18.5. Internet Protocol Version 6

Objective

18.5.1. IPv6 is disabled until it is ready to be deployed.

Context

Scope

18.5.2. This section covers information on IPv6 and its deployment within networks. Where this manual specifies requirements for network devices, the requirements apply equally whether deploying IPv6 or IPv4.

18.5.3. IPv6 was officially launched by the Internet Society in June 2012. With the change from IPv4 to IPv6, there is the potential to introduce vulnerabilities to agency networks through incorrect or mis-configuration, poor design and poor device compatibility. Attackers will also be actively seeking to exploit vulnerabilities that will inevitably be exposed.

18.5.4. Agencies unable to meet the compliance requirements as specified for a control when deploying IPv6 network infrastructure will need to follow the procedures as specified in this manual for varying from a control and the associated compliance requirements.

DNS Security Extensions (DNSSEC)

18.5.5. DNSSEC has been developed to enhance Internet security and can digitally 'sign' data to assure validity. It is essential that DNSSEC is deployed at each step in the lookup from root zone to final domain name (e.g., www.icann.org). Signing the root (deploying DNSSEC on the root zone) is a necessary step in this overall process. Importantly it does not encrypt data. It just attests to the validity of the address of the site you visit. DNSSEC and IPv6 have been engineered to integrate and thus enhance Internet security.

References

18.5.6.

Reference	Title	Publisher	Source
	A strategy for the transition to IPv6 for Australian Government agencies. (archived document)	Australian Government Information Management Office	https://www.hpc.mil/images/hpcdocs/ipv6/endorsed_strategy_for_the_transition_to_ipv6_for_australian_government_agencies_v2.pdf [PDF, 466 KB]
	IPv6 First-Hop Security Concerns	Cisco	https://www.cisco.com/c/en/us/products/ios-nx-os-software/ipv6-first-hop-security-ffs/index.html
	Manageable Network Plan	NSA	NSA Manageable Network Plan.pdf (PDFy mirror): Free Download, Borrow, and Streaming : Internet Archive
	Router Security Configuration Guide Supplement – Security for IPv6 Routers, 23 May 2006 Version: 1.0	NSA	https://hpc.mil/images/hpcdocs/ipv6/nsa-router-security-configuration-supplement-guide-for-ipv6.pdf [PDF, 1.37 MB]
	Firewall Design Considerations for IPv6, 10/3/2007	NSA	https://www.hpc.mil/images/hpcdocs/ipv6/nsa-firewall-design-ipv6-i733-041r-2007.pdf [PDF, 332 KB]
NIST Special Publication 800-41, Revision 1, September 2009	Guidelines on Firewalls and Firewall Policy,	NIST	https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final
NIST Special Publication 800-119, December 2010	Guidelines for secure deployment of IPv6	NIST	https://csrc.nist.gov/publications/detail/sp/800-119/final
	A Complete Guide on IPv6 Attack and Defense	SANS Institute	https://www.sans.org/white-papers/33904/?show=complete-guide-ipv6-attack-defense-33904&cat=detection
RFC 2460	Internet Protocol, Version 6 (IPv6) Specification, December 1998	IETF	https://datatracker.ietf.org/doc/html/rfc2460
RFC 4291	IP Version 6 Addressing Architecture, February 2006	IETF	https://datatracker.ietf.org/doc/html/rfc4291
RFC 5952	A Recommendation for IPv6 Address Text Representation, ISSN: 2070-1721, August 2010	IETF	https://datatracker.ietf.org/doc/html/rfc5952
RFC 6052	Ipv6 Addressing of IPv4/IPv6 Translators, ISSN: 2070-1721, October 2010	IETF	https://datatracker.ietf.org/doc/html/rfc6052
RFC 7136	Significance of IPv6 Interface Identifiers, ISSN: 2070-1721, February 2014	IETF	https://datatracker.ietf.org/doc/html/rfc7136
RFC 6781	DNSSEC Operational Practices, Version 2	IETF	https://datatracker.ietf.org/doc/rfc6781/
RFC 6840	Clarifications and Implementation Notes for DNS Security (DNSSEC)	IETF	https://datatracker.ietf.org/doc/html/rfc6840
RFC 6841	A Framework for DNSSEC Policies and DNSSEC Practice Statements	IETF	https://datatracker.ietf.org/doc/html/rfc6841
RFC 7123	Security Implications of IPv6 on IPv4 Networks	IETF	https://datatracker.ietf.org/doc/html/rfc7123
RFC 4861	Neighbor Discovery for IP version 6 (IPv6)	IETF	https://datatracker.ietf.org/doc/html/rfc4861
RFC 5942	IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes	IETF	https://datatracker.ietf.org/doc/html/rfc5942
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	IETF	https://datatracker.ietf.org/doc/html/rfc3315
RFC 6104	Rogue IPv6 Router Advertisement Problem Statement	IETF	https://datatracker.ietf.org/doc/html/rfc6104
	DNSSEC – What Is It and Why Is It Important?	Internet Corporation for Assigned Names and Numbers (ICANN)	https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en#

Rationale & Controls

Use of dual-stack equipment

18.5.7.R.01. **Rationale**

In order to reduce the attack surface area of agency systems, it is good practice that agencies disable unused services and functions within network devices and operating systems. If agencies are deploying dual-stack equipment but not using the IPv6 functionality, then that functionality should be disabled. It can be re-enabled when required. This will reduce the opportunity to exploit IPv6 functionality before appropriate security measures have been implemented.

18.5.7.C.01.

Control System Classifications(s): All Classifications; Compliance: Must [CID:3951]

Agencies not using IPv6, but which have deployed dual-stack network devices and ICT equipment that supports IPv6, MUST disable the IPv6 functionality, unless that functionality is required.

18.5.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3952]

Network security devices on IPv6 or dual-stack networks MUST be IPv6 capable.

Using IPv6

18.5.8.R.01. **Rationale**

The information security implications around the use of IPv6 are still largely unknown and un-tested. As many of the deployed network protection technologies, such as firewalls and IDSs, do not consistently support IPv6, agencies choosing to implement IPv6 face an increased risk of systems compromise.

18.5.8.R.02. **Rationale**

A number of tunnelling protocols have been developed to facilitate interoperability between IPv4 and IPv6. Disabling IPv6 tunnelling protocols when this functionality is not explicitly required will reduce the risk of bypassing network defences by means of encapsulating IPv6 data inside IPv4 packets.

18.5.8.R.03. **Rationale**

Stateless Address Autoconfiguration (SLAAC) is a method of stateless IP address configuration in IPv6. SLAAC reduces the ability to maintain complete logs of IP address assignment on the network. To avoid this constraint, stateless IP addressing SHOULD NOT be used.

18.5.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3960]

Agencies using IPv6 MUST conduct a security risk assessment on risks that could be introduced as a result of running a dual stack environment or transitioning completely to IPv6.

18.5.8.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3961]

Agencies implementing a dual stack or wholly IPv6 network or environment MUST re-accredit their networks.

18.5.8.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3962]

IPv6 tunnelling MUST be disabled on all network devices, unless explicitly required.

18.5.8.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3965]

Dynamically assigned IPv6 addresses SHOULD be configured with DHCPv6 in a stateful manner and with lease information logged and logs stored in a centralised logging facility.

New systems and networks

18.5.9.R.01. **Rationale**

Planning and accommodating changes in technology are an essential part of securing architectures and systems development.

18.5.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3971]

Any network defence elements and devices MUST be IPv6 aware.

18.5.9.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3972]

New network devices, including firewalls, IDS and IPS, MUST be IPv6 capable.

18.5.9.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3974]

Agencies SHOULD consider the use of DNSSEC.

Introducing IPv6 capable equipment to gateways

18.5.10.R.01. **Rationale**

Introducing IPv6 capable network devices into agency gateways can introduce a significant number of new security risks. Undergoing reaccreditation when new IPv6 equipment is introduced will ensure that any IPv6 functionality that is not intended to be used cannot be exploited by an attacker

before appropriate information security mechanisms have been put in place.

18.5.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4012]

IPv6 tunnelling MUST be blocked by network security devices at externally connected network boundaries.

18.5.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4014]

Agencies deploying IPv6 equipment in their gateway but not enabling the functionality SHOULD undergo reaccreditation.

Enabling IPv6 in gateways

18.5.11.R.01. **Rationale**

Once agencies have completed the transition to a dual-stack environment or completely to an IPv6 environment, reaccreditation will assist in ensuring that the associated information security mechanisms for IPv6 are working effectively.

18.5.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4018]

Agencies enabling a dual-stack environment or a wholly IPv6 environment in their gateways MUST reaccredit their gateway systems.