Forcepoint ONE and Palo Alto IPSec Configuration Guide

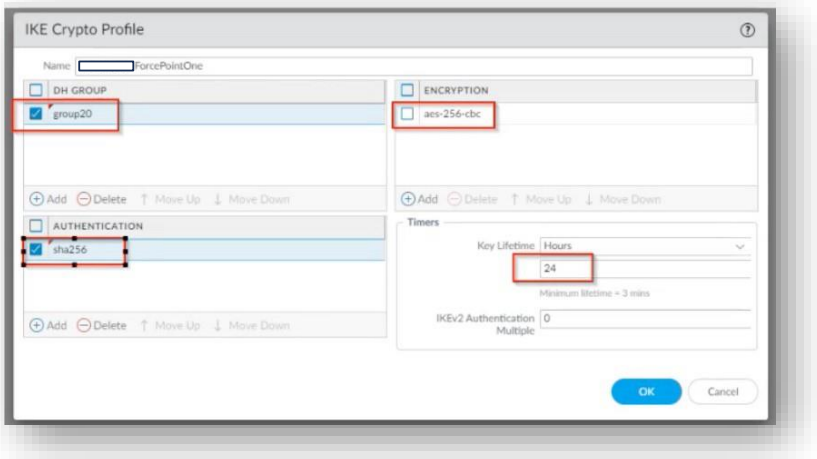
Forcepoint

Forcepoint ONE Integrated with Palo Alto IPSec

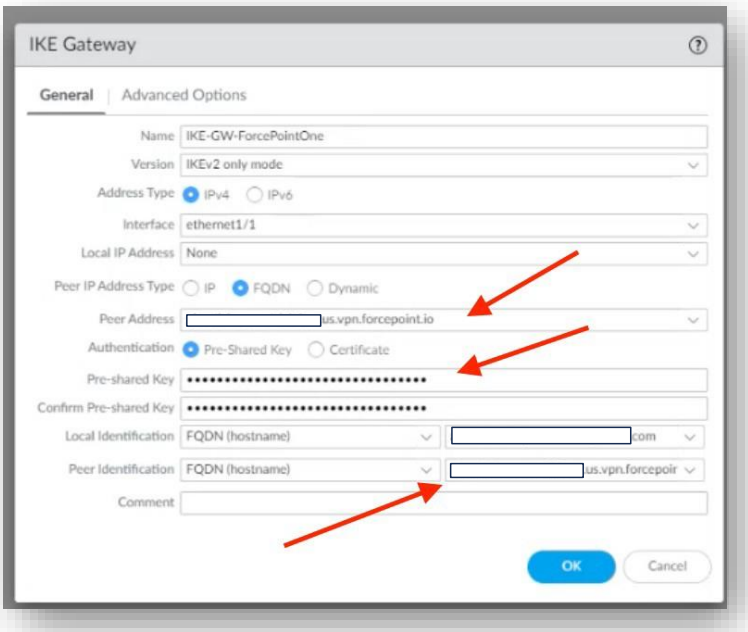
This guide will provide you with a step-by-step walkthrough for establishing the IPSec tunnel between Forcepoint ONE and the Palo Alto Firewall envirnonment.

The first step in the IPsec VPN tunnel creation is to configure the IKE Crypto profiles, IKE Gateway, IPsec Crypto, IPsec tunnel and security profile.

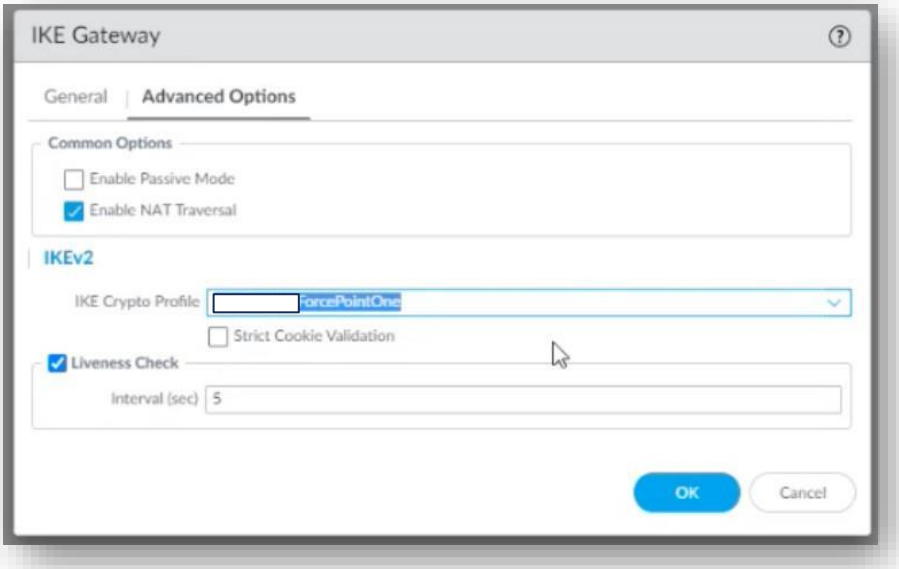
1. Create IKE Crypto Profile
    - Go to **Network** > **Network Profile** > **IKE crypto** > **Create a profile**, then configure the encryption algorithm, autherntication algorithm and lifetime values according to your requirements.



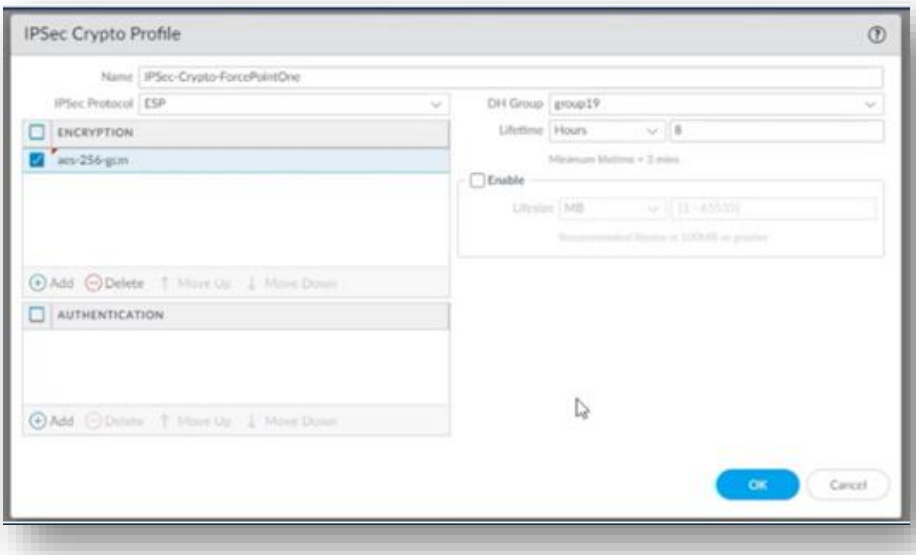
2. Configure IKE Gateway
    - Peer Address is “Cloud IKE ID”
    - Location Identification is “Site IKE ID”
    - Peer Identification is “Cloud IKE ID”



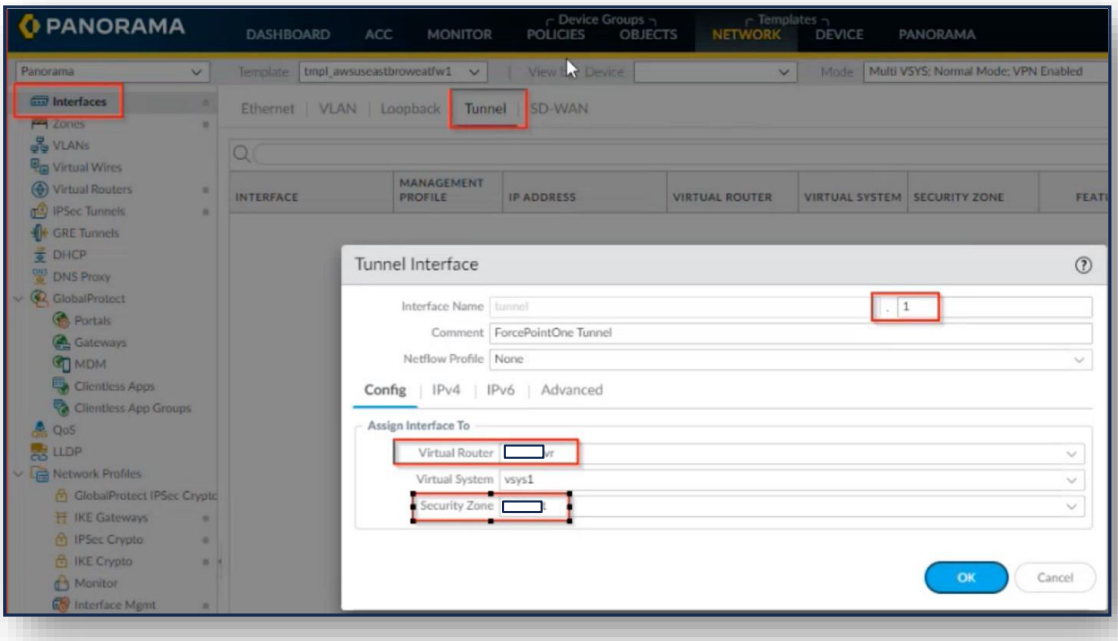
- If NAT is involved, then you will need to enable NAT Traversal. Go to **Advance Options** > **Enable NAT Traversal** > click **OK.**



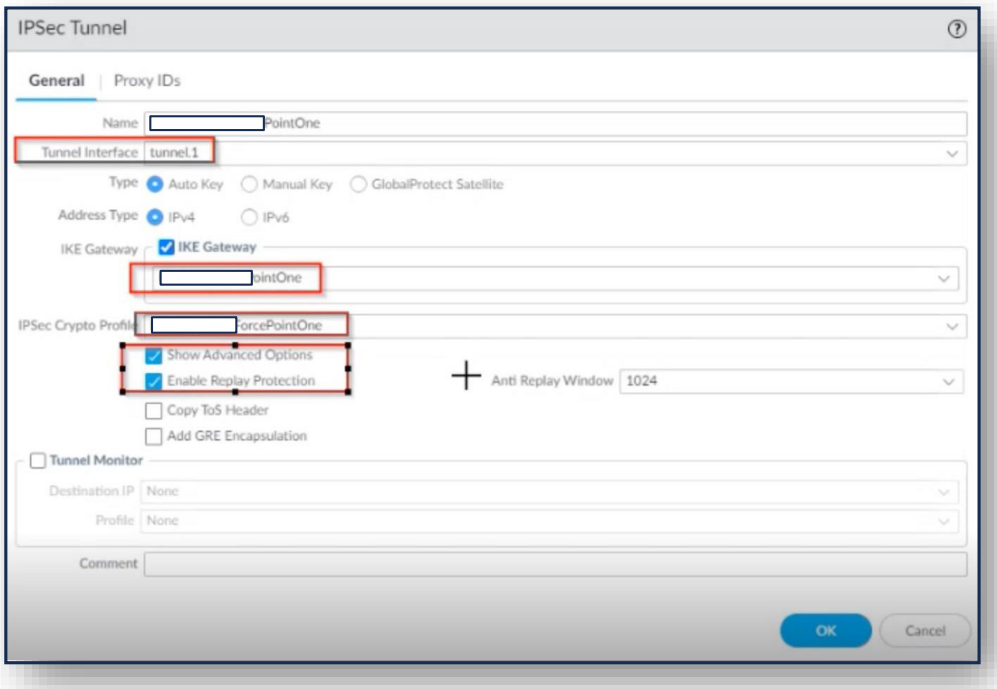
3. Configure IPsec tunnel prameters
   - Go to **Network** > **Network Profiles** > **IPSec Crypto**
   - Create a new IPSec Crypto profile.
   - Configure the encryption algorithm, dh-group and lifetime values according to your requirements.



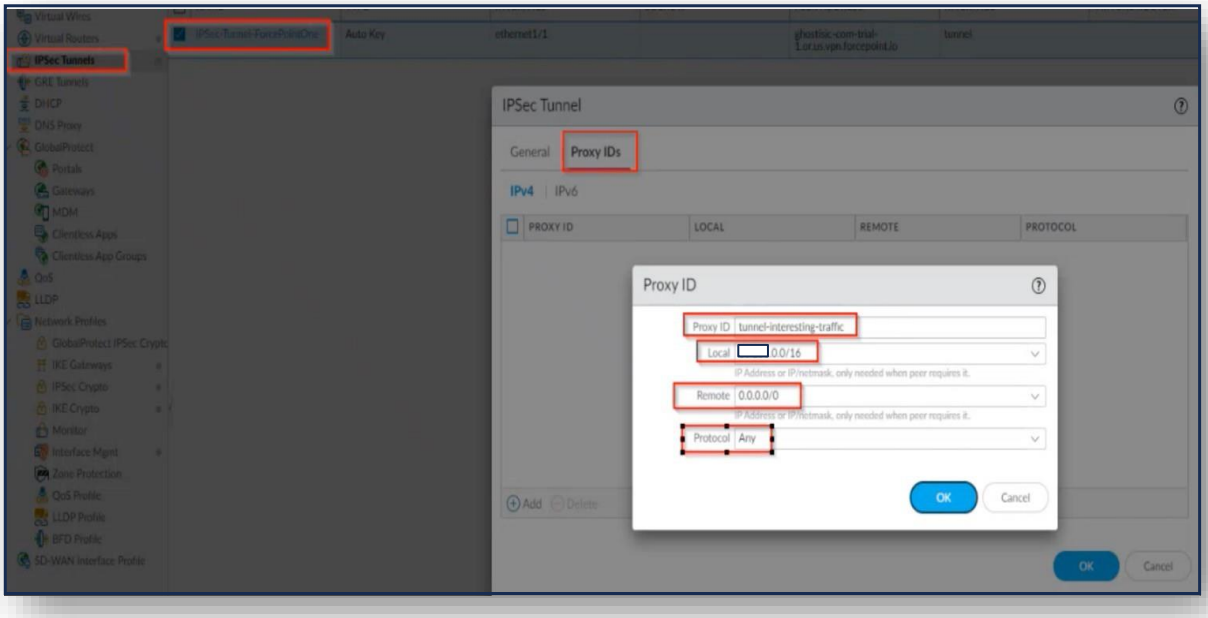
4. Create a New Tunnel Interface
   - Select Tunnel Interface > New Tunnel Interface
   - In the **Interface Name** field, specify a numeric suffix such as 1.
   - In the Configuration tab, select the Virtual Router and the Security Zone.



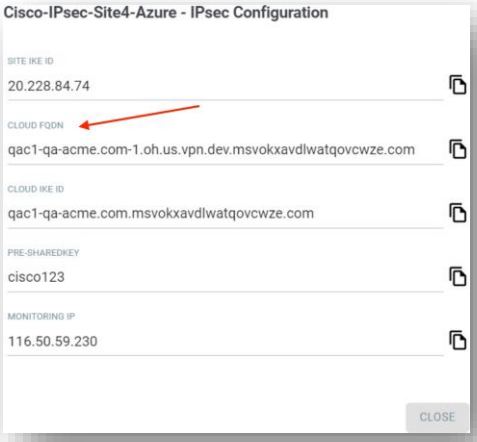
5. Create IPSec Tunnel
   - Go to **Network** > **IPSec Tunnels** and click on **Add**
   - Provide a name for the tunnel and select the tunnel interface created in Step 4.

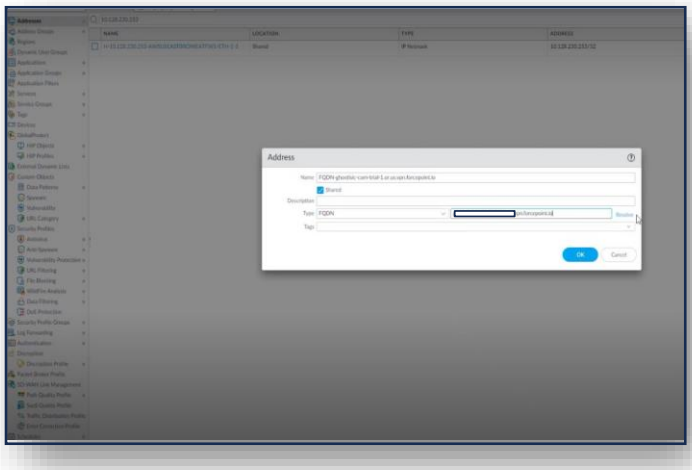


6. Create a Proxy ID to identify the VPN peers
    - Select the **Proxy IDs** tab.
    - Select the **IPv4** tab.
    - Click **Add** and enter the **Proxy ID** name.
    - Enter the local IP address or subnet for the VPN gateway.
    - Remote address for the VPN gateway is 0.0.0.0/0

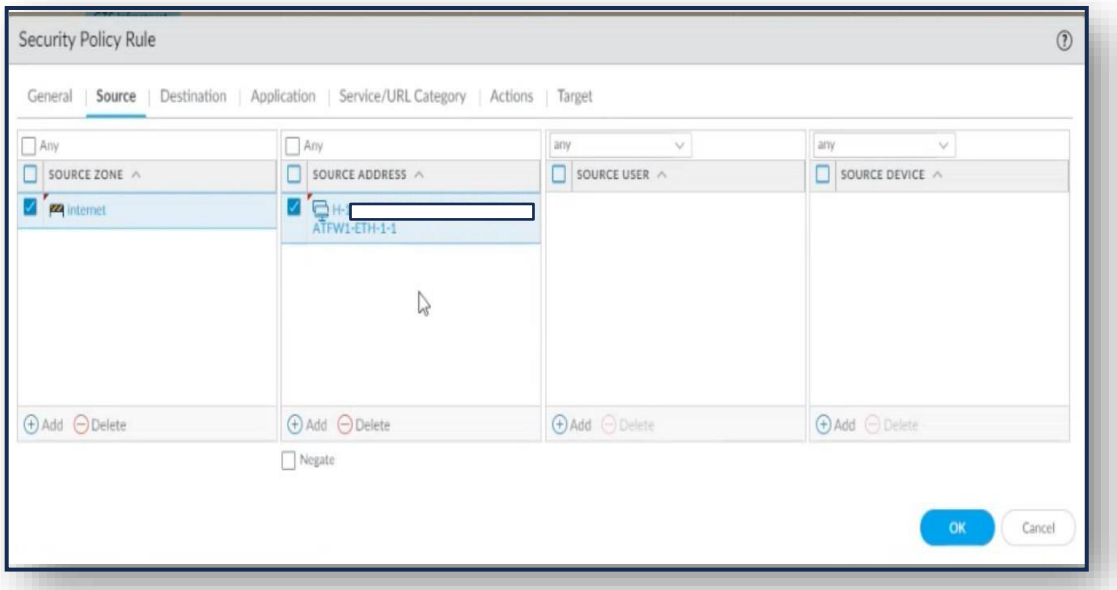


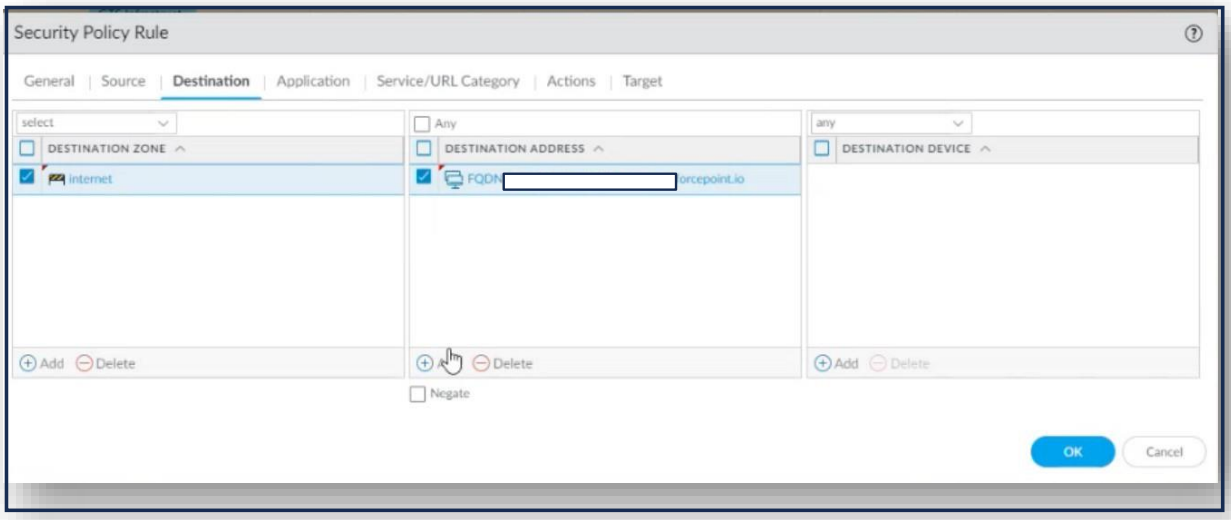
7. Create a Policy-Based Forwarding (PBF) rule.
    - When creating a PBF rule, you must specify a name for the rule, a source zone or interface and an egress interface. All other components are either optional or have default value.
    - To begin configuration of Destination Interface, go to **Objects** > **Addresses**
        - Note: You can copy **Cloud FQDN** from the Forcepoint ONE setup information.



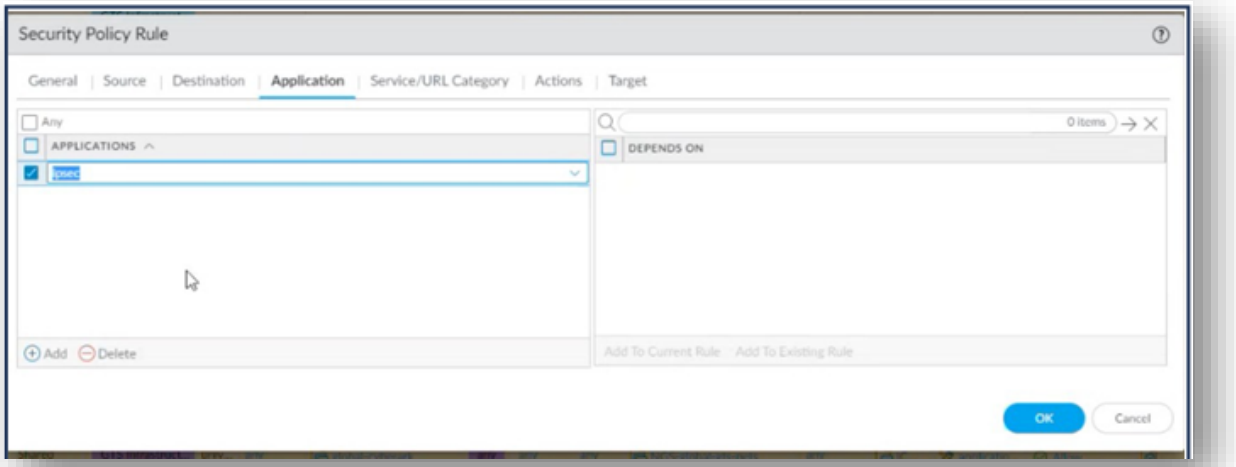


8. To configure security polices:
   - Select **Palo Alto Networks** > **Pre Rules** > **Security Policy Rule**
   - Click **Add** to create a new security policy rule.
   - Configure **Source** and **Destination** policy rules.

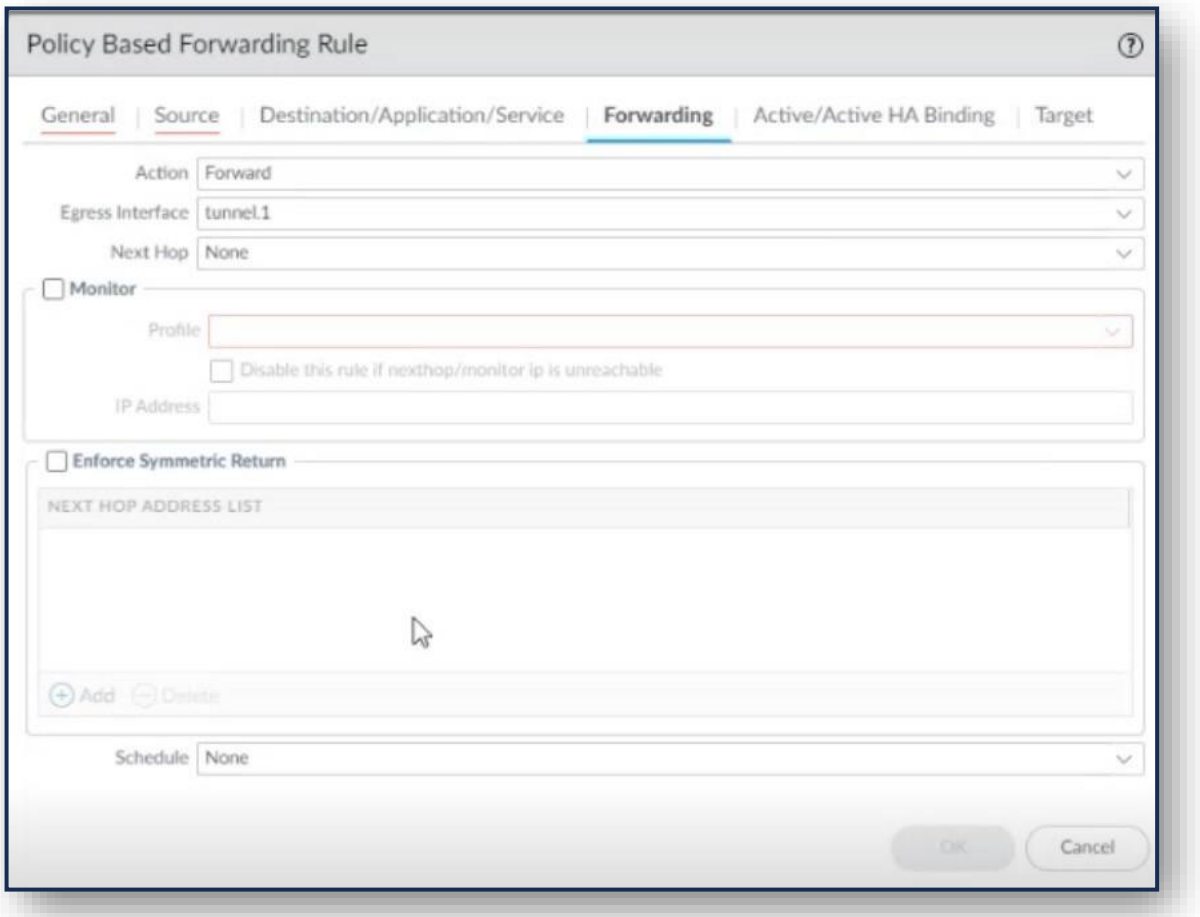




- Application should be IPSec.



9. Forwarding
   - The next hop egress interface will be the tunnel that you created in Step 4.
   - Save and commit the changes.



Troubleshooting PAN

- Useful CLI commands
- Show vpn ike-sa gateway <name>
- Test vpn ike-sa gateway <name>
- Debug ike stat
- Check if the firewalls are negotiating the tunnels and ensure the two unidirectional SPIs exist
- Show vpn ispec-sa
- Show vpn ipsec-sa tunnel <tunnel.name>

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP ONE and Palo Alto IPSec Configuration Guide] 10Oct2023