PROJECT DESCRIPTION

SECURE IPV6-ONLY IMPLEMENTATION IN THE ENTERPRISE

Doug Montgomery
Murugiah Souppaya

National Institute of Standards and Technology

William C. Barker

Dakota Consulting

Yemi Fashina
Parisa Grayeli
Joe Klein

The MITRE Corporation

DRAFT

December 2021

ipv6-transition@nist.gov

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov/.

This document describes the challenge of securely evolving a modern enterprise network to fully support IPv6, eventually transitioning to only support IPv6. The technical issues that must be addressed are relevant to vendors of network and security technologies and the operators of enterprise networks and their network service providers. NCCoE cybersecurity experts, in collaboration with industry partners, will address this challenge through the design and development of reference demonstrations that address the security and privacy issues encountered during transition to IPv6. The resulting reference design will detail approaches that can be used to prepare enterprises to support IPv6-only networks.

Abstract

The NCCoE is planning a project to provide guidance and a reference architecture that address operational, security, and privacy issues associated with the evolution to IPv6-only network infrastructures. The project will demonstrate tools and methods for securely implementing IPv6, whether as a "greenfield" implementation in which there is no current IPv4 enterprise infrastructure, or as a transition from an IPv4 infrastructure to an IPv6-only network. While the focus is on enterprise networks, use case scenarios may address other technologies commonly found in modern enterprise environments such as hybrid public/private cloud services, mobile devices, remote/telework, and advanced transport services. The primary focus of the demonstration project will be on the security technologies, services, and recommended practices necessary to ensure that evolving enterprise IT environments to be IPv6-only can be accomplished in a secure and robust manner. This project will result in the publication of a NIST Cybersecurity Practice Guide, which can serve as a source of guidance and support for IPv6 acquisition, a reference for secure implementation requirements, and a source of test cases.

Keywords

Internet; IPv6; IPv6-only; IPv6 transition mechanisms; network security; networking

Disclaimer

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

Comments on NCCoE Documents

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov/.

Comments on this publication may be submitted to ipv6-transition@nist.gov

Public comment period: December 9, 2021 to January 27, 2022

TABLE OF CONTENTS

1 Executive Summary

Purpose

This document defines a National Cybersecurity Center of Excellence (NCCoE) project focused on providing guidance and an example implementation that address operational, security, and privacy issues associated with migration from IPv4 network infrastructures to IPv6-only network infrastructures.

Internet Protocol version 6 (IPv6) is the Internet's next-generation protocol, designed to replace the legacy IPv4 protocol that has been in use since 1983. Internet Protocol (IP) addresses are the global numeric identifiers necessary to uniquely identify entities that communicate over the Internet. The free pool of available IPv4 addresses was exhausted in 2015, and the demand for global IP addresses continues to grow exponentially as the number of users, devices, and virtual entities connected to the Internet increases. According to the Internet Society [1], in the last five years IPv6 momentum in industry has dramatically increased. There have been large commercial IPv6 deployments in several industry sectors (e.g., data centers [2], cellular carriers [3], content providers, and cloud service providers). These deployments have been driven by business goals of reducing cost, decreasing complexity, improving security, and eliminating barriers to innovation in networked information systems.

Impediments to migration from IPv4 to IPv6 include general reluctance to expend the resources and deal with implementation challenges associated with any change to existing networks, lack of IPv6 expertise on the part of those who would have to deploy and support it, concern that there is a less mature set of IPv6-capable management and security applications and tools than is the case for IPv4, and concerns regarding compatibility with and support for legacy applications.

While there has been significant IPv6 deployment progress in some use case scenarios, widescale adoption in general enterprise settings continues to lag. There are significant potential benefits [4] to transitioning enterprise networks to IPv6, but questions about the viability of technologies and deployment guidance necessary to do so securely remain a barrier to progress for many.

On November 19, 2020, Office of Management and Budget (OMB) Memorandum M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)* [5] communicated requirements for completing the operational deployment of IPv6 across all federal information systems and services, and provided milestones and guidance for agencies to transition significant portions of their networks to IPv6-only environments by 2025. The policy states that “the strategic intent is for the Federal government to deliver its information services, operate its networks, and access the services of others using only IPv6.”

The OMB Memorandum required the heads of executive departments and agencies to identify opportunities for IPv6 pilots, complete at least one pilot of an IPv6-only operational system by the end of fiscal year 2021, and report the results of the pilot to OMB upon request. The Memorandum further states: “In order to expedite progress towards IPv6-only enterprise deployments, NIST, through the National Cyber Center of Excellence (NCCoE), will establish a cooperative Federal government and industry pilot project to the demonstrate commercial viability and to document a practice guide for secure IPv6-only enterprise deployment scenarios.”

This project aims to demonstrate the feasibility of securely migrating common enterprise network environments to IPv6-only networks. In doing so, the project will also address the technologies necessary to maintain interoperability between IPv4 and IPv6 systems during such a transition.

This project will result in the publication of a National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge. This Practice Guide represents an example implementation, and it can serve as a source of guidance and support for IPv6 acquisition, a reference for secure implementation requirements, and a source of test cases.

Scope

The scope of this project is to demonstrate the tools and methods for secure incremental deployment of IPv6 in modern enterprise networks. The proposed scope of the project may include items from the following list, as well as others:

- Security technologies and architectures commonly used in modern enterprise networks to configure, operate, protect and monitor networked information technology (IT) systems. Examples include:
    - identity, credential, and access management (ICAM)
    - endpoint security and mobile device management (MDM)
    - security information and event management (SIEM)
    - configuration and vulnerability management
    - continuous diagnostics and mitigation (CDM)
    - threat intelligence and reputation
    - network access control, micro-segmentation, and network policy enforcement
    - software-defined perimeters and zero trust networks
    - next-generation firewalls and intrusion detection/prevention
- Common enterprise use case scenarios that include client/service access within the enterprise network, enterprise client access to external enterprise/cloud services, enterprise client access to public Internet services, external fixed and mobile client access to enterprise services (both on-premises and cloud), and public internet access to enterprise services (both on-premises and cloud).
- IPv6 adoption scenarios that typically evolve through stages of IPv4-only environments, ubiquitous IPv4/IPv6 dual-stack deployments, IPv6-dominant environments, and eventually IPv6-only environments. Different elements of an enterprise IT environment may evolve through these stages at different times. For example, an enterprise might IPv6-enable its public-facing internet services (both transport and applications) before enabling its internal networks and applications.
- Modern enterprise IT environments are comprised of different broad categories of elements, each of which have different issues to consider in the transition to IPv6. Examples of such elements include:
    - **Cloud services** – both private and public cloud instantiations, with both public-facing services and virtual private enterprise services

- **Internet/WAN transport networks** – external wide area network (WAN) services, both virtual private and public internet services and their supporting routing, switching, and security, management, and monitoring tools
- **Enterprise intra-networks** – routing, switching, and security, management, and monitoring tools
- **Clients** – both enterprise on-premises intranet clients and external/mobile enterprise clients operating over the public internet and virtual private networks
- **Enterprise services/servers** – systems and services operating on-premises to enterprise IT services
- **Security, management, and monitoring services** – the suite of tools and services necessary to secure a modern enterprise environment

While in the abstract one might consider all possible scenarios defined by the cross product of deployment stage (i.e., IPv4, dual-stack, IPv6-only) and elements (above) for each use case, examining that range of possible scenarios is neither feasible from a project resource perspective nor, for many such combinations, likely to be encountered in real transition strategies. Instead, we focus on a small set of common scenarios that are found in typical enterprise transition strategies (see proposed scenarios below). The exact set of scenarios and technologies addressed will depend upon the level of interest and participation from potential project collaborators and the broader community of interest.

Assumptions/Challenges

Mature IPv6 implementations exist in almost all client/server operating systems and network routing and switching platforms. Today, there are few technical barriers to deploying robust dual-stack enterprise control and data-planes. Support for IPv6 in security, management, and monitoring technologies and services has historically lagged behind that of popular platforms and is often identified as a perceived barrier to ubiquitous IPv6 adoption in the enterprise [6].

This project assumes that in general this is no longer the case, and that current product and service offerings are capable of supporting robust and secure IPv6-enabled infrastructures that include the security, management, and monitoring capabilities required for federal enterprise networks. It is the objective of the first phase of this project to demonstrate such capabilities using commercial product and service offerings.

The second phase of this project, completing the transition to IPv6-only enterprise networks, is more challenging. It requires the introduction of various transition technologies to allow IPv6-only and IPv4-only systems to interoperate and adds additional challenges for products to support their full range of operation and support functions using only IPv6. While there are many commercial products that support scalable, standardized transition mechanisms, we expect to identify some technology gaps when we explore the extent to which the full range of typical enterprise networked IT systems can be migrated to IPv6-only environments. The project will identify these technology gap areas and seek to document practical approaches to mitigate them.

Background

IPv6 is the most recent version of IP, the communications protocol that provides the ability to uniquely identify (i.e., address) systems on networks around the world and to route data between those systems, typically over the public internet. IPv6 was developed in response to a recognition in the 1990s that the rate of allocation of IPv4 addresses was such that the internet would soon run out of address space. The current IPv6 specification, published in 2017, offers a vastly greater address space and supports significant new capabilities for modern networks (e.g., segment routing, auto-configuration, advanced wireless support).

In its early stages of commercialization, adoption of IPv6 was slow. However, today adoption of IPv6 is well underway. The Internet Society in its State of IPv6 Deployment 2018 report [1] notes that "IPv6 has emerged from the 'Innovators' and 'Early Adoption' stages of deployment, and is now in the 'Early Majority' phase." In fact, IPv6 deployment has been progressing steadily for several years and is emerging as a viable alternative to IPv4 in many contexts [7]. In some contexts, IPv6 is already the dominant protocol in use today [8].

There is a growing body of experience about deploying dual-stack network environments [9][10]. While general knowledge of deploying IPv6 in dual-stack networks is growing, there are specific challenges to doing so in federal IT environments. Many intersecting federal IT policies and initiatives (e.g., Trusted Internet Connections [11], Continuous Diagnostics and Mitigation [12], Event Log Management [13], Zero Trust [14]) levy other requirements on federal networks that must be coordinated with IPv6 adoption plans.

The November 19, 2020 OMB Memorandum M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)* [5] recognized a dramatic increase in IPv6 momentum in industry, with large IPv6 commercial deployments in many business sectors being driven by needs to reduce cost, decrease complexity, improve security, and eliminate barriers to innovation in networked information systems. The memorandum communicated the requirements for completing the operational deployment of IPv6 across all federal information systems and services, and to address barriers that impede agencies from migrating to IPv6-only network environments. The stated strategic intent is for the federal government to deliver its information services, operate its networks, and access the services of others using only IPv6.

While there has been significant progress in the adoption of IPv6, and in particular IPv6-only, in some environments (e.g., residential and mobile access networks, special purpose data centers), widescale deployment in enterprises lags behind. The diversity and complexity of enterprise IT network systems, the range of services that they must interoperate with, and the vast scope of the applications space all contribute to the slow adoption in enterprise networks.

Examples of issues to be addressed when transitioning an enterprise to IPv6 can be found in many technology areas, including the following:

- Network infrastructure services like naming and routing, and associated technologies for monitoring, troubleshooting, management, etc.
- Security devices and services like security proxies, firewalls, intrusion detection and prevention systems (IDPS), content inspection and filtering, data loss and prevention systems (DLPS), software-defined perimeter/micro-segmentation, zero-trust technology, etc.
- Authentication and authorization, public key infrastructure (PKI), data protection, backup, data governance, and business continuity systems
- Endpoint operating systems deployed across the enterprise, to include monitoring, management, and security tools, agents, etc. that are part of the organization-approved baseline operating system image

- Enterprise commercial off-the-shelf (COTS) applications built on top of database servers, middleware, web servers, etc.
- Enterprise-developed applications and software development platforms
- Education and training of the workforce to support this technology

In response to M-21-07's tasking of the NCCoE to establish a cooperative federal government and industry pilot project to demonstrate commercial viability and to document a practice guide for secure IPv6-only enterprise deployment scenarios, this project aims to demonstrate the feasibility of overcoming challenges to implementing IPv6 and completing the migration from IPv4 to IPv6-only networks.

2 Proposed Architectures and Scenarios

The proposed high-level architecture consists of an enterprise with internal enterprise services, private cloud services, and enclaves serving various users. A DMZ and enterprise internet/virtual private network (VPN) are used to connect the enterprise to external resources such as public cloud services and other internet services. Mobile users using enterprise managed devices or unmanaged devices connect to the enterprise or cloud and internet services through their residential/mobile broadband providers. This high-level architecture will be leveraged in each of the proposed demonstration scenarios.

As noted earlier, it is impossible to explore all possible combinations of incremental and partial deployment scenarios across the full range of broad enterprise IT components. Instead, we will focus on a few common scenarios that are found in typical enterprise transition strategies.

In each scenario we will focus on the broad security and privacy implications of adding IPv6 (or removing IPv4) for the elements in question, including the security implications of deploying any IPv6 transition mechanisms necessary to bridge interoperability gaps between IPv4-only and IPv6-only systems and services. In each scenario we will demonstrate and document technologies, configurations, and best practices necessary to maintain the security, privacy, and robustness of the resulting enterprise IT environment.

In each scenario there may be multiple choices for transition and security technologies to address the scenario. Final choices as to specific technologies to be used will be a function of the collaborators and community of interest for the project.

The legend shown in Figure 1 is used for all the scenarios. It differentiates IPv4-only, IPv6/IPv4, and IPv6-only networks and capabilities. It also shows the clients, services/servers, switches/router, and transition mechanisms using various shapes. Enterprise owned/operated resources are depicted on a green background. Other resources are assumed to be public/external to the enterprise IT environment.

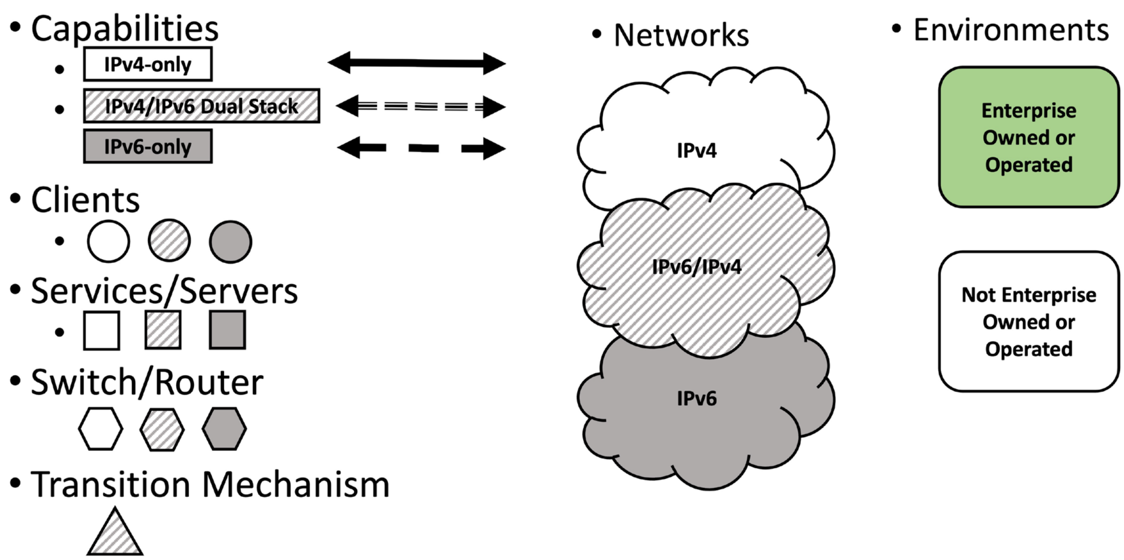

Figure 1. Legend for components depicted in architecture and scenario diagrams

Scenario 1: Secure IPv4-Only Enterprise IT Environment

Figure 2 depicts an IPv4-only enterprise in which enterprise services, enclaves, and private cloud service clients and servers connect by switches/routers through an intranet and border switches/routers—or private cloud services through a DMZ—to enterprise internet and VPN resources.

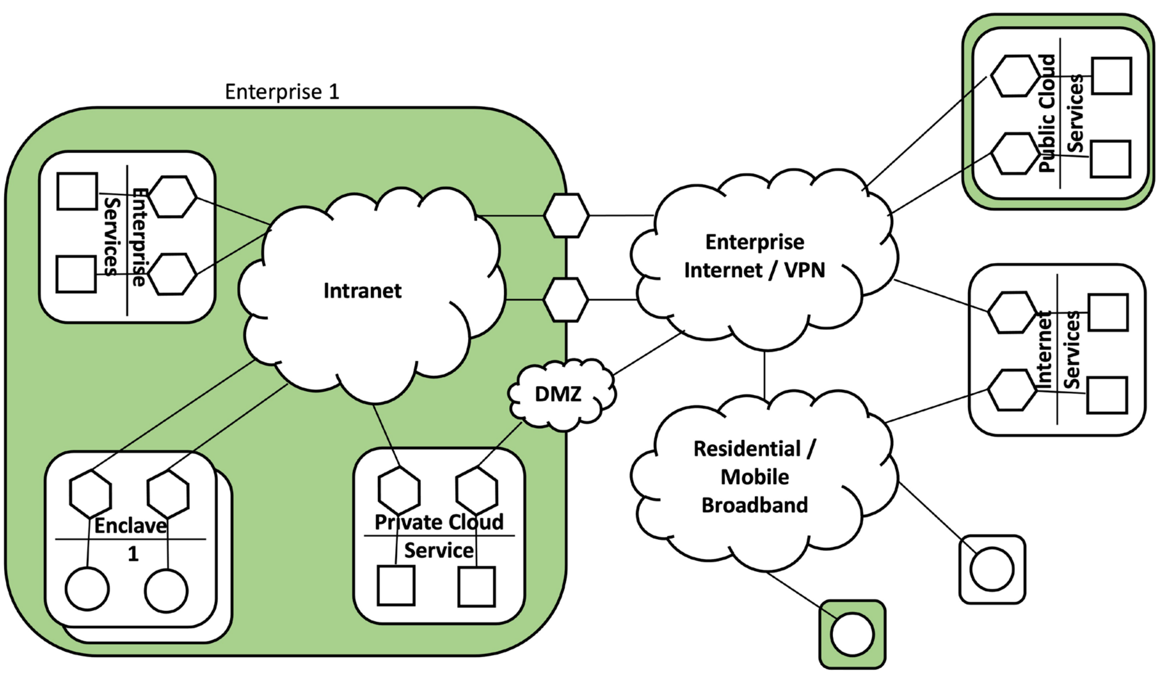

Figure 2. Architecture for Scenario 1, Secure IPv4-Only Enterprise IT Environment

This will be our baseline configuration of a secure enterprise IT environment including internal and external network capabilities, on-premises and cloud-based services (both public and private), on-premises and external/mobile clients, and the required security, management, and monitoring capabilities.

Using this baseline configuration, we will demonstrate and document the secure support of the following use cases:

- UC-1 - public internet access to public-facing services (both on-premises and cloud-based)
- UC-2 - enterprise client access to public internet services
- UC-3 - enterprise client access to internal enterprise services
- UC-4 - enterprise client access to external enterprise/cloud services
- UC-5 - external and mobile client access to enterprise services (both on-premises and cloud-based)

Scenario 2: Secure IPv6-Enabled Public-Facing Services

Figure 3 depicts an enterprise that is primarily IPv4-only, though at least one of the private cloud servers and switches uses IPv4/IPv6 dual stack. At least one of the external enterprise clients is assumed to employ IPv6, and the enterprise DMZ, internet/VPN, and residential/mobile broadband facilities, and public cloud are assumed to be dual-stack-capable.

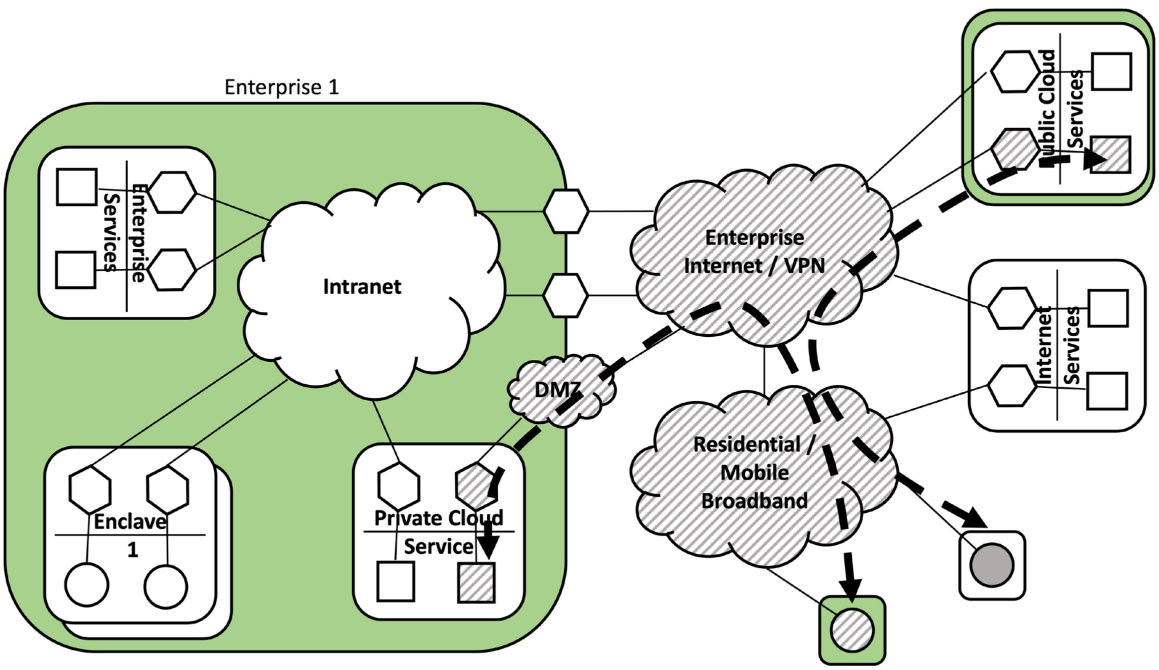

Figure 3. Architecture for Scenario 2, Secure IPv6-Enabled Public-Facing Services

This scenario will enable native IPv6 dual-stack support for public Internet services (e.g., DNS, web, email) implemented both in the cloud and on-premises. IPv6-enabling on-premises public-facing services will require changes to the security infrastructure that supports Internet facing services (e.g., DMZ, IDPS, firewalls).

Using this configuration, we will demonstrate and document the secure support of the following use case:

- UC-1 - public internet dual-stack IPv6 access to public-facing services (both on-premises and cloud-based)

Scenario 3: Secure IPv6-Enabled Enterprise Clients

Figure 4 is similar to that depicted in Figure 3 except that the enterprise intranet, at least one enclave, private cloud switches, and border routers are dual stack.

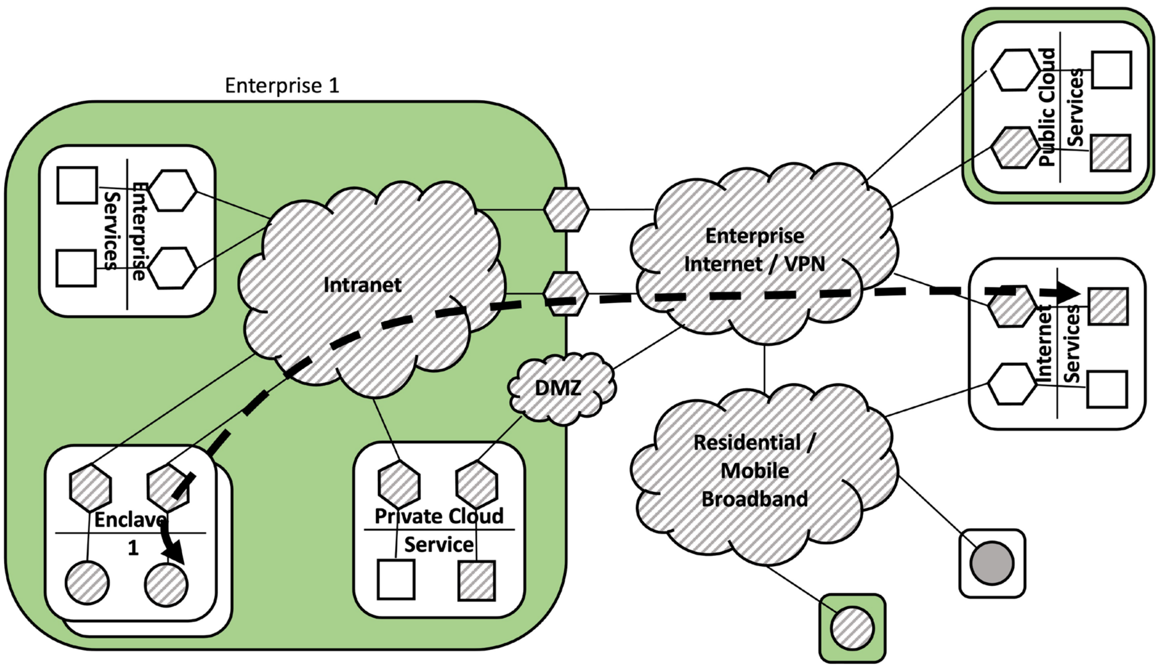

Figure 4. Architecture for Scenario 3, Secure IPv6-Enabled Enterprise Clients

This scenario will fully enable IPv6 dual-stack support across the enterprise intranet and out to individual enterprise client systems. IPv6-enabling the enterprise intranet and end clients will require changes to the security infrastructure that supports all enterprise clients (e.g., Dynamic Host Configuration Protocol [DHCP], intranet routing, IDPS, firewalls) and their traffic to/from the Internet.

Using this configuration, we will demonstrate and document the secure support of the following use case:

- UC-2 - enterprise client dual-stack IPv6 access to public internet services

Scenario 4: Secure IPv6-Enabled Enterprise Services

Figure 5 depicts the scenario in which all local enterprise clients, servers, and switches are dual stack. Otherwise, the build is essentially unchanged from that for Scenario 3.

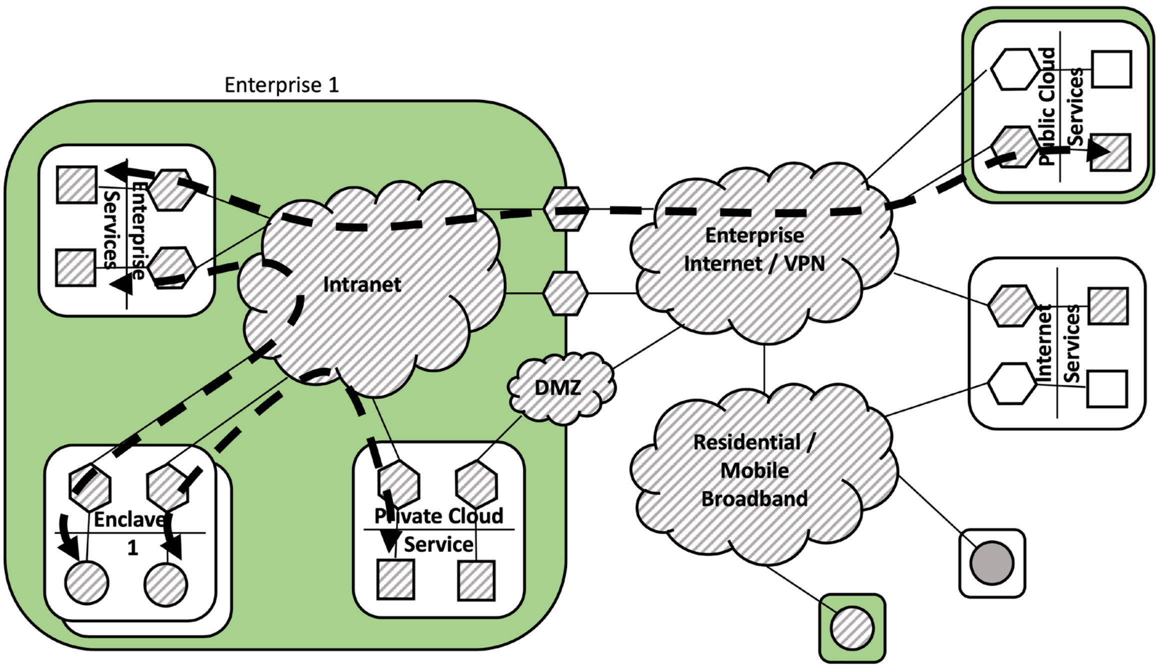

Figure 5. Architecture for Scenario 4, Secure IPv6-Enabled Enterprise Services

This scenario will fully enable IPv6 dual-stack support on all enterprise intranet and cloud services – both security, management, and monitoring services and basic enterprise application services.

Using this configuration, we will demonstrate and document the secure support of the following use cases:

- UC-3 - enterprise client dual-stack IPv6 access to internal enterprise services
- UC-4 - enterprise client dual-stack IPv6 access to external enterprise/cloud services
- UC-5 - external and mobile client dual-stack IPv6 access to enterprise services (both on-premises and cloud-based)

Scenario 5: Secure IPv6-Only Enterprise Clients

Figure 6 depicts the addition of some IPv6-only clients within the enterprise. IPv6-only clients will rely on IPv6 transition mechanisms to legacy IPv4 services both internal and external to the enterprise.

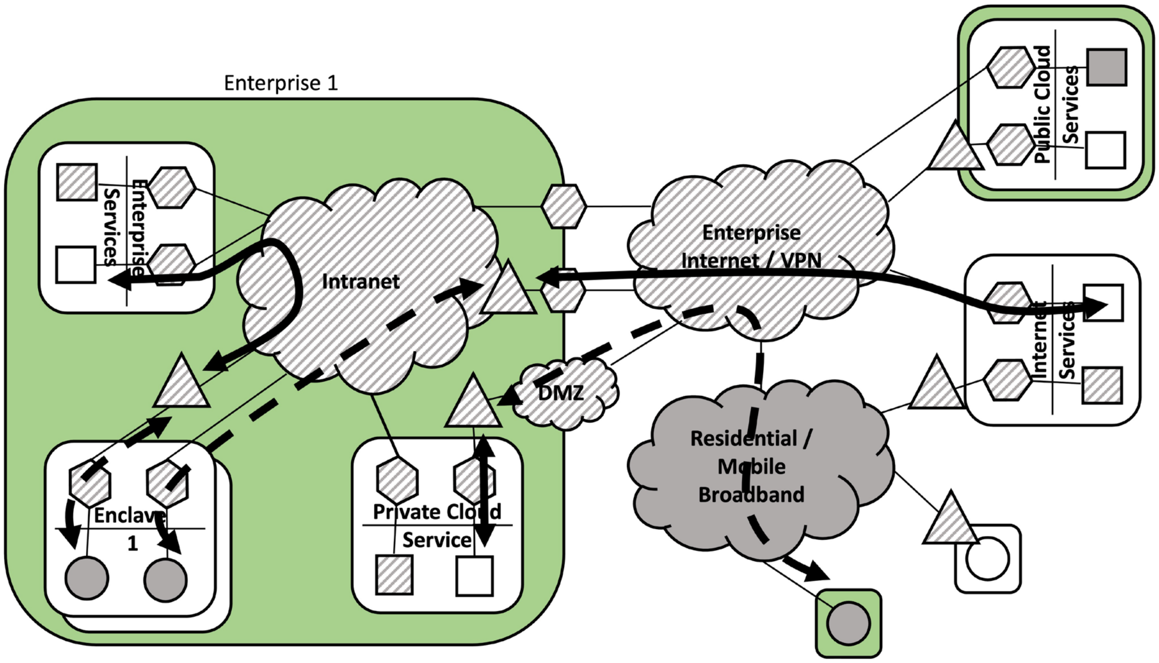

Figure 6. Architecture for Scenario 5, Secure IPv6-Only Enterprise Clients

This scenario will remove IPv4 support for individual enterprise client systems. IPv6-only clients will for some time need to communicate with IPv4-only systems and services both within the enterprise and on the public Internet. This scenario will require the introduction of one or more IPv6-transition mechanisms capable of enabling scalable interoperability between IPv6-only and IPv4-only systems. Addressing the security and robustness implications of wide-scale deployment of such transition mechanisms, and the removal of IPv4 support for clients will be the focus of this scenario.

Using this configuration, we will demonstrate and document the secure support of the following use cases:

- UC-2 - enterprise IPv6-only client access to public dual-stack and IPv4-only Internet services
- UC-3 - enterprise IPv6-only client access to internal dual-stack and IPv4-only enterprise services
- UC-4 - enterprise IPv6-only client access to external dual-stack and IPv4-only enterprise/cloud services
- UC-5 - external and mobile enterprise IPv6-only client access to dual-stack and IP-v4 only enterprise services (both on-premises and cloud-based)

Scenario 6: Secure IPv6-Only Public Services

Figure 7 depicts the addition of IPv6-only servers, switches, and routers within the enterprise's private cloud and an IPv6-only public cloud. Both the private cloud service and the public cloud service feature "transition mechanisms" that support connection of IPv6-only services to external IPv4 enterprise clients (note that here, the external clients support only IPv4).

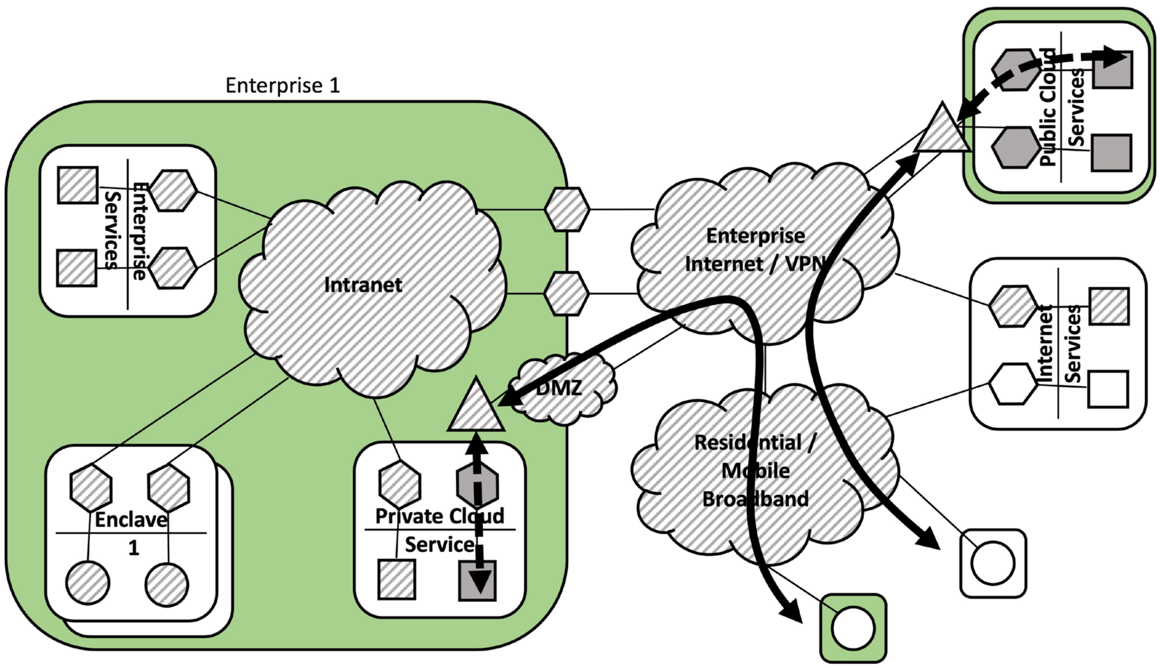

Figure 7. Architecture for Scenario 6, Secure IPv6-Only Public Services

This scenario will remove IPv4 support for public-facing services both on-premises and in the cloud. Given that an enterprise cannot control the pace of IPv6 deployment in the rest of the internet that may want to access these services, appropriated transition mechanisms must be deployed to maintain interoperability to these services for IPv4-only systems on the Internet. In this scenario all security, management, and monitoring systems for the servers that implement public-facing systems must support IPv6 natively.

Using this configuration, we will demonstrate and document the secure support of the following use case:

- UC-1 - public internet dual-stack and IPv4-only access to IPv6-only public services (both on-premises and cloud-based)

Scenario 7: Secure IPv6-Only Enterprise Infrastructure

In Figure 8, enterprise services include IPv4-only and IPv6-only servers and clients, and at least one enclave. The intranet and private cloud services are primarily IPv6-only, though some legacy dual-stack servers may be retained. Residential/broadband facilities are IPv6-only. Some internal and external clients are IPv4-only, and transition mechanisms are employed to permit interoperability with these legacy elements.

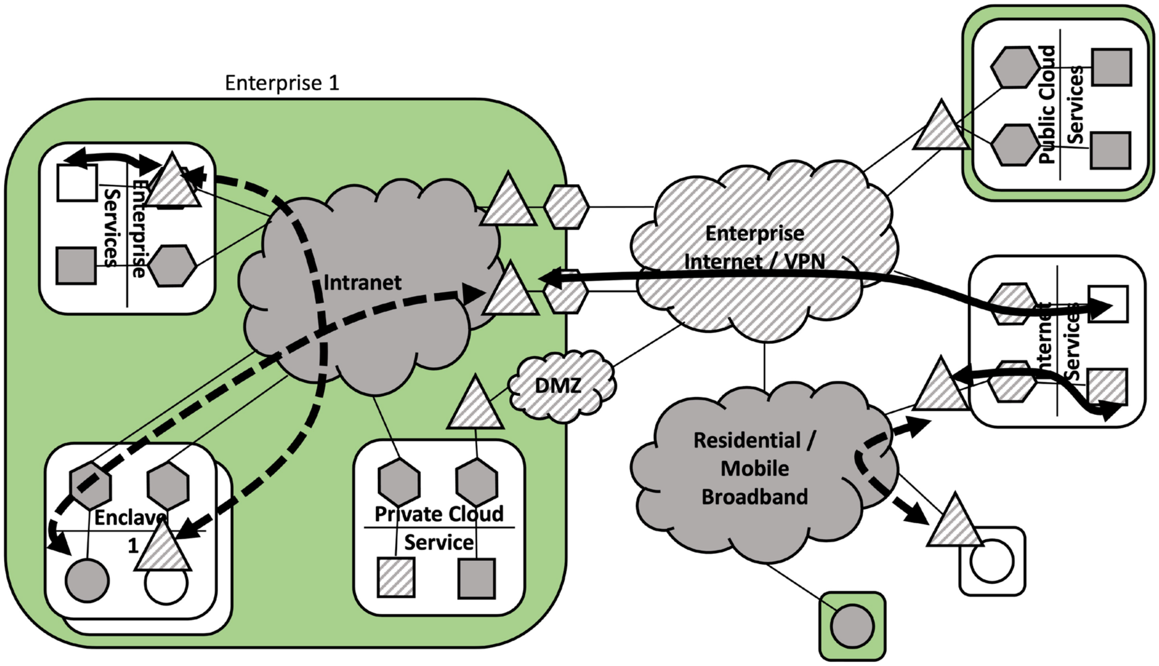

Figure 8. Architecture for Scenario 7, Secure IPv6-Only Enterprise Infrastructure

This scenario will remove IPv4 support for all possible enterprise services (on-premises and cloud-based), clients, and intranet routing services. In this scenario all security, management, and monitoring technologies must be capable of operating using only IPv6. Some clients, applications, and servers will be maintained as “IPv4-legacy” systems to demonstrate the use of transition mechanisms to maintain interoperability between IPv6-only clients and services and legacy IPv4-only clients and services.

Using this configuration, we will demonstrate and document the secure support of the following use cases:

- UC-3 - enterprise dual-stack and IPv4-only client access to internal IPv6-only enterprise services
- UC-4 - enterprise dual-stack and IPv4-only client access to external IPv6-only enterprise/cloud services
- UC-5 - external and mobile enterprise dual-stack and IPv4-only client access to IPv6-only enterprise services (both on-premises and cloud-based)

Component List

The IT components below are relevant to the architectures and scenarios proposed for this demonstration project. The specific components to be included in the project will be a function of the collaborators and community of interest.

Security, management, and monitoring services - the suite of tools and services necessary to secure a modern enterprise environment, including:

- ICAM
- endpoint security and MDM
- SIEM

- configuration and vulnerability management
- CDM
- threat intelligence and reputation services
- Internet Protocol address management (IPAM)
- zero trust technology

Clients – both enterprise on-premises intranet clients and external/mobile enterprise clients operating over the public internet and VPNs. They are common enterprise client platforms (workstations, laptops) and mobile devices (tablets, smartphones) using a variety of commodity operating systems.

Enterprise services/servers – systems and services operating on-premises to enterprise IT services, including:

- commodity server platforms, virtualization platforms, containers
- support for both public and private services
- enterprise services such as storage/file sharing, collaboration platforms, email, remote access, version control, backup, web platforms, and databases

Cloud services – both private and public cloud instantiations, with both public-facing services and virtual private enterprise services, including:

- support for both on-premises private and public cloud services such as storage/file sharing, collaboration platforms, email, remote access, version control, backup, web platforms, and databases
- infrastructure as a service (IaaS) in a hybrid-cloud deployment with virtual private cloud
- for public cloud services, both platform as a service (PaaS) and software as a service (SaaS)
- PaaS configurations with supporting security, monitoring, and management (e.g., load balancing) capabilities

Internet/WAN transport networks – external WAN services, both virtual private and public internet services and their supporting routing, switching, and security, management, and monitoring tools, including:

- next-generation firewalls and intrusion detection/prevention
- VPN technologies
- software-defined WAN technologies
- mobile wireless technologies

Enterprise intra-networks – routing, switching, and supporting security, management and monitoring tools, including:

- network access control, micro-segmentation, and network policy enforcement
- software-defined perimeters and zero trust technologies
- wireless access networks
- commodity network service technologies (e.g., DNS, Network Time Protocol [NTP], DHCP, proxy/load-balancing services)

Desired Security Characteristics and Properties

The planned IPv6 proof-of-concept build will demonstrate the ability to securely implement IPv4, dual-stack, and IPv6-only protocols in an enterprise environment, and dual-stack and IPv6-only protocols in a public-facing environment. The proposed project will demonstrate the security and privacy properties associated with a number of the IPv6 transition mechanisms in use today. The goal is to demonstrate that IPv6 can be ubiquitously deployed within modern federal enterprise networks while providing security, privacy, and robustness properties on par with or better than that of current IPv4 networks.

3 Relevant Standards and Guidance

The following resources and references provide additional information to be leveraged to develop this solution:

Government Directives

- OMB Memorandum M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*, November 19, 2020. https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf
- Department of Defense, Internet Protocol Version 6 Implementation Direction and Guidance, February 2019. https://www.hpc.mil/images/hpcdocs/ipv6/dod_cio_ipv6_guidance_memorandum_27_feb_2019.pdf
- OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, November 8, 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-06.pdf
- OMB, *Transition to IPv6*, September 28, 2010. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf

Security Standards and Deployment Guidelines

- NIST Special Publication (SP) 800-119, Guidelines for the Secure Deployment of IPv6, December 2010. https://doi.org/10.6028/NIST.SP.800-119
- Internet Engineering Task Force (IETF) Request for Comments (RFC) 9099, Operational Security Considerations for IPv6 Networks, August 2021. https://datatracker.ietf.org/doc/rfc9099/
- IETF RFC 7707, Network Reconnaissance in IPv6 Networks, March 2016. https://datatracker.ietf.org/doc/rfc7707/
- IETF RFC 7610, DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers, August 2015. https://datatracker.ietf.org/doc/rfc7610/
- IETF RFC 7404, Using Only Link-Local Addressing inside an IPv6 Network, November 2014. https://datatracker.ietf.org/doc/rfc7404/
- IETF RFC 7381, Enterprise IPv6 Deployment Guidelines, October 2014. https://datatracker.ietf.org/doc/rfc7381/

- IETF RFC 7359, Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks, August 2014. https://datatracker.ietf.org/doc/rfc7359/
- IETF RFC 7123, Security Implications of IPv6 on IPv4 Networks, February 2014. https://datatracker.ietf.org/doc/rfc7123/
- IETF RFC 6883, IPv6 Guidance for Internet Content Providers and Application Service Providers, March 2013. https://datatracker.ietf.org/doc/rfc6883/
- IETF RFC 6169, Security Concerns with IP Tunneling, April 2011. https://datatracker.ietf.org/doc/rfc6169/
- IETF RFC 6036, Emerging Service Provider Scenarios for IPv6 Deployment, October 2010. https://datatracker.ietf.org/doc/rfc6036/
- IETF RFC 4942, IPv6 Transition/Coexistence Security Considerations, September 2007. https://datatracker.ietf.org/doc/rfc4942/
- IETF RFC 4864, Local Network Protection for IPv6, May 2007. https://datatracker.ietf.org/doc/rfc4864/
- IETF RFC 4215, Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks, October 2005. https://datatracker.ietf.org/doc/rfc4215/
- IETF RFC 4057, IPv6 Enterprise Network Scenarios, June 2005. https://datatracker.ietf.org/doc/rfc4057/
- IETF RFC 4029, Scenarios and Analysis for Introducing IPv6 into ISP Networks, March 2005. https://datatracker.ietf.org/doc/rfc4029/

Network Standards and Protocols

- NIST SP 500-267B Revision 1, USGv6 Profile, November 2020. https://doi.org/10.6028/NIST.SP.500-267Br1
- NIST SP 500-267A Revision 1, NIST IPv6 Profile, November 2020. https://doi.org/10.6028/NIST.SP.500-267Ar1

Other References

- American Registry for Internet Numbers (ARIN), *Microsoft Works Toward IPv6-only Single Stack Network*, April 3, 2019. https://www.arin.net/blog/2019/04/03/microsoft-works-toward-ipv6-only-single-stack-network/
- Internet Society, *State of IPv6 Deployment 2018*, June 6, 2018. https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018
- Internet Society, *Case Study: T-Mobile US Goes IPv6-only Using 464XLAT*, June 13, 2014. https://www.internetsociety.org/resources/deploy360/2014/case-study-t-mobile-us-goes-ipv6-only-using-464xlat
- Internet Society, *Case Study: Facebook Moving To An IPv6-Only Internal Network*, June 6, 2014. https://www.internetsociety.org/resources/deploy360/2014/case-study-facebook-moving-to-an-ipv6-only-internal-network

Appendix A References

[1] Internet Society. *State of IPv6 Deployment 2018*. Available: https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018

[2] Internet Society. *Case Study: Facebook Moving To An IPv6-Only Internal Network*. Available: https://www.internetsociety.org/resources/deploy360/2014/case-study-facebook-moving-to-an-ipv6-only-internal-network

[3] Internet Society. *Case Study: T-Mobile US Goes IPv6-only Using 464XLAT*. Available: https://www.internetsociety.org/resources/deploy360/2014/case-study-t-mobile-us-goes-ipv6-only-using-464xlat

[4] American Registry for Internet Numbers (ARIN). *Microsoft Works Toward IPv6-only Single Stack Network*. Available: https://www.arin.net/blog/2019/04/03/microsoft-works-toward-ipv6-only-single-stack-network/

[5] Office of Management and Budget (OMB), *Completing the Transition to Internet Protocol Version 6 (IPv6)*, OMB Memorandum 21-07, November 19, 2020. Available: https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf

[6] National Cybersecurity Center of Excellence (NCCoE). *Security for IPv6 Enabled Enterprises workshop*, June 12, 2019. Available: https://www.nccoe.nist.gov/events/security-ipv6-enabled-enterprises

[7] Asia Pacific Network Information Centre (APNIC) Labs. *IPv6 Capable Rate by country (%)*. Available: https://stats.labs.apnic.net/ipv6

[8] Akamai. *IPv6 Adoption By Country/Region*. Available: https://www.akamai.com/visualizations/state-of-the-internet-report/ipv6-adoption-visualization

[9] Internet Society. *IPv6 Case Studies*. Available: https://www.internetsociety.org/deploy360/ipv6/case-studies

[10] ARIN. *IPv6 Case Studies*. Available: https://www.arin.net/blog/ipv6

[11] Cybersecurity & Infrastructure Security Agency (CISA). *Trusted Internet Connections*. Available: https://www.cisa.gov/trusted-internet-connections

[12] CISA. *Continuous Diagnostics and Mitigation (CDM)*. Available: https://www.cisa.gov/cdm

[13] OMB, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, OMB Memorandum 21-31, August 27, 2021. Available: https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

[14] OMB and CISA. *Federal Zero Trust Strategy*. Available: https://zerotrust.cyber.gov/federal-zero-trust-strategy

556 # Appendix B Acronyms and Abbreviations

3GPP	Third Generation Partnership Project
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity & Infrastructure Security Agency
COTS	Commercial Off-the-Shelf
DHCP	Dynamic Host Configuration Protocol
DLPS	Data Loss and Prevention System
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
IaaS	Infrastructure as a Service
ICAM	Identity, Credential, and Access Management
IDPS	Intrusion Detection and Prevention System
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPAM	Internet Protocol Address Management
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
MDM	Mobile Device Management
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OMB	Office of Management and Budget
PaaS	Platform as a Service
PKI	Public Key Infrastructure
RFC	Request for Comments
SaaS	Software as a Service
SIEM	Security Information and Event Management
SP	Special Publication

VPN	Virtual Private Network
WAN	Wide Area Network