



## HP ProCurve Threat Management Services zl Module

### Product overview

The HP ProCurve Threat Management Services (TMS) zl Module is a multifunction security system for the HP ProCurve Switch 5400zl and Switch 8212zl Series. It is comprised of a stateful firewall, intrusion detection/prevention system (IDS/IPS), and 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)
- Module form factor
- ProCurve Lifetime Warranty, 5-year disk warranty

## Features and benefits

### Industry-leading warranty



### 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

### Application support

- **HP ProCurve ONE application support:** is compatible with ProCurve ONE applications; non-ProCurve ONE applications will not run on the services module, which prevents rogue applications in mission-critical network environments

### 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, 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

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

- **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

- **Signature-based detection:** detects known attacks that have known attack patterns; IPS maintains a signature database that contains the pattern definitions for known attacks that can be automatically updated via a subscription service

- **Protocol anomaly-based detection:** detects attacks that use anomalies in application protocol payloads

- **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

\* For as long as you own the product, with next-business-day advance replacement (available in most countries). The following hardware products and their related series modules have a one-year hardware warranty with extensions available: HP ProCurve Routing Switch 9300m Series, HP ProCurve Switch 8100f Series, HP ProCurve Network Access Controller 800, and HP ProCurve DCM Controller. The following hardware mobility products have a one-year hardware warranty with extensions available: HP ProCurve M111 Client Bridge, HP ProCurve MSM3xx-R Access Points, HP ProCurve MSM7xx Mobility and Access Controllers, HP ProCurve RF Manager IDS/IPS Systems, HP ProCurve MSM Power Supplies, HP ProCurve 1-Port Power Injector, and HP ProCurve CNMS Appliances. Disk drives in the HP ProCurve ONE Services z1 Modules have a five year hardware warranty. Standalone software, upgrades, or licenses may have a different warranty duration. For details, refer to the ProCurve Software License, Warranty, and Support booklet at [www.procurve.com/warranty](http://www.procurve.com/warranty).

## 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):** an industry standard-based traffic encapsulation mechanism supported by many common operating systems; will tunnel the PPP traffic over the IP and non-IP networks; may use the IP/UDP transport mechanism in IP networks
- **Generic Routing Encapsulation (GRE):** can be used to transport Layer 2 connectivity over a Layer 3 path in a secured way; enables the segregation of traffic from site to site
- **Manual or automatic key exchange (IKE):** provides both manual or automatic (IKE) 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 importing certificates through a Simple Certificate Enrollment Protocol (SCEP) server
- **Remote access VPN client:** provides the flexibility to use either the ProCurve VPN client or a Microsoft Windows XP or Vista native VPN client
- **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
- **Secure remote access:** allows remote users to connect to the VPN gateway for secure communication to the corporate network over the public network

## 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:** through secure Web browser or command-line interface (CLI)
- **Secure Web GUI:** provides a secure, easy-to-use graphical interface for configuration of the module via HTTPS
- **Command-line interface (CLI):** provides a secure, easy-to-use command-line interface for configuration of the module via SSH or switch console; provides direct real-time session visibility
- **HP ProCurve Manager:** central management through ProCurve Manager Plus for discovery, logging, and status management
- **Logging:** 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

## 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:** two internal wire-speed 10-GbE ports to the switch backplane
- **High-performance processor system:** Intel Core 2 Duo T7500 Processor 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 provide 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 read/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

- **Redundant network connections:** two internal 10-GbE connections are provided between the switch and the services module; applications can take advantage of both links to provide a redundant network connection to the switch backplane

- **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

## Manageability

- **Console port:** application console is available as a pass-through to the switch console function

## Ease of use

- **Locator LED:** 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 based on destination and source IP address, port number, and protocol filter selector

- **Logging/Alerts:** logs messages in the WebTrends Enhance Log Format (WELF); logs are sent to syslog server and are sent via e-mail messages

- **Enhanced Firewall Features:** port triggering, resource reservation, service-based time-outs, traffic rate limiting, and connection rate limiting

- **IPS/IDS Features:**

- **Anomaly Engine:** patternless attack detection (ICMP, UDP smurf, DNS spoofing), protocol header integrity checks (mandatory fields, duplicate fields, buffer limits), SMTP, MIME, SMTP, FTP, DNS, NNTP, IP, UDP, and TCP

- **Intrusion Protection:** intrusion protection mechanisms, TCP buffering, 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; Diffie-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

## Warranty and support

- **ProCurve Lifetime Warranty:** for as long as you own the product, with next-business-day advance replacement (available in most countries)

- **Electronic and telephone support:** limited electronic and telephone support is available from HP; refer to the HP Web site at [www.procurve.com/support](http://www.procurve.com/support) for details on the support provided and the period during which support is available

# HP ProCurve Threat Management Services zl Module

## Specifications



HP ProCurve 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	3.0 Gbps
IPS/IDS throughput	1.5 Gbps
VPN throughput	300 Mbps AES and 70 Mbps 3DES
Dedicated IPsec VPN tunnels	4,800
Concurrent sessions	600,000
New sessions/second	15,000
Number of policies	20,000
Number of users	Unrestricted
Number of VLANs	19

### 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), non-condensing
Non-operating/Storage temperature	14°F to 149°F (-10°C to 65°C)
Non-operating/Storage relative humidity	15% to 95% @ 149°F (65°C), non-condensing
Altitude	up to 10,000 ft. (3 km)

### Electrical characteristics

Maximum heat dissipation	272 BTU/hr (287 kJ/hr)
Power consumption	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

Chassis operating temperature specifications of the 5400/8212 switch when the services module are installed:

- 40°C when any services module is installed in the right side of the chassis
- 50°C when all services modules are installed in the left side of the chassis

Up to four services modules can be installed in a 5400/8212 chassis simultaneously. Up to three services modules are supported (all installed in the left half of the chassis) in the 5406 chassis if a 50°C temperature specification is desired.

When the services module is installed, the maximum relative humidity for the switch drops from 95% to 90%.

### Services

Refer to the HP Web site at [www.procurve.com/services](http://www.procurve.com/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 ProCurve Threat Management Services zl Module accessories

**NEW** HP ProCurve Network Immunity Manager 2.0 software-50-device license (J9161A)

**NEW** HP ProCurve Network Immunity Manager 2.0 software-+100-device license (J9162A)

**NEW** HP ProCurve Network Immunity Manager 2.0 software-unlimited-device license (J9163A)

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

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

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

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

---

**Technology for better business outcomes**

To learn more, visit [www.hp.com/go/procurve](http://www.hp.com/go/procurve)

© Copyright 2009 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.

March 2009

