

August 11th, 2008

To whom it may concern,

This document should serve as a statement for compliance for IPv6 in conjunction with TippingPoint's N-Series IPS portfolio. Since the IPS sits inline and is transparent to the network it does not participate in protocol exchanges on the IPv6 segment. It is capable of packet inspection on the inline segment, and it does apply the same intrusion prevention action sets that are supported on our IPv4 capable products. Many of the IPv6 RFC's supported on the IPS are specific to the management port (i.e. RFC 4861 Neighbor Discovery for IPv6)

We would like to formally request to be scheduled for testing.

Description of the product & agreed upon Profile

TippingPoint IPS is a purpose built network element (specialized hardware such as Network Processors and FPGAs) designed to run TippingPoint's proprietary deep packet inspection engine at wire-speed.

TippingPoint IPS ASIC-based Threat Suppression Engine (TSE) is the underlying technology that has revolutionized network protection. Through a combination of pipelined and massively parallel processing hardware, the TSE is able to perform thousands of checks on each packet flow simultaneously. The TSE architecture utilizes custom ASICs, a 20 Gbps backplane and high performance network processors to perform total packet flow inspection at Layers 2-7. Parallel processing ensures that packet flows continue to move through the IPS with a bounded latency of less than 84 microseconds, independent of the number of filters that are applied.

The filters used are not based on another product. The filters used are written with a sophisticated proprietary tool that makes use of protocol decoders and complex pattern matching algorithms. Each filter is capable of deep packet inspection (both anchored and unanchored searches) while tracking the state of the flow.

If any of the filters identifies the packet and its associated flow as negative (malicious traffic or a designated service flow of interest), it is dropped or identified along with any subsequent packets belonging to the same flow. TSE hardware acceleration is a competitive advantage, and is critical for IPS functionality. Traditional software and appliance solutions must check filters serially, consequently sacrificing performance and greatly increasing latency as more filters are activated.

TippingPoint TSE filters covers 3 main area of protection:

- Application Protection
 - Application layer attacks via deep packet inspection, For example, these filters

inspect traffic for RPC, SMB, DNS, telnet, finger, IRC, ICQ, Spyware, LDAP, rservices, SMTP, POP, SNMP, HTTP, FTP, Operating System, IIS, Apache, SQL, fragmentation, numerous worms, numerous viruses, numerous backdoors, DOS, SSH, buffer overflow, port/host scans/sweeps, numerous IP/TCP/UDP/ICMP specific attacks.

- Infrastructure Protection
 - Infrastructure layer protection via deep packet inspection. For example, these filters inspect traffic for invalid IP options, invalid/spoofed source addresses, invalid or malicious IP/TCP/UDP/ICMP/ARP traffic, IOS specific attacks, SYN floods, Established Connection floods, Connections Per Second attacks, statistical traffic anomalies,
- Performance Protection
 - Traffic that is considered misuse and abuse via deep packet inspection. For example, these filters inspect traffic for p2p control/setup/file transfer, P2P tunneling, SuperNode discovery, IM setup/activity/file transfer, and Spyware.
 - Traffic that matches a Traffic Management Filter. For example, an operator creates a TMF to block all FTP coming from a specific source address.

The product should be tested using the Information Assurance profile.

The Security Management System (SMS) is also provided as a separate appliance. The SMS is used to provision the IPS and configure policy for Peer-to-Peer, Exploits, and other categories. It is also used to collect event information from the IPS that are deployed. The SMS is a management application that runs on Linux version 2-6-15 (Fedora Core 5 Dist). SMS represents IPv6 addresses in their native form (i.e. not translated to IPv4) and allows the administrator to define named resources to abstract the IPv6 address into a friendly format (i.e. datacenter, core, Finance subnet, etc...). SMS is an optional component of the TippingPoint solution since the IPSs can be managed locally using a CLI or a web based local management interface called LSM. The SMS version tested is SMS 3.0.

Software Version

The TOS 3.0 will be used for testing on the IPS. SMS version will be 3.0.

Standards Supported and Not Supported

Below is a list of IPv6 RFC's that are either supported on the inspection and management segment

Information Assurance (IA) Device: IPS & IDS LoC Requirements

IPv6 Base

- ❑ RFC 1981 Path MTU Discovery for IPv6
 - (TippingPoint Response – Yes)
- ❑ RFC 2460 Internet Protocol v6 (IPv6) Specification
 - (TippingPoint Response – Yes)
- ❑ RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
 - (TippingPoint Response – Yes)
- ❑ RFC 4861 Neighbor Discovery for IPv6
 - (TippingPoint Response – Yes RFC 2461)
 - RFC 2461 Neighbor Discovery for IPv6 is acceptable until July 2009
- ❑ RFC 4862 IPv6 Stateless Address Autoconfiguration
 - (TippingPoint Response – Yes RFC 2462 with support for DAD and link-local generation only. Static configuration of the global unicast address is currently supported as this is normally required on the element management network)
 - RFC 2462 IPv6 Stateless Address Auto-configuration is acceptable until July 2009
 - Only link-local addresses and Duplicate Address Detection
 - Section 5.5 Disable autoconfiguration
- ❑ RFC 4007 IPv6 Scoped Address Architecture
 - (TippingPoint Response – Yes)
- ❑ RFC 4291 IP Version 6 Addressing Architecture
 - (TippingPoint Response – Yes RFC 3513)
- ❑ RFC 4443 Internet Control Message Protocol (ICMPv6)
 - (TippingPoint Response – Yes RFC 2463)
- ❑ RFC 2710 Multicast Listener Discovery (MLD) for IPv6
 - (TippingPoint Response – Yes)
 - Listener mode

(Required support for at least one of the below)

- ❑ RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
 - (TippingPoint Response – Yes)
- ❑ RFC 2467 Transmission of IPv6 Packets over FDDI Networks
 - (TippingPoint Response – No)
- ❑ RFC 5072 IP Version 6 over PPP
 - (TippingPoint Response – No)
 - RFC 2472 IP Version 6 over PPP is acceptable until July 2009
- ❑ RFC 3572 IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH) (JITC Recommended)
 - (TippingPoint Response – No)

Optional additional connection technologies)

- ❑ RFC 2491 IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks
 - (TippingPoint Response – No)
- ❑ RFC 2492 IPv6 over ATM Networks January 1999
 - (TippingPoint Response – No)
- ❑ RFC 2497 Transmission of IPv6 Packets over ARCnet Networks

- (TippingPoint Response – No)
- ❑ RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification
 - (TippingPoint Response – No)
- ❑ RFC 3146 Transmission of IPv6 over IEEE 1394 Networks
 - (TippingPoint Response – No)
- ❑ RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel
 - (TippingPoint Response – No)

IPv6 Address Autoconfiguration: Can be one of the below options

(TippingPoint Response - Our OS has support for stateless autoconfiguration (RFC 2462) and partial support for DHCPv6 (RFC 3315). However, we currently plan to only allow static configuration except for the link-local IPv6 address since it is deployed on an element management network.)

- ❑ RFC 4862/2462 IPv6 Stateless Address Autoconfiguration
- ❑ RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

IPSec: Conditional for IA Devices if IPSec is a managed service

(TippingPoint Response – No)

- ❑ RFC 4301 Security Architecture for the Internet Protocol
- ❑ (Optional) RFC 4302 IP Authentication Header (AH)
- ❑ RFC 4303 IP Encapsulating Security Payload (ESP)
- ❑ RFC 4835 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
 - RFC 4305 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) is acceptable until July 2009
- ❑ RFC 4308 Cryptographic Suites for IPsec (July 2009 In-Effect Date)
- ❑ RFC 4869 Suite B Cryptographic Suites for IPsec (July 2009 In-Effect Date)

IPSec Fallback: If product cannot comply with 43XX Series of IPSec, then 24XX Series is acceptable

(TippingPoint Response – No)

- ❑ RFC 2401 Security Architecture for the Internet Protocol
- ❑ (Optional) RFC 2402 IP Authentication Header (AH)
- ❑ RFC 2406 IP Encapsulating Security Payload (ESP)

IKEv1

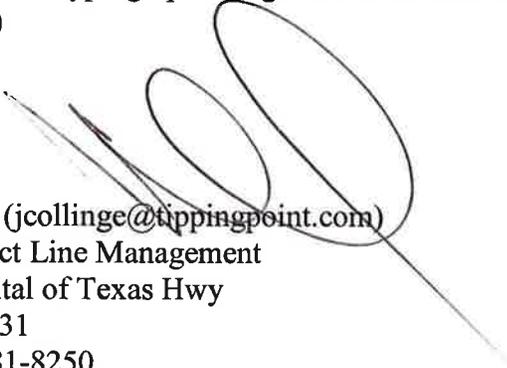
(TippingPoint Response – No)

- ❑ RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- ❑ RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- ❑ RFC 2409 The Internet Key Exchange (IKE)
- ❑ RFC 4109 Algorithms for Internet Key Exchange Version 1 (IKEv1)

IKEv2: If product supports IKEv2, it must also support IKEv1 for backwards compatibility. In effect date for IKEv2 support is July 2010

(TippingPoint Response – No)

- ❑ RFC 4306 Internet Key Exchange (IKEv2) Protocol
- ❑ RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)



James Collinge (jcollinge@tippingpoint.com)
Director, Product Line Management
7501-B N. Capital of Texas Hwy
Austin, TX 78731
Office: (512) 681-8250
Fax: (512) 681-8299
TippingPoint