

NetScaler: A comprehensive replacement for Microsoft Forefront Threat Management Gateway



Microsoft's Forefront Threat Management Gateway (TMG) is a network security and protection solution for enterprise users. It has traditionally been a key component of various Microsoft application deployments including Lync, SharePoint and Exchange. A principle benefit of TMG has been that it offers customers a way of publishing and protecting workload servers-particularly in Internet facing scenarios. In these environments a clean separation between the Internet and critical datacenter infrastructure is required.

TMG provides this capability through an integrated solution featuring threat protection technologies including URL filtering, HTTPS inspection, malware protection, and signature-based detection of known operating system and application vulnerabilities. Advantages of a TMG deployment include:

- Secured access to approved content
- Enhanced enterprise network security
- Lowered liability risk by content based filtering

With Microsoft's announcement that the TMG family of products are end-of-sale Citrix recommends the use of NetScaler application delivery controllers as a replacement. NetScaler provides all the feature and benefits of TMG plus much more. NetScaler is also deployed in a similar manner within the network for ease-of-installation.

TMG features

TMG protects employees from Web-based threats by integrating multiple layers of security into an easy-to-manage solution. It includes four components: "Forefront TMG Server", "TMG web protection service", "Management console" and "Management Server". It can be deployed in a "standard server" mode to maximise performance or as a "virtualized machine" to reduce hardware cost. Specific modules include:

- URL filtering
 - URL categorization, time based blocking, and report only mode

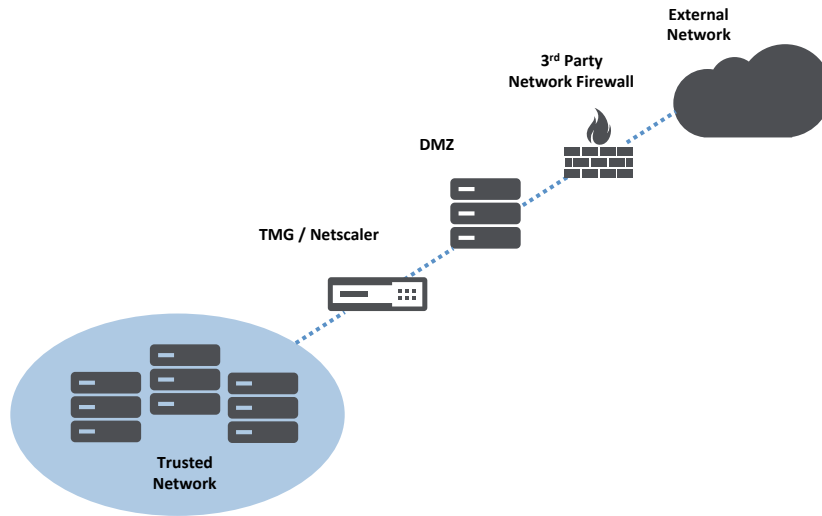
- HTTPS inspection
 - Offload SSL processing from application servers
 - Detection of possible malware and enforcement of corporate policies
 - Exclusion of specific sites
- Malware inspection
 - Inspects outbound web traffic including attachments and files
 - Enhanced user experience by the following delivery methods
 - Trickle - sends partial content to the user as the files are inspected.
 - Progress notification by sending status HTML page to client computer
- Network inspection system (NIS)
 - Based on protocol analysis, NIS enables the blocking of attacks while minimizing false positives
 - Automatic update of signature sets and engine
 - Granular control and policy configuration to comply with specific organization needs
- Caching
 - Centralized rule mechanism
 - Interoperability with Branch Cache solution
- Routing and remote access feature
 - Can act as a Router, Internet gateway, VPN server, NAT server, proxy server

Citrix NetScaler supports all these features and provides both physical hardware (MPX and SDX) as well as virtual appliance (VPX) solutions.

Deployment topologies

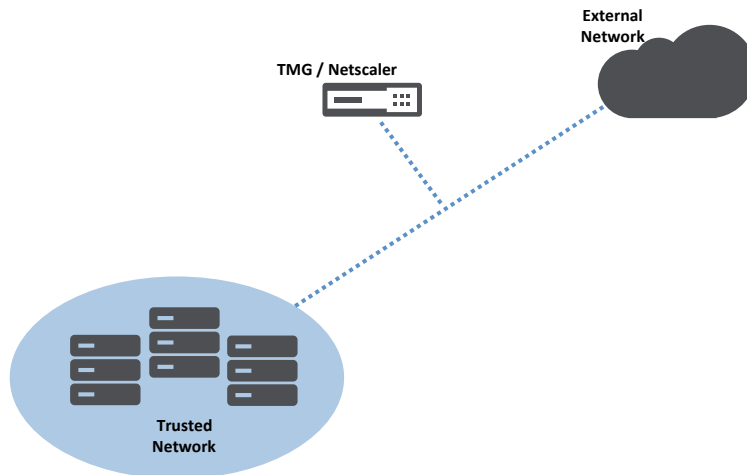
Microsoft TMG solutions are deployed in a variety of scenarios. The following methodologies are the most common. In each case, NetScaler is deployed in a like manner with straightforward installation and configuration.

- **Back Firewall:** TMG is located at the network's back end, and another network element, such as a perimeter network or an edge security device, is located between the Forefront TMG and the external network.



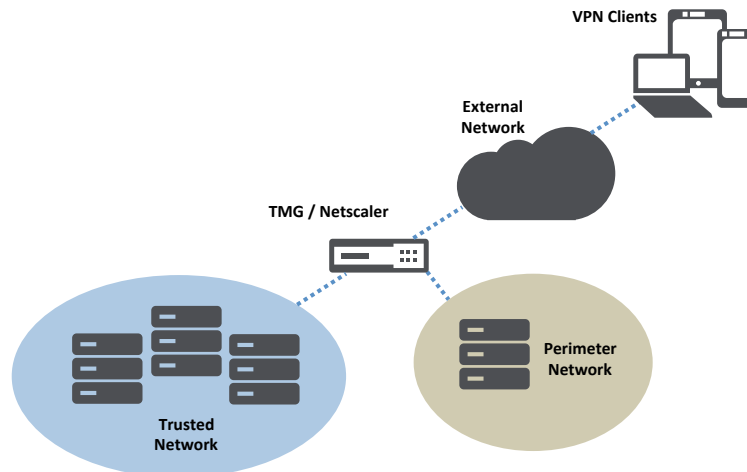
This is similar to the 'inline' mode for NetScaler deployments behind the edge firewall. This is the most common deployment for NetScaler.

- **Single network adapter:** TMG is connected to only one network, to either the internal network or a perimeter network. This topology gives limited functionality of Forefront TMG.



This is similar to the 'One-Arm' mode of NetScaler where traffic needs to be routed through the NetScaler appliance.

- **3-Leg perimeter:** This topology implements a perimeter network where TMG is connected to at least three physical networks.



This also is similar to 'One-Arm' deployment of NetScaler.

Citrix NetScaler: An ideal replacement for Microsoft TMG

NetScaler fulfils not only all the functionality in Forefront Threat Management Gateway, but adds many additional features to optimize, protect and scale web-based applications. One of the principle uses of NetScaler is to front-end applications such as Microsoft Lync, SharePoint and Exchange in enterprise data-centres of all sizes.

Citrix NetScaler is the most comprehensive Application Delivery Controller available. NetScaler not only includes all the capabilities of TMG but it is the most complete ADC on the market. NetScaler adds load balancing and Layer 4 connection management along with caching, compression, Layer 7 content optimization, content filtering, URL filtering, content rewrite, policy processing, application layer firewall, , network access control, SSL VPN and many other modules. NetScaler installations may start by replacing TMG features but the impact of NetScaler on application networking services has tremendous upside as additional features are utilized. NetScaler took the added step in supporting applications with the use of 'AppExpert Templates'; these are abstractions of application deployments through NetScaler. These predefined and freely available templates provide IT administrators with configurations that optimize the performance for a specific application.

NetScaler has been tested and validated with key Microsoft Apps including Exchange, Lync, and SharePoint and complete deployment guides are available. NetScaler has demonstrated proven secure access technology working in conjunction with extensive authentication, optimization and acceleration modules. With the broader set of application oriented features NetScaler is not just the best product available for replacement of TMG, but it provides additional value for Microsoft Apps and environments.

NetScaler: A superset of TMG

NetScaler provides all the features of Microsoft TMG and more. The following table provides a comparison of the principal TMG capabilities and NetScaler's support.

Feature Comparison

Feature	TMG	NetScaler
URL Filtering	Categorisation and other advanced feature	Advance Policy Infrastructure with Responder
HTTPS Inspection	Policy Based	SSL Offloading and Policies
Malware Inspection	Capable of scanning attachments	Application Firewall including XML and other attachments
Network Inspection System	Traffic inspection based on protocol analysis, update support	Application Firewall—signature based protection with automatic updates
Caching	Basic	AppCache – Static and dynamic caching
Routing and remote access	Basic	Static and Dynamic Routing with Secure remote access
Authentication	Basic, Form based, Certificate based	Basic (401+), Form Based, Certificate Based
Traffic Management	Basic, No Active Sync roaming	Advanced (HA, Scalable, Health Aware, GSLB), AAA for Traffic Management, content switching
L3-L7 Firewall	Basic	Advanced (ACL, DDOS), Network Firewall mode, Application Firewall f or L7, HTTP DoS Protection mode

Feature	TMG	NetScaler
Optimization (SSL offload, TCP optimization, Caching), Acceleration	No performance gain	Higher performance leads to better server use and much better optimization: SSL Offload TCP connection multiplexing HTTP optimization HTTP Caching HTTP Compression
IPV6	No Support	SLB64, SLB46, NAT64, NAT46, DNS64, End to End IPV6 support
Forward and reverse Web Proxy	Supports	Supports including all layer 7 processing (e.g., rewrite, responder)
VPN Server	Support	Full tunnel VPN, CVPN
Site to Site VPN	Support	Cloud Connector
SSL Bridging	Support	Support
Web App Firewall	Support	HTML, XML firewall
High Availability (HA)	Complex, require 3 Nodes	Active - Active, Active Passive, Cluster
Publishing Apps	Multi step process	Support of AppExpert Templates to publish application in most optimal way
Administration / Automation	No Automation mechanism	API support for third party integration, Command Centre for centralized administration

Deployment topology comparison

There are three main deployment options for TMG. NetScaler is used in an equivalent fashion for each scenario.

TMG	NetScaler
Back Firewall	In-Line
Single Network Adapter	One-Arm
3-Leg Perimeter	One-Arm

NetScaler Advantages

IT administrators can deploy NetScaler as a complete TMG replacement. NetScaler, installed with either the MPX/SDX physical or VPX virtual version has all the necessary features to fully ensure network security and provide protection to enterprise users. NetScaler goes much further and includes many more server availability, security, and application acceleration features in a single integrated appliance. When the administrator is ready, many more functional modules can be enabled to provide the most comprehensive application optimization solution available. NetScaler includes a greatly expanded list of core capabilities which can be utilized, one at a time or all at once. Unlike other ADC solutions, only NetScaler allows full simultaneous use of all features. With TriScale technology, NetScaler appliances scale in three dimensions for unprecedented growth for any environment. A partial list of features include:

- **IPv6 capabilities**
Transitioning and translation technologies to connect IPv6 and IPv4 networks
- **Dynamic Routing**
Support of key DR protocols like OSPF, BGP, RIP, IS-IS
- **Surge Protection**
Ability to protect backend App servers from traffic surge
- **HTTP Compression**
Compressing the HTTP payload to save bandwidth and faster response
- **Web 2.0 Push**
Enabling Web 2.0 app deployments and technologies
- **AAA-Traffic Management**
Enabling authentication, authorization and auditing for all kind of Apps
- **App Firewall**
Full blown Application firewall with HTML and XML payload protection
- **Rewrite**
Providing the ability of changing content of application request/response on fly
- **Advance health check**
Ensuring that backend apps are UP and working effectively
- **Global Server Load Balancing (GSLB)**
Ability to load balance globally dispersed application deployment
- **AppExpert Callout**
Excellent way to speak with external resources
- **DataStream**
Provides load balancing, optimization and connection multiplexing for SQL database servers

- **AppFlow**
The framework and protocol layer to export visibility information for L3 to L7
- **NetScaler Insight**
Module to consume and provide analytic reports on AppFlow info
- **Command Center**
Centralized monitoring and management solution
- **Platform**
Choice of platforms available in Virtual, Physical and Multi-tenant form
- **TriScale Technology**
Centralized NetScaler appliances “scale-up” to 5x performance with software license, “scale-in” with up to 80 NetScaler fully isolated instances on one appliance and “scale-out: with the clustering of up to 32 appliances in one system image.

Conclusion

Microsoft’s Forefront TMG has been a versatile device. It served as a web proxy, firewall, secure gateway, app publisher and more. While many solutions claim to replace TMG deployments in specific usage scenarios, only NetScaler can provide a comprehensive replacement solution. NetScaler goes beyond TMG for complete optimization of applications and provides superior application availability, acceleration and security.

Reference Deployment Guides

Citrix NetScaler Deployment Guide for Microsoft Exchange 2010

Microsoft SharePoint 2010 Citrix NetScaler Solution Guide

Microsoft Lync Server 2010 Citrix NetScaler Solution Guide

Deploying Citrix NetScaler DataStream in Microsoft SQL Server 2008 R2 Environments

How to allow Smart Access to Web Interface for SharePoint (WISP) with NetScaler

Configuring Kerberos Constrained Delegation on a NetScaler Appliance



Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix

Citrix (NASDAQ:CTXS) is the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was \$2.59 billion. Learn more at www.citrix.com.

Copyright © 2013 Citrix Systems, Inc. All rights reserved. Citrix, NetScaler, NetScaler SDX, MPX, VPX and TriScale are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.