US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Technical Information Paper TIP-12-225-01
Fundamental Filtering of IPv6 Network Traffic [1]

Tim Stahl, Michael King, Robert Renstrom

June 19, 2012

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's 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.

[1] 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/***.

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 an authoritative word in IPv6 network security; it is merely a baseline if nothing has been done to secure your network from IPv6 security threats.

Though format and address length are different between IPv4 and IPv6, many of the features of the protocols remain the same, rules included. All inbound or outbound traffic that is not specifically permitted should be blocked regardless of the protocol version. 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 at the same level of competency as the infrastructure used with IPv4 traffic. This also applies to those networks that do not allow IPv6 traffic to enter or traverse the network.[2]

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.[3,4] This 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 footnote 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 preceding subsections.

If your enterprise infrastructure is not currently set up to run IPv6, then it is recommended all devices on the network have the IPv6 interface disabled. This will help prevent known and unknown IPv6-based attacks.

[2] 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.
[3] The Internet Big Picture, Internet Usage Statistics, World Internet Users and Population Stats, http://www.internetworldstats.com/stats.htm. Last accessed on July 24, 2012.
[4] http://fiber.google.com/about/. Last accessed on July 27, 2012.

- All traffic from these address or ranges should be blocked both inbound and outbound.
  - The loopback address is → `::1/128`.[5]
    - 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.[6]
    - 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 network but should not appear on the internet or be routed to it.
  - The IPv4-mapped address is → `::FFFF:0:0/96`.[7]
    - 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 addresse*s 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 in the *internet.* [8]
  - Link-local unicast addresses[9]
    - 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 border in either direction.
  - Site-local addresses are → `fc00::/7`.[10]
    - This range functions the same as the IPv4 private address ranges.

[5] Internet Engineering Task Force, RFC 4291, http://tools.ietf.org/html/rfc4291. Last accessed on July 5, 2012.
[6] RFC4291
[7] NIST SP800-41
[8] NIST SP800-41
[9] NIST SP800-41
[10] Internet Engineering Task Force, RFC 3879, http://tools.ietf.org/html/rfc3879. Last accessed on July 5, 2012.

- The documentation addresses are → `2001:db8::/32.`[11]
  - 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.
- Orchid
  - Overlay Routable Cryptographic Hash Identifiers (ORCHID) addresses are → `2001:10::/28.`[12] These addresses are used as identifiers and should not be routable.
- IPv6 Benchmarking Addresses are → `2001:2::/48`
- Discard-Only Prefix for remote triggered blackhole routing addresses are → `0100::/64.`[13]
- IANA Special Purpose Address Block[14]
  - `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**[15]	**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, and Multicast, and the reasons for 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.[16,17]

[11] Internet Engineering Task Force, RFC 3849, http://tools.ietf.org/html/rfc3849. Last accessed on July 5, 2012.
[12] Internet Engineering Task Force, RFC 4843, http://tools.ietf.org/html/rfc4843. Last accessed on July 5, 2012.
[13] Internet Assigned Numbers Authority, http://www.iana.org/assignments/icmpv6-parameters. Last accessed July 4, 2012.
[14] Internet Engineering Task Force, RFC 4773, http://tools.ietf.org/html/rfc4773. Last accessed on July 5, 2012.
[15] 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.
[16] Internet Engineering Task Force RFC 5156, http://tools.ietf.org/html/rfc5156. Last accessed on July 30, 2012.

- 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.`[18]
    - The second instances of the 6bone experimental network were → `3ffe::/16.`[19]
    - The following addresses were returned to IANA → `5f00::/8 and 3ffe::/16.`[20]
  - 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 items in the list below have specific reasons for blocking; for example, type 0 can be exploited for generating denial-of-service traffic.[21]

- 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 –` experimental.[22]
    - 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.

[17] RFC 4291
[18] Internet Engineering Task Force, RFC 1897, http://tools.ietf.org/html/rfc1897. Last accessed on July 5, 2012.
[19] Internet Engineering Task Force, RFC 2471, http://tools.ietf.org/html/rfc2471. Last accessed on July 5, 2012.
[20] Internet Engineering Task Force, RFC 3701, http://tools.ietf.org/html/rfc3701. Last accessed on July 5, 2012.
[21] Internet Engineering Task Force, RFC 5095, http://tools.ietf.org/html/rfc5095. Last accessed on July 30, 2012.
[22] 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.[23]

IPv6 Option Types to Block:

- C3 – unassigned
- 7 – Calypso[24]
  - 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.)[25]
- 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 scope values of E are global and should be allowed to pass your network's border, meaning those with the 4th hex value of "`E`" `(FFXE)`.

ICMPv6 Filtering

In keeping with the security best practices of IPv4, much of the same could be applied to ICMPv6. An administrator will need to know what they want to allow in and out of their network when monitoring devices. This section touches on a couple of the types of blocking that is recommended via the RFC.

[23] 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.
[24] Internet Engineering Task Force, RFC 5570, http://tools.ietf.org/html/rfc5570. Last accessed on July 5, 2012.
[25] RFC4291

- Recommended Blocking
  - Seamoby Experimental Protocol (ICMP Type 150)[26]
    - 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).[27]
    - 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 forwarded across site boundaries.
    - 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)[13,28]

- 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).[27]
    - 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 and another running IPv6. Tunneling can provide the connectivity, but it also presents security considerations since it can also provide a method to surreptitiously gain access to a network. The suggestions listed below help to mitigate the security issues.

[26] Internet Engineering Task Force, RFC 4065, http://tools.ietf.org/html/rfc4065. Last accessed on July 5, 2012.
[27] Internet Engineering Task Force, RFC 4443, http://tools.ietf.org/html/rfc4443. Last accessed on July 5, 2012.
[28] IANA ICMPv6

- 6to4 tunneling
  - 6to4 addresses are → `2002::/16`.[29] 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`.[30]
    - 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).
    - 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. 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.[31]
    - "Use access control lists at border routers to block protocols 41 (used by 6to4), 43, 44, 58, 59, 60, and 192.88.99.1 (default anycast address of some 6to4 systems) would be a good place to start."[32]

---

[29] Internet Engineering Task Force, RFC 3056, http://tools.ietf.org/html/rfc3056. Last accessed on July 5, 2012.
[30] Internet Engineering Task Force, RFC 4380, http://tools.ietf.org/html/rfc4380. Last accessed on July 5, 2012.
[31] RFC 4291
[32] 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 on 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/

Document FAQ

What is a TIP? A Technical Information Paper (TIP) is issued for a topic that is more informational in nature, describing an analysis technique, case study, or general cybersecurity issue. Depending on the topic, this product may be published to the public website.

I see that this document is labeled as TLP: GREEN. Can I distribute this to other people? Information in this category can be circulated widely within a particular community. However, the information may not be published or posted publicly on the internet, nor released outside of the community. Please contact US-CERT with specific distribution inquiries.

Can I edit this document to include additional information? This document is not to be edited, changed, or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.