Example SSL VPN Resource Configurations

https://campus.barracuda.com/doc/41116143/

This article provides examples of how to set up these types of SSL VPN resources:

Web Resource

This example configures access to an internal web resource.

1. Open the **SSL-VPN** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service**).
2. In the left menu, click **Web Resources**.
3. Click **Lock**.
4. In the **Web Resources** section, click the **+** icon to add an entry for the internal web resource. Configure the following settings for the entry:
5. In the **Name** field, enter `Company web server`. Then click **OK**.
6. Select the **Active** check box to enable the link.
7. In the **Visible Name** field, enter `Our internal website`.
   Every resource has a **Name** and a **Visible Name**. The name of the resource should differ from the visible name that is displayed on the SSL VPN portal. For example, a server can be named as "sales-portal" and users will know it as "intranet."
8. In the **Link Description** field, enter: `This is the internal website of our company`.
9. In the **URL** field, enter the URL of the web resource.
10. Leave the other settings as default.
11. Click **OK**.
12. Click **Send Changes** and **Activate**.

WebDAV

This example configures access for a specific MSAD group to the company file server. To minimize the risk of virus infiltration for such a setup, the Barracuda Access Monitor health check is recommended.

1. Open the **SSL-VPN** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service**).
2. In the left menu, click **WebDAV/Sharepoint**.
3. Click **Lock**.
4. In the **WebDAV Resources** section, click the **+** icon to add an entry for the resource. Configure the following settings for the entry:

1. In the **Name** field, enter `WebDAV share`. Then click **OK**.
2. Select the **Active** check box to enable the link.
3. In the **Visible Name** field, enter `Our internal website`.
4. In the **Link Description** field, enter `This is the internal website of our company.`
5. In the **WebDAV Address** field, enter the address of the WebDAV share.
6. In the **WebDAV Sharename** field, enter the WebDAV share name.
7. Select the **Must Be Healthy** check box to require health checks for the client.
8. In the **Allowed User Groups** section, delete the asterisk (*) and enter the MSAD group name. For example: `CN=sales*`

5. Click **OK**.
6. Click **Send Changes** and **Activate**.

SharePoint

This example provides steps to configure access for a specific MSAD group to a network drive that is mapped in SharePoint. In the example, SharePoint has already been configured.

Step 1. Map the Network Drive

In SharePoint, map the network drive:

1. Log into your SharePoint account and browse to the desired library.
2. To display the URL for the library, click the address bar. You can copy and save the address to the clipboard.
3. Go to my computer and select **Map network drive**.
4. Select the hyperlink and connect to the web drive.
5. Click **Next** to start the *Add Network Location Wizard*.
6. Click **Choose a custom network location** and then click **Next**.
7. Enter or paste the URL from the document library that you found in the address line, and then click **Next**.
8. Enter a descriptive name for the network drive and click **Next**. You are prompted with a message stating that your web folder has been successfully mapped.

Step 2. Add the Share to the SSL VPN Service

On the Barracuda NG Firewall, create an SSL VPN resource for the mapped share.

1. Open the **SSL-VPN** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service**).
2. In the left menu, click **WebDAV/Sharepoint**.
3. Click **Lock**.
4. In the **WebDAV Resources** section, click the **+** icon to add an entry for the resource. Configure

the following settings for the entry:

1. In the **Name** field, enter a name for the mapped network drive.Then click **OK**.
2. Select the **Active** check box to enable the link.
3. In the **Visible Name** field, enter a descriptive name that should be displayed.
4. In the **Link Description** field, enter an optional description if required.
5. In the **WebDAV Address** field, enter or paste the URL of the mapped network drive.
6. In the **WebDAV Sharename** field, enter the name of the mapped network drive.
7. Select the **Must Be Healthy** check box to require health checks for the client.
8. In the **Allowed User Groups** section, delete the asterisk (*) and enter the MSAD group name. For example: `CN=sales*`

5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Application Tunneling

The following examples configure tunneling for these applications:

Windows Terminal Service

This example configures access for for a specific MSAD group to a Windows terminal service.

1. Open the **SSL-VPN** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service**).
2. In the left menu, click **Application Tunneling**.
3. Click **Lock**.
4. In the **Service Configuration** section, click the **+** icon to add an entry for the resource. Configure the following settings for the entry:
   1. In the **Name** field, enter `Windows terminal service`. Then click **OK**.
   2. Select the **Active** check box to enable the link.
   3. In the **Visible Name** field, enter `Windows RDP`.
   4. In the **Link Description** field, enter `Company terminal server.`
   5. In the **Application Server IP** field, enter the IP address of the Windows terminal server.
   6. From the **Application Protocol** list, select **RDP**.
   7. For the **Application TCP Port** field, no changes are necessary if port 3389 is configured at the terminal server. If port 3389 is not being used, select **Other** and enter the appropriate port number.
   8. Leave the **RDP Application Path** field empty.
   9. From the **Tunnel Client Application** list, select *yes* because port forwarding should be used.
   10. In the **Client Loopback TCP Port** field, enter `3390.`
   11. In the **Allowed User Groups** table, delete the asterisk (*) and then add the assigned MSAD group name. For example: `CN=accounting*`
5. Click **OK**.

6. Click **Send Changes** and **Activate**.

SAP Application

This example configures access for all sales staff members to the SAP application at the sales terminal server. Users are only allowed to execute the SAP application.

- Do not include spaces in directory names.
- Only *.exe files can be executed.
- Separate directories with a forward slash (/) or double forward slash (//). Backslashes (\) are not allowed.

1. Open the **SSL-VPN** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service**).
2. In the left menu, click **Application Tunneling**.
3. In the **Service Configuration** section, click the **+** icon to add an entry for the resource. Configure the following settings for the entry:
   1. In the **Name** field, enter `terminalsales`. Then click **OK**.
   2. Select the **Active** check box to enable the link.
   3. In the **Visible Name** field, enter **SAP**.
   4. In the **Link Description** field, enter: `This is the SAP application of the Sales Department.`
   5. In the **Application Server IP** field, enter `192.168.10.10.`
   6. From the **Application Protocol** list, select **RDP**.
   7. For the **Application TCP Port** field, no changes are necessary if port 3389 is configured at the terminal server. If port 3389 is not being used, select **Other** and enter the appropriate port number.
   8. In the **RDP Application Path** field, enter `C:/SAP/sap.exe or C://SAP//sap.exe`
   9. From the **Tunnel Client Application** list, select **yes** because port forwarding should be used.
   10. In the **Client Loopback TCP Port** field, enter `3390`.
   11. In the **Allowed User Groups** table, delete the asterisk (*) and then add the assigned MSAD group name of the sales department. For example: `CN=sales*`
4. Click **OK**.
5. Click **Send Changes** and **Activate**.

Generic Application Tunneling

This example configures access for all staff members to a Citrix server at 10.0.0.112. All staff members working at a home office are required to have a running virus scanner and firewall. Because application browsing is based on UDP, the applications must be configured.

1. Open the **SSL-VPN** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service**).
2. In the left menu, click **Application Tunneling**.
3. In the **Generic Application Tunneling** section, click the **+** icon to add an entry for the resource. Configure the following settings for the entry:
4. In the **Name** field, enter `Citrix.` Then click **OK**.
5. Select the **Active** check box to enable the link.
6. In the **Visible Name** field, enter `Company Citrix server`.
7. In the **Link Description** field, enter an appropriate description for users.
8. In the **SSL Tunnels** table, click the **+**icon and add the required connections. In this example, all TCP ports are required so the following entries are added:

Name	Server IP Address	Client Loopback TCP Port	Application TCP Port
ICA	10.0.0.112	1494	1494
IMA	10.0.0.112	2512	2512
SSL	10.0.0.112	443	443
STA(ISS)	10.0.0.112	80	80
Citrix LicenseManagementConsole	10.0.0.112	8082	8082
PresentationServerLicensing	10.0.0.112	27000	27000
ICA session w/SessionReliabilityenabled	10.0.0.112	2598	2598
Access Gateway Standard and Advanced Editions	10.0.0.112	9001	9001
		9002	9002
		9005	9005
Managerservice daemonserver	10.0.0.112	2897	2897

9. Select the **Must Be Healthy** check box to require health checks for the clients.
10. In the **Allowed User Groups** section, leave the asterisk (*) to grant access to all staff members.
11. Click **OK**.
12. Click **Send Changes** and **Activate**.

Next Steps

Configure the connections of the client software to the loopback address.