# Threat Management Services module

## Contents

- **Introduction** .......................................................... 2
- **HP ProCurve ProActive Defense** ............................... 2
- **Threat Management Services module overview** .......... 3
- **Major Threat Management Services module functions** .................................................. 3
- **Major Threat Management Services module as an IPS** .................................................. 5
- **Common deployment scenarios** ............................. 8
- **Conclusion** ............................................................. 10
Introduction

Most companies today are aware of the numerous security threats that can threaten their digital assets such as intellectual property, customer data, or provided services. There is a need for effective and cost-efficient ways to secure their data and services. Even though security is a great concern, quite often security is “bolted on” to existing network infrastructure, making it difficult and costly to manage.

To alleviate this, HP ProCurve Networking has designed a security vision and strategy called ProCurve ProActive Defense, which is explained in more detail in this document. One of the products designed to fit into ProActive Defense is the ProCurve Threat Management Services (TMS) module, which provides three functionalities in one device:

• Firewall
• Intrusion detection systems (IDS)/intrusion prevention system (IPS)
• Virtual private network (VPN)

The device is a blade that integrates with certain ProCurve chassis switches, eliminating the need for extra rack space and extra cables, providing easy-to-use management interfaces. The TMS modules can also be managed by HP ProCurve Manager Plus and its plug-ins, such as Network Immunity Manager, which provides a single interface for managing switches, access points, and TMS modules. This reduces the cost required with multiple management software applications. It also decreases the complexity of managing different types of devices by having a single pane of glass.

This technical brief describes the major features and common deployment scenarios of the TMS module.
To further improve the threat management aspect of the ProCurve ProActive Defense, ProCurve released the Threat Management Services (TMS) module. The TMS module is a multifunctional security system capable of performing multiple roles for securing a networking environment. The key features to achieve this are:

- Integrated Stateful Firewall
- IPS/IDS
- IPsec VPN

Each of these features can be used separately or together, depending on the needs of the network. The form factor of the TMS module allows it to be placed in ProCurve switch chassis that accept zl modules, such as the HP ProCurve Switch 5400zl Series and Switch 8200zl Series. This allows for tight integration with the networking hardware to boost performance and provide interchassis failover as well as intrachassis failover.

The TMS module can be used in two modes:

- **Routing mode**, which allows the TMS module to route packets while inspecting them
- **Monitor mode**, which allows the TMS module to inspect packets, but not forward them, allowing the TMS module to operate purely as an IDS

Management of TMS modules can be done in multiple ways, giving the network administrator options. Each TMS module has an intuitive Web interface, from where all features can be configured, as well as an overview of the module’s performance which can be obtained and its log can be viewed. The same is true for using the TMS module’s command-line interface (CLI). The CLI can be reached from the chassis it is located in and provides similar syntax as the switch.

When deploying and managing multiple TMS modules, ProCurve Manager Plus, together with Network Immunity Manager can be used to centralize management as well as to provide a single pane of glass for all ProCurve devices.

**Major TMS module functions**

Each of the main features (firewall, IPS/IDS, VPN) of the TMS module can be used in different scenarios at the same time. This section will focus on each feature separately, although many environments would use multiple functions at the same time.

**TMS module as a firewall**

The TMS module has a built-in firewall with advanced features, which help ensure that network traffic stays where it should be, without getting in the way of legitimate traffic. To achieve this, the TMS module provides the following firewall features:

- Stateful Deep Packet Inspection
- Route mode (Layer 3) and transparent mode (Layer 2)
- Policy-based NAT (one to one, one to many, many to many)
- Application-aware policy controls
- Authenticated network access
- Denial of Service (DoS) attack prevention
- Traffic rate limiting
- Uniform Resource Identifier (URI) filtering

---

**Threat Management Services module overview**

<table>
<thead>
<tr>
<th>Breadth of solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProVision intelligence</td>
</tr>
<tr>
<td>Appropriate secure response</td>
</tr>
<tr>
<td>ProCurve Mobility Manager</td>
</tr>
<tr>
<td>ProCurve Network Immunity Manager</td>
</tr>
<tr>
<td>TMS module management</td>
</tr>
<tr>
<td>ProCurve Manager</td>
</tr>
<tr>
<td>Automated policies</td>
</tr>
<tr>
<td>Control</td>
</tr>
<tr>
<td>Monitor</td>
</tr>
<tr>
<td>Report</td>
</tr>
<tr>
<td>Accountable</td>
</tr>
</tbody>
</table>

**Improved network performance**

**TMS Module**
Firewalls are typically used to segregate traffic between zones in a network. The TMS module allows zones to include multiple VLANs, which makes it easy to create policies for traffic between them. The internal zone could include all department VLANs, whereas the external zone could only contain the VLAN connected to the Internet. Alternatively, each department can be put in its own zone to segregate traffic between departments.

In figure 1, the TMS module is used to control traffic to and from the internal network, the DMZ, and the Internet. By ensuring that only valid traffic is allowed, the servers in the DMZ are safe from attacks on services that should not be reachable from the Internet, while internal clients are still able to reach those services. When we take a closer look at the implementation, we will see how some of the features are used.

**Stateful Firewall**

The TMS module uses a stateful firewall. It only opens ports for returning traffic when an allowed outbound connection is made. For example, as in figure 2 the TMS module is configured to allow HTTP (port 80) traffic from the internal zone to the Internet. When a client wants to contact a Web server over HTTP, it sends a packet with the SYN flag set to the Web server on port 80. The TMS module sees this and automatically opens the port for return traffic.

**Policy-based NAT**

Most companies do not have enough public IP addresses to give each client on their network a public IP address. In most cases, the ranges used are private IP addresses. In figure 3, multiple clients need access to the Internet, but there is only one public IP address available. By using many-to-one NAT, the TMS module can use the same public IP address to allow connections from all clients. The TMS module rewrites each packet source address to be its own and holds a table so it knows for which client returning packets are intended.

**Application-aware policy controls**

Some applications work by opening extra ports or by using ports that are not in the initial connection. An example is FTP in active mode. In figure 4, the client connects to port 21 on the FTP server for its control connection. It lets the server know which high port it wants to receive the data connection on. When the client requests data from the server, the server will connect to the server on that high port from port 20. Because the high port on the client is dynamic, the TMS module needs to know which port will be used. It learns this by inspecting the FTP packets, and then opens the appropriate ports. The TMS module provides this functionality for multiple protocols.
Authenticated network access
Different users might have different access needs through the firewall. This is usually solved by putting similar users in the same VLANs and zones, as well as differentiating access for the zones. Sometimes a user will not be in his or her VLAN. To still provide the user with appropriate access, it is possible to have the user authenticate to the firewall, and obtain a different set of firewall policies. Supported authentications are Web authentication and VPN authentication.

In figure 5, the TMS module firewall is set up to be restrictive so that clients only have access to allowed resources. The database server in the DMZ is not directly reachable from the clients. The database administrator is on one of those clients and needs to update some tables directly. The administrator opens a Web browser and authenticates to the TMS module. The TMS module then uses a different set of policies for the database administrator that provides the administrator with direct access to the database.

DoS attack prevention
Denials of Service (DoS) attacks are usually used not to gain access to a system, but to deprive legitimate clients access to a service. The TMS module has the capability to detect different DoS attacks and prevent them from occurring. An example is a SYN flood attack as shown in figure 6, an attacker can forge connection requests to a server. For each request, the server will allocate some resources. By not completing the connection requests, the server can run out of resources. The TMS module is capable of detecting this and filtering the forged requests.

Traffic rate limiting
The TMS module is able to limit traffic on each policy, making sure that certain connections are not able to starve the available bandwidth. The TMS module can enforce limits on the number of connections, the number of kilobytes, and the number of packets in configurable time frames. For example, as shown in figure 7 the TMS module can limit HTTP connections to the Web server to 2 Mbps, helping to ensure that enough bandwidth is available for other connections.

TMS module as an IPS
The TMS module can act as an intrusion prevention system (IPS). Because the TMS module is in front of critical services, it adds defense against known and unknown attacks. To achieve this, the TMS module provides the following IPS features:

- Severity-based action policies
- Multiple intrusion detection methods
  - Signature-based detection
  - Protocol anomaly detection
  - Traffic anomaly detection
- Signature update services
The IPS can be deployed in different modes, depending on the environment needs. It can be deployed in route mode or monitor mode. In route mode the TMS module can actively block or reset attacks, whereas in the monitor mode, the TMS module only detects and reports attacks. IPSs are usually strategically placed in front of critical servers or servers that are likely to be targeted. As shown in figure 8A, it is placed in such a way that it is able to detect attacks targeted at servers in the DMZ. By using deep packet inspection on each packet that traverses the TMS module is able to mitigate the attack before it reaches the Web server. When we take a closer look at the implementation, we will see how some of the features are used.

**Severity-based action policy**

When the TMS module detects an attack, it can do one of three things. It can allow the malicious packets, it can drop the malicious packets, or it can send a reset (RST) packet to terminate the session. The administrator can configure which action to take based on the severity of the attack (critical, severe, warning, or information).

Figure 8 shows that the TMS module detects malicious traffic. In this case, someone is trying to enumerate the root Web server directory by using an old vulnerability. Because the vulnerability is old, it is classified as informational. Because the administrator configured the system to allow packets classified informational, it does get forwarded to the Web server. Because the Web server is not vulnerable, the system returns a HTTP 404 not found message.

Figure 9 the TMS module detects malicious traffic. Someone is trying to gain access of the FTP root of the FTP service on the web server. This is classified as a warning, and since it is something a legitimate user could accidentally do, the administrator configured the TMS module to send a RST packet to reset the connection. This will disconnect the user, alerting him he or she did something that is not allowed.

Figure 10 shows TMS module detecting malicious traffic. In this case, someone is trying to perform a FTP List buffer overflow, in an attempt to gain administrator access to the server. This is classified as critical. The TMS module is configured by the administrator to silently drop packets classified as critical and disrupt attacks without providing any feedback.

**Multiple intrusion detection methods**
The TMS module provides two different methods to detect malicious traffic and help ensure that it can detect known and unknown threats.
Figure 11 shows an example of the TMS module using signature-based detection. The TMS module has a signature database of known exploits, vulnerabilities, viruses, and so on. By performing deep packet inspection, the TMS module can compare the packet’s payload to its signatures. When it finds a match, the TMS module will take action as configured, as well as logging it.

Figure 12 here provides an example of the TMS module using protocol anomaly detection. The TMS module is aware of well-known protocol specifications and regular behavior. Sometimes attacks use a legal field inside of a protocol to initiate an attack. In the example here, the TMS module detects a possible attack on the SMTP server by using an excessively long header. Even though there is not a signature match, it could constitute a new attack. Some protocol anomalies can be configured to suit the network requirements, such as the maximum size of an SMTP header.

**Signature update service**

New attacks and exploits are constantly being developed. Servers are the most vulnerable between the time that an exploit starts being used and the software vendor releases a security patch against that exploit. Because it can take a lot of effort and time for a software vendor to release a patch, the time that the server is vulnerable can be a significant period. Signatures for those exploits are often available before the patch, and can be used to help ensure that the server does not become exploited. ProCurve provides a subscription-based signature update service. This allows the TMS module to automatically check for new signatures at configured intervals, and install them when available, allowing the TMS module to have the most recent signature database possible as shown in figure 12.

**TMS module as a VPN gateway**

In figure 13, the TMS module can act as a VPN gateway. By positioning the TMS in front of a secured site, it is possible to provide secure, encrypted access to that network, either for users directly or for another site. The TMS module supports GRE as well as L2TP over IPsec. To achieve this, the TMS module provides the following VPN features:

- Site-to-site VPN
- Remote access VPN
- Xauth
- Certificate management (Simple Certificate Enrollment Protocol [SCEP]/CRL support)
Site-to-site VPN

The TMS module is able to provide secure, encrypted connections between sites, even when those sites are connected through an unsecured, untrusted, or public network, such as the Internet, as shown in figure 14. By using TMS modules for site-to-site tunnels, it is possible to connect remote sites, without needing to buy or lease expensive dedicated lines, while still being secure.

Remote access VPN

When the TMS module is used as a remote access VPN, as shown in figure 15, it is able to provide multiple types of users with access to the corporate network, without opening the internal network to unauthorized users. Types of users can include sales representatives accessing the network on the road or employees working from home.

Xauth

VPN has its own authentication mechanism to establish tunnels. By using Xauth on the TMS module, it is also possible to identify and authenticate each separate user against a RADIUS server. This leverages existing user directories, such as Active Directory or eDirectory. By using Xauth, it is possible to assign different access policies to different users, limiting what traffic is allowed through the VPN tunnel.

As in figure 16, an administrator would be able to access all servers for remote assistance, whereas a traveling sales representative would only be able to access an e-mail server and the sales servers.

Certified management (SCEP/CRL)

The TMS module supports the SCEP. This protocol allows the TMS module to automatically request and install a certificate, without requiring administrators to perform each step manually as shown in figure 17. SCEP also allows the TMS module to retrieve the Certificate Revocation List (CRL) from a CA, making sure that the TMS module does not allow connections from nodes with a revoked certificate.

Common deployment scenarios

The TMS module is a multifunctional device, and can therefore be used in many different scenarios. Because of the TMS module’s flexibility and the numerous different network designs, it is impossible to list all deployment scenarios. This section will show three common scenarios and what role the TMS module plays in each. Even though each scenario here only lists one TMS module, in many cases it would be beneficial to have at least two TMS modules to enhance availability and/or performance.
Compartmentalization

In figure 18, the TMS module is used in separate zones and VLANs with different security needs, making sure that only legitimate traffic is allowed to cross its VLAN boundary. Legitimate traffic here does not only mean traffic that is allowed by the built-in TMS firewall, but also traffic that is not harmful, as detected by the IPS functionality of the TMS module. For example, the Sales department is allowed to access resources in the Finance department, so that it can update its sales numbers. But the Sales department is not allowed to access any resources of the Research department. However, if someone from Sales would try to use an exploit on a Finance resource, the TMS module would detect this and would act accordingly, depending on how the administrator configured the TMS module.

Even though this scenario does not show a use for VPN, there are cases where VPN would be useful, for example, granting certain cross-function employees secured access to multiple security zones.

Data center

Data centers often are designed to improve uptime and availability of the resources they house, which are often mission critical. They include redundant power, cooling, and controlled physical access, to name a few. To help ensure that data centers meet their required uptime, it is important to have all resources secured also. By using the TMS module in front of the data center, the module can protect these resources. It can control who and what can access which resources by using its built-in firewall, while also checking those connections for harmful traffic using its IPS feature.

For example in figure 19, the TMS module can allow access to the application servers and file servers from clients, but not access to the database server. This all occurs while doing deep packet inspection on the traffic, looking for known exploits. Even though this scenario does not show a use for VPN, there are cases where VPN would be useful, for example, granting full access to all servers when an administrator sets up a VPN to the module.

Perimeter defense

The most traditional placement of firewalls, IPSs, and VPN gateways is at the perimeter of the network, where the internal network connects to an external, untrusted network such as the Internet. One TMS module is able to provide all of these features. It can control what traffic is allowed, while inspecting that traffic for exploits, offering site-to-site and remote VPN access.
For example, in figure 20, the TMS module would allow Web traffic from the Internet to the Web server in the DMZ, but not traffic to the database server in the DMZ, or traffic to the internal network. If someone were to use a known exploit on the Web server, the TMS module would detect this and act accordingly, depending on how it is configured. The TMS module at the same time is providing access for mobile sales representative and has a VPN tunnel set up to a remote site.

**Conclusion**

By using the TMS module, it is possible to increase network security without creating unnecessary complexity with separate devices. The TMS module integrates with existing switches and can use the same management interface by using ProCurve Manager Plus and Network Immunity Manager, driving down management costs. The TMS module provides advanced features to increase security for its three major functions, the firewall, IDS/IPS, and VPN.

By providing flexibility, the TMS module can be used in many different environments, whether it is using only one of its major functions or all three at once. When multiple TMS modules are used, a highly available environment can be created, preventing downtime cause by power outages and other disruptions.