



***North American IPv6 Task Force (NAv6TF) Technology Report  
“Firewall Design Center and Architecture Requirements IPv6”***

***Final Version***

***October 2006***

***Jim Bound***

***Chair NAv6TF/CTO IPv6 Forum***

***[Jim.Bound@ipv6forum.com](mailto:Jim.Bound@ipv6forum.com)***

***(See also NAv6TF SME Acknowledgements)***

**Contents**

1. SCOPE ..... 3

2. DESIGN CENTER MODEL..... 3

3. PACKET FILTERING..... 4

4. NON-ENCRYPTED PAYLOADS..... 5

5. ENCRYPTED PAYLOADS ..... 5

6. NEIGHBOR DISCOVERY ..... 5

7. ICMPV6 ..... 6

8. WIRELESS NETWORK INTERFACE ..... 6

9. LINK LAYER ENCRYPTION..... 6

10. MOBILITY..... 7

11. IPV4 ENCAPSULATION AND DECAPSULATION ..... 7

12. SECURITY MANAGEMENT AND CONTAINMENT ..... 8

13. MOONV6 TESTING AND ANALYSIS ..... 8

14. NAV6TF SUBJECT MATTER EXPERT (SME) ACKNOWLEDGEMENTS ..... 8

15. NAV6TF DISCLAIMER..... 9

16. ABOUT NAV6TF..... 9

17. ABOUT THE AUTHOR ..... 9

## 1. Scope

This NAv6TF Technology Report provides a Firewall Design Center and Architecture Requirements IPv6 view of the processing components that should be part of a Firewall deployment model on a network. In this document a model is defined to be a reference implementation view, which can be used to identify a set of architecture requirements. The model will dereference the processing components in the model using an architectural view, rather than an implementation view. Thus, this document does not suggest, nor reference any product requirements. This document also does not suggest or reference any policy requirements, but identifies policy as a processing component within the design center, which can be defined by organizations whom would use this document as a point of reference to develop specific language for their Firewall security. This is a living document that can be updated at any point in time by the NAv6TF.

## 2. Design Center Model

The Design Center Model makes the following network architecture assumptions:

- The network uses IPv6 Global Unicast, Multicast, and Anycast Addresses; therefore there is no processing component for Network Address Translation provided within the model.
- The principles of net centricity are supported and no processing component within the Firewall should prohibit connectivity, interoperability, security, discovery, or end-to-end (see abstract definitions below) as a reference architecture model.
- The network protocol and architecture assumed for network packets in this model is the Internet Protocol (IP).
- The protocol for link layer or physical layer processing when security-in-depth is required for processing before IP layers will have a processing component.
- The model supports that some or all packets entering the Firewall will have their payload encrypted after the IPv6 header and any option headers, using an IPsec header.
- The model does not address the processing of IPv4 packets other than it is assumed there is an IPv4 processing component from current Firewall models and implementations.
- The model does not discuss a processing component for policy or identify the many possible per packet permissions or restrictions that can be implemented by a Firewall. There is a discussion of the possible requirements within the Security Management and Containment processing component.
- The model does not assume any network location, physical layer interface, routing or packet forwarding component, or physical node identity (e.g. Radio/Hand-held-Device, Router, Gateway, Client, Server, Satellite, etc), and this design center is idempotent to all of these attributes as a Firewall reference architectural view.

- The model does not discuss implementation attributes such as performance, scalability, high-availability, data structure abstractions, or other such details imperative for any implementation requirements of a Firewall.

An abstract definition for net centricity is provided below and is assumed in the systems thinking model and requirements for this design center:

- Provides a network view rather than platform view to manage and secure the operations, and solutions used on an Internet network.
- Provides connectivity, interoperability, security, and discovery across an Internet network.
- Provides information across an Internet network expeditiously and in a predictable time frame.
- Provides implementation view and reference model to verify that all functions of a platform or a network of platforms (should the Firewall use a distributed platform model for implementation, support the necessary network software infrastructure components, to permit interoperable communications to share information on a network.

An abstract definition for end-to-end is provided below.

The term end-to-end is typically used in a networking environment to refer to a direct communication between source and destination nodes. End-to-end as an attribute within the IP reference model for a Firewall takes on additional context. One example is as a prefix expression for other communications functions like end-to-end security, mobility, or QoS. End-to-End also implies that any network component or function between two end points is transparent to either end point for transmission or reception of information at the end points. This implies various options for an implementation of end-to-end and to set requirements to support net centricity across the IP layers. Thus, end-to-end is a network attribute that must be considered when constructing an IPv6 Firewall Design Center Model to support an architecture reference model.

The Design Center Model is a set of processing components that exist within the Firewall architectural view. Those processing components are as follows: Packet Filtering, Non-Encrypted Payloads, Encrypted Payloads, Neighbor Discovery, ICMPv6, Wireless Interface, Link Layer Encryption, Mobility,, IPv4 Encapsulation and Decapsulation, and Security Management and Containment. Each of these processing components is discussed below. A future version of this document could consider other processing components for a Firewall such as Quality of Service (QoS) or Network Services Elements.

This version of the document assumes that the reader is familiar with the IPv6, Firewall, IPsec, Mobility, and other Internet Protocol reference model specifications within the IETF [www.ietf.org](http://www.ietf.org), relative to the Firewall Design Model and architecture presented. Please contact the author for questions.

### 3. Packet Filtering

The Packet Filtering processing component is the main entry point to the Firewall Design Center model, and interacts with all other processing components as sub-components. The Packet Filter

---

defines the rule sets to process IP headers and data payloads, identifies packets that may have specific security credentials for entry or exit to the network per user or network as an optimization for filtering, and maintains the state for all processing with other processing components per packet. The Packet Filtering component must have an interface to set the security policy of an organization, and must be configurable dynamically from both a secure user interface and cyberspace network interface as a module within the Firewall Design Center model.

#### **4. Non-Encrypted Payloads**

The Non-Encrypted Payloads processing component applies the rule sets and processing on a per packet basis and returns those results to the Packet Filter. The security policies would be enforced within this processing component such as granting entry or exit to the network to specific IPv6 addresses, protocol headers, packet size, error messages, etc. This processing component for the Firewall Design Center would identify the Packet Filter security policy rules for an IP packet by the organization defining their Firewall permissions and restrictions.

#### **5. Encrypted Payloads**

The Encrypted Payload processing component is called by the Packet Filter when it is identified that the packet contains an IPv6 next header value of IPsec after either the IP header or after an option header below the IP header. Note with IPv6 an option header may exist after the IP header before the IPsec header.

The Encrypted Payload processing component has the choice to apply the security policy rule sets to the IP header and option header (if present) and then to grant or not grant permission within this Firewall architecture model on a per packet basis for this packet to enter or exit the network.

The Encrypted Payload processing component also has the choice after the IP header or option processing (if present) to decrypt or authenticate the IPsec packet and then send that result to the Non-Encrypted processing component for that security policy processing.

The other option for Firewalls for encrypted payloads is to simply not inspect the packet and trust the encryption in process end-to-end.

#### **6. Neighbor Discovery**

The Neighbor Discovery processing component must be able to recognize the IPv6 node discovery messages on the link of the Firewall and respond or not respond as a node on the link according to the security policy defined by the organization deploying the Firewall. For example if the Firewall provides Neighbor Advertisements on the link then all nodes will be able to send packets to the node that contains the Firewall. Because all packets will be routed to the Firewall it is not necessary for the Firewall node to send out Neighbor Advertisements in response to Neighbor Solicitations, but only Router Solicitations, as an example.

It is recommended that the Neighbor Discovery processing component be called by the Packet Filter, thus it is assumed in the Firewall architecture reference model that the Firewall nodes IPv6

Neighbor Discovery implementation can communicate with the Firewall Packet Filter processing component, or a Firewall node would require a custom IPv6 Neighbor Discovery implementation and the risk of breaking compliance to that IPv6 required processing would be high and breaking the principles of net centrality. Thus the Packet Filter processing component should have a means to set the configurable security policy for IPv6 Neighbor Discovery.

## **7. ICMPv6**

The ICMPv6 processing component is required for the Firewall Design Center model to process error messages for an IP packet session initiated on the network. This component would be called by the Non-Encrypted or Encrypted processing component and return the results to the Packet Filter processing component for entry or exit to the network. This processing component should also have cohesive relationship to the Neighbor Discovery processing component. Or the Packet Filter, through an identified security policy, could keep the state of existing IP packet sessions based on source and destination addresses to grant permission or not grant permission based on such an algorithm, depending on the security policy requirements of the network or some identified access control policy for those source and destination addresses. The ICMPv6 processing component would be tightly coupled with the Neighbor Discovery processing component.

## **8. Wireless Network Interface**

The Wireless Network Interface component would be required to be called by the Packet Filtering processing component any time the packet is delivered to the Firewall by an over-the-air interface. The reason for this is that IPv6 permits the use of stateless Autoconfiguration of nodes on a network and packets from such nodes require additional security policy verification that may be required by a fixed network link such as identification as a secure node for entry or exit to the network. The Firewall architecture view presented suggests strongly that Wireless access to the Firewall have a processing component for over-the-air physical links. This permits specific Firewall security policy requirements to be developed by an organization for over-the-air interfaces.

## **9. Link Layer Encryption**

When the physical layer of the network provides Link Layer Encryption that is defined in this document as a security in depth feature. What this means is that the IP packet is not exposed in the clear at all on the link to the point where it reaches the Firewall node. The Firewall node may still have the responsibility to verify that this packet is granted permission to entry or exit to the network. Thus, the Firewall Design Center model architecture view suggests that the Packet Filter processing component should be cognizant of link encryption and support a Link Encryption processing component. This would permit an organization to identify their security policy requirements within the Firewall Design Center model.

## 10. Mobility

Firewalls supporting IPv6 will have to support network node entry and exit that supports seamless mobility on the network. Seamless mobility is defined in this document to be any node that changes their IP source address attachment point on a network because it has changed network location. Thus, there is a need to have a Mobility processing component within the Firewall architecture view.

It is not possible to identify if a node is seamless mobile from the IP header, but only by identifying an IPv6 Mobile Home Agent header extension within the IPv6 packet data payload. Thus, as the Packet Filter processing component parses an IP packet and identifies mobility (as the node may be using a source address that is a care-of-address) there could be additional security policy requirements and Firewall processing for seamless mobility nodes that require additional processing.

If the payload below the IP header and options (if present) in the packet is an IPsec or other encrypted form of packet then unless the packet is decrypted or authenticated identification of seamless mobility for this IP packet is not possible.

The security policy requirements of the Firewall for mobility should be congruent with network operational policy to support seamless mobility of nodes for IPv6, as defined by the organization.

## 11. IPv4 Encapsulation and Decapsulation

An important requirement for the deployment of IPv6 is the set of IPv6 Transition views and mechanisms available to an organization from implementations of IPv6. This Firewall architecture view is for IPv6, assuming a separate set of current processing components exist for IPv4. But, IPv4 packets will be encapsulated within IPv6, and IPv6 packets will be encapsulated within IPv4.

When the IPv4 current Firewall processing detects an encapsulated IPv6 packet and must decapsulate that packet to permit entry or exit to the network, after performing IPv4 Firewall processing in general, should forward the IPv6 packet to the IPv6 Packet Filter processing component who will call the IPv4 Encapsulation and Decapsulation processing component to apply the required security policy for IPv6 packets encapsulated within IPv4.

When the IPv6 Packet Filter processing component identifies an encapsulated IPv4 packet, after completing the required IPv6 processing, should forward that packet to the IPv4 Firewall processing module. If the packet is to enter or exit the network with the IPv6 header then the IPv6 Firewall processing should return the packet back to the IPv6 Packet Filtering processing component.

Identifying this processing component permits an organization to develop the necessary security policy for IPv4 encapsulation and decapsulation required for the Firewall Design Center Model. There could also be the identification of integration with current use of IPv4 Firewall processing to interact with the IPv6 Firewall architecture view presented in the form of call-out modules and components within current IPv4 Firewall processing components installed today.

## 12. Security Management and Containment

The deployment of IPv6 also means the possibility of deployment supporting end-to-end and though that provides a stronger security paradigm than a non-end-to-end security view, it also means that there must be mechanisms to enforce that the end-to-end communications is in fact secure in many cases through the use of a Firewall. The Firewall Design Center model presented in this document views a Firewall as we know them to day to evolve to a network Security Manager for networks that provides the traditional mechanisms of current existing practice, but now supports the pass-through connections of end-to-end encrypted IP packets. In addition the Security Manager should be able to interact with an organizations intrusion detection and prevention security policy and implementation for IPv6.

The Security Management and Containment processing component would be called by the Packet Filter processing component when there was a security breach identified whether real or suspected, to report Firewall activity to a reporting process for network managers or cyberspace security records, interact with any of the organizations intrusion detection systems, to shut down completely all end-to-end connections that may be permitted pass-through by the security policy within the Firewall forcing for example decryption of all packets by the Firewall and applying traditional Firewall processing, and to shut down the Firewall completely not permitting any packets to enter or exit the network.

An organization can use the Security Management and Containment processing component to identify the security policy requirements for the management of the Firewall and the integration with other security systems views required by the organization such as access control, threat levels, trusted computing node requirements, etc.

## 13. Moonv6 Testing and Analysis

The NAv6TF Moonv6 project and pilot network [www.moonv6.org](http://www.moonv6.org) has begun the testing of Firewalls and IPsec within the scope of test scenarios identified as important for the deployment of IPv6. The NAv6TF is willing to share the test cases we use and the general result of those tests, but will not be able to identify actual test results of any of our vendors. If readers of this document wish to learn of these tests and NAv6TF plans please contact [Jim.Bound@ipv6forum.org](mailto:Jim.Bound@ipv6forum.org).

## 14. NAv6TF Subject Matter Expert (SME) Acknowledgements

The author of this document acknowledges direct input to this document and previous technology works within the NAv6TF on security in general from the following NAv6TF SMEs: Merike Kaeo, Yanick Pouffary, Renee Esposito, and Ben Schultz. In addition the author wants to acknowledge NAv6TF previous technology works reviewed when developing ideas for this document from the following NAv6TF SMEs: Dave Green, Joe Klein, Gene Cronk, John Baird, and Mike Warfield. The author was just a catalyst, and SME, for this document to be created encapsulating the inherent knowledge base and discussions from within the NAv6TF SME community.

## 15. NAv6TF Disclaimer

Data and information is provided for informational purposes only, and is not intended for business purposes. Neither IPv6 Forum/NAv6TF or its affiliates nor any of its data or content providers shall be liable for any errors in the content, or for any actions taken in reliance thereon. IPv6 Forum/NAv6TF shall not be liable for any damages or costs of any type arising out of or in any way connected with your use of the content published herein.

## 16. About NAv6TF

The North American IPv6 Task Force (NAv6TF) [www.nav6tf.org](http://www.nav6tf.org) is a sub-chapter of the IPv6 Forum [www.ipv6forum.org](http://www.ipv6forum.org) dedicated to the advancement and propagation of IPv6 (Internet Protocol, version 6) in the North American continent. Comprised of individual members, rather than corporate sponsors, the NAv6TF mission is to provide technical leadership and innovative thought for the successful integration of IPv6 into all facets of networking and telecommunications infrastructure, present and future.

Through its continued facilitation of technical and business case whitepapers, IPv6-centric conferences, IPv6 test and interoperability events, IPv6 deployment readiness guides, and collaboration with IPv6 task forces from around the globe, the NAv6TF will strive to be the guiding force for IPv6 adoption and readiness in the U.S. and Canada.

## 17. About the Author

Jim Bound is the Chief Technology Officer (CTO) IPv6 Forum [www.ipv6forum.org](http://www.ipv6forum.org), Chair NAv6TF [www.nav6tf.org](http://www.nav6tf.org), and Hewlett-Packard Senior Fellow, where he leads a Network Technical Office. Jim has been an engineer and architect within the sphere of networking for 28 years. Jim's Networking SME areas are: IPv6 Transition, Mobility, QoS, Routing, Network Security, Ad Hoc Networks, and Net Centricity. Jim is a consistent contributor and member of the IETF [www.ietf.org](http://www.ietf.org) community, Networking SME and Chair Emeritus within the NCOIC [www.ncoic.org](http://www.ncoic.org) Mobility Working Group, Networking SME to the Internet Society [www.isoc.org](http://www.isoc.org), and is Networking SME who works with Industry, Governments, and Consortia's world wide as required.

Regards

/jim

Email: [Jim.Bound@ipv6forum.com](mailto:Jim.Bound@ipv6forum.com)

