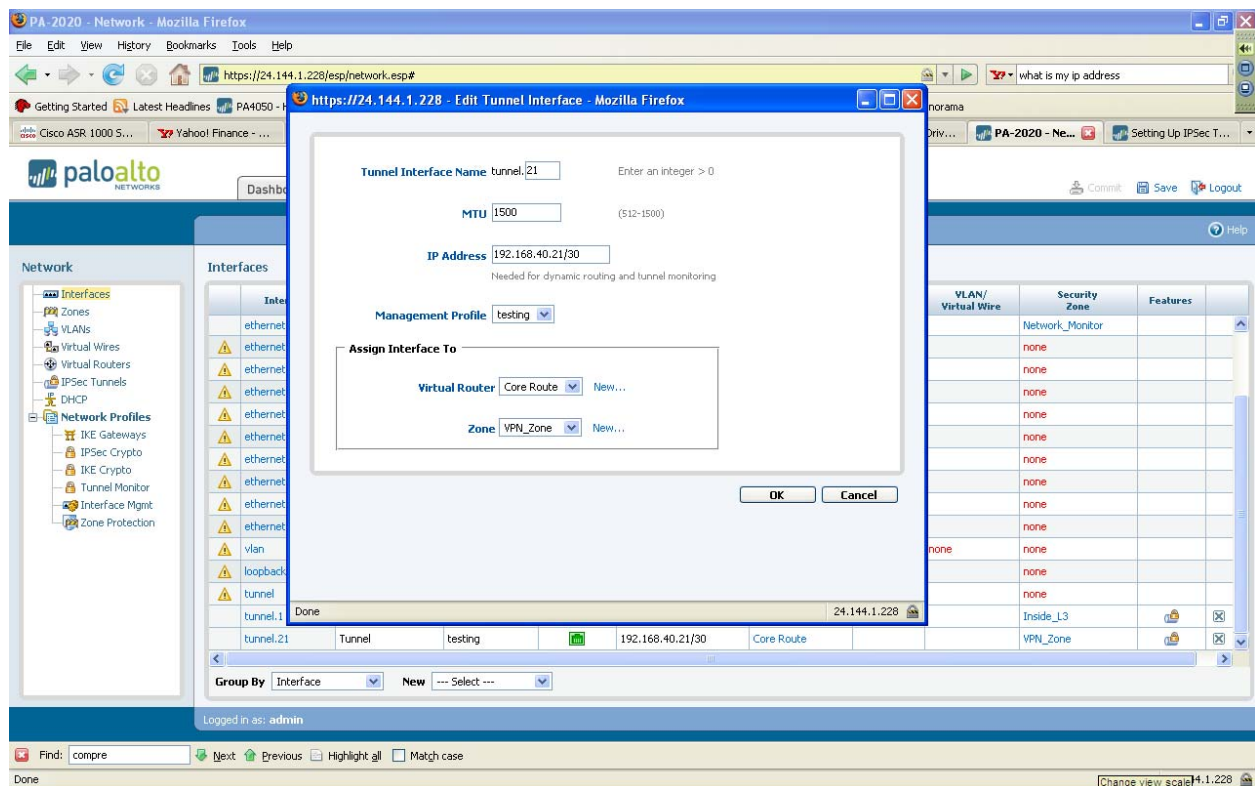


Palo Alto Networks & Watchguard - IPSec Settings

This document describes the common settings on the Palo Alto firewall and Watchguard firewall to create an IPSec tunnel between the two devices. The Palo Alto firewall is a 2020 model running PAN-OS 2.0.3 and the Watchguard is a Firebox X.

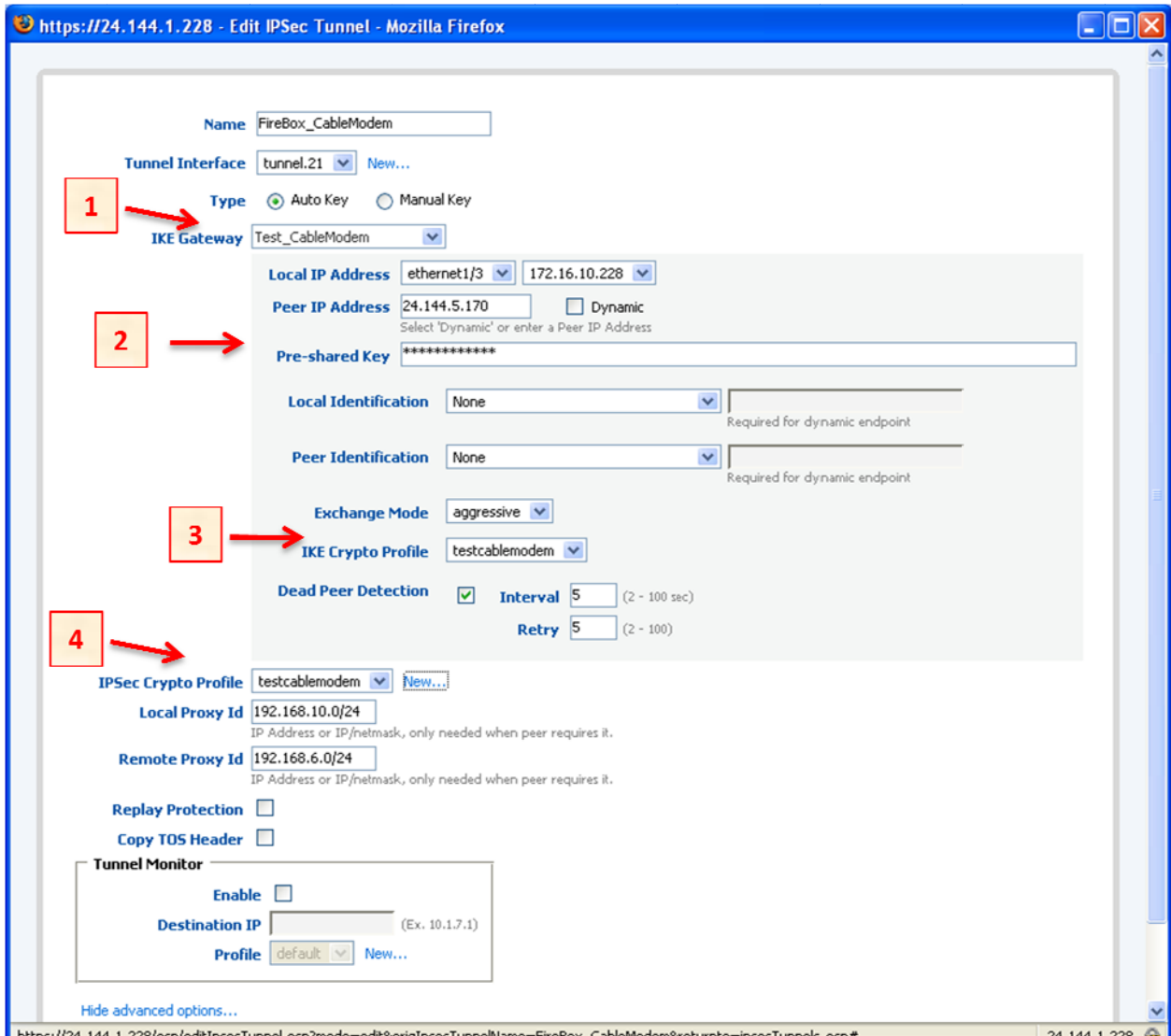
The 1st step is to create a tunnel interface on the Palo Alto. See Figure 1.

Figure 1: New IPSec tunnel on Palo Alto firewall. From GUI, under Network tab → at the bottom, select **New: Tunnel Interface**.



Then edit the IPSec tunnel and configure the settings for the Phase 1 and Phase 2 IPSec parameters. Below are screenshots from both the Palo Alto and the Watchguard.

Figure 2: Settings for the IPSec tunnel on Palo Alto firewall.



- 1) Define a unique IKE Gateway per tunnel.
- 2) The **Local IP address** should be the outbound interface (Internet facing interface) where the tunnel will originate. The **Peer IP Address** = Watchguard's public IP address for tunnel to connect.
Select a **Pre-shared Key** that matches the '**Shared Key**' on the Watchguard.
- 3) The **Exchange Mode** = **aggressive** because there was NAT'ing involved at the upstream. Should work with **Exchange Mode** = **main**.

See **IKE Crypto Profile** settings in **Figure 3** below.

- 4) Watchguard uses the Remote Network ID as the static route. If all traffic is to use the IPSec tunnel, then set 'Remote Network' on Watchguard to 0.0.0.0/0 which is equivalent to default route. On Palo Alto, Local Proxy ID=0.0.0.0/0 to denote default route.

See **IPSec Crypto Profile** settings in **Figure 4** below.

Palo Alto's **Local Proxy ID** ← (matches) → Watchguard's **Remote Network**

Palo Alto's **Remote Proxy ID** ← (matches) → Watchguard's **Local Network**

Figure 3: IKE Crypto Profile settings (Phase 1).

Name

DH Group			
Priority			
1	⌵	<input checked="" type="checkbox"/>	group2
2	⌵	<input type="checkbox"/>	group1
3	⌵	<input type="checkbox"/>	group5
4	⌵	<input type="checkbox"/>	group14

Encryption			
Priority			
1	⌵	<input checked="" type="checkbox"/>	3des
2	⌵	<input type="checkbox"/>	aes128
3	⌵	<input type="checkbox"/>	aes192
4	⌵	<input type="checkbox"/>	aes256

Hash Algorithm			
Priority			
1	⌵	<input checked="" type="checkbox"/>	sha1
2	⌵	<input type="checkbox"/>	md5

Lifetime
Minimum lifetime = 3 mins

Done 24.144.1.228

Figure 4: IPSec Crypto Profile settings (Phase 2). Note the DH group = no-pfs.

https://24.144.1.228 - Edit IPSec Crypto Profile - Mozilla Firefox

Name: testcablemodem

AH

DH Group: no-pfs

Lifetime: 24 Hours
Minimum lifetime = 3 mins

ESP

Authentication

Priority		
1	<input type="checkbox"/>	md5
2	<input checked="" type="checkbox"/>	sha1
3	<input type="checkbox"/>	none

Encryption

Priority		
1	<input checked="" type="checkbox"/>	3des
2	<input type="checkbox"/>	aes128
3	<input type="checkbox"/>	aes192
4	<input type="checkbox"/>	aes256
5	<input type="checkbox"/>	null

OK Cancel

Done 24.144.1.228

Make sure you have defined the routes to the remote IP network on the other side of the IPsec tunnel. In Figure 5, the static route for IP network 192.168.6.0/24 is reachable across tunnel.21.

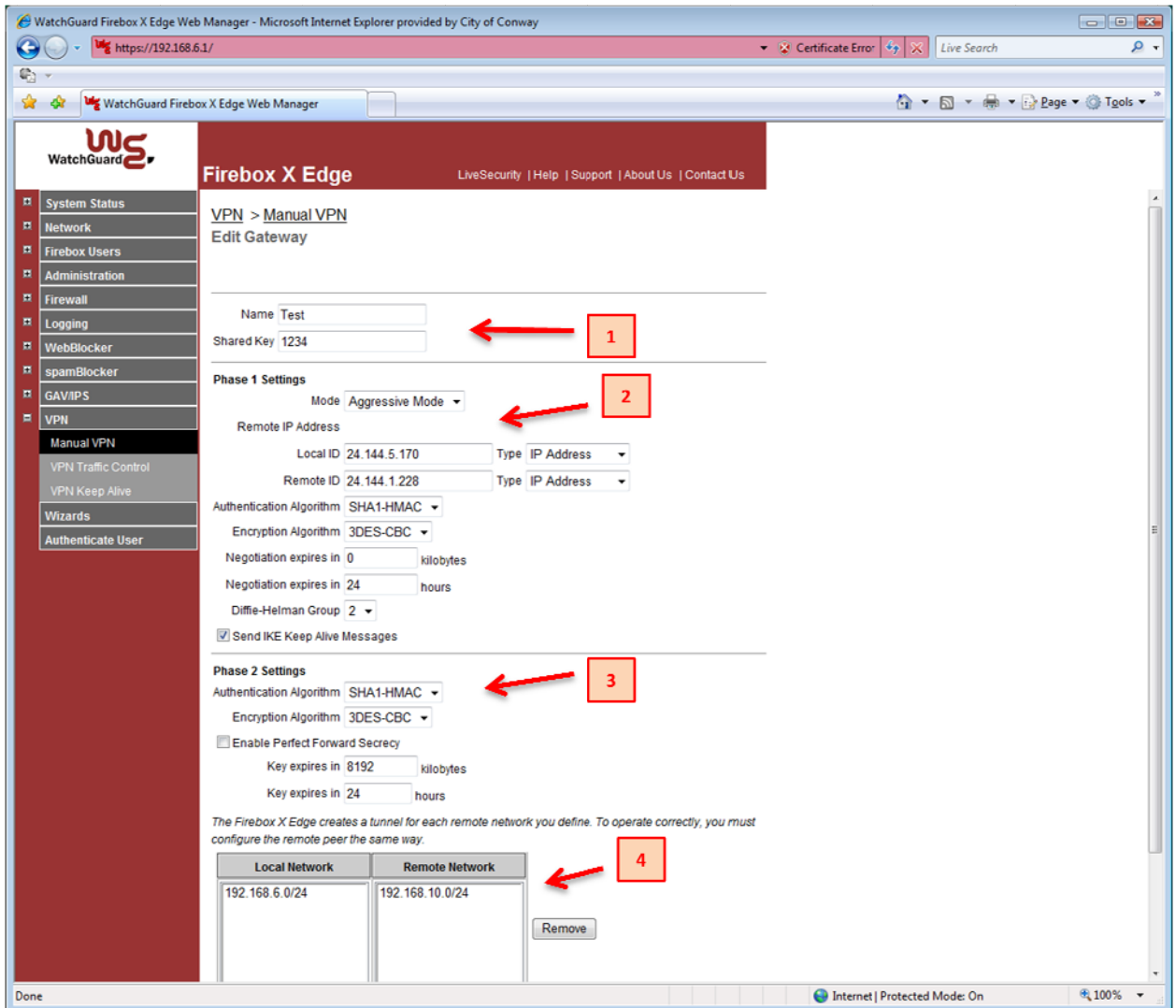
Figure 5: Static routes for networks across tunnels.

Virtual Router Core Route	
Conway IT	192.100.23.0/24

StaticRoutes	
Sanitation	192.168.12.0/24
City Attorney	192.168.21.0/24
cablemodem	192.168.6.0/24
McGee	192.168.22.0/24
Street_Dept	192.168.5.0/24
Pine_Street	192.168.20.0/24
Don_Owens	192.168.19.0/24

Below is the IPsec configuration on the Watchguard as depicted in Figure 6.

Figure 6: Manual IPsec VPN settings.



- 1) Define the **Shared Key** to match the '**Pre-shared Key**' on Palo Alto.
- 2) Configure the Phase 1 Settings to match Palo Alto.
- 3) Configure the Phase 2 Settings to match Palo Alto. Note there is no Diffie-Helman group setting, which matches setting '**DH group = no-pfs**' on Palo Alto.
- 4) **Local Network 192.168.6.0/24** matches Palo Alto's **Remote Proxy ID**. Remote Network 192.168.10.0/24 matches Palo Alto's **Local Proxy ID**. This value can be set 0.0.0.0/0 as the default route and all traffic will use the IPsec tunnel.