TippingPoint Intrusion Prevention Systems

DATASHEET

The Platform For Unrivaled Security and Performance

Protection has never been more powerful. TippingPoint is the industry's leading Intrusion Prevention System (IPS), unrivaled in security, performance, high availability and ease-of-use. As the only Intrusion Prevention System to receive the NSS Gold Award and to be certified as the first multi-gigabit Network IPS by ICSA Labs, among many other awards, TippingPoint is the defining benchmark for network-based intrusion prevention.

Proactive Network Security

Intrusion Detection Systems, by definition, only detect and do not block unwanted traffic. The TippingPoint IPS operates in-line in the network, blocking malicious and unwanted traffic, while allowing good traffic to pass unimpeded. In fact, TippingPoint optimizes the performance of good traffic by continually cleansing the network and prioritizing applications that are mission critical. TippingPoint's high performance and extraordinary intrusion prevention accuracy have redefined network security, and fundamentally changed the way people protect their organization.

No longer is it necessary to clean up after cyber attacks have compromised your servers and workstations. No more ad-hoc and emergency patching. No more out of control, rogue applications like Peer-to-Peer and Instant Messaging running rampant throughout the network. Denial-of-Service attacks that choke Internet connections or crash mission critical applications are a thing of the past.

TippingPoint solutions continuously decrease IT security cost by eliminating ad-hoc patching and alert response, and continuously increase IT productivity and profitability through bandwidth savings and protection of critical applications.

Unparalleled Performance

TippingPoint has the best performing products in the industry. Blocking cyber-attacks at multi-gigabit speeds with extremely low latency requires purpose-built

> "TippingPoint is a visionary in the intrusion prevention market."
>
> *Eric Ogren, Yankee Group*

hardware, and only TippingPoint has taken such a revolutionary architectural approach needed for true Intrusion Prevention. Traditional software and appliance solutions operate on general-purpose hardware and processors and are simply unable to perform without degrading network performance. Through rigorous third-party testing, TippingPoint has demonstrated Intrusion Prevention at multi-gigabit speeds, with extraordinary attack prevention accuracy. TippingPoint is proven in the industry as the most secure, highest performing platform for Intrusion Prevention.

> "The TippingPoint IPS is the best security solution I have come across. Its performance has been nothing short of amazing. The solution more than paid for itself within the first year. It's simple to deploy and manage because it can interoperate with all kinds of hardware."
>
> *Richard Cross, Information Security Officer*
> *Toyota Motor Europe*

Switch-Like Performance
- Multi-Gigabit Per Second Attack Filtering
  - TippingPoint X505 (50 Mbps IPS/VPN/FW)
  - TippingPoint X506 (50 Mbps IPS/100 Mbps VPN/100 Mbps FW)
  - TippingPoint 50 (50 Mbps)
  - TippingPoint 200 (200 Mbps)
  - TippingPoint 200E (200 Mbps)
  - TippingPoint 600E (600 Mbps)
  - TippingPoint 1200E (1.2 Gbps)
  - TippingPoint 2400E (2.0 Gbps)
  - TippingPoint 5000E (5.0 Gbps)
- Latency < 84 µsec
- Real World TCP/UDP Traffic Mix
- Two Million+ Simultaneous Sessions
  - TCP/UDP/ICMP
- 1,000,000+ Connections Per Second

Comprehensive Threat Protection
- VoIP
- OS Vulnerabilities
- Spyware
- Quarantine
- Phishing
- DDoS
- Viruses
- Worms
- P2P
- ZDI

Client and Server Protection
- Prevent Attacks on Vulnerable Applications and Operating Systems
- Eliminate Costly Ad-Hoc Patching
- Multiple Filtering Methods

Network Infrastructure Protection
- Protect Cisco IOS, DNS and Other Infrastructure
- Protect Against Traffic Anomaly, DDoS, SYN Floods, Process Table Floods
- Access Control Lists

Traffic Normalization
- Increase Network Bandwidth and Router Performance
- Normalize Invalid Network Traffic
- Optimize Network Performance

Application Performance Protection
- Increase Bandwidth and Server Capacity
- Rate-Limit or Block Unwanted Traffic
  - Peer-to-Peer/Instant Messaging
- Guarantee Bandwidth for Critical Applications

Digital Vaccine® Real-Time Inoculation
- World-Renowned Security Research Team
- Protection Against Zero-Day Attacks
- Automatic Distribution of Latest Filters

Security Management System
- Manage Multiple TippingPoint Systems
- At-A-Glance Dashboard
- Automatic Reporting
- Device Configuration and Monitoring
- Advanced Policy Definition and Forensic Analysis

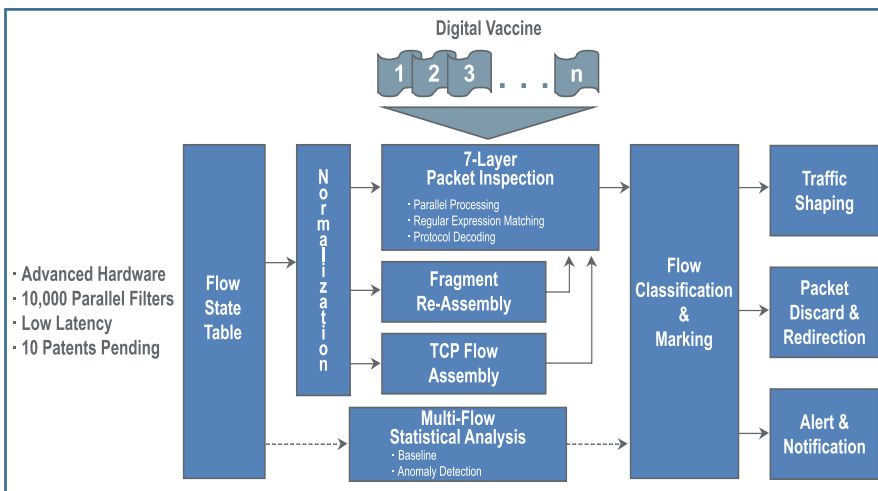### High Availability and Stateful Network Redundancy
- Dual-Power Supplies
- Layer 2 Fallback
- Active-Active or Active-Passive Stateful Redundancy (IPS and SMS)
- Zero Power High Availability

Threat Suppression Engine

TippingPoint's ASIC-based Threat Suppression Engine (TSE) is the underlying technology that has revolutionized network protection. Through a combination of pipelined and

Digital Vaccine

- Advanced Hardware
- 10,000 Parallel Filters
- Low Latency
- 10 Patents Pending

Flow State Table

Normalization

7-Layer Packet Inspection
- Parallel Processing
- Regular Expression Matching
- Protocol Decoding

Fragment Re-Assembly

TCP Flow Assembly

Multi-Flow Statistical Analysis
- Baseline
- Anomaly Detection

Flow Classification & Marking

Traffic Shaping

Packet Discard & Redirection

Alert & Notification

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 150 microseconds, independent of the number of filters that are applied.
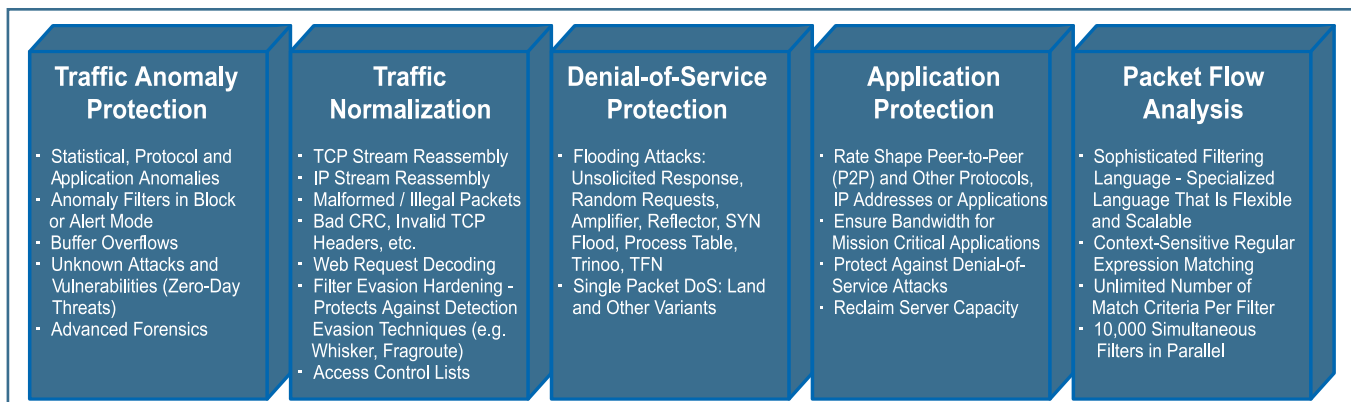
The TSE architecture also enables traffic classification and rate shaping. Sophisticated algorithms baseline "normal" traffic allowing for automatic thresholds and throttling so that mission critical applications are given a higher priority on the network.

Complete Security

Built on outstanding performance, TippingPoint delivers uncompromising security. TippingPoint performs comprehensive total packet flow inspection through Layer 7 to continually cleanse Internet and Intranet traffic and accurately eradicate attacks (worms, viruses, Trojans, blended threats, Phishing, Spyware, VoIP Threats, DoS, DDoS, Backdoors, Walk-in Worms*, Bandwidth Hijacking) before damage occurs. TippingPoint protects network infrastructure by blocking attacks against routers, switches, DNS and other infrastructure equipment. Through TippingPoint's Zero-Day Initiative (ZDI), customers are protected against new threats before vulnerabilities are disclosed to the public.

*Walk-in Worm: a Worm that spreads from within an organization by "walking in" on a laptop computer.

TippingPoint provides statistical, protocol and application anomaly protection to protect against traffic surges, buffer overflows, unknown attacks and unknown vulnerabilities. TippingPoint delivers traffic normalization to eliminate malformed or illegal packets, and performs TCP reassembly and IP defragmentation, thus increasing network bandwidth and protecting against evasion techniques. TippingPoint can also act as an access control firewall that can replace CPU intensive router and switch access control lists. Additionally, by rate limiting or blocking unwanted traffic, TippingPoint conserves bandwidth and server capacity to provide complete application protection. A comprehensive list of protection mechanisms is detailed in the figure below.

TippingPoint's revolutionary Quarantine protection offers an radical new approach to LAN security. By extending the protective power of the IPS down to every endpoint, TippingPoint Quarantine blocks insider

Traffic Anomaly Protection	Traffic Normalization	Denial-of-Service Protection	Application Protection	Packet Flow Analysis
- Statistical, Protocol and Application Anomalies - Anomaly Filters in Block or Alert Mode - Buffer Overflows - Unknown Attacks and Vulnerabilities (Zero-Day Threats) - Advanced Forensics	- TCP Stream Reassembly - IP Stream Reassembly - Malformed / Illegal Packets - Bad CRC, Invalid TCP Headers, etc. - Web Request Decoding - Filter Evasion Hardening - Protects Against Detection Evasion Techniques (e.g. Whisker, Fragroute) - Access Control Lists	- Flooding Attacks: Unsolicited Response, Random Requests, Amplifier, Reflector, SYN Flood, Process Table, Trinoo, TFN - Single Packet DoS: Land and Other Variants	- Rate Shape Peer-to-Peer (P2P) and Other Protocols, IP Addresses or Applications - Ensure Bandwidth for Mission Critical Applications - Protect Against Denial-of-Service Attacks - Reclaim Server Capacity	- Sophisticated Filtering Language - Specialized Language That Is Flexible and Scalable - Context-Sensitive Regular Expression Matching - Unlimited Number of Match Criteria Per Filter - 10,000 Simultaneous Filters in Parallel

threats and walk-in worms, then communicates with switching infrastructures to isolate offending endpoints with remediation VLANs that prevent network infection. Unlike cumbersome client-based solutions which merely check for endpoint configurations on Windows PCs, TippingPoint Quarantine Protection offers an agentless solution that constantly monitors all endpoint activities, instantly eliminating LAN-based threats automatically.

X-Series Integrated Security Platform

The TippingPoint X-Series product line combines a full enterprise-class IPS with VPN, firewall, Web content filtering, and advanced routing for a complete perimeter security appliance for remote branch offices and SMB networks. Specially crafted inspection modules allow for inspection of encrypted VPN traffic, and can even prioritize the applications within a VPN tunnel. This powerful QoS mechanism allows remote sites to leverage a centrally located VoIP deployment across a VPN tunnel without degrading VoIP quality.

World-Class Vulnerability Analysis

The security team at TippingPoint leads the industry in vulnerability analysis. TippingPoint is the primary author of the SANS @RISK newsletter, containing the latest information on new and existing network security vulnerabilities, with a subscriber base of nearly 300,000 network security professionals worldwide. Coordinated by the SANS Institute and delivered every Thursday, the SANS @RISK newsletter summarizes newly discovered vulnerabilities, details their impact and informs of actions large organizations have taken to protect their users. The SANS @RISK newsletter is available for free at http://www.sans.org/newsletters/risk/.

Digital Vaccine® Real-Time Inoculation

Ensuring total security, TippingPoint offers ongoing threat prevention against emerging vulnerabilities. In providing the vulnerability analysis for SANS every week, the TippingPoint security team simultaneously develops new attack filters to address the vulnerabilities and incorporates these filters into Digital Vaccines. Vaccines are created not only to address specific exploits, but also potential attack permutations, protecting customers from Zero-Day threats. Digital Vaccines are delivered to customers every week, or immediately when critical vulnerabilities emerge, and can be deployed automatically with no user interaction required.
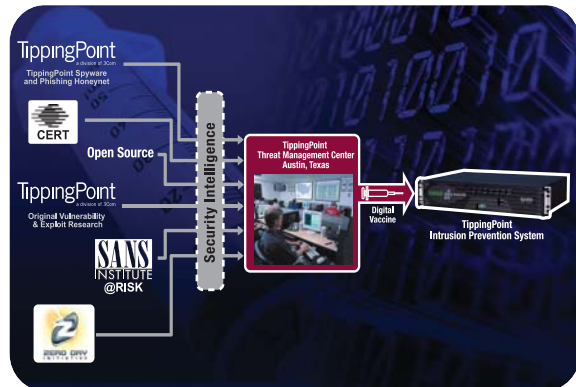
This unique and valuable service allows customers to restore efficiency to the security patching process. The burden of emergency and ad-hoc vulnerability patching is alleviated, as IT personnel can apply patches only as required and at regularly scheduled times.

Enterprise Management

TippingPoint delivers best-of-breed management capabilities that are simple to use and extremely powerful. The TippingPoint Security Management System (SMS) is a hardened appliance that provides global vision and control for multiple TippingPoint systems. The SMS is responsible for discovering, monitoring, configuring, diagnosing and reporting for multiple TippingPoint systems. The TippingPoint SMS is a rack mountable appliance that features a state-of-the-art secure Java client interface that enables "big picture" analysis with trending reports, correlation and real-time graphs on traffic statistics, filtered attacks, network hosts and services, and IPS inventory and health.
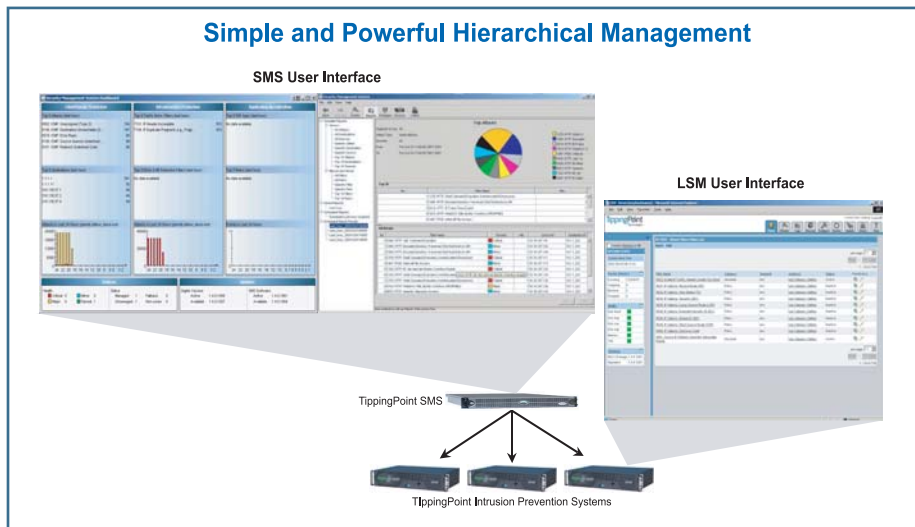
Because the TippingPoint SMS provides a scalable, policy-based operational model, it enables straightforward management of large-scale IPS deployments. A typical network-wide TippingPoint deployment consists of SMS Clients (secure Java), a centralized Security Management System (SMS), and multiple TippingPoint systems.
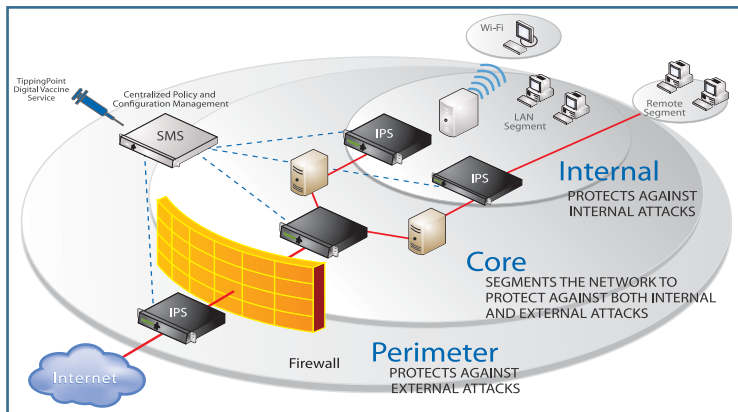
A very effective component of TippingPoint's SMS is the SMS dashboard. The dashboard provides at-a-glance monitors and launch capabilities into targeted

> "The management system is powerful and flexible, yet easy and intuitive to use. The profile editor is the best we have seen on any IPS/IDS device."
>
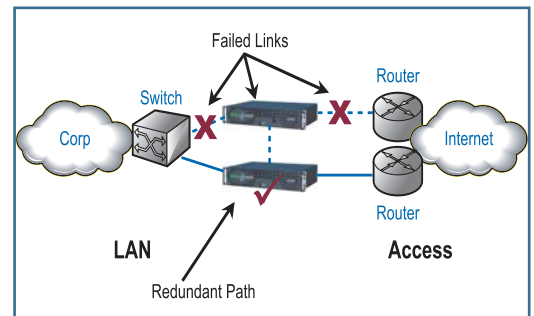> *Bob Walder, President*
> *The NSS Group*

Simple and Powerful Hierarchical Management

Internal
PROTECTS AGAINST
INTERNAL ATTACKS

Core
SEGMENTS THE NETWORK TO
PROTECT AGAINST BOTH INTERNAL
AND EXTERNAL ATTACKS

Perimeter
PROTECTS AGAINST
EXTERNAL ATTACKS

"It gave us one less thing to worry about. It is truly a turnkey solution. We have the IPS set to automatically download the Digital Vaccine updates with the recommended settings to block attacks. Now, when a new threat terrorizes others in the early morning hours, we rest easy knowing that TippingPoint's IPS has a Digital Vaccine protecting us at all times."

Jonas Hirshfield
Director of Infrastructure Development
Blackboard

Intrinsic High Availability

management applications. The SMS dashboard displays an overview of current performance for all TippingPoint systems in the network, including notifications of updates and potential problems that may need attention.

Additionally, every IPS is shipped with an embedded Local Security Manager (LSM) and Command Line Interface (CLI). The LSM is a Web GUI management application that provides administration, configuration and reporting capabilities in an easy-to-use, secure Web interface.

Easy to Deploy
The TippingPoint IPS is designed for network transparency:

• The TippingPoint IPS is deployed seamlessly into the network with no IP address or MAC address, and immediately begins filtering out malicious and unwanted traffic.

• The extremely high speed and low latency capabilities of the IPS enable deployment at the network edge or core, protecting from external as well as internal threats. TippingPoint enables traffic shaping to support critical applications and infrastructure, and also provides attack isolation and network discovery of vulnerable devices.

• State of the art "Recommended Filter" settings allow instant deployment out-of-the-box with no tuning required.

High Availability
TippingPoint Intrusion Prevention Systems are unparalleled in High Availability. TippingPoint's IPS is designed to guarantee that network traffic always flows at wire speed in the event of network error, internal device error or even complete power loss. Two complementary High Availability modes of operation - Intrinsic High Availability and Stateful Network Redundancy - ensure

maximum uptime and availability for both the IPS devices and the SMS management devices.

Several built-in features of the IPS enable Intrinsic High Availability. First, all TippingPoint IPS devices have dual hot swappable power supplies. Secondly, watchdog timers continuously monitor the security and management engines. If an internal error is detected, TippingPoint can automatically or manually fall back to a simple Layer 2 device, configurable per segment. Additionally, TippingPoint offers a Zero Power High Availability (ZPHA) option for copper interfaces. In the event of full data center power loss, the interfaces can switch over to the ZPHA external relay to pass all traffic.

Stateful Network Redundancy
Two TippingPoint IPS's can be provisioned to operate in a transparent High Availability mode. Because the IPS is a "bump in the wire," does not have an IP address and does not participate in routing protocols, pairs of

TippingPoint systems can be deployed in existing high availability network designs without changing the network configuration. High availability routing protocols such as Virtual Router Redundancy Protocol (VRRP), Open Shortest Path First (OSPF), and Cisco Hot Standby Router Protocol (HSRP) are passed transparently by the TippingPoint IPS and therefore operate equally well with a TippingPoint IPS in-line. The pair of TippingPoint systems can be configured in either Active-Active or Active-Passive modes to appropriately share state information so that attack protection is fully maintained during and after network outages.

TippingPoint
a division of 3Com