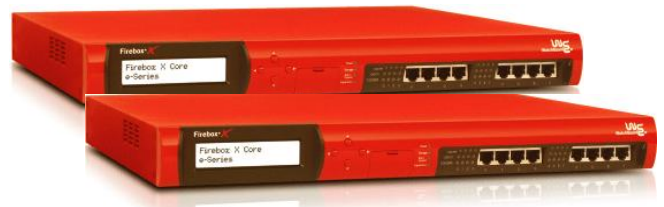


Universal Threat Management

As the industry evolves from traditional firewalls and VPNs, more advanced security is required to address the sophisticated and destructive Internet threats. Universal Threat Management (UTM) is the most advanced network security available, based on Watchguard's industry leading Firebox® X technology. Using a layered security approach, UTM provides industry-leading protection against blended security threats to ensure your server infrastructure is safe. Our UTM solution offers a broad set of features including: intrusion detection and prevention; zero-day protection; and defense against port scanning, Denial of Service (DoS), Distributed DoS attacks, and policy violations.

Benefits

- Continuous Security Updates - Continuous, automatic updates of threat management subscriptions & attack signatures ensures your security is never out of date.
- True Zero Day Protection - Critical capabilities defend against attacks even without signatures, protecting against the newest threats until attack signatures arrive; so your network has the strongest protection available.
- Superior Multi-Layered Security - Building on Intelligent Layered Security (ILS), with security layers that work together, strengthens your overall protection without sacrificing performance.



Network Security Features

- Advanced Firewall Protection - UTM utilizes a powerful, stateful packet inspection firewall that provides protection by dictating what network traffic to permit or restrict based on the source IP, destination IP, and ports. The advanced firewall also shields your systems and data from unauthorized access through its network address translation (NAT). On a continuous automatic basis, all firewall software subscriptions and attack signatures are updated with the most current versions to ensure UTM is ready to block the next malicious network attack. Online Tech will handle all firewall rule changes and analyze log files on a regular basis.
- Intrusion Detection and Intrusion Prevention Service (IPS) - Intrusion prevention protects your servers from attacks based on malicious content. By scanning network traffic at the gateway, malicious threats can be blocked before they enter the network and execute their hazardous payload. The signature-based IPS service works together with other layers of UTM to defend against a wide range of threats including: SQL injections, cross-site scripting, buffer overflows, and policy violations.
- Denial of Service (DoS) and Distributed DoS Attack Protection - Denial-of-Service attacks are defined as attempts to make server resources unavailable to its intended end-user group. DoS attacks typically originate from malicious effort of a person or group in order to make an Internet site or service unusable. UTM protects against DoS attacks or Distributed DoS (DDoS) attacks by detecting and dropping traffic associated with the DoS attack, while allowing

safe network to pass. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers, such as banks, credit card payment gateways, and even root servers.

- **Port Scanning Prevention** - Port scanning is defined as the process of using software to scan a network for open ports and therefore find possible network vulnerabilities. UTM protects against port scanning by identifying hackers causing malicious network traffic and blocking the originating IP address before the attack occurs. Multiple layers in the UTM platform can identify, coordinate, and lockout the port scan behavior before the damage is done.
- **Zero Day Protection** UTM protects against zero day attacks, which are categorized as unknown attack types but having similar characteristics of past attack classes. Zero day protection is critical because as new attacks emerge, the network remains safe with no window of exposure to attack. Other network intrusion detection techniques used by UTM include: pattern matching, protocol anomaly detection (PAD), command limiting, cloaking, header filtering and blocking, port scanning protection, and protection against IP address spoofing.

UTM Options

Universal Threat Management is available in 3 levels of service from Online Tech:

<u>Options</u>	<u>Description</u>	<u>VLANs, IP Addresses & Bandwidth Supported</u>	<u>Application</u>
Shared UTM	Your servers are protected by OTC's shared Watchguard Firebox X appliances.	1 VLAN 61 IP Addresses 25 Mbps	Delivers cost effective advanced network security.
Dedicated UTM	OTC deploys and manages a dedicated Watchguard Firebox X appliance specifically for your servers.	25 VLANs 512 IP Addresses 300 Mbps	Ideal for HIPAA, PCI, and CISP applications.
Dedicated High Availability UTM	OTC deploys and manages 2 Watchguard appliances in high availability mode with automatic failover.	25 VLANs 512 IP Addresses 300 Mbps	Ideal for HIPAA, PCI, and CISP applications that require a higher level of availability.

About Online Tech

Online Tech is Michigan's premier Managed Data Center Operator. Online Tech helps companies manage their growing demand for data and computing capacity through it's highly secure and reliable data centers across Southeast Michigan. With a full range of colocation, dedicated server and managed service options, industry leaders trust Online Tech to ensure their servers are always on, always online, and always safe. Contact us at (734) 213-2020 or visit our website at www.onlinetech.com to learn more about our services.

