Palo Alto Remote Access VPN Certificates

Reed Holman | Cybersecurity | 5/30/2023



Purpose:

To configure Remote Access VPN using Certificates

Background:

A VPN or a Virtual Private Network is a way to have a secure connection between different devices or networks. There were many different types of VPNs with different uses like Remote access, site-to-site, etc. VPNs are very useful for using a public network and wanting to access the internet securely. They are also very commonly used companies and other organizations to have employees to securely access the private network form a remote location. Last time we configured a site-site VPN where two different networks connect securely to each other. This time we used remote access which allows an individual to connect securely to a network.

Since we are using Palo Alto firewalls, we used an application called GlobalProtect which we used to create a secure connection using remote access. In this Lab instead of a pre-shared key we used self-signed certificates. Certificates are another way of authenticating and establishing a secure connection between networks.

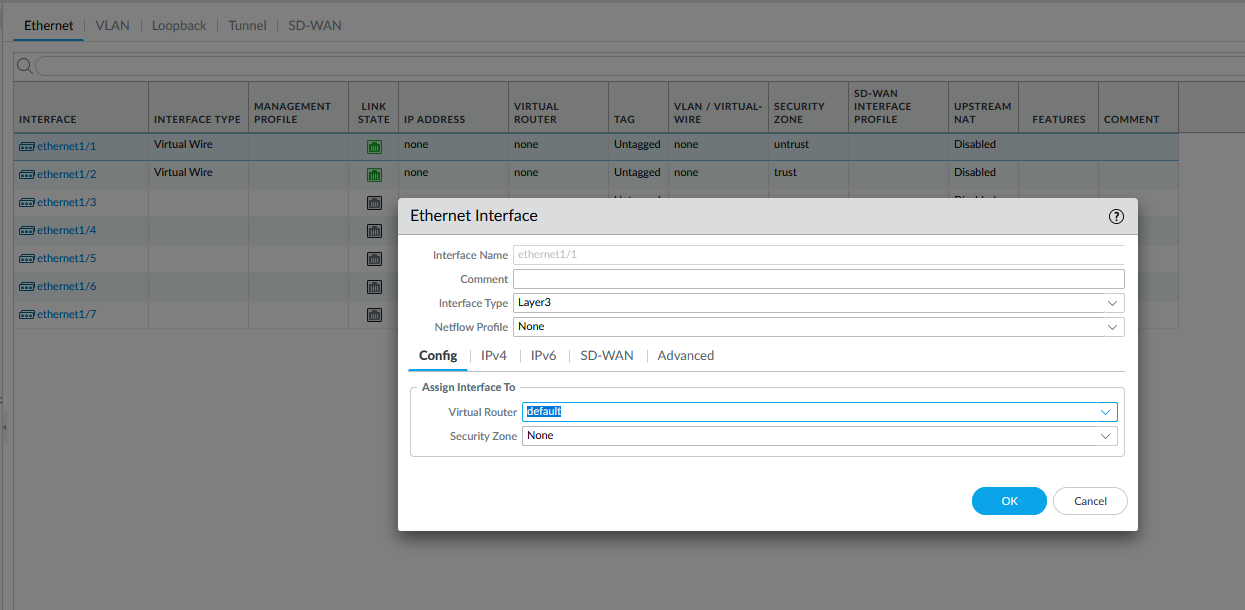
Diagram:

Diagram

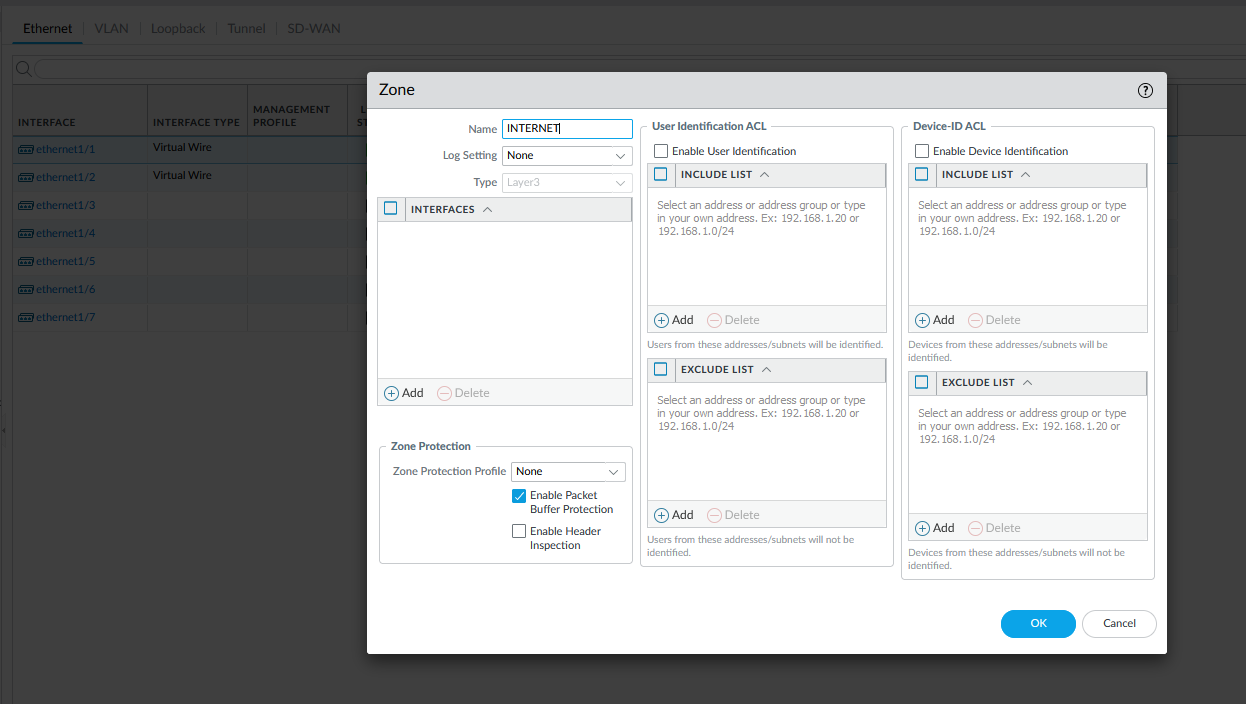
Description automatically generated

Configurations:

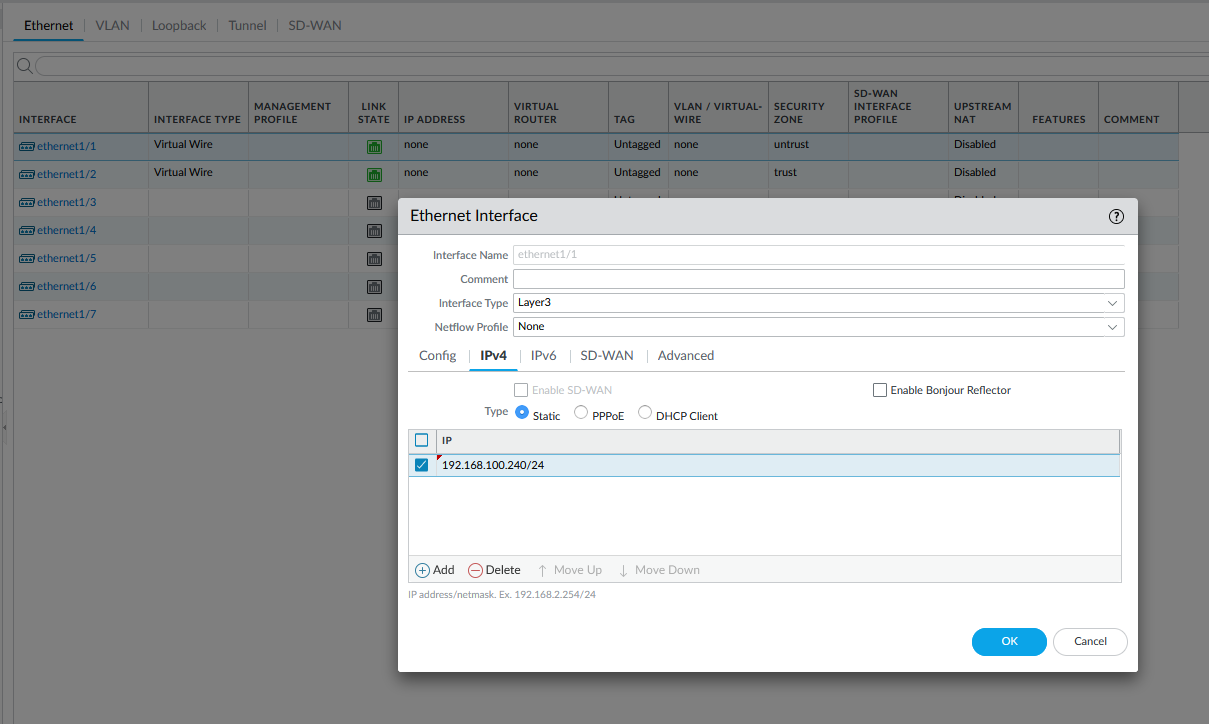
Config 1/1 int w/ default virtual router and type as layer 3



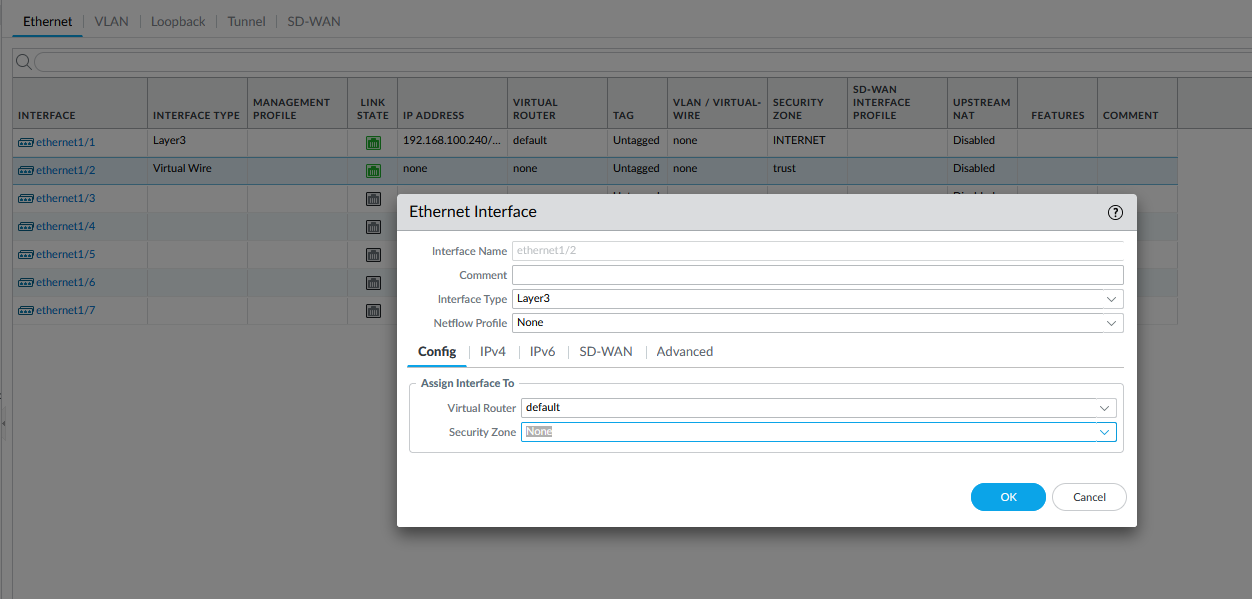
Put 1/1 in a new security zone called INTERNET



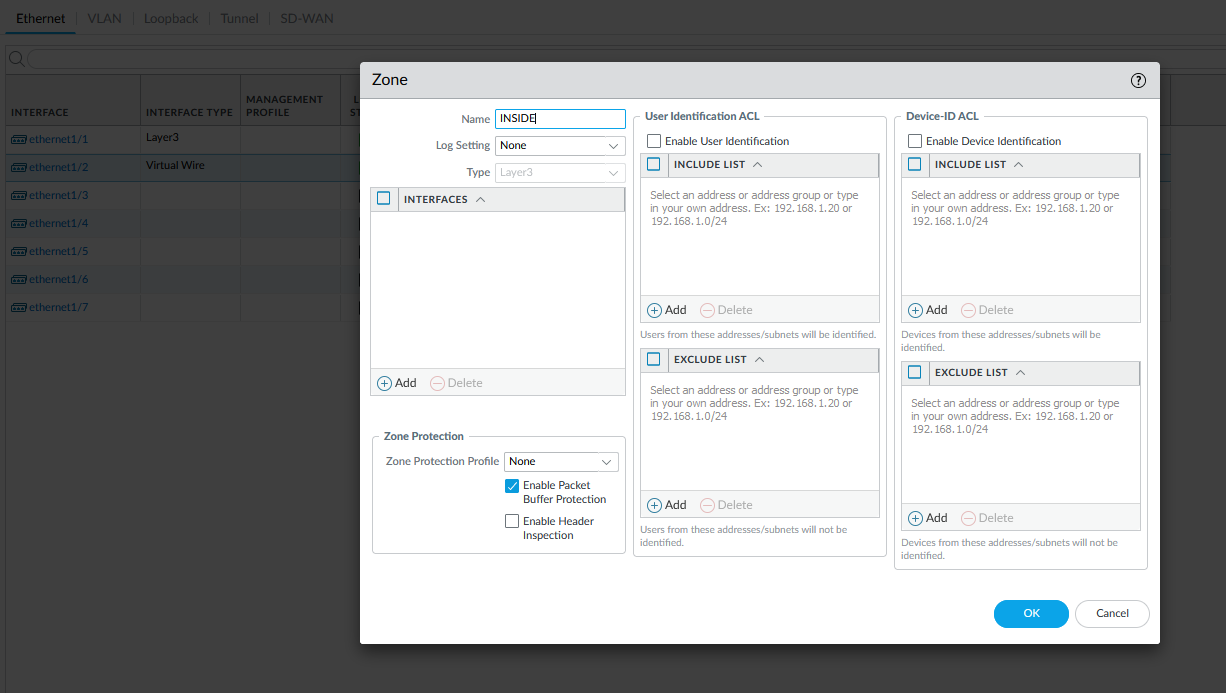
Put a static IP address on 1/1



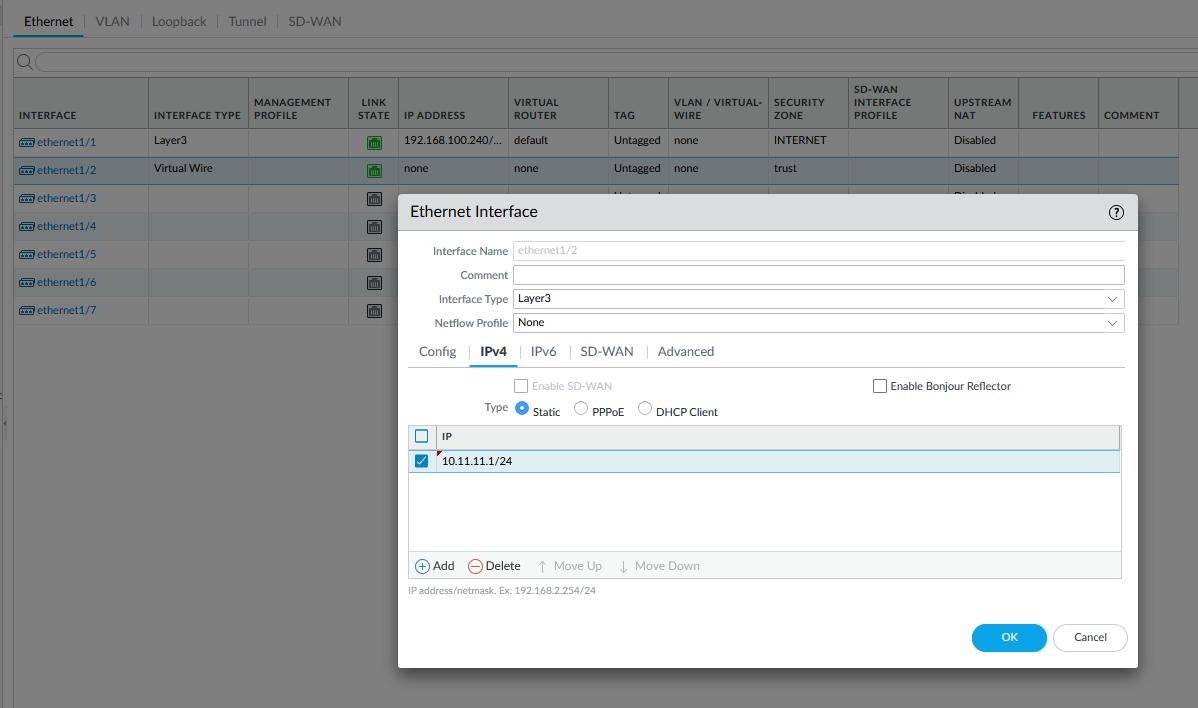
Conf 1/2 as Layer 3 with default virtual router



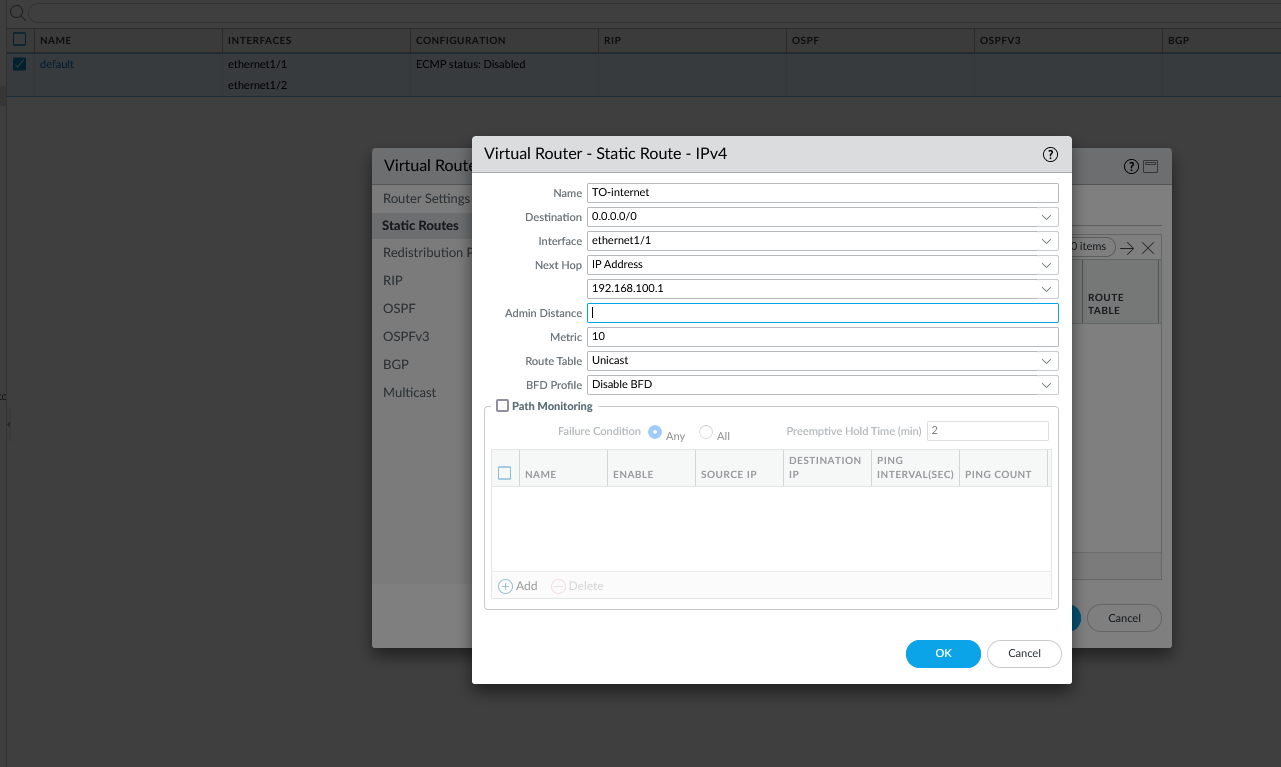
Put 1/2 in a new security zone call INSIDE



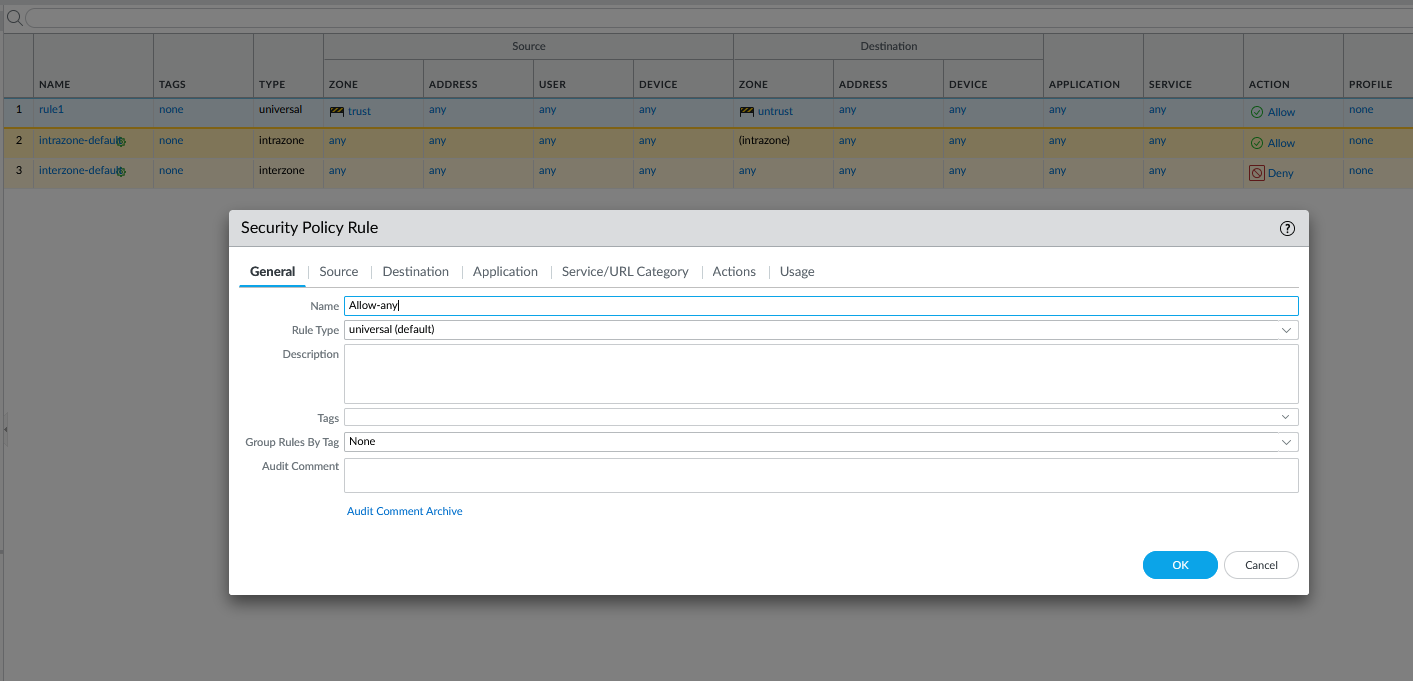
Set a static IP address



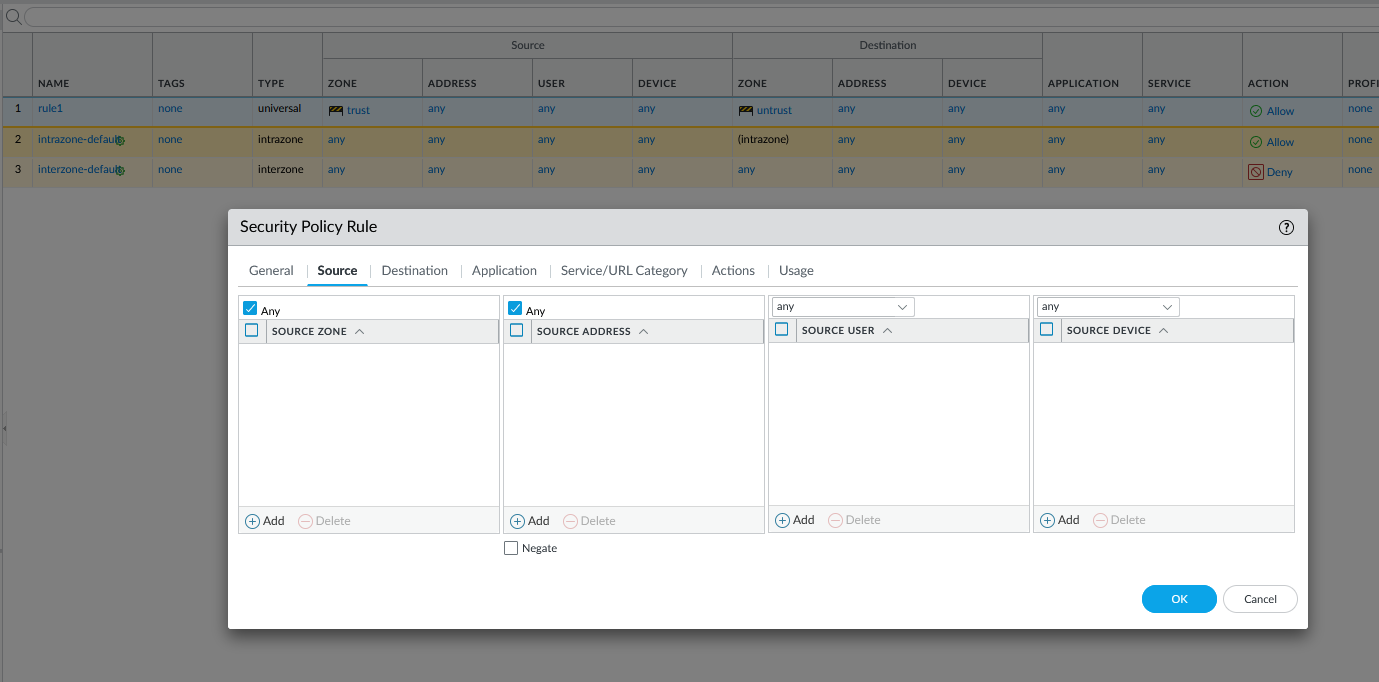
Create a default static router to the internet on the virtual router



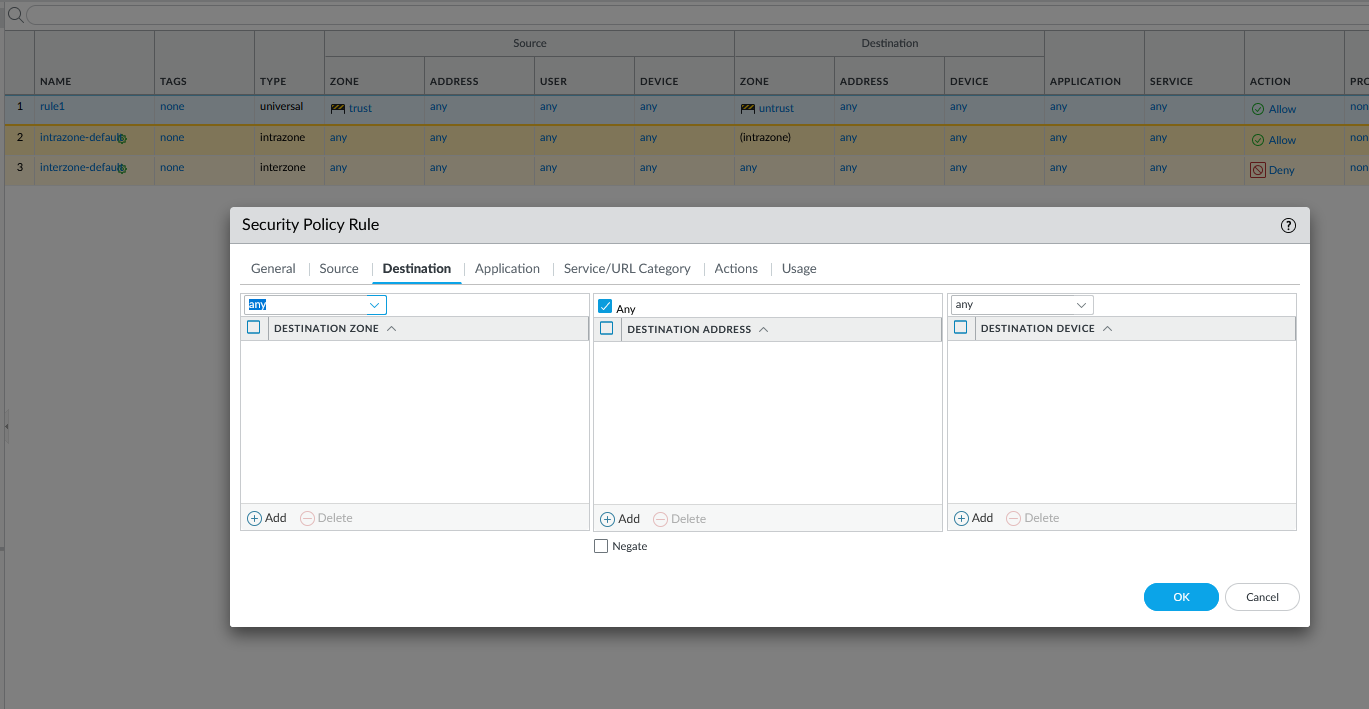
Edit the Security Policy Rule



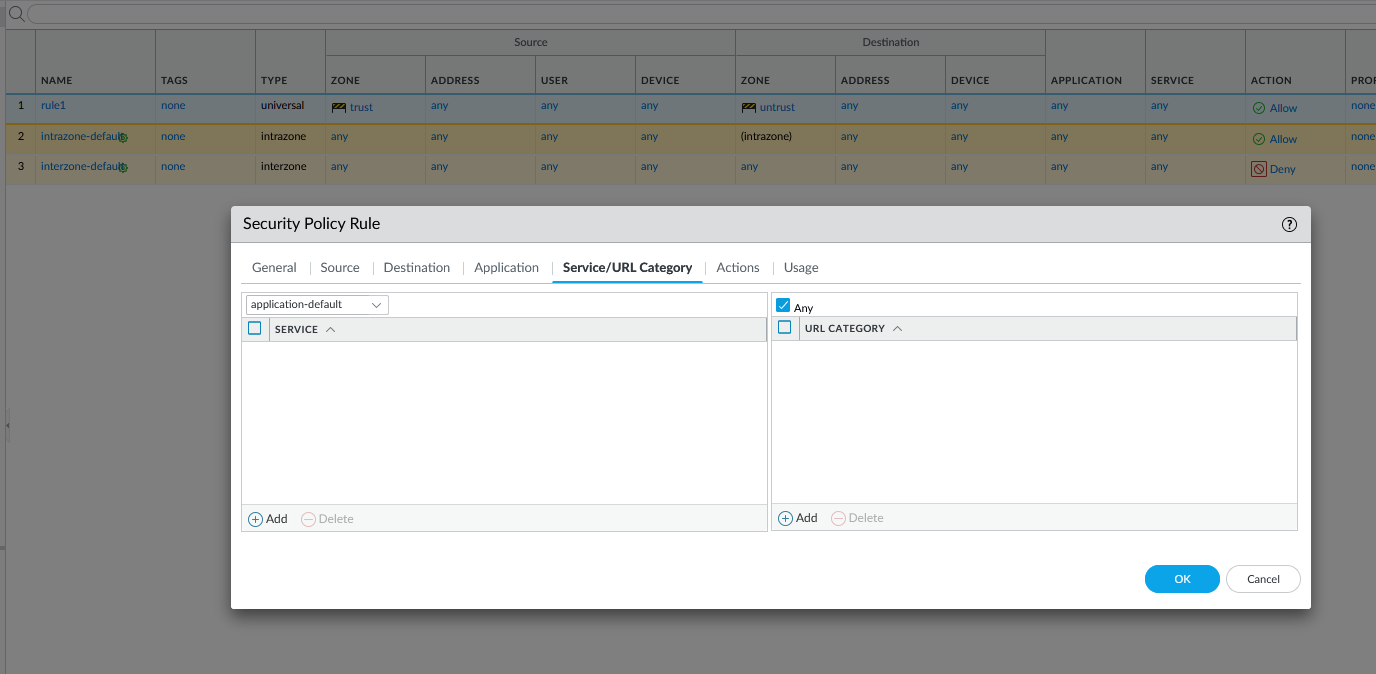
Make the source any



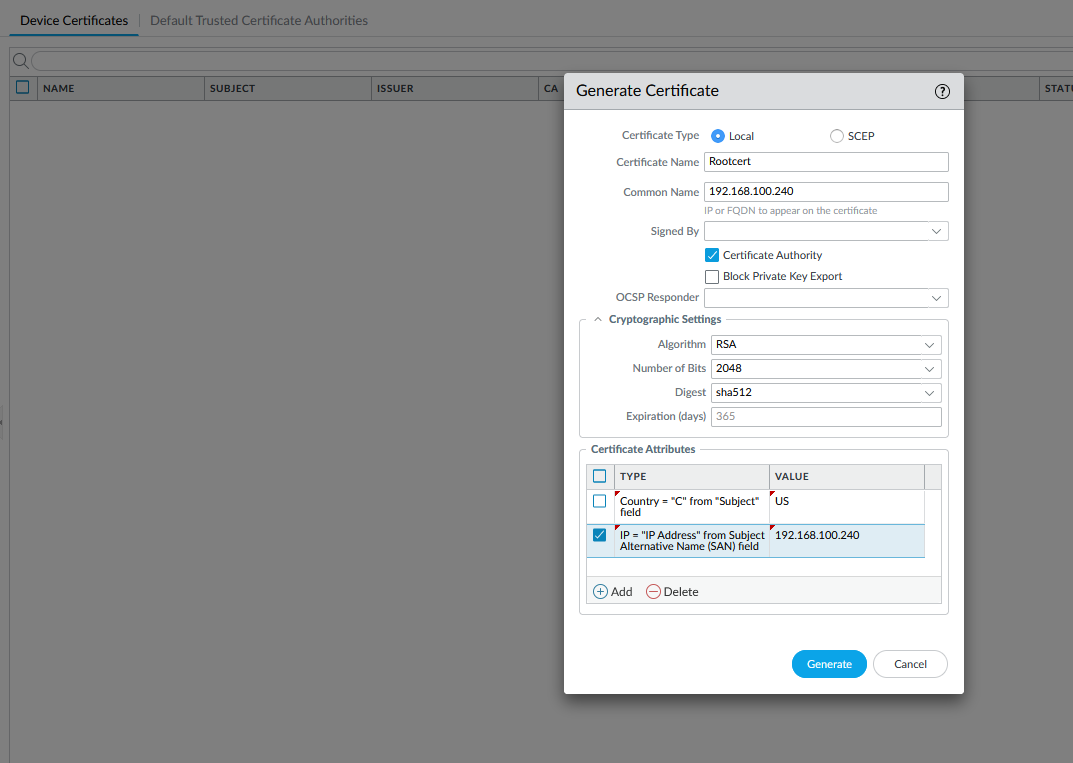
Make the destination Any



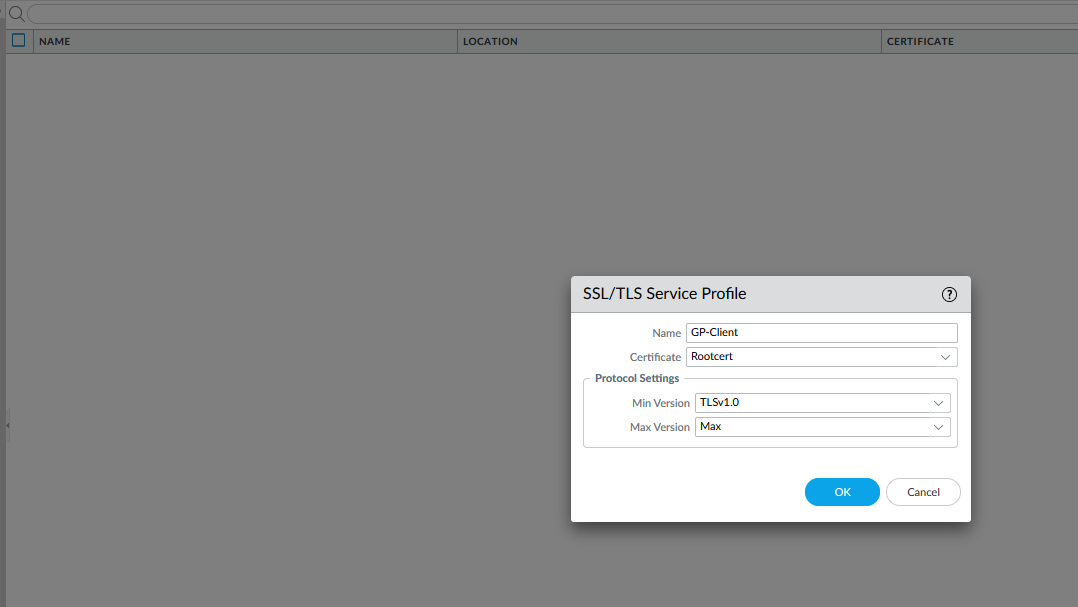
Service/URL Category as application-default and as any in the URL category



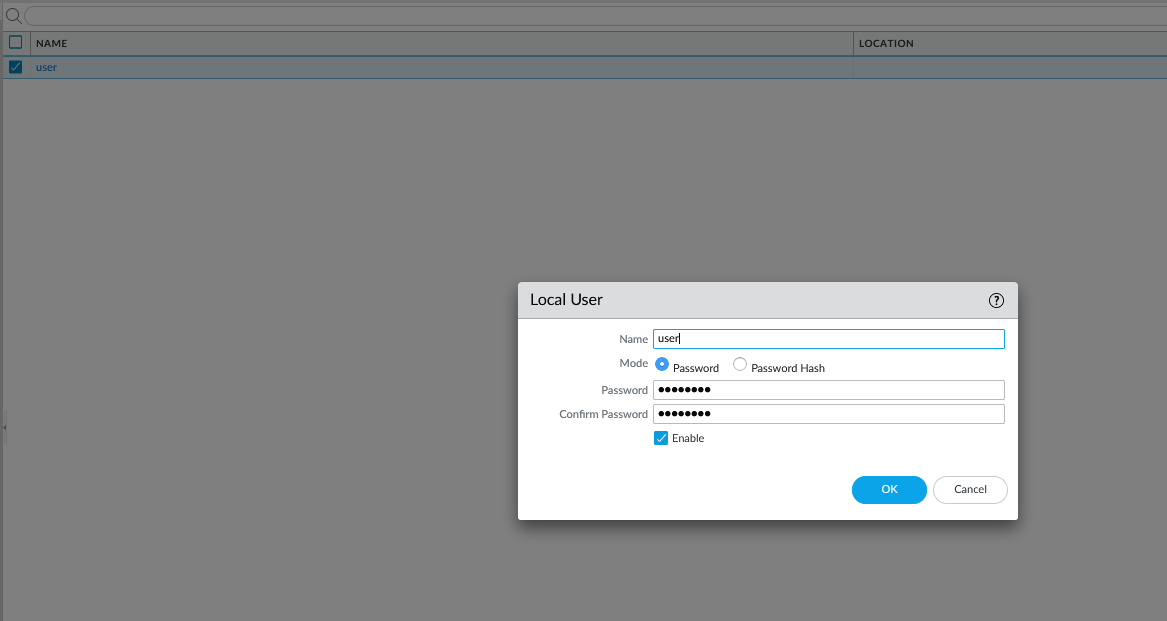
Generate Certificate



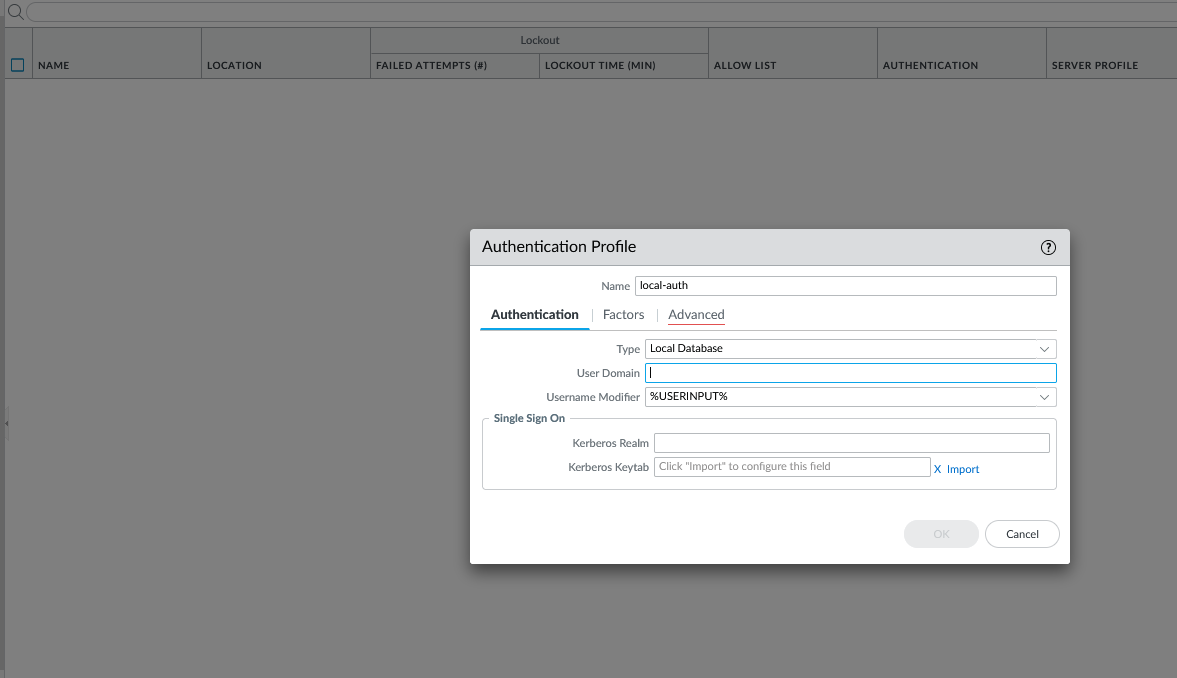
Create a new SSL/TLS Service Profile



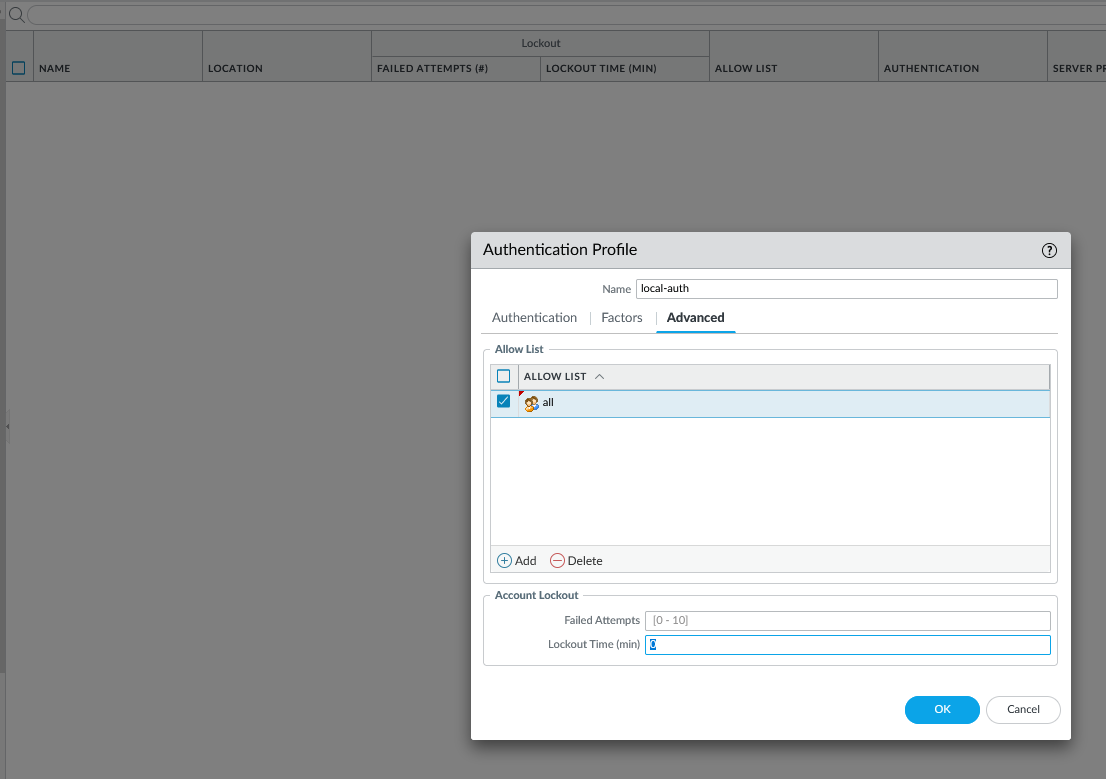
Create a new User profile



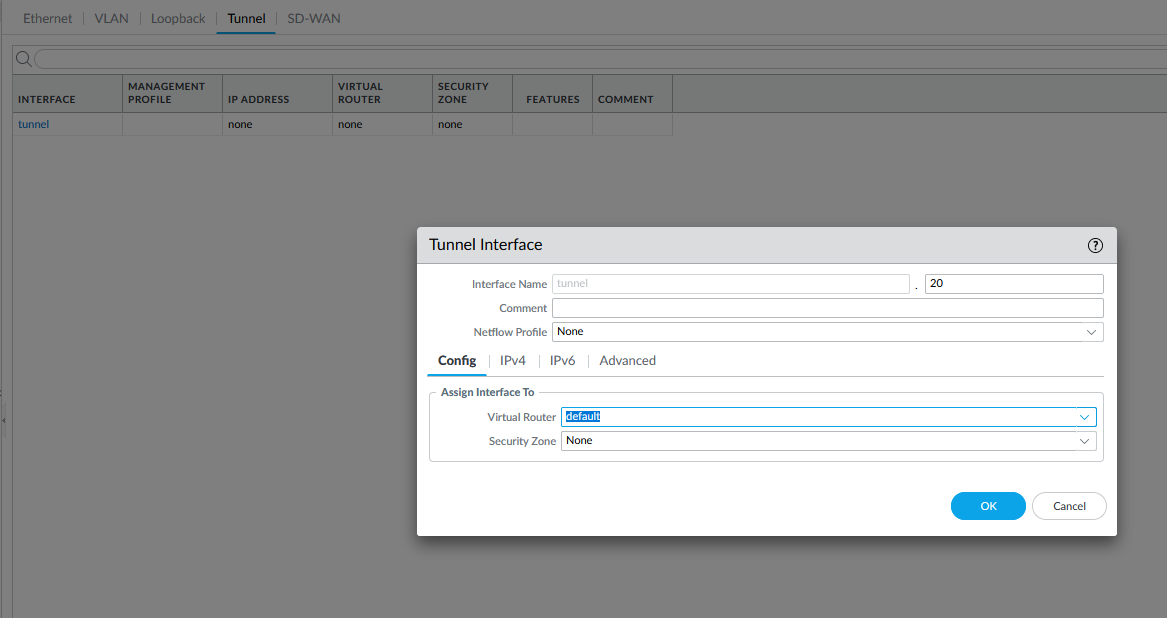
Create a new Authentication Profile



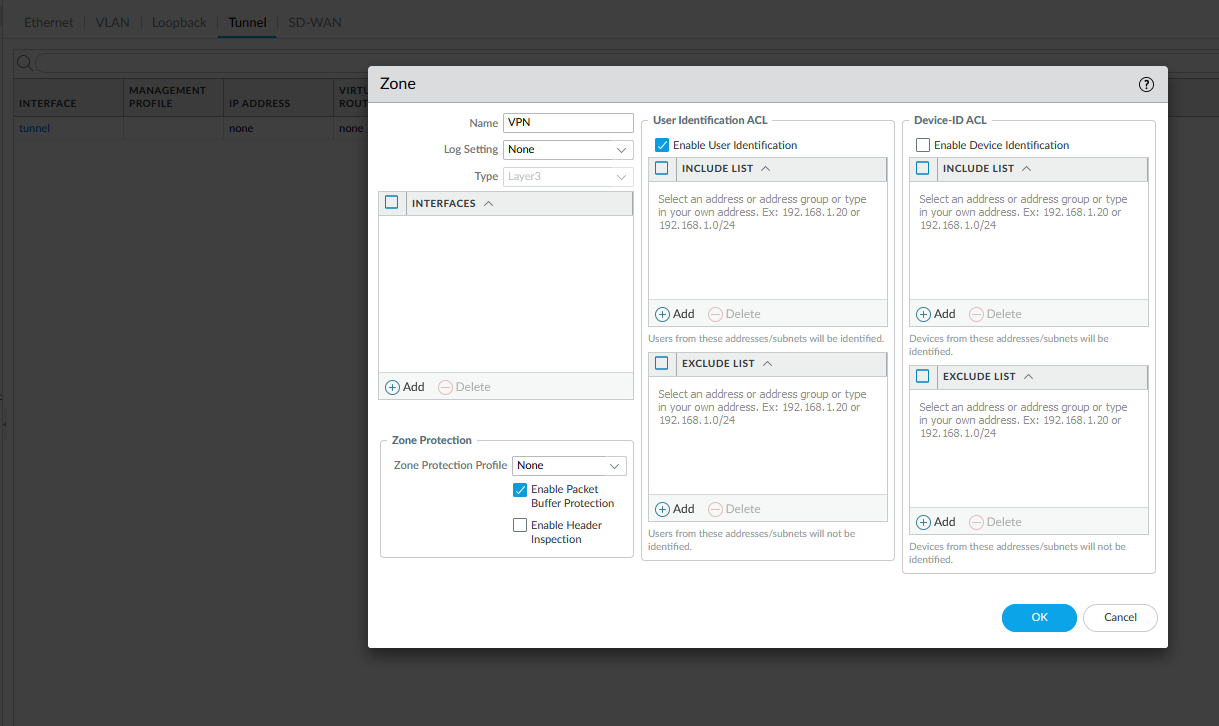
Set the Allow list to all



Create a new Tunnel Interface



Put that tunnel into a new zone called VPN



Problems:

Are main and only issue was getting our firewall to get updates so we could use the latest version of global protect. We eventually ended up resting the firewall and then we were able to get new updates.