This guide focuses on describing the configuration required on NetScaler SWG for replacement of a Microsoft TMG setup.
NetScaler is a world-class application delivery controller (ADC) with the proven ability to load balance, accelerate, optimize and secure enterprise applications.

The NetScaler SWG solution offers tools that enterprises can use to protect against internet threats, in addition to the functionality of a comprehensive SSL forward proxy and basic application delivery capabilities.

This deployment guide focuses on defining solutions for replacing Microsoft Forefront Threat Management Gateway (Forefront TMG) with Citrix NetScaler Secure Web Gateway (SWG) for various enterprise proxy, filtering and validation scenarios.

NetScaler is a world-class application delivery controller (ADC) with the proven ability to load balance, accelerate, optimize and secure enterprise applications. The NetScaler SWG solution offers tools that enterprises can use to protect against internet threats, in addition to the functionality of a comprehensive SSL forward proxy and basic application delivery capabilities.

Microsoft Forefront TMG, formerly known as Microsoft Internet Security and Acceleration Server (ISA Server), is a network router, firewall, antivirus program, VPN server and web cache from Microsoft Corporation. It runs on Windows Server 2008 and works by inspecting all network traffic that passes through it. On 9 September 2012, Microsoft announced no further development will take place on Forefront Threat Management Gateway 2010 and the product was no longer be available for purchase as of 1 December 2012. Mainstream support has ceased post 14 April 2015 and extended support will end on 14 April 2020.

Forefront TMG offers several useful network protection features, including:

• Routing and remote access features: Microsoft Forefront TMG can act as a router, an Internet gateway, a virtual private network (VPN) server, a network address translation (NAT) server or as a proxy server.
• Security features: Microsoft Forefront TMG is a firewall capable of inspecting network traffic (including web contents, secure web contents and emails) to filter out malware, security vulnerability exploit attempts and content filtering according to predefined security policies. Therefore, Microsoft Forefront TMG can provide application layer protection, stateful and content filtering and anti-malware protection.
• Network performance features: Microsoft Forefront TMG can help improve network performance with web traffic compression. Web caching allows caching of frequently-accessed web resources so they can be accessed faster. Microsoft Forefront TMG 2010 can also cache data received through Background Intelligent Transfer Service (BITS), such as Microsoft Updates.

In this guide, we will look to replicate TMG functionality for forward proxy scenarios with NetScaler SWG and then highlight the additional possibilities that NetScaler SWG enables.
The following TMG features will be replicated with NetScaler -

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sub-features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Forward Proxy</td>
<td>Secure Forward Proxy</td>
</tr>
<tr>
<td></td>
<td>URL Filtering</td>
</tr>
<tr>
<td></td>
<td>Traffic Visibility</td>
</tr>
<tr>
<td></td>
<td>Access Blocking</td>
</tr>
<tr>
<td></td>
<td>Content Control</td>
</tr>
</tbody>
</table>

Configuration Details

The test deployment topology is shown in Figure 1. This features a parallel setup for both TMG and NetScaler SWG.

Figure 1: Deployment Topology

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Forefront TMG</td>
<td>2010 SP1</td>
</tr>
<tr>
<td>NetScaler SWG</td>
<td>SWG - 12.0 51.24+ (Available on MPX and VPX)</td>
</tr>
</tbody>
</table>
About NetScaler SWG

The NetScaler SWG appliance acts as a clients’ proxy to connect to the internet and SaaS applications. Traffic is intercepted by the proxy to determine the traffic protocol. Unless the traffic is HTTP or SSL, it is forwarded to the destination as is. When the appliance receives a request from a client, it intercepts the request and performs some actions, such as user authentication, site categorization, and redirection. It uses policies to determine which traffic to allow and which traffic to block.

The appliance maintains two different sessions. One session is established between the client and the proxy and another session is established between the proxy and the origin server. The proxy relies on customer defined policies to allow or block HTTP and HTTPS traffic. Therefore, it is important that you define policies to bypass sensitive data, such as financial information or emails. The appliance offers a rich set of L4-L7 traffic attributes and user-identity attributes to create traffic management policies.

For SSL traffic, the proxy verifies the origin server’s certificate and establishes a legitimate connection with the server. It then emulates the server certificate, signs it using a CA certificate installed on NetScaler SWG, and presents the created server certificate to the client. You must add the CA certificate as a trusted certificate to the client’s browser in order for the SSL session to be successfully established.

The appliance supports transparent and explicit proxy modes. In explicit proxy mode, the clients must specify an IP address in their browsers, unless the organization pushes the setting onto the client’s device. This address is the IP address of a proxy server that is configured on the appliance. All client requests are sent to this IP address. For explicit proxy, you must configure a content switching virtual server of type PROXY and specify an IP address and a valid port number.

Transparent proxy, as the name implies, is transparent to the client. That is, the clients are not aware that a proxy server is mediating their requests. For transparent proxy, you must configure a content switching virtual server of type PROXY, with asterisks (**) as the IP address and port. When using the Secure Web Gateway wizard in the GUI, you do not have to specify an IP address and port.

Note: To intercept protocols other than HTTP and HTTPS in transparent proxy mode, you must add a listen policy and bind it to the proxy server.

Solution Description

There are multiple means of replacing the forward proxy functionality provided by TMG with NetScaler.

- For limited applications (without requiring authentication, policy driven access control or URL filtering and traffic inspection), a basic forward proxy can be implemented using the Cache Redirection capability of NetScaler ADC (Refer to Appendix 2)
- The recommended method for replacing forward proxy capabilities is through the use of NetScaler Secure Web Gateway (SWG). The Secure Web Gateway provides all the capabilities of the TMG forward proxy, and adds on additional capabilities for authentication, load balancing, inspection and filtering.

The NetScaler SWG helps users

- Gain visibility into otherwise bypassed secure traffic.
- Block access to malicious or unknown sites and avoid infecting users within the enterprise.
- Control access to some websites, such as personal mail, social networking, and job search websites, from the enterprise network.
- Apply intelligent content control policies to ensure maximum user productivity.
Forefront TMG Configuration Summary

Configuring TMG as a forward proxy

TMG can be setup with different configurations for different requirements. Here, we will summarize the configuration of TMG as a forward proxy.

1. Post installation, the Network Setup wizard is shown. Here, begin with the single network adapter option as shown below -

![Network Setup Wizard](image)

2. In the next screen, setup network parameters.

![Local Area Network (LAN) Settings](image)

If a dynamic IP address is used (DHCP), clients on the internal network must either have their Web browsers configured to use Forefront TMG as their Web proxy or should be running the Forefront TMG Client software.
3. This will complete the Network Setup wizard. After completing this, configure system settings as the next section of TMG setup.

**Getting Started Wizard**

Welcome to Forefront TMG!

To get started, follow the three steps below:

- **Configure network settings**
  Define network settings for Forefront TMG, including IP settings, routing rules, and network relationships.

- **Configure system settings**
  Define local system settings for Forefront TMG.

- **Define deployment options**
  Specify Forefront TMG deployment settings such as how this Forefront TMG server receives Microsoft updates.

4. Configure host details for the TMG server

**Getting Started - System Configuration Wizard**

**Host Identification**

Enter the identification details for this Forefront TMG computer.

- **Computer name:** WIN-9G1V7F59695
- **Member of:**
  - Windows domain: [Field]
  - Workgroup: WORKGROUP
- **Help about domain and workgroup membership**

**Primary DNS Suffix**

- **DNS suffix:** [Field]
  - In a domain, the primary DNS suffix is provided by the domain controller.
5. Next, define deployment settings for the TMG Server

Getting Started - Deployment Wizard

Welcome to the Deployment Wizard

This wizard helps you deploy Forefront TMG. This includes specifying update settings and joining the Customer Experience Improvement Program.

To continue, click Next.

Help about the Deployment Wizard

6. The next step asks for configuration of Microsoft Updates. Make a selection as appropriate for your environment, then the next step asks for definition of settings for the network inspection system (NOTE: the Microsoft Reputation Service used here for URL categorization is not available now)

Getting Started - Deployment Wizard

Forefront TMG Protection Features Settings
Use this page to activate licenses required for receiving updates and to enable Forefront TMG protection mechanisms.

Network Inspection System (NIS)
License: Activate complementary license and enable NIS
What is NIS?

Web Protection
License: Activate evaluation license and enable Web Protection
Key: Evaluation Expiration date: 12/19/2017
Enable Malware Inspection
Enable URL Filtering

The URL Filtering Feature queries Microsoft Reputation Service for URL categorization. The full URL string is sent to the service, using a secure connection.

Learn about updating license agreements
Read our Privacy Statement
7. Now, navigate to the Networking section of the Forefront TMG menu and select the Internal Network, as shown below. Right click and select Properties.

8. In the Properties window, select the Web Proxy tab and Enable HTTP/SSL proxies as required.
9. The next step is configuring authentication for the web proxy. This can be done using the Authentication button in Web Proxy settings.

![Authentication settings](image)

10. The Advanced settings button allows configuration of the maximum number of connections per server.

![Advanced settings](image)
11. Next, to define URL filtering and other protection, switch to the Web Access Policy section. Here, rules for settings including HTTPS and malware inspection, URL filtering and categorization can be configured in the right hand pane.

![Web Access Policy](image)

12. On clicking on one of the configuration items, you will be presented with the settingsscreen for each individual protection item -

![URL Filtering Settings](image)

**NOTE:** As stated earlier, the Microsoft Reputation Service is no longer available.
Configuring the NetScaler SWG Forward Proxy

Using the Configuration Wizard

The recommended method to configure SWG as a forward proxy is by using the Configuration Wizard. The Configuration wizard is a prompt-driven approach to configuring the reverse proxy as per the requirements of the user. The following steps describe the process for this configuration:
1. Initiate the wizard from the Secure Web Gateway Getting Started section in the GUI:

   2. Click on Get Started on the wizard’s welcome page
3. The next screen describes the functioning of the SWG appliance and the capabilities of the SWG and MAS components of the setup. It also describes the transparent and explicit proxy modes.

4. The next screen begins the configuration of the proxy. Here, provide an appropriate name and a capture mode (Transparent or Explicit, depending on your requirement). Note that only one transparent proxy can exist at a given time.

Secure Web Gateway Configuration

Proxy Settings

Configure a proxy server in transparent or explicit mode. In transparent proxy mode, configuring a \( P \) to either an IP address that the clients configure in their browsers or an IP address that the organization

Name*  

Capture Mode*

Transparent

Explicit

Please enter value
5. In the next step, depending on the Capture Mode selected, setup the IP address and port that the proxy will listen on. (for a Transparent proxy, both will be set to *)

Secure Web Gateway Configuration

Proxy Settings

Configure a proxy server in transparent or explicit mode. In transparent proxy mode, configuring a proxy to either an IP address that the clients configure in their browsers or an IP address that the organization

Name*
Test

Capture Mode*
Explicit

IP Address*
1.2.3.4

Port*
80

Continue Cancel

6. Now, configure SSL Interception (Enable or Disable) and specify the SSL profile and the CA certificate to be used for SSL Interception. Click on Bind after adding the key pair and any relevant SSL policies.

SSL Interception

Encrypted traffic between a client’s device and the internet is intercepted to enforce compliance rules. Create an SSL profile to bind to the proxy server and specify a CA certificate to use for SSL interception.

- Enable SSL interception
- SSL Profile*
  rs_default_ssl_profile_frontend
- Select SSL Interception CA Certificate-Key Pair*
  swg_ca_cert

Bind Unbind

Policy Name
No items
7. Next, configure user authentication, if required. User authentication will enable user logging in logs and on the MAS dashboard.

Secure Web Gateway Configuration

<table>
<thead>
<tr>
<th>Proxy Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Name</td>
</tr>
<tr>
<td>Test</td>
</tr>
</tbody>
</table>

SSL Interception

SSL Profile: ns_default_ssl_profile_frontend

Identity Management

Enable authentication to view user details in the logs and on the MAS dashboard.

Enable user authentication

8. The next section allows you to enable URL filtering based on either URL categorization or URL lists. URL categorization is driven by pre-determined categorization of websites, while URL lists deal with specific URLs that need to be filtered. Upon enabling these features, policies for specific categories/lists can be bound to the proxy server.

URL Filtering

URL Filtering restricts user access to specific websites or web pages. There are two types of filtering services - UI access to websites.

Control access to websites on the basis of the incoming URL or on the basis of metadata associated with the incoming URL. Click Edit to associate a URL categorization policy with the proxy server.

Enable URL Categorization

Control access to websites on the basis of the incoming URL or on the basis of metadata associated with the incoming URL. Click Edit to associate a URL list policy with the proxy server.

Enable URL List
To bind policies, click on the Bind button after enabling URL Categorization/URL List, as below:

**URL Filtering**

URL Filtering restricts user access to specific websites or web pages. There are two types of filtering:
- Access to websites
- Control access to websites on the basis of the incoming URL or on the basis of metadata associated with each URL.

Click Bind to associate a URL categorization policy with the proxy server.

- **Enable URL Categorization**

<table>
<thead>
<tr>
<th>Bind</th>
<th>Unbind</th>
</tr>
</thead>
</table>

**Policy Name**

*No items*.

9. After completing URL filtering configuration, the next step is complete Security configuration. This section allows control of website access based on the website’s Reputation Score.

**URL Filtering**

<table>
<thead>
<tr>
<th>URL Categorization</th>
<th>false</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL List</td>
<td></td>
</tr>
</tbody>
</table>

**Security Configuration**

Configure URL reputation policy to control Website access based on the URL Reputation score.

- **Reputation Score**

**Continue** | **Cancel**
10. The next section is Analytics, which controls whether analytics and reporting using NetScaler MAS is enabled. If yes, the requisite data is generated and made available to MAS. Note that to view the metrics, the SWG appliance should be added as an instance to MAS.

**Analytics**

Enable Analytics to monitor the outbound traffic and user transactions by using NetScaler Manager. NetScaler SWG appliance as an instance to NetScaler MAS.

- Enable Analytics

**Continue**  **Cancel**

11. The final screen (in case Analytics is enabled) is to specify the NetScaler MAS IP address and port. This defines the MAS appliance where logs are to be sent. (Note: Please change the port to 5557 if shown differently)

**Analytics**

Enable Analytics to monitor the outbound traffic and user transactions by using NetScaler Manager. NetScaler SWG appliance as an instance to NetScaler MAS.

- Enable Analytics

NetScaler MAS IP Address

Port

5557

Transport Mechanism: LogStream

**Continue**  **Cancel**

This completes the GUI based configuration for the SWG forward proxy. The configured proxies can be viewed in the GUI as follows –

**Secure Web Gateway(s)**

- **Proxy Name**  **IP Address**
  - explicit-proxy-113  
    - 10.102.216.113
  - *swg-vserver*

**Cross-referenced Library**

This section is a reference to the library, but it is not applicable here.
Appendix 1
Manual Configuration

To configure SSL forward proxy using the NetScaler SWG CLI
At the command prompt, type:
add cs vserver <name> PROXY <ipaddress> <port>

Arguments
Name
   Name for the proxy server. Must begin with an ASCII alphanumeric or underscore (_&) character, and
must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and
hyphen (-) characters. This setting cannot be changed after the CS virtual server is created.
The following requirement applies only to the NetScaler CLI:
   - If the name includes one or more spaces, enclose the name in double or single quotation marks (for
     example, “my server” or ‘my server’).
   - This is a mandatory argument. Maximum Length: 127
IPAddress
   IP address of the proxy server.
port
   Port number for proxy server. Minimum value: 1

Example for explicit proxy
add cs vserver swg-vserver PROXY 10.1.1.1 80

Example for transparent proxy
add cs vserver swg-vserver PROXY *

Example Configuration
Add the SSL vserver intercept policy as follows –
add ssl policy interceptall _ ssli -rule true -action INTERCEPT
NOTE: This policy will result in interception of all traffic. If certain types of traffic (banking etc.) should be by-
passed without interception, a bypass policy should also be bound to the vserver.

Add and bind policy patsets as shown below -
add policy patset bypasspolicy _ ssli _ cat
bind policy patset bypasspolicy _ ssli _ cat "Online Trading" -index 1
bind policy patset bypasspolicy _ ssli _ cat Insurance -index 2
bind policy patset bypasspolicy _ ssli _ cat "Financial Products" -index 3
bind policy patset bypasspolicy _ ssli _ cat "Web based Mail" -index 4
bind policy patset bypasspolicy _ ssli _ cat "E-Mail Subscriptions" -index 5
add ssl policy bypasspolicy _ ssli -rule "client.ssl.client_hello.SNI.URL_CATEGORY.EGORIZE(0,0).CATEGORY.EQUALS_ANY("bypasspolicy _ ssli _ cat")" -action BYPASS

(for more on patsets refer to https://www.citrix.com/blogs/2011/09/02/patsets-on-netscaler-and-their-use-for-filtering-on-ip-tables-and-rate-limiting/)
To bind URL Filtering categories from the command line:

```
sh urlfiltering Categories
```

This command will show the URL filtering categories available. The policies that are bound to the proxy CS vserver can be created with the following commands (this example shows a policy blocking Facebook access):

```
add policy patset fbSelected _ patset
bind policy patset fbSelected _ patset "Facebook: Friends" -index 1
bind policy patset fbSelected _ patset "Facebook: Photo Upload" -index 2
bind policy patset fbSelected _ patset "Facebook: Events" -index 3
bind policy patset fbSelected _ patset "Facebook: Chat" -index 4
bind policy patset fbSelected _ patset "Facebook: Questions" -index 5
bind policy patset fbSelected _ patset "Facebook: Video Upload" -index 6
bind policy patset fbSelected _ patset "Facebook: Groups" -index 7
bind policy patset fbSelected _ patset "Facebook: Games" -index 8
```

Next, add the responder action and policy for this patset -

```
add responder action responder-act1 redirect "https://www.citrix.com" -responseStatusCode 302
add responder policy fbSelected _ url _ cat "!HTTP.REQ.METHOD.EQ("CONNECT") && (HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL _ CATEGORIZE(0,0).CATEGORY.EQUALS _ ANY("fbSelected _ patset") || HTTP.REQ.URL.URL _ CATEGORIZE(0,0).CATEGORY. EQUALS _ ANY("fbSelected _ patset")))" responder-act1
```

Finally, set up the proxy as follows –

```
add cs vserver explicit-proxy-113 PROXY 10.102.216.113 80 -cltTimeout 180
bind cs vserver explicit-proxy-113 -policyName fbSelected _ url _ cat -priority 100 -gotoPriorityExpression END -type REQUEST
set ssl vserver explicit-proxy-113 -sslProfile ns _ default _ ssl _ profile _ frontend
set ssl profile ns _ default _ ssl _ profile _ frontend -sslInterception ENABLED
bind ssl profile ns _ default _ ssl _ profile _ frontend -ssliCACertkey swg _ cert
bind ssl vserver explicit-proxy-113 -policyName interceptall _ ssl _i -priority 13 -type INTERCEPT _ REQ
bind ssl vserver explicit-proxy-113 -policyName bypasspolicy _ ssl _i -priority 10 -type INTERCEPT _ REQ
```
Appendix 2
Basic (Non-SSL) Forward Proxy with NetScaler ADC

The following commands will configure a basic cache redirection based forward proxy:

Define a Cache Redirection (CR) vserver

```
add cr vserver vs_cache_forward HTTP 1.2.3.4 80 -cachetype forward -redirect origin
```

where forward defines this as a forward proxy vserver and origin directs all traffic to the origin server.

(1.2.3.4 is the proxy server address)

This defines an explicit VIP address that the NetScaler can listen on. This IP address:port needs to be configured in the user browsers as the proxy location. For example, in Firefox, this would be under Preferences\Advanced\Connection tab.

Other options for the -cachetype parameter include TRANSPARENT and REVERSE. Other options for the -redirect option include CACHE and POLICY.

Define a DNS vserver to do name resolution; Bind to your local DNS server(s).

```
add lb vserver vs_dns DNS 1.2.3.5 53
add service svc_dns_120 1.2.3.120 DNS 53
bind lb vserver vs_dns svc_dns_120
```

If there are multiple DNS servers, you can load balance traffic among them by defining multiple services.

Configure the CR vserver to use the DNS vserver for name resolution

```
set cr vserver vs_cache_forward -dnsVservername vs_dns
```

Now, configure your browser as necessary to point to the CR vserver defined in Step 1 above and you are good to go. This configuration will direct all the traffic to the origin servers (the redirect parameter in step 2). If cache servers are configured, then you need to set the redirect parameter to cache or policy.
Conclusion

Citrix NetScaler enables a complete replacement of Microsoft Forefront TMG for users looking to securely host multiple, load balanced websites. NetScaler, as has been indicated through the NetScaler Advantage callout below, presents benefits over TMG for end users. Also, the deployment of similar functionality on NetScaler is not only more flexible in scope, but also much simpler with the SWG wizard.

NetScaler SWG Advantage

As compared to TMG, NetScaler supports several additional capabilities. TMG utilized Microsoft Reputation Services (MRS) for website filtering, however that service has now been discontinued. With the additional policy driven as well as cloud powered filtering capabilities and NetScaler analytics using MAS, NetScaler SWG provides significantly improved functionality.