

Securing Networks with
Cisco FTD

Chapter 17

Virtual Private Network

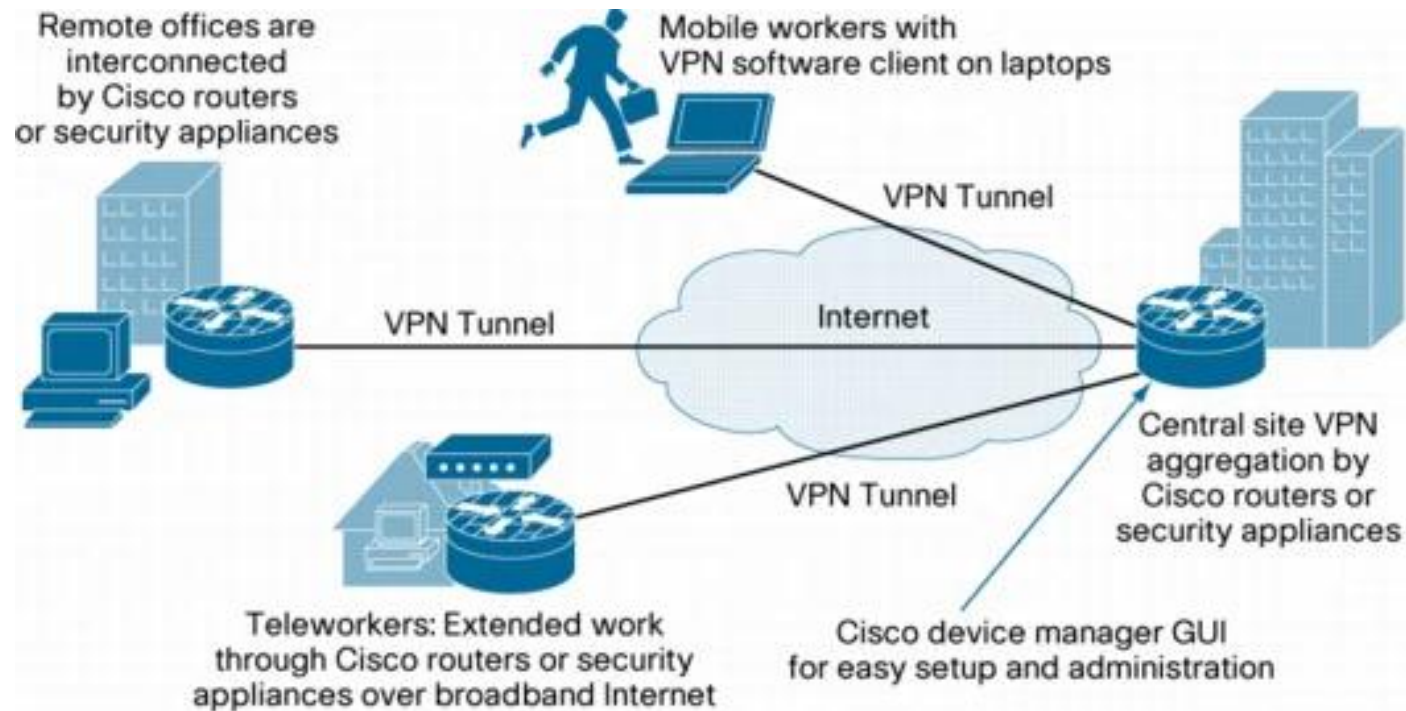
(VPN)

Mohsen Kheradmand

Virtual private network

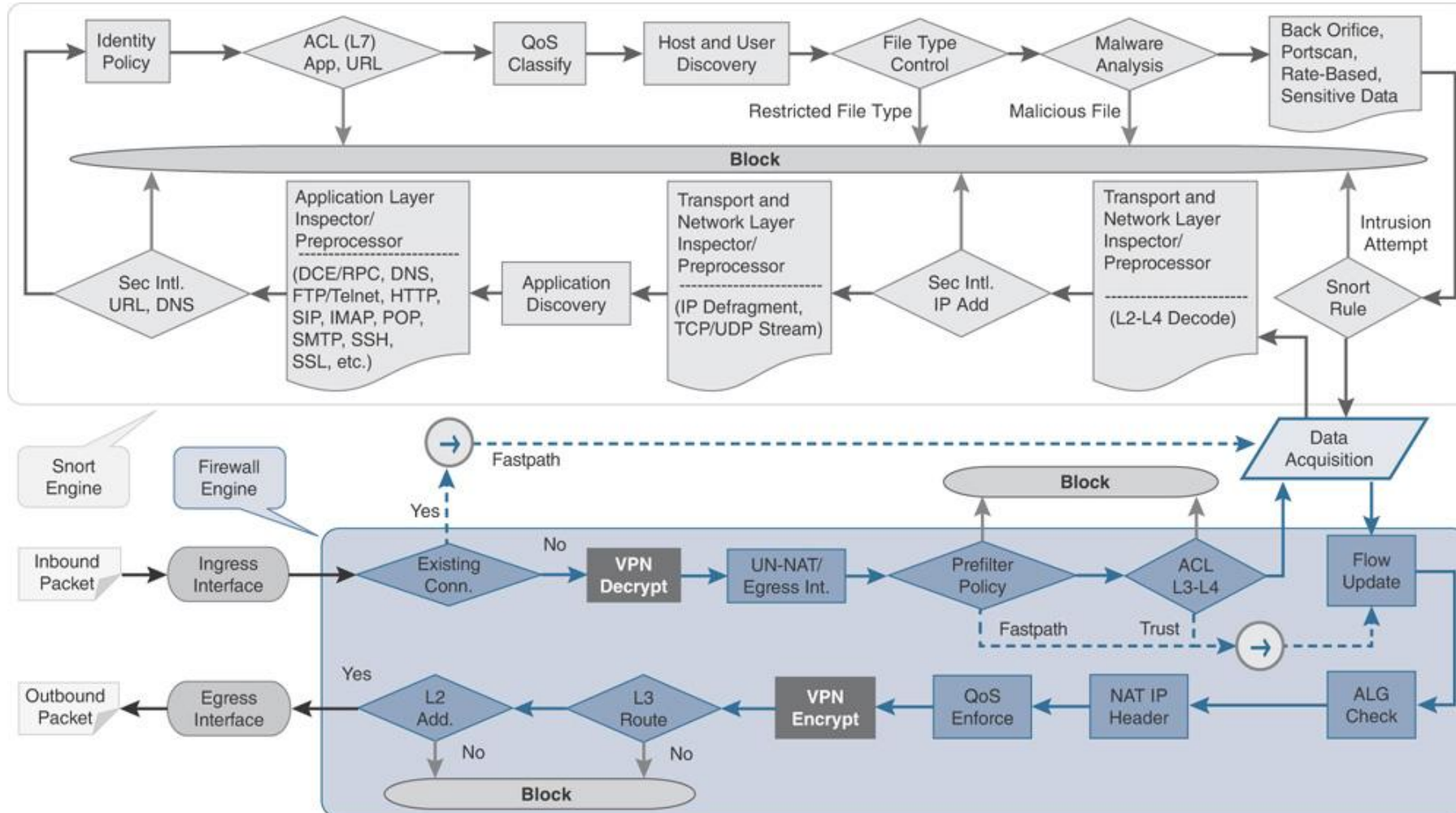
The VPN architectures are mainly two types:

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



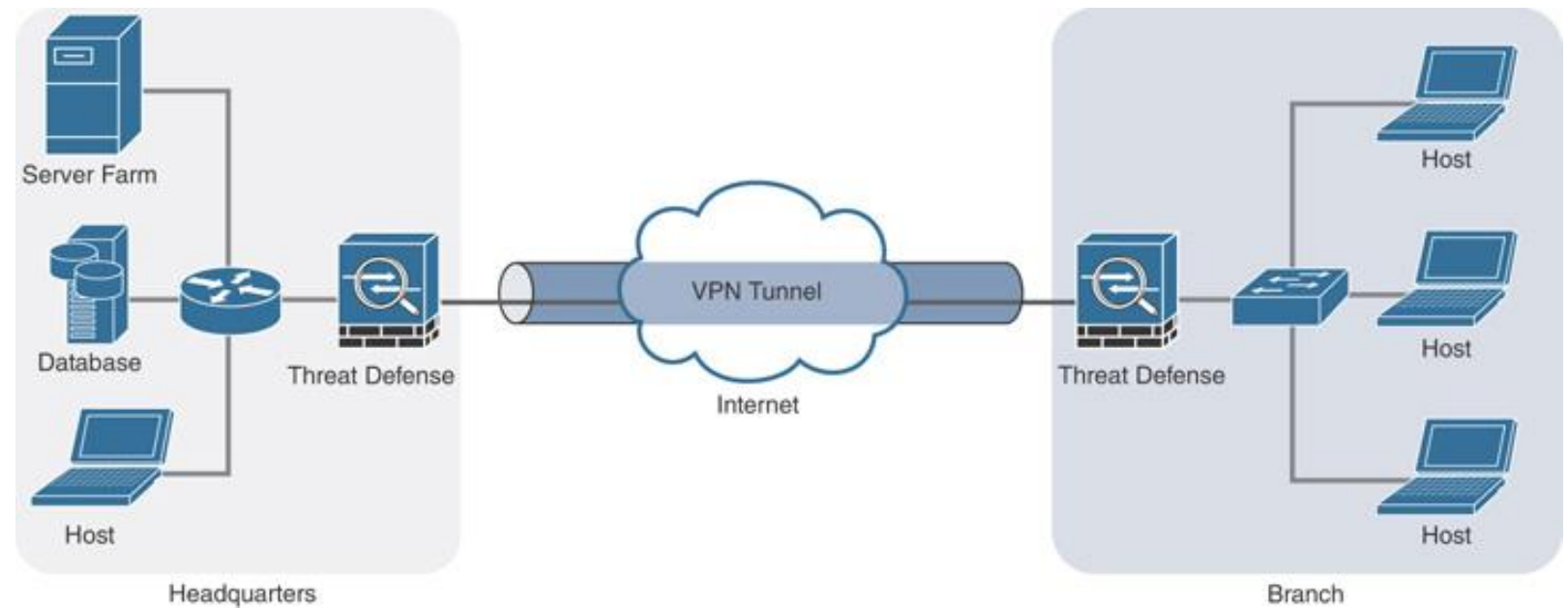
Virtual private network

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



Site-to-Site VPN

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



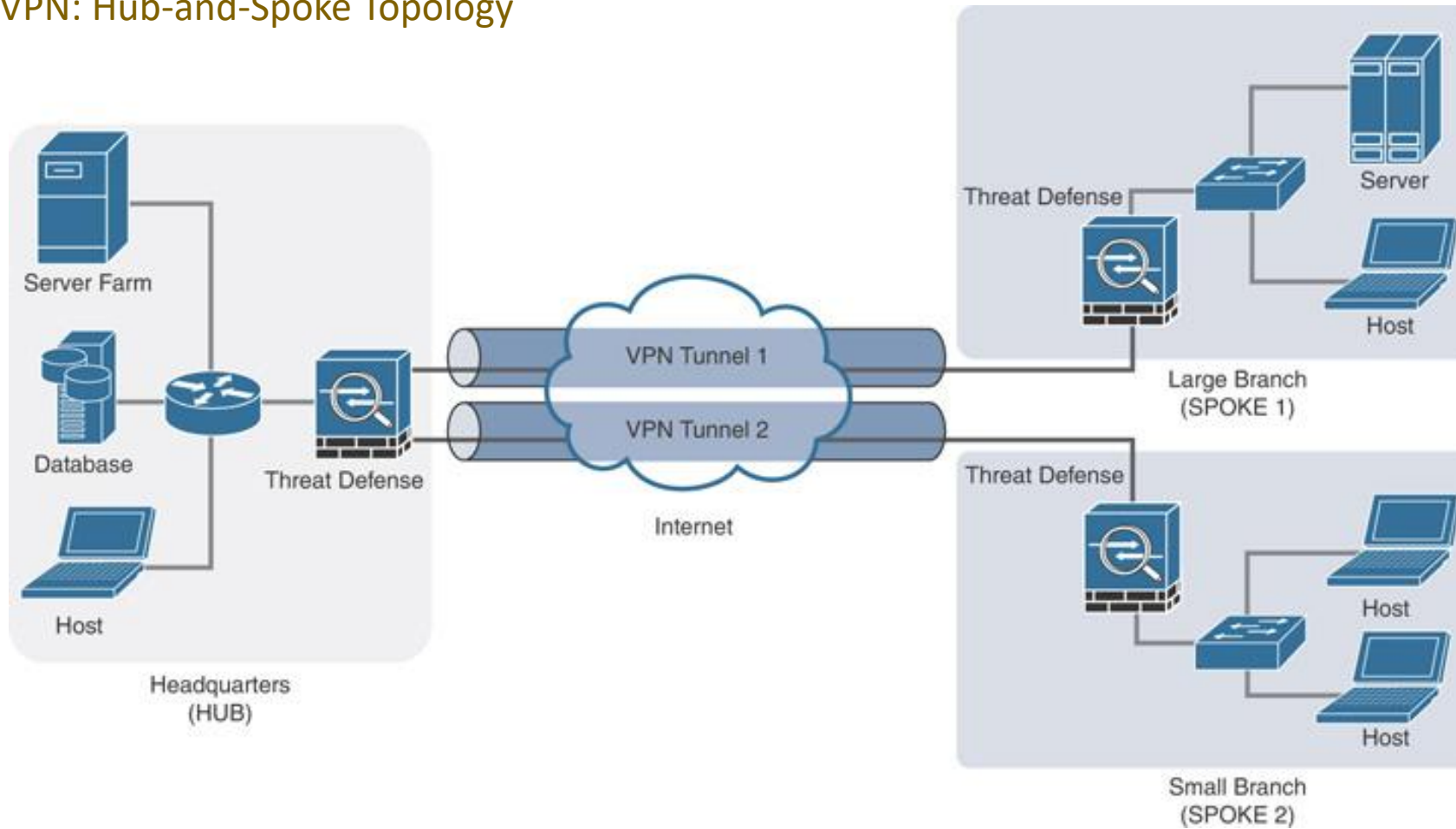
Site-to-Site VPN: Point-to-Point Topology

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.

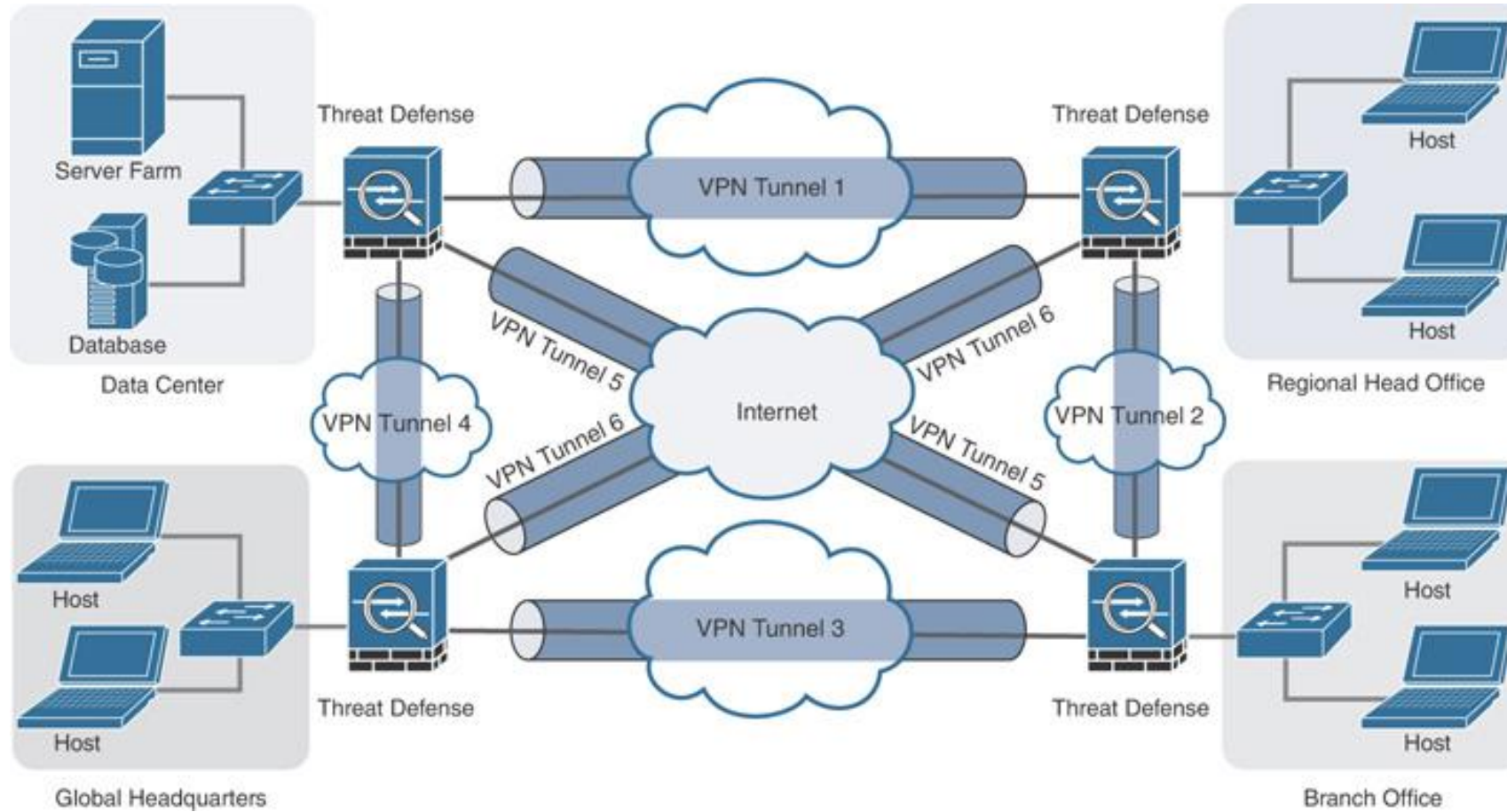
Site-to-Site VPN

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



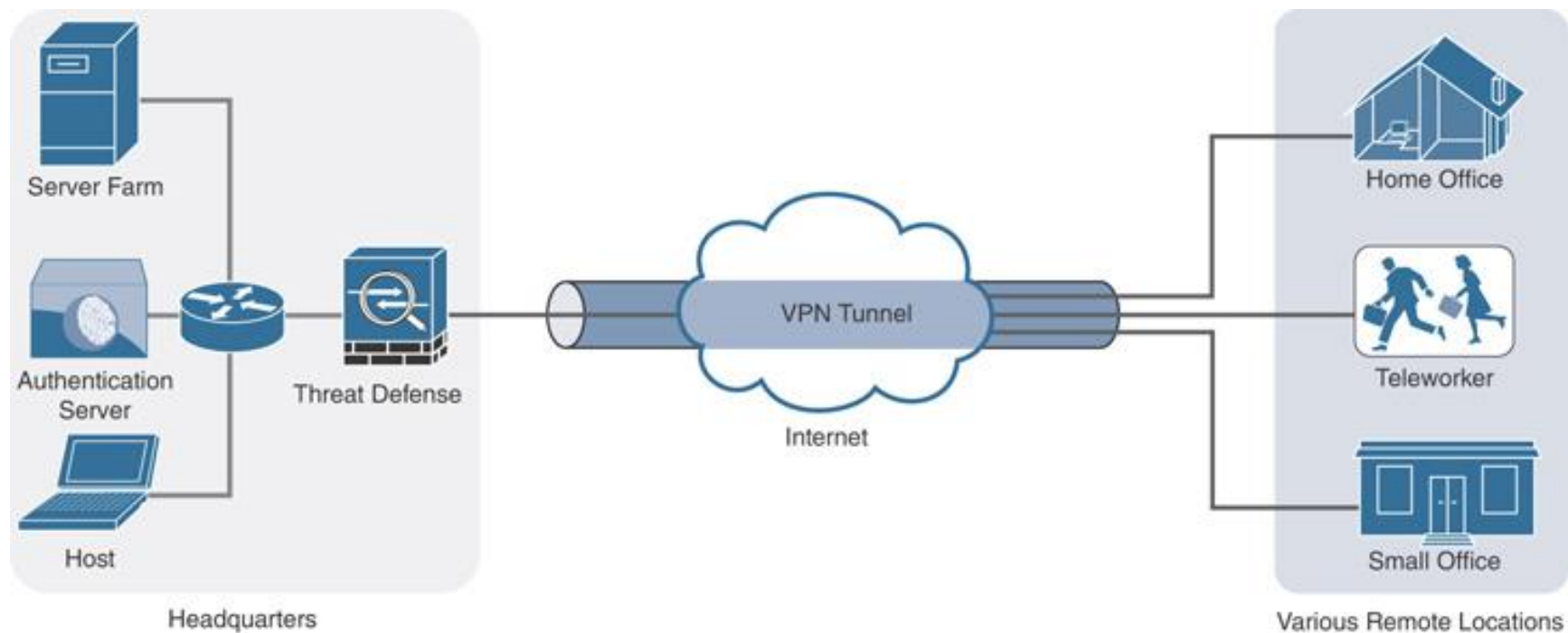
Site-to-Site VPN

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

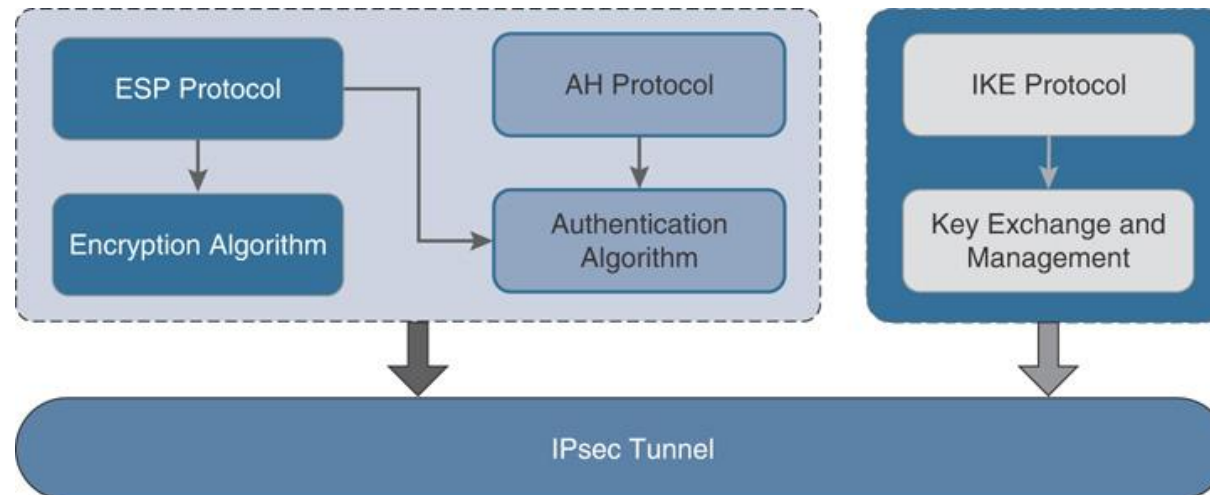
Replay detection

- 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.

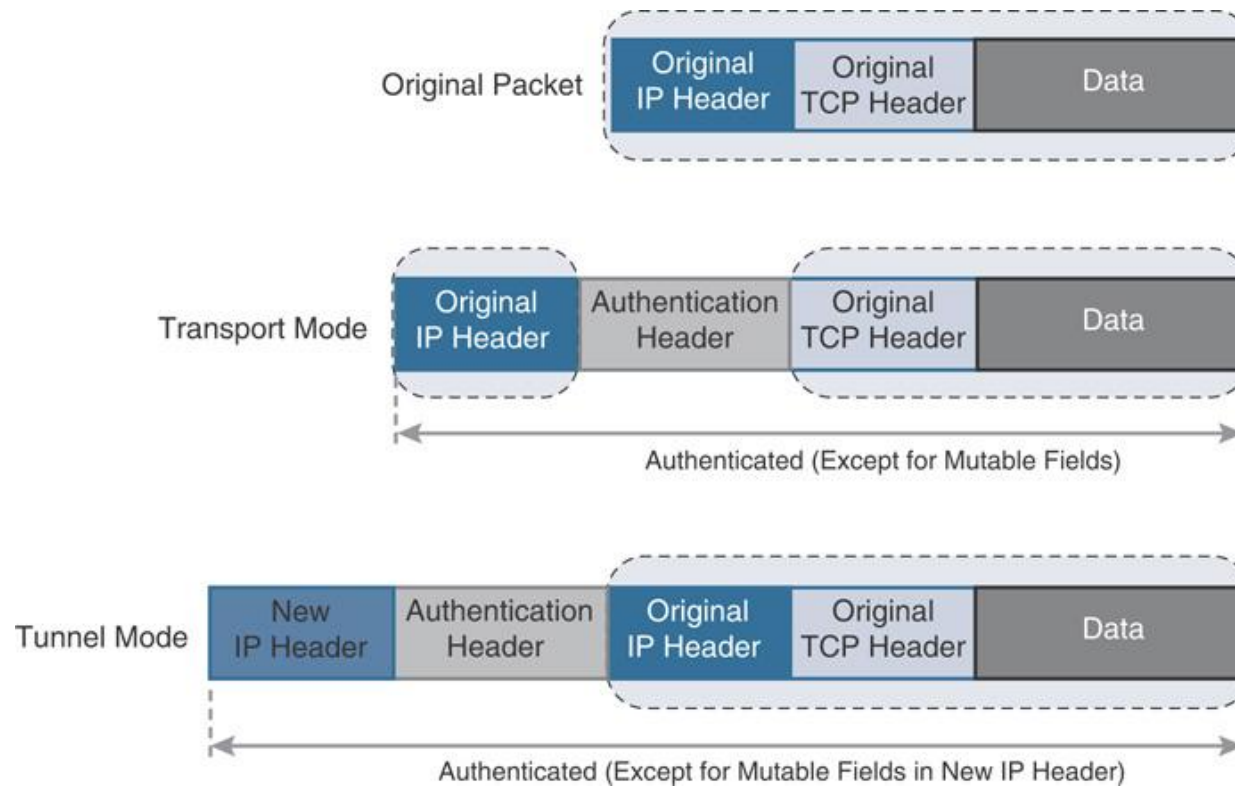
➤ Tunnel mode

- 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

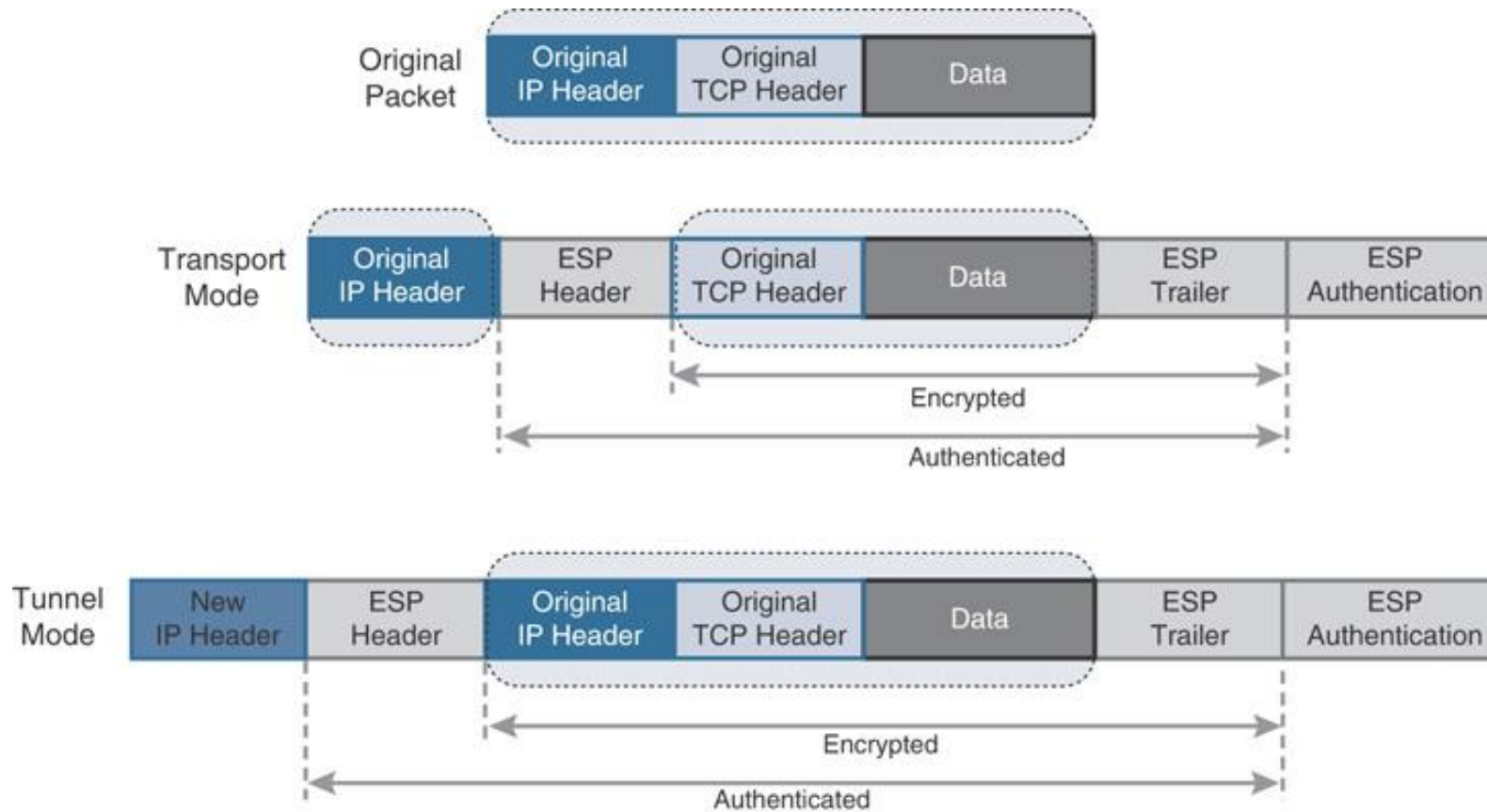
IPsec Essentials

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



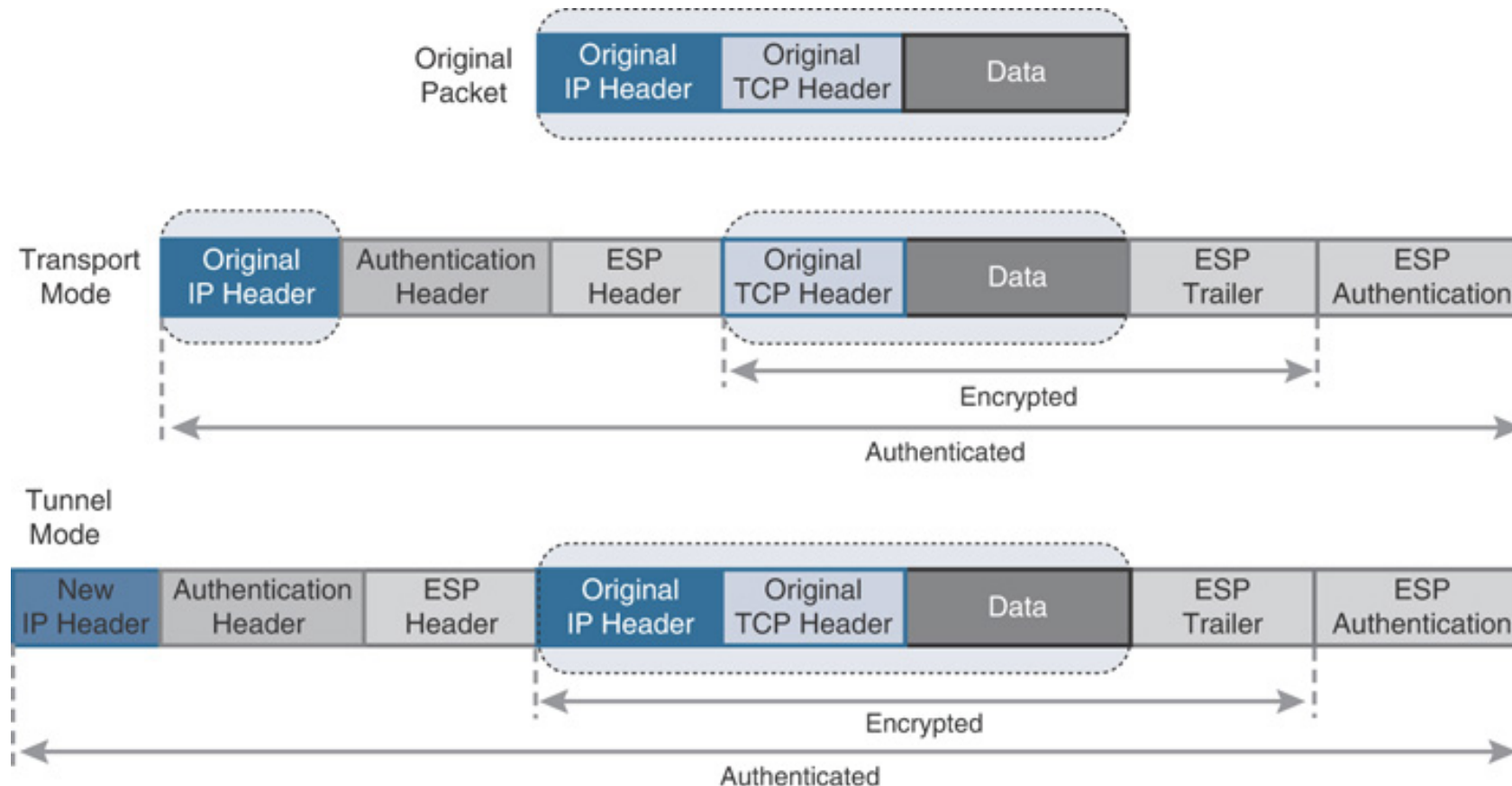
IPsec Essentials

- 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

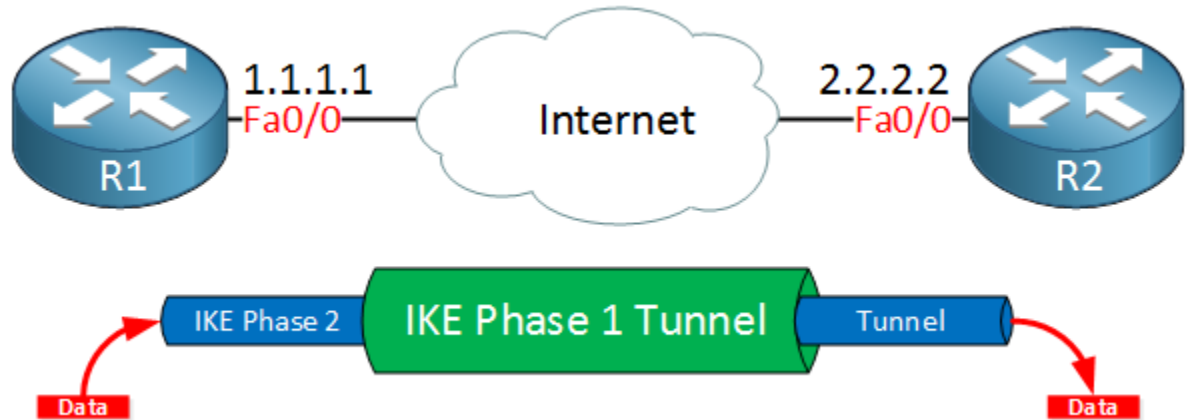
IPsec (IP Security) tunnel

- ✓ 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.

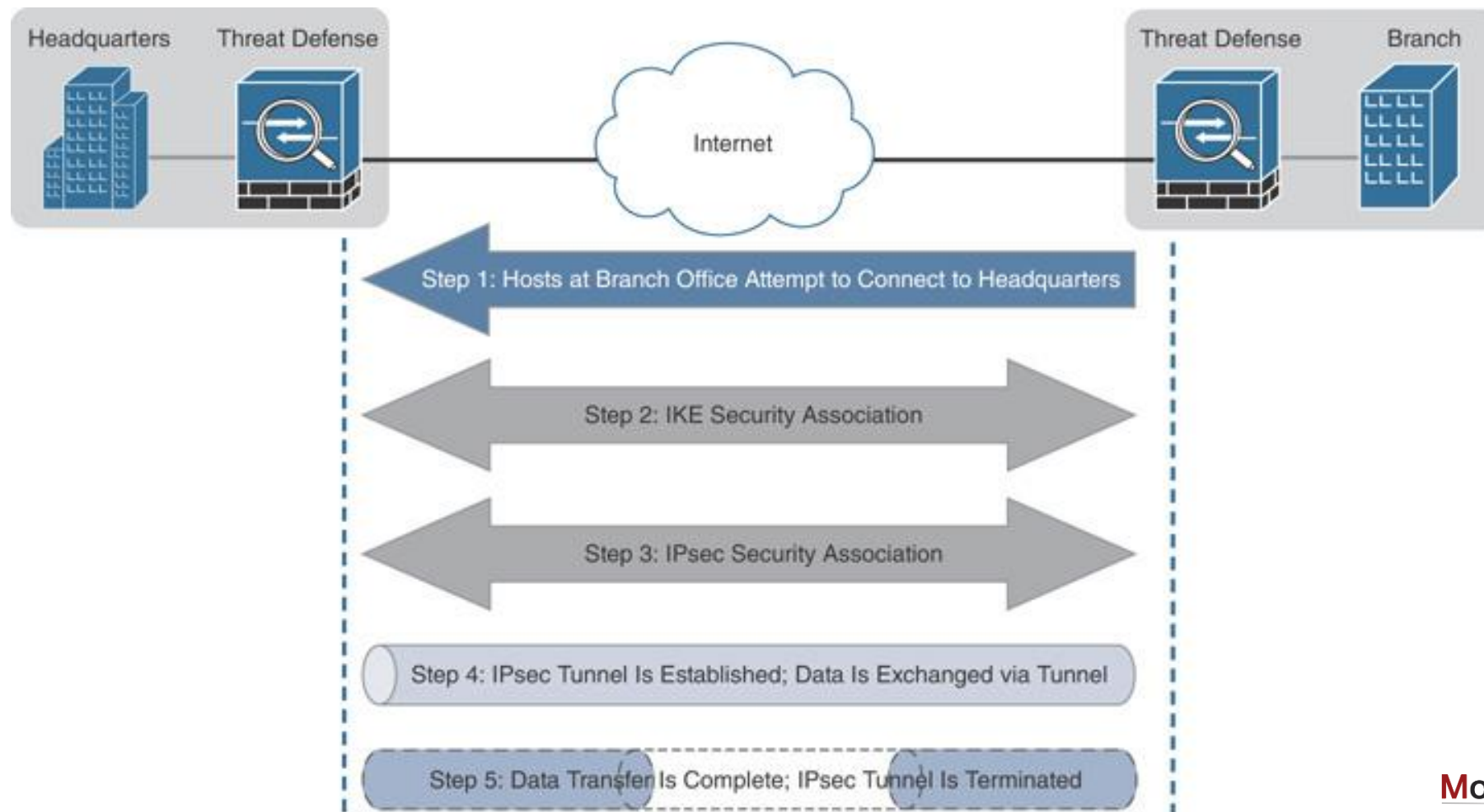
QM2: This message from the responder has matching IPsec parameters.

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 :

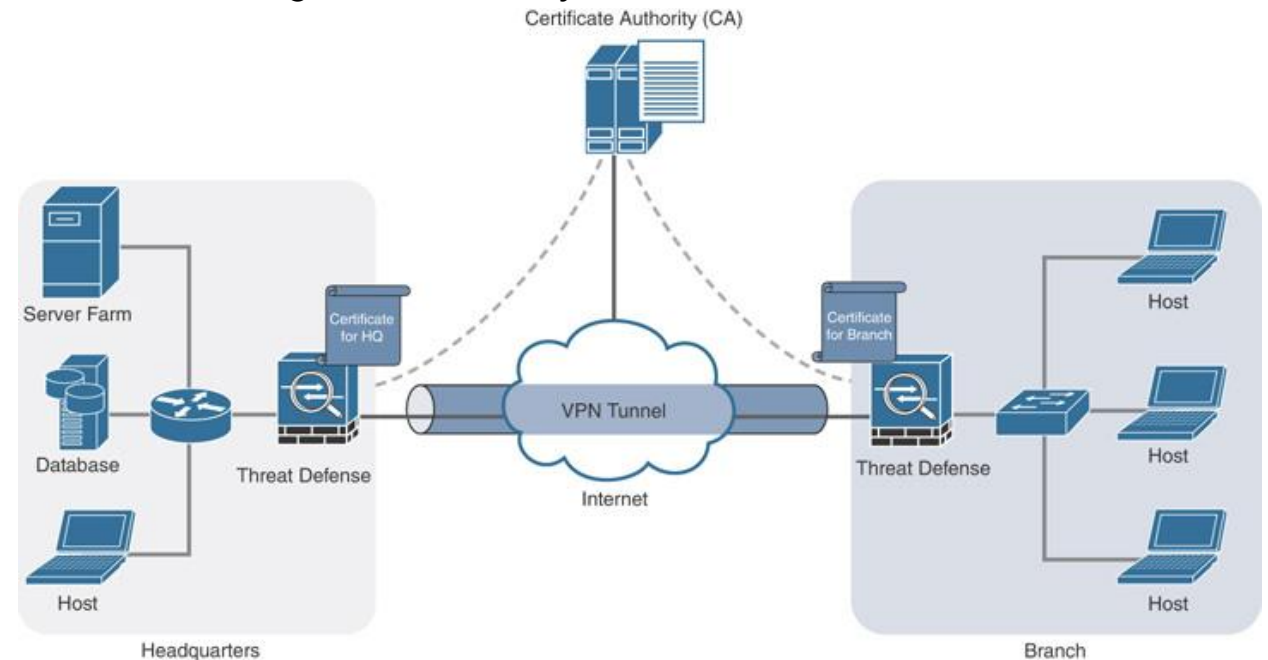
- VPN peers can exchange this message to notify each other of events related to IKE operation.

- 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)

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account: Firepower

Description:

* Expire After: Days
Between 1 - 365, 30 days recommended

Max. Number of Uses:

The token will be expired when either the expiration or the maximum uses is reached

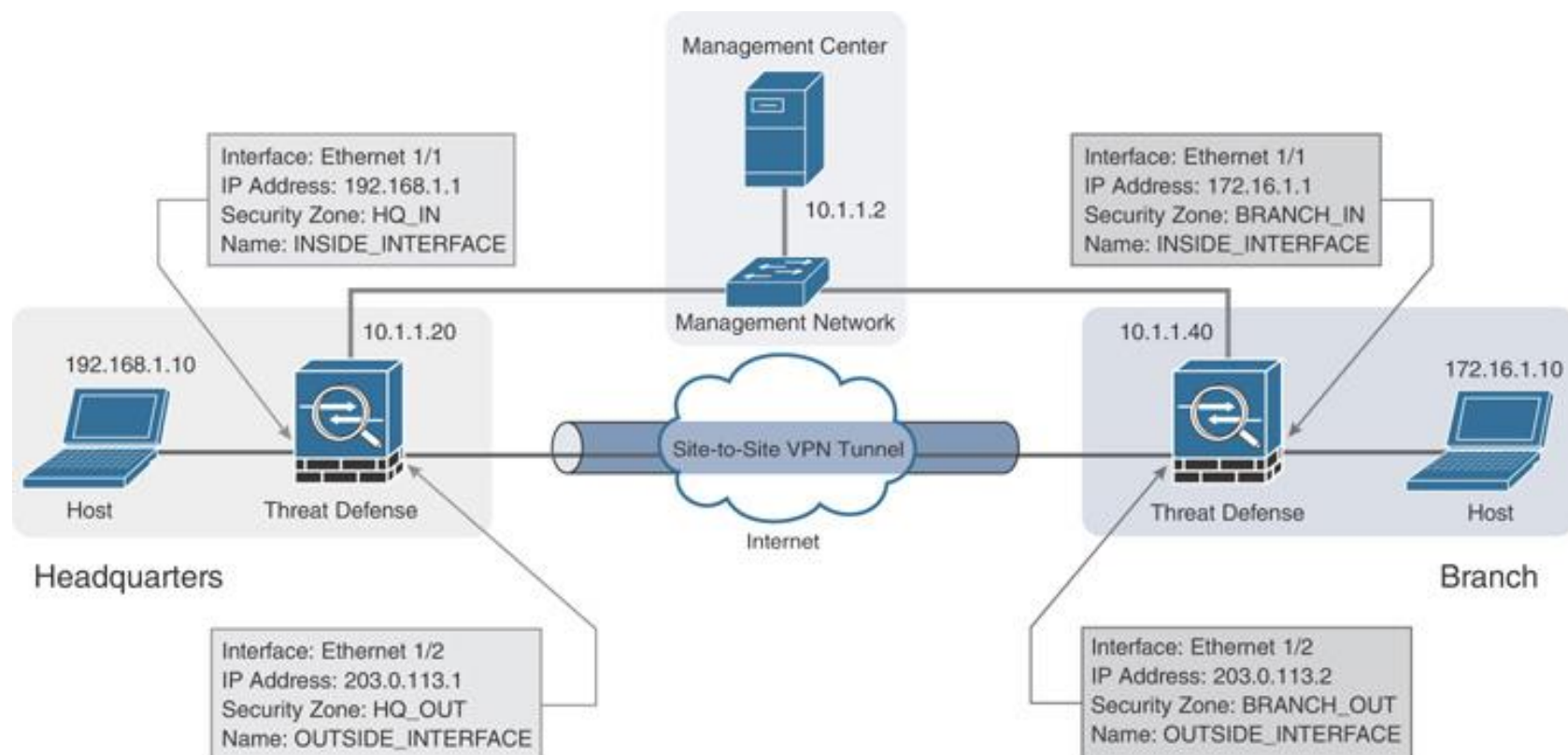
☒ Allow export-controlled functionality on the products registered with this token ⓘ

Create Token **Cancel**

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
ODFjYTU0...	2021-Feb-22 16...		Allowed	Cisco Firepower	nrajib	Actions

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

FMC NGFW Interfaces

Overview Analysis Policies **Devices** Objects AMP Intelligence

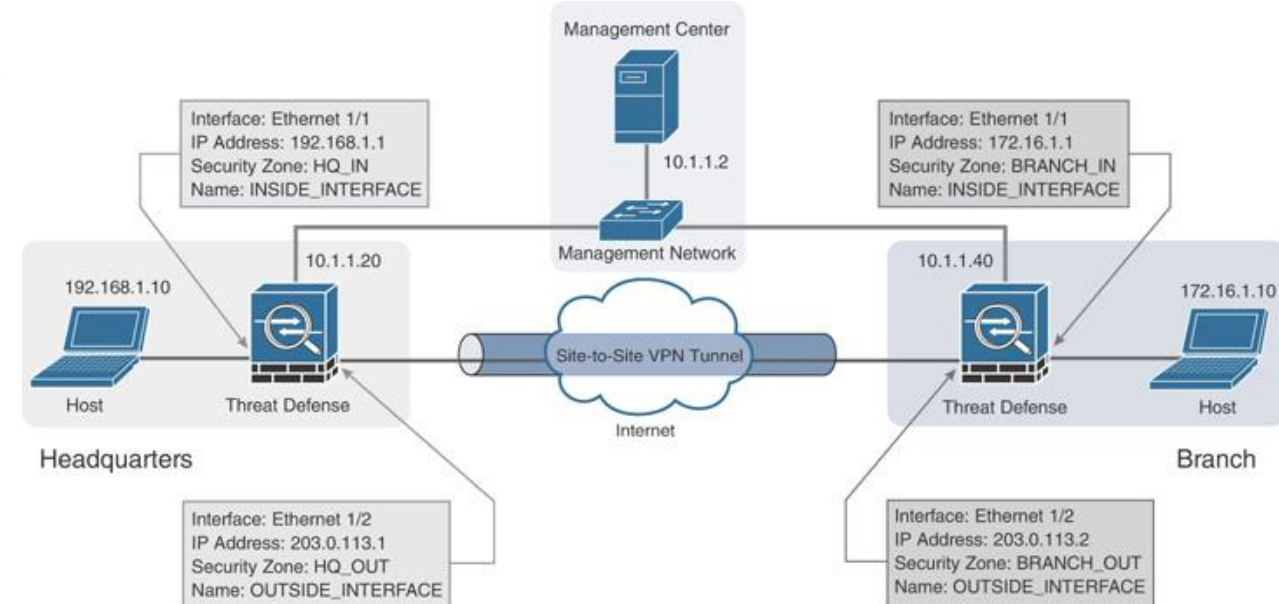
Headquarters Threat Defense

Cisco Firepower 1010 Threat Defense

Device Routing **Interfaces** Inline Sets DHCP SNMP

Search by name

Interface	Logical Name	Type	Security ...	MAC Address...	IP Address	Port...
Diagnostic1/1	diagnostic	Physical				
Ethernet1/1	INSIDE_INTERFACE	Physical	HQ_IN		192.168.1.1/255...	
Ethernet1/2	OUTSIDE_INTERFACE	Physical	HQ_OUT		203.0.113.1/255...	



FMC NGFW Interfaces

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy

Branch Threat Defense

Cisco Firepower 1010 Threat Defense

Device Routing **Interfaces** Inline Sets DHCP SNMP

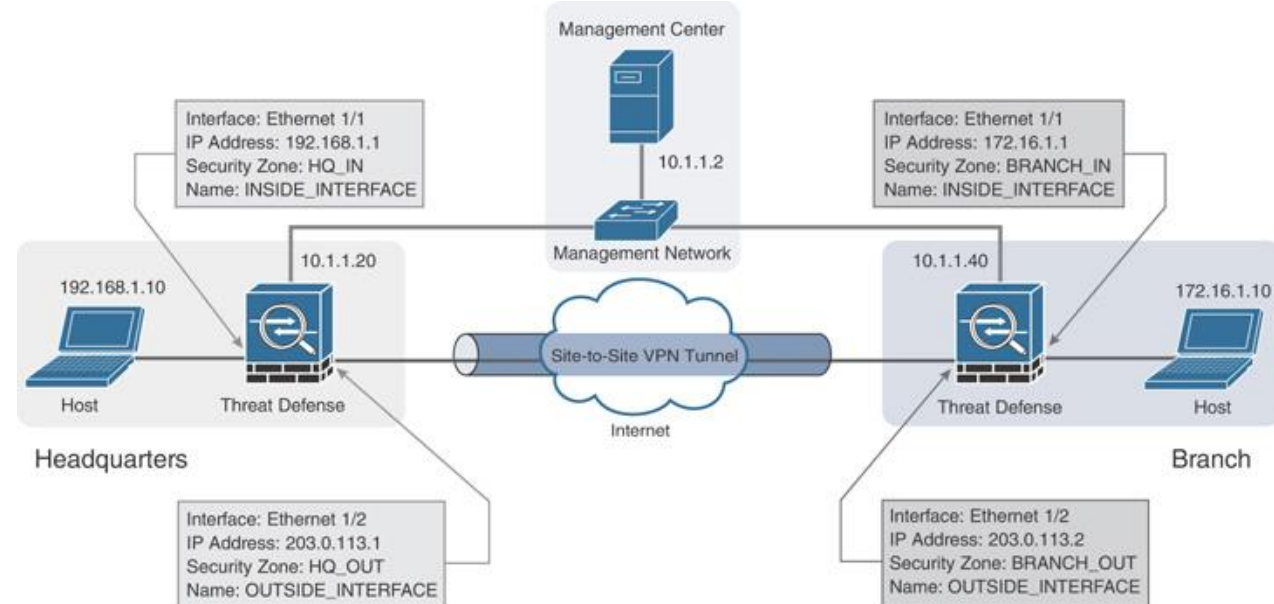
Search by name Sync Device

Interface	Logical Name	Type	Security Zon...	MAC Add...	IP Address	Port...	VLAN
Diagnostic1/1	diagnostic	Physical					
Ethernet1/1	INSIDE_INTERFACE	Physical	BRANCH_IN		172.16.1.1/255...		
Ethernet1/2	OUTSIDE_INTERFACE	Physical	BRANCH_OUT		203.0.113.2/255...		

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



FMC Object Management

Overview Analysis Policies Devices **Objects** AMP Intelligence Deploy

Network

Add Network Filter

☐ Show Unused Objects

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

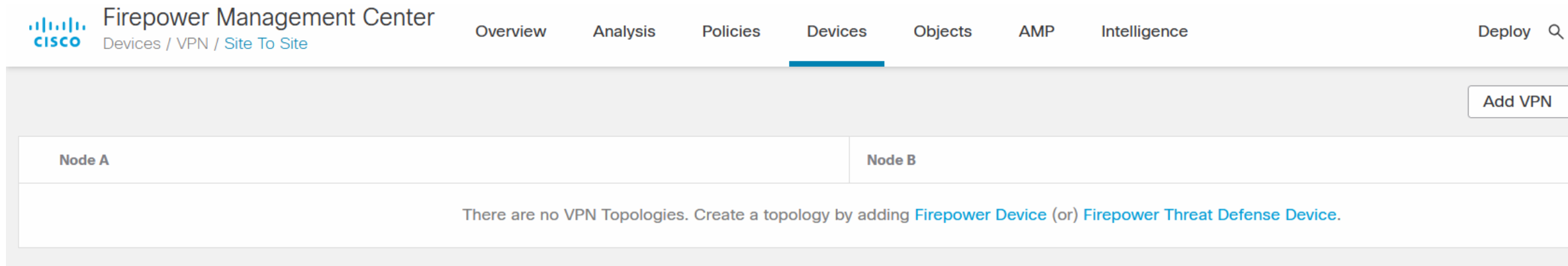
Name	Value	Type	Override
BRANCH_LAN	172.16.1.0/24	Network	
HQ_LAN	192.168.1.0/24	Network	
IPv4-Benchmark-Tests	198.18.0.0/15	Network	
IPv4-Link-Local	169.254.0.0/16	Network	

Site-to-Site VPN Deployment

- Example of P-to-P configuration

➤ VPN Configurations

- Devices > VPN > Site To Site
- Firepower Threat Defense Device



The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title "Firepower Management Center", and a breadcrumb trail "Devices / VPN / Site To Site". The main navigation menu contains tabs for Overview, Analysis, Policies, Devices (which is currently selected), Objects, AMP, and Intelligence. On the far right of the navigation bar are "Deploy" and a search icon. Below the navigation bar, there is a light gray header area with an "Add VPN" button on the right. The main content area is divided into two columns: "Node A" on the left and "Node B" on the right. A message at the bottom of the content area states: "There are no VPN Topologies. Create a topology by adding [Firepower Device](#) (or) [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)

Create New VPN Topology ?

Topology Name:*

☒ Policy Based (Crypto Map) ☐ Route Based (VTI)

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

Node A: +

Device Name	VPN Interface	Protected Networks	

Node B: +

Device Name	VPN Interface	Protected Networks	

i Ensure the protected networks are allowed by access control policy of each device.

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

Add Endpoint

Device:*
Headquarters Threat Defense

Interface:*
OUTSIDE_INTERFACE

IP Address:*
203.0.113.1

☐ This IP is Private

Connection Type:
Bidirectional

Certificate Map:
+

Protected Networks:*
☒ Subnet / IP Address (Network) ☐ Access List (Extended)

HQ_LAN

Cancel OK

Add Endpoint

Device:*
Branch Threat Defense

Interface:*
OUTSIDE_INTERFACE

IP Address:*
203.0.113.2

☐ This IP is Private

Connection Type:
Bidirectional

Certificate Map:
+

Protected Networks:*
☒ Subnet / IP Address (Network) ☐ Access List (Extended)

BRANCH_LAN

Cancel OK

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

The screenshot shows the 'Create New VPN Topology' configuration window in the Cisco FMC interface. The window is titled 'Create New VPN Topology' and has a 'Topology Name' field set to 'Headquarters-Branch'. Below this, there are two radio buttons: 'Policy Based (Crypto Map)' (selected) and 'Route Based (VTI)'. Under 'Network Topology', there are three tabs: 'Point to Point' (selected), 'Hub and Spoke', and 'Full Mesh'. The 'IKE Version' section shows 'IKEv1' as an option and 'IKEv2' as the selected option. Below this, there are four tabs: 'Endpoints', 'IKE', 'IPsec', and 'Advanced'. The 'Endpoints' tab is active, showing two nodes: 'Node A' and 'Node B'. Each node has a table with columns for 'Device Name', 'VPN Interface', and 'Protected Networks'. For Node A, the device is 'Headquarters Threat Defense', the interface is 'OUTSIDE_INTERFACE/203.0.113.1', and the protected network is 'HQ_LAN'. For Node B, the device is 'Branch Threat Defense', the interface is 'OUTSIDE_INTERFACE/203.0.113.2', and the protected network is 'BRANCH_LAN'. At the bottom of the window, there is a note: 'Ensure the protected networks are allowed by access control policy of each device.' and two buttons: 'Cancel' and 'Save'.

Topology Name:*
Headquarters-Branch

☒ Policy Based (Crypto Map) ☐ Route Based (VTI)

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Node A:

Device Name	VPN Interface	Protected Networks
Headquarters Threat Defense	OUTSIDE_INTERFACE/203.0.113.1	HQ_LAN

Node B:

Device Name	VPN Interface	Protected Networks
Branch Threat Defense	OUTSIDE_INTERFACE/203.0.113.2	BRANCH_LAN

❗ Ensure the protected networks are allowed by access control policy of each device.

Cancel Save

Site-to-Site VPN Deployment

- Example of P-to-P configuration
 - VPN Configurations
 - ❖ Additional security parameters
- You can strengthen the VPN tunnel security
- From IKE setting you can set new policy and customize it

The screenshot shows the 'Create New VPN Topology' configuration window. The 'Topology Name' is 'Headquarters-Branch'. The 'Policy Based (Crypto Map)' option is selected. The 'Network Topology' is 'Point to Point'. The 'IKE Version' is 'IKEv2'. The 'Endpoints' tab is active, showing 'IKEv1 Settings' and 'IKEv2 Settings'. The 'IKEv2 Policy' is 'SHA512-AES256-SHA512-DH21'. The 'Authentication Type' is 'Pre-shared Automatic Key'. The 'Pre-shared Key Length' is '24 Characters (Range 1-127)'. The 'New IKEv2 Policy' dialog is open, showing the 'Available Algorithms' list with 'SHA512' selected under 'Integrity Algorithms'. The 'Selected Algorithms' list also contains 'SHA512'. The 'Cancel' and 'Save' buttons are visible at the bottom of the dialog.

Create New VPN Topology

Topology Name:*
Headquarters-Branch

☒ Policy Based (Crypto Map) ☐ Route Based (VTI)

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

IKEv1 Settings
Policy:* preshared_sha_aes256_dh14_3 +
Authentication Type: Pre-shared Automatic Key
Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings
Policy:* SHA512-AES256-SHA512-DH21 +
Authentication Type: Pre-shared Automatic Key
Pre-shared Key Length:* 24 Characters (Range 1-127)

New IKEv2 Policy

Name:*
SHA512-AES256-SHA512-DH21

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)
86400

Available Algorithms

Integrity Algorithms	Encryption Algorithms	PRF Algorithms	Diffie-Hellman Group
MD5	SHA	SHA512	SHA256
			SHA384
			NULL

Selected Algorithms
SHA512

Cancel Save

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

FMC Policy Editor

Overview Analysis Policies Devices Objects AMP Intelligence Deploy

AC Policy

Enter Description

Analyze Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (3)

Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy SSL Policy:...

Filter by Device Search Rules Show Rule Conflicts Add Category Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	Source Ports	Dest Ports	Action	
Mandatory - AC Policy (1-2)									
1	HQ to Branch	Any	Any	HQ_LAN	BRANCH_LAN	Any	Any	Allow	
2	Branch to HQ	Any	Any	BRANCH_LAN	HQ_LAN	Any	Any	Allow	
Default - AC Policy (-)									
There are no rules in this section. Add Rule or Add Category									

Default Action Access Control:Block all traffic

Displaying 1 - 2 of 2 rules Page 1 of 1 Rules per page: 100

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)

The screenshot shows the Cisco FMC NGFW NAT Policy Editor interface. The page title is "Headquarters NAT". It features a "Rules" tab and a "Filter Rules" section. Below the filter, there is a table of NAT rules. The table has columns for Direction, Type, Source Interface Objects, Destination Interface Objects, Original Sources, Original Destination, Original Services, Translated Sources, Translated Destinations, Translated Services, and Options. A rule is visible under "NAT Rules After" with Type "Dynamic", Source "HQ_IN", Destination "HQ_OUT", and Options "Interface" and "Dns:false".

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destination	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
NAT Rules Before											
Auto NAT Rules											
#	x	Dynamic	HQ_IN	HQ_OUT	HQ_LAN			Interface			Dns:false
NAT Rules After											

1) Click add Rule

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

The screenshot shows the 'Add NAT Rule' configuration window in a Cisco NGFW interface. The window is titled 'Add NAT Rule' and has a 'Cancel' button in the top right corner. The 'NAT Rule' dropdown is set to 'Manual NAT Rule'. The 'Insert' dropdown is set to 'In Category' and the 'NAT Rules Before' dropdown is set to 'NAT Rules Before'. The 'Type' dropdown is set to 'Static'. The 'Enable' checkbox is checked. The 'Description' field is empty. The 'Add Rule' button is visible on the right side of the window.

The 'Translation' tab is selected, showing the 'Original Packet' and 'Translated Packet' sections. The 'Original Packet' section has the following fields:

- Original Source: * (dropdown menu) +
- Original Destination: (dropdown menu) +
- Original Source Port: (dropdown menu) +
- Original Destination Port: (dropdown menu) +

The 'Translated Packet' section has the following fields:

- Translated Source: (dropdown menu) +
- Translated Destination: (dropdown menu) +
- Translated Source Port: (dropdown menu) +
- Translated Destination Port: (dropdown menu) +

The 'Original Source' is set to 'HQ_LAN' and the 'Translated Source' is set to 'Address'. The 'Original Destination' is set to 'Address' and the 'Translated Destination' is set to 'BRANCH_LAN'. The 'Original Source Port' and 'Original Destination Port' are set to empty. The 'Translated Source Port' and 'Translated Destination Port' are set to empty.

Site-to-Site VPN Deployment

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

FMC

CISCO

NGFW NAT Policy Editor

Overview

Analysis

Policies

Devices

Ob

Headquarters NAT

Enter Description

Rules

Filter by Device

Filter Rules

					Original Packet		Translated Packet					
#	Dir	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Orig Ser	Translated Sources	Translated Destinations	Tran Ser	Option	
NAT Rules Before												
1		Static	BRANCH_IN	BRANCH_OUT							Dns:fa route- no-pr	
Auto NAT Rules												
#		Dynamic	BRANCH_IN	BRANCH_OUT							Dns:fa	
NAT Rules After												

FMC

CISCO

NGFW NAT Policy Editor

Overview

Analysis

Policies

Devices

Ob

Headquarters NAT

Enter Description

Rules

Filter by Device

Filter Rules

					Original Packet		Translated Packet					
#	Direct	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Origr Servr	Translated Sources	Translated Destinations	Trans Servr	Options	
NAT Rules Before												
1		Static	HQ_IN	HQ_OUT							Dns:fa route-li no-pro	
Auto NAT Rules												
#		Dynamic	HQ_IN	HQ_OUT							Dns:fa	
NAT Rules After												

FMC

CISCO

NGFW NAT Policy Editor

Overview

Analysis

Policies

Devices

Objects

AMP

Intelligen...

Deploy

admin

Branch NAT

Enter Description

Rules

Filter by Device

Filter Rules

					Original Packet		Translated Packet					
#	Dir	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Orig Ser	Translated Sources	Translated Destinations	Tran Ser	Option	
NAT Rules Before												
1		Static	BRANCH_IN	BRANCH_OUT							Dns:fa route- no-pr	
Auto NAT Rules												
#		Dynamic	BRANCH_IN	BRANCH_OUT							Dns:fa	
NAT Rules After												

FMC

CISCO

NGFW NAT Policy Editor

Overview

Analysis

Policies

Devices

Ob

Headquarters NAT

Enter Description

Rules

Filter by Device

Filter Rules

					Original Packet		Translated Packet					
#	Direct	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Origr Servr	Translated Sources	Translated Destinations	Trans Servr	Options	
NAT Rules Before												
1		Static	HQ_IN	HQ_OUT							Dns:fa route-li no-pro	
Auto NAT Rules												
#		Dynamic	HQ_IN	HQ_OUT							Dns:fa	
NAT Rules After												

Site-to-Site VPN Deployment

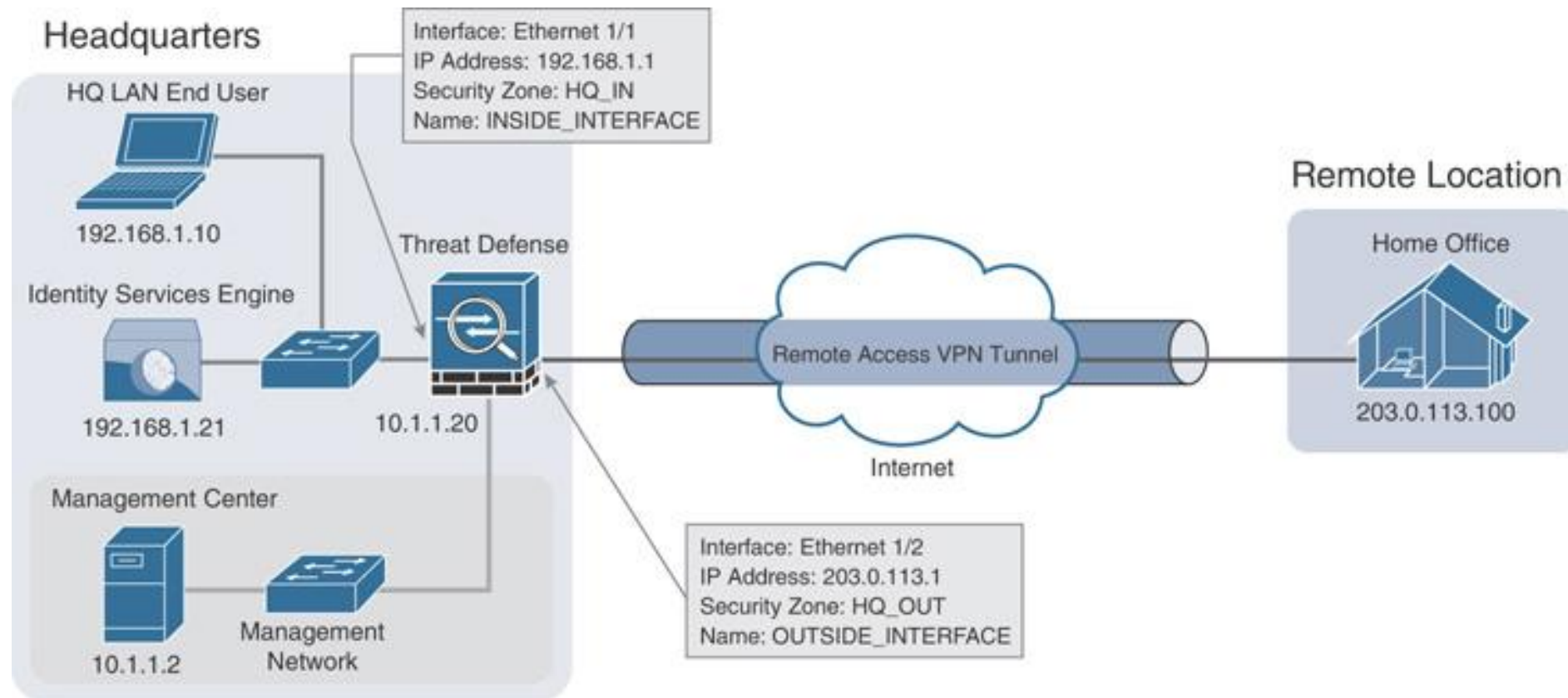
- Example of P-to-P configuration

➤ 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

Firepower Management Center
Devices / NGFW Device Summary

Overview Analysis Policies **Devices** Objects AMP

FTD1
Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP

General	
Name:	FTD1
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled

License	
Performance Tier :	FTDv5 - Tiered (Core 4 / 8 GB)
Base:	☒
Export-Controlled Features:	☐
Malware:	☒
Threat:	☒
URL Filtering:	☒
AnyConnect Apex:	☒
AnyConnect Plus:	☒
AnyConnect VPN Only:	☐

License

License Types

Performance Tier: FTDv5 - Tiered (Core 4 / 8 GB)

Base: ☒

Export-Controlled Features: ☐

Malware: ☒

Threat: ☒

URL Filtering: ☒

AnyConnect Apex: ☒

AnyConnect Plus: ☒

AnyConnect VPN Only: ☐

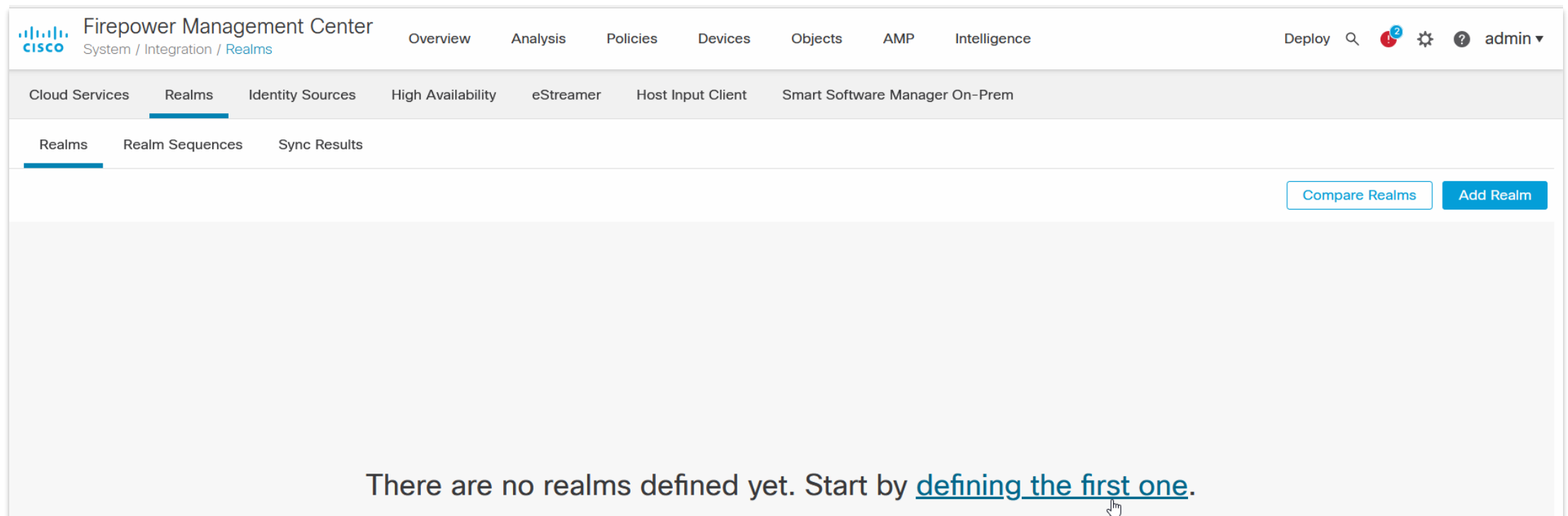
If a device already has VPN Only they cannot have Apex or Plus.
If a device has Apex or Plus it cannot have VPN Only

Cancel Save

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

Add New Realm? ×

Name*

Local-identity

Description

local users as a fallback solution

Type

LOCAL

Local User Configuration

▼ Raymond

▼ Alex

▲ Arman

Username

Arman

Password

Confirm Password

Add another local user

Cancel

Save

MohsenKheradmand 

Remote Access VPN Deployment

➤ User Authentication.

- Creating a Active directory as a Realm

Add New Realm

Name*

Dena-Directory

Description

Domain controller

Type

AD

AD Primary Domain

dena.local

Directory Username*

kheradmand@dena.local

Directory Password*

••••••

Base DN

Group DN

E.g. user@domain.com

E.g. domain.com

E.g. ou=group,dc=cisco,dc=com

E.g. ou=group,dc=cisco,dc=com

Directory Server Configuration

192.168.10.10:389

Hostname/IP Address*

192.168.10.10

Port*

389

Encryption

None

CA Certificate

Select certificate

Interface used to connect to Directory server

Resolve via route lookup

Choose an interface

Default: Management/Diagnostic Interface

Test

Test connection succeeded

Add another directory

Cancel

Configure Groups and Users

Remote Access VPN Deployment

➤ User Authentication.

 Firepower Management Center
System / Integration / Realms

OverviewAnalysisPoliciesDevicesObjectsAMPIntelligence

Deploy 🔍 3 ⚙️ ? admin ▼

Dena-Directory

You have unsaved changes Save Cancel

Group and User Sync

Directory

Realm Configuration

AD Primary Domain

dena.local

E.g. domain.com

Enter query to look for users and groups

Enter the directory tree on the server where the Firepower Management Center should begin searching for user and group data.

Base DN

DC=Dena,DC=local

E.g. ou=group,dc=cisco,dc=com

Group DN

DC=Dena,DC=local

E.g. ou=group,dc=cisco,dc=com

Load Groups

Available Groups

Limit the groups to use in policy by moving them to either the Included Groups or Excluded Groups list. Moving one group to the Included Groups list, for example, allows that group only to be used in policy. [Learn more](#)

Available Groups (All groups are included by default)

Search

Administrators

IT-Admins

Server Operators

Include

Exclude

Included Groups and Users

IT-Admins

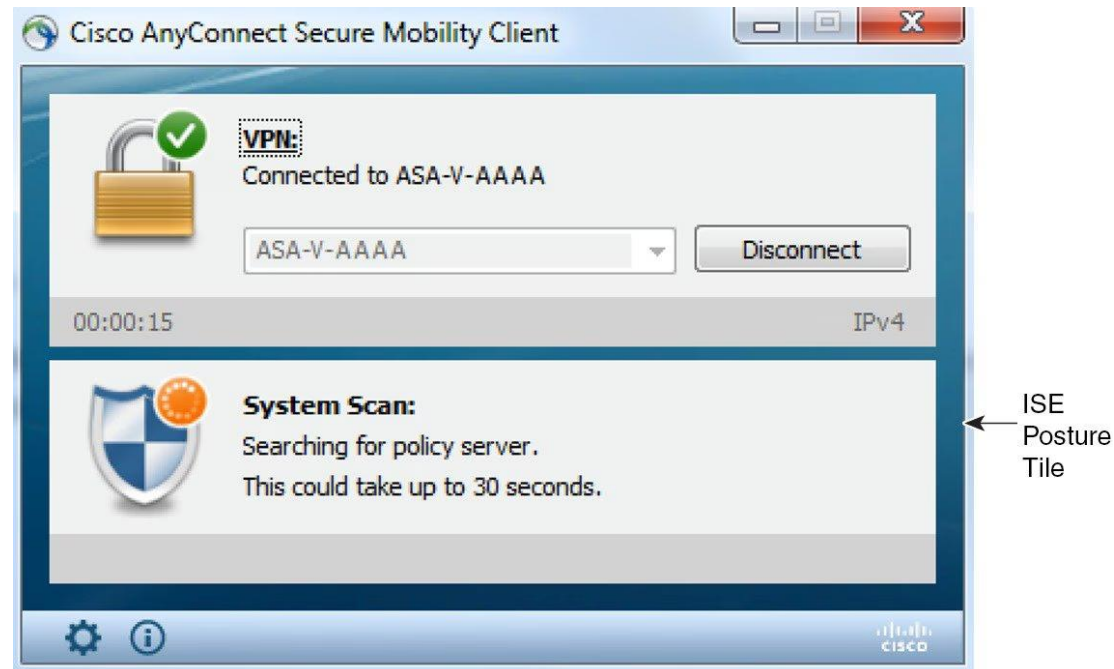
Excluded Groups and Users

None

Add groups and users to let connect via VPN

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

AnyConnect File [Add AnyConnect File](#)

File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image files.

Name	Value	Type	
AnyConnect-Linux	anyconnect-linux64-4.10.00093-webdepl...	AnyConnect Client Image	Download Edit Delete
AnyConnect-MacOS	anyconnect-macos-4.10.00093-webdepl...	AnyConnect Client Image	Download Edit Delete
AnyConnect-Windows	anyconnect-win-4.10.00093-webdeploy-...	AnyConnect Client Image	Download Edit Delete

✓ These are 3 different AnyConnect client software package files for Linux, Mac OS, and Windows

Displaying 1 - 3 of 3 rows | < < Page 1 of 1 > > | C

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

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the text "Firepower Management Center", and a breadcrumb trail "Objects / Object Management". Navigation tabs for "Overview", "Analysis", "Policies", "Devices", "Objects", "AMP", and "Intelligence" are present, with "Objects" being the active tab. On the right side of the top bar, there are links for "Deploy", a search icon, a notification icon, a settings icon, a help icon, and a user profile labeled "admin".

The left sidebar shows a tree view of configuration objects under the "AAA Server" category. The "RADIUS Server Group" option is selected and highlighted in blue. Other visible options include "Single Sign-on Server", "Access List", "Address Pools", "Application Filters", "AS Path", "Cipher Suite List", "Community List", "Distinguished Name", "DNS Server Group", "External Attributes", "File List", "FlexConfig", "Geolocation", "Interface", and "Key Chain".

The main content area is titled "RADIUS Server Group". It features a blue button labeled "Add RADIUS Server Group" and a search box labeled "Filter". Below this, a descriptive text states: "RADIUS Server Group objects contain one or more references to RADIUS Servers. These AAA servers are used to authenticate users logging in through Remote Access VPN connections." A table with two columns, "Name" and "Value", is shown, but it is empty, with the text "No records to display" centered below it.

Remote Access VPN Deployment

➤ RADIUS Server Group

Enter appropriate information of RADIUS servers (AAA)

Add RADIUS Server Group

Name:*
RAD1

Description:
RADIUS server 1

Group Accounting Mode:
Single

Retry Interval:* (1-10) Seconds
10

Realms:
Dena-Directory

☒ Enable authorize only

☒ Enable interim account update

Interval:* (1-120) hours
24

☒ Enable dynamic authorization

Port:* (1024-65535)
1700

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname	
192.168.10.100	 

Cancel Save

New RADIUS Server

IP Address/Hostname:*
192.168.10.50

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)
1812

Key:*
..... 

Confirm Key:*
..... 

Accounting Port: (1-65535)
1813

Timeout: (1-300) Seconds
10

Connect using:
☒ Routing ☐ Specific Interface 

Default: Diagnostic Interface  +

Redirect ACL:
 +

Cancel Save

Remote Access VPN Deployment

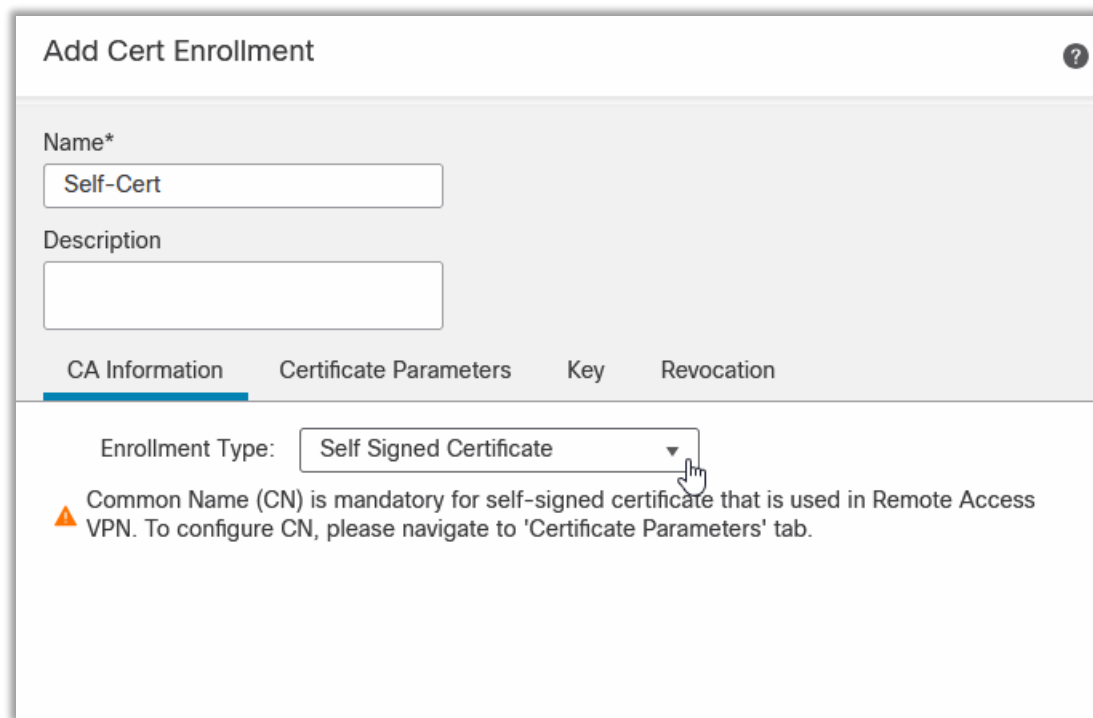
➤ Certificate Enrollment

- 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

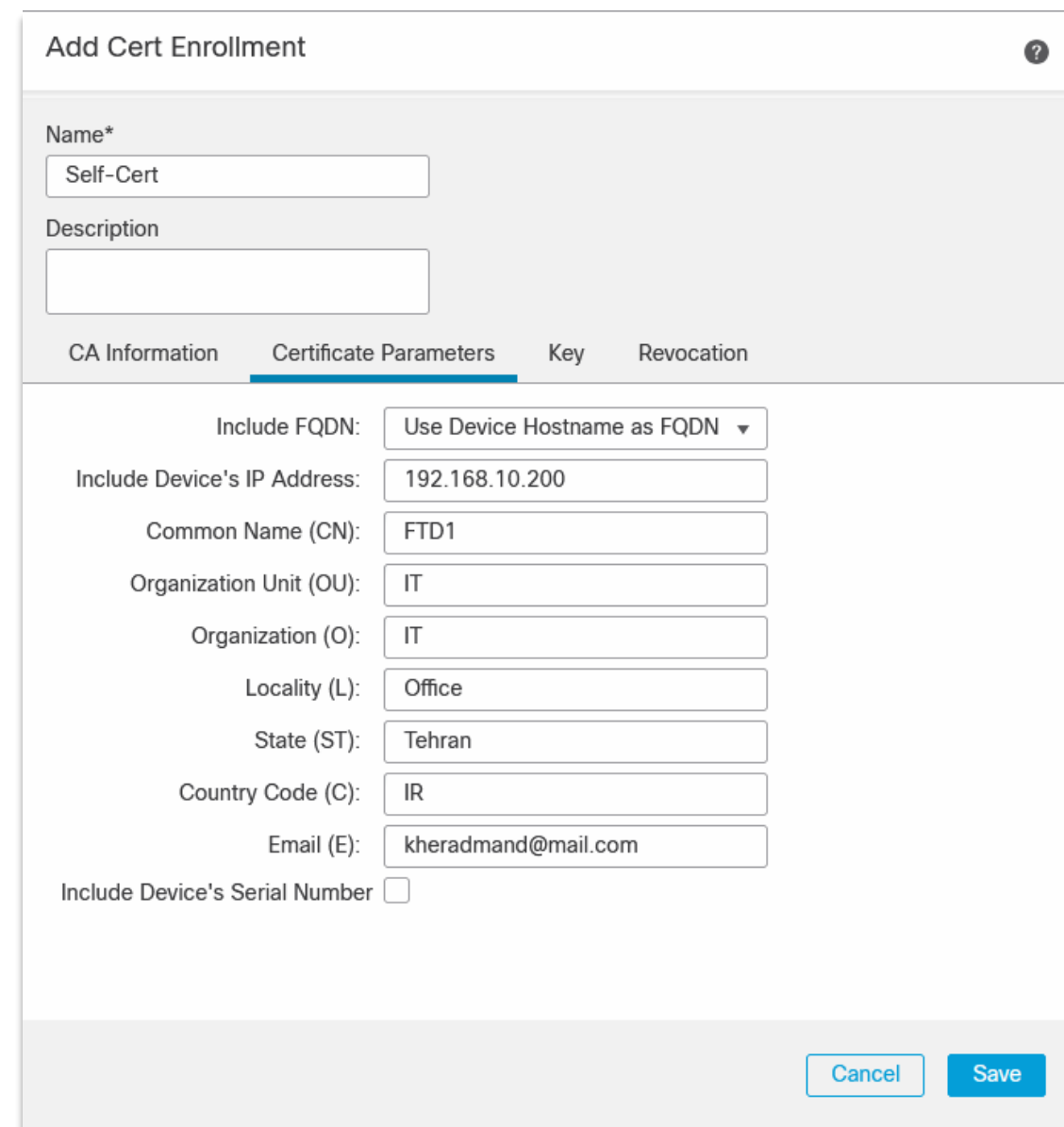
Remote Access VPN Deployment

➤ Certificate Enrollment

- Objects > Object Management > PKI > Cert Enrollment
 > Add Cert Enrollment
- ✓ You can use Self Signed Cert if any CA is not accessible



The screenshot shows the 'Add Cert Enrollment' form with the 'CA Information' tab selected. The 'Name*' field contains 'Self-Cert' and the 'Description' field is empty. Below the tabs, the 'Enrollment Type' dropdown is set to 'Self Signed Certificate'. A warning message is displayed: 'Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configure CN, please navigate to 'Certificate Parameters' tab.'



The screenshot shows the 'Add Cert Enrollment' form with the 'Certificate Parameters' tab selected. The 'Name*' field contains 'Self-Cert' and the 'Description' field is empty. The 'Certificate Parameters' tab contains the following fields:

- Include FQDN: Use Device Hostname as FQDN (dropdown)
- Include Device's IP Address: 192.168.10.200
- Common Name (CN): FTD1
- Organization Unit (OU): IT
- Organization (O): IT
- Locality (L): Office
- State (ST): Tehran
- Country Code (C): IR
- Email (E): kheradmand@mail.com
- Include Device's Serial Number: ☐

At the bottom right, there are 'Cancel' and 'Save' buttons.

Remote Access VPN Deployment

➤ Certificate Enrollment

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

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title 'Firepower Management Center', and tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The 'Devices' tab is selected, and the 'Certificates' sub-tab is active. A modal dialog box titled 'Add New Certificate' is open in the foreground. It contains the following fields and information:

- Name:** A text input field.
- Device*:** A dropdown menu with 'FTD1' selected.
- Cert Enrollment*:** A dropdown menu with 'Self-Cert' selected, followed by a '+' icon.
- Cert Enrollment Details:**
 - Name: Self-Cert
 - Enrollment Type: Self-Signed
 - Enrollment URL: N/A

At the bottom of the dialog are 'Cancel' and 'Add' buttons. In the background, a sidebar menu shows 'Certificates' selected, and a table with an 'Add' button is visible.

Remote Access VPN Deployment

➤ Network and IP Address Pool

- Objects > Object Management:
- Address pools:
The pre-allocated IP addresses for remote users

 Firepower Management Center
Objects / Object Management

Overview

- > AAA Server
- > Access List
- ✓ Address Pools

IPv4 Pools

IPv6 Pools

Application Filters

AS Path

IPv4 Pools

IPv4 pool contains list of IP

Name

Add IPv4 Pool

Name*

Remote-VPN-Users

IPv4 Address Range*

192.168.10.10-192.168.10.50

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

255.255.255.0

Description

☒ Allow Overrides

 Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

► Override (0)

Cancel

Save

No records to display

Deploy

Add IPv4 Pools

Filter

Value

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

The screenshot shows the Cisco FMC Setup Wizard for Remote Access VPN Policy. The interface includes a top navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, and Deploy. The main content area is titled "Remote Access VPN Policy Wizard" and features a progress bar with five steps: 1. Policy Assignment (active), 2. Connection Profile, 3. AnyConnect, 4. Access & Certificate, and 5. Summary.

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*

Headquarters-RAVPN-Profile

Description:

VPN Protocols:

- ☒ SSL
- ☒ IPsec-IKEv2

Targeted Devices:

Available Devices

- Branch Threat Defens
- Headquarters Threat
- Threat Defense

Selected Devices

- Headquarters Threat

Buttons: Cancel, Back, Next

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure [LOCAL](#) or [Realm](#) or [RADIUS Server Group](#) or [SSO](#) to authenticate VPN clients.

AnyConnect Client Package

Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

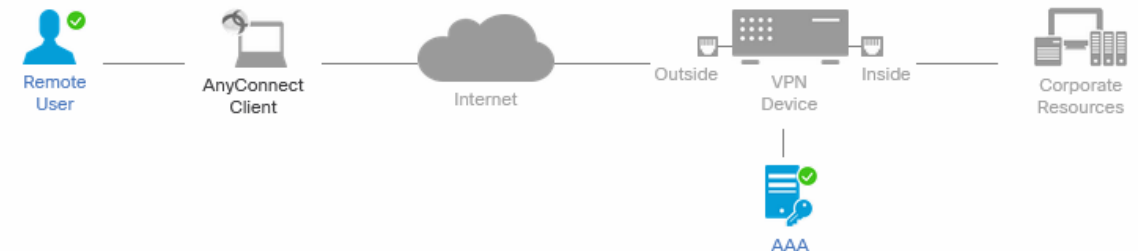
Remote Access VPN Deployment

➤ 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 Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary



Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:* RAVPN

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: AAA Only

Authentication Server:* RADIUS-Server
(LOCAL or Realm or RADIUS)
☒ Fallback to LOCAL Authentication

Local Realm:* Local-identity

Authorization Server: RADIUS-Server
(Realm or RADIUS)

Accounting Server: RADIUS-Server
(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are

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 Policy Wizard

1 Policy Assignment — 2 **Connection Profile** — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Authorization Server: +
(Realm or RADIUS)

Accounting Server: +
(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

☒ Use AAA Server (Realm or RADIUS only) ⓘ

☒ Use DHCP Servers

Use DHCP Servers: ✎

☒ Use IP Address Pools

IPv4 Address Pools: ✎

IPv6 Address Pools: ✎

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* +

[Edit Group Policy](#)

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

The screenshot shows the Cisco FMC Setup Wizard for Remote Access VPN Policy. The wizard is at step 3, 'AnyConnect', which is highlighted in blue. The previous steps are 'Policy Assignment' (1) and 'Connection Profile' (2). The next steps are 'Access & Certificate' (4) and 'Summary' (5). Below the step indicators is a diagram showing the VPN architecture: a Remote User connects via an AnyConnect Client to the Internet, then to a VPN Device (labeled 'Outside' and 'Inside'), which connects to Corporate Resources. A AAA server is also shown connected to the VPN Device. Below the diagram, the 'AnyConnect Client Image' section explains that the VPN gateway can automatically download the latest AnyConnect package. It provides a link to the Cisco Software Download Center. A table lists the available AnyConnect client packages for Linux, Mac OS, and Windows. The 'AnyConnect-Windows' package is selected with a checkmark. At the bottom right, there are 'Cancel', 'Back', and 'Next' buttons.

FMC Setup Wizard

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile **3 AnyConnect** 4 Access & Certificate 5 Summary

Remote User AnyConnect Client Internet Outside VPN Device Inside Corporate Resources AAA

AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

Show Re-order buttons +

AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
☐ AnyConnect-Linux	anyconnect-linux64-4.10.00093-webdeploy...	Linux
☐ AnyConnect-MacOS	anyconnect-macos-4.10.00093-webdeploy...	Mac OS
☒ AnyConnect-Windows	anyconnect-win-4.10.00093-webdeploy-k9...	Windows

Cancel Back 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

The screenshot shows the Cisco FMC Setup Wizard for Remote Access VPN Policy. The wizard is divided into five steps: 1. Policy Assignment, 2. Connection Profile, 3. AnyConnect, 4. Access & Certificate (current step), and 5. Summary. A diagram at the top illustrates the network flow: Remote User connects via AnyConnect Client to the Internet, then through an Outside interface to a VPN Device, and finally through an Inside interface to Corporate Resources. The VPN Device is also connected to an AAA server.

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +

☒ Enable DTLS on member interfaces

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

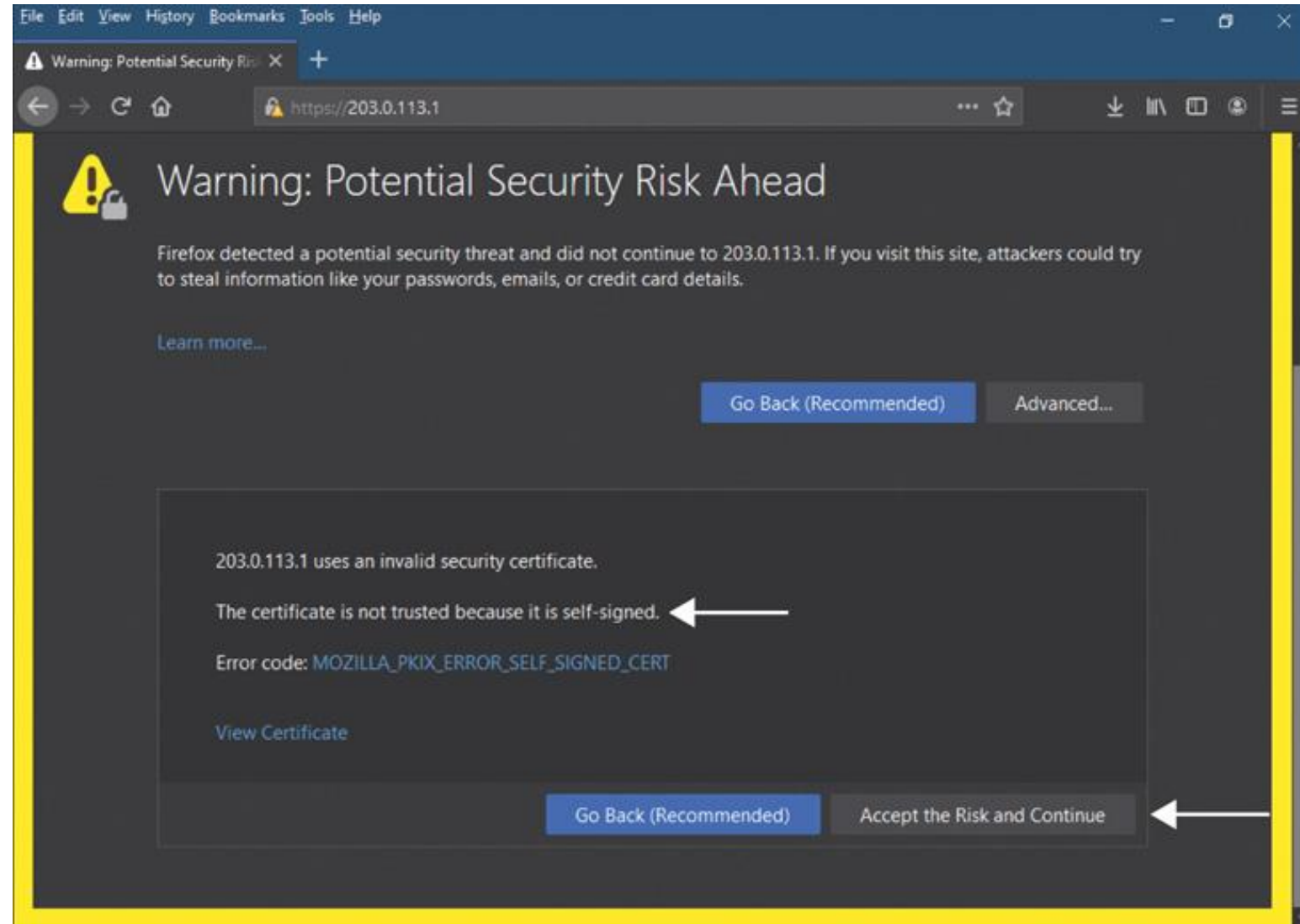
☐ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and

Buttons at the bottom: Cancel, Back, Next.

Remote Access VPN Deployment

➤ Verification

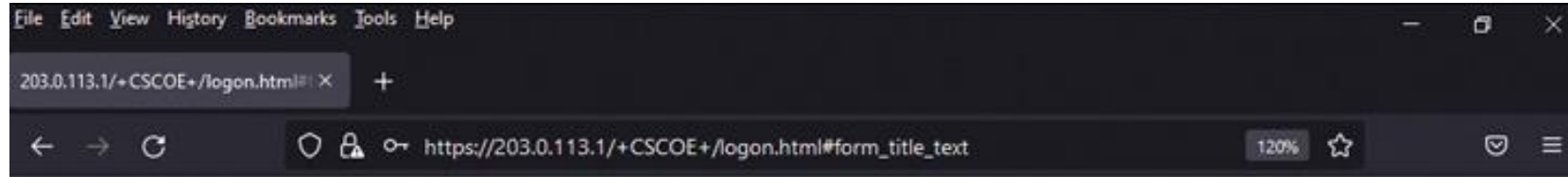
- a) In the remote host open a browser.
- b) Enter the IP address of the FTD's outside interface
- c) If you used a self-certificate, you are prompt to Accept the risk



Remote Access VPN Deployment

➤ Verification

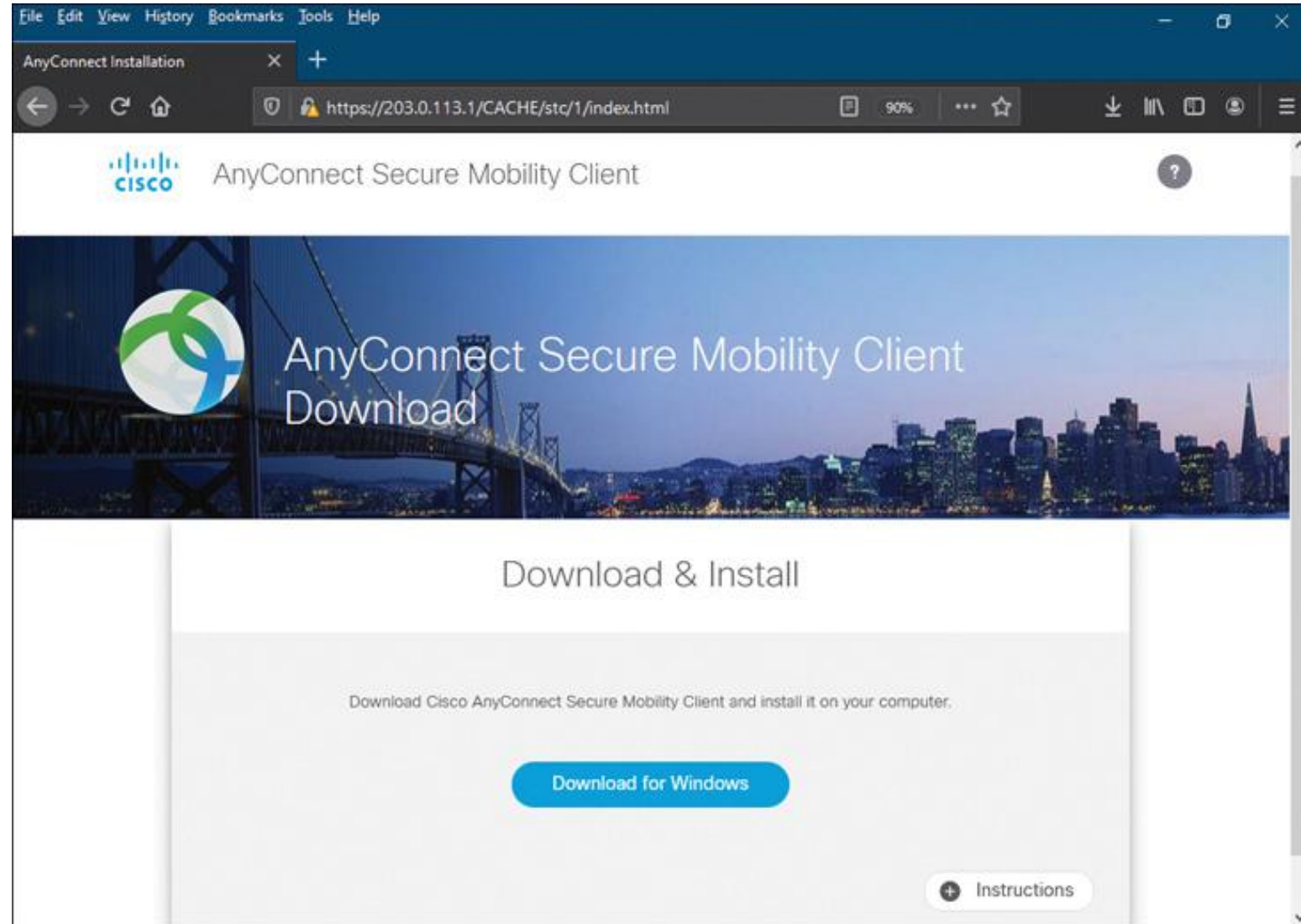
- a) Select the VPN name from Group
- b) Enter the username and password
- c) Click the Logon

A screenshot of a "Logon" dialog box. It has a title bar with a key icon and the word "Logon". Inside the dialog, there are three fields: "Group" with a dropdown menu showing "Headquarters-RAVPN-Profile", "Username" with the text "student", and "Password" with masked characters "*****". Below these fields is a "Logon" button.

Remote Access VPN Deployment

➤ Verification

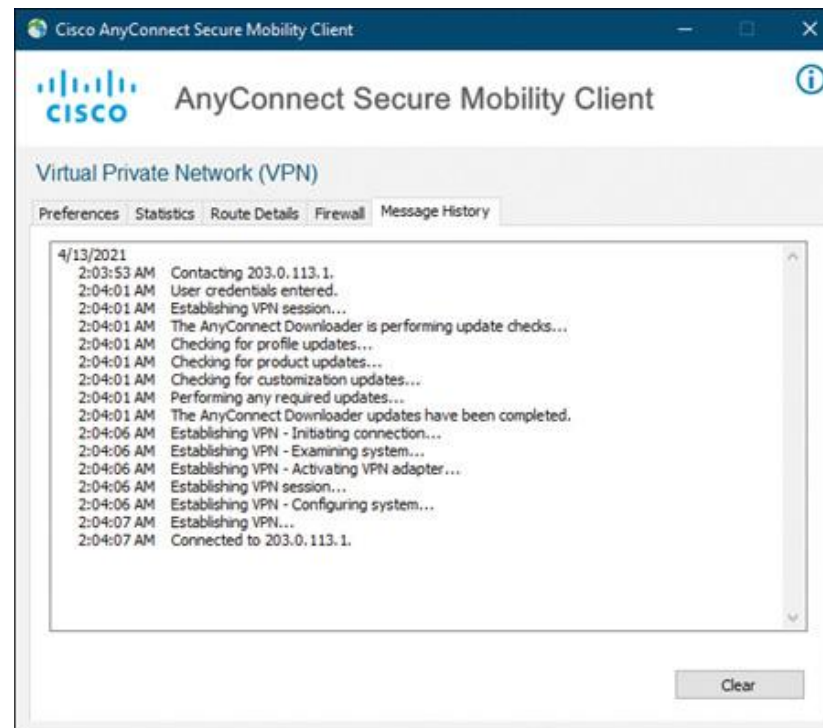
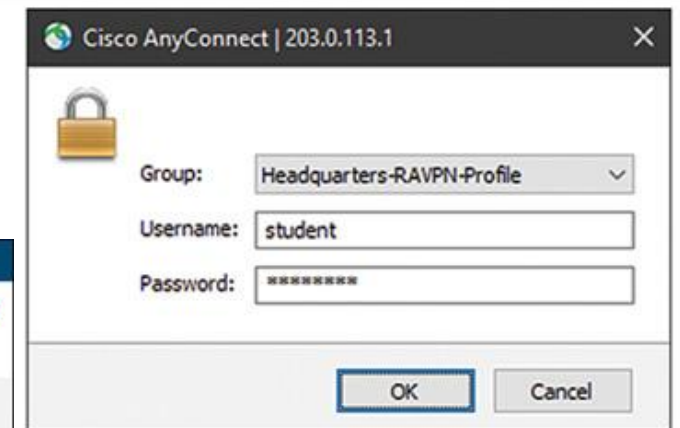
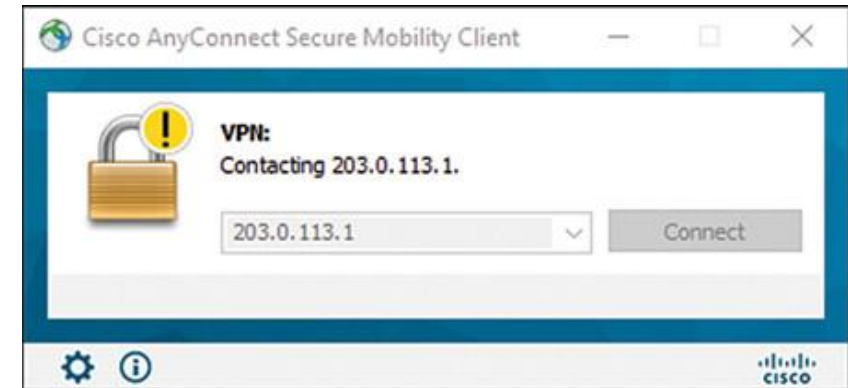
- a) Select the VPN name from Group
- b) Enter the username and password
- c) Click the Logon
- d) The browser prompts you to download and install the AnyConnect Secure Mobility Client



Remote Access VPN Deployment

➤ Verification

- When the installation is complete, open the AnyConnect client , enter the IP address of the FTD's outside interface
- Click the Connect button. A login window appears
- Enter the username and password again and click Ok

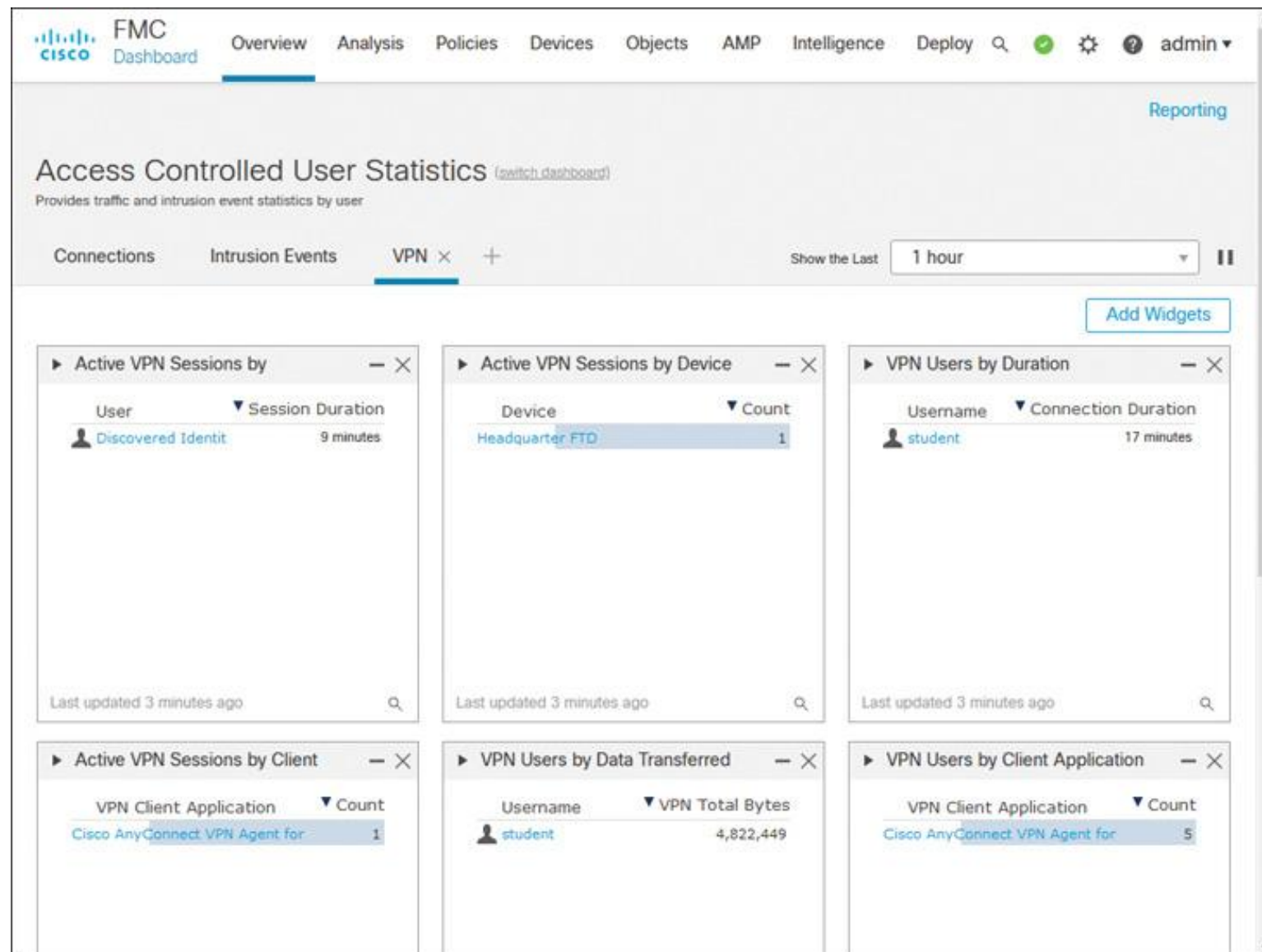


Remote Access VPN Deployment

➤ 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