BROCADE

DEPLOYMENT GUIDE

Brocade Virtual Traffic Manager and Microsoft Exchange 2010 Deployment Guide

53-1004909-02
27 February 2017

Contents

Preface

About This Guide

The *Brocade Virtual Traffic Manager and Microsoft Exchange 2010 Deployment Guide* describes how to configure Brocade Virtual Traffic Manager (Brocade vTM) to load-balance and optimize Microsoft Exchange 2010 Client Access Servers (CASs). This deployment guide is designed to be used together with the Brocade vTM documentation.

For more details on the Brocade vADC product family, see http://www.brocade.com/vADC.

Audience

This guide is written for network administrators, Microsoft Exchange administrators, and developer operations (DevOps) professionals who are familiar with administering and managing both application delivery controllers (ADCs) and Microsoft Exchange network protocols including HTTP, SMTP, POP, and IMAP. You should also be familiar with installing and configuring a virtual appliance in a virtual VMware, Hyper-V, or dedicated Linux environment.

About Brocade

Brocade® (NASDAQ: BRCD) networking solutions help the world's leading organizations transition smoothly to a world where applications and information reside anywhere. This vision is designed to deliver key business benefits such as unmatched simplicity, non-stop networking, application optimization, and investment protection.

Innovative Ethernet and storage networking solutions for data center, campus, and service provider networks help reduce complexity and cost while enabling virtualization and cloud computing to increase business agility.

To help ensure a complete solution, Brocade partners with world-class IT companies and provides comprehensive education, support, and professional services offerings (www.brocade.com).

Contacting Brocade

This section describes how to contact departments within Brocade.

Internet

You can learn about Brocade products through the company website: http://www.brocade.com.

Technical Support

If you have problems installing, using, or replacing Brocade products, contact Brocade Support or your channel partner who provides support. To contact Brocade Support, see http://www.brocade.com/en/support.html.

Professional Services

Brocade Global Services has the expertise to help organizations build scalable and efficient cloud infrastructures. Leveraging 15 years of expertise in storage, networking, and virtualization, Brocade Global Services delivers world-class professional services, technical support, and education services, enabling organizations to maximize their Brocade investments, accelerate new technology deployments, and optimize the performance of networking infrastructures.

Document History

Date	Part Number	Description
December 2016	53-1004909-01	Initial release.
February 2017	53-1004909-02	Added vWAF and Web Accelerator content.

Solution Overview

This chapter describes how Brocade Virtual Traffic Manager provides advanced load balancing and application delivery controller features for Microsoft Exchange 2010; the factors that you must consider when designing your Virtual Traffic Manager deployment; and how and when to implement the most commonly used features.

Brocade Virtual Traffic Manager Overview

Brocade Virtual Traffic Manager (Brocade vTM) is a software-based application delivery controller (ADC) designed to deliver faster and more reliable access to public websites and private applications. Brocade vTM frees applications from the constraints of legacy, proprietary, hardware-based load balancers, which enables them to run in any physical, virtual, or cloud environment. With vADC products from Brocade, organizations can:

- Make applications more reliable with local and global load balancing.
- Scale application servers by up to 3x by offloading TCP and SSL connection overhead.
- Accelerate applications by up to 4x by using web content optimization (WCO).
- Secure applications from the latest application attacks, including SQL injection, XSS, CSRF, and more.
- Control applications effectively with built-in application intelligence and a full-featured scripting engine.

Virtual Traffic Manager offers much more than basic load balancing. It controls and optimizes end-user services by inspecting, transforming, prioritizing, and routing application traffic. The powerful TrafficScript® engine facilitates the implementation of traffic management policies that are unique to an application by allowing organizations to build custom functionality or to leverage existing features in Virtual Traffic Manager in a specialized way. With vTM, organizations can deliver the following:

- **Performance**—Improve application performance for users by offloading encryption and compression from the web server by dynamic caching and reducing the number of TCP sessions on the application.
- **Reliability and Scalability**—Increase application reliability by load-balancing traffic across web and application servers, balancing load across multiple data centers (private or public clouds), monitoring the response time of servers in real-time to decide the fastest way to deliver a service, protecting against traffic surges, and managing the bandwidth and rate of requests used by different classes of traffic.
- **Advanced Scripting and Application Intelligence**—Manage application delivery more easily with fine-grained control of users and services using TrafficScript, an easy-to-use scripting language that can parse any user transaction and take specific, real-time action based on the user, application, request, or more. Development teams use TrafficScript to enable a point of control in distributed applications, whereas operations teams use it to quickly respond to changing business requirements or problems within an application before developers can fix it.
- **Application Acceleration**—Dramatically accelerate web-based applications and websites in real-time with optional web content optimization (WCO) functionality. It dynamically groups activities for fewer long-distance round trips, resamples and sprites images to reduce bandwidth, and minifies and compresses JavaScript and combines style sheets to give the best possible response time for loading a web page on any browser or device.
- **Application-Layer Security**—Enhance application security by filtering out errors in web requests and protecting against external threats, with the option of a comprehensive Layer 7 firewall to defend against deliberate attacks.

What's New in Microsoft Exchange 2010

Microsoft Exchange 2010 has two primary components: Client Access Server (CAS) and Database Availability Group, which consists of Mailbox Servers. The Client Access Server's primary role is as a proxy that connects and authenticates clients to the Exchange 2010 Mailbox Server. The Mailbox Server is responsible for rendering all data, including rendering web content and routing e-mail. As the result of this change, persistence (sticky sessions) is not required on load balancers, since the CAS is a stateless proxy server for connecting clients to a Mailbox Server.

Built to deliver the enterprise-grade security and reliability that businesses require, Microsoft Exchange provides e-mail, calendar, and contacts on your PC, phone, and web browser:

- Support for a variety of browsers, including Internet Explorer, Firefox, Safari, and Chrome, allows you to work and collaborate no matter where you are.
- Mobile sync to hundreds of devices, including Windows Phone, iPhone, and Android, means that you can access and update your info while on the go.
- Multilayered anti-spam filtering with continuous updates helps guard against spam and phishing threats.
- A new, unified approach to high availability and disaster recovery helps your business achieve increased levels of reliability.

There are a number of services that run under Exchange 2010. A good number of these services use HTTP/HTTPS (TCP ports 443 and 80) for their transport; for example, Outlook Web App, Exchange ActiveSync, Outlook Anywhere, and Exchange Web Services. Depending on the client software used in the environment, POP3 and IMAP4 may also be required (TCP ports 110 and 143 unencrypted; 993 and 995 under SSL).

Other Exchange services, such as RPC Client Access and Exchange Address Book, are RPC services. When an Outlook client connects directly to the Client Access Server using these protocols, instead of using Outlook Anywhere, the endpoint TCP ports for these services are allocated by the RPC endpoint manager. Allocation occurs when the services are started. This allocation is based on a "random" port being selected from a range. The Virtual Traffic Manager configuration requires that a node be added to the pool using the IP address and port number, but, if the TCP port is not known beforehand, this pool configuration cannot be added. Therefore, a static port mapping must be made for the RPC services.

Why Brocade vTM to Load-Balance and Optimize Microsoft Exchange 2010

Brocade Virtual Traffic Manager has significant advantages over other ADCs for load-balancing and optimizing Microsoft Exchange 2010.

Application-Centric View

- Ability to deploy a separate ADC per application or tenant
- Ability to dynamically right-size the Brocade virtual deployment to fit the application needs
- Dynamic provisioning and scaling of ADC resources

Designed with Service Providers in Mind

- 64-bit software that can be deployed in a VMware or Hyper-V environment or as a dedicated software installation, instead of a physical appliance
- Multicore packet processing for scalability

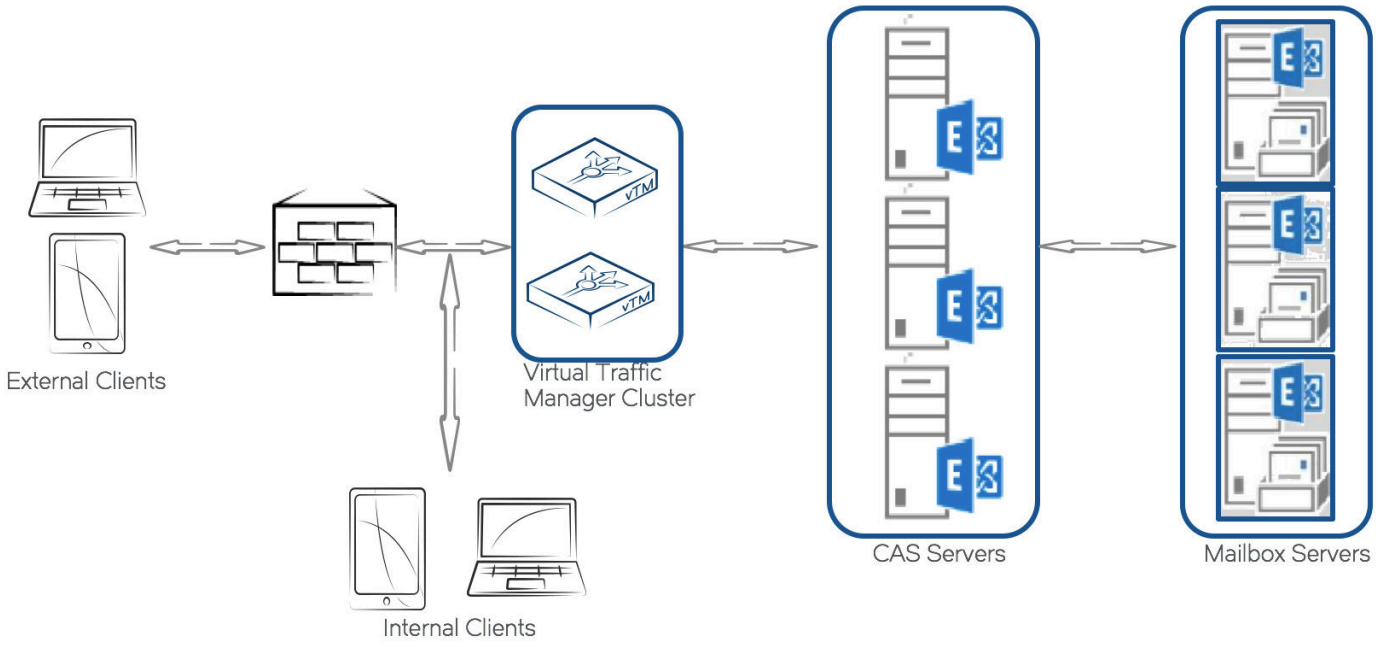
- Robust APIs for simple automated provisioning and management

Designed for Services

- Global load balancing, SSL offload, caching, and service-level management
- Application firewalling and web content optimization
- Robust and open APIs

Microsoft Exchange 2010 Architecture

Brocade Virtual Traffic Manager can be easily deployed to an existing network infrastructure with little to no changes required on the network. DNS configuration is used to redirect traffic for Outlook clients to Brocade Virtual Traffic Manager. Brocade vTMs can be clustered to provide high availability and load balancing to support a large amount of traffic and fault tolerance.



Deploying Microsoft Exchange 2010 Servers

To ensure that the Microsoft Exchange 2010 services are set up properly for load-balancing Exchange 2010, the configuration steps are provided below. For detailed information on how to deploy or configure Microsoft Exchange 2010, refer to appropriate Microsoft documentation.

Setting Up the Microsoft Exchange 2010 CAS Array

Microsoft Exchange 2010 CAS servers must be set up as a CAS array first so that they can be set up behind Traffic Manager for load balancing. Refer to documentation on Microsoft Exchange 2010 and to the TechNet article that explains the steps involved in setting up a CAS array (http://blogs.technet.com/b/ucedsg/archive/2009/12/06/how-to-setup-an-exchange-2010-cas-array-to-load-balance-mapi.aspx).

RPC Client Access (MAPI)

Configuring Static Port Mapping for RPC-Based Services

The following information is taken directly from Microsoft's TechNet website located at:

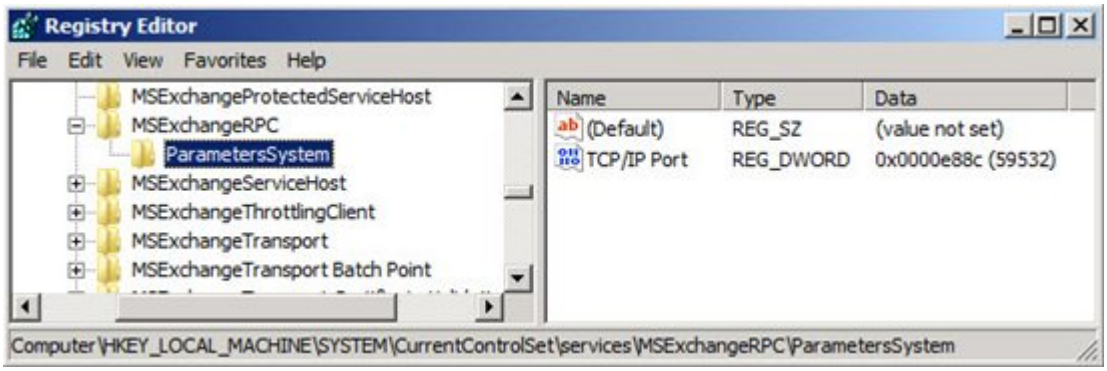
http://social.technet.microsoft.com/wiki/contents/articles/configure-static-rpc-ports-on-an-exchange-2010-client-access-server.aspx

By default, the RPC Client Access service on an Exchange 2010 Client Access server uses the TCP End Point Mapper port (TCP/135) and the dynamic RPC port range (6005–59530) for outgoing connections, every time an Outlook client establishes a connection to Exchange. There are two static port mappings needed, the configuration of which is described below. To set a static port for the RPC Client Access service on an Exchange 2010 Client Access server, open the registry on the respective server and navigate to:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeRPC

Here, create a new key named **ParametersSystem**, and under this key create a **REG_DWORD** named **TCP/IP Port**. The value for **DWORD** should be the port number that you want to use.

FIGURE 1 Configuring a Static Port for the RPC Client Access Service



NOTE
Microsoft recommends that you set this to a unique value between 59531 and 60554 and use the same value on all CASs in any one AD site.

When you've configured the port, you must restart the Microsoft Exchange RPC Client Access service in order for the changes to be applied.

Exchange 2010 Address Book Service

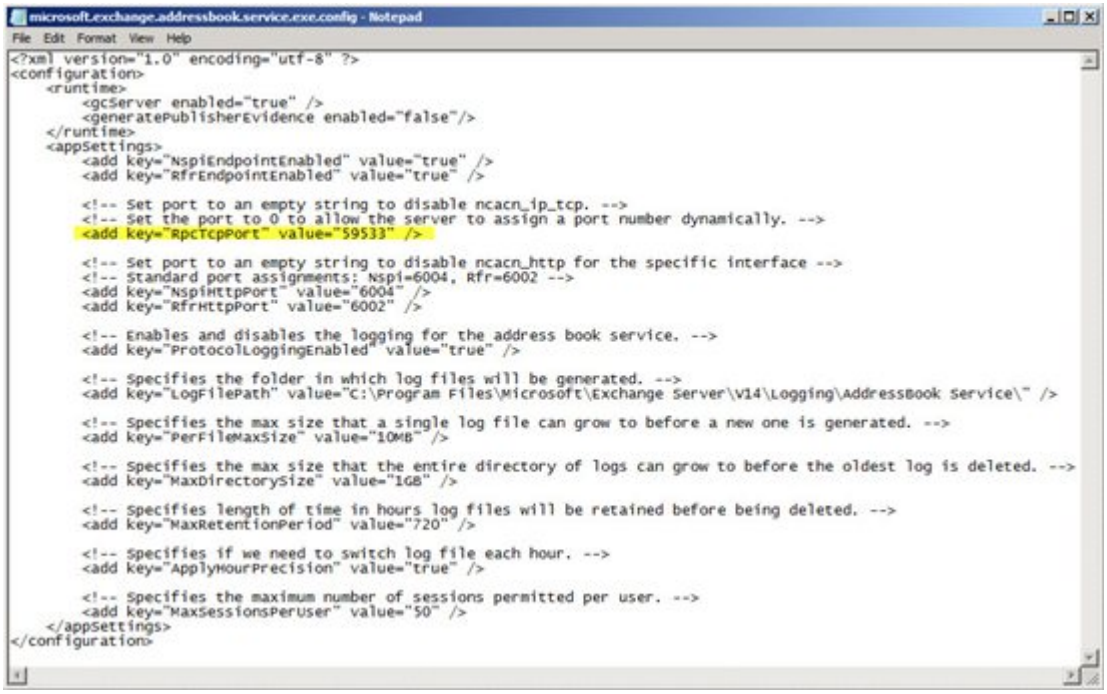
By default, the Exchange Address Book service on an Exchange 2010 Client Access server uses the TCP End Point Mapper (TCP/135) and the dynamic RPC port range (6005–59530) for outgoing connections, every time an Outlook client establishes a connection to Exchange.

Exchange 2010 RTM

In Exchange 2010 RTM, a static port for the Exchange Address Book service is set using the following steps:

1. Using Notepad, open the microsoft.exchange.addressbook.service.exe.config configuration file located in C:\Program Files \Microsoft\Exchange Server\V14\Bin.
2. Change the value for the key **RpcTcpPort** to the port that you want to use as the static port for this service. Remember that you cannot use the same port that you configured for the RPC Client Access service.

FIGURE 2 Configuring a Static Port for the Exchange Address Book Service in Exchange 2010 RTM



NOTE
Microsoft recommends that you set this to a unique value between 59531 and 60554 and that you use the same value on all Exchange 2010 Client Access servers in any one AD site.

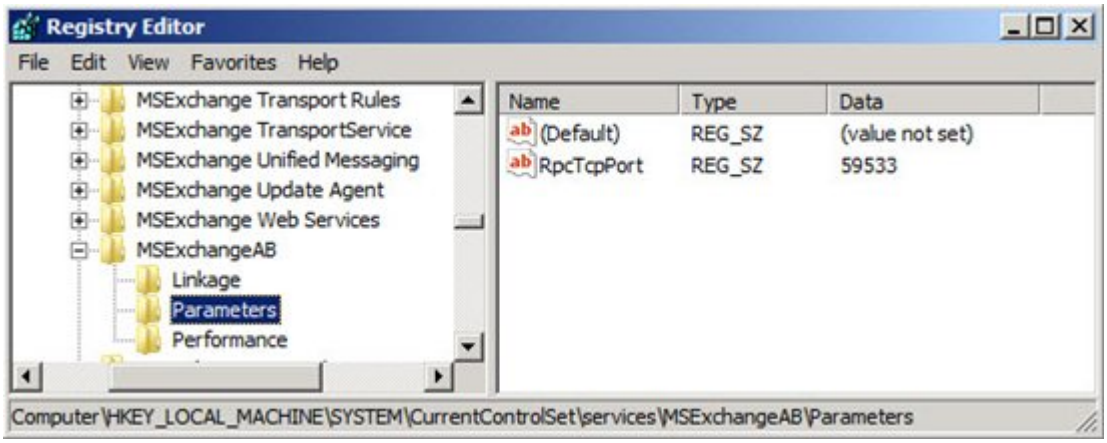
3. When you've configured the port, restart the Microsoft Exchange Address Book service in order for the changes to be applied.

Exchange 2010 SP1

1. With Exchange 2010 SP1, you no longer use the Microsoft.exchange.addressbook.service.exe.config file to assign a static RPC port to the Exchange Address Book service. Instead, this configuration setting is controlled using the registry. To set a static RPC port for the Exchange Address Book service, create a new **REG_SZ** registry key named **RpcTcpPort** under:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeAB\Parameters

FIGURE 3 Configuring a Static Port for the Exchange Address Book Service in Exchange 2010 SP1



IMPORTANT
When upgrading from Exchange 2010 RTM to SP1, set this key manually after the upgrade.

NOTE
Microsoft recommends that you set this to a unique value between 59531 and 60554 and use the same value on all Exchange 2010 Client Access servers in any one AD site.

2. When you've configured the port, restart the Microsoft Exchange Address Book service in order for the changes to be applied.

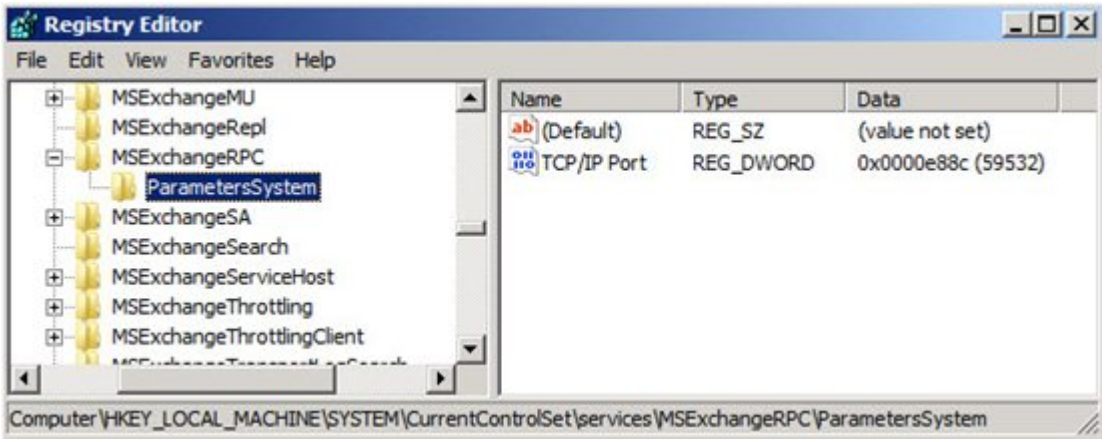
Exchange 2010 Public Folder Connections

By default, public folder connections use the TCP End Point Mapper (TCP/135) and the dynamic RPC port range (49152–65535) for outgoing connections, every time an Outlook client establishes a connection to Exchange.

NOTE
Exchange 2010 public folder connections from the Outlook client directly occur with the Mailbox server, and the configuration below is not relevant for the Virtual Traffic Manager. Follow the below section only if you want to assign a static port for public folder access from clients.

To set a static port for public folder connections, follow the same steps as those required to configure static ports for the RPC CA service. Just bear in mind that you must perform the steps on the Exchange 2010 servers that store public folder databases. This is because public folder connections from an Outlook client occur against the RPC Client Access service on the Mailbox server role.

FIGURE 4 Configuring a Static Port for Public Folder Connections



When the port has been set for public folder connections, restart the Microsoft Exchange RPC Client Access service on the Mailbox server in order for the changes to be applied.

NOTE

Unlike previous versions of Exchange Server, you configure static RPC ports for an Exchange 2010 Mailbox server under the MSExchangeRPC key and not under MSExchangeSA\Parameters since all MAPI connections to an Exchange 2010 Mailbox server are handled by the RPC Client Access service. For information on configuring static RPC ports in Exchange 2007 and earlier, see the Microsoft KB article: Exchange Server static port mappings.

Changing the External URLs of Exchange HTTP Services for Respective Virtual Directories on a CAS IIS Server

The following is a list of EMS (Exchange Management Shell) cmdlets that can be used to set up the external URLs for all Exchange applications.

Outlook Web App (OWA)

```
Set-OwaVirtualDirectory -Identity "CAS_Server\OWA (Default Web Site)" -ExternalURL https://
mail.domain.com/OWA
```

Exchange Control Panel (ECP)

```
Set-EcpVirtualDirectory -Identity "CAS_Server\ECP (Default Web Site)" -ExternalURL https://
mail.domain.com/ECP -FormsAuthentication $True -BasicAuthentication $True
```

Exchange ActiveSync (EAS)

```
Set-ActivesyncVirtualDirectory -Identity "CAS_Server \Microsoft-Server-ActiveSync (Default Web
Site)" -ExternalURL https://mail.domain.com/Microsoft-Server-Activesync -BasicAuthentication $True
```

Offline Address Book (OAB)

```
Set-OABVirtualDirectory -Identity "CAS_Server\oab (Default Web Site)" -ExternalUrl https://
mail.domain.com/oab
```

Exchange Web Services (EWS)

```
Set-WebServicesVirtualDirectory -Identity "CAS_Server\EWS (Default Web Site)" -ExternalUrl https://
mail.domain.com/ews/exchange.asmx
```

Unified Messaging (UM)

```
Set-UMVirtualDirectory -Identity "CAS_Server\unifiedmessaging (Default Web Site)" -InternalUrl
https://mail.domain.com/unifiedmessaging/service.asmx
```

Deploying Brocade Virtual Traffic Manager

This chapter describes the procedures for deploying Brocade Virtual Traffic Manager for load-balancing and optimizing Microsoft Exchange 2010 Client Access Servers (CASs).

Requirements

- Brocade Virtual Traffic Manager (10.1 or later)
- Microsoft Exchange 2010

Configuring OWA

This section walks through the steps required to configure Outlook Web App on a dedicated/separate traffic IP group.

Component	Procedure	Description
Virtual Traffic Manager	Creating a Traffic IP Group for OWA	A traffic IP group must be created for OWA. For details, see Creating Traffic IP Groups on page 16.
	Creating a Pool for OWA	Enter the hostname or IP address of the CAS server nodes along with the port number. For details, see Creating Pools on page 17.
	Selecting a Monitor for the Pool	Select a health monitor for the pool. For details, see Creating Monitors on page 17.
	Creating a Virtual Server for OWA	Create and associate the virtual server to the server pool of choice and the traffic IP group to listen on. For details, see Creating Virtual Servers on page 18.
	Configuring SSL Decryption	Configure SSL Decryption to enable SSL offloads. For details, see Configuring SSL Decryption on page 18.
	Configuring Session Persistence for OWA Pool	Transparent Session Affinity persistence is required for the OWA pool. For details, see Configuring Session Persistence on page 18.
	Creating and Associating a Traffic Script That Forwards HTTP Requests to SSL	Configure a traffic script to forward HTTP requests to SSL. For details, see Creating and Associating a Traffic Script on page 19.

Creating Traffic IP Groups

Identify Exchange HTTP services being offered by CAS servers, and create a traffic IP group for each service. Create a traffic IP group (also known as a virtual IP) on which the virtual server will be listening.

1. Navigate to **Services** > **Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.

2. Fill in the fields as follows:
   - **Name**—A descriptive name for the traffic IP group (e.g., owa.company.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of this service
3. Click the **Create Traffic Group** button.

Creating Pools

For each of the identified Exchange HTTP services, create a pool using the following steps.

1. Navigate to **Services** > **Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name**—A descriptive name for the pool. (e.g., OWA Service)
   - **Nodes**—hostname:80 or ipaddress:80
   - **Monitor**—No Monitor (This will be covered in detail in later section.)
3. In the next screen, click **Load Balancing**.
4. Under **Algorithm**, select **Perceptive**.
5. Click the **Update** button to apply changes.
6. Click **SSL Settings**.
7. Check the **Yes** button next to **ssl_encrypt**.
8. Click the **Update** button to apply changes.

Creating Monitors

This section details the steps to create health monitors.

> NOTE
> Advanced external monitors can be written in any language of choice and be associated with the pool. Create a health monitor that will monitor the health of a pool.

1. Navigate to **Catalogs** > **Monitors**.
2. Scroll down to **Create new monitor**.
3. Give the new monitor a descriptive name.
4. Set the type to **HTTP monitor** and the scope to **Node**.
5. Click **Create Monitor** to create the monitor.
6. Change **host_header** to the service URL path (e.g., owa.company.com).
7. Change **Path**: to **/owa**.
8. Change **status_regex** to **^200$**.
9. Scroll down to **Apply Changes** and click the **Update** button.
10. Navigate to **Services** > **Pools** and select the pool that the monitor will be attached to.
11. Scroll down and click **Health Monitoring**.
12. Add the appropriate health monitor.

Creating Virtual Servers

For OWA, create a virtual server using the following steps.

1. Navigate to **Services** > **Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name**—A descriptive name for the virtual server (e.g., owa.company.com)
   - **Protocol**—HTTP
   - **Port**—443
   - **Default Traffic Pool**—The pool created for this service in the previous section
3. Click **Create Virtual Server**.
4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the appropriate traffic IP group that was created for the OWA service.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply changes.

Configuring SSL Decryption

To perform SSL decryption, the certificate and the private key used for the virtual server created previously must be imported into the Traffic Manager.

1. Navigate to **Catalogs** > **SSL** > **SSL Certificates catalog**.
2. Click **Import Certificate** to import the appropriate certificate.

   After importing the certificate, enable SSL decryption on the virtual server created.
3. Navigate to **Services** > **Virtual Servers** and select the virtual server created for OWA that will be performing SSL decryption.
4. Scroll down and click **SL Decryption**.
5. Set **ssl_decrypt** to **Yes**.
6. Select the certificate imported in Step 2.
7. Scroll down to the bottom of the page and click **Update**.

Configuring Session Persistence

Transparent session affinity persistence is required for the OWA pool. To configure session persistence.

1. Navigate to **Catalogs** > **Persistence**.
2. Provide a descriptive name for the persistence class.
3. Click **Create Class**.
4. Select **Transparent session affinity** in **Basic Settings**.
5. Click **Update** to apply changes.
6. Navigate to **Services** > **Pools** and select the appropriate pool that was created earlier.
7. Navigate to **Session Persistence** and click **Edit**.
8. Select the session persistence class created, and click **Update** to apply changes.

Creating and Associating a Traffic Script

Since vTM will be handling SSL traffic only for OWA, clients who try to access using HTTP should be redirected to connect back on SSL. The following steps walk through the configuration of the virtual server with a traffic script that will redirect all clients trying to connect on port http.

1. Create a new virtual server by navigating to **Services** > **Virtual Servers**.
2. Set the port to **80** and pool to **Discard**.
3. Navigate to **Catalogs** > **Rules**.
4. Create a new rule:
   - **Name**—A descriptive name for the rule (e.g., OWA Rule)
   - Use TrafficScript Language
5. Click **Create Rule**.
6. Use the TrafficScript as shown here.

```
#// TS Rule for redirecting OWA HTTP traffic to use SSL
$debug = 0; // Change value to 1 if debug needed
$hostheader = http.getHostHeader();
if( http.getPath() == "/" ) {
    if ($debug > 0) { log.info("Redirecting OWA service to use https");}
    http.redirect( "https://".$hostheader."/owa" );
}
```

7. Click the **Update** button.
8. Navigate to **Services** > **Virtual Servers** and select the virtual server created for SharePoint apps that will be performing the TrafficScript created.
9. Scroll down and click **Rules**.
10. Assign the TrafficScript to the request rules by clicking **Add Rule**.

Configuration Summary

By accessing **Services** > **Config Summary** on the web GUI, a complete snapshot of all configured services is provided. This is a very useful table to glance through to get a good understanding of how the services are configured.

Configuring Outlook Anywhere

Outlook Anywhere for Exchange 2010 allows you to use Microsoft Outlook clients to connect to your Exchange server over the Internet, using HTTPS to encapsulate RPC (MAPI) traffic. This section walks through the steps required to configure Outlook Anywhere on a dedicated/separate traffic IP group.

NOTE

To enable and require SSL for all communications between the Client Access server and the Outlook clients, a trusted certificate signed by a certificate authority should be obtained and published at the default website level. It is recommended that the certificate be purchased from a third-party certification authority whose certificates are trusted by a wide variety of web browsers. By default, applications and web browsers do not trust a root certification authority when there is an internal/non-trusted certification authority, such as a Virtual Traffic Manager self-signed certificate. When a user tries to connect to Microsoft Outlook by using Outlook Anywhere, and the user's computer does not trust the certificate and root certificate authority, the connection fails. For more information on this topic, see the following Microsoft TechNet article: http://technet.microsoft.com/en-us/library/aa997703.aspx.

Component	Procedure	Description
Virtual Traffic Manager	Creating a Traffic IP Group for the Outlook Anywhere Service	A traffic IP group must be created for Outlook Anywhere. For details, see Creating Traffic IP Groups on page 20.
	Creating a Pool for the Outlook Anywhere Service	Enter the hostname or IP address of the CAS server nodes along with the port number. For details, see Creating Pools on page 20.
	Selecting a Monitor for the Pool	Select a health monitor for the pool. For details, see Creating Monitors on page 21.
	Creating a Virtual Server for the Outlook Anywhere Service	Create and associate the virtual server to the server pool of choice and the traffic IP group to listen on. For details, see Creating Virtual Servers on page 21.
	Configuring SSL Decryption	Configure SSL decryption to enable SSL offloads. For details, see Configuring SSL Decryption on page 22.
	Configuring Session Persistence for the Outlook Anywhere Service	Universal session affinity persistence is required for the Outlook Anywhere service. For details, see Configuring Session Persistence on page 22.

Creating Traffic IP Groups

Create a traffic IP group (also known as a virtual IP) for the Outlook Anywhere service on which the virtual server will be listening. To create a new traffic IP group.

1. Navigate to **Services** > **Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.
2. Fill in the fields as follows:
   - **Name**—A descriptive name for the traffic IP group (e.g., oa.company.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of this service
3. Click the **Create Traffic Group** button.

Creating Pools

For the Outlook Anywhere service, create a pool using the following steps.

1. Navigate to **Services** > **Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name**—A descriptive name for the pool. (e.g., OA Service)
   - **Nodes**—hostname:80 or ipaddress:80
   - **Monitor**—No Monitor (This will be covered in detail in a later section.)
3. In the next screen, click **Load Balancing**.
4. Under **Algorithm**, select **Perceptive**.
5. Click the **Update** button to apply changes.

Creating Monitors

This section details the steps to create health monitors.

The TCP transaction monitor enables vTM to send a customer URL string. Since there are no authentication headers in the request sent to the server, the expected response is to get a page that states, "You do not have permission to access this page." Also, external Perl scripts can be written and associated with this monitor. At a minimum, set the monitor to **TCP Connect** if only Layer 4 monitoring is needed.

1. Navigate to **Catalogs** > **Monitors**.
2. Scroll down to **Create new monitor**.
3. Give the new monitor a descriptive name.
4. Set the type to **TCP transaction monitor** and the scope to **Node**.
5. Click **Create Monitor** to create the monitor.
6. Under **Advanced settings** of the monitor, change the **write-string** based on the FQDN used. For example:

```
RPC_IN_DATA /rpc/rpcproxy.dll?oa.company.com:6001 HTTP/1.1\r
User-Agent: MSRPC\r
Host: oa.company.com\r
```

7. Change **response_regex**: to **do not have permission**.
8. Scroll down to **Apply Changes** and click the **Update** button.
9. Navigate to **Services** > **Pools** and select the pool that the monitor will be attached to.
10. Scroll down and click **Health Monitoring**.
11. Add the appropriate health monitor.

Creating Virtual Servers

For the Outlook Anywhere service, create a virtual server using the following steps.

1. Navigate to **Services** > **Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name**—A descriptive name for the virtual server (e.g., oa.company.com)
   - **Protocol**—HTTP
   - **Port**—443
   - **Default Traffic Pool**—The pool created for this service in the previous section
3. Click **Create Virtual Server**.
4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the appropriate traffic IP group that was created for the Outlook Anywhere service.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply changes.

   Note that the port is configured as 443, whereas the protocol is HTTP. This is due to the fact that Traffic Manager will be offloading SSL from the Microsoft Exchange 2010 CAS servers. In order to configure SSL offloading on the CAS servers for all HTTP-based applications (OWA, ECP, EWS, OAB), follow the guidelines highlighted at http://social.technet.microsoft.com/wiki/contents/articles/how-to-configure-ssl-offloading-in-exchange-2010.aspx.

Configuring SSL Decryption

To perform SSL decryption, the certificate and the private key used for the virtual server created in the previous section must be imported into the Traffic Manager.

1. Navigate to **Catalogs** > **SSL** > **SSL Certificates catalog**.
2. Click **Import Certificate** to import the appropriate certificate.

   After importing the certificate, enable SSL decryption on the virtual server created.
3. Navigate to **Services** > **Virtual Servers** and select the virtual server created for the Outlook Anywhere service that will be performing SSL decryption.
4. Scroll down and click **SSL Decryption**.
5. Set **ssl_decrypt** to **Yes**.
6. Select the certificate imported in Step 2.
7. Scroll down to the bottom of the page and click **Update**.

Configuring Session Persistence

Outlook Anywhere requires persistence as clients split the RPC connections into two (RPC_IN_DATA and RPC_OUT_DATA). If the CAS servers are behind a load balancer, load balancer must make sure that both connections are sent to the same CAS server. Traffic Manager's Universal Persistence type is used to create persistence records based on the type of the client accessing the service. The reason for tracking a different type of Outlook client is that some of the older versions of Outlook clients (before Outlook 2010) do not support the OutlookSession cookie. So for these older versions of Outlook clients, the value of the Authorization HTTP header is used to create persistence records, and for clients from Outlook 2010, persistence records are created using the OutlookSession cookie. The settings for configuring the session persistence and the TrafficScript used are documented below. Note that the persistence configuration steps highlighted in this document are for the BASIC AUTH authentication method and not for NTLM.

1. Navigate to **Catalogs** > **Persistence**.
2. Provide a descriptive name for the persistence class.
3. Click **Create Class**.
4. Select **Universal Session Persistence** under **Basic Settings**.
5. Click **Update** to apply changes.
6. Navigate to **Services** > **Pools** and select the appropriate pool that was created earlier.
7. Navigate to **Session Persistence** and click **Edit**.
8. Select the **Session Persistence Class** created, and click **Update** to apply the changes.
9. Navigate to **Catalogs** > **Rules**.
10. Create a new rule:
    - **Name**—A descriptive name for the rule (e.g., OA Rule)
    - Use TrafficScript Language
11. Click **Create Rule**.

12. Use the TrafficScript as shown here:

```
#// TS Rule for Session Persistence
$debug = 0; // Change value to 1 if debug needed
# Extract the value of Authorization header and OutlookSession cookie
$auth = http.getHeader( "Authorization" );
$outlooksession = http.getCookie( "OutlookSession" );

# Please declare the names of the session persistence classes you have created
$universal_session_persistence  = "Exchange 2010 Outlook Anywhere Persistence";

# Validating if the cookie named OutlookSession exists and has value to track Outlook 2010 clients
and create persistence based on the cookie value as the key

if ( $outlooksession) {
if ($debug > 0) { log.info("Exchange control panel persistence based on outlooksession cookie");}
connection.setPersistence( $universal_session_persistence );
connection.setPersistenceKey( $outlooksession);
}
# Create persistence records for all other clients based on the value of Authorization header
else {
if ($debug > 0) { log.info("Exchange control panel persistence based on auth header");}
connection.setPersistence( $universal_session_persistence );
connection.setPersistenceKey( $auth);
}
```

13. Click the **Update** button.
14. Navigate to **Services** > **Virtual Servers** and select the virtual server created for the Outlook Anywhere service.
15. Scroll down and click **Rules**.
16. Assign the TrafficScript to the request rules by clicking **Add Rule**.

Configuration Summary

By accessing **Services** > **Config Summary** on the web GUI, a complete snapshot of all configured services is provided. This is a very useful table to glance through to get a good understanding of how the services are configured.

Configuring ActiveSync

Exchange ActiveSync is a synchronization protocol based on HTTP and XML that is designed to work over a cellular, wireless Internet or other similar low-bandwidth, high-latency connections. Exchange ActiveSync can synchronize e-mail messages, contacts, calendar, and task data.

This section walks through the steps required to configure ActiveSync on a dedicated/separate traffic IP group.

Component	Procedure	Description
Virtual Traffic Manager	Creating a Traffic IP Group for the Outlook Anywhere Service	A traffic IP group must be created for Outlook Anywhere. For details, see Creating Traffic IP Groups on page 24.
	Creating a Pool for the ActiveSync Service	Enter the hostname or IP address of the CAS server nodes along with the port number. For details, see Creating Pools on page 24.
	Selecting a Monitor for the Pool	Select a health monitor for the pool. For details, see Creating Monitors on page 24.
	Creating a Virtual Server for the ActiveSync Service	Create and associate the virtual server to the server pool of choice and the traffic IP group to listen on. For details, see Creating Virtual Servers on page 25.
	Configuring SSL Decryption	Configure SSL decryption to enable SSL offloads. For details, see Configuring SSL Decryption on page 25.

Component	Procedure	Description
	Configuring Session Persistence for the ActiveSync Service	Universal session affinity persistence is required for the ActiveSync service. For details, see Configuring Session Persistence on page 25.

Creating Traffic IP Groups

Create a traffic IP group (also known as a virtual IP) for the ActiveSync service on which the virtual server will be listening.

1. Navigate to **Services** > **Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.
2. Fill in the fields as follows:
   - **Name**—A descriptive name for the traffic IP group (e.g., activesync.company.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of this service
3. Click the **Create Traffic Group** button.

Creating Pools

For the ActiveSync service, create a pool using the following steps.

1. Navigate to **Services** > **Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name**—A descriptive name for the pool. (e.g., ActiveSync Service)
   - **Nodes**—hostname:80 or ipaddress:80
   - **Monitor**—No Monitor (This will be covered in detail in a later section.)
3. Click the **Update** button to apply the changes.

Creating Monitors

This sections details the steps to create health monitors.

Fill in the FQDN of ActiveSync service. Since the request is not sending any authentication credentials, the expected response is the "Access is denied" page, which is what response_regex is catching to mark the health of the server. Advanced external monitors can be written in any language of choice and be associated with the pool.

1. Navigate to **Catalogs** > **Monitors**.
2. Scroll down to **Create new monitor**.
3. Give the new monitor a descriptive name.
4. Set the type to **TCP transaction monitor** and the scope to **Node**.
5. Click **Create Monitor** to create the monitor.
6. In **Advanced settings** of the monitor, change the **write-string** based on the FQDN used. For example:

```
GET /Microsoft-Server-ActiveSync/ HTTP/1.1\r
Host: activesync.company.com\r
\r
```

7. Change **response_regex**: to **.*Access is denied**.
8. Scroll down to **Apply Changes** and click the **Update** button.
9. Navigate to **Services** > **Pools** and select the pool that the monitor will be attached to.

10. Scroll down and click **Health Monitoring**.
11. Add the appropriate health monitor.

Creating Virtual Servers

For the ActiveSync service, create a virtual server using the following steps.

1. Navigate to **Services** > **Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name**—A descriptive name for the virtual server (e.g., oa.company.com)
   - **Protocol**—HTTP
   - **Port**—443
   - **Default Traffic Pool**—The pool created for this service in the previous section
3. Click **Create Virtual Server**.
4. In the next screen, under **Listening on**, select traffic IP groups and check the appropriate traffic IP group that was created for the ActiveSync service.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.

   Note that the port is configured as 443, whereas the protocol is HTTP. This is due to the fact that Traffic Manager will be offloading SSL from the Microsoft Exchange 2010 CAS servers. In order to configure SSL offloading on the CAS servers for all HTTP-based applications (OWA, ECP, EWS, OAB), follow the guidelines highlighted at http://social.technet.microsoft.com/wiki/contents/articles/how-to-configure-ssl-offloading-in-exchange-2010.aspx.

Configuring SSL Decryption

To perform SSL decryption, the certificate and the private key used for the virtual server created in the previous section must be imported into the Traffic Manager.

1. Navigate to **Catalogs** > **SSL** > **SSL Certificates catalog**.
2. Click **Import Certificate** to import the appropriate certificate.

   After importing the certificate, enable SSL decryption on the virtual server created.
3. Navigate to **Services** > **Virtual Servers** and select the virtual server created for the ActiveSync service that will be performing SSL decryption.
4. Scroll down and click **SL Decryption**.
5. Set **ssl_decrypt** to **Yes**.
6. Select the certificate imported in Step 2.
7. Scroll down to the bottom of the page and click **Update**.

Configuring Session Persistence

The settings for configuring session persistence and the TrafficScript used are documented below.

1. Navigate to **Catalogs** > **Persistence**.
2. Provide a descriptive name for the persistence class.

3. Click **Create Class**.
4. Select **Universal Session Persistence** under **Basic Settings**.
5. Click **Update** to apply the changes.
6. Navigate to **Services** > **Pools** and select the appropriate pool that was created earlier.
7. Navigate to **Session Persistence** and click **Edit**.
8. Select the **Session Persistence Class** created, and click **Update** to apply the changes.
9. Navigate to **Catalogs** > **Rules**.
10. Create a new rule:
    - **Name**—A descriptive name for the rule (e.g., ActiveSync Rule)
    - Use TrafficScript Language
11. Click **Create Rule**.
12. Use the TrafficScript as shown here:

```
#// TS Rule for session persistence
$debug = 0; // Change value to 1 if debug needed
#Extract the value of Authorization Header
$auth = http.getHeader( "Authorization" );

# Please declare the names of the session persistence classes you have created
$universal_session_persistence  = "Exchange 2010 ActiveSync Persistence";

# Create persistence based on the cookie value

if ( $auth) {
if ($debug > 0) { log.info("Exchange control panel persistence based on cookie value");}
connection.setPersistence( $universal_session_persistence );
connection.setPersistenceKey( $auth);
}
```

13. Click the **Update** button.
14. Navigate to **Services** > **Virtual Servers** and select the virtual server created for the ActiveSync service.
15. Scroll down and click **Rules**.
16. Assign the TrafficScript to the request rules by clicking **Add Rule**.

NOTE
The persistence configuration steps highlighted above in this document are not applicable when SSL Client Certificate Authentication is enabled.

Configuration Summary

By accessing **Services** > **Config Summary** on the web GUI, a complete snapshot of all configured services is provided. This is a very useful table to glance through to get a good understanding of how the services are configured.

Configuring Auto Discover

The Auto Discover service provides automatic configuration information to recent versions of Outlook and some mobile clients. The Auto Discover service does not need any kind of persistence.

NOTE
Auto Discover will not work unless you follow the guidelines found at http://technet.microsoft.com/en-us/library/bb124251.aspx.

This section walks through the steps required to configure Auto Discover on a dedicated/separate traffic IP group.

Component	Procedure	Description
Virtual Traffic Manager	Creating a Traffic IP Group for the Auto Discover Service	A traffic IP group must be created for Auto Discover. For details, see Creating Traffic IP Groups on page 27.
	Creating a Pool for the Auto Discover Service	Enter the hostname or IP address of the CAS server nodes along with the port number. For details, see Creating Pools on page 27.
	Creating a Virtual Server for the Auto Discover Service	Create and associate the virtual server to the server pool of choice and the traffic IP group to listen on. For details, see Creating Virtual Servers on page 27.
	Configuring SSL Decryption	Configure SSL decryption to enable SSL offloads. For details, see Configuring SSL Decryption on page 28.

Creating Traffic IP Groups

Create a traffic IP group (also known as a virtual IP) for the Auto Discover service on which the virtual server will be listening.

1. Navigate to **Services** > **Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.
2. Fill in the fields as follows:
   - **Name**—A descriptive name for the traffic IP group (e.g., Auto Discover.company.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of this service
3. Click the **Create Traffic Group** button.

Creating Pools

For the Auto Discover service, create a pool using the following steps.

1. Navigate to **Services** > **Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name**—A descriptive name for the pool. (e.g., Auto Discover Service)
   - **Nodes**—hostname:80 or ipaddress:80
   - **Monitor**—Select the **Full HTTP** monitor
3. Click the **Update** button to apply changes.

Creating Virtual Servers

For the Auto Discover service, create a virtual server using the following steps.

1. Navigate to **Services** > **Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name**—A descriptive name for the virtual server (e.g., oa.company.com)
   - **Protocol**—HTTP
   - **Port**—443
   - **Default Traffic Pool**—The pool created for this service in the previous section

3. Click **Create Virtual Server**.
4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the appropriate traffic IP group that was created for the Auto Discover service.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.

   Note that the port is configured as 443, whereas the protocol is HTTP. This is due to the fact that Traffic Manager will be offloading SSL from the Microsoft Exchange 2010 CAS servers. To configure SSL offloading on the CAS servers for all HTTP-based applications (OWA, ECP, EWS, OAB), follow the guidelines highlighted at http://social.technet.microsoft.com/wiki/contents/articles/how-to-configure-ssl-offloading-in-exchange-2010.aspx.

Configuring SSL Decryption

To perform SSL decryption, the certificate and the private key used for the virtual server created in the previous section must be imported into the Traffic Manager.

1. Navigate to **Catalogs** > **SSL** > **SSL Certificates catalog**.
2. Click **Import Certificate** to import the appropriate certificate.

   After importing the certificate, enable SSL decryption on the virtual server created:
3. Navigate to **Services** > **Virtual Servers** and select the virtual server created for the Auto Discover service that will be performing SSL decryption.
4. Scroll down and click **SSL Decryption**.
5. Set **ssl_decrypt** to **Yes**.
6. Select the certificate imported in Step 2.
7. Scroll down to the bottom of the page and click **Update**.

Configuration Summary

By accessing **Services** > **Config Summary** on the web GUI, a complete snapshot of all configured services is provided. This is a very useful table to glance through to get a good understanding of how the services are configured.

Configuring MAPI RPC Client Access

Outlook clients that use native MAPI access the service via CAS servers in Exchange 2010, which is an architectural change from earlier versions of Exchange. vTM can load-balance the native MAPI access to CAS servers. MAPI RPC client access connects over a large range of dynamically negotiated ports. Since vTM does not natively support virtual servers to listen on range of ports, this section of MAPI configuration is based on a static mapping of Mailbox and Address Book ports on CAS servers as mentioned in the perquisites section for configuration of Microsoft Exchange 2010 CAS servers. There will be three virtual servers configured.

- A virtual server for the MAPI End Point Mapper service on TCP port 135
- A virtual server for the Mailbox Access service on TCP port 55001 (randomly chosen based on Microsoft's recommendation)
- A virtual server for the Address Book service on TCP port 55003 (randomly chosen based on Microsoft's recommendation)

All the virtual servers will be associated with the same traffic IP group and the same persistence class of type IP persistence.

This section walks through the steps required to configure MAPI on a dedicated/separate traffic IP group.

Component	Procedure	Description
Virtual Traffic Manager (once for all three services)	Creating a Traffic IP Group for MAPI RPC Client Access	A traffic IP group must be created for MAPI RPC Client Access. For details, see Creating Traffic IP Groups on page 29.
Virtual Traffic Manager (once for the MAPI End Point Mapper, once for Mailbox Access, and once for the Address Book service)	Creating a Pool for the ActiveSync Service and Selecting a Monitor for the Pool	Enter the hostname or IP address of the CAS server nodes along with the port number. For details, see Creating Pools on page 29.
	Creating a Virtual Server for the ActiveSync Service	Create and associate the virtual server to the server pool of choice and the traffic IP group to listen on. For details, see Creating Virtual Servers on page 30.
	Configuring Session Persistence for the ActiveSync Service	Universal session affinity persistence is required for the ActiveSync service. For details, see Configuring Session Persistence on page 31.

Creating Traffic IP Groups

Create a traffic IP group (also known as a virtual IP) for RPC Client Access on which all three above-mentioned virtual servers will be listening.

1. Navigate to **Services** > **Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.
2. Fill in the fields as follows:
   - **Name**—A descriptive name for the traffic IP group (e.g., cas.company.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of this service
3. Click the **Create Traffic Group** button.

Creating Pools

MAPI End Point Mapper Service

For the MAPI End Point Mapper service, create a pool using the following steps.

1. Navigate to **Services** > **Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name**—A descriptive name for the pool (e.g., MAPI End Point Service)
   - **Nodes**—hostname:135 or ipaddress:135
   - **Monitor**—Connect
3. Click the **Update** button to apply the changes.
4. Navigate to the **Connection Management** settings under the pool and change the **node_connclose** setting to **Yes**.
5. Click the **Update** button to apply the changes.

MAPI Mailbox Service

For the MAPI Mailbox service, create a pool using the following steps.

1. Navigate to **Services** > **Pools** and scroll down to **Create a new Pool**.

2. Fill in the fields as follows:
   - **Pool Name**—A descriptive name for the pool (e.g., MAPI Mailbox Service)
   - **Nodes**—hostname:55001 or ipaddress:55001
   - **Monitor**—Connect
3. Click the **Update** button to apply the changes.
4. Navigate to the **Connection Management** settings under the pool and change the **node_connclose** setting to **Yes**.
5. Click the **Update** button to apply the changes.

MAPI Address Book Service

For the MAPI Address Book service, create a pool using the following steps.

1. Navigate to **Services** > **Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name**—A descriptive name for the pool (e.g., MAPI Address Book Service)
   - **Nodes**—hostname:55003 or ipaddress:55003
   - **Monitor**—Connect
3. Click the **Update** button to apply the changes.
4. Navigate to the **Connection Management** settings under the pool and change the **node_connclose** setting to **Yes**.
5. Click the **Update** button to apply the changes.

Creating Virtual Servers

MAPI End Point Mapper Service

For the MAPI End Point Mapper service, create a virtual server using the following steps.

1. Navigate to **Services** > **Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name**—A descriptive name for the virtual server (e.g., MAPI End Point Mapper Service)
   - **Protocol**—Generic Client First
   - **Port**—135
   - **Default Traffic Pool**: The pool created for this service in the previous section
3. Click **Create Virtual Server**.
4. In the next screen, under **Listening on**, select the traffic IP group created for MAPI RPC Client Access.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.
7. Navigate to the **Connection Management** settings under the virtual server and set the **timeout** value to **7200** based on the Microsoft KB article (http://support.microsoft.com/kb/2535656).

MAPI Mailbox Service

For the MAPI Mailbox service, create a virtual server using the following steps.

1. Navigate to **Services** > **Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name**—A descriptive name for the virtual server (e.g., MAPI Mailbox Service)
   - **Protocol**—Generic Client First
   - **Port**—55001
   - **Default Traffic Pool**—The pool created for this service in the previous section
3. Click **Create Virtual Server**.
4. In the next screen, under **Listening on**, select the traffic IP group created for MAPI RPC Client Access.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.
7. Navigate to the **Connection Management** settings under the virtual server and set the **timeout** value to **7200** based on the Microsoft KB article (http://support.microsoft.com/kb/2535656).

MAPI Address Book Service

For the MAPI Address Book service, create a virtual server using the following steps.

1. Navigate to **Services** > **Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name**—A descriptive name for the virtual server (e.g., MAPI Address Book Service)
   - **Protocol**—Generic Client First
   - **Port**—55003
   - **Default Traffic Pool**—The pool created for this service in the previous section
3. Click **Create Virtual Server**.
4. In the next screen, under **Listening on**, select the traffic IP group created for MAPI RPC Client Access.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.
7. Navigate to the **Connection Management** settings under the virtual server and set the **timeout** value to **7200** based on the Microsoft KB article (http://support.microsoft.com/kb/2535656).

Configuring Session Persistence

For all three services (MAPI End Point Mapper service, MAPI Mailbox service, and MAPI Address Book service), the settings for configuring the session persistence is documented below.

1. Navigate to **Catalogs** > **Persistence**.
2. Provide a descriptive name for the persistence class.
3. Click **Create Class**.
4. Select **IP-Based Persistence** under **Basic Settings**.
5. Click **Update** to apply the changes.
6. Navigate to **Services** > **Pools** and select the appropriate pool that was created earlier.

7. Navigate to **Session Persistence** and click **Edit**.
8. Select the session persistence class created, and click **Update** to apply changes.

   Repeat the steps above for each of the three services.

Configuration Summary

By accessing **Services** > **Config Summary** on the web GUI, a complete snapshot of all configured services is provided. This is a very useful table to glance through to get a good understanding of how the services are configured.

Configuring POP3 and IMAP4

The POP3 service on Exchange CAS servers enables mail clients that support the POP3 protocol to access Exchange CAS servers running the POP3 service. There are a variety of clients including Outlook, Outlook Express, Eudora, and other third-party clients.

The IMAP4 service enables mail clients that support the IMAP4 protocol to access Exchange CAS servers running the IMAP4 service. There are variety of clients including Outlook, Outlook Express, Eudora, and other third-party clients.

For more information about how to manage POP3 and IMAP4 in Exchange 2010, see *Understanding POP3 and IMAP4* on Microsoft TechNet at http://technet.microsoft.com/en-us/library/bb124107%28EXCHG.140%29.aspx.

This section walks through the steps required to configure the POP3 and IMAP4 service on a dedicated/separate traffic IP group.

Component	Procedure	Description
Virtual Traffic Manager	Creating Traffic IP Group for Both POP3 and IMAP4 Services	A traffic IP group must be created for both POP3 and IMAP4 services. For details, see Creating Traffic IP Groups on page 32.
Virtual Traffic Manager (once each for the POP3 and IMAP4 services)	Creating a Pool for Each Service	Enter the hostname or IP address of the CAS server nodes along with the port number. For details, see Creating Pools on page 33.
	Creating a Virtual Server for Each Service	Create and associate the virtual server to the server pool of choice and the traffic IP group to listen on. For details, see Creating Virtual Servers on page 33.
	Configuring SSL Decryption	Configure SSL decryption to enable SSL offloads. For details, see Configuring SSL Decryption on page 34.

Creating Traffic IP Groups

Create a traffic IP group (also known as a virtual IP) for both POP3 and IMAP4 services on which the virtual server will be listening.

1. Navigate to **Services** > **Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.
2. Fill in the fields as follows:
   - **Name**—A descriptive name for the traffic IP group (e.g., pop3-imap4.company.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of this service
3. Click the **Create Traffic Group** button.

Creating Pools

POP3

For the POP3 service, create a pool using the following steps.

1. Navigate to **Services** > **Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name**—A descriptive name for the pool (e.g., POP3 Service)
   - **Nodes**—hostname:110 or ipaddress:110
   - **Monitor**—POP
3. Click the **Update** button to apply the changes.

IMAP4

For the IMAP4 service, create a pool using the following steps.

1. Navigate to **Services** > **Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name**—A descriptive name for the pool (e.g., IMAP4 Service)
   - **Nodes**—hostname:143 or ipaddress:143
   - **Monitor**—Connect
3. Click the **Update** button to apply the changes.

Creating Virtual Servers

POP3

For the POP3 service, create a virtual server using the following steps.

1. Navigate to **Services** > **Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name**—A descriptive name for the virtual server (e.g., pop3.company.com)
   - **Protocol**—POP3
   - **Port**—995
   - **Default Traffic Pool**—The pool created for this service in the previous section
3. Click **Create Virtual Server**.
4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the appropriate traffic IP group that was created for the POP3 and IMAP4 services.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.

IMAP4

For IMAP4 service, create a virtual server using the following steps.

1. Navigate to **Services** > **Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name**—A descriptive name for the virtual server (e.g., imap4.company.com)
   - **Protocol**—IMAPv4
   - **Port**—993
   - **Default Traffic Pool**—The pool created for this service in the previous section
3. Click **Create Virtual Server**.
4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the appropriate traffic IP group that was created for the POP3 and IMAP4 services.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.

Configuring SSL Decryption

Enable SSL decryption using the same certificate/key pair used for OWA since it supports the SAN DNS Name for IMAP4 service. If there is a dedicated certificate/key pair for IMAP4/POP3 services, then follow the normal procedure of importing the key and certificate and use the same procedure as shown below to enable SSL decryption.

1. Navigate to **Catalogs** > **SSL** > **SSL Certificates catalog.**
2. Click **Import Certificate** to import the appropriate certificate.

   After importing the certificate, enable SSL decryption on the virtual server created:
3. Navigate to **Services** > **Virtual Servers** and select the virtual server created for the POP3/IMAP4 service that will be performing SSL decryption.
4. Scroll down and click **SSL Decryption**.
5. Set **ssl_decrypt** to **Yes**.
6. Select the certificate imported in Step 2.
7. Scroll down to the bottom of the page and click **Update**.

Configuration Summary

By accessing **Services** > **Config Summary** on the web GUI, a complete snapshot of all configured services is provided. This is a very useful table to glance through to get a good understanding of how the services are configured.

Configuring a Single Virtual Server for All Exchange HTTP Services with Multiple Pools

This approach uses a single IP address that is mapped to the FQDN of all Exchange HTTP services and uses multiple pools. The following are the detailed configuration steps on Traffic Manager to configure a single virtual server for all services.

Creating Traffic IP Groups

Create a traffic IP group (also known as a virtual IP) for all services on which the virtual server will be listening.

1. Navigate to **Services** > **Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.
2. Fill in the fields as follows:
   - **Name**—A descriptive name for the traffic IP group (e.g., webmail.company.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of this service
3. Click the **Create Traffic Group** button.

Creating Pools

Create a pool for each of the services (OWA, Outlook Anywhere, ActiveSync, Auto Discover).

1. Navigate to **Services** > **Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name**—A descriptive name for the pool (e.g., OWA Service)
   - **Nodes**—hostname:80 or ipaddress:80
   - **Monitor**—HTTP
3. Click the **Update** button to apply changes.

Creating Virtual Servers

Create a virtual server and associate the Exchange 2010 Outlook Web Access Pool to the virtual server and also associate the traffic IP group created earlier. This would be the default pool for this virtual server, and TrafficScript will be used to direct the traffic to the appropriate pool based on the URLs (services). Create a virtual server using the following steps.

1. Navigate to **Services** > **Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name**—A descriptive name for the virtual server (e.g., webmail.company.com)
   - **Protocol**—HTTP
   - **Port**—443
   - **Default Traffic Pool**—The OWA pool
3. Click **Create Virtual Server**.
4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the appropriate traffic IP group that was created for all services.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.

Configuring SSL Decryption

Enable SSL decryption using the same certificate/key pair used for OWA since it supports the SAN DNS name for all services.

1. Navigate to **Services** > **Virtual Servers** and select the virtual server created for all services that will be performing SSL decryption.
2. Scroll down and click **SSL Decryption**.

3. Set **ssl_decrypt** to **Yes**.
4. Select the certificate that has the SAN DNS names for all applications.
5. Scroll down to the bottom of the page and click **Update**.

Configuring Session Persistence and TrafficScript

Create two persistence classes: one class of type "Universal Session Persistence" for holding all records other than Outlook Web App persistence records; and another class of type "Transparent Session Affinity". Then create a TrafficScript rule to create appropriate persistence records and also to redirect traffic to appropriate pools. The following are the settings for configuring session persistence and the TrafficScript used.

1. Navigate to **Catalogs** > **Persistence**.
2. Provide a descriptive name for the persistence class.
3. Click **Create Class**.
4. Select **Universal Session Persistence** under **Basic Settings**.
5. Click **Update** to apply the changes.
6. Create another class of type **Transparent Session Affinity** using the steps above.
7. Navigate to **Services** > **Pools** and select the appropriate pool that was created earlier.
8. Navigate to **Session Persistence** and click **Edit**.
9. Select the session persistence class created, and click **Update** to apply changes.
10. Navigate to **Catalogs** > **Rules**.
11. Create a new rule:
    - **Name**—A descriptive name for the rule (e.g., All Services Rule)
    - Use TrafficScript Language
12. Click **Create Rule**.

13. Use the TrafficScript as shown here:

```
$debug = 0; // Change value to 1 if debug needed
# Declare the names of the pools you have configured, and ensure
# that the trafficscript!variable_pool_use Global setting is set to 'yes'
$active_sync_pool = "Exchange 2010 ActiveSync Pool";
$owa_pool     = "Exchange 2010 Outlook Web Access Pool";
$oa_pool     = "Exchange 2010 Outlook Anywhere Pool";
$ad_pool     = "Exchange 2010 Auto Discover Pool";

# Declare the names of the session persistence classes you have created
$universal_session_persistence  = "Exchange Universal Session Persistence";
$transparent_session_persistence = "Exchange Cookie Insert Persistence";

# --------- end of user-defined parameters
$path = http.getPath();
$outlooksession = http.getCookie( "OutlookSession" );
$auth = http.getHeader( "Authorization" );
$userdata = request.getRemoteIP();
$useragent = http.getHeader( "User-Agent" );
$pool = "";
$sessiondata = "";
# Active Sync persistence based on Authorization Header if not persist on Client IP address
if( $path == "/Microsoft-Server-ActiveSync" ) {
   if( $auth ){
   $sessiondata = $auth;
       if ($debug > 0) { log.info("Active Sync service Persistence based on Auth Header");}
   } else {
   $sessiondata = $userdata;
       if ($debug > 0) { log.info("Active Sync service Persistence based on Client IP");}
   }
  $pool = $active_sync_pool;
}
# Exchange Web Services persistence based on client IP address
else if( string.startsWithI( $path, "/ews" ) ) {
  $sessiondata = $userdata;
     if ($debug > 0) { log.info("Exchange web services persistence based on Client IP");}
  $pool = $owa_pool;
}
# Exchange Control Panel persistence based on Transparent Session persistence #(Cookie Insert)
else if( string.startsWithI( $path, "/ecp" ) ) {
  $pool = $owa_pool;
  if ($debug > 0) { log.info("Exchange control panel persistence based on Transparent session
persistence");}
}
# Exchange Offline Address Book doesn't need persistence so set $sessiondata to #"none"
else if( string.startsWithI( $path, "/oab" ) ) {
  $sessiondata = "none";
  $pool = $owa_pool;
  if ($debug > 0) { log.info("Exchange offline address book does not need   persistence");}
}
# Exchange Outlook Anywhere needs persistence based on the client type. Outlook #2010 needs
outlooksession cookie else Authorization header
else if( $path == "/rpc/rpcproxy.dll" ) {
   if( string.ContainsI( $useragent, "msrpc" ) ) {
     if( $outlooksession ){
    $sessiondata = $outlooksession;
         if ($debug > 0) { log.info("Exchange outlook anywhere persistence based on outlooksession
cookie");}
    }
     else $sessiondata = $auth;
  }
   else if( string.ContainsI( $useragent, "microsoft office" ) ) {
     $sessiondata = $auth ;
           if ($debug > 0) { log.info("Exchange outlook anywhere persistence based on auth header");}
  }
  $pool = $oa_pool;
}
# Exchange Autodiscover doesn't need persistence so set $sessiondata to "none"
else if( string.startsWithI( $path, "/autodiscover" ) ) {
```

```
  $sessiondata = "none"
  $pool = $ad_pool;
      if ($debug > 0) { log.info("Exchange autodiscover does not need   persistence");}

}
# Exchange Outlook Web Access needs persistence based on Transparent Session #persistence ( Cookie
Insert) which is default in this rule.
else {
   $pool = $owa_pool;
      if ($debug > 0) { log.info("Exchange control panel persistence based on Transparent session
persistence");}
}
pool.select( $pool );

if( $sessiondata != "none" ) {
  if( $sessiondata ) {
   connection.setPersistence( $universal_session_persistence );
   connection.setPersistenceKey( $sessiondata );
  } else {
   connection.setPersistence( $transparent_session_persistence );
  }
}
```

14. Click the **Update** button.
15. Navigate to **Services** > **Virtual Servers** and select the virtual server created for all services.
16. Scroll down and click **Rules**.
17. Assign the TrafficScript to the request rules by clicking **Add Rule**.

Configuration Summary

By accessing **Services** > **Config Summary** on the web GUI, a complete snapshot of all configured services is provided. This is a very useful table to glance through to get a good understanding of how the services are configured.

Additional Optional Functionality on Brocade Virtual Traffic Manager

Brocade Virtual Traffic Manager is much more than a simple load balancer; there are a number of other functions/features that you may wish to deploy with your Exchange 2010 CAS. These have been described in this separate section since they are not necessary, but they could enhance the performance or manageability of your environment. Further descriptions of these features can be found in the *Brocade Virtual Traffic Manager: User's Guide*.

- Service Level Monitoring—This feature monitors the responses of your CAS and can send alerts should these fall below an expected threshold of performance.
- Global Load Balancing—This enables clients to be distributed across multiple locations, either for DR purposes or based on their geographic proximity to a datacenter.

Physical Network Deployment

As a reverse proxy, the Brocade vTM deployment options are extremely flexible. In most instances, there are no changes required to the existing network infrastructure. Brocade vTM will simply be added to the network, and traffic will be directed to it via DNS.

A whole chapter in the *Brocade Virtual Traffic Manager: User's Guide* addresses this aspect of the deployment. We suggest that you reference it for a complete understanding.

Domain Name Service

As mentioned previously, traffic that would have been sent directly to the CAS before the deployment of the Traffic Manager now must terminate at the Brocade vTM. This is quite easy to achieve; the zone files for the domain must be altered. The records that relate the name of the service to the IP address of the CAS must now point to the traffic IPs of the Traffic Manager.

These changes can take some time to become effective in every location (due to caching of previous results). Testing before the move of the IPs can be done by using static mappings in the client host file or by using the IP address of the Traffic Manager only.

Clustering of Brocade Virtual Traffic Managers

To provide high availability and fault tolerance for Brocade Virtual Traffic Manager, two or more vTMs can be joined into a cluster and configured to load-balance or act in active-passive mode for fault tolerance.

Use the following steps to join a Brocade vTM to an existing cluster.

1. Navigate to **System** > **Traffic Managers**.
2. Scroll down to **Add or Remove Traffic Managers** and click **Join a Cluster**.
3. Click **Next** on **Getting Started**.
4. Select the cluster to join and click **Next**.

5. Check the certificate used for the cluster, provide a username and password for the cluster, and click **Next** to continue.
6. Select **Yes, and allow it to host Traffic IPs immediately** and click **Next**.
7. In the **Summary** page, click **Finish** to join the vTM to the cluster.

Monitoring

Brocade vTM has some great tools to assist in managing and monitoring your online application traffic. These tools can be accessed via the web UI of the device from the **Activity** tab.

Real-time graphs can be used to show the traffic passing through the Brocade vTM in a very granular way; you can change the data being monitored down to an individual node or see all traffic for the entire deployment.

There is also a map view and connection list to aid further visibility of the traffic.

Web Accelerator and vWAF Functions

ATTENTION

Reach out to the Brocade support team for help on more advanced and customized configuration of the Web Accelerator and Web Application Firewall.

Web Accelerator

Web Accelerator is a Traffic Manager feature that is available in the Enterprise edition of the Brocade vTM. Web Accelerator enables vTM to perform a full range of optimization techniques on HTML pages including inspecting and modifying them. It also performs the following optimizations on the page resources as the client fetches them:

- Minification and compression of JavaScript files
- Minification and compression of style sheets
- Background images inlined or versioned
- Web fonts versioned
- Resampling of image content
- Compression of all resources

Full control over the above-mentioned individual optimization parameters is also possible with Web Accelerator. There are built-in Web Accelerator profiles available with the Express profile being the most common one designed to match a wide range of applications. Other profiles for Microsoft SharePoint Applications are also available in the product.

For Microsoft Exchange, enable the Web Accelerator for the OWA service using the following procedure.

1. Click the virtual server on which Web Accelerator is be enabled. Within that, click **Web Accelerator**.
2. In the **Basic Settings** section, enable the Web Accelerator functionality by selecting **yes** in the options for **aptimizer!enabled**.
3. Under **Catalogs > Web Accelerator > Application Scopes**, create a new application scope.
4. Enter any name for the application scope. This name will show up in the list of scopes to choose under the **Virtual Server Web Accelerator Settings**.
5. Under **hostnames**, enter the hostname for the HTTP service.
6. Keep the rest of the settings as defaults, and click **Create Application Scope**.
7. Under the virtual server settings for Web Accelerator, expand the **Web Accelerator Profiles** section, and select the newly created application scope.
8. To the right of the application scope selected, select **Web Accelerator Profile**. In this case, select **Express**.
9. Click **Update**.

Web Application Firewall

Brocade Virtual Web Application Firewall (Brocade vWAF) is a scalable security platform for off-the-shelf solutions and custom applications. It lets you apply business rules to online traffic, screening for attacks such as SQL injection and cross-site scripting (XSS), while securing outgoing traffic to help compliance with PCI-DSS and HIPAA. Brocade vWAF can be run as an add-on to the vTM to enable both load-balancing and application firewall services on a single instance.

Apart from custom rule configurations that are possible on the vWAF, there is a rule set called baseline protection that protects applications from the most common application-layer attacks that exist today, such as the following:

- Path Traversal
- Shell Command Injection
- SQL Injection
- Code Injection
- Cross-Site Scripting (XSS)
- Common Attacks
- LDAP Injection
- Scanner
- XPATH Injection

The following procedure documents the configuration of the Web Application Firewall for baseline protection of the Microsoft Exchange application, specifically for the HTTP services.

1. On the vTM, navigate to **System > Application Firewall**, and click the **afm_enabled** radio button, followed by **Update** (ensure that the **Confirm** checkbox is checked).
2. Click the **Application Firewall** tab on the vTM.
3. Click **Administration**, and then select **Baseline Management**.
4. From this screen, either download the latest Virtual Web Application Firewall baseline signatures from Brocade Communities and click **Upload** or click the **Download from Server** option if your vTM+vWAF has Internet connectivity.
5. In the **Application Firewall** UI, click **Application Control**, and select **Application Creation Wizard**.
6. Enter a name for the application, and click **Continue**.
7. Choose the detection mode that will enable the firewall rules to be applied to production traffic. Choose the protection mode for not affecting production traffic and whether you want to test the rules and check the logs for accuracy. Click **Continue**.
8. In the customer key screen, leave the default and click **Continue**.
9. In the hostname screen, enter the exact FQDN/IP address (typically, this is the TIP group address) by which users/clients will access the application. You can enter multiple values for one application simply by clicking **Add hostname** after adding one. Click **Continue**.
10. In the next screen, leave the default logging level to reduced logging unless there is a need to monitor the complete logs. Click **Continue**.
11. In the next screen, choose the option to enable full request logging and selecting the number of days for data retention. If indefinite, leave it to the default **0**. Click **Continue**.
12. In the next screen, choose to run the **Baseline Protection** wizard. Click **Continue** and then click **Finish**.
13. In the **Baseline Protection** wizard, click **Next** on the **Overview** screen.
14. Choose the baseline version to use. Click **Next**.
15. Leave the rest of the screens to their defaults, and, finally, click **Finish**.

16. Click the **Virtual Traffic Manager** tab to go back to the vTM UI.
17. Select the virtual server on which the vWAF service is to be enabled, and select **enabled** for the **Application Firewall** option, and click **Update**.

RPC over HTTP

By design, RPC over HTTP is not compatible with Brocade vWAF. However, we can prevent RPC traffic from going to the vWAF by using TrafficScript and checking for the URL path.

The following example TrafficScript checks for "rpc" in the URL path, whitelists the traffic, and bypasses the vWAF for such traffic.

```
if ( string.startswith($path, "/rpc/") ) {
   connection.data.set("enforcer.whitelist", 1);
}
```

Select the virtual server of interest, and add this TrafficScript rule to the Request rules. Make sure to place this TrafficScript rule ahead of the Enforcer rule such that it is executed before the Enforcer TrafficScript.

Common Troubleshooting Tips

This chapter describes tips for troubleshooting common deployment issues.

Uploading Certificates to Traffic Manager

When uploading certificates to Traffic Manager, these must be in PEM format. For your certificates that are not in PEM format, tools are available to convert CER (without a key) and PFX (with a key) formats to PEM format, such as OpenSSL. To upload a certificate used by an Exchange server, export the certificate once with a private key and once without a private key. Use the following commands to convert the certificate to PEM format.

Convert a DER File (.crt .cer .der) to PEM

```
openssl x509 -inform der -in <certificate filename>.cer -out certificate.pem
```

Convert a PKCS#12 File (.pfx .p12) Containing a Private Key and Certificates to PEM

```
openssl pkcs12 -in <certificate key filename>.pfx -out certificatekey.pem -nodes
```

Conclusion

This document discusses how to configure Brocade Virtual Traffic Manager to optimize the deployment of the Microsoft Exchange 2010 application. Traffic Manager is able to make intelligent load-balancing decisions and improve the performance, security, reliability, and integrity of the traffic in this environment. Refer to the product documentation on the Brocade Community Forums (http://community.brocade.com) for examples of how Brocade Virtual Traffic Manager can be deployed to meet a range of service hosting problems.