

An IPv6 Security Guide for U.S. Government Agencies

Executive Summary

The desire to connect with anyone at anytime has made Internet security an oxymoron. As you transition to IPv6 and continue movement towards IP-convergence, security will become even more important. In this report, we discuss the following:

- Critical security issues to consider during the transition
- Security architectures and approaches suitable for IPv6 deployment
- IPv6 as part of a holistic approach to enterprise security
- IPv6 and increasing security within the enterprise

Introduction

The convergence of voice, video, and data in the enterprise has arrived, and the IP-based infrastructure has become the underlying engine that allows advanced capabilities to be quickly developed and deployed to support a wide range of U.S. Government (USG) functions. Many agencies are moving toward the introduction of next-generation systems to support collaborative architectures, geospatial application, net-centric warfare, mobility, and continuity of operations (COOP), as well as other numerous applications to better suit their mission.

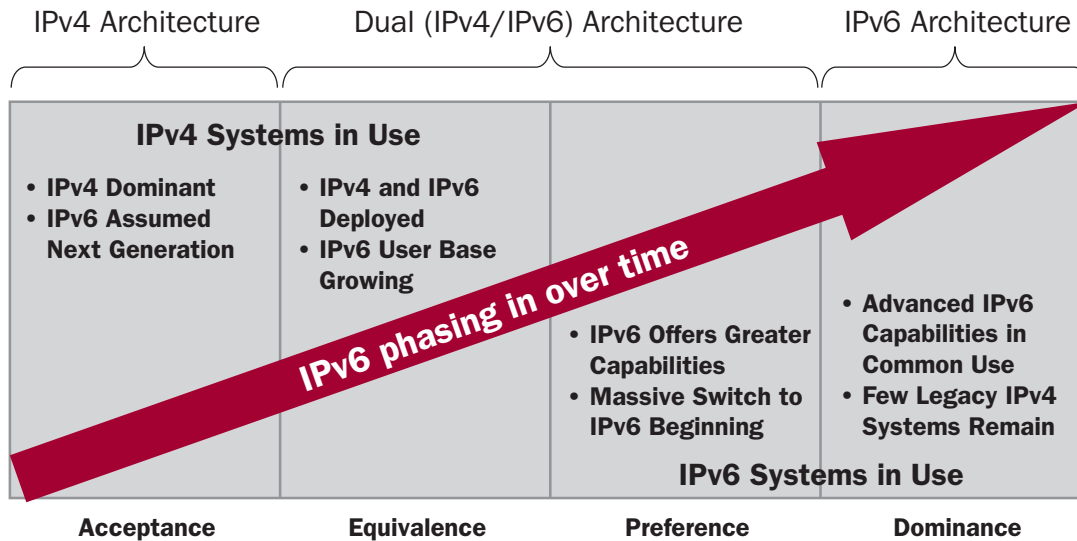
One challenge agencies must face while transitioning to IPv6 is the area of security. While IPv6 is not directly compatible with its predecessor, it poses many of the same risks associated with IPv4. In addition, IPv6 offers a number of new capabilities that could potentially offer additional vulnerabilities and threats to agencies. However, if properly implemented, IPv6 has the potential to provide a foundation for creating a secure infrastructure for an agency's enterprise as well as the Internet as a whole.

This volume covers numerous aspects of security related to the transition to IPv6. In addition to providing a high-level overview of the core concepts of IPv6, it goes into detail on the USG-wide policies and the planning that must be accomplished to ensure a successful and secure transition. This volume also goes into great technical detail not only on the underlying protocols and products that are part of IPv6, but also on related technologies that should be considered when looking at a holistic enterprise security approach.

IPv6 Security Phases

The security challenges during the transition will change as the method and use of IPv6 changes over time. The initial deployment of IPv6 is expected to operate very similarly to IPv4 in the beginning phases of the transition. However, agencies will most likely move away from pure enclave-based architectures to support the growing requirement for end-to-end services that will be necessary to implement many of the advanced IPv6 capabilities. This will require new thinking about security and a stronger push towards node-based security architectures. The result will be a phased IPv6 security rollout:

- Security Today
 - Enclave level
 - Centrally administrated
- Security Tomorrow
 - Node level
 - Integrate with policy-based networking
- Security In-Between
 - Enclave or node focused?
 - How long will there be overlap?
 - Unique security issues can/will arise due to mixed environment
 - Careful planning and testing required



Benefits of IPv6 Security

IPv6 will provide agencies a foundation to create a number of next-generation services that can deliver major benefits. But agencies will be hard pressed to find short-term operational benefits in their IPv6 deployments. In fact, many issues, especially security, will require agencies to spend incremental resources during their initial transition phases. If agencies view the transition to IPv6 as an opportunity and invest in proper planning, they can realize a number of security benefits associated with IPv6, including the following:

Secure Architectures: Transitioning to IPv6 provides agencies a chance to significantly modify and enhance their enterprise architecture around the capabilities of IPv6. It provides the opportunity to implement new security architectures and could significantly improve an agency's overall security posture.

Ubiquitous Security Layer: Numerous security protocols have been and are being developed within the Internet Engineering Task Force (IETF) to support greater security capabilities within IP, such as IP security (IPsec). While many of these will operate with both IPv4 and IPv6, currently entrenched deployments of IPv4 make spending the resources necessary to modify the equipment and architectures to implement them unlikely. In addition, IPsec is considered a mandatory part of IPv6.

Node and Topology Hiding: One of the weaknesses in IPv4 is the ability for malicious entities to quickly scan and identify nodes on the Internet. Once a hacker has access to an organization's subnet, it is a fairly quick and simple process to identify all of the nodes and focus on the ones with the greatest weakness. IPv6 provides a significant advantage due to the sheer number of potential addresses on a single subnet. There are 264 or 18,446,744,073,709,551,616 potential IPv6 nodes on each subnet, making typical network scanning virtually impossible.

New Capabilities: The IPv6 foundation enables the development and deployment of new capabilities and delivers the inherent security benefits of utilizing an established and approved framework. Currently, as new services are required for the Internet, inventive companies are identifying issues and design workarounds. While this is great from a service delivery standpoint, many of these workarounds exploit or create new security vulnerabilities. However, developers and users are left with little recourse to implement their requirement. Thus, IPv6 will provide an environment that can be focused on security and also provide the flexibility for quickly delivering new services.

Unique Identification: Significant security issues on the Internet stem today from the use of Network Address Translation (NAT) and private IPv4 address space. It is virtually impossible to obtain a level of assurance based on IP addresses. Most users sit behind one or more NAT or similar devices that prevent the direct association of an IP address to a specific user or node. With the changes in IPv6 structure and tremendously increased address space, architectures and services can be developed to prevent address spoofing and establish the necessary association to support true network-level access control and authentication.

Communities of Interest (COI): IPv6 makes it easy for nodes to have multiple IPv6 addresses on the same network interface. This can create the opportunity for agencies to establish overlay or COI networks on top of other physical IPv6 networks. Thus, department, groups, or other users and resources can belong to one or more COIs, with each can having its own established security policies. That way, security can become more granular and easier to implement based on grouping common requirements.

High Availability: One of the major strengths of IPv6 will be the ability to quickly setup and modify networks on the fly. This ad-hoc capability will allow not only nodes on the network, but entire networks to become much more resistant to denial-of-service scenarios. When deployed in mesh configurations, nodes and potentially networks could quickly identify and establish new routes as existing or preferred routes are disrupted.

What Agencies Need to Consider

During the transition process a number of critical implementation issues must be considered from a security perspective, including:

- Governance and Policy Needed
- Training
- Compliance Testing
 - Security Certification
- Institutionalized IPv6
 - Make Security Features Available
- New Attack Surface
 - New technology and processes needed
 - Eliminate IPv4 attack surface ASAP

First Steps

Some of the first steps any agency should accomplish with regard to security include:

- IPv6 Security Plan
- Policy
- Routers/Switches
 - Disable IPv6/Tunnels
 - ACL to Block IPv6/Tunnels on core/edge/outside enclave
- Network Protection Devices/Tools
 - Contact vendors for IPv6 advice
- Block IPv6 (Type 41) Tunnels
- Enable IPv6 IDS/IPS features
- End Nodes
 - Enable IPv6 host firewalls on all end devices
 - Disable IPv6 if not used
- Monitor Core and Enclave Boundaries

Recommendations for Initial IPv6 Deployment Architectures

Agencies should consider a number of IPv6 deployment approaches or philosophies as they design their initial IPv6 implementations, including:

- **Keep it Simple:** Designing complex solutions for initial IPv6 deployments within agencies will only add to operational issues and potential security problems. Initial IPv6 deployment designs should focus on achieving well identified success goals, providing a baseline approach from which agencies can grow future enterprise solutions based on IPv6, and providing the means from which their staff can gain first hand operational experience.
- **Segregate IP Connections:** Enclave approaches dictate a limited number of ingress and egress points for the enterprise architecture that need to be closely guarded and monitored. Thus, in many cases, these have become significant traffic points for interconnecting to the outside world. Agencies should consider installing parallel sets of IPv6 connections to the outside as opposed to running both IPv4 and IPv6 on their primary peering or Internet service provider (ISP) connections. This approach has no operational impact on established connections and allows agencies to be much more vigilant in analyzing the connections and traffic on IPv6 connections.
- **Divide and Conquer:** IP-based attacks have become increasingly sophisticated. This fact has driven the need for better and better security capabilities housed not only within specific security devices, such as firewalls and intrusion detection systems, but also in all devices connected to the network. This not only increases the complexity of the security devices, but also requires they support much more processor-intensive applications. Compounding the issue even more is that many security products have been slower to adopt IPv6 capabilities than other networking devices.

Similar to the rationale for segregating IP connections, agencies should consider implementing security devices specifically to meet their IPv6 needs. This approach allows agencies to maintain their current IPv4 security posture and to utilize specific security equipment solely focused on IPv6. While some modification will be necessary to the IPv4

equipment, the majority of the work and complexity can be relegated to the IPv6 specific devices. This approach provides minimal processing impact on existing infrastructure and can be used to significantly mitigate risks in deploying IPv6 within an agency's enterprise.

- **Information is Power:** One of the most effective security tools available is information. Not just raw data, but a thorough comprehension of information, preferably in real-time, of what is happening now. Agencies should focus on incorporating IPv6 solutions for data gathering and reporting into their routines as early as possible. In fact, agencies may want to provide an additional focus on this area during their IPv6 deployment and for a period of time following the initial roll out. The use of network sniffers and analysis tools designed to collect frame and packet-level information can be utilized to supplement other data collection techniques, and provide an in-depth benchmark to determine how well the agency's implementation of their security policy is working.
- **Slow (but Steady) Growth:** The initial deployment of IPv6 services within agencies in June 2008 primarily focuses on building the confidence and success that agencies will need to transform their entire enterprise to support IPv6. Thus, many agencies will not have a hard operational requirement in 2008 other than the ability to transport IPv6 packets. Therefore, agencies should develop a plan that promotes steady growth of IPv6 across their enterprise, but limits the deployments based on needs and the agency's ability to provide sufficient security to implement new capabilities. Initial deployments can utilize limited bandwidth and support a limited number of applications that can be closely monitored, while trials of other new capabilities such as VoIPv6 can be cordoned off to specific enclaves that will not create greater risks to the remainder of the enterprise.

To learn more:

This executive summary provides an overview of *An IPv6 Security Guide for U.S. Government Agencies*. This is the fourth volume in the IPv6 World Report Series. To request the complete version, please go to www.juniperIPv6.net.

Request the entire IPv6 World Report Series:

- Volume 1, *A Guide for Federal Agencies Transitioning to IPv6*
- Volume 2, *IPv6 Capable – A Guide for Federal Agencies: Understanding IPv6 Requirements and Technology to Enable the Next Generation Internet*
- Volume 3, *An Essential U.S. Government Agency Transition Guide to IPv6 Routing and Addressing*

Visit www.juniperIPv6.net or call 1.866.298.6428 for more information.

