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

Special Publication 500-267
(Draft)

A Profile for IPv6 in the U.S. Government – Version 1.0

Recommendations of the National Institute of Standards and Technology

Stephen Nightingale, Doug Montgomery, Sheila Frankel and Mark Carson

NIST Special Publication 500-267 (Draft)

A Profile for IPv6 in the U.S. Government (Draft) – Version 1.0

Recommendations of the National Institute of Standards and Technology

Stephen Nightingale, Doug Montgomery, Sheila Frankel and Mark Carson

Internetwork Technologies

Advanced Network Technologies Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

January 2007

U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

Technology Administration

Robert C. Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology

William Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 500-series reports on ITL's research, guidance, and outreach efforts in Information Technology and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 500-267 (Draft)
Natl. Inst. Stand. Technol. Spec. Publ. 500-267, 47 pages (January 2007)

Acknowledgements

The authors, Stephen Nightingale, Doug Montgomery, Sheila Frankel and Mark Carson, of the National Institute of Standards and Technology (NIST), wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would like to acknowledge the members of the Federal Government IPv6 Working Group for their keen and insightful assistance throughout the development of the document, and the members of the wider Federal Government who offered useful technical and editorial comments.

Table of Contents

List of Appendices

Executive Summary

The suite of protocols commonly known as Internet Protocol version 6 (IPv6) [1] has been under design and development within the Internet Engineering Task Force (IETF) and the Internet industry for over 10 years. This industry lead effort was initiated in the early 1990's to address perceived scaling problems in the Internet's addressing and routing architectures. Today, stable standards exist for basic IPv6 functionality, commercial implementations and services are emerging and vendors and large user groups are pursuing significant product development and technology adoption plans.

The United States Government (USG) is one such large user group, and most Agencies across the government are beginning to plan for the adoption and deployment of IPv6 technologies in response to mission driven technical and economic assessments of the technology [62], broad government policies [63], the product release plans of major vendors, and the plans and actions of other organizations on the Internet.

Given the prevalence and importance of Internet technologies in Federal information technology (IT) systems today and the nature and scale of both the opportunities and risks associated with significant deployments of new networking technologies, NIST undertook an effort to evaluate the need for additional standards and testing infrastructures to support USG plans for IPv6 deployment. As part of this effort we examined the state of base IETF standards; the present state of maturity of commercial implementations; the Department of Defense IPv6 profile [3] and product testing capability [4]; and, national and international profiles and testing programs driven by the vendor communities [5]. The objective of this analysis was to determine: (a) where significant technical gaps exist in the near term technical landscape for IPv6 deployment; (b) what, if any, additional standards and testing infrastructures and processes are needed to assist federal agencies towards safe and economical adoption of this new technology.

Our findings from these efforts include:

1. A core set of IPv6 standards have stabilized and operationally viable commercial implementations of these specifications are becoming available. Agency budgeting, procurement and deployment planning, could benefit from a common identification and definition of these base IPv6 capabilities.

2. While significant commercial implementations have and continue to emerge, broad vendor product lines are currently at varying levels of maturity and completeness. Until there is time for significant market forces to effectively define *de facto* standard levels of completeness and correctness, product testing services may be needed to ensure the confidence and to protect the investment of early IPv6 adopters.

3. The current state of IPv6 security technologies and operational knowledge lags behind that of IPv4 and the existing Internet. Additional efforts are required to "raise the bar" in these areas to ensure the safety of IPv6 deployments in operational Federal IT systems.

4. While, in general, the proliferation of technology standards is to be avoided, the existing DoD and industry profiling and testing efforts are not well suited in content, nor governance, for the perceived requirements of the USG as a whole. In the near term, the broad requirements of civilian agencies can be best met by a distinct profile and testing program. In the long term, it would be desirable to converge and harmonize these efforts into broader user/vendor initiatives in which the technical and process requirements of the USG can be accommodated.

5. Some key IPv6 design issues remain unresolved. As the USG begins to undertake significant operational deployments and investments in IPv6 technology, additional efforts are warranted to ensure that the eventual resolution of these design issues remains consistent with USG requirements and investments.

This document recommends a technology acquisition profile for common IPv6 devices to be procured and deployed near term, in operational USG IT systems. It is intended to address several aspects of findings 1, 3, 4 and 5 above and will be augmented by additional documents and activities including:

- Development of operational guidance for the secure adoption of IPv6 [65] to further address findings 3 and 5.

- Development of a near term testing strategy for IPv6 technologies [2] to further address finding 2.

This standards profile is meant to: (a) define a simple taxonomy of common network devices; (b) define their minimal mandatory IPv6 capabilities and identify significant options so as to assist agencies in the development of more specific acquisition and deployment plans; and, (c) provide the basis to further define the technical meaning of specific policies. The scope of the device taxonomy and the selection of mandatory capabilities and identified options are purposefully conservative in some ways; defining systems and capabilities that are thought to be of common utility to the USG as a whole. In other ways, this profile "raises the bar" for some areas of IPv6 technology that are thought vital to protect the current and future security of federal IT systems and to protect the economic investment of early adopters.

It is fully expected that agencies would further augment these specifications to meet the requirements of specific IT system procurements and deployment policies.

1. Introduction

This profile has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should this profile be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the Office of Management and Budget, or any other Federal official.

1.1 Purpose and Scope

This publication seeks to assist Federal Agencies in formulating plans for the acquisition and operational deployment of IPv6 technologies. To achieve this, we define a standards profile for IPv6 in the U.S. Government that is intended to be applicable to all future uses of IPv6 in non-classified federal IT systems. The standards profile is meant to: (a) define a simple taxonomy of common network devices; (b) define their minimal mandatory IPv6 capabilities and identify significant options so as to assist agencies in the development of more specific acquisition and deployment plans; and, (c) provide the basis to further define the technical meaning of specific policies. It presents information in principle independent of particular hardware platforms, operating systems, and applications, though intimately connected with their networking capabilities.

The scope of the device taxonomy and the selection of mandatory capabilities and identified options are purposefully conservative in some ways; defining systems and capabilities that are thought to be of common utility to the USG as a whole. In other ways, this profile "raises the bar" for some areas of IPv6 technology that are thought vital to protect the current and future security of federal IT systems and to protect the economic investment of early adopters.

The profile is meant to be a landmark to guide the acquisition and deployment of significant new IPv6 capabilities in operational federal IT systems. No attempt has been made to grandfather existing early implementations, nor cover potential non-production level uses of the technology in test-beds, pilots, etc. In summary, the profile is meant as a strategic planning guide for future acquisitions and deployments in operational networks. Other uses of this profile, without agency specific refinement, is not recommended.

It is fully expected that agencies may further augment these specifications to meet the unique requirements of specific IT system procurements and deployment policies.

1.2 Audience

This publication is intended to serve a diverse federal audience of information system and information security professionals including: (i) individuals with information system and information security management and oversight responsibilities (chief information officers, senior agency information security officers, and authorizing officials); (ii) individuals with information system development responsibilities (program and project managers, mission/application owners, system designers, system and application programmers); (iii) individuals with information security implementation and operational responsibilities (information system owners, information owners, information system administrators, information system security officers,); and (iv) individuals with information system and information security assessment and monitoring responsibilities (auditors, inspectors general, evaluators, and certification agents).

Commercial companies producing information technology products and systems, creating information security-related technologies, and providing Internet services can also benefit from the information in this publication. When used as the basis for acquisition requirements, the profile defined in this publication will be of direct interest to:

- Internet device implementors, including developers of Host, Router and Network Protection hardware and software.

- Internet test device implementors and operators, the latter including conformance, Interoperability and performance test houses.

All members of this audience, and others, are encouraged to carefully review and comment on this draft version of the profile.

1.3 Document Structure

The remainder of this document is organized into 7 major sections. Section 2 on Architectural Issues contains text motivating the choices of IPv6 related protocols as they affect Agency Intranet and Internet infrastructure. This section also motivates the device types and functional categories for which specification is required.

Please note the modularization principle of this specification. The 3 device types of Host, Router and Network Protection Device are specified as selections from the functional categories. Hosts and Routers are specified in sections 3 and 4 respectively. Uniquely, while Network Protection Devices (Firewalls, Intrusion Detection and Prevention systems, and their like) have been vital elements in enterprise and network security architectures for years, few, if any, consensus standards exist to define their capabilities. Given the lack of such standards, as an initial step, we define in section 5 a lowest common denominator specification for these devices.

Functional categories are elaborated in text in section 6. These textual descriptions are intended as commentary to help understand the spreadsheet in Appendix D, which is the definitive specification.

For a specification to be implementable, there must also be a means of determining compliance with it. The parameters of a potential test program for this profile are sketched out in Section 7, though more fully elaborated in a separate document [2].

The Bibliography is given in Appendix A, while terms used in the text are defined in B. The Profile is condensed into a tabular form, and the key to its interpretation is given in C, but the table itself constitutes Appendix D. Where the text descriptions in sections 3, 4, 5 and 6 of this document conflict with Appendix D, or where they fail to specify functionality, Appendix D takes precedence.

Normative Terminology:

The terminology used to describe requirements levels in this profile include: “mandatory”, “optional” (with their common meaning), and "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" which are to be interpreted as described in RFC 2119 [61]. In addition, this profile adopts the use of the term “SHOULD+”to indicate a requirement that is equivalent to “SHOULD” in this version of this specification, but is expected to be elevated to a “MUST” in future versions.

2. Architectural Issues

As Agencies begin to adopt IPv6 technologies and connect to the Internet via IPv6, they will need to establish a common interoperability strategy across the entire USG. While interoperability is important, it is also important that, for the sake of flexibility in adapting to individual agency's needs, the requirements intended to assure such interoperability not be overdetermined. Similarly, it is essential that throughout the transition process, even as new technologies are introduced, each agency's infrastructure be continually protected. There are a number of ramifications explored here, which have in particular motivated the selection of device IPv6 capabilities for USG use.

The first step towards the successful adoption and widespread use of IPv6 is the establishment a core network infrastructure capable of providing IPv6 data services to the applications that will eventually follow. This profile addresses the devices and capabilities necessary to develop operationally viable IPv6 network services. In particular, this version of the profile primarily focuses on the network layer; specifying the minimal required IPv6 capabilities necessary for production level data-plane services that can operate at potentially large scales.

The key to IPv6 evolution in core network infrastructures resides in the capabilities of routers and their control (routing) protocols. This profile provides the minimal mandatory definition of an IPv6 router. It identifies two types of router devices, interior gateways and exterior gateways.

Establishing an IPv6 core network opens the door to creating new host applications adapted to exploit the added capabilities of the new infrastructure. It is exactly this potential, to develop new applications, at larger scales, that is the real promise of IPv6. This profile provides the minimal mandatory definition of an IPv6 host. While it seems premature at this time to define specific IPv6 applications, the basic host IPv6 infrastructure here does provide the basis for building future applications. We anticipate the future, incremental expansion of this profile as needed and appropriate to accommodate such applications.

This is a profile for IPv6 technologies; it places no requirements on the capabilities or uses of IPv4 technologies within the USG, other than addressing how the IPv6 systems can and should coexist and interoperate with existing IPv4 systems. These IPv4-IPv6 transition mechanisms are a vital element of most IPv6 deployment plans. The basic features are described in *RFC 4213 "Transition Mechanisms for IPv6 Hosts and Routers*" [6], specifying dual-stack and tunneling mechanisms.

The Internet is not the safe academic space it was during the initial development of IPv4 in the 1970s and early 1980s. With the rise of dangers such as viruses, worms [10] and denial of service attacks, network security technologies have become paramount in ensuring the viability and trustworthiness of networked IT systems. These technologies can be thought of in two groups: (1) IP security (IPsec) technologies designed to protect the trustworthiness and privacy of wanted communications, and (2) Network Protection Devices (NPDs) designed to detect and block unwanted communications.

- IPsec technologies are defined by the current compendium specification *RFC 4301 "Security Architecture for the Internet Protocol"* [11] which identifies encryption, authentication, integrity and secure transport mechanisms. However IPsec is undergoing generational changes that make the selection of a profile a little less than straightforward. We specify an IPsec profile in detail based on the current view of best security practices.

- Although the IPv4 device industry is replete with Firewalls, guidance documents, test specifications and even test and certification programs, an actual consensus specification for such devices seems to be absent. For this reason, this publication contains in section 7 a specification for *Network Protection Devices*.

In sum, this profile is a reasoned selection of standards, mostly RFCs, grouped into Subprofiles and device profiles. The complete list of designated RFCs is included in Appendix D.

Summarization of Device Types

In the general case the IETF defines an IPv6 Node as a device that implements IPv6. The IETF recognizes two types of Node, Hosts and Routers. It may be possible to shoehorn Network Protection Devices (NPD) into one or both of these categories, but we believe that their functionality is sufficiently specialized that it be defined in a separate category. Thus, there are three types of devices in this profile: Hosts, Routers and Network Protection Devices, defined as:

1. **Host:** any Node that is not a Router.

2. **Router:** a Node that forwards IPv6 packets not explicitly addressed to itself.

3. **Network Protection Devices:** Including Firewalls and Intrusion Detection / Prevention devices that examine and selectively block or modify network traffic.

3. Host Profile

This part of the USG profile is applicable to Host systems accessible by an end user or end application. This includes network level access by host operating systems and their associated networked applications. Most such applications are unspecified at this time. Specific Host requirements should be put together by selecting Functional Categories from the definitive spreadsheet in Appendix D, cross referencing with the normative designation under the 'Host' column. Functions marked here as Should or Optional required in particular procurements can be upgraded to Must, according to local need.

At a minimum, Hosts MUST support:

Host specific Base criteria as in Subsection 6.1.

Host specific Transition criteria as in Subsection 6.4.

Host specific Link Technologies as in Subsection 6.5.

Host specific Addressing requirements as in Subsection 6.6.

Host specific IPsec Security criteria as in Subsection 6.7.

Host specific Application criteria as in Subsection 6.8.

Host specific Network Management criteria as in Subsection 6.9.

Host specific Multicasting criteria as in Subsection 6.10.

Host specific Mobility criteria as in Subsection 6.11.

4. Router Profile

The Internet can be viewed as having (at least) two layers of routing system for forwarding IP packets toward their ultimate destination. Typically, within a local organization or site (Autonomous System, in networking terminology), interior routing protocols are used to distribute routing information among its various subnetworks. Between different Autonomous Systems, exterior routing protocols are used. An individual router may fall into one or both categories. The profile defined here covers either possibility.

Specific Router requirements should be put together by selecting Functional Categories from the definitive spreadsheet in Appendix D, cross referencing with the normative designation under the 'Router' column. Functions marked here as Should or Optional required in particular procurements can be upgraded to Must, according to local need.

At a minimum, Routers MUST support:

Base criteria as in Subsection 6.1.

Routing criteria as in Subsection 6.2.

Router specific Quality of Service criteria as in Subsection 6.3.

Router specific Transition criteria as in Subsection 6.4

Router specific Link Technologies as in Subsection 6.5.

Router specific Addressing requirements as in Subsection 6.6.

Router specific IPsec Security criteria as in Subsection 6.7.

Router specific Network Management criteria as in Subsection 6.9.

Router specific Multicasting criteria as in Subsection 6.10.

Router specific Mobility criteria as in Subsection 6.11.

5. Network Protection Device Profile

Network protection devices may effectively operate as either routers or hosts, with respect to network traffic flow. However, given their specialized functionality, they are not normally expected to operate as general-purpose nodes. In fact, some classes of network protection devices are deployed in combination with general-purpose routers and hosts to effect a desired security architecture.

Rather than attempt to characterize the entire range of such potential combined devices, we instead focus on the specialized security functionality that differentiates network protection devices from typical hosts and routers. These specialized requirements are discussed in Subsection 6.12 and listed in Appendix D.

Clearly providing network protection services in IPv6 networks requires at least partial support for many IPv6 standards (e.g., ability to parse IPv6 packets, support IPv6 addressing, encapsulate IPv6 on specific Link technologies, etc). Hybrid devices that provide router or host functions may in fact be required to meet the full requirements of these device profiles. The exact extent to which network protection devices must fully support IPv6 standards beyond those capabilities defined in subsection 6.12 is left for further refinement.

6. Functional Categories

There is a good deal of complexity in the RFCs relating to IPv6, but this can be clustered according to particular functions. These are articulated in the subsections below. Functional Categories, standards, and specific protocol functions can also be classified by the clauses that describe their implementation requirement level, or normative status, within the profile. The Base IPv6 functionality (6.1) applies across all systems, but it is treated as a functional category here for the purposes of modularity.

Routing standards (6.2) apply to Routers only. Quality of Service functions (6.3) apply only to Routers. Transition mechanisms between IPv4 and IPv6 (6.4) apply across the board, but are MUST for Routers and Optional for USG Hosts. Link technologies (6.5) entail a selection of one or more for every IPv6 Node. Addressing requirements (6.6) entail support across all IPv6 Nodes of a compendium of Internet Standards. A set of standards for IP security (IPsec, 6.7) is adopted in this profile. There are initial provisions for some Application infrastructure (6.8), which apply to Hosts. This functional category is anticipated to be further articulated as IPv6 Applications mature. There are minimal MUST requirements levied for Network Management (6.9), Multicasting (6.10) and Mobility (6.11). It is expected that future versions of this profile, or use specific refinements will further enhance the requirements in these areas. Network Protection Devices are elaborated in Subsection 6.12.

Appendix D includes a spreadsheet giving the cross-reference of recommendations between IPv6 device types and detailed functionalities. This enumerates the relevant standards under each subprofile and selects requirement levels for each standard and appropriate paragraphs. Where the text descriptions in 3, 4, 5 and 6 of this document conflict with Appendix D, or where they fail to specify functionality, Appendix D takes precedence.

6.1 Base

Deploying IPv6 at the network layer requires use of a quite large set of interrelated standards. These can be structured as a basic set, plus groups of function specific specifications. The Base set comprises packet structure, transmission mechanisms and error reporting mechanisms, device address allocation, and basic discovery of other local Nodes.

Where protocol functional requirements are not specified in the Appendix, the USG requirement remains the same as the RFC.

The basis for IPv6 is defined in RFC2460 *IPv6 Specification* [1], and RFC 4443 *Internet Control Message Protocol (ICMPv6)* [18]. Full support of appropriate parts of both specifications are a MUST for Hosts and Routers.

RFC 1981 *Path MTU Discovery* [12] as a whole is a MUST for both Hosts and Routers. This is the mechanism for discovering the maximum packet size supported along a complete end-to-end path. Nodes that do not implement all the details of RFC 1981 must be cognizant of the minimum requirement, which is to implement an MTU of 1280 bytes.

RFC 2461 *Neighbor Discovery* [13] is a reengineering of the IPv4 functions of Address Resolution, Router Discovery and ICMP Redirection. It MUST be implemented by every IPv6 Node. Further, *IPv6 Node Requirements* [14] asks that Hosts SHOULD implement Section 8 Redirect functionality and Routers MUST implement it. This USG specification follows that requirement.

RFC 3971 *Secure Neighbor Discovery* [15] is brought under the Base profile in this USG profile and specified as SHOULD+ for both Hosts and Routers.

Address Autoconfiguration is the method by which Hosts acquire IPv6 addresses, and may occur through RFC 2462 *Stateless Address Autoconfiguration [16]*, or its stateful equivalent, RFC 3315 *DHCPv6 [17]*. These two methods are complementary, not necessarily mutually exclusive. This profile designates Stateless Address Autoconfiguration as a MUST for both Hosts and Routers, and DHCP based mechanisms as a SHOULD+ for Hosts.

RFC 4443 *ICMPv6* [18] is the mechanism in the Internet for returning status information within the IP layer. It is a MUST in both Hosts and Routers.

6.2 Routing

The function of Routing is to select a path among two or more viable choices, and forward a packet towards its intended destination along that path. The current model of Routing in the Internet identifies Interior and Exterior Routing functions. Most Agencies will use both Interior Routers and Exterior Routers. Hence, a USG Router device may be an Interior Router or an Exterior Router, or both.

For Interior Routers, RFC 2740 OSPF [7] is the mandatory routing protocol, and *RFC 4552 Authentication for OSPFv3* [19] is strongly recommended.

For Exterior Routers, BGP MUST be supported. This includes RFCs 4271, 1772, 2545 and 2858 [20] - [23].

6.3 Quality of Service

The development of new scalable Quality of Service (QoS) mechanisms for IPv6 remains a work in progress. Todate, the only mechanisms that have proven of general broad utility and viability is the support of Differentiated Services mechanisms in Routers. Accordingly, RFC 2474 *Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers* MUST be supported in all routers.

As QoS technologies mature, future versions of this profile may incorporate additional QoS requirements (e.g., signaling protocols, APIs) for Hosts and Routers.

6.4 Transition

The key to a successful IPv6 transition is compatibility with the large installed base of IPv4 Hosts and Routers. Maintaining compatibility with IPv4 while deploying IPv6 will streamline the task of transitioning the Internet to IPv6. Most Nodes will need such compatibility for a long time to come, and perhaps even indefinitely. Transition and co-existence mechanisms are defined in RFC 4213 *Basic Transition Mechanisms for IPv6 Hosts and Routers [6]*. These mechanisms include Dual Stack, and Tunneling. The mechanisms mandated for USG Routers include Dual Stack IPv4-IPv6 and Configured Tunnels. In addition, for those networks relying on Multiprotocol Label Switching in their core, this

profile notes that technologies that leverage IPv4 based MPLS to interconnect islands of IPv6 are a viable option.

6.5 Link Technology

When implemented natively, IPv6 operates over a variety of Layer 2 link technologies, for which the IETF has defined interface standards. These include interfaces for Ethernet, Fiber Distributed Data Interface (FDDI), Point to Point (PPP), Non-Broadcast Multiple Access (NBMA), Asynchronous Transfer Mode (ATM), Frame Relay, Institute for Electrical and Electronic Engineers (IEEE) 1394 Firewire, and others. Routers typically forward between two or more instances of these. IPv6 Hosts and Routers in this profile must support at least one such identified interface standard. This is specified in the spreadsheet as 'O:1' meaning "Optional, Pick One". A full description of the key is given in Appendix C.

6.6 Addressing

This profile mandates support, in both Hosts and Routers, for the RFC 4291 *IP Version 6 Addressing Architecture [26],* with its scoping rules and its support for Unique Local Unicast addresses defined in RFC4007, and address source address selection rules defined in RFC3484.

Privacy Addresses and Cryptographicaly Generated Addresses are recommended, but not mandated at this time. See Appendix D for details.

The scope of this document is limited to the definition of recommended minimal device capabilities. There are many significant issues associated with strategies for IPv6 address allocation and assignment. While many of these issues (e.g., provider independence, multi-homing, routing scalability, operational security) are critical to the eventual long term success of IPv6, they are beyond the scope of this specification. Other Federal guidance documents and policies are expected to be developed to address these issues.

6.7 IPsec

The most common current use of IPsec is to provide a Virtual Private Network (VPN), either between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway). IPsec is also used by other Internet protocols (e.g. Mobile IPv6 a.k.a. MIPv6) to protect some or all of their traffic. End-to-End (host-to-host) IPsec protection is less commonly employed, since encrypted traffic is impenetrable to analysis. Thus, it would require the enterprise Network Protection Devices (firewall, IDS, IPS) to allow the IPsec-protected traffic to enter the enterprise network without inspection by these devices. That would place the total responsibility for the enterprise's security on the host and/or the host's user, which is generally not viewed as a prudent approach in today's networks.

In order to use automated key management protocols such as the Internet Key Exchange (IKE) to negotiate and manage IPsec protections and secret keys between two peers, those peers must be able to definitively authenticate each other (i.e. verify each others' identities) in the course of the IKE negotiation. The most common methods are the use of Public Key Certificates or, for host-to-gateway IPsec, a combination of a certificate for the gateway and an Extensible Authentication Protocol (EAP)-based authentication method for the host. These methods require either a previous relationship between the peers, or the use of Public Key Certificates whose Certificate Authorities (CA) are mutually recognized. This is the reason that IPsec is most commonly used within a VPN, rather than for totally opportunistic communication with formerly unknown peers.

The protections provided by IPsec, and the protection that IKE provides to its own traffic, require the use of cryptographic algorithms, which include encryption algorithms (to provide confidentiality), MACs or Message Authentication Codes (to provide integrity protection), and PRFs or Pseudo-Random Functions (to generate secret keys). For government users, these algorithms must be FIPS-140 [27] compliant; thus, the cryptographic operations performed by IPsec and IKE implementations must reside within FIPS-140-validated cryptographic modules.

Currently, implementations are available for two versions of IPsec. IPsec-v3, consisting of RFC 4301 (Architecture) [11], RFC 4303 (ESP) [28] and RFC 4302 (AH) [29], is preferred but may not yet be widely available. IPsec-v2, consisting of RFC 2401 (Architecture) [30], RFC 2406 (ESP) [31] and RFC 2402 (AH) [32] has been made obsolete by IPsec-v3, but is still the most commonly available version of IPsec. In either case, this profile classifies AH as optional. Null authentication (i.e. encryption only) is mandatory in IPsec-v2, but optional in IPsec-v3. However, if null authentication is used, the traffic must be integrity-protected through some other mechanism (e.g., a broader IPsec SA that also covers the segment with null authentication).

There are also two versions of IKE. IKEv2 (RFC 4306) [33] implementations are in their early stages; this is the preferred version. IKEv1, consisting of RFC 2409 (IKE) [34], RFC 2408 (ISAKMP) [35] and RFC 2407 (DOI) [36], is currently the most commonly available version of IKE.

This profile references only IETF RFCs (the IETF's standards documents), not Internet Drafts, which are works in progress that may or may not be promoted to RFC status. However, there are several IPsec-related Internet Drafts that are expected to become RFCs in the near future. "*Requirements for an IPsec Certificate Management Profile*" [37] has been recommended for RFC status, and "*The IPsec PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX*" [38] is expected to be recommended for RFC status in the near future. Certificate format, contents and interpretation have been a source of interoperability problems within IKE, so it is expected that these RFCs will be added to the IPsec profile.

Cryptographic Algorithms within IPsec and IKE

Both versions of IKE relate to cryptographic algorithms in two distinct contexts. In the course of an IKE negotiation, IKE selects an encryption algorithm and an integrity protection algorithm to protect its own traffic (the IKE Security Association). IKE also negotiates the selection of an encryption algorithm and/or an integrity protection algorithm to protect future IPsec traffic between the negotiating peers (IKEv1's IPsec SA; IKEv2's child SA). In the Appendix D spreadsheet, the IKE SA algorithms are identified as "IKEv1" or "IKEv2" in the Condition/Context column; the ESP/AH algorithms are identified as "ESP," "AH," or "ESP/AH" in that column. The ESP/AH algorithms must be implemented in IPsec and IKE must be capable of negotiating their use.

Although HMAC-SHA-1 [39] is still considered secure, the IETF is encouraging the standardization of HMAC-SHA-256 [40] to ensure an orderly transition to a more secure MAC, should that be deemed necessary. The draft "*Using HMAC-SHA-256 with IPsec*" (IETF draft-kelly-ipsec-ciph-sha2-00.txt) defines the use of HMAC-SHA-256 as a MAC within IKE, ESP and AH; and as a PRF within IKE. It is expected to progress rapidly to RFC status, and will be added to the profile at that time.

AES-GCM [41] is a counter-based, combined-mode algorithm (provides both encryption and integrity protection) for ESP that is suitable for high-speed parallelizable processing. AES-GMAC [42] is the variant of AES-GCM that provides authentication only; it can be used within both AH and ESP, but when used with ESP, it acts like a combined-mode algorithm. These algorithms have a number of variants (both have multiple key sizes; AES-GCM has multiple ICV sizes) and are somewhat complex to use. Some of these complexities (cannot be used with manual keys) are imposed by the nature of the algorithm, but

some are a result of the protocol definition (in IKE, key size must be specified for ESP, but for AH the transform ID includes the keysize info, etc.) They are not yet widely implemented in IPsec implementations, and potential interoperability issues have not been addressed at IPsec interoperability events or by standardized testing organizations. Thus, at this time, they are designated as optional algorithms in this profile.

Several of the algorithms (AES-CCM, AES-CTR, AES-GCM, and AES-GMAC) only retain their security properties if a given IV is never used more than once with the same secret key. Therefore, these algorithms cannot be used with static (manually established) keys; they are secure only if used in conjunction with IKE or another secure key negotiation protocol. Furthermore, IKE negotiates different keys for inbound and outbound traffic. If a key negotiation protocol is used that generates the same key for use in both directions, the peers must be sure to use different nonces (AES-CTR) or salts (AES-CCM, AES-GCM, AES-GMAC); otherwise, the algorithm's security is compromised.

The RFCs contain 2 contradictions related to the requirement level of algorithms. In ESP-v3 (RFC4303/section 5), null authentication is a MAY. However, in "*Cryptographic Algorithms for ESP/AH*" (RFC4305/section 3.1.1) [43], null authentication is a MUST. This profile makes it optional, as does an Internet Draft (IETF draft-manral-ipsec-rfc4305-bis-errata-02.txt) which is planned as an update to RFC4305. In "*Cryptographic Algorithms for ESP/AH*" (RFC4305/section 3.1.1), null encryption is a MUST. However, in "*Algorithms for IKEv2*" (RFC4307/section 3.1.1) [44], null encryption is a MAY, i.e., IKEv2 does not have to be able to negotiate null encryption for ESP. This profile makes null encryption a MUST.

6.8 Application Environment

As noted, it seems premature and inadvisable to broadly mandate specific applications in this version of the profile. Instead, we focus on specifying the infrastructural services of an application environment upon which future applications can be built.

To the extent that Domain Name resolution is a requirement for all systems the provisions of RFC 3596 *DNS Extensions for IPv6* [45] apply to both Hosts and Routers. Quad-A resource records are in particular mandated for both, along with Extension mechanisms for DNS queries and responses.

In some relation to this is the specification of URIs. The Host part of a URI may be specified as a registered domain name (e.g. nist.gov), or an address. IPv4 addresses take the form ‘192.168.0.1’, while IPv6 addresses have a more complex syntax including such styles as ‘2001:db8::7’. The provisions of RFC 3986 *Uniform Resource Identifier: Generic Syntax [46]*, are mandatory for Hosts, to cover these formats.

There is a set of RFCs (3493, 3542, 4584 [47]-[49]) relating to Socket API extensions for IPv6, and these SHOULD be implemented in hosts that provide such interfaces to applications.

6.9 Network Management

This profile is addresses capabilities for production level, large scale deployment of IPv6 devices. As such, it is a general requirement of this profile that all IPv6 Hosts and Routers have a network management capability. In particular all nodes must support a basic Simple Network Management Protocol (SNMP) capability and provide the basic IPv6 Management Information Base (MIB) specified in RFC4293 [66]. Routers, in addition, must support the Forwarding Table and Tunnel MIBs. Future

versions of this profile are expected to require full support of IPv6 MIBs at the Network and Transport layers.

6.10 Multicasting

This profile provides the basic Host-to-Router multicast building blocks to enable the development of more detailed Multicast capabilities in the future, or through Agency specific augmentation of this specification. In particular, Routers are required to be capable of discovering Multicast listeners – which may themselves be either Hosts or Routers, so RFC 3810 [52] is Mandated for both. In addition, MLD version 2 has extensions for Source Specific Multicast, encoded in RFC 4604 [53]. These are designated SHOULD for both Hosts and Routers.

These building blocks for multicast services form a vital foundation, but are not enough to enable multicasting on a wide scale. As IPv6 multicast routing technologies mature, it is expected that future versions of this profile will adopt additional requirements for Routers in these areas.

6.11 Mobility

RFC 3775 "*Mobility Support in IPv6*" [54] allows a Host to be mobile, and any other Host, static or mobile, to communicate with it. To this extent any Host MUST be prepared to act as a Mobile IPv6 (MIPv6) Correspondent Node. The remainder of MIPv6 functionality is optional and only applicable if an agency decides that a Host should be a mobile node, or a router should be a home agent. In these cases, appropriate functions of the Mobile IP standards are mandated (see Appendix D). Finally, to secure MIPv6 signaling, both Hosts and Routers MUST implement RFC 3776 *Using IPsec to protect MIP signaling between MNs and HAs* [55], if MIPv6 is implemented at all.

6.12 Network Protection Devices

Network protection devices (firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and the like) are nowadays a necessary part of any external network connection. This situation will no doubt continue with the change to IPv6; indeed, unlike with the original introduction of IPv4, no significant "grace period" for the development of strong IPv6 network protection technology can be expected, as hackers are already developing attack suites for IPv6 networks.

Given this situation, it is essential that IPv6 network protection devices which are just as capable as their IPv4 counterparts be immediately available with the introduction of IPv6 into government networks. Ensuring this capability exists is the goal of these requirements.

The requirements listed here concentrate on the IPv6-specific features required for network protection devices. Any other features an agency may require for its network devices (e.g., support for a particular administrative model or a special authentication method) should be addressed through the agency's usual specification and validation methods.

In particular, IPv4-only features are not addressed here. While it is to be expected that IPv4 traffic will continue for the foreseeable future, and hence IPv4 network protection devices will be required, an agency may well choose to use separate network protection devices for IPv4 and IPv6 traffic; in such a case, only the IPv6 functionality of the second device is of interest.

In general, these requirements seek merely to establish the minimal threshold of functionality required for IPv6 network protection devices. For firewalls, this means basic port-blocking and (for application firewalls) application data filtering, while for intrusion detection and prevention systems, this means the ability to detect (and, in the case of IPSs, to prevent or disrupt) known attack patterns, including IPv6 version of known IPv4 attacks. In both cases, network protection devices will typically offer other more sophisticated features, such as statistical anomaly detection, but given the minimal nature of these requirements, they will not be addressed here.

6.12.1 Source of requirements

The sort of functionality provided by network protection devices is not well-covered by protocol or interoperability specifications such as Internet RFCs. Hence, we cannot create the same sort of profiles as for host systems or routers, where we can specify desired functionality by listing relevant RFCs and options. Instead, we must list all requirements explicitly.

There are, however, two lists of firewall requirements we have used as reference sources in composing this list: the *Internet Protocol Version Six Information Assurance Test Plan* [56] public release document from DoD, and the *ICSA Labs Modular Firewall Certification Criteria* [57] version 4.1. Our firewall requirements in the main follow these documents, though as mentioned above, we concentrate solely on that functionality required for IPv6.

By contrast, there are no comparable lists of functionality requirements for intrusion detection and prevention systems. NIST Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems* [58], and NIST IR 7007, *An Overview of Issues in Testing Intrusion Detection Systems* [59] do however discuss the sorts of functionality provided by these systems and the challenges involved in testing them.

6.12.2 Common requirements for network protection devices

6.12.2.1 Basic host or router IPv6 connectivity requirements

Depending on its means of connection, a network protection device is set up either as an end node or as a router, and hence MUST provide the corresponding functionality. The exception, however, is that even when acting as a router in the sense of forwarding packets, a network protection device typically does not participate in routing protocols, but simply forwards based on static routes. Hence, we do not require implementation of any IPv6 routing protocol for network protection devices.

6.12.2.2 Dual stack

As part of the requirements for host or router functionality, network protection devices MUST implement dual IPv4 and IPv6 stacks. While it is expected that most such devices will provide protection functionality for both IPv4 and IPv6 traffic, only IPv6 protection functionality is addressed here. Other functionality (such as administrative interfaces) MAY be available over only one network stack (generally IPv4).

6.12.2.3 Administrative functionality

A network protection device must offer sufficient administrative controls to allow effective use of the facilities it offers. This includes controls over the configuration of its protective functionality, its logging and alert facilities, and access to the administrative facilities themselves. Such administrative functionality MUST be available either directly on the device console or equivalent, or through remote communications using openly-defined means.

6.12.2.4 Authentication and authorization

All administrative access to a network protection device MUST be controlled through appropriate authentication mechanisms, and restricted to appropriately authorized users. In the case of network protection devices which do not separate administrative roles, authentication as an administrator may be viewed as sufficient authorization.

6.12.2.5 Security of control and communications

All administrative controls MUST be secure from non-authorized access, and all administrative communications with a network protection device must be secure from outside observation. This may be done through local console-type access; through FIPS-approved encrypted network communication; or through network communications which are secured through other means from outside access (such as VLAN separation or firewall blocking).

6.12.2.6 Persistence

All device settings MUST persist through loss and restoration of electrical power.

6.12.2.7 Logging and alerts

Network protection devices MUST provide sufficient logging capability to allow inspection of all administratively-controlled settings and give assurance of their proper functioning. Such logging MUST be controllable by, and accessible to, properly authorized administrators.

Intrusion detection systems have additional logging requirements, as described below.

6.12.2.8 Fragmented packet handling

Network protection devices MUST be able to handle fragmented packets, whether by provisionally reassembling and applying appropriate controls based on the reassembled packet, or (in the case of firewalls) by blocking fragments that cannot otherwise be handled.

6.12.2.9 Tunneled traffic handling

Network protection devices MUST be able to handle all v4/v6 tunneling schemes, no matter how embedded, either by analyzing and applying the appropriate controls based on the embedded packet header, or (in the case of firewalls) by simply blocking all unanalyzed tunneled packets.

6.12.3 Firewall requirements

6.12.3.1 Common (port-blocking) requirements

6.12.3.1.1 Asymmetrical blocking

Firewalls MUST, either through software or hardware configuration, distinguish between external and internal connected networks, and allow imposing asymmetrical controls on traffic between these networks. In particular, firewalls MUST have the ability to allow bidirectional traffic flow over connections initiated from hosts on the internal network to hosts on the external network, while blocking connection initiation from the external network.

6.12.3.1.2 Port/protocol/address blocking

Firewalls MUST allow selective blocking/admission of traffic by source and/or destination address, by protocol, and, for IPv6 packets, by the appropriate per-protocol subfields - ports for UDP and TCP, and type and code for ICMP. Such blocking/admission MUST be equally effective for both normal and IPsec traffic, the latter to the extent such fields are visible in the packet.

Port blocking/admission functionality MUST be sufficiently rich to allow discrete controls in both directions down to the individual port level, for any desired ports. While it is desirable to be able to block/admit any possible combination of ports, at a minimum the port-blocking functionality MUST have sufficient capacity to selectively include or exclude any and all of the following services (TCP and (where relevant) UDP):

ftp (active and passive)
ssh
telnet
smtp
dns/domain (including zone transfers)
http, https
pop3, pop3s
imap, imaps

Address blocking functionality MUST be sufficiently rich to allow blocking of all traffic with source or destination addresses which should not be present in traffic sent between external and internal networks, such as local addresses (including loopback, link local, site local, and RFC 4193-style unique local addresses), or source multicast addresses.

Firewalls MUST allow blocking of all traffic which has not been explicitly authorized.

6.12.3.1.3 IPsec traffic handling

Firewalls MUST either be capable of terminating IPsec connections (security gateways), or be capable of selectively blocking IPsec traffic.

6.12.3.1.4 Performance under load, fail-safe

Firewalls MUST perform properly up to their design load; in circumstances which exceed this load or otherwise result in operational degradation or failure, they MUST fail in such a manner as not to allow unauthorized access.

6.12.3.2 Application firewall requirements

6.12.3.2.1 No violation of trust barriers

Application firewall mediation of data transversal (session, file, etc.) through the firewall MUST NOT violate trust barriers, either by improperly rewriting incoming untrusted data to appear trusted, or by improperly exposing information (such as internal network structures) to external untrusted networks.

6.12.3.2.2 Session traffic authorization

Application firewalls MUST have means of controlled authorization for the establishment of sessions initiated from the external network to internal hosts.

6.12.3.2.3 Email, file filtering

Application firewalls MUST have configurable means for examining files (such as email attachments) that are transferred from the external network to internal hosts for the presence of undesired elements, and, when such elements are found, selectively blocking or stripping them.

6.12.4 Intrusion detection and prevention system requirements

6.12.4.1 Common (detection) requirements

6.12.4.1.1 Known attack detection

Intrusion detection systems MUST provide a configurable capability to detect suspicious traffic based on known attack patterns, including those embedded in HTTP and SMTP traffic.

6.12.4.1.2 Malformed packet detection

Intrusion detection systems MUST detect malformed packet types, such as non-standard or unassigned protocols, reserved header bits being set, undefined ICMP codes, improper (e.g., local or undefined) packet addresses, bad fragments and bad TTL values.

6.12.4.1.3 Port-scanning detection

Intrusion detection systems MUST detect typical port scanning (multiple ports of a single host) and host scanning (single port across multiple hosts) techniques, including "stealth" scans. (Note that while "blind" host scanning across a subnet is not considered feasible for IPv6, other techniques such as scanning based on DNS data are still a concern.)

6.12.4.1.4 Tunneled traffic detection

Intrusion detection systems MUST be able to detect threat patterns even when packet data contents are embedded with multiple headers. For tunneling methods for which content examination is not supported, it is sufficient merely to flag all such tunneled packets.

6.12.4.1.5 Logging and alerts

Intrusion detection systems MUST provide means to log all suspicious traffic and send notification to the appropriate administrators.

6.12.4.1.6 Performance under load, fail-safe

Intrusion detection systems MUST perform properly up to their design load; in circumstances which exceed this load or otherwise result in operational degradation or failure, they MUST provide notification of such failure. (In cases of overload, intrusion detection systems should prioritize their processing to preferentially examine the highest-risk traffic.)

6.12.4.2 Intrusion prevention requirements

6.12.4.2.1 Intrusion prevention

Intrusion prevention devices MUST provide means to stop or attenuate detected attacks, either (when inline) directly or through manipulation of other network devices (e.g., updating a router ACL or firewall ruleset). Such prevention means may include dropping or rejecting suspect packets, throttling bandwidth usage from suspect sources, or rewriting or removing malicious content.

7. IPv6 Device Testing Issues

It is not sufficient for the U.S. Government to publish a specification for IPv6 devices and expect that what is asked for and what is supplied will be fortuitously congruent. Claims of compliance must be demonstrable. Forms of testing that help reconcile claims and functions include conformance and interoperability. In the earlier stages of product evolution, conformance testing to establish a basic level of compliance testing against the specification is needed;, so that later, as the tested, installed base grows, interoperability testing against it should be sufficient. In a companion to this document [2] we will describe a testing program that includes both conformance and interoperability components in which the conformance component can be reduced after the viability of the installed base is established.

8. Conclusion

This document is a technical specification of IPv6 devices intended to benefit U.S. Federal Agencies in their procurement and use. In this version, the specification focuses on the capabilities necessary to establish a core IPv6 network infrastructure, with basic data-plane services, and secure its use. Future versions of this profile are expected to enhance these basic network services (e.g., in the areas of security, quality of service, mobility) and define specific application uses of IPv6.

Appendix A—Bibliography and References

[1] RFC 2460 Internet Protocol Version 6 Specification, IETF Draft Standard, S. Deering and R. Hinden, December 1998.

[2] A U.S. Government Testing Strategy for IPv6, National Institute of Standards and Technology, S. Nightingale and D. Montgomery, NIST SP-??, (forthcoming).

[3] DoD IPv6 Standard profiles for IPv6 Capable Products, Version 1.1, DISR IPv6 Standards Technical Working Group, POC Ralph Liguori, December 2006.

[4] Department of Defense Internet Protocol Version 6 Generic Test Plan, Defense Information Systems Agency, Joint Interoperability Test Command, Fort Huachuca, Arizona, POC Captain Jeremy Duncan, May 2006.

[5] IPv6 Ready Logo Phase-2, http://www.ipv6ready.org/about_phase2_test.html, October 2006.

[6] RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers, IETF Proposed Standard, E. Nordmark and R. Gilligan, October 2005.

[7] RFC 2740 OSPF for IPv6, IETF Proposed Standard, R. Coltun, D. Ferguson and J. Moy. December 1999.

[8] RFC 2453 RIP Version 2, IETF Standard, G. Malkin, November 1998.

[9] RFC 1772 Application of the Border Gateway Protocol in the Internet, IETF Draft Standard, Y. Rekhter and P. Gross, March 1995.

[10] RFC1135 Helminthiasis of the Internet, Informational, J.K. Reynolds, December 1989.

[11] RFC 4301 Security Architecture for the Internet, IETF Proposed Standard, S. Kent and K. Seo, December 2003.

[12] RFC1981 Path MTU Discovery for IPv6, Draft Standard, J. McCann, S. Deering and J. Mogul, August 1996.

[13] RFC 2461 Neighbour Discovery for IPv6, Draft Standard, T>. Narten, E. Nordmark, W. Simpson, December 1998.

[14] RFC 4294 IPv6 Node Requirements, Informational, J. Loughney (ed), April 2006.

[15] RFC 3971 Secure Neighbour Discovery, Proposed Standard, J. Arkko (ed), J. Kempf, B. Zill, P. Nikander, March 2005.

[16] RFC 2462 IPv6 Stateless Address Autoconfiguration, IETF Draft Standard, S. Thomson and T. Narten, December 1998.

[17] RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6), IETF Proposed Standard, R. Droms. Ed, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, July 2003.

[18] RFC 4443 ICMPv6, Draft standard, A. Conta, S. Deering, M. Gupta (ed), March 2006.

[19] RFC 4552 Authentication/Confidentiality for OSPFv3, Proposed Standard, M. Gupta, N. Melam, June 2006.

[20] RFC 4271 A Border Gateway Protocol 4 (BGP-4), Draft Standard, Y. Rekhter (ed), T. Li, S. Hares, January 2006.

[21] RFC 1772 Application of the Border Gateway Protocol in the Internet, Draft Standard, Y. Rekhter, P. Gross, March 1995.

[22] RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing, Proposed Standard, P. Marques, F. Dupont, March 1999.

[23] RFC 2858 Multiprotocol Extensions for BGP-4, Proposed Standard, T. Bates, Y. Rekhter, R. Chandra, D. Katz, June 2000.

[24] RFC 2473 Generic Packet Tunneling, Proposed Standard, Conta A and Deering S, December 1998.

[25] IPv6 Tunnel Broker, Informational, A. Durand, P. Fasano, I. Guardini, D. Lento, January 2001.

[26] IP Version 6 Addressing Architecture, Draft Standard, R. Hinden, S. Deering, February 2006.

[27] FIPS-140-2 Security Requirements for Cryptographic Modules, NIST May 2001.

[28] RFC 4303 IP Encapsulating Security Payload (ESP), Proposed Standard, S. Kent, December 2005.

[29] RFC 4302 IP Authentication Header, Proposed Standard, S. Kent, December 2005.

[30] RFC 2401 Security Architecture for the Internet Protocol, Obsoleted by RFC 4301, S. Kent, R. Atkinson, November 1998.

[31] RFC 2406 IP Encapsulating Security Payload, Obsoleted by RFC 4305, S. Kent, R. Atkinson, November 1998.

[32] RFC 2402 IP Authentication header, Obsoleted by RFC 4302, S. Kent, R. Atkinson, November 1998.

[33] RFC 4306 Internet Key Exchange (IKEv2) Protocol, Proposed Standard, C. Kaufman (ed), December 2005.

[34] RFC 2409 The Internet Key Exchange, Obsoleted by RFC 4306, D. Harkins, D. Carrel, November 1998.

[35] RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP), Obsoleted by RFC 4306, D. Maughan, M. Schertler, M. Schneider, J. Turner, November 1998.

[36] RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP, Obsoleted by RFC 4306, D. Piper, November 1998.

[37] Requirements for an IPsec Certification Management Profile, Internet Draft, C. Bonatti, S. Turner, G. Lebovitz, November 2006.

[38] The IPsec PKI Profile of IKEv1/ISAKMP, IKEv2 and PKIX, Internet Draft, ???, ???

[39] RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH, Proposed Standard, C. madosn, R. Glenn, November 1998.

[40] Using HMAC-SHA-256 with IPsec, Internet Draft, draft-kelly-ipsec-ciph-sha2-00.txt

[41] RFC4106 The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP). J. Viega, D. McGrew. June 2005. PROPOSED STANDARD

[42] RFC4543 The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH. D. McGrew, J. Viega. May 2006. PROPOSED STANDARD

[43] RFC4305 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH). D. Eastlake 3rd. December 2005. PROPOSED STANDARD

[44] RFC4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2). J. Schiller. December 2005. PROPOSED STANDARD

[45] RFC3596 DNS Extensions to Support IP Version 6. S. Thomson, C. Huitema, V. Ksinant, M. Souissi. October 2003. DRAFT STANDARD

[46] RFC3986 Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee, R. Fielding, L. Masinter. January 2005. STANDARD

[47] RFC3493 Basic Socket Interface Extensions for IPv6. R. Gilligan, S. Thomson, J. Bound, J. McCann, W. Stevens. February 2003. INFORMATIONAL

[48] RFC3542 Advanced Sockets Application Program Interface (API) for IPv6. W. Stevens, M. Thomas, E. Nordmark, T. Jinmei. May 2003. INFORMATIONAL

[49] RFC4584 Extension to Sockets API for Mobile IPv6. S. Chakrabarti, E. Nordmark. July 2006. INFORMATIONAL

[50] RFC3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. D. Harrington, R. Presuhn, B. Wijnen. December 2002. STANDARD

[51] RFC3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). U. Blumenthal, B. Wijnen. December 2002. STANDARD

[52] RFC3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6. R. Vida, Ed., L. Costa, Ed.. June 2004. PROPOSED STANDARD

[53] RFC4604 Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast. H. Holbrook, B. Cain, B. Haberman. August 2006. PROPOSED STANDARD

[54] RFC3775 Mobility Support in IPv6. D. Johnson, C. Perkins, J. Arkko. June 2004. PROPOSED STANDARD

[55] RFC3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. J. Arkko, V. Devarapalli, F. Dupont. June 2004. PROPOSED STANDARD

[56] Internet Protocol Version Six Information Assurance Test Plan, Draft Version 0.1, National Security Agency/I151.

[57] The Modular Firewall Certification Criteria, Baseline Module version 4.1, ICSA Labs, January 2005.

[58] NIST SP 800-94 Guide to Intrusion Detection and Prevention (IDP) Systems (DRAFT), K. Kent and P. Mell, U.S. National Institute of Standards and Technology, August 2006.

[59] NIST IR 7007 An Overview of Issues in Testing Intrusion Detection Systems, U.S. National Institute of Standards and Technology, Internal Report, P. Mell and V. Hu, June 2003.

[60] RFC2026 The Internet Standards Process -- Revision 3. S. Bradner. October 1996. BEST CURRENT PRACTICE

[61] RFC2119 Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. March 1997. BEST CURRENT PRACTICE.

[62] Technical and Economic Assessment of Internet Protocol Version 6 (IPv6), IPv6 Task Force, U.S. Department of Commerce, January 2006.

[63] M-05-22 Transition Planning for Internet Protocol Version 6 (IPv6), Office of E-Government and Information Technology, Office of Management and Budget, August 2005.

[64] RFC 3413 SNMP Applications, D. Levi, P. Meyer and B. Stewart, Standard, December 2002.

[65] NIST SP800-TBD Guidelines for the Secure Adoption of IPv6, To Be Published.

[66] RFC 4293 Management Information Base for the Internet Protocol, S. Routhier (ed), Proposed Standard, April 2006.

[67] RFC 4601 Protocol Independent Multicast – Sparse Mode (PIM-SM), B. Fenner, M. Handley, H. Holbrook, I. Kouvelas, Proposed Standard, August 2006.

Appendix B— Terms Used in the Text

Authentication: The process of determining whether some entity is who or what it is declared to be.

Autonomous System: A collection of IP networks and routers under the control of one entity, that presents a common routing policy to the Internet, and as further defined in RFC 1930.

Conformance Testing: Testing to determine if a device satisfies the criteria specified in a controlling document, such as an RFC.

DISR: DoD Information Technology Standards Registry.

Dual-Stack: An Internet Node capable of communicating using either or both of IPv4 and IPv6.

Encryption: The process of translating a *plaintext* message into an encoded *ciphertext* message, usually accomplished using a secret key and a cryptographic cipher.

Exterior Routing: Routing IP packets between Administrative Domains, or Autonomous Systems. Commonly achieved with a protocol such as the Border Gateway Protocol (BGP).

Firewall: A device that acts as a barrier to prevent unauthorized or unwanted communications between sections of a computer network.

Header: That portion at the beginning of a packet containing the information specific to a given protocol.

Host: A computer system attached to the Internet that is a source and recipient of IP packets.

Integrity: Whether the transmitted information is reliable and can be trusted.

Interoperability Testing: Testing to ensure that two or more communications devices can interwork and exchange data.

IPv4 Address: The 32 bit address of a device connected to the Internet.

IPv6 Address: The 128 bit address of a device connected to the Internet, for Nodes that communicate using the IPv6 protocol.

Interior Routing: Routing IP packets within a single Administrative Domain, or Autonomous System. Commonly achieved with a protocol such as OSPF or RIP.

Multicasting: The transmission of an IP packet to a “host group”, a set of zero or more hosts identified by a single IP destination address.

Network Protection Device: A device such as a Firewall or Intrusion Detection device that selectively blocks packet traffic based on configurable and emergent criteria.

Packet Forwarding: The degenerate case of Routing where only a single outgoing link is available to forward the packet (different from the incoming link).

Performance Testing: Testing to evaluate the compliance of a device to specified performance requirements.

PRF: Pseudo Random Function.

RFC: Request for Comments. A publication of the Internet Engineering Task Force (IETF). The basic Internet standards are published as RFCs.

Router: A computer networking device that forwards packets towards a destination using a routing function.

Tunnel: Two endpoints that communicate using an IP packet header or address space, through a network which uses another packet header or address space. This is usually achieved by encapsulating an IP packet (v4 or v6) within another IP packet (v4 or v6).

USG: The United States Government, comprising the Federal Agencies.

Appendix C—Profile Key

THIS KEY TELLS YOU HOW TO READ THE SPREADSHEET IN THE NEXT APPENDIX.

The spreadsheet given in the next Appendix summarizes the recommendations for USG uptake of IPv6 devices. These are grouped by Subprofile, referring to the categories in Section 3 of this document, including Base, Addressing, Routing, IPsec, Link Technology, Transition, Network Management, Multicast, Mobility, Applications, Wireless and Network Protection Devices. Each category identifies the recommendations by Specification, and most of these are RFC numbers. Where a specific detail within a specification is identified, this is listed by its Section number. The Title of each standard is given, or with section numbers, the title of the section or paragraph.

Each standard has a Status and Year of publication. In the case of RFCs the status of the document, including PS (Proposed Standard) and DS (Draft Standard) is determined by its maturity on the standards track. This is specified by RFC 2026 "The *Internet Standards Process – Revision 3*" [60] which itself has a status of "Best Current Practice". The status levels exclusively refer to a specification's position in the standards process. As a practical matter, the currency of an implementation generally lags behind the currency of the standard it is based on. It is not unusual in an evolving technology to find that the most current implementation base refers to a standard that is categorized as obsolete, marked here as OBE. Indeed, this explicitly happens within IPsec, where the RFC 2401 "*Security Architecture*" [30] recommended here as MUST, reflects the current state of operational implementations. RFC 4301 "*Security Architecture*" [11] is designated as SHOULD+ in this profile, indicating that the next round of implementations will migrate to this specification, and agencies are encouraged to acquire it in their next technology refresh cycle. The difference between RFC 2401 and RFC 4301 could metaphorically be described as the difference between the State of the Practice and the State of the Art.

The 'Host' and 'Router' columns refer to whether a provision in a standard is required or optional. The actual set of words used to designate this, including MUST, SHOULD, MAY, are given in RFC 2119 *Key Words for Use in RFCs to Indicate Requirement Levels* [61]. Here we initialize M to mean MUST, S and S+ for SHOULD/SHOULD+, and O for Optional (same as MAY).

The Condition column denotes a constraint which applies under a particular circumstance. For example under the IPsec profile, RFC4109, Section 3, mandates the inclusion of 3DES-CBC within IKEv1, whereas RFC4307, Section 3.1.1 makes 3DES-CBC mandatory within IKEv2. If no condition is given, then the standards designation given under the USGIPv6 device column applies generally to the Node. The complete list of conditions in the USG profile, and their interpretations, is given in the table below.

Condition	Explanation
AH	Applies to the Authentication Header protocol.
APFW	Applies to Application Firewalls.
DHCP	Applies to DHCP servers.
DNS	Applies to DNS servers.

EGW	Applies to Exterior Gateway Routing protocols.
ESP	Applies to the Encapsulating Security Protocol
FW	Applies to Firewalls.
IDS	Applies to Intrusion Detection Systems.
IGW	Applies to Interior Gateway Routing protocols.
IKEv1	Applies to an Internet Key Exchange version 1 implementation.
IKEv2	Applies to an Internet Key Exchange version 2 implementation..
IPsec	Applies wherever IPsec is required.
IPsec-v2	Applies where IPsec version 2 is required.
IPsec-v3	Applies where IPsec version 3 is required.
Link	Applies to Link layer interface
MIP	Applies where the Mobility profile is implemented.
MIP-HA	Under Mobility, this applies only in the case of Home Agents.
MIP-MN	Under mobility, applies only in the case of Mobile Nudes.
NPD	Applies across all Network Protection Devices.
O:1	While each individual standard is optional, at least 1 must be chosen.
SA	Security Association
SOCK	Applies in the case of a Socket implementation.
SSM	Applies in the case of Source Specific Multicast.

Appendix D—The Profile

Group	Spec / Condition	Section	Title / Definition	Status	Year	Condition/ Context	USGIPv6-V1.0		
							Host	Router	NPD
Basic			**IPv6 Basic Protocol Functionality**						
	RFC2460		**IPv6 Specification**	DS	1998		M	M	
		2	IPv6 Packets: send, receive				M	M	
		2	IPv6 packet forwarding					M	
		4	Extension headers: processing				M	M	
		4.3	Hop-by-Hop & unrecognized options				M	M	
		4.5	Fragment headers: send, receive, process				M	M	
		4.6	Destination Options extensions				M	M	
	RFC1981		**Path MTU Discovery M&S**	DS	1996		M	M	
	RFC2675		**IPv6 Jumbograms**	PS	1999		O	O	
	RFC4443		**ICMPv6**	DS	2006		M	M	
	RFC2461		**Neighbour Discovery for IPv6**	DS	1998		M	M	
		4.1, 4.2	Router Discovery				M	M	
		4.6.2	Prefix Discovery				M	M	
		7.2	Address Resolution				M	M	
		7.2.5	NA and NS processing				M	M	
	(RFC2462)	7.2.3	Duplicate Address Detection				M	M	
		7.3	Neighbour Unreachability Detection				M	M	
		8	Redirect functionality				S	M	
	RFC3971		**Secure Neighbour Discovery**	PS	2005		S+	S+	
	RFC2462		**IPv6 Stateless Address Autoconfig**	DS	1998		M	M	
		5.3	Creation of Link Local Addresses				M	M	
	(RFC2461)	5.4	Duplicate Address Detection				M	M	
		5.5	Creation of Global Addresses				M		

Group	Spec / Condition	Section	Title / Definition	Status	Year	Condition/ Context	USGIPv6-V1.0		
							Host	Router	NPD
			Manual Address Config & Ability to Administratively Disable 2462 Creation of Global Addresses				M	M	
	RFC3736		**Stateless DHCP Service for IPv6**	PS	2004		S+		
	RFC3315		**Dynamic Host Config Protocol (DHCPv6)**	PS	2003		S+		
			Ability to Administratively Disable			DHCP	M		
Addr			**Addressing Requirements**						
	RFC4291		**IPv6 Addressing Architecture**	DS	2006		M	M	
	RFC4007		IPv6 Scoped Address Architecture	PS	2005		M	M	
	RFC4193		Unique Local IPv6 Unicast Address	PS	2005		M	M	
	RFC3879		Deprecating Site Local Addresses	PS	2004		M	M	
	RFC3041		Privacy Extensions for IPv6 Stateless Address Autoconfig	PS	2001		S	S	
			Mobile Hosts on Open public networks			MIP	M		
	RFC3484		Default Address Selection for IPv6	PS	2003		M	M	
			Support multiple global addresses				S+	S+	
	RFC3972		Cryptographically Generated Addresses	PS	2005		S+	S+	
Apps			**Application Environment**						
	RFC3986		**URI: Generic Syntax**	S-66	2005		M		
	RFC3596		**DNS Extensions for IPv6**	DS	2003	DNS	M	M	
		2.1	Support of AAAA records			DNS	M	M	
		2.5	Support of ipv6.arpa PTR records			DNS	M	M	
	RFC2671		**Extenstion Mechanisms for DNS (EDNS0)**	PS	199	DNS	M	M	
	RFC3493		**Basic Socket API for IPv6**	INF	2003	SOCK	S+		
	RFC3542		Advanced Socket API for IPv6	INF	2003	SOCK	S		
	RFC4584		Extension to Sockets API for Mobile IPv6	INF	2006	SOCK and MIP	S		
	DNS		***Node uses Domain Name Services***						

Group	Spec / Condition	Section	Title / Definition	Status	Year	Condition/ Context	USGIPv6-V1.0		
							Host	Router	NPD
	SOCK		***Node OS provides Socket API***						
	MIP		***Node implements Mobile IP Subprofile.***						
Routing			**Routing Protocol Requirements**						
			Interior Routing Protocol						
	RFC2740		**OSPF for IPv6**	PS	1999	IGW		M	
	RFC4552		Authentication/Confidentiality for OSPFv3	PS	2006	IGW		S+	
			Exterior Routing Protocol						
	RFC4271		**BGP-4**	DS	2006	EGW		M	
	RFC1772		BGP Application in the Internet	DS	1995	EGW		M	
	RFC2545		BGP Multi-Protocol Extensions for IPv6 IDR	PS	1999	EGW		M	
	RFC2858		BGP Multi-Protocol Extensions	PS	2000	EGW		M	
	IGW		***Node is Interior Gateway Router***						
	EGW		***Node is Interior Gateway Router***						
IPsec			**Security Subprofile**						
			IPsec-v2						
	RFC2401		**Security Architecture for the Internet Protocol**	PS/OBE	1998		M	M	
	RFC2406		ESP	PS/OBE	1998	IPsec-v2	M	M	
		5	Null Authentication			IPsec-v2	M	M	
	RFC2402		AH	PS/OBE	1998	IPsec-v2	O	O	
			IPsec-v3						
	RFC4301		**Security Architecture for the Internet Protocol**	PS	2005		S+	S+	
	RFC4303		ESP	PS	2005	IPsec-v3	M	M	
		5	Null Authentication			IPsec-v3	O	O	
	RFC4302		AH	PS	2005	IPsec-v3	O	O	

Group	Spec / Condition	Section	Title / Definition	Status	Year	Condition/ Context	USGIPv6-V1.0		
							Host	Router	NPD
			IPsec-v2 or IPsec-v3						
	RFC3948		UDP Encapsulation of ESP Packets	PS	2005	IPsec	O	O	
	RFC4305		Cryptographic Algorithms for ESP and AH	PS	2005	IPsec	S	S	
	RFC4308		Cryptographic Suites for IPsec	PS	2005	IPsec	O	O	
		2.1	VPN-A			IPsec	S-	S-	
		2.2	VPN-B			IPsec	S+	S+	
			IKEv1						
	RFC2409		**IKEv1**	PS/OBE	1998		M	M	
	RFC2407		The Internet IP Security DOI for ISAKMP	PS/OBE	1998	IKEv1	M	M	
	RFC2408		ISAKMP	PS/OBE	1998	IKEv1	M	M	
	RFC4109		Algorithms for IKEv1	PS	2005	IKEv1	M	M	
		3	Pre-shared secrets			IKEv1	M	M	
		3	Diffie-Hellman MODP group 2			IKEv1	M	M	
		3	Diffie-Hellman MODP group 14			IKEv1	S	S	
		3	RSA sig auth			IKEv1	S	S	
	RFC3947		NAT-T in IKEv1	PS	2005	IKEv1	O	O	
	RFC4304		ESN Addendum to IPsec DOI for ISAKMP	PS	2005	IKEv1	M	M	
			IKEv2						
	RFC4306		**IKEv2**	PS	2005		S+	S+	
		4	Pre-shared secrets			IKEv2	M	M	
		4	RSA sig auth			IKEv2	M	M	
		4	NAT-T in IKEv2			IKEv2	M	M	
		3.3.3	ESN			IKEv2	M	M	
	RFC4307		Cryptographic Algorithms for IKEv2	PS	2005	IKEv2	M	M	
		3.1.2	Diffie-Hellman MODP group 2			IKEv2	M	M	
		3.1.2	Diffie-Hellman MODP group 14			IKEv2	S+	S+	
			IKEv1 or IKEv2						
	RFC3526		More MODP DH Groups for IKE	PS	2003	IKEv1 | IKEv2	S	S	
	RFC3706		Detecting Dead IKE Peers	PS	2004	IKEv1 | IKEv2	O	O	

Group	Spec / Condition	Section	Title / Definition	Status	Year	Condition/ Context	USGIPv6-V1.0		
							Host	Router	NPD
			Uses of Cryptographic Algorithms						
	RFC2410	18	NULL Encryption	PS	1998		M	M	
	RFC4305	3.1.1	NULL Encryption			ESP	M	M	
	RFC2451		ESP CBC-mode Algorithms	PS	1998		M	M	
		2.6	3DES-CBC			ESP	M	M	
	RFC4305	3.1.1	3DES-CBC			ESP	M	M	
	RFC4109	3	3DES-CBC			IKEv1	M	M	
	RFC4307	3.1.1	3DES-CBC			IKEv2	M	M	
	RFC3602		AES-CBC	PS	2003		M	M	
	RFC4305	3.1.1	AES-CBC with 128 bit keys			ESP	M	M	
	RFC4109	3	AES-CBC with 128 bit keys			IKEv1	M	M	
	RFC4307	3.1.1	AES-CBC with 128 bit keys			IKEv2	M	M	
	RFC3686		AES-CTR	PS	2004		S	S	
	RFC4305	3.1.1	AES-CTR with 128-bit keys			ESP	S	S	
	RFC4309		AES-CCM	PS	2005		O	O	
	RFC4305	3.1.2	AES-CCM with 128 bit keys			ESP	O	O	
	RFC4106		AES-GCM	PS	2005		O	O	
		6	128-bit ICV			ESP	O	O	
		8.1	AES-GCM with 128 bit keys			ESP	O	O	
	RFC4543		AES-GMAC	PS	2006		O	O	
	RFC4543	5.4	AES-GMAC with 128 bit keys			ESP	O	O	
	RFC2404		HMAC-SHA-1-96	PS	1998		M	M	
	RFC4305	3.1.1/3.2	HMAC-SHA-1			ESP/AH	M	M	
	RFC4109	3	HMAC-SHA-1			IKEv1	M	M	
	RFC4307	3.1.1	HMAC-SHA-1			IKEv2	M	M	
	RFC4109	3	HMAC-SHA-1 as a PRF			IKEv1	M	M	

	RFC4307	3.1.4	HMAC-SHA-1 as a PRF			IKEv2	M	M	
Group	**Spec / Condition**	**Section**	**Title / Definition**	**Status**	**Year**	**Condition/ Context**	**USGIPv6-V1.0 Host**	**Router**	**NPD**
	RFC3566		AES-XCBC-MAC-96	PS	2003		S+	S+	
	RFC4305	3.1.1/3.2	AES-XCBC-MAC-96			ESP/AH	S+	S+	
	RFC4434		AES-XCBC-PRF-128	PS	2006		S	S	
	RFC4109	3	AES128-XCBC-PRF			IKEv1	S	S	
	RFC4307	3.1.4+D3	AES128-XCBC-PRF			IKEv2	S+	S+	
	RFC4543		AES-GMAC	PS	2006		O	O	
		5.4	AES-GMAC with 128 bit keys			AH	O	O	
Transition			**IPv6 Transition Mechanisms Subprofile**						
	RFC4213		**Transition Mechanisms for IPv6 Hosts and Routers**	PS	2005		M		
		2	Dual Stack IPv4 and IPv6				M	M	
		3	Configured Tunnels				O	M	
	RFC2473		Generic Packet Tunneling in IPv6	PS	1998		O	M	
	RFC????		**6PE - Connecting IPv6 Islands over IPv4 MPLS**	PS	2006	EGW		O	
Net Mgmt			**Network Management Supbrofile**						
	RFC3411		**SNMP v3 Management Framework**	S62	2002		M	M	
	RFC3412		SNMP Message Process and Dispatch	S62	2002		M	M	
	RFC3413		SNMP Applications	S62	2002		M	M	
		1.2	Command Responder				M	M	
		1.3	Notification Generator				M	M	
	RFC3414		User-based Security Model for SNMPv3	S62	2002		M	M	
	RFC4293		MIB for the IP	PS	2006		M	M	
	RFC4292		MIB for IP Forwarding Table	PS	2006		S+	M	
	RFC4022		MIB for TCP	PS	2006		S+	S+	
	RFC4113		MIB for UDP	PS	2005		S+	S+	
	RFC4087		MIB for IP Tunnels	PS	2005		O	M	

Group	Spec / Condition	Section	Title / Definition	Status	Year	Condition/ Context	USGIPv6-V1.0		
							Host	Router	NPD
Multicast			**Multicast Subprofile**						
	RFC3810		**MLD Version 2 for IPv6**	PS	2004		M	M	
	RFC4604		Using MLDv2 for Source Specifice Multicast (SSM)			SSM	S	S	
Mobile			**Mobility Subprofile**						
	RFC3775		**Mobility Support in IPv6**	PS	2004		S	O	
		8.1	All Nodes as Correspondent Node				M		
		8.2	Route Optimization			MIP	S+		
		8.2	Allow route optimization to be administratively disabled.			MIP	M		
		8.3	All IPv6 Routers					M	
		8.4	Home Agents			MIP-HA		M	
		8.5	Mobile Nodes			MIP-MN	M		
	RFC4283		Mobile Node Identifier option for MIPV6	PS	2005	MIP	S	S	
	RFC3776		Using Ipsec to Protect MIP Signaling Between MNs and HAs	PS	2004	MIP-HA or MIP-MN	M	M	
	MIP		***Node supports Mobility Subprofile***						
	MIP-HA		***MIP AND (is Home Agent)***						
	MIP-MN		***MIP AND (is Mobile Node)***						
QoS			**QoS Profile**						
	RFC2474		Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.	PS	1988			M	
	RFC3260		New Terminology and Clarifications for Diffserv	INF	2002			M	
	RFC3168		The Addition of Explicit Congestion Notification (ECN) to IP	PS	2001			O	

Group	Spec / Condition	Section	Title / Definition	Status	Year	Condition/ Context	USGIPv6-V1.0		
							Host	Router	NPD
Link			**Link Specific Technologies**						
	RFC2464		IPv6 over Ethernet	PS	1998	Link	O:1	O:1	
	RFC2467		IPv6 over FDDI	PS	1998	Link	O:1	O:1	
	RFC2472		IPv6 over PPP	PS	1998	Link	O:1	O:1	
	RFC2491		IPv6 over Non-Broadcast Multiple Access (NBMA) networks	PS	1999	Link	O:1	O:1	
	RFC2492		IPv6 over ATM Networks	PS	1999	Link	O:1	O:1	
	RFC2497		IPv6 over ARCnet	PS	1999	Link	O:1	O:1	
	RFC2590		IPv6 over Frame Relay	PS	1999	Link	O:1	O:1	
	RFC3146		IPv6 over IEEE 1394 Networks	PS	2001	Link	O:1	O:1	
	RFC3572		IPv6 over MAPOS (SONET/SDH)	INF	2003	Link	O:1	O:1	
	RFC4338		Transmission of IPv6 & IPv4 over Fibre Channel	PS	2006	Link	O:1	O:1	
			Header Compression Technologies						
	RFC2507		IP Header Compression	PS	1999		O	O	
	RFC3095		Robust Header Compression (ROHC)	PS	2001		O	O	
	RFC3241		ROHC over PPP	PS	2002		O	O	
	RFC3843		ROHC for IP	PS	2004		O	O	
	RFC4362		ROHC: Link Assisted for IP/UDP/RTP	PS	2006		O	O	
NPD			**Network Protection Subprofile**						
	SP500-26	3.11.2.1	IPv6 connectivity			NPD			M
	SP500-26	3.11.2.2	Dual Stack			NPD			M
	SP500-26	3.11.2.3	Administrative Functionality			NPD			M
	SP500-26	3.11.2.4	Authentication and Authorization			NPD			M
	SP500-26	3.11.2.5	Security of Control and Comms			NPD			M
	SP500-26	3.11.2.6	Persistence			NPD			M
	SP500-26	3.11.2.7	Logging and Alerts			NPD			M
	SP500-26	3.11.2.8	Fragmented Packets Handling			NPD			M
	SP500-26	3.11.2.9	Tunneled Traffic Handling			NPD			M
	SP500-26	3.11.3.1.1	Asymmetrical blocking			FW			M
	SP500-26	3.11.3.1.2	Port/protocol/address blocking			FW			M
	SP500-26	3.11.3.1.3	Performance under load			FW&IDS			M
	SP500-26	3.11.3.2.1	No violation of trust barriers			APFW			M

	SP500-26	3.11.3.2.2	Session Traffic Auth			APFW			M
Group	**Spec / Condition**	**Section**	**Title / Definition**	**Status**	**Year**	**Condition/ Context**	**USGIPv6-V1.0**		
							Host	**Router**	**NPD**
	SP500-26	3.11.3.2.3	Email, File Filtering			APFW			M
	SP500-26	3.11.4.1.1	Known Attack Detection			IDS			M
	SP500-26	3.11.4.1.2	Malformed pkt detection			IDS			M
	SP500-26	3.11.4.1.3	Port scan detection			IDS			M
	SP500-26	3.11.4.1.4	Tunneled traffic detection			IDS			M