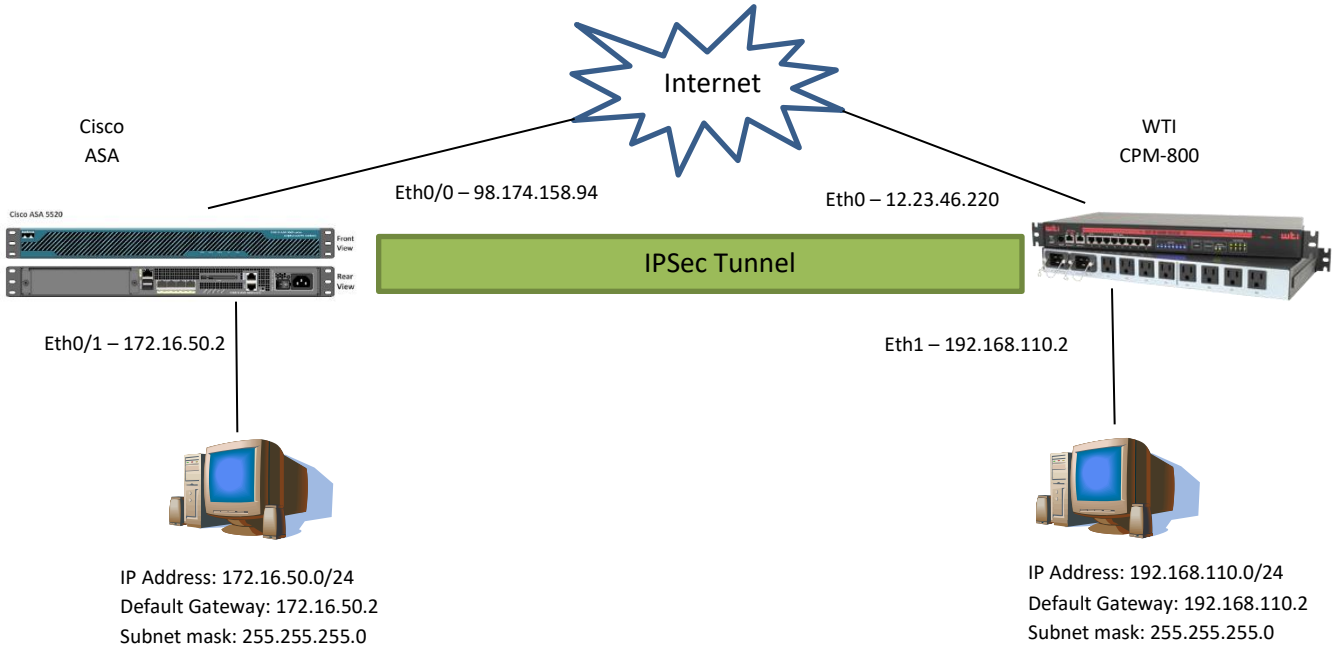


Cisco ASA5510 to WTI IPsec VPN



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)

The screenshot displays the Cisco ASDM Home Overview for ASA 172.16.50.2. The interface includes a navigation pane on the left with options like Home, Configuration, and Monitoring. The main content area is divided into several sections:

- Device Information:** Host Name: Site-A, ASA Version: 9.1(7)23, ASDM Version: 7.8(1), Firewall Mode: Routed, Total Flash: 256 MB, Device Uptime: 0d 1h 58m 13s, Device Type: ASA 5510-K8, SSH-CSC-10, Context Mode: Single, Total Memory: 1024 MB.
- Interface Status:** A table showing interface details for 'inside' and 'outside'.
- VPN Summary:** IPsec: 0, Clientless SSL VPN: 0, AnyConnect Client(SSL,TLS,DTLS): 0.
- System Resources Status:** CPU Usage (percent) and Memory Usage (MB) graphs.
- Failover Status:** Failover not configured.
- Traffic Status:** Connections Per Second Usage and 'outside' Interface Traffic Usage (Kbps) graphs.
- Latest ASDM Syslog Messages:** A table of recent log entries.

Interface	IP Address/Mask	Line	Link	Kbps
inside	172.16.50.2/24	up	up	7
outside	98.174.158.94/24	up	up	5

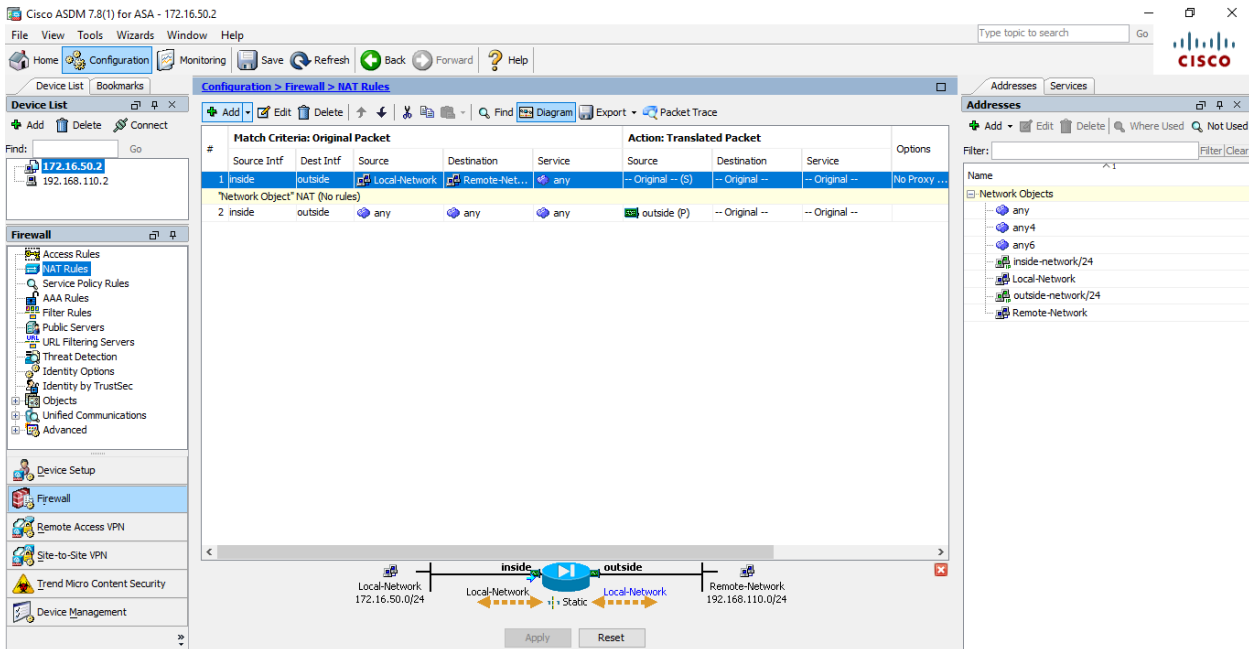
Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	Feb 10 2020	18:01:18	725007	172.16.50.5	55165	172.16.50.2	443	SSL session with client inside:172.16.50.5/55165 terminated.
6	Feb 10 2020	18:01:18	106015	172.16.50.5	55165	172.16.50.2	443	Deny TCP (no connection) from 172.16.50.5/55165 to 172.16.50.2/443 flags FIN ACK on interface inside
6	Feb 10 2020	18:01:18	302014	172.16.50.5	55165	172.16.50.2	443	Tear-down TCP connection 1394 for inside:172.16.50.5/55165 to identity:172.16.50.2/443 duration 0:00:00 bytes 308 TCP R...

2. Firewall Network Object/Group Overview

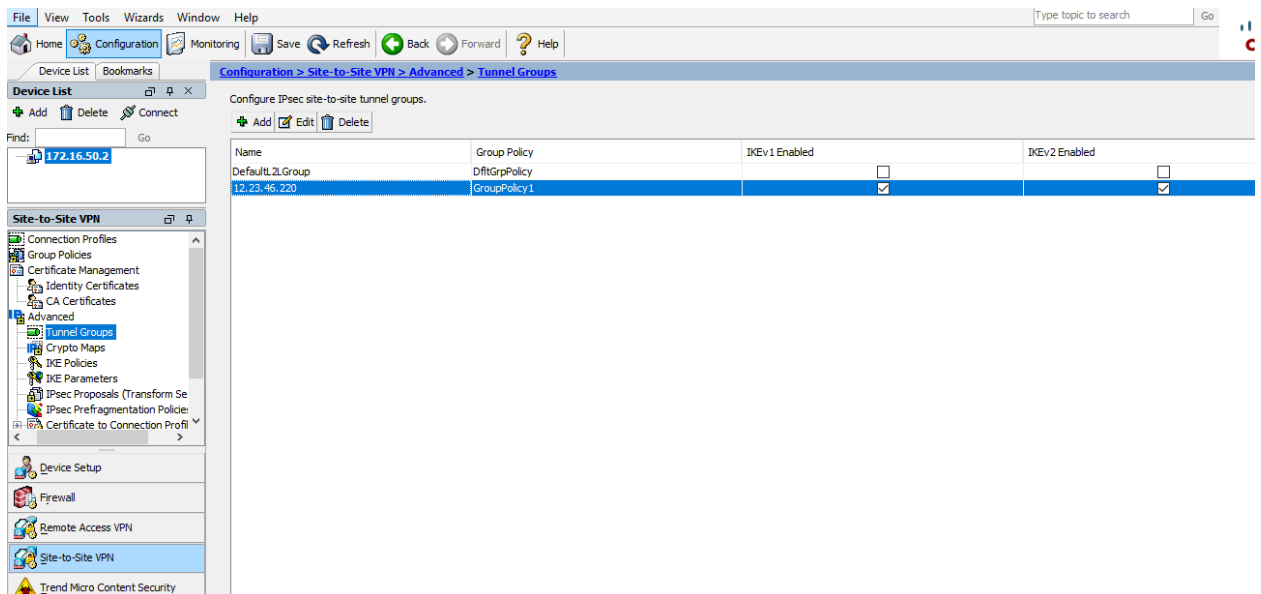
The screenshot displays the Cisco ASDM Firewall Network Object/Group Overview for ASA 172.16.50.2. The interface shows a list of network objects with columns for Name, IP Address, Netmask, Description, and Object NAT Address.

Name	IP Address	Netmask	Description	Object NAT Address
any				
any4				
any6				
inside-network	172.16.50.0	255.255.255.0		
Local-Network	172.16.50.0	255.255.255.0		
outside-network	98.174.158.0	255.255.255.0		
Remote-Network	192.168.110.0	255.255.255.0		

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

Edit IPsec Site-to-site Tunnel Group: 12.23.46.220 ✕

Name:

IPsec Enabling

Group Policy Name: Manage...

(Following two fields are attributes of the group policy selected above.)

Enable IKE v1 Enable IKE v2

IPsec Settings

IKE v1 Settings IKE v2 Settings

Authentication

Pre-shared Key:

Device Certificate: Manage...

IKE Peer ID Validation:

IKE Keepalive

Disable keepalives

Monitor keepalives

Confidence Interval: seconds

Retry Interval: seconds

Headend will never initiate keepalive monitoring

OK Cancel Help

IKE v2 setting

Name:

IPsec Enabling

Group Policy Name:

(Following two fields are attributes of the group policy selected above.)

Enable IKE v1 Enable IKE v2

IPsec Settings

IKE v1 Settings IKE v2 Settings

Authentication

Local Pre-shared Key:

Local Device Certificate:

Remote Peer Pre-shared Key:

Remote Peer Certificate Authentication: Allowed

IKE Peer ID Validation:

IKE Keepalive

Disable keepalives

Monitor keepalives

Confidence Interval: seconds

Retry Interval: seconds

Headend will never initiate keepalive monitoring

5. Crypto Map Section overview

The screenshot shows the Cisco ASDM 7.8(1) for ASA - 172.16.50.2 interface. The configuration path is Configuration > Site-to-Site VPN > Advanced > Crypto Maps. The left pane shows the 'Crypto Maps' configuration tree. The main area displays a table for the 'outside' interface with the following data:

Type:Priority	#	Source	Destination	Service	Action	Transform Set (IKEv1)	IPsec Proposal (IKEv2)	Peer	PFS	NAT-T Enabled	Reverse Route Enabled	Col
static: 1	1	Local-Network	Remote-Net...	ip	Protect	ESP-3DES-SHA	3DES	12.23.46.220		<input checked="" type="checkbox"/>	<input type="checkbox"/>	bid
	2	Local-Network	Remote-Net...	icmp	Protect		DES					
	3	Local-Network	Remote-Net...	tcp	Protect		AES					
	4	Remote-Net...	Local-Network	icmp	Protect		AES192					
	5	Remote-Net...	Local-Network	tcp	Protect		AES256					

Click Add to create crypto map.

In Tunnel Policy (Crypto Map) - Basic Tap

The screenshot shows the 'Tunnel Policy (Crypto Map) - Basic' configuration window. The configuration is as follows:

- Interface: outside
- Policy Type: static
- Priority: 1
- IPsec Proposals (Transform Sets):
 - IKE v1 IPsec Proposal: ESP-3DES-SHA
 - IKE v2 IPsec Proposal: 3DES, DES, AES, AES192, AES256
- Peer Settings - Optional for Dynamic Crypto Map Entries:
 - Connection Type: bidirectional
 - IP Address of Peer to Be Added: 12.23.46.220
- Enable Perfect Forwarding Secrecy:
- Diffie-Hellman Group: [Dropdown menu]

In Tunnel Policy (Crypto Map) - Advance

Tunnel Policy (Crypto Map) - Basic | **Tunnel Policy (Crypto Map) - Advanced** | Traffic Selection

Enable NAT-T

Enable Reverse Route Injection

Security Association Lifetime Settings

Time: : : hh:mm:ss

Traffic Volume: unlimited KBytes

Static Crypto Map Only Settings

Pre-shared Key: (for IKEv2 only)

Device Certificate: ▾

Send CA certificate chain

IKE Negotiation Mode: ▾

Diffie-Hellman Group: ▾

ESP v3

Validate incoming ICMP error messages

Enable Do Not Fragment (DF) policy

Enable Traffic Flow Confidentiality (TFC) packets. This is unavailable if IKEv1 is enabled.

In traffic Section

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | **Traffic Selection**

Action: Protect Do not Protect

Source Criteria

Source: Local-Network ...

Destination Criteria

Destination: Remote-Network ...

Service: ip ...

Description:

More Options ^

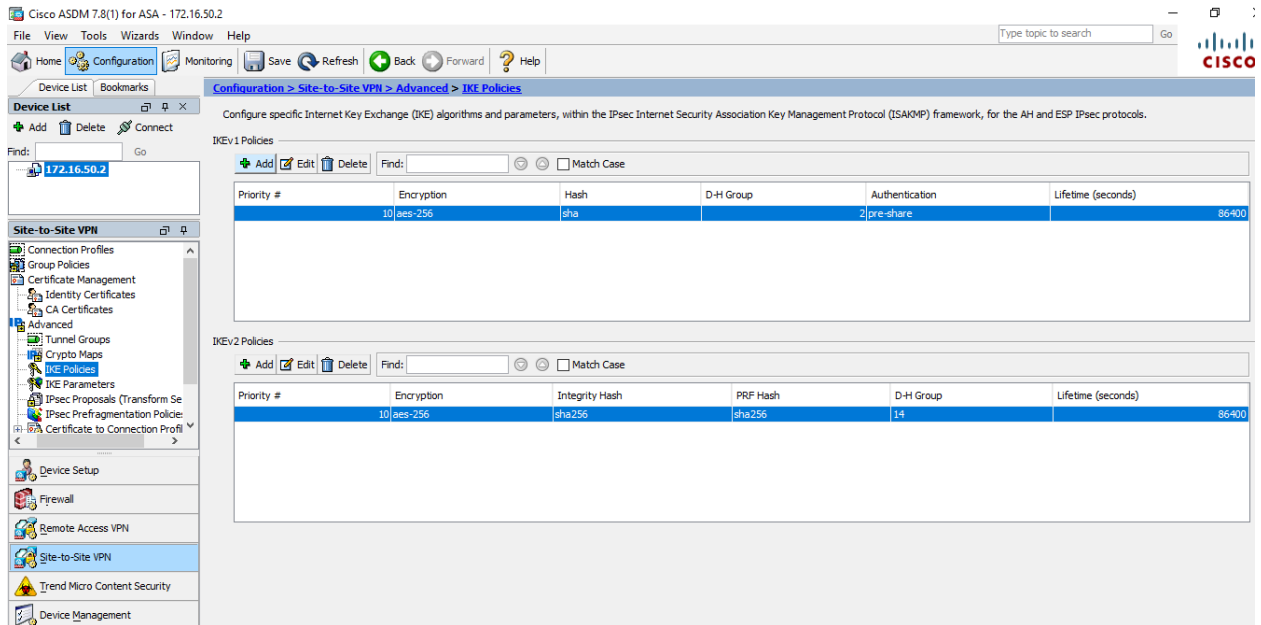
Enable Rule

Source Service: ... (TCP or UDP service only) ⓘ

Time Range: ...

OK Cancel Help

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



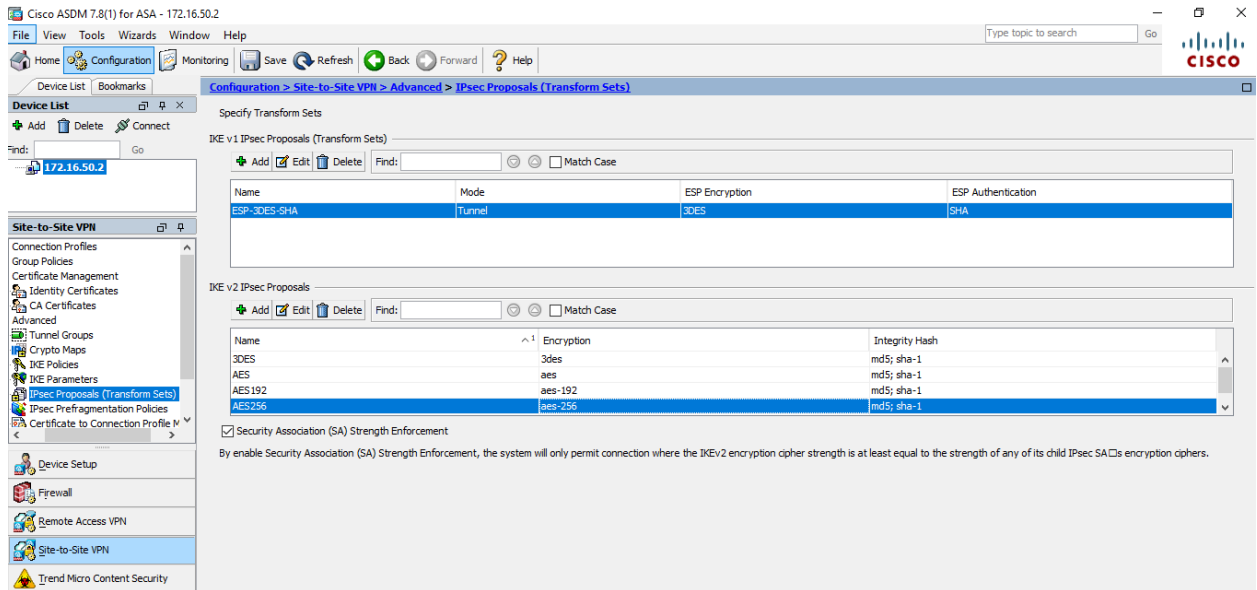
In IKEv2 Policy click Add to create a policy and apply the setting as below screenshot.

The screenshot shows the configuration dialog for an IKEv2 Policy. The fields are as follows:

- Priority: 10
- D-H Group: 14
- Encryption: aes-256
- Integrity Hash: sha256
- Pseudo Random Function (PRF) Hash: sha256
- Lifetime: Unlimited

The OK button is highlighted in blue.

7. In IPsec Proposals (Transform set) overview.



Configuration > Site-to-Site VPN > Advanced > IPsec Proposals (Transform Sets)

Specify Transform Sets

IKE v1 IPsec Proposals (Transform Sets)

Name	Mode	ESP Encryption	ESP Authentication
ESP-3DES-SHA	Tunnel	3DES	SHA

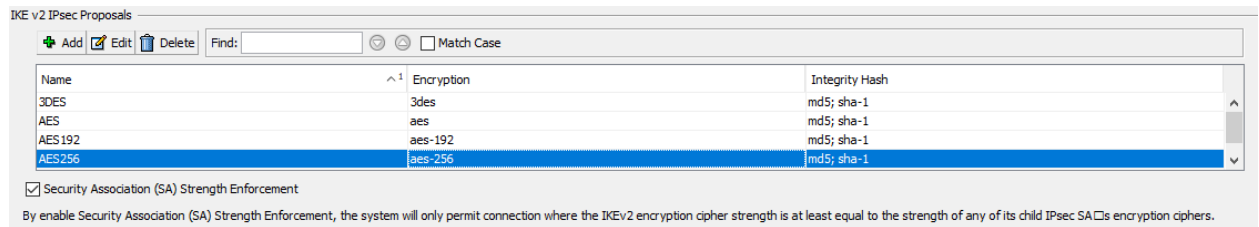
IKE v2 IPsec Proposals

Name	Encryption	Integrity Hash
3DES	3des	md5; sha-1
AES	aes	md5; sha-1
AES 192	aes-192	md5; sha-1
AES 256	aes-256	md5; sha-1

Security Association (SA) Strength Enforcement

By enable Security Association (SA) Strength Enforcement, the system will only permit connection where the IKEv2 encryption cipher strength is at least equal to the strength of any of its child IPsec SA's encryption ciphers.

We're using IKE v2 IPsec Proposal.



IKE v2 IPsec Proposals

Name	Encryption	Integrity Hash
3DES	3des	md5; sha-1
AES	aes	md5; sha-1
AES 192	aes-192	md5; sha-1
AES 256	aes-256	md5; sha-1

Security Association (SA) Strength Enforcement

By enable Security Association (SA) Strength Enforcement, the system will only permit connection where the IKEv2 encryption cipher strength is at least equal to the strength of any of its child IPsec SA's encryption ciphers.

8. ACL Manager Overview

Cisco ASDM 7.8(1) for ASA - 172.16.50.2

Configuration > Site-to-Site VPN > Advanced > ACL Manager

#	Enabled	Source	User	Security Group	Destination	Security Group	Service	Action	Logging
1	<input checked="" type="checkbox"/>	Local-Network			Remote-Network		ip	Permit	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	Local-Network			Remote-Network		kmp	Permit	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	Local-Network			Remote-Network		tcp	Permit	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>	Remote-Network			Local-Network		kmp	Permit	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>	Remote-Network			Local-Network		tcp	Permit	<input checked="" type="checkbox"/>

9. Connection Profile section overview.

Cisco ASDM 7.8(1) for ASA - 172.16.50.2

Configuration > Site-to-Site VPN > Connection Profiles

Manage site-to-site VPN connections. Here is a [video](#) on how to setup a site-to-site VPN connection.

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled	Group Policy	NAT Exempt
12.23.46.220	outside	Local-Network	Remote-Network	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	GroupPolicy1	<input checked="" type="checkbox"/>

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

The screenshot shows the 'Advanced' tab of an IPsec configuration wizard. The settings are as follows:

- Peer IP Address:** Static, 12.23.46.220
- Connection Name:** Same as IP Address, 12.23.46.220
- Interface:** outside
- Protected Networks:**
 - Local Network: Local-Network
 - Remote Network: Remote-Network
- IPsec Enabling:**
 - Group Policy Name: GroupPolicy1
 - (Following two fields are attributes of the group policy selected above.)
 - Enable IKE v1 Enable IKE v2
- IPsec Settings:**
 - Authentication:**
 - Local Pre-shared Key: [redacted]
 - Local Device Certificate: -- None --
 - Remote Peer Pre-shared Key: [redacted]
 - Remote Peer Certificate Authentication: Allowed
 - Encryption Algorithms:**
 - IKE Policy: aes-256-sha256-sha256
 - IPsec Proposal: 3DES, DES, AES, AES192, AES256

At the bottom, there is a 'Find:' search box, 'Next' and 'Previous' navigation buttons, and 'OK', 'Cancel', and 'Help' action buttons.

WTI unit

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

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

The screenshot displays the Cisco ASA Monitoring Session interface. It features a 'Session Details' section with a table of connection profiles and a 'Details' section with a table of ACL entries.

Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
12.23.46.220	IKEv2 IPsec	17:46:11 UTC Tue May 26 2020	152700
12.23.46.220	IKEv2: (1)AES256 IPsec: (...0h:22m:26s		152700

ID	Type	Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port	Encryption	Other	Bytes Tx Bytes Rx
	IKEv2		AES-256	Tunnel ID: 1.1 Loc Auth Mode: preSharedKeys Rem Auth Mode: preSharedKeys UDP Source Port 4500 UDP Destination Port 4500 Authentication Mode: preSharedKeys UDP Source Port 4500 UDP Destination Port 4500 Hashing: SHA256 PRF:: SHA256 Authentication Mode: preSharedKeys UDP Source Port 4500 UDP Destination Port 4500 IKE Negotiation Mode: none Hashing: SHA256 Diffie-Hellman Group: 14 Rekey Time Interval: 86400 Seconds Rekey Left(T): 85054 Seconds	
	IPsec	172.16.50.0/255.255.255.0/0/0 192.168.110.0/255.255.255.0/0/0	AES-256	Tunnel ID: 1.2 Hashing: SHA1 Encapsulation: Tunnel Rekey Time Interval: 28800 Seconds Rekey Left(T): 28305 Seconds Rekey Data Interval: 4608000 K-Bytes	152700 152700

Buttons: Refresh, Close, Help

Last Updated: 5/26/20 12:19:37 PM

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

!
```