Best Practice - DNS Configuration

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

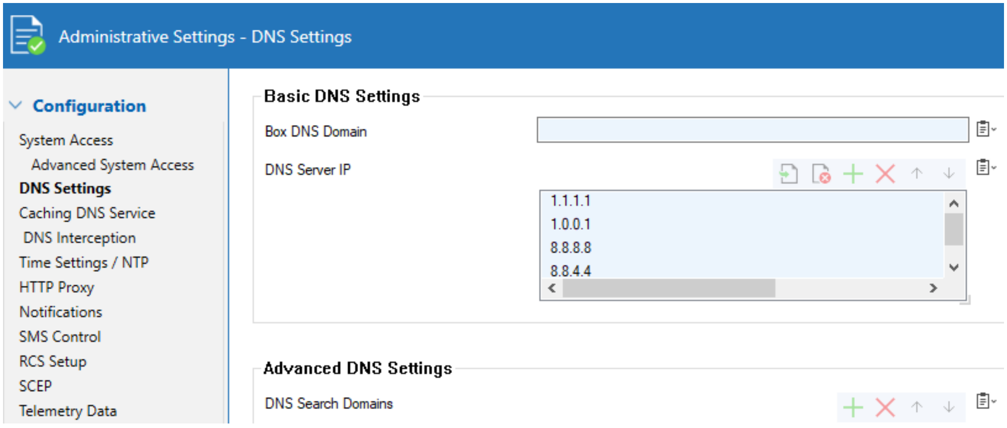
The following cases should be considered when configuring a VPN using the Barracuda VPN Client 5.1.7 and higher on macOS.

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.



Administrative Settings - DNS Settings

Basic DNS Settings

Box DNS Domain

DNS Server IP: 1.1.1.1, 1.0.0.1, 8.8.8.8, 8.8.4.4

Advanced DNS Settings

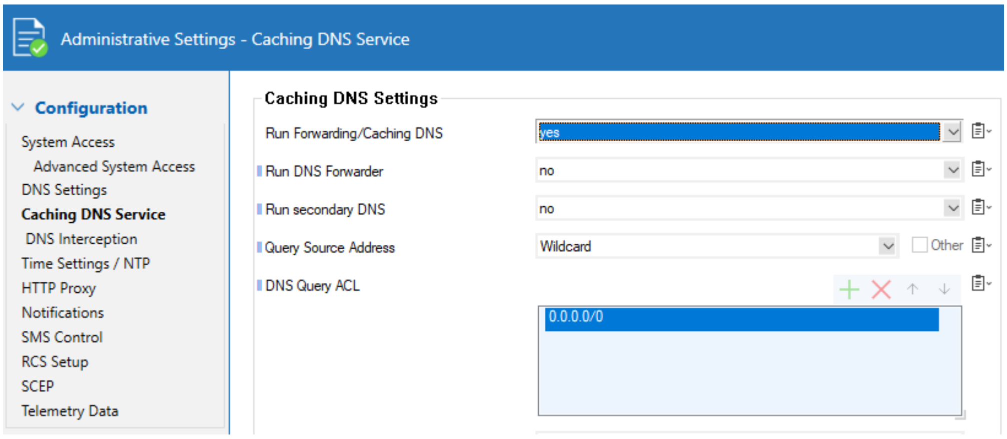
DNS Search Domains

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.

6. 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.



Administrative Settings - Caching DNS Service

Caching DNS Settings

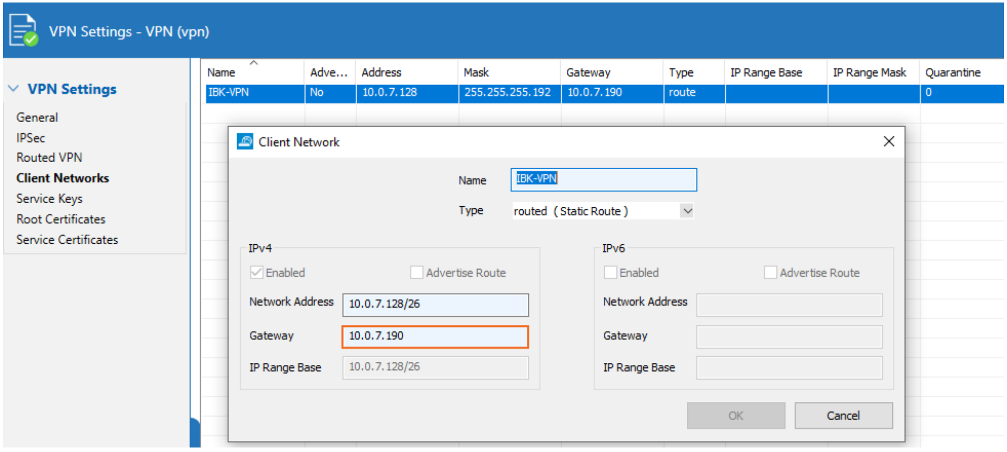
Run Forwarding/Caching DNS	yes
Run DNS Forwarder	no
Run secondary DNS	no
Query Source Address	Wildcard □ Other
DNS Query ACL	0.0.0.0/0

7. 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

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



VPN Settings - VPN (vpn)

Name	Adve...	Address	Mask	Gateway	Type	IP Range Base	IP Range Mask	Quarantine
IBK-VPN	No	10.0.7.128	255.255.255.192	10.0.7.190	route			0

Client Network

Name: IBK-VPN

Type: routed (Static Route)

IPv4

☑ Enabled □ Advertise Route

Network Address: 10.0.7.128/26

Gateway: 10.0.7.190

IP Range Base: 10.0.7.128/26

IPv6

□ Enabled □ Advertise Route

Network Address:

Gateway:

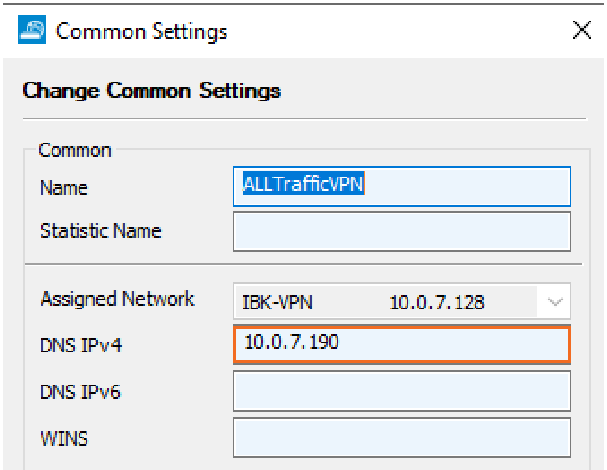
IP Range Base:

6. Click **Send Changes** and **Activate**.

Configure Common Settings

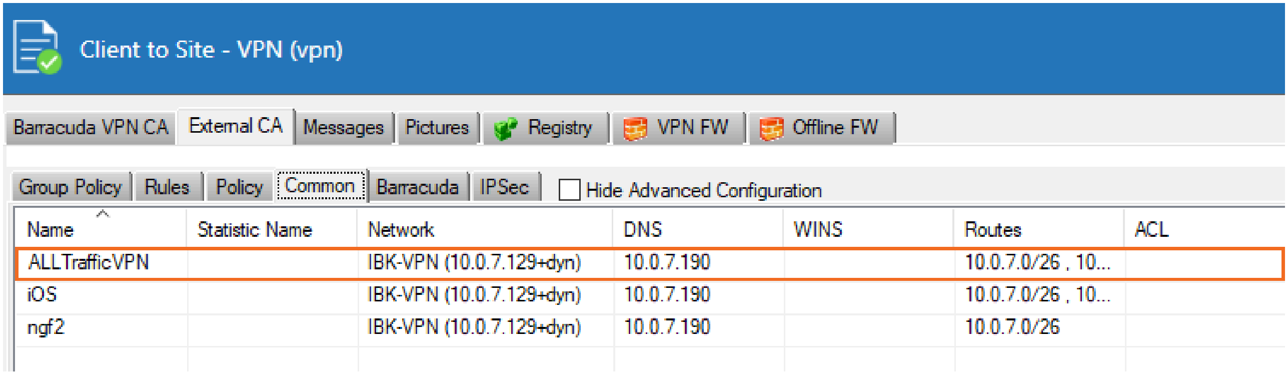
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Client-to-Site**.
2. Click the **External CA** tab and then click the **Common** tab.
3. Click **Lock**.

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.



Name	ALLTrafficVPN
Statistic Name	
Assigned Network	IBK-VPN 10.0.7.128
DNS IPv4	10.0.7.190
DNS IPv6	
WINS	

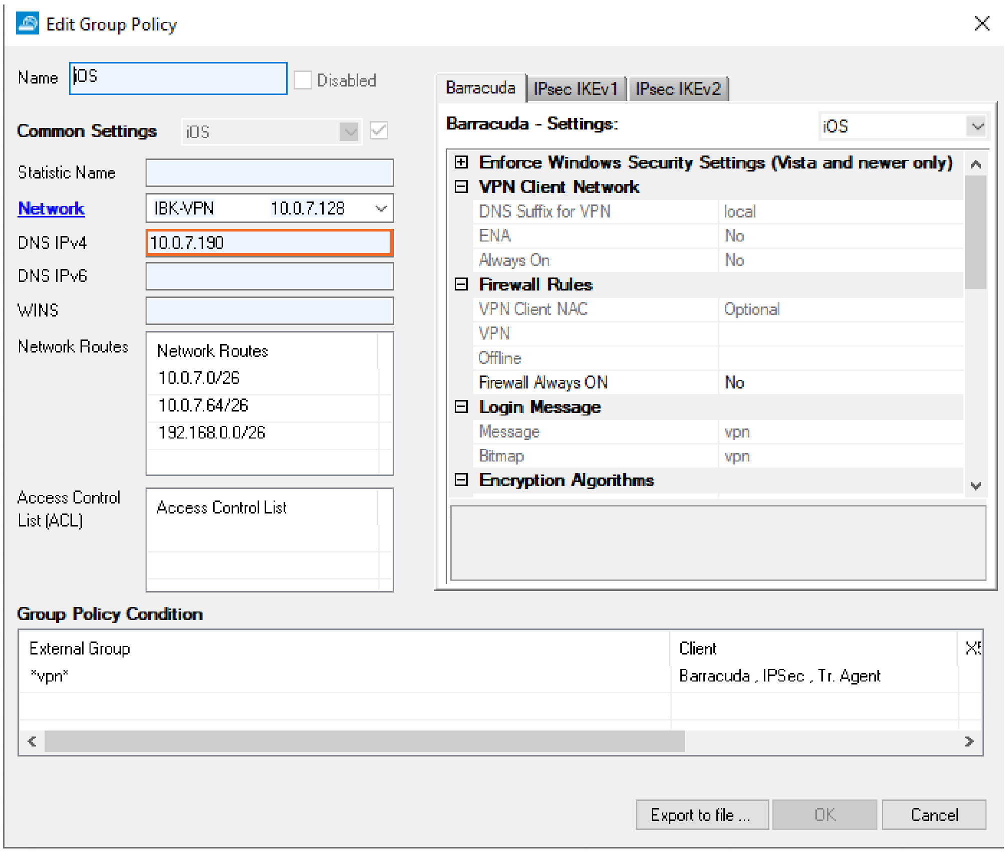
8. In the **Network Routes** section, enter the VPN network IP address, and click **Add**.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.



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: iOS □ Disabled

Common Settings: iOS ☑

Statistic Name	
Network	IBK-VPN 10.0.7.128
DNS IPv4	10.0.7.190
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 | IPsec IKEv1 | IPsec IKEv2

Barracuda - Settings: iOS

⊞ **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

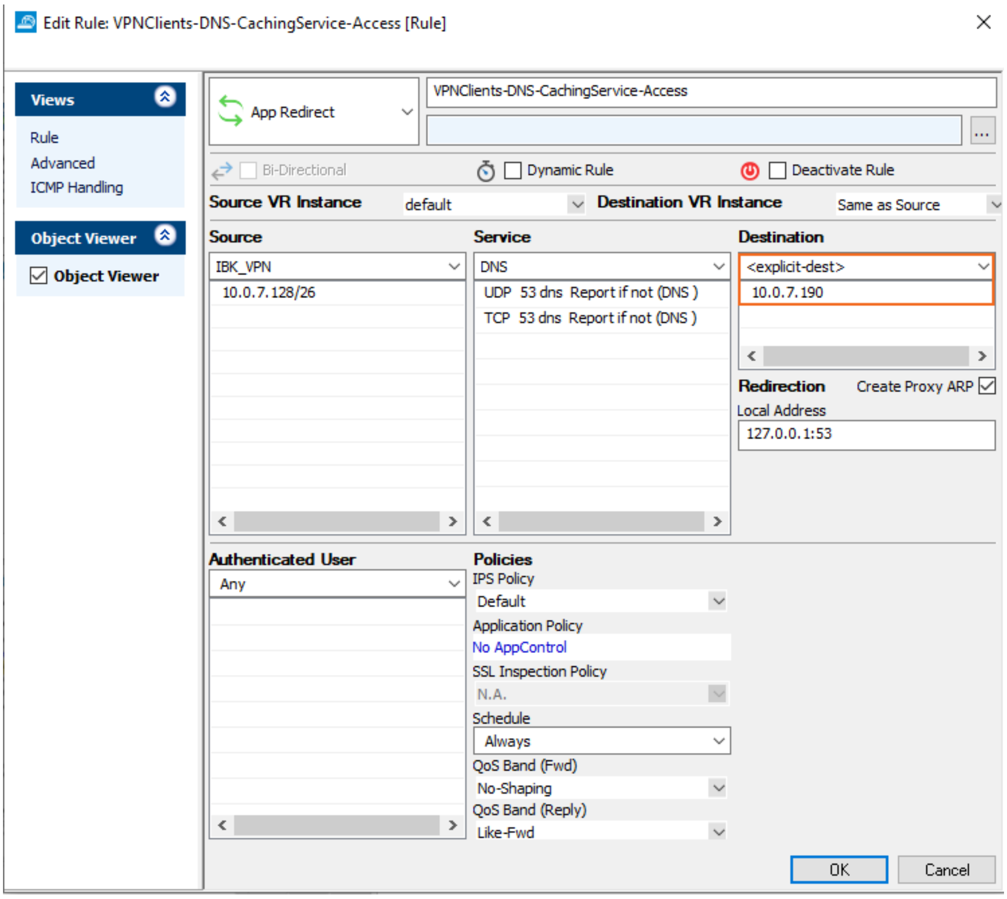
External Group	Client	X5
vpn	Barracuda , IPSec , Tr. Agent	

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.

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Assigned Services** > **Firewall** > **Forwarding Rules**.
2. 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]

App Redirect — VPNClients-DNS-CachingService-Access

□ Bi-Directional □ Dynamic Rule □ Deactivate Rule

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

Source: IBK_VPN
10.0.7.128/26

Service: DNS
UDP 53 dns Report if not (DNS)
TCP 53 dns Report if not (DNS)

Destination: <explicit-dest>
10.0.7.190

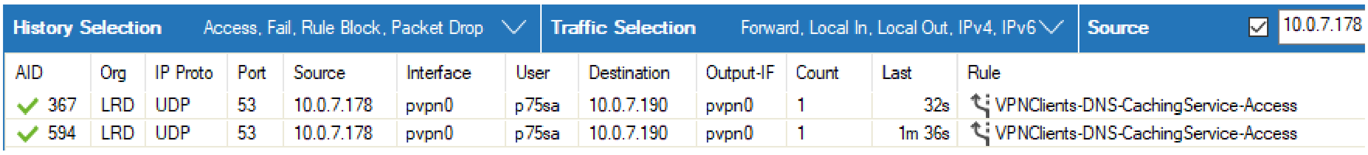
Redirection — Create Proxy ARP ☑
Local Address: 127.0.0.1:53

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

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: Access, Fail, Rule Block, Packet Drop — Traffic Selection: Forward, Local In, Local Out, IPv4, IPv6 — Source ☑ 10.0.7.178

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