SOPHOS
simple + secure

Why switch to IPv6?

Internet Protocol (IP), one of the core components of the Internet, is the system that allows machines and devices to find and connect to each other online. The version we use today, IPv4, was designed in the early 1980s — a time when no one could have predicted the explosive growth of the Internet. Its successor-in-waiting, IPv6, has the features and solutions the modern Internet requires that IPv4 can't provide: greater connection integrity and security as well as the ability to support the vast number of web-capable devices we'll need for a long time to come. But even as IPv6 brings some security enhancements, its significant changes could also introduce security holes into your environment. So why would anyone want to adopt IPv6 if it could be troublesome?

By James Lyne, Director of Technology Strategy, Sophos

A Sophos white paper - May 2011

For years, regulators and Internet experts have warned about the impending exhaustion of IPv4's limited pool of addresses. Although estimates vary from years to decades, lately they've converged on the next few years. More and more new devices, platforms and services include support for IPv6, but so far mass migration has been delayed again and again. The lack of widespread public understanding of the benefits along with general fears of the difficulty and complexity of the migration process all contribute to the slow pace of IPv6's adoption.

The transition to IPv6 is inevitable, but migration to IPv6 requires considerable effort, preparation and consideration. If done incorrectly or incompletely, it can leave gaping security holes in your network systems. Without careful planning, you could accidentally run both IPv4 and IPv6 in parallel, effectively nullifying any security measures you have in place around either protocol.

That's why it's vital that security solutions and practices provide full compatibility with the new infrastructures, while users delaying the migration process need to make sure any potential holes in their current protective layers are covered.

What's the problem with IPv4?

When IPv4 first emerged in 1981, the 4 billion or so addresses it could provide seemed like a massive figure, given the relatively limited number of computers at the time. Three decades later, computers are commonplace and a wide variety of other devices also use network connections, from smartphones, tablets and handhelds to game consoles, TVs and even cars and fridges. Suddenly those 4 billion addresses in the available address pool seem massively inadequate.

Of course, there are workarounds to the address shortage — notably network address translation (NAT), which lets a large number of devices connect from behind a single address, stretching the available public addresses further. NAT, shared services and Classless Inter-Domain Routing (CIDR) all help mitigate the scarcity of available addresses. These workarounds have been in use for some time, but even they are becoming challenged by Internet growth. Internet regulators are frantically trying to claw back unused addresses, renumbering and tightening distribution rules to squeeze as much as they can from the current system. But these measures are temporary and inefficient, and represent serious challenges in designing and implementing proper security and scalability.

The advantages of IPv6

IPv6 offers a significantly larger pool of addresses by using 128-bit addresses: 340 undecillion (3.4×1038), compared with the 4.3 billion available in 32-bit IPv4 addresses. This extended pool of addresses provides scalability, but also introduces additional security by making host scanning and identification more challenging for attackers. But IPv6 provides more than just new addresses — it also provides a range of benefits for security, integrity and performance.

Security benefits

IPv6 was built from the ground up to be capable of end-to-end encryption. While this technology was retrofitted into IPv4, it remains an optional extra and isn't universally used. The encryption and integrity-checking used in current VPNs is a standard component in IPv6, available for all connections and supported by all compatible devices and systems. Widespread adoption of IPv6, when properly implemented, could therefore make man-in-the-middle (MITM) attacks significantly more difficult.

IPv6 also supports more-secure name resolution. The Secure Neighbor Discovery (SEND) protocol is capable of enabling cryptographic confirmation that a host is who it claims to be at connection time. This renders Address Resolution Protocol (ARP) poisoning and other naming-based attacks much more difficult. And while not a replacement for application- or service-layer verification, it still offers a greatly improved level of trust in connections. In an IPv4 network it's fairly easy for an attacker to redirect traffic between two legitimate hosts, allowing him to manipulate the conversation or at least observe it. IPv6 makes this very hard. (Not all device and OS implementations of IPv6 have applied this feature yet.)

This added security depends entirely on proper design and implementation, and the more complex and flexible infrastructure of IPv6 makes for more work ensuring every "t" is crossed and every "i" dotted. Nevertheless, properly configured IPv6 networking will be significantly more secure than its predecessor.

Performance benefits

Data packets transferred under IPv4 are severely size-restricted, and those that are too big must be fragmented and reassembled. Routers and other intermediary devices along the transport path handle this fragmentation, but the work involved can be inefficient, time-consuming and ultimately costly. Under IPv6, the protocol design incorporates end-to-end fragmentation, simplifying and lightening the load of handling fragmented packets. With less work required to identify and properly split data, speed goes up and the workload along the transport path goes down.

IPv6 also does away with the need for integrity-checking of packets during transit, leaving this to higher-level protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), freeing up valuable router time that can be better spent pushing data around as fast as possible.

There are also notable benefits in IPv6 for mobile devices, which will be able to maintain the same address when moving from one connection to another — going from a 3G network to Wi-Fi provided by your local coffee shop, for example. Rather than picking up a new address from the new connection service, the mobile device can keep the same "home" address at all times. This removes the need for "triangular routing," in which data sent to the mobile device must first go through the network of the mobile provider. These changes not only provide greater speed, simplicity and usability, but also make connections more resilient and secure. Given the prevalence of mobile devices today, this enhancement should be most welcome.

Thanks to improved identity checking, IPv6 avoids many of the performance and security issues surrounding Multicast and Anycast broadcasting, and offers better autoconfiguration, with ICMP6 messages used to determine an appropriate address and configuration. Upgraded DCHP6 is also available for those who require more stateful control of network connections, and of course conventional static address assignment is possible if needed. The combination of a wider address pool and a more sophisticated address structure solves a lot of address conflict issues, which arise most commonly when company mergers or takeovers lead to integration and readdressing of networks. Organization-specific prefixes are a core part of the IPv6 infrastructure, and ensure no collisions even when lower portions of address overlap. Changing addressing structures is also simpler and more efficient.

What are the problems with IPv6?

Several vulnerabilities in the IPv6 infrastructure have already come to light. One issue, which has been fixed since its discovery, concerns the Router Heading Type 0 (RH0) "feature," which proved potentially useful in running DDOS attacks and forging host identities. It's likely we'll see more problems as adoption of IPv6 picks up and people spend more time and effort analyzing how to subvert its built-in security. Similar issues were and still are present in IPv4, and as new problems are uncovered, we'll need new methods and tools to overcome them.

Proper deployment and configuration is also a serious issue. Because attempting to deploy IPv6 in the same way as IPv4 guarantees problems, IT administrators must learn a whole new approach to networking, from simple network troubleshooting to configuring firewalls and monitoring security logs. The new knowledge so administrators will need leave many opportunities for confusion and mistakes.

There's no instant switch to change from IPv4 to IPv6, so partial adoption means using tunneling technologies to transport IPv6 over IPv4. This kind of workaround is another potential source of confusion, misconfiguration and security gaps.

So far the bad guys have paid little attention to IPv6, thanks mainly to its limited adoption, but already we've seen widespread malware with IPv6-based command-and-control capabilities. Given the relative lack of attention paid to IPv6, this technique can bypass existing protection completely. (Your server might enable IPv6 by default but your firewall might not.) As adoption picks up and more people look in to IPv6, we'll inevitably see more flaws and ways of abusing the system for malicious ends.

What help can I expect from my security provider?

Security providers need to be on the ball regarding the IPv6 switchover. Many security products will require changes to handle new networking patterns, both as a transport medium for updates, lookups, and management and reporting systems and as a means to ensure continued provision of scanning and protection features.

Going forward, it's inevitable that fundamental approaches to security will evolve as network practices change. We'll see new vulnerabilities and threat vectors appear — and security providers must be ready to face them.

One of the clearest shifts in security practices will be toward the endpoint, as greater use of end-to-end encryption makes perimeter security difficult and inefficient. For example, network DLP technologies will struggle to inspect content as it is encrypted until it reaches the endpoint. Combined with users' tendency to roam (their traffic not necessarily even routing through the corporate network), this forces a much more endpoint-centric approach to security. Corporate, academic and government networks will face such significant decisions as whether to implement Internet Protocol security across the board or to keep existing gateway-level filters and scanners, and whether to allow encryption to ensure data reaches the endpoint intact and unseen, or to disable it to allow internal checking, filtering and possible snooping. This is a deep and complex question, involving a potential conflict between security and privacy, but given the growing trend away from the perimeter for other reasons, all quality security providers must be moving toward enabling more complete security provision at the desktop level.

Security vendors will need to invest time and money to ensure proper and complete support for IPv6, and must stay alert for the new dangers IPv6's adoption will bring.

So what do I need to do?

Migration to IPv6 is no longer a question of if, but when. Services like Google and Facebook are already available via IPv6. Several large ISPs, telecommunications and web service providers are now either running trials or actively migrating. Mobile operators are increasingly pushing for wider IPv6 implementation to support their high-speed networks. This means all businesses should consider their adoption plans, if they haven't already. On June 8, 2011, World IPv6 Day will see major providers around the world running full public tests on IPv6. We should all watch the results carefully and start to build our own pragmatic plans.

You should think through the design and configuration of your adoption plans to ensure minimal disruption and maximum satisfaction. There are a number of key issues to bear in mind when planning and implementing the switch:

1. Be cautious when using tunneling during the initial overlap period. While tunnels can provide vital connectivity between IPv4 and IPv6 components, or enable partial IPv6 in parts of networks still based on IPv4, they can also introduce notable security risks. For example, tunnels can cut through your perimeter firewall rules, but might be less restricted than your firewall. This could allow attackers to connect to resources inside the "hard shell" of your network without your knowledge. Complexity is always a danger, so keep tunnels to a minimum and use them only where absolutely necessary. Carefully check the setup of "automatic tunneling" tools such as "6to4" and Teredo. Traffic tunneling will also make network security systems (e.g., IPS devices) much less likely to identify attacks.

2. Remember to look at the bigger picture. Network layout under IPv6 is very different from that under IPv4, so simply replicating your existing setup will not provide ideal results. You need to significantly redesign your network structures to get the best out of IPv6 (detailed guides are available from vendors such as Cisco and Microsoft). Plan for this at the outset, rather than running multiple migrations, to avoid problems with performance and security. Also, be sure to consider the architecture of both the Internet facing and LAN resources — don't casually get rid of your DMZ!

3. Check that your entire networking infrastructure is compatible and up to date. It's easy to miss switches and routers in patching regimes, and you may need to update these to the latest versions of firmware and software. Check that these devices are ready for IPv6; if they aren't, have a plan to make them so over time. At first, IPv6 could introduce more risks at the protocol level (as we all learn about using it in a real environment), so make sure you pay close attention to patching. Many organizations do not include their network infrastructure in their patching plans, which can leave them open to very nasty attacks. This would be a good time to check your processes in this area.

4. Make sure all your security solutions are up to the job. More use of IPSec is a great idea and fully supported by IPv6, but the end-to-end encryption may interfere with some perimeter-level security processes. Protection may have to migrate closer to the desktop level, so ensure desktop security includes Data Loss Prevention (DLP) and web security. You may need to upgrade or reconfigure your firewalls as well. Check that your endpoint provider has the full range of controls you require to replace conventional perimeter controls.

5. Don't enable IPv6 until you're fully ready. Many platforms come with IPv6 enabled by default, but make sure it's switched off until properly configured. Many current firewalls focus exclusively on IPv4 and will not filter IPv6 traffic at all — leaving systems completely exposed. Disable unnecessary services and check the ports and protocols used by the services you need. I've seen numerous customer systems running IPv6 by default, which could allow attackers to bypass their security controls and wreak havoc. You can find easy instructions online for enabling/disabling IPv6 on Linux, Mac and Windows.

Sophos Products

Sophos has already invested in capabilities in our endpoint product to restrict the use of IPv6 until you're ready to use it. We continue to invest in developing IPv6 capabilities at the endpoint to ensure readiness in appropriate time frames for enterprise transition. As use of IPv6 increases, the implementation and security requirements for IPv6 will evolve. We will continue to make sure we deliver the right protection to our customers.

Above all, don't panic! It's far better to spot potential problems at the planning stage than halfway through implementation. Start planning as soon as possible to avoid rushing as global migration gathers speed. The switch to IPv6 may seem like a big deal, but the key is to take it step by step and make sure all your bases are covered before you begin.

Consider both security and usability at every step, and the migration process can be smooth, straightforward and problem-free.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK

SOPHOS