How to Deploy Microsoft Exchange Server 2010 in a Two-Armed Configuration

https://campus.barracuda.com/doc/19333222/

Product Versions and Prerequisites

This article applies to the Barracuda Load Balancer ADC version 5.1 and above, with Microsoft® Exchange Server 2010.

For a full list of the prerequisites for this deployment, see Microsoft Exchange Server 2010 Deployment.

Follow the steps in this article to deploy the Microsoft® Exchange Server 2010 in a two-armed configuration.

Configuring Clustered Barracuda Load Balancer ADCs

If your Barracuda Load Balancer ADCs are clustered, the configuration between the active and passive units is synchronized; you only need to configure the active Barracuda Load Balancer ADC.

Step 1. Create Services

On the Barracuda Load Balancer ADC, create services for the Exchange services.

1. Log into the Barracuda Load Balancer ADC, and go to the **BASIC > Services** page.
2. Add all of the services listed in Table 1. For each service, add all the real servers in the CAS array. To add a service, click **Add Service** and enter the values in the corresponding fields. To add a real server, click **Add Server** and enter the IP address and port for the server.

Table 1. Required Services

Name	Type	IP Address	Port	Session Time	SSL Settings	Certificates	Load Balancing	Real Server Port
Exchange	Layer 4 - TCP	VIP address for the FQDN that resolves to the CAS array e.g. `exchange.domain.local` **Note**: This service is helpful in cases where there is no port restriction.	ALL	N/A	N/A	N/A	**Persistence Time:** 1200	N/A

OWA-HTTPS	Instant SSL	VIP address for that FQDN that clients use to access OWA e.g., `owa.domain.local`	Port: 443 HTTP Service Port: 80	1200	◦ **Secure Site Domain** – Enter the domain name of your Exchange server. If the internal and external domain are different, you can use wildcard characters. For example: `*.barracuda.com` ◦ If your Barracuda Load Balancer ADC is running version *5.1.1 and above*, set the **Rewrite Support** option to **On**. For versions *below 5.1.1*, this option is named **Instant SSL**.	Select the certificate that you uploaded when preparing your environment for SSL offloading. See Step 2 in the "Deploying Exchange Services on the Barracuda Load Balancer ADC" section of Microsoft Exchange Server 2010 Deployment.	◦ **Persistence Type:** HTTP Header ◦ **Persistence Time:** 1200 ◦ **Header Name:** Authorization	80

3. If you have the Barracuda Load Balancer ADC 640 and above, you can enable **Application Security** for OWA-HTTPS.
    1. For **Application Security**, select **Enable**.
    2. For **Security Mode**, select the **Passive** mode. It is recommended that you run the service in Passive mode before going active.
    3. From the **Security Policy** list, select **owa2010**. This policy is predefined for all Exchange applications. If you want to edit the policy settings, go to the **SECURITY > Security Policies** page
    4. You need to modify the default **owa2010** policy. Go to the **SECURITY > Security Policies** page and select the **owa2010** security policy. In the **Cookie Security** section, set **Tamper Proof Mode** to **None**.

        > If you want to use Integrated Windows Authentication with the OWA-HTTPS service, go to the **Request Limits** section of the security policy settings and increase the **Max Header Value Length** to `800`.
4. For OWA-HTTPS *only*, enable health checks for its real servers.
    1. Next to the entry of the real server, click **Edit**.
    2. Scroll to the **Server Monitor** section, and enter the values in the corresponding fields.

Testing Method	Port	Test Target	Test Match	Additional Headers	Status Code	Test Delay
Simple HTTPS	443	/owa/auth/logon.aspx (unless you modified the default path of logon.aspx)	Microsoft Corporation	User-Agent: Barracuda Load Balancer ADC Server Monitor	200	30

    3. Click **Save**.
5. If SNI is enforced on the Microsoft Exchange server(s), you need to configure the following options. Go to the **BASIC > Services** page and click **Edit** for each affected server.
    1. Change the port on the server to 443.
    2. Navigate to the **SSL** section and set **Server uses SSL** to **On**.

   3. Expand **Settings** and set **Enable SNI** to **Yes**.
6. If you deployed the Hub Transport Role on servers other than those in the CAS array, add the following services in Table 2.

   Table 2. (If applicable) SMTP Services

Name	Type	IP Address	Port	Real Server Port	Monitor Port
SMTP	Layer 4 - TCP	VIP address for the FQDN that resolves to HUB Services e.g., `smtp.domain.local`	25	25	25
(Optional) SMTP_SSL	Layer 4 - TCP	VIP address for the FQDN that resolves to HUB Services e.g., `smtp.domain.local`	587	587	587

7. Update the TCP timeout values on the Barracuda Load Balancer ADC.
   1. Go to the **ADVANCED > System Configuration** page.
   2. Set the **TCP Connections Timeout** and **TCP Closed Connections Timeout** to **1200** seconds.

Step 2. Configure an HTTP Request Rewrite Rule

To simplify access to the Outlook Web Access site for your users, configure a rewrite rule to add `/OWA` to the end of the URL.

1. Go to the **TRAFFIC > Web Translations** page.
2. From the **Service** list, select the **OWA-HTTPS** service.
3. In the **HTTP Request Rewrite** section, add the following rule. Click **Add Rule** and enter the values in the corresponding fields.

Rule Name	Sequence number	Action	Old Value	Rewrite Value	Rewrite Condition
OWA	3	Redirect URL	/	/OWA	*

4. Click **Save**.

Next Steps

Your installation is complete. You can now test your setup and configure access control to your applications. For instructions, see:

- How to Test the Microsoft Exchange Server 2010 Deployment Configuration
- Access Control