SOLUTION GUIDE

IPv6 and Fortinet: Network Security in the Next Generation of IP Communication

Abstract

With the recent exhaustion of the IPv4 address space, many organizations are interested in learning more about the migration to IPv6. This document examines the major benefits of IPv6 and the rate of adoption of IPv6 around the world. It also provides an overview of some of the major challenges organizations face with IPv6, and how Fortinet supports IPv6 today.

Internet Protocol v4 Life Cycle

Internet Protocol version 4 (IPv4) is 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 U.S. 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. In February 2011, the Internet Assigned Numbers Authority (IANA) allocated the last blocks of available IPv4 addresses.

IPv6, the next generation Internet communication protocol, was developed as the replacement protocol for IPv4. Although the U.S. Government and many service providers have IPv6 initiatives in place, there has been little private-sector adoption of IPv6. Nonetheless, many enterprises now 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.

The Benefits of IPv6

IPv6 drastically changes the supply of IP addresses from 4 billion IPv4 addresses to 340 trillion trillion trillion IPv6 addresses (2^{128} addresses). IPv6 also promises enhancements over IPv4 including better security, improved addressing, routing efficiency, and quality of service. IPv6 is designed to improve upon some of the shortfalls and lessons learned from IPv4. The architecture of IPv6 includes a number of features and benefits that will address the future needs for global end-to-end communication. Here is a brief summary of some of the IPv6 improvements over IPv4:

- **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 340,282,366,920,938,463,463,374,607,431,768, 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. The volume of addresses available means that large-scale address scanning by an attacker becomes virtually impossible. Similarly, it will be improbable to identify an assigned address through the random generation of IPv6 addresses, meaning that hackers will no longer be able to benefit from a lucky guess to find a vulnerable system.
- **Security**
  The other significant enhancement in IPv6 is the security baked 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 becomes a protocol requirement 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 smartphone, tablet and netbooks, 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.

IPv6 around the world

IPv6 adoption has historically varied from region to region, with the Asia Pacific region being having the most advanced private sector initiatives. 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 offers 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 is limited. An IPv6 implementation survey in 2009, 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), showed 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. Vendor support, cost, and viable business cases were the top three hurdles viewed by the survey respondents who have and haven't implemented IPv6. However, over 70% of the respondents voted the main driver to IPv6 deployment is to be "ahead of the game".

In the U.S., the government's Office of Management and Budget (OMB) set a deadline for all the federal agencies to be up and running with IPv6 by June 2008. The U.S. Department of Defense (DOD) set IPv6 as the mandatory standard in 2005. In September 2010, White House CIO Vivek Kundra announced that all the public-facing networks of the U.S. agencies are to switch to IPv6 by September 30, 2012, while the agencies can continue to use IPv4 in their internal network until Sept. 30, 2014. Kundra noted that the move would reduce the complexity of Internet service as it eliminates the reliance on network address translation (NAT) technologies. Furthermore, transition 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 provider side, some are moving more aggressively than the others. Comcast is one of the most vocal proponents of IPv6 in the cable service provider industry, with current public trials that have attracted over 7,000 business and residential customers. Comcast is targeting to transition its nationwide network to support IPv6 by 2012. Verizon began deploying IPv6 protocol in 1998 for its very high-performance backbone network service (vBNS) for its government customers, and continues to deploy additional IPv6 services on its public and private IP global networks used by enterprise customers. It began testing its all-fiber FiOS network with IPv6 protocol in 2010.

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 of the IPv6 proponents had wished, IPv6 is inevitable now that there are no more IPv4 address blocks to allocate.

Implications of the IPv6 Migration

A detailed explanation of IPv4 to IPv6 migration is beyond the scope of this paper, but it is essential for organizations to understand the implications of IPv6 on their network infrastructure in general and security infrastructure in particular.

IPv4 to IPv6 Migration Mechanisms

Until IPv6 replaces IPv4, there are mechanisms in place to enable communication between IPv6-only devices and networks with IPv4-only devices and networks. The three most common are dual-stack, tunneling, and network address translation/protocol translation:

- "Dual-Stack" refers to separate IPv4 and IPv6 protocol stacks running at the same time, to enable the network to support the data regardless of the version of the protocol. This approach is the best of the three, as devices can run both IPv4 and IPv6, with IPv6 the preferred protocol. A device running dual stacks has the ability to process data in both protocols natively.
- "Tunneling" refers to encapsulating IPv6 packets in IPv4 packets, to enable IPv4-only devices to support the handling of IPv6 data. Although it provides a work-around for IPv4 networks to work with IPv6 traffic, it has the limitation of preventing non-IPv6 compliant security devices from inspecting the traffic. The IPv4 headers allow the packets to traverse a device, but lack of native protocol support blocks any content inspection.
- "Network Address Translation – Protocol Translation" refers to the translating of IPv6 packets into IPv4 packets, to enable an IPv4-only device to connect directly to an IPv6-only device. This approach is significantly more complex than dual-stack and tunneling

Potential Security Blind Spots

The most important issue facing organizations of any size is the inability of legacy security, network, and peripheral devices to support IPv6. Many older firewalls, UTM systems, intrusion preventions systems, routers, switches, and printers, will not be able to run the most recent versions of firmware needed to support IPv6 natively. As there is very little content delivered via IPv6 today, this issue is not critical. However, as more content and service providers begin to transition to IPv6, it is essential that organizations deploy network security devices that can deliver the same level of protection for IPv6 content as IPv4.

With only limited IPv6 support, a security device may be able pass a packet of data from one side of the firewall to the other, but will not be able to inspect the contents for malicious code or unwanted content. This represents a significant blind spot in any organization's security infrastructure, as content-based threats are independent of network protocol. In other words, the malicious behavior initiated by an unknown application or the malware used to propagate bots within a network will occur over IPv4 as well as IPv6.

Fortinet 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. FortiOS™, our purpose-built operating system for the FortiGate™ family of consolidated security appliances, delivers the same core network security technologies via IPv6 as it does via IPv4. To be able to support both IPv4 and IPv6, FortiOS implements a dual stack architecture that recognizes and separately routes both IPv4 and IPv6. In addition to routing, most vital FortiOS network and content protection security features are now fully supported in IPv6. FortiOS uses IPv6 firewall policies to provide UTM protection for IPv6 traffic. Antivirus, web filtering, FortiGuard™ Web Filtering, email filtering, FortiGuard Email Filtering, data leak prevention

(DLP), and VoIP protection features can be enabled in IPv6 firewall policies using normal FortiOS UTM profiles for each UTM feature. This protection is transparent to IPv6 Users.

Certified Security

FortiGate platforms have supported IPv6 since 2007, 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

JITC Certified

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 since 2008. 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. Figure 1 below shows the configuration page for Firewall policies for IPv6 traffic, and Figure 2 shows an antivirus policy detecting malware and identifying the source and destination IPv6 addresses.

The current version of FortiOS supports the following IPv6 features:

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

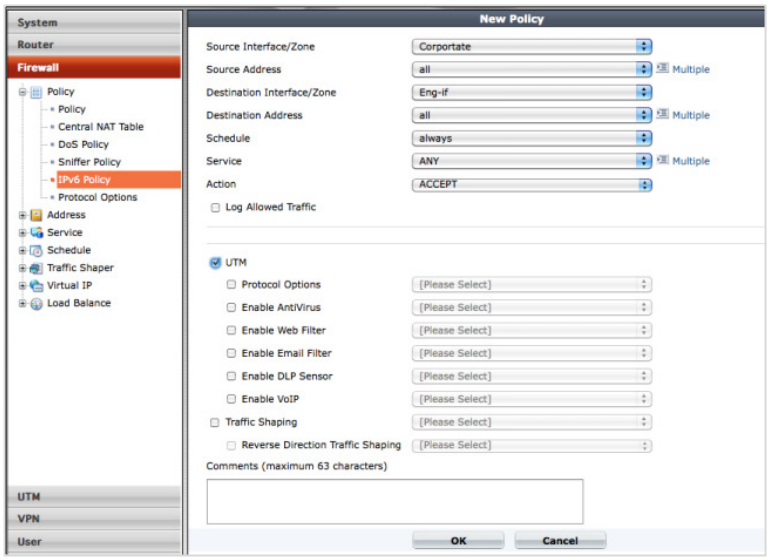

Fig 1: FortiOS GUI – IPv6 Firewall Policy Creation

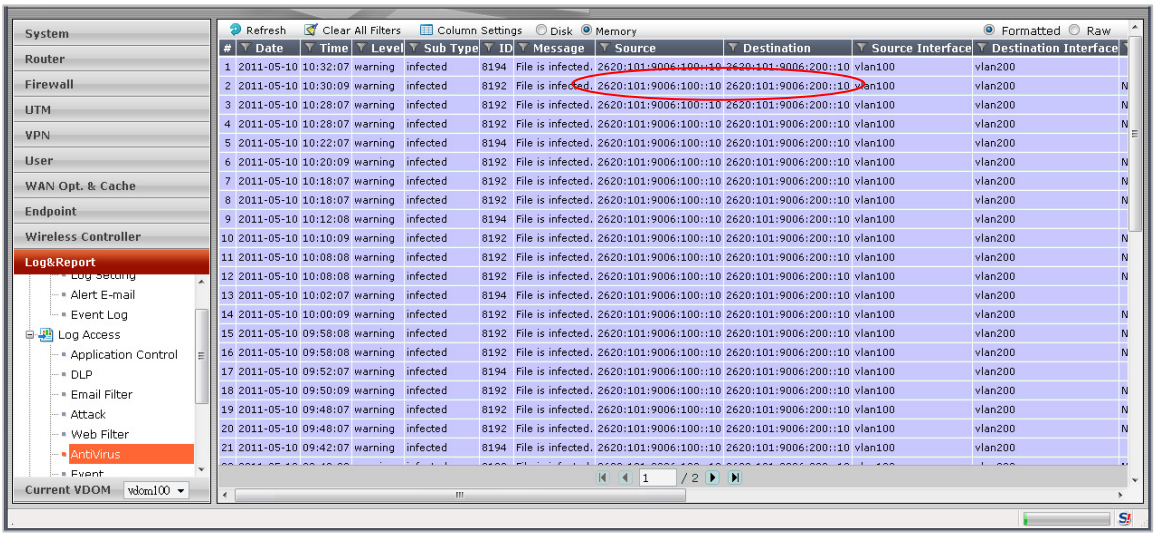

Fig 2: FortiOS GUI – IPv6 Antivirus Policy in Action

Hardware-accelerated IPv6 Security

Fortinet also delivers hardware-accelerated IPv6 support with its FortiGate-5000 series chassis-based devices, FortiGate-3000 series appliances and the FortiGate-1240B appliance. BreakingPoint validated the FortGate-5140 chassis' ability to deliver high performance protection for IPv6 traffic as IPv4.

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. You can also refer to the Inside FortiOS Internet Protocol version 6 document available on http://docs.fortinet.com for more information on how to architect a FortiGate appliance for different IPv6 implementations.

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. 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. Fortinet has the expertise and vision to ensure that any corporation or government agency migrating to an IPv6 network will receive the highest levels of protection against any emerging threats.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road #20-01, The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

SG-IPV6-R3-201106