

## Microsoft Office SharePoint Server 2007, 2010 and 2013 Deployment

<https://campus.barracuda.com/doc/24674713/>

This article describes how to deploy your Barracuda Load Balancer with Microsoft Office SharePoint Server 2007, 2010 and 2013 to increase the scalability and reliability of your SharePoint deployment.

This article applies to:

- Barracuda Load Balancer running firmware version 3.6.1.009 or higher
- Barracuda Load Balancer model 340 or above
- Microsoft Office SharePoint Server 2007, 2010 or 2013

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

If you wish to increase the reliability of your Microsoft Office SharePoint Server deployment with High Availability, you must first have a pair of [Barracuda Load Balancers joined in a cluster](#). If your Barracuda Load Balancers are already clustered, the configuration between the active and passive systems is synchronized automatically, so you do not need to modify any passive Barracuda Load Balancers.

### Example Installation

This article is written for a SharePoint deployment where SharePoint servers support traffic over both HTTP and HTTPS. In this environment, create two Services on the Barracuda Load Balancer, one for each type of traffic. The incoming traffic will be load-balanced among the servers. The Barracuda Load Balancer will monitor the server health by periodically requesting a page from each server.

### Install the SharePoint Certificate on the Barracuda Load Balancer

1. Obtain the SSL certificate for SharePoint.
2. Install the certificates, certificate chain, and private key using the **BASIC > Certificate** page in the Barracuda Load Balancer web interface.

## Configure Services

1. Go to the **BASIC > Services** page. Make sure the **Add New Service** section is in the advanced view, and add each Service listed in the following table:

Service Name	Service Type	Virtual IP Address	SSL Certificate	Real Servers
SharePoint HTTP Service	Layer 7 - HTTP	IP address for the fully qualified domain name (FQDN) that clients use to access SharePoint; Port 80		Internal IP addresses of your SharePoint Servers; Port 80
SharePoint HTTPS Service	Layer 7 - HTTPS	IP address for the fully qualified domain name (FQDN) that clients use to access SharePoint; Port 443	SharePoint SSL certificate	Internal IP addresses of your SharePoint Servers; Port 443

2. In the **Services Configuration** table, click the **Edit** icon in the **Actions** column for each of the newly added Services. On the **Service Detail** page that appears:
  - In the **Service Monitor** section, select the **MS Sharepoint** or **MS Sharepoint Secure** and complete the fields for the test. This test issues an HTTP/S request to the specified page and checks the returned page for the expected text. Authentication information for the SharePoint server is required.
  - In the **Persistence** section, enter **1200** in the **Persistence Time (Seconds)** field, and set the **Persistence Type** to **HTTP Cookie**; additional fields display, but leave them at their default values.
  - In the **Advanced Options** section, set **Session Timeout** to **0** (session never times out).

## Encrypted Traffic to Real Servers

The Barracuda Load Balancer decrypts the incoming traffic in order to maintain session persistence using HTTP cookies. By default, this unencrypted traffic is passed to the Real Servers.

If you want the traffic to be sent encrypted instead, then edit each Real Server from the **BASIC > Services** page and change the **Enable HTTPS/SSL** setting to **Yes**.

As a result of deploying the Barracuda Load Balancer, the traffic sent to the Real Servers changes from encrypted to unencrypted, you may have to configure Alternate Access Mappings through SharePoint Central Administration.



© Barracuda Networks Inc., 2024 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.