How to Configure Network Places

https://campus.barracuda.com/doc/50266391/

After you enable and configure the SSL VPN, you can add network places. Network places give your end users direct access to network file shares in your corporate network. Users accessing the file share are prompted for the username and password. Access and privileges on the file share are determined by the permissions set for the user by the admin of the network file share.

Network places are available for the web portal only. To use a network place resource a Java browser plugin is required on the client.

The following network file systems are supported:

- **SMB** – Connect to SMB1 and SMB2 shares, but must be able to negotiate a CIFS session.
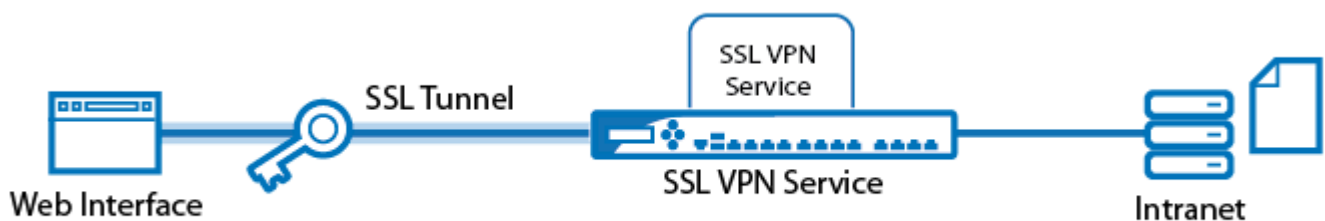
Before you begin

Enable the SSL VPN service. For more information, see How to Enable SSL VPN and CudaLaunch.

Configure Network places

Create a network place resource to let your users access internal SMB network shares.

1. Go to **VPN > SSL VPN** and click the **Resources** tab.
2. In the **Network Places** section, click **Add Network Place**.
3. In the **Add Network Place** window, set **Enable** to **Yes**.
4. (optional) Click **Browse** to upload a PNG file for the web portal, less than 30 kB and not larger than 80x80 pixel.
5. In the **Name** field, enter the visible name for the resource. This is the name used in the web

portal for this resource.

6. Enter the hostname or IP address of the web server.
7. Enter the sharename in the following format: "/" followed by the path and file name.

8. (optional) To restrict access to the web forward by user group, remove the ***** entry in the **Allowed User Groups** list. Enter the user groups that can access the web forward, and click **+** after each entry. If no groups are added, the web forward cannot be accessed. Use question marks (?) and asterisks (*) as wildcard characters.
9. Click **Save**.

Figures

1. sslvpn_network_places.png
2. ssl_res02.png