Securing Networks with

Cisco FTD

Chapter 17

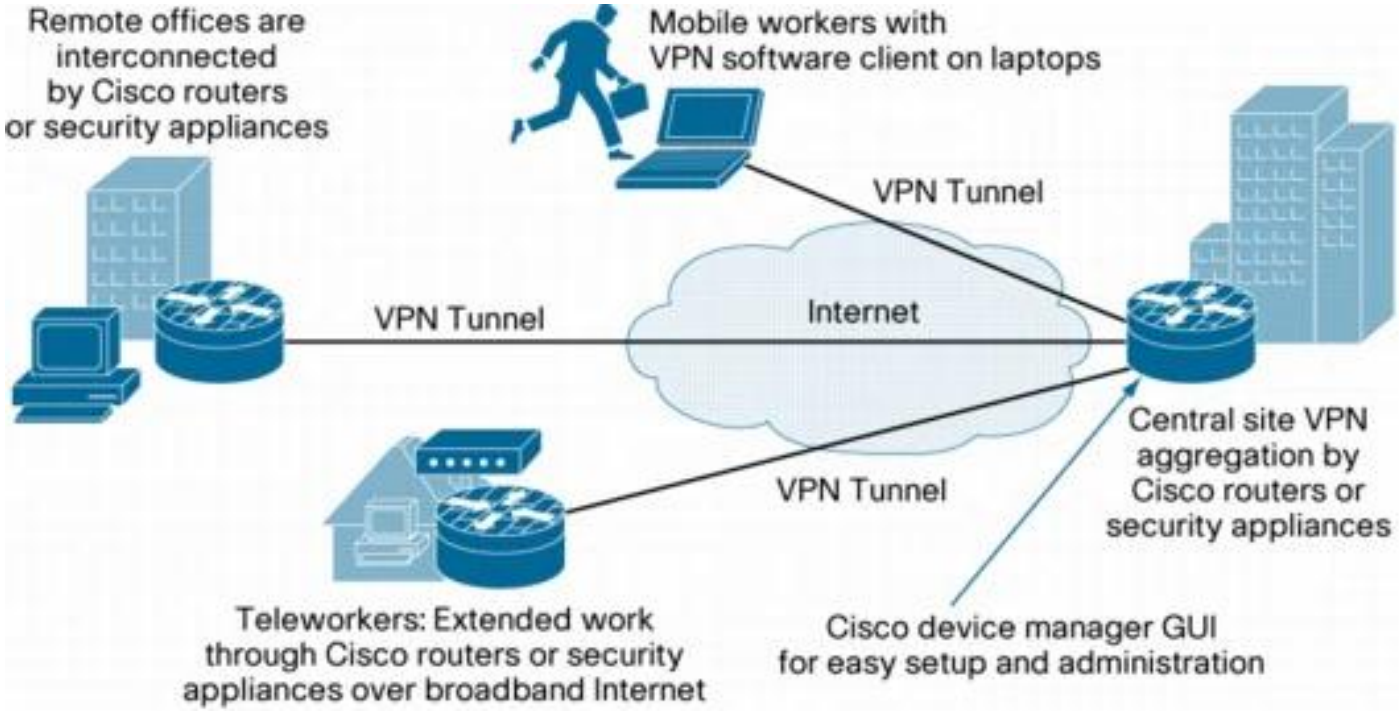
Virtual Private Network (VPN)

Mohsen Kheradmand

Virtual private network

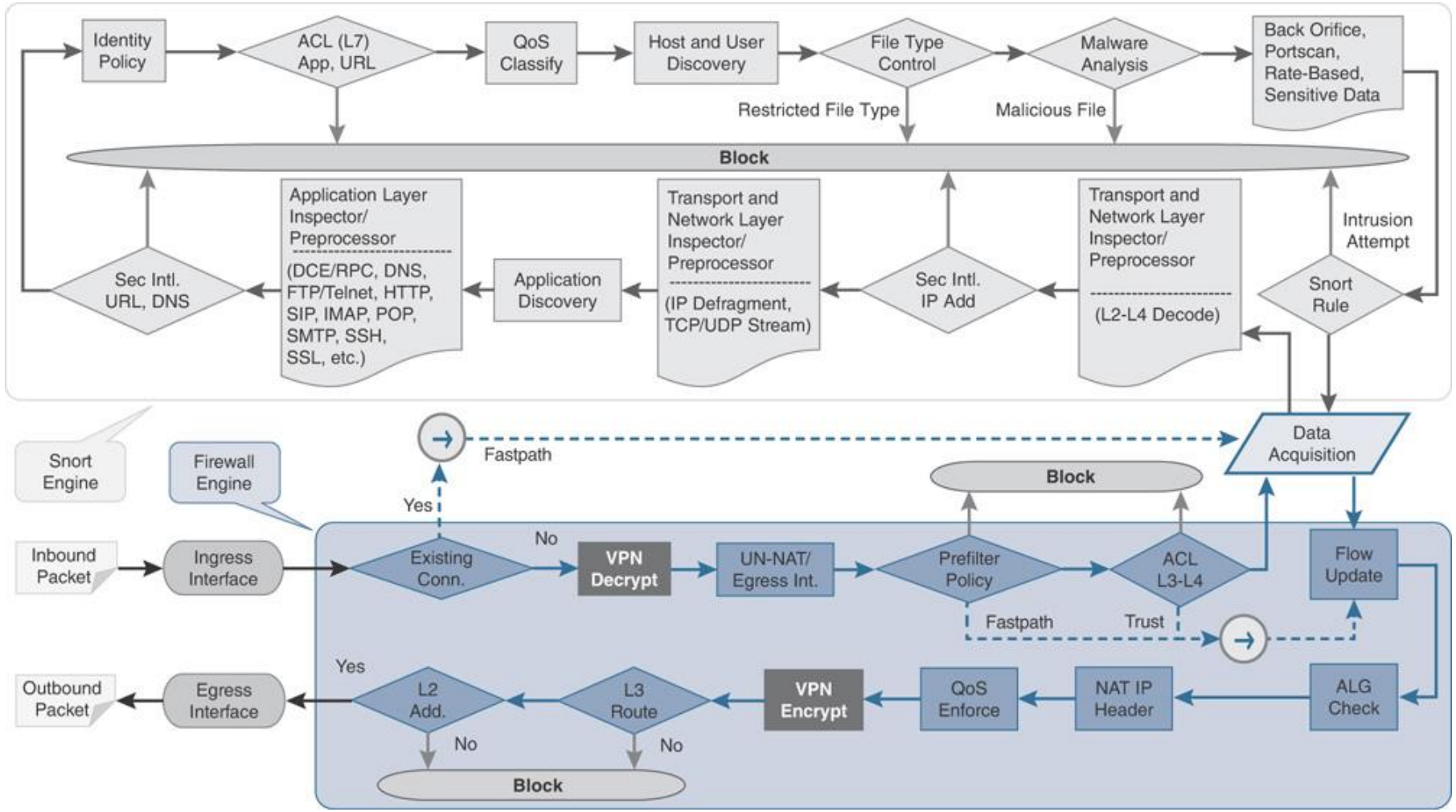
The VPN architectures are mainly two types:

- Site-to-Site VPN (S2S VPN)
- Remote Access VPN (RAVPN)



Virtual private network

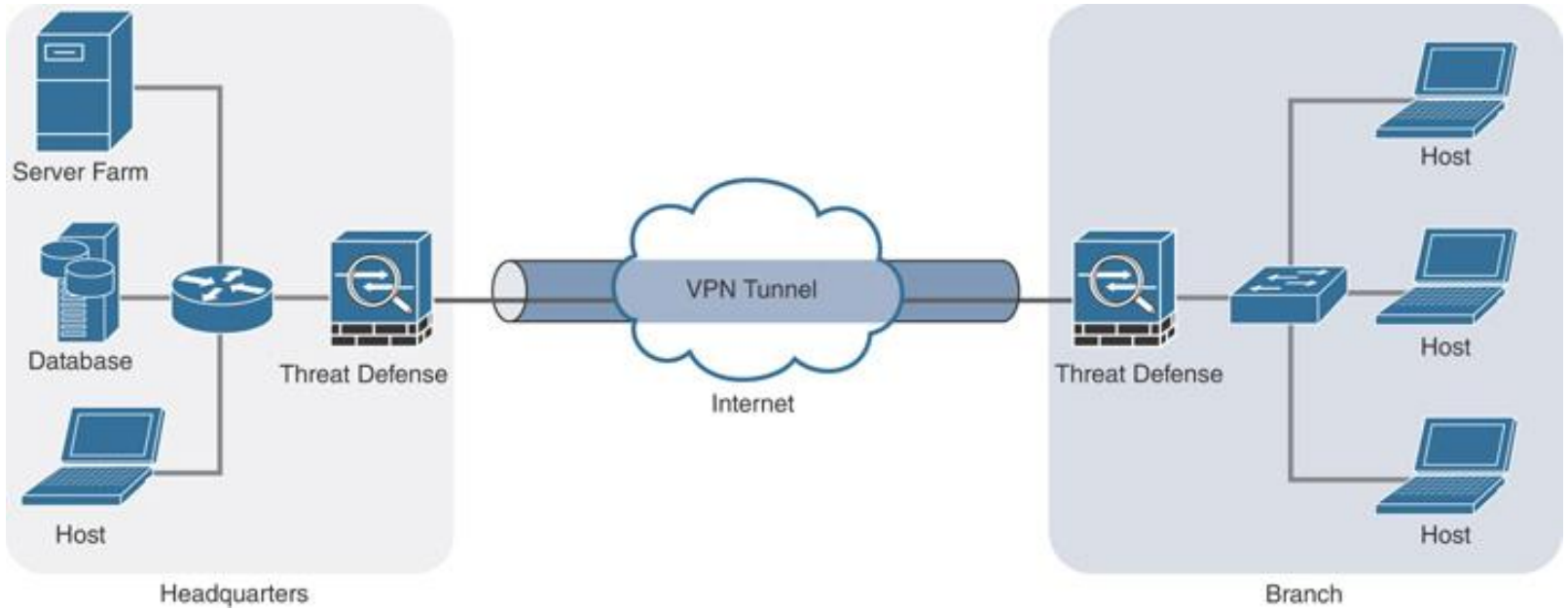
- Processing of Packets by Various Components of Security Engines (Highlighting VPN Operations)



MohsenKheradmand MK

Site-to-Site VPN

- This type of VPN connects the separated networks via a secure tunnel over the internet (underlay)



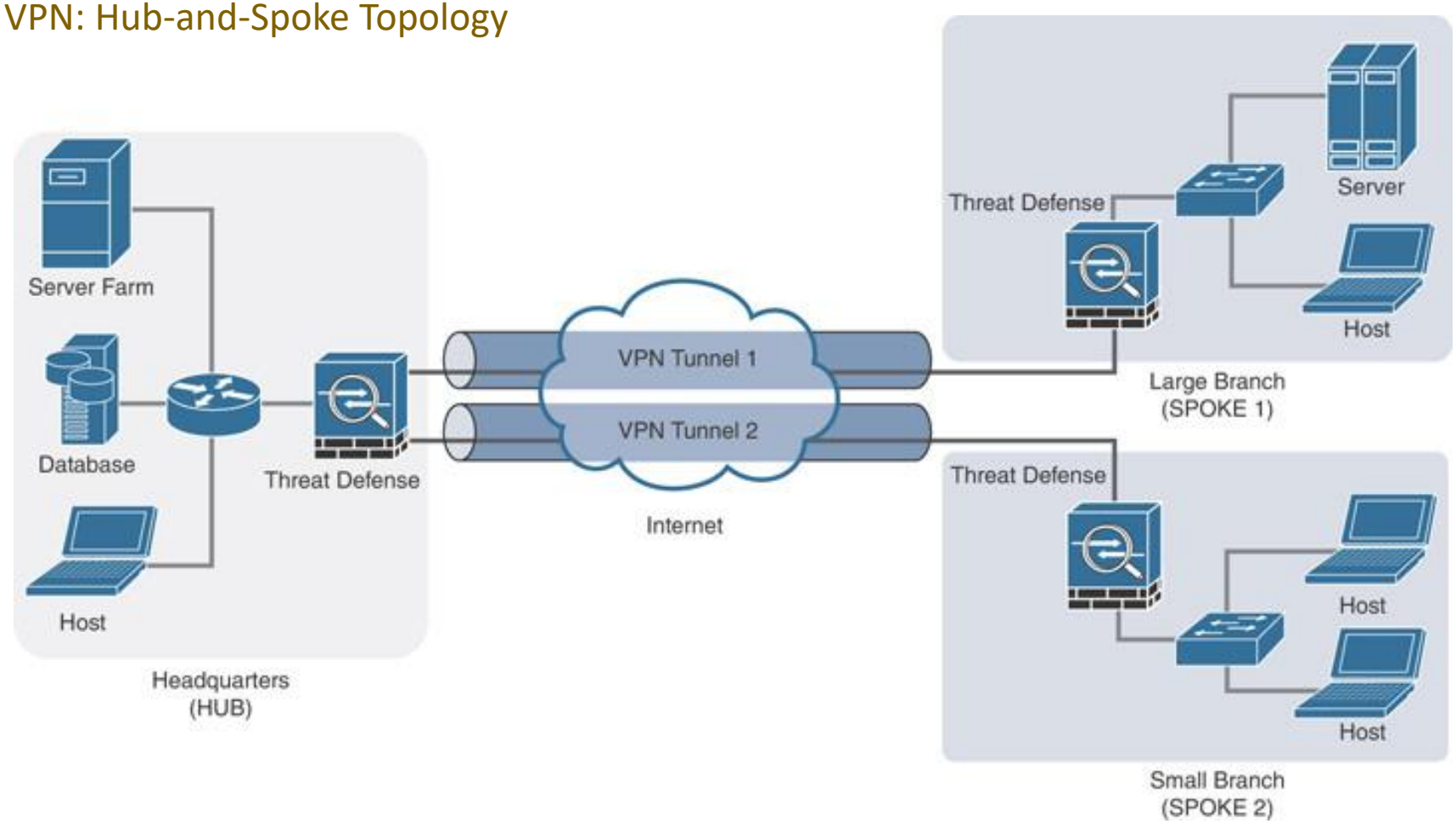
Site-to-Site VPN: Point-to-Point Topology

Secure Firewall can support three types of site-to-site VPN topologies:

- Point-to-Point : Two VPN gateways are connected via a secure tunnel.
- Hub and Spoke : A VPN gateway (hub) connects to multiple VPN gateways (spoke nodes) via independent secure tunnels.
- Full Mesh : VPN gateways in a group connect to each other via multiple secure tunnels.

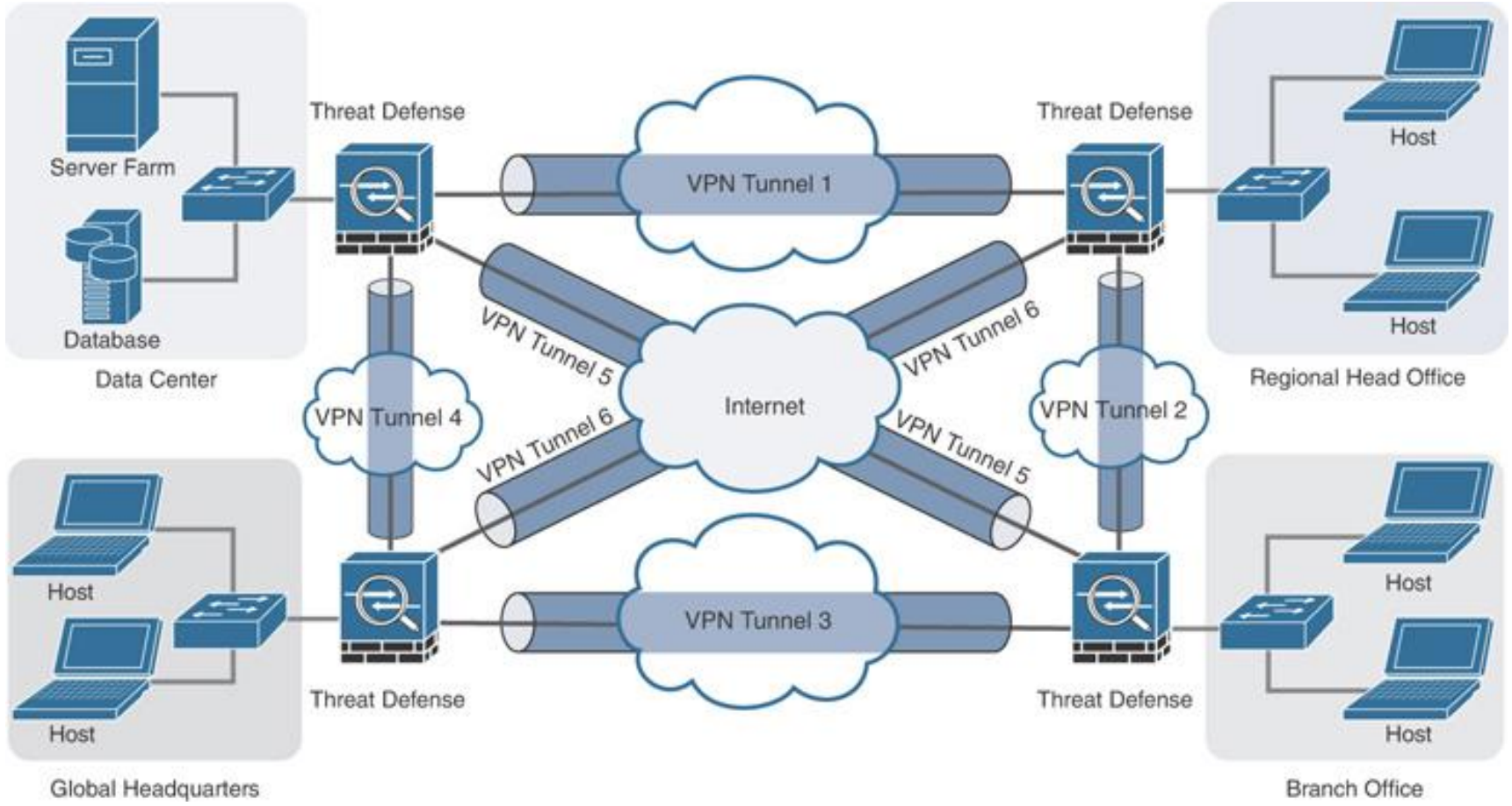
Site-to-Site VPN

Site-to-Site VPN: Hub-and-Spoke Topology



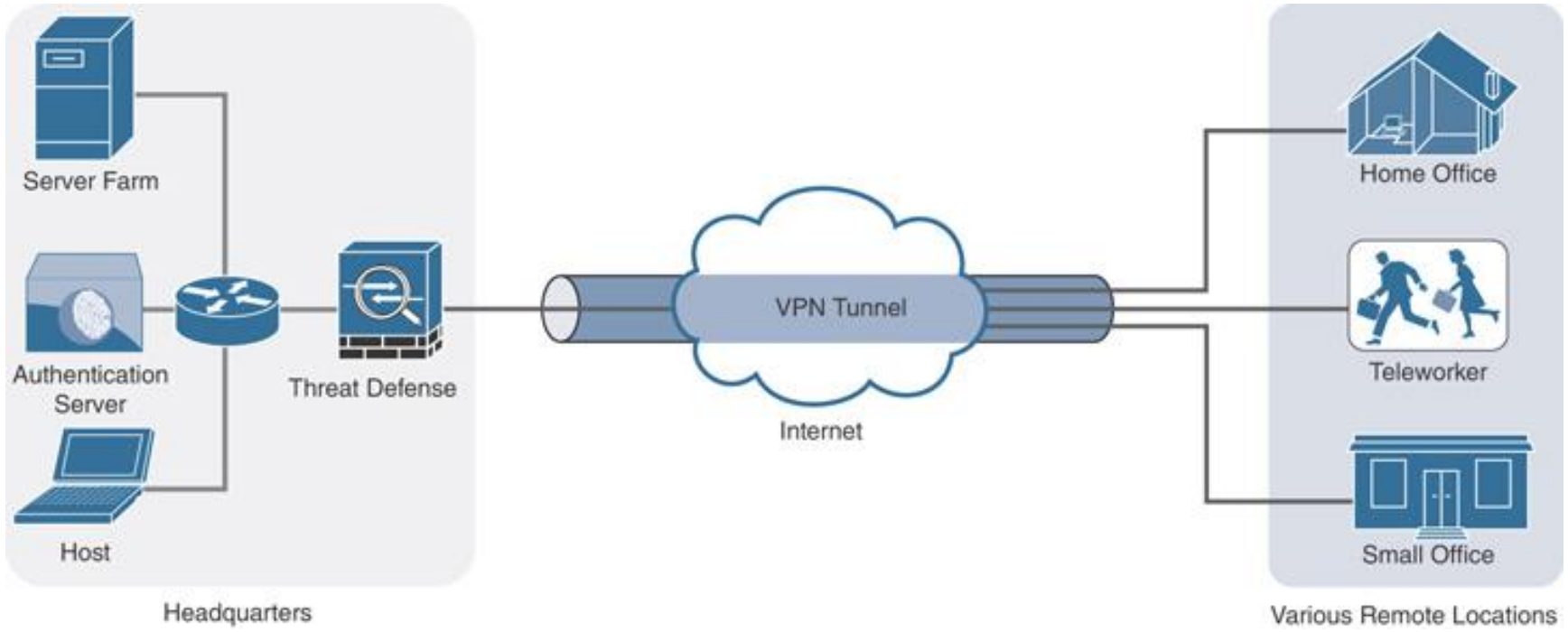
Site-to-Site VPN

Site-to-Site VPN: Full Mesh Topology



Remote Access VPN

- In this type of tunnel , a remote user from an outside can connect to an organization’s internal network via a VPN
- The endpoint device uses Cisco AnyConnect Secure Mobility Client to establish a secure tunnel
- The AnyConnect client supports Windows, Mac, Linux, Apple iOS, and Android operating systems



IPsec Essentials

- Internet Protocol Security (IPsec) is not a single networking protocol.
- It is a group of protocols and algorithms that work together to establish a secure connection over the public Internet

Peer authentication

- Verifies the identity of the VPN peer through authentication

Data confidentiality(Encryption)

- Changes plaintext into encrypted ciphertext Data

Integrity (Hashing)

- Prevents (MitM) attacks (Prevent tampering)
- Hash Message Authentication Code for data authentication

Replay detection

- Prevents capturing VPN traffic and replays it back to a VPN peer
- By using unique sequence number

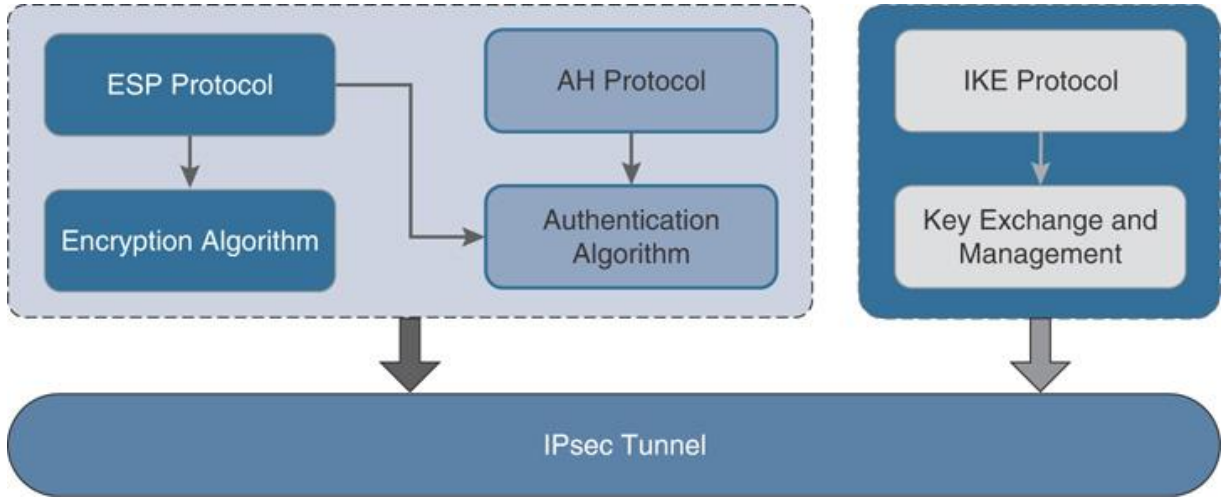
IPsec Essentials

The IETF defines the standards for implementing IPsec using three distinct protocols:

- - - - Authentication Header (AH) : Integrity, authentication, anti-replay (IP Protocol 51)

- - - - Encapsulating Security Payload (ESP) : Confidentiality, integrity, authentication, anti-replay (IP Protocol 50)

- - - - Internet Key Exchange (IKE) : Key exchange (UDP port 500)



IPsec Essentials

Some Cryptographic Algorithms and their strengths

Purpose	Cryptographic Algorithm	Key Strength
Encryption	Advanced Encryption Standard (AES)	AES256
	Data Encryption Standard (DES)	3DES (Triple DES)
Integrity	Secure Hash Algorithm (SHA)	SHA-2 with 512-bit digest
	Message-Digest Algorithm	MD5
Key Exchange	Diffie-Hellman (DH) Key Agreement Algorithm	DH Group 14 (2048-bit modulus)
	Elliptic-Curve Diffie-Hellman (ECDH)	DH Group 21 (521-bit random ellipticcurve)

- ✓ From Version 6.7, Secure Firewall does not support the 3DES, AES-GMAC, AES-GMAC-192, and AES-GMAC-256 encryption
- ✓ Secure Firewall only allows to enable the DES in Evaluation Mode or in a deployment without export-controlled licenses

IPsec Essentials

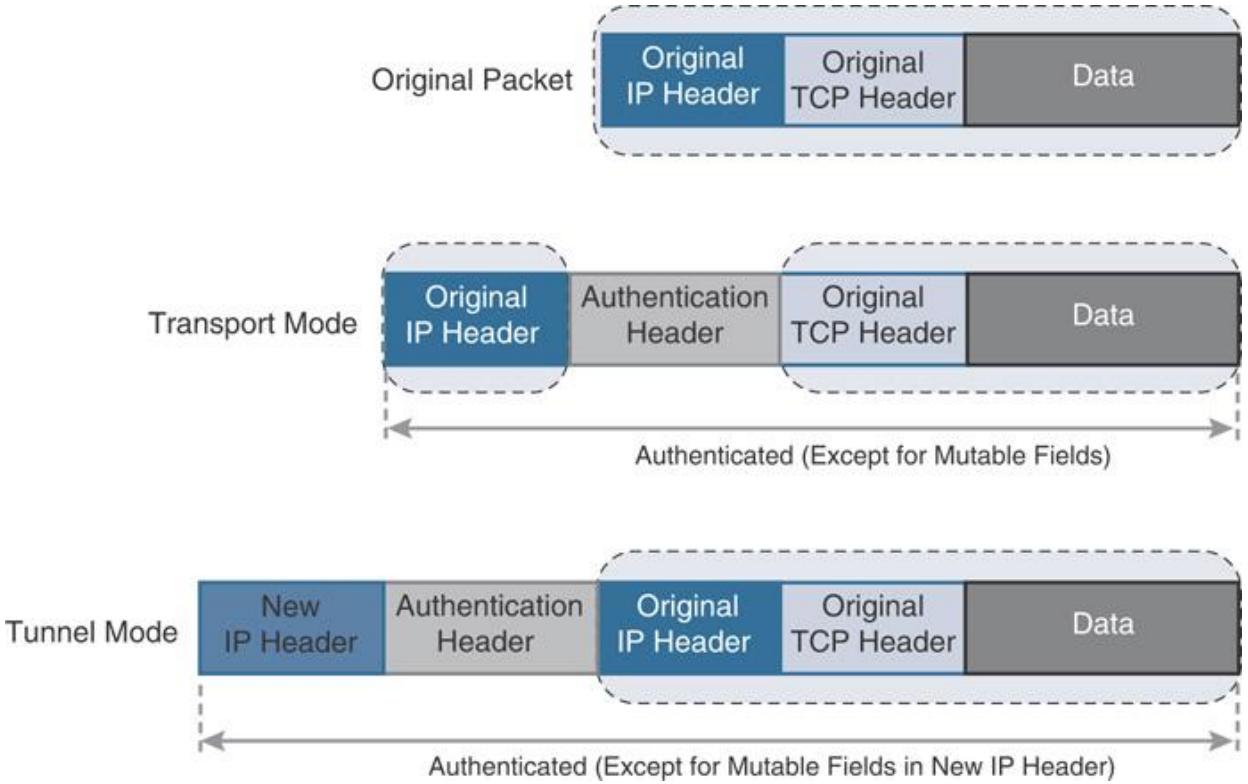
An IPsec tunnel between two VPN gateways can operate in two modes:

- **Transport mode**
  - In this mode, only the payload is encrypted or authenticated.
  - The original IP header remains unmodified and unencrypted.
- **Tunnel mode**
  - In this mode, the entire packet (IP header and payload) is encrypted, authenticated, and
  - Then encapsulated into a new IP packet , which uses a new IP header.

✓ You can configure the VPN peers with the AH or ESP protocol individually (such as only the AH protocol or only the ESP protocol) , or in combination with both AH and ESP protocols at the same time

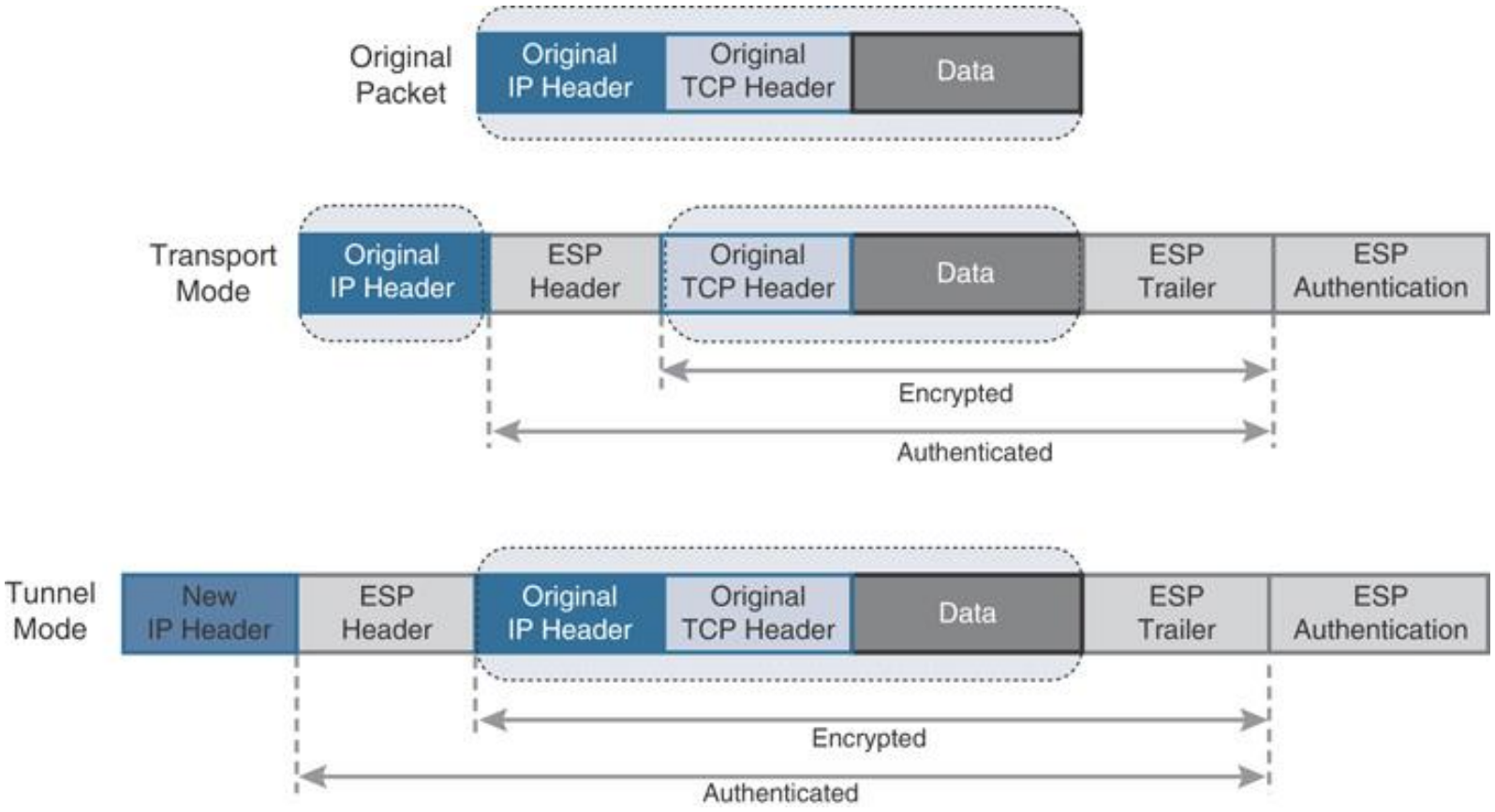
IPsec Essentials

- An Authentication Header (AH) in an IPv4 Packet
- Insertion of authentication header in both transparent mode and tunnel mode



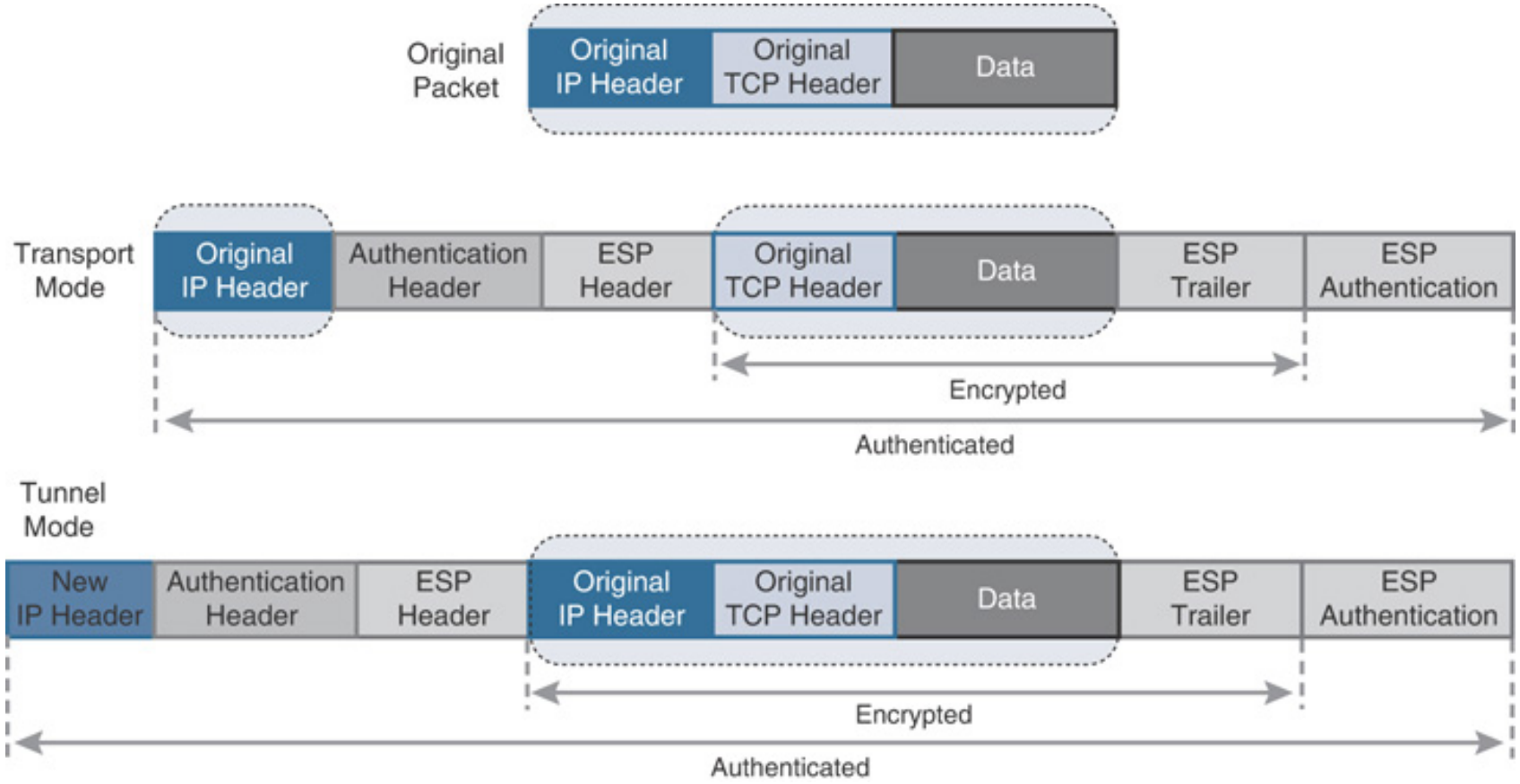
IPsec Essentials

- An Encapsulating Security Payload (ESP) Header in an IPv4 Packet
  - Insertion of the ESP header in both Transport and tunnel modes



IPsec Essentials

- Encapsulation of AH and ESP Headers Simultaneously
  - Insertion of both AH and ESP headers together at the same time.



IPsec Essentials

➢ Security Association and Key Exchange

Transform Set :

- A proposal of security protocols and algorithms that the VPN peers support to establish an IPsec tunnel

Security Association (SA)

- After negotiating a proposal, VPN peers establish a *security association* **(SA)** between them.
- To build a security association and exchange secret keys, VPN peers use the :

  - - - - - **IKE** (Internet Key Exchange) protocol

  - - - - - **ISAKMP** (Internet Security Association and Key Management Protocol) framework

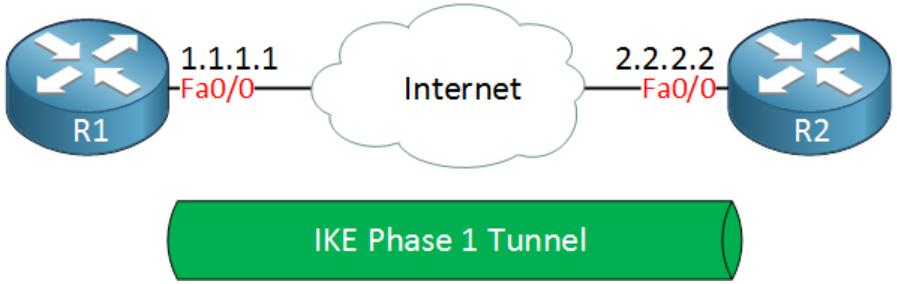
IPsec Essentials

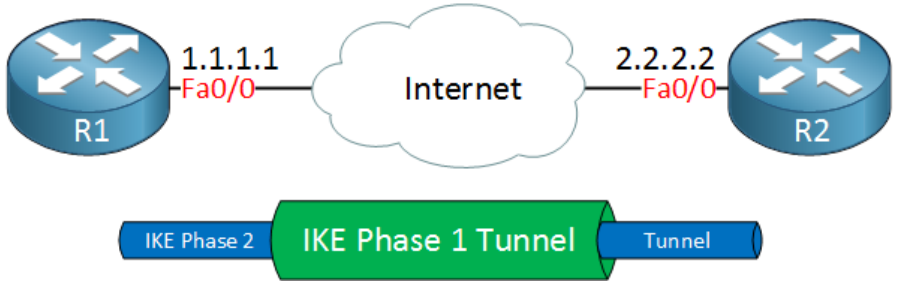
Internet Key Exchange (IKE)

The IKEv1 negotiations between two VPN peers complete in two phases

IKE phase 1

- 2 peers negotiate about the encryption, authentication, hashing and other parameters (bidirectional)
- The collection of parameters that the two devices will use is called a **SA (Security Association)**
- Establishes a **ISAKMP** SA between two IKE peers





IKE phase 2

- Establishes **IPsec** (unidirectional), using the ISAKMP SA , established in phase 1 for the negotiation.

IPsec Essentials

Internet Key Exchange (IKE)

IKE phase 1

- IKE phase 1 can operate in two modes :

Main mode (MM)
6 message

MM1) One or multiple SA proposals are offered, and the responder needs to match one of the them
Hash algorithm , Encryption algorithm , Authentication , (DH) group , Lifetime
MM2) From the responder to the initiator with the SA proposal that it matched
MM3) The initiator starts the DH key exchange
MM4) The responder sends its own key to the initiator (encryption is established)
MM5) The initiator starts authentication by sending the peer router its IP address
MM6) The responder sends back a similar packet and authenticates the session.

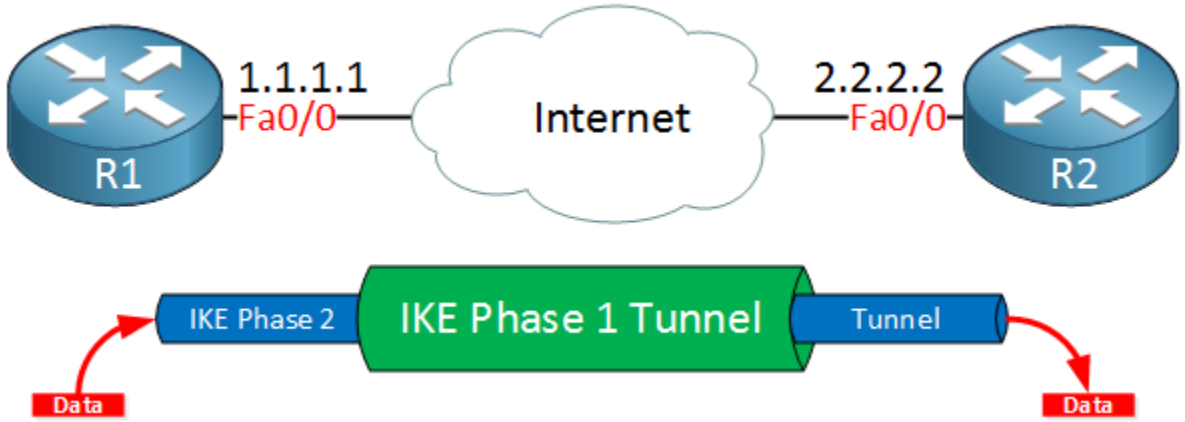
Aggressive mode (AM)
3 message

AM1) the initiator sends all the information contained in MM1 through MM3 and MM5.
AM2) This message sends all the same information contained in MM2, MM4, and MM6.
AM3) This message sends the authentication that is contained in MM5

✓ Main mode is slower than aggressive mode but main mode is more secure and more flexible

IPsec Essentials

Internet Key Exchange (IKE)



IKE phase 2

Unidirectional negotiation

IPsec (IP Security) tunnel

- ✓ Phase 2 uses the existing bidirectional IKE SA to securely exchange messages to establish IPsec SAs
- ✓ The method used to establish the IPsec SA is known as quick mode:

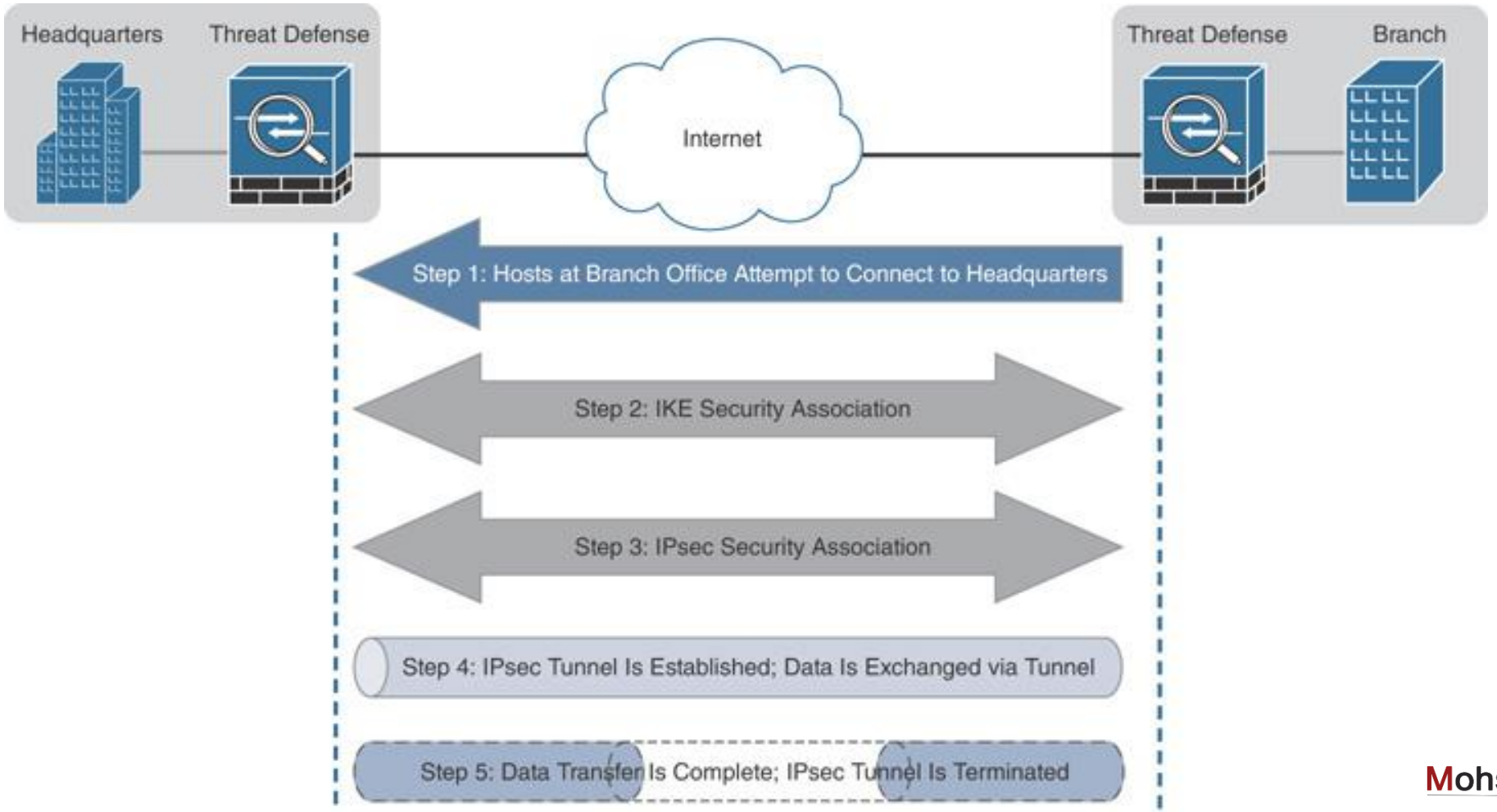
QM1: The initiator starts multiple IPsec SAs in a single exchange message.

QM2: This message from the responder has matching IPsec parameters.

QM3: After this message, there should be two unidirectional IPsec SAs between the two peers.

IPsec Essentials

Internet Key Exchange (IKE)



IPsec Essentials

IKE version 2

- IKEv2 requires less bandwidth than IKEv1. (4 messages for negotiation & exchange)

  IKE_SA_INIT :
  - The VPN peers negotiate cryptographic algorithms, exchange random numbers and perform a key exchange.
  - Using the security attributes negotiated at this stage, VPN peers protect the following messages cryptographically.

  IKE_AUTH :
  - 2nd message authenticate the previous messages, exchange identities and certificates, and establish the first Child SA

  CREATE_CHILD_SA :
  - 3rd message creates new Child SAs and rekeys both IKE SAs and Child SAs.

  INFORMATIONAL :
  - VPN peers can exchange this message to notify each other of events related to IKE operation.

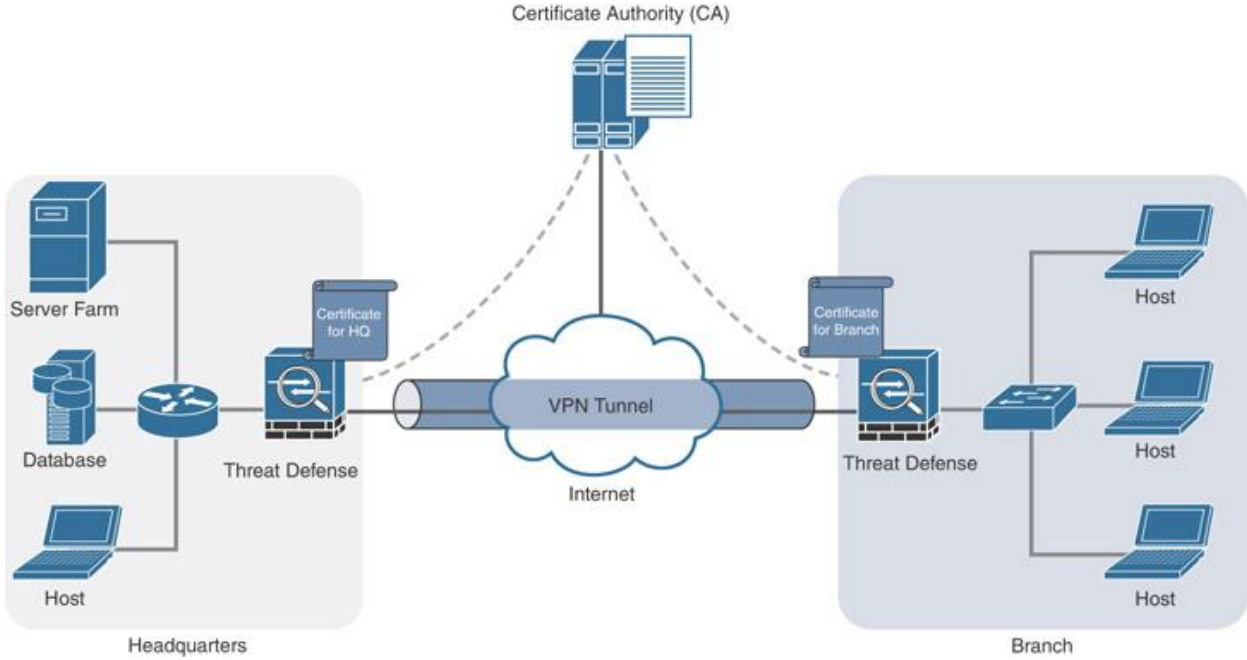
- IKEv2 supports EAP authentication (next to pre-shared keys and digital certificates).
- IKEv2 has built-in support for NAT traversal (required when your IPsec peer is behind a NAT router).
- Anti-DoS , Next generation encryption (NGE) , Elliptic Curve Digital Signature Algorithm (ECDSA-SIG)

IPsec Essentials

Authentication

- During the IKE negotiation process, the VPN peers can authenticate each other by using **pre-shared** keys
- For scalability in larger network , the VPN peers can obtain digital certificates from the CA server to authenticate
- In the real network VPN peers should obtain Certs from CA server rather than internal CA (in FTD)
- Upon a successful certificate enrollment, the FTD devices exchange their identity certificates to validate each other.

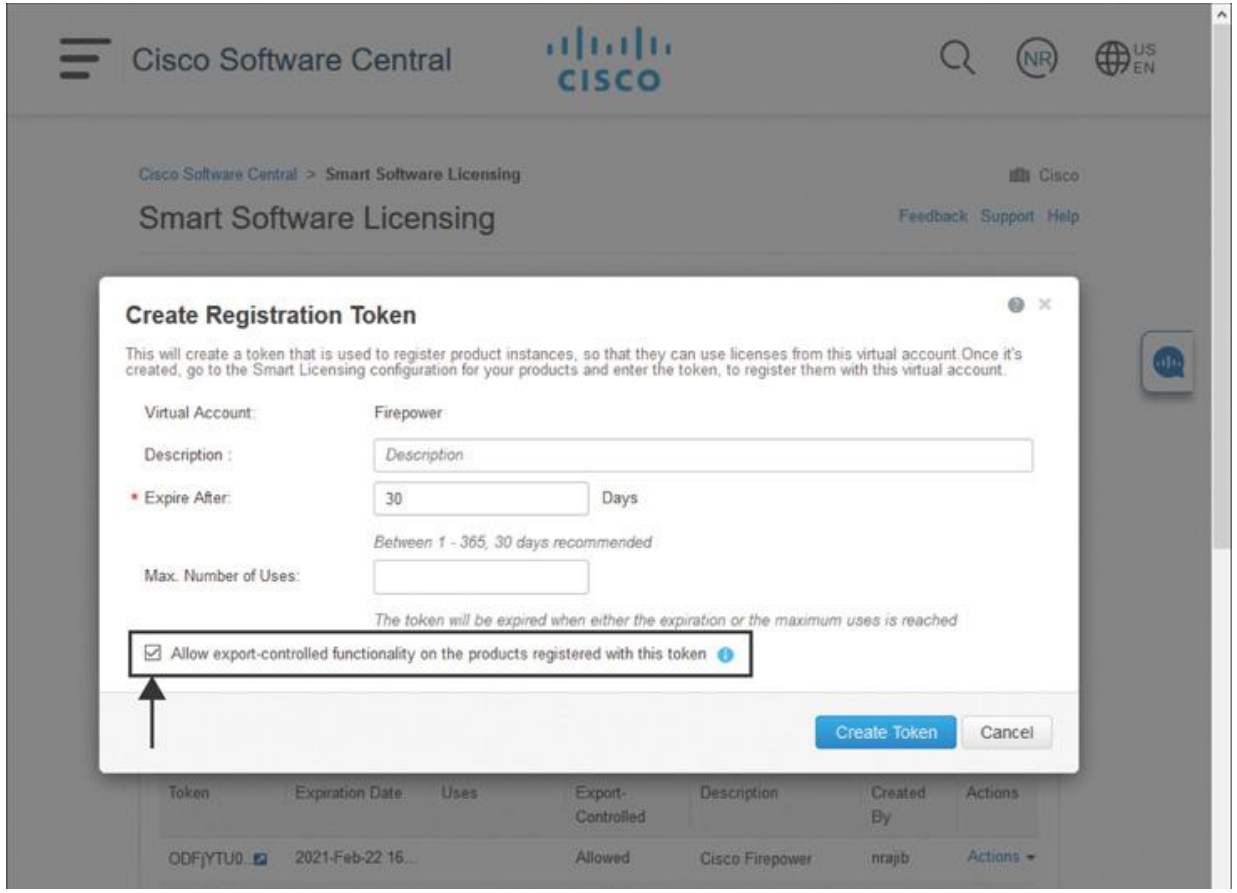
- Additionally, the IKEv2 protocol supports the Extensible Authentication Protocol (EAP) authentication to authenticate the IKE SAs
- The authentication methods in EAP-IKEv2 protocol are based on asymmetric key pairs, passwords, and symmetric keys



Site-to-Site VPN Deployment

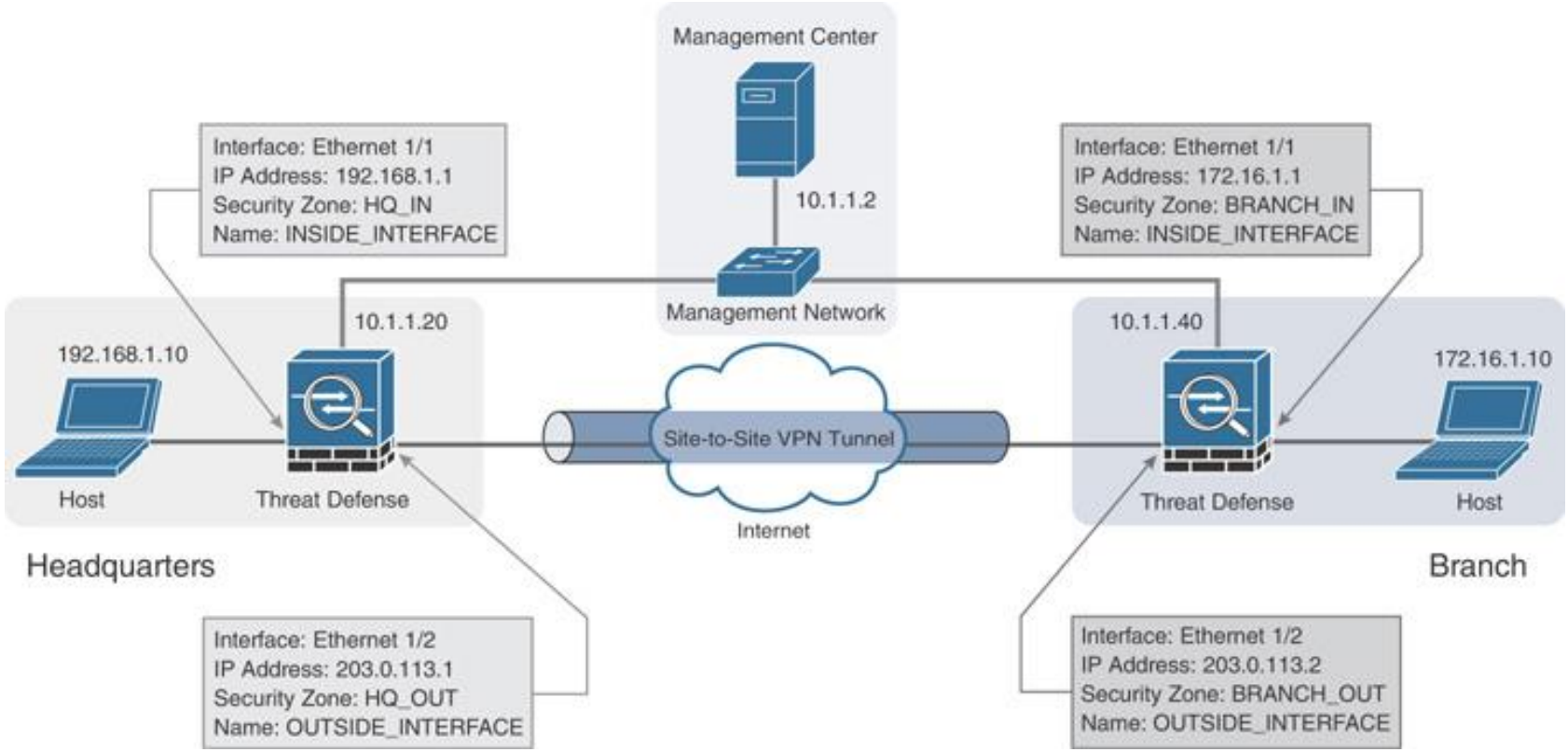
Prerequisites

- When registering the FMC with Cisco Smart Software Licensing, you must allow the export-controlled functionality (enables strong cryptographic) If the export-controlled functionality is not allowed, you can use only the (DES)



Site-to-Site VPN Deployment

- Example of P-to-P configuration



Headquarter inside LAN = 192.168.1.0/24

Headquarter Outside interface =203.0.113.1

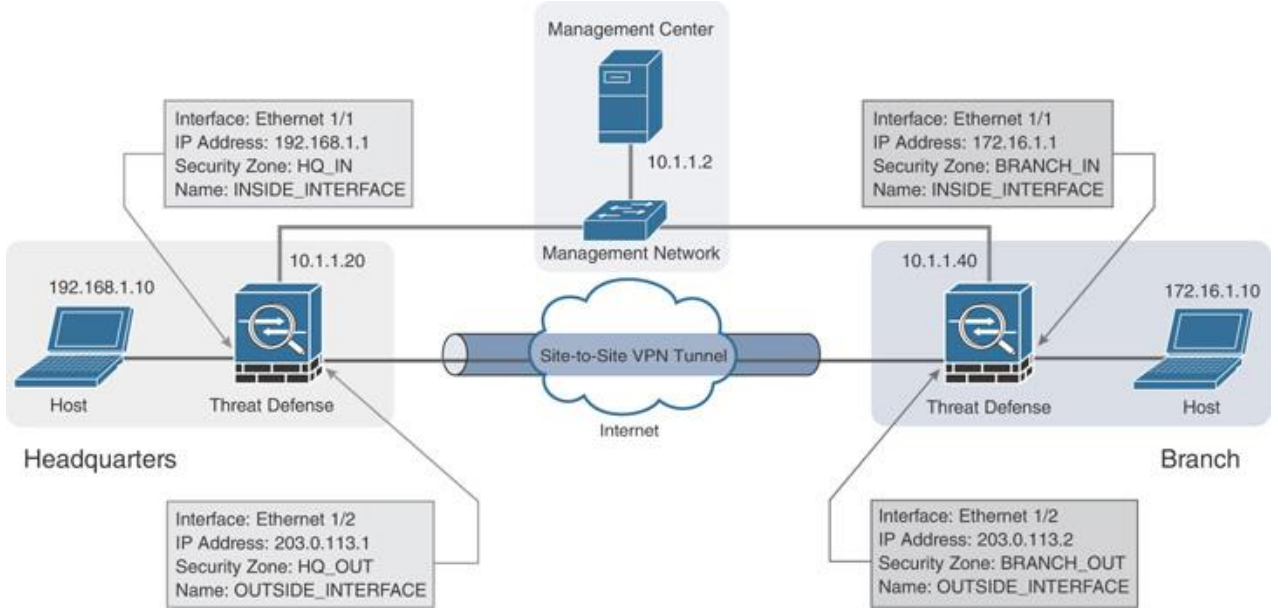
Branch inside LAN = 172.16.1.0/24

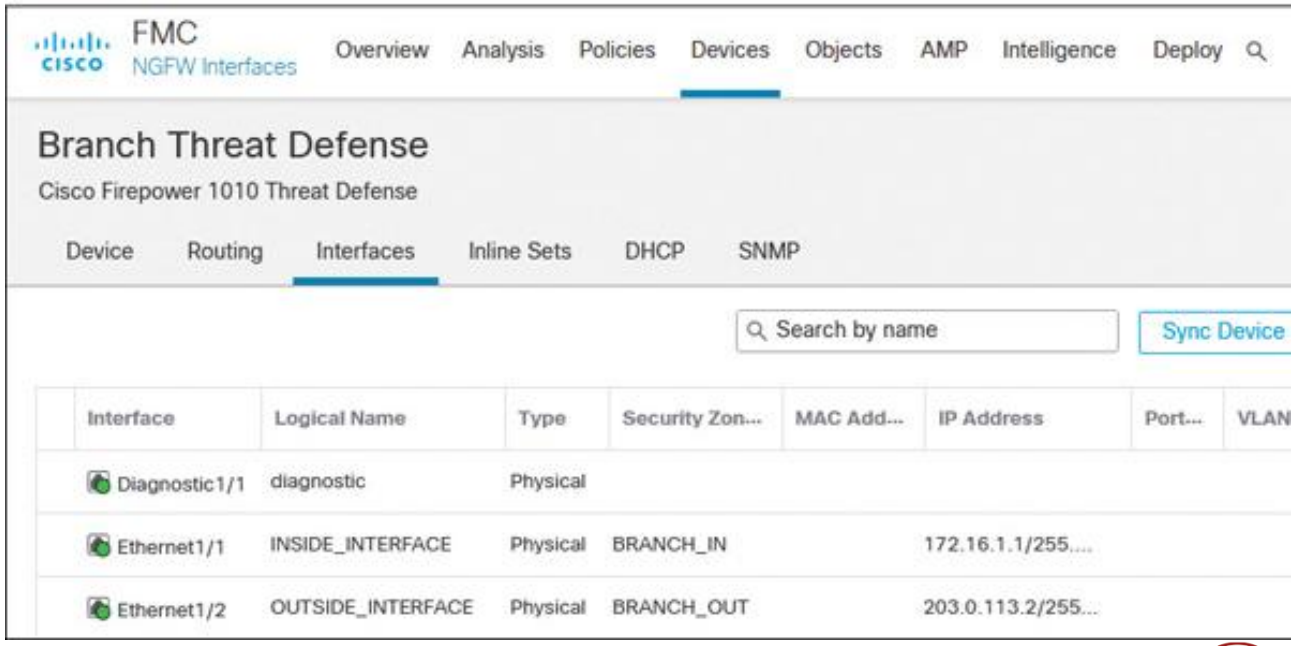
Branch outside interface = 203.0.113.2

Management interface IP = 10.1.1.0

Site-to-Site VPN Deployment

- Example of P-to-P configuration
  - Inside and outside interface configuration

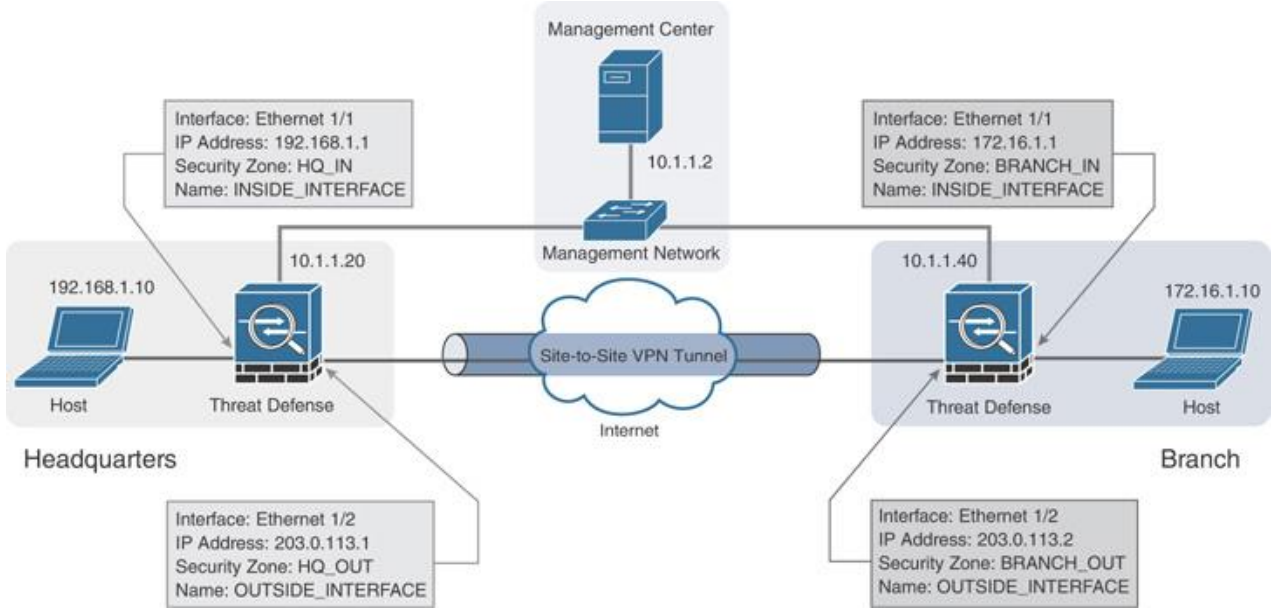


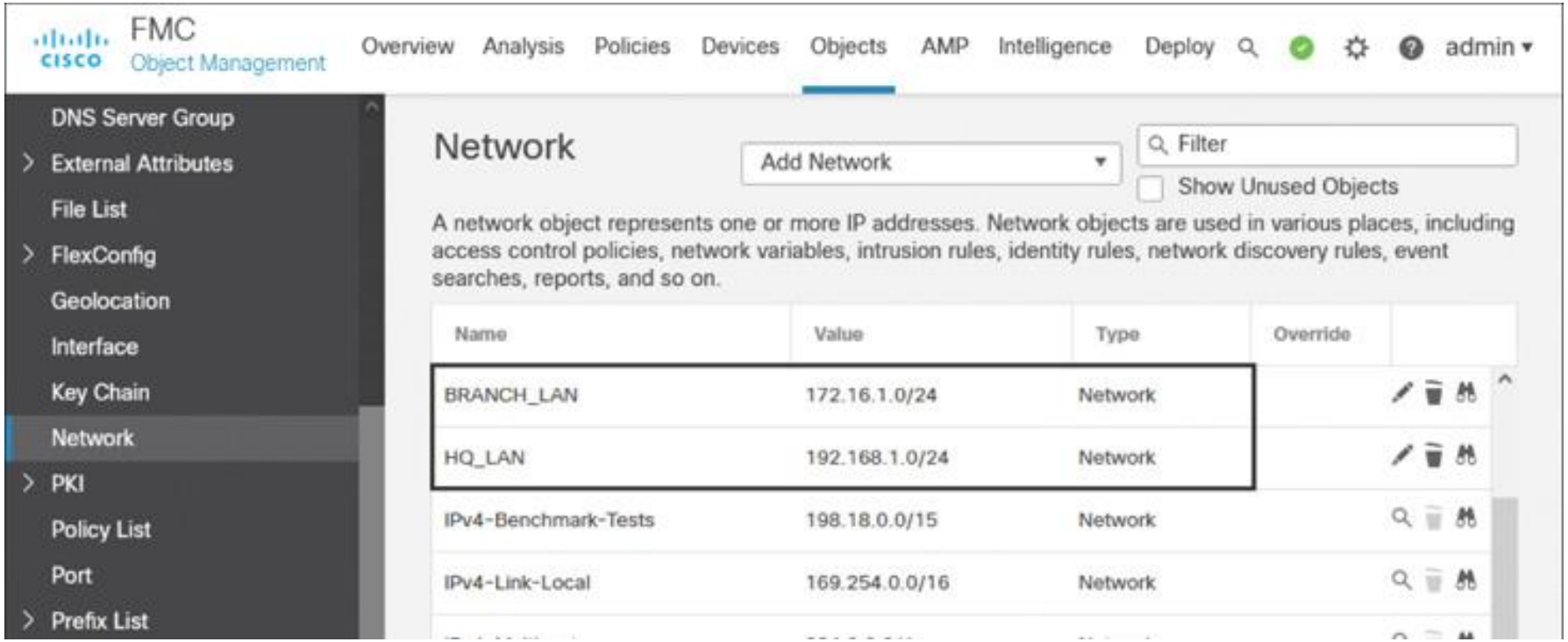


Site-to-Site VPN Deployment

- Example of P-to-P configuration
  - ➢ Network Objects for Headquarters and Branch Networks

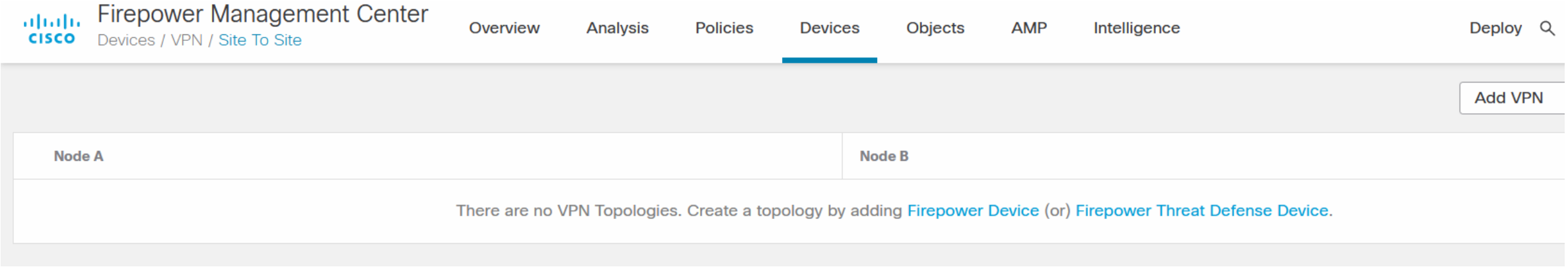
- This networks will be routed via the new VPN tunnel





Site-to-Site VPN Deployment

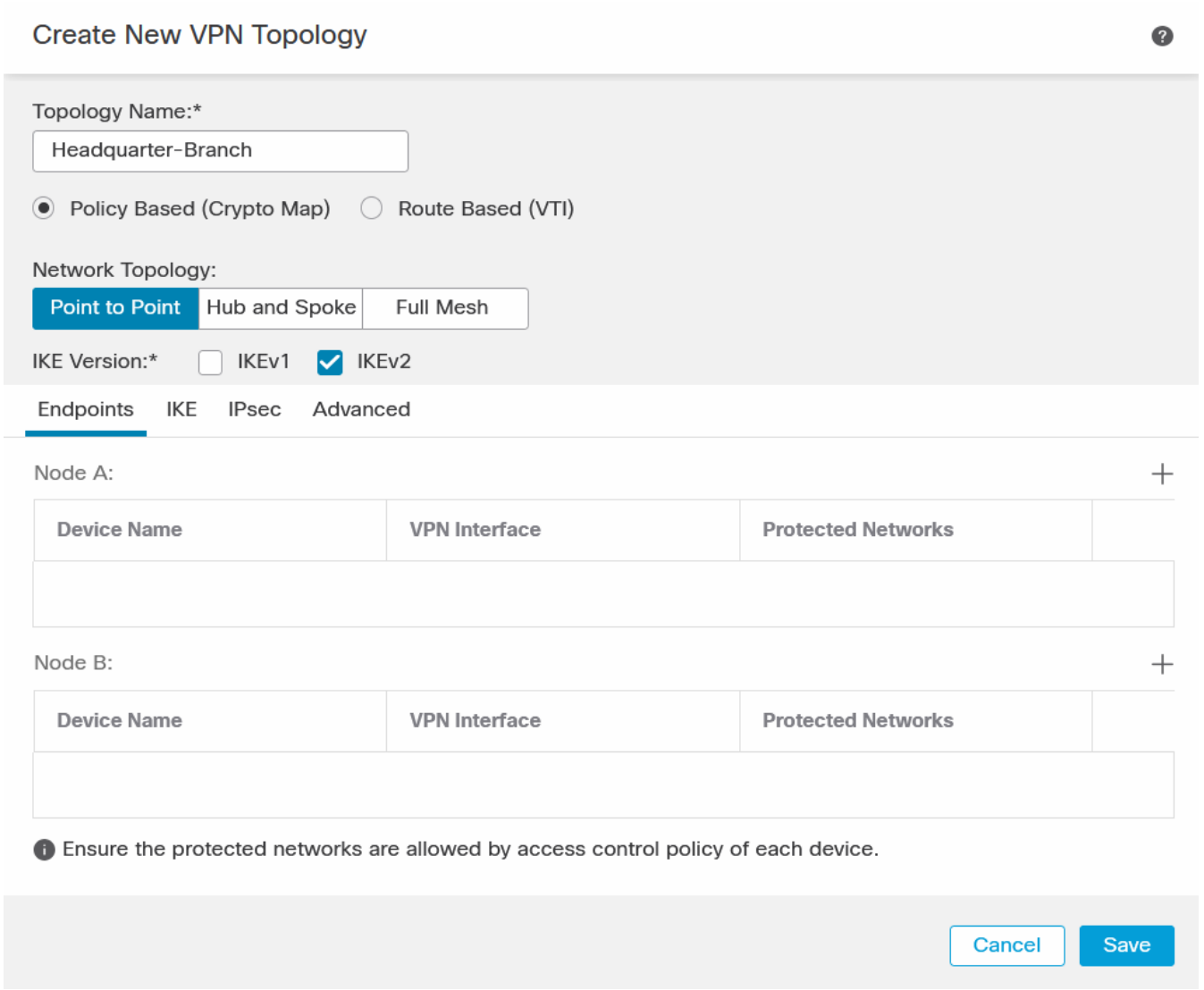
- Example of P-to-P configuration
  - ➢ VPN Configurations
    - Devices > VPN > Site To Site
    - Firepower Threat Defense Device



Site-to-Site VPN Deployment

- Example of P-to-P configuration
  - ➢ VPN Configurations

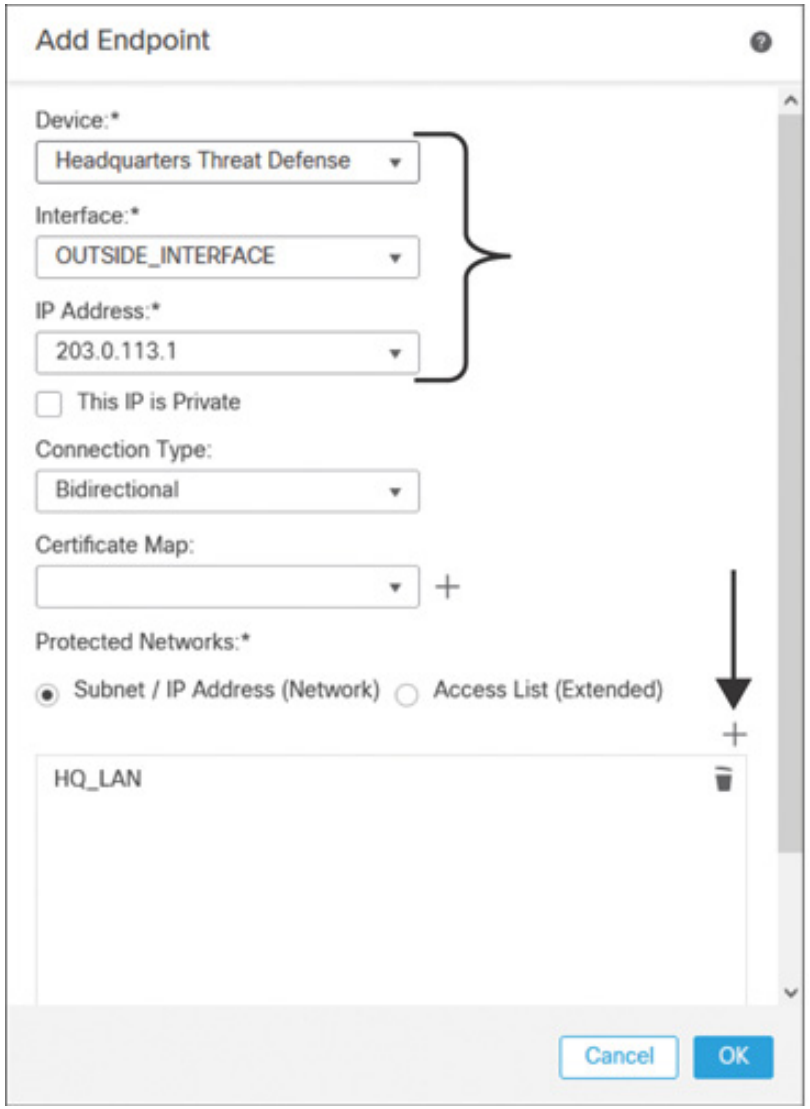
- Type a name for VPN connection
- Select Policy Based (Crypto Map)
- Select Point to Point
- (Optionally select IKEv2 or IKEv2)
- On Node A & B : click + (add endpoints)

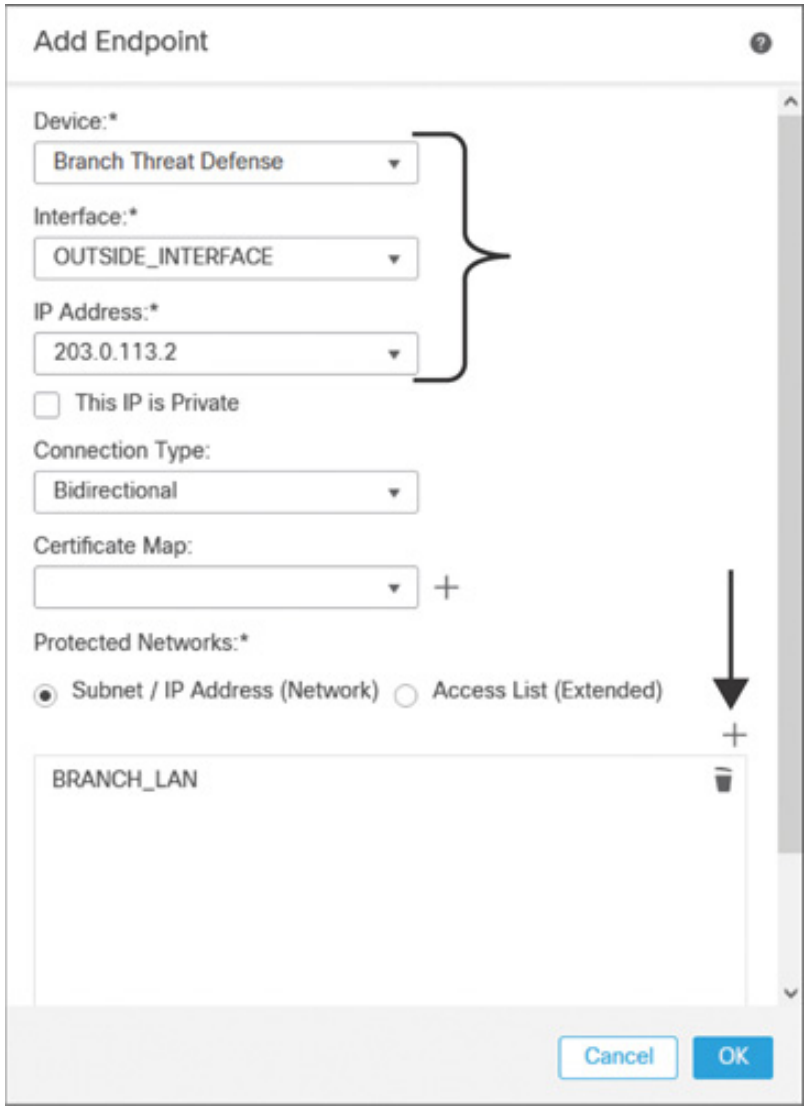


Site-to-Site VPN Deployment

- Example of P-to-P configuration
  - ➢ VPN Configurations
    - ❖ Add Endpoints

- Select FTD device to participate
- Select outside interface
- Type : bidirectional
- Click + to add inside networks to securely route via VPN tunnel

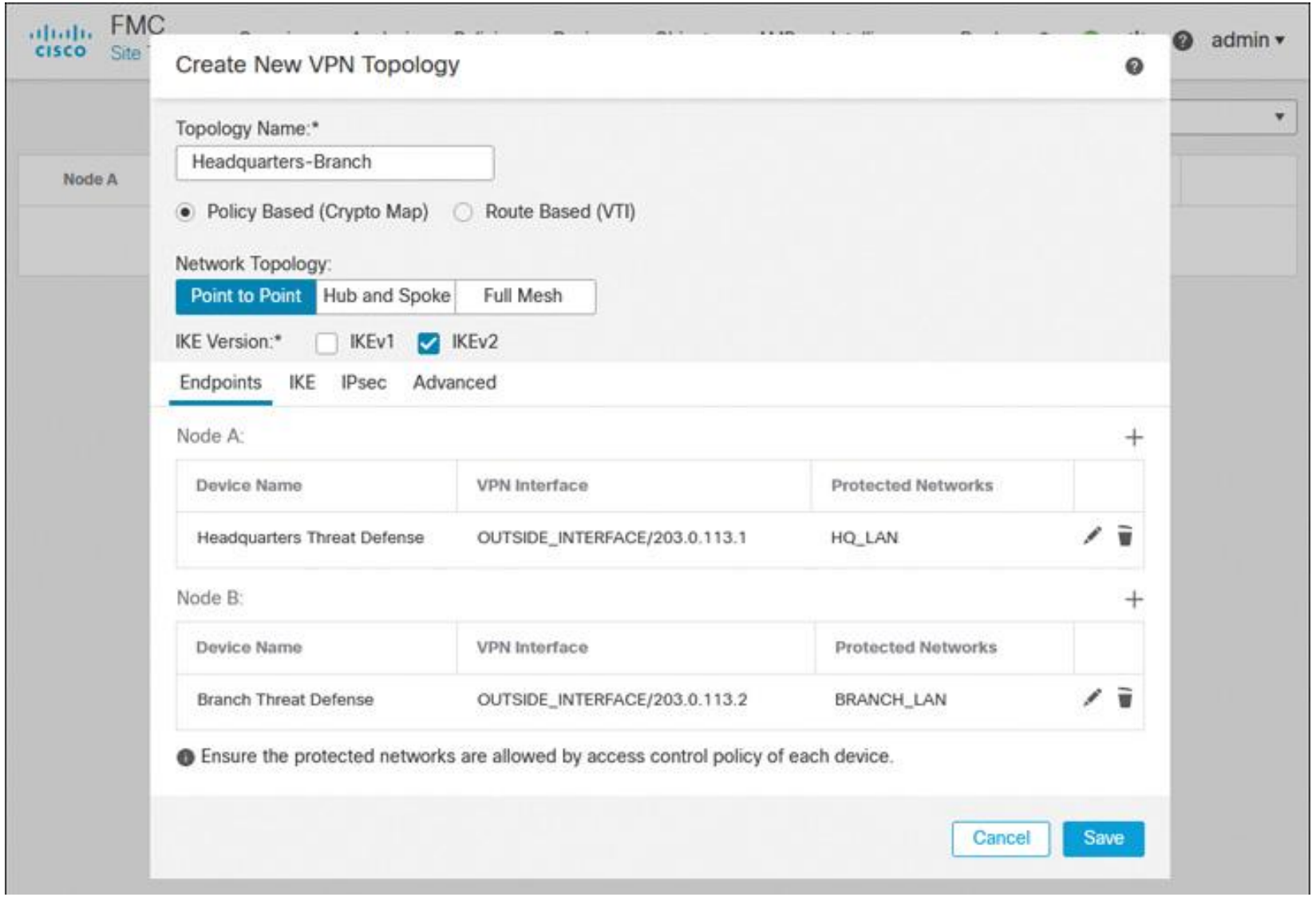




Site-to-Site VPN Deployment

- Example of P-to-P configuration
  - ➢ VPN Configurations

    - After both nodes are added click the Save button
    - Deploy the configurations
    - Now both VPN side should be able to connect via tunnel

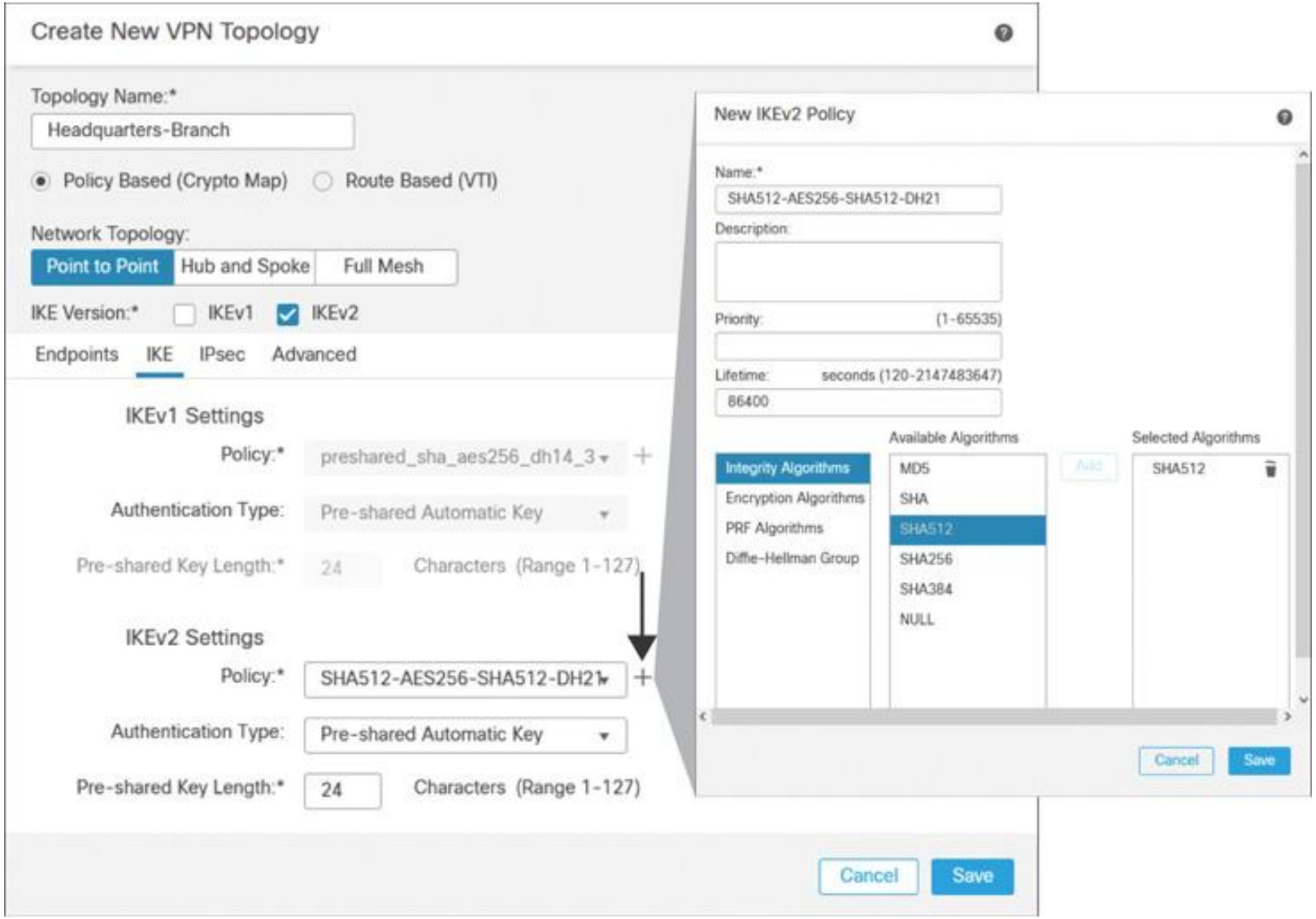


Site-to-Site VPN Deployment

- Example of P-to-P configuration
  - ➢ VPN Configurations
    - ❖ Additional security parameters

- You can strengthen the VPN tunnel security

- Form IKE setting you can set new policy and customize it



Site-to-Site VPN Deployment

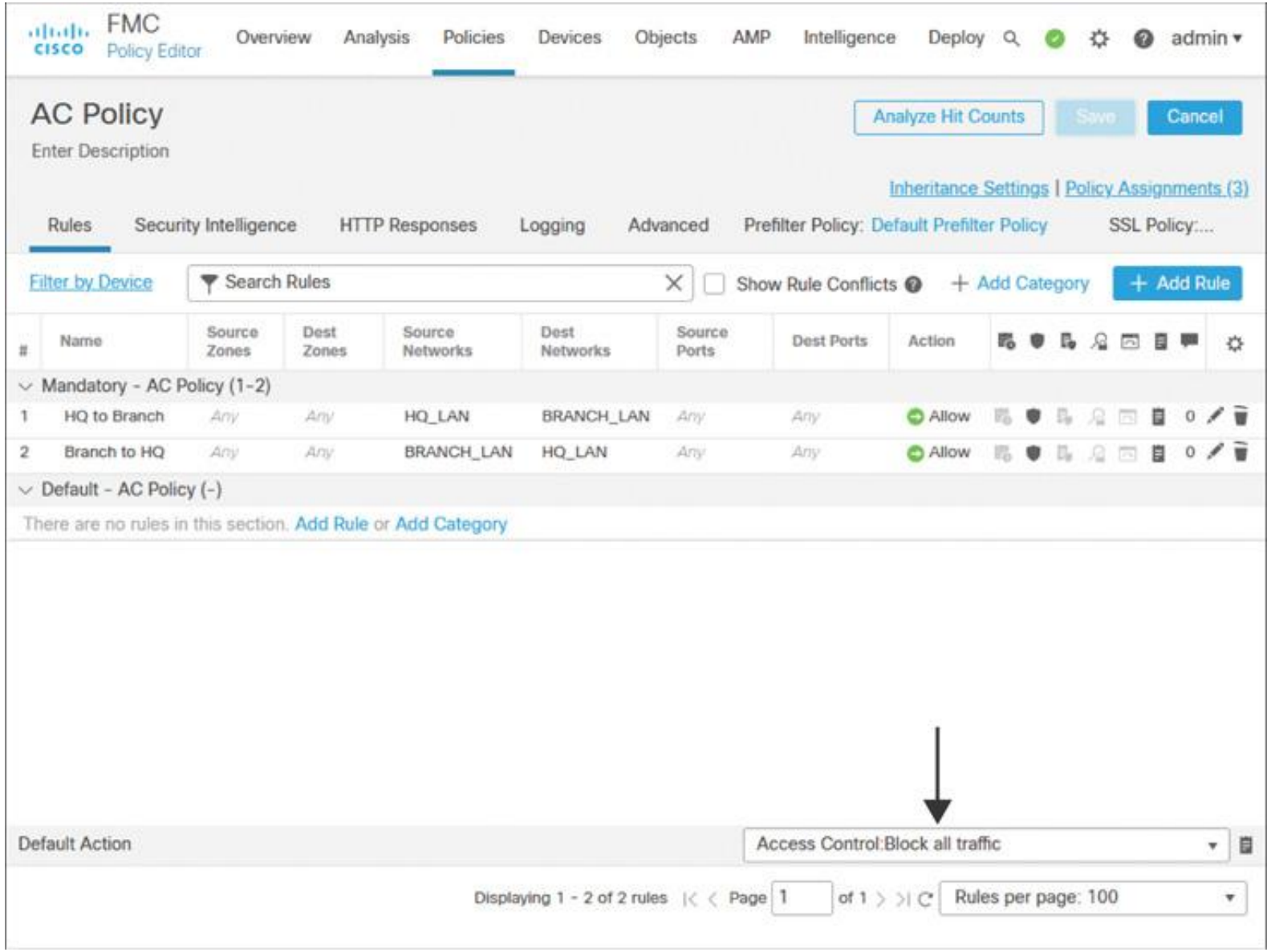
- Example of P-to-P configuration

➢ Access Control Policy

- If end-user traffic is blocked by the access control policy so :

✓ Create a rule to allow traffic of the inside LANs

✓ Or you can change Default Action to allow all traffic

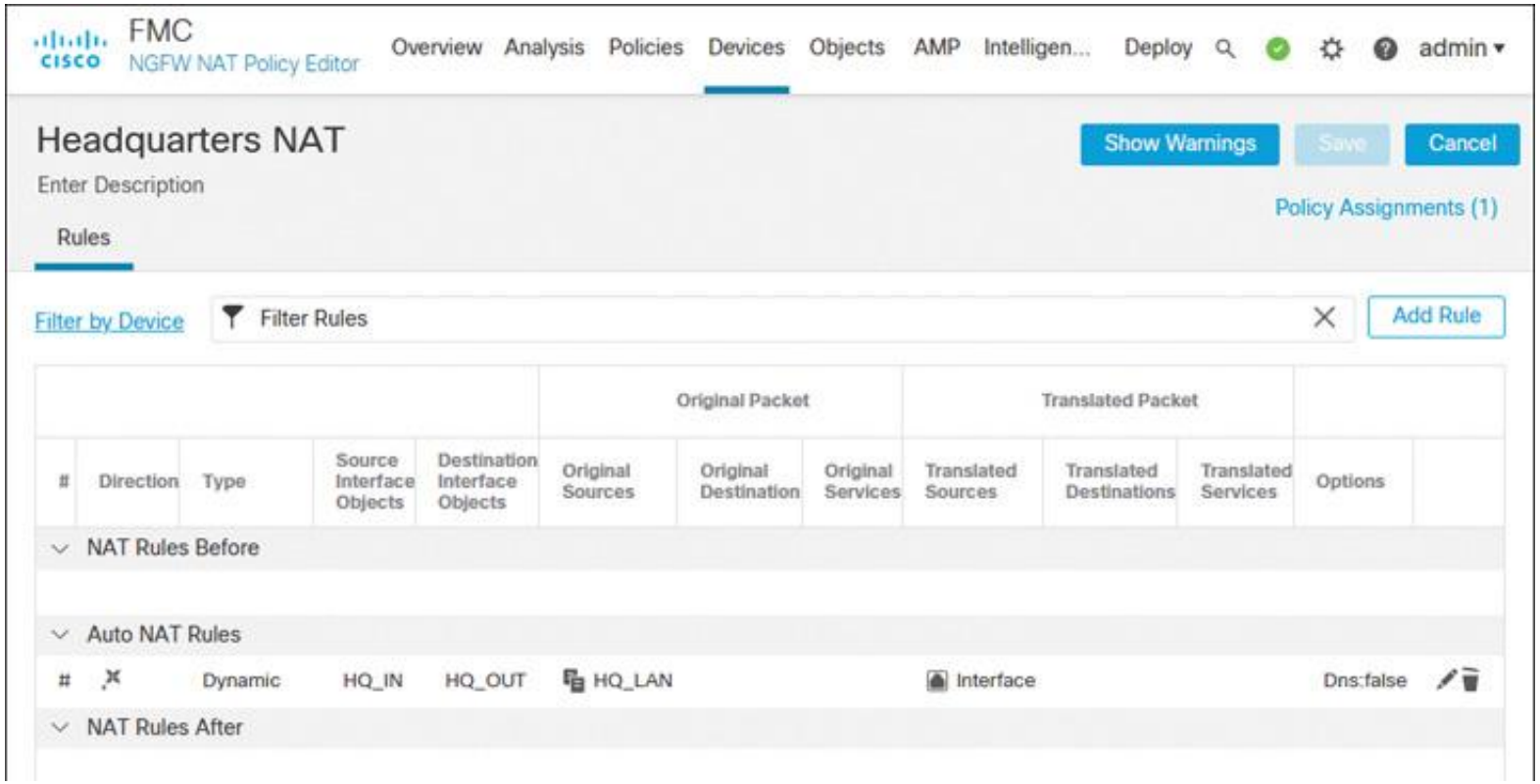


Site-to-Site VPN Deployment

- Example of P-to-P configuration

➢ NAT Policy

- If you configured NAT on outside-interface, exempt the internal traffic from being translated by adding an identity NAT rule
- This is known as a NAT exemption
  (The original source address and the translated source address are the same . The same for the destination address)



1) Click add Rule

MohsenKheradmand MK

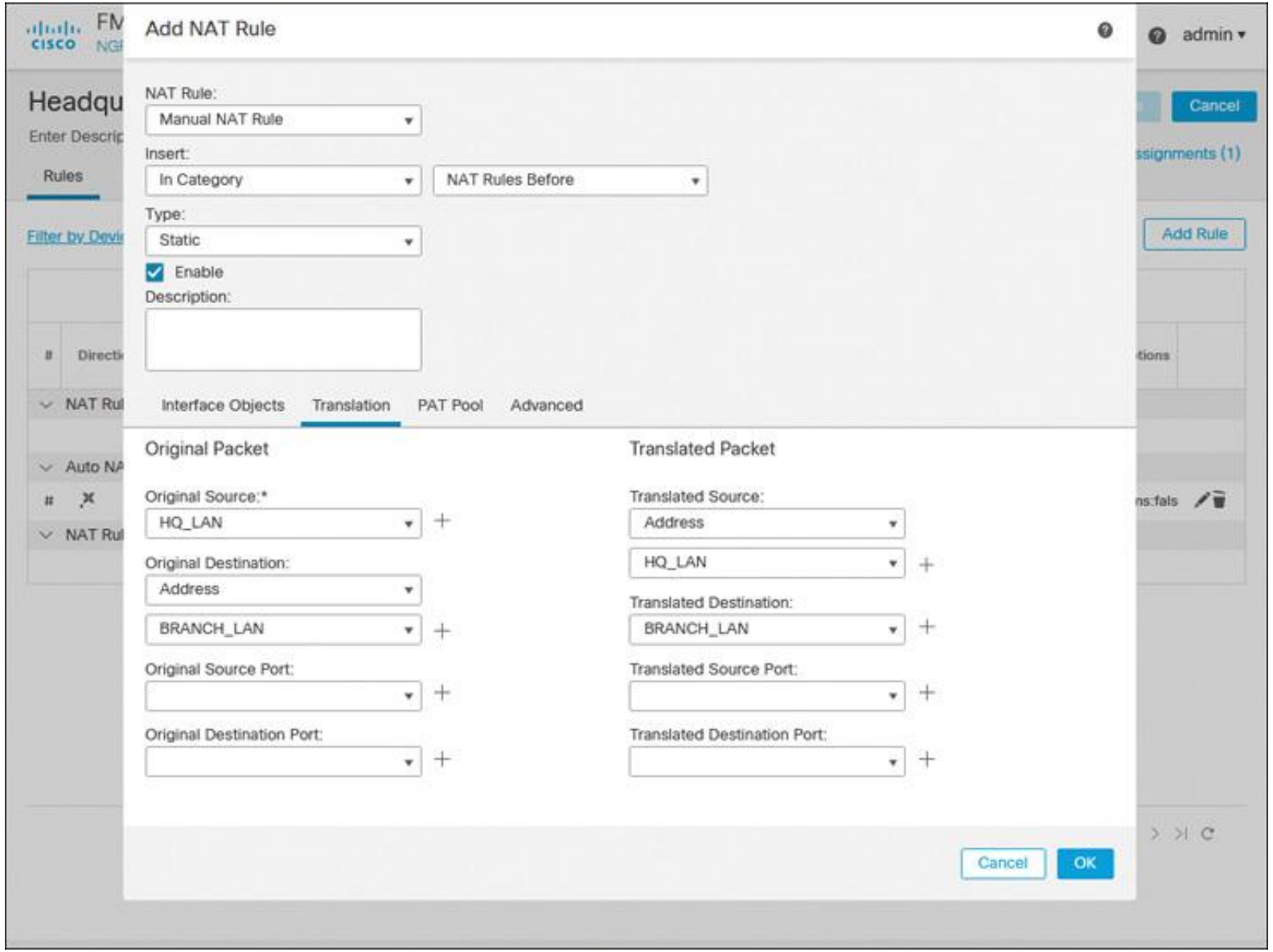
Site-to-Site VPN Deployment

- Example of P-to-P configuration

  ➢ NAT Policy

1) Enter a name for the new rule
2) Select Static from type
3) Original and translated source must be the same
4) Also set the original and translate destination same

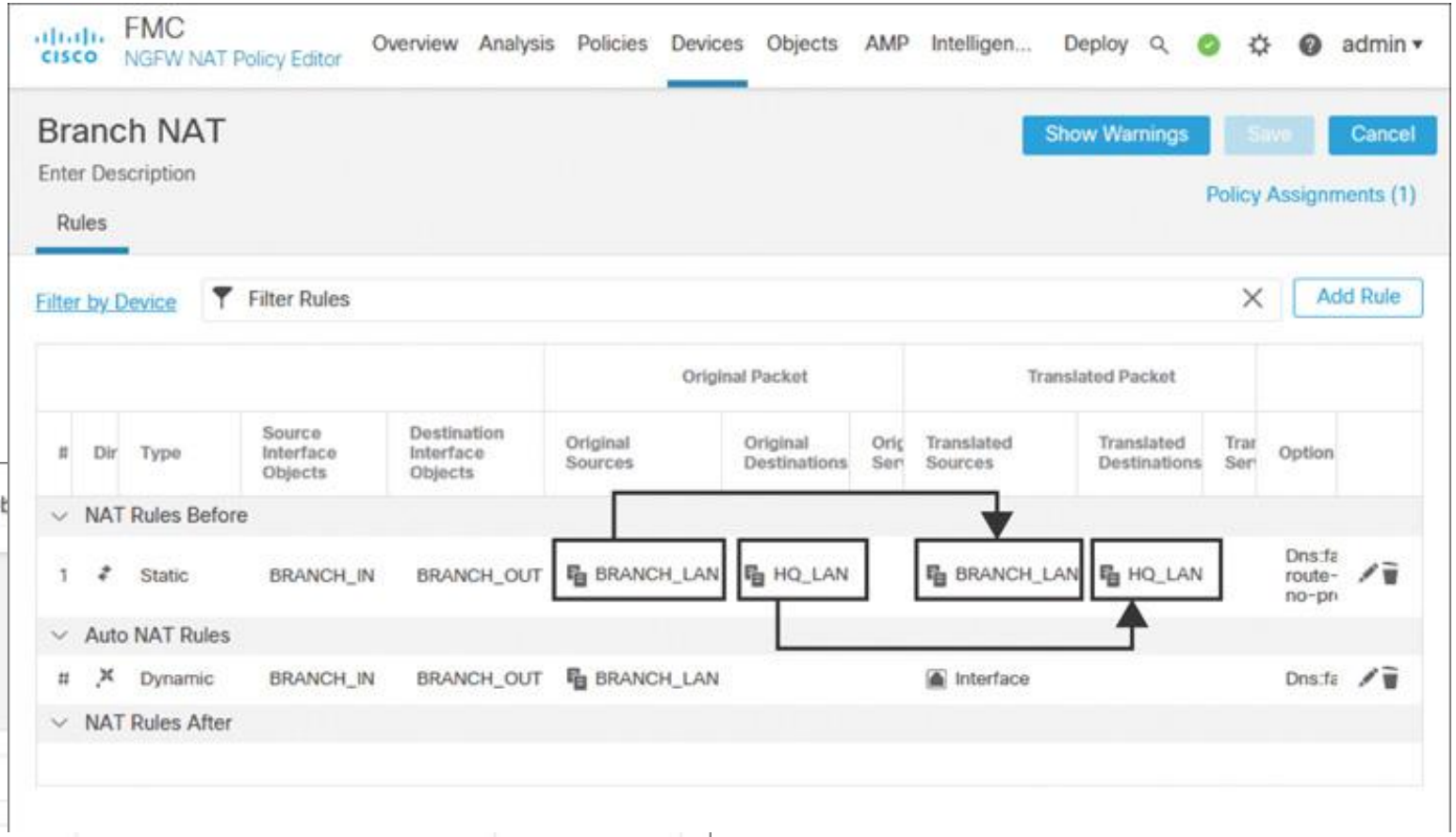
5) Do this on 2 side of VPN tunnel

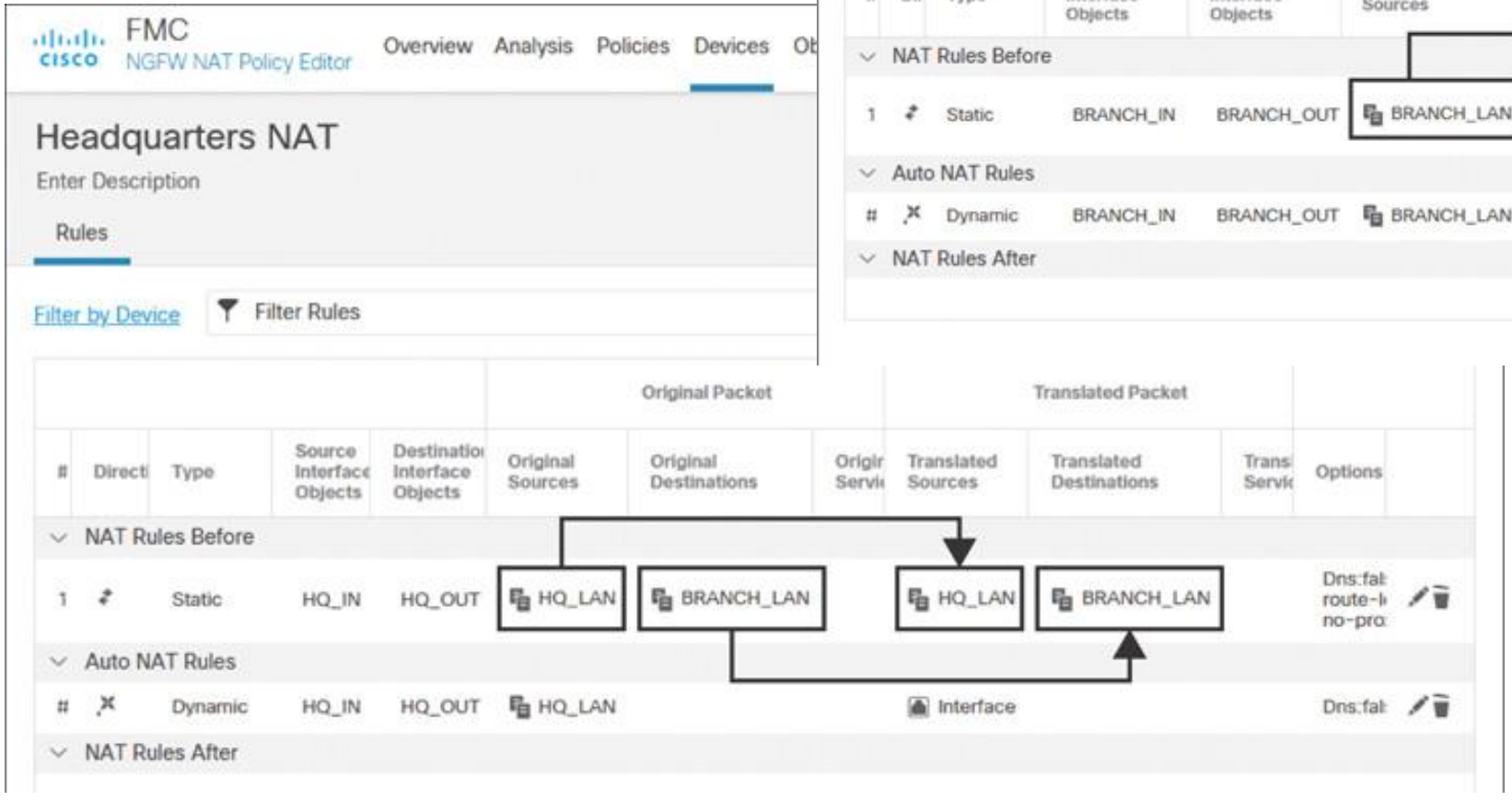


MohsenKheradmand MK

Site-to-Site VPN Deployment

- Example of P-to-P configuration
  - ➢ NAT Policy





MohsenKheradmand MK

Site-to-Site VPN Deployment

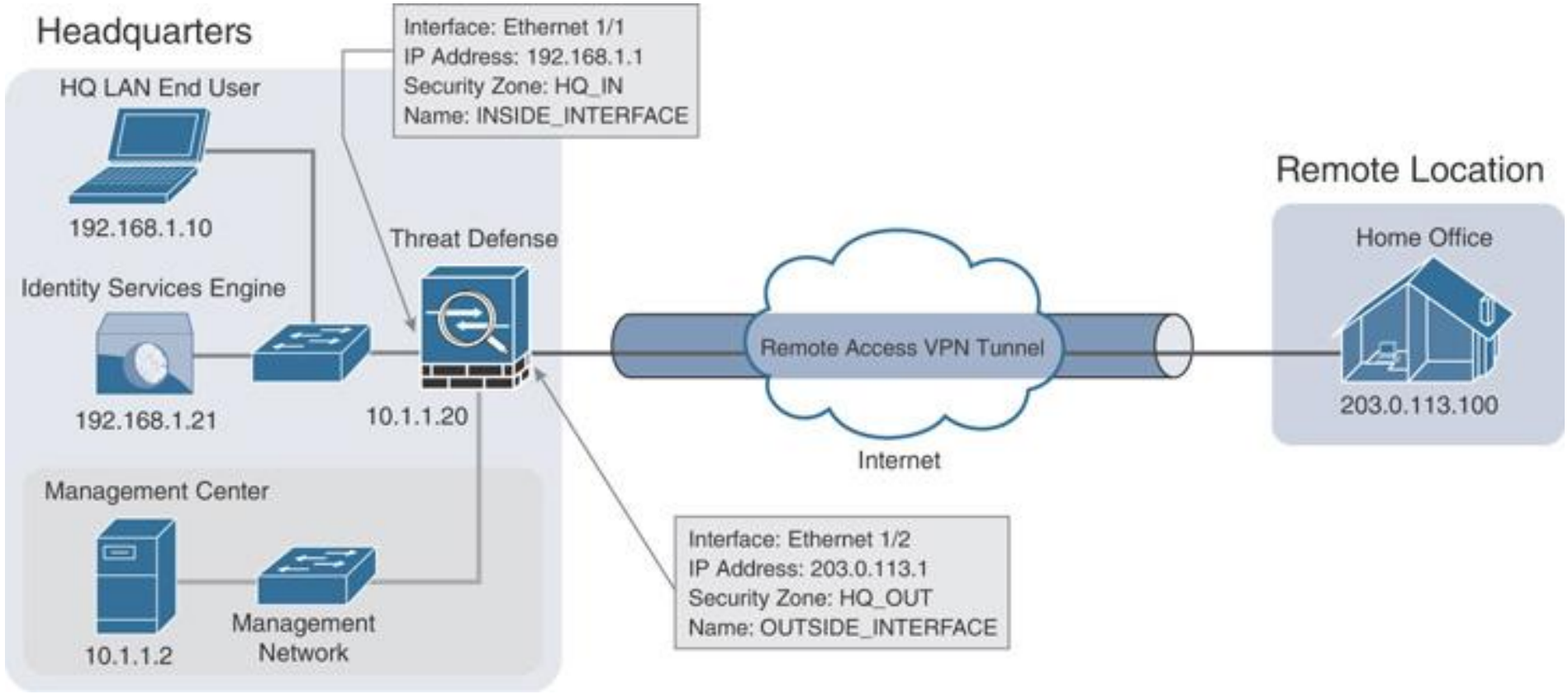
- Example of P-to-P configuration

  - Verification

> show running-config crypto

```
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-gcm-256 aes-gcm-192 aes-gcm
 protocol esp integrity null
crypto ipsec security-association pmtu-aging infinite
crypto map CSM_Outside_Interface_map 1 match address CSM_IPSEC_ACL_1
crypto map CSM_Outside_Interface_map 1 set peer 203.0.113.2
crypto map CSM_Outside_Interface_map 1 set ikev2 ipsec-proposal CSM_IP_1
crypto map CSM_Outside_Interface_map 1 set reverse-route
crypto map CSM_Outside_Interface_map interface OUTSIDE_INTERFACE
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption aes-256
 integrity sha512
 group 21
 prf sha512
 lifetime seconds 86400
crypto ikev2 enable OUTSIDE_INTERFACE
crypto ikev1 am-disable
```

Remote Access VPN Deployment



- If the interfaces of the Headquarters FTD are configured as a part of the site-to-site VPN , you can reuse them now

Remote Access VPN Deployment

➢ Prerequisites

✓ Enable one of the AnyConnect features licenses

There are three tiers of AnyConnect licenses:

- AnyConnect Plus (Advantage) :
  - - Offers the basic remote-access VPN services
  - - Must consider the total number of unique users
- AnyConnect Apex (Premier) :
  - - Advanced features in addition to the basic features
  - - Must consider the total number of unique users
- AnyConnect VPN Only :
  - - Allows any number of unique users to connect to a threat defense

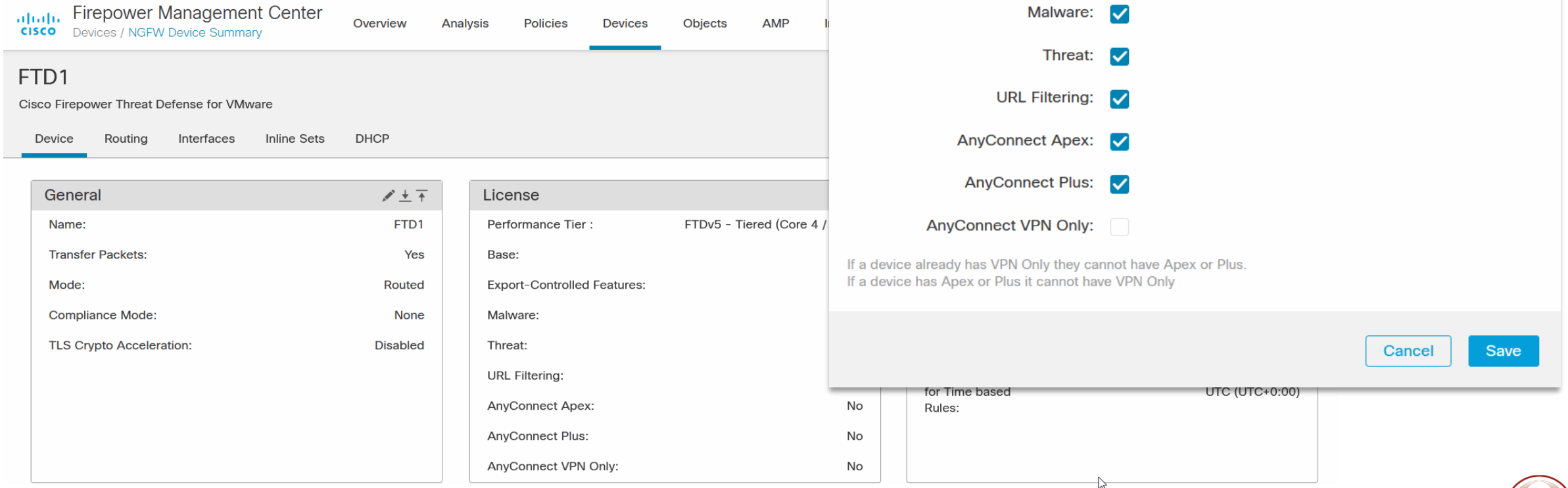
❑ License costs vary based on license type, duration, and user count.
❑ Not simultaneous connections & not total active remote access users.
❑ If you have 500 users authorized to use the VPN, you should buy licenses for 500 users.

Remote Access VPN Deployment

➢ Prerequisites

✓ Enable one of the AnyConnect features licenses

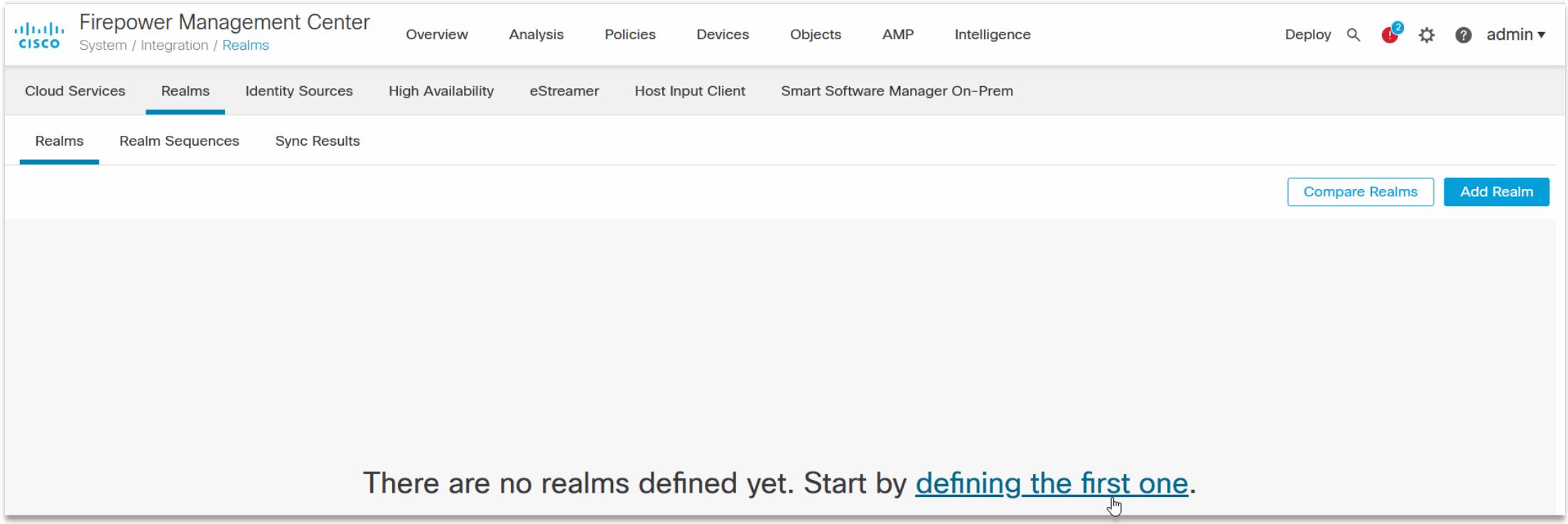
- Device > Device management > Device tab > License



Remote Access VPN Deployment

➢ User Authentication.

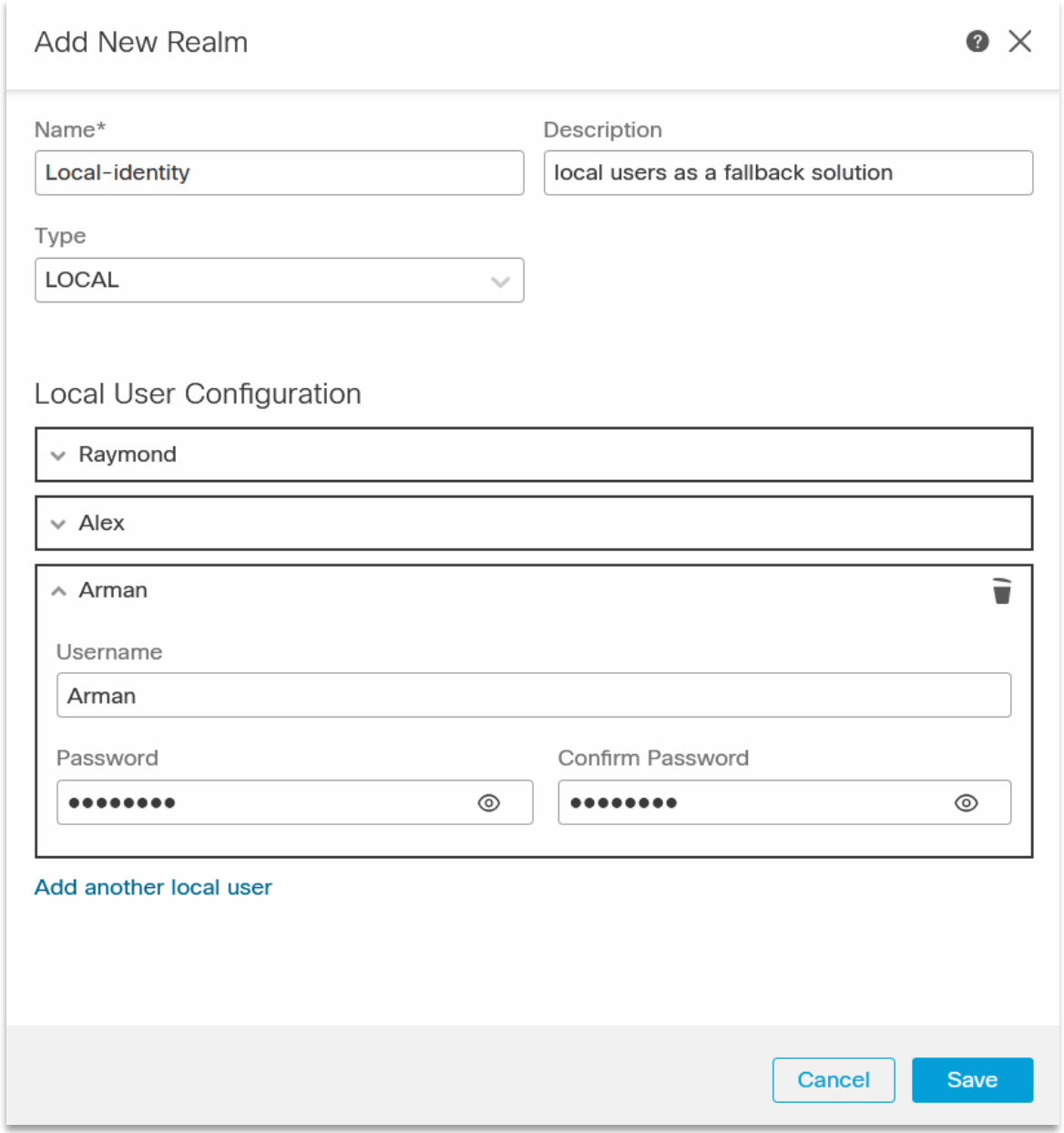
- Secure Firewall Version 7.x or higher supports local user authentication using local user database
- A large organization requires a dedicated AAA server to manage thousands of users
- You can add a new realm for local users by going to **System > Integration > Realms**



Remote Access VPN Deployment

- User Authentication.

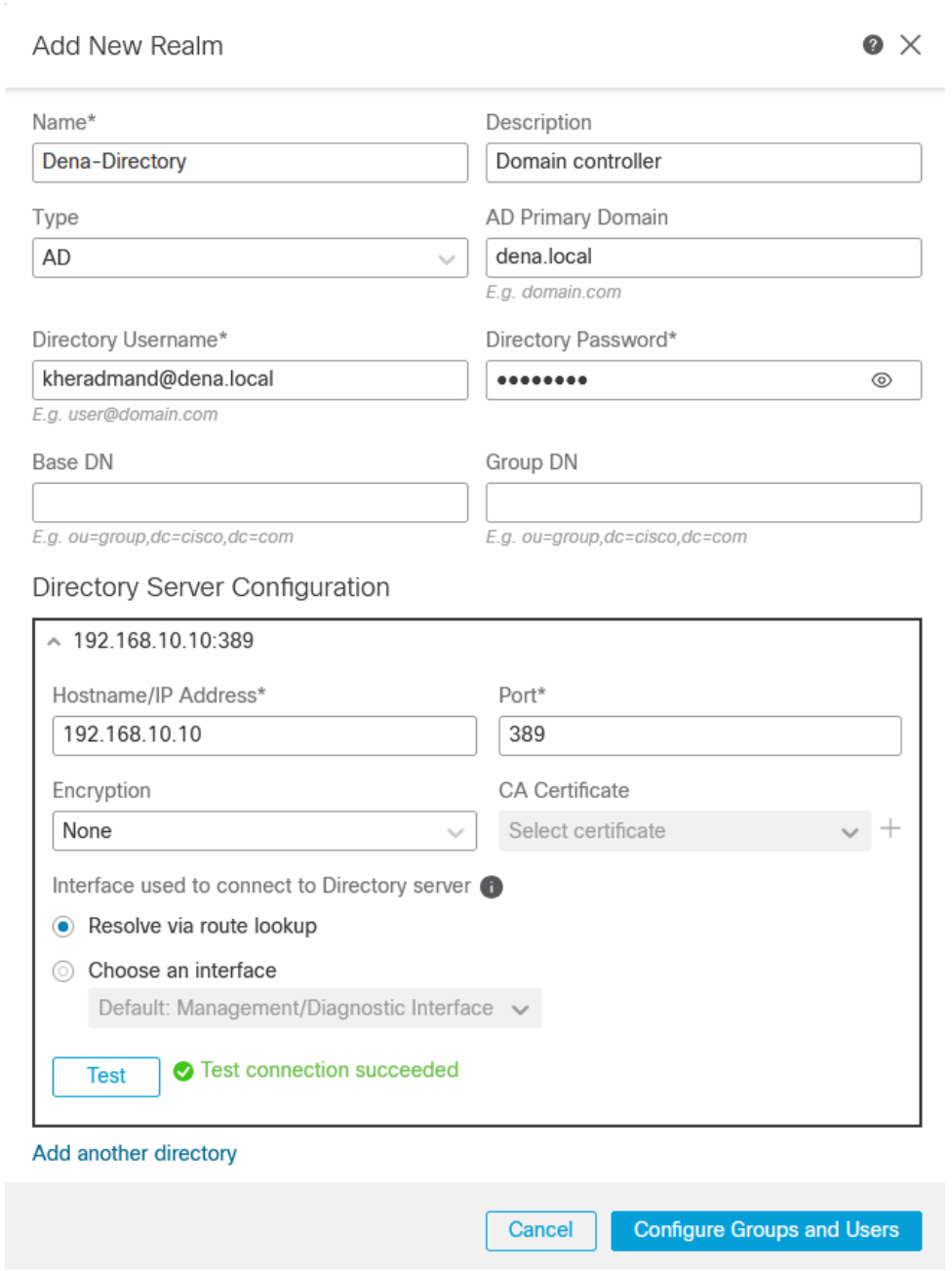
- Creating a local users as a Realm



Remote Access VPN Deployment

- User Authentication.

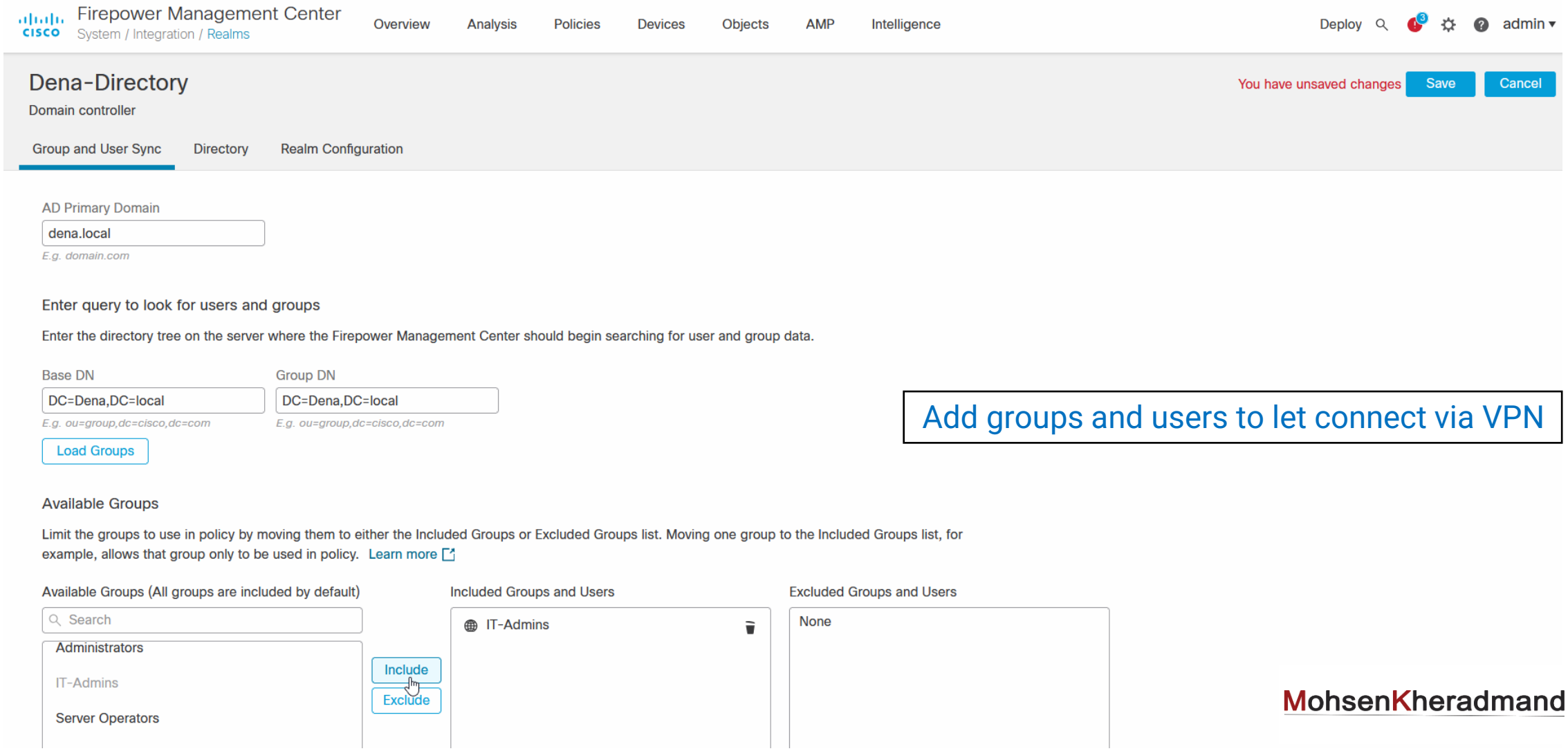
- Creating a Active directory as a Realm



MohsenKheradmand MK

Remote Access VPN Deployment

➢ User Authentication.

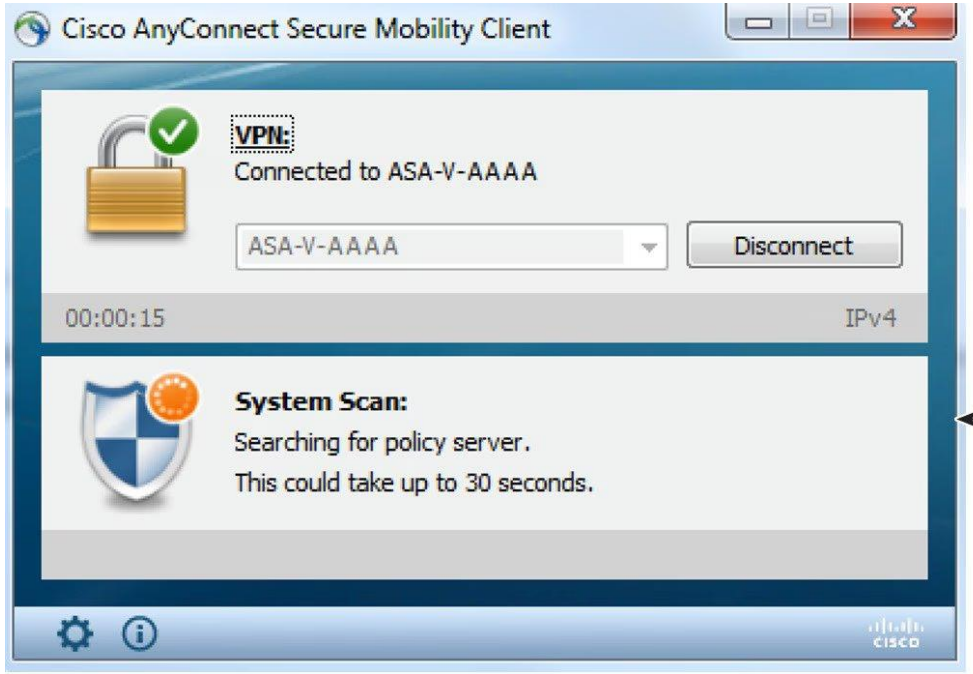


Add groups and users to let connect via VPN

MohsenKheradmand MK

Remote Access VPN Deployment

- AnyConnect Secure Mobility Client software
  - AnyConnect empowers a remote user to connect to the internal network from any geographic location
  - It supports both SSL and IPsec IKEv2 protocols
  - The AnyConnect client supports various operating systems, such as Windows, Mac OS, and Linux
  - Download from the Cisco Software Download Center and upload them to the management center



Remote Access VPN Deployment

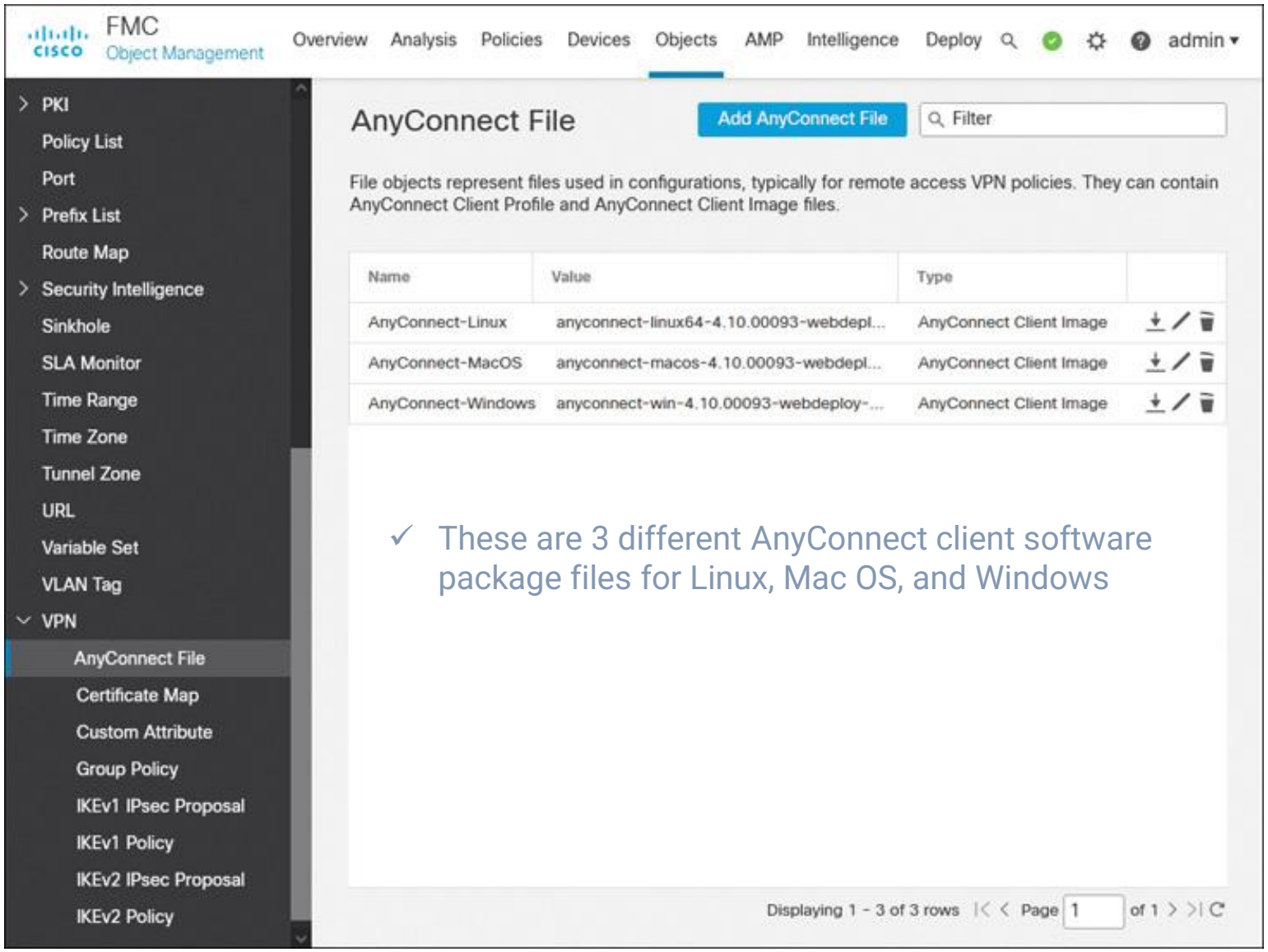
- AnyConnect Secure Mobility Client

Steps to Upload the AnyConnect:

- Objects > Object Management

- - VPN > AnyConnect File

- - - > Add AnyConnect File

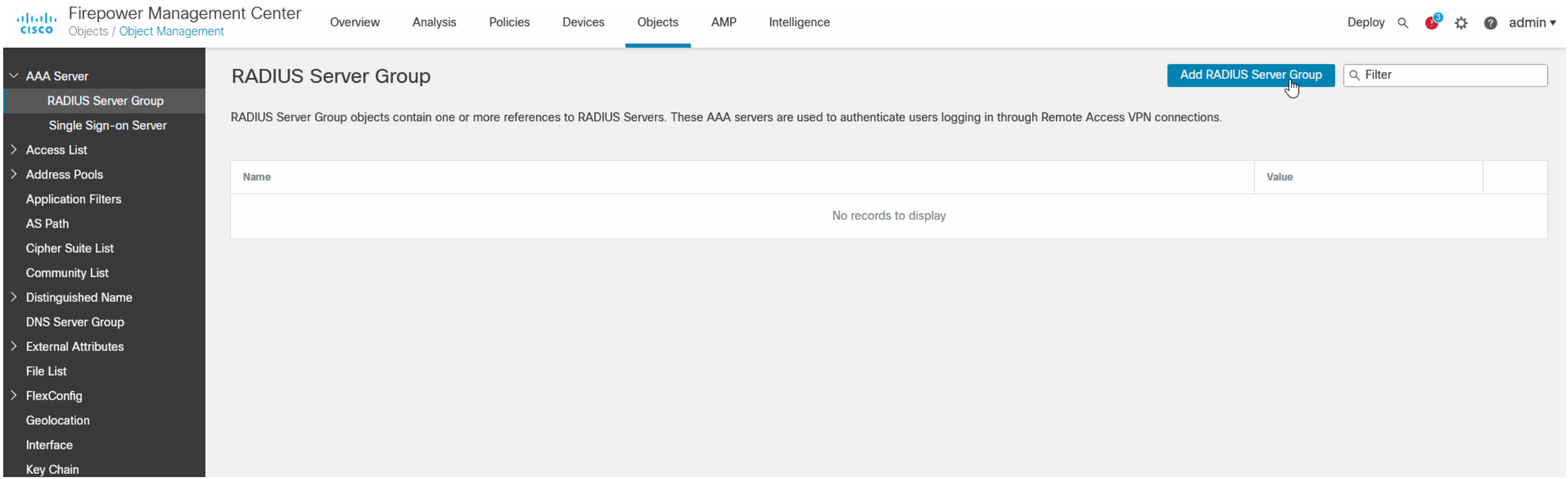


Remote Access VPN Deployment

➢ RADIUS Server Group

- Using the AAA servers , you can add a single server or a group of servers to authenticate remote access VPN users

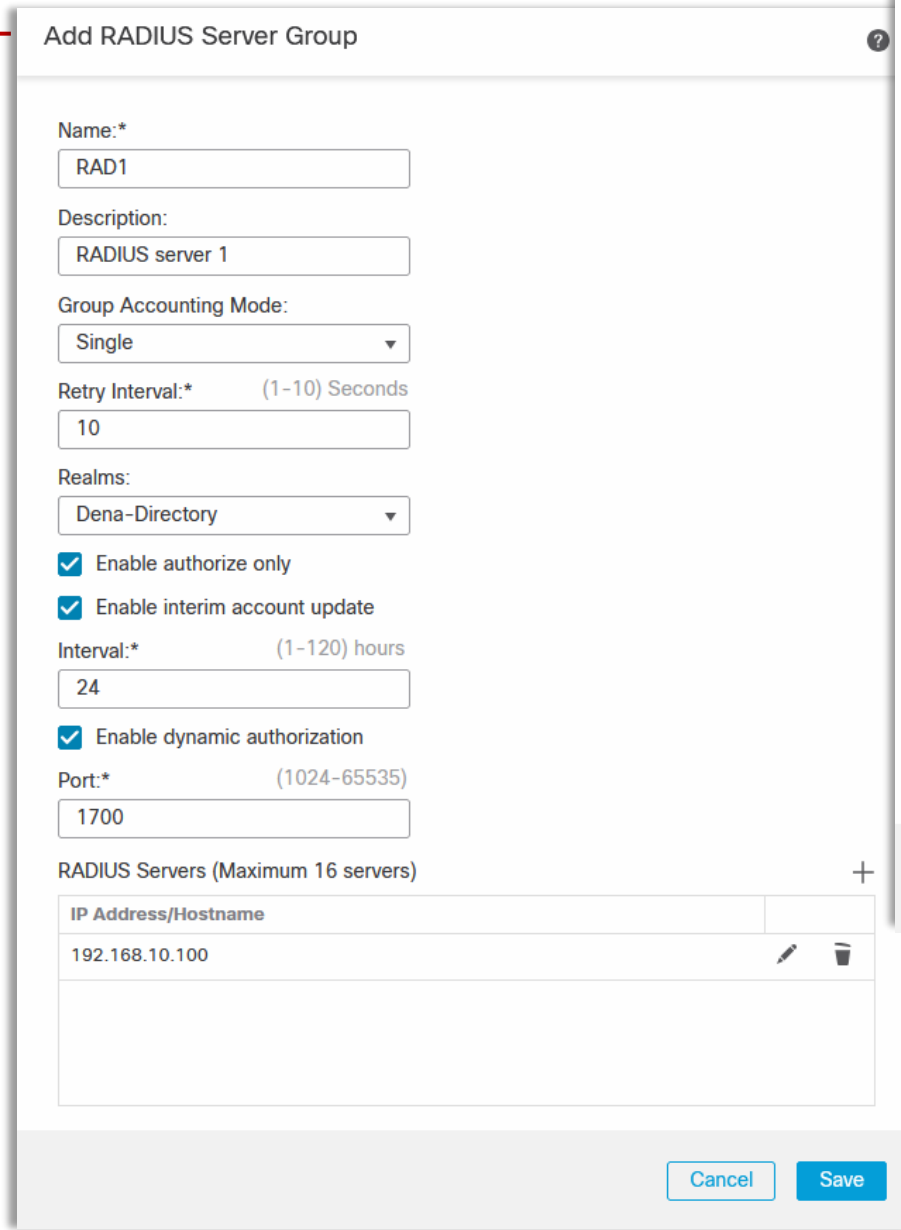
AAA Server > RADIUS Server Group

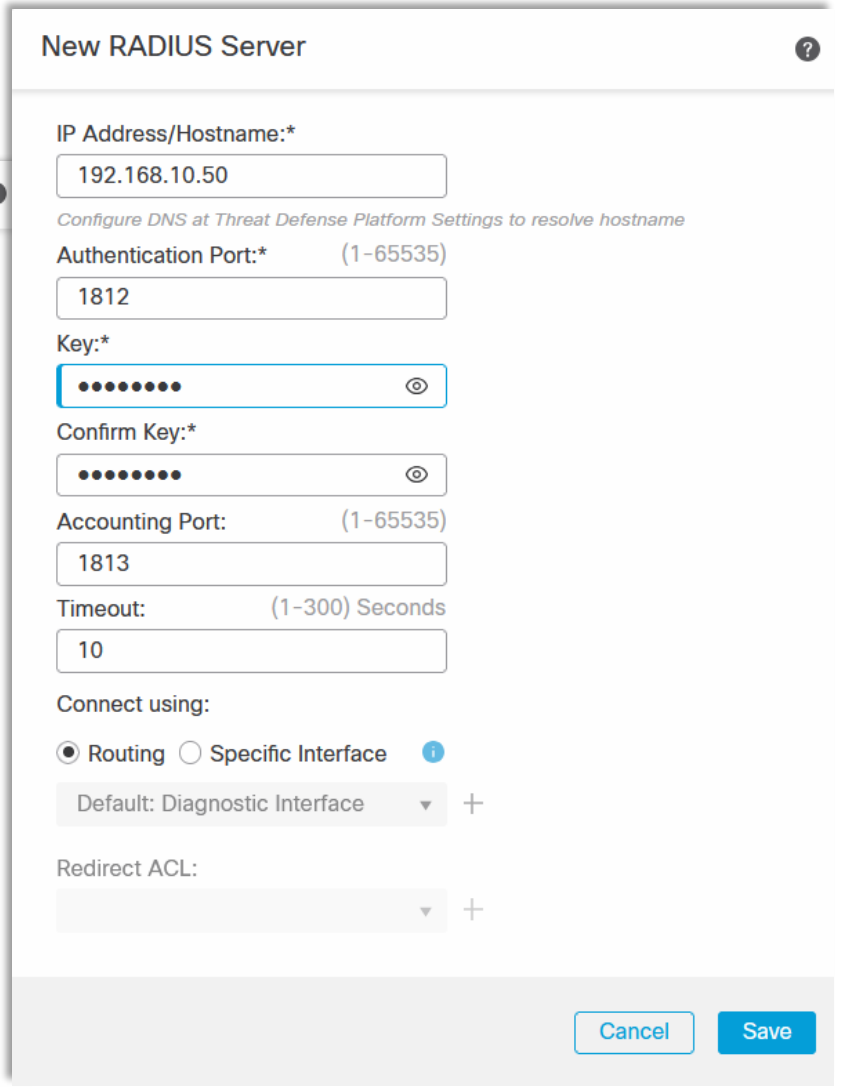


Remote Access VPN Deployment

➢ RADIUS Server Group

Enter appropriate information of RADIUS servers (AAA)





Remote Access VPN Deployment

➢ Certificate Enrollment

- You can use the Cert Enrollment object to enter information about the certification authority (CA) server in your (PKI).
- Secure Firewall offers many ways to select an enrollment type:

✓ PKCS12 File:

- - Public Key Cryptography Standard (PKCS) file is a single encrypted file that can contain information about the server certificate, any intermediate certificates, and the private key.

✓ SCEP:

- - Simple Certificate Enrollment Protocol (SCEP) , establishes a direct connection between a threat defense and a CA server, and allow the threat defense to obtain an identity certificate directly from the CA.

✓ Manual:

- - Copy the certificate information that you obtain from a CA server and paste it manually on Secure Firewall.

✓ Self-signed:

- - Allow the threat defense to act as a CA server using its self-signed root certificate.

✓ EST

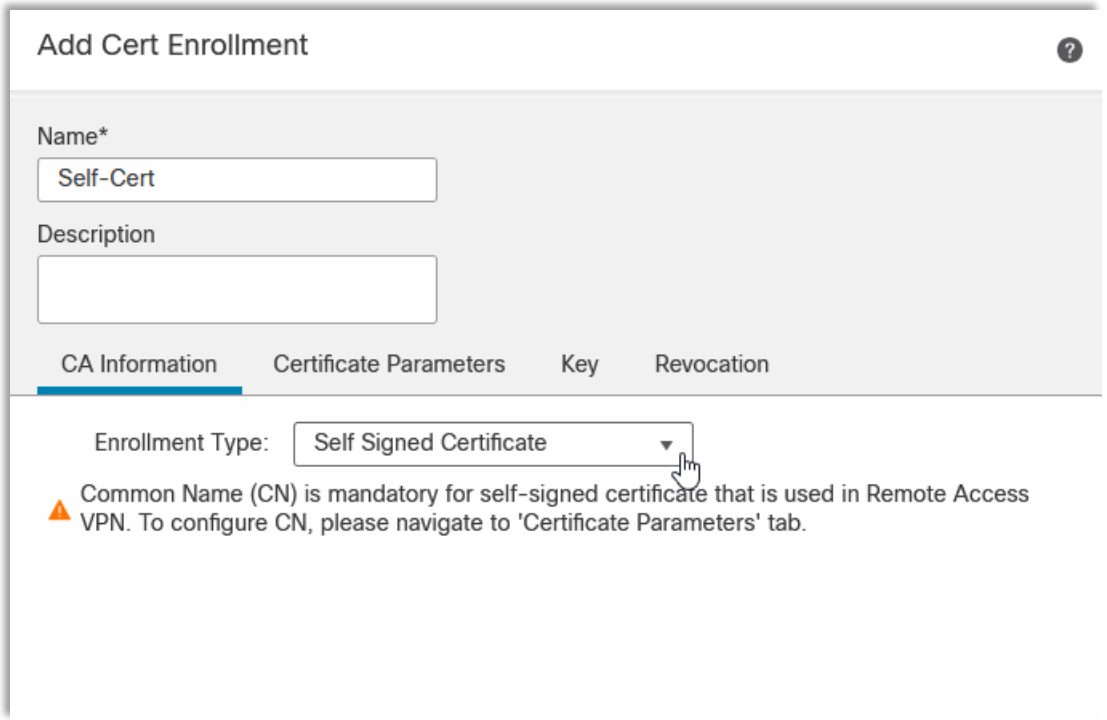
- - Enroll / re-enroll device certificates from CA services using secure channels, specifically HTTP over TLS

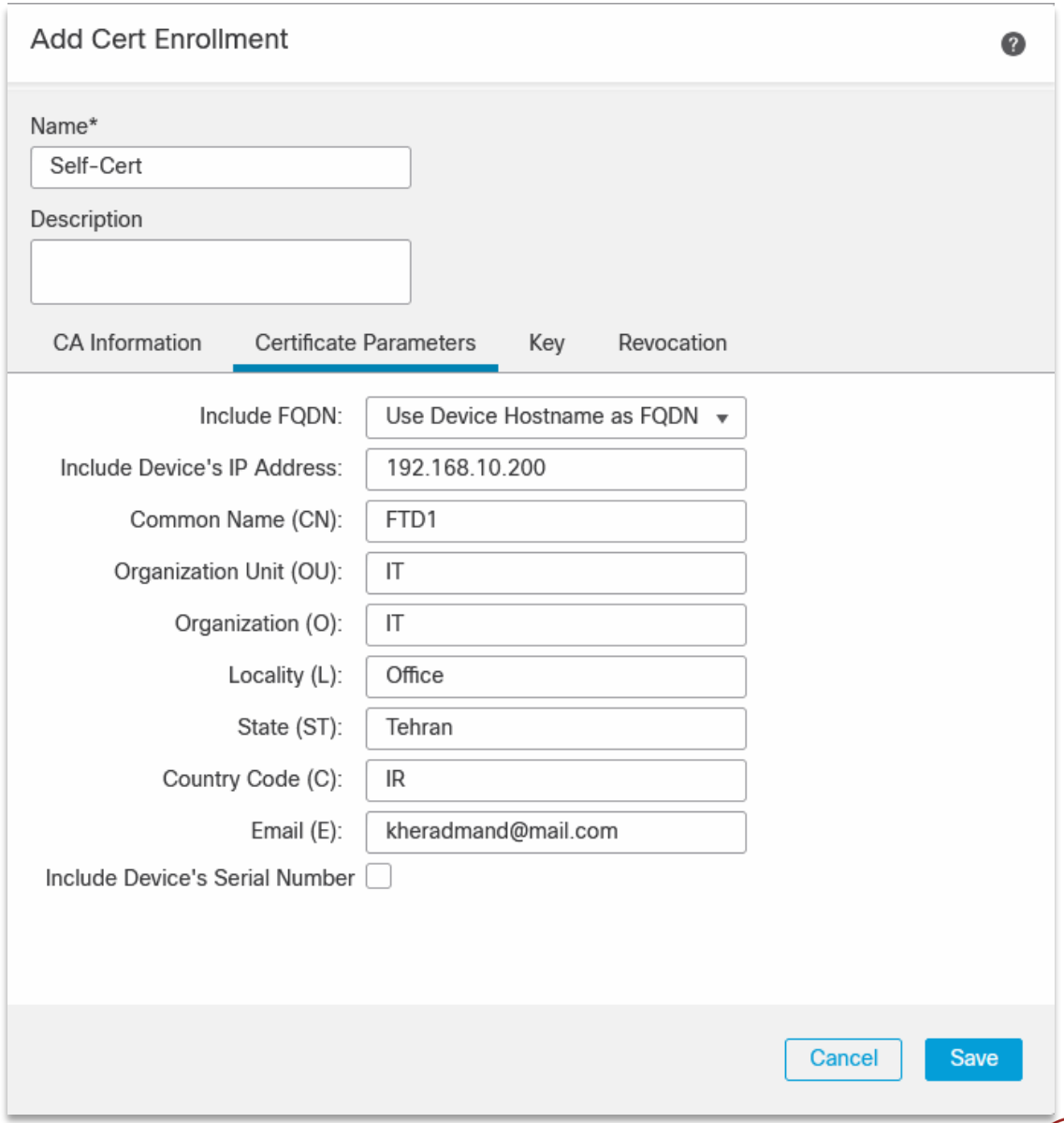
Remote Access VPN Deployment

➢ Certificate Enrollment

- Objects > Object Management > PKI > Cert Enrollment > Add Cert Enrollment

✓ You can use Self Signed Cert if any CA is not accessible

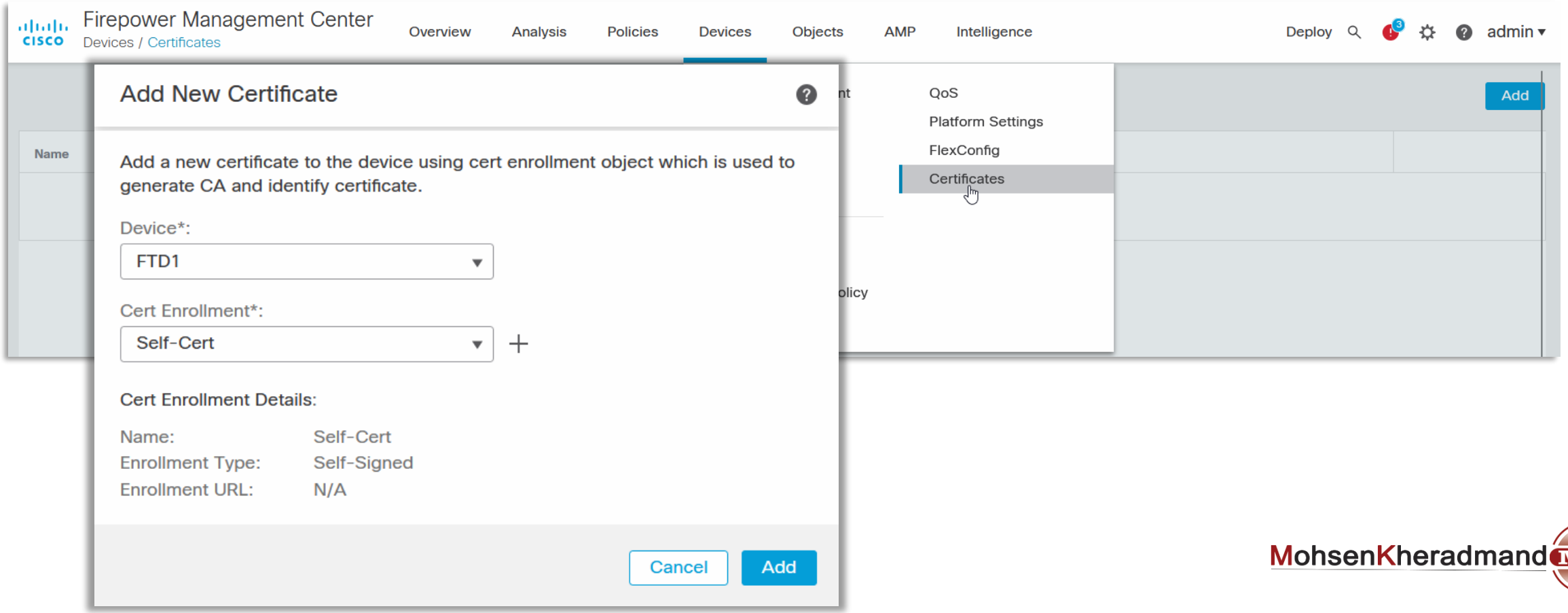




Remote Access VPN Deployment

➢ Certificate Enrollment

- Devices > Certificates
- Add the certificate to your Secure Firewall

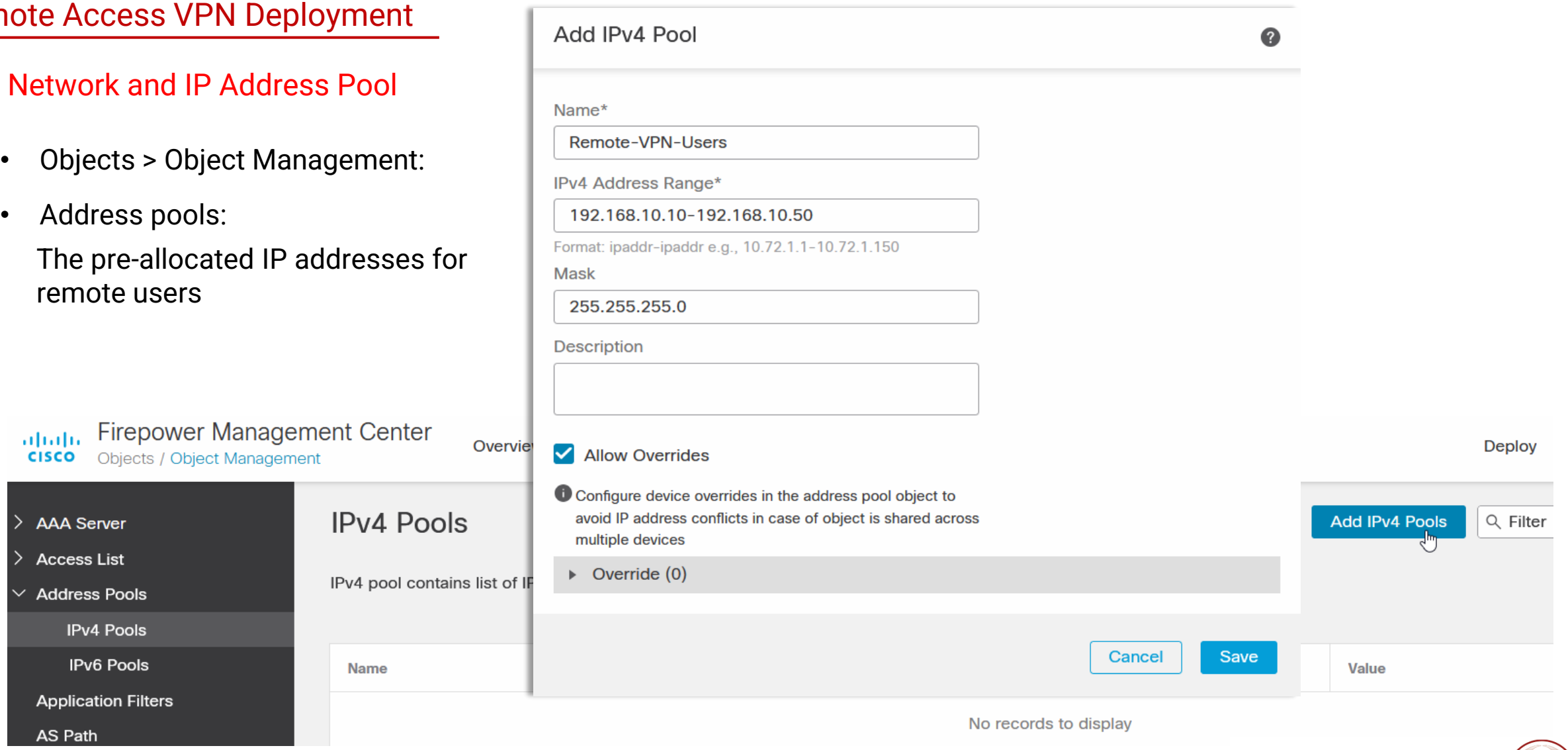


Remote Access VPN Deployment

➢ Network and IP Address Pool

- Objects > Object Management:
- Address pools:

  The pre-allocated IP addresses for remote users

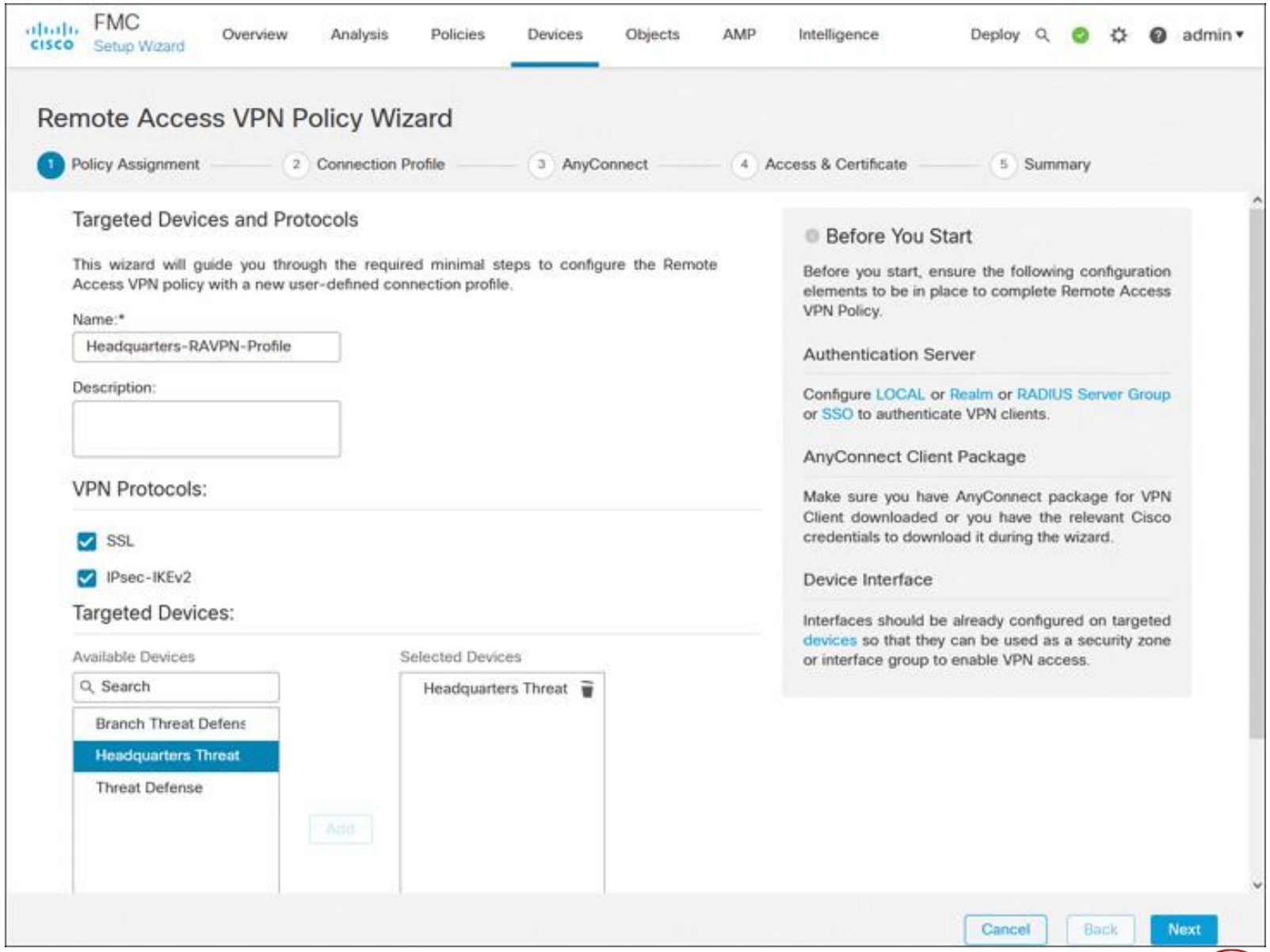


Remote Access VPN Deployment

➢ Remote Access VPN Policy

1) Devices > VPN > Remote Access.
2) Click the Add
3) Name the VPN policy.
4) select SSL or IPsec IKEv2, or both.
5) Add the FTD to deploy the policy

- Click Next



Remote Access VPN Deployment

➢ Remote Access VPN Policy

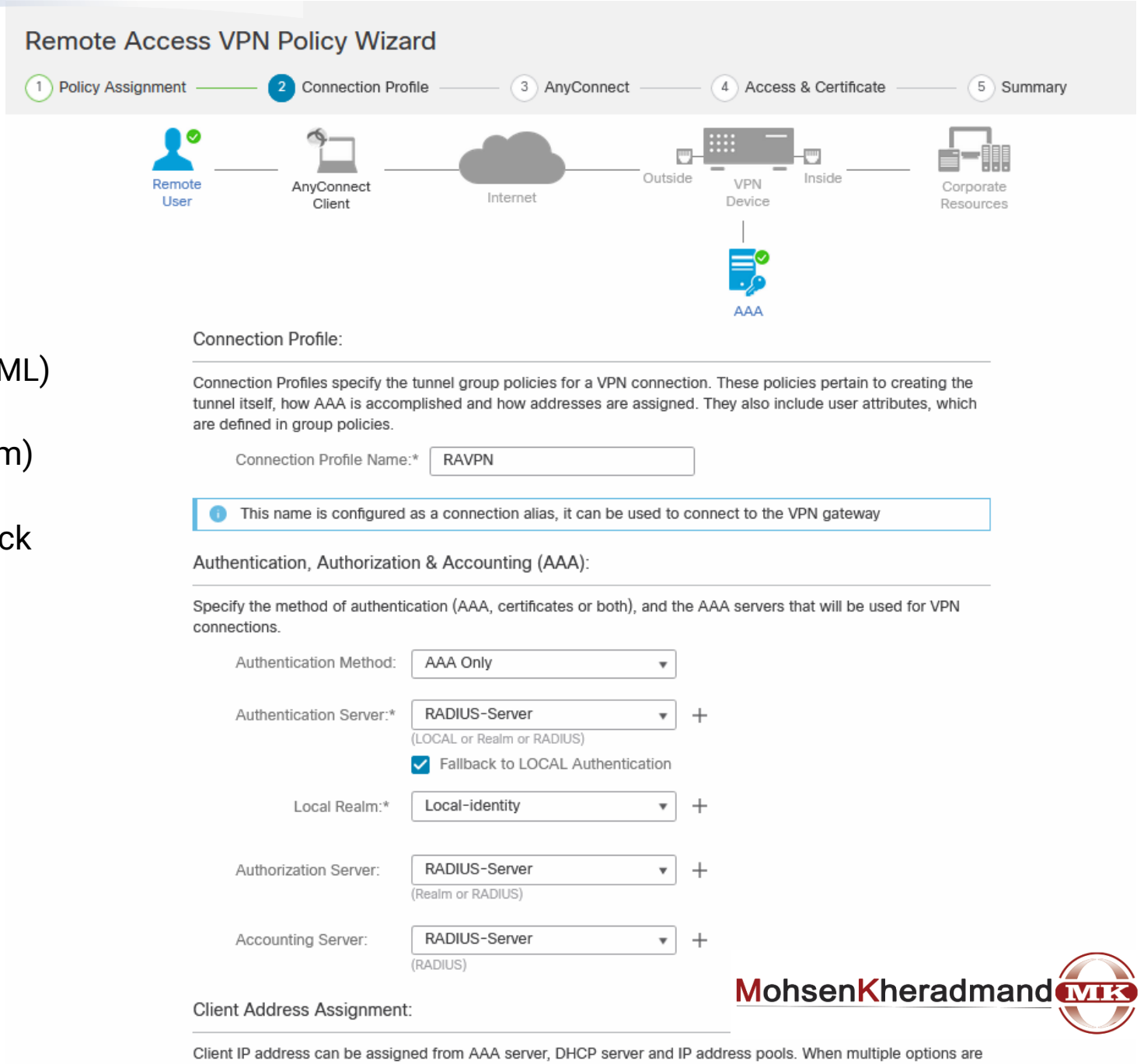
6) Enter a name for connection profile

7) Select authentication method (AAA , Cert , SAML)

8) Select Authentication server (i.e. AAA or realm)

9) Optionally, select the Local Realm as a fallback

10) Select authorization and accounting servers



Remote Access VPN Deployment

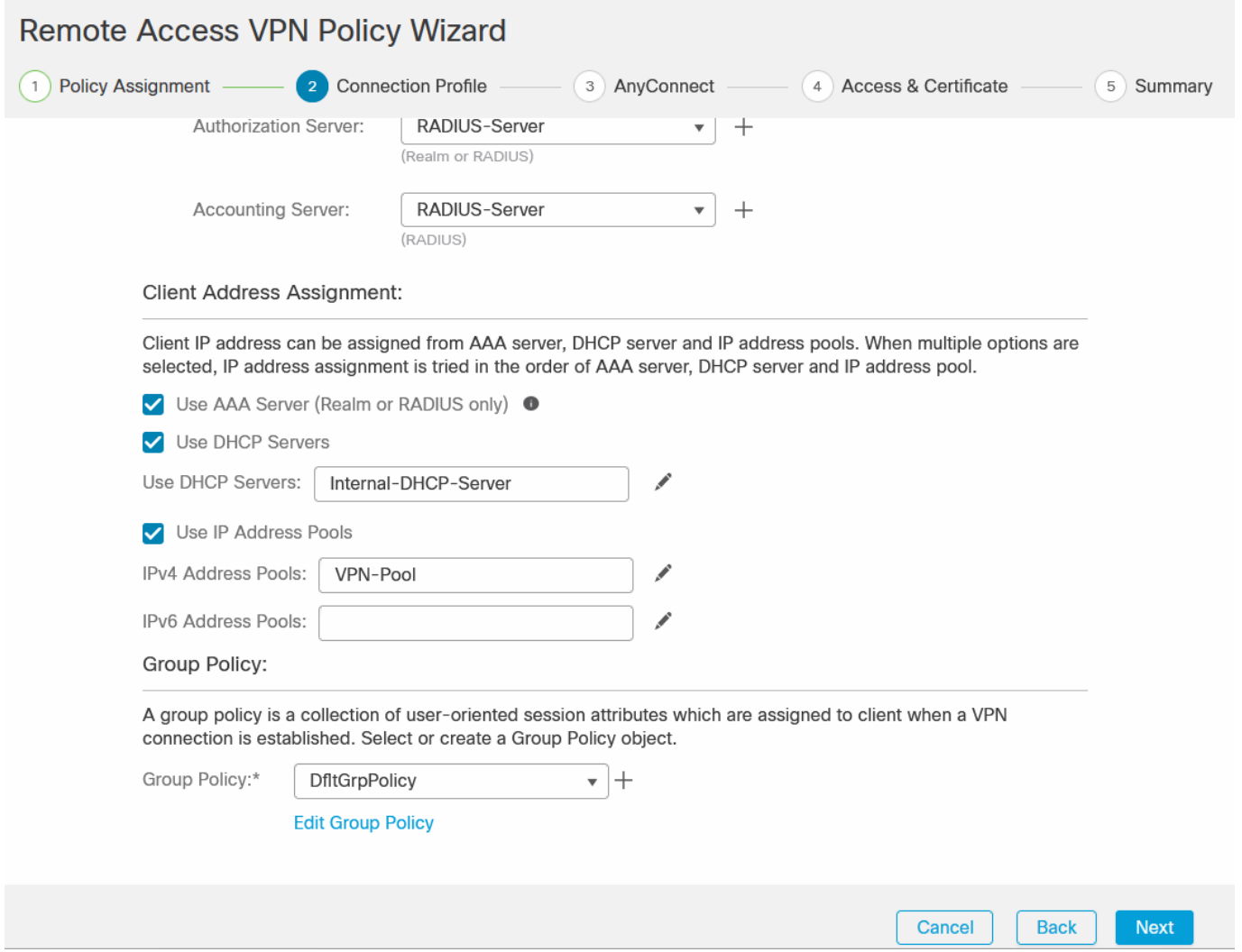
➢ Remote Access VPN Policy

11) Select Client Address Assignment method

- Use AAA server address range
- Use the DHCP server
- Use local address range (predefined in FMC)

12) Select DfltGrpPolicy

- Click Next

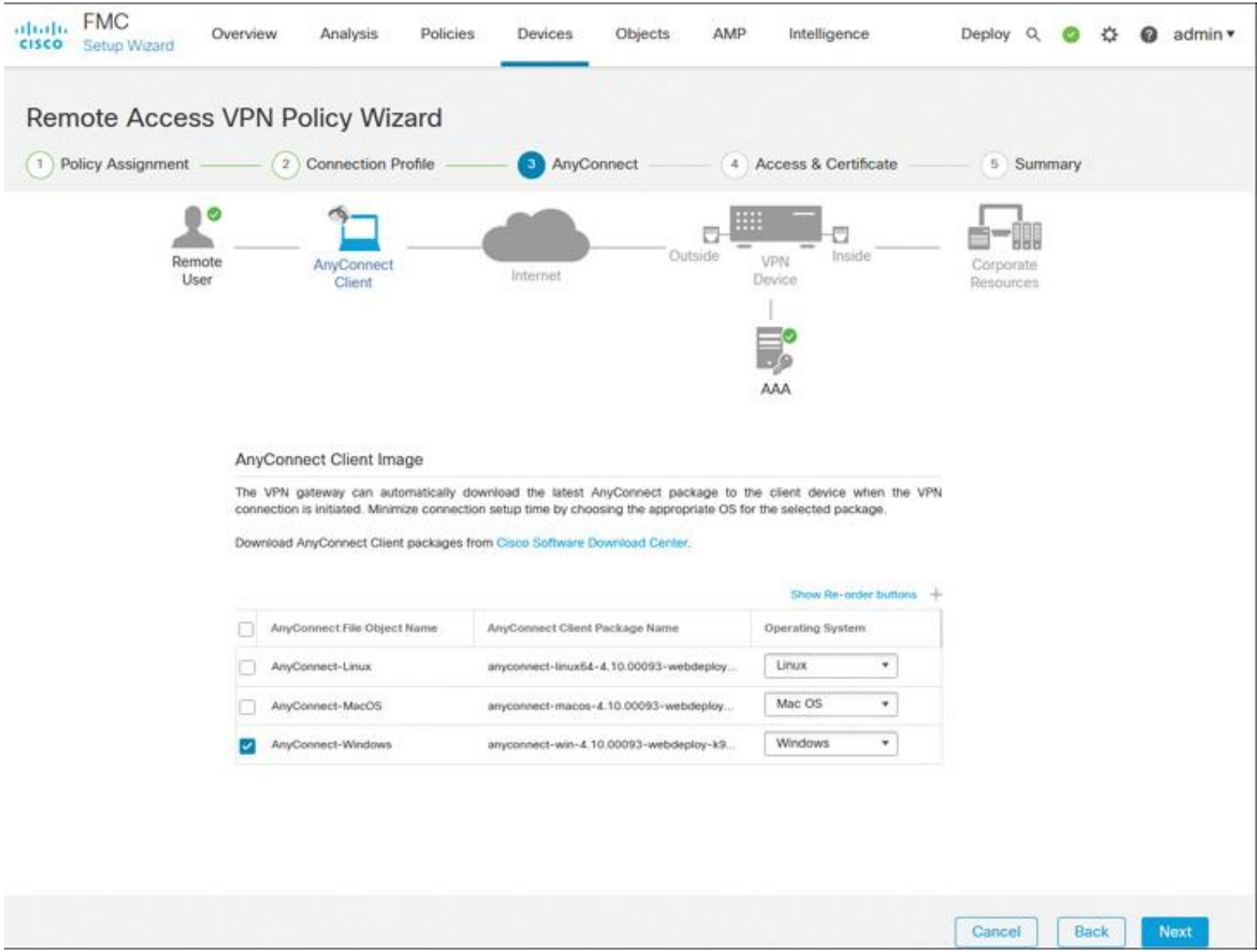


Remote Access VPN Deployment

- Remote Access VPN Policy

13) select one or more AnyConnect client images that you uploaded to the FMC earlier

- Click Next



Remote Access VPN Deployment

- Remote Access VPN Policy

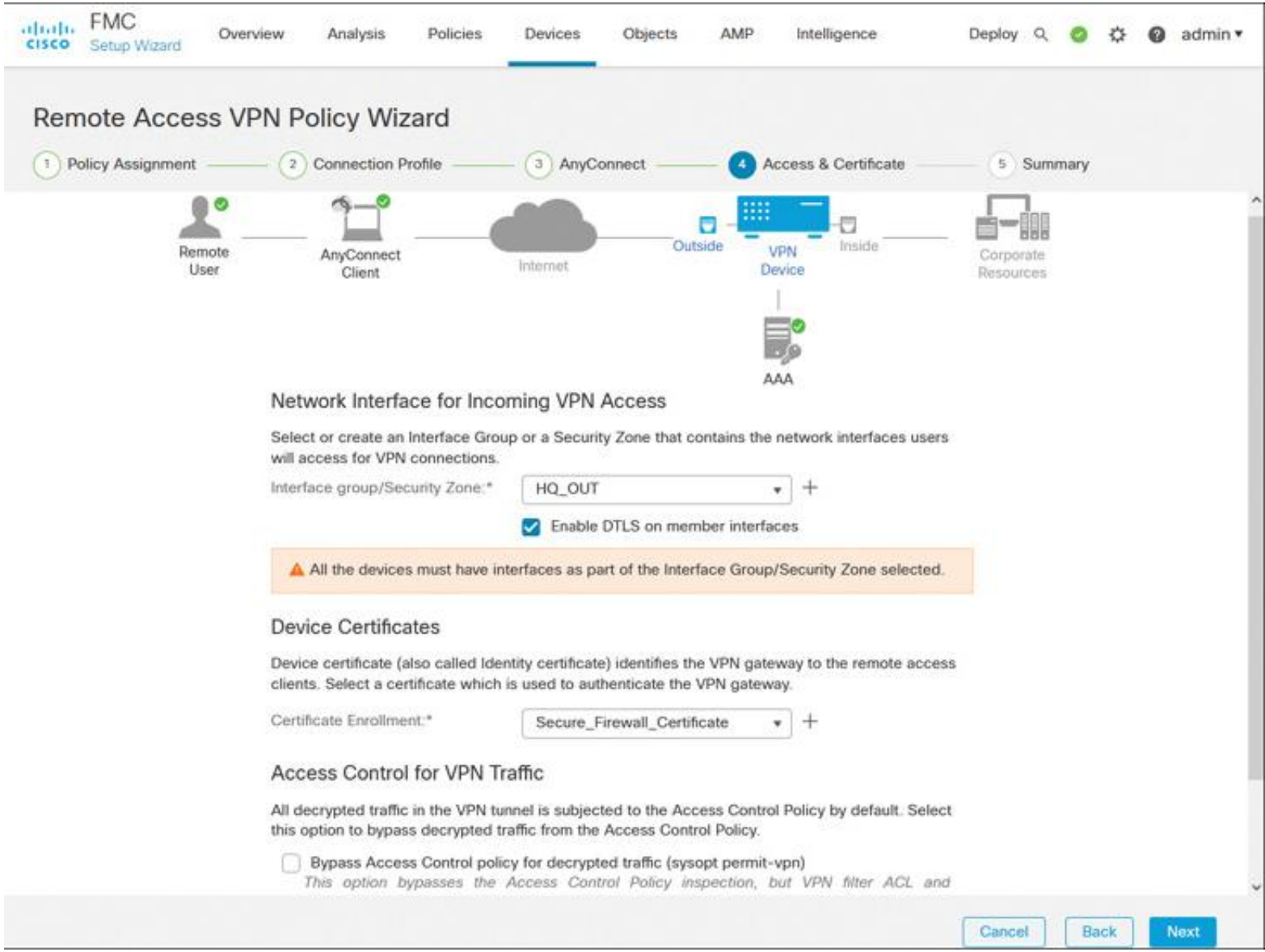
13) Select the security zone, (HQ_OUT) which is associated with the outside interface

14) Select the Certificate, which you installed on the threat defense earlier.

- - This certificate is used to authenticate the VPN headend.

13) Click Next and click Finish

14) Deploy > Deployment



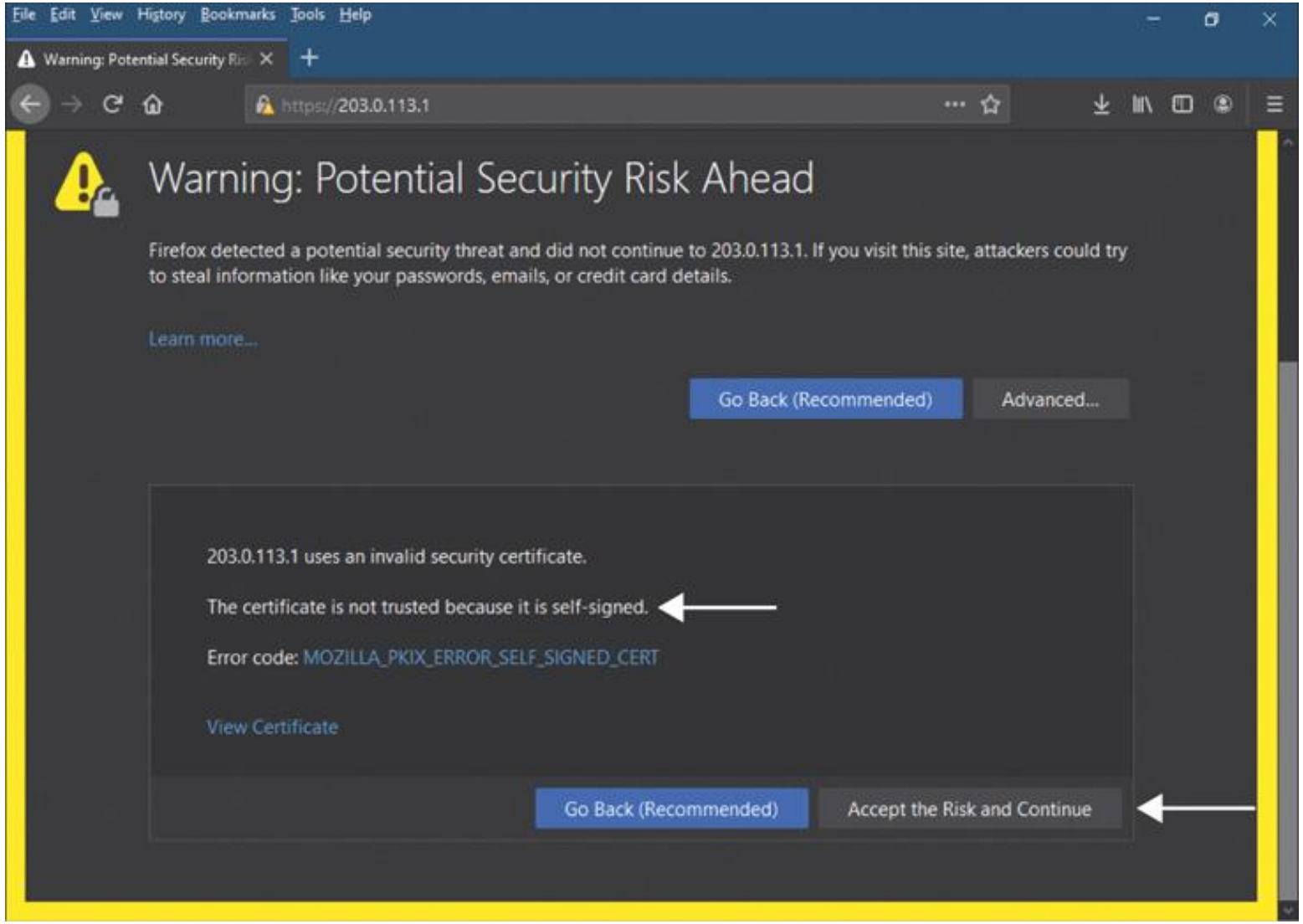
Remote Access VPN Deployment

- Verification

a) In the remote host open a browser.

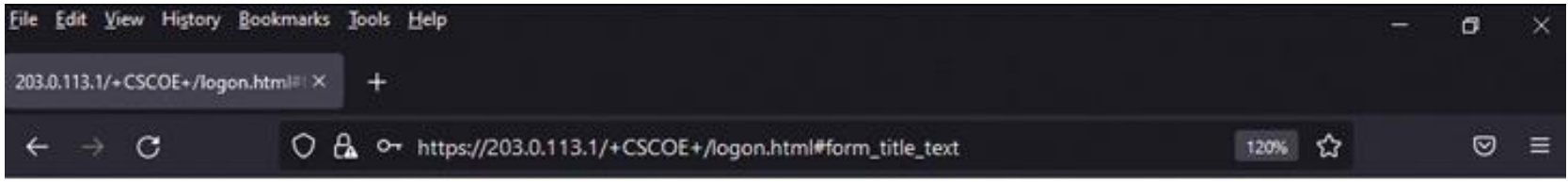
b) Enter the IP address of the FTD's outside interface

c) If you used a self-certificate , you are prompt to Accept the risk



Remote Access VPN Deployment

- Verification



a) Select the VPN name from Group

b) Enter the username and password

c) Click the Logon

Remote Access VPN Deployment

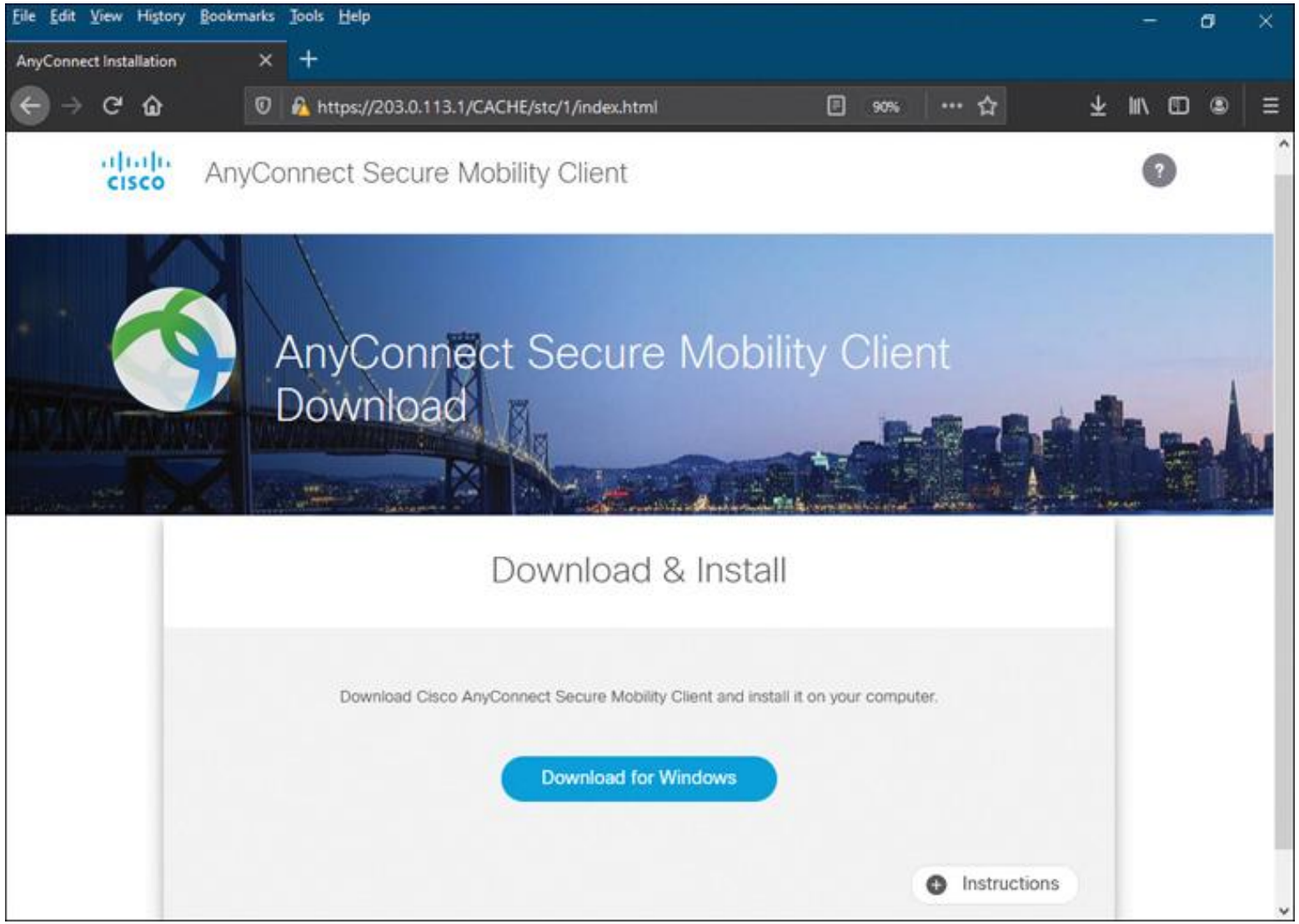
- Verification

a) Select the VPN name from Group

b) Enter the username and password

c) Click the Logon

d) The browser prompts you to download and install the AnyConnect Secure Mobility Client



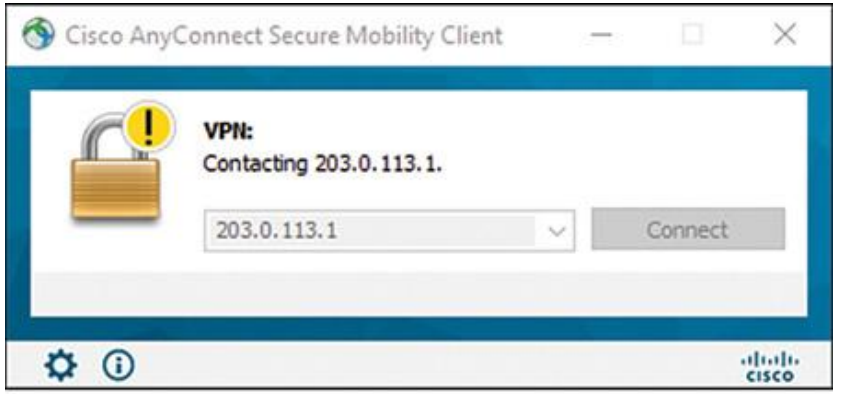
Remote Access VPN Deployment

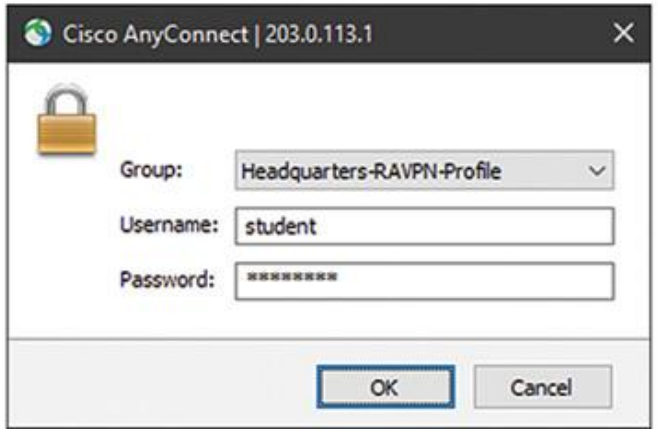
➢ Verification

a) When the installation is complete, open the AnyConnect client , enter the IP address of the FTD's outside interface

b) Click the Connect button. A login window appears

c) Enter the username and password again and click Ok



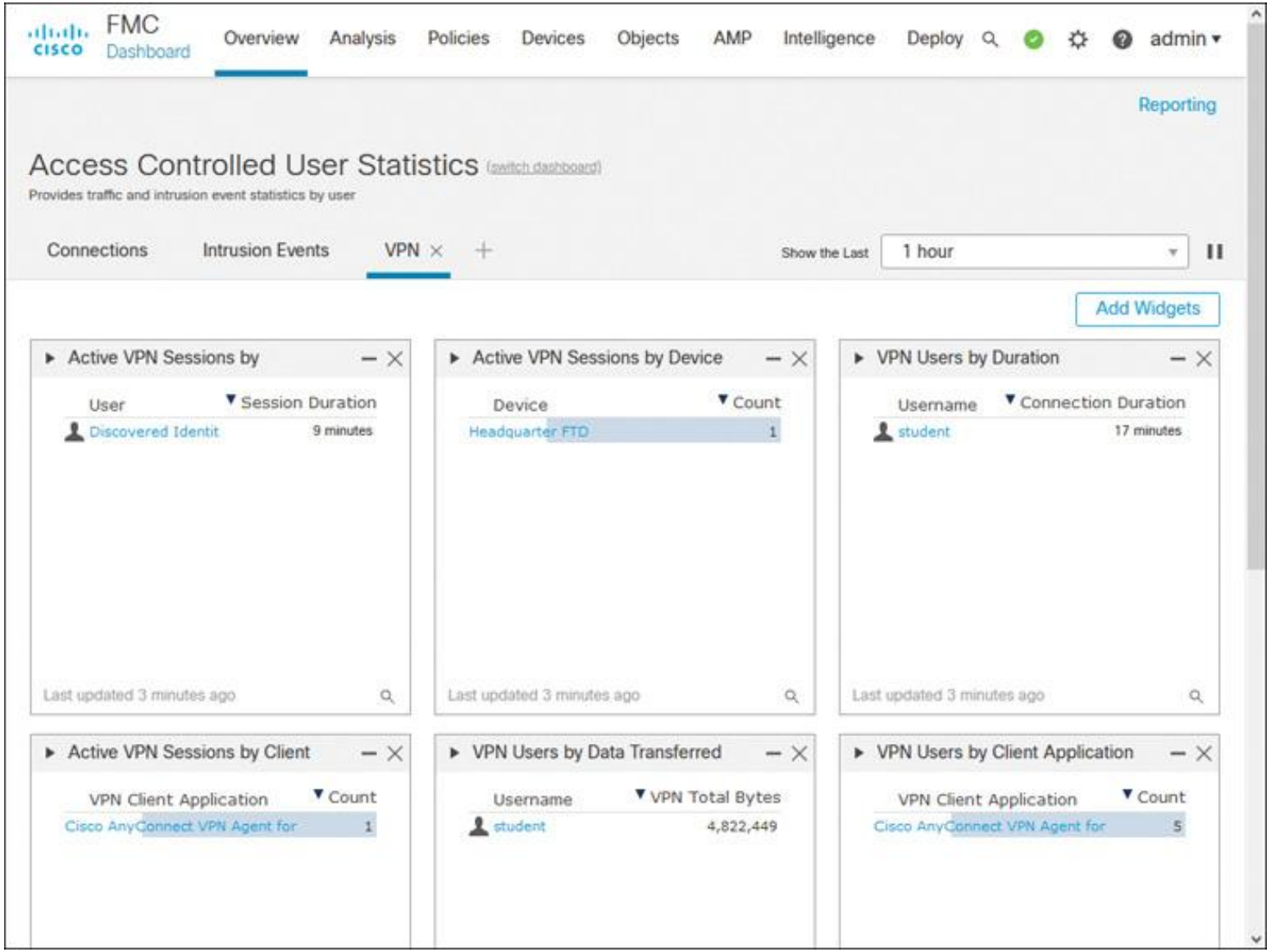


Remote Access VPN Deployment

- Verification

The FMC Dashboard Shows VPN User Sessions

You can also check the connection properties of LAN interface of the user's machine



Remote Access VPN Deployment

➢ Verification

Viewing the VPN Session Database

> show vpn-sessiondb detail

Viewing the AnyConnect Client Details

> show vpn-sessiondb anyconnect

Viewing the Detail Session

> show vpn-sessiondb detail anyconnect