FEDInsider

Preparing, Transitioning & Securing IPv6 Networks in Government

Agencies and industry are working together to transition from IPv4 to IPv6 networks making room for more IoT and additional connected devices.

Featured Experts:

- **Jennifer Franks**
  Director, IT & CS Team,
  U.S. GAO

- **Scott Hogg**
  CTO & Co-Founder,
  Hexabuild

- **Chris Hessman**
  IT Specialist & Cloud Engineer Expert, GSA Information Technology Category (ITC), GSA

- **Chris Usserman**
  Director of Security Architecture,
  Infoblox

- **Allen McNaughton**
  Director of Pre-Sales Engineering,
  Infoblox

The Federal Energy Regulatory Commission published a mandate that all new networked federal information systems must be Internet Protocol version 6-enabled, so that the overall IPv6-only requirement is met by the end of FY 2023. This shift to IPv6 is largely driven by the explosion of IoT and connected devices, and a need for more available IP addresses.

However, there are security challenges associated with the move, as it requires that end-to-end encryption is built into devices and systems, and new threats are also sure to emerge. So, members of government and industry recently spoke at a FedInsider panel to discuss these changes, how to prepare for the needs of an IPv6 security landscape, and how to assess potential new risks.

PREPARING FOR THE IPV6 TRANSITION

On Jan. 18, the National Security Agency released initial IPv6 security guidance recommendations, and addressed initial security concerns as the government prepares to make the transition. Based on this release, from the perspective of the Government Accountability Office, "we would be focusing our audits and reviews on oversight efforts looking at compliance…are the people, processes and tools going to be able to handle both IPv4 and IPv6 compliance areas?" asked Jennifer Franks, the GAO's director of IT and the CS Team.

Specifically, GAO will be looking into how agencies are training its employees and investigators to use IPv6, which Franks said will be key for organizations to properly monitor networks.

For training teams to be compliant, they must know how to defend IPv6 networks, and most resources currently available focus on IPv4 networking. To better understand transition pain points, the General Services Administration tested how a small agency would handle its base network within its cloud environment as if it were IPv6 only. "The IPv6 button had always been there. It was in the network settings," said Chris Hessman, IT specialist and cloud engineer expert at the GSA's Information Technology Category. "Everything in our environment was generally able to do dual stack, so there were no surprises."

Hessman and his team discovered that the design and making of the Windows and Linux environments work at the base level, and ultimately, "it was an okay transition." However, the challenge is configuring the smaller details and overcoming a lack of general education on the topic.

TAKING THE IPV6 PLUNGE

While organizations begin to understand how to transition to IPv6, Scott Hogg, chief technology officer and co-founder of Hexabuild, said it starts with education. "Things like the abundance of the IPv6 address space change reconnaissance techniques; IPv6's use of extension

headers, and how IPv6 functions on a LAN," Hogg explained, "...these nuances have security implications, so having security teams educated about these characteristics of IPv6 help them design for the threats."

Conducting GSA-like testing, Hogg said, will greatly help security teams better understand how to deploy IPv6, get visibility to the traffic and validate security controls.

It's also worth considering and preparing for the security components that are unique to IPv6. Chris Usserman, director of security architecture at Infoblox, said that starts with infrastructure. Even if the networks aren't yet running dual stack or haven't shifted over to IPv6, the infrastructure can support it, and firewalls may not be looking for IPv6 activity.

"That gives [threat actors] the ability to set up an IPv6 overlay network within the victim's environment," Usserman said. It serves as a good practice for agencies to monitor for IPv6 activity today within their environment, even if the network is still IPv4 at the hosts, because it will make any threat activity leveraging IPv6 significantly easier to identify.

DUAL STACK SECURITY AND ZERO TRUST

When environments are running both IPv4 and IPv6 at the same time, the attack surface is doubled. Each device may have two points of entry rather than one. To address this, Hessman said GSA is pushing increased monitoring and security right from the start of their IPv6 transition through Enterprise Infrastructure Solutions contracts.

"From your point of delineation, getting your internet at the front, you should be IPv6, that is the spirit of the law, and they are saying that you have a lot of time to be dual stack but Zero Trust and IPv6 go hand-in-hand," he said. This way, rather than spending the money twice at a later point to comply, it is done upfront when modernizing networks. CDM and other device tracking systems must also be capable of handling the IPv6 addresses.

Hogg said enterprises will use the same security protection measures used for IPv4 to defend against IPv6 threats, like firewalls, IPS and anti-DDoS platforms. "IPv6 is not going to change where those are positioned," he said. Still, enterprises must reach out to vendors or test to ensure that products and services that can block domains in IPv4 can be enabled to do the same in IPv6.

IPv6 also opens up opportunities to support a zero trust architecture. Hogg said it creates an abundance of IP addresses and prefixes that enable enterprises to cleanly represent security zones or create granular or simpler filters with IPv6 prefixes and IPv6 prefixes split up into micro segments. "Because the [IPv6] addresses are very large, we can use the addresses in creative ways that we have not thought of using IPv4 addresses for in the past," he said.

Likewise, Usserman said IP address management is critical to IPv6 device security. It's about "understanding what is on your network and being able to utilize that in both the network management or net operations as well as security operations," he said.

IPV6 SECURITY TRANSITIONS: WHAT TO EXPECT

Configuring security and ensuring zero trust properly transitions to IPv6 will take time. Hessman said to expect IT experts and program managers to "nitpick" the network, as this is what happened in the lab. "It was figuring the small things out and how do they affect this other aspect of the network," he said. "It is touching both education and hands-on learning to get very good at what I'm doing so I can be as fluent on my network as I was previously, both dual stack and now IPv6 only."

In terms of compliance, Franks said the GAO is looking for the tools that can handle and secure both IPv4 and IPv6 across federal agencies; and whether those tools help agencies comply with regulations, legislations, policies and procedures.

"The reality is that agencies really need to be able to communicate with an increasing number of devices, not just internally but externally to all of our organizations," Franks said. "It's really good for us to start making some decisions to increase the opportunity to utilize investments now, and also to really take the security measures seriously and implement IPv6 into our organizations."

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

(202) 237-0300
Info@FedInsider.com
www.FedInsider.com
@FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

carahsoft.

Carahsoft
1493 Sunset Hills Road
Reston, VA 20190
Contact: **Jenna Tabatabaian**

(703) 889-9726
Jenna.Tabatabaian@Carahsoft.com
www.Carahsoft.com
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

Infoblox

Infoblox
One Dulles Technology Center
13454 Sunrise Valley Drive, Suite 570
Herndon, VA 20171
Contact: **Matt Jacoby**

(631) 496-1615
MJacoby@Infoblox.com
www.Infoblox.com
Facebook.com/Infobloxinc
Linkedin.com/company/Infoblox
@Infoblox