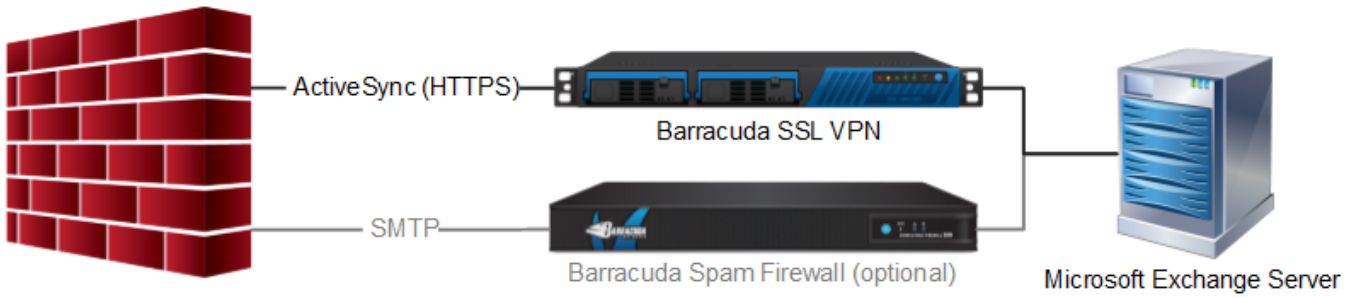
Best Practice - Protect your Exchange Server with the Barracuda SSL VPN

https://campus.barracuda.com/doc/39815463/To protect the Microsoft Exchange server from the direct external access, you can deploy a Barracuda SSL VPN as a Threat Management Gateway (TMG) to handle all HTTPS traffic for the Exchange server coming from the Internet. The client connects to the Barracuda SSL VPN using Outlook Anywhere (formerly known as RPC over HTTPS). Authentication and proxying of all traffic is also handled by the SSL VPN. Optionally deploy a Barracuda Spam Firewall to scan SMTP traffic.



Before you begin

- Make sure that you have a valid SSL certificate signed by a trusted root Certification Authority (CA) or a self-signed certificate. If you are using a self-signed certificate, you must import it to the local certificate store on all the client machines on which you want to use Outlook.
- If required, open port 443 on your internal firewall so that the Barracuda SSL VPN can communicate with the Exchange Server.
- Create an Authentication Scheme using a Microsoft Active Directory Server user database.

Step 1. Configure the Barracuda SSL VPN

Configure the Barracuda SSL VPN to act as an RPC Proxy.

1. Log into the SSL VPN web interface.
2. Open the **Mange System > RESOURCES > Configuration** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Outlook** section, configure the following settings:
    1. In the **Exchange Server** field, enter the Exchange server's hostname.
    2. In the **Exchange Port** field, enter 443 (unless you have configured the Exchange server to listen on a different port).
    3. In the **Protocol** area, select the **HTTPS** option.
    4. In the **Authorized Policies** section, select one or more policies that contain the users

that should have access to the Outlook proxy and click **Add** to add them to the **Selected Policies** area.

5. Click **Save Changes**.

Step 2. Configure the Exchange server

For each Exchange server, complete the following steps:

1. Open the Exchange 2013 web interface.
2. From the left hand panel of the **Exchange admin center** page, go to **servers** and select **servers** from the main menu.
3. Double click the Exchange Server that you want to configure.
4. From the left hand panel of the server configuration window, select **Outlook Anywhere**.
5. Enter the external host name for your Exchange Server, for example: *mail.mycompany.com.*
6. Set the authentication type to *Basic.* By default, authentication is set to *NTLM*, which does not work for clients that are connecting from a different domain than the Exchange Server.

Step 3. Configure the Outlook 2013 client

On the client's Windows system, configure the Outlook 2013 client:

1. Open the **Control Panel**.
2. Double-click the **Mail**.
3. Click **Show Profiles**.
4. Click **Add** to add a new mail profile.
5. Enter a unique **name** for the mail profile and click **OK**.
6. Select the **Manually configure server settings or additional server types** option and click **Next**.
7. Select the **Microsoft Exchange or compatible service** option and click **Next**.
8. In the **Server** field, enter the Barracuda SSL VPN hostname, for example: `sslvpn.example.com`
9. In the **User Name** field, enter your username in the following format: `username@domain.` Do NOT click **Check Name**.
10. Click **More Settings**.
11. Select the **Connection** tab.
12. In the **Outlook Anywhere** section, select the **Connect to Microsoft Exchange using HTTP** option and click **Exchange Proxy Settings**...
13. In the **Connection settings** section, complete the following steps:
    1. In the **Use this URL to connect to my proxy server for Exchange** field, enter the Barracuda SSL VPN hostname.
    2. Check the option for **On fast networks, connect using HTTP first, then connect**

   using TCP/IP.
   3. Check the option for **On slow networks, connect using HTTP first, then connect using TCP/IP**.
   4. In the **Proxy authentication settings** area, select *Basic Authentication* from the **Use this authentication when connecting to my proxy server for Exchange** drop-down menu.
   5. Click **OK** and then click **Next**.
14. The **Exchange Server** prompts you to connect and requests your credentials:
   1. In the **User Name** field, enter your username using the following format: *domain\username*
   2. In the **Password** field, enter your password and click **OK**.
15. Click **Finish** and then click **OK**.

Step 4. Test the configuration from an external network

Use the following procedure to determine if your Outlook 2013 clients are successfully connecting to your Exchange Server 2013 using Outlook Anywhere:

1. From the command line, start **outlook.exe /rpcdiag**. The Outlook email client and an extra diagnostic window opens. Keep this window open to test your configuration.
2. If prompted, select the new Outlook profile and click **OK**.
3. The Exchange Server prompts you to connect and requests your credentials. Using the format *domain\username,* type your username and password, and click **OK**. The Outlook client then retrieves the client's email from the Exchange Server through the Outlook Anywhere connection.
4. Check the **Connection Status** window.

When the Outlook client is fully connected, you will
see 4 connections (2 Mail types and 2 Directory types) to your Exchange Server. All of these connections should show a connection (**Conn)** type of HTTPS. If they do, the test is successful.

Troubleshooting Outlook Anywhere

If the connection type is TCP/IP, then the Outlook client is connected directly to the Exchange Server and is not using RPC. If this is the case, verify the following points to troubleshoot the issue:

- Verify your Outlook 2013 client configuration.
- Verify your Exchange Server 2013 configuration.
- Verify that you have a valid SSL certificate signed by a trusted root Certification Authority (CA) or a self-signed certificate installed on the Barracuda SSL VPN.
- If you are using a self-signed certificate, verify that you have imported it to the local certificate

store on all the client systems that are using Outlook 2013.
- If required, verify that you have opened port 443 on your internal firewall for the Barracuda SSL VPN to communicate with your Exchange Server.
- Make the appropriate Outlook and Exchange Server configuration changes, and test your configuration from your external network.

Figures

1. OutlookAnywhere.png

© 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.