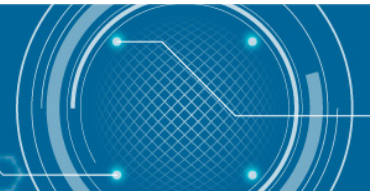




US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM



Technical Information Paper TIP-12-248-01

Fundamental Filtering of IPv6 Network Traffic

Tim Stahl, Robert Renstrom, Michael King

September 5, 2012

Notification

This report is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this report, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the report.

The DHS does not endorse any commercial product or service, including the subject of the analysis in this report. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

The display of the DHS official seal or other DHS visual identities, including the US-CERT name or logo, on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security, including US-CERT. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS, US-CERT, or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

Overview

This paper begins a series of IPv6 TIPs to assist network defenders with the security implications of IPv6 deployment. This document will not duplicate existing published documentation concerning the theoretical aspects of IPv6 based network security, but will focus more on the first steps of a “HowTo” for network defenders.

You will find non-vendor specific provisioning of IPv6 based network traffic filtering via basic types of traffic blocking suggestions, identification of deprecated addresses, a brief discussion on ICMPv6, tunneling and additional topics to consider when developing an IPv6 implementation strategy.

Implementing IPv6 introduces a myriad of challenges including providing security at network borders as well as internal controls. By design, IPv6 enables each host direct connection to the internet with a completely routable address.

Please ensure each recommendation in this TIP is vetted in a test network prior to implementation in your production environment.

Details

The following recommendations are not written in specific firewall or IDS/IPS syntax because of the great variety of infrastructure filtering devices and software with differing syntax that are available. However, using the guidance provided below for the types of traffic and addresses, an administrator should be able to construct the appropriate rule syntax for their environment. It is not meant to be authoritative for all IPv6 network security; it is merely a baseline if nothing has been done to secure your network from IPv6 security threats.

Though IPv6 differs greatly from IPv4, many of the most basic security concepts still apply. All in or outbound traffic that is not specifically permitted should be blocked by default. No traffic that is deemed by a protocols standard as experimental, unroutable, or undefined should be allowed to cross the network boundary in either direction. These are the types of security considerations that will be addressed in this document.

There are a great variety of capabilities for infrastructure devices and their abilities to filter IPv6 traffic. If an organization is connected to the internet, it needs the network infrastructure capable of filtering IPv6 traffic. Though many vendors advertise that their devices support IPv6, but the level of support and security implementation may not be the same as implemented in their IPv4 stack – IPv6 security needs to be thoroughly investigated and tested independent of IPv4 capabilities for each device. This also applies to those networks that do not allow IPv6 traffic to enter or traverse the network.¹

IPv6 continues to evolve and mature and vendor implementations to comply with the applicable RFCs will vary. Changes will continue to occur to the 150 or so IETF standards that govern it. This will occur at a faster pace than the IT world has ever had to deal with before. This TIP will be a living document, with revisions reflecting both changes to the standard as well as lessons learned.

Note: The numbers in superscript following an alphanumeric text string are footnoted references and should not be considered part of the IPv6 address.

Access Control

As the digital world transitions to using IPv6, administrators need to understand how to implement security based access controls. Therefore, a common baseline is needed which this part of the document will address. Examples of the vendor agnostic type of IPv6 related traffic that should be blocked are provided in the following subsections. If your enterprise infrastructure is not currently setup to explicitly run IPv6 it is recommended that **all devices on the network** have the IPv6 interface disabled. This will help in the prevention of known and unknown IPv6 based attacks.

¹ National Institute of Standards Special Publication 800-41, Section 4.1.2, (NIST SP800-41), <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf> . Last accessed on July 5, 2012.

It is possible that any of the examples in this section may be seen on your internal network. While they represent legitimate types of internal network traffic, none of them are routable on the Internet and all of the entries in this section should be blocked, both inbound and outbound, at the network boarder.

- All traffic from these addresses or ranges should be blocked both inbound and outbound .
 - The loopback address is → `::1/128`.²
 - Can be displayed as
 - `0:0:0:0:0:0:0:1`
 - `::1`
 - The unspecified address, similar to the IPv4 address 0.0.0.0, is → `::/128`, and is only used when an interface doesn't know what its link local address is yet.³
 - Can be displayed as
 - `0:0:0:0:0:0:0:0`
 - `::/0`
 - `::`
 - Depending on your IPv6 implementation this address may be seen within your local network but should not appear on the Internet or be routed to it.
 - The IPv4-mapped address range → `::FFFF:0:0/96`.⁴
 - The IPv4 address `129.107.86.36` can be displayed as
 - `0:0:0:0:0:FFFF:129.107.86.36`
 - `::FFFF:129.107.86.36`
 - *IPv4 mapped addresses* should not be confused with the similar, and deprecated, *IPv4-compatible addresses*. IPv4 mapped addresses can be used in a dual-stack environment to map IPv4 addresses to IPv6 addresses allowing IPv6 only applications to operate with IPv4 nodes.
 - While they can be used internally on your network, they are not routable on the Internet.
 - Link-local unicast addresses⁵
 - `fe80::/10`, `fe90::/10`, `fea0::/10`, `feb0::/10`
 - Should be treated similarly to the private address space in IPv4. Expect to see these on your internal network but don't allow it to cross your network boarder in either direction .
 - Site-local addresses are → `fc00::/7`.⁶

² Internet Engineering Task Force, RFC 4291, <http://tools.ietf.org/html/rfc4291>. Last accessed on July 5, 2012.

³ [RFC4291](#)

⁴ [RFC4291](#)

⁵ [RFC4291](#)

- This range functions the same as the IPv4 private address ranges
- The documentation addresses are → 2001:db8::/32.⁷
 - These addresses are used for documentation purposes such as user manuals, RFCs, etc. Similar in function to the 555 telephone numbers used on TV and in Movies.
 - Address with this prefix should not be seen on any network. If it is seen, it is at the very least, an indication of a misconfiguration and should be examined.
- Orchid
 - Overlay Routable Cryptographic Hash Identifiers (ORCHID) addresses are → 2001:10::/28.⁸
- IPv6 Benchmarking Addresses are → 2001:2::/48
- Discard-Only Prefix for remote triggered blackhole routing addresses are → 0100::/64.⁹
- IANA Special Purpose Address Block¹⁰
 - 2001:0000::/29 - 2001:01F8::/29
- Address ranges Reserved by the IETF

0000::/8	0100::/8	0200::/7	0400::/6
0800::/5	1000::/4	2000::/3 ¹¹	4000::/3
6000::/3	8000::/3	A000::/3	C000::/3
E000::/4	F000::/5	F800::/6	FE00::/9
FEC0::/10			

Deprecated Addresses

A compilation of special use IPv6 addresses have been discontinued in the following categories: Node-Scoped Unicast, IPv4-Mapped Addresses, IPv4-Compatible Addresses, Link-Scoped Unicast, Unique-Local, Documentation Prefix, 6to4, Teredo, 6bone, ORCHID, Default Route, IANA Special-Purpose IPv6 Address Registry, Multicast and the reasons for

⁶ Internet Engineering Task Force, RFC 3879, <http://tools.ietf.org/html/rfc3879>. Last accessed on July 5, 2012.

⁷ Internet Engineering Task Force, RFC 3849, <http://tools.ietf.org/html/rfc3849>. Last accessed on July 5, 2012.

⁸ Internet Engineering Task Force, RFC 4843, <http://tools.ietf.org/html/rfc4843>. Last accessed on July 5, 2012.

⁹ Internet Assigned Numbers Authority, <http://www.iana.org/assignments/icmpv6-parameters>. Last accessed July 4, 2012.

¹⁰ Internet Engineering Task Force, RFC 4773, <http://tools.ietf.org/html/rfc4773>. Last accessed on July 5, 2012.

¹¹ It is US-CERT's position that, since this address space has not been allocated, blocking this address space at the firewall is a business case decision to be made by each entity with respect to their business needs and architecture.

removing them are in the referenced RFCs. However, US-CERT has selected the following address types, again to form the foundation of information for your consideration.^{12,13}

- These have been removed from the IPv6 standard and should not appear on any network:
 - The IPv4 compatible addresses are → `::<ipv4-address>/96.`
 - 6bone – experimental network ranges used for early testing of IPv6.
 - Addresses of the first instance of the 6bone experimental network were → `5f00::/8.`¹⁴
 - The second instances of the 6bone experimental network were → `3ffe::/16.`¹⁵
 - The following addresses were returned to IANA → `5f00::/8` and `3ffe::/16.`¹⁶
 - The deprecated address range of → `FEC0::/10`, is no longer routable and should be blocked on all routers and firewalls.

Routing

IPv6 routing has also introduced additional capabilities, but the list below have specific reasons for blocking, e.g. type 0 can be exploited for generating denial-of-service traffic.¹⁷

- Routing Headers
 - Block packets containing “type 0” routing header extensions (source routing)
 - Block packets containing “type 1” routing header extensions (NIMROD routing, deprecated in 2009)
 - Extension Header type 43, variant 0 and 1
 - Be careful NOT to block all packets with header type 43, not all routing header extensions are dangerous, just variant 0
 - Block routing header types 4 – 252, unassigned
 - Block routing header types 253 & 256 – experimental¹⁸
 - Block routing header type 255 – reserved
 - Some IP protocols are rarely passed between an outside network and an organization’s LAN, and therefore can simply be blocked in both directions at the firewall. For example, IGMP is a protocol used to control multicast networks, but multicast is rarely used, and when it is, it is often not used across the Internet.

¹² Internet Engineering Task Force RFC 5156, <http://tools.ietf.org/html/rfc5156>. Last accessed on July 30, 2012.

¹³ [RFC 4291](http://tools.ietf.org/html/rfc4291)

¹⁴ Internet Engineering Task Force, RFC 1897, <http://tools.ietf.org/html/rfc1897>. Last accessed on July 5, 2012.

¹⁵ Internet Engineering Task Force, RFC 2471, <http://tools.ietf.org/html/rfc2471>. Last accessed on July 5, 2012.

¹⁶ Internet Engineering Task Force, RFC 3701, <http://tools.ietf.org/html/rfc3701>. Last accessed on July 5, 2012.

¹⁷ Internet Engineering Task Force, RFC 5095, <http://tools.ietf.org/html/rfc5095>. Last accessed on July 30, 2012

¹⁸ Internet Engineering Task Force, RFC 4727, <http://tools.ietf.org/html/rfc4727>. Last accessed on July 5, 2012.

Therefore, blocking all IGMP traffic in both directions is feasible if multicast is not used.¹⁹

IPv6 Option Types to Block:

- C3 – unassigned
- 7 – Calypso²⁰
 - only useful in closed networks and shouldn't be seen on the Internet, and thus can be safely blocked
- 1e, 3e, 5e, 7e, 9e, be, de, fe – experimental
- ff – unassigned

Multicast Addresses

- Multicast addresses that contain a 4-bit scope in the address field that indicates the packets scope are → ff00::/8. (Only addresses with “global” scope should be allowed to cross the network boundary.)²¹
- Understanding multicast scope
 - The 4th hex character indicates the “scope” of a multicast address, with the values ranging from 0 to F, each indicating a scope
 - Address will begin with ffXY
 - ff identifies the address as multicast
 - X = a hex character that represents some set of flags that aren't relevant to this topic
 - Y = the Scope of the multicast address that determines its “range”
 - Only cope values of E are global and should be allowed to pass your networks border meaning those with the 4th hex value of “E” (FFXE)

• ICMPv6 Filtering

ICMP performs similar functions in both IPv4 and IPv6 it's slightly more ingrained into IPv6, with some messages being integral to network operation. The following rules will ensure the necessary ICMP messages are allowed to pass the network boarder, while those that could potentially be used for malicious purposes are blocked. This section touches on a couple of the types of blocking that is recommended via the RFC.

- Recommended Blocking at the network boarder, both inbound and outbound.
 - Seamoby Experimental Protocol (ICMP Type 150)²²

¹⁹ National Institute of Standards Special Publication 800-41, <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf>. Last accessed on July 5, 2012.

²⁰ Internet Engineering Task Force, RFC 5570, <http://tools.ietf.org/html/rfc5570>. Last accessed on July 5, 2012.

²¹ [RFC4291](http://tools.ietf.org/html/rfc4291)

- experimental protocol designed to accelerate IP handover between wireless access routers
 - All informational messages currently unassigned by Internet Assigned Numbers Authority (IANA): (Types 154-199 and 202-254)²³
 - ICMPv6 specification requires informational messages of unknown types must be silently discarded, which can be accomplished by simply blocking them at the firewall
 - This list should be reviewed periodically for changes as new message numbers get assigned
 - Node Information enquiry messages should generally not be allowed to cross the network boundary in either direction.
 - Node Information Query (Type 139)
 - Node Information Response (Type 140)
 - Router Renumbering messages should not be forwarded across site boundaries (Type 138)
 - Experimental message types: 100, 101, 200, and 201
 - Reserved extension types (127 and 255)²⁴
- As stated in the Overview caveat, implementation of the following will be dependent (requires research and judgment) upon your specific environments:
- Error messages not currently defined by IANA: (Types 5-99 and 102-126).²⁵
 - The ICMPv6 specification recommends allowing unknown error messages in the hopes that a higher level protocol can understand them
 - Could allow a communication channel for malicious traffic like C&C communication
 - This list should be reviewed periodically for changes as new message numbers get defined

• Tunneling

If an organization cannot obtain an IPv6 address natively then creating a tunnel is a viable method to establish connectivity between an IPv4 device and another running IPv6.

Tunneling can provide the connectivity but it also presents security considerations since it can provide a method to surreptitiously gain access to a network. The suggestions listed below help to mitigate the security issues.

- 6to4 tunneling

²² Internet Engineering Task Force, RFC 4065, <http://tools.ietf.org/html/rfc4065>. Last accessed on July 5, 2012.

²³ Internet Engineering Task Force, RFC 4443, <http://tools.ietf.org/html/rfc4443>. Last accessed on July 5, 2012.

²⁴ [IANA ICMPv6](http://tools.ietf.org/html/rfc4890)

²⁵ Internet Engineering Task Force, RFC 4890, <http://tools.ietf.org/html/rfc4890>. Last accessed on July 5, 2012.

- 6to4 addresses are → 2002::/16.²⁶ The 6to4 addresses may be routed when the site is running a 6to4 relay or offering a 6to4 transit service. If not then can be blocked.
- Teredo /Miredo (Unix, Linux) tunneling
 - Teredo addresses are → 2001::/32.²⁷
 - If you aren't using or allowing this type of tunneling these addresses can be blocked
- Intra-site Automatic Tunnel Addressing Protocol (ISATAP tunneling)
 - Filter for this string → 0000:5EFE:(followed by the 32 bit IPv4 address) if ISATAP is not used
 - Additional tunneling information
 - Tunneled IPv6 within IPv4 traffic should be isolated to IPv4 protocol 41
 - Tunneled IPv6 within IPv6 will contain a “next header” value of 41. This indicates that the type of packet contained within the IPv6 packet is also IPv6, where you would normally expect this to be ICMPv4 (next header value of 1), TCP (next header value of 6) or some other higher level protocol or possibly an extension header like a fragmentation or routing extension header.
 - Organizations that do not yet use IPv6 should block all native and tunneled IPv6 traffic at their firewalls, both inbound and outbound. Note that such blocking limits testing and evaluation of IPv6 and IPv6 tunneling technologies for future deployment. To permit such use, the firewall administrator can selectively unblock IPv6 or the specific tunneling technologies of interest for use by the authorized testers.²⁸
 - “Use access control lists at border routers to block protocols 41 (used by 6to4), 43, 44, 58, 59, 60, and IP address 192.88.99.1 (default anycast address of some 6to4 systems) would be a good place to start.”²⁹

²⁶ Internet Engineering Task Force, RFC 3056, <http://tools.ietf.org/html/rfc3056>. Last accessed on July 5, 2012.

²⁷ Internet Engineering Task Force, RFC 4380, <http://tools.ietf.org/html/rfc4380>. Last accessed on July 5, 2012

²⁸ [RFC 4291](#)

²⁹ CERT/CC Blog, Bypassing firewalls with IPv6 tunnels, by Ryan Giobbi, April 2, 2009, http://www.cert.org/blogs/certcc/2009/04/bypassing_firewalls_with_ipv6.html. Last accessed on July 4, 2012.

References

1. National Institute of Standards Special Publication 800-41, Section 4.1.2, (NIST SP800-41), <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf>. Last accessed on June 19, 2012.
2. Internet Engineering Task Force, RFC 4291, <http://tools.ietf.org/html/rfc4291>. Last accessed on June 19, 2012.
3. Internet Engineering Task Force, RFC 3879, <http://tools.ietf.org/html/rfc3879>. Last accessed on June 19, 2012.
4. Internet Engineering Task Force, RFC 3849, <http://tools.ietf.org/html/rfc3849>. Last accessed on June 19, 2012.
5. Internet Engineering Task Force, RFC 4843, <http://tools.ietf.org/html/rfc4843>. Last accessed on June 19, 2012.
6. Internet Assigned Numbers Authority, <http://www.iana.org/assignments/icmpv6-parameters>. Last accessed July 4, 2012.
7. Internet Engineering Task Force, RFC 4773, <http://tools.ietf.org/html/rfc4773>. Last accessed on June 19, 2012.
8. Internet Engineering Task Force, RFC 1897, <http://tools.ietf.org/html/rfc1897>. Last accessed on June 19, 2012.
9. Internet Engineering Task Force, RFC 2471, <http://tools.ietf.org/html/rfc2471>. Last accessed on June 19, 2012.
10. Internet Engineering Task Force, RFC 3701, <http://tools.ietf.org/html/rfc3701>. Last accessed on June 19, 2012.
11. Internet Engineering Task Force, RFC 4727, <http://tools.ietf.org/html/rfc4727>. Last accessed on June 19, 2012.
12. National Institute of Standards Special Publication 800-41, <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf>. Last accessed on June 19, 2012.
13. Internet Engineering Task Force, RFC 5570, <http://tools.ietf.org/html/rfc5570>. Last accessed on June 19, 2012.
14. Internet Engineering Task Force, RFC 4065, <http://tools.ietf.org/html/rfc4065>. Last accessed on June 19, 2012.
15. Internet Engineering Task Force, RFC 4443, <http://tools.ietf.org/html/rfc4443>. Last accessed on June 19, 2012.
16. Internet Engineering Task Force, RFC 3056, <http://tools.ietf.org/html/rfc3056>. Last accessed on June 19, 2012.
17. Internet Engineering Task Force, RFC 4380, <http://tools.ietf.org/html/rfc4380>. Last accessed on June 19, 2012.
18. Internet Engineering Task Force, RFC 5095, <http://tools.ietf.org/html/rfc5095>. Last accessed on July 30, 2012.
19. Internet Engineering Task Force RFC 5156, <http://tools.ietf.org/html/rfc5156>. Last accessed on July 30, 2012.
20. CERT/CC Blog, Bypassing firewalls with IPv6 tunnels, by Ryan Giobbi, April 2, 2009, http://www.cert.org/blogs/certcc/2009/04/bypassing_firewalls_with_ipv6.html, Last accessed on July 4, 2012.

- **Contact US-CERT**

For any questions related to this report, please contact US-CERT at:

Email: soc@us-cert.gov

Voice: 1-888-282-0870

Incident Reporting Form: <https://forms.us-cert.gov/report/>

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: <https://forms.us-cert.gov/ncsd-feedback/>