

How to Configure VPN Access via a Dynamic WAN IP Address

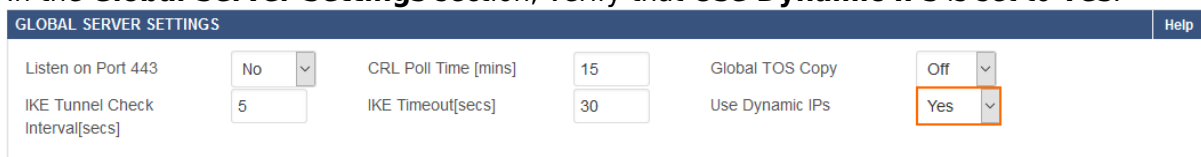
<https://campus.barracuda.com/doc/72516281/>

You can configure VPN connections to use a dynamically assigned WAN IP address on the firewall. In the VPN settings, enable 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. Go to **VPN > VPN Settings**.
2. In the **Global Server Settings** section, verify that **Use Dynamic IPs** is set to **Yes**.



GLOBAL SERVER SETTINGS			Help		
Listen on Port 443	No	CRL Poll Time [mins]	15	Global TOS Copy	Off
IKE Tunnel Check Interval[secs]	5	IKE Timeout[secs]	30	Use Dynamic IPs	Yes

3. To make your VPN available through a DNS hostname, register the hostname with <http://dyn.com/dns>. For more information, see [How to Configure a ISP with Dynamic IP Addresses \(DHCP\)](#).

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 **FIREWALL > Access Rules**.
2. Click **Add Access Rule**. The **Add Access Rule** window opens.
3. In the **Add Access Rule** window, 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, WWAN, 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 NextGen Firewall.
Bi-directional - Source and destination networks are interchangeable.

Name: Redirect-to-VPN

Description:

Connection: Original Source IP

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

SSL Interception: Yes No

URL Filter: Yes No

Virus Scanner: Yes No

ATP: Yes No

Mail Security: Yes No

Safe Search: Yes No

Source

Any +

Ref. Internet -

Network Objects IP Addresses 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

Any +

Ref. DHCP1 Local IP -

Network Objects IP Addresses Geo Loc.

Cancel
Save

4. Click **Save**.
5. Move the access rule above the BLOCKALL rule.
6. Click **Save**.

Figures

1. VPN_global_settings.png
2. dynamic-IP_VPN-access.png

© Barracuda Networks Inc., 2020 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.