

Configura VPN ad accesso remoto su FTD Gestito da FDM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Licenze](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Verifica delle licenze sull'FTD](#)

[Definizione di reti protette](#)

[Crea utenti locali](#)

[Aggiungi certificato](#)

[Configura VPN di accesso remoto](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Problemi del client AnyConnect](#)

[Problemi iniziali di connettività](#)

[Problemi specifici del traffico](#)

Introduzione

In questo documento viene descritto come configurare la distribuzione di una VPN ASR su FTD gestita dal manager integrato FDM con versione 6.5.0 e successive.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della configurazione della VPN (Virtual Private Network) di accesso remoto su Firepower Device Manager (FDM).

Licenze

- Firepower Threat Defense (FTD) registrato con il portale delle licenze intelligenti con le funzionalità controllate da esportazione abilitate (per consentire l'attivazione della scheda di configurazione della VPN dell'Autorità registrazione)

- Una delle licenze AnyConnect abilitata (APEX, Plus o VPN Only)

Componenti usati

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

- Cisco FTD con versione 6.5.0-115
- Cisco AnyConnect Secure Mobility Client versione 4.7.01076

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.

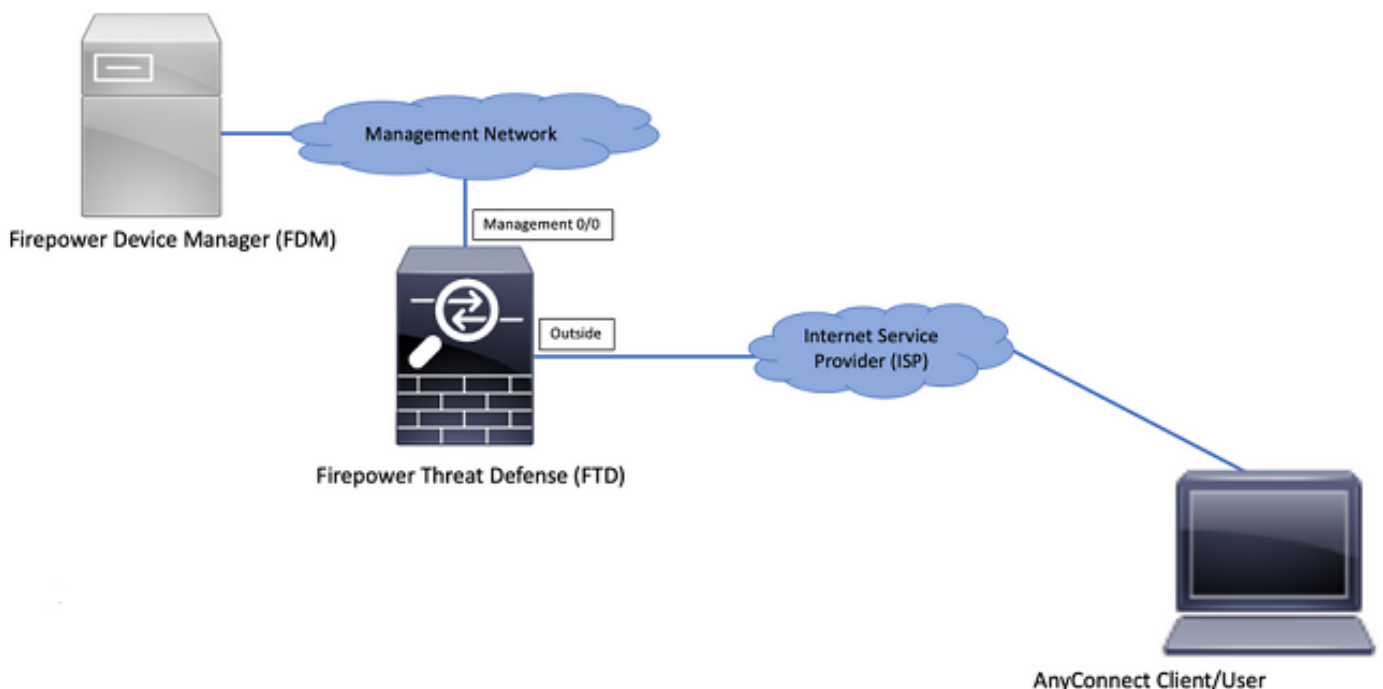
Premesse

La configurazione di FTD tramite FDM crea problemi quando si cerca di stabilire connessioni per i client AnyConnect tramite l'interfaccia esterna e si accede alla gestione tramite la stessa interfaccia. Si tratta di una limitazione nota di FDM. Richiesta di miglioramento [CSCvm76499](https://cisco.cisco.com/web/bugtools/bugsearch/bug?bugid=CSCvm76499) archiviata per questo problema.

Configurazione

Esempio di rete

Autenticazione del client AnyConnect con l'uso di Local.

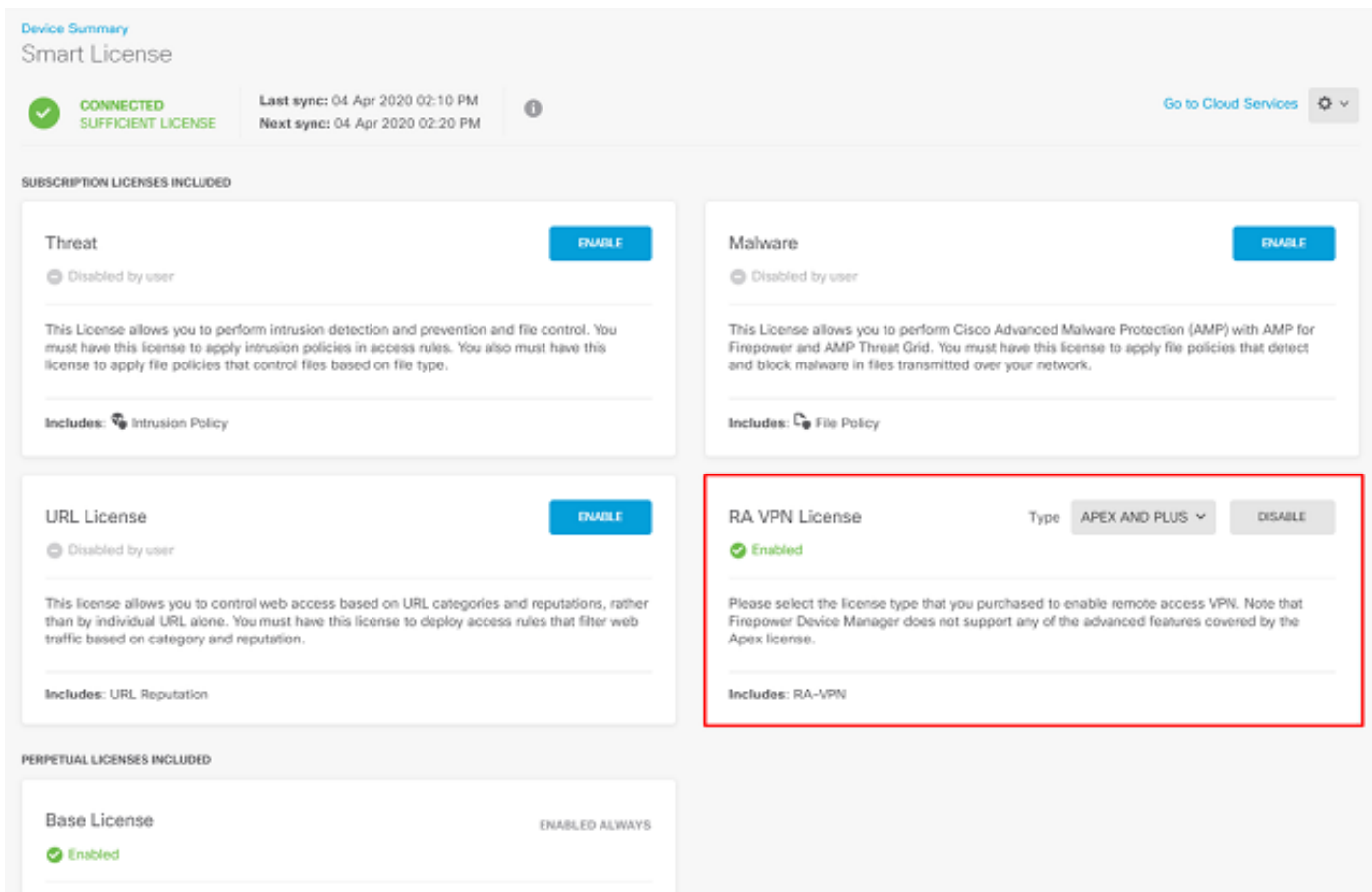


Verifica delle licenze sull'FTD

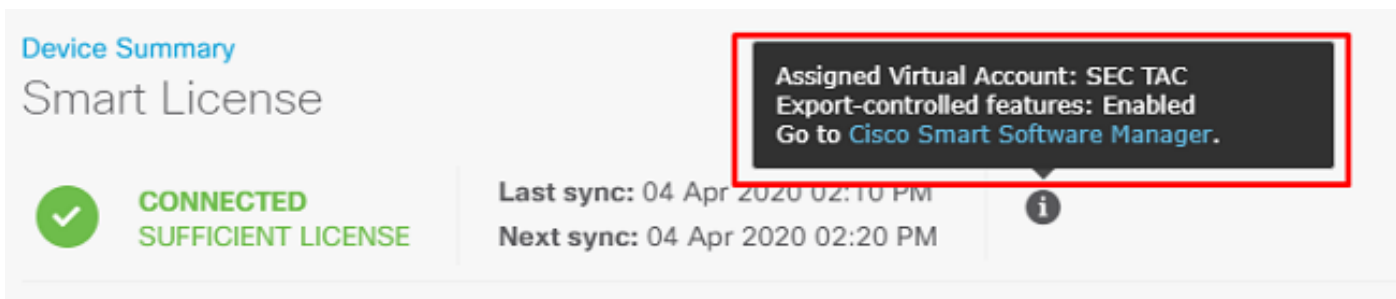
Passaggio 1. Verificare che il dispositivo sia registrato in Smart Licensing, come mostrato nell'immagine:

The screenshot displays the Cisco Firepower Device Manager interface for a device named 'firepower'. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main content area shows a network diagram with an 'Inside Network' connected to a 'Cisco Firepower Threat Defense for VMWa...' device. The device has interfaces 'o/0', 'o/1', and 'o/2' marked with green checkmarks, and a 'CONSOLE' port. To the right, an 'ISP/WAN/Gateway' is connected to an 'Internet' cloud, which includes services like 'DNS Server', 'NTP Server', and 'Smart License'. Below the diagram is a grid of configuration tiles. The 'Smart License' tile is highlighted with a red border and shows the status 'Registered' with a green checkmark. Other tiles include 'Interfaces' (Connected, Enabled 3 of 4), 'Routing' (no routes yet), 'Updates' (Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds), 'System Settings' (Management Access, Logging Settings, DHCP Server, DNS Server, Management Interface, Hostname, NTP, Cloud Services, Reboot/Shutdown, Traffic Settings, URL Filtering Preferences), 'Backup and Restore' (no files created yet), 'Troubleshoot' (no files created yet), 'Site-to-Site VPN' (no connections yet), 'Remote Access VPN' (requires RA VPN license, no connections), 'Advanced Configuration' (includes FlexConfig, Smart CLI), and 'Device Administration' (audit events, deployment history, download configuration).

Passaggio 2. Verificare che le licenze AnyConnect siano abilitate sul dispositivo, come mostrato nell'immagine.

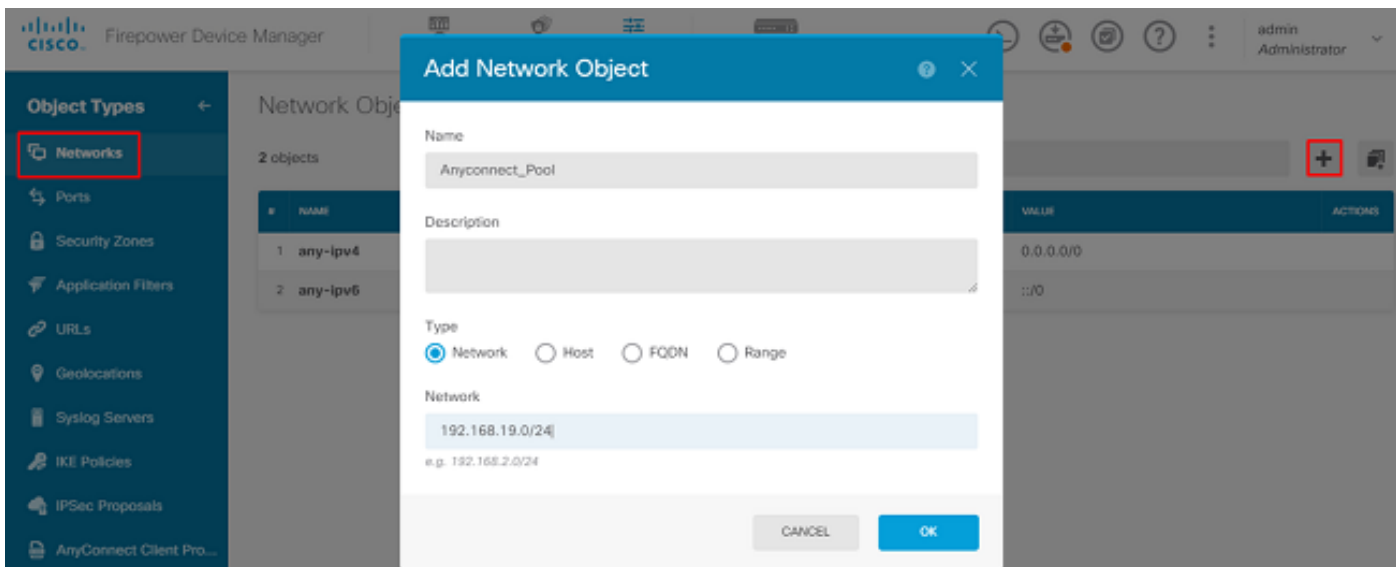


Passaggio 3. Verificare che le funzionalità controllate per l'esportazione siano abilitate nel token, come mostrato nell'immagine:

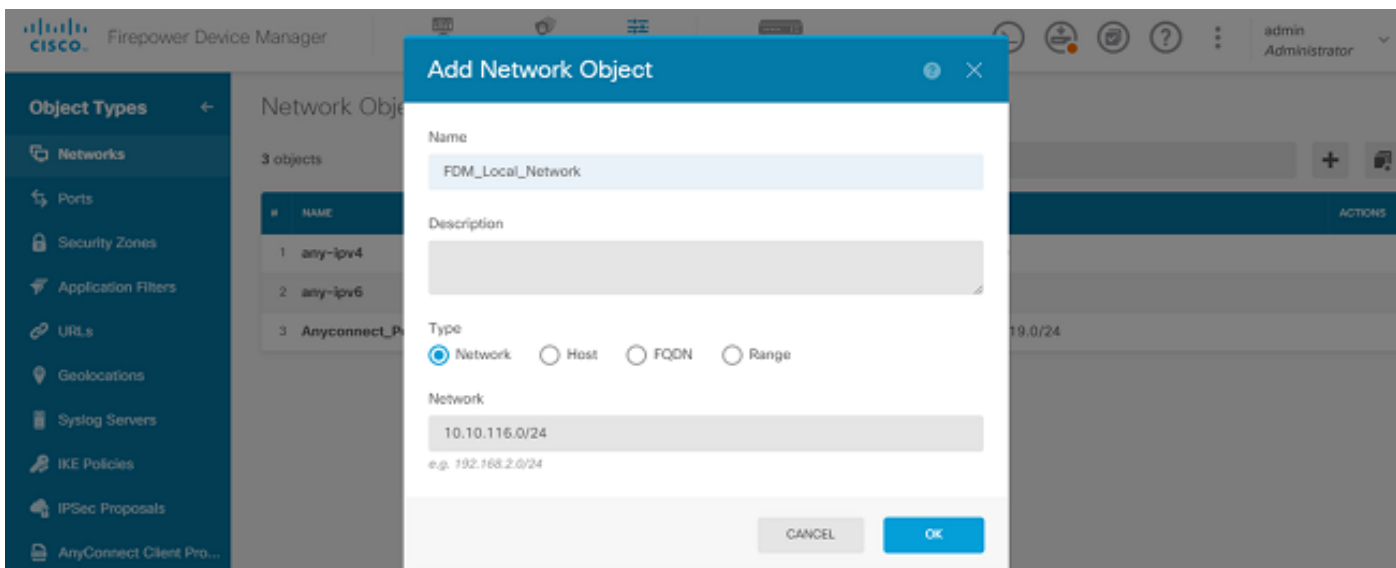


Definizione di reti protette

Passa a **Objects > Networks > Add new Network**. Configurare il pool VPN e le reti LAN dall'interfaccia utente di FDM. Creare un pool VPN da utilizzare per l'assegnazione dell'indirizzo locale agli utenti AnyConnect, come mostrato nell'immagine:

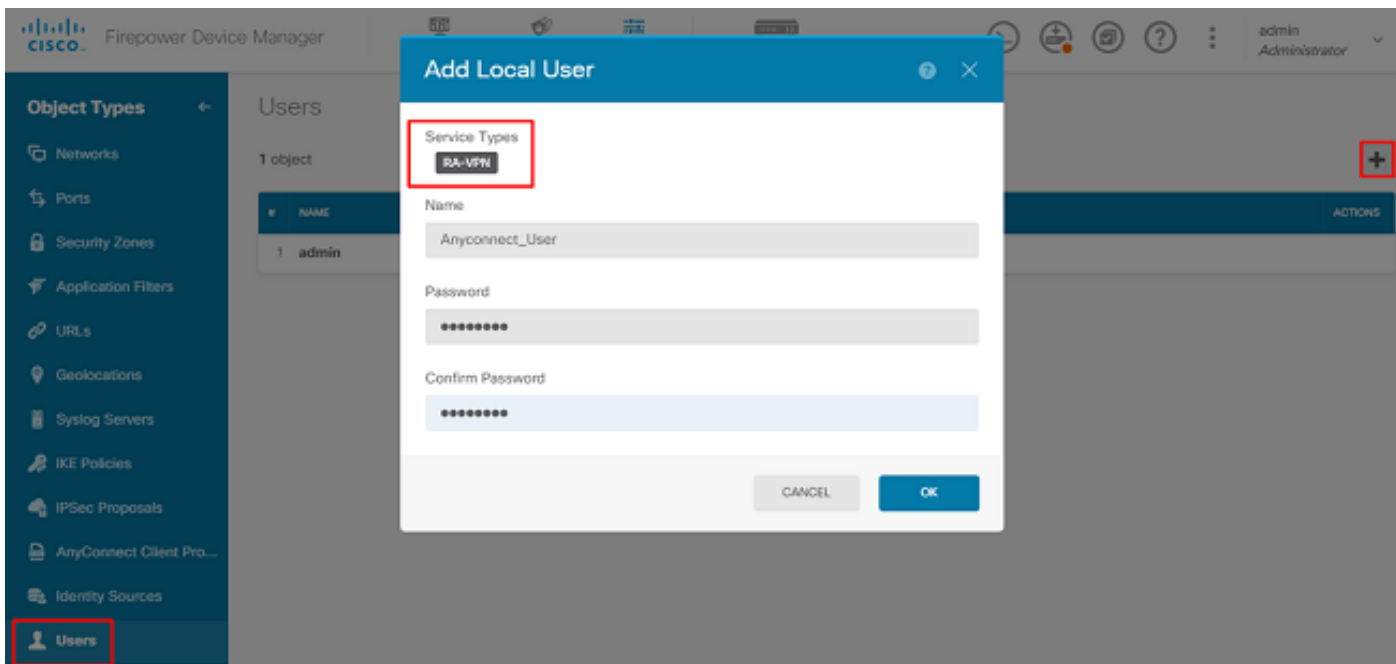


Creare un oggetto per la rete locale dietro il dispositivo FDM come mostrato nell'immagine:



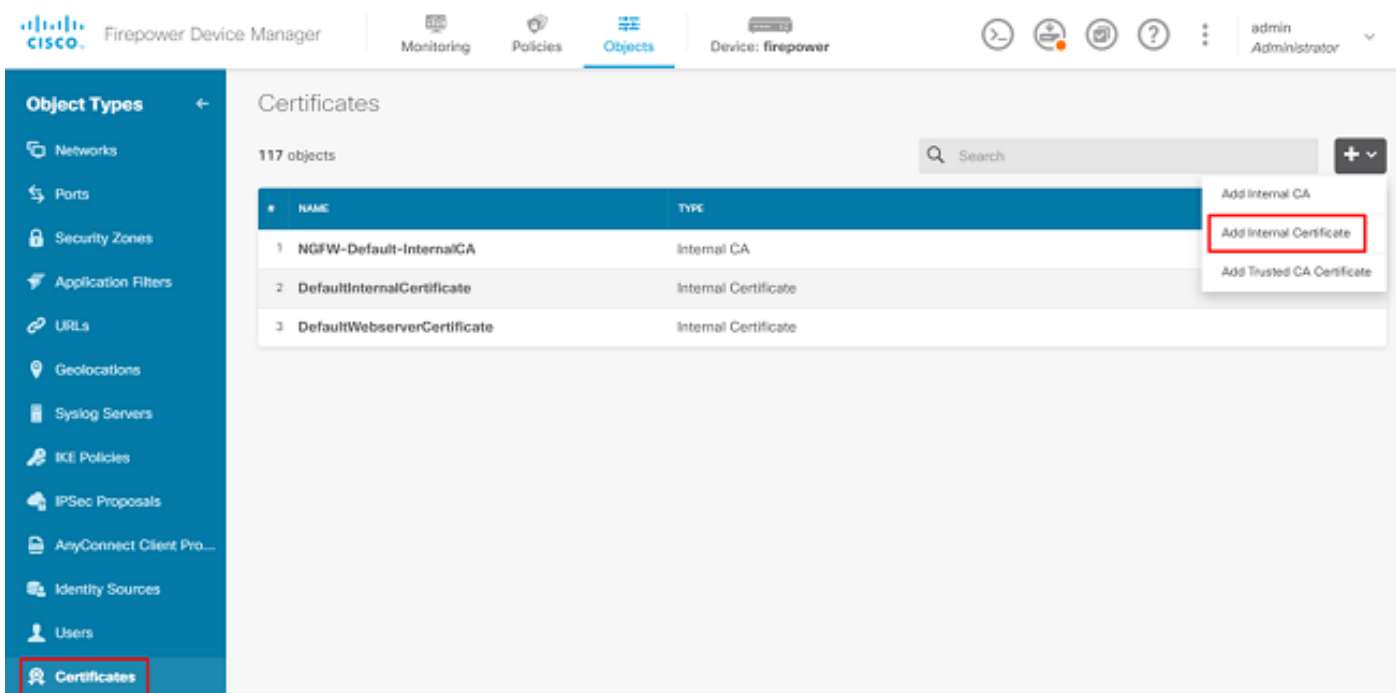
Crea utenti locali

Passa a **Objects > Users > Add User**. Aggiungere utenti locali VPN che si connettono a FTD tramite Anyconnect. Creare utenti locali come mostrato nell'immagine:



Aggiungi certificato

Passa a Objects > Certificates > Add Internal Certificate. Configurare un certificato come illustrato nell'immagine:



Caricare sia il certificato che la chiave privata, come mostrato nell'immagine:



Choose the type of internal certificate you want to create



Upload Certificate and Key

Create a certificate from existing files.
PEM and DER files are supported.



Self-Signed Certificate

Create a new certificate that is signed
by the device.

Il certificato e la chiave possono essere caricati tramite copia e incolla o il pulsante di caricamento per ciascun file, come mostrato nell'immagine:

Add Internal Certificate



Name

Anyconnect_Certificate

SERVER CERTIFICATE (USER AGENT)

Paste certificate, or choose file:

UPLOAD CERTIFICATE

The supported formats are: PEM, DER.

```
wkM7QqtRuyzBzGhnoSebJkP/Hiky/Q+r6UrYSnv++UJSrg777/9NgonwTpLI/8/J
idGSN0b/ic6iPh2aGpB1Lra3MGCL1pJaRqxq3+1yBDsfVFCaKT9wWcnUveQd6LZp
k+iaN+V24yOj3vCJILihtxwdllqeSs8F8XdaL4LQObcTfZ/3YNBWqvwV2TL
-----END CERTIFICATE-----
```

CERTIFICATE KEY

Paste key, or choose file:

UPLOAD KEY

The supported formats are: PEM, DER.

```
QzYPpjCgYEAqJ9nlk8sfPfmotyOwprlBEdwMMDeKLX3KDY58jviv1/8a/wsX+uz
3A7VQn6gA6ISWHgxHdmqYnD38P6kCuK/hQMUCqdIKUITXkh0ZpglQbfW2lJ0VD4M
gKugRI5t0Zva5j+bO5q0f8D/mtYYTBf8JGgqEfSju0Zsy2ifWtsbJrE=
-----END RSA PRIVATE KEY-----
```

CANCEL

OK

Configura VPN di accesso remoto

Passa a Remote Access VPN > Create Connection Profile. Navigare attraverso la Creazione guidata RMA VPN su FDM come mostrato nell'immagine:

Firepower Device Manager

Monitoring Policies Objects Device: firepower

Model Cisco Firepower Threat Defense for VMWa... Software 6.5.0-115 VDB 309.0 Rule Update 2019-08-12-001-vrt High Availability Not Configured CONFIGURE

Interfaces
Connected
Enabled 3 of 4
View All Interfaces

Smart License
Registered
View Configuration

Site-to-Site VPN
There are no connections yet
View Configuration

Remote Access VPN
Configured
No connections | 1 Group Policy
View Configuration

Routing
There are no routes yet
Create the first static route

Updates
Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds
View Configuration

Troubleshoot
No files created yet
REQUEST FILE TO BE CREATED

Advanced Configuration
Includes: FlexConfig, Smart CLI
View Configuration

System Settings
Management Access
Logging Settings
DHCP Server
DNS Server
Management Interface
Hostname
NTP
Cloud Services
Reboot/Shutdown
Traffic Settings
URL Filtering Preferences

Device Administration
Audit Events, Deployment History, Download Configuration
View Configuration

Firepower Device Manager

Monitoring Policies Objects Device: firepower

RA VPN

Connection Profiles

Group Policies

Device Summary
Remote Access VPN Connection Profiles

Search

+	NAME	AAA	GROUP POLICY	ACTIONS
There are no Remote Access Connections yet. Start by creating the first Connection.				

CREATE CONNECTION PROFILE

Creare un profilo di connessione e avviare la configurazione come mostrato nell'immagine:

Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

Connection Profile Name

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

Anyconnect

Group Alias

Anyconnect

[Add Group Alias](#)

Group URL

[Add Group URL](#)

Scegliere i metodi di autenticazione come illustrato nell'immagine. In questa guida viene utilizzata l'autenticazione locale.

Primary Identity Source

Authentication Type

AAA Only Client Certificate Only AAA and Client Certificate

Primary Identity Source for User Authentication

LocalIdentitySource

Fallback Local Identity Source

Please Select Local Identity Source

Strip Identity Source server from username

Strip Group from Username

Secondary Identity Source

Secondary Identity Source for User Authentication

Please Select Identity Source

Advanced

Authorization Server

Please select

Accounting Server

Please select

Scegliere il Anyconnect_Pool come mostrato nell'immagine:

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool



Anyconnect_Pool

IPv6 Address Pool

Endpoints are provided an address from this pool



DHCP Servers



CANCEL

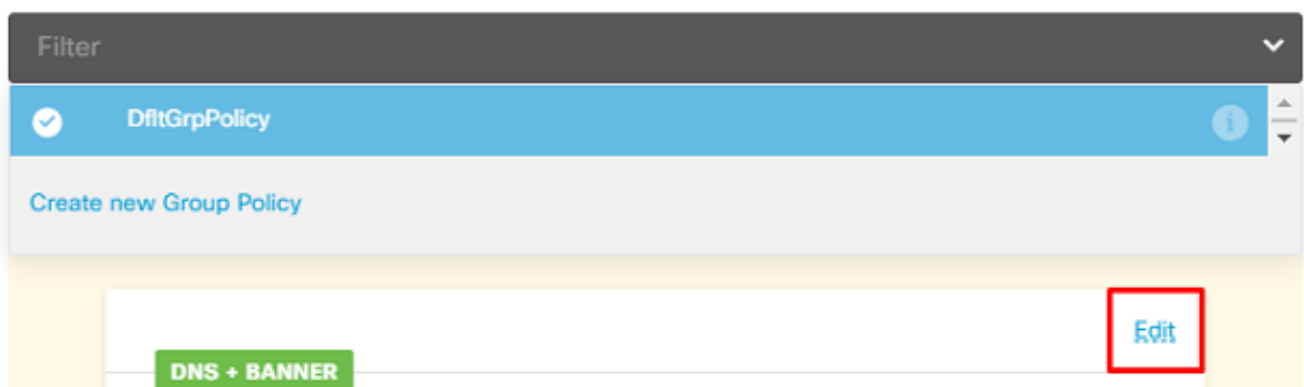
NEXT

Nella pagina successiva verrà visualizzato un riepilogo dei Criteri di gruppo predefiniti. È possibile creare un nuovo criterio di gruppo quando si preme l'elenco a discesa e si sceglie l'opzione per Create a new Group Policy. In questa guida viene utilizzato il criterio di gruppo predefinito. Scegliere l'opzione di modifica nella parte superiore del criterio, come mostrato nell'immagine:

Remote User Experience

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.

View Group Policy



Nei Criteri di gruppo, aggiungere il tunneling suddiviso in modo che gli utenti connessi a Anyconnect inviino solo il traffico destinato alla rete FTD interna sul client Anyconnect, mentre tutto il resto del traffico esce dalla connessione ISP dell'utente, come mostrato nell'immagine:

Corporate Resources (Split Tunneling)

IPv4 Split Tunneling

Allow specified traffic over tunnel



IPv6 Split Tunneling

Allow all traffic over tunnel



IPv4 Split Tunneling Networks



FDM_Local_Network

Nella pagina successiva scegliere il pulsante `Anyconnect_Certificate` aggiunto nella sezione certificato. Quindi, scegliere l'interfaccia su cui l'FTD resta in ascolto delle connessioni AnyConnect. Scegliere il criterio Ignora controllo di accesso per il traffico decrittografato (`sysopt permit-vpn`). Si tratta di un comando facoltativo se `sysopt permit-vpn` non è stato scelto. È necessario creare un criterio di controllo dell'accesso che consenta al traffico proveniente dai client Anyconnect di accedere alla rete interna, come mostrato nell'immagine:

Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity

Anyconnect_Certificate



Outside Interface

outside (GigabitEthernet0/0)



Fully-qualified Domain Name for the Outside Interface

e.g. `ravpn.example.com`

Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic



Bypass Access Control policy for decrypted traffic (`sysopt permit-vpn`)

L'esenzione NAT può essere configurata manualmente in `Policies > NAT` oppure può essere configurato automaticamente dalla procedura guidata. Scegli l'interfaccia interna e le reti di cui hanno bisogno i client Anyconnect per accedere, come mostrato nell'immagine.

NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside (GigabitEthernet0/1)

Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



FDM_Local_Network

Scegliere il pacchetto Anyconnect per ciascun sistema operativo (Windows/Mac/Linux) a cui gli utenti possono connettersi, come mostrato nell'immagine.

AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from software.cisco.com. You must have the necessary AnyConnect software license.

Packages

UPLOAD PACKAGE

Windows: anyconnect-win-4.7.04056-webdeploy-k9.pkg

BACK

NEXT

L'ultima pagina fornisce un riepilogo dell'intera configurazione. Verificare che siano stati impostati i parametri corretti, fare clic sul pulsante Fine e distribuire la nuova configurazione.

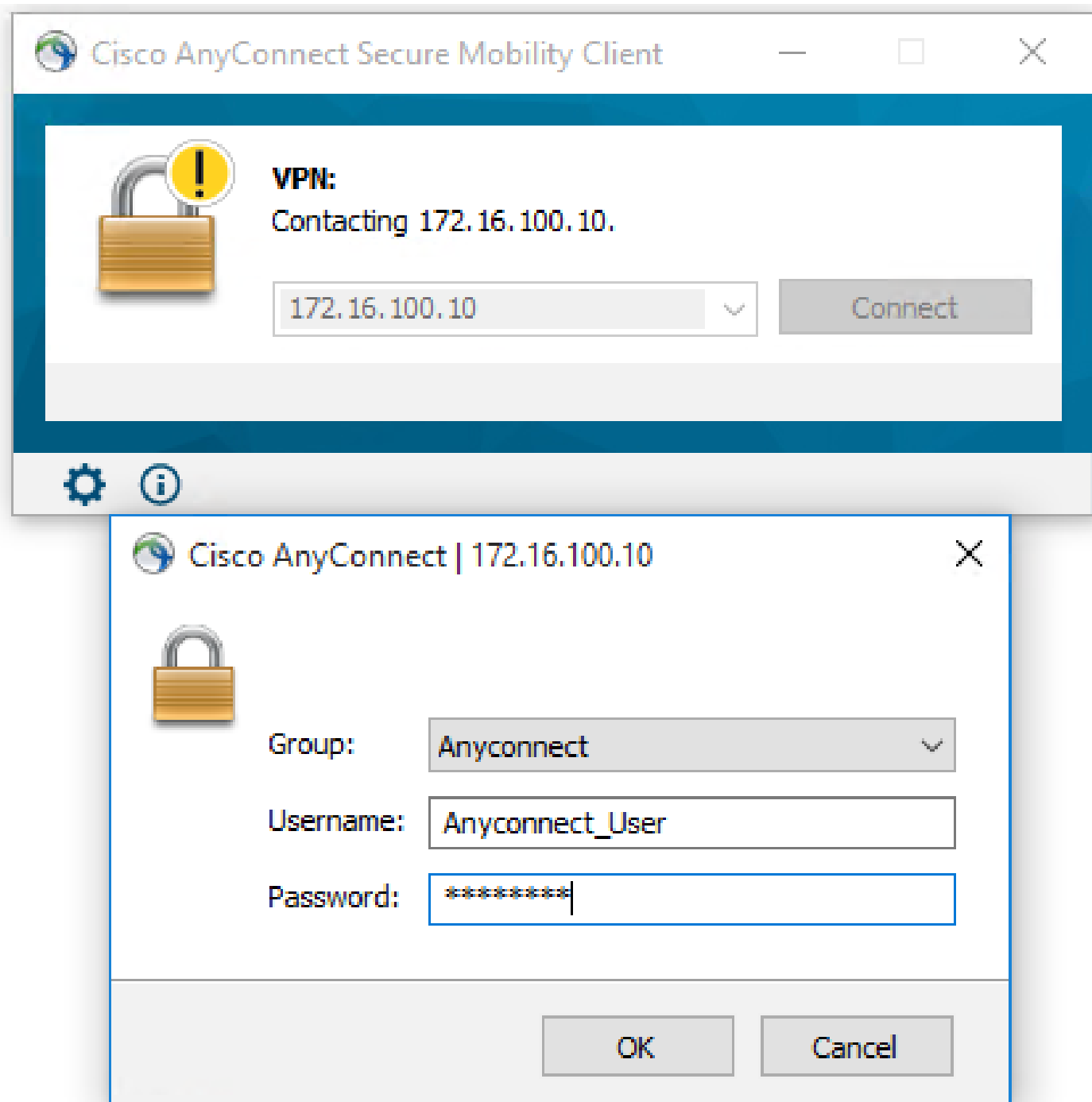
Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

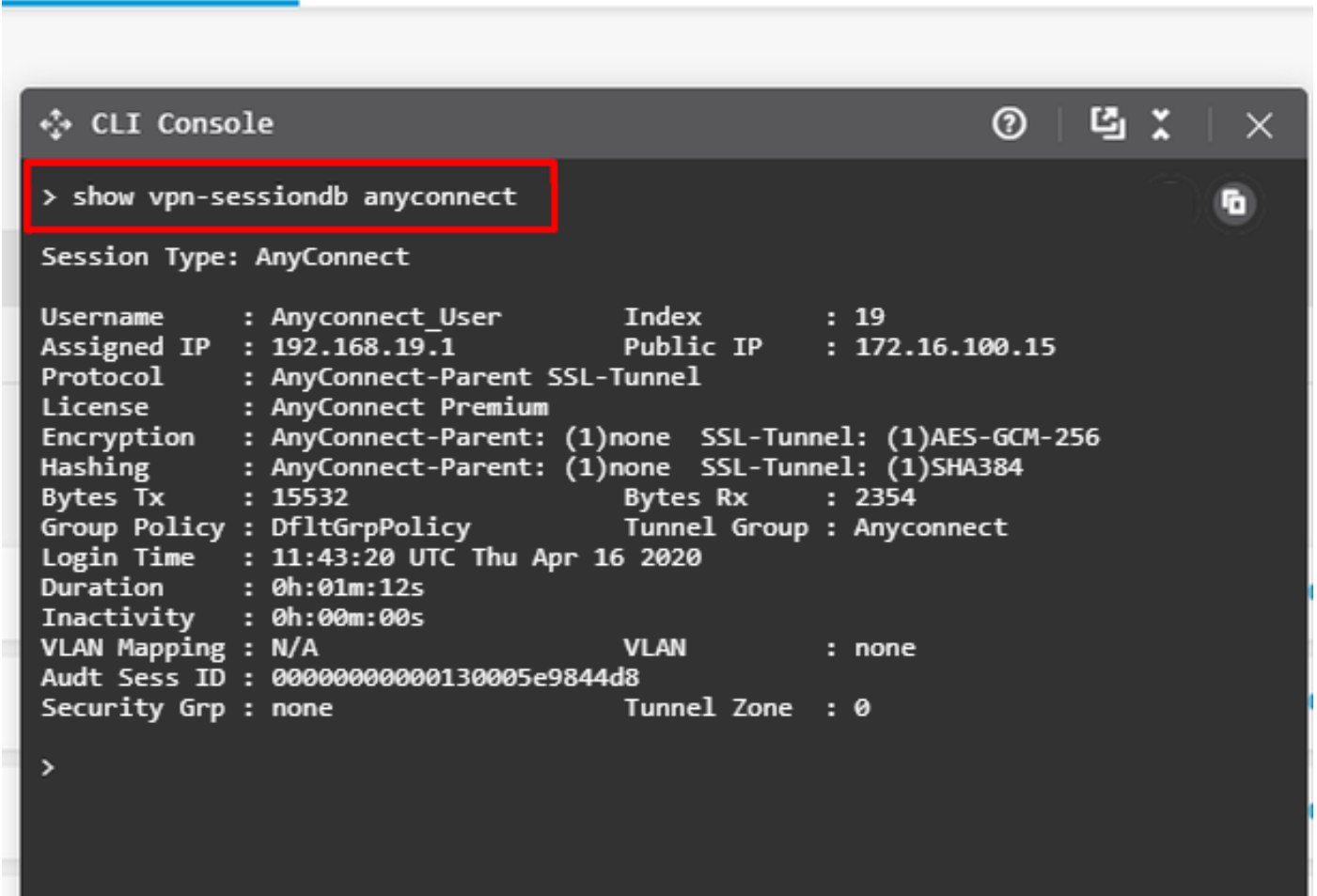
Una volta distribuita la configurazione, tentare la connessione. Se si dispone di un FQDN che si risolve nell'IP esterno dell'FTD, immetterlo nella casella della connessione Anyconnect.

Nell'esempio, viene usato l'indirizzo IP esterno dell'FTD. Utilizzare il nome utente e la password

creati nella sezione relativa agli oggetti di FDM, come illustrato nell'immagine.



A partire dalla versione FDM 6.5.0, non è possibile monitorare gli utenti Anyconnect tramite l'interfaccia utente di FDM. L'unica opzione è monitorare gli utenti Anyconnect dalla CLI. È possibile utilizzare la console CLI della GUI di FDM anche per verificare che gli utenti siano connessi. Utilizzare questo comando, `Show vpn-sessiondb anyconnect`.



lo stesso comando può essere eseguito direttamente dalla CLI.

```
> show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username      : Anyconnect_User      Index      : 15
Assigned IP   : 192.168.19.1          Public IP  : 172.16.100.15
Protocol      : AnyConnect-Parent SSL-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx      : 38830                Bytes Rx   : 172
Group Policy  : DfltGrpPolicy        Tunnel Group : Anyconnect
Login Time    : 01:08:10 UTC Thu Apr 9 2020
Duration      : 0h:00m:53s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                 VLAN       : none
Audt Sess ID  : 000000000000f0005e8e757a
Security Grp  : none                 Tunnel Zone : 0
```


Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Se un utente non è in grado di connettersi all'FTD con SSL, eseguire la procedura seguente per isolare i problemi di negoziazione SSL:

1. Verificare che sia possibile eseguire il ping dell'indirizzo IP esterno a FTD tramite il computer dell'utente.
2. Utilizzare uno sniffer esterno per verificare se l'handshake a tre vie TCP ha esito positivo.

Problemi del client AnyConnect

In questa sezione vengono fornite linee guida per la risoluzione dei due problemi più comuni dei client VPN AnyConnect. Una guida alla risoluzione dei problemi per il client AnyConnect è disponibile qui: [Guida alla risoluzione dei problemi dei client VPN AnyConnect](#).

Problemi iniziali di connettività

Se un utente ha problemi di connettività iniziali, abilitare il debug `webvpn` AnyConnect sull'FTD e analizzare i messaggi di debug. I debug devono essere eseguiti sulla CLI dell'FTD. Utilizzare il comando `debug webvpn anyconnect 255`.

Raccogliere un bundle DART dal computer client per ottenere i log da AnyConnect. Le istruzioni su come raccogliere un bundle DART sono disponibili qui: [Raccolta dei bundle DART](#).

Problemi specifici del traffico

Se la connessione ha esito positivo ma il traffico sul tunnel VPN SSL ha esito negativo, esaminare le statistiche sul traffico sul client per verificare che il traffico venga ricevuto e trasmesso dal client. Le statistiche dettagliate sui client sono disponibili in tutte le versioni di AnyConnect. Se il client mostra che il traffico è in fase di invio e ricezione, controllare l'FTD per il traffico ricevuto e trasmesso. Se il FTD applica un filtro, il nome del filtro viene visualizzato ed è possibile controllare le voci dell'ACL per controllare se il traffico viene scartato. Di seguito sono riportati i problemi più comuni che gli utenti riscontrano nel traffico:

- Problemi di routing dietro l'FTD - la rete interna non è in grado di indirizzare i pacchetti indietro agli indirizzi IP e ai client VPN assegnati
- Access Control List che bloccano il traffico
- Non è possibile ignorare Network Address Translation per il traffico VPN

Per ulteriori informazioni sulle VPN ad accesso remoto sull'FTD gestito da FDM, consultare la guida alla configurazione completa qui: [FTD ad accesso remoto gestito da FDM](#).

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).