NETGEAR® ProSecure®UTM Series Unified Threat Management Appliance Reviewer's Guide

Table of Contents

NETGEAR® Contact Info

If you have any questions or technical issues, please contact your assigned NETGEAR® contacts listed below.

Peter Chen
Technical Marketing Engineer
(408) 890-3182
(408) 921-1689
Peter.Chen@netgear.com

Before You Start

Prior to any testing, please make sure the UTM is registered and running the latest firmware by following the directions outlined in the Testing & Deployment section.

Product Category

Switches	Wireless	Storage	**Security**

Product Description

Thank you for taking the time to evaluate the NETGEAR® ProSecure® UTM line of Unified Threat Management appliances. The UTM is a reliable, affordable, and simple all-in-one next generation firewall which provides small businesses with an array of security layers such as application control firewall, anti-virus, Web filtering, anti-spam, SPI firewall, IPS, and IPSec and SSL VPN.

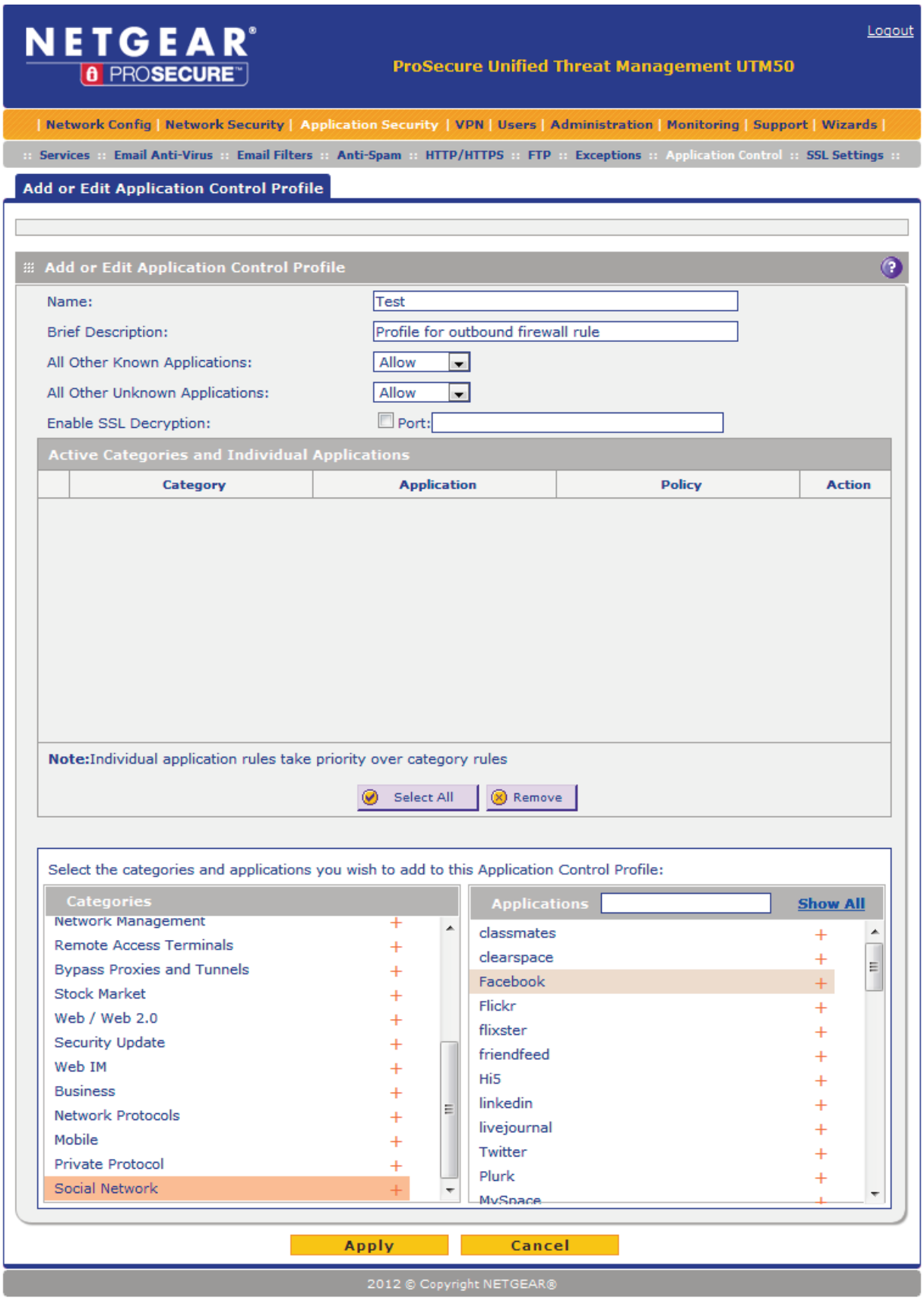
- **Reliable** – Stops more threats than the competition
  – Lifetime Warranty
- **Affordable** – More threats stopped per $ than other competitors
  – Premium anti-spam, 24x7 support, SSL VPN all included in bundle
- **Simple** – Purposely designed to make a sophisticated solution easy to deploy and manage

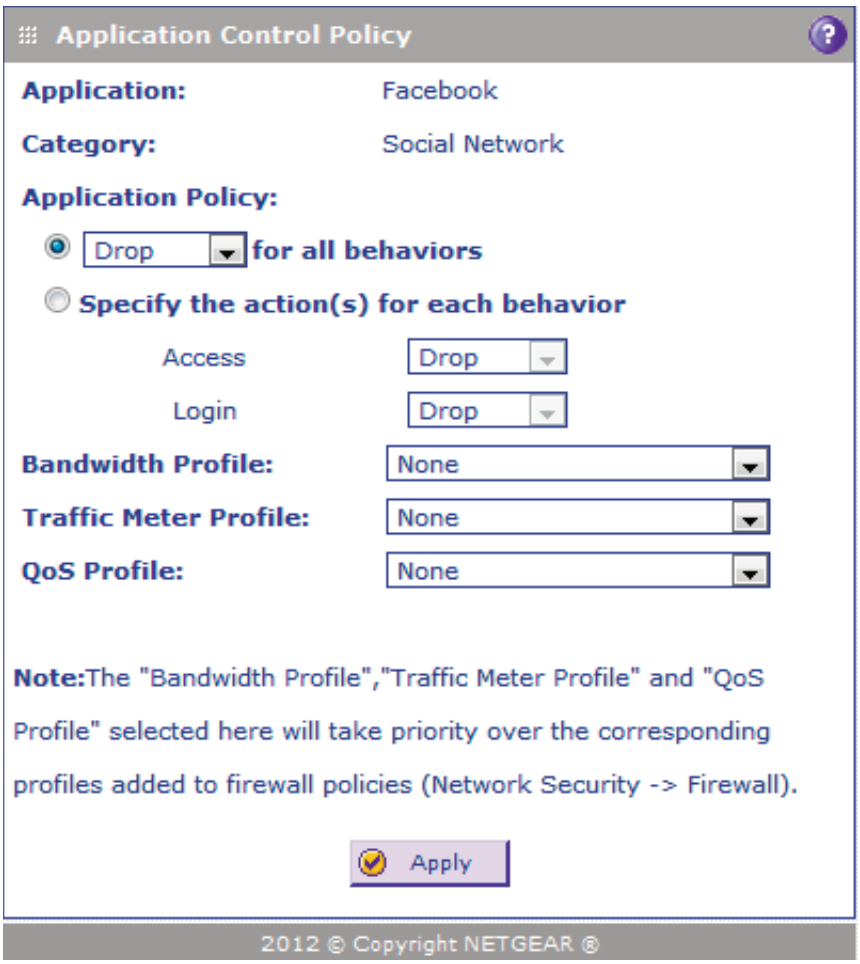
What's New

We are always working on adding new useful features to our products. Below is a list of recently added features to the UTM line. Be sure to take these features into consideration during the review.

- **UTM25S** – The UTM25S is the follow up to the award winning UTM9S which was the industry's first modular UTM for the SMB market. It features a flexible modular slot system where customers can easily install different modules to adapt to different network connectivity requirements. For example, if the customer needs wireless, they can simply install the UTM wireless-N module. If the customer needs DSL, they can also easily install the UTM DSL module. Installation typically takes less than 2 minutes. The UTM25S has two slots which supports up to two simultaneous installed modules.

- **Advanced Application Control Firewall** – Traditional firewalls can only block/accept traffic based on IP addresses and ports and offer little protection outside of that. This approach is quickly becoming obsolete in today's Internet where many applications send/receive traffic over ports that are typically allowed by traditional firewalls. The built-in application firewall of the UTM overcomes the limitations of yesterday's firewall and allows the UTM to monitor, control, and block hundreds of applications such as Skype, Facebook, BitTorrent®, and Yahoo! Messenger, helping enhance employee productivity and enforce network usage policies.

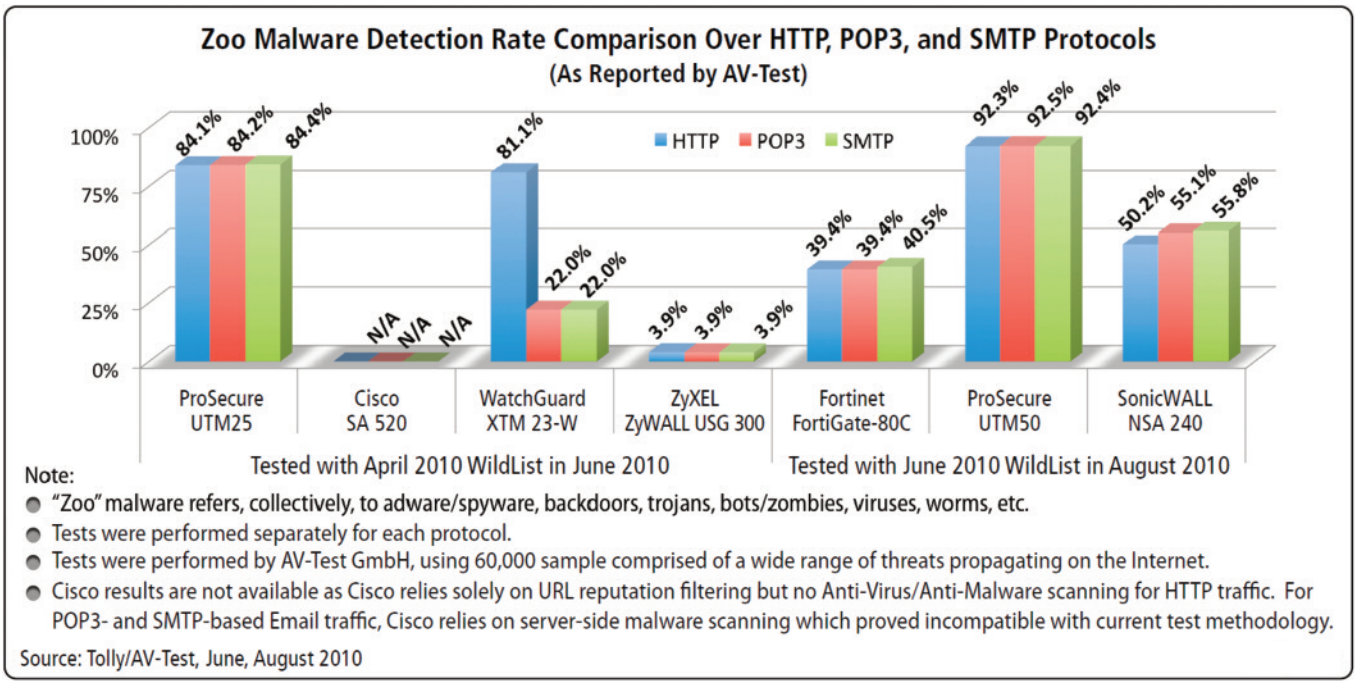

NETGEAR
PROSECURE
Logout
ProSecure Unified Threat Management UTM50
| Network Config | Network Security | Application Security | VPN | Users | Administration | Monitoring | Support | Wizards |
:: Services :: Email Anti-Virus :: Email Filters :: Anti-Spam :: HTTP/HTTPS :: FTP :: Exceptions :: Application Control :: SSL Settings ::
Add or Edit Application Control Profile
Add or Edit Application Control Profile
Name:
Test
Brief Description:
Profile for outbound firewall rule
All Other Known Applications:
Allow
All Other Unknown Applications:
Allow
Enable SSL Decryption:
Port:
Active Categories and Individual Applications
Category
Application
Policy
Action
Note:Individual application rules take priority over category rules
Select All
Remove
Select the categories and applications you wish to add to this Application Control Profile:
Categories
Network Management
Remote Access Terminals
Bypass Proxies and Tunnels
Stock Market
Web / Web 2.0
Security Update
Web IM
Business
Network Protocols
Mobile
Private Protocol
Social Network
Applications
Show All
classmates
clearspace
Facebook
Flickr
flixster
friendfeed
Hi5
linkedin
livejournal
Twitter
Plurk
MySpace
Apply
Cancel
2012 © Copyright NETGEAR®



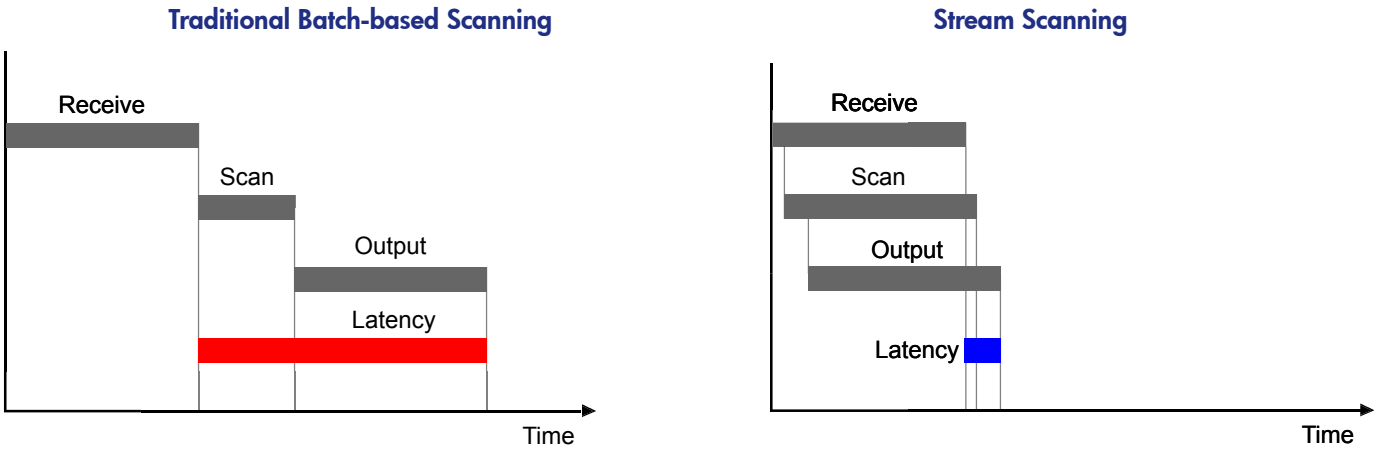
Product Highlights

Key Features	Benefits
Advanced Application Control Firewall	Monitor, control, and block hundreds applications such as Skype, Facebook, and BitTorrent with the UTM application firewall.
Best of breed Sophos™ virus engine with over 1.2 million malware signatures	Up to 400x the coverage of traditional all-in-one solutions
Patented Stream Scanning Technology	High throughput, low latency scanning
ReadyNAS Integration	Use the NETGEAR ReadyNAS to store logs and quarantined files from the UTM
Hybrid In-the-Cloud anti-spam	Requires no "tuning" to work, high accuracy, minimal false positives
Hybrid In-the-Cloud 64 category Web filter	Hundreds of millions of categorized URLs
Zero hour threat protection	Stops unknown threats in real time
Robust stateful inspection firewall and IPS	Prevent hackers and other network based attacks
IPSec, SSL, PPTP, L2TP VPN	Many options for secure remote access

- **Best-of-breed Virus Detection Partnered with Sophos** – The NETGEAR ProSecure UTM features a full enterprise grade anti-malware engine with advanced scanning algorithms and a signature library of over 1.2 million malware signatures – up to 400x the virus and malware coverage of other all-in-one solutions. Below are the results of an anti-malware shootout between mid-market all-in-one security appliances performed by AV-Test GmbH in 2010.



- **NETGEAR Patented[1] Stream Scanning** – This is based on the simple observation that network traffic travels in streams. The UTM scan engine starts receiving and analyzing traffic as the stream enters the network while at the same time another thread starts outputting the data already scanned data. The UTM's multi-threaded approach, in which the receiving, scanning, and outputting processes occur concurrently, ensures that network performance is not impeded. The result is that the time to scan a file is up to many times faster than traditional AV solutions - a performance advantage that is easily noticeable to the end-user. The technology also enables organizations to withstand massive spikes in traffic, as in the event of a malware outbreak.



[1] U.S. Patent No. 7,971,254

Models

	UTM5	UTM9S	UTM10	UTM25	UTM25S	UTM50	UTM150
Number of Concurrent Users	1-5	1-15	1-15	1-30	1-30	1-60	1-150
Concurrent Connections	12000	16000	16000	40000	40000	40000	65000
Maximum Firewall Throughput	500 Mbps	933 Mbps	566 Mbps	700 Mbps	980 Mbps	980 Mbps	980 Mbps
Application Firewall Throughput	400 Mbps	900 Mbps	450 Mbps	630 Mbps	905 Mbps	905 Mbps	940 Mbps
Anti-virus Throughput	20 Mbps	23 Mbps	23 Mbps	25 Mbps	30 Mbps	42 Mbps	110 Mbps
IPS Throughput	130 Mbps	172 Mbps	150 Mbps	200 Mbps	240 Mbps	320 Mbps	620 Mbps
WAN Ports (Gigabit)	1	2	1	2	2	2	4
LAN Ports (Gigabit)	4	4	4	4	4	6	4
Flash Memory/RAM	2GB/512MB	2GB/512MB	2GB/512MB	2GB/1GB	2GB/1GB	2GB/1GB	2GB/1GB
Module Slots	0	2	0	0	2	0	0

For more information about sizing in deployments, go to:
http://prosecure.netgear.com/products/prosecure-utm-series.php#guidelines

Support and Maintenance Options

Global Malware Support

- Comprehensive signature library consisting of over 1 million malware signatures
- Dual anti-malware scan engines
- Worldwide malware activity monitored, new malware threats researched
- Automatic daily and emergency malware signature updates: malware signatures are automatically updated

Technical Support

- 24x7 live telephone and email support
- Next business day Advanced Replacement
- Virtual on-site support
- Automatic software product updates and upgrades

Certifications & Technology Partners

Certifications	Technology Partners	
VPNC CERTIFIED Basic Interop AES Interop ICSA labs CERTIFIED ANTI-VIRUS	SOPHOS	Anti-virus
	mailshell™	Anti-spam
	commtouch®	URL Filtering

Testing & Deployment

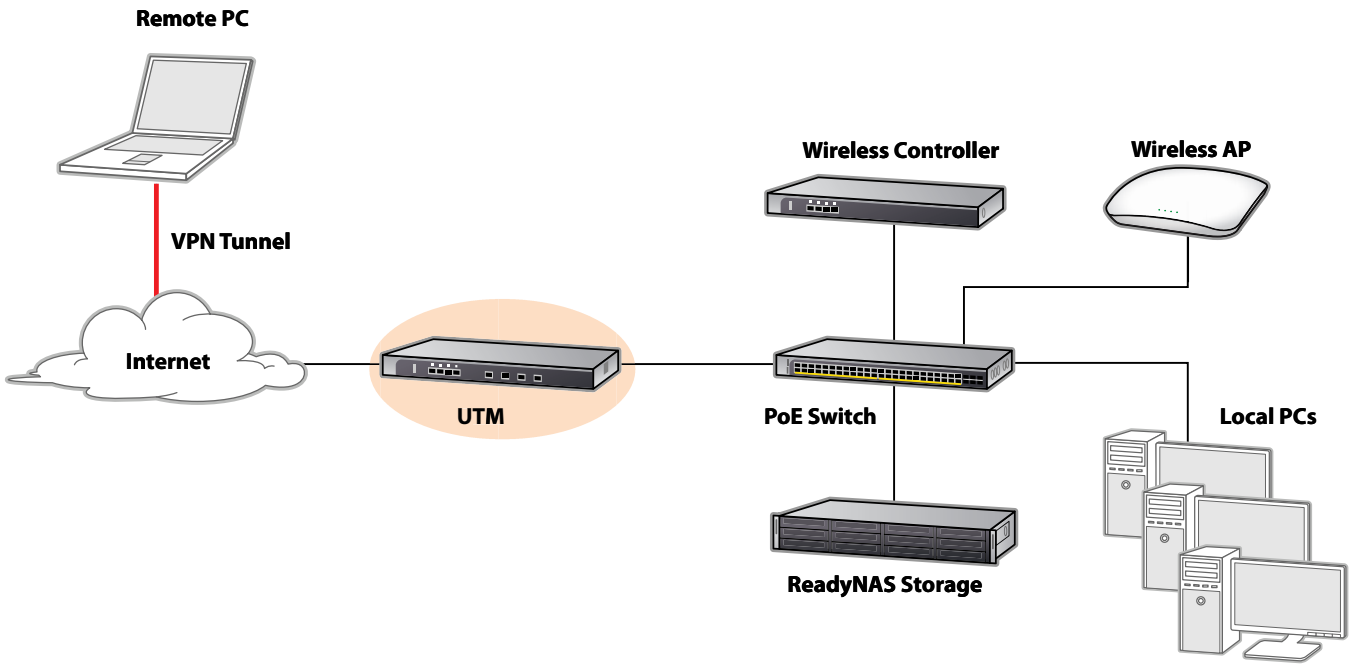
Note: Please make sure the UTM is able to access the Internet and is registered and has the latest firmware before testing.
To Register: Login to the UTM web GUI and go to Support -> Registration and click "Register".
To Update Firmware: Login to the UTM web GUI and go to Administration -> System Update -> Firmware

1. Make sure the UTM is connected to the Internet and is registered.
2. Click on **Query** and a list of available firmware will be displayed. The newest one is displayed at the bottom.
3. Select the firmware you wish to download and click **Download**.
4. Once the download is complete click **Install Downloaded Firmware**.
5. Once the installation is complete, the new firmware will show up in the **Firmware Reboot** section as the secondary firmware. Under **Activation**, select the new firmware and click **Reboot**.
6. The UTM will now boot into the new firmware.

   For complete step by step instructions on how to upgrade firmware please refer to the UTM Reference Manual or go to the following link (simple registration required):
   http://forums.prosecure.netgear.com/showthread.php?t=300

Where to Install the UTM

The UTM is situated between an organization's internal network and the Internet. The UTM acts as a stateful packet inspection firewall, keeping track of TCP connection state for every connection that is maintained through the UTM. The UTM also inspects layer 4-7 traffic for applications, malware, spam, and unwanted URLs.

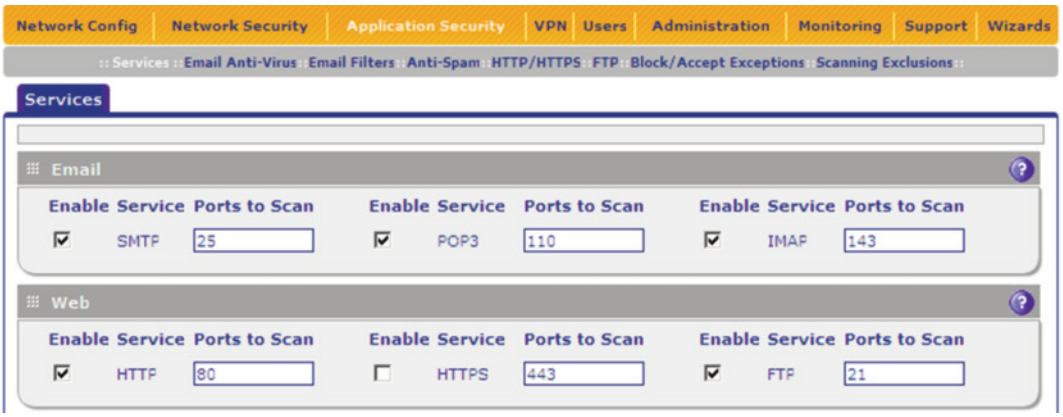


Connect the UTM to Your Network

For detailed instructions on the installation steps, please reference the **UTM Installation Guide** included in the box.

Testing the UTM Malware Scanning Features

1. Configure the UTM according to the **UTM Installation Guide**.
2. Make sure the licenses are activated (**Support -> Registration**).
3. Make sure HTTP scanning is enabled (**Application Security -> Services**).



4. While behind the UTM, go to http://www.eicar.org/85-0-Download.html

IMPORTANT NOTE
EICAR cannot be held responsible when these files or your AV scanner in combination with these files cause any damage to your computer. **YOU DOWNLOAD THESE FILES AT YOUR OWN RISK.** Download these files only if you are sufficiently secure in the usage of your AV scanner. EICAR cannot and will not provide any help to remove these files from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

Download area using the standard protocol http

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

Download area using the secure, SSL enabled protocol https

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

5. Click on each of the links in the **Download area using the standard protocol http** section. This tests to see if the UTM anti-malware engine supports the scanning of each of these file types. The **eicar_com.zip** and **eicarcom2.zip** files test the support of scanning compressed files.
6. Verify that each link is detected by the UTM as malware.
7. If you wish to test the files in the **Download area using the secure, SSL enabled protocol https** section, be sure to enable HTTPS scanning on the UTM from the management Web GUI. For instructions on how to configure HTTPS scanning for maximum transparency, please refer to the **UTM Reference Manual**.
8. If you wish to test the UTM against real malware, please do so in an isolated environment.

Note: The UTM has a scan exception threshold. Any file over the threshold will not be scanned. The default scan threshold is 2 Megabytes, and the maximum scan threshold is 10 Megabytes.

NETGEAR® Inc.
350 E. Plumeria Drive
San Jose, California 95134
Telephone: (408) 907-8000
Fax: (408) 907-8097

sales@netgear.com
www.netgear.com

NETGEAR®
Connect with Innovation™