

Threat Management Gateway Appliance

Integrated Enterprise and Branch Office Security Gateway

- Cost-effective, high performance Unified-Threat-Management security appliance platform
- Firewall, IPS, remote access, Web caching, secure application publishing, URL and anti-malware filtering and Email protection functionalities
- Comprehensive branch-office infrastructure manageability



- nAppliance Net-Gateway nTMGE network security appliance delivers comprehensive, multi-layered defense against threats to networks and Microsoft applications, content acceleration, intuitive management, and scalability - fully integrated, with turnkey "out of the box" convenience.
- At the heart of the nTMGE is Microsoft Forefront Edge TMG 2010 Enterprise Edition, an advanced Stateful packet and application-layer inspection firewall, virtual private network (VPN) and a Web cache solution that enables all size enterprise customers with branch offices to easily maximize existing information technology (IT) investments by improving network security and performance with seamless Active Directory Service (ADS) Support.

nTMGE Turn-Key Appliance Platform Highlights

- Integrated Enterprise Gateway Security solution for businesses of all sizes
- Four Models to choose from
- Maximum Reliability through Redundant Hotswap Disks and PS Modules
- Large Network Port Density & Remote KVM Support
- Oneface™ Appliance Management System
- Powered by Forefront Threat Management Gateway 2010 – Enterprise Edition

UTM Security: Microsoft Forefront Threat Management Gateway (TMG)

Firewall | IPS | VPN | Caching | Web-Publishing | Proxy | Web-Filtering | Anti-Virus | Anti-Spyware | Anti-Spam

Remote Access Gateway	Branch Office Gateway	Secure Web Gateway	Secure Messaging Email Gateway	Add-On Security Integration
<ul style="list-style-type: none"> • Dial-in VPN • Site-Site VPN • Secure Web Publishing • Multi-Factor Auth* 	<ul style="list-style-type: none"> • Site-Site Connectivity • Intelligent Caching • Bandwidth Optimization • Central Management 	<ul style="list-style-type: none"> • Anti-Spyware • Web Anti-Virus • URL Filtering • HTTPS Inspection 	<ul style="list-style-type: none"> • Anti-Spam • Anti-Virus • Email Filtering • Data Loss Prevention 	<ul style="list-style-type: none"> • WAN Optimization • Multi-Factor Auth • Single Sign-On • Remote Access Control

1 Multi-Layer Stateful Firewall Support:

- Offers all three functionality, packet-filtering, stateful filtering and deep application-level content filtering
- Stateful filtering supports dynamic packet filtering which opens ports only when necessary, it examine data crossing the firewall in the context of its protocol and the state of the connection and protect against number of sub-application layer attacks, such as session hijacking
- Flood resiliency feature protect from being permanently unavailable, compromised, or unmanageable during a flood attack

2 Smart Application-Layer Firewall Support:

- Full featured application aware firewall comprehensively helps protect from both external and internal threats. It performs deep inspection of Internet protocols such as HTTP, FTP, SMTP, streaming media applications, H.323, IDS, RPC, SOCKS and Web Proxy filters which enables it to detect many threats that traditional firewalls cannot detect

3 VPN – Secure Remote Client Access and Regional Office Connectivity:

- Integrated VPN client access Integrated based on Windows Server 2008 functionality
- VPN Client stateful filtering, deep inspection and quarantine, helping protect networks from attacks that enter through a VPN connection
- Site-Site IPSec Connectivity between two separate offices, stateful filtering and inspection of remote office resource access

4 Securely Publish Business Application for Remote Access:

- Secure access to remote users outside the corporate network, protects web application behind the firewall such as Web Servers, Share-Point Portal, IIS, E-mail server applications like "outlook anywhere" access to Exchange using Outlook Web and Mobile Access (OWA/OMA), Active Sync and RPC over HTTPS.

5 High Performance Web Caching and Bandwidth Optimization:

- Increased web performance with accelerated web caching
- Active content caching of popular content, content distribution and mirroring, and scheduled content download.

6 Secure Web and Messaging Protection:

- URL filtering for compliance with corporate policy
- Preventing malware outbreaks caused by inadvertent employee visits to malicious sites or by downloads of infected files.
- Preventing the latest viruses, spam, worms, and inappropriate content from reaching inboxes with e-mail protection at the network perimeter.

7 Monitoring, Logging and Reporting:

- Monitoring tools to help track network status create alerts to get status on firewall behavior, configure and view logs graphically to track TMG activity, and create reports to customize and summarize log information.
- Supports standard data formats such as W3C and ODBC



Secure Web Gateway for Corporate Networks

Microsoft® Forefront™ Threat Management Gateway 2010 is a secure Web gateway that enables employees to use the Internet safely and productively without worrying about malware and other threats. To help block the latest Web-based threats, it provides multiple layers of continuously updated protections including URL filtering, malware inspection, and intrusion prevention.

Better Protection Against Web-Based Threats

Forefront TMG 2010 protects employees from Web-based threats by integrating multiple layers of security into an easy-to-manage solution. Deployed on corporate networks as a unified gateway, Forefront TMG 2010 inspects Web traffic at the network, application, and content layers to help ensure a single, consistent Web policy. In addition to comprehensive protection, it also helps improve firewall performance by offloading processor-intensive functions like inspection for malware.

The secure Web gateway solution includes four components:

- The Forefront TMG 2010 server, which provides multiple inspection technologies, including application- and network-layer firewall, intrusion prevention, and malware filtering to keep users safe from Web-based attacks. It connects to the Forefront TMG Web Protection Service* for URL filtering and anti-malware updates. Forefront TMG Web Protection Service, which delivers anti-malware updates and provides a real-time connection to cloud-based URL filtering technologies that can be used to monitor or block employee Web usage.
- The management console, which offers both local and remote policy management for servers.
- A management server (included with Forefront TMG Enterprise Edition), which enables the creation of enterprise-wide policies that can be assigned to an array of servers.
- Forefront TMG 2010 can scale performance when administrators cluster multiple gateways or deploy Forefront TMG 2010 at individual sites.

Forefront Threat Management Gateway (TMG) 2010 is designed to increase the security of corporate Web usage by:

- Preventing malware outbreaks caused by inadvertent employee visits to malicious sites or by downloads of infected files.
- Enforcing a consistent Web security policy for application protection, malware inspection, and URL filtering through integration with Forefront TMG Web

Unified Web Security Interface: Single interface for managing Web security policy

Key Features and Benefits

Forefront nTMG delivers comprehensive protection against Web-based threats, integrated into a unified gateway that reduces the cost and simplifies the complexity of Web security.

Comprehensive Protection:

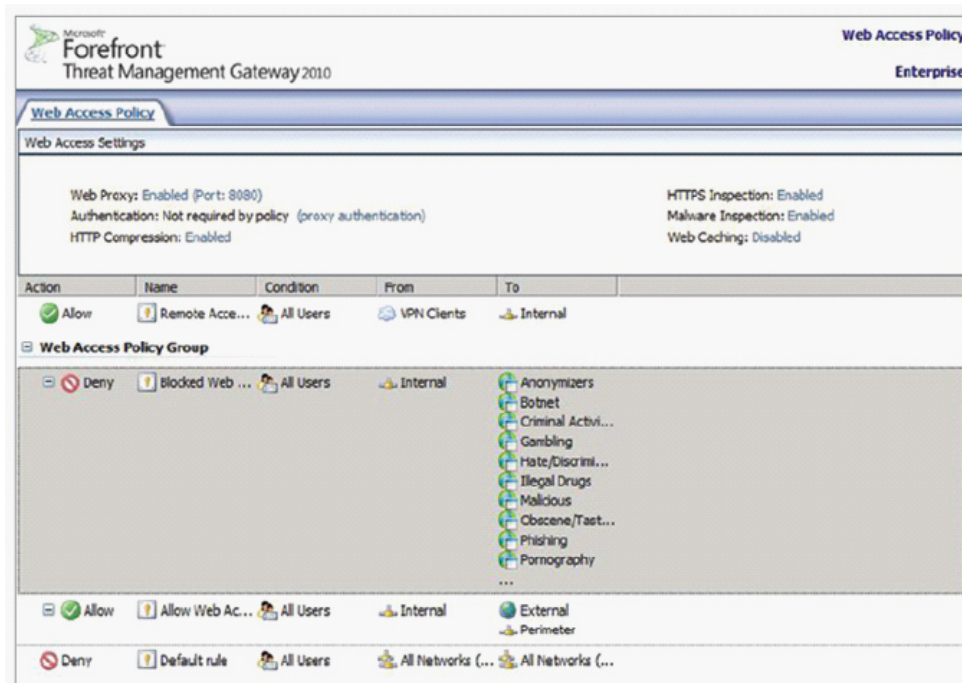
- Blocks malicious sites more effectively
- Prevents Exploitation of vulnerabilities
- Catches Web-based malware
- Delivers core network protection features
- Extends enforcement to encrypted web-traffic

Integrated Security:

- Delivers a single source for web security
- Reduces Costs
- Leverages existing infrastructure investments

Simplified management:

- Centralizes management in a single, easy-to-use console
- Delivers comprehensive custom reports



- Four Models to choose from, custom-built for Enterprise-Wide Branch Office deployments
- Redundant Hotswap Disks and Power Supply Modules
- Large Network Port Density & Remote KVM Support
- Built-in Dual Node High Availability NLB Support
- Powered by Microsoft Forefront TMG 2010 – Branch Edition

nTMGB Series Gateway
Connecting & Securing
Your Branch Offices



Branch Office Gateway

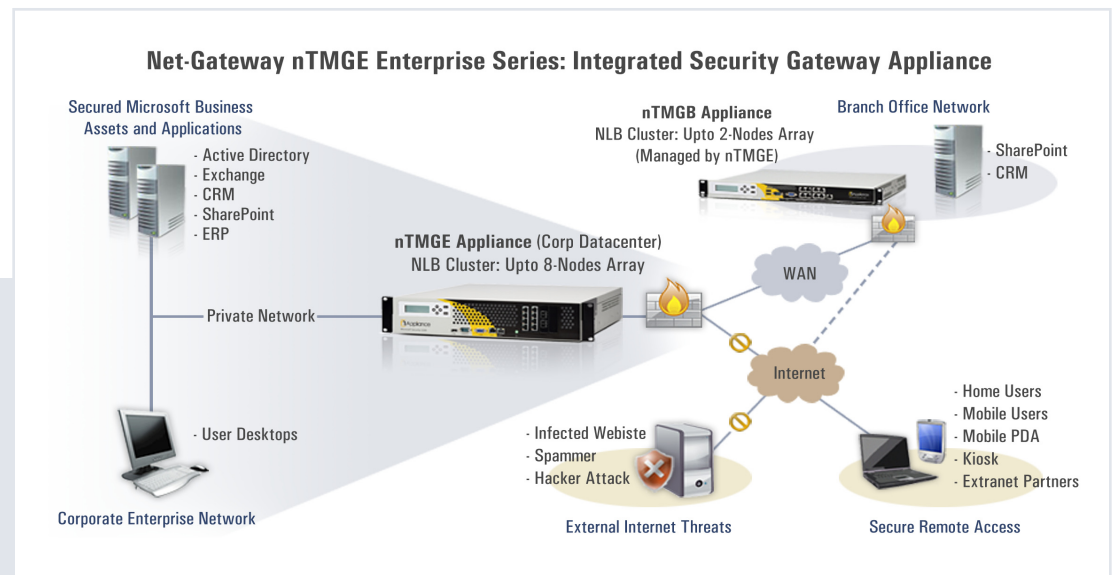
- ✓ Site-Site Connectivity
- ✓ Intelligent Caching
- ✓ Bandwidth Optimization
- ✓ Central Management

nTMGB Series: Secure Branch Office Gateway

Helps connect remote-site branch offices to their corporate headquarters

Organizations can use nTMGB series appliance to connect to and secure their branch offices, while efficiently utilizing network bandwidth. By providing HTTP compression, caching of content (including software updates), and site-to-site virtual private network (VPN) capabilities integrated with application-layer filtering

Net-Gateway nTMGE Enterprise Series: Integrated Security Gateway Appliance



Deployment Scenarios:

The nAppliance nTMGB is a fully integrated branch office security gateway appliance, it is easy to deploy with out-of-box turnkey convenience which includes:

1 Connect and Secure Branch Offices Network Infrastructure

Robust way to securely expand corporate networks while reducing network costs by leveraging existing network connections. Secure Site-Site Connectivity to nTMGE gateway appliance located at main corporate datacenter through site-to-site VPN and firewalling, and remote access VPN for users to connect to their branch office network while working from home or on business trips.

2 Simplified Branch Office Deployment and Efficient Management via EMS Console from Central Location

Unattended Deployment at Remote Office: Easy deployment at branch office and remote locations without the need of local IT staff to setup the firewall or VPN.

Efficient Management of Remote

Office Security Infrastructure:

Automatically propagate enterprise security policy from central office to branch office. Helps secure remote management of firewall and web cache services.

3 Intelligent Content Caching and Acceleration

- Branch Office Desktop Updates: BITS caching and scheduling help accelerate the deployment of software updates and keep remote computers protected. Active enterprise-wide BITS content caching, software update caching and scheduling helps keep remote computers protected and enhance bandwidth efficiency.

- Web Page Caching: HTTP traffic compression and caching improves web page load times and reduces WAN costs for users in branch offices.
- Active enterprise-wide distributed Caching: Integrated web caching in corporate data centers, cache server array functionality, and distributed caching helps increase network performance and optimize branch office content delivery

Add-On Security Integration

- ✓ WAN Optimization
- ✓ Multi-Factor Authentication
- ✓ Single Sign-On
- ✓ Remote Access Control

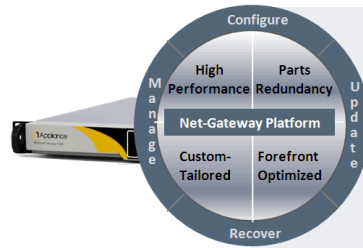
3rd Party Add-On Integration:

Offers Comprehensive ISV security application support

nAppliance Forefront appliance platforms are purpose-built, high performance hardware devices integrated with nAppliance designed Oneface™ system management tools and Microsoft Forefront Edge Security Software Solutions.

nAppliance Forefront Security products are pre-integrated with a number of additional industry leading and useful 3rd party security software modules to greatly increase the capabilities of

TOTAL SECURITY: Purpose-Built, Microsoft Forefront TMG Optimized Appliance



Oneface® Appliance Management System

Embedded Recovery Manager

Embedded Lights-Out Manager

Embedded LCD Manager

Integrated Windows System Manager

- HA and Fail-Over
- Backup/Snapshot
- Security Manager
- Component Manager
- Update Manager
- Configuration Manager
- SNMP Agents

Forefront Optimized

"Turn-Key" Appliance Platform

nAppliance Forefront appliance platforms are purpose-built, high performance hardware devices integrated with nAppliance designed Oneface system management tools and Microsoft Forefront Edge Security Software Solutions.

each of the appliance. These optional-packages are tested, pre-load and made available as an install options for your convince. Customers can choose needed optional-packages for installation manually and purchase a software license for activation. All security software application packages run on a hardened operating system, securely managed and updated via ONEface, the nAppliance appliance management services interface.

"Best-of-the-Breed" ISV Add-On Security Application Support. These 3rd party add-ons include QoS, Bandwidth and WAN Optimization, Content Management, Multi-Factor Authentication, Single-Sign-On and Advance Reporting software components. nAppliance Component Manager, a MMC based snap-in tool allows the customers to add and remove additional components as desired.

Comprehensive ISV Support

nAppliance Integrated 3rd Party Security Components

- WAN Optimization
- QoS, Traffic Shaping
- Multi-Factor Authentication
- Single-Sign-On

Forefront Gateway Appliance Platform Benefits

- **Intelligent Application Gateway Platform.** Integrated appliance for network perimeter defense, remote access, application-layer protection, web content caching, email and web protection for Microsoft based Infrastructures
- **Centralized Policy Based Access Control.** Centralizes policy management, controlling access by protocol or application type and by user, group, roles, schedules, content type tied to Active Directory
- **Easy Windows MMC based Manageability.** Traditionally, enterprise-class firewalls have had a reputation for being difficult to learn, configure and maintain. Net-Gateway nTMGE series offers industry most advance feature and familiar windows interface and is the most complete product in its class
- **Lowest Total Cost of Ownership.** Exceptional ease of implementation enables IT leaders to be confident that their network, users, client devices, and application are protected with the leading Microsoft security appliance family celebrated for assured performance and lowest TCO
- **Centralized Appliance Management through ONEface™.** Our Intuitive Web GUI management tool offers easy network setup, configuration, backup/restore, updates, logging, reporting, 3rd party security applications add-on and centralized appliance management
- **Appliance Recovery and Remote Management (ARRMS™).** Our recovery system combined with advanced LCD functionality offers appliance recovery to factory defaults enables multiple system image copies backup to local disk or network, and instant restore to last good known state.
- **Superior Product Technology, Value and Support.** State of the art system and application integration, best price-to-performance-ratios in the industry, deployment assistance for Microsoft Forefront Gateway technologies, global technical support, efficient appliance life cycle management and upgrades, and above all future proofing with Microsoft security architecture.

Microsoft Forefront TMG Appliance Editions Comparison

	Business Standalone	Corporate Datacenter	Corporate Branch Office
Microsoft Forefront Threat Management Gateway 2010	TMG Standard Edition	TMG Enterprise Edition	TMG Branch-Office Edition
Deployment Type:			
Business Type	SMB	Enterprise	Branch Office
nAppliance Net-Gateway Platform Series	nTMG Series	nTMGE Series	nTMGB Series
Supported deployment scenarios	Standalone	Server in a standalone array or an array managed by EMS*	Server in a standalone array or an array managed by EMS*
High Availability:			
NLB Arrays for Load Balancing & Failover	No	✓	✓
Scale Out: Number of Supported TMG Server in Array	1	Unlimited	2
Non-domain joined gateway	✓	✓	✓
ISP Link redundancy	✓	✓	✓
Unified Threat Management Functionalities:			
Firewall - Stateful	✓	✓	✓
Firewall - Application Layer	✓	✓	✓
Network IPS (NIS)	✓	✓	✓
VPN (site-to-site and remote access)	✓	✓	✓
Web Proxy	✓	✓	✓
Web Publishing	✓	✓	✓
HTTPS inspection	✓	✓	✓
Caching, Cache Compression	✓	✓	✓
NLB Arrays for CARP Support	✓	✓	✓
Web Anti-Malware Protection**	✓	✓	✓
E-mail Protection***	✓	✓	✓
Configuration Storage Server (CSS)			
Local Management of Firewall Policies and Config Settings	✓	✓	✓
Remote Management of Firewall Policies and Config Settings		✓	
Enterprise Management: EMS for Centralized			
Management of Enterprise (nTMGE) Edition Gateways		✓	
Management of Branch (nTMGB) Edition Gateways*			✓
Management of Branch Standard (nTMG) Edition Gateway*	✓		
Type of Microsoft Forefront TMG Editions			
Scale Up: Processor Support	Standard Up to 4 CPU's	Enterprise Unlimited	Branch Office Up to 4 CPU's

* Requires at least one Enterprise Edition nTMGE appliance license, EMS: Enterprise Management Server; ** Requires subscription; *** Requires Exchange License

nAppliance delivers Integrated Appliance "Turnkey" Solutions:

nAppliance Networks, an ISO 9001:2000 is a provider of mission critical network edge security infrastructure provider. Unlike alternatives that are simply based on general-purpose server hardware, our appliances are designed for highest reliability, optimized for maximum performance, and manufactured to exact quality specifications. Trust nAppliance Net-Gateway Forefront appliance series to deliver reliable and comprehensive solutions.



nAppliance Networks, Inc.

540 Dado Street, San Jose, CA 95131, USA

Phone: 1-408-895-5000 (Local) 1-877-895-nAPP (6277) (US-Toll Free) 011-408-895-5000 (International)

Fax: 1-408-943-8222/8101 Email: info@nappliance.com Website: http://www.nappliance.com