How to Configure Authentication Through a Site-to-Site VPN Tunnel

https://campus.barracuda.com/doc/48660879/

If your authentication server is located at a remote location connected via a site-to-site VPN tunnel. By default the firewall uses source-based VPN routing. To be able to connect to the remote authentication server the VPN routes must be added to the main routing table. VPN routes are always added with a metric of 10.

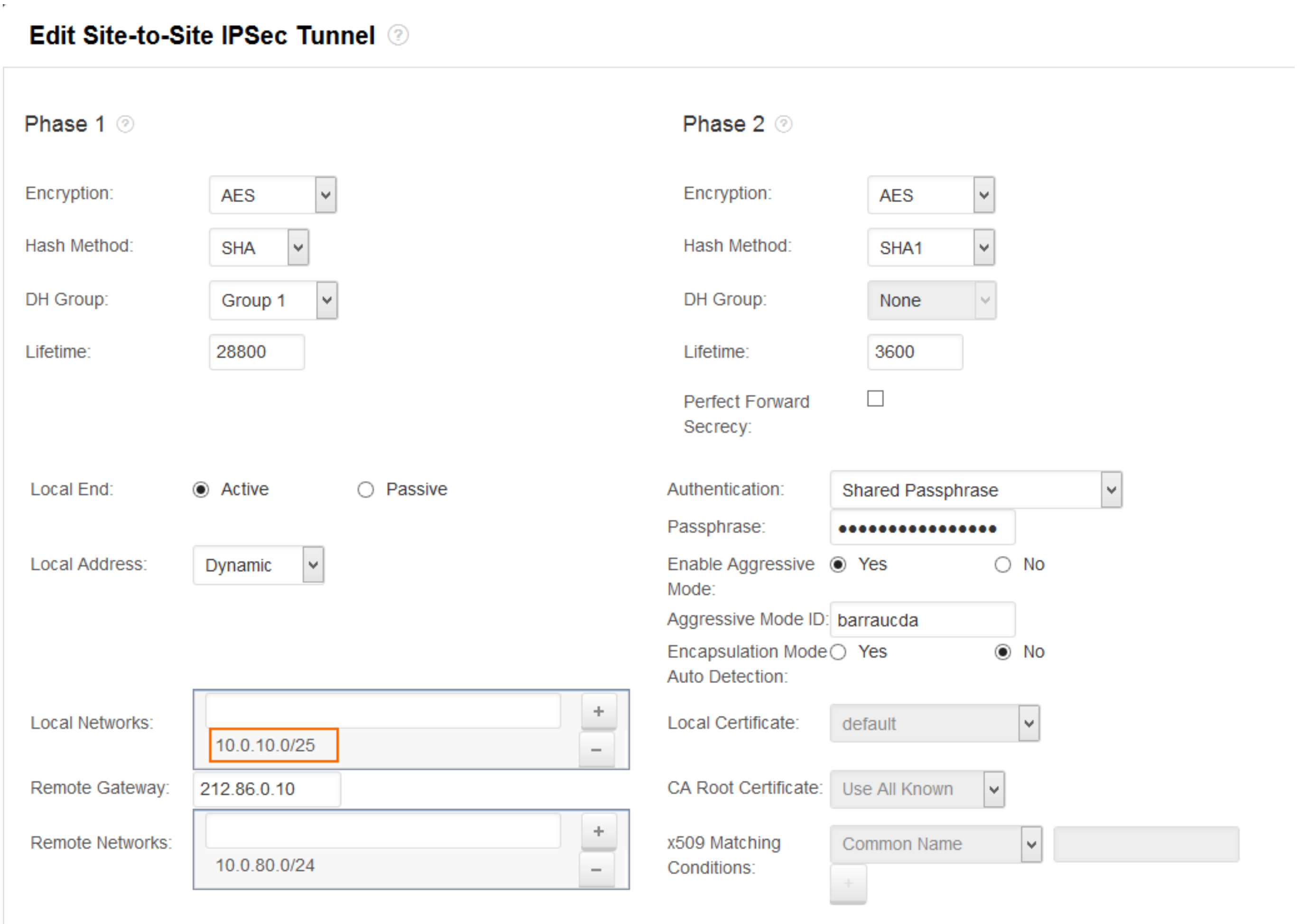
Before you begin

- Verify that at least one static interface configuration or the management IP address is part of the local published network you want to use for the site-to-site VPN tunnel.
- Go to **NETWORK > Routing** and verify that the VPN routes for the remote published networks will not break your existing routing configuration.

Step 1. Configure a site-to-site VPN tunnel

Configure a site-to-site VPN tunnel. At least one local published network must be directly attached to the firewall and configuration as a static network interface or as the management network.

For more information, see How to Configure a Site-to-Site VPN with IPsec or Example - Configuring a Site-to-Site IPsec VPN Tunnel.



Edit Site-to-Site IPSec Tunnel

Phase 1

Encryption: AES
Hash Method: SHA
DH Group: Group 1
Lifetime: 28800

Phase 2

Encryption: AES
Hash Method: SHA1
DH Group: None
Lifetime: 3600
Perfect Forward Secrecy: □

Local End: ● Active ○ Passive
Local Address: Dynamic
Local Networks: 10.0.10.0/25
Remote Gateway: 212.86.0.10
Remote Networks: 10.0.80.0/24

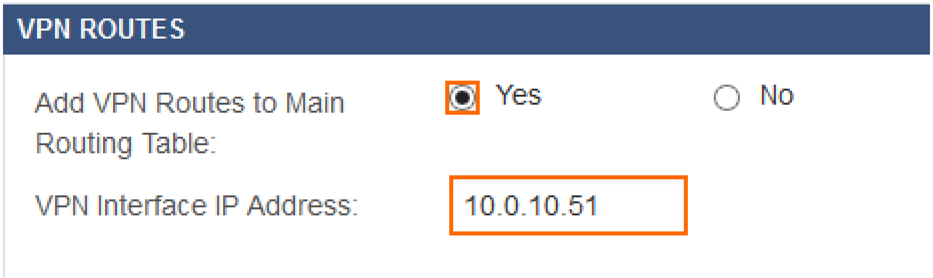
Authentication: Shared Passphrase
Passphrase: ●●●●●●●●●●●●●●●●
Enable Aggressive Mode: ● Yes ○ No
Aggressive Mode ID: barraucda
Encapsulation Mode Auto Detection: ○ Yes ● No
Local Certificate: default
CA Root Certificate: Use All Known
x509 Matching Conditions: Common Name

Step 2. Change VPN settings to add VPN routes to main routing table

In expert mode, switch from the default source-based routing to adding the VPN routed to the main routing table.

> Replacing VPN source-based routing without a proper migration plan may break your current setup and cause loss of connectivity. VPN routes are always added with the metric set to 10.

1. Go to **VPN > Settings**.
2. Append `&expert=1` to the URL to switch to expert mode.
3. In the **VPN Routes** section, set **Add VPN Routes to Main Routing Table** to **Yes**.
4. Enter the **VPN Interface IP address**. The IP address must meet the following criteria:
    - The IP address must be in one of the site-to-site VPN local published networks.
    - The IP address must be assigned to a static network interface as a primary or secondary IP address, or the management or secondary IP address in the management network.



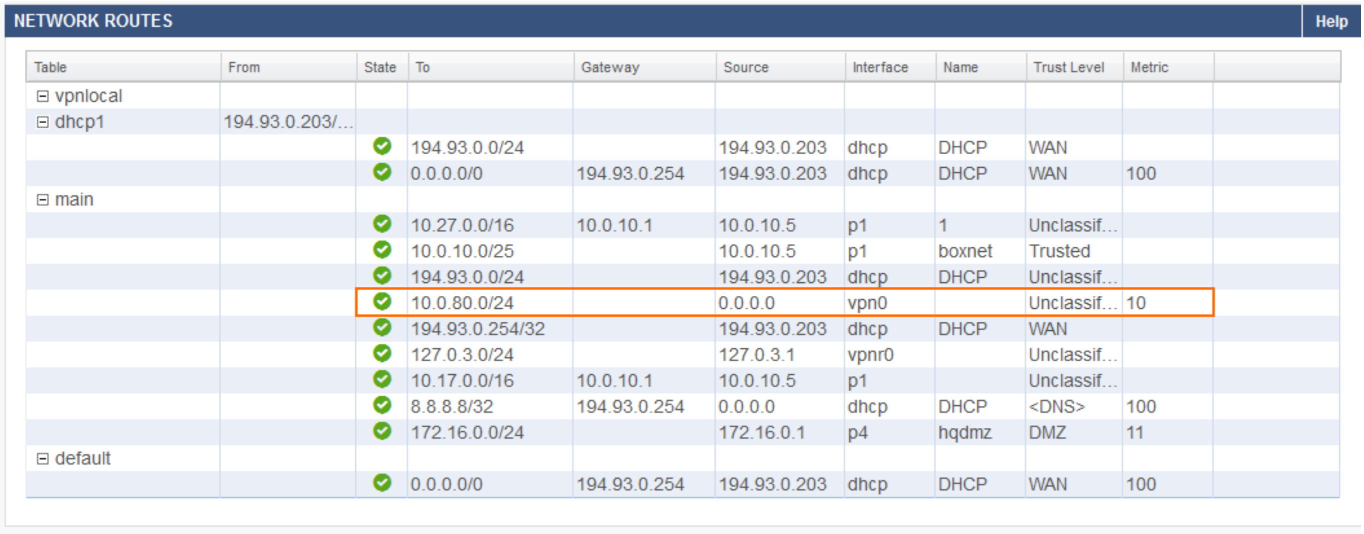
VPN ROUTES

Add VPN Routes to Main Routing Table: ● Yes ○ No

VPN Interface IP Address: 10.0.10.51

5. Click **Save**.

Go to **NETWORK > Routing** and verify that the VPN routes are now in the main routing table:



NETWORK ROUTES

Table	From	State	To	Gateway	Source	Interface	Name	Trust Level	Metric
⊟ vpnlocal									
⊟ dhcp1	194.93.0.203/...								
		✓	194.93.0.0/24		194.93.0.203	dhcp	DHCP	WAN	
		✓	0.0.0.0/0	194.93.0.254	194.93.0.203	dhcp	DHCP	WAN	100
⊟ main									
		✓	10.27.0.0/16	10.0.10.1	10.0.10.5	p1	1	Unclassif...	
		✓	10.0.10.0/25		10.0.10.5	p1	boxnet	Trusted	
		✓	194.93.0.0/24		194.93.0.203	dhcp	DHCP	Unclassif...	
		✓	10.0.80.0/24		0.0.0.0	vpn0		Unclassif...	10
		✓	194.93.0.254/32		194.93.0.203	dhcp	DHCP	WAN	
		✓	127.0.3.0/24		127.0.3.1	vpnr0		Unclassif...	
		✓	10.17.0.0/16	10.0.10.1	10.0.10.5	p1		Unclassif...	
		✓	8.8.8.8/32	194.93.0.254	0.0.0.0	dhcp	DHCP	<DNS>	100
		✓	172.16.0.0/24		172.16.0.1	p4	hqdmz	DMZ	11
⊟ default									
		✓	0.0.0.0/0	194.93.0.254	194.93.0.203	dhcp	DHCP	WAN	100

Step 3. Configure authentication server

Configure the external authentication server. Click **Test Connection** to verify that the firewall can connect to the remote authentication server through the site-to-site VPN.

For more information, see How to Configure an External Authentication Service

Figures