IPv6 Security: Follow Guidelines to Mitigate Risks Introduced During the Integration

Abstract
As federal government agencies continue integrating IPv6 into their infrastructures, security questions arise. What previous risks does IPv6 mitigate? What new risks does it introduce? In fact, designing a secure network is less about the protocol than the way it is planned and implemented. IPv6 itself is inherently no more or less secure than IPv4 – just different:

- An advantage of IPv6 for security is that huge subnets help to lessen automated scanning and worm propagation.
- A disadvantage is that transition techniques for managing a dual-stack environment increase complexity and can create new vulnerabilities, such as attacks with extension headers.
- Similarities between IPv6 and IPv4 security are that upper-layer protocol vulnerabilities remain unchanged, and risks associated with IPv4 Address Resolution Protocol (ARP) resemble risks associated with IPv6 Neighbor Discovery (ND) protocol.

The good news is that your government agency can ensure that your dual-stack network will be as secure as your current IPv4 network by making informed decisions based on your mission needs. This paper, intended for technology and security executives in federal government, provides recommendations for IPv6 security policy planning, architecture planning, and deployment that will affect the security of dual-stack and pure IPv6 networks in years to come.

Policy Planning and Architecture Considerations
Agencies with dual-stack environments need to address not one, but two sets of security requirements. That is, your agency must continue to protect against IPv4 vulnerabilities at the same time it addresses new IPv6 considerations, such as stateless autoconfiguration, neighbor discovery, router advertisement, parsing or filtering extension headers, and the potential for host-to-host IPsec encrypted attacks. The IT group must also mitigate the potential for cross-protocol abuse, such as when threats embedded in IPv6 packets go undetected as the packets travel through IPv4 tunnels. A dual-stack host must be prevented from using IPv6 to attack the IPv4 network by using another inside trusted host.

It is crucial to approach security from an overall architectural perspective rather than simply considering it for individual devices. Following are advantages, risks, and recommendations for tunneling, fragmentation, use of single-protocol or dual-protocol security devices, and firewall and intrusion prevention system (IPS) placement.

Tunneling
As your agency gradually integrates IPv6, tunneling allows IPv6 packets to travel across the existing IPv4 infrastructure. The advantage of tunneling as a transition mechanism is that your agency can accomplish the IPv6 integration at its own pace, adding IPv6 “islands” in individual departments or subnets without disrupting operations. To make sure that an attack using IPv6 does not go undetected, you need to filter IPv6 traffic before it travels over the IPv4 tunnel and block any suspicious traffic. The techniques used to filter IPv6 traffic are already familiar to many agency IT groups because they are required for IPv4 Generic
Routing Encapsulation (GRE) tunnels. Dynamic Multipoint VPN (DMVPN) is another useful tunneling technology. Scheduled to be released soon for IPv6, DMVPN provides excellent network security as well as low overhead and operational efficiency for network devices.

Cisco recommends the following guidelines for agencies that decide to allow tunneling:

- Select which tunnels will be allowed in your network and the specific places in the network that they can operate. Then enact policies to deny all other tunnels. Types of tunnels include: manual IPv6, automatic IPv4-compatible, GRE, automatic 6to4, Teredo, and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). Cisco recommends against the use of automatic tunnels for certain deployment scenarios. For more information on the security implications of tunneling options, see the *IPv6 and IPv6 Threat Comparison and Best-Practice Evaluation (v1.0)* white paper.\(^1\)
- Be cautious about allowing multilayer tunneling. It can be useful in geographically dispersed environments that cross service provider core boundaries. However, the difficulty of inspecting tunneled traffic can increase the risk that an attack might go undetected.
- Amend policies regularly as the IPv6 portion of the network matures. For example, after adding IPv6 firewall capabilities and intrusion prevention systems (IPSs), determine if the new devices provide increased tunnel inspection capabilities and then adjust tunnel policies accordingly. Consider terminating tunneled traffic outside a firewall and then passing it natively through the firewall for full inspection. This option is described in the “Separate or Integrated Devices” section of this paper.

**Fragmentation**

Fragmentation refers to splitting up large packets into smaller packets for transmission over the network and then reassembling the packets at the destination. In IPv6 environments, the end hosts – not the network infrastructure – manage fragmentation. The advantage of allowing fragmentation is that hosts use path Maximum Transmission Unit (MTU) discovery to detect the optimal packet size for end-to-end communication across the network. The risk is that security attacks can go undetected if the attack is split up across multiple packets.

General IPv6 best practices call for minimizing fragmentation as much as possible. To avoid the need for fragmentation, perform a network audit to determine the MTU based on network capability and then configure devices accordingly. The minimum MTU for IPv6 is now 1280 bytes. Any non-final fragments less than 1280 bytes should be dropped. For additional protection, some agencies might choose to drop all fragments if the TCP/UDP portion of the header does not appear in the first fragment.

**Separate or Integrated Devices**

Early in the planning process, agencies need to decide whether to deploy a single security device to handle IPv4 as well as IPv6 traffic or to separate traffic at the ingress point and use separate security devices. In the early stages of IPv6 integration, a single security device might be easier to deploy and maintain because of the minimal amount of IPv6 traffic transiting the security boundary. Even so, Cisco recommends separating security functions (IPsec VPN, firewall, IPS) among multiple devices to increase resilience and

\(^{1}\) The paper is available at: [www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf](http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf)
performance. Using separate devices is a good option at any stage of IPv6 integration because it prepares the network to carry more IPv6 traffic.

**Placement of Firewalls and IPS**

Most agencies currently deploy firewalls and IPS devices only at the edge of the network and in front of data centers, an approach called perimeter security. The advantage of perimeter security is that it is easy to implement and is effective against outside attacks. However, an increase in mobility services and mobile users within federal government increases the risk of internal attacks to the network. If an attack gets past the perimeter, the agency’s network and assets might be at risk because few security measures are embedded in the network.

Your agency can view the IPv6 integration as an opportunity to consider a pervasive security approach, which is more advanced and provides defense in depth. Figure 1 shows a general architectural view of pervasive security and indicates overall best practices for network security: application security, anti-x defenses, and containment and control. With this approach, security mechanisms are integrated throughout the network to more quickly react to attacks at their source. Keep in mind that IPv6 security offerings continue to mature. As you plan your IPv6 architecture, find out which tools you can use today and when others will be available.

![Figure 1 Pervasive Security](image)

Figure 2 shows a more detailed dual-stack architecture that incorporates pervasive security. It also separates IPv4 and IPv6 security functions so that agencies can isolate traffic based on protocol version. Distributing security elements throughout the network mitigates the risk of a security breach occurring at any one place in the network.

In this architecture, all site-to-site tunneled traffic is terminated at a router outside the firewall so that the firewall and IPS devices can inspect the traffic for security threats. Remote access traffic, encrypted with
IPsec or SSL, is terminated by the VPN functionality of the Cisco® ASA 5500 Series Adaptive Security Appliance. This allows the Cisco ASA 5500 Series to inspect the unencrypted traffic by checking it against firewall and IPS access rules. [[figure notes: (left side) change “IPSec” to “Ipsec”; use the entire name “Cisco IOS Software”, as “Cisco IOS” is a trademarked name; (center) spell out “asymmetric”]]

**Figure 2  IPv4 / IPv6 Dual Stack Security**

**Deployment Best Practices**
Following are recommendations for IPv6 deployment:

- Consider security at every step as you develop the overall network architecture: Decisions made in the planning stage will have long-lasting ramifications on security.
- Use all available security technologies that can work collaboratively to protect your network. This includes router capabilities such as access control lists (ACLs), firewalls, IPS devices, IPsec, host security agents, web and email filters, and network analysis and reporting. The IPv6 security technology is continually advancing, so stay current on when new tools will be introduced.
- Make reconnaissance more difficult through proper address planning for network infrastructure. Consider using Unique Local Addresses (ULAs) for management addressing and then placing them in a separate VLAN.
- Control management access to the campus switches and routers. Infrastructure devices should use loopback interfaces configured for management and routing. Be sure that the IPv6 address for the loopback interfaces is not easy to guess.
- Control ingress traffic from the access layer. Filter the prefixes that are allowed to source traffic to help protect against basic spoofing. Also protect against spoofing at the exit point to the service provider and partners.
• Upgrade to IPv6-aware firewalls and IPS. Adapt the agency’s IPv4 security architecture to handle IPv6 transport. This requires redefining current firewall rules – for example, to specify which Internet Control Message Protocol Version 6 (ICMPv6) messages can traverse the firewall and allowed transition mechanisms.

• Monitor and control all transition mechanisms. You can do this with Cisco IOS® NetFlow or the Cisco Network Analysis Module (NAM). Turn off transitions that are built into certain applications. Applications that use automated tunneling, for example, can traverse firewalls, thereby exposing the network to the outside world. In agencies that have a mobile workforce, disable transition mechanisms on devices when they are used within the enterprise and enable them when they are used outside. Disable unneeded transition methods. If you use Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) internally, then leave it enabled and disable all others, including 6to4 and Teredo. Depending on the agency’s Microsoft Active Directory policies, the IT group might be able to use Active Directory to restrict the transition methods that are active on a host.

**Conclusion**

IPv6 is no more or less secure than IPv4. Your government agency’s security posture depends not only on the protocol, but also on the integration planning and implementation. Careful planning is especially important now – before IPv6 has been integrated into your agency’s security appliances and services. The recommendations and best practices in this paper can help your agency make its dual-stack network as secure as its IPv4 network. Cisco is committed to enhancing its security portfolio and will continue to provide recommendations as the federal government progresses with its IPv6 integration efforts.

**For More Information**

For guidance on next steps for the IPv6 integration, contact Cisco Advanced Services at:
 ipv6_services_practice@cisco.com

To read a white paper on IPv6 deployment in federal government, visit: