Microsoft SharePoint Server Deployment

https://campus.barracuda.com/doc/24674793/

The Barracuda Load Balancer ADC increases the scalability and reliability of your Microsoft Office SharePoint Server 2007, 2010, or 2013 deployment. You can deploy SharePoint servers in clusters with two or more front-end servers, an SQL server, and an application server. The Barracuda Load Balancer ADC can provide advanced Layer 7 load balancing and Layer 7 application security for your SharePoint servers.

Product Versions and Prerequisites

You must have:

- Barracuda Load Balancer ADC version 5.1 or above.
- Microsoft® SharePoint Server 2007, 2010, or 2013.
- Installed your Barracuda Load Balancer ADC(s), connected to the web interface, and activated your subscription(s).
- If you want to deploy SharePoint Server with high availability, clustered your Barracuda Load Balancer ADCs. For more information, see High Availability.

Terminology

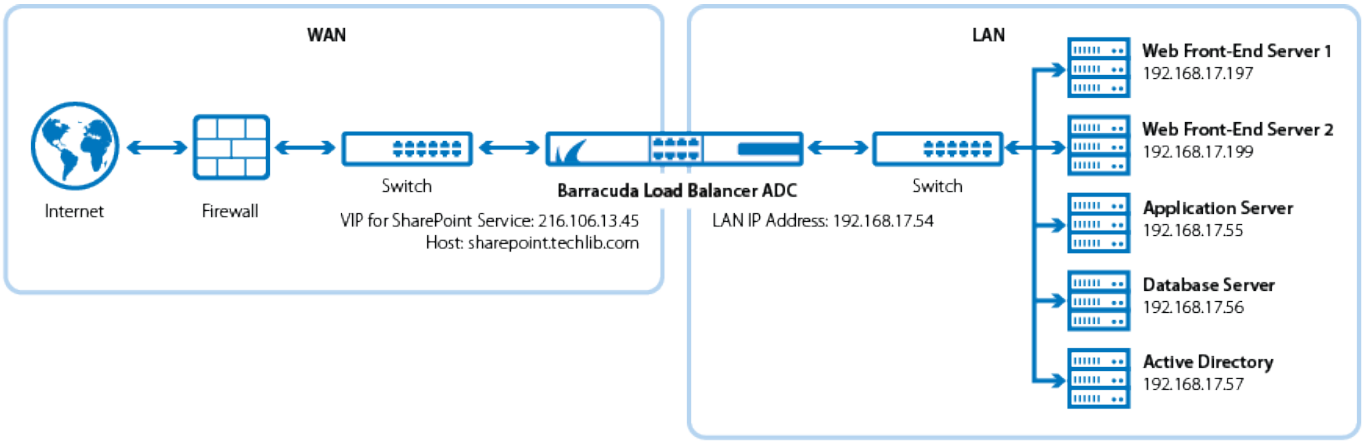
Term	Definition
Service	A combination of a virtual IP (VIP) address and one or more TCP/UDP ports that the Barracuda Load Balancer ADC listens on. Traffic arriving over the specified port(s) is directed to one of the real servers associated with that service.
Instant SSL	The Instant SSL Service allows clients to talk to the service using HTTPS while the Barracuda Load Balancer ADC talks to the server using HTTP. In the Instant SSL service settings, you must specify one secured site domain whose links must be converted from HTTP to HTTPS. When the redirect service receives a request from the specified domain, it forwards the request to the service on port 443 (HTTPS), which then forwards the request to the servers. In any responses, the HTTPS service rewrites the HTTP request into an HTTPS request. For example, if you specify `http://www.barracuda.com/` every occurrence is rewritten to `https://www.barracuda.com/` in outgoing responses. After you add the Instant SSL service, you can edit the HTTPS service to add more domains that must be rewritten in responses.

Deployment Options

Microsoft recommends a three-tier system of deploying SharePoint servers. For instructions, see these Microsoft TechNet articles:

- **(SharePoint 2013)** Install SharePoint 2013 across multiple servers for a three-tier farm – http://technet.microsoft.com/en-us/library/ee805948.aspx
- **(SharePoint 2010)** Multiple servers for a three-tier farm – http://technet.microsoft.com/en-us/library/ee805948%28v=office.14%29.aspx
- **(SharePoint 2007)** Install Office SharePoint Server 2007 in a server farm environment – http://technet.microsoft.com/en-us/library/cc262901(v=office.12).aspx

Deployment Scenario



Barracuda Load Balancer ADC Service Options

On the Barracuda Load Balancer ADC, create services which correspond to the type of traffic supported by your SharePoint servers, and considering the desired traffic type for client access. You can use the table below to decide whether Instant SSL, HTTP, or HTTPS services are your best option:

Deployment Scenario	Service Options
The SharePoint servers support traffic over HTTP only and you want clients to access on HTTP only.	Create an HTTP service
The SharePoint servers support traffic over HTTP only and you want clients to access over HTTPS	Create an Instant SSL service.

The SharePoint servers support traffic over HTTPS only.	Create an HTTPS service.
The SharePoint servers support traffic over HTTP and HTTPS.	See above scenarios for HTTP and HTTPS.

Deploying SharePoint Services on the Barracuda Load Balancer ADC

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

> If your Barracuda Load Balancer ADCs are clustered, the active and passive unit configurations are synchronized; you only need to configure the active Barracuda Load Balancer ADC.

Step 1. (HTTPS and Instant SSL Services) Export and Upload a SharePoint Certificate

If you are creating an HTTPS or Instant SSL service, export a certificate from your SharePoint server and upload it to the Barracuda Load Balancer ADC.

1. Export a certificate from your SharePoint front-end server. For instructions on how to export a server certificate from your IIS server, see the Microsoft TechNet article at http://technet.microsoft.com/en-us/library/cc731386%28v=ws.10%29.aspx.
   > If the SharePoint servers are not bound to a certificate, you can create a self-signed certificate. For instructions, see How to Add an SSL Certificate.
2. Log into the Barracuda Load Balancer ADC as an administrator.
3. Go to the **BASIC > Certificates** page and upload the certificate from your SharePoint front-end server.
   - If you are importing a certificate from IIS, it is in PKCS12 format.
   - Enter a password for the certificate.

Step 2. Create Services for the SharePoint Servers

Add services according to the type of traffic supported by your SharePoint servers.

1. Go to the **BASIC > Services** page.
2. For each service that you add from Table 1, click **Add Service** and enter the values in the corresponding fields.

Table 1. Available Services

Name	Type	IP Address	Port	Caching	Compression

SharePoint_HTTP	HTTP	IP address for the fully qualified domain name (FQDN) that clients use to access SharePoint	80	Select **On**. Then expand the caching settings, and add the types of files that are used by your servers.	Select **On**. Then expand the compression settings, and add these content types: ◦ `application/vnd.ms-publisher` ◦ `application/pdf` ◦ `application/xml`
SharePoint_HTTPS	HTTPS	IP address for the fully qualified domain name (FQDN) that clients use to access SharePoint	443		
SharePoint_InstantSSL	Instant SSL	IP address for the fully qualified domain name (FQDN) that clients use to access SharePoint	**Port**: 443 **HTTP Service Port**: 80		

3. If you have an active subscription for **Application Security**, enable it and configure these settings:
   - **Security Mode** – Select the **Passive** mode. It is recommended that you run the service in Passive mode before going active.
   - **Security Policy** – For SharePoint 2007 and 2010, select **SharePoint**. For SharePoint 2013, select **SharePoint 2013**. These policies are predefined for all SharePoint applications. To edit these policies, go to the **SECURITY > Security Policies** page.
4. For Instant SSL services *only*, configure these settings in the **SSL Settings** section:
   1. In the **Secure Site Domain** field, enter the domain name of your SharePoint server . If the internal and external domain are different, you can use wildcard characters. For example: `*.barracuda.com`
   2. 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**. Then enable **SharePoint Rewrite Support** in the settings.

      Ensure that your alternate access mappings in Microsoft SharePoint are set correctly to support SSL offloading. To configure Microsoft SharePoint, go to

> **SharePoint Central Administration**, **Application Management**, **Configure alternate access mappings**, and ensure that the public URL for **Internet Zone** is set to https:// and the **Internal URL** is set to http://.

5. For HTTPS and Instant SSL services *only*, select the **Certificate** that you uploaded for your SharePoint server.
6. If your servers are configured in a cluster, specify these settings in the **Load Balancing** section:
   - **Algorithm** – Select **Round Robin**.
   - **Persistence Type** – Select **Cookie Insert** and then configure the cookie settings that appear. Name the cookie `Persistence`.
7. Click **Create**.
8. If you have integrated Business Connectivity Services (BCS) with your SharePoint deployment for any of the services created from Table 1, go to the **Other** section and set **Ignore Expect Headers** to **Yes**.

Step 3. Add the Real Servers

Add your SharePoint servers to your services. For each SharePoint server:

1. On the **BASIC > Services** page, verify that the correct service for the server is displayed.
2. Click **Add Server**.
3. Enter the IP address and port of the front-end servers.
4. If the server is part of a cluster, specify whether it is a **Backup server** and enter its **Weight** for the load balancing algorithm.
5. If traffic must be encrypted before being passed to the server, configure these settings in the **SSL** section:
   - **Servers uses SSL** – Select **On**.
   - **Settings** – Expand this section,and then select the SSL protocols to use.

   If you do not enable the server to use SSL, unencrypted traffic is passed to the server because the Barracuda Load Balancer ADC decrypts incoming traffic in order to maintain session persistence using HTTP cookies.
6. If you are adding the server to an HTTPS or Instant SSL service, select the **Certificate** that you uploaded for your SharePoint server.
7. In the **Server Monitor** section, specify the method, port, login credentials, and settings for monitoring the availability of the server.
   - For the **Testing Method**, select **MS SharePoint** or **MS SharePoint Secure**.
   - For **Username**, enter the administrator username you configured for your SharePoint site, beginning with the domain (for example, `domain\adminuser`).
   - For **Password**, enter the password for the user account specified above.
   - For **Test Target**, enter your SharePoint site (for example, `/sites/demo_site/`).
   - For **Test Match**, enter `Microsoft SharePoint`.
   - For **Additional Headers**, specify the host (this should be the same host specified in your SharePoint Central Administration for your SharePoint application).
   - For the **Status Code**, specify 200.
   - For the **Test Delay**, specify 10 seconds.
8. Click **Create**.

Step 4. Configure Mapping for De-encrypted Traffic to Real Servers

If traffic sent to the back-end servers changes from encrypted to unencrypted as a result of deploying the Barracuda Load Balancer ADC, you may need to configure Alternate Access Mappings through SharePoint Central Administration.

Step 5. Change DNS and NAT for Barracuda Load Balancer ADC VIP Address

Change your internal DNS and external NATs or external DNS to point to the Barracuda Load Balancer ADC VIP address.

Next Step

You can configure an authentication server with the Barracuda Load Balancer ADC. For Microsoft SharePoint, Kerberos authentication is supported.

- For information on how to configure Kerberos authentication, see the **Kerberos** section of How to Integrate an External Authentication Server
- For information on how to configure your application to accept authentication from the Barracuda Load Balancer ADC, see the SharePoint 2007, 2010, or 2013 for Kerberos Authentication section under How to Configure Access Control (AAA)

Figures

1. SharePoint_Deployment_new.png