

---

## How to Configure SSL VPN Access via DynDNS

<https://campus.barracuda.com/doc/48660716/>

You can configure SSL VPN connections to use a DynDNS hostname on the Barracuda NextGen Firewall X-Series instead of an IP address. To enable access to the SSL VPN portal via a DynDNS hostname, enable the DynDNS service. Then, configure an access rule that redirects HTTPS traffic to the SSL VPN service.

### Before you begin

---

- Configure the SSL VPN service. For more information, see [How to Enable SSL VPN and CudaLaunch](#).
- On the **VPN > Settings** page, in the **Global Server Settings** section, verify that **Use TCP Port 443** is set to **No**.

### Step 1. Configure VPN access via a DynDNS hostname

---

To allow SSL VPN access via a dynamic DNS hostname:

1. Go to **NETWORK > IP Configuration**.
2. In the **Dynamic Interface Configuration** section, enable **Use Dynamic DNS** for the required interface.

### Step 2. Create an access rule to redirect SSL VPN traffic

---

Create a **Redirect to Service** access rule that redirects incoming VPN connections on the dynamic interface to the SSL VPN service:

1. Go to the **FIREWALL > Firewall Rules** page.
2. Add an access rule with the following settings:
  - **Name** – Enter a name for the access rule. For example, **Redirect-to-SSL-VPN**.
  - **Action** – Select **Redirect to Service**.
  - **Source** – Select **Internet**, and click **+**.
  - **Redirected To Service Details** – Select **SSL VPN**.
  - **Destination** – Select the network object representing your incoming Internet connection, and click **+**.

## Add Access Rule ?

General
Advanced

Action: Redirect to Service



*DNAT (port forwarding) - Redirect traffic to a specific IP address.  
Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.  
Bi-directional - Source and destination networks are interchangeable.*

Name: Redirect-to-SSL-VPN

Description:

Connection: Default (SNAT)

Adjust Bandwidth: Internet

The interface must have bandwidth management enabled on the NETWORK > IP Configuration page for this policy to be applied.

Bi-directional:  Yes  No

Disable:  Yes  No

IPS:  Yes  No

Application Control:  Yes  No

URL Filter:  Yes  No

Virus Protection:  Yes  No

SSL Inspection:  Yes  No

URL Filter, Virus Protection and SSL Inspection depend on Application Control enabled. URL Filter and Virus Protection require a valid Web Security subscription.

Source

Any +

Ref: Internet

Network Objects  IP Address  Geo Loc.

Redirect to Service Details

SSL VPN

The following protocols and port/protocol combinations are automatically selected upon the chosen Service **SSL VPN**:

TCP 443

Destination

Barracuda Update Servers +

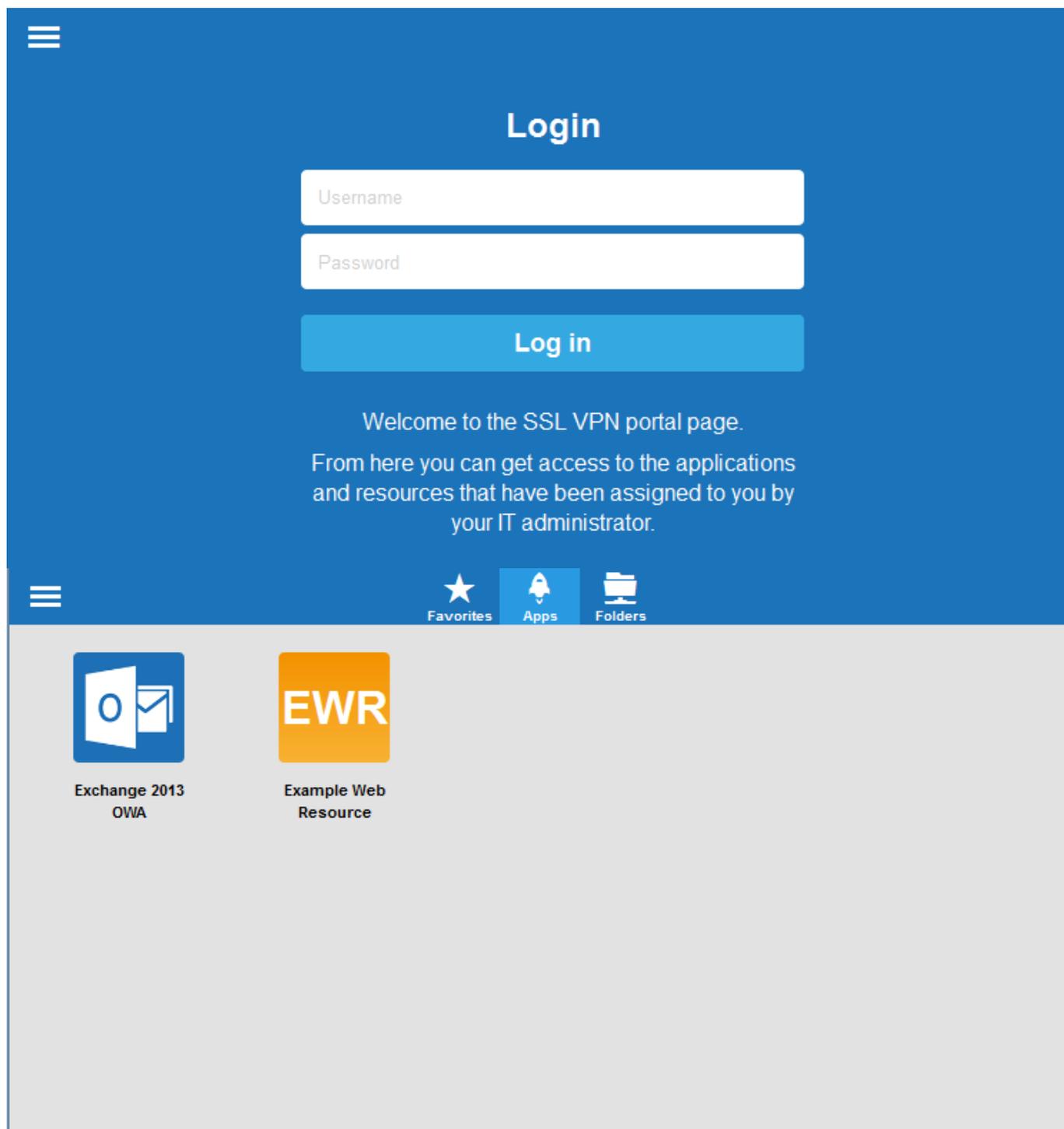
Ref: DHCP1 Local IP

Network Objects  IP Address  Geo Loc.

3. Click **Save**.
4. Drag and drop the access rule so that it is the first rule that matches the traffic you want to forward.
5. Click **Save**.

### Step 3. Access the SSL VPN

End users can now access the SSL VPN portal page via the DynDNS hostname by opening <https://sslvpn/>.



The screenshot shows the login interface of the Barracuda NextGen Firewall X SSL VPN portal. The page has a blue header with a hamburger menu icon on the left. The main content area is also blue and features a 'Login' heading. Below the heading are two white input fields for 'Username' and 'Password', followed by a blue 'Log in' button. A welcome message reads: 'Welcome to the SSL VPN portal page. From here you can get access to the applications and resources that have been assigned to you by your IT administrator.' At the bottom of the blue header, there is another hamburger menu icon and three navigation icons: 'Favorites' (star), 'Apps' (bell), and 'Folders' (folder). The main content area below is light gray and displays two application tiles. The first tile is for 'Exchange 2013 OWA' with a blue icon showing a mail envelope and a checkmark. The second tile is for 'Example Web Resource' with an orange icon containing the letters 'EWR'.

## Figures

1. ssl\_von\_config\_02.png
2. web\_01.png
3. web\_02.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.