

Best Practice - DNS Configuration

<https://campus.barracuda.com/doc/95262089/>

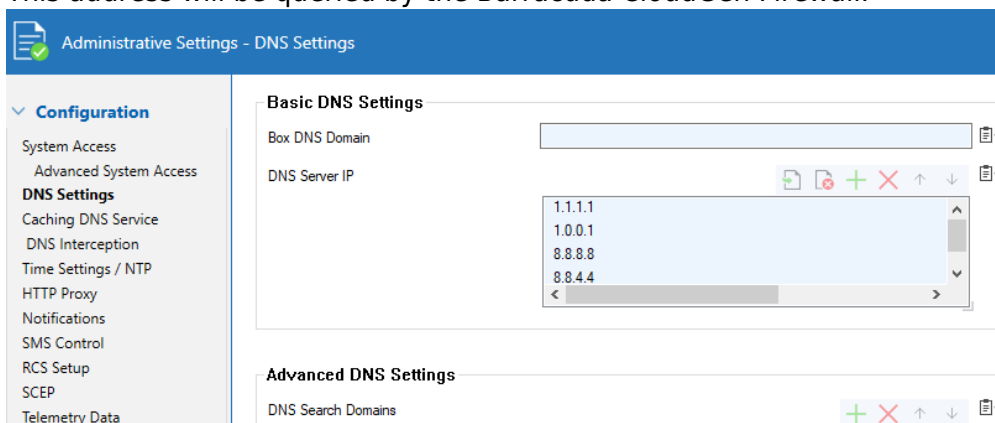
The following cases should be considered when configuring a VPN using the Barracuda VPN Client 5.1.7 and higher on macOS.

No Internal DNS Server Available

If the VPN Group Policy is set up with an external DNS server without any further configurations, the DNS will not be used for any external traffic. It is recommended to use an internal DNS server to bypass this behavior. The following example shows the introduction of an App Redirect rule with the DNS caching service enabled while the gateway IP is used as a DNS server. This configuration ensures a correct DNS resolution.

Step 1. Configure DNS Settings on the Barracuda CloudGen Firewall

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. In the left menu, click **DNS Settings**.
3. Click **Lock**.
4. In the **DNS Server IP** table, add the public DNS Server IP address to the **DNS Server IP** list. This address will be queried by the Barracuda CloudGen Firewall.

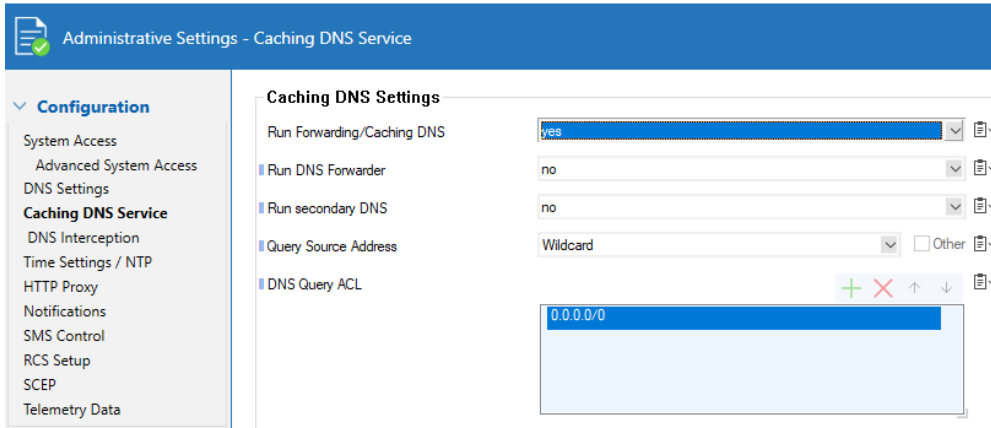


5. Click **Send Changes** and **Activate**.

Step 2. Enable Caching DNS on the Barracuda CloudGen Firewall

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. From the **Configuration Mode** menu, select **Switch to Advanced View**.
3. In the left menu, click **Caching DNS Service**.
4. Click **Lock**.
5. From the **Run Forwarding/Caching DNS** list, activate the local caching/forwarding DNS service.

- In the **DNS Query ACL** table, add the network address 0.0.0.0/0 to allow access to the DNS service via an App Redirect rule.



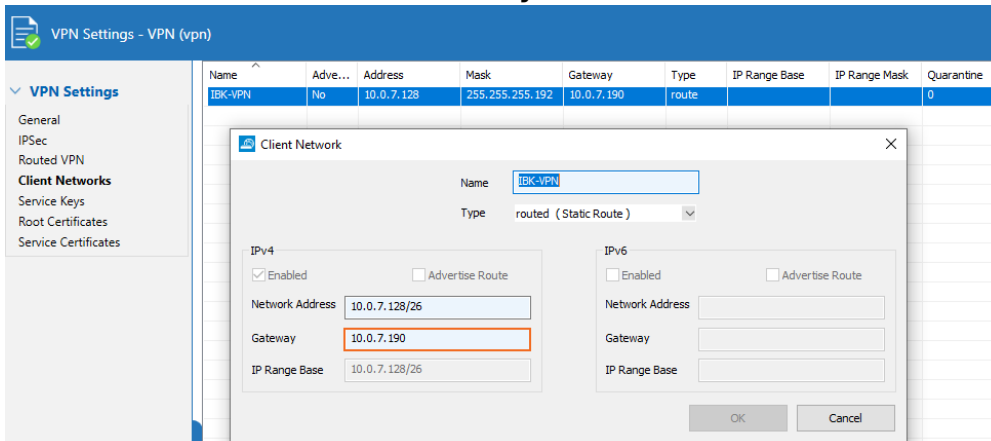
The screenshot shows the 'Administrative Settings - Caching DNS Service' page. On the left is a 'Configuration' sidebar with options like System Access, Advanced System Access, DNS Settings, Caching DNS Service (selected), DNS Interception, Time Settings / NTP, HTTP Proxy, Notifications, SMS Control, RCS Setup, SCEP, and Telemetry Data. The main area is titled 'Caching DNS Settings' and contains several configuration options: 'Run Forwarding/Caching DNS' (set to 'yes'), 'Run DNS Forwarder' (set to 'no'), 'Run secondary DNS' (set to 'no'), 'Query Source Address' (set to 'Wildcard'), and 'DNS Query ACL'. The 'DNS Query ACL' section shows a table with one entry: '0.0.0.0/0'.

- Click **Send Changes** and **Activate**.

For general instructions on how to configure DNS settings on the Barracuda CloudGen Firewall, see [How to Configure DNS Settings](#) and [How to Configure a Caching DNS Service](#).

Step 3. Configure the Client Network

- Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
- Click **Lock**.
- In the left menu, select **Client Networks**.
- Configure the VPN client network. As the **Type**, select **routed (Static Route)**.
- Enter **Network Address** and **Gateway**.



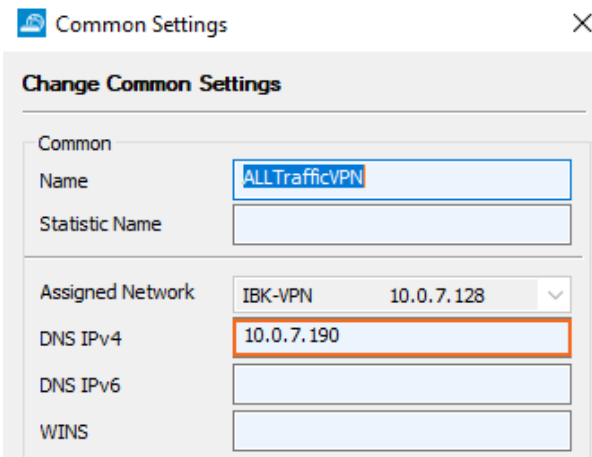
The screenshot shows the 'VPN Settings - VPN (vpn)' page. On the left is a sidebar with options like General, IPSec, Routed VPN, Client Networks (selected), Service Keys, Root Certificates, and Service Certificates. The main area displays a table with VPN settings. A 'Client Network' dialog box is open, showing configuration for a 'routed (Static Route)' network. The dialog has fields for Name (IBK-VPN), Type (routed (Static Route)), and IPv4/IPv6 settings. The IPv4 section is enabled, and the Network Address is 10.0.7.128/26, Gateway is 10.0.7.190, and IP Range Base is 10.0.7.128/26. The IPv6 section is disabled.

- Click **Send Changes** and **Activate**.

Configure Common Settings

- Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Client-to-Site**.
- Click the **External CA** tab and then click the **Common** tab.
- Click **Lock**.

4. Right-click the table and select **New Common**.
5. Enter a descriptive **Name**.
6. Select the network you created from the **Assigned Networks** list.
7. In the **DNS IPv4** field, enter the gateway IP address.



Common Settings

Change Common Settings

Common

Name:

Statistic Name:

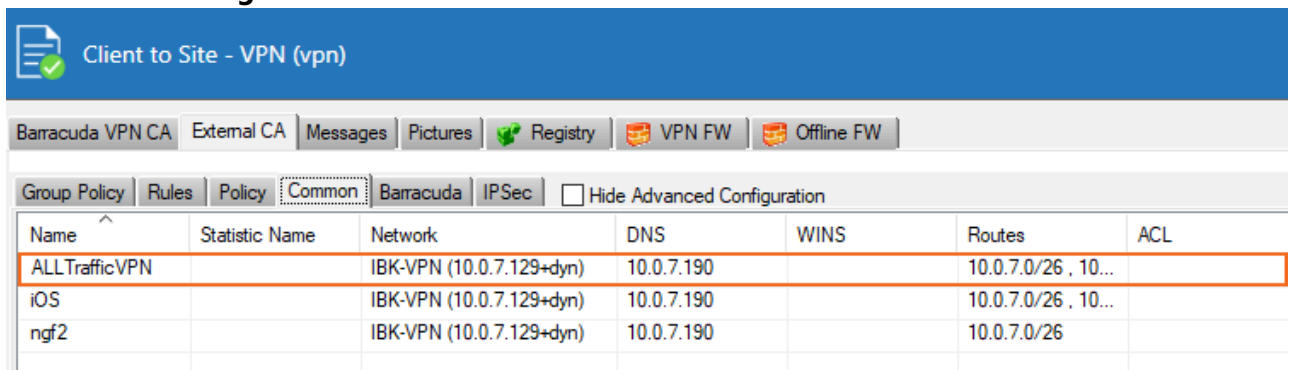
Assigned Network: IBK-VPN 10.0.7.128

DNS IPv4:

DNS IPv6:

WINS:

8. In the **Network Routes** section, enter the VPN network IP address, and click **Add**.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.



Client to Site - VPN (vpn)

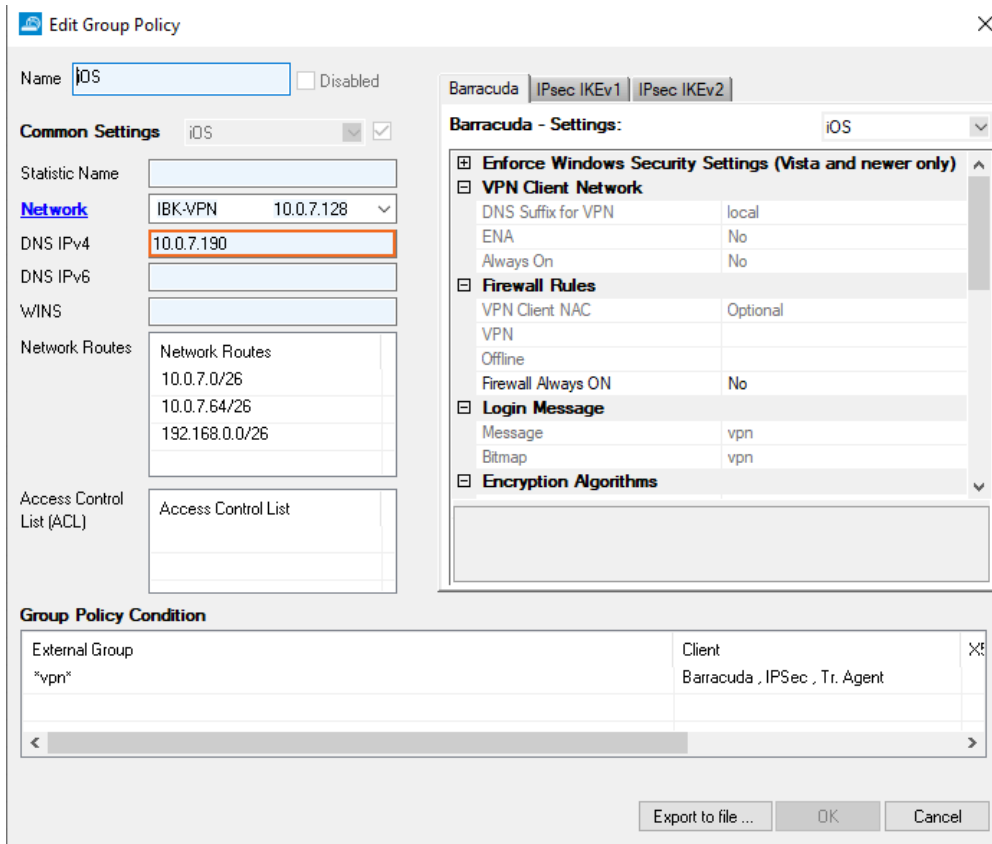
Barracuda VPN CA External CA Messages Pictures Registry VPN FW Offline FW

Group Policy Rules Policy Common Barracuda IPSec ☐ Hide Advanced Configuration

Name	Statistic Name	Network	DNS	WINS	Routes	ACL
ALLTrafficVPN		IBK-VPN (10.0.7.129+dyn)	10.0.7.190		10.0.7.0/26 , 10...	
iOS		IBK-VPN (10.0.7.129+dyn)	10.0.7.190		10.0.7.0/26 , 10...	
ngf2		IBK-VPN (10.0.7.129+dyn)	10.0.7.190		10.0.7.0/26	

Configure the VPN Group Policy

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Client-to-Site**.
2. Click **Lock**.
3. Configure the VPN Group Policy using the gateway IP address as DNS IPv4. For more information, see Step 2 in [How to Configure a Client-to-Site VPN Group Policy](#).



Edit Group Policy

Name: ☐ Disabled

Common Settings ☒

Statistic Name:

Network

DNS IPv4:

DNS IPv6:

WINS:

Network Routes:

Network Routes
10.0.7.0/26
10.0.7.64/26
192.168.0.0/26

Access Control List (ACL):

Access Control List

Barracuda - Settings:

☒ **Enforce Windows Security Settings (Vista and newer only)**

☒ **VPN Client Network**

DNS Suffix for VPN	local
ENA	No
Always On	No

☒ **Firewall Rules**

VPN Client NAC	Optional
VPN	
Offline	
Firewall Always ON	No

☒ **Login Message**

Message	vpn
Bitmap	vpn

☒ **Encryption Algorithms**

Group Policy Condition

External Group	Client	Action
vpn	Barracuda , IPSec , Tr. Agent	

Export to file ... OK Cancel

4. Click **Send Changes** and **Activate**.

Step 4. Create an App Redirect Rule

Create an access rule to allow the VPN client network to access the DNS service.

- Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
- Create an access rule with the following settings:
 - Action** – Select **App Redirect**.
 - Source** – Select the VPN client network.
 - Destination** – Select **explicit** and enter the gateway IP address.
 - Service** – Select **DNS**.
 - Redirection** – Enter the local IP address and port of the DNS service.

Edit Rule: VPNClients-DNS-CachingService-Access [Rule]

Views: Rule, Advanced, ICMP Handling

Object Viewer: ☒ Object Viewer

App Redirect: VPNClients-DNS-CachingService-Access

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source VR Instance: default Destination VR Instance: Same as Source

Source	Service	Destination
IBK_VPN	DNS	<explicit-dest>
10.0.7.128/26	UDP 53 dns Report if not (DNS)	10.0.7.190
	TCP 53 dns Report if not (DNS)	

Redirection: ☒ Create Proxy ARP

Local Address: 127.0.0.1:53

Authenticated User: Any

Policies:

- IPS Policy: Default
- Application Policy: No AppControl
- SSL Inspection Policy: N.A.
- Schedule: Always
- QoS Band (Fwd): No-Shaping
- QoS Band (Reply): Like-Fwd

OK Cancel

For general instructions on how to create an App Redirect rule on the Barracuda CloudGen Firewall, see [How to Create an App Redirect Access Rule](#).

The VPN configuration should now be up and running with the gateway acting as DNS server IP address.

History Selection						Traffic Selection						Source	10.0.7.178
Access, Fail, Rule Block, Packet Drop						Forward, Local In, Local Out, IPv4, IPv6							
AID	Org	IP Proto	Port	Source	Interface	User	Destination	Output-IF	Count	Last	Rule		
✓ 367	LRD	UDP	53	10.0.7.178	pvpn0	p75sa	10.0.7.190	pvpn0	1	32s	VPNClients-DNS-CachingService-Access		
✓ 594	LRD	UDP	53	10.0.7.178	pvpn0	p75sa	10.0.7.190	pvpn0	1	1m 36s	VPNClients-DNS-CachingService-Access		

DNS Probing

The VPN configuration, such as changes to the resolve.conf file, is now done exclusively by the system. To get information about the current DNS configuration, use **scutil --dns**

Note that **nslookup** is not using the default system API.

Figures

1. DNS_1.png
2. DNS_2.png
3. client_net.png
4. common_settings.png
5. common_list.png
6. gp.png
7. edit_rule.png
8. DNS_5.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.