IPv6: Network Security and the Next Generation of IP Communication
Summary

Many enterprises have IPv6 adoption on their technology roadmap due to the exhaustion of the IPv4 address space. To help organizations understand how IPv6 may affect their network security strategy, we will look at some of the issues related to migrating to IPv6.

A Brief History of the Internet Protocol Life Cycle

Internet Protocol version 4 (IPv4) was the first version of the Internet Protocol (IP) that was widely accepted and deployed by organizations worldwide. Defense Advanced Research Projects Agency (DARPA), the research and development office of the US Department of Defense, initially created IP addressing over thirty years ago. Although once projected to be exhausted in the 1990s, the IPv4 address space has been extended several times over the last three decades. The last block of IPv4 addresses was allocated in 2011, necessitating the migration to IPv6.

IPv6, the next generation Internet communication protocol, was developed as the replacement protocol for IPv4. The US Government and many service providers have embraced this new protocol in their networks. The public, on the other hand, has not had much interaction with this new protocol, and there has been limited private-sector adoption of IPv6. Nonetheless, many enterprises have IPv6 adoption on their technology roadmap due to the exhaustion of the address space, and are looking to understand how IPv6 may affect their network security strategy. In this document, we will examine IPv6 and how it may affect you.

The Benefits of IPv6

IPv6 was designed to improve upon some of the shortfalls and lessons learned from IPv4, which was originally designed in the late 1960s. The architecture of IPv6 includes a number of features and benefits that will address the future needs for global end-to-end communication. Some of the significant improvements in IPv6 over IPv4 include:

• **Addressing Capacity**
  Without any doubt, the most significant benefit of IPv6 is the drastic increase in addressing capacity over the existing IPv4 addressing space. Changing from 32-bit address to 128-bit address scheme, IPv6 supports 340,282,366,920,938,463,463,374,374,607,431,768, 211,456 addresses. That is 340 trillion trillion trillion addresses (compared to the 4 billion IPv4 addresses), enough to allocate billions of addresses per person.

• **Security**
  The other significant enhancement in IPv6 is the security incorporated into the protocol. IPsec is a proven standard for securing IP communications by encrypting the information contained in the IP datagram through encapsulation. IPsec provides data integrity, confidentiality, and authenticity to end-to-end IP based communication. IPsec in IPv4 is optional and proprietary in some implementations, which leads to compatibility issues. IPsec is required in IPv6 and it provides a standard-based security solution for devices, applications and services.

• **Quality of Service**
  Support for Quality of Service (QoS) in IPv4 networks is typically a “best level of effort” service, but there is no way for IPv4 protocol to differentiate time-sensitive packets from non-time-sensitive packets. IPv6 supports a more sophisticated approach to handle priority request and supports parameter adjustment to fit what the network can handle. IPv6 also supports “flow label” filed in the headers
whereby application flow-based resources reservation scheme can be added to complement the existing standard for IPv4 QoS.

- **Mobility**
  With the growing success of mobile devices such as smartphones and tablets, wireless broadband IP connectivity on mobile devices has become an essential service. Mobile IP (MIP) is the most widely accepted solution to handle IP handover between wireless networks and cell towers. Although there are standards to support MIP on IPv4, mobility is integrated into IPv6. Mobile IPv6 (MIPv6) allows mobile devices to move from one network to another network and still maintain existing connections. Built-in IPsec support in IPv6 enables secure signaling and communication between MIPv6 devices.

### Security Issues Related to IPv6

The transition from IPv4 to IPv6 is under way as more network and content providers embrace IPv6. As the amount of IPv6 traffic (and IPv6-based threats) increases in your network, it’s essential that you deploy a network security solution that can deliver the same level of protection for IPv6 content as IPv4. Organizations of all sizes need to understand the security implications of IPv6, which include:

- **IPv4 security devices cannot inspect IPv6 traffic**
  Although there are work-around measures to enable IPv4 network and security devices to forward IPv6 packets, IPv4 devices cannot inspect those packets for malicious content. This lack of visibility enables a simple evasion technique to avoid detection by legacy security devices—send malicious content via IPv6. This allows old threats to bypass policies that may have been in place for years. And, as long as the victim system can process IPv6, the attack will reach its intended target.

- **IPv6 is likely in your network today, as many systems (such as Windows 7) natively support IPv6 and ship with IPv6 support enabled**
  Many systems ship today with IPv6 support enabled by default. And, unless that support is specifically disabled, these devices will be vulnerable to threats transported via IPv6.

- **Some legacy security devices will never support IPv6 and will need to be replaced**
  Many network security devices require recently released versions of their operating systems to support IPv6. Unfortunately, not all devices can support the most recent releases due to lack of memory or other hardware-based limitations, requiring an upgrade to the latest hardware device. Without replacing the device, the network segments protected by these legacy systems will be blind to threats embedded within IPv6 traffic.

- **Many security vendors have limited support for IPv6 today, leading to potential gaps in protection**
  Supporting IPv6 with a dual-stack architecture is not a trivial development exercise; it requires a significant allocation of development resources to build a new stack and incorporate it with the existing IPv4 stack. Many vendors have only recently committed development resources to supporting IPv4, choosing to wait until demand for IPv6 support increased before allocating the necessary resources. One result of the delayed investment is that they will not be able to offer feature parity with their IPv4 devices, which has the potential to lead to years of gaps in IPv6 policy enforcement, as these vendors will struggle to make all key IPv4 features functional in IPv6.

- **IPv6 support is often at much slower performance**
  In addition to reduced functionality in their IPv6 support, many vendors rely on software only to filter traffic to detect threats. As stated above, the implementation of IPv6 support in a network security
device is not a trivial exercise. It requires significant investment and, like any other new technology, several product releases to deliver stable, mature functionality. One way to accelerate the speed with which they can bring IPv6 support to market, vendors of devices that utilize custom processors will release IPv6 support in software only. The advantage is that a software-only approach reduces the amount engineering effort required to bring the functionality to market. The disadvantage is that the performance of a software-only approach is significantly slower than a hardware-accelerated approach.

IPv6 around the World

NTT Research in Japan started one of the world’s largest IPv6 trial networks in 1996 and NTT Communication began its IPv6 tunneling trial services with more than 200 subscribers in 1999. By the end of 2003, IPv6 services were offered in NTT Europe, Korea, Taiwan, NTT Com Asia and Australia. Since 2009, NTT has offered a Service Level Agreement (SLA) guaranteeing 100% network availability with latency and packet loss levels to customers using IPv6 services on their global Tier 1 IP network.

In Europe, the growth of IPv6 implementation isn’t quite as rapid. An IPv6 implementation survey based on the response from the RIPE community, the Regional Internet Registry that consists mainly of ISPs, telecommunications organizations and large corporations in Europe, the Middle East and parts of Central Asia, in 2009 has shown a slow deployment amongst its members. Although 80% of the respondents have an IPv6 presence in their network, the majority of them indicated that the IPv6 traffic was insignificant. To jumpstart adoption of IPv6, there are pilot projects in many EU countries (such as the IPv6 pilot GEN6, for public agencies).

In the U.S., the Office of Management and Budget (OMB) set a deadline for all federal agencies to upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012 (the agencies can continue to use IPv4 in their internal network until Sept. 30, 2014). Elements of the US government have embraced IPv6, such as the Department of Defense (DOD), which set IPv6 as the mandatory standard in 2005. Migrating to IPv6 enables ubiquitous security services for end-to-end network communication, which will provide the foundation for the future security of federal IT systems.

On the service and content provider side in the US, many of the largest service providers have permanently enabled IPv6:

- AT&T
- Comcast
- Free Telecom
- Internode
- KDDI
- Time Warner Cable
- XS4ALL

Many large content providers have also permanently enabled IPv6 traffic, including:

- Facebook
- Google
- Microsoft Bing
- Yahoo!

Clearly, the deployment of IPv6 is occurring across the world in both public and private sectors. While the transition from IPv4 to IPv6 may not have happened as rapidly as some IPv6 proponents had wished, IPv6 is certainly gaining ground as the next generation communication protocol.
Fortinet's IPv6 Security Solution

The Fortinet FortiGate consolidated security platforms offer unmatched performance, flexibility, and security from remote offices to large enterprises, service providers, and carriers.

Certified Security

FortiGate platforms have supported IPv6 since 2003, and achieved the US Department of Defense (DoD) IPv6 product certification conducted by the Joint Interoperability Test Command (JITC). FortiGate appliances have been listed on the DoD’s Unified Capabilities Approved Products List (UC APL) for IPv6 since 2008. [http://jitc.fhu.disa.mil/apl/ipv6.html#security](http://jitc.fhu.disa.mil/apl/ipv6.html#security)

The FortiOS operating system running on all FortiGate consolidated security appliances has also received the IPv6 Ready Logo Program from IPv6 Forum, a worldwide consortium that provides technical guidance for the deployment of IPv6 technology. The FortiOS operating system has successfully fulfilled all the requirements for IPv6 Phase-2 Core Support as a router product validating the interoperability of FortiGate appliances with other IPv6 products. [http://www.fortinet.com/press_releases/080225.html](http://www.fortinet.com/press_releases/080225.html)

Compatible with both IPv4 and IPv6

FortiOS has implemented a dual stack architecture that recognizes both IPv4 and IPv6 traffic. Dual stack support is critical to the implementation of IPv6 networks, as it will not be possible to operate an IPv6 network without interoperating with IPv4. FortiOS supports the following IPv6 features:

- Complete content protection for IPv6 traffic including Firewall, IPS, Application Control, Antivirus, Web filtering, DLP and Email Filtering
- IPsec VPN
- Dynamic routing protocol for IPv6: RIPv6, OSPFv3 and BGP+
- Routing access lists and prefix lists
- IPv6 tunnel over IPv4
- IPv4 tunnel over IPv6
- Dual protocol stack support
- Firewall policies
- Packet and network sniffing
- Bi-directional traffic shaping
- NAT/Route and Transparent mode
- Logging and reporting
- IPv6 specific troubleshooting such as ping6

For the most up to date IPv6 features list, refer to the latest FortiOS operation system release notes and System Administration Guide for details, available at [http://docs.fortinet.com](http://docs.fortinet.com). You can also refer to *Inside FortiOS*
Internet Protocol version 6 available on http://docs.fortinet.com for more information on how to architect a FortiGate appliance for different IPv6 implementations.

Unmatched IPv6 Performance - The World’s Fastest IPv6 Firewall

The FortiGate-5140B chassis, loaded with FortiGate-5101C blades, delivered 536 Gbps IPv6 throughput performance in a test using BreakingPoint FireStorm CTM™ devices to generate real-world traffic. The results of the testing, available on www.fortinet.com, demonstrate that the FortiGate solution is the World’s Fastest IPv6 Firewall, several times faster than the competition. In addition to measuring over 500 Gbps of IPv6 performance, the testing also measured 1.4 million new connections per second during the tests with application content, as well as a low frame latency of 4.5 s.

These test results demonstrate the ability of the FortiGate solution to deliver the extremely high throughput needed when transferring large volumes of content and application traffic across a network. The high connections per second rate verify the FortiGate solution’s ability to support today’s mobile traffic, which generates connections at a much higher rate than traditional wired networks. Lastly, the low latency illustrates that the FortiGate solution can seamlessly support IPv6-based network applications such as VoIP or video without degrading the end-user experience.

Summary

The deployment of IPv6 enables worldwide IP–based devices to seamlessly communicate and interoperate much more efficiently. Global communication networks have begun a major transition period from IPv4 to IPv6 that will last for years, and Fortinet offers unmatched network security to both IPv4 and IPv6 networks. Support for IPv4 and IPv6 on FortiGate consolidated security appliances has been tested and verified by 3rd party test labs appointed by the U.S. government, and deployed in many major organizations and government agencies. With comprehensive global security threat research team in-house, Fortinet also delivers continuous updates to its security platforms, delivering real-time protection for any corporation or government agency migrating to an IPv6 network.