Microsoft Exchange Server 2010 Deployment

https://campus.barracuda.com/doc/19333216/

Barracuda Networks has conducted interoperability tests using the Barracuda Load Balancer ADC and Microsoft® Exchange Server 2010. Follow the steps in this guide to deploy the Barracuda Load Balancer ADC to increase the scalability and reliability of your Microsoft Exchange Server 2010 deployment. Using a Barracuda Load Balancer ADC allows load balancing of a Client Access server (CAS) array.

Product Versions and Prerequisites

You must have:

- Barracuda Load Balancer ADC version 5.1 or 5.2.
- Microsoft® Exchange Server 2010 (Barracuda recommends that you upgrade to the latest service pack, SP3).
- Installed your Barracuda Load Balancer ADC(s), connected to the web interface, and activated your subscription(s).
- If you want to deploy the Microsoft Exchange Server with high availability, clustered your Barracuda Load Balancer ADCs. For more information, see High Availability.
- Completed the steps in the following Deploying Exchange Services on the Barracuda Load Balancer ADC section.

Terminology

Term	Description
Microsoft Exchange Server	A Microsoft Exchange Server deployment consists of Client Access Servers (CAS), Hub transport Server, and Exchange Mailbox servers.
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 ADC 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 ADC.
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.

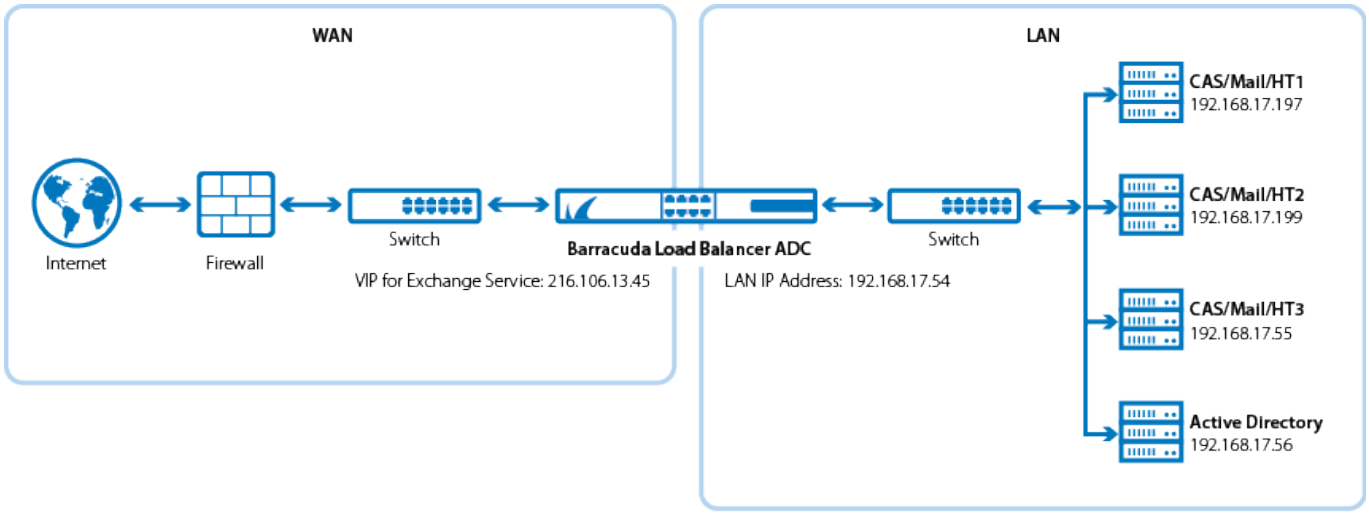
Deployment Options

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

- If your Exchange servers are on the same subnet as the rest of your topology, choose a one-armed, Route-Path deployment.
- If the Exchange servers are on a separate subnet from the rest of the topology and connected to the LAN side of the Barracuda Load Balancer ADC, choose a two-armed, Route-Path deployment.

Deploying in Direct Server Return with Microsoft Exchange 2010 is untested and unsupported.

Two-Arm Deployment Scenario



Microsoft TechNet Resources

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

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

Deploying Exchange Services on the Barracuda Load Balancer ADC

To deploy the Exchange servers with the Barracuda Load Balancer ADC, complete the following steps:

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. Configure the Client Access Server (CAS) Array

To configure MAPI client access (for example, Microsoft Outlook clients), configure the CAS array for the Exchange domain. You only need to complete this configuration on one Exchange Server. For any other options that you might want to consider, consult Microsoft documentation. Note that Microsoft only allows one CAS array per site.

Clients access their mailboxes with RPC and connect to the FQDN of the RPC CAS array set on the mailbox database. The FQDN resolves to a virtual IP address on the Barracuda Load Balancer ADC. In turn, the Barracuda Load Balancer ADC connects with one of the Client Access servers.

Help for Multi-Site Exchange Environments

The following steps assume a single-site Exchange environment. If you need help with configuring a CAS array in a multi-site environment, contact Microsoft.

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 is used by clients to connect to the CAS Array.

2. On one Exchange server in the array, open the Exchange Management Shell and create a new CAS array.
    1. Verify that there are no existing CAS arrays. Enter the following command:
    Get-ClientAccessArray
    In an unconfigured single-site deployment, the command returns nothing.
    2. Create a new CAS array. Enter the following command:
    New-ClientAccessArray -Fqdn *exchange.domain.local* -Site *Default-First-Site-Name*
    where *exchange.domain.local* is the FQDN of the CAS array and *Default-First-Site-Name* is the Active Directory site to which the CAS array belongs.
3. Ping the FQDN (e.g. exchange.domain.local). The ping fails because the service has not yet been created on the Barracuda Load Balancer ADC, but verify that the domain name resolves correctly to the VIP address.
4. Add a mailbox database to the CAS array. In the Exchange Management Shell, enter the following command:
    Get-MailboxDatabase | Set-MailboxDatabase -RpcClientAccessServer exchange.domain.local
    where *exchange.domain.local* is the FQDN of the CAS array.
    If you are deploying in a multiple-site Exchange environment, restrict the Set-MailboxDatabase cmdlet with -Identity '*mailbox database name*' to return only the databases that you want to include in the CAS Array. For the cmdlet syntax, see the Microsoft TechNet article Get-MailboxDatabase .

Step 2. Prepare Your Environment for SSL Offloading

Offload SSL processing to the Barracuda Load Balancer ADC. To maintain session persistence using HTTP cookies, SSL encryption and decryption must occur on the Barracuda Load Balancer ADC. Offloading the SSL processing to the Barracuda Load Balancer ADC 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 ADC 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), see the Microsoft TechNet article Export an Exchange Certificate for instructions on exporting your Exchange certificate.
2. In the Barracuda Load Balancer ADC web interface, go to the **BASIC > Certificates** page and install the certificates, certificate chain, and private key.
3. Configure the Exchange 2010 Services to be SSL offloaded. For more information on configuring OWA, Outlook Anywhere (OA), Exchange Control Panel (ECP), Exchange Web Services (EWS), and ActiveSync (EAS) for SSL offloading, see the Microsoft TechNet article How to Configure SSL Offloading in Exchange 2010.

Next Step

If your Exchange servers are on the same subnet as the rest of your topology, continue with:

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

If your Exchange servers are not on the same subnet as the rest of your topology, and are connected to the interface configured for the internal network side of the Barracuda Load Balancer ADC, continue with:

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

Figures

1. Exchange2010_deployment_new.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.