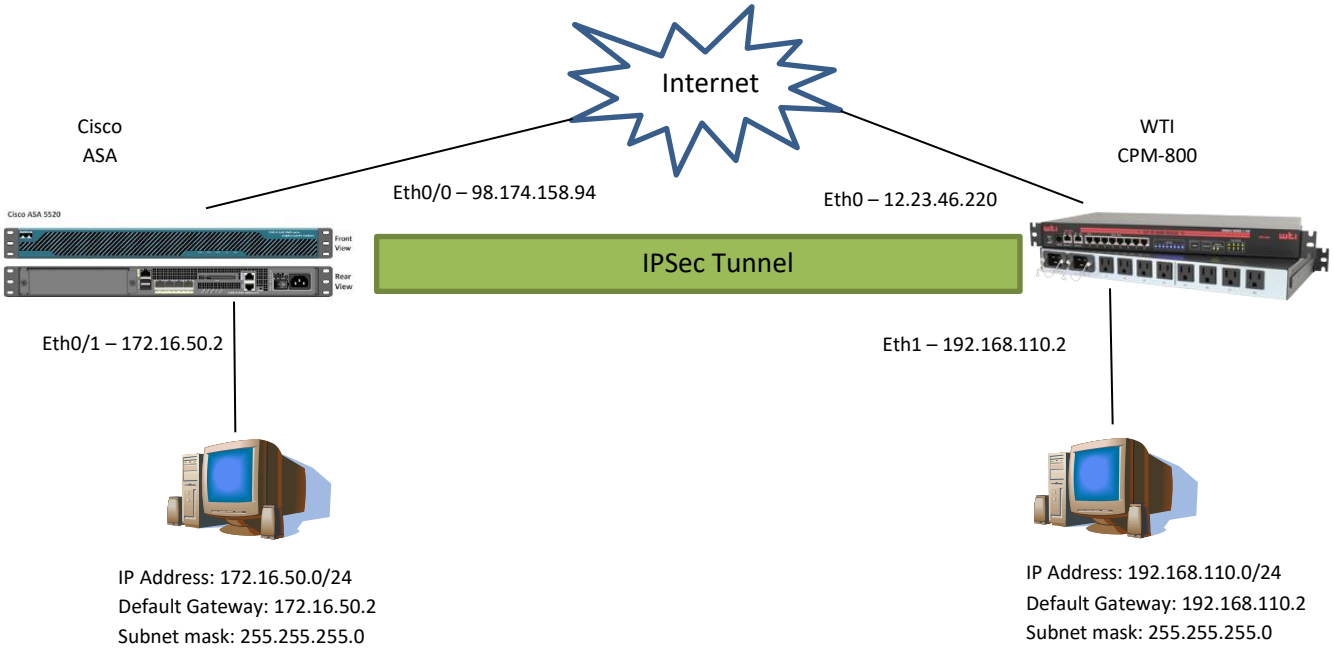
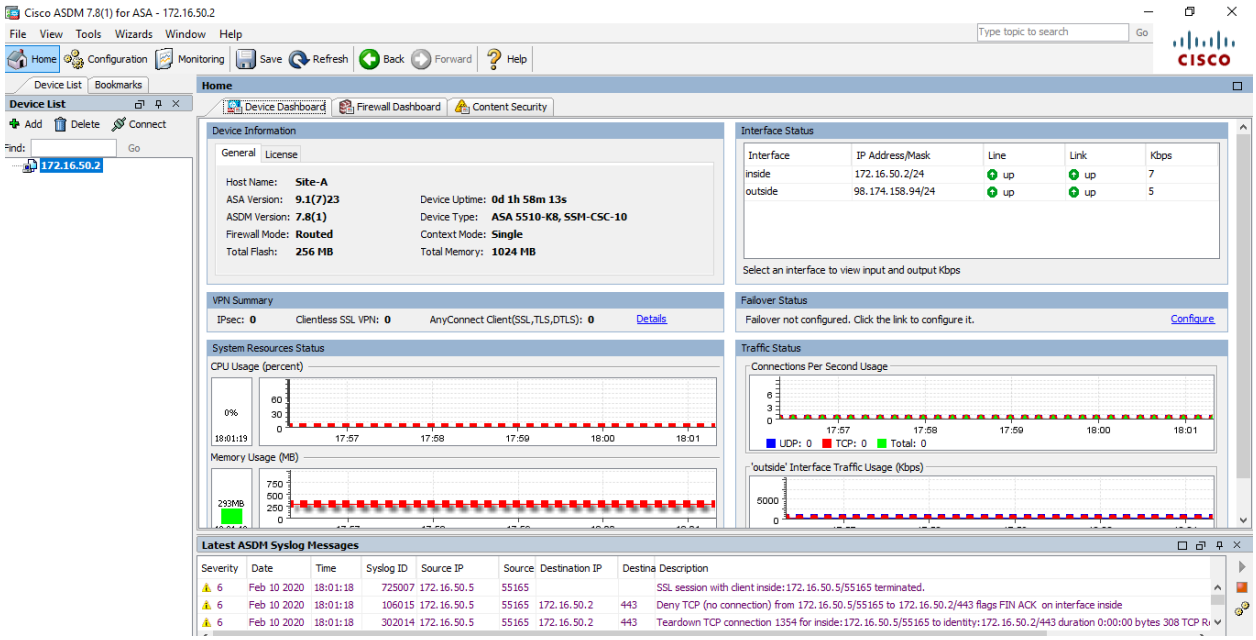
Cisco ASA5510 to WTI IPsec VPN



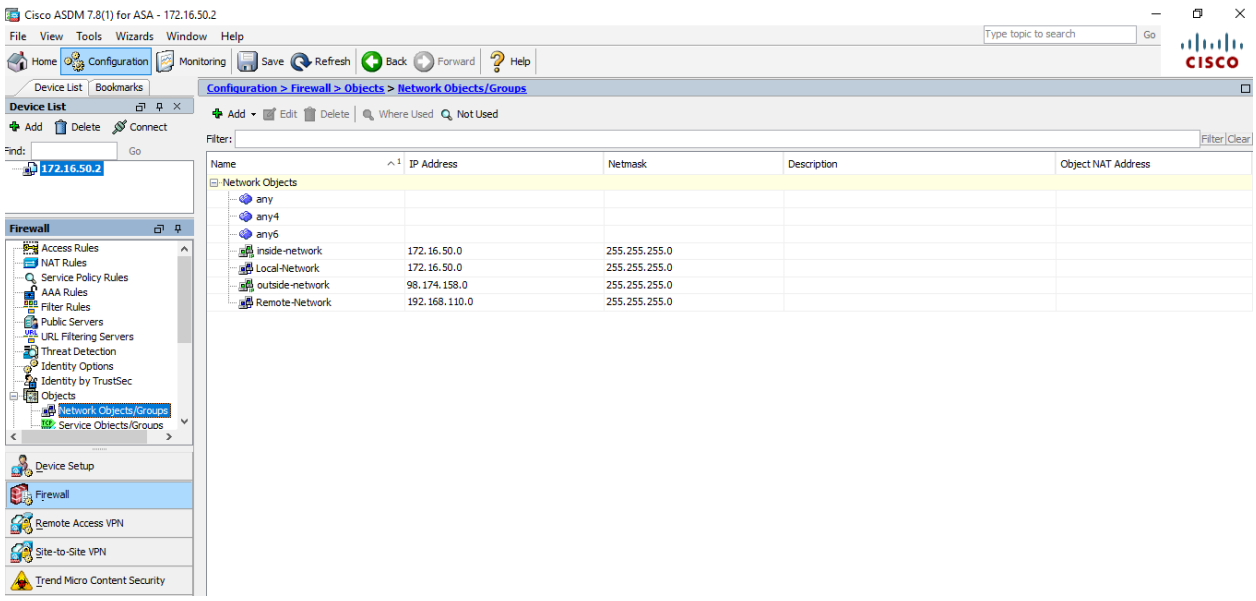
Cisco ASA Network Firewall	
Eth0/0 – Outside (WAN)	98.174.158.94
Eth0/1 – Inside (LAN)	172.16.50.2
Tunnel Group Name	12.23.46.220 (Tunnel Name)
Local Network	192.168.110.0/24
Remote Network	172.16.50.0/24
WTI Network	
Eth0 – Outside (WAN)	12.23.46.220
Eth1 – Inside (LAN)	192.168.110.2
Tunnel Name	12.23.46.220 (Tunnel Name)
Local Network	192.168.110.0/24
Remote Network	172.16.50.0/24

Cisco ASA5510

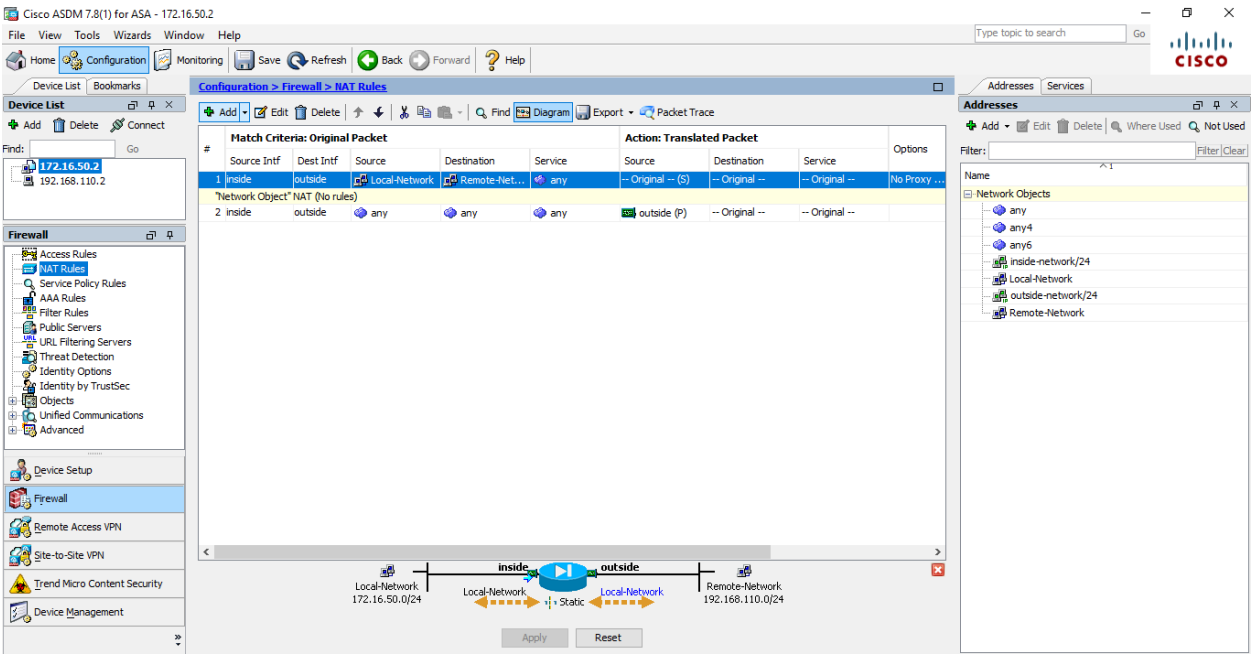
1. ASDM Home Overview.
   ASA Version 9.1(7)23
   ASDM Version 7.8(1)



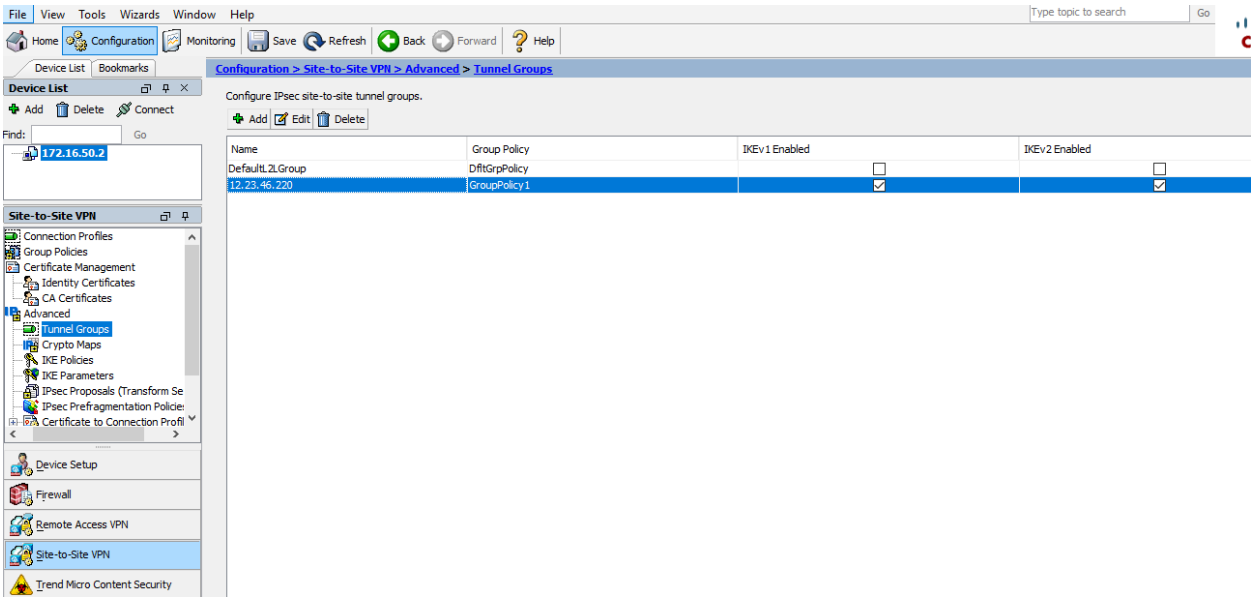
2. Firewall Network Object/Group Overview



3. Firewall NAT Rule Overview

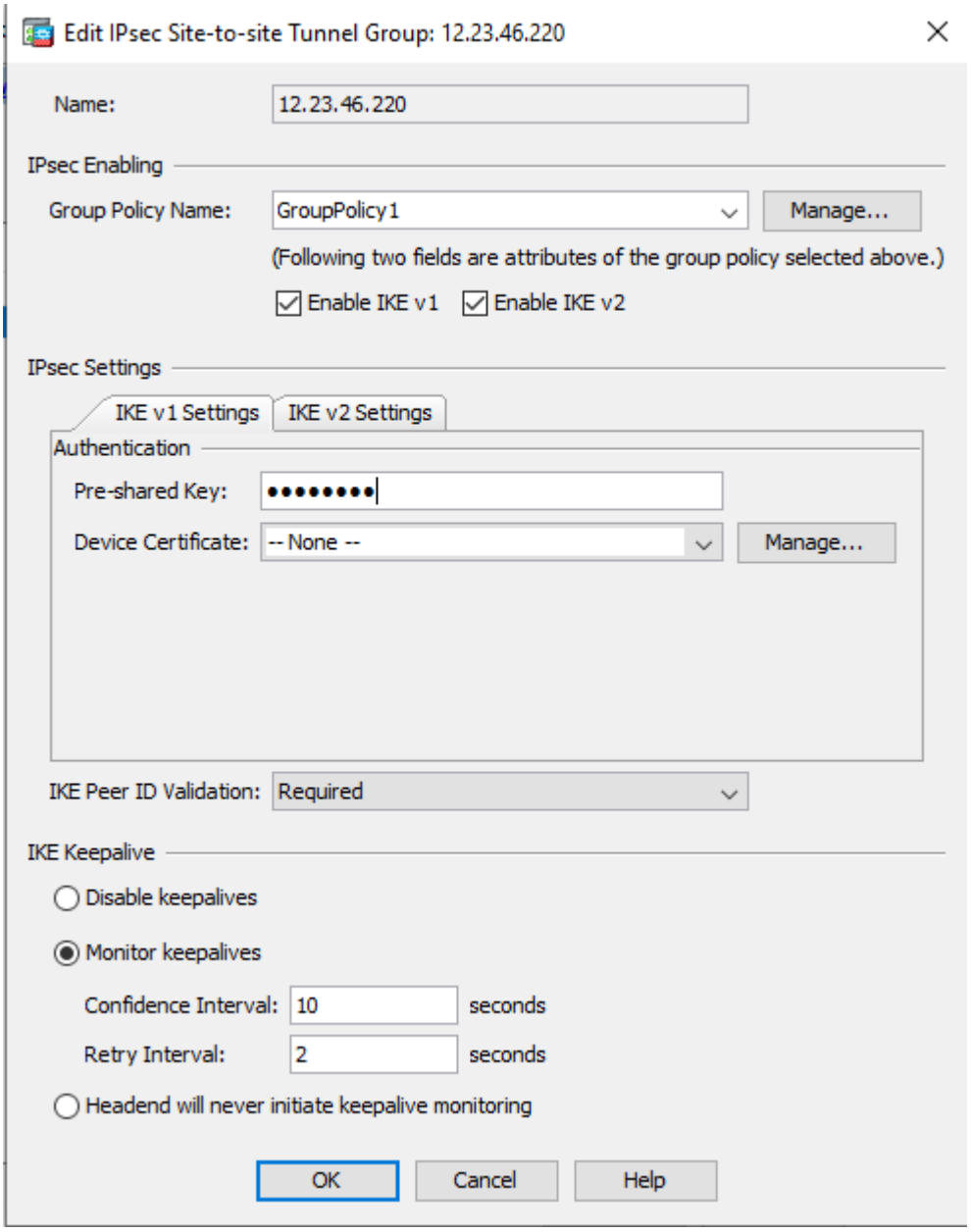


4. In Site-To-Site VPN Tunnel Group section overview. As Example, we're creating a tunnel group name as the peer ip address **12.23.46.220**.

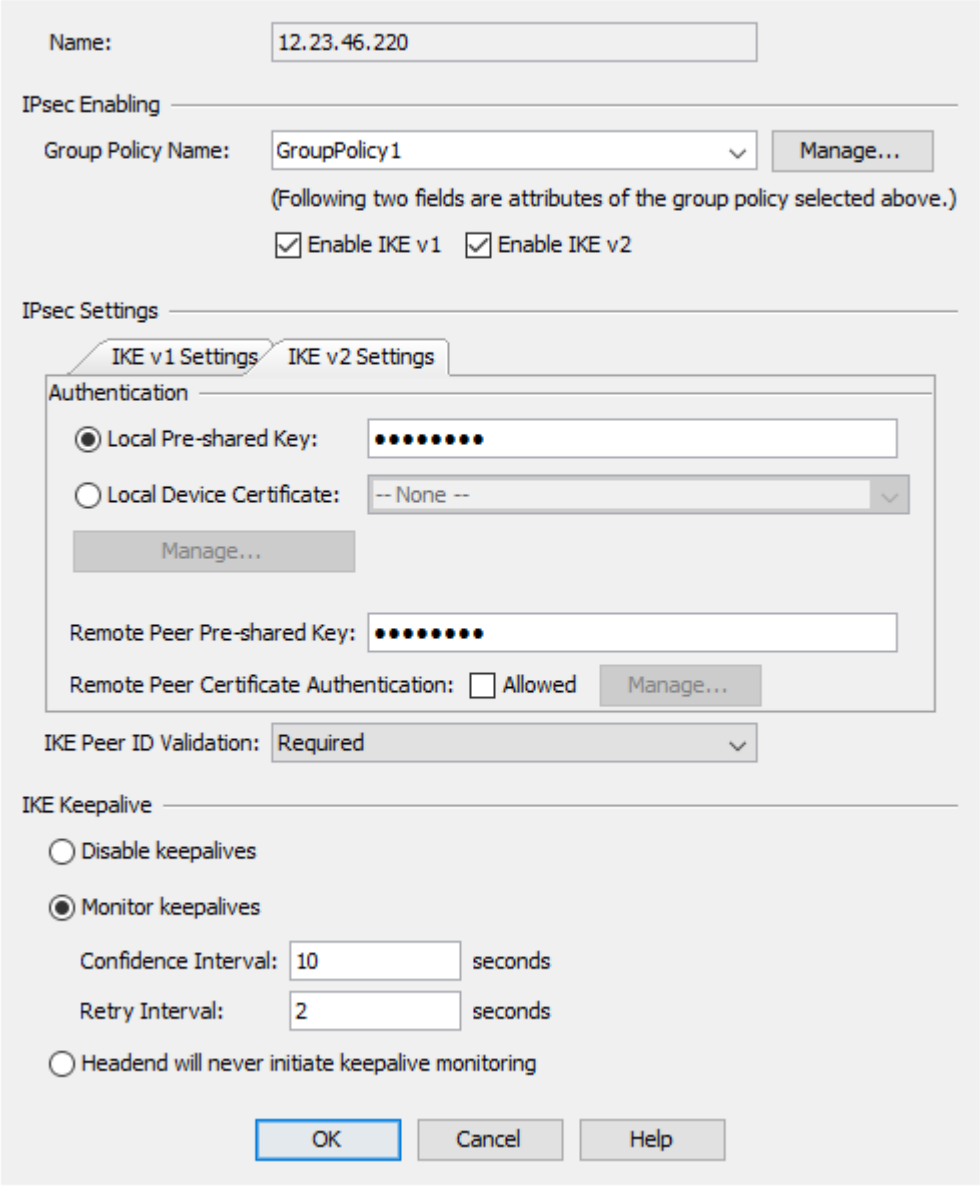


Click Add to create a tunnel group name. As example we're using a pre-shared-key on both IKEv1 and IKEv2 as **cisco123**

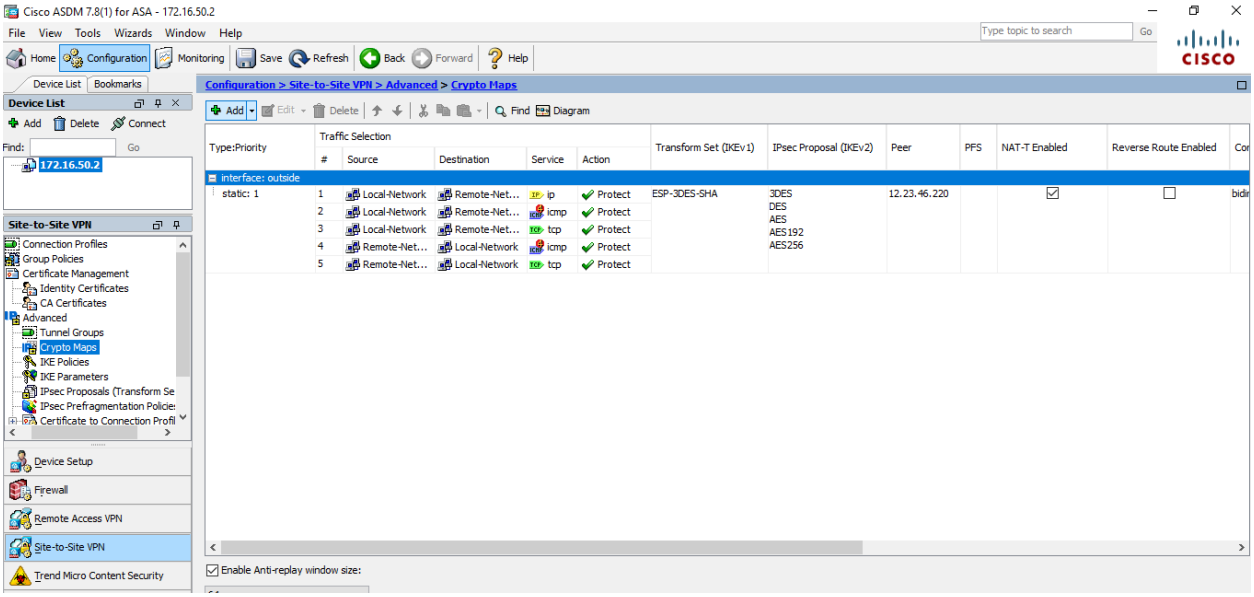
IKE v1 setting



IKE v2 setting

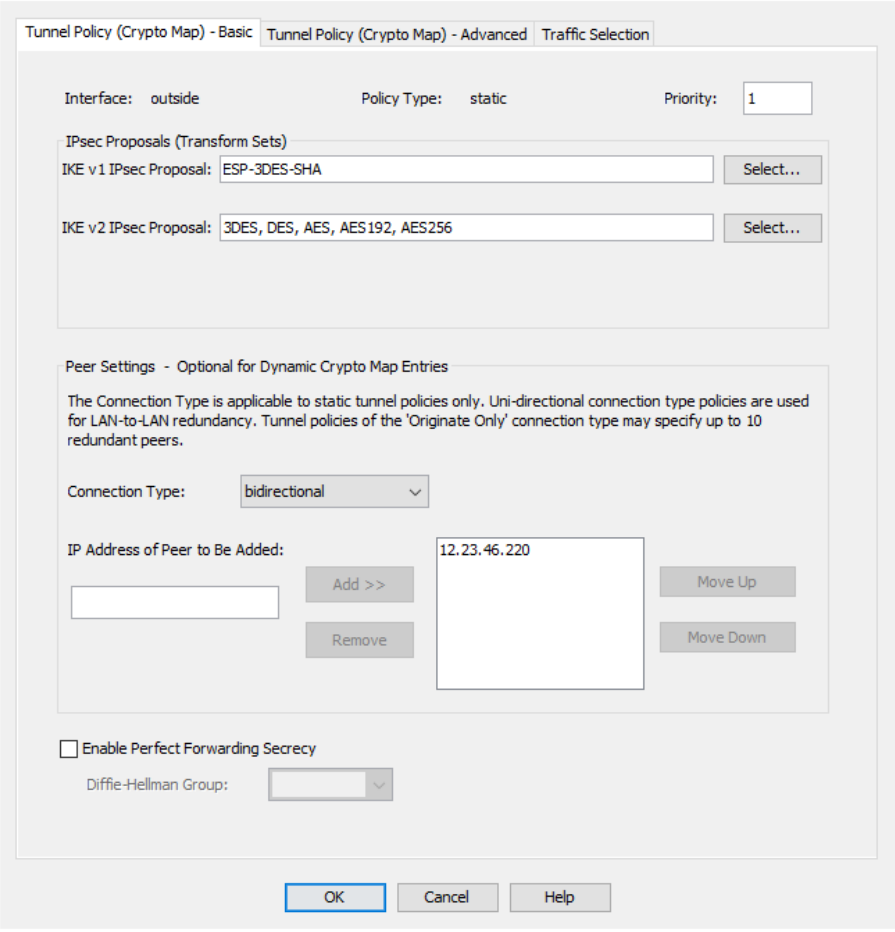


5. Crypto Map Section overview

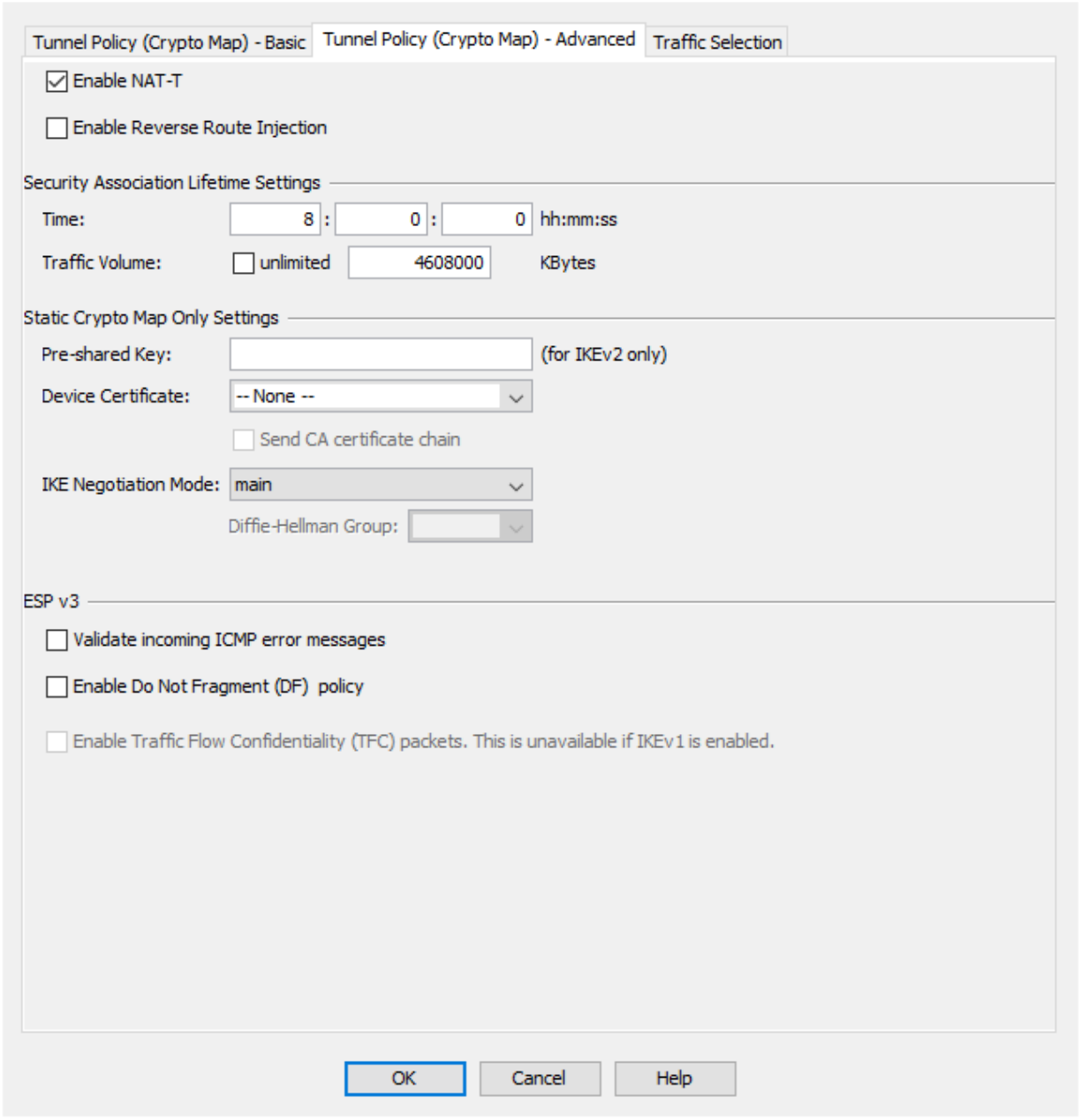


Click Add to create crypto map.

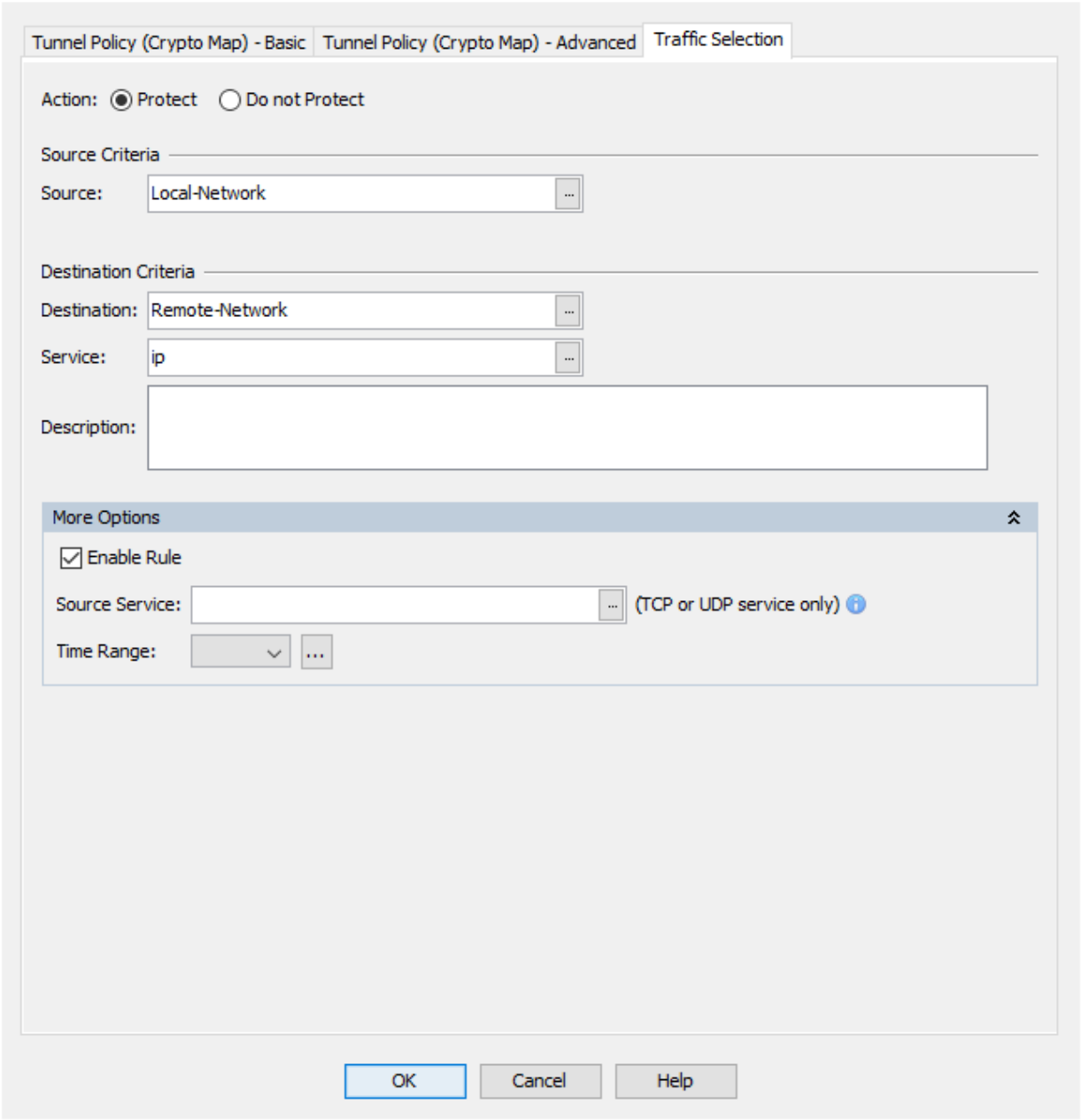
In Tunnel Policy (Crypto Map) - Basic Tap



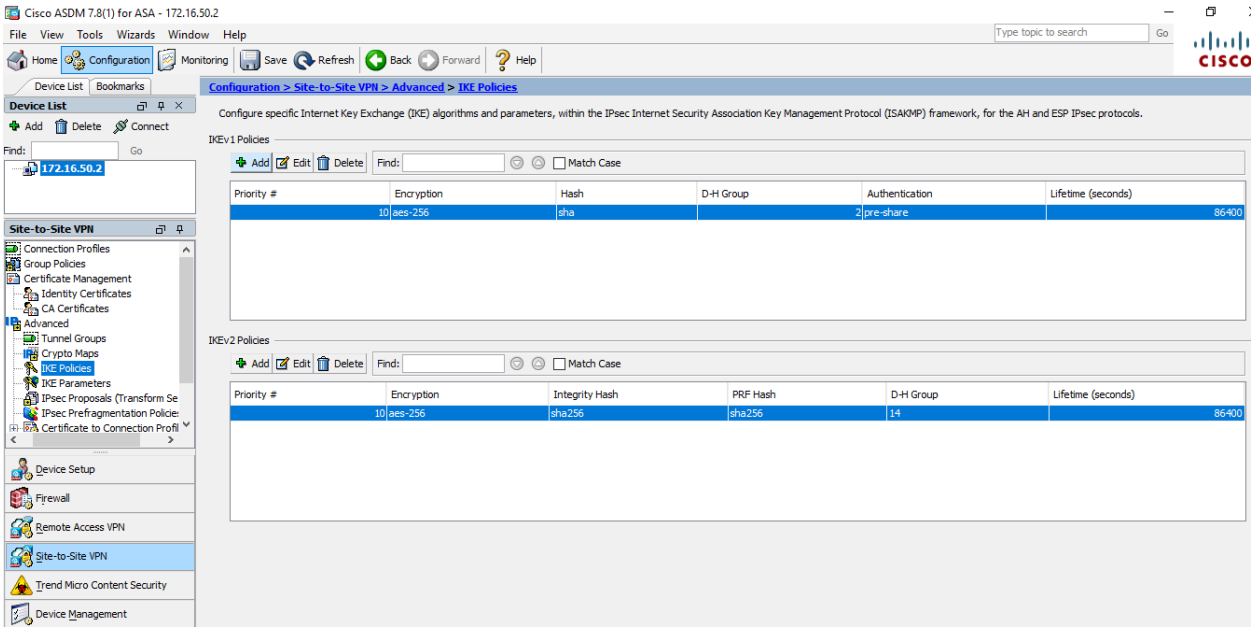
In Tunnel Policy (Crypto Map) - Advance



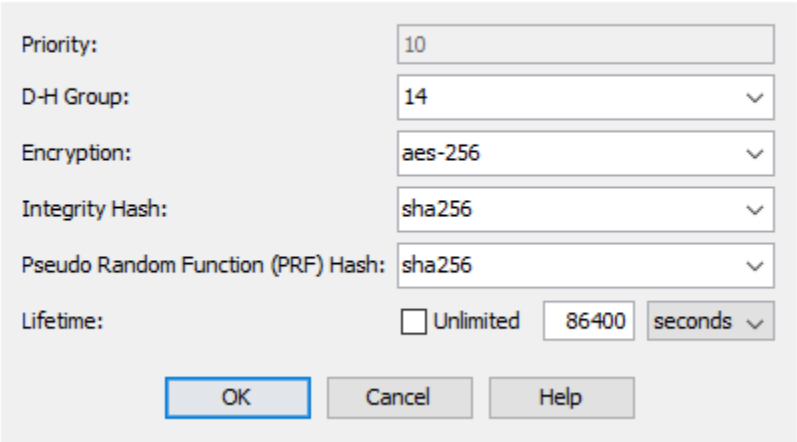
In traffic Section



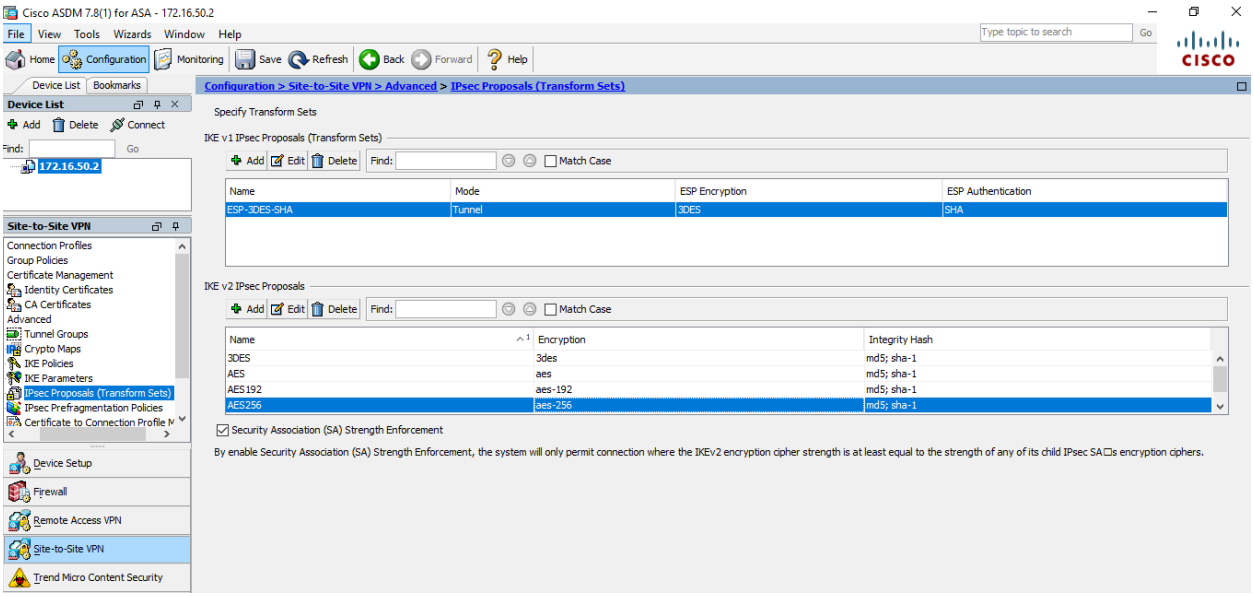
6. IKE Policy Section overview. In IKE Policy section we're using IKEv2 Policy.



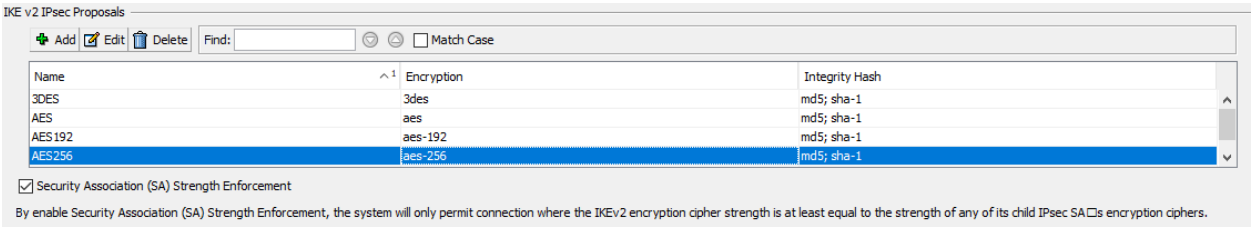
In IKEv2 Policy click Add to create a policy and apply the setting as below screenshot.



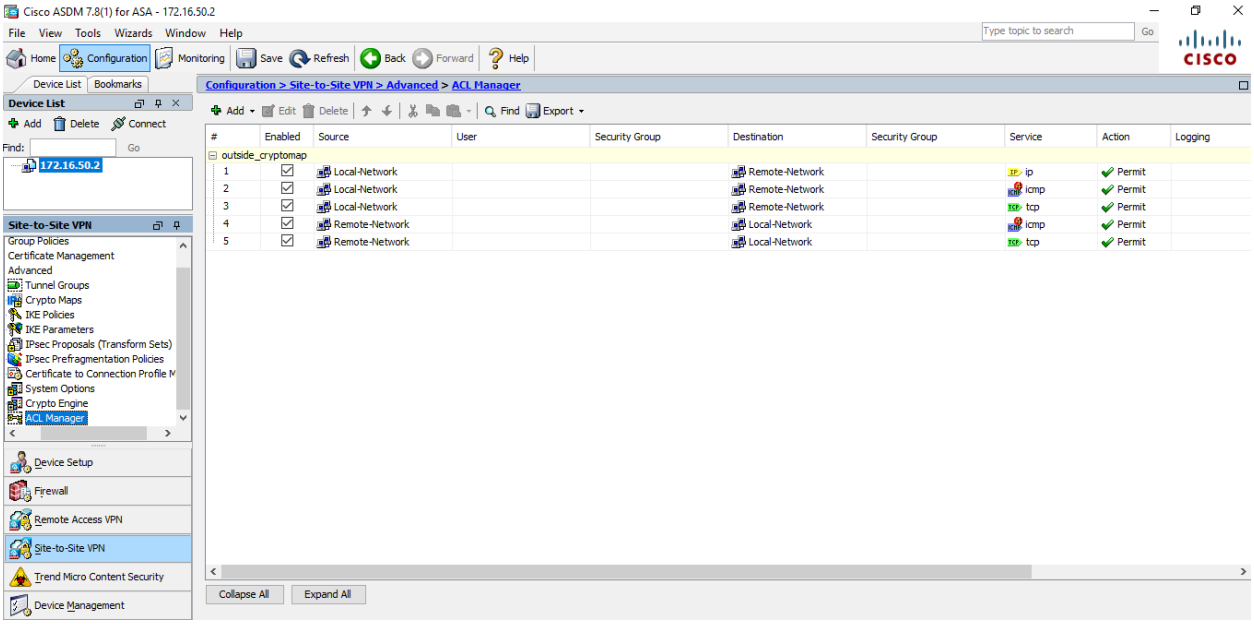
7. In IPsec Proposals (Transform set) overview.



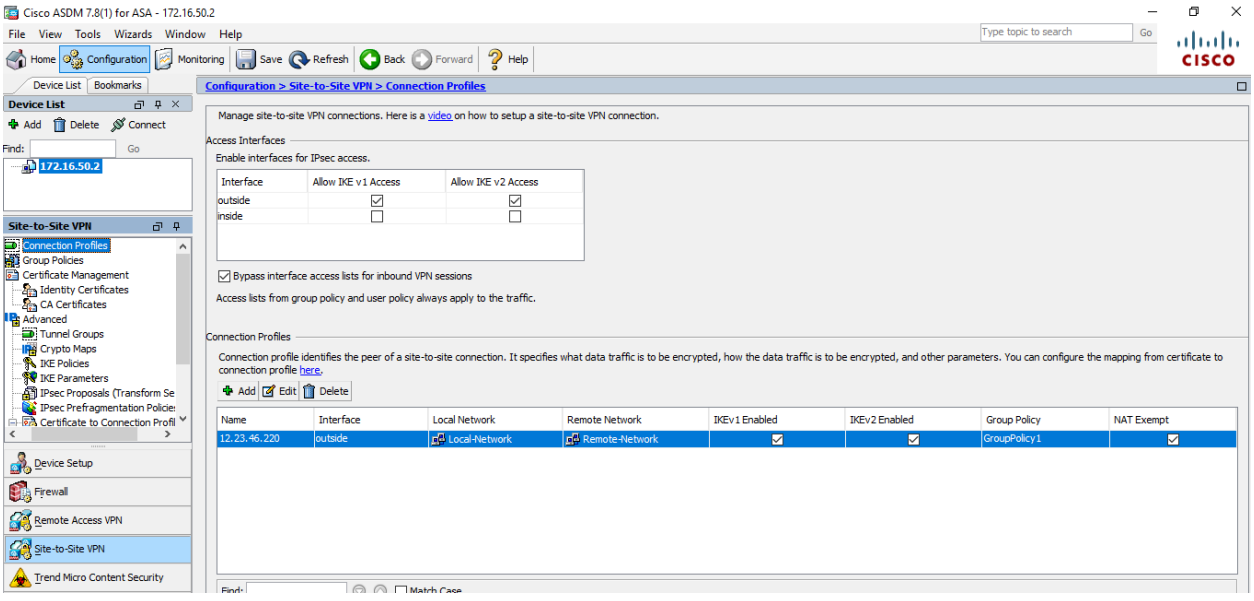
We're using IKE v2 IPsec Proposal.



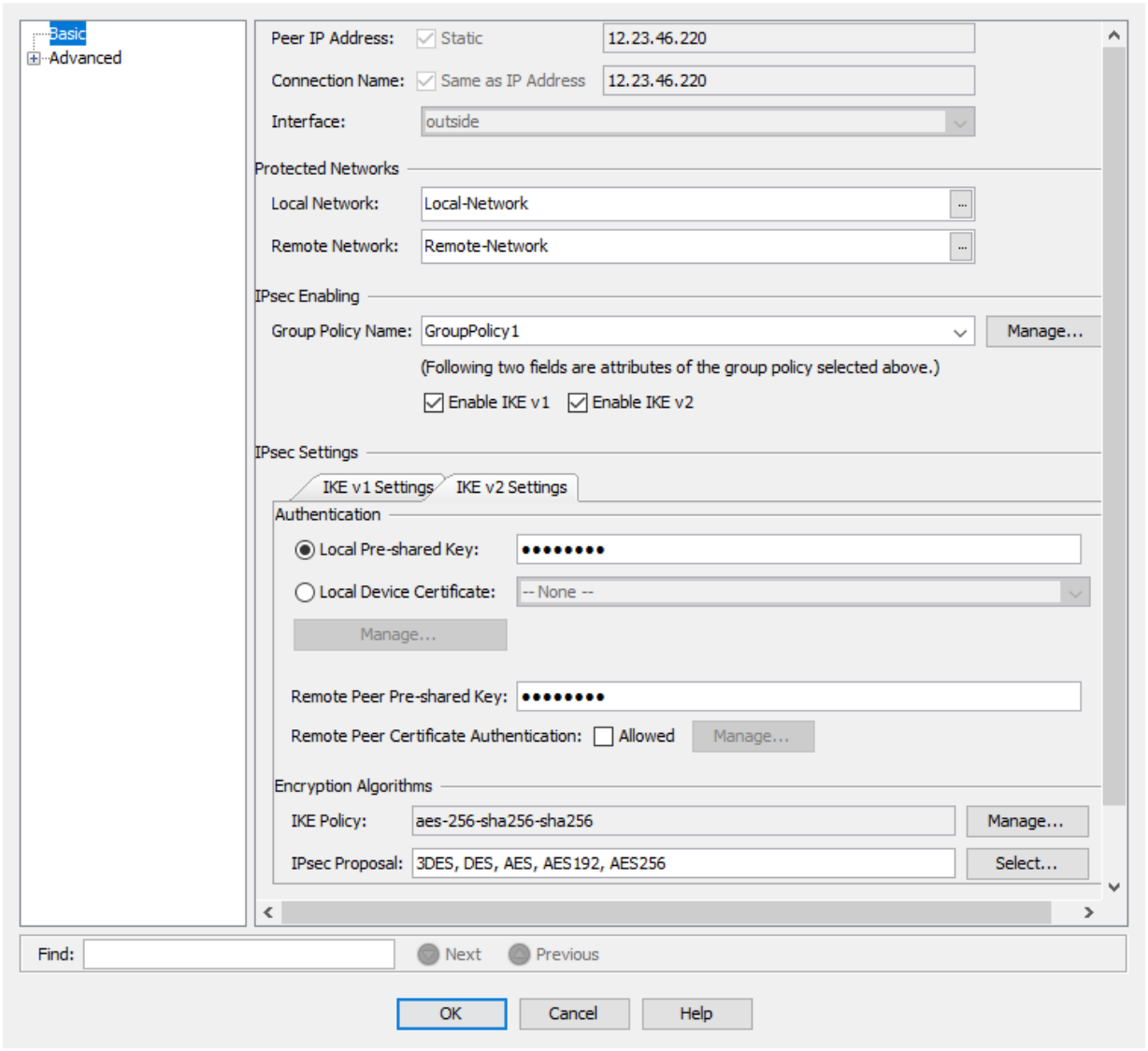
8. ACL Manager Overview



9. Connection Profile section overview.



Click Add to create IPsec connect profile as below. We're using IKE v2 as example.



WTI unit

In VPN Option IPsec (Client Site-To-Site)

IPSEC_CLIENT VPN DETAILS [12.23.46.220]		
Enable:	On	
Tunnel Name:	12.23.46.220	
Security:	Pre-shared Secret (Static Key File)	
Authentication Type:	ESP	
Left Address:	12.23.46.220	# WTI outside address
Left ID:	12.23.46.220	# IKEID Sent by WTI
Left Subnet:	192.168.110.0/24	# Subnet Local Network behind WTI
Right Address:	98.174.158.94	# Cisco ASA outside address
Right ID:	98.174.158.94	# IKEID Sent by Cisco ASA
Right Subnet:	172.16.50.0/24	# Subnet Local Network behind Cisco ASA
Tunnel Options:	(Show Options)	
Option 1:	keyexchange	ikev2
Option 2:	ike	aes128-sha256-modp2048
Option 3:	esp	aes256-sha1
Pre-Shared Key	cisco123	
Change VPN Parameters		

Set IPTABLES on Eth0

Example:

Eth0 is outside (WAN)
Eth1 is inside (LAN)

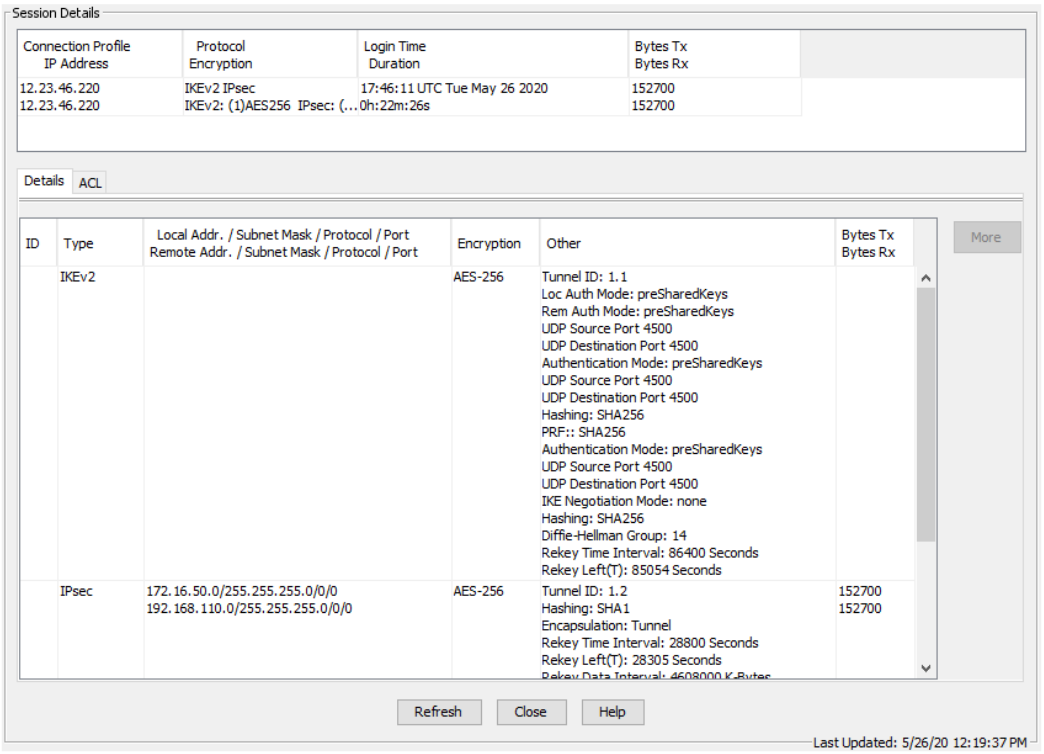
1. **iptables -A INPUT -i eth1 -j ACCEPT** #Allow traffic from the LAN side
2. **iptables -A INPUT -i eth0 -j ACCEPT** #Always accept loopback traffic
3. **iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT** #Allow established connections
4. **iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE** #Masquerade
5. **iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT** #Forwarding
6. **iptables -A FORWARD -i eth1 -o eth0 -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

Verify the connection by issuing a command in WTI unit.

/bash ipsec status

```
CPM> /bash ipsec status
Security Associations (1 up, 0 connecting):
12.23.46.220[1]: ESTABLISHED 4 minutes ago, 12.23.46.220[12.23.46.220]...98.174.158.94[98.174.158.94]
12.23.46.220{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c2ccce97_i 8e7d2b1e_o
12.23.46.220{1}:   192.168.110.0/24 === 172.16.50.0/24
```

Cisco ASA Monitoring Session



Cisco ASA 5510 Command line

```
ASA Version 9.1(7)23
!
hostname Site-A
names
!
interface Ethernet0/0
 description COX Internet
 nameif outside
 security-level 0
 ip address 98.174.158.94 255.255.255.0
!
interface Ethernet0/1
 description ITLAB
 nameif inside
 security-level 100
 ip address 172.16.50.2 255.255.255.0
!
object network Local-Network
  subnet 172.16.50.0 255.255.255.0
object network Remote-Network
  subnet 192.168.110.0 255.255.255.0

access-list outside_cryptomap extended permit ip object Local-Network object Remote-Network
access-list outside_cryptomap extended permit icmp object Local-Network object Remote-Network
access-list outside_cryptomap extended permit tcp object Local-Network object Remote-Network
```

```
access-list outside_cryptomap extended permit icmp object Remote-Network object Local-Network
access-list outside_cryptomap extended permit tcp object Remote-Network object Local-Network

nat (inside,outside) source static Local-Network Local-Network destination static Remote-Network
Remote-Network no-proxy-arp route-lookup

nat (inside,outside) after-auto source dynamic any interface

!

router eigrp 100

 network 172.16.50.0 255.255.255.0

!

route outside 0.0.0.0 0.0.0.0 98.174.158.1 1

crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev2 ipsec-proposal 3DES


crypto map outside_map0 1 match address outside_cryptomap
crypto map outside_map0 1 set peer 12.23.46.220

crypto map outside_map0 1 set ikev1 transform-set ESP-3DES-SHA
crypto map outside_map0 1 set ikev2 ipsec-proposal 3DES DES AES AES192 AES256
crypto map outside_map0 interface outside
crypto ca trustpoint _SmartCallHome_ServerCA

crypto ikev2 policy 10
  encryption aes-256
  integrity sha256
   group 14
   prf sha256
   lifetime seconds 86400

crypto ikev2 enable outside
crypto ikev1 enable outside

crypto ikev1 policy 10
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

```
group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes

 vpn-tunnel-protocol ikev1 ikev2

tunnel-group 12.23.46.220 type ipsec-l2l
tunnel-group 12.23.46.220 general-attributes
  default-group-policy GroupPolicy1

tunnel-group 12.23.46.220 ipsec-attributes
  ikev1 pre-shared-key cisco123
  ikev2 remote-authentication pre-shared-key cisco123
  ikev2 local-authentication pre-shared-key cisco123

policy-map global-policy
  class class-default
  inspect icmp

!
```