8 security considerations for IPv6 deployment

The likely vulnerabilities as we transition to the next generation of IP addressing

By Danny McPherson, CSO, Verisign Inc., Network World
June 01, 2011

Although vendor-written, this contributed piece does not advocate a position that is particular to the author's employer and has been edited and approved by Network World *editors.*

Feb. 3, 2011, came and went without much fanfare, but it was a milestone for Internet stakeholders, whether they knew it or not. On that Thursday, the last available IPv4 addresses were allocated by the Internet Assigned Numbers Authority (IANA). Though some Regional Internet Registries (RIRs) have a reasonable inventory of IP addresses that could last another year or two, the days of "new" IPv4 address allocations are largely over.

Now that we're out of IPv4 allocations, it's time to get serious about adopting the next generation of Internet Protocol, IPv6. With a 128-bit address space (compared to IPv4's 32-bit space), IPv6 can accommodate the ongoing and exponential growth of the Internet, which currently is adding about a million new devices every hour. In fact, compared with the 4.3 billion IP addresses that IPv4 allows, IPv6 will enable another 340 trillion, trillion, trillion addresses -- enough to accommodate global Internet demand for the foreseeable future.

Coupled with the continued deployment of DNS Security Extensions (DNSSEC), IPv6 will ultimately provide the stable and secure base for the future Internet. But for the transition from IPv4 to IPv6 to be successful, everyone from infrastructure operators and service providers to application developers and users will have to work together on a range of activities, including:

- supporting and developing IPv6 capabilities and establishing functional IPv4 parity;
- debugging issues with new IPv6-only software and applications;
- refining interworking and transitional co-existence with IPv4.

A crucial part of that effort will involve security. IPv6 represents new territory for most Internet stakeholders, and its rollout will introduce some unique security challenges. While the following list is by no means comprehensive, it does point to eight considerations and problem areas that the industry will need to address as IPv6 adoption continues. Because we're still in the early stages, the solutions to some of these risks will only come after real-world use leads to proven best practices.

* **Translating from IPv4 to IPv6, transactions may become vulnerable.**

Because IPv4 and IPv6 are not "bits on the wire" compatible, protocol translation is seen as one path to wider deployment and adoption. Translating traffic from IPv4 to IPv6 will inevitably result in mediating transactions as they move through the network. Think of a mail sorter at a post office transfer facility that must open every IPv4 envelope to put each letter in an IPv6 one to ensure it reaches the correct address, at times changing content in the documents contained within in order to coincide with the new IPv6 external envelop information. Each time this happens, an opportunity arises for a poor implementation or a bad actor to tickle or exploit a potential vulnerability. Additionally, it compromises the end-to-end principle by introducing middle boxes that must maintain transaction state and complicates the network. In general, security staff should pay attention to security aspects of all translation and transition mechanisms (to include tunneling), and only enable such mechanisms explicitly after they have been thoroughly evaluated.

* **Large network segments are both good and bad.**

IPv6 introduces network segments that are significantly larger than those we see today. The current recommended prefix length for an IPv6 subnet is /64 (264), which can accommodate some 18 quintillion hosts on a single segment! While this enables virtually unlimited LAN growth, its size also presents challenges. For instance, it would take years to scan a single IPv6 /64 block for vulnerabilities, while a single /24 IPv4 subnet 28 would only take seconds. Since a comprehensive scan is impossible, a better approach may be to utilize only the first /118 (the same number of hosts as a /22 in IPv4) of addresses to narrow the range of IPs to scan, or perhaps allocate all addresses explicitly and deny all others implicitly. This will make careful IP management and monitoring even more crucial than it is today. One might also expect passive domain name system (DNS) analysis and other reconnaissance techniques to be employed by attackers in place of traditional scanning.

* **Neighbor discovery and solicitation can expose networks to problems.**

Neighbor discovery (ND) in IPv6 utilizes five different types of Internet Control Message Protocol version 6 (ICMPv6) messages for several purposes, including to determine the link layer addresses of neighbors on the attached links, to purge cached values that become invalid, and to discover neighbors willing to forward packets on their behalf. While ND offers many useful functions -- including duplicate address detection (DAD) -- it can also present opportunities to attackers. ND attacks in IPv6 will quite likely replace their IPv4 counterparts such as ARP spoofing. In general, it's a good idea to keep ports disabled unless explicitly provisioned, implement link layer access control and security mechanisms, and be sure to disable IPv6 completely where it's not in use.

* **Choking on large extension headers, firewalls and security gateways could fall prey to DDoS attacks.**

In IPv6, the IP options function has been removed from the main header and is instead implemented via a set of additional headers called extension headers (EH) that specify destination options, hop-by-hop options, authentication and an array of other options. These extension headers follow the IPv6 main header, which is fixed at 40 bytes, and are linked together to create an IPv6 packet (fixed header + extension headers + payload). IPv6 traffic with large numbers of extension headers could overwhelm firewalls and security gateways, or perhaps even introduce router forwarding performance degradation, and thus serve as a potential vector for DDoS and other attacks. Disabling "IPv6 source routing" on routers may be necessary to protect against DDoS threats, and explicitly codifying which extension headers are supported and checking network equipment for proper implementation is critical. In general, IPv6 adds many more components to be filtered or require scoped propagation, to include some extension headers, multicast addressing, and increased uses for ICMP.

* **6to4 and 6RD proxying may encourage attacks and abuse.**

6to4 -- along with its ISP rapid deployment cousin, 6RD -- allows IPv6 packets to jump the IPv4 moat without having to configure dedicated tunnels. But deploying IPv6 proxy servers may avail proxy operators to a world of trouble, including discovery attacks, spoofing and reflection attacks, and proxy operators themselves can be leveraged as a "source" for attacks and abuse.

* **Support for IPv6 services could expose existing IPv4 applications or systems.**

One limitation is that existing security fixes may only be applied to IPv4 support, yet most kernels will prefer IPv6 interfaces before IPv4 when engaging in such activities as DNS lookups in order to foster more rapid IPv6 deployment. Indeed, the dynamic between IPv6 and IPv4 could result in a doubling of traffic for each DNS lookup (with both AAAA and A records requested, or worse, each over IPv4 and IPv6). This could result in large amounts on unnecessary DNS traffic in order to optimize for user experience. OS and content vendors frequently put hacks in place to mitigate or optimize for this behavior (e.g., AAAA whitelisting), which creates added system load and state. Additionally, it should certainly be observed that with new IPv6 stacks being accessible new vulnerabilities are sure to surface. Dual-stacking during a long transitional coexistence period, and inter-dependences between routers, end systems, and network services such as the DNS are sure to serve as fertile ground for miscreants.

* **Many users may be obscured behind fixed sets of addresses.**

Obscuring users behind large network address translation protocol translation (NAT-PT) devices could break useful functions like geolocation or tools that enable attribution of malicious network behaviors, and make number and namespace reputation-based security controls more problematic.

* **Even IPSec could pose problems when tunneling to other networks.**

IP Security (IPSec) makes it possible to authenticate the sender, provide integrity protection, and optionally, encrypt IP packets to provide confidentiality of transmitted data. IPSec was an optional feature for IPv4, but it's mandatory with IPv6. In tunnel mode -- which essentially creates a VPN for network-to-network, host-to-network and host-to-host communications -- the entire packet is encapsulated into a new IP packet and given a new IP header. But a VPN connection with a network that's beyond the originator's control could result in security exposures or be used to exfiltrate data, etc. Because the negotiation and management of IPSec security protections and the associated secret keys are handled by additional protocols (e.g., Internet Key Exchange -- IKE) and adds complexity, it isn't likely IPSec will be any more widely supported with IPv6 than it is with IPv4 initially.

It will be some time before IPv6 is universally deployed and IPv4 devices begin to decline. Until then, we will all be working to build on the protocol that enabled the Internet's first 4 billion devices.

Now that the milestone of Feb. 3 has come and gone, we soon will have little choice but to develop and propagate the best practices that will make the next generation of IP addresses stable, reliable and secure, and that starts with the awareness and knowledge of network and security staff.