SOLUTION NOTE

ENHANCING ZERO TRUST ARCHITECTURE WITH IPV6 MIGRATION AND DNS SECURITY

WHY ZERO TRUST?

The Zero Trust security model can help cybersecurity professionals to secure enterprise networks and sensitive data. The Zero Trust model does this by eliminating trust in any single element by continuously assuming that a breach is inevitable or has already occurred. Zero Trust is a data centric model and seeks to limit access while also trying to identify anomalous or malicious activity.

The Zero Trust mindset brings substantial benefits. System administrators can better control devices, processes, and users that engage in any way with data. The basic principles of Zero Trust can reduce the dangerous risks associated with insider threats, supply chain malicious activity, the compromise of user credentials, remote exploitation, and many other types of cyberattacks.

WHY IPV6?

IPv4 has been in use since 1983 and IPv6 is the next-generation Internet protocol designed to replace it. The worldwide demand for Internet Protocol (IP) addresses has grown exponentially since the advent of IPv4, with constantly increasing numbers of users, devices (such as internet of things (IoT)) and virtual entities that need to connect to the Internet. The result is that both public and private IPv4 addresses have become highly constrained.

In the last few years, the momentum towards implementation of IPv6 has grown significantly as the benefits have become compelling. This momentum has been sustained by reducing cost, decreasing complexity, improving security and eliminating barriers to innovation in networked information systems. Many large and significant deployments of IPv6 are now in production. Some organizations are moving to “IPv6-only” infrastructure to reduce operational issues and costs associated with maintaining two networking regimes, and, in the case of Federal Government agencies, to align with recent OMB guidance.

IPV6 AND ZERO TRUST

IPv6 has some unique characteristics that lend itself to new ways of thinking about network and host security and for facilitating the security of end users and application services. One of the important characteristics of IPv6 is its abundance of global IPv6 addresses, obsoleting the need for network address translation (NAT) to solve the public IPv4 depletion problem. Without NATs in the middle of client-server communications, the application server actually receives the unmodified connection from the source IPv6 address of the client.

With the constraints of IPv4 addresses, the use of NATs has become ubiquitous, obfuscating client IPv4 addresses while providing anonymity for attackers. As a result, servers may not be able to validate the identity of client connections. Other forms of authenticating the end user become important. This creates problems for reputation filtering and for applications trying to use client IPv4 addresses as a method of authentication or detecting and blocking fraudulent transactions. Now, IPv4 addresses have become only “locally significant” within the domain where they are used. This makes us question the legitimacy of IPv4 connections and possibly consider IPv6 connections as more trustworthy. IPv6 addresses become more authentic and facilitate security forensic activities and improves situational awareness.

Moving Target IPv6 Defense (MT6D) was a system created in 2011 within the IT Security Laboratory (ITSL) at Virginia Tech to obscure IPv6 addresses and prevent eavesdropping. MT6D uses an algorithm that a pair of hosts used to change their IPv6 addresses dynamically, and that allows the hosts to predict the other's next IPv6 address. The IIDs of both ends of the communications change, based on some algorithm and key only known to the two nodes. This method makes interception of the communications very difficult and prevents any attacker from sending an IPv6 packet to either node because their IPv6 addresses are constantly changing. Moving Target Defense (MTD) methods can now be realized with IPv6 because the IID offers far more potential than IPv4's constrained address space. However, it would likely require that a full /64 be routed to the host to avoid potential neighbor exhaustion issues if many devices on the same /64 networks were also using this technique.

One innovative approach is to have an IPv6-capable DNS service coordinate its responses with a web-tier application front-end. One example of this is a custom DNS function that works with web servers, or load balancers that have Web Application Firewall (WAF) capabilities. The communication is initiated by a client, asking its caching DNS resolver the address of a server's fully-qualified domain name (FQDN). The authoritative DNS server returns an AAAA record response with an IPv6 address with a seemingly random IID (and a very low TTL value). The IID is actually a unique identifier that is solely specified for that particular client device (or DNS resolver). The authoritative DNS server coordinates the IID selected for the AAAA response with the front-end web-tier application service. The client makes the connection to the IPv6 address with the curated IID. When the connection from the client is initiated, the front-end web server knows that the client is the device that made the connection. This method can be used to separate legitimate traffic from DDoS traffic. This technique could be extended to have the IID of the AAAA record response use some type of client-identifier for Zero-Trust application access or as part of a Cloud Access Security Broker (CASB) service.

IPv6's address abundance allows us to think differently about how IPv6 addresses are used for securing client-server communications. It is certain that IPv6 will facilitate further innovation, and we will see many more techniques developed along these lines to improve security and help achieve resilient Zero-Trust architectures.

One of the unique characteristics of IPv6 is the incredibly large 128-bit addresses. The address space is so large that there is the potential to use the last 64-bits of the address (the Interface Identifier, or IID) for security purposes. These techniques are not feasible with the limited supply of IPv4 addresses. Methods of changing the IPv6 node's IID frequently take a page from the network attacker's playbook and "fast flux" techniques. An example of this is when temporary IPv6 IIDs change periodically to help preserve the privacy of the end user.

WHY INFOBLOX?

The ability to associate a security incident to a user has long been key to threat investigation and making rapid response decisions. In a world with more devices on a network than users, including BYOD and IoT/OT, it has become just as crucial for SecOps to have access to device details. Infoblox provides DHCP and network discovery capabilities to identify sanctioned and unsanctioned (rogue) devices on the network, supporting a dual-method approach to asset discovery. This process allows both security and networking teams to collect device details and extensive metadata, which are then stored in the Infoblox IP Address Management (IPAM) solution for fast, on-demand access by either network or SecOps personnel or automatically sharing the data with SIEM, SOAR, or other tools.

Infoblox uses distributed probes and a central data consolidator to provide a continuous import of IP and network addresses, convert discovered assets into IPAM objects and sync them into a central authoritative IPAM database. This approach delivers precise contextual visibility, accuracy and shorter, integrated workflows, improving operational efficiencies and resource utilization, lowering operational costs and increasing confidence in data reliability for workflow automation.

Infoblox discovery, whether in on-prem, virtualized, or hybrid, multi-cloud environments, reduces IT silos through shared access to the integrated, authoritative database of protocol, IP address, network infrastructure device, end-host, connectivity and port data. It reduces security and service interruption risk through the detection of rogue devices, errors and unmanaged devices and networks that go unseen in standard IPAM tools. Infoblox's comprehensive inventory of switch-ports makes port-resource management easy. Additionally, Infoblox automates data collection and correlation for visibility, analysis, design validation, provisioning, troubleshooting, managing and delivering effective core network, value-added and security services.

Infoblox DNS, DHCP, and IPAM (DDI) products provide support for DNS over IPv6, and visual IPAM tools for IPv6 address space allocation and management. The IPAM tools automate IPAM procedures, to reduce human error associated with complex IPv6 addresses and to eliminate repetitive tasks, allowing organizations to easily scale management processes across their enterprise with existing IT staff. Infoblox capabilities address the IPv6 migration issues related to taking inventory of, visually mapping, and configuring network equipment. Infoblox will also help you optimize performance on the network and analyze the network for internal and regulatory policy compliance.

Viewed from the network infrastructure point of view, IPv6 impacts many of the traditional tasks of managing the routers, switches, and other core devices. Infoblox can help organizations automate the discovery, analysis, and management of the network infrastructure as you migrate from IPv4 to IPv6.

The operation of IPv6 networks using our DDI is also closely integrated with our DNS security. DNS has a key role to play in a Zero Trust architecture, as it provides better-centralized visibility and control of all computing resources, including users and servers in a micro-segment, all the way to an individual IP address. Since most traffic, including malicious traffic, goes through DNS resolution first, it is an important source of telemetry providing detailed client information, helping to detect anomalous behavior, and protecting east-west traffic between micro segments. DNS security can also continuously check for, detect, and block Command and Control (C&C) connections and attempts to access websites that host malware. For all of these reasons, DNS security is a core enabler of Zero Trust strategy today.

Infoblox provides robust automation solutions for DNS, DHCP and IPAM and network change and configuration management to help plan, implement and operate IPv6 networks. Our teams have broad experience in the deployment and design of IPv6 architectures and the closely related network infrastructure. Infoblox is also a worldwide leader in the provision of DNS security. DNS security is core to the deployment of a Zero Trust architecture.

DNS security restores DNS as an absolute Zero Trust control point where every internet address can be scanned for potentially malicious behavior as identified by integrated threat intelligence. DNS security provides a single point of control to administer and manage all of your environments including cloud, on-premise, WFA, and mobile devices. This provides one DNS security administration point for all of your security stacks, which can easily be integrated with SOAR and other critical cybersecurity ecosystem controls. Organizations must always be in control of, and have complete visibility to, DNS traffic. It is best practice that all DNS traffic is resolved by servers controlled by the organization, not external resolvers over which the IT team has no control.

INFOBLOX SOLUTIONS FOR IPV6 MIGRATION AND MANAGEMENT

IPv6 Capable External DNS	• DNS for IPv6 • Dual-stack DNS Appliance
IPv6 IPAM	• Automated IP Address Management • Role-based accessibility • Integrated with DNS/DHCP • Visibility to IP address usage
Planning Tools for Internal IPv6 Migration	• Current Network Equipment Inventory (with OS version running) • Current Network Topology and Connectivity • Current Subnet Inventory
Internal IPv6 Capabilities	• IPv6 IP Address Allocation, Tracking and Reclaiming • IPv6 Subnet Allocation and Tracking • Dual-stack Device Tracking (Smart Folders) • Reduced Complexity of Dual-stack Environment & IP Address Explosion
IPv6 Network Infrastructure Management	• Automated Network Change and Configuration for IPv6 • Compliance, Policy Enforcement and Auditing

Chart Updated: 6.23.2022

WHY ZERO TRUST AND IPV6 NOW?

The priority for the deployment of both Zero Trust and IPv6 within the Federal government has accelerated. Together they bring a multitude of compelling benefits to include cost reduction, reduction in risk, and enhanced cyber defense. Both Zero Trust and IPv6 are core components of the same future architecture and require agency compliance. The deliverables required for mandatory agency compliance are closer than ever and require agencies to move assertively to execute on plans to get these technologies in place.

The emphasis behind the adoption of Zero Trust was accelerated with the January 2022 publication of the Office of Management and Budget memorandum "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles." Note that the OMB memorandum requires agencies to achieve specific Zero Trust security goals by the end of the Fiscal Year (FY) 2024 with interim planning and management deliverables. Also note the National Security Agency guidance, "Embracing a Zero Trust Security Model" which was published in early 2021.

In November 2020, the United States Office of Management and Budget issued a memorandum "Completing the Transition to Internet Protocol Version 6 (IPv6)" which provides updated timeline and guidance on the Federal government's operational deployment and use of IPv6 across all Federal information systems and services.

Time is of the essence. A full and complete transition to Zero Trust and IPv6 is essential for the Federal government to meet necessary goals and initiatives over the coming years and to capitalize on new capabilities. The benefits to implementing these technology initiatives remain compelling for the Federal government.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20231030v1