Secure your Network

HP TIPPINGPOINT SECURITY - A COMPLETE SET OF SECURITY SOLUTIONS THAT ADDRESS TODAY'S SOPHISTICATED SECURITY THREATS AT THE PERIMETER AND INTERIOR OF YOUR BUSINESS.

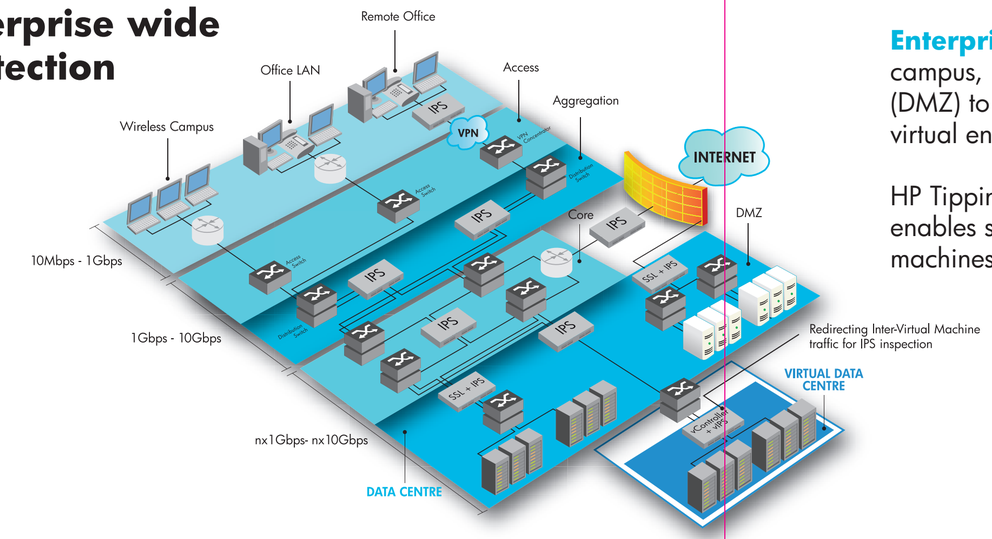
Solution Overview

The HP TippingPoint Intrusion Prevention System (IPS) achieves a new level of in-line, real-time protection, providing a proactive network security for today's and tomorrow's real-world network traffic and data centers. The IPS platform's next-generation architecture adds significant capacity for deep packet traffic inspection, and its modular software design enables the addition of valuable network protection services to its proven intrusion protection solution. This new best-of-breed IPS Platform redefines intrusion prevention as a foundation for comprehensive network security.

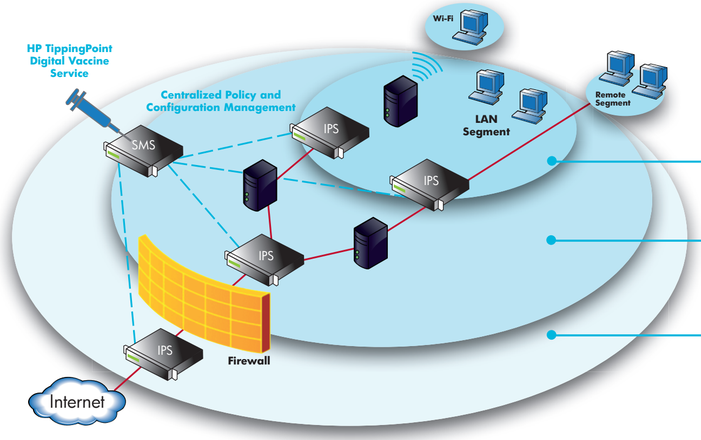
Key Features:

- Industry-proven proactive network security
- Up-to-date and broad IPS protection
- Industry leading security research team – Dvlabs
- Minimized overall security costs and complexity
- Security compliance best practices

Enterprise wide protection



Flexible Deployment From Core to Edge



Enterprise wide protection from wireless campus, remote offices, Demilitarized Zones (DMZ) to Data Centers in both physical and virtual environments.

HP TippingPoint virtual Controller (vController) enables security policy enforcements in virtual machines and mobile VMs.

Protection against Internal Attacks from

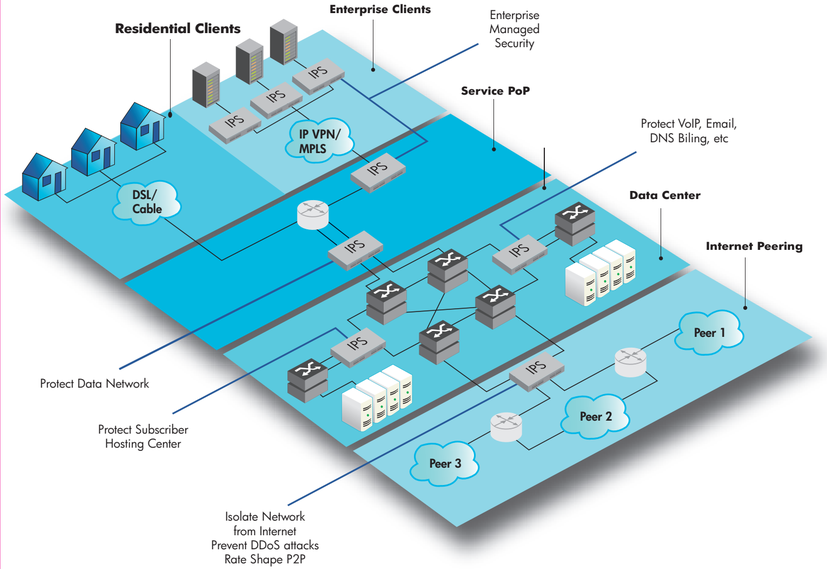
- Wired / Wireless LAN infrastructure
- Data Center

Security at the Core for major network segments

Protection at the Perimeter against external attacks from:

- Corporate WAN perimeter
- Web Application infrastructures
- Remote Office Branch Office (ROBO)
- Service Providers / partner peering points

Security for service providers



Hardware	HP S110 100Mbps (JC186A)	HP S330 300Mbps (JC187A)	HP S660N 750Mbps (JC019A)	HP S1400N 1.5Gbps (JC020A)	HP S2500N 3Gbps (JC021A)	HP S5100N 5Gbps (JC022A)	HP S6100N 8Gbps (JC577A)
Performance							
IPS / IDS Throughput[1]	100 Mbps	300 Mbps	750 Mbps	1.5 Gbps	3 Gbps	5 Gbps	8 Gbps
Network Throughput[2]	100 Mbps	300 Mbps	750 Mbps	1.5 Gbps	15 Gbps	15 Gbps	15 Gbps
Typical Latency[3]	< 600 microseconds	< 600 microseconds	< 80 microseconds	< 80 microseconds	< 80 microseconds	< 80 microseconds	< 80 microseconds
Concurrent Network Sessions[4]	1,000,000	1,000,000	6,500,000	6,500,000	10,000,000	10,000,000	10,000,000
Security Contexts[6]	250,000	250,000	1,200,000	1,200,000	2,600,000	2,600,000	2,600,000
Connections Per Second	9,700	18,500	115,000	115,000	230,000	230,000	230,000
Scalability							
Interfaces	1 GbE	1 GbE	1 GbE	1 GbE	10 GbE 1 GbE	10 GbE 1 GbE	10 GbE 1 GbE
Ethernet Ports	(8) 10/100/1000	(8) 10/100/1000	(20) 10/100/1000	(20) 10/100/1000	(2) 10 GbE XFP (20) 10/100/1000	(2) 10 GbE XFP (20) 10/100/1000	(2) 10 GbE XFP (20) 10/100/1000
Port Quantity/Type	Copper (8)	Copper (8)	(10) Copper/(10) SFP	(10) Copper/(10) SFP	(2) 10 GbE XFP (10) Copper/(10) SFP	(2) 10 GbE XFP (10) Copper/(10) SFP	(2) 10 GbE XFP (10) Copper/(10) SFP
Number of Port Segments	4	4	10	10	1 10	1 10	1 10
Zero Power HA	Integrated	Integrated	External	External	Modular External	Modular External	Modular External
Power Dissipation							
Units	AC	AC	AC	AC	AC DC	AC DC	AC DC
Amps (Max. Fused Power)	3A-2A	6A-3A	8A-5A	8A-5A	8A-5A 16A-8A	8A-5A 16A-8A	8A-5A 16A-8A
V	100-240	100-240	100-240	100-240	100-240 -36 to -60 VDC	100-240 -36 to -60 VDC	100-240 -36 to -60 VDC
Efficiency			66%	66%	71% 76%	71% 76%	71% 76%
Freq. Range (Hz)	50-60	50-60	50-60	50-60	50-60 n/a	50-60 n/a	50-60 n/a
Power Consumption - Watts			323	323	542 507	542 507	542 507
Power Consumption - BTU/hr	412	412	1,102	1,102	1851 1731	1851 1731	1851 1731
Dimensions							
Height (in)	1.74 (1U)	1.74 (1U)	3.42 (2U)	3.42 (2U)	3.42 (2U)	3.42 (2U)	3.42 (2U)
Height (cm)	4.42	4.42	8.69	8.69	8.69	8.69	8.69
Width (in)	16.75	16.75	16.8	16.8	16.8	16.8	16.8
Width (cm)	42.55	42.55	42.86	42.86	42.86	42.86	42.86
Depth (in)	18.25	18.25	24	24	24	24	24
Depth (cm)	46.36	46.36	60.96	60.96	60.96	60.96	60.96
Weight (lb)	14.99	14.99	29	29	31.5	31.5	31.5
Weight (kg)	6.8	6.8	13.2	13.2	14.3	14.3	14.3

[1] Represents throughput levels measured with recommended security profiles
[2] Represents maximum throughput levels that can be achieved with the use of traffic forwarding
[3] Measured on packet sizes up to 1518 bytes
[4] Maximum number of concurrent network sessions that can be supported by the IPS
[5] Measured number limited by available test equipment
[6] Maximum number of sessions with security state that can be supported by the IPS

High Availability
> Dual-Power Supplies (on models 660N, 1400N, 2500N, 5100N, 6100N)
> Layer 2 Fallback
> Active-Active or Active-Passive Stateful Redundancy (IPS + SMS)
> Zero Power High Availability

Security Certifications
> Common Criteria EAL2+: Analyzer, Sensor, Scanner, System
> Joint Interoperability Test Command (JITC) Certification for IPv6 Capability
> FIPS Validated 140-2

Attack Filters
> Number of Attack Filters – 5,000+
> Categories
• Worm • Phishing • Spyware
• Virus • Suspicious • DDoS
• Trojan • Reconnaissance • Bandwidth Hijacking
• P2P • Walk-in Worm • Blended Threat
• VoIP • Backdoor • Zero Day Initiative

Actions
> Block > Copy > Log > Quarantine
> Permit > Alert > E-Mail > Rate Limit

Protocols/Applications (partial list)
> IP > DNS > VLAN > IMAP > TCP > RPC > MPLS > SMB > ICMP > HTTP > FTP > Telnet > SMTP > UDP

Messaging
> E-Mail > Script > Pager > Syslog > SNMP

LED Indicators
> Status > Network Activity > Link State > System Power

Management Interfaces
> 110/100/1000 Ethernet > 1 Serial Port > 1 Front Panel LCD

Attack Filter Delivery Service
Digital Vaccine® Real-Time Inoculation

System Management (Three Options)
> Command Line Interface (CLI)
> Local Security Manager (LSM)
• On-Box Web-based Management
> Enterprise Security Management System (SMS)
• Manages multiple TippingPoint systems
• 1U Appliance
• Operating System – TippingPoint OS
• Client Requirements – Windows XP, 2000, NT or 9X, or Linux with X-Windows

Safety
> UL60950-1
> CSA 22.2-60950-1
> EN60825: Safety of Laser Products
> EN60950-1
> IEC60950-1
> 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 A: Regulations for Radio Frequency Devices for Electromagnetic Compliance
> ICES-003, Class A
> EN 55022 Class A
> VCCI Class A
> AS/NZS-3548 Class A

Warranty
The standard warranty is for a 12-month period.

Services
3-year, 24x7 next-business-day hardware advance exchange, 24x7 SW phone support and SW updates (UX067E)
Refer to the HP website at www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.

Notes
Performance footnotes:
• IPS/IDS Throughput represents the inspection throughput levels measured with recommended security profiles.
• Network Throughput represents the maximum throughput levels that can be achieved with the use of traffic forwarding.
• Typical Latency is measured on packet sizes up to 1518 bytes.
• Concurrent Network Sessions is the maximum number of concurrent network sessions that can be supported by the IPS.
• Security Contexts is the maximum number of sessions with security state that can be supported by the IPS.

DVLabs

HP TippingPoint DVLabs, a premier research organization for vulnerability analysis and discovery, helps ensure clients have pre-emptive protection for vulnerabilities and zero-day attacks. The team applies cutting-edge engineering, reverse engineering and critical analysis to create comprehensive security filters that are automatically delivered to HP TippingPoint intrusion prevention systems through the Digital Vaccine® service

DV Labs Research & QA

DVLabs Services:

DIGITAL VACCINE

Digital Vaccines are packages of filters automatically delivered to customers on a regular weekly release schedule to identify and detect traffic that is exploiting vulnerabilities. Application DV, part of the standard Digital Vaccine service, provides a simple way to manage granular application control within an enterprise. Organizations can limit network bandwidth consumption by these applications to ensure mission-critical applications are available. When it comes to filter development, HP TippingPoint DVLabs is the industry leader in the three most important filter metrics: (1) filter accuracy, (2) breadth of filter coverage, and (3) speed and timeliness of filter releases.

THREAT LINQ

ThreatLinQ security intelligence portal is an easy-to-use, real-time threat monitoring console that provides a means to evaluate the changing threat landscape and connect that to specific intrusion prevention system (IPS) policy changes. This gives organizations the ability to proactively optimize their network security in order to reduce unnecessary business risks based on a detailed real-time analysis of today's threat landscape.

WEB APP DIGITAL VACCINE

Web App Digital Vaccine services provide for the creation of custom Web application filters that block attacks that are directed at the unique vulnerabilities of custom Web applications. The service takes the vulnerability insight provided by a Web application scan, develops specific filters, and enforces protection through the HP TippingPoint IPS.

REPUTATION DIGITAL VACCINE

Reputation Digital Vaccine provides IPv4, IPv6 and Domain Name System (DNS) security intelligence feeds from a global reputation database so that you can actively enforce and manage reputation security policies using the HP TippingPoint Intrusion Prevention System (IPS) Platform. The HP TippingPoint IPS Platform acts as an enforcement point, inspecting traffic in real-time, identifying "known bad" traffic and enforcing Rep DV security policies.

DIGITAL VACCINE TOOLKIT

DVToolkit provides advanced users with a tool kit to develop customized filters in-house, eliminating the risk associated with sharing sensitive application information with third party vendors. By utilizing the DVToolkit, qualified analysts can also author filters to address the specific threats within their organization, allowing them to define parameters and triggers that dictate what, when, and how events are inspected. The ability to craft custom filters allows customers to significantly extend the value of their investment in our HP TippingPoint Intrusion Prevention System

© Copyright 2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA3-3739ENN, Created March 2011