

Configurazione del client VPN AnyConnect su FTD: esclusione hairpin e NAT

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Passaggio 1. Importa certificato SSL](#)

[Passaggio 2. Configurare un server RADIUS](#)

[Passaggio 3. Crea pool IP](#)

[Passaggio 4. Crea un profilo XML](#)

[Passaggio 5. Carica profilo XML Anyconnect](#)

[Passaggio 6. Carica immagini AnyConnect](#)

[Passaggio 7. Creazione guidata VPN ad accesso remoto](#)

[Esenzione NAT e hairpin](#)

[Passaggio 1. Configurazione esenzione NAT](#)

[Passaggio 2. Configurazione Hairpin](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare Cisco Remote Access VPN Solution (AnyConnect) su Firepower Threat Defense (FTD), versione 6.3, gestito da FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di VPN ad accesso remoto, SSL (Secure Sockets Layer) e IKEv2 (Internet Key Exchange versione 2)
- Autenticazione di base, autorizzazione e accounting (AAA) e conoscenza RADIUS
- Conoscenze base del CCP
- Conoscenze base FTD

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco FMC 6.4
- Cisco FTD 6.3
- AnyConnect 4.7

Questo documento descrive la procedura per configurare la soluzione VPN ad accesso remoto Cisco (AnyConnect) su Firepower Threat Defense (FTD), versione 6.3, gestita da Firepower Management Center (FMC).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento deve includere la configurazione sui dispositivi FTD. se si cerca l'esempio di configurazione ASA, consultare il documento: <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>

Limitazioni:

Al momento, queste funzionalità non sono supportate su FTD, ma sono ancora disponibili sui dispositivi ASA:

- Doppia autenticazione AAA (disponibile con FTD versione 6.5)
- Criterio di accesso dinamico
- Scansione host
- Postura ISE
- RADIUS CoA
- VPN load-balancer
- Autenticazione locale (disponibile in Firepower Device Manager 6.3. ID bug Cisco ([CSCvf92680](#)))
- Mappa attributi LDAP (disponibile tramite FlexConfig, ID bug Cisco [CSCvd64585](#))
- Personalizzazione AnyConnect
- Script AnyConnect
- Localizzazione AnyConnect
- VPN per app
- Proxy SCEP
- Integrazione WSA
- SSO SAML (ID bug Cisco [CSCvq90789](#))
- Mappa crittografica dinamica IKEv2 simultanea per RA e VPN L2L
- Moduli AnyConnect (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security e così via). DART è l'unico modulo installato per impostazione predefinita in questa versione.
- TACACS, Kerberos (autenticazione KCD e RSA SDI)
- Proxy browser

Configurazione

Per eseguire la procedura guidata della VPN ad accesso remoto nel FMC, è necessario completare i seguenti passaggi:

Passaggio 1. Importa certificato SSL

I certificati sono essenziali quando si configura AnyConnect. Per SSL e IPsec sono supportati solo i certificati basati su RSA.

I certificati ECDSA (Elliptic Curve Digital Signature Algorithm) sono supportati in IPsec, tuttavia non è possibile distribuire un nuovo pacchetto AnyConnect o un nuovo profilo XML quando si utilizza un certificato basato su ECDSA.

Può essere utilizzato per IPsec, ma è necessario pre-distribuire i pacchetti AnyConnect insieme al profilo XML. Tutti gli aggiornamenti del profilo XML devono essere push manualmente su ciascun client (ID bug Cisco [CSCtx42595](#)).

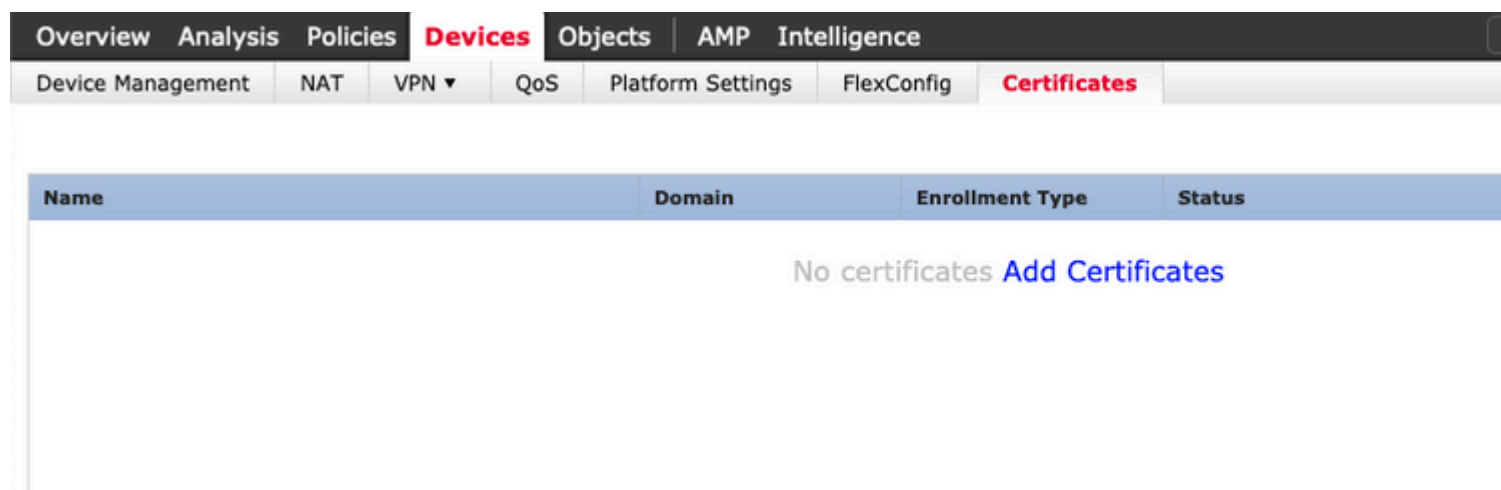
Inoltre, il certificato deve contenere un'estensione del nome comune (CN) con nome DNS e/o indirizzo IP per evitare errori di tipo "Certificato server non attendibile" nei browser Web.

Nota: nei dispositivi FTD è necessario il certificato CA (Certification Authority) prima che venga generata la richiesta CSR (Certificate Signing Request).

- Se il CSR viene generato in un server esterno, ad esempio Windows Server o OpenSSL, il **metodo di registrazione manuale** non riuscirà, in quanto FTD non supporta la registrazione manuale delle chiavi.
- Utilizzare un metodo diverso, ad esempio PKCS12.

Per ottenere un certificato per l'accessorio FTD con il metodo di registrazione manuale, è necessario generare un CSR, firmarlo con una CA e quindi importare il certificato di identità.

1. Passare a **Dispositivi > Certificati** e selezionare **Aggiungi** come mostrato nell'immagine.



2. Selezionare il **dispositivo** e aggiungere un nuovo oggetto **Registrazione certificato**, come mostrato nell'immagine.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

Add Cert Enrollment

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

Enrollment URL:*

Challenge Password:

Confirm Password:

Retry Period: Minutes (Range 1-60)

Retry Count: (Range 0-100)

Fingerprint:

Allow Overrides

3. Selezionare il **tipo di registrazione** manuale e incollare il certificato CA (il certificato che deve firmare il CSR).

Add Cert Enrollment

? X

Name* Anyconnect-certificate

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: Manual

CA Certificate: *

```
/3C4h07uzuRDyggwKEBaMdg4DI/z
4x3nk3tTUhyppmbWqWAXM7GNDRVWG9BZ1svk3shDK2Bogkzou6
RqV66G9IE7Z2
xiVrSrJFqhrT795kMb8amBxhb4eXYXUjJmODtPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFsKuZay27a48e/IJG2LgRDrA0Kt+jwb57DGSK4mfZsZqhFdQP
LhBNFbyBVb9
dOJukmd5vzQDR5qSo+HINEm3E8/q20wrtIzP4MpAabyhr+hEpeP
VMYhIVBOT8h
H8eMJSQjGhhHkuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDv
mwNgy5mTP9cHh
9Or3RIWRzEa11HE3mHO4Rj6DOnmgujx+TZRYczownSKLL7LcW1
D8ZcLYmfaIdC
W2CZuBR0yVDxvCq4f04ISEIBFOWFSd5rAD/bvk2n6xrJI1SLqABMJ
uslu9KTGH1
bIVKEYACKVYETw==
-----END CERTIFICATE-----
```

Allow Overrides

Save Cancel

4. Selezionare la scheda **Parametri certificato** e selezionare "FQDN personalizzato" per il campo **Includi FQDN** e compilare i dettagli del certificato come mostrato nell'immagine.

Add Cert Enrollment

? X

Name* Anyconnect-certificate

Description

CA Information **Certificate Parameters** Key Revocation

Include FQDN: Use Device Hostname as FQDN

Include Device's IP Address:

Common Name (CN): vpn.cisco.com

Organization Unit (OU): TAC

Organization (O): Cisco

Locality (L): MX

State (ST): Mexico

Country Code (C): MX

Email (E):

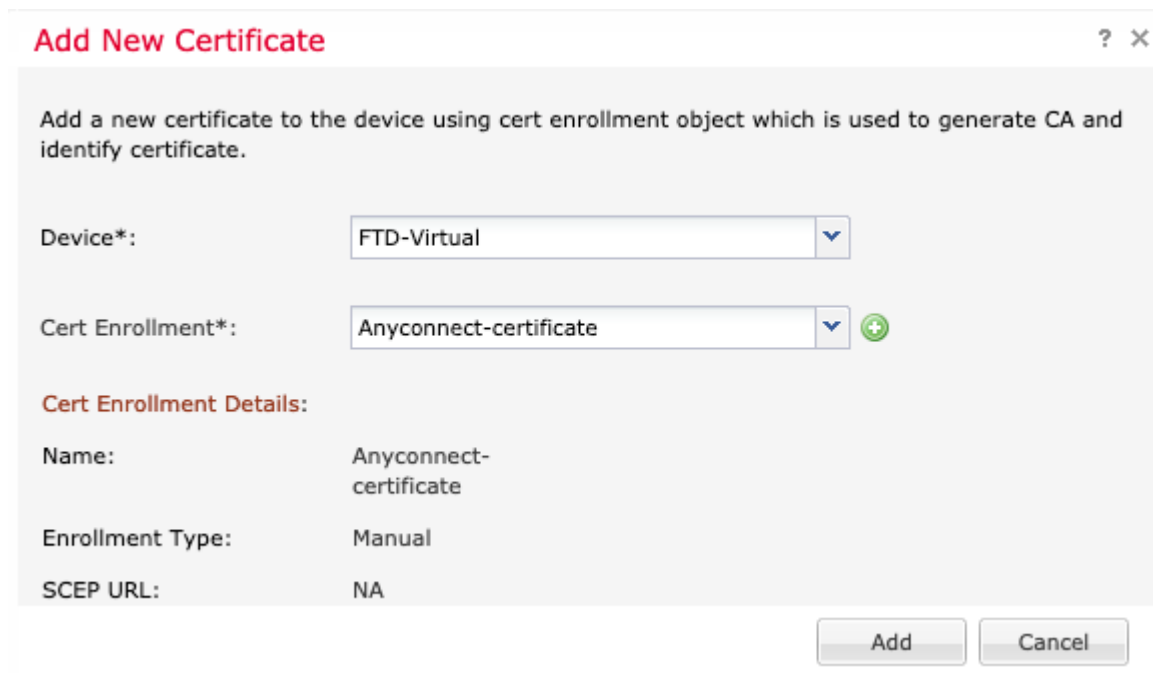
Include Device's Serial Number

Allow Overrides

Save Cancel

5. Selezionare la scheda **Chiave** e selezionare il tipo di chiave, è possibile scegliere il nome e la dimensione. Per RSA, sono richiesti almeno 2048 byte.

6. Selezionare Salva, confermare il **dispositivo** e in **Registrazione certificato** selezionare il trust point appena creato, selezionare **Aggiungi** per distribuire il certificato.



Add New Certificate ? x

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: FTD-Virtual

Cert Enrollment*: Anyconnect-certificate

Cert Enrollment Details:

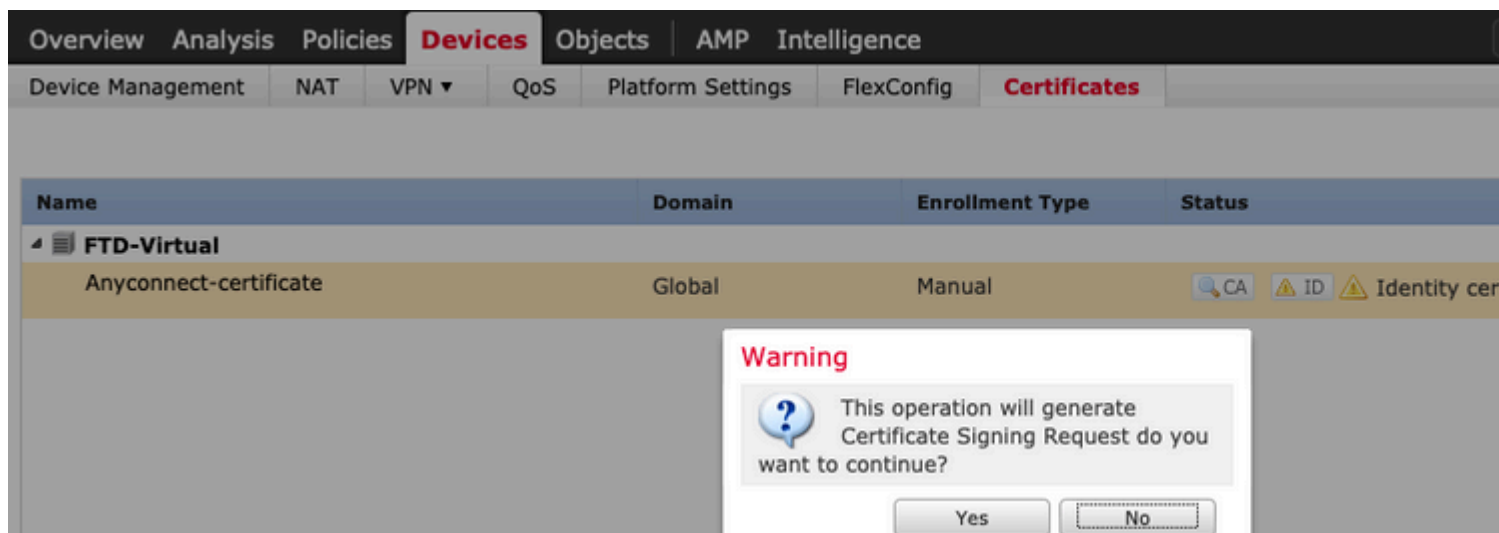
Name: Anyconnect-certificate

Enrollment Type: Manual

SCEP URL: NA

Add Cancel

7. Nella colonna **Stato**, selezionare l'icona **ID** e selezionare **Sì** per generare il CSR come illustrato nell'immagine.



Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Name	Domain	Enrollment Type	Status
FTD-Virtual			
Anyconnect-certificate	Global	Manual	CA ID Identity cer

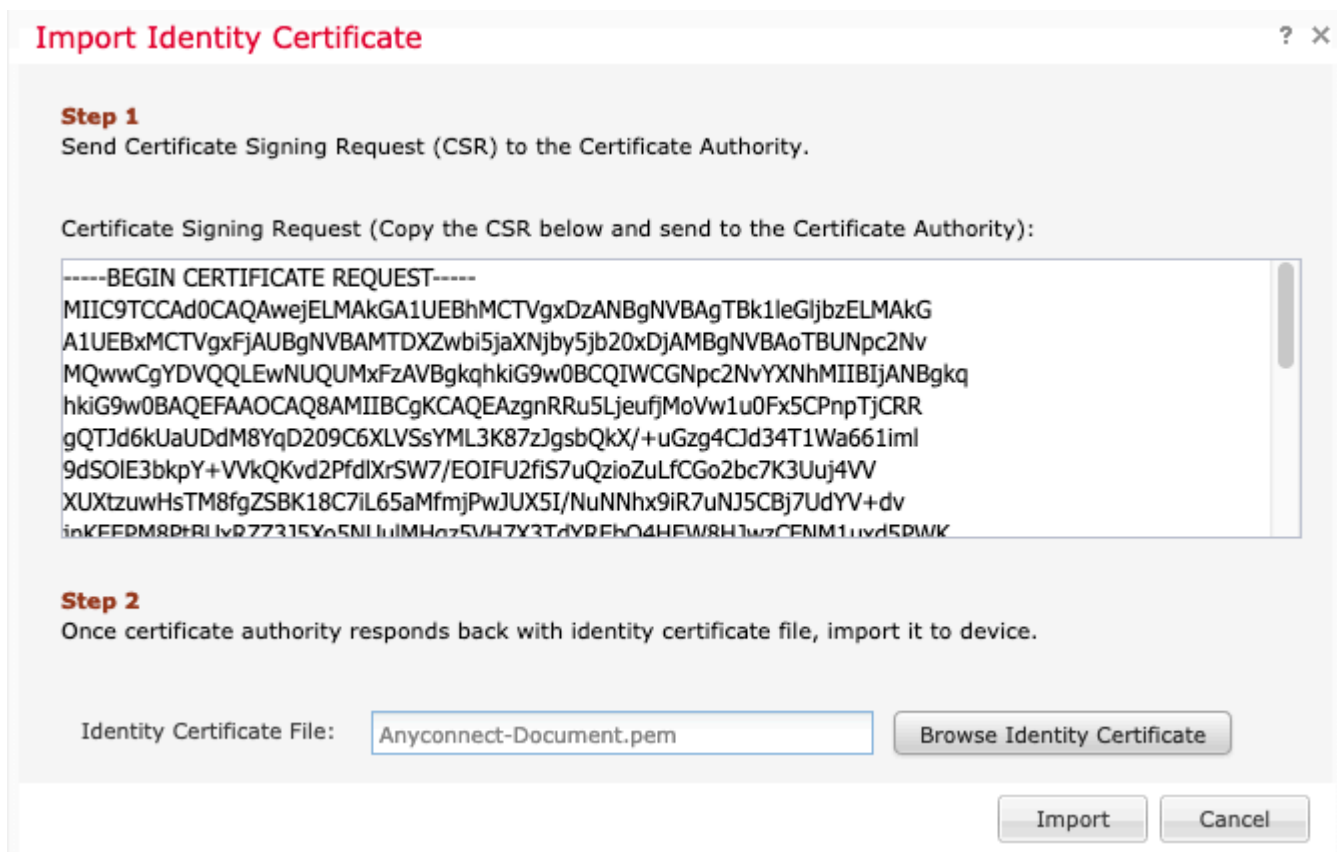
Warning

This operation will generate Certificate Signing Request do you want to continue?

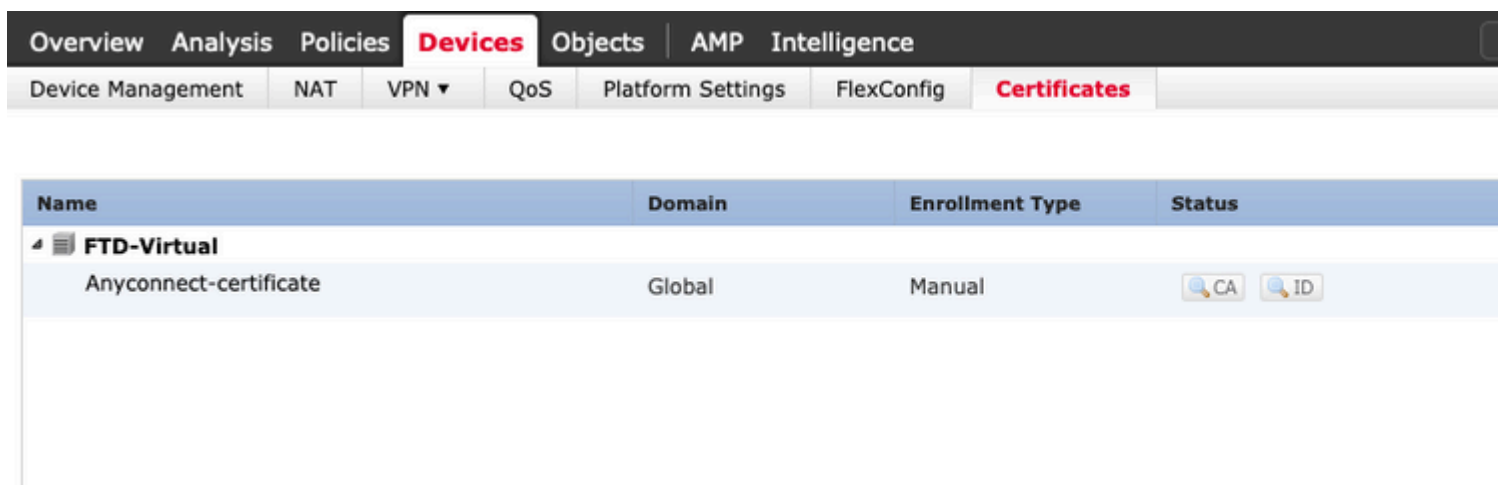
Yes No

8. Copiare CSR e firmarlo con la CA preferita (ad esempio, GoDaddy o DigiCert).

9. Dopo aver ricevuto il certificato di identità dalla CA (che deve essere nel formato base64), selezionare **Sfogliare certificato di identità** e individuare il certificato nel computer locale. Selezionare **Importa**.



10. Dopo l'importazione, saranno disponibili per la visualizzazione sia i dettagli del certificato CA che quelli del certificato ID.



Passaggio 2. Configurare un server RADIUS

Nei dispositivi FTD gestiti da FMC, il database degli utenti locale non è supportato. È necessario utilizzare un altro metodo di autenticazione, ad esempio RADIUS o LDAP.

1. Passare a **Oggetti > Gestione oggetti > Gruppo server RADIUS > Aggiungi gruppo server RADIUS** come mostrato nell'immagine.

Add RADIUS Server Group



Name:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms: ▼


Enable authorize only

Enable interim account update

Interval:* (1-120) hours

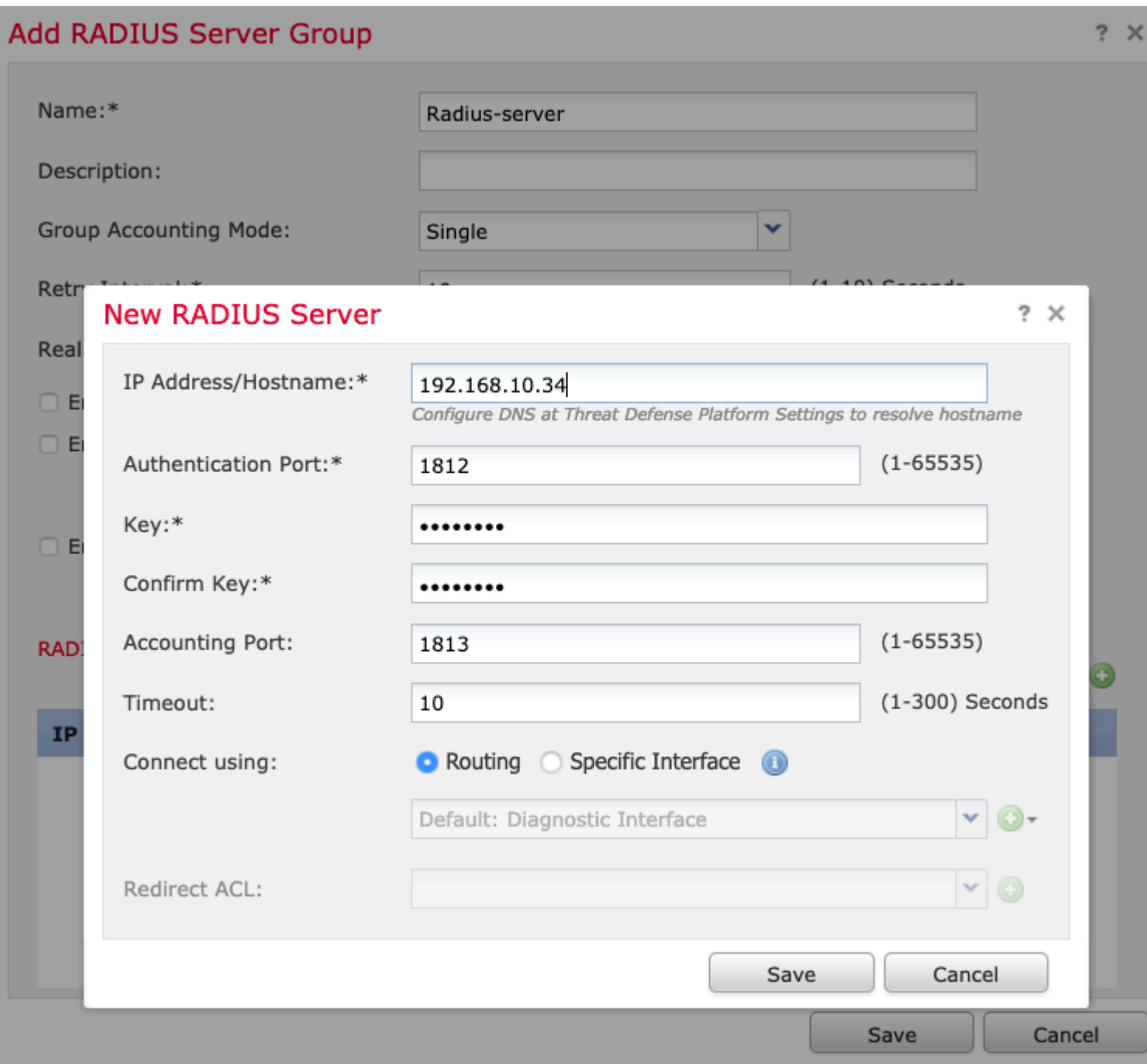
Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers) 

IP Address/Hostname
No records to display

2. Assegnare un nome al **gruppo di server Radius** e aggiungere l'indirizzo IP del server Radius insieme a un segreto condiviso (il segreto condiviso è necessario per accoppiare l'FTD al server Radius), selezionare **Salva** una volta completato il modulo, come mostrato nell'immagine.



3. Le informazioni sul server RADIUS sono ora disponibili nell'elenco dei server RADIUS come mostrato nell'immagine.

Add RADIUS Server Group



Name:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms: ▼

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

192.168.10.34



Save

Cancel

Passaggio 3. Crea pool IP

1. Passare a **Oggetti > Gestione oggetti > Pool di indirizzi > Aggiungi pool IPv4**.

2. Assegnare il nome e l'intervallo di indirizzi IP, il campo **Maschera** non è obbligatorio, ma può essere specificato come mostrato nell'immagine.

Add IPv4 Pool

Name*

IPv4 Address Range*
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

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

Passaggio 4. Crea un profilo XML

1. Scaricare lo strumento **Editor di profili** da Cisco.com ed eseguire l'applicazione.
2. Nell'applicazione Editor di profili, passare a **Elenco server** e selezionare **Aggiungi** come mostrato nell'immagine.

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

Hostname	Host Address	User Group	Backup Server List	SCEP

Note: it is highly recommended that at least one server be defined in a profil

3. Assegnare un **nome visualizzato**, un **nome di dominio completo (FQDN)** o un **indirizzo IP** e selezionare **OK** come mostrato nell'immagine.

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) Corporate - FTD (SSL)

FQDN or IP Address User Group

vpn.cisco.com / ssl

Group URL

Connection Information

Primary Protocol SSL

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address

Add

Move Up

Move Down

Delete

OK Cancel

4. La voce è ora visibile nel menu **Elenco server**:

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

Profile: Untitled

Hostname	Host Address	User Group	Backup Server ...	SCEP	Mobil
Corporate - FTD (SSL)	vpn.cisco.com	ssl	-- Inherited --		

Note: it is highly recommended that at least one server be defined in a profile.

Add... Edit...

5. Selezionare **File > Salva con nome**.

Nota: salvare il profilo con un nome facilmente identificabile con estensione **.xml**.

Passaggio 5. Carica profilo XML Anyconnect

1. Nel FMC, selezionare Oggetti > **Gestione oggetti** > **VPN** > **File AnyConnect** > **Aggiungi file AnyConnect**.

2. Assegnare un **nome** all'oggetto e fare clic su **Sfoggia**, individuare il profilo client nel sistema locale e selezionare **Salva**.

Attenzione: selezionare **Anyconnect Client Profile** come tipo di file.

Add AnyConnect File

Name:* Corporate-profile(SSL)

File Name:* FTD-corp-ssl.xml

File Type:* AnyConnect Client Profile

Description:

Passaggio 6. Carica immagini AnyConnect

1. Scarica le immagini webdeploy (**.pkg**) dalla pagina Web dei download di Cisco.

AnyConnect Headend Deployment Package (Mac OS)	26-Jun-2019	51.22 MB	↓
anyconnect-macos-4.7.04056-webdeploy-k9.pkg			

2. Passare a Oggetti > **Gestione oggetti** > **VPN** > **File AnyConnect** > **Aggiungi file AnyConnect**.

3. Assegnare un nome al file del pacchetto Anyconnect e selezionare il file **.pkg** dal sistema locale, una volta selezionato il file.

4. Selezionare **Salva**.

Add AnyConnect File ? X

Name:*

File Name:*

File Type:* ▼

Description:

Nota: è possibile caricare pacchetti aggiuntivi in base ai requisiti (Windows, Mac, Linux).

Passaggio 7. Creazione guidata VPN ad accesso remoto

In base ai passaggi precedenti, è possibile seguire la procedura guidata di Accesso remoto.

1. Passare a **Dispositivi > VPN > Accesso remoto**.

2. Assegnare il nome del criterio di accesso remoto e selezionare un dispositivo FTD da **Dispositivi disponibili**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 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:* TAC

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices:

Available Devices

Search

FTD-Virtual

Selected Devices

FTD-Virtual

Add

Before You Start

Before you start, configuration elements to complete Remote Access VPN.

Authentication Server

Configure [Realm](#) or to authenticate VPN.

AnyConnect Client

Make sure you have for VPN Client download the relevant Cisco client during the wizard.

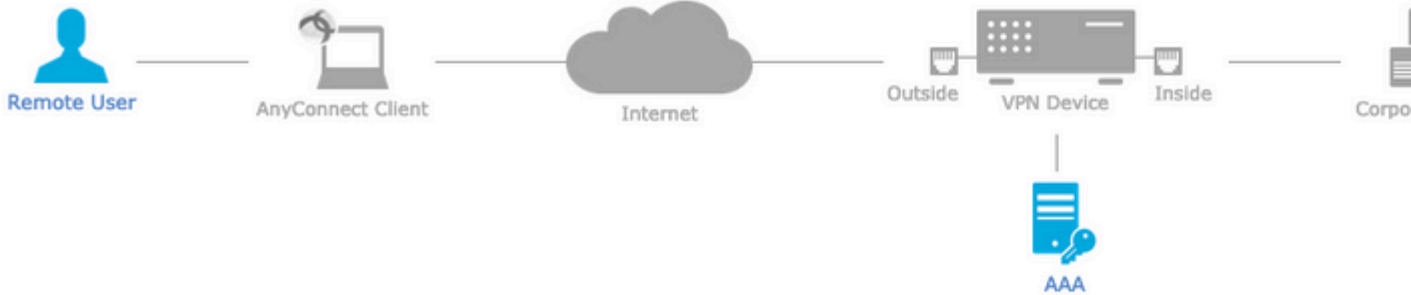
Device Interface

Interfaces should be targeted [devices](#) so as a security zone enable VPN access.

3. Assegnare il **nome del profilo di connessione** (il nome del profilo di connessione è il nome del gruppo di tunnel), selezionare **Server di autenticazione** e **Pool di indirizzi** come mostrato nell'immagine.

Remote Access VPN Policy Wizard

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



Connection Profile:

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

Connection Profile Name:*

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: ▼
 Authentication Server:* ▼ + (Realm or RADIUS)
 Authorization Server: ▼ + (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 (RADIUS only) i
 Use DHCP Servers
 Use IP Address Pools
 IPv4 Address Pools: ✎
 IPv6 Address Pools: ✎

Group Policy:

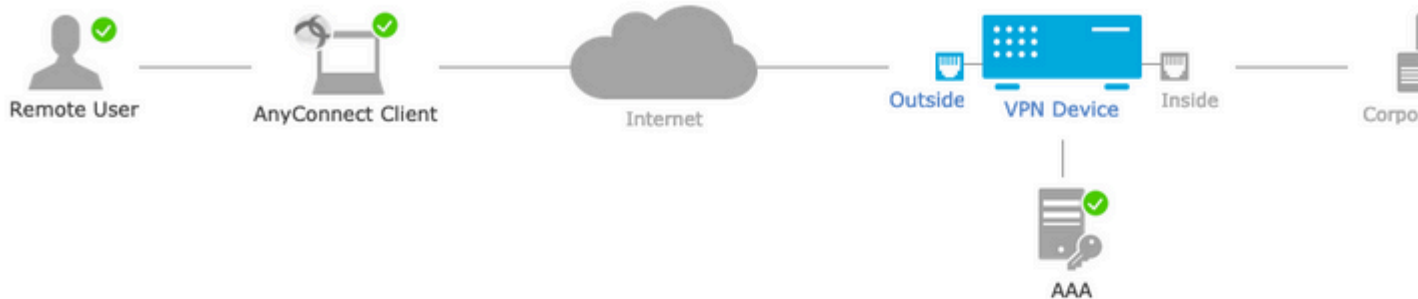
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. or create a Group Policy object.

Group Policy:* ▼ +
[Edit Group Policy](#)

in questo scenario, l'FTD è configurato in modo da non ispezionare il traffico VPN. Ignorare l'opzione Access Control Policies (ACP).


Remote Access VPN Policy Wizard

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



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 authorization ACL downloaded from AAA server are still applied to VPN traffic.

Back

Next

10. Selezionare **Finish** (Fine) e **Deploy** (Distribuisci) per le modifiche:

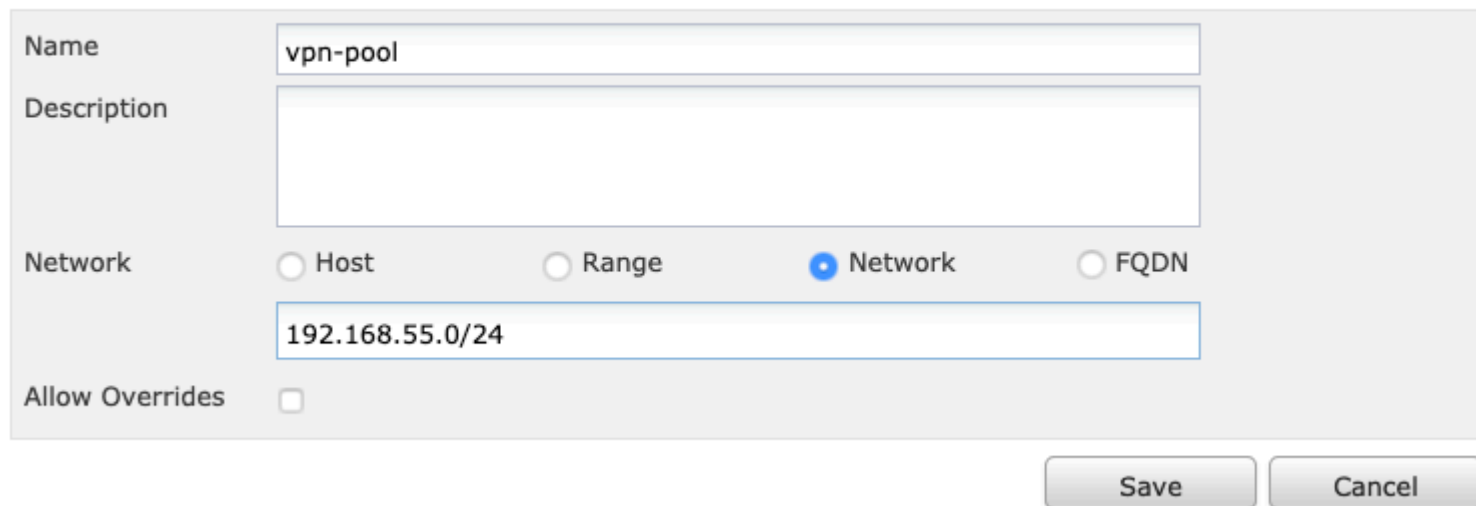
Tutta la configurazione relativa ai certificati VPN, SSL e ai pacchetti AnyConnect viene sottoposta a

è un metodo di traduzione preferito utilizzato per impedire il routing del traffico a Internet quando il traffico deve passare su un tunnel VPN (accesso remoto o da sito a sito).

Questa operazione è necessaria quando il traffico proveniente dalla rete interna deve passare attraverso i tunnel senza alcuna conversione.

1. Passare a **Oggetti > Rete > Aggiungi rete > Aggiungi oggetto** come mostrato nell'immagine.

New Network Object



Name: vpn-pool

Description:

Network: Host Range Network FQDN

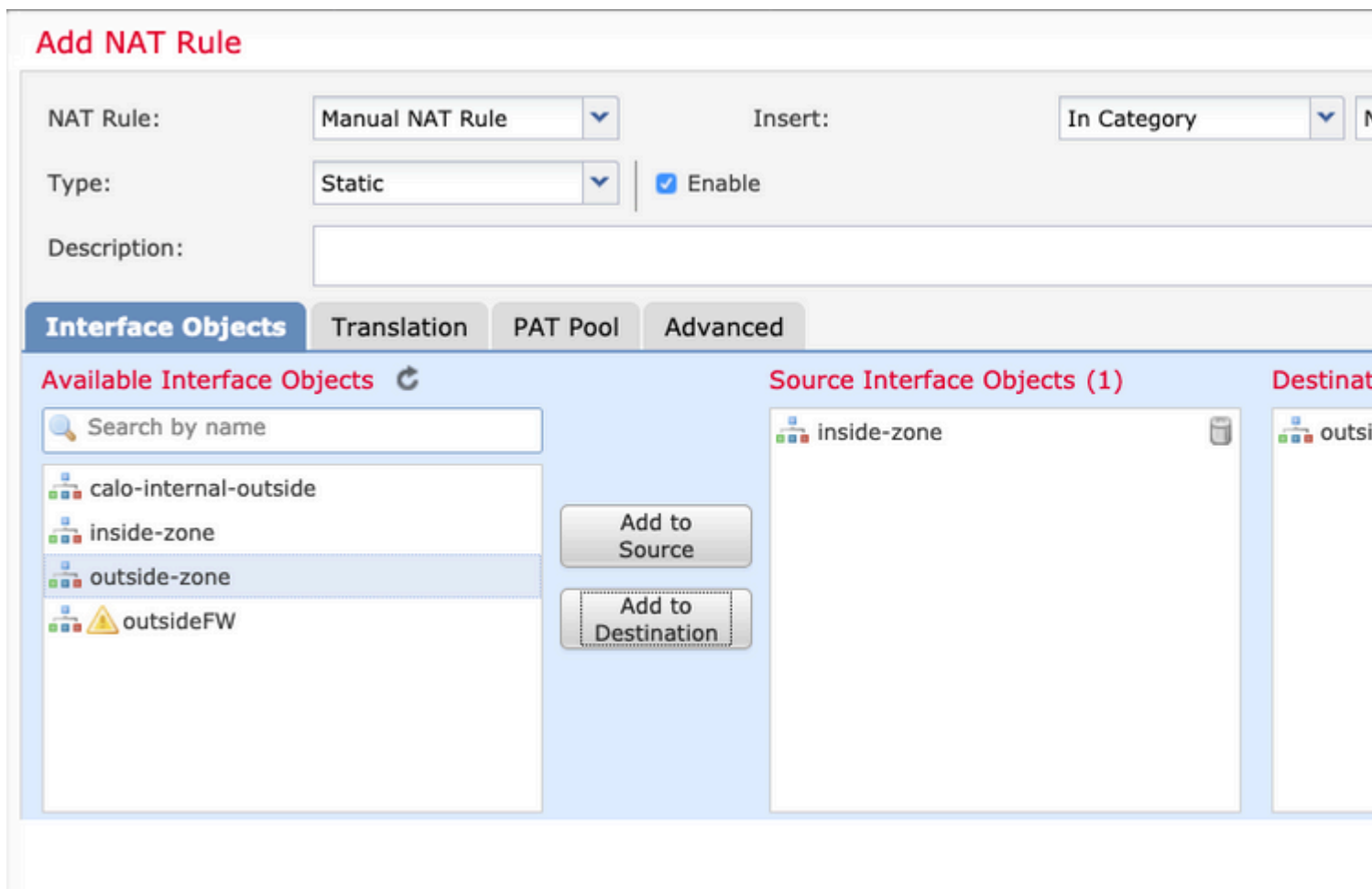
192.168.55.0/24

Allow Overrides:

Save Cancel

2. Passare a **Dispositivo > NAT**, selezionare il criterio NAT utilizzato dal dispositivo in questione e creare una nuova istruzione.

Nota: il traffico va dall'interno all'esterno.



3. Selezionare le risorse interne dietro l'FTD (**origine originale** e **origine tradotta**) e la destinazione come pool locale IP per gli utenti Anyconnect (**destinazione originale** e **destinazione tradotta**), come mostrato nell'immagine.

Add NAT Rule

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* <input type="text" value="FTDv-Inside-SUPERNE"/>	Translated Source: <input type="text" value="Address"/>
Original Destination: <input type="text" value="Address"/> <input type="text" value="vpn-pool"/>	Translated Destination: <input type="text" value="vpn-po"/>
Original Source Port: <input type="text"/>	Translated Source Port: <input type="text"/>
Original Destination Port: <input type="text"/>	Translated Destination Port: <input type="text"/>

4. Accertarsi di attivare o disattivare le opzioni (come mostrato nell'immagine), per abilitare "no-proxy-arp" e "route-lookup" nella regola NAT, selezionare **OK** come mostrato nell'immagine.

Edit NAT Rule

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

- Translate DNS replies that match this rule
- Fallthrough to Interface PAT(Destination Interface)
- IPv6
- Net to Net Mapping
- Do not proxy ARP on Destination Interface
- Perform Route Lookup for Destination Interface
- Unidirectional

5. Questo è il risultato della configurazione di esenzione NAT.

1 Static inside-zone outside-zone FTDv-Inside-SUPERNE vpn-pool FTDv-Inside-SUPERNE vpn-pool

Gli oggetti utilizzati nella sezione precedente sono quelli descritti di seguito.

Name

Description

Network Host Range Network

Allow Overrides

Name	<input type="text" value="vpn-pool"/>
Description	<input type="text"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input checked="" type="radio"/> Network <input type="radio"/>
	<input type="text" value="192.168.55.0/24"/>
Allow Overrides	<input type="checkbox"/>

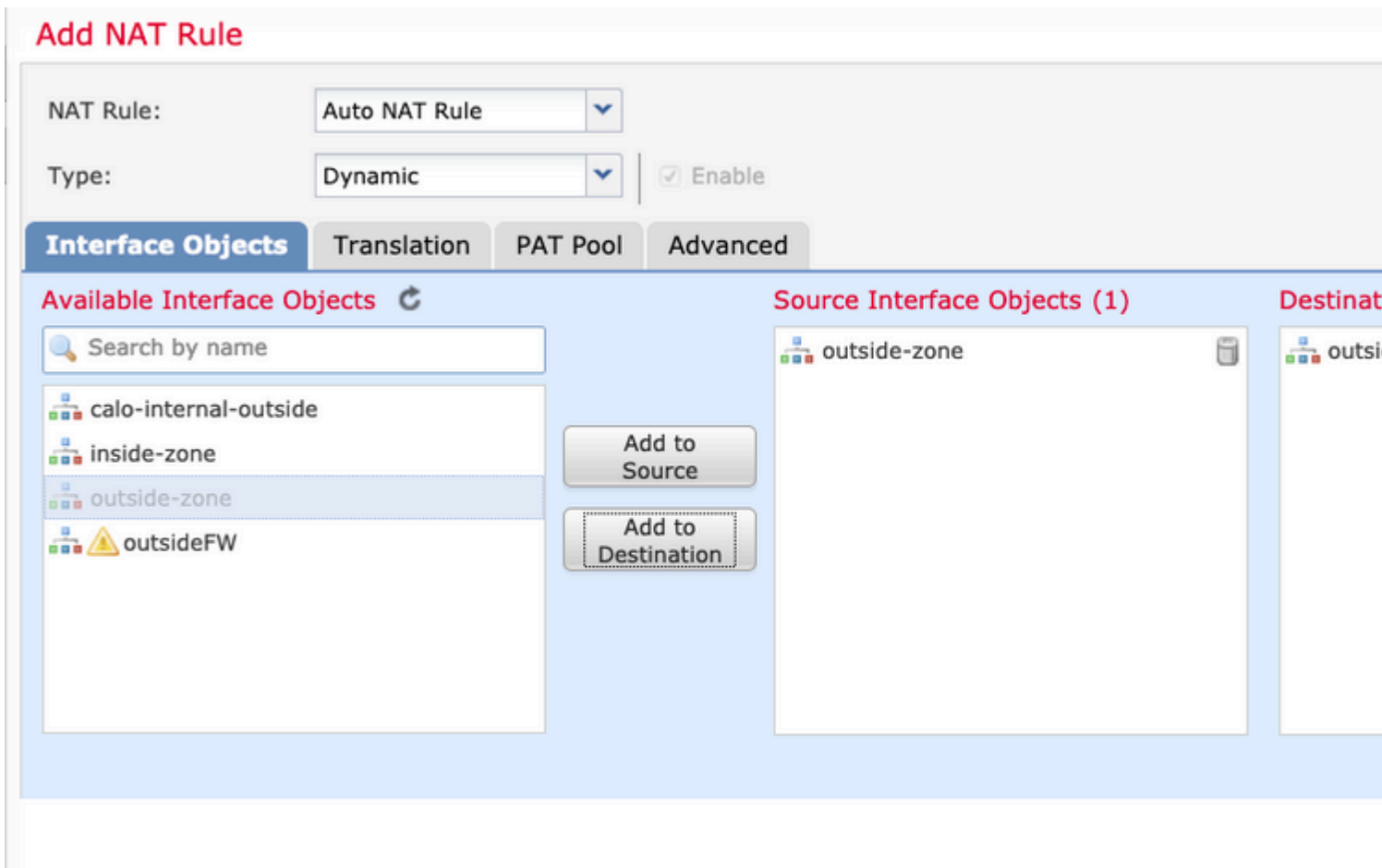
Passaggio 2. Configurazione Hairpin

Questo metodo di traduzione, noto anche come **U-turn**, consente al traffico di passare attraverso la stessa interfaccia su cui viene ricevuto il traffico.

Ad esempio, quando si configura Anyconnect con un criterio di split-tunnel **completo**, è possibile accedere alle risorse interne in base al criterio di esenzione NAT. Se il traffico del client Anyconnect deve raggiungere un sito esterno su Internet, il dispositivo NAT (o inversione a U) è responsabile del routing del traffico dall'esterno verso l'esterno.

È necessario creare un oggetto pool VPN prima della configurazione NAT.

1. Creare una nuova istruzione NAT, selezionare **Regola NAT automatica** nel campo **Regola NAT** e selezionare **Dinamica** come **Tipo NAT**.
2. Selezionare la stessa interfaccia per gli oggetti dell'interfaccia di **origine** e di destinazione (esterni):



3. Nella scheda Traduzione, selezionare come **Origine originale** l'oggetto vpn-pool e selezionare **Destination Interface IP** come **Origine tradotta**, selezionare **OK** come mostrato nell'immagine.

Add NAT Rule

NAT Rule: ▼

Type: ▼ Enable

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source:* ▼ +

Original Port: ▼

Translated Packet

Translated Source: ▼ i The va Object

Translated Port:

4. Questo è il riepilogo della configurazione NAT come mostrato nell'immagine.

Rules									
Filter by Device Filter Rules									
#	Direction	Type	Source Interface Obje...	Destination Interface Obje...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destination
▼ NAT Rules Before									
1	↔	Static	inside-zone	outside-zone	FTDv-Inside-SUPERNE	vpn-pool		FTDv-Inside-SUPERNE	vpn-pool
▼ Auto NAT Rules									
#	→	Dyna...	outside-zone	outside-zone	vpn-pool			Interface	
▼ NAT Rules After									

5. Fare clic su **Salva** e **distribuisi** le modifiche.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Eeguire questi comandi nella riga di comando FTD.

- **certificati ca di crittografia sh**
- **show running-config ip local pool**
- **show running-config webvpn**
- **show running-config tunnel-group**

- **show running-config criteri-gruppo**
- **show running-config ssl**
- **show running-config nat**

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche sulla risoluzione dei problemi per questa configurazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).