Microsoft Exchange Server 2010 Deployment

https://campus.barracuda.com/doc/3539043/

This article applies to:

- Barracuda Load Balancer running firmware version 3.6.1.009 or higher
- Barracuda Load Balancer 340 or above
- Microsoft® Exchange Server 2010

This article assumes you are connected to the Barracuda Load Balancer web interface and have an activated subscription.

If you wish 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 Understanding Barracuda Load Balancer High Availability for details.

Introduction

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 and here provides details for deploying the Barracuda Load Balancer in this environment.

Table 1. 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 (HUB)	The Hub Transport server role handles all mail flow inside the organization and delivers messages to a recipient's mailbox.
Outlook Web App (OWA)	Originally called Outlook Web Access, OWA is the Webmail component of Microsoft Exchange Server 2010.

Deployment Options

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.

Deployment Tasks

The following sections provide instructions for 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.

Second, prepare to offload the SSL processing of Exchange services onto the Barracuda Load Balancer.

Third, configure the Service or Services that the clients use to access the CAS array on the Barracuda Load Balancer using the deployment instructions specific to your desired configuration.

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.

Configure the Client Access Server (CAS) Array

In this task you configure MAPI client access (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 access their mailboxes using RPC, and connect to the FQDN of the RPC Client Access Array set on the mailbox database. The FQDN 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.

> The following steps assume a single-site Exchange environment; contact Microsoft if you need assistance configuring a CAS Array in a multi-site environment.

To configure the CAS Array,

1. On the DNS Server, add an A record to the DNS zone that associates the VIP address with the FQDN (e.g., exchange.domain.local) that will be used by the clients to connect to the Client Access server array.
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 FQDN (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. In a single-site Exchange environment, use the Exchange Management Shell to 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 FQDN of the Client Access server array.
   If you are deploying in a multiple-site Exchange environment, you should restrict the **Set-MailboxDatabase cmdlet** with **–Identity *'mailbox database name'*** to return only databases you wish to include in the CAS Array. Refer to the Microsoft TechNet online library

article Get-MailboxDatabase for the cmdlet syntax.

Prepare Your Environment for SSL Offloading

Use the following steps to offload SSL processing to the Barracuda Load Balancer. You must complete these steps for both deployment options.

In order to maintain session persistence using HTTP cookies, SSL encryption and decryption must occur 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.

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 Microsoft TechNet online library article Export an Exchange Certificate for instructions on exporting your Exchange certificate.
2. Install the certificates, certificate chain, and private key on the Barracuda Load Balancer on the **BASIC > Certificate** page in the Barracuda Load Balancer web interface.
3. Configure the Exchange 2010 Services to be SSL offloaded.
   Follow all of the steps in the the Microsoft TechNet online library article How to Configure SSL Offloading in Exchange 2010 for how to configure OWA, Outlook Anywhere (OA), Exchange Control Panel (ECP), Exchange Web Services (EWS), and ActiveSync (EAS) for SSL offloading.
   If you do not wish to turn off SSL on the Exchange IIS website, ensure you complete the optional steps when setting up services to enable Backend SSL on each Real Server.
4. There are a few more steps related to SSL offloading that will be performed in the next task.

Select Your Deployment Option

- If your Exchange servers must be on the same subnet as the rest of your topology, choose a one-armed, Route-Path deployment. Continue with: How to Deploy Microsoft Exchange Server 2010 in a One-Armed Configuration
- 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. Continue with: How to Deploy Microsoft Exchange Server 2010 in a Two-Armed Configuration

Refer to the Microsoft TechNet online library for more information on the following topics:

- Load Balancing Requirements for Exchange Protocols
- Configure SSL Offloading for Outlook Anywhere
- Microsoft Exchange Network Port Reference
- Understanding Load Balancing in Exchange 2010
- Create a New Exchange Certificate