TippingPoint_Intrusion_Prevention_System_(IPS)

IPS-Secured_Networks

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.

IPS

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.

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

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

"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

Unparalleled_Performance

Blocking cyber-attacks at multi-gigabit speeds with extremely low latency requires purpose-built hardware. 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.

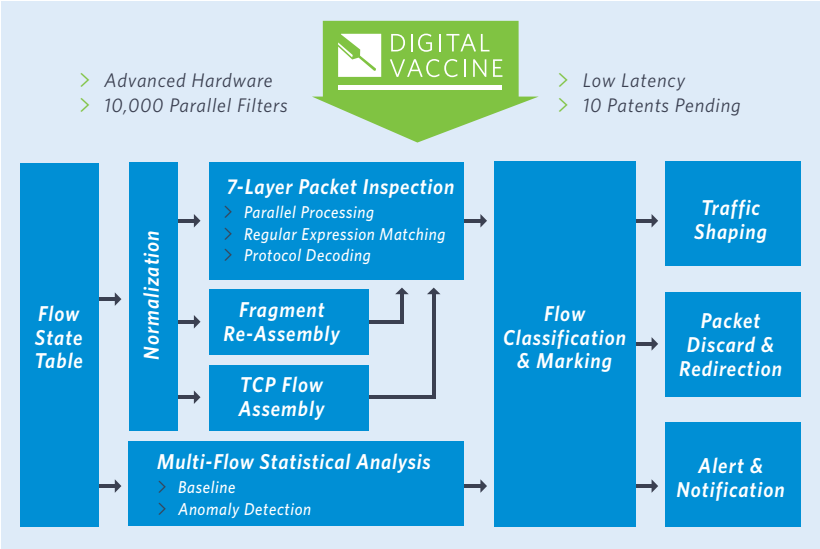
Threat_Suppression_Engine

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

TippingPoint_Intrusion_Prevention_System_(IPS)

IPS-Secured_Networks

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 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.

"The way we know the filters actually improve security is that we have a TippingPoint IPS protecting our customer facing Web applications. We see Slammer, port 445 and SQL Server exploits, and exploits that normally come through on port 80. Some of these exploits would have made it through the firewall and infected the production systems. Because of our TippingPoint IPS deployment, the servers were never touched."

Scott Davis
Enterprise Security Network Manager
T. Rowe Price

Comprehensive_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.

TippingPoint provides statistical, protocol and application anomaly protection to protect against traffic surges, buffer overflows, unknown attacks and unknown vulnerabilities. The TippingPoint IPS 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.

TippingPoint's Quarantine protection offers a radical new approach to LAN security. By extending the protective power of the IPS down to every endpoint, TippingPoint Quarantine blocks insider threats and walk-in worms, and 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's Quarantine Protection offers an agentless solution that constantly monitors all endpoint activities, instantly eliminating LAN-based threats automatically.

World-Class_Vulnerability_Analysis_and_Research

TippingPoint's DVLabs team is a premier security research organization for vulnerability analysis and discovery. Recognized in 2007 as the fastest growing discoverer of new vulnerabilities and the leader in the discovery of high-severity and Microsoft vulnerabilities by Frost & Sullivan[1], the team consists of industry recognized security researchers that apply their cutting-edge engineering, reverse engineering and analysis talents in their daily operations. The by-product of these efforts fuels the creation of vulnerability filters that are automatically delivered to TippingPoint customers' intrusion prevention systems through the Digital Vaccine® service. The DVLabs Web site (dvlabs.tippingpoint.com) serves as a portal into the research laboratories headquartered in Austin, Texas. The portal includes

upcoming and published advisories as well as blogs, RSS feeds and other security resources.

TippingPoint is also the primary author of the SANS @ RISK newsletter, which contains the latest information on new and existing network security vulnerabilities. Coordinated by The SANS Institute, 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

TippingPoint offers ongoing threat prevention against emerging vulnerabilities through the Digital Vaccine service. Digital 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 twice a 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.

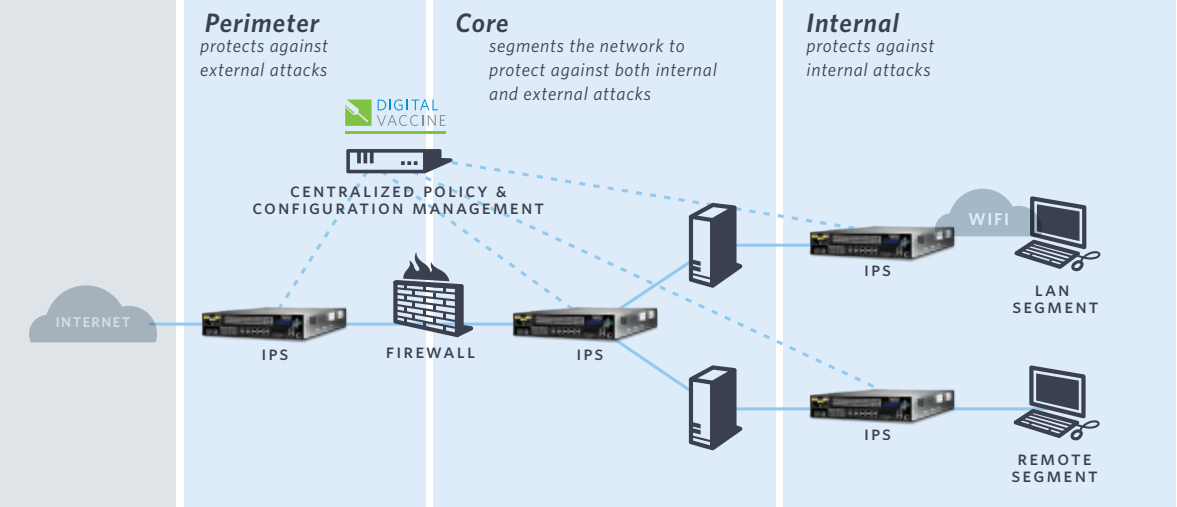
Centralized_Enterprise_Management

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 the TippingPoint IPS. 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, as well as 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 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.

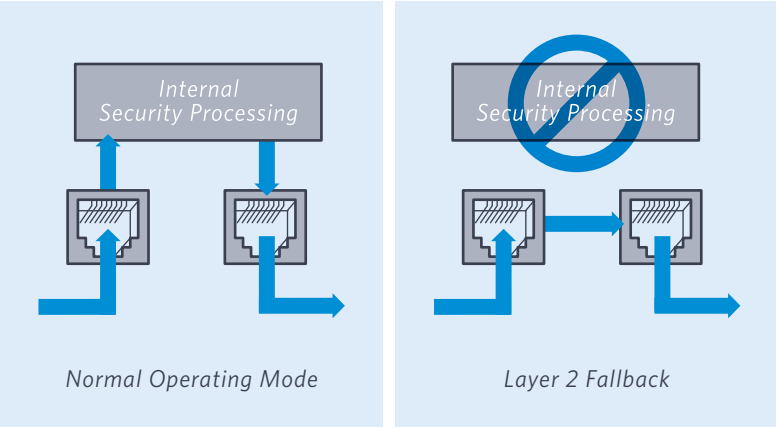
Every IPS also has an embedded Local Security Manager (LSM) and Command Line Interface (CLI). The LSM is a Web GUI management application



that provides administration, configuration and reporting capabilities in an easy-to-use, secure Web interface.

"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



Easy_Deployment

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 ensure 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.

ROI_for_Intrusion_Prevention

TippingPoint's Intrusion Prevention System provides continuous benefits in any network environment:

Automatically Block Attacks – By blocking attacks and allowing IT staff to test security patches before deployment, system uptime is ensured

Eliminate Emergency Patching – TippingPoint's Digital Vaccine filters alleviate the need for ad-hoc and emergency patching.

TippingPoint_Intrusion_Prevention_System_(IPS)

IPS-Secured_Networks

"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

Protect Unpatched Systems – Most environments cannot control all end user desktops. Some environments such as service providers or universities have very little control. TippingPoint provides network segmentation to stop the spread of malicious traffic from infected users, while notifying the administrator where attacks are originating.

Reclaim Bandwidth – Blocking malicious traffic and rate shaping rogue applications can increase bandwidth availability by 40-70 percent.

Accelerate Network Performance – By continually cleansing the network of malicious and unwanted traffic, network performance is accelerated for mission critical applications.

Even one of these components can offer 100% return on investment. When combined, these ROI elements provide a powerful business case for the TippingPoint Intrusion Prevention System.

[1] Frost and Sullivan press release. "Frost & Sullivan Recognizes TippingPoint's Valuable Contribution to Vulnerability Research." 11 May 2007 Frost & Sullivan. http://www.frost.com/prod/servlet/press-release.pag?docid=98552761&ctxst=FcmCtx1&ctxht=FcmCtx2&ctxhl=FcmCtx3&ctxixpLink=FcmCtx3&ctxixpLabel=FcmCtx4

Features and Benefits

Switch-Like Performance
- Multi-Gigabit Per Second Attack Filtering
- Latency < 84 µsec
- Real World TCP/UDP Traffic Mix
- Two Million+ Simultaneous Sessions – TCP/UDP/ICMP
- 350,000+ Connections Per Second

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

Client and Server Protection
- Prevent Attacks on Vulnerable Applications & 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 (P2P/IM)
- 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 & SMS)
- Zero Power High Availability

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS
European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450
Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999

Copyright © 3Com Corporation. TippingPoint and Digital Vaccine are registered trademarks of 3Com Corporation or its subsidiaries. All other company and product names may be trademarks of their respective holders. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors which may arise. Specifications and other information in this document may be subject to change without notice. 400917-010 12/09

TippingPoint
www.tippingpoint.com