

Sponsored by:



This story appeared on Network World at <http://www.networkworld.com/news/2009/071309-rogue-ipv6.html>

## Invisible IPv6 traffic poses serious network threat

Odds are you have hidden tunnels on your network carrying IPv6 traffic--and possibly IPv6-based attacks

By [Carolyn Duffy Marsan](#), Network World, 07/13/2009

Sponsored by:

[IPv6](#) — the next-generation Internet protocol — isn't keeping too many U.S. CIOs and network managers up worrying at night. But perhaps it should.

[View our slideshow on The Evolution of the Internet](#)  
[See what's driving a Florida university to IPv6.](#)

Experts say that most U.S. organizations have hidden IPv6 traffic running across their networks, and that few network managers are equipped to see, manage or block it. Increasingly, this rogue IPv6 traffic includes attacks such as [botnet](#) command and controls.

"If you aren't monitoring your network for [IPv6](#) traffic, the IPv6 pathway can be used as an avenue of attack," says Tim LeMaster, director of systems engineering for Juniper's federal group. "What network managers don't understand is that they can have a user running IPv6 on a host and someone could be sending malicious traffic to that host without them knowing it."

Most U.S. network managers are blind to rogue IPv6 traffic because they don't have [IPv6-aware firewalls](#), intrusion detection systems or network management tools. Also, IPv6 traffic is being [tunneled](#) over IPv4 connections and appears to be regular IPv4 packets unless an organization has deployed [security](#) mechanisms that can inspect tunneled traffic. (See also: [5 of the biggest IPv6-based threats facing](#) CIOs.)

"At least half of U.S. CIOs have IPv6 on their networks that they don't know about, but the hackers do," says Yanick Pouffary, technology director for the North American [IPv6 Task Force](#) and an HP Distinguished Technologist. "You can't ignore IPv6. You need to take the minimum steps to secure your perimeter. You need firewalls that understand IPv4 and IPv6. You need network management tools that understand IPv4 and IPv6."

"Although they're not thinking about IPv6, for most of the Fortune 500, it's in their networks anyways," agrees Dave West, director of systems engineering for Cisco's public sector group. "You may not see IPv6 today as a business driver. But like it or not, you are running IPv6 in your network."

IPv6 is the long-anticipated upgrade to the Internet's main communications protocol, known as IPv4. IPv6 features vastly more address space, built-in security and enhanced support for streaming media and peer-to-peer applications. Available for a decade, IPv6 has been slow to catch on in the United States. Now that unallocated IPv4 addresses are expected to [run out in 2011](#), the pressure is on U.S. carriers and corporations to deploy IPv6 in the next few years.

IPv6-based threats are not well understood, but they are becoming more prominent. For example, the issue of IPv6-based attacks was raised at a June meeting of the [National Security Telecommunications Advisory Committee](#), a high-level industry group that advises the White House about cybersecurity.

"We are seeing quite a bit of command and control traffic that is IPv6," says Jason Schiller, senior Internet network engineer, global IP network engineering for the public IP network at Verizon Business. "Hackers are trying to leverage IPv6 to fly under the radar. We're seeing a lot of bot networks where the command and control is under IPv6. We're also seeing illegal file

sharing that leverages IPv6 for peer-to-peer communications."

Rogue IPv6 traffic is an emerging threat for network managers. The biggest risk is for organizations that have decided to [delay IPv6 deployment](#) because they don't see a business driver for the upgrade – a category that includes most U.S. corporations.

U.S. federal agencies are in a better position to protect themselves against IPv6-based threats because they have enabled IPv6 across their backbone networks. [Federal agencies](#) are moving ahead with plans to integrate IPv6 into their enterprise architectures and capital investments.

Rogue IPv6 traffic "is a very real threat," says Sheila Frankel, a computer scientist in the Computer Security Division of the National Institutes of Standards and Technology (NIST).

"People can have IPv6 running on their networks and not know it. Computers and other devices can ship with IPv6 turned on. Ideally, if you're not prepared to protect against IPv6, it should be turned off for all the devices on your network. You need to be prepared to block it at your perimeter. You want to block it coming in and going out," Frankel says.

Frankel recommends that organizations that don't want to run IPv6 in production mode buy firewalls and intrusion-prevention systems that can block both native and tunneled IPv6 traffic.

"You should be blocking not only pure IPv6 traffic but also IPv6 traffic tunneled inside of other traffic," Frankel says. "Network operators have to be aware of the ways IPv6 would normally be tunneled in IPv4 traffic and in the different types of transition mechanisms, and they have to become aware of the rules necessary to block these various classes of traffic."

Where does rogue IPv6 traffic come from?

IPv6 traffic gets on your network because many operating systems—including Microsoft Vista, Windows Server 2008, Mac OS X, Linux and Solaris — ship with IPv6 enabled by default. Network managers have to disable IPv6 on every device that they install on their networks or these devices are able to receive and send IPv6 traffic.

"We're probably talking about 300 million systems that have IPv6 enabled by default," estimates Joe Klein, director of IPv6 Security at Command Information, an IPv6 consultancy. "We see this as a big risk."

Experts say it's likely that network managers will forget to change the IPv6 default settings on some desktop, server or mobile devices on their networks. At the same time, most organizations have IPv4-based firewalls and network management tools that don't automatically block IPv6 traffic coming into their networks.

"The most common IPv6-based attacks that we're seeing right now are when you have devices on the edge of your network that are dual stack, which means they're running IPv4 and IPv6. If you only have an IPv4 firewall, you can have IPv6 running between you and the attacker," Klein says. "The attacker is going through your firewall via IPv6, which at that point is wide open."

Another common problem is IPv6 traffic tunneled over IPv4 using such techniques as [Teredo](#), which is supported by Microsoft, or the alternative 6to4 and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) approaches.

"The typical IPv4 security devices are not tuned to look for IPv6 tunnels," Klein says. "They offer very weak defense, which is kind of scary."

Klein says the only way network managers can discover IPv6 devices on their network is to run IPv6. Even then, it's extremely difficult to discover IPv6 tunnels.

"You might be able to find the top three tunnels but not all the other sub-tunnels," Klein says. "You can tunnel IPv6 over HTTP over IPv4. How are you going to find that?"

To battle these threats, Command Information is offering software called Assure6, which operates in conjunction with deep packet inspection systems to identify IPv6 traffic tunneled over IPv4. Similarly, the McAfee Network Security Platform offers full IPv6 and tunnel inspection. [Cisco](#) and Juniper offer IPv6-enabled routers, firewalls and other systems that allow network managers to set IPv6-related security policies.

Klein says he gets one or two calls a month from organizations that have been attacked through rogue IPv6 traffic.

"One of our honeypots that we have set up saw a botnet using an IPv6-only attack," Klein says. "It was hiding itself as IPv4

through our router, and it was attacking and issuing command and controls to a botnet in the Far East."

The number of IPv6 attacks is small but growing, LeMaster says.

"There are fewer people that have IPv6 enabled, so it's not as rich a target as IPv4," LeMaster adds. "The majority of the vulnerabilities are over HTTP. They're application related, where IPv6 is just the transport for those security concerns."

Frankel says IPv6-based threats are common enough that every network manager needs a plan for mitigating them.

"Nobody today will deny that they have to do something about viruses or about spam," Frankel adds. "It's fair to say that rogue IPv6 traffic is in this category of threats that's going to hit you if you ignore it."

### **To block or not to block IPv6**

Experts disagree about whether it's best for network managers to block IPv6 traffic or to enable IPv6 traffic for monitoring purposes.

Most say that if an organization isn't prepared to support IPv6, it should block IPv6 traffic coming into and leaving its network using IPv6-enabled routers, firewalls, intrusion-prevention systems and intrusion-detection systems.

Network managers "should be creating policies...that look for IPv6 traffic and if they see it to drop that packet," LeMaster says. "Within their security incident manager solution they need to look at the profiles of traffic coming into their network. They need that visibility. If they see IPv6 traffic, they need to find out what host it's coming from or going to, and turn that traffic off."

But these experts admit that blocking IPv6 traffic is a temporary solution because a growing number of your customers and business partners will be supporting IPv6.

"If you're not prepared for IPv6, then the prudent thing to do is not to allow it into your network," LeMaster says. "But you shouldn't be blocking all IPv6 traffic for the next five years. You should only block it until you have a policy and understand the threats."

Long term, the better solution is to start running IPv6 so you can gain visibility into your IPv6 traffic and experience with the new protocol, experts say.

"We don't recommend that you block IPv6 traffic. We are recommending that you do an audit and find out how many IPv6 devices and applications are on your network. If you have IPv6 traffic on your network, then you've got to plan, train and implement IPv6," says Lisa Donnan, vice president of advanced technology solutions at Command Information.

Cisco recommends that its customers adopt the same security policies for IPv4 and IPv6, and that these policies be implemented using a layered approach.

"Configuration management, configuration control and policy are going to be pretty critical now as all of these IPv6 devices just show up on the network," West says. "Configuration management may be the largest threat we have around IPv6."

Frankel says now is the time for corporations to start training staff in IPv6 and getting experience with IPv6 so they can protect themselves against IPv6-based attacks.

"Companies need to acquire a minimal level of expertise in IPv6, which will help protect them against threats," Frankel says. "The other thing they should do is to take their outward-facing servers, those that are external to the corporation's firewalls, and enable IPv6 on them. That way customers from Asia with IPv6 addresses will be able to reach these servers and their own people will acquire expertise in IPv6. This will be a first step in the process."

IPv6 is "coming," Frankel says. "The best way is to face it head on and to decide you're going to do it in the most secure manner possible."

All contents copyright 1995-2009 Network World, Inc. <http://www.networkworld.com>