

TippingPoint_10_Intrusion_Prevention_System

Intrusion_Prevention_for_Remote_Offices



Protecting today's complex networks from malicious threats and targeted attacks requires more than simply securing the WAN perimeter and core network. Remote offices are often the "weak link" in network security. TippingPoint provides smaller form factor Intrusion Prevention Systems (IPS) to extend its powerful security solutions to these remote networks. The TippingPoint 10 (TP 10) IPS operates in-line, blocking malicious and unwanted traffic, while allowing good traffic to pass unimpeded. TippingPoint is the industry's leading IPS, unrivaled in security, reliability, performance and ease of use.



"TippingPoint not only offers powerful security, it delivers the means to easily manage multiple remote systems, ensuring their ongoing efficacy and greatly reducing ownership costs. We eliminate the expense of having onsite personnel to fine-tune the devices or load the latest filters."

K. Kim

Telecom Director

Hawaii Department of
Education

Unparalleled Reliability and Performance

The TP 10 is optimized for sub 20 Mbps link speeds that are predominant in business DSL and Metro Ethernet services. The solution can be deployed in front or behind the remote location's router/firewall immediately protecting the network and applications from inbound threats. It has integrated Zero Power High Availability capabilities, so a simple power failure does not cause network outages. The TP 10 is designed to preserve availability, performance and security on remote office networks.

Industry Leading Security Coverage

The TP 10 receives automated security updates from the TippingPoint Digital Vaccine® Service ensuring evergreen protection against emerging threats. 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 regularly and can be deployed automatically with no local user interaction.

Like all of TippingPoint's industry leading IPS solutions, the TP 10 provides comprehensive flow

inspection through Layer 7 to cleanse Internet and Intranet traffic and eradicate attacks before damage occurs. In fact, TippingPoint IPS solutions are known for their pinpoint accuracy in blocking attacks meaning no legitimate traffic is blocked.

TippingPoint IPS solutions protect a broad range of network infrastructure including routers, switches, DNS and e-mail servers, Web and enterprise application servers, and much more. And TippingPoint provides the best vulnerability coverage in the IPS industry including protection of Cisco, Microsoft, Sun O/S, EMC, SAP, CA, Mozilla, Novell, Oracle, Apple O/S, Citrix O/S, Adobe, IBM, and many other enterprise application vulnerabilities.

Reduced Overall Costs and Complexity

TippingPoint Intrusion Prevention Systems block attacks and allow IT staff to spend time on strategic projects instead of reacting to remote security breaches on hosts and workstations. The TP 10 provides network segmentation to stop the spread of malicious traffic from infected users, while notifying the administrator where attacks are originating.

TippingPoint_10_Intrusion_Prevention_System

Intrusion_Prevention_for_Remote_Offices

The TP 10 also provides traffic management to stop bandwidth hogging applications like Peer-to-Peer and Instant Messaging. In short, TippingPoint solutions decrease IT security cost by eliminating ad-hoc patching and alert response, while simultaneously increasing IT productivity through bandwidth savings and protection of critical applications.

Easy_to_Manage

The TP 10 is easily installed in remote office networks by local personnel in minutes and immediately begins filtering out malicious and unwanted traffic. The IPS is deployed seamlessly with no IP or MAC address configurations. All systems ship with “Recommended Settings” meaning no “out-of-the-box” configurations are required locally.

TippingPoint 10 Technical Specifications		
Performance	Inspection Throughput	> 20 megabits per second
	Typical Latency	> < 500 microseconds
	Total Sessions	> 250,000
	Connections / Second	> 3,600
Hardware Specifications	Scalability	> 4x10/100/1000BaseT (2 segments)
	Power – AC	> AC power adapter > Power Adapter: 110-240 VAC universal, 50-60 Hz, 1.8A > Power Output: 12 VDC , 5A
	Power – Optional DC	> Not available
	Physical Dimensions	> Height (in): 2.01 in. Height (cm): 5.1 cm > Width (in): 10.63 in Width (cm): 27 cm > Depth (in): 7.32 in Depth (cm): 18.6 cm
	Weight	> Weight (lb): 5.1 lbs > Weight (kg): 2.3 kg
Environmental	Temperature	> Operating: 0° to 40°C (32° to 104°F) > Storage: -25° to 70°C (-25° to 158°F)
	Relative Humidity	> Operating: 0% to 95% (non-condensing) > Storage: 5% to 95% (non-condensing)
Certifications	Safety	> UL60950-1 Standard for Safety of Information Technology Equipment > CSA 22.2- 60950-1 > EN60825: Safety of Laser Products > EN60950 -1 > IEC 60950 -1 > ROHS Compliance
	Immunity	> EN-61000-3-2: Harmonic Emissions > EN-61000-3-3: Voltage Fluctuations and Flicker > EN-61000-4-2: ESD Immunity > EN-61000-4-3: Radiated Immunity > EN-61000-4-4 EFT: Burst Transients > EN-61000-4-5: Surge Protection > EN-61000-4-6: Injected RF > EN-61000-4-11: Dips and Sags
	Emissions	> FCC Class B: Regulations for Radio Frequency Devices for Electromagnetic Compliance > ICES -003, Class B > EN 55022 Class B > VCCI Class B > AS/NZS-3548 Class B
Warranty	The standard warranty is for a 12-month period. Phone support and training courses are available from TippingPoint.	

TippingPoint_10_Intrusion_Prevention_System

Intrusion_Prevention_for_Remote_Offices

Once installed, the TP 10 is easily managed with the TippingPoint Security Management System (SMS) that discovers, monitors, configures, diagnoses and reports on multiple IPS systems. Every TP 10 has an embedded Local Security Manager (LSM) and Command Line Interface (CLI) that provide local administration, configuration and reporting in an easy-to-use Web interface.

threat landscape, and increasing regulatory requirements. In the face of these stringent security policies and other regulatory demands, TippingPoint IPS provides automated enforcement of network security policies. Reporting from the IPS and SMS show internal and external auditors the network is protected from the latest threats.

Demonstrate_Best_Practices_for_Compliance

TippingPoint IPS solutions can be a critical component in any IT compliance program. Today's organizations have to deal with increasingly stringent security policies in the face of an ever changing

Key IPS Features

High Availability and Stateful Network Redundancy

- > Layer 2 Fallback
- > Integrated Zero Power High Availability
- > Auto Filter Control
- > Link Down Synchronization
- > Transparent to Router Protocols

Client and Server Protection

- > Prevent Attacks on Vulnerable Applications & Operating Systems
- > Eliminate Costly Ad-Hoc Patching
- > Multiple Filtering Methods

Traffic Normalization

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

Network Infrastructure Protection

- > Protect Cisco IOS, DNS and Other Infrastructure
- > Access Control Lists

Application Performance Protection

- > Increase Bandwidth and Server Capacity
- > Rate-Limit or Block Unwanted Applications (P2P/IM)
- > Ensure Bandwidth for Critical Applications

Digital Vaccine® Real-Time Filter Service

- > World-Renowned Security Research Team
- > Protection Against Zero-Day Attacks
- > Automatic Distribution of Latest Filters

Enterprise Security Management System (SMS)

- > Manage Multiple TippingPoint Systems
- > At-A-Glance Dashboard
- > Automatic Reporting

Comprehensive Threat Protection

Filter Categories

- | | |
|-----------------------|-------------------|
| > Worm | > Virus |
| > Phishing | > Spyware |
| > Trojan | > Suspicious |
| > P2P | > Reconnaissance |
| > Bandwidth Hijacking | > IM |
| > Walk-in Worm | > Blended Threats |
| > VoIP | > Backdoor |
| > OS Vulnerabilities | |

Protocols / Applications (Partial List)

- | | | |
|--------|--------|----------|
| > IP | > RPC | > FTP |
| > DNS | > MPLS | > Telnet |
| > VLAN | > SMB | > SMTP |
| > IMAP | > ICMP | > UDP |
| > TCP | > HTTP | |

Actions

- | | |
|--------------------------|--------------|
| > Block | > Permit |
| > Copy | > Alert |
| > Log | > E-mail |
| > Responder (Quarantine) | > Rate Limit |

Messaging

- | | |
|----------|----------|
| > E-mail | > Script |
| > Pager | > Syslog |
| > SNMP | |

Features and Benefits

- > Purpose-Built Hardware and Software
- > Comprehensive Protection
- > Unmatched Filter Accuracy
- > Industry Leading Filter Timeliness
- > Zero-Day Protection
- > Traffic Rate Shaping
- > Virtual Patching Protects PCs and Servers
- > Easy to Install and Manage
- > Deploys in Minutes
- > No Local Configuration Required
- > Easy Remote Management

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