# HP Threat Management Services zl Module

Data sheet

## Product overview

The HP Threat Management Services (TMS) zl Module is a multifunction security system for the HP E5400 zl and E8200 zl Switch Series. It is comprised of a stateful firewall, an intrusion detection/prevention system (IDS/IPS), and a virtual private network (VPN) concentrator. It enables network administrators to compartmentalize department traffic, protect the network from malware, and provide secure remote access and site-to-site connectivity.

## Key features

- Stateful firewall
- Intrusion detection/prevention system (IDS/IPS)
- Virtual private network (VPN)
- zl Module form factor
- Industry-leading warranty

## Features and benefits

### Intrusion detection/prevention system (IDS/IPS)

- **Deep packet inspection:** module supports deep packet inspection and examines the packet payload as well as the frame and packet headers; packets are dropped if attacks or intrusions are detected using signature-based or protocol anomaly-based detection
- **Severity-based action policies:** involve action taken against attacks based on their severity; available actions are "allow," "block," and "terminate connection" to provide appropriate mitigation
- **Signature update service:** provides regular updates to the signature database, helping to ensure that the latest available signatures are installed
- **Signature-based detection:** detects known attacks that have known attack patterns; the IPS maintains a signature database that contains the pattern definitions for known attacks, and can be automatically updated using a subscription service
- **Protocol anomaly-based detection:** detects anomalies in application protocol header using signatures

### Data center protection

- **Server protection:** stateful firewall controls traffic to the data center; intrusion protection system (IPS) detects and blocks threats such as worms and viruses to maintain service and application availability

### Compartmentalization

- **Departmental protection:** allows organizations to define departmental security policies to protect local resources with a stateful firewall and IPS while at the same time allowing high-performance access to common resources

### VPN concentration

- **Site-to-site connectivity:** IPSec-encrypted tunnels help ensure privacy between sites with optional Generic Routing Encapsulation (GRE) tunneling, which is available for full deployment flexibility; intersite links can be deployed quickly and controlled with tunnel policies
- **Secure remote access:** can be delivered for remote users via securely authenticated IPSec tunnels

### Firewall

- **Stateful firewall:** enforces firewall policies to control traffic and filter access to network services; maintains session information for every connection passing through it, enabling the firewall to control packets based on existing sessions
- **Zone-based access policies:** logically groups virtual LANs (VLANs) into zones that share common security policies; allows both unicast and multicast policy settings by zones instead of by individual VLANs
- **Application-level gateway (ALG):** deep packet inspection in the firewall discovers the IP address and service port information embedded in the application data; the firewall then dynamically opens appropriate connections for specific applications
- **NAT/PAT:** choice of dynamic or static network address translator (NAT) preserves a network's IP address pool or conceals the private address of network resources, such as Web servers, which are made accessible to users of a guest or public wireless LAN
- **DoS attack prevention:** firewall is able to detect various denial-of-service attacks and take appropriate action to mitigate the threat
- **Authenticated network access:** firewall can authenticate the user at a given IP address using RADIUS or a local user directory before allowing connections from that location

### Virtual private network (VPN)

- **IPSec:** provides secure tunneling over an untrusted network such as the Internet or a wireless network; offers data confidentiality, authenticity, and integrity between two endpoints of the network
- **Layer 2 Tunneling Protocol (L2TP):** is an industry standard-based traffic encapsulation mechanism supported by many common operating systems; will tunnel the PPP traffic over IP and non-IP networks; and may also use the IP/UDP transport mechanism in IP networks

- **Manual or automatic key exchange (IKE):** provides both manual or automatic key exchange required for the algorithms used in encryption or authentication; auto-IKE allows automated management of the public key exchange, providing the highest levels of encryption
- **Network Address Translation-Traversal (NAT-T):** enables IPSec-protected IP datagrams to pass through a network address translator (NAT)
- **Digital certificate management:** digital certificates can be utilized to authenticate to an IPSec VPN gateway; this also supports certificate revocation list (CRL) and allows certificates to be imported through a Simple Certificate Enrollment Protocol (SCEP) server
- **Site-to-site connectivity:** two IPSec VPN gateways can be configured to provide secure site-to-site communication between offices, partners, or suppliers; both IPSec or GRE tunnels are available
- **Generic Routing Encapsulation (GRE):** can be used to transport Layer 2 connectivity over a Layer 3 path in a secured way over IPsec; enables the segregation of traffic from site to site; provides dynamic routing and static failover
- **Secure remote access:** allows remote users to connect to the VPN gateway for secure communication to the corporate network over the public network; provides the flexibility to use the following VPN clients: Openswan VPN client for Linux, Shrew Soft VPN client, IPSecuritas VPN client for Macintosh OS X, Microsoft® Windows® XP native VPN client, Microsoft Windows Vista® native VPN client, and Microsoft Windows 7 native VPN client (both 32 bit and 64 bit)

## Operating modes

- **Route Mode:** provides the deployment of the firewall, VPN, and IPS in line with traffic for deep packet inspection to control and filter traffic; supports static routes, RIP, RIPv2, OSPF, IGMP, and PIM
- **Monitor Mode:** provides the deployment of the intrusion detection system (IDS) to monitor traffic passively out of band with the traffic

## Management

- **Remote configuration and management:** is available through a secure Web browser or a command-line interface (CLI)
- **Secure Web GUI:** provides a secure, easy-to-use graphical interface for configuring the module via HTTPS
- **Command-line interface (CLI):** provides a secure, easy-to-use command-line interface for configuring the module via SSH or a switch console; provides direct real-time session visibility
- **HP PCM Plus and HP Network Immunity Manager:** provides central management of multiple TMS zl Modules for discovery, status management, and configuration
- **Logging:** provides local and remote logging of events via SNMP (v2c and v3) and syslog; provides log throttling and log filtering to reduce the number of log events generated; support for email logging

## Connectivity

- **Two 10-GbE connections to the switch:** two 10-GbE wire-speed internal connections help ensure that the network connections from application to switch backplane will not limit the performance of the application

## Performance

- **High-performance network bandwidth:** includes two internal wire-speed 10-GbE ports to the switch backplane
- **High-performance processor system:** Intel® Core™ 2 Duo Processor T7500 with 2.2 GHz, 4 MB cache provides a high-performance compute environment in a small footprint using a single switch slot
- **Memory subsystems:** 4 GB of DDR2-667 dual-channel memory provides for quick application performance
- **Disk drive:** 250 GB SATA II 7200 rpm hard disk drive (210 GB application space plus 40 GB diagnostic/maintenance space) allows quick data reads/writes to speed applications along

## Resiliency and high availability

- **Redundant power supplies:** services module has the same level of power supply redundancy as the switch in which it is installed
- **High availability:** two modules can work together to provide high availability and redundancy; modules in the high-availability cluster share connection state information to provide stateful failover; active-standby failover is supported

## Ease of use

- **Locator LED (module):** allows users to set the locator LED on a specific module to either turn on, blink, or turn off; simplifies troubleshooting by making it easy to locate a specific module among other identical or similar modules

## Technical features

- **Firewall features:**
  - **Stateful packet inspection:** filters are based on destination and source IP address, port number, and protocol filter selector
  - **Logging/Alerts:** log messages in the WebTrends Enhance Log Format (WELF); logging of events via SNMP (v2 and v3); logs are sent to syslog server and are sent via email messages
  - **Enhanced firewall features:** port triggering, resource reservation, service-based time-outs, traffic rate limiting, and connection rate limiting
- **IPS/IDS features:**
  - **Anomaly Engine:** provides patternless attack detection (ICMP, UDP smurf, and DNS spoofing), protocol header integrity checks (mandatory fields, duplicate fields, and buffer limits), SMTP, MIME, SMTP, FTP, DNS, NNTP, IP, UDP, and TCP
  - **Intrusion protection:** provides intrusion protection mechanisms, and signature updates
- **VPN features:**
  - **IPSec:** AH, ESP, DES-CBC, 3DES-CBC, AES-128/192/256, HMAC-SHA1, HMAC-MD5, AES-XCBC, Tunnel mode, Transport mode, Extended Sequence Number Support, and UDP encapsulation for NAT traversal
  - **IKEv1:** Main mode; Aggressive mode; Quick mode; Config mode; Diffe-Hellman Group 1, 2, and 5 support; SHA1; MD5; Pre-shared keys; RSA/DSA signatures; Xauth; and PFS
  - **PKI:** SCEP client with PKCS#7 support

# HP Threat Management Services zl Module

## Specifications

**HP Threat Management Services zl Module (J9155A)**

| | |
|---|---|
| **Physical characteristics** | |
| Dimensions | 9.75(d) x 8.13(w) x 1.75(h) in. (24.77 x 20.65 x 4.45 cm) |
| Weight | 3.25 lb. (1.47 kg) |
| **Performance** | |
| Firewall throughput | up to 5.0 Gbps (performance may vary depending on network traffic and environment) |
| IPS/IDS throughput | up to 1.5 Gbps (performance may vary depending on network traffic and environment) |
| VPN throughput | up to 300 Mbps AES-128 and 70 Mbps 3DES (performance may vary depending on network traffic and environment) |
| Dedicated IPsec VPN tunnels | 4800 (100 w/L2TP) |
| Concurrent sessions | 600,000 |
| New sessions/second | 15,000 |
| Number of policies | 20,000 |
| Number of users | Unrestricted |
| Number of VLANs | 256 |
| **Environment** | |
| Operating temperature | 32°F to 122°F (0°C to 50°C); important: see note for 50°C temperature specification rules |
| Operating relative humidity | 15% to 90% @ 122°F (50°C), noncondensing |
| Nonoperating/Storage temperature | 14°F to 149°F (-10°C to 65°C) |
| Nonoperating/Storage relative humidity | 15% to 95% @ 149°F (65°C), noncondensing |
| Altitude | up to 10,000 ft. (3 km) |
| **Electrical characteristics** | |
| Maximum heat dissipation | 272 BTU/hr (287 kJ/hr) |
| Maximum power rating | 80 W |
| Notes | Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated. |
| **Notes** | Following are chassis operating temperature specifications of the 5400zl/8212zl switch when services modules are installed:<br>• 40°C when any services module is installed in the right side of the chassis<br>• 50°C when all services modules are installed in the left side of the chassis<br>Up to four services modules can be installed in a 5400zl/8212zl chassis simultaneously. Up to three services modules are supported (all installed in the left half of the chassis) in the 5406zl chassis if a 50°C temperature specification is desired.<br>When the services module is installed, the maximum relative humidity for the switch drops from 95% to 90%. |
| **Services** | 3-year, 4-hour onsite, 13x5 coverage for hardware (UQ589E)<br>3-year, 4-hour onsite, 24x7 coverage for hardware (UQ590E)<br>3-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support (UQ591E)<br>3-Year, 9x5 SW phone support, software updates (UQ592E)<br>3-year, 24x7 SW phone support, software updates (UQ593E)<br>1-year, post-warranty, parts only, global next-day advance exchange (UQ594PE)<br>1-year, post-warranty, 4-hour onsite, 13x5 coverage for hardware (UQ595PE)<br>1-year, post-warranty, 4-hour onsite, 24x7 coverage for hardware (UQ596PE)<br>1-year, post-warranty, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support (UQ597PE)<br>Installation with HP-provided configuration, system-based pricing (US668E)<br>3 Yr 6 hr Call-to-Repair Onsite (UW374E)<br>4 Yr 6 hr Call-to-Repair Onsite (UW375E)<br>5 Yr 6 hr Call-to-Repair Onsite (UW376E)<br><br>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. |

# HP Threat Management Services zl Module accessories

## License

HP Threat Management Services 1-year IPS subscription (J9157A)

HP Threat Management Services 2-year IDS/IPS subscription (J9158A)

HP Threat Management Services 3-year IDS/IPS subscription (J9159A)

## Appliance

HP Threat Management Services zl Module with 1-year IDS/IPS subscription (J9156A)

## To learn more, visit www.hp.com/networking



4AA2-6512ENW, Created May 2009; Updated October 2010, Rev. 2