

How to Allow VPN Access via a Dynamic WAN IP Address

<https://campus.barracuda.com/doc/14320422/>

You can configure VPN connections to use a dynamically assigned WAN IP address on the Barracuda NextGen Firewall X-Series. In the VPN settings, enable use of dynamic IP addresses. Then configure an access rule that redirects VPN traffic to the VPN server.

Step 1. Configure VPN Access via a Dynamic WAN IP Address

To allow VPN access via a dynamic WAN IP address:

1. On the **VPN > VPN Settings** page, in the **Global Server Settings** section, verify that **Use Dynamic IPs** is set to **Yes**.
2. If you want to make your VPN available through a DNS hostname, you can register the hostname with <http://dyn.com/dns> . For more information, see [How to Configure a DHCP Connection](#).

Step 2. Create an Access Rule to Redirect VPN Traffic to the VPN Server


Create a new access rule that redirects the VPN traffic to the VPN server to establish the tunnel:

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule**.
3. In the **Add Access Rule** windows, configure a **Redirect to Service** firewall rule that redirects incoming VPN connections on the dynamic interface to the VPN server listening on the local IP address. For the **Destination**, select the network object corresponding to your Internet connection type (DHCP, 3G, or DSL).

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-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
VPN
The following protocols and port/protocol combinations are automatically selected upon the chosen Service **VPN**:
UDP 691, UDP 500, UDP 4500, UDP 1701, TCP 1723, TCP 691, TCP 443

Destination
Barracuda Update Servers
Ref: DHCP1 Local IP

☒ Network Objects ☐ IP Address ☐ Geo Loc.

- At the top of the **Add Access Rule** window, click **Add**.
- Move the access rule above the BLOCKALL rule. For more information, see [Firewall Rules Order](#).
- Click **Save**.

Figures

1. DynamicIPVPNAccess_67.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.