

Organizations use the Barracuda Load Balancer to distribute the load and increase the availability of their Microsoft Exchange Server 2010 deployments. Using a Barracuda Load Balancer allows load balancing of a Client Access Server (CAS) array.

Barracuda Networks has conducted interoperability tests between the Barracuda Load Balancer and Microsoft Exchange Server 2010. This document describes the procedure to deploy the Barracuda Load Balancer in this environment.

Prerequisites

- Microsoft Exchange Server 2010
- Barracuda Load Balancer running firmware version 3.3.1.005 or higher
- Barracuda Load Balancer model 340 or above is required

This document assumes that you have installed your Barracuda Load Balancer(s), have connected to the Web interface, and have activated your subscription(s). To scale your Microsoft Exchange Server 2010 deployment with High Availability, you must first have a pair of Barracuda Load Balancers joined in a cluster. See the [Barracuda Load Balancer Administrator's Guide](#) for assistance with these steps.

Additional References

- [Barracuda Load Balancer Administrator's Guide](#)
<http://www.barracudanetworks.com/documentation/>
- Load Balancing Requirements of Exchange Protocols
<http://technet.microsoft.com/en-us/library/ff625248.aspx>
- Configure SSL Offloading for Outlook Anywhere
<http://technet.microsoft.com/en-us/library/aa998346.aspx>
- Microsoft Exchange Network Port Reference
<http://technet.microsoft.com/en-us/library/bb331973.aspx>
- Understanding Load Balancing in Exchange 2010
<http://technet.microsoft.com/en-us/library/ff625247.aspx>
- Create a New Exchange Certificate
<http://technet.microsoft.com/en-us/library/dd351057.aspx>

Terminology

Term	Description
Fully Qualified Domain Name (FQDN)	The unique name for a specific computer or host that can resolve to an IP address, e.g. www.example.com
Virtual IP (VIP) Address	The IP address assigned to a Service. Clients use the Virtual IP address to connect to the load-balanced Service.
Service	A combination of a Virtual IP address and one or more TCP/UDP ports that the Barracuda Load Balancer listens on. Traffic arriving on the specified port(s) is directed to one of the Real Servers associated with a Service.
Client Access Server (CAS)	Client Access Server supports various protocols used by end users to access their mailboxes. This includes services such as RPC Client Access, IMAP, POP3, OWA, and ActiveSync.
Real Server	A server associated with a Service that handles the requests forwarded to it by the Barracuda Load Balancer.
Hub Transport Server	The Hub Transport server role handles all mail flow inside the organization and delivers messages to a recipient's mailbox.
Outlook Web Application (OWA)	Originally called Outlook Web Access, OWA is the webmail component of Microsoft Exchange 2010.

Choosing a Deployment

There are two configurations that are supported when adding a Barracuda Load Balancer to a Microsoft Exchange Server 2010 environment:

- ❖ If your Exchange servers must be on the same subnet as the rest of your topology, choose a **one-armed**, Route-Path deployment.
- ❖ If the Exchange servers may be deployed on a separate subnet from the rest of the topology, connected to the LAN side of the Barracuda Load Balancer, choose a **two-armed**, Route-Path deployment.

Deploying in Bridge-Path or Direct Server Return with Microsoft Exchange 2010 is **untested** and **unsupported**.

More information about one-armed and two-armed deployments can be found in the [Barracuda Load Balancer Administrator's Guide](#).

Deployment Tasks

The following sections contain instructions to complete the three tasks required to deploy the Barracuda Load Balancer in the Microsoft Exchange Server environment. The third task differs based on whether this is a one-armed or two-armed deployment.

For both deployment options, the first task is to configure a Client Access server array for your Exchange site. This step needs to be done only on one Exchange Server. Instructions can be found in the section called *Configuring the Client Access Server (CAS) Array*.

Second, prepare to offload the SSL processing of Exchange services onto the Barracuda Load Balancer. Instructions are found in the section called *Preparing Your Environment for SSL Offloading*.

Third, configure the Service or Services that the clients will use to access the CAS array on the Barracuda Load Balancer. For a one-armed deployment, see *Deploying Exchange 2010 in a One-armed Configuration*. For a two-armed deployment, see *Deploying Exchange 2010 in a Two-armed Configuration*.

Note: If your Barracuda Load Balancers are clustered, the configuration between the active and passive systems is synchronized automatically, so you will not need to modify any passive Barracuda Load Balancers at this time.

When all the configuration steps are complete, you can test your installation by referring to the section called *Testing Your Microsoft Exchange Installation*.

Configuring the Client Access Server (CAS) Array

In this task you will configure access for MAPI clients (for example, Microsoft Outlook clients). Perform the following steps once for the Exchange domain. There are many more options you may wish to consider, and you should consult Microsoft documentation for further information. Note that Microsoft only allows one Client Access server array per site.

The clients will access their mailboxes using RPC. They will connect to a domain, which resolves to a Virtual IP address on the Barracuda Load Balancer. In turn, the Barracuda Load Balancer connects with one of the Client Access servers.

Note: These instructions assume a single site configuration. Contact Microsoft if you need assistance configuring a CAS Array in a multi-site environment.

To configure this do the following steps:

1. On the DNS Server, add an A record to the DNS zone that associates the VIP address with the fully qualified domain name (FQDN) that will be used by the clients to connect to the Client Access server array.

Optionally, if deploying ActiveSync, add a second A record that associates the VIP address with the FQDN that will be used by mobile users to connect to Exchange.

2. On one Exchange server in the array, open the Exchange Management Shell.
3. Using the Exchange Management Shell, enter the following command to verify that there are no existing CAS arrays:

Get-ClientAccessArray

The command should return nothing in an unconfigured single-site deployment.

4. Using the Exchange Management Shell, enter the following command to create a new CAS array:

New-ClientAccessArray -Fqdn *exchange.domain.local* -Site *Default-First-Site-Name*

where *exchange.domain.local* is the FQDN of the Client Access server array, and *Default-First-Site-Name* is the Active Directory site to which the Client Access server array belongs.

5. Ping the domain name (e.g. *exchange.domain.local*). The ping should fail because the Service has not yet been created on the Barracuda Load Balancer, but make sure that the domain name resolves correctly to the VIP address.
6. Using the Exchange Management Shell, enter the following command to add a mailbox database to the CAS Array:

**Get-MailboxDatabase | Set-MailboxDatabase -RpcClientAccessServer
*exchange.domain.local***

where *exchange.domain.local* is the fully qualified domain name (FQDN) of the Client Access server array.

Now that the Client Access Array is configured, go to the *Preparing Your Environment for SSL Offloading* section.

Preparing Your Environment for SSL Offloading

In this task you will perform steps required to offload SSL processing to the Barracuda Load Balancer. This task is performed in all cases, regardless of deployment option.

In order for session persistence to be maintained using HTTP cookies, SSL encryption and decryption must be done on the Barracuda Load Balancer. Offloading the SSL processing to the Barracuda Load Balancer also frees up processing power on your servers.

When SSL offloading is turned on, clients access the VIP address using the SSL port 443. The decrypted traffic passes between the Barracuda Load Balancer and the servers using the same VIP address but on port 80.

Perform the following steps:

1. Retrieve the certificates, certificate chain and private key for your Exchange OWA website from your CAS servers. If you do not already have a certificate in pfx form that includes the private key and intermediaries (if applicable), refer to the following instructions on exporting your Exchange certificate:

<http://technet.microsoft.com/en-us/library/dd351274.aspx>

2. Install the certificates, certificate chain and private key on the Barracuda Load Balancer. Go to the **Basic > Certificate** page in the Web interface of the Barracuda Load Balancer to upload the exported certificate exported in the previous step from Exchange.
3. Configure the SSL offloading settings for OWA on each CAS Server:
 - a. On each CAS server, open the IIS Manager Console
 - b. Expand the Server container and the Sites container. Click on the Web Site for OWA. By default this is called **Default Web Site**.
 - c. In the Features View, under the **IIS** section, click **SSL Settings**. Clear the **Require SSL** check box. Apply your settings.
 - d. Follow and apply the steps in the following article:

[http://technet.microsoft.com/en-us/library/bb885060\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb885060(EXCHG.80).aspx)

4. Configure the SSL offloading settings for Outlook Anywhere on each CAS Server by following the steps in the following article:

<http://technet.microsoft.com/en-us/library/aa998346.aspx>

5. There are a few more steps related to SSL offloading that will be performed in the next task. Select the next task based on the deployment mode best suited for your environment.

Deploying Exchange 2010 in a One-armed Configuration

In a one-armed configuration, the ports to be used by internal Outlook clients when communicating with the Exchange 2010 server using RPC must be pre-configured on both Exchange 2010 and the Barracuda Load Balancer.

In this final task you will perform the following steps:

Step 1. Configure Exchange 2010 to use a static port on every CAS server, and

Step 2. Create a Service for each port on the active Barracuda Load Balancer.

Step 1. Configure Exchange 2010 to use a static port

By default, the Exchange 2010 RPC client dynamically selects a port between 1024 and 65535. To allow for a one-armed deployment, configure Exchange to use a static port instead.

Microsoft maintains a support document that describes the configuration of Exchange 2010 with static ports and hardware Load Balancers at <http://technet.microsoft.com/en-us/library/ff625248.aspx>. For the convenience of our customers we have summarized the configuration steps in the following sections of this document.

On each CAS server do the following steps:

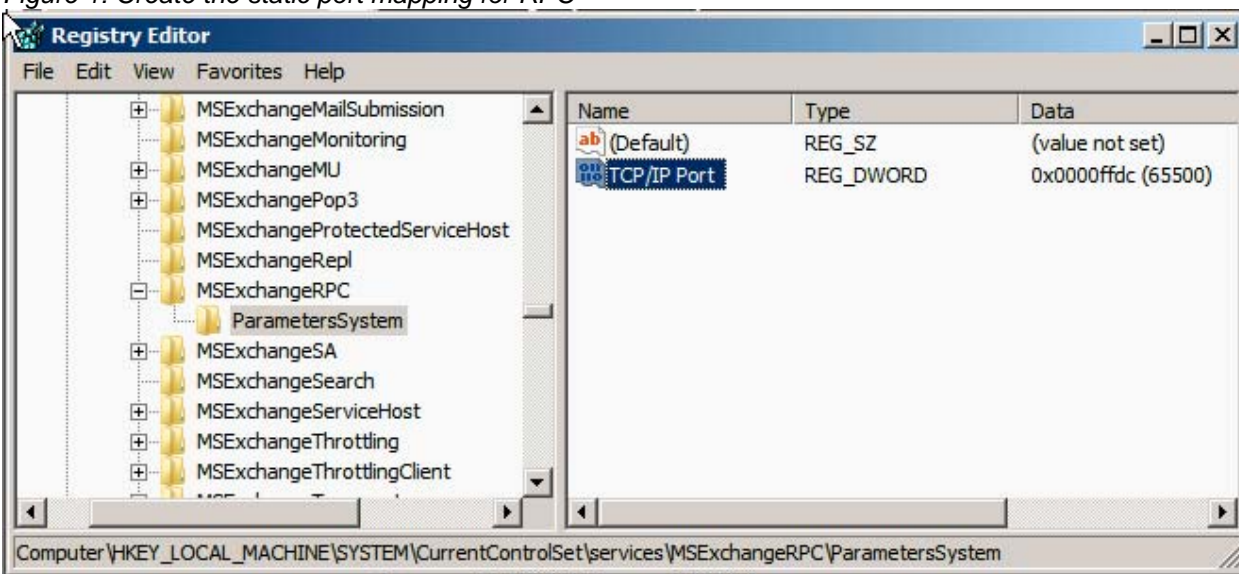
1. Configure the static port in the registry. Open the Registry Editor by typing `regedit` in the Start Menu. Add a DWORD (32-bit) value named **TCP/IP Port** under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeRpc\ParametersSystem`

Note: You may need to create the `ParametersSystem` key prior to adding the `DWORD` registry value. Refer to *Figure 1: Create the static port mapping for RPC*.

When prompted, change the Base to **Decimal** and set the value data to **65500** (or a port of your choice between 1024 and 65535).

If you have Public Folders in your deployment, you must also repeat this step on each server with the mailbox role installed.

Figure 1: Create the static port mapping for RPC



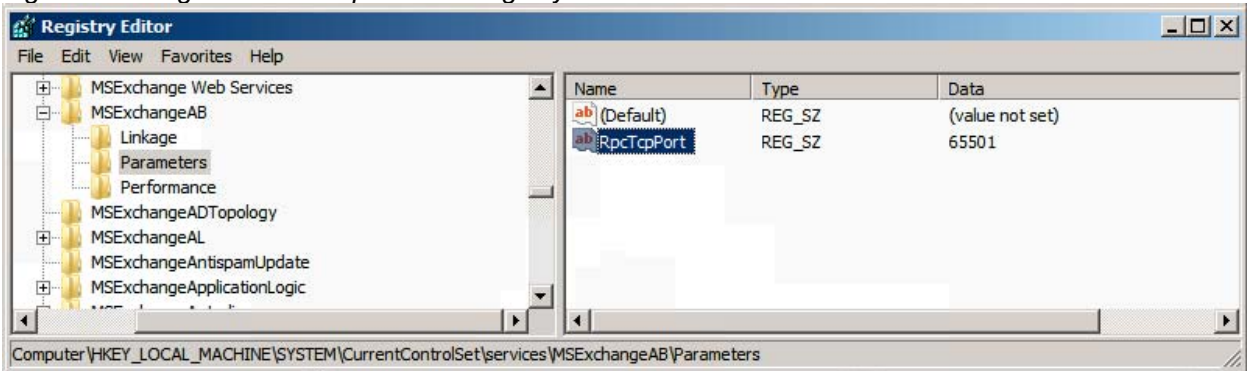
2. Change the port that clients use to connect to the NSPI endpoint for directory access. On every CAS server:
 - ❖ If you are running Microsoft Exchange 2010 RTM (including RTM Rollup 1 – 4) follow these instructions:
 - a. In Windows Explorer, navigate to the **Microsoft.exchange.addressbook.service.exe.config** file. This file is located in the `\Bin` folder in the root directory of your Exchange 2010 install.
 - b. Open this file using Notepad.
 - c. Change the default value of **0** on line 13 to **65501** (or a port of your choice within the prior specified range) so it appears as follows, including the quotations:


```
<add key="RpcTcpPort" value="65501" />
```
 - ❖ If you are running Microsoft Exchange 2010 SP1 follow these instructions:
 - a. Configure the static port in the registry. To do this, open the Registry Editor by typing `regedit` in the Start Menu. Add a String value (`REG_SZ`) with Value name **RpcTcpPort** under


```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MExchangeAB\Parameters
```

Note: You may need to create the `Parameters` key prior to adding the `REG_SZ` registry value. Refer to *Figure 2: Configure the static port in the registry*. Change the value data to **65501** (or a port of your choice between 1024 and 65535).

Figure 2: Configure the static port in the registry



3. Restart both the “Microsoft Exchange Address Book” and “Microsoft Exchange RPC Client Access” services on all CAS and Mailbox servers that you modified.
4. To test that your Client Access servers are using ports **65500** and **65501**, open a Windows command prompt and run **netstat -na**.

In the output, look for **TCP** entries marked as **LISTENING** with the ports **65500** and **65501**. You will see an entry marked as **LISTENING** for 0.0.0.0:65500 and 0.0.0.0:65501

Step 2. Configure Services on the Barracuda Load Balancer

On each active Barracuda Load Balancer, complete the following steps to configure Services for Exchange 2010:

1. Go to the **Basic > Services** page in the Web interface.
2. For each entry in the following tables, add a Service. To add a Service:
 - In the **Service Name** box, enter the name for the Service.
 - In the **Virtual IP** box, enter the VIP address specified in the table.
 - Select the protocol and in the **Port** box, enter the port for the Service in the table.
 - In the **Real Servers** box, enter the IP address for every server in the CAS array.
 - You will change the Service Type (from the default of Layer 4) in the next step.

All of the Services in the first table are **required**. Add each Service in the second and third tables only if you have deployed that feature.

Service Name	Virtual IP Address	Protocol	Service Type	Service Port	Real Server Port	Monitor Port
MAPI / DCOM	VIP address for FQDN that resolves to CAS array e.g. exchange.domain.local	TCP	TCP Proxy	135	135	65500

MAPI / RPC Client Access	VIP address for FQDN that resolves to CAS array e.g. exchange.domain.local	TCP	TCP Proxy	65500	65500	65500
MAPI / Global Address Book	VIP address for FQDN that resolves to CAS array e.g. exchange.domain.local	TCP	TCP Proxy	65501	65501	65501
Outlook Web App – HTTP Redirect	VIP address for FQDN that clients use to access OWA e.g. exchange.domain.local	TCP	Layer 7 - HTTP (Redirect)	80	N/A (Redirect Service)	N/A
Outlook Web App – HTTPS / Outlook Anywhere	VIP address for FQDN that clients use to access OWA e.g. exchange.domain.local	TCP	Layer 7 - HTTPS	443	80	80


The Services in the following table are **optional**. Add only those Services that correspond to an Exchange 2010 feature that you plan to use.

Note that the Service in the following table uses a different VIP address than the preceding Services. You must add this Service if you plan to deploy ActiveSync.

Service Name	Virtual IP Address	Protocol	Service Type	Service Port	Real Server Port	Monitor Port
ActiveSync	VIP address for FQDN that resolves to CAS array e.g. activesync.domain.local	TCP	TCP Proxy	443	443	443


Service Name	Virtual IP Address	Protocol	Service Type	Service Port	Real Server Port	Monitor Port
IMAP4 (optional)	VIP address for FQDN that resolves to CAS array e.g. exchange.domain.local	TCP	TCP Proxy	143	143	143
IMAP4 SSL (optional)	VIP address for FQDN that resolves to CAS array e.g. exchange.domain.local	TCP	TCP Proxy	993	993	993
POP3 (optional)	VIP address for FQDN that resolves to CAS array e.g. exchange.domain.local	TCP	TCP Proxy	110	110	110
POP3 SSL (optional)	VIP address for FQDN that resolves to CAS array e.g. exchange.domain.local	TCP	TCP Proxy	996	996	996

3. Edit the settings for each Service created:

- a. On the **Basic > Services** page, edit the Service by clicking the Service Edit () graphic.
- b. The Service Detail page will appear. For each Service in this table, edit the settings and save your changes.

Service Name	Service Detail Page Settings
<ul style="list-style-type: none"> • Outlook Web App – HTTPS / Outlook Anywhere (Port 443) 	<ul style="list-style-type: none"> • In the General section, set the value of Service Type to Layer 7 - HTTP. • In the SSL Offloading section, set Enable HTTPS/SSL to Yes. In the SSL Certificate menu, select the certificate that you uploaded in <i>Preparing Your Environment for SSL Offloading</i>. • In the Persistence section, set Persistence Type to HTTP Cookie. • In the Advanced Options section, set Session Timeout to 0. This means that the Barracuda Load Balancer never times out the session, ensuring that Ajax and login features of Outlook Web App will work.
<ul style="list-style-type: none"> • Outlook Web App – HTTP Redirect 	<ul style="list-style-type: none"> • In the General section, set the value of Service Type to Layer 7 – HTTP. Set the value of Enable HTTP Redirect to Yes.
<ul style="list-style-type: none"> • IMAP4 (Port 143) • IMAP4 / SSL (Port 993) • POP3 (Port 110) • POP3 SSL (Port 996) 	<ul style="list-style-type: none"> • In the General section, set the value of Service Type to TCP Proxy. Persistence is not required for these Services as they are transactional based.
<ul style="list-style-type: none"> • MAPI / RPC Client Access (Port 65500) • MAPI / DCOM (Port 135) • MAPI / Global Address Book (Port 65501) • ActiveSync (Port 443) 	<ul style="list-style-type: none"> • In the General section, set the value of Service Type to TCP Proxy. • In the Advanced Options section, set the Session Timeout to 0. This means that the Barracuda Load Balancer never times out the session, ensuring that the heartbeat works for push Services with ActiveSync and Outlook client connectivity.

4. Edit all Real Servers for the OWA – HTTPS / Outlook Anywhere Service:

- a. On the **Basic > Services** page, edit each Real Server associated with the OWA – HTTPS Service by clicking the Real Server Edit () graphic. The Real Server Detail page will appear.
- b. In the **Server Monitor** section, set the **Testing Method** to **HTTP**.
 - i. Change the **Port** value to **80**.
 - ii. Change the **Test Target** value to the FQDN of the VIP address that clients will use to access OWA. This document has thus far referred to this as `http://owa.domain.local`
 - iii. Change **Test Match** to **2006 Microsoft Corporation**


5. If the CAS server is also a HUB transport server, create the following Services for your transport servers. This will allow you to load balance the SMTP traffic to your HUB transport servers.

Note: Exchange Hub Transport should *never* be configured to communicate with other internal Microsoft Exchange Hub Servers via the Barracuda Load Balancer. The Service on the Barracuda Load Balancer should only be used for client connections or inbound connections from other organizations.

- a. Go to the **Basic > Services** page in the Web interface.
- b. For each entry in the following table, add a Service.

Service Name	Virtual IP Address	Protocol	Service Type	Service Port	Real Server Port	Monitor Port
SMTP	VIP address for FQDN that resolves to CAS array e.g. exchange.domain.local	TCP	TCP Proxy	25	25	25
SMTP / SSL (optional)	VIP address for FQDN that resolves to CAS array e.g. exchange.domain.local	TCP	TCP Proxy	456	456	456

Change the Service type for the SMTP and SMTP / SSL Services to TCP Proxy:



- a. On the **Basic > Services** page, edit the Service by clicking the Service Edit () graphic.
 - b. The Service Detail page will appear.
 - In the **General** section, set the value of **Service Type** to **TCP Proxy**.
 - c. Save your changes.
6. When this has been done on the active Barracuda Load Balancer, your installation is complete. Continue to *Testing Your Microsoft Exchange Installation*.




Deploying Exchange 2010 in a Two-armed Configuration

In this final task you will create Services that identify the servers in the CAS array on the active Barracuda Load Balancer by doing the following steps:

1. Go to the **Basic > Services** page in the Web interface.
2. For each entry in the following table, add a Service. To add a Service:
 - In the **Service Name** box, enter the name for the Service.
 - In the **Virtual IP** box, enter the VIP address specified in the table.
 - Select the protocol and in the **Port** box, enter the port for the Service in the table.
 - In the **Real Servers** box, enter the IP address for every server in the CAS array.
 - You will change the Service Type (from the default of Layer 4) in the next steps.

Service Name	Virtual IP Address	Protocol	Service Type	Service Port	Real Server Port	Monitor Port
Exchange	VIP address for FQDN that resolves to CAS array e.g. exchange.domain.local	TCP	TCP Proxy	ALL	N/A	443
OWA – HTTPS	VIP address for FQDN that clients use to access OWA e.g. owa.domain.local	TCP	TCP Proxy	443	80	80
OWA – HTTP (Redirect)	VIP address for FQDN that clients use to access OWA e.g. owa.domain.local	TCP	TCP Proxy	80	N/A (Redirect Service)	80

3. Edit the Exchange Service:
 - a. On the **Basic > Services** page, edit the Exchange Service by clicking the Service Edit () graphic. The Service Detail page will appear.
 - b. In the **Persistence** section, set **Persistence Time (Seconds)** to **3600**.
 - c. Save your changes.
4. Edit the OWA – HTTPS Service:
 - a. On the **Basic > Services** page, edit the OWA – HTTPS Service by clicking the Service Edit () graphic. The **Service Detail** page will appear.
 - b. In the **General** section, set the value of **Service Type** to **Layer 7 - HTTP**.
 - c. In the **SSL Offloading** section, set **Enable HTTPS/SSL** to **Yes**.
 - d. In the **SSL Certificate** menu, select the certificate you uploaded in *Preparing Your Environment for SSL Offloading*.
 - e. In the **Persistence** section, set **Persistence Type** to **HTTP Cookie**.
 - f. Save your changes.
5. Edit all Real Servers for the OWA – HTTPS Service:

- a. On the **Basic > Services** page, edit each server added to the OWA – HTTPS service by clicking the Real Server Edit () graphic. The Real Server Detail page will appear.
 - b. In the **Server Monitor** section, set the **Testing Method** to **HTTP**.
 - i. Change the **Port** value to **80**.
 - ii. Change the **Test Target** value to the FQDN of the VIP in DNS that clients will connect to access OWA. This document has thus far referred to this as `http://owa.domain.local`
 - iii. Change **Test Match** to **2006 Microsoft Corporation**
6. Edit the OWA – HTTP Service:
- a. On the **Basic > Services** page, edit the OWA – HTTPS Service by clicking the Service Edit () graphic. The Service Detail page will appear.
 - b. In The **General** section, set the value of **Service Type** to **Layer 7 – HTTP**. Set **Enable HTTP Redirect** to **Yes**.
 - c. Save your changes.
7. Change the port for every Real Server associated with the OWA – HTTPS Service:
- a. On the **Basic > Services** page, edit each Real Server listed under the OWA – HTTPS Service by clicking the Server Edit () graphic. The Real Server Detail page will appear.
 - b. In the **Real Server Detail** section, set **Port** to **80**.
 - c. Save your changes.
8. Update TCP timeout values on the Barracuda Load Balancer:
- a. Go to the **Advanced > System Settings** page in the Web interface.
 - b. Set the **TCP Connections Timeout** and **TCP Closed Connections Timeout** to 1200 seconds.
9. Your installation is complete. Continue to *Testing Your Microsoft Exchange Installation*.

Testing Your Microsoft Exchange Installation

1. Configure an Outlook client on your local network:
 - a. If Autodiscover is enabled, ensure clients are connected to your CAS array and the VIP address that you just configured and that there are no certificate errors.
 - b. If Autodiscover is not enabled, configure an Outlook client to connect to the FQDN of the new CAS array you just configured. While configuring a new Exchange e-mail account, type in the FQDN of one of the Real Servers (members) of the CAS array. Enter a valid email account name and click **Check Name**. Ensure that the Exchange Server name gets rewritten as the FQDN of the CAS array and the account name is underlined.
 - c. Open the Global Address book in Outlook and make sure it behaves normally.
 - d. Watch an authenticated and connected Exchange client and ensure that it remains connected to Exchange while idle and does not disconnect and reconnect within one or two minutes.

2. Test SSL Offloading:
 - a. Open a browser and go to the FQDN of the VIP address for your SSL offloaded HTTPS Service (for Outlook Anywhere and Outlook Web App). Ensure the browser has no certificate errors or warnings and that the certificate presented by the browser is the correct certificate that should be assigned to the SSL offloaded Service.