**Eve-ng project**

**1-add Paloalto Eve-ng**

**Used image PA-VM-KVM-10.0.2.qcow2**

**Download link**

<https://drive.google.com/file/d/1oW2Jn7twgaC18rTNHDt4tONmEv3SOmaE/view?usp=sharing>

**2-add Fortinet Eve-ng**

**Used image FGT\_VM64\_KVM-v6-build1066-FORTINET.out.kvm.qcow2**

**Download link**

<https://drive.google.com/file/d/18SnS8OT0ihr4MkFHjzG-Uq18aG6mNqrj/view?usp=sharing>

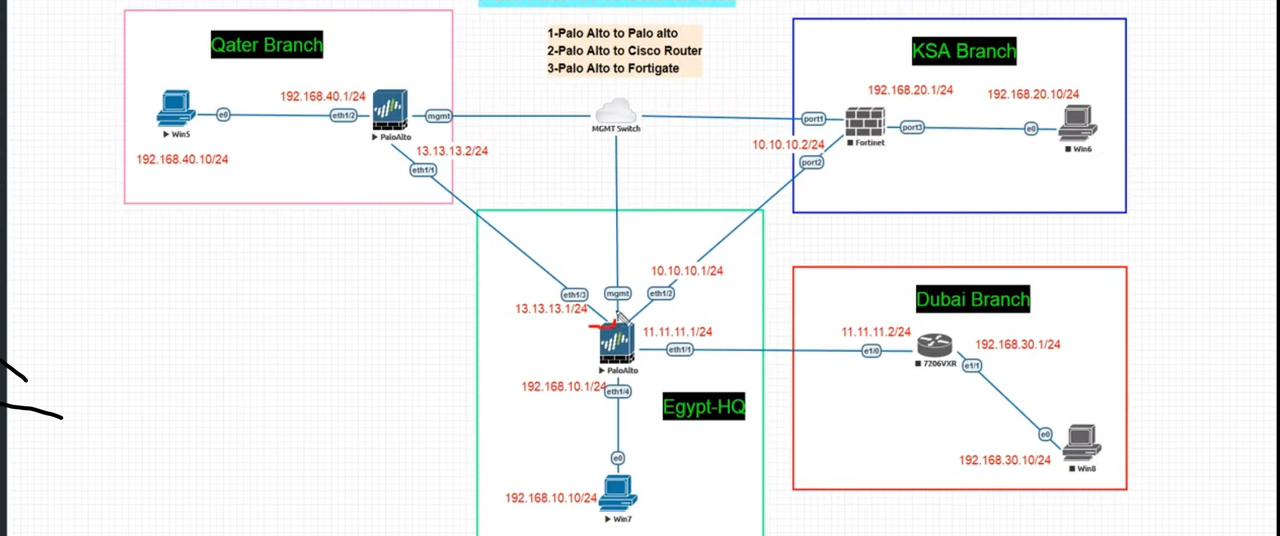
**3-CISCO router config**

**Used image c7200-adventerprisek9-mz.152-4.S7.bin**

**Download link**

<https://drive.google.com/file/d/1YlCPoMQ49JmAx8pqpsLThvfj8k9t_9a8/view?usp=sharing>

<https://drive.google.com/file/d/1ualdxmzCgTrpnyOI7c2-OCWOGXwf3XWA/view?usp=sharing>

****

**Part1 tunnel lab (PAloAlto & Fortigate & Cisco Router) EVE-ng**

<https://www.youtube.com/watch?v=StvZU8fG75Q>

**part2 tunnel lab (PAloAlto & Fortigate & Cisco Router) EVE-ng**

<https://www.youtube.com/watch?v=zuQvCnbgHvQ>

**Add windows 7**

# IPSec VPN between two Palo Alto Network Firewalls

# 

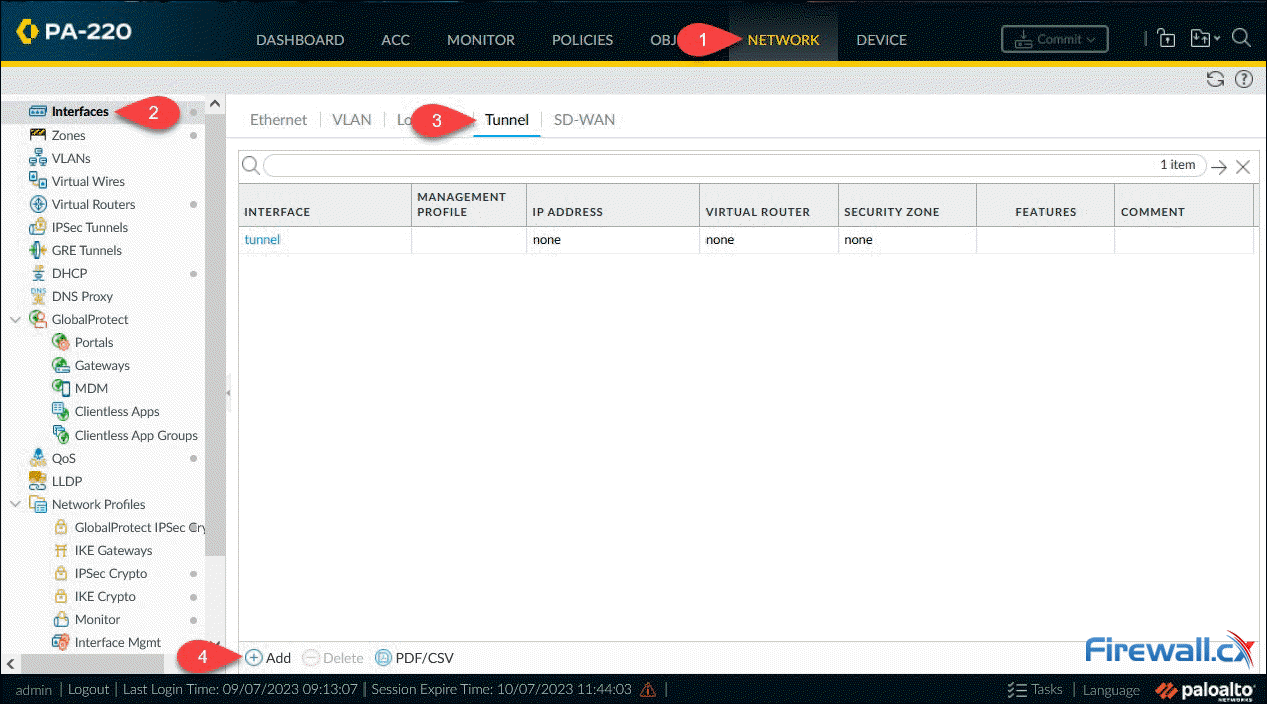
**New PA -to – PA**

**Palo Alto Firewall Setup**

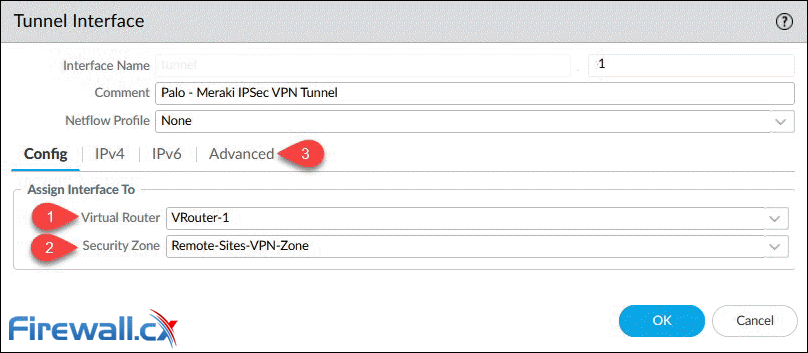
* [Step 1 – Create a Tunnel Interface](https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-meraki-mx-ipsec-vpn-setup.html#create-tunnel-interface)
* [Step 2 – Configure IKE Crypto Profile (IKEv1 - Phase 1)](https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-meraki-mx-ipsec-vpn-setup.html#configure-ike-crypto-profile)
* [Step 3 – Configure IKE Gateway](https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-meraki-mx-ipsec-vpn-setup.html#configure-ike-gateway)
* [Step 4 – Configure IPSec Crypto Profile – (IKE Phase 2)](https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-meraki-mx-ipsec-vpn-setup.html#configure-ipsec-crypto-profile)
* [Step 5 – Create IPSec Tunnel](https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-meraki-mx-ipsec-vpn-setup.html#create-ipsec-tunnel)
* [Step 6 – Configure VPN Routing (Remote Site Traffic)](https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-meraki-mx-ipsec-vpn-setup.html#configure-vpn-routing)
* [Step 7 – Configure Security Policies (IKE/IPSec & Remote Site Traffic)](https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-meraki-mx-ipsec-vpn-setup.html#configure-security-policies)

## **Step 1 – Create A Tunnel Interface**

Under **Network**, select **Interfaces** then the **Tunnel** menu option. The firewall will now show all configured tunnel interfaces. The interface ‘**tunnel’**, as shown below, by default exists on all firewalls:

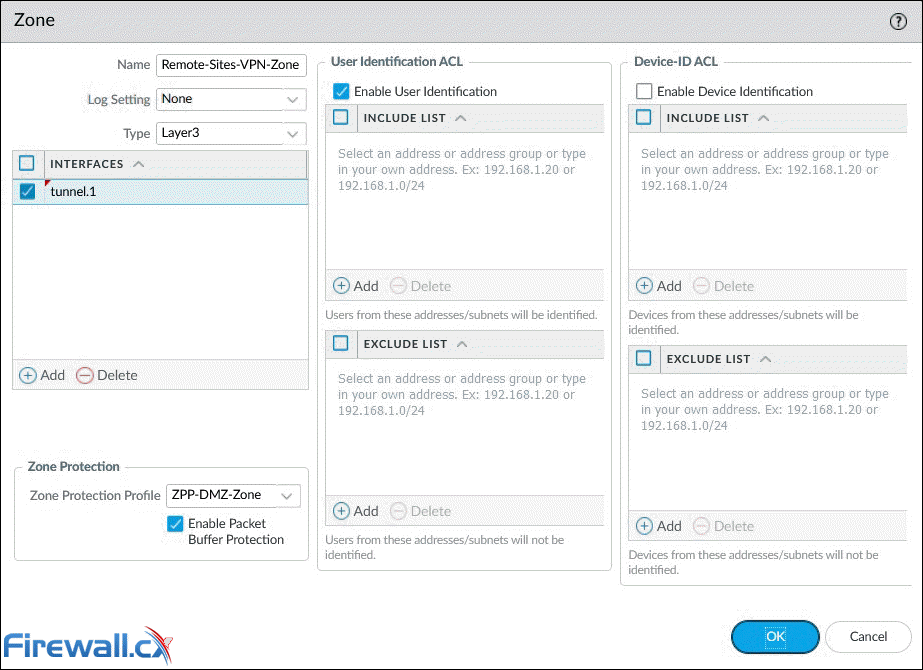


Finally, **Click** on **Add** to create and configure the new tunnel interface. The **Virtual Router** and **Security Zone** are the bare minimum that need to be configured:

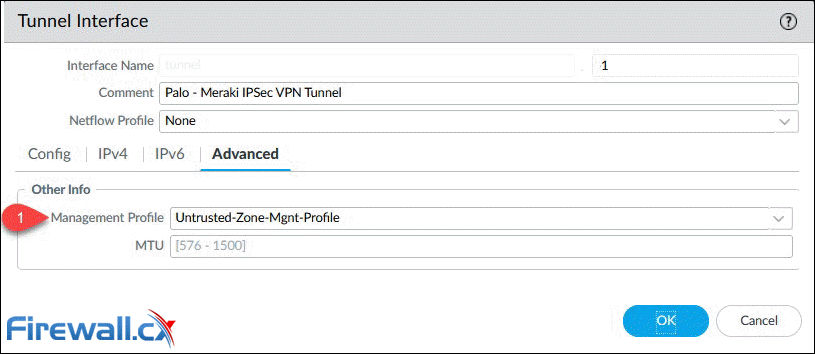


Note: Configuring an IP address (IPv4) on the tunnel interface is required only if you intend to run [dynamic routing protocols](https://www.firewall.cx/networking/routing-protocols.html) over the tunnel interface.

If there is no suitable **Security Zone** available, leave the field empty, then proceed to **create** a **new Zone**. This can then be attached to the previously created **Tunnel Interface**:

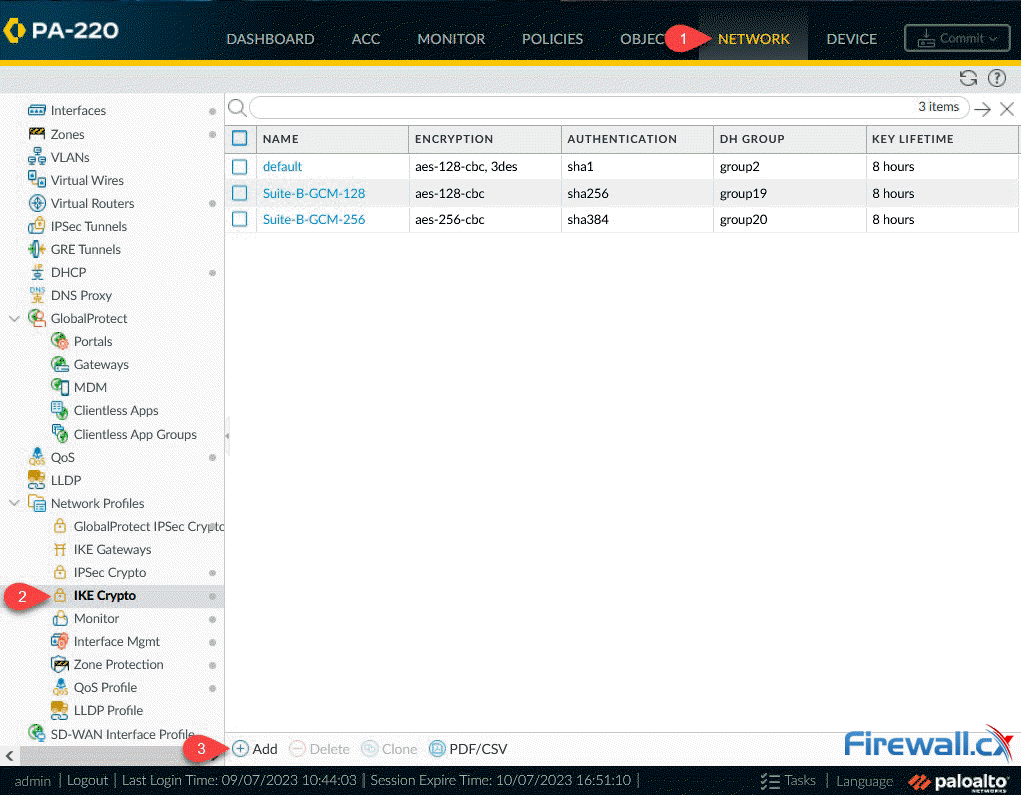


Optionally, **select** a preconfigured **Management Profile** under the **Advanced** tab:

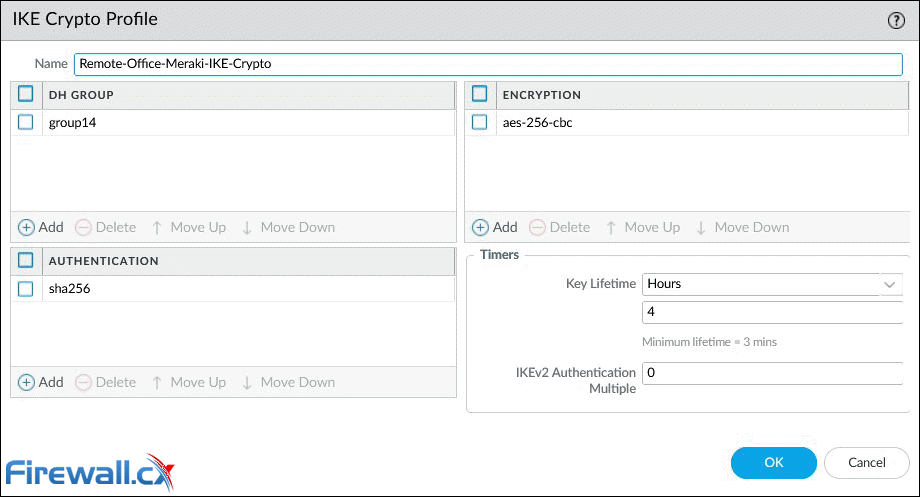


## **Step 2 – Configure IKE Crypto Profile (IKEv1 - Phase 1)**

To configure the **Crypto IKE profile** (IKEv1 – Phase 1), go to **Network** and select **IKE Crypto** under **Network Profiles**. Finally **click** on the **Add** button:



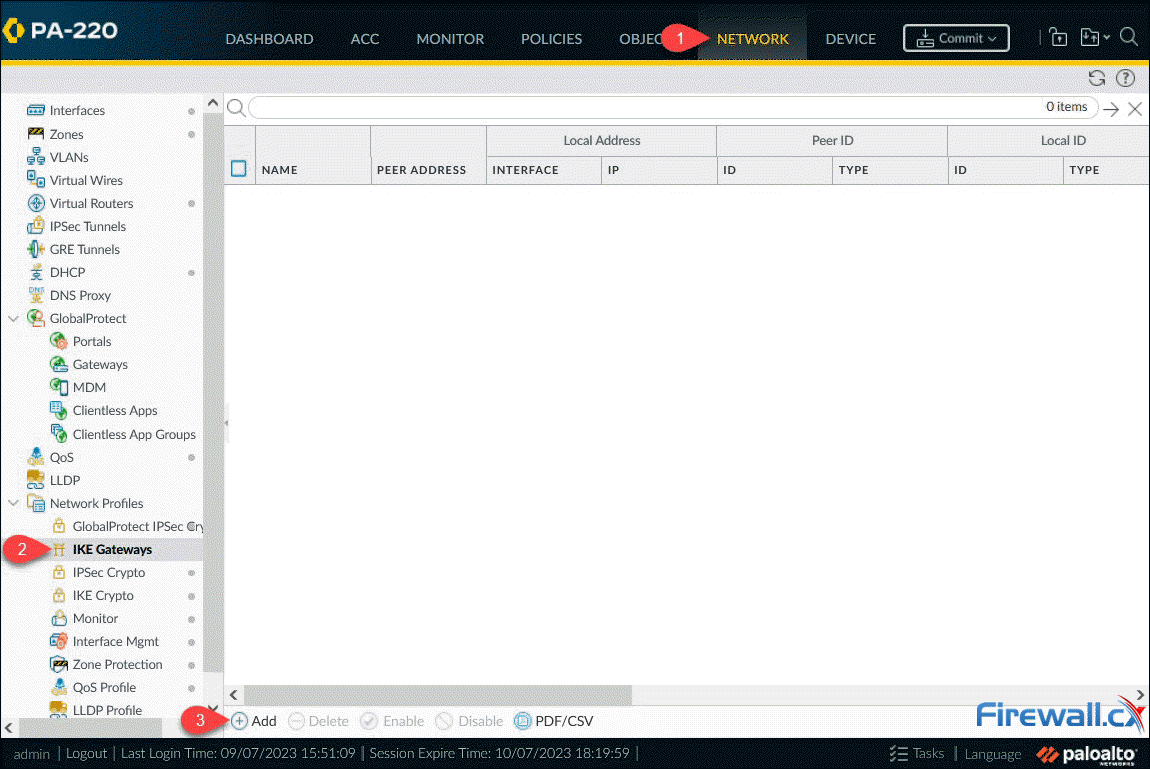
We can now define the **IKE Crypto profile** parameters. In the popup window, enter the name for the **IKE profile** and select a compatible **DH Group**, **Authentication** and **Encryption method**. Our setup shows the most secure options (**DH Group**, **Authentication**, **Encryption**) currently supported by our Meraki MX appliance:



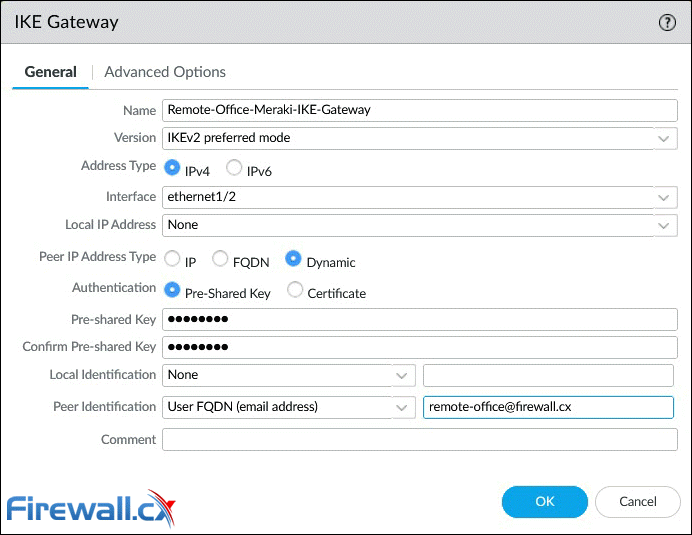
* **DH Group**: group14 (2048-bit)
* **Authentication**: sha256
* **Encryption**: aes-256-cbc
* **Key Lifetime**: 4 hours (8 hours is the default value)

## **Step 3 – Configure IKE Gateway**

Next step is to configure the IKE Gateway. Select **Network**, **Network Profiles** and finally **IKE Gateways**. When ready, **click** on the **Add** button:



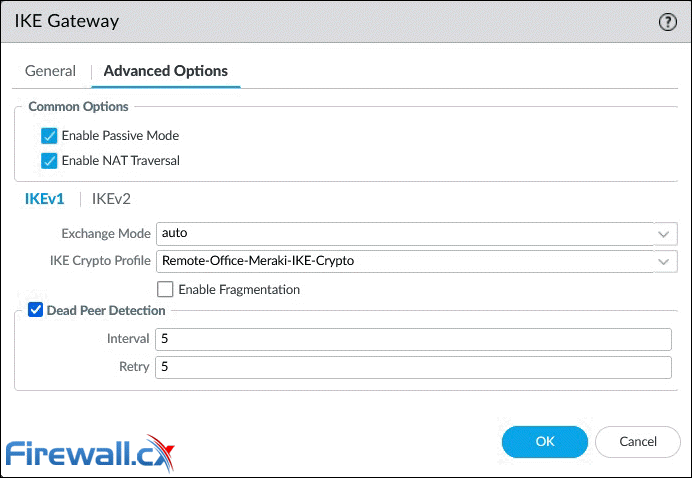
The **IKE Gateway** window contains a number of different parameters that need to be populated:



Below are a few options that require special consideration:

* **Version**: The IKE version must be identical with the remote peer. Supported options are **IKEv1**, **IKEv2** and **IKEv2 preferred mode**. With **IKEv2 preferred mode**, the firewall will attempt to negotiate **IKEv2** but will fail back to **IKEv1** if it’s not supported.
* **Interface**: This is the public facing interface. Select a **Physical** or **Aggregate interface** (AE).
* **Local IP Address**: This is the IP address for the interface where the tunnel terminates. Option **None** can be used if the Palo Alto firewall has a dynamic public IP (like our case) or only a single static IP. Alternatively you can specify the public IP to be used.
* **Peer IP Address Type**: **Static IP** is the most secure, followed by **FQDN** and finally **Dynamic**. With the **Dynamic** option, the peer always initiates the IKE gateway negotiation. If the peer is subject to dynamic IP address changes, it’s recommended to use **FQDN (hostname)** or **FQDN (email address)**for the**Peer Identification** (see below).
* **Authentication**: The type of authentication that will occur with the peer gateway.
* **Local Identification**: Format and identification of the local VPN gateway used with the pre-shared key for both **IKEv1 Phase 1 SA** and **IKEv2 SA**. If none set, the gateway will use the **local public IP address** as the **Local Identification** value.
* **Peer Identification**: Format and identification of the peer VPN gateway used with the pre-shared key for both **IKEv1 Phase 1 SA** and **IKEv2 SA**. If none set, the gateway will use the **public IP address** of the peer. In our setup, we configured the **User FQDN (email address)** option. This will also need to be set as the **Local ID** at the **remote VPN gateway** (Meraki MX).

Moving to the **Advanced Options** tab, we’ll find additional parameters that need to be configured:



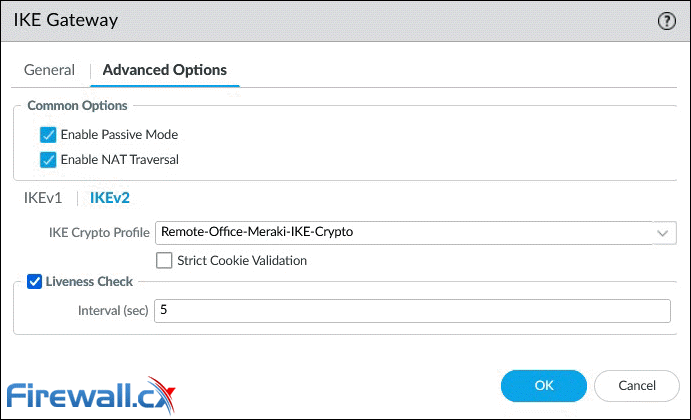
Below are a few options that require special consideration:

* **Enable Passive Mode**: Forces the firewall to only respond to IKE connections and never initiate them.
* **Enable NAT Traversal**: [NAT Traversal](https://www.firewall.cx/networking/network-protocols/ipsec-modes.html) should be enabled when there is [Network Address Translation (NAT)](https://www.firewall.cx/networking/network-address-translation.html) configured on a device between the IPSec VPN terminating points. For example, when the remote peer (Meraki MX) is behind a router/firewall that has NAT enabled. With this option **enabled**, **UDP encapsulation** is used on **IKE** and **UDP** protocols, so they can pass through NAT devices.

**IKEv1 Tab**

* **Exchange Mode**: Enables the device to accept **main** and **aggressive** mode negotiation requests. This setting must be identical for both VPN gateways. **Auto mode** accepts both negotiation requests.
* **IKE Crypto Profile**: Select a profile. Our example uses the **IKE Crypto profile** created in the previous step.
* **Enable Fragmentation**: Allows the local gateway to receive fragmented IKE packets. Maximum fragmented packet size is 576 bytes.
* **Dead Peer Detection**: Identify inactive or unavailable IKE peers. Useful to help restore access to remote resources that are lost when a peer is unavailable.

Below are the options available when **IKEv2** is enabled under **IKE Gateway: General > Version** parameter:

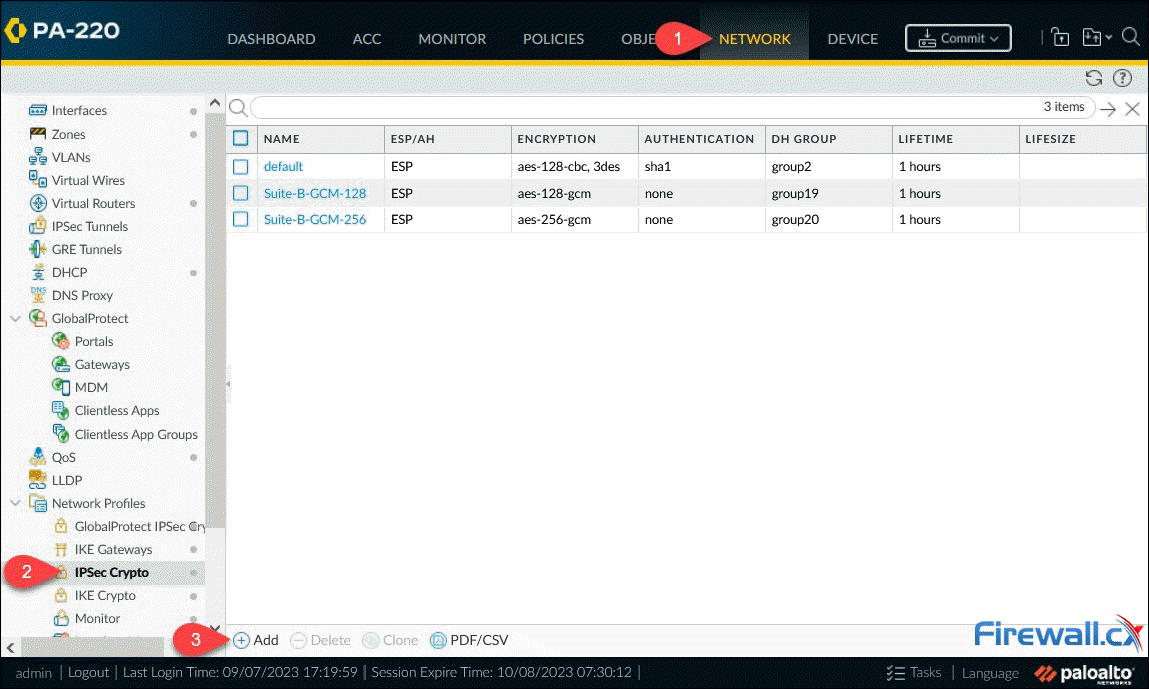


**IKEv2 Tab**

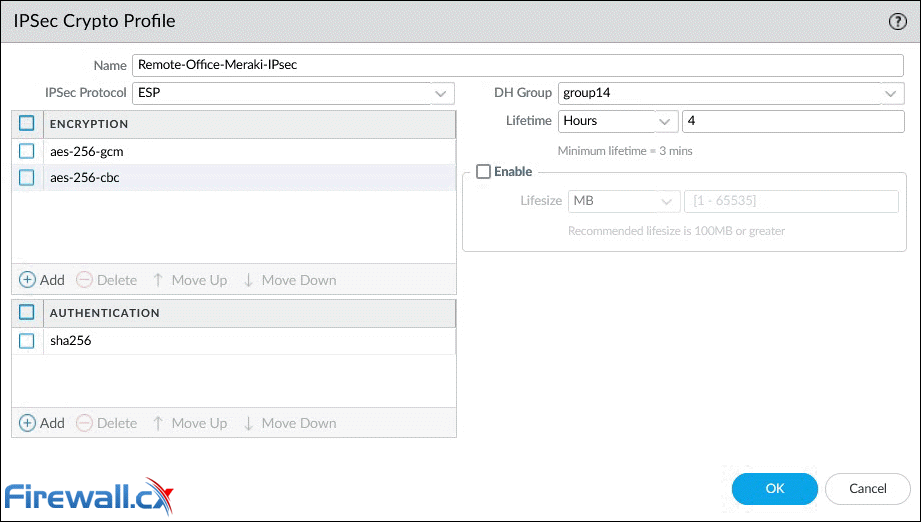
* **IKE Crypto Profile**: Select a profile. Our example uses the **IKE Crypto profile** created in the previous step.
* **Strict Cookie Validation**: When enabled, IKEv2 cookie validation is always enforced. The initiator must send an **IKE\_SA\_INIT** containing a cookie.
* **Liveness Check**: All IKEv2 packets are used as liveness checks. When this option is checked, the firewall will send empty information packets after the peer has been idle for the specified number of seconds (2 – 100).

## **Step 4 – Configure IPSec Crypto Profile - IKE Phase 2**

Next step is to configure the **IPSec Crypto profile**. This is used to specify the protocols and algorithms for identification, authentication and encryption based on IPSec SA negotiation (IKEv1 Phase 2). Navigate to **Network > Network Profiles** and then **IPSec Crypto**. When ready, **click** on the **Add** button:



After clicking **Add**, the **IPSec Crypto Profile** window will appear, allowing us to configure the profile. The parameters must match with the remote peer for the **IKE Phase-2** negotiation to be successful:

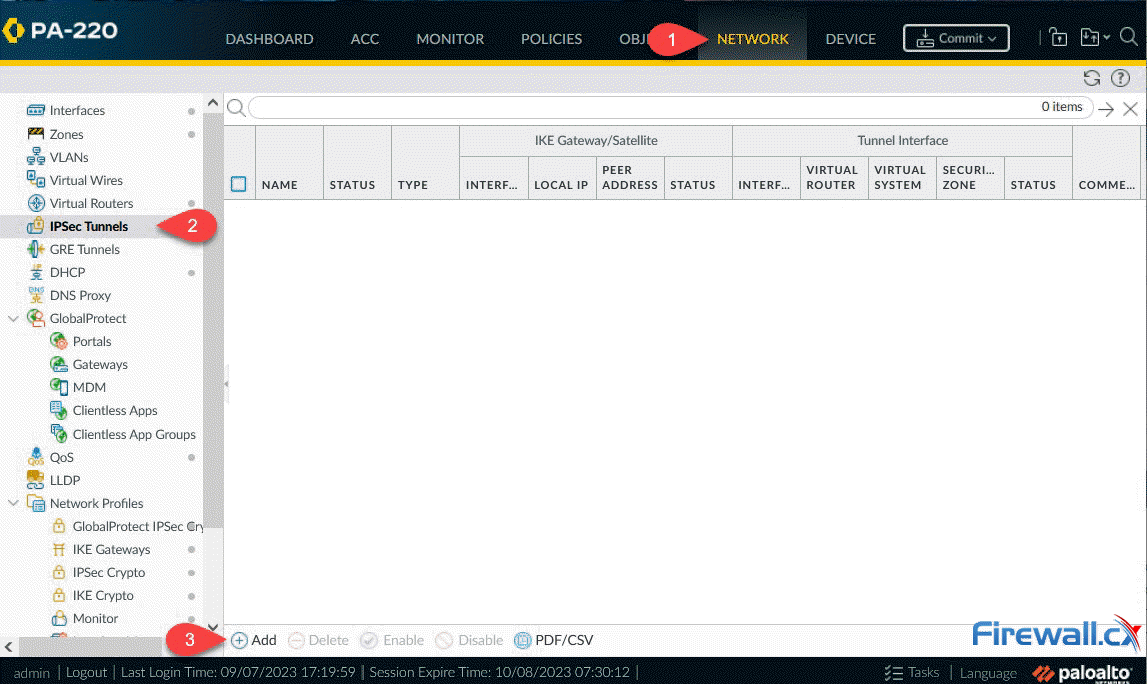


Below are a few options that require special consideration:

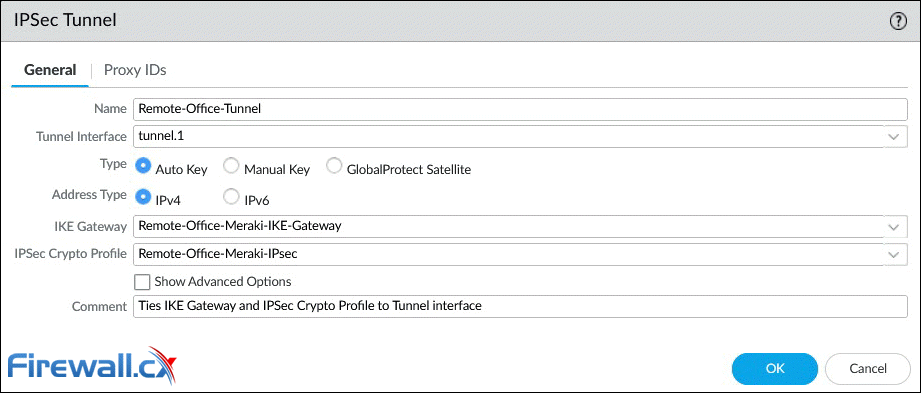
* **IPSec Protocol**: Used to secure data traversing the VPN tunnel. [ESP protocol](https://www.firewall.cx/networking/network-protocols/ip-security-protocol.html) is recommended as it provides connection confidentiality (encryption) and authentication (AH).
* **Encryption**: Only available when ESP is selected above. It’s recommended to use AES encryption as DES/3DES are weak and vulnerable algorithms.
* **Authentication**: **SHA256** or stronger is recommended as **MD5** and **SHA1** are not consider secure.
* **DH Group**: Diffie-Hellman (DH) **group 14** (2048-bit) for **IKE**. Higher group numbers provide higher security.
* **Lifesize**: Optionally, select the amount of data that the key can used for before renewing.

## **Step 5 – Create IPSec Tunnel**

This is the final step required to configure the IPSec tunnel between the two endpoints. To being, navigate to **Network > IPSec Tunnels**, then **click** on the **Add** button:



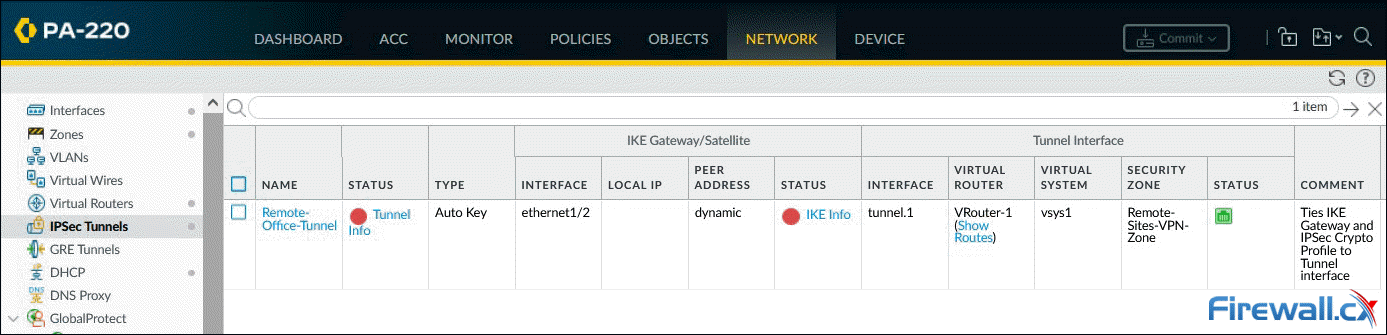
Next, we can configure the **IPSec Tunnel** parameters as shown below:



Below are a few options that require special consideration:

* **Tunnel Interface**: **Click** and select from the dropdown list interface **tunnel.1**.
* **Type**: Contains a number of additional complex settings around IKE, IPSec, Replay protection and more. Leave this to **Auto Key**.
* **Address Type**: Select the IP address type **IPv4** (default).
* **IKE Gateway**: Select from the dropdown list, the **IKE Gateway profile** previously configured.
* **IPSec Crypto Profile**: Select from the dropdown list the **IPSec profile** previously configured.
* **Tunnel Monitor (Advanced Options)**: An optional parameter, not used in our setup, that allows the monitoring of tunnel failures and automatic failover to another interface. Requires IP address assigned to the tunnel interface.

When ready, **click** on **OK** to save your settings. The dashboard will now show the configured **IPSec Tunnel**:



The Red dot **IKE Info** status indicates that **IKE Phase-1 SA** is not available or has expired. The Red dot **Tunnel info** status indicates that **IPSec Phase-2 SA** is not available or has expired.

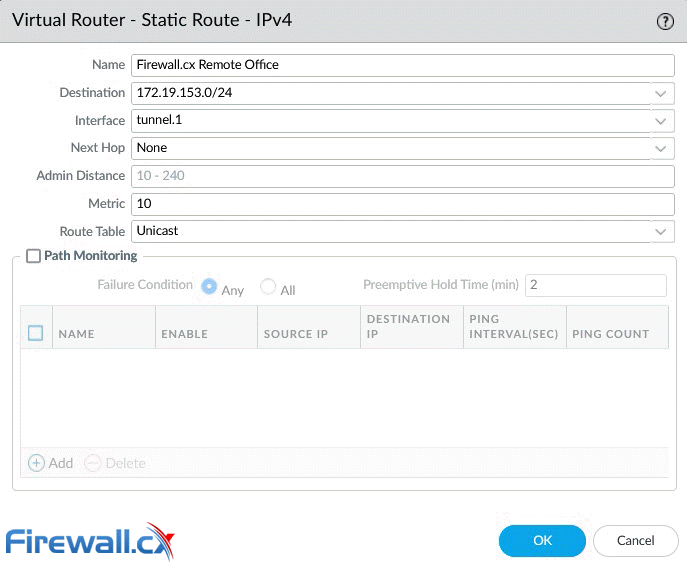
As soon as the **peer VPN gateway (Meraki MX)** is configured and the VPN is established, both status indicators will turn green.

The IPSec tunnel configuration is complete at this point, however we still need to configure the VPN traffic routing and security policies to allow VPN traffic through.

## **Step 6 – Configure VPN Routing (Remote Site Traffic)**

This step involves configuring the Palo Alto firewall to route interesting traffic (VPN traffic) through the IPSec tunnel.

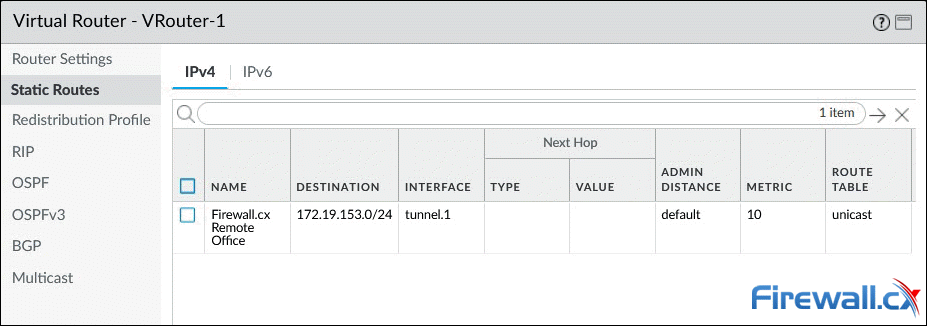
Under **Network > Virtual Router**, **click** on **Static Routes** to add a new route to the remote network(s):



Be sure to enter the correct **remote IP network** (172.19.153.0/24) and **tunnel interface** (tunnel.1). **Click** OK when done.

Note: While the remote network is a [Class C network](https://www.firewall.cx/networking/network-protocols/ip-protocol/protocols-ip-network-id.html) split into smaller VLAN networks ([subnetted](https://www.firewall.cx/networking/network-protocols/subnetting.html)), at this point we [summarize](https://www.firewall.cx/networking/network-protocols/supernetting-and-cidr/supernetting.html) it with a single entry (172.19.153.0/24).

Below is the configured static entry:

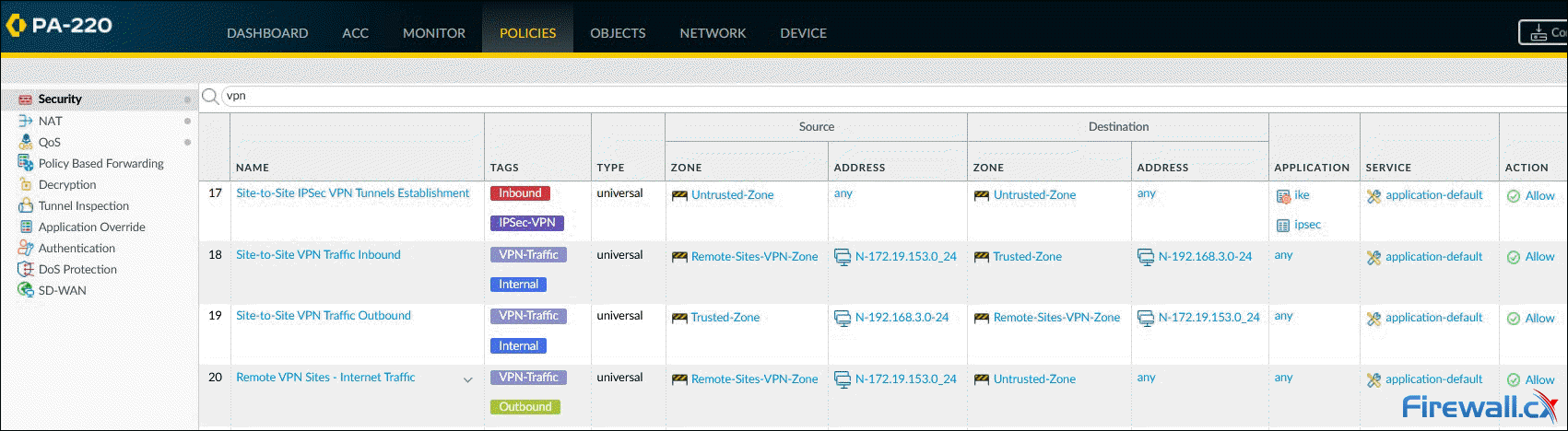


## **Step 7 – Configure Security Policies (IKE/IPSec & Remote Site Traffic)**

The final step involves configuring the necessary security policies to:

* Allow **IKE negotiation** and **IPSec tunnel** to be established. See policy 17 below.
* Allow the remote office (172.19.153.0/24) access local resources (192.168.3.0/24) and vice versa. See policies 18-19 below.
* Allow the remote office access the internet (**Full Tunnel mode**). Note that a NAT policy, for the remote network, will also be required for outbound internet traffic. See policy 20 below.

Pay extra attention to the **Source** and **Destination** Zone in **policy 17**. The VPN tunnel **initiates** and **terminates** on the firewall's **public (untrusted) interface**. Once the tunnel is established, site-to-site user traffic (Policies 18 & 19) flows between zones **Remote-Sites-VPN-Zone** (Tunnel.1) and **Trusted-Zone** (internal interface).



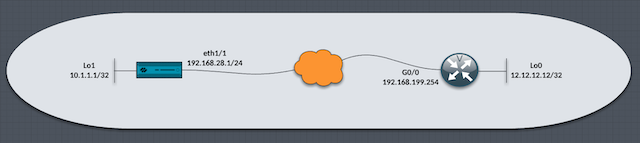
The remote site's internet traffic will flow between zones **Remote-Sites-VPN-Zone** (Tunnel.1) and **Untrusted-Zone** (public interface).

At this point we've completed the Palo Alto firewall setup and can now continue configuring the Meraki MX security appliance.

# IPSec VPN between a Palo Alto Networks Firewall and a Cisco Router

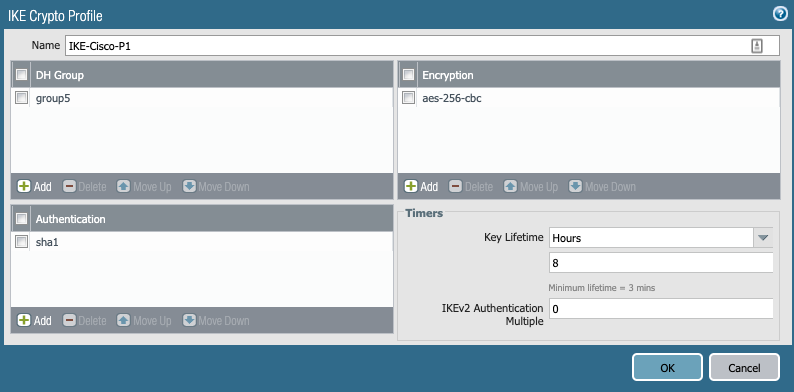
# 

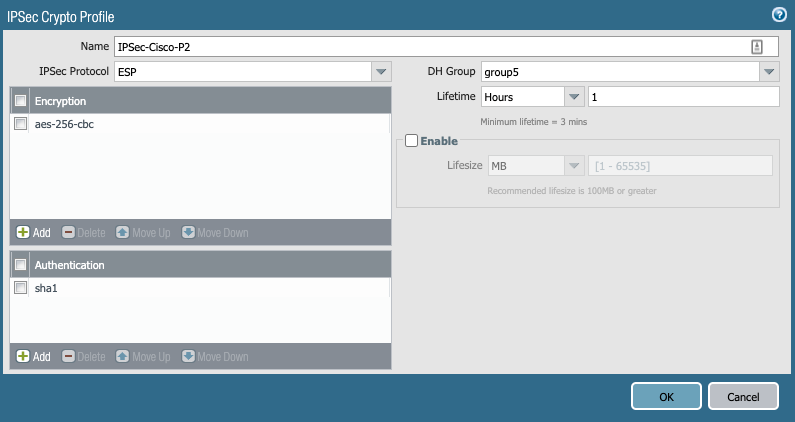
<https://www.mbtechtalker.com/palo-alto/>



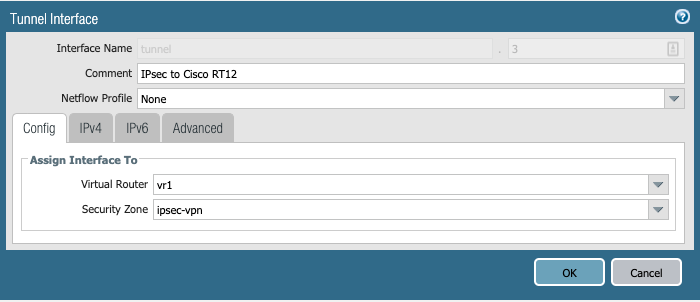
## Firewall Configuration

1. **IKE (Phase1) and IPsec Crypto(Phase2) Profiles.**I chose aes256, sha1, PFS group 5 and a lifetime of 8hrs.

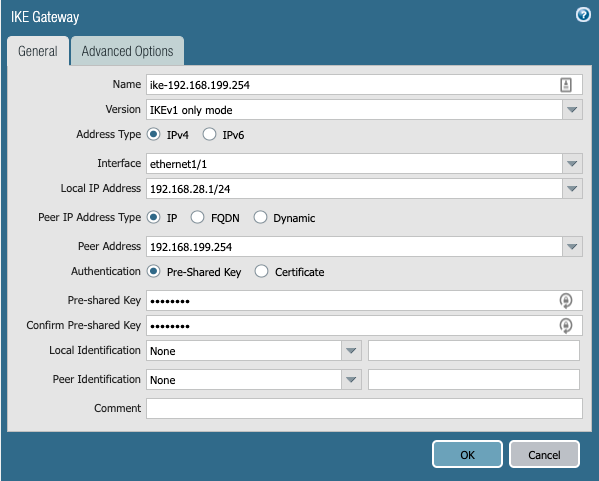


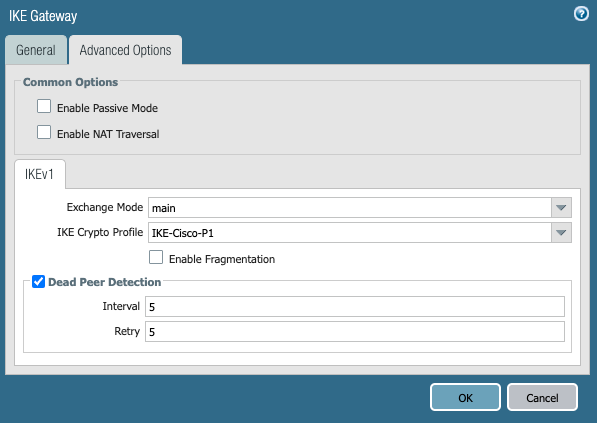


2.**Tunnel interface.**I assigned it to the vr1 virtual router and the IPSec-VPN security zone. There is no need for me to configure an IP address as I'm not using dynamic routing protocols in this lab.

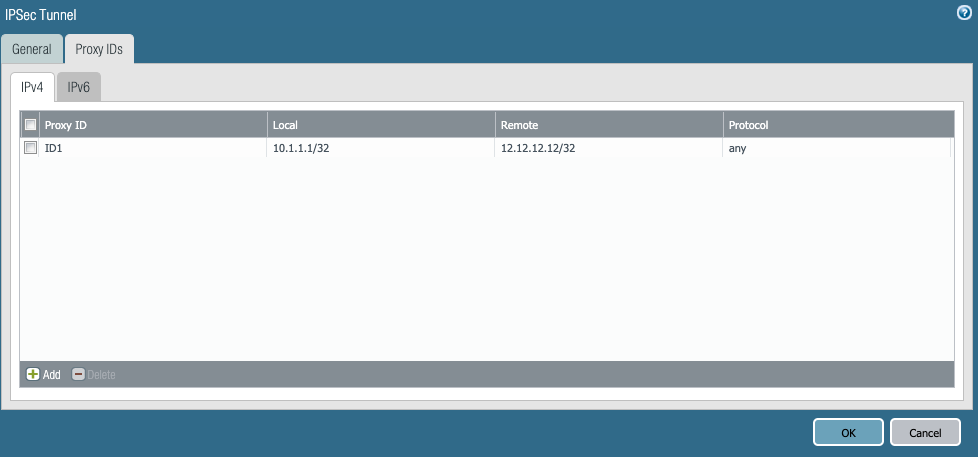


3. **IKE Gateway** configuration, I configured the egress interface of the firewall, including the local IP address, the remote peer IP address and I chose to use a pre-shared key (password) as the authentication method. The password here needs to be the same on the remote peer device. In the advanced options tab and under the IKEv1 section, I selected main as the exchange mode and chose the IKE Crypto Profile (Phase1) I defined earlier.

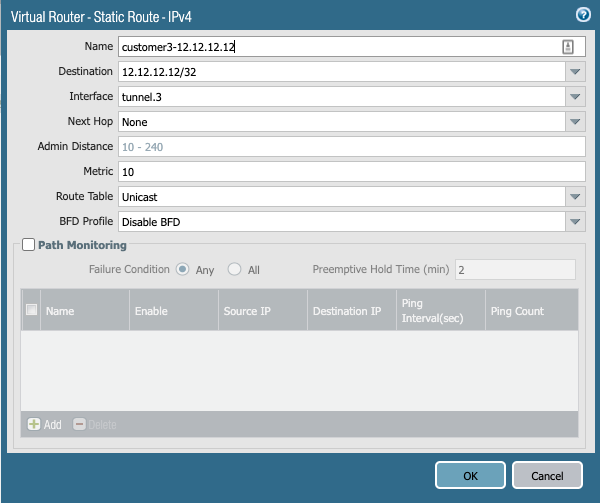




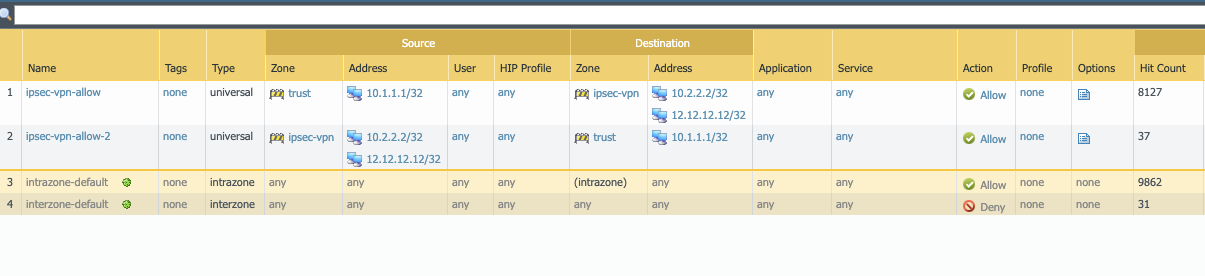
4.**IPSec tunnel.** Now it's time to bring all this configuration together in the IPSec section of the firewall, I selected the tunnel.3 interface, the IKE gateway (remote peer) and the IPSec Crypto profile (Phase2). I'm aware that Palo Alto Networks Firewalls only support route-based VPNs and the fact I will be configuring a Policy-Based VPN on the remote Cisco router, I will need to use Proxy ids. Devices that support policy-based VPN use specific security rules and policies or access lists (source addresses, destination addresses and ports) for permitting interesting traffic through an IPSec tunnel. These rules are referenced during quick mode/IKE phase 2 negotiation and are exchanged as proxy IDs in the first or the second message of the process. So that being said, I went ahead and configured a Proxy ID specifying the local and remote networks, which in my case is the two /32 IP addresses.



5 . **Static route**needs to be configured in the virtual router to route the correct traffic through the corresponding tunnel. The destination is 12.12.12.12/32 which needs to be sent to tunnel3 with the next hop of none.



6. **Security Policies** then need to be configured to allow traffic in both directions. I have two VPN tunnels configured on the firewall, that's why I have an additional address object. For this lab, traffic should allow bi-directional traffic between 10.1.1.1/32 and 12.12.12.12/32.



## Cisco Router Configuration

1.The **ISAKMP (Phase1) Policy** and the authentication key needs to be configured to peer with the remote Palo Alto Firewall. Below is for policy 1 which uses AES 256 for encryption, the authentication method is pre-shared key (password) Diffie-Hellman Group 5 and an IKE lifetime of 28800 secs which is 8hrs. I used the simple password Pal0Alto as the preshared key password and specified the remote peer's IP address.

crypto isakmp policy 1encr aes 256authentication pre-sharegroup 5lifetime 28800

crypto isakmp key ***Pal0Alt0*** address 192.168.28.1

2.  An **Access-List** is used to identify interesting traffic, in my case I wanted to identify traffic sourcing from 12.12.12.12/32 destined to 10.1.1.1/32 networks.

access-list 100 permit ip host 12.12.12.12 host 10.1.1.1

3. The **IPSec (Phase2) policy** needs to be defined by specifying exactly which hashing and encryption methods to use. In Cisco land, this policy is called a "transform-set"

crypto ipsec transform-set MYTRANSET esp-aes 256 esp-sha-hmac

4. A **Crypto Map** is used to bind all the configurations together. This is how the Crypto Map is processed. If traffic matched is by access-list 100, then set my peer to be 192.168.28.1 (firewall) and use the transform-set MYTRANSET , use Perfect Forward Secrecy using Diffie-Hellman Group 5 (make sure both sides support this)

crypto map MYMAP 1 ipsec-isakmpset peer 192.168.28.1set transform-set MYTRANSETset pfs group5match address 100

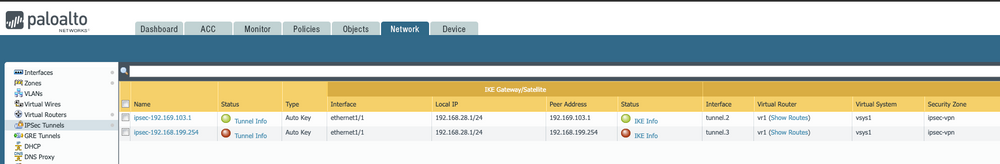
5. Apply the **Crypto Map "MYMAP"**to the egress interface, this turns on the policy and kicks starts the IPSec Tunnel setup.

interface Loopback0ip address 12.12.12.12 255.255.255.255!interface GigabitEthernet0/0ip address 192.168.199.254 255.255.255.0duplex autospeed automedia-type rj45***crypto map MYMAP***

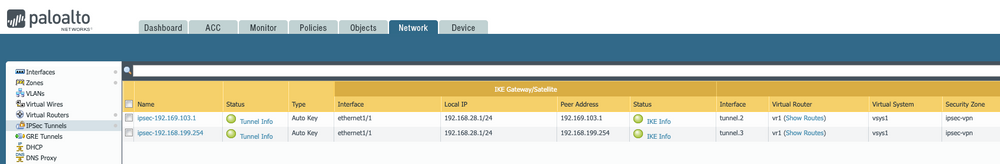
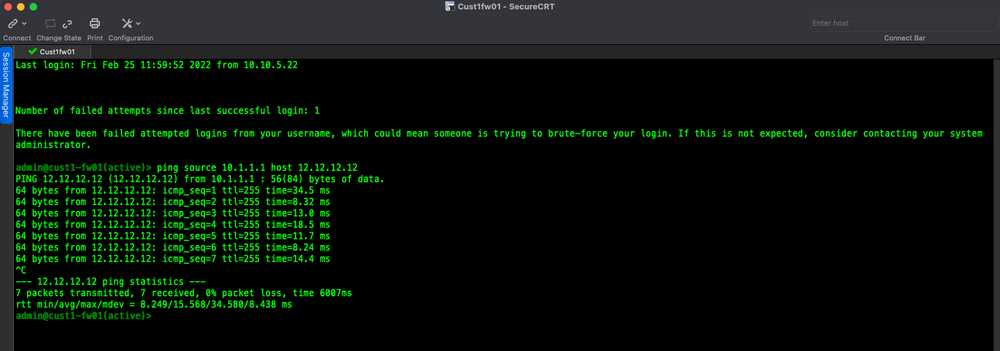
6. Now we can verify if the Tunnel has come up. On the Palo Alto Network Firewall under the Network tab and the IPSec Tunnels section, in the Status Column traffic lights, colours are used. If the statuses are green then everything is looking good. If they are red, some further troubleshooting is required.

**NOTE: There is no requirement to add a static route, unlike the Palo Alto Firewall, as this is a policy-based VPN that makes routing decisions based on the access list.**

Initially, the IPSec Tunnel to the Cisco router is showing down.

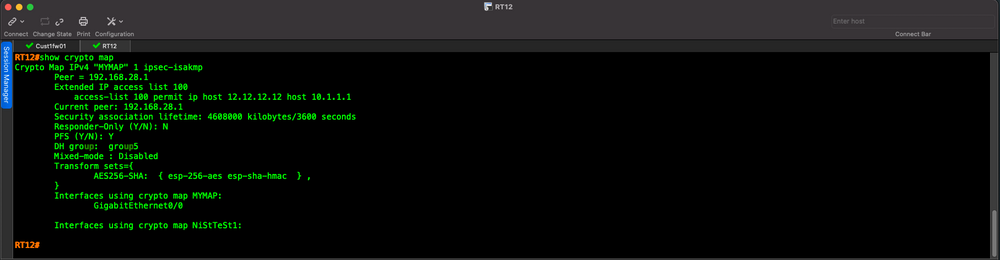
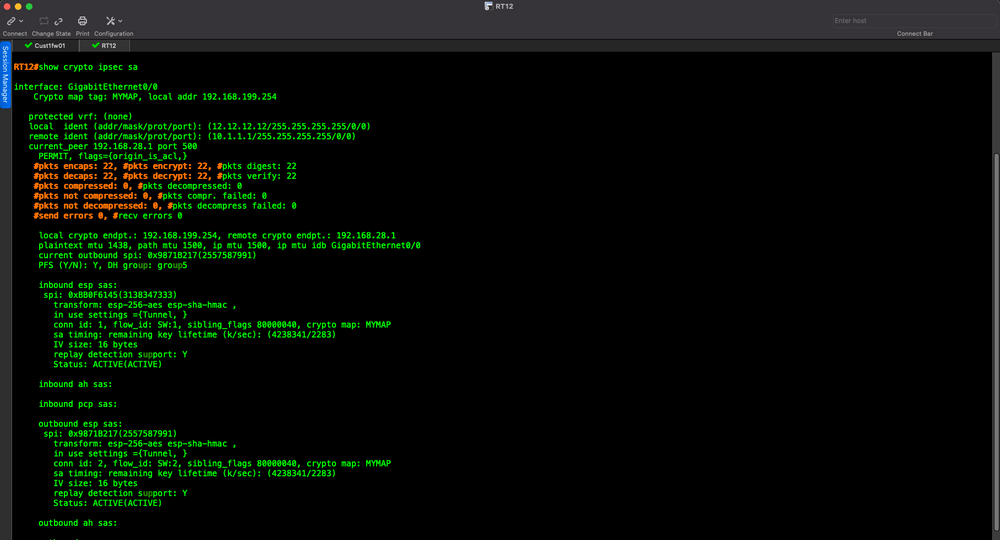
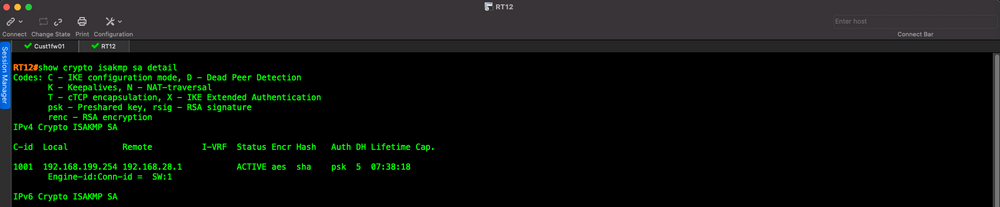


I performed a source ping - **ping source 10.1.1.1 host 12.12.12.12**and I got a response, I can now see that the status has turned green in the Firewall WebUI.

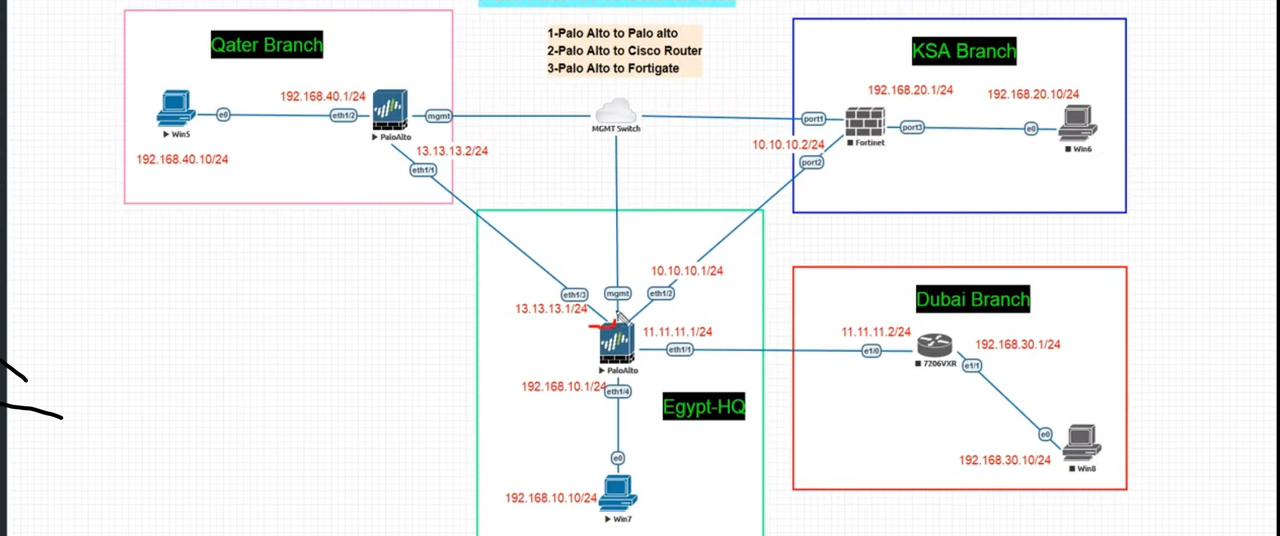


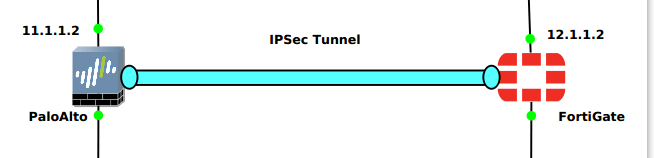
**The Cisco router can show details on IPSec VPN Tunnel using these commands:**

* show crypto isakmp sa detail
* show crypto ipsec sa
* show crypto map



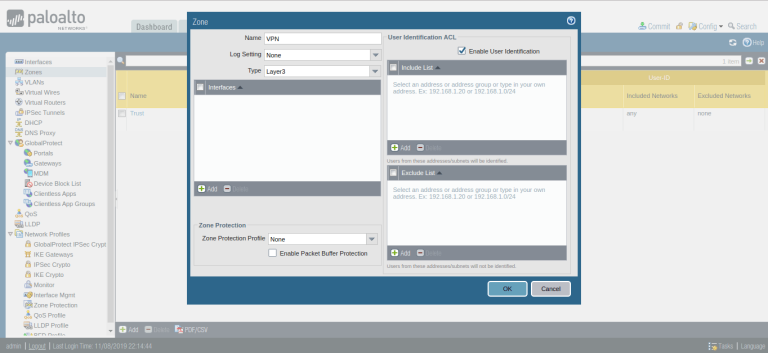
# IPSec VPN between a Palo Alto Networks Firewall and a Fortigate Firewall





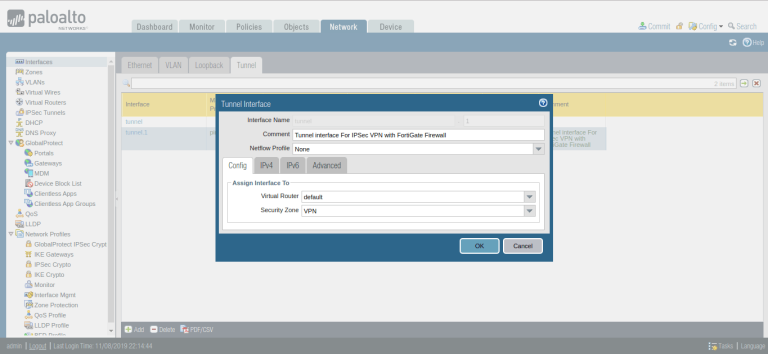
**Creating a Security Zone on Palo Alto Firewall**

**Network** >> **Zones** >> **Add**.

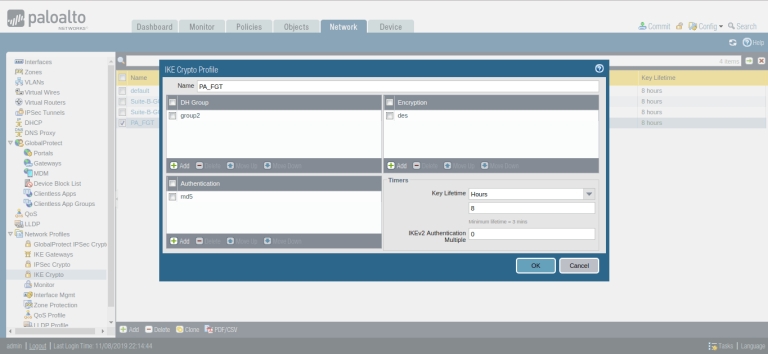
****

**Creating a Tunnel Interface on Palo Alto Firewall**

**Network** >> **Interfaces** >> **Tunnel**

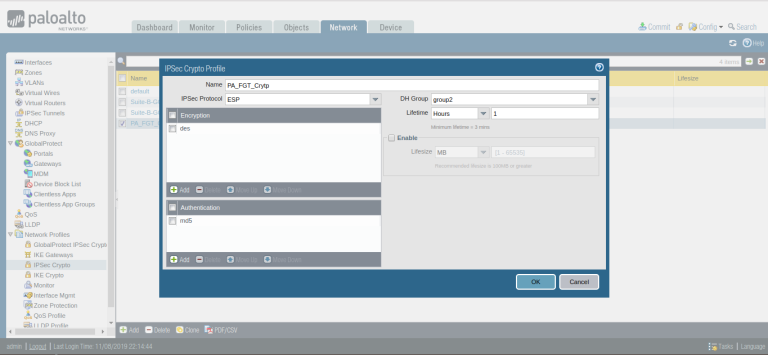
Select the **Virtual Router**, default in my case. 

### Defining the IKE Crypto Profile [Phase 1 of IPSec Tunnel]

**Network** >> **Network Profiles** >> **IKE Crypto** >>**Add**. 

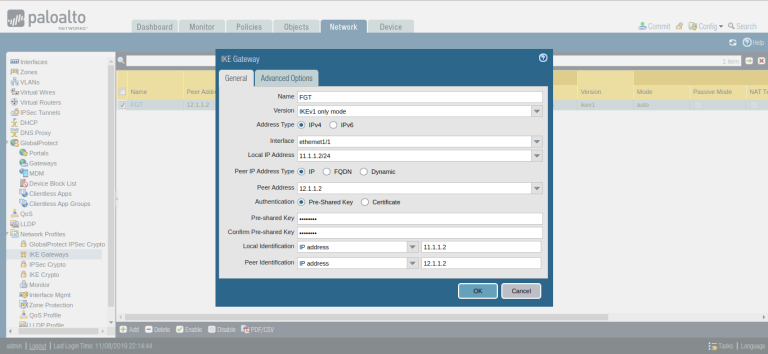
### Defining the IPSec Crypto Profile [Phase 2 of IPSec Tunnel]

**Network** >> **Network Profiles** >> **IPSec Crypto** >>**Add**.

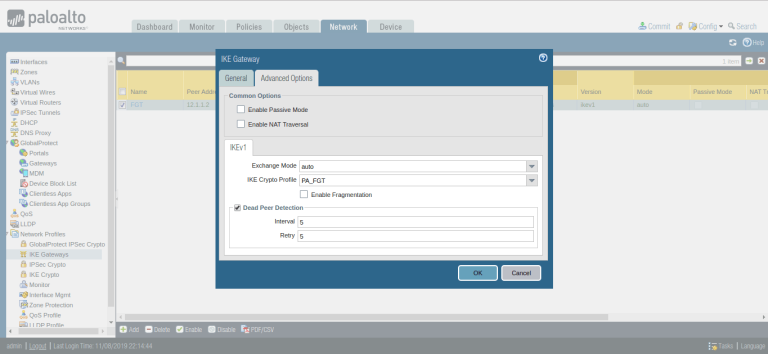


### Defining the IKE Gateway Profile

**Network** >> **Network Profiles** >> **IKE Gateways** >>**Add**.

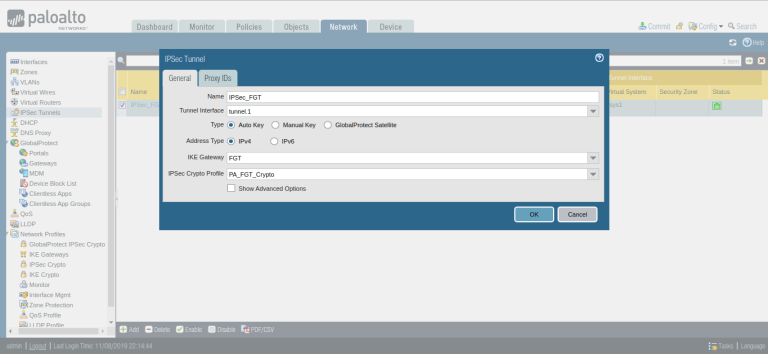


Click on **Advanced Option**, In **IKEv1**, select **IKE Crypto Profile**, which defines in Step 3.

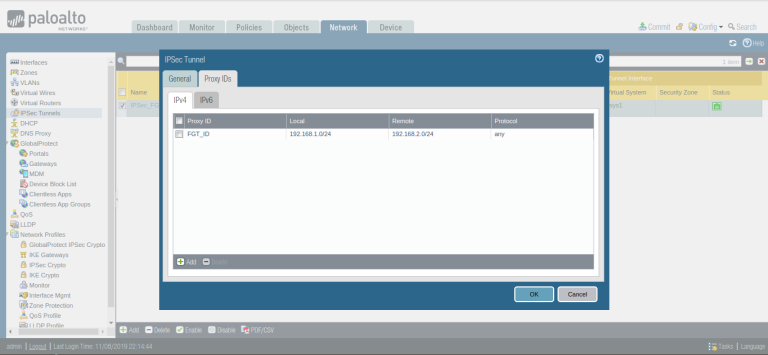


### Creating the IPSec Tunnel

We have defined IKE Gateway and IPSec Crypto profile for our IPSec Tunnel. Now, we have to define the IPSec Tunnel. Go to **Network** >> **IPSec Tunnels** >> **Add**. Define the user-friendly name for IPSec Tunnel. Next, select the tunnel interface, which defined in Step 2. Select the profiles for **IKE Gateway** and **IPSec Crypto** **Profile**, which defined in Step 3 and Step 5 respectively.

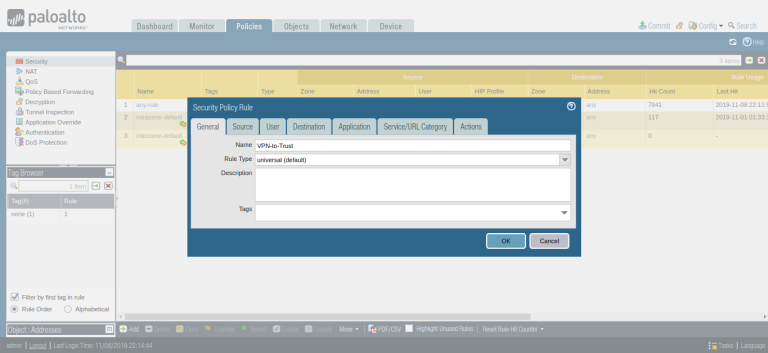


Go to the Proxy IDs Tab, and define Local and Remote Networks. In this scenario, I’m using 192.168.1.0/24 and 192.168.2.0/24 in LAN Networks.

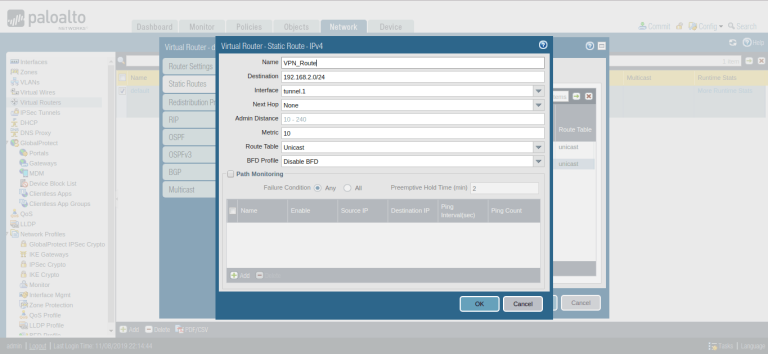


### Creating the Security Policy for IPSec Tunnel Traffic

**Policies** >> **Security** >> **Add**

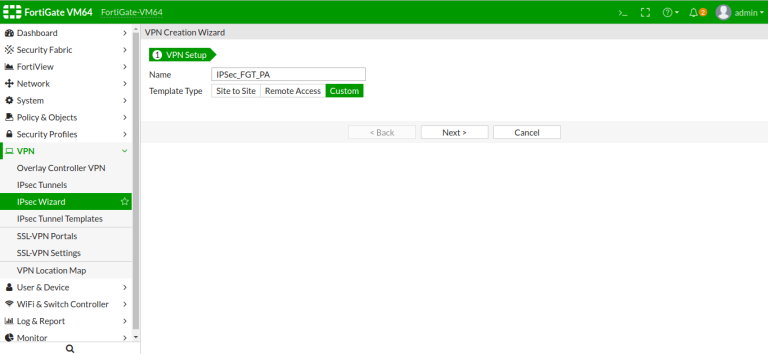


### Configuring Route for Peer end Private Network

**Network** >> **Virtual Routers** >> **Default** >> **Static Routes** >> **Add**

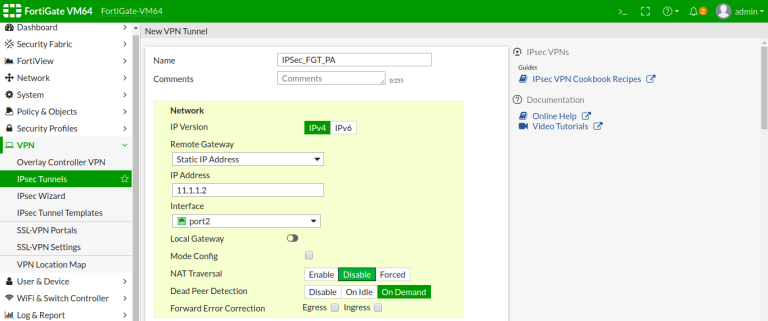
## Steps to configure IPSec Tunnel in FortiGate Firewall

**VPN** >> **IPSec Tunnels** >> **Create New**

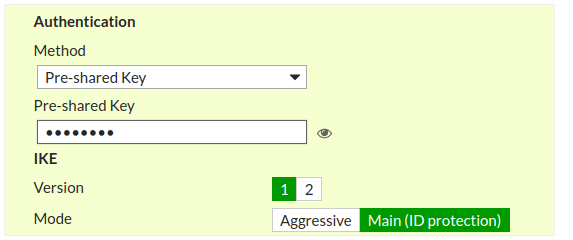
****

### IPSec Tunnel Phase 1 & Phase 2 configuration

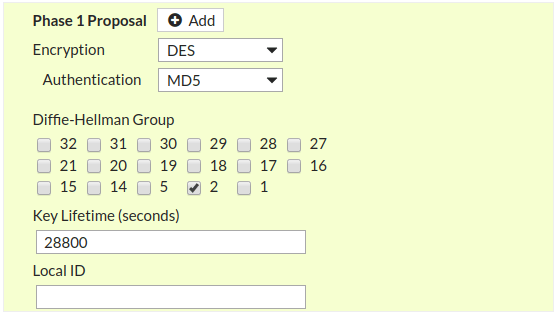
Select, **IP Version** IPv4/IPv6, In the **Remote Gateway** select Static IP Address. In the IP Address field, give the remote site Palo Alto Firewall Public IP i.e. 11.1.1.2.

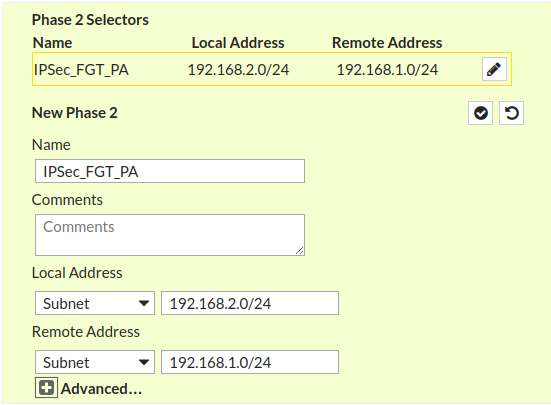


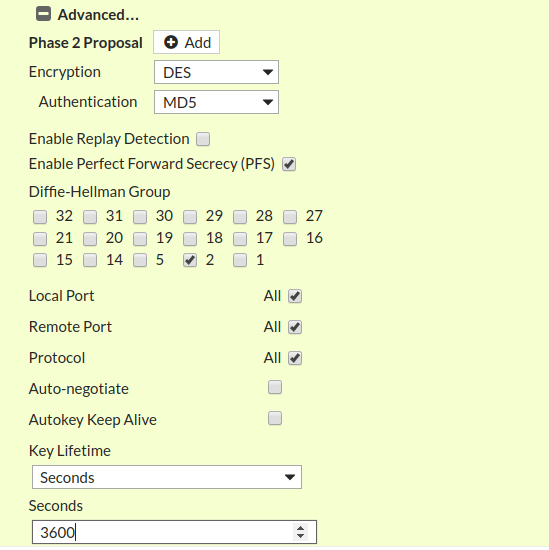
Scroll down the page, and in the **Authentication field,** select the authentication method **Pre-Shared Key** and Provide the exact same key here as shown in the below image. Select the **IKE version** 1 and **Mode** as Main (ID Protection).



we use **DES**, **MD5** and **Group 2** for Encryption

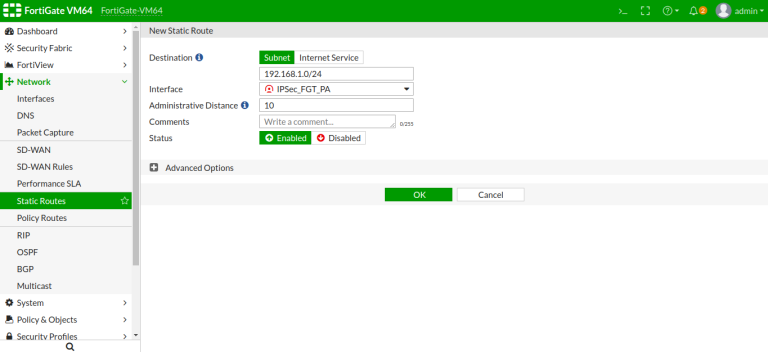


****

****

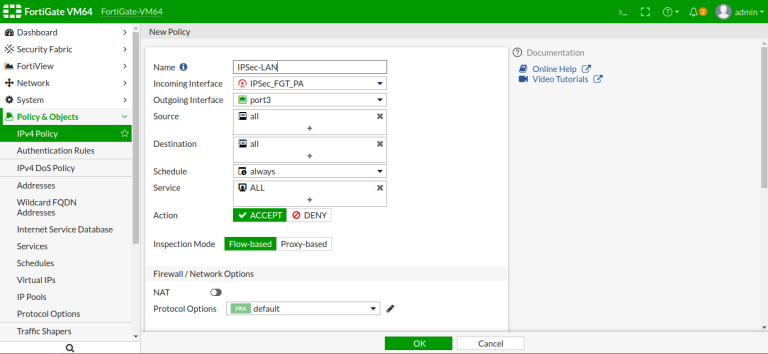
### Configuring Static Route for IPSec Tunnel

**Network** >> **Static Route** >>**Create New**

****

### Configuring the Security Policy for IPSec Tunnel

**Policy & Objects** >> **IPv4 Policy** >>**Create New**

****

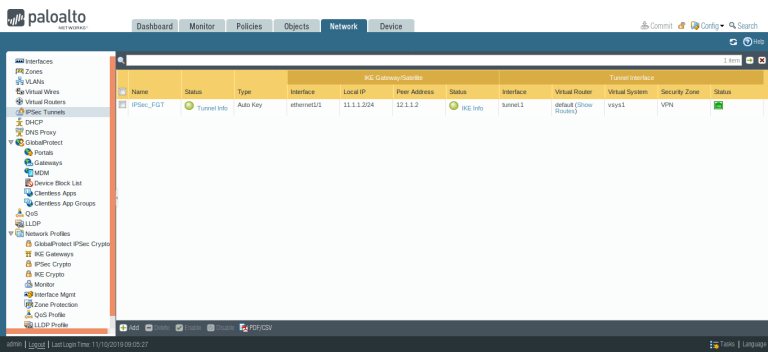
### Finally Initiating the tunnel and verify the configuration

test vpn ike-sa gateway FGT

test vpn ipsec-sa tunnel IPSec\_FGT:FGT\_ID

PA

**Network** >> **IPSec Tunnels**

****

**Monitor** >> **IPSec Monitor**

****

unetlab\_export-20240222-165802

<https://drive.google.com/file/d/1LX718lHvKk0hfjAgKloYp6YsTF6pPI8e/view?usp=sharing>