Deployment Guide

Document Version 1.4

What's inside:

Microsoft Partner Network

Deploying F5 with Microsoft Forefront Threat Management Gateway 2010

Welcome to the F5 deployment guide for the BIG-IP Local Traffic Manager and Microsoft Forefront Threat Management Gateway (TMG). This document provides detailed guidance for intelligently directing network traffic through a Microsoft Forefront TMG 2010 array, as well as for publishing Microsoft Outlook Web Access and SharePoint Server 2010 applications with BIG-IP for increased performance and scaling of your TMG 2010 servers.

With the BIG-IP Local Traffic Manager, you can set up high availability firewall load balancing for Microsoft Forefront Threat Management Gateway 2010. You can effectively load balance inbound and outbound traffic across all members of a TMG array, taking advantage of Forefront's security features while also using LTM to optimize availability and performance.

Chapter 2, *Deploying BIG-IP APM for Reverse Proxy Access to SharePoint and Outlook Web App on page 18*, contains guidance on configuring the BIG-IP Access Policy Manager (APM) to proxy authentication to all services and enable secure portal access to Outlook Web App and SharePoint 2010 web sites.

Products and versions

Product	Version
BIG-IP LTM and LTM VE	10.2.1, 10.2.2, 10.2.3, 10.2.4, 11, 11.0.1, 11.1, 11.2, 11.3, 11.4, 11.4.1, 11.5, 11.5.1
Microsoft Forefront TMG	2010 Enterprise
Microsoft Exchange Server	2010 and 2010 SP1
Microsoft SharePoint	2010

For more information on Microsoft Forefront Threat Management Gateway 2010, see *http://www.microsoft.com/en-us/server-cloud/forefront/threat-management-gateway.aspx*

For more information on the F5 devices in this guide, see *http://www.f5.com/products/big-ip/*.

You can also visit the Microsoft page of F5's online developer community, DevCentral, for Microsoft forums, solutions, blogs and more: *http://devcentral.f5.com/Microsoft/*.

What is two-way firewall load balancing?

Two-way firewall load balancing is appropriate for any enterprise that wants to provide information by way of the Internet, while limiting traffic to a specific service, and also wants to maintain a large intranet with fast access to the Internet for internal users. This configuration calls for two BIG-IP redundant pairs:

- A BIG-IP unit on the outside (that is, the side nearest the Internet) of the firewalls, to balance inbound traffic across the firewalls and outbound traffic across a pool of internet gateways (optional).
- A BIG-IP unit on the inside (that is, the side nearest the intranet) of the firewalls to balance outbound traffic across the firewalls, and also to balance inbound traffic across internal server resources.

This is also known as a *firewall sandwich* configuration, because the BIG-IP units are on either side of the firewalls, sandwiching them.

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- This document is written with the assumption that you are familiar with both F5 devices and the Microsoft Forefront TMG. For more information on configuring these devices, consult the appropriate documentation. While we provide general guidance on applicable TMG configuration settings for this implementation, consult the Microsoft documentation for specific configuration instructions.
- This guide assumes you are running an array of Microsoft Forefront TMG 2010 servers in Domain mode.
- This guide contains instructions for configuring the BIG-IP LTM and Forefront TMG for Microsoft Exchange 2010 Outlook Web App. To configure your Client Access servers to support SSL offloading, you must first follow the Microsoft documentation. See *http://social.technet.microsoft.com/wiki/contents/articles/how-to-configure-ssl-offloading-in-exchange-2010.aspx*.
  Make sure you follow the correct steps for the version of Exchange Server that you are using (Exchange Server 2010 or Exchange Server 2010 SP1).

Important

- This guide is written with the assumption you are offloading SSL processing on the BIG-IP LTM. When configuring the TMG devices for the BIG-IP LTM and Outlook Web App as described in this document, you need the script found in this Microsoft TechNet article: *http://technet.microsoft.com/en-us/library/cc995313.aspx*

Configuring F5 and Microsoft Forefront TMG 2010 for two-way firewall load balancing to Microsoft Outlook Web App

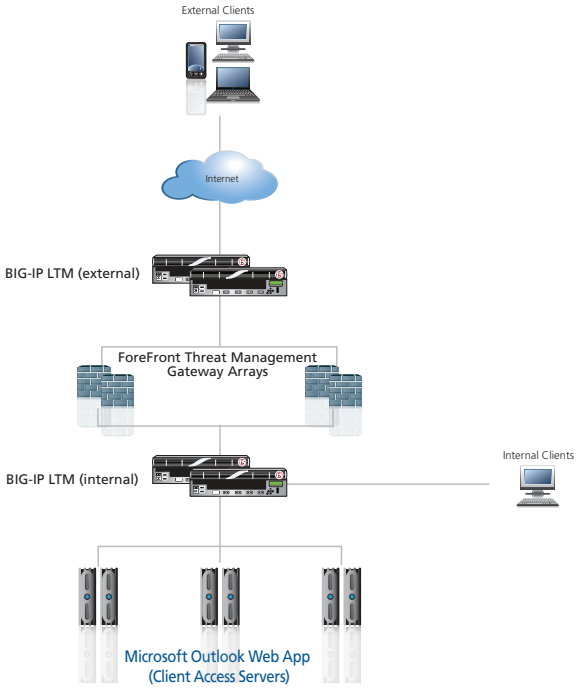
The following steps represent the minimum configuration necessary to pass traffic through Forefront TMG, including successful monitoring of the Forefront TMG servers and the example virtual servers shown in the configuration.

This section describes how to publish the Outlook Web App role of Microsoft Exchange Server 2010 with TMG, through the BIG-IP LTM. It is important to note that in this scenario, the BIG-IP LTM is offloading SSL from the CAS servers and the TMG servers.

For specific instructions on configuring Forefront TMG, see the Microsoft documentation.

Configuration example

The following logical configuration diagram shows our example implementation for two-way firewall load balancing to Microsoft Outlook Web App.



Threat Management Gateway Server configuration

- Network adapters – Forefront TMG Console>Networking>Network Adapters
  - External network adapters should use the external LTM internal VLAN floating self-ip as their default gateway
  - Configure one network adapter on each array member for each network that Forefront TMG will manage
- Networks – Forefront TMG Console>Networking>Networks

- » Define each network that will be internal to TMG servers by right-clicking Internal>Properties>Addresses and adding each adapter or range to the list.
- » In this guide, the network relationship for all network is: SNAT
- » All undefined networks will be classified by TMG as "External" (including the internal VLAN of the external LTM)

➤ Network rules – Forefront TMG Console>Networking>Network Rules

- » Create rules to establish a relationship between each network:
  - Rule allowing traffic to and from both Internal and External networks (Firewall policy will determine which hosts, protocols, and ports are allowed)

➤ Firewall policy – Forefront TMG Console>Firewall Policy

- » Create policies and objects allowing specific network/port/protocol traffic through TMG:
  - Create address ranges for the floating self-IPs of internal/external LTMs (Firewall Policy>Toolbox>Network Objects>New>Address Range)
  - Create an access rule allowing PING protocol from LTM self-IP network objects (see previous step) to both internal/external networks
  - Create an access rule allowing All Outbound Protocols from Internal/Local Host to External

➤ Web Access policy – Forefront TMG Console>Web Access Policy

Important: *The web access policy as listed allows all traffic from internal networks and the local host to external networks. You should determine the appropriate outbound firewall rules for your organization before creating this policy*

- » Specify the conditions under which internet access is allowed
  - Create a policy allowing all traffic from Internal/Local Host to External

Outlook Web App-specific TMG Server configuration

➤ Create an Outlook Web App Client Listener (Toolbox>Network Objects>Web Listeners): Note that you must chose a unique port for each listener because the TMG cannot listen on the same IP/Port combination for multiple listeners

- » Select External Networks
- » Client Connection Type: (do NOT require SSL))
- » Authentication: HTML Form Authentication
- » Authentication Validation Method: Windows (Active Directory)
- » Authentication>Advanced>check box for "Allow authentication over HTTP"
- » Connections>Client Connection Type>Enable HTTP connections on port: 8082
- » After creating the Listener, you need to run this command from the location where you downloaded the script (*http://technet.microsoft.com/en-us/library/cc995313.aspx)*:
  `cscript SetSSLAcceleratorPort.vbs "<name of OWA Listener>`.
  Enter 443 for port number and click OK.

  This script configures TMG to rewrite all outgoing links to port 443, to match the service port of the BIG-IP LTM.

- Create Outlook Web App Client Firewall Policy (Tasks>Publish Exchange Web Client Access):
  - From: Anywhere
  - To: Computer Name>Enter IP address of the Outlook Web App virtual server on the Internal LTM
  - Forward the original host header: checked
  - Proxy Requests: Appear to come from TMG computer
  - Listener: Select OWA Client Listener
  - Public Name: Enter FQDN of your OWA site
  - Authentication Delegation: Basic
  - Bridging: Web Server>Redirect requests to HTTP port 80>Checked
- Create Outlook Web App HTTP Monitor Firewall Policy (allows external BIG-IP to monitor the internal virtual server):
  - Action: Allow
  - Protocols: HTTP
  - From: Address Ranges corresponding to BIG-IP Self IP addresses
  - To: Address Range corresponding to Outlook Web App virtual server on the Internal BIG-IP

Configuring the Exchange 2010 Client Access Servers

There are two requirements on the Exchange 2010 Client Access servers for this deployment

- To configure your Client Access servers to support SSL offloading, you must first follow the Microsoft documentation. See *http://social.technet.microsoft.com/wiki/contents/articles/how-to-configure-ssl-offloading-in-exchange-2010.aspx*.
  Make sure you follow the correct steps for the version of Exchange Server that you are using (Exchange Server 2010 or Exchange Server 2010 SP1).
- You must set the Authentication method for all HTTP-based Client Access Servers to Basic. Using Forms authentication on TMG requires the Client Access Servers to be set to Basic. The TMG form collects the logon information and passes it to the Client Access Servers.

Disabling TMG caching and compression for Outlook Web App

Because data is cached and compressed by the external BIG-IP system, the next task is to disable caching and compression for applications published by TMG (OWA in this example).

To disable caching

1. In TMG, click Web Access Policy>Web Access Settings>Web Caching>Enabled
2. From the Cache Rules tab, click New.
3. Name: Disable OWA Cache
4. From the To tab, under Cache content requested from these destinations, click Add
5. For the first entry, type OWA for the name
6. Click Add and type wildcard URLs for the Outlook Web Access site, e.g. http://mail.tmg2010.tc.f5net.com/* and https://mail.tmg2010.tc.f5net.com/*

7. On the Cache Store and Retrieval tab, select the "Only if a valid version of the object exists…" and "Never, no content will ever be cached" buttons and click OK.
8. On the HTTP tab, uncheck the box for Enable HTTP Caching

To disable compression

1. In TMG, click Web Access Policy>Web Access Settings>HTTP Compression>Enabled
2. On the Return Compressed Data tab, highlight the OWA listeners in the "Compress HTTP responses when requested…" box and then click Remove.

Configuring the BIG-IP LTM for two-way firewall load balancing

You need to create the following objects on the internal and external BIG-IP LTM units, respectively. On the internal LTMs, wildcard virtual servers forward traffic for all destinations to pools consisting of Forefront TMG servers, which have a default gateway corresponding to the floating Self IP address of the internal VLAN on the external BIG-IP LTMs.

Outbound traffic is then directed to another wildcard virtual server which forwards it to a pool containing the address of your default internet gateway. Incoming traffic is directed through Forefront TMG to individual virtual servers configured on the internal BIG-IP LTM.

Internal BIG-IP objects

The table on the following page contains a list of BIG-IP LTM configuration objects for the Internal BIG-IP LTM, along with any non-default settings. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

Internal BIG-IP objects

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitors (*Local Traffic-->Monitors*)	***HTTP monitor for OWA***	
	Name	Type a unique name
	Type	**HTTP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Gateway ICMP	
	Name	Type a unique name
	Type	**Gateway ICMP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Transparent	**Yes**
	Alias Address	One or more external IP addresses
	Alias Service Port	***All Ports**
Pools (*Local Traffic -->Pools*)	***Internal TMG device pool***	
	Name	Type a unique name
	Health Monitor	Select the ICMP monitor you created above
	Slow Ramp Time[1]	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the IP Address of a Internal TMG device.
	Service Port	***All Ports** (click **Add** to repeat Address and Service Port for all nodes)
	Outlook Web App pool	
	Name	Type a unique name
	Health Monitor	Select the HTTP monitor you created above
	Slow Ramp Time	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the IP Address of the Client Access servers using port 80
	Service Port	**80** (click **Add** to repeat Address and Service Port for all nodes)
Local Traffic General Properties (*System -->Configuration-->Local Traffic-->General*)	***SNAT Packet Forwarding***	Select **All Traffic** from the list.
iRules (*Local Traffic-->iRules*)	***Name***	Type a unique name

	Definition	`when HTTP_REQUEST {`
		`  persist uie [HTTP::header  "Authorization"] 7200`
		`  pool outlook-web-app-pool-name`
		`}`
		(replace red text with the name of your pool)

Virtual Servers (*Local Traffic-->Virtual Servers*)	**Outbound TCP**	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Address Translation	Uncheck the box to **Disable** Address Translation

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Local Traffic-->Virtual Servers*)	**Outbound TCP - Continued**	
	Port Translation	Uncheck the box to **Disable** Port Translation
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the Internal VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the Internal TMG pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)
	Outbound UDP	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Protocol	Select **UDP** from the list.
	Address Translation	Uncheck the box to **Disable** Address Translation
	Port Translation	Uncheck the box to **Disable** Port Translation
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the Internal VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the Internal TMG pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)
	ICMP	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Type	Select **Performance L4** from the list.
	Address Translation	Uncheck the box to **Disable** Address Translation
	Port Translation	Uncheck the box to **Disable** Port Translation
	SNAT Pool	**Automap**
	Default Pool	Select the Internal TMG pool you created above
	Outlook Web App - Internal	
	Name	Type a unique name.
	Destination Type	**Host** (option button)
	Address	Type the IP address for this virtual server
	Service Port	**80**
	Protocol Profile (client)	**tcp-wan-optimized**
	Protocol Profile (server)	**tcp-lan-optimized**
	OneConnect	**oneconnect**
	HTTP Profile	Select **HTTP** from the list.
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the External VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	iRule	Enable the iRule you created
	Default Pool	Select the Web Server pool you created above
	Persistence Profile	**Cookie**

External BIG-IP Objects

The following table contains a list of BIG-IP LTM configuration objects for the External BIG-IP LTM.

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitors (*Local Traffic-->Monitors*)	***HTTP - Outlook Web App***		
	Name	Type a unique name	
	Type	**HTTP**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
	Transparent	**Yes**	
	Send String	Type this string on one line. Replace red text with your FQDN. `GET /owa/auth/logon.aspx?url=https://mail.example.com/owa/&reason=0 HTTP/1.1\r\nUser-Agent: Mozilla/4.0\r\nHost: mail.example.com\r\n\r\n`	
	Receive String[1]	**OutlookSession=** (see note[1])	
	Alias Address	The OWA-internal virtual server address on the internal LTM	
	Alias Service Port	**80** (for example to monitor a web server)	
	Gateway ICMP - Router		
	Name	Type a unique name	
	Type	**Gateway ICMP**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
	Transparent	**Yes**	
	Alias Address	One or more external IP addresses	
	Alias Service Port	***All Ports**	
Pools (*Local Traffic -->Pools*)	***Router***		
	Name	Type a unique name	
	Health Monitor	Select the ICMP monitor you created above	
	Slow Ramp Time	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the IP Address of a the External Router.	
	Service Port	***All Ports** (click **Add** to repeat Address & Port for all nodes)	
	Outlook Web App pool		
	Name	Type a unique name	
	Health Monitor	Select the HTTP monitor you created for OWA	
	Slow Ramp Time	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the external IP address of the TMG servers.	
	Service Port	**8082** (click **Add** to repeat Address and Service Port for all nodes)	
Profiles (*Local Traffic-->Profiles*)	***Client SSL*** (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate	Select the Certificate and Key you imported
Local Traffic General Properties (*System -->Configuration-->Local Traffic-->General*)	***SNAT Packet Forwarding***	Select **All Traffic** from the list.	
Virtual Servers (*Local Traffic--> Virtual Servers*)	**Outbound TCP**		
	Name	Type a unique name.	
	Destination Type	**Network** (option button)	

[1] *This response string is part of a Cookie header that OWA returns. Although you may elect to use another string on the page, it must be on the first 5,120 bytes of the received data (including headers and payload). Strings found near the end of the HTTP response from OWA will not be properly detected. See http://support.f5.com/kb/en-us/solutions/public/3000/400/sol3451.html for more details.*

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Local Traffic--> Virtual Servers*)	***Address***	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Address Translation	Uncheck the box to **Disable** Address Translation
	Port Translation	Uncheck the box to **Disable** Port Translation
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the Internal VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the Internal TMG pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)
	Outbound UDP	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Protocol	Select **UDP** from the list.
	Address Translation	Uncheck the box to **Disable** Address Translation
	Port Translation	Uncheck the box to **Disable** Port Translation
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the Internal VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the Internal TMG pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)
	ICMP	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Type	Select **Performance L4** from the list.
	Address Translation	Uncheck the box to **Disable** Address Translation
	Port Translation	Uncheck the box to **Disable** Port Translation
	SNAT Pool	**Automap**
	Default Pool	Select the Internal TMG pool you created above
	Outlook Web App - External	
	Name	Type a unique name.
	Destination Type	**Host** (option button)
	Address	Type the IP address
	Service Port	**80**
	HTTP Profile	Select **http-wan-optimized-compression-caching**
	SSL Profile (Client)	Select the Client SSL profile you created above
	SNAT Pool	**None**
	Default Pool	Select the pool you created above
	Persistence Profile	**Cookie**

This completes the configuration for BIG-IP LTM with TMG and Microsoft Outlook Web App.

Configuring F5 and TMG for firewall load balancing with a three-homed perimeter network (DMZ) for SharePoint

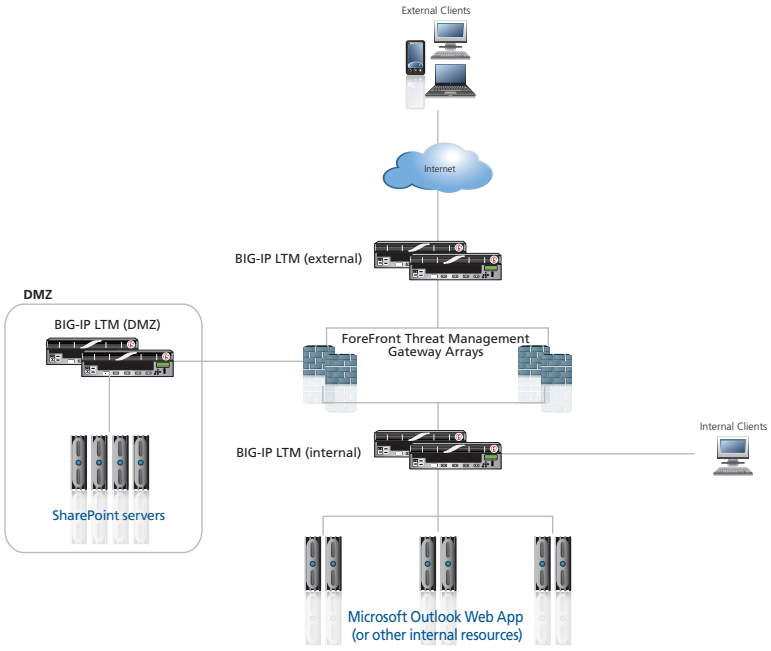
The following procedures describe how to configure external access to a SharePoint deployment located in the perimeter network (DMZ) through Forefront TMG, as well as allow access to Microsoft Windows Update sites from web servers located in the perimeter network.

Configuring the Forefront TMG server array

Use the following guidance to configure your TMG devices. On the Forefront TMG server array, you will need to create a perimeter network and a network topology route for the DMZ network. You will also create network rules and firewall policies to allow traffic from the internet to web servers located in the DMZ, and from those web servers to Microsoft Windows Update websites.

Configuration example

The following logical configuration diagram shows our example implementation for two-way firewall load balancing to Microsoft Outlook Web App.



Threat Management Gateway Servers Configuration

- Networks – Forefront TMG Console>Networking>Networks
  - Create a New Network>Perimeter Network>Addresses>Add Adapter><Select all adapters for the DMZ network>.
- Network Topology – Forefront TMG Console>Networking>Routing
  - Create Network Topology Route><Add behind-the-DMZ network range(s) and specify the external floating self-IP of the DMZ BIG-IP as the gateway>.
- Network Rules – Forefront TMG Console>Networking>Network Rules
  - Modify the network rule previously created to include the DMZ perimeter network as both a source and destination of traffic

- Firewall Policies – Forefront TMG Console>Firewall Policy – Add policies to allow External to DMZ (internet to DMZ web server) and DMZ to External HTTP (DMZ to Windows Update) access
  - Create an address range including the self-IP address of the external VLAN on the DMZ LTM
  - Create an access rule allowing the HTTP protocol from the External network to the DMZ perimeter network
  - Modify the access rule allowing PING (see above) to include the DMZ LTM address range in the From/Listener field
  - Create an access rule allowing the DNS protocol from the DMZ perimeter network to the External network (for DNS lookups)
  - Create an access rule allowing the HTTP and HTTPS protocols from the DMZ perimeter network to the Microsoft Update Sites Domain Name Set (for access to Windows Update)

SharePoint-specific TMG Server configuration

- Create SharePoint DMZ Listener (Toolbox>Network Objects>Web Listeners):
  - Select External Networks
  - Client Connection Type: (do NOT require SSL)
  - Authentication: No Authentication
  - Connections>Client Connection Type>Enable HTTP connections on port:8081. You must chose a unique port for each listener because the TMG cannot listen on the same IP/Port combination for multiple listeners.
  - After creating the Listener, you need to run this command from the location where you downloaded the script (*http://technet.microsoft.com/en-us/library/cc995313.aspx)*: **`cscript SetSSLAcceleratorPort.vbs "<name of SharePoint Listener>`**. Enter 443 for port number and click OK.

- Create SharePoint Firewall Policy (Tasks>Publish Exchange Web Client Access):
  - From: Anywhere
  - Web Farm: Add VIP to Servers List; Connectivity Verification: http://*/SitePages/Home.aspx (modify as applicable)
  - Load Balance Mechanism: leave at default
  - Forward the original host header: checked
  - Proxy Requests: Appear to come from TMG computer
  - Internal Site Name: FQDN of SharePoint Site
  - Listener: Select SharePoint DMZ Listener
  - Public Name: Enter FQDN of your SharePoint site
  - Authentication Delegation: No delegation, but client may authenticate directly
  - Bridging: Web Server>Redirect requests to HTTP port 80>Checked

- Create SharePoint HTTP Monitor Firewall Policy (allows external BIG-IP to monitor internal virtual server):
  - Action: Allow

- Protocols: HTTP
- From: Address Ranges corresponding to BIG-IP Self IP addresses
- To: Address Range corresponding to SharePoint VIP on internal BIG-IP

Disabling TMG caching and compression for SharePoint
Because data is cached and compressed by the external BIG-IP system, the next task is to disable caching and compression for applications published by TMG (SharePoint in this example).

To disable caching

1. In TMG, click Web Access Policy>Web Access Settings>Web Caching>Enabled
2. From the Cache Rules tab, click New.
3. Name: Disable SharePoint Cache
4. From the To tab, under Cache content requested from these destinations, click Add
5. For the first entry, type OWA for the name
6. Click Add and type wildcard URLs for the SharePoint site, e.g. http://sharepoint.example.com/*
7. On the Cache Store and Retrieval tab, select the "Only if a valid version of the object exists…" and "Never, no content will ever be cached" buttons and click OK.
8. On the HTTP tab, uncheck the box for Enable HTTP Caching

To disable compression

1. In TMG, click Web Access Policy>Web Access Settings>HTTP Compression>Enabled
2. On the Return Compressed Data tab, highlight the SharePoint listeners in the "Compress HTTP responses when requested…" box and then click Remove.

Configuring the BIG-IP LTM

For this configuration, you need to create a standard virtual server on the DMZ LTM and a virtual server on the external LTM, which will have a destination address matching the address of the DMZ LTM virtual server.

If you want to allow outbound internet access from servers in the DMZ, you can create wildcard virtual servers similar to those on the internal LTM, or you can create NAT objects to allow individual servers access to the internet. The BIG-IP configuration objects to allow outbound access are marked as optional in the DMZ BIG-IP configuration table.

The table on the following page contains a list of BIG-IP LTM configuration objects for the External BIG-IP LTM, along with any non-default settings. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

External BIG-IP Objects

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (*Local Traffic-->Monitors*)	***SharePoint HTTP - DMZ monitor***	
	Name	Type a unique name
	Type	**HTTP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Transparent	**Yes**
	Alias Address	This is the IP address of the BIG-IP LTM SharePoint DMZ virtual server on the DMZ BIG-IP LTM
	Alias Service Port	**80** (for example to monitor a web server)
Pool (*Local Traffic -->Pools*)	***SharePoint DMZ pool***	
	Name	Type a unique name
	Health Monitor	Select the monitor you created above
	Slow Ramp Time[1]	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the external IP Address of the TMG servers
	Service Port	**8081** (click **Add** to repeat Address and Service Port for all nodes)
Virtual Servers (*Local Traffic--> Virtual Servers*)	**SharePoint - DMZ virtual**	
	Name	Type a unique name.
	Destination Type	**Host** (option button)
	Address	Type the IP address for this SharePoint DMZ virtual server
	Service Port	**80**
	HTTP Profile	Select **http-wan-optimized-compression-caching**
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the External VLAN and move it to the Selected box.
	SNAT Pool	**None**
	Default Pool	Select the pool you created above

DMZ BIG-IP LTM

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitors (*Local Traffic-->Monitors*)	***SharePoint HTTP monitor***	
	Name	Type a unique name
	Type	**HTTP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Gateway ICMP - Forefront DMZ (optional: for allowing outbound access)	
	Name	Type a unique name
	Type	**Gateway ICMP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Transparent	**Yes**
	Alias Address	One or more external IP addresses
	Alias Service Port	***All Ports**
Pools (*Local Traffic -->Pools*)	***Forefront DMZ Pool (optional: for allowing outbound access)***	
	Name	Type a unique name
	Health Monitor	Select the ICMP monitor you created above
	Slow Ramp Time[1]	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the DMX IP Address of TMG server
	Service Port	***All Ports** (click **Add** to repeat Address and Service Port for all nodes)

BIG-IP LTM Object	Non-default settings/Notes	
Pools (*Local Traffic -->Pools*)	***SharePoint DMZ pool***	
	Name	Type a unique name
	Health Monitor	Select the HTTP monitor you created above
	Slow Ramp Time[1]	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the external IP address of the SharePoint servers
	Service Port	**80** (click **Add** to repeat Address and Service Port for all nodes)
Local Traffic General Properties (*System -->Configuration-->Local Traffic-->General*)	***SNAT Packet Forwarding***	Select **All Traffic** from the list.
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**Outbound TCP** ***(optional: for allowing outbound access)***	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Address Translation	Uncheck the box to **Disable** Address Translation
	Port Translation	Uncheck the box to **Disable** Port Translation
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the Internal VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the Internal TMG pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)
	Outbound UDP ***(optional: for allowing outbound access)***	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Address Translation	Uncheck the box to **Disable** Address Translation
	Port Translation	Uncheck the box to **Disable** Port Translation
	Protocol	Select **UDP** from the list.
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the Internal VLAN and move it to the Selected box.
	SNAT Pool	**Automap** (optional; see footnote)
	Default Pool	Select the Internal TMG pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)
	SharePoint- DMZ virtual	
	Name	Type a unique name.
	Destination Type	**Host** (option button)
	Address	Type the IP address
	Service Port	**80**
	HTTP Profile	Select **HTTP** from the list.
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the External VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the Web Server DMZ pool you created above

This completes the configuration.

Configuring WMI monitoring of TMG 2010 Servers

If you find your TMG servers are under high performance load, you can dynamically load balance between them using F5's WMI monitor. This monitor checks the CPU, memory, and disk usage of the nodes and, in conjunction with Dynamic Ratio load balancing mode, sends the connection to the server most capable of processing it.

For an overview of the WMI performance monitor, see *http://support.f5.com/kb/en-us/solutions/public/6000/900/sol6914.html*.

Installing the F5 WMI handler

The first task is to copy the F5 WMI handler to the TMG server and configure IIS to use the F5 Data Gathering Agent. For instruction on installing the Data Gathering Agent, see: *http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm_configuration_guide_10_0_0/ltm_appendixb_monitor_considerations.html#1185026*

Be sure to follow the procedures for the version of IIS you are using.

Creating the WMI Monitor on the BIG-IP LTM

The next task is to create the WMI monitor on the applicable BIG-IP LTM systems. Use the following table:

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitors (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**WMI**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	User Name	Type the appropriate user name
	Password	Type the associated password
	URL:	**/scripts/F5Isapi.dll** (for IIS 6, 7, and 7.5)

Create this monitor on all applicable BIG-IP LTM systems.

Creating a firewall rule on TMG

The next task is to create a firewall rule on the TMG server. Use the following guidance. For specific instructions, see the TMG documentation.

- Firewall Policy>Create Access Rule
  - From: BIG-IP External address range
  - To: Local Host
  - Protocol: HTTP
  - Action: Allow

Apply the monitor on the BIG-IP LTM devices

Next, we apply the monitor to the TMG nodes on the BIG-IP LTM system. This can be any or all of the BIG-IP LTM devices that are sending traffic to the TMG servers.

To apply the monitor to the nodes

1. On the Main tab, expand **Local Traffic** and then click **Nodes**.
2. From the list of nodes, click a node for the external IP address of your TMG server.
3. In the Configuration section, from the **Health Monitor** list, select **Node Specific**.
4. From the Available list, select the WMI monitor you created, and then click the Add (<<) button.
5. Click **Update**.
6. Repeat for all appropriate nodes.
7. Repeat this procedure for all applicable BIG-IP LTM systems.

Modifying the pool(s) to use the Dynamic Ratio load balancing method

The next task is to modify the BIG-IP LTM pools to use the Dynamic Ratio load balancing method. Make this change for each pool that contains the TMG nodes to which you added the WMI monitor.

To modify the load balancing method on the pool

1. On the Main tab, expand **Local Traffic** and then click **Pools**.
2. Click the name of the appropriate Pool. The Pool Properties page opens.
3. On the Menu bar, click **Members**.
4. From the **Load Balancing Method** list, select **Dynamic Ratio (Node)**.
5. Click the **Update** button.
6. Repeat this procedure for all applicable pools on this BIG-IP LTM.
7. Repeat this procedure on all applicable BIG-IP LTM systems.

Chapter 2

Deploying BIG-IP APM for Reverse Proxy Access to SharePoint and Outlook Web App

This chapter provides instruction on how to securely publish and optimize access to Microsoft Outlook Web App and SharePoint Server 2010 using a redundant pair of F5 BIG-IP devices.

In this scenario, F5's Access Policy Manager (APM) proxies authentication to all services and enables secure portal access to OWA and SharePoint 2010 web sites. The BIG-IP Application Security Manager (ASM) module's policy builder allows administrators granular control over application security, with the BIG-IP LTM improving performance with caching, compression, and TCP optimizations.

Because the BIG-IP is a default-deny device, only those inbound connections that you choose are allowed access to your network resources. This chapter shows you how to configure logging on the BIG-IP system to better monitor traffic and diagnose problems.

This chapter also describes the configuration of LTM to work with Microsoft Threat Management Gateway 2010. All outbound traffic is routed through the TMG array, where an administrator can use Forefront's built-in caching, compression, and security features to control web access and optimize internally-sourced web traffic.

Prerequisites

The following are prerequisites and configuration notes for this chapter:

- To use BIG-IP APM, you must have the module licensed and provisioned on the BIG-IP system before beginning the template.
- If you want to take advantage of the BIG-IP ASM to provide application-level security for SharePoint or Outlook Web App, you must have the module licensed and provisioned before starting this configuration. If you do not use ASM, the BIG-IP APM still provides secure Portal Access to the applications.
- This section is divided into two sections, one for configuring the BIG-IP system for SharePoint, and one for Outlook Web App. Use the section applicable for your configuration.

Configuring the BIG-IP APM for Reverse Proxy Application Access to SharePoint

The following configuring the BIG-IP APM and ASM for Microsoft SharePoint 2010.

Before beginning, there are two prerequisites for the SharePoint configuration:

- The SharePoint authentication method must be NTLM.
- Do NOT configure SharePoint Alternate Access Mappings to support SSL offload (do not add an internal URL for HTTPS://.

BIG-IP Object	Non-default settings		
AAA Servers (*Access Policy--> AAA Servers*)	***If you are using a single Active Directory Server***		
	Name	Type a unique name.	
	Type	**Active Directory**	
	Domain Controller	Type the IP address or FQDN name of an Active Directory Domain Controller	
	Domain Name	Type the Active Directory domain name	
	Admin Name[1]	Type the AD user name with administrative permissions (optional)	
	Admin Password[1]	Type the associated password (optional). Type it again in the Verify Password box	
	If you are using a pool of Active Directory Servers		
	Name	Type a unique name.	
	Type	**Active Directory**	
	Domain Name	Type the FQDN of the Windows Domain name	
	Server Connection	Click **Use Pool** if necessary.	
	Domain Controller Pool Name	Type a unique name	
	Domain Controllers	**IP Address**: Type the IP address of the first domain controller **Hostname**: Type the FQDN of the domain controller Click **Add**. Repeat for each domain controller in this configuration.	
	Server Pool Monitor	Select the monitor you created above.	
	Admin Name[2]	Type the Administrator name	
	Admin Password[2]	Type the associated password	
SSO Configurations (*Access Policy--> SSO Configurations*)	***Name***	Type a unique name.	
	SSO Method	**NTLM v1**	
	NTLM Domain Name	Type the NTLM Domain name	
APM Access *(depends on your version of BIG-IP APM)*	***BIG-IP APM v11***		
	Portal Access (*Access Policy-->Portal Access*)	***Name***	Type a unique name
		Application URI[3]	Type the URL of the SharePoint site (such as http://dc.tmg2010.example.com) Click **Create**. Stay on the Portal Access page to add Resource item.
	BIG-IP APM v10		
	Web Application (*Access Policy-->Web Applications*)	***Name***	Type a unique name All other fields are optional. Click **Create**. Stay on the Web Application page to add Resource item
Resource Items (*Web Application page--> Resource Items section--> Add)*	***Destination Type***[4]	Click **Host Name** option button, if necessary.	
	Destination Host Name	Type the Host Name of the SharePoint site (for example dc.tmg2010.example.com.	
	Scheme	**HTTP**	
	Port	Type the appropriate port. We use 80.	
	Paths	Type **/***	
	Compression	**GZIP Compression** (optional)	
	SSO Configuration	Select the NTLM SSO Configuration you created above.	
Connectivity Profile (*Access Policy --> **v11.x**: Secure Connectivity **v10.x**:Connectivity Profiles)*	***Name***	Type a unique name	
	Parent Profile	**Connectivity** (in v11.4 and later: **Common/connectivity**)	
Webtop (*Access Policy -->Webtops*)	***BIG-IP APM v11***		
	Name	Type a unique name.	
	Type	**Portal Access**	
	Portal Access Start URI[1]	Type the URL of the SharePoint site (for example, http://dc.tmg2010.example.com)	

[1] Only necessary if using a pool of Active Directory servers
[2] Optional; Admin Name and Password are only required if anonymous binding to Active Directory is not allowed in your environment
[3] In versions 11.4 and later, you must first select **Application URI** from the **Link Type** list.
[4] In versions 11.4 and later, you must first select **Paths** from the **Link Type** list.

BIG-IP Object	Non-default settings		
Webtop (*Access Policy -->Webtops*)	***BIG-IP APM v10***		
	Name	Type a unique name.	
	Type	**Web Applications**	
	Web Application Start URI	Type the URL of the SharePoint site (for example, http://dc.tmg2010.example.com)	
Access Profile (*Access Policy--> Access Profiles*)	***Name***	Type a unique name	
	SSO Configuration	Select the SSO Configuration you created above	
	Languages	Move the appropriate language(s) to the **Accepted** box.	
Access Policy (*Access Policy -->Access Profiles*)	***Edit***	Edit the Access Profile you created using the Visual Policy Editor. See the following page for instructions.	
Profiles (*Local Traffic-->Profiles*)	***Rewrite Profile*** (*Profiles-->Services*) (*In 11.4+, Access Profiles--> Portal Access-->Rewrite)*	Name	Type a unique name
		Parent Profile	**rewrite** (in v11.4 and later: **Common/rewrite**) All other settings at default.
	HTTP (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**http**
	HTTP Compression (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**wan-optimized-compression**
	HTTP Class (optional) *(versions prior to 11.4 only)* (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**httpclass**
		Application Security	**Enabled**
	TCP WAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	Client SSL (*Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select appropriate Certificate and Key
Virtual Server (*Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	IP Address	Type the IP address clients will use for access.	
	Service Port	**443**	
	Protocol Profile (client)	Select the WAN optimized TCP profile you created	
	Protocol Profile (server)	Select the LAN optimized TCP profile you created	
	HTTP Profile	Select the HTTP profile you created	
	HTTP Compression Profile	Select the HTTP Compression profile you created	
	SSL Profile (Client)	Select the Client SSL profile you created	
	SNAT Pool	**Auto Map** (if you expect more than 64,000 concurrent connections, create a SNAT Pool)	
	Access Profile	Select the Access profile you created and edited	
	Connectivity Profile	Select the Connectivity profile you created	
	Rewrite Profile	Select the Rewrite profile you created	
	HTTP Class Profile	If using a version prior to 11.4, select the HTTP Class profile you created	
Security Policy *(versions 11.4+ only and optional)* (*Security -->Application Security --> Security Policies*)	***Local Traffic Deployment Scenario***	**Existing virtual server**	
	Type of protocol	**HTTPS**	
	HTTPS Virtual Server	Select the virtual server you created from the list	
	Deployment Scenario	**Create a security policy manually or use templates (advanced)** Configure the properties as applicable	
	Application-Ready Security Policy	**SharePoint 2010 (https)**	

[1] In versions 11.4 and later, you must first select **Application URI** from the **Link Type** list.

Editing the Access Policy

In the following procedure, we show you how to configure edit the Access Policy on the APM using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy. The Policy shown in the following procedure is just an example, you can use this Access Policy or create one of your own.

To configure the Access Policy

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you created, and then, in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Logon Page** option button, and then the **Add Item** button at the bottom.
5. Configure any of the options as applicable for your configuration. In our example, we leave the defaults.
6. Click the **Save** button.
7. Click the **+** symbol between **Logon Page** and **Deny**.
8. Click the **AD Auth** option button, and then the **Add Item** button at the bottom.
9. From the **Server** list, select the AAA server you created above.
10. All other settings are optional. Click the **Save** button. You now see two paths, Successful and Fallback.
11. On the Successful path, click the + symbol between **AD Auth** and **Deny**.
12. Click the **SSO Credentials Mapping** option button, and then the **Add Item** button.
13. Configure any of the options as applicable for your configuration. In our example, we leave the defaults.
14. Click the **Save** button.
15. Click the **+** symbol between **SSO Credentials Mapping** and **Deny**.
16. The next steps depend on which version of the BIG-IP APM you are using:
    - *Versions 11.0 - 11.4.1*:
      a. Click the **Webtop and Webtop Links Assign** option button, and then the **Add Item** button.
      b. Click the **Add/Delete** link next to Webtop.
      c. Click the option button for the Webtop you created above.
      d. Click **Save**.
    - *Versions 11.5 and later*:
      a. Under Resource Assignment, click the Add new entry button
      b. Under Expression, click Add/Delete
      c. Click the Portal Access tab and select the radio button next to the APM Portal Resource you previously created.
      d. Click the Webtop tab and select the radio button next to the APM Webtop you previously created.
      e. Click the Update button.
      f. Click the Save button.
      g. Continue with Step 20 on the following page.
17. Click the + symbol between **Webtop and Webtop Links Assign** (or **SSO Credential Mapping** in v10.x) and **Deny**.
18. Click the **Resource Assign** option button, and then click the **Add Item** button.

19. The next steps depend on which version of the BIG-IP APM you are using:
    - *v11.0 - 11.4.1*
        a. Click the **Add/Delete** Link next to **Portal Access Resources**.
        b. Check the box for the Portal Access object you created in the APM Access section of the table.
        c. Click the **Save** button.
    - *v10.x*
        a. Click the **Add New Entry** button.
        b. Click the **Add/Delete Web Application Resources** link.
        c. Check the box for the Web Application you created in the APM Access section of the table.
        d. Click **Update**.
        e. Click the **Set Webtop** link.
        f. Check the box for the Webtop you created in the table.
        g. Click the **Save** button.
20. On the Fallback path after **Resource Assign** click the **Deny** box link.
21. Click the **Allow** option button, and then click **Save**.
22. Click the yellow **Apply Access Policy** link in the upper left part of the window. You must apply an access policy before it takes effect.

This completes the APM configuration for SharePoint.

Configuring the BIG-IP APM for Reverse Proxy Application Access to Outlook Web App

The following configuring the BIG-IP APM and ASM for Outlook Web App. Before beginning, there are two prerequisites for OWA:

- The authentication method for your Exchange 2010 Client Access Servers must be set to **Forms Auth**.
- The Client Access Servers must be configured for SSL offload.

BIG-IP Object	Non-default settings		
AAA Servers (*Main tab-->Access Policy -->AAA Servers*)	***Name***	Type a unique name	
	Type	**Active Directory**	
	Domain Controller	Type the IP address of the Domain controller	
	Domain Name	Type the Windows Fully Qualified Domain Name (FQDN)	
	Admin Name	If required, type the Admin name	
	Admin Password	Type and verify the Admin password	
SSO Configurations (*Main tab-->Access Policy -->SSO Configurations*)	***Name***	Type a unique name.	
	SSO Method	**Form Based**	
	Start URI	**/owa/auth/logon.aspx**	
	Form Method	**POST**	
	Form Action	**/owa/auth/owaauth.dll**	
	Form Parameter for User Name	**username**	
	Form Parameter for Password	**password**	
	Hidden Form Parameters/Values	**destination** **http://ex.tmg2010.example.com/owa/auth/logon.aspx** (replace red text with FQDN) **flags 0** **forcedownlevel 0** **isUtf8 1** **trusted 0** (each entry on a separate line)	
APM Access *(depends on your version of BIG-IP APM)*	***BIG-IP APM v11***		
	Portal Access (*Main tab-->Access Policy -->Portal Access*)	***Name***	Type a unique name
		Application URI	Type the URL of the Internal URL of the site (for example, http://tmg2010.example.com/owa) Click **Create**. Stay on the Portal Access page to add Resource item
	BIG-IP APM v10		
	Web Application (*Access Policy-->Web Applications*)	***Name***	Type a unique name All other fields are optional. Click **Create**. Stay on the Web Application page to add Resource item
Resource Items (*Web Application page-->Resource Items section-->Add*)	***Destination Type***	Click **Host Name** option button, if necessary.	
	Destination Host Name	Type the Host Name of the SharePoint site (for example dc.tmg2010.example.com.	
	Scheme	**HTTP**	
	Port	Type the appropriate port. We use 80.	
	Paths	Type **/***	
	Compression	**GZIP Compression** (optional)	
	SSO Configuration	Select the Basic SSO Configuration you created above.	
Connectivity Profile (***v11***: *Access Policy --> Secure Connectivity*) (***v10.x***: *Access Policy --> Connectivity Profiles*)	***Name***	Type a unique name	
	Parent Profile	**Connectivity**	
Webtop (*Access Policy--> Webtops*)	***BIG-IP APM v11***		
	Name	Type a unique name.	
	Type	**Portal Access**	
	Portal Access Start URI	http://ex.tmg2010.example.com/owa/auth/logon.aspx (replace red text with your URI)	
	BIG-IP APM v10		
	Name	Type a unique name.	
	Type	**Web Applications**	
	Web Application Start URI	http://ex.tmg2010.example.com/owa/auth/logon.aspx (replace red text with your URI)	

BIG-IP Object	Non-default settings		
Access Profile (*Access Policy-->Access Profiles*)	***Name***	Type a unique name	
	SSO Configuration	Select the SSO Configuration you created above	
Access Policy (*Access Policy-->Access Profiles*)	***Edit***	Edit the Access Profile you created using the VPE. See *Editing the Access Policy on page 24* for instructions.	
Profiles (*Local Traffic-->Profiles*)	***HTTP*** (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**http**
		Redirect Rewrite	**Matching**
	HTTP Compression (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**wan-optimized-compression**
	HTTP Class (*Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**httpclass**
		Application Security	**Enabled**
	TCP WAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	Rewrite Profile (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**rewrite** (in v11.4 and later:**Common/rewrite**) All other settings at default.
	Client SSL (*Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select your OWA Certificate and key
Virtual Server (*Local Traffic--> Virtual Servers*)	***Name***	Type a unique name.	
	IP Address	Type the IP clients use for access.	
	Service Port	**443**	
	Protocol Profile (client)	Select the WAN optimized TCP profile you created above	
	Protocol Profile (server)	Select the LAN optimized TCP profile you created above	
	HTTP Profile	Select the HTTP profile you created above	
	HTTP Compression Profile	Select the HTTP profile you created above	
	SSL Profile (Client)	Select the Client SSL profile you created above	
	SNAT Pool	**Auto Map** (if you expect more than 64,000 concurrent connections, create a SNAT Pool)	
	Access Profile	Select the Access profile you created and edited above	
	Connectivity Profile	Select the Connectivity profile you created above	
	Rewrite Profile	Select the Rewrite profile you created above	
	HTTP Class Profile	Select the HTTP Class profile you created above	

Editing the Access Policy

In the following procedure, we show you how to configure edit the Access Policy on the APM using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy. The Policy shown in the following procedure is just an example, you can use this Access Policy or create one of your own.

To configure the Access Policy

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you created, and then, in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.

4. Click the **Logon Page** option button, and then the **Add Item** button at the bottom.
5. Configure any of the options as applicable for your configuration. In our example, we leave the defaults.
6. Click the **Save** button.
7. Click the **+** symbol between **Logon Page** and **Deny**. A box opens with options for different actions.
8. Click the **AD Auth** option button, and then the **Add Item** button at the bottom.
9. From the **Server** list, select the AAA server you created above.
10. All other settings are optional. Click the **Save** button. You now see two paths, Successful and Fallback.
11. On the Successful path, click the + symbol between **AD Auth** and **Deny**.
12. Click the **SSO Credentials Mapping** option button, and then the **Add Item** button.
13. Configure any of the options as applicable for your configuration. In our example, we leave the defaults.
14. Click the **Save** button.
15. Click the **+** symbol between **SSO Credentials Mapping** and **Deny**.
16. ***For v11 Only***: Click the **Webtop and Webtop Links Assign** option button, and then the **Add Item** button.
    a. Click the **Add/Delete** link next to Webtop.
    b. Click the option button for the Webtop you created above.
    c. Click **Save**.
17. Click the + symbol between **Webtop and Webtop Links Assign** (or **SSO Credential Mapping** in v10.x) and **Deny**.
18. Click the **Resource Assign** option button, and then click the **Add Item** button.
19. The next steps depend on which version of the BIG-IP APM you are using:
    - ***v11***
      a. Click the **Add/Delete** Link next to **Portal Access Resources**.
      b. Check the box for the Portal Access object you created in the APM Access section of the table.
      c. Click the **Save** button.
    - ***v10***
      a. Click the **Add New Entry** button.
      b. Click the **Add/Delete Web Application Resources** link.
      c. Check the box for the Web Application you created in the APM Access section of the table.
      d. Click **Update**.
      e. Click the **Set Webtop** link.
      f. Check the box for the Webtop you created in the table.
      g. Click the **Save** button.
20. On the Fallback path after **Resource Assign** click the **Deny** box link.
21. Click the **Allow** option button, and then click **Save**.
22. Click the yellow **Apply Access Policy** link in the upper left part of the window. You must apply an access policy before it takes effect.

Configuring the BIG-IP LTM with TMG as a Forward Web Proxy

The follow table shows how to configure the BIG-IP system to send outbound traffic through Microsoft TMG servers. You can then use TMG's web and firewall policies to control access to the internet, as well as cache external content to accelerate performance.

The following are prerequisites for this scenario:

- Clients must set their default gateway to the BIG-IP LTM ***internal VLAN self IP***.
- Set TMG servers default gateway to BIG-IP LTM ***TMG VLAN self IP***.
- Configure the TMG devices using the guidance for outbound traffic found in *Threat Management Gateway Server configuration on page 3*.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (*Local Traffic-->Monitors*)	***Name***	Type a unique name
	Type	**Gateway ICMP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Transparent	**Yes**
	Alias Address	One or more external IP addresses
	Alias Service Port	***All Ports**
Pools (*Local Traffic -->Pools*)	***TMG device pool***	
	Name	Type a unique name
	Health Monitor	Select the ICMP monitor you created above
	Slow Ramp Time[1]	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the ***internal*** IP Address of a TMG device.
	Service Port	***All Ports** (click **Add** to repeat Address and Service Port for all nodes)
	Router pool	
	Name	Type a unique name
	Health Monitor	Select the HTTP monitor you created above
	Slow Ramp Time	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the IP Address of the External routers
	Service Port	**80** (click **Add** to repeat Address and Service Port for all nodes)
Local Traffic General Properties (*System -->Configuration--> Local Traffic-->General*)	***SNAT Packet Forwarding***	Select **All Traffic** from the list.
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**Outbound TCP - TMG**	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Address Translation	Uncheck the box to **Disable** Address Translation
	Port Translation	Uncheck the box to **Disable** Port Translation

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**Outbound TCP - TMG: Continued**	
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the Internal VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the TMG pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)
	Outbound UDP - TMG	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Protocol	Select **UDP** from the list.
	Address Translation	Uncheck the box to **Disable** Address Translation
	Port Translation	Uncheck the box to **Disable** Port Translation
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the Internal VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the TMG pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)
	Outbound TCP - Router	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Address Translation	Uncheck the box to **Disable** Address Translation
	Port Translation	Uncheck the box to **Disable** Port Translation
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the TMG VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the Router pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)
	Outbound UDP - Router	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Protocol	Select **UDP** from the list.
	Address Translation	Uncheck the box to **Disable** Address Translation
	Port Translation	Uncheck the box to **Disable** Port Translation
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the TMG VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the Router pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**L4 Performance - TMG**	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Type	**Performance (Layer 4)**
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the Internal VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the TMG pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)
	L4 Performance - Router	
	Name	Type a unique name.
	Destination Type	**Network** (option button)
	Address	**0.0.0.0** (this is a wildcard virtual server)
	Mask	Type the associated mask
	Service Port	***All Ports**
	Type	**Performance (Layer 4)**
	VLAN and Tunnel Traffic	Select **Enabled On** from the list.
	VLANs and Tunnels	Select the TMG VLAN and move it to the Selected box.
	SNAT Pool	**Automap**
	Default Pool	Select the Router pool you created above
	Default Persistence Profile	**dest_addr** (Destination Address Affinity)

This completes the forward proxy configuration.

Configuring logging on the BIG-IP LTM version 11 (optional)

In this section, we show you how to configure High Speed Logging on the BIG-IP version 11 and later (**ONLY**). This is optional, but provides visibility into network traffic you may find useful. To use this feature, you must configure a pool of logging servers and a logging profile.

Alternatively, you can configure ICSA logging. This will enable you to view real-time connection information on the BIG-IP; however, ICSA logging may impact performance. If you wish to enable logging permanently, we recommend you configure BIG-IP to send logs to a pool of logging servers as described in the following high speed logging section.

The following table shows the non-default settings for the BIG-IP objects related to high speed logging. For specfic information on configuring individual objects, see the online help or LTM documentation.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**UDP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name
	Health Monitor	Select the UDP monitor you created above
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the IP Address of a syslog server.
	Service Port	**514** (the default port for syslog, adjust if necessary) Repeat Address and Service port for all syslog devices.
Request Logging Profile (*Main tab-->Local Traffic -->Profiles-->Other*)	***Name***	Type a unique name
	Parent Profile	**request-log**
	Request Logging	**Enabled**
	Pool Name	Select the Pool of syslog servers you created above
	Response Logging	**Enabled**
	Pool Name	Select the Pool of syslog servers you created above

Configuring ICSA logging

In this section, we show you how to configure ICSA logging on the LTM. This is optional, but provides visibility into network traffic you may find useful. As mentioned, this may negatively impact performance.

To enable ICSA logging, you must have command line access to the BIG-IP system. You can then view the logs from the web-based Configuration utility or the command line.

To enable ICSA monitoring

1. Log on to the BIG-IP system from the command line.
2. Type the following command to enter the TMSH shell: **tmsh**
3. Once in TMSH, type **sys**
4. Type the following command:

   ```
   modify db tmm.lognonsessionpackets value enable
   ```

5. Type the following command:

   ```
   modify db icsa.forceadminpacketlogging value enable
   ```

6. You can now exit the command line.

To view the logs from the Configuration utility, on the Main tab, expand **System**, click **Logs**, and then on the menu bar, click **Local Traffic**.

To view the logs from the command line, check **/var/log/ltm**. For example, to view packets to and from 192.168.1.1, you could type the command: **tail -f /var/log/ltm | grep 192.168.1.1**

Document Revision History

Version	Description	Date
1.0	New document	10-25-2011
1.1	Updated the WMI monitor configuration with the proper URL to the script file (**/scripts/F5Isapi.dll**).	05-24-2012
1.2	Added support for BIG-IP versions 10.2.3, 10.2.4, 11.0.1, 11.1, and 11.2.	07-23-2012
1.3	- Added support for BIG-IP versions 11.3 - 11.4.1. - Added Rewrite profile configuration in the profile section of the BIG-IP APM configuration tables	11-22-2013
1.4	- Added support for BIG-IP versions 11.5 and 11.5.1. - Updated the BIG-IP APM configuration table on *page 19* with changes for BIG-IP APM 11.5 and later.	04-04-2014

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com