the-box Open Source firewall
    - Based on Linux kernel 2.4.x series, using the built-in netfilter framework
  - Current version: 1.4.15 (released Mar 10, 2007)
    - No IPv6 support and also not mentioned on roadmap
- **firestarter** **http://www.fs-security.com/**
  - Personal client firewall for Linux systems
    - Using the built-in netfilter framework
  - Current version: 1.0.3 (released Jan 29, 2007)
    - No IPv6 support and nothing was found about future plans.

Open Source based firewall products

- **m0n0wall** **http://m0n0.ch/wall/**
  - Ready-to-use out-of-the-box Open Source firewall
    - Based on FreeBSD and uses the IPFilter framework
  - Current version: 1.231 (Apr 4, 2007)
    - No IPv6 support, also nothing related was found on the TODO
- **pfSense** **http://pfsense.com/**
  - Derived from m0n0wall
    - But based on OpenBSD and uses the pf filter framework
  - Current version: 1.2-BETA-2 (Jul 4, 2007)
    - No IPv6 support, but according to CVS Trac Timeline under development

Status of IPv6 support

in

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

Linux based Operating Systems

- **Red Hat Enterprise Linux** **http://www.redhat.com/**

Release	Published in	Used kernel version
3	October 2003	2.4.21
4	February 2005	2.6.9
5	March 2007	2.6.18

  - Uses kernel's built-in netfilter framework for firewalling
  - No support of stateful IPv6 firewalling in current versions
  - Stateful IPv6 firewalling finally expected in release 6 (expected end of 2008)

Linux based Operating Systems

- **Fedora Linux** **http://fedoraproject.org/**

Release	Published in	Initial kernel vers.	Current kernel vers.
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

  - Uses kernel's built-in netfilter framework for firewalling
    - Fedora Core Linux 6 started with stateless IPv6 firewalling support, but got now stateful
    - Fedora Linux 7 has stateful IPv6 firewalling support
  - Probably stateful IPv6 firewalling is not enabled, see *system-config-securitylevel* later

Linux based Operating Systems

- **Debian GNU/Linux** **http://debian.org/**
  - Uses kernel's built-in netfilter framework for firewalling
  - Debian 4.0 “etch” comes with Linux kernel version 2.6.18
    - Only supports stateless IPv6 firewalling
    - Kernel update to “etch” is planned in early 2008 with “etch r3”
  - Debian 4.1 “lenny” will include stateful IPv6 firewalling
- **Ubuntu Linux** **http://ubuntu.com/**
  - Ubuntu release 7.04 “feisty” ships with the 2.6.20 kernel
    - Supports stateful IPv6 firewalling

BSD based Operating Systems

- **BSD based Open Source operating systems**
  - 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** **http://www.sun.com/software/solaris/**
  - Supports IPv6 since version 8
  - Usually using the IPFilter framework from BSD
  - Currently, no release supports IPv6 packet filtering
    - Planned for Solaris 10 U4

Status of IPv6 support

in

Open Source tools for filter generation

Open Source tools for filter generation

- **system-config-securitylevel**

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

  - Supports: netfilter on Red Hat Enterprise Linux / Fedora (Core) Linux
  - Simple tool for creating a lightweight filter setup
  - Version: 1.7.0-5.fc7 (released Aug, 2 2007)
    - IPv6 support is included
    - “lokkit” (the underlying rule generator) uses still wrong ICMPv6 messages for rejects
  - Older versions create only stateless rules

    ➔ Regeneration of filter setup recommended for Fedora (Core) Linux

Open Source tools for filter generation

- **fwbuilder** http://www.fwbuilder.org/
  - Supports: netfilter, IPFilter, pf, Cisco PIX, Cisco router ACL
  - Graphical tool with an object and policy database
    - Create filter setup for several frameworks and also commercial firewall and router products
  - Version: 2.1.12 (released Jun 5, 2007)
    - No IPv6 support, also nothing was found about future support

Open Source tools for filter generation

- **ip-firewalling** ftp://ftp.aerasec.de/pub/linux/ip-firewalling/
  - Supports: netfilter on at least Red Hat Enterprise Linux, Fedora (Core) Linux and OpenWRT
  - Script framework (initscript, shell written library, configuration file) for creation of a filter setup
  - Version: 0.2.1 (released Jul 5, 2007)
    - Supports IPv6 depending on the used kernel version stateless or stateful
    - Can also create an equal filter setup for IPv4 and IPv6 in an abstract manner (ICMP type/code mapping included), keeping the IPv6 overhead small

Status of IPv6 support

in

Commercial firewall products for gateways

Commercial gateway firewall products

- **Check Point FW-1** **http://www.checkpoint.com/**
  - Support of IPv6 started in FW-1 NG R54 on Sun Solaris and Nokia IPSO
  - Evaluated version: FW-1 NGX R65 on “SecurePlatform” (“SPlat”)
    - Supports IPv6 firewalling in common ruleset
    - “Splat” still misses support of persistent IPv6 configuration
    - Some strangeness in logging, policy editor and intrusion prevention
  - Outlook:
    - Known bugs will be fixed in R65 IPv6Pack, but at this time, no release date is known

Commercial gateway firewall products

- **Fortinet FortiGate** http://www.fortinet.com/
  - Support of IPv6 started 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
    - Supports IPv6 firewalling in separate ruleset
    - IPv6 system and firewall configuration only via CLI
    - Transparent content filtering is not supported for IPv6
  - Outlook:
    - FortiOS v4, planned for Q2/Q3 2008 will support full content inspection for IPv6 (URL, AV filtering etc.)

Commercial gateway firewall products

- **Juniper SSG** **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
    - Supports IPv6 firewalling in separate ruleset
    - IPv6 system and firewall configuration via CLI and WebUI
    - Transparent content filtering is not supported for IPv6
  - Outlook:
    - The next release of ScreenOS (6.0r2) will support IPv6 on the ISG 1000 device

Commercial gateway firewall products

- **Cisco Adaptive Security Appliance (ASA)**
  http://www.cisco.com/
  - 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)
    - Supports IPv6 firewalling
    - IPv6 system and firewall configuration only via CLI
    - IPv6-ICMP is stateful, if added as “inspect icmp” to default inspection class (required to enable PMTU discovery)
    - Separate ruleset for IPv4 and IPv6 can be bind to each interface

Status of IPv6 support

in

Commercial products for endpoint security

Commercial endpoint security products

- **Kaspersky Internet Security 7.0**
  http://www.kaspersky.com/
  - Combination of a personal firewall and Anti-Virus solution including transparent HTTP traffic analysis
  - Evaluated version: 7.0.0.124 (released Jun 27, 2007)
    - 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

Commercial endpoint security products

- **F-Secure Client Security 7** http://www.f-secure.com/
  - Combination of a personal firewall and Anti-Virus solution including transparent HTTP traffic analysis
  - Evaluated version: 7.10beta build 169 (released Jul 2, 2007)
    - 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

Summary & Outlook

Summary

- **IPv6 was defined in 1996**
  - Implementation started soon afterwards in some operating systems
    - Improvements and updates to changed standards over time
- **But support of IPv6 firewalling is a lot behind**
  - Open Source solutions
    - Stateful IPv6 firewalling
      - For Linux finally available in 2007
      - BSD related frameworks got this already earlier
  - Commercial solutions
    - Still work-in-progress

Outlook

- **Commercial software for client security**
  - Speed-up caused by the roll-out of Microsoft Windows Vista
  - Features are still missing in comparison to IPv4 support
- **Open Source and commercial gateway security**
  - All tested implementations support IPv4 and IPv6
    - But still using separate objects and mostly separate rules
      - Hard to maintain objects and policy in the future

    ➔ Open issue for vendors and some Open Source tools!

Thank you for listening!

Q&A

Credits to

Benedikt Stockebrand (invitation)

Martin F. Krafft (review & suggestions)

AERAsec Network Services and Security GmbH (supplying with hard- and software)

Distributor ComputerLinks and vendors Juniper & Cisco (for supplying with appliances)

Contact Information

pb@bieringer.de

http://www.bieringer.de/pb/

http://www.bieringer.de/linux/IPv6/

peter@deepspace6.net

http://www.deepspace6.net/

info@aerasec.de

http://www.aerasec.de/