FORTINET

WHITE PAPER

Biting the Bullet: A Practical Guide for Beginning the Migration to IPv6

Abstract

As many network administrators initiate their IPv6 migration projects, other IT professionals do not know where to begin. This white paper first describes the importance of securing the network against IPv6 threats well before the introduction of any IPv6 traffic. It then outlines the steps involved to begin securing a transitional IPv4/IPv6 network.

Introduction

Most Information Technology professionals subscribe to a proven philosophy: “If it isn’t broken, there’s no need to fix it.” This approach has served the industry well, and it remains the dominant thinking regarding the global networking communications standard, IP (Internet Protocol). IP version 4 works just fine. Yes, the address space is nearly exhausted, but Network Address Translation (NAT) solves this particular problem, and it will take years before organizations are forced to transition their networks to the next version of IP. Crisis averted; back to solving real problems.

IP version 6 is, nevertheless, inevitable. One day, a strategic customer or service provider will make the transition, forcing you to follow. Or, a new, highly desirable application or service will work only with IPv6. The amount of IPv6 traffic might even be relatively insignificant. Regardless, it could expose the organization to some new and serious threats, and suddenly the network would, in fact, be broken to one extent or another—perhaps catastrophically.

This white paper, intended for IT managers, consists of two main sections followed by a brief conclusion. The first section describes the importance of securing the network against IPv6 threats well before the introduction of any IPv6 traffic. The second section outlines the steps involved to begin securing a transitional IPv4/IPv6 network.

First: Do No Harm

This other proven philosophy, which physicians use for patient care, applies equally here to IT. Some organizations believe the proper way to begin the migration to IPv6 is to upgrade the network infrastructure first, usually in the routers from the core to the edge. This fundamental change might even be occurring unintentionally because of a scheduled technology refresh and/or during routine software updates. For example, it is common for vendors to enable new features supporting IPv6 by default.

The problem is: If the core network security products, including the firewall, application control, intrusion prevention and anti-malware provisions have not yet been upgraded to support IPv6, but the IP routing infrastructure has, then the network is now vulnerable to real harm. In other words, it could be broken and in urgent need of fixing.

IPv4-to-IPv6 migration is a very complex subject that is well beyond the scope of this document. Indeed, a wealth of guidance is available from numerous sources on the many issues involved. However, it is necessary here, in the context of security, to consider at least some of the vulnerabilities that might accompany the introduction of IPv6 traffic into the network infrastructure.

The specific vulnerabilities that could exist in any network infrastructure depend on the existing security provisions and their configuration. Every network does have one important characteristic in common, however: an increase in the number of attack vectors in two of the transitional techniques used, traffic tunneling and translation.

With IPv6-in-IPv4 (6in4) tunneling, for example, it may be impossible to enforce security policies that depend on the source and destination addresses embedded in the packets. Alternatively, the processor used for deep packet inspection may stumble on the unusual packet formats used for both tunneling and translation. Or an increase in packet fragmentation could similarly confuse and/or overwhelm traffic inspection algorithms.

Another consideration is that some security or networking systems, which currently process IPv4 in hardware, may process IPv6 packets exclusively in software. It takes time to implement key features in an ASIC or other form of hardware-based acceleration, and many vendors have chosen to wait until there is sufficient demand for native IPv6 support before investing scarce R&D resources in the effort. In addition to reducing system performance, executing complex packet inspection calculations in software inevitably makes systems more vulnerable to Denial of Service (DoS), Distributed DoS and other forms of attack that attempt to overwhelm CPU resources.

Hackers clearly recognize the existence of these new vulnerabilities, and have already begun to exploit them. According to an *InformationWeek Analytics* report on IPv6 security: “There are black hats out there who see IPv6 as a once-in-a-lifetime opportunity. So much new code, so much time to probe for flaws.” Fortunately, organizations can minimize the potential flaws in any network with some cost-effective changes.

Three Steps to IPv6-Ready Network Security

Even if your organization wishes to postpone beginning the migration to IPv6, it is important to consider this cruel irony: To avoid having any IPv6 traffic on the network it is necessary to implement IPv6. This is the only way to block all (or at least all unwanted) native, tunneled and/or translated IPv6 traffic. Then, when the organization is ready to begin the migration, it can change the security policies to permit IPv6 traffic for some or all applications.

The migration to IPv6 (whether now or later) will occur gradually, which will require the security provisions to support both IPv4 and IPv6 for an extended period. The preferred method is a “dual stack” configuration, which supports IPv6 traffic in its native mode (in the IPv6 stack) and its tunneled or translated form (in the IPv4stack).

Here are three steps organizations should take to prepare for the inevitable migration:

1. **Take an inventory** IPv6 will ultimately affect every device and application in the network. The first step in a successful migration, therefore, is to inventory all devices that are connected to the network. The most critical devices are those in the network infrastructure itself, especially the routers and security systems, from the core to the edge. It is also important, however, to inventory the servers, network attached storage (if IP-based), peripheral devices like printers, and clients.

2. **Research available alternatives** After taking inventory, review each vendor's IPv6 roadmap and timeframe for full compliance. This research will reveal both the vendor's level of preparedness and whether its systems require a simple software update, a hardware upgrade or a "forklift" replacement. Here are some additional guidelines for conducting this research:

    - *Be sure to look under the hood*. It is important to be certain that your vendors will deliver feature parity in IPv6. In the network security industry, for example, many vendors claim to support IPv6. But being able to pass an IPv6 packet from one side of a firewall to the other is not the same as being able to perform deep packet inspection to eliminate malicious content and/or block unwanted applications.

    - *Don't believe everything you read*. Make sure you can validate the vendor's claims. For network security, this may require testing a product's ability to detect and block the same threats for IPv6 that it can for IPv4.

    - *Examine the robustness of the IPv6 solution*. Is the vendor shipping complete and fully compliant IPv6 products? On the other hand, is it currently offering only limited support for IPv6, which will require a potentially costly and disruptive upgrade later? The best

Fortinet's Support for IPv6

Fortinet began supporting IPv6 on the FortiGate® consolidated security solutions in 2007. The dual-stack implementation has been tested and verified by third-party test labs appointed by the U.S. government. Many large enterprises, service provider, and government agency networks have successfully deployed it. Fortinet also provides regular updates to its security platforms via its FortiGuard Security Services, delivering real-time protection for any organization migrating to IPv6.

The dual-stack FortiGate solution achieved the U.S. Department of Defense (DoD) IPv6 product certification conducted by the Joint Interoperability Test Command (JITC), and FortiGate appliances have been listed on the DoD's Unified Capabilities Approved Products List (UC APL) for IPv6 since 2008. The FortiOS™ operating system running on all FortiGate appliances has also received IPv6 Ready Logo Program certification from the IPv6 Forum, a worldwide consortium that provides technical guidance for the deployment of IPv6 technology.

The FortiOS operating system has successfully fulfilled all requirements for IPv6 Phase-2 Core Support as a router product, thereby validating the interoperability of FortiGate appliances with other IPv6 products. Fortinet's FortiAnalyzer™ and FortiManager™ systems provide integrated centralized management, advanced provisioning, reporting, logging, alerts and event correlation for Fortinet's security products.

way to do this is to verify that respected, vendor-neutral third parties have certified the products.

3. **Budget for and implement the desired solution** Research into the options available for all systems should reveal the best course of action for each. Some systems may support IPv6 satisfactorily with a routine update or an inexpensive hardware and/or software upgrade. Budget for and implement these first. Then address those systems that require replacement. Ideally, the replacement would fit into a scheduled technology refresh cycle. However, it could be a mistake to postpone replacing critical security provisions that might expose the organization to some potentially serious vulnerabilities. The last thing any IT manager needs, after all, it to have to explain why she needs an emergency budget allocation to address a problem that could and should have been foreseen.

Conclusion

If it isn't broken now, it will be soon. The "it" here is your enterprise network. IPv6 is inevitable, and so too are the vulnerabilities that will continue to exist in networks that remain unprotected. An IT manager's top priority should be, therefore, to ensure first that he does no to the patient (read: the organization's network).

Yes, upgrading and/or replacing the security provisions throughout the entire network infrastructure will take hard work and could be expensive. But in IT's role as the physician taking care of the enterprise network, one additional old adage is worth remembering: *An ounce of prevention is worth a pound of cure.*

To learn more about IPv6 support in Fortinet's family of enterprise network security solutions, please visit Fortinet at www.fortinet.com.

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

WP-IPV6-R3-201106