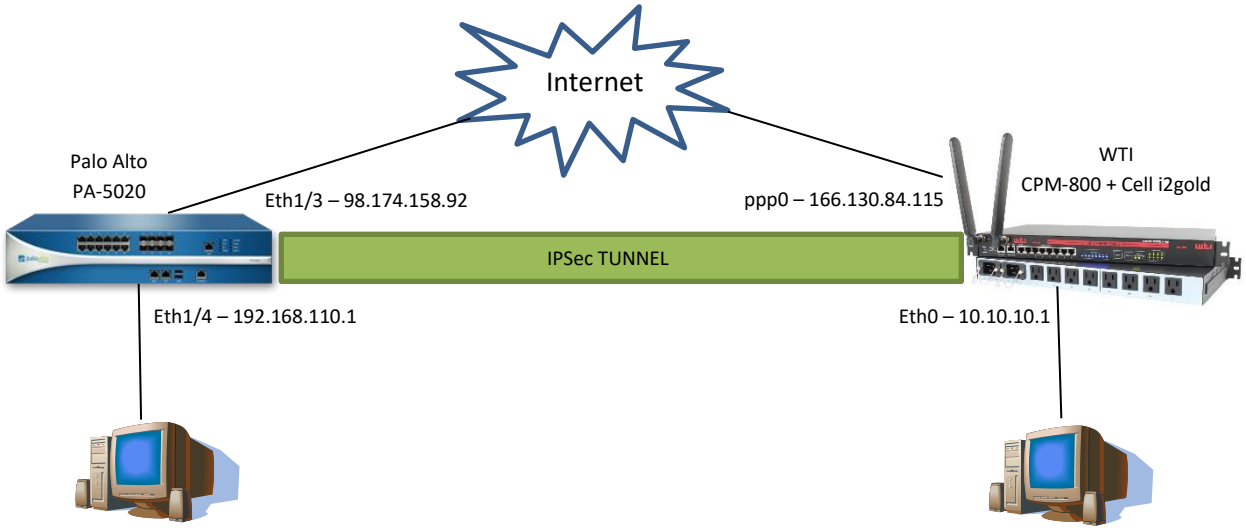
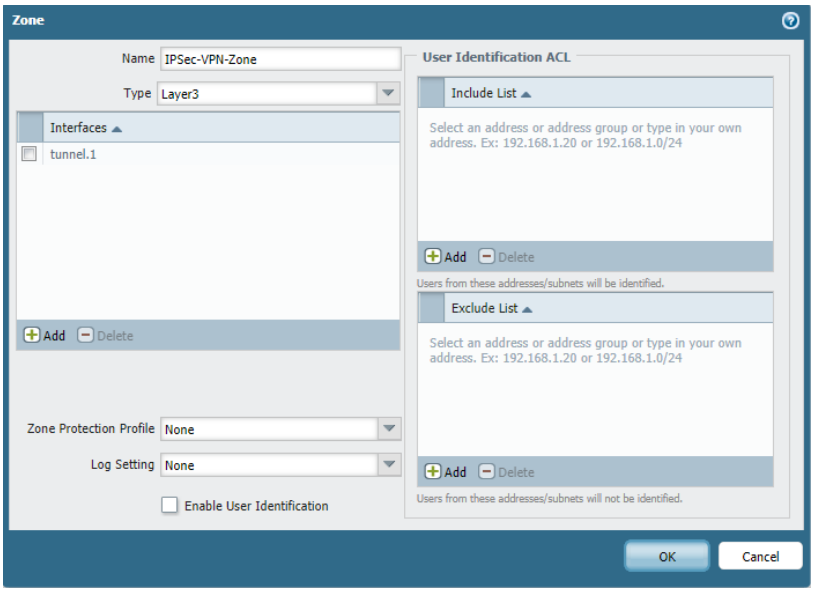



| **Palo Alto Network Firewall** | |
|---|---|
| Eth1/3 – Outside (WAN) | 98.174.158.92 |
| Eth1/4 – Inside (LAN) | 192.168.110.1 |
| Tunnel Interface | tunnel.1 |
| Local Network | 192.168.110.0/24 |
| Remote Network | 10.10.10.0/24 |
| | |
| **WTI Network** | |
| ppp0 – Cell (i2gold) | 166.130.84.115 |
| Eth0 – Inside (LAN) | 10.10.10.1 |
| Tunnel Name | tunnel.1 |
| Local Network | 10.10.10.0/24 |
| Remote Network | 192.168.110.0/24 |

1. Creating a security zone on Palo Alto Firewall

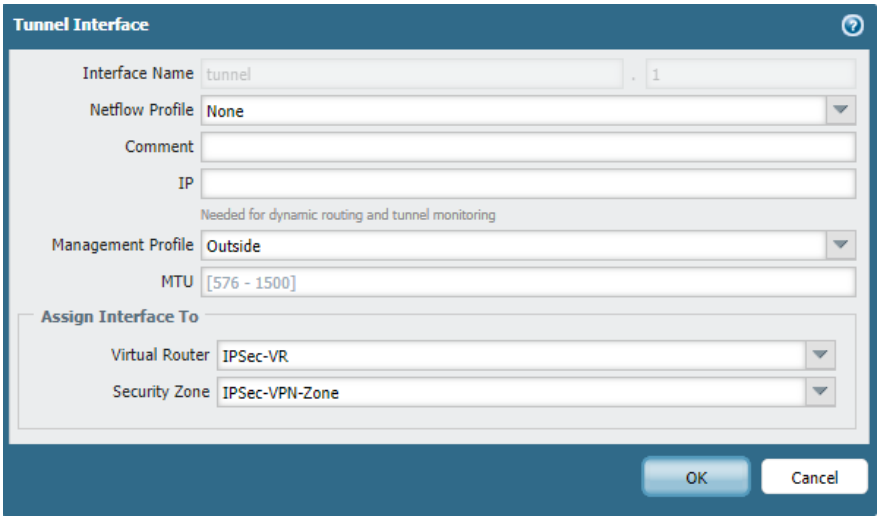
   First, we need to create a separate security zone on Palo Alto Firewall. In order to configure the security zone, you need to go **Network** >> **Zones** >> **Add**. Here, you need to provide the Name for the Security Zone. You can provide any name as per your convenience.



2. Creating a tunnel interface on Palo Alto Firewall

You need to define a separate virtual tunnel interface for IPsec Tunnel. To define the tunnel interface, Go to **Network** >> **Interfaces** >> **Tunnel**. Select the **Virtual Router**, an *IPsec-VR* in my case. Also, in **Security Zone** filed, you need to select the security zone as defined in Step 1.

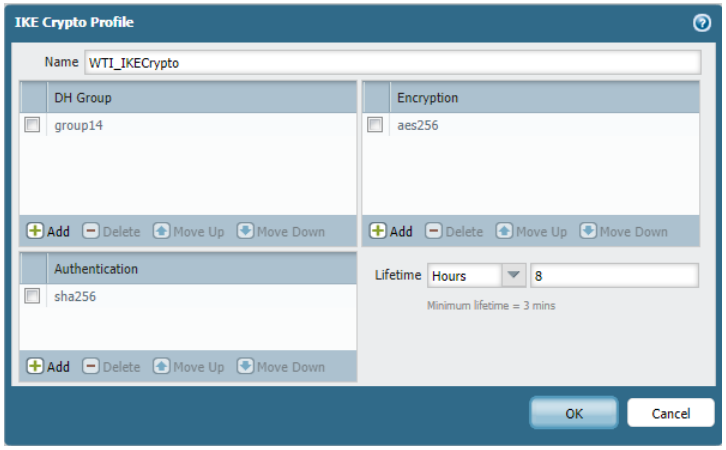
Interface Name: **tunnel.1**
Virtual Router: **IPSec-VR**
Security Zone: **IPSec-VPN-Zone**




3. Defining IKE Crypto Profile [Phase 1 of IPSec Tunnel]

Now, you need to define Phase 1 of the IPSec Tunnel. You need to go **Network** >> **Network Profiles** >> **IKE Crypto** >> **Add**.

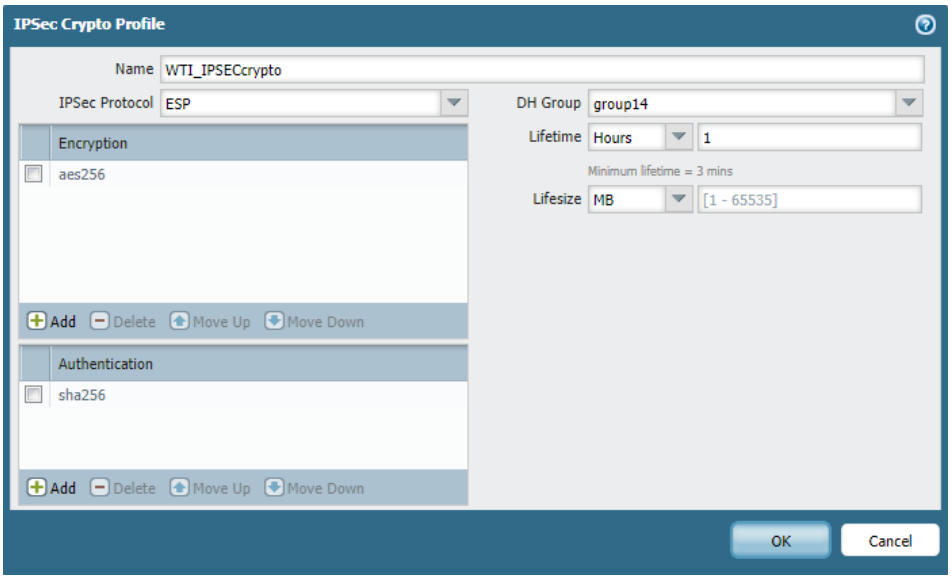
Name: **WTI_IKECrypto**
DH Group: **group14**
Encryption: **aes256**
Authentication: **sha256**
Lifetime: **8 Hours**



4. Defining the IPSec  Crypto Profile [Phase 2 of IPsec Tunnel]

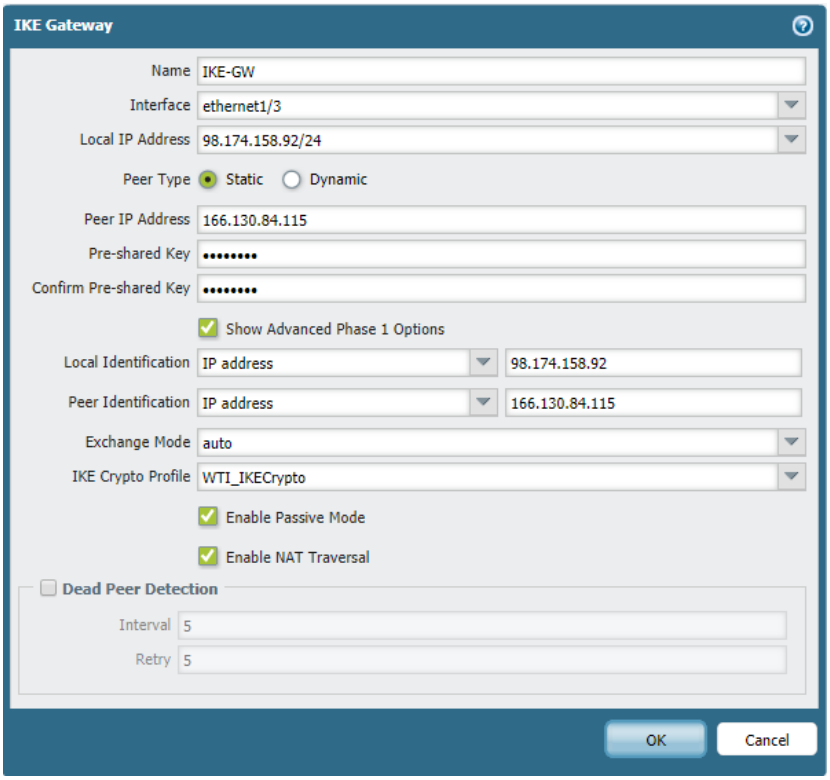
   Now, you need to define Phase 2 of the IPSec Tunnel. You need to go **Network** >> **Network Profiles** >> **IPSec Crypto** >> **Add**.

   Name: **WTI_IPSECcrypto**
   IPSec Protocol: **ESP**
   Encryption: **aes256**
   Authentication: **sha256**
   DH Group: **group14**
   Lifetime: **1 Hours**



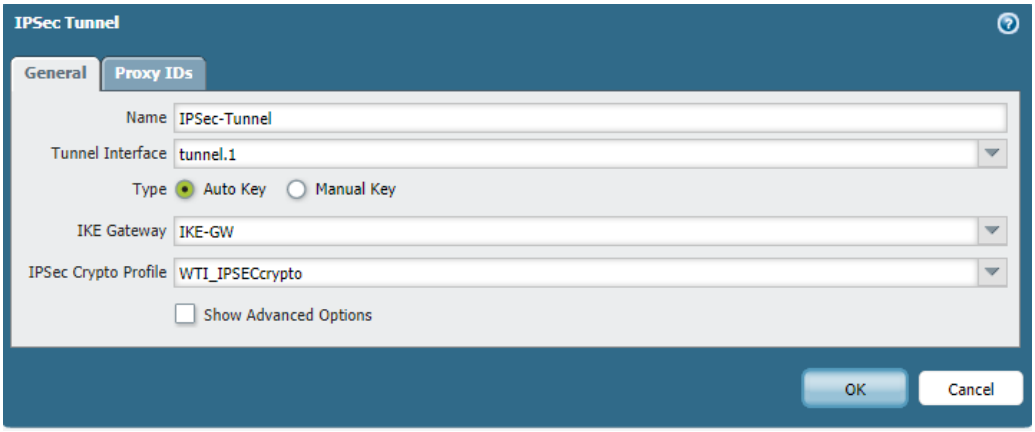

5. Defining the IKE Gateway Profile

   Now, you need to go **Network** >> **Network Profiles** >> **IKE Gateways** >> **Add**. In **General** Tab, You need to define the name of the IKE Gateway Profile. In Interface filed, you need to define your Internet-facing Interface, in my case, Ethernet 1/3, which has **98.174.158.92** IP Address. Select Peer Type as **Static**. Define the Peer IP Address, in my case **166.130.84.115 (i2gold Cell)**. Select the Authentication Method, i.e. Pre Shared Key or Certificate. In this scenario, I'm using the Pre-shared Key as **WTI949**. Define the Local and Peer IP address in the **Local Identification** and **Peer Identification** field and select IKE Crypto Profile as **WTI_IKECrypto**.

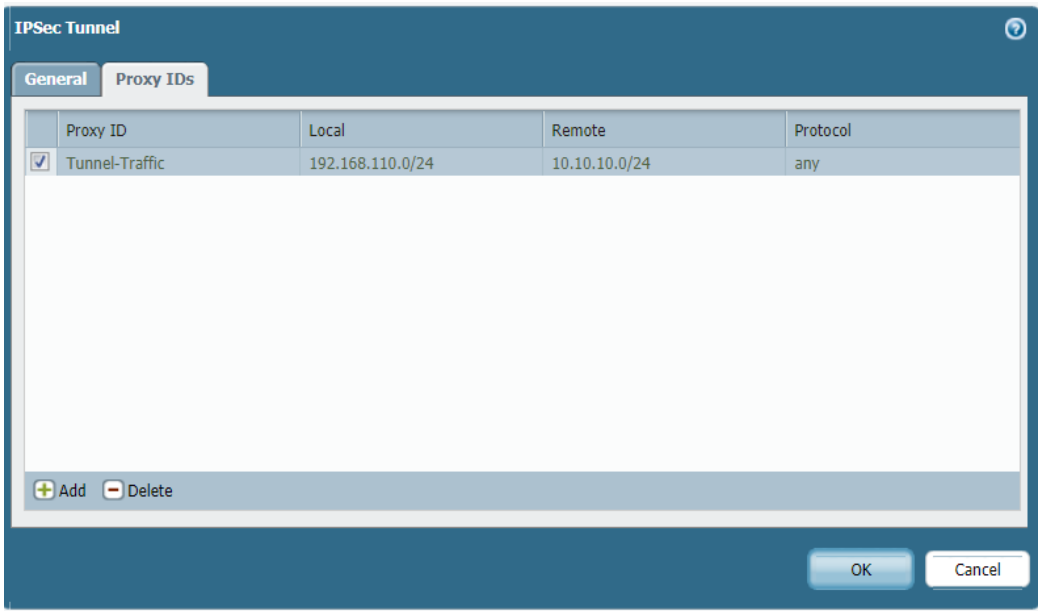



6. Creating the IPSec Tunnel

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**.

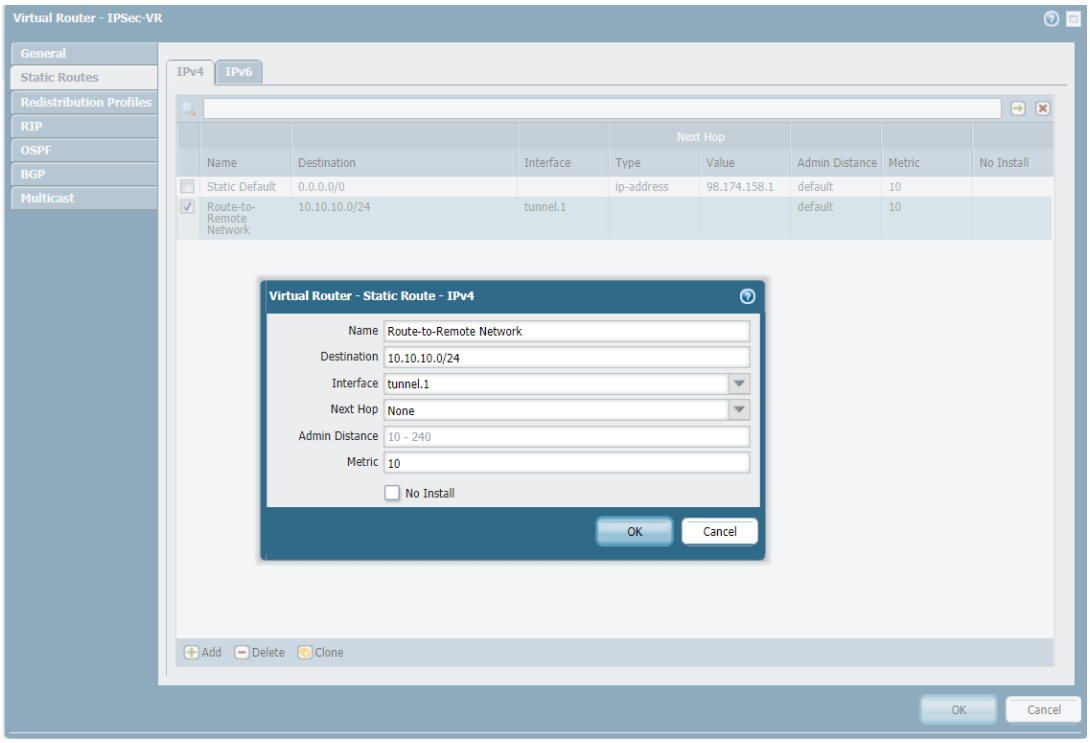


Go to the Proxy IDs Tab, and define Local and Remote Networks. In this scenario, I'm using 192.168.110.0/24 and 10.10.10.0/24 in LAN Networks.




7. Configuring Route for Peer end Private Network

   Now, you need to provide a static route for Peer end Private Network. Just go to **Network** >> **Virtual Routers** >> **Default** >> **Static Routes** >> **Add**. Select the Name for this Route and define the destination network for this route, i.e. 10.10.10.0/24 in this example.



8. Creating the Security Policy for IPSec Tunnel Traffic.

   Now, you need to create a security profile that allows the traffic from VPN Zone to Trust Zone. You need to Go **Policies** >> **Security** >> **Add** to define a new Policy.

Security Policy overview

| | | Source | | | | Destination | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Name | Tag | Zone | Address | User | HIP Profile | Zone | Address | Application | Service | Action | Profile | Options |
| allow-ike-ipsec | none | Outside | 166.130.84.115<br>98.174.158.92 | any | any | Outside | 116.130.84.115<br>98.174.158.92 | any | any | | none | |
| allow-tunnel-traffic-in | none | IPSec-VPN-Z... | 10.10.10.0/24 | any | any | Inside | 192.168.110.0/24 | any | any | | none | |
| allow-tunnel-traffic-out | none | Inside | 192.168.110.0/24 | any | any | IPSec-VPN-Z... | 10.10.10.0/24 | any | any | | none | |
| Inside To Outside | none | Inside | any | any | any | Outside | any | any | any | | none | |

1. Creating NAT to allow Inside (LAN) access Internet.

NAT overview

| | | Original Packet | | | | | | Translated Packet | |
|---|---|---|---|---|---|---|---|---|---|
| Name | Tag | Source Zone | Destination Zone | Destination Interface | Source Address | Destination Address | Service | Source Translation | Destination Translation |
| Inside To Outside | none | Inside | Outside | any | any | any | any | dynamic-ip-and-port<br>ethernet1/3<br>98.174.158.92/24 | none |

We finished the configuration of the IPSec tunnel in the Palo Alto firewall. Now, we will configure the IPSec tunnel in WTI unit

WTI IPsec Setting

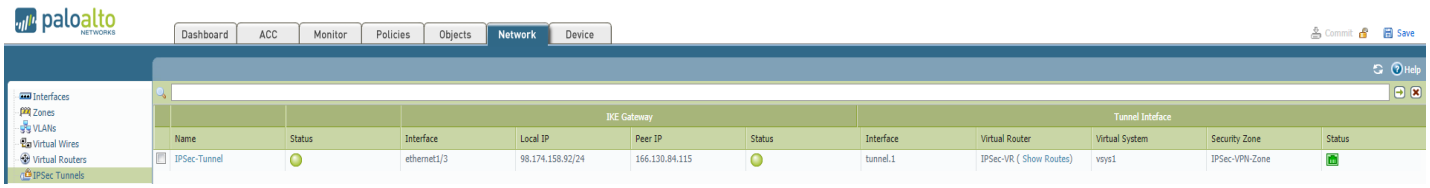
| IPSEC_CLIENT VPN DETAILS [tunnel.1] | | |
|---|---|---|
| Enable: | On | |
| Tunnel Name: | tunnel.1 | |
| Security: | Pre-shared Secret (Static Key File) | |
| Authentication Type: | ESP | |
| Left Address: | 166.130.84.115 | #Cell (i2gold) Unit address |
| Left ID: | 166.130.84.115 | #IKEID Sent by Cell (i2gold) |
| Left Subnet: | 10.10.10.0/24 | #Subnet Local Network behind WTI |
| Right Address: | 98.174.158.92 | #Palo Alto outside address |
| Right ID: | 98.174.158.92 | #IKEID Sent by Palo Alto |
| Right Subnet: | 192.168.110.0/24 | #Subnet Local Network behind Palo Alto |
| Tunnel Options: | (Show Options) | |
| Option 1: | keyexchange | ikev1 |
| Option 2: | ike | aes256-sha256-modp2048 |
| Option 3: | esp | aes256-sha256-modp2048 |
| | | |
| Pre-Shared Key | WTI949 | |
| | | |
| Change VPN Parameters | | |

**Set IPTABLES on Eth0**

In this Example:
- ppp0 is Cell (i2gold)
- Eth0 is inside (LAN)

1. **iptables -A INPUT -i eth0 -j ACCEPT** #Allow traffic from the LAN side
2. **iptables -A INPUT -i ppp0 -j ACCEPT**#Always accept loopback traffic
3. **iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT** #Allow established connections
4. **iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE**#Masquerade
5. **iptables -A FORWARD -i ppp0 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT**#Forwarding
6. **iptables -A FORWARD -i eth0 -o ppp0 -j ACCEPT** #Allow outgoing connections from the LAN side
7. **iptables -t nat -I POSTROUTING 1 -m policy --pol ipsec --dir out -j ACCEPT** #NAT IPsec Traffic

Monitoring VPN Session in Palo Alto




Monitoring VPN Session in WTI

```
CPM> /bash ipsec status
Security Associations (1 up, 0 connecting):
    tunnel.1[1]: ESTABLISHED 2 minutes ago, 166.130.84.115[166.130.84.115]...98.174.158.92[98.174.158.92]
    tunnel.1{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c117e769_i b0b96ce9_o
    tunnel.1{1}:   10.10.10.0/24 === 192.168.110.0/24
```