NETGEAR PROSECURE™

ProSecure™ Unified Threat Management Appliance
UTM Series

Data Sheet

Unified Gateway Security for the SMB – Without Compromises

Viruses and malware hosted on Web pages, email phishing attacks, spam, virus infested emails, and other threats are now all part of a regular repertoire of sophisticated blended attacks that bypass traditional firewalls with ease. Small businesses have been the ones most seriously affected as small businesses, unlike their enterprise counterparts, often lack the time and resources to fully harden and secure their networks from these threats.

Moreover, such threats have signaled a change in the threat landscape: previously, threats to small businesses could largely be considered "push" type threats wherein hackers specifically targeted small businesses – a relatively rare occurrence given the prevalence of larger and richer targets in the medium and large business space. However, the advent of Web 2.0 technologies and cloud computing has largely shifted the threat landscape to one characterized largely by "pull" attacks wherein end users use Web 2.0 and cloud computing technologies to "pull" threats into the organization.

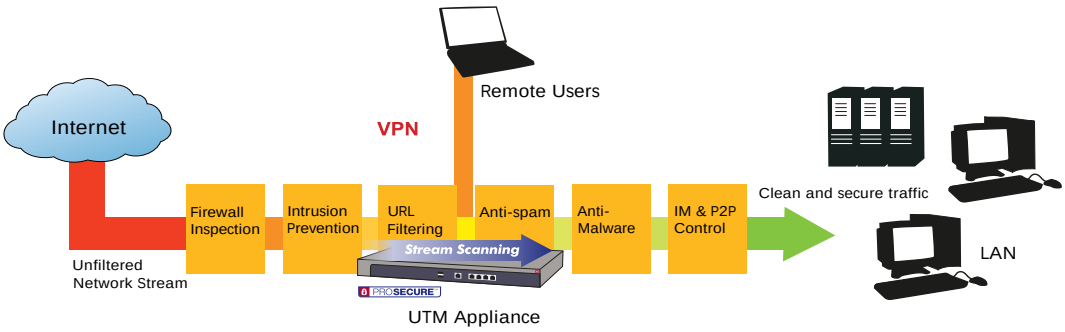
Because comprehensive network security solutions require an abundance of processing power to examine network traffic in real time, existing SMB all-in-one security solutions often use rudimentary security technologies that trade comprehensiveness for speed. True security must satisfy the requirements in both speed and coverage.

The NETGEAR ProSecure UTM Features and Highlights

- **Best-of-Breed Anti-malware Engine**
  - Enterprise-class malware scan engine
  - Up to 200 times the coverage of legacy SMB all-in-one solutions
  - Detects over 13 million threats
  - Hourly automatic signature updates
- **NETGEAR Patent Pending Stream Scanning Technology**
  - Data streams are processed as they enter the network
  - Low latency Web traffic scanning
- **Distributed Spam Analysis Anti-spam Technology**
  - Hybrid in-the-cloud architecture
  - Gathers threat data from over 50 million global sources
  - New spam is classified and detected within minutes
  - No learning period, works right out of the box
  - Minimal false positives
  - Highly adaptive all types of spam
- **Distributed Web Analysis URL Filtering**
  - Next generation hybrid in-the-cloud URL filtering technology
  - Hundreds of millions of categorized URLs
  - New Web sites are categorized in real-time
  - 64 categories
  - User- and group-based filtering
- **Zero Hour Threat Protection**
  - Heuristic-based detection
  - Detect unknown threats at zero hour
  - Limits the network's exposure to new unclassified threats

All-in-one Network Security Without Compromise

NETGEAR ProSecure Unified Threat Management (UTM) Appliances combine performance with comprehensive security coverage. Patent-pending Stream Scanning Technology enables the use of an extensive virus and malware database while maintaining a high level of throughput and minimizing scanning induced latency. The flexible modular software design architecture leverages patent-pending Stream Scanning technology to scan files and data streams up to 5x faster than conventional methods. This architecture in turn enables ProSecure UTM to utilize virus and malware threat databases from NETGEAR and Sophos™ that are hundreds of thousands of signatures in size - up to 200x more comprehensive than legacy small business UTM platforms. This architecture, combined with best-of-breed hybrid in-the-cloud Web filter and anti-spam technologies and with proven NETGEAR firewall and VPN functionality, form the ideal SMB gateway security solution.



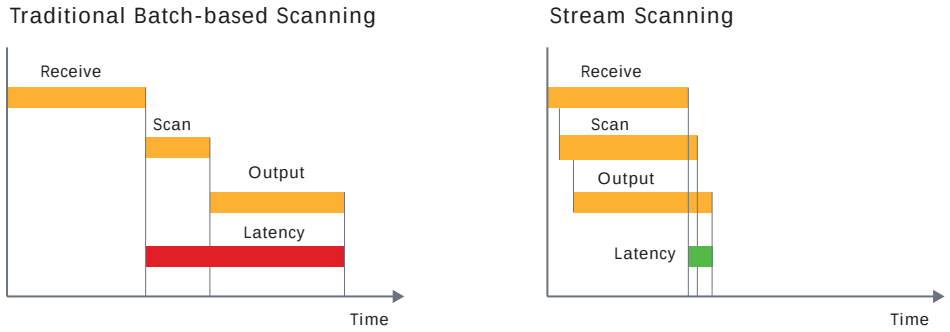
Revolutionary Stream Scanning Platform

Given the high performance requirements of scanning latency sensitive Web traffic, incorporating enterprise-grade security software technologies onto traditional SMB all-in-one platforms has been a very difficult task. That is why the NETGEAR ProSecure UTM features patent-pending Stream Scanning Technology which analyses data streams as they enter the network. The NETGEAR Stream Scanning approach is many times faster than that of more traditional batch-based scanning methods where the entire file is buffered before it is scanned.

commtouch® mailshell™ SOPHOS

- **NETGEAR Intrusion Prevention System**
  - Rules-driven language
  - Prevent hackers from penetrating the network perimeter
- **IM and P2P Application Control**
  - Blocks access to public IM clients
  - Blocks peer-to-peer (P2P) clients
  - Preserve productivity and save bandwidth
- **SSL & IPsec VPN Remote Access**
  - SSL VPN - clientless remote access, anywhere, anytime
  - IPsec VPN - secure site-to-site tunnels and client-based remote access.
  - No additional licenses to purchase
- **Built-in VPN/Firewall**
  - Dual WAN Gigabit Firewall* provides load balancing and failover
  - Four Gigabit LAN ports, one configurable DMZ port
  - Stateful packet inspection (SPI)
  - Denial-of-service (DoS) protection

Because of its nature, traditional batch-based scanning methods introduce latency to network traffic. While latency is more tolerable for email traffic, for large amounts of HTTP Web traffic, such latency often slows Web browsing to a crawl. All-in-one solutions in the past have tried to overcome the latency issue by minimizing the malware signature set, scanning only a handful of file types, or by avoiding Web traffic scanning altogether. This approach exposes an entire vector of the network to malware-based attacks.



Simple Setup, Ease of Management

The NETGEAR ProSecure UTM will easily replace any existing firewall or router. A simple 10-step setup wizard guides you through installation and the UTM will be up and running in minutes. Administration is performed through an intuitive Web-based interface. Set granular policies and alerts, check summary statistics and graphical reports, drill down to IP address-level data, and integrate log data with standard network management tools using SNMP. Malware and IPS signature, software, and firmware updates are all handled by the UTM - online and automatically.

For many administrators and IT personnel one of their biggest nightmares is the management of individual licenses or “seats.” Buying additional licenses when computers and personnel are added to the network is time-consuming and costly. The NETGEAR ProSecure UTM offers Web and email protection subscriptions **with no “per-user” licensing.**

UTM SERIES COMPARISON

MODEL	UTM10	UTM25
SIZING GUIDELINES		
Customer Type	Small Networks	Small Networks
Recommended Number of Concurrent Users	1-15	10-30
AV Throughput	31 Mbps	45 Mbps
Stateful Packet Inspection Firewall Throughput	133 Mbps	153 Mbps
IPS Throughput	TBD	TBD
VPN Throughput	TBD	TBD
Concurrent Sessions	8,000	20,000
VLANs	4,096	4,096
CONTENT SECURITY		
Web (HTTP, HTTPS, FTP)	●	●
Email (SMTP, POP3, IMAP)	●	●
Stream Scanning	●	●
Inbound and Outbound Inspection	●	●
Intrusion Detection & Prevention	●	●
Signature-Less Zero Hour Protection	●	●
Malware Signatures	600,000	600,000
Automatic Signature Updates	Hourly	Hourly
True HTTPS Scanning and Filtering	●	●
Web Content Filters	Filter By: HTML Body Keywords, File Extension	

MODEL	UTM10	UTM25
Web Object Filters	ActiveX, Java™, Flash, JavaScript™, Proxy, Cookies	
Email Content Filters	Filter By: Subject Keywords, Password-protected Attachments, File Extension, File Name	
Distributed Spam Analysis	●	●
Anti-spam Real-time Blacklist (RBL)		
User-defined Spam Allowed/Block Lists	Filter By: Sender Email Address, Domain, IP Address, Recipient Email Address, Domain	
Distributed Web Analysis w/ 64 categories	●	●
Instant Messaging (IM) Control	MSN® Messenger, Yahoo!® Messenger, Skype, mIRC, Google Talk	
Peer to Peer (P2P) Control	BitTorrent™, eDonkey, Gnutella	
Maximum Number of Users	Unlimited	
FIREWALL FEATURES		
Stateful Packet Inspection (SPI)	Port/Service Blocking, Denial-of-service (DoS) Prevention, Stealth Mode, Block TCP Flood, Block UDP Flood, WAN/LAN Ping Response Control	
WAN Modes	NAT, Classical Routing	
ISP Address Assignment	DHCP, Static IP Assignment, PPPoE, PPTP	
NAT Modes	1-1 NAT, PAT	
Routing	Static, Dynamic, RIPv1, RIPv2	
VoIP	SIP ALG	
DDNS	DynDNS.org, TZO.com, Oray.net	
Firewall Functions	Port Range Forwarding, Port Triggering, DNS proxy, MAC Address Cloning/spoofing, Network Time Protocol NTP Support, Diagnostic Tools (ping, DNS lookup, trace route, other), Auto-Uplink on Switch Ports, L3 Quality of Service (QoS) ,LAN-to-WAN and WAN-to-LAN (ToS)	
DHCP	DHCP Server, DHCP Relay	
User Authentication	Active Directory, LDAP, Radius, Local User Database	
PCI Compliance Two Factor Authentication Support	●	●
VPN		
Site to Site VPN Tunnels	10	25
SSL VPN for Remote Access	5	13
IPsec Encryption Algorithm	DES, 3DES, AES(128,192,256 bit)	
IPsec Authentication Algorithm	SHA-1, MD5	
Key Exchange	IKE, Manual Key, Pre-Shared Key, PKI, X.500	
IPsec NAT Traversal	●	●
SSL Version Support	SSLv3, TLS1.0	
SSL Encryption Support	DES, 3DES, ARC4, AES(128,256 bit)	
SSL Message Integrity	MD5, SHA-1, MAC-MD5/SHA-1, HMAC-MD5/SHA-1	
SSL Certificate Support	RSA, Diffie-Hellman, Self	
SSL VPN Platforms Supported	Windows 2000 / XP / Vista®, Mac® OS X 10.4+	
DEPLOYMENT		
VLAN Support	●	●
Dual-WAN Fail-over	●	●
Intelligent Traffic Load Balancing Based on Traffic Byte Count		●
Configuration Wizards	Setup, IPsec VPN, SSL VPN	
LOGGING AND REPORTING		
Management	HTTP/HTTPS, SNMP v2c	
Reporting	Summary Statistics, Graphical Reporting, Automatic Outbreak Alerts, Automatic Malware Notifications, System Notifications	

NETGEAR®

350 E Plumeria Dr
San Jose, CA 95134 USA
1-888-NETGEAR (638-4327)
E-mail: info@NETGEAR.com
www.NETGEAR.com