Configura VPN ad accesso remoto su FTD Gestito da FDM

Sommario

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.

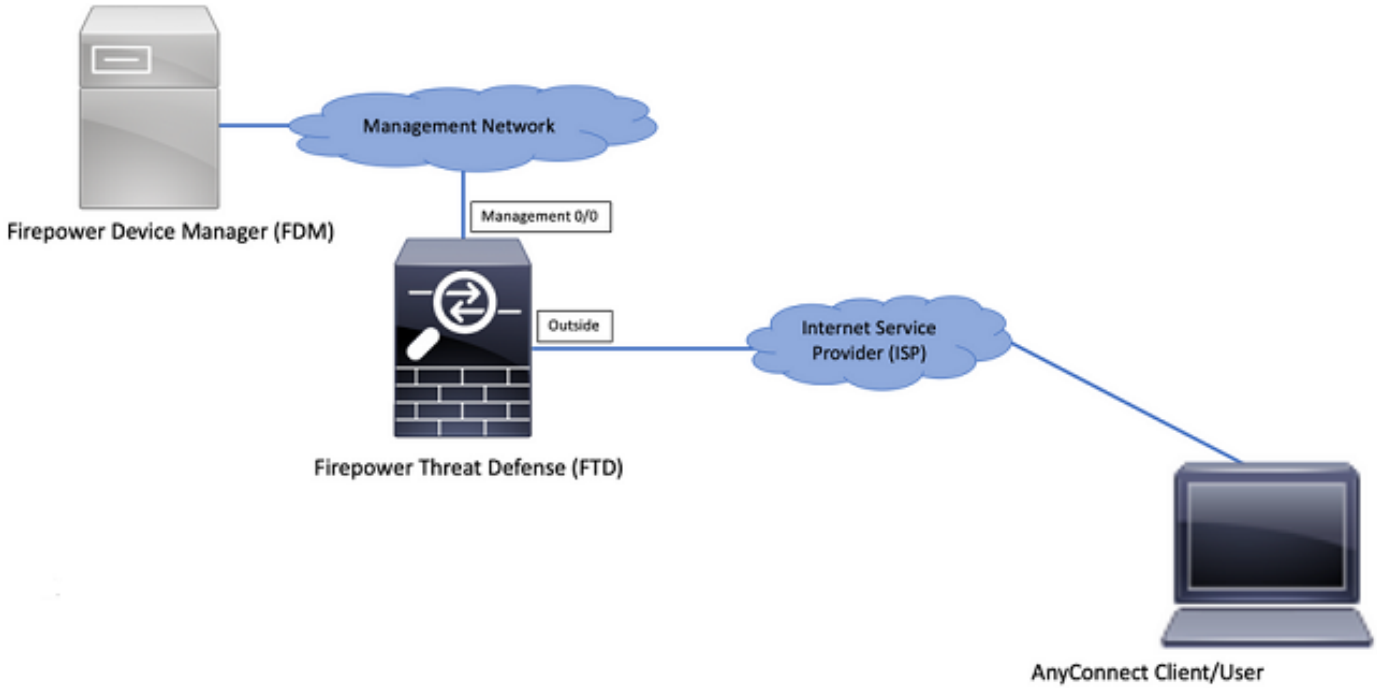
Premesse

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 archiviata per questo problema.

Configurazione

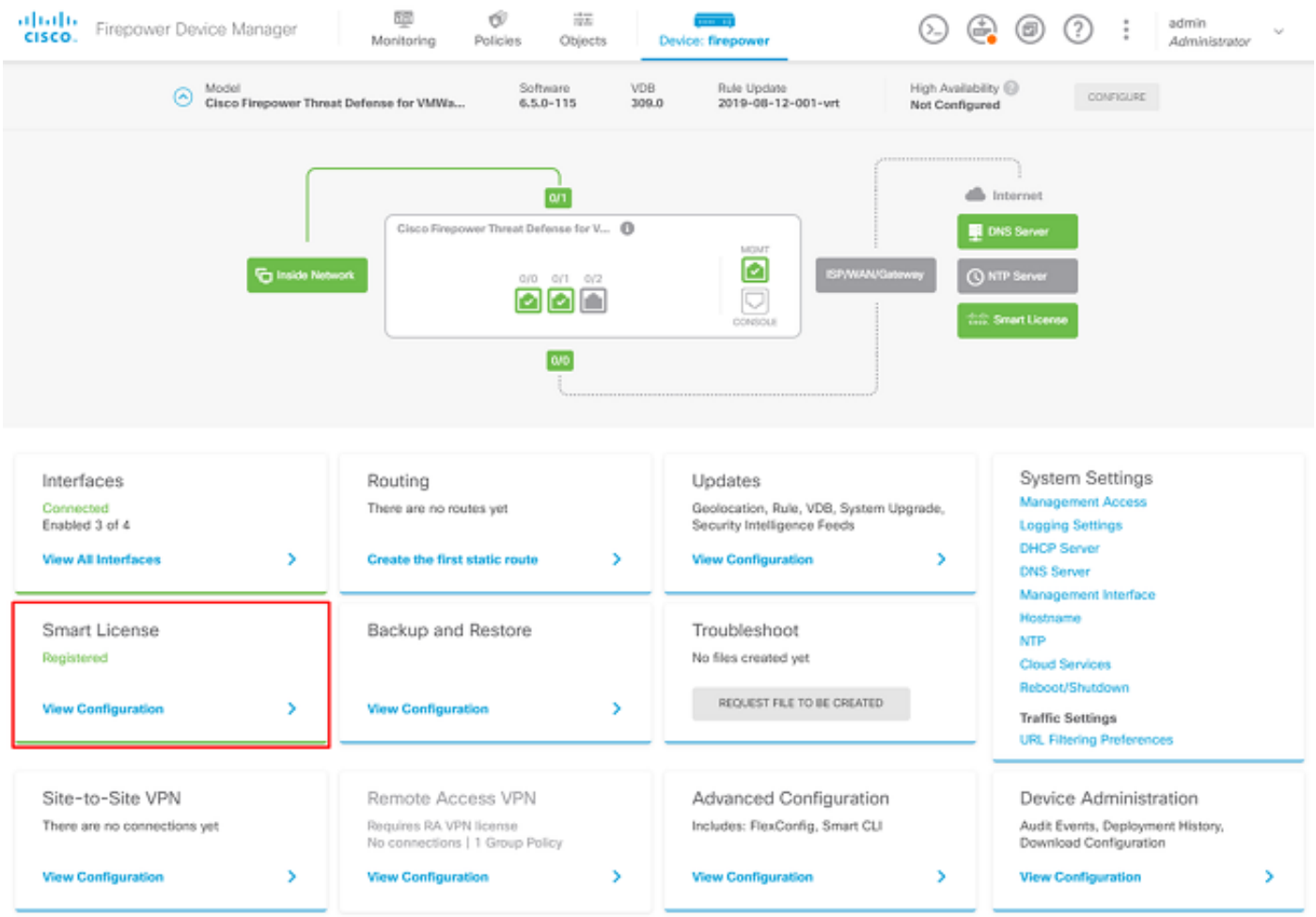
Esempio di rete

Autenticazione del client AnyConnect con l'uso di Local.

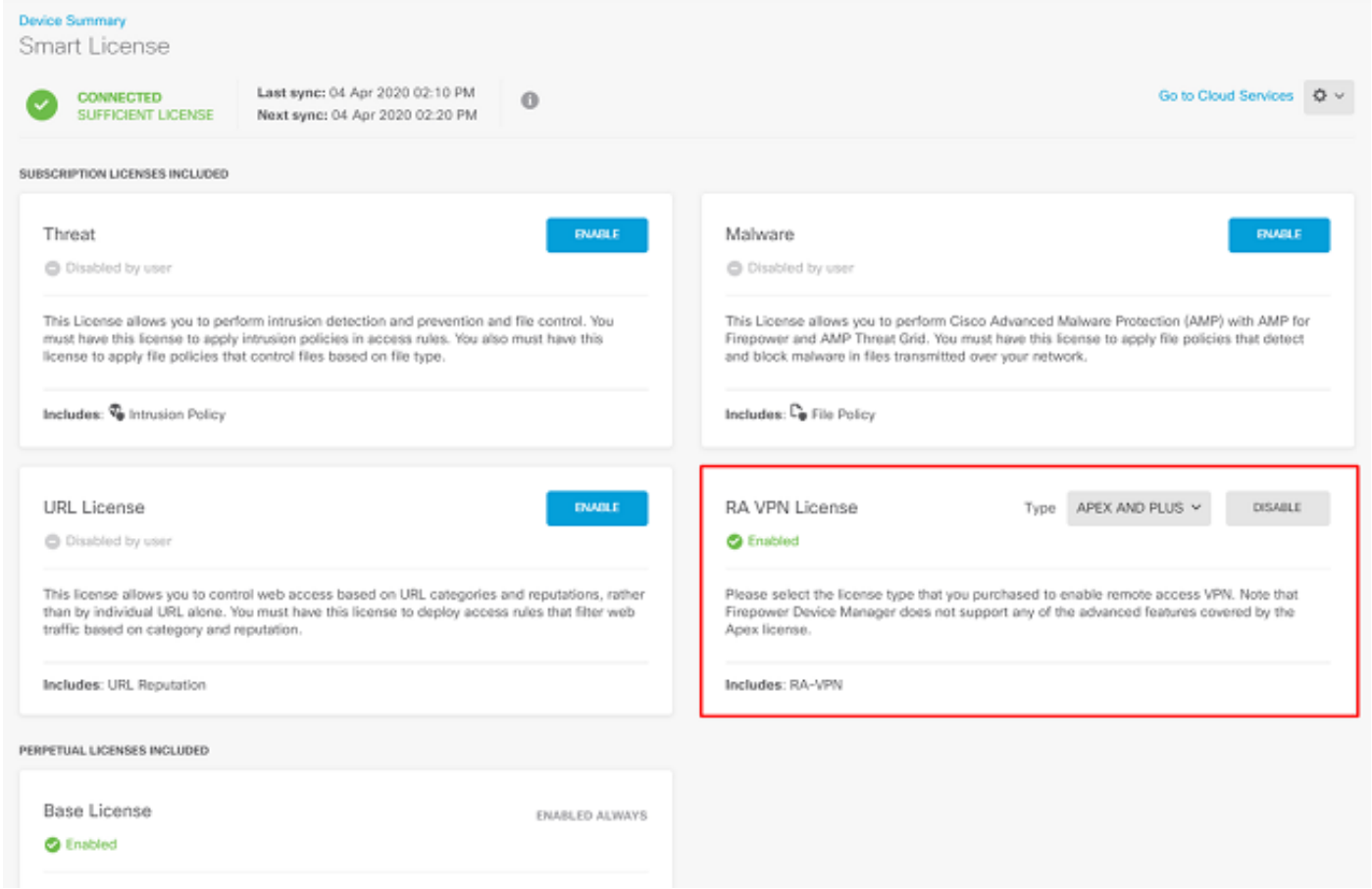


Verifica delle licenze sull'FTD

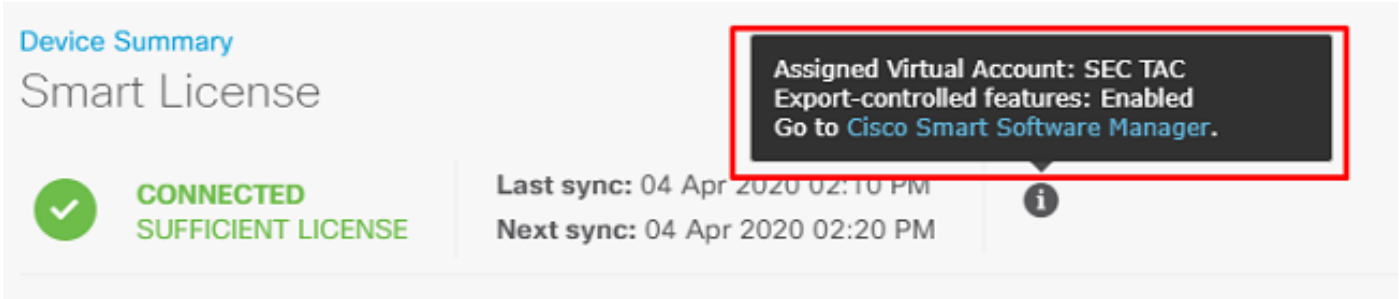
Passaggio 1. Verificare che il dispositivo sia registrato in Smart Licensing, come mostrato nell'immagine:



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

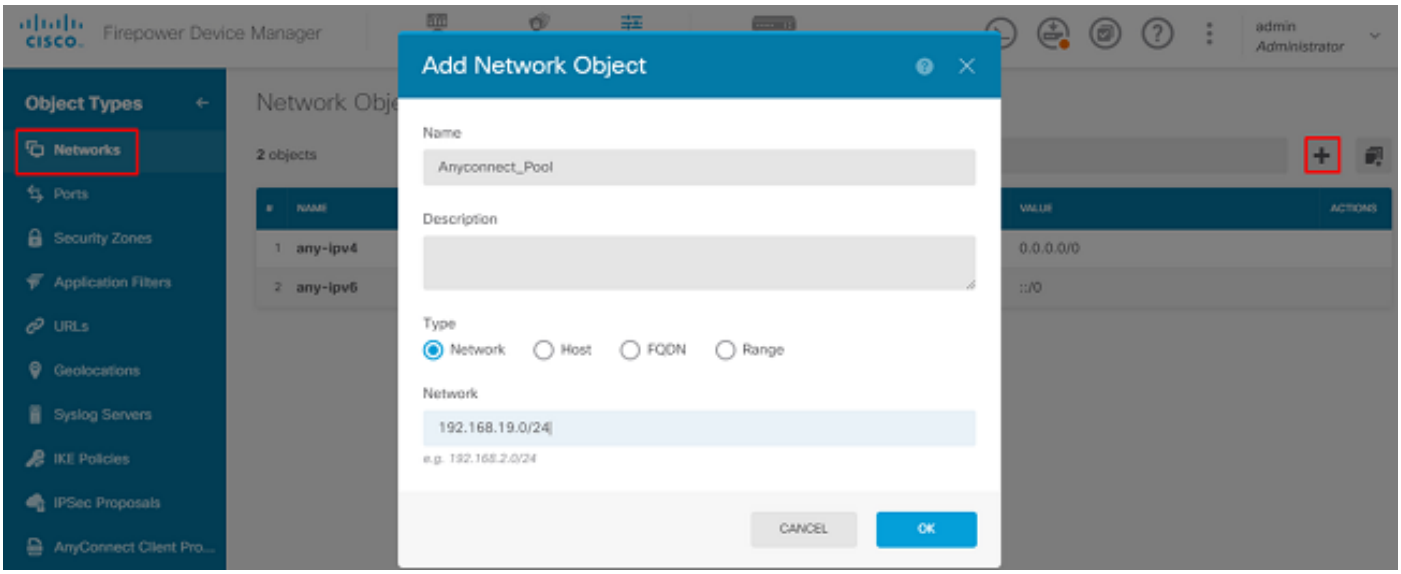


Passaggio 3. Verificare che le funzionalità controllate per l'esportazione siano abilitate nel token, come mostrato nell'immagine:

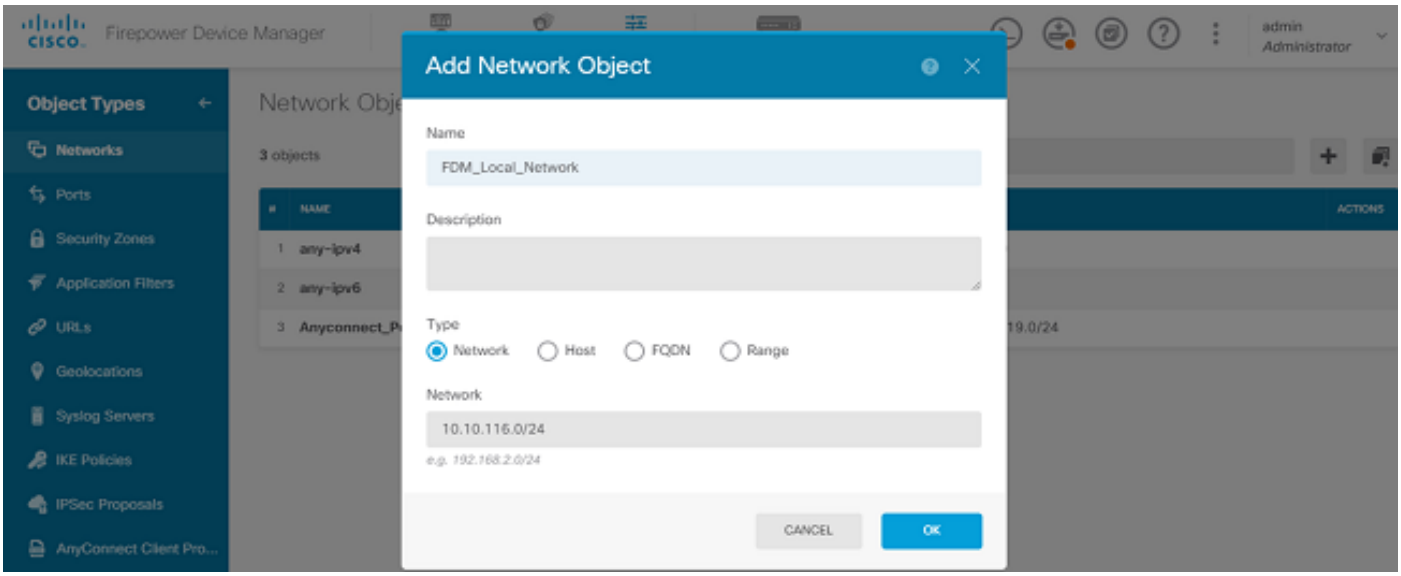


Definizione di reti protette

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:

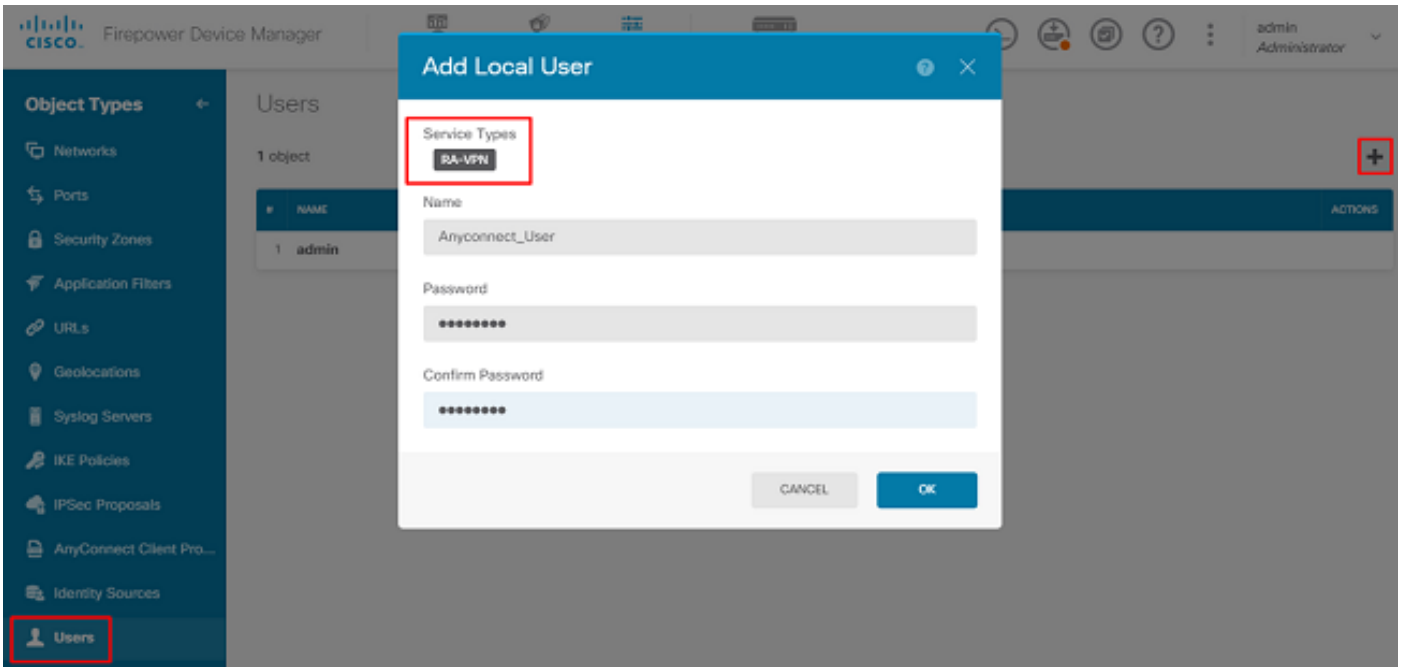


Creare un oggetto per la rete locale dietro il dispositivo FDM come mostrato nell'immagine:



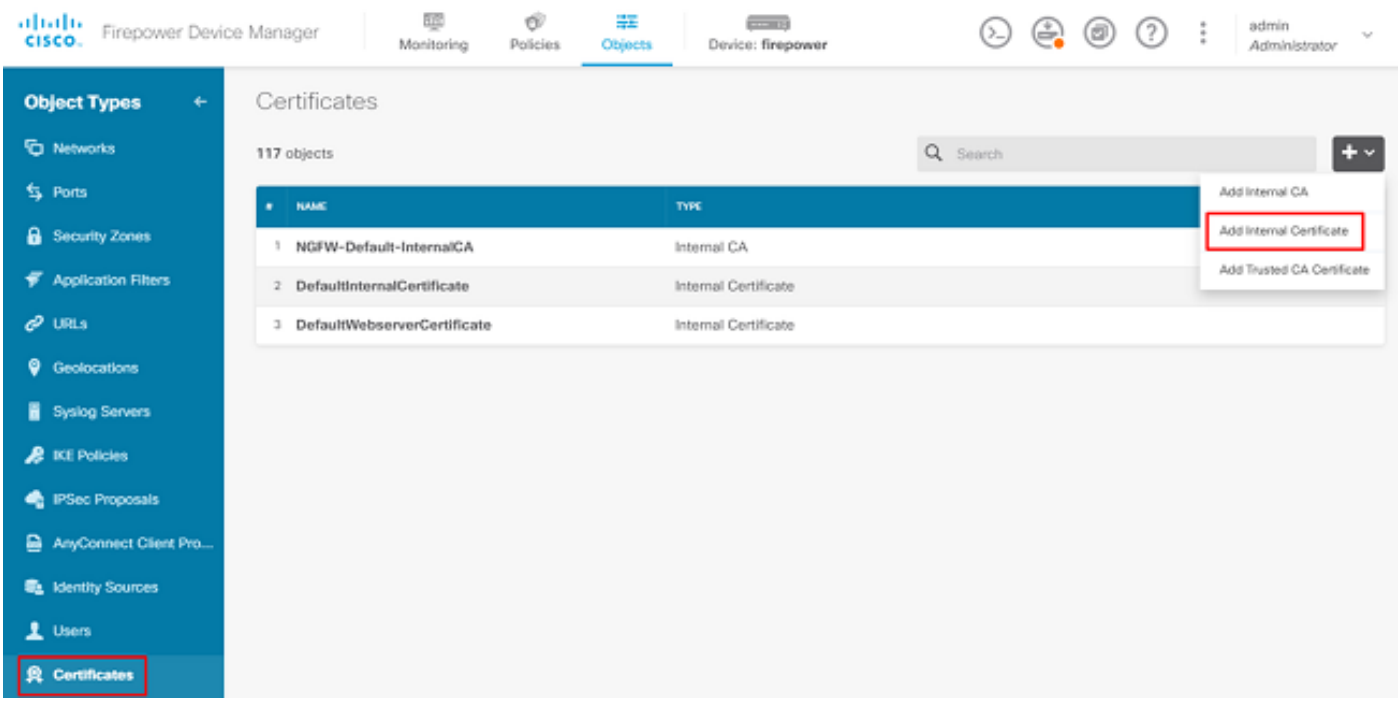
Crea utenti locali

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

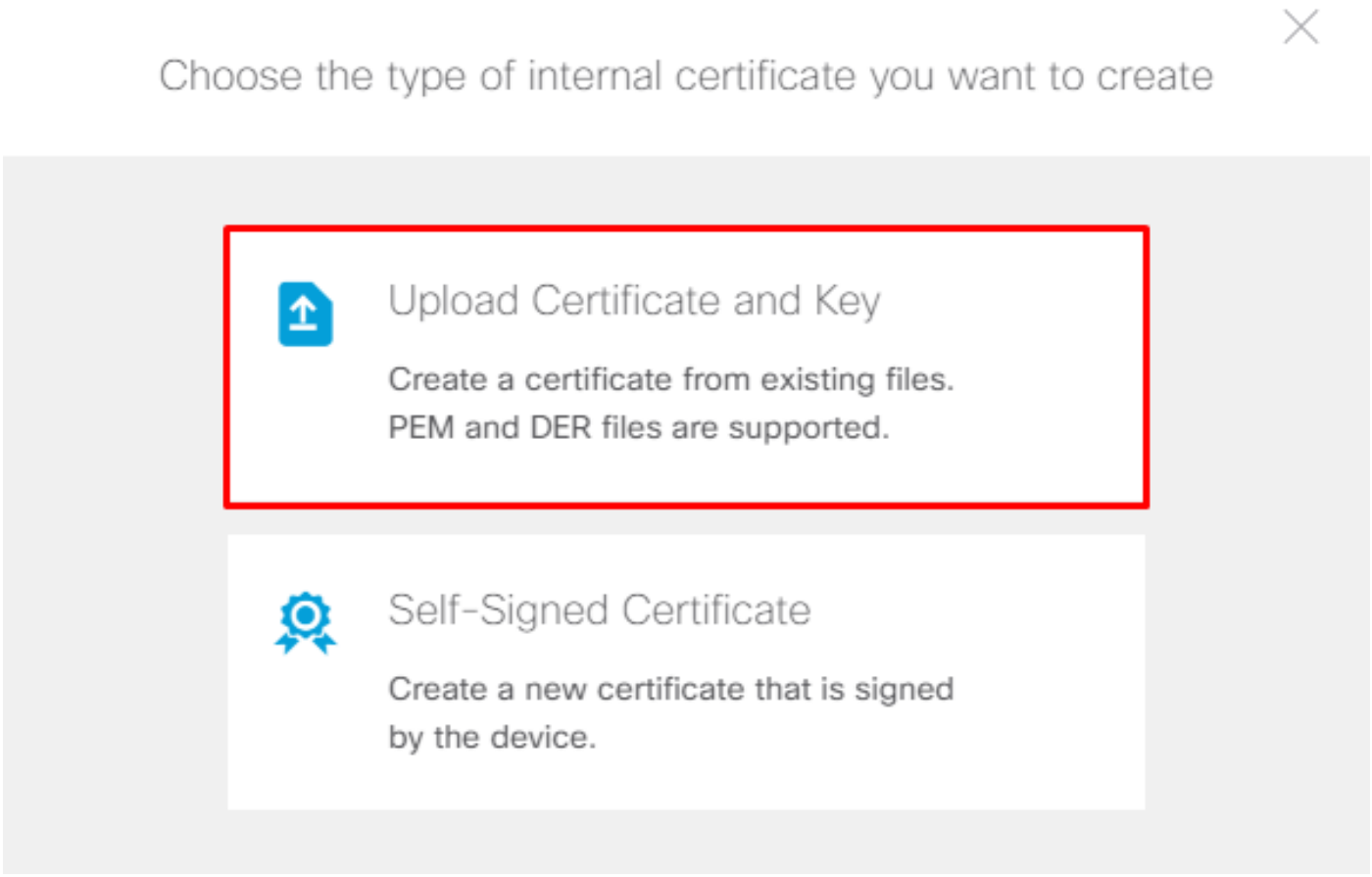


Aggiungi certificato

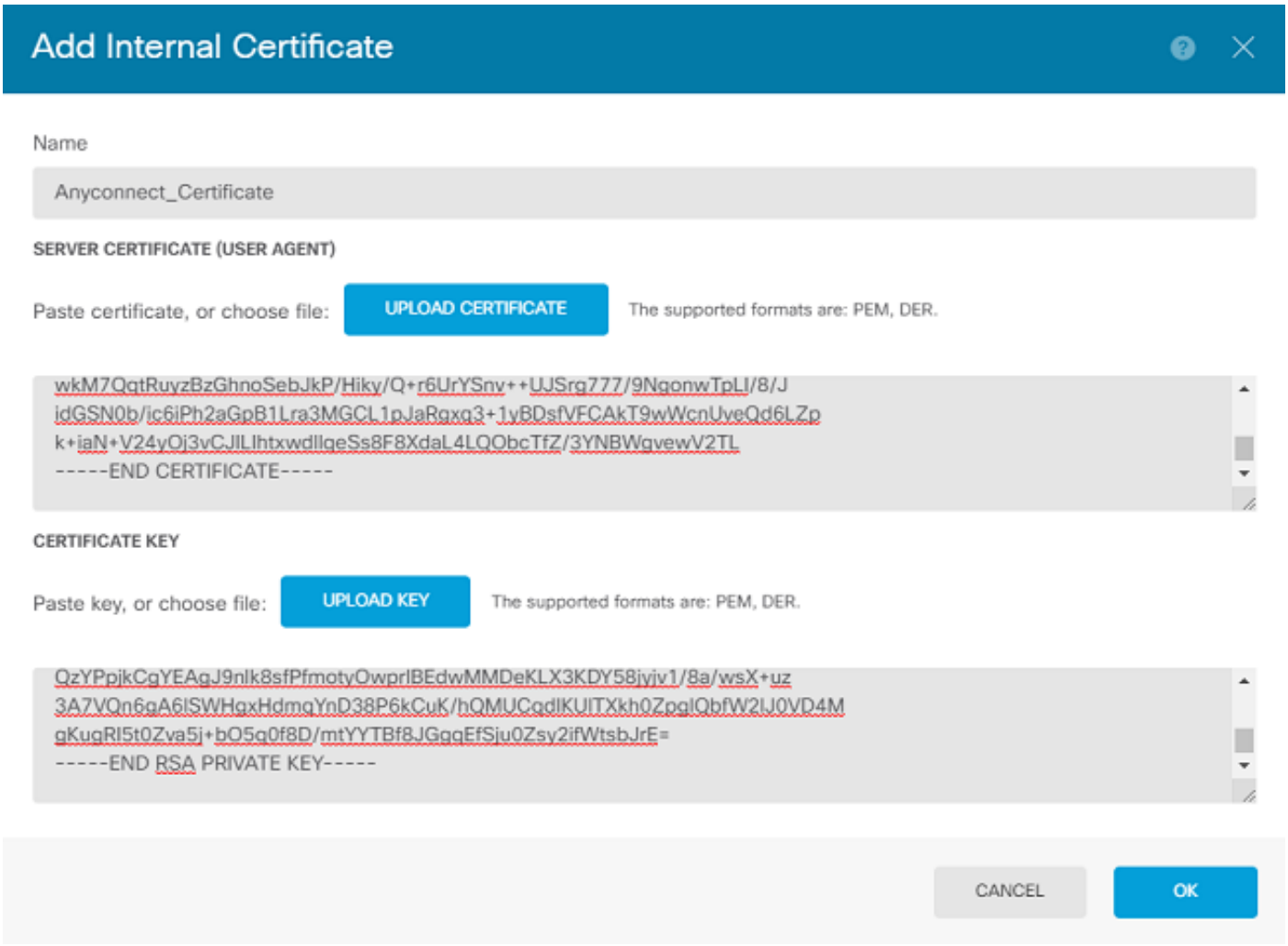
Passa a Objects > Certificates > Add Internal Certificate. Configurare un certificato come illustrato nell'immagine:



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

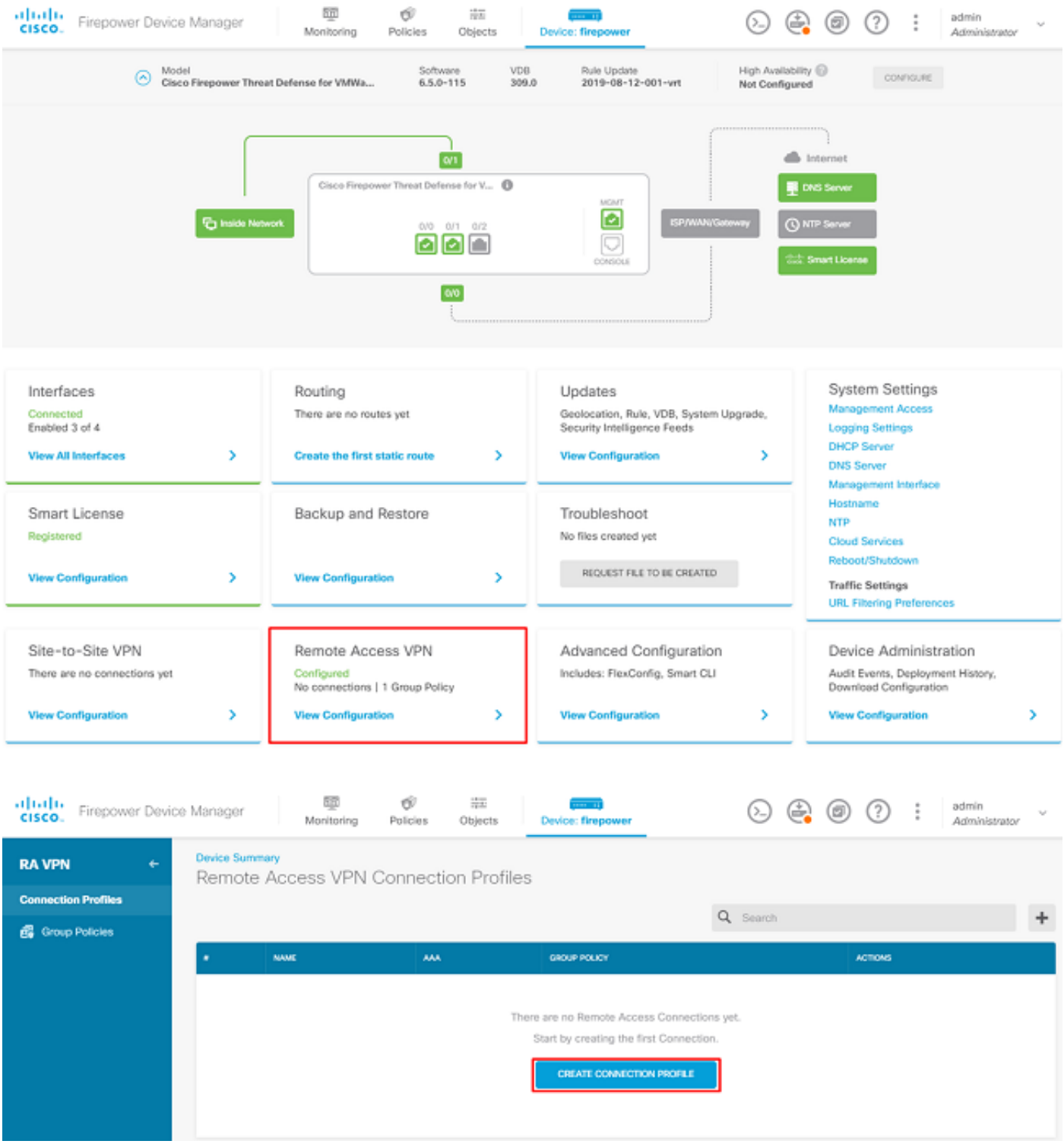


Il certificato e la chiave possono essere caricati tramite copia e incolla o il pulsante di caricamento per ciascun file, come mostrato nell'immagine:

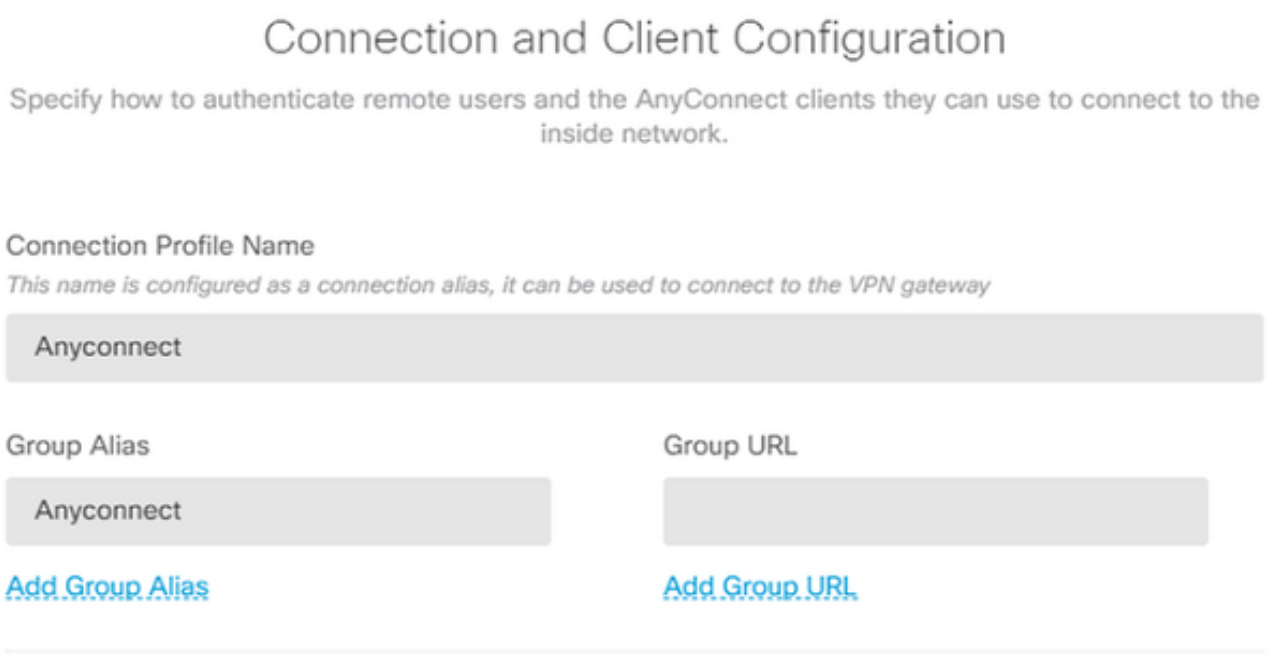


Configura VPN di accesso remoto

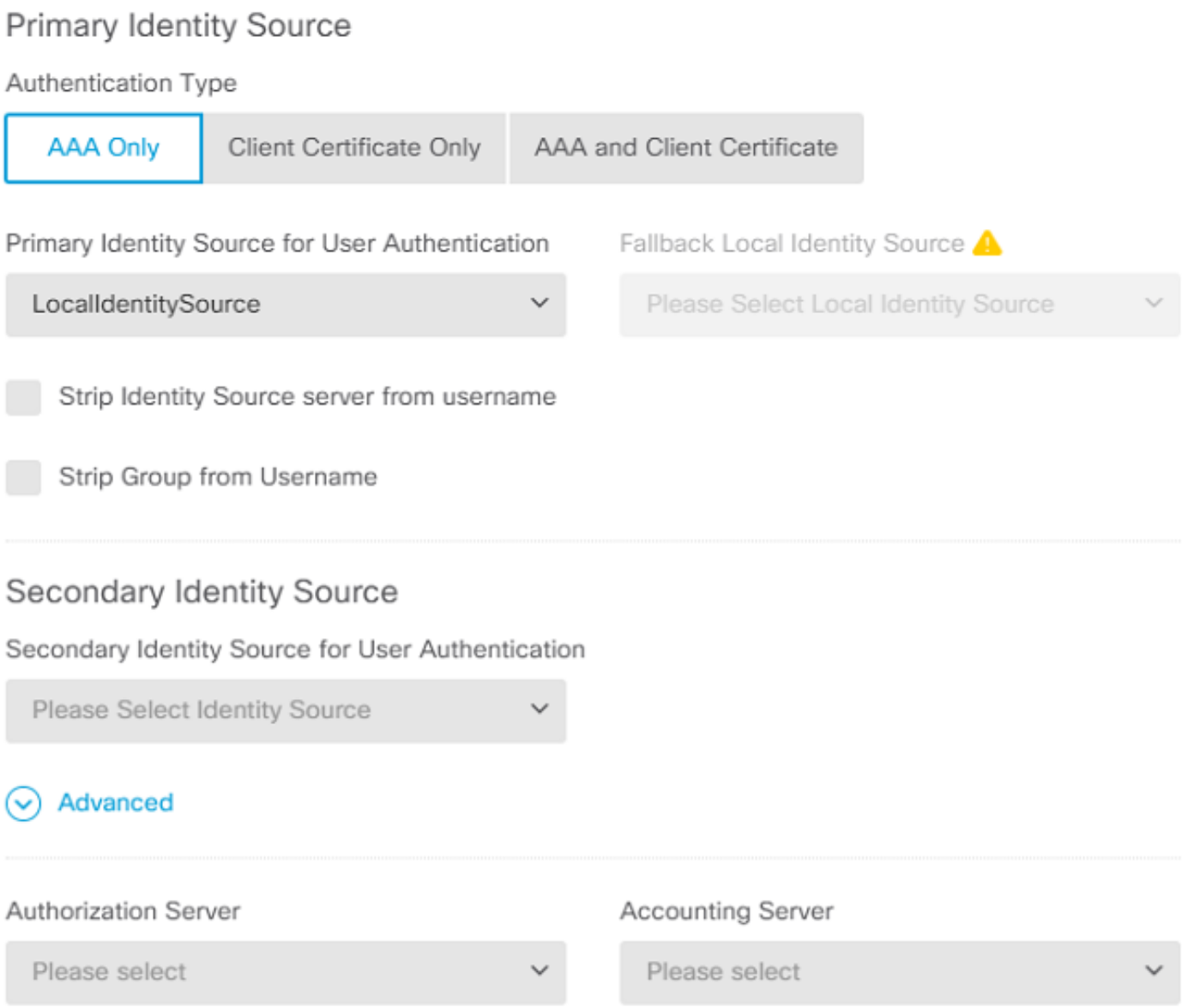
Passa a Remote Access VPN > Create Connection Profile. Navigare attraverso la Creazione guidata RMA VPN su FDM come mostrato nell'immagine:



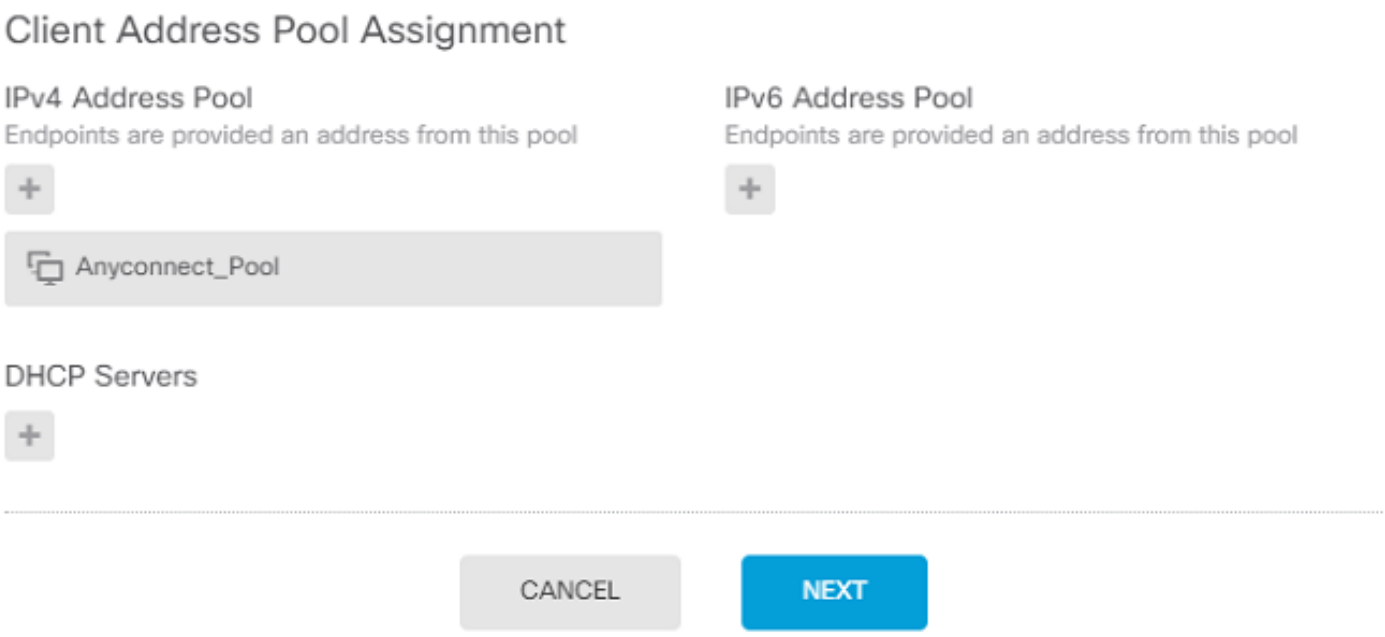
Creare un profilo di connessione e avviare la configurazione come mostrato nell'immagine:



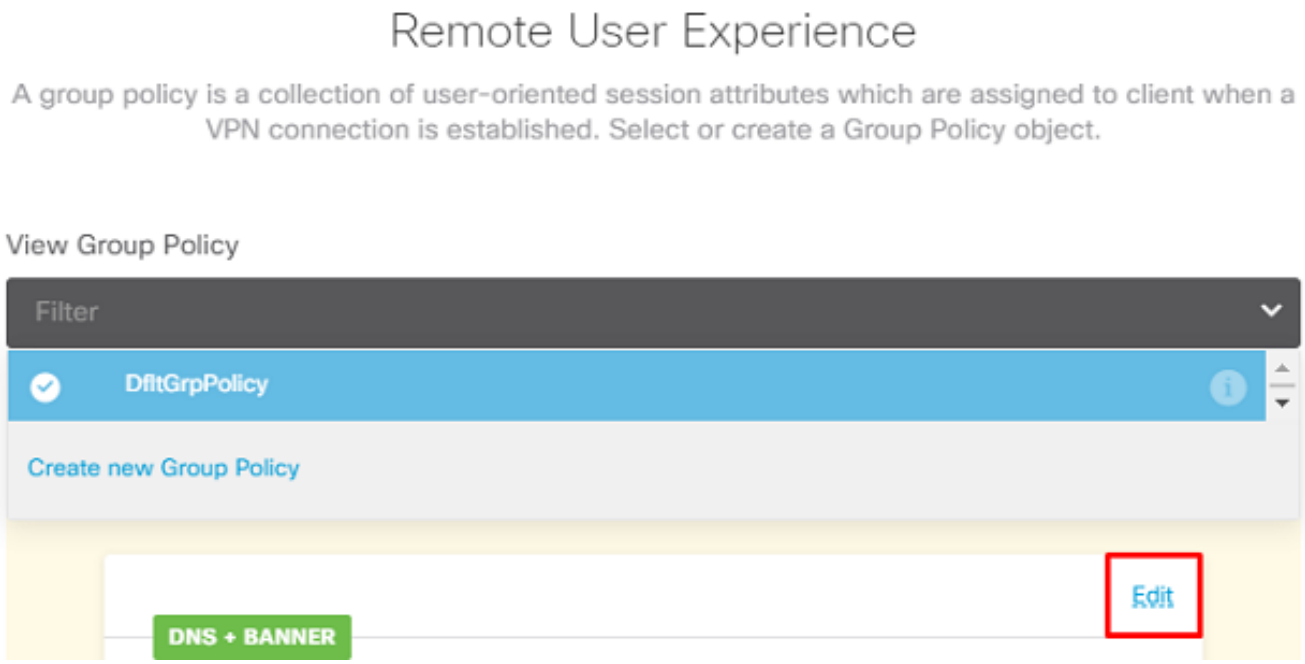
Scegliere i metodi di autenticazione come illustrato nell'immagine. In questa guida viene utilizzata l'autenticazione locale.



Scegliere il Anyconnect_Pool come mostrato nell'immagine:

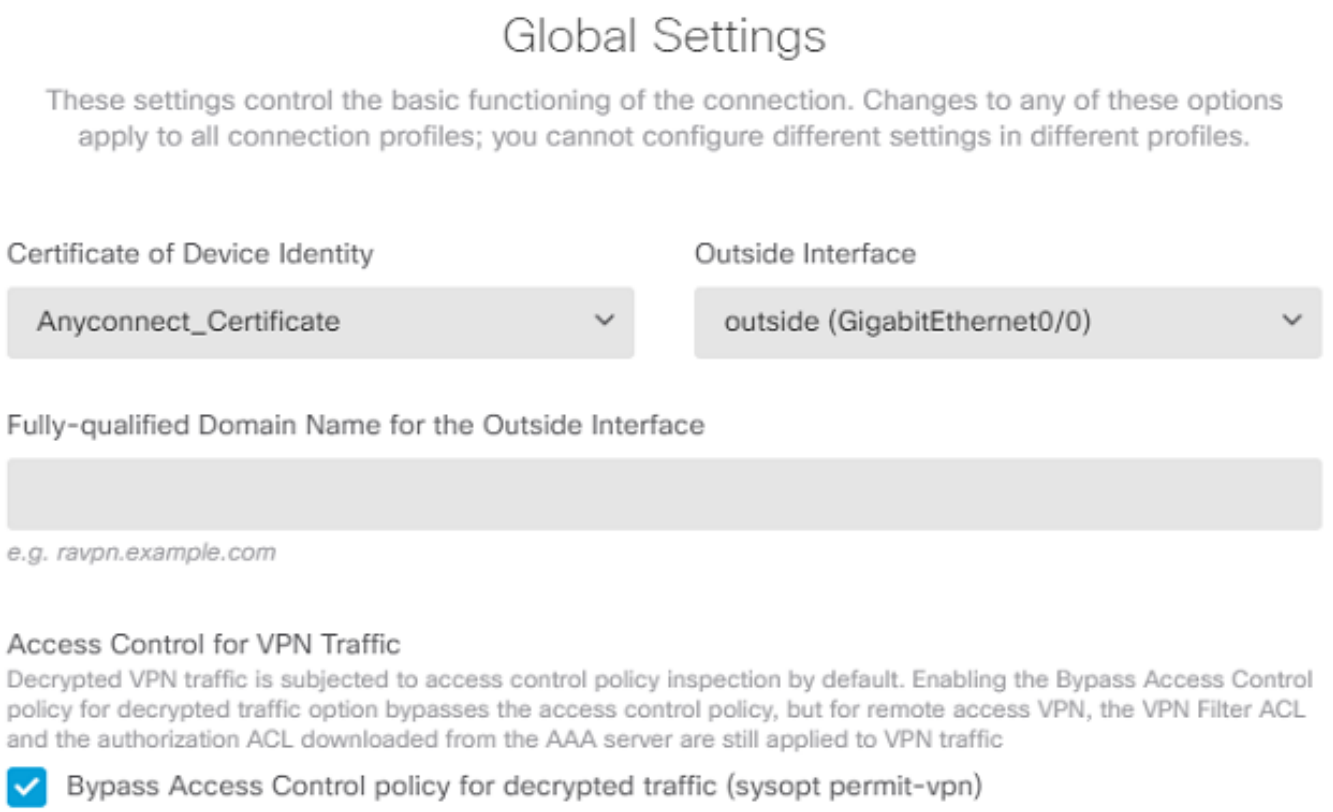


Nella pagina successiva verrà visualizzato un riepilogo dei Criteri di gruppo predefiniti. È possibile creare un nuovo criterio di gruppo quando si preme l'elenco a discesa e si sceglie l'opzione per Create a new Group Policy. In questa guida viene utilizzato il criterio di gruppo predefinito. Scegliere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

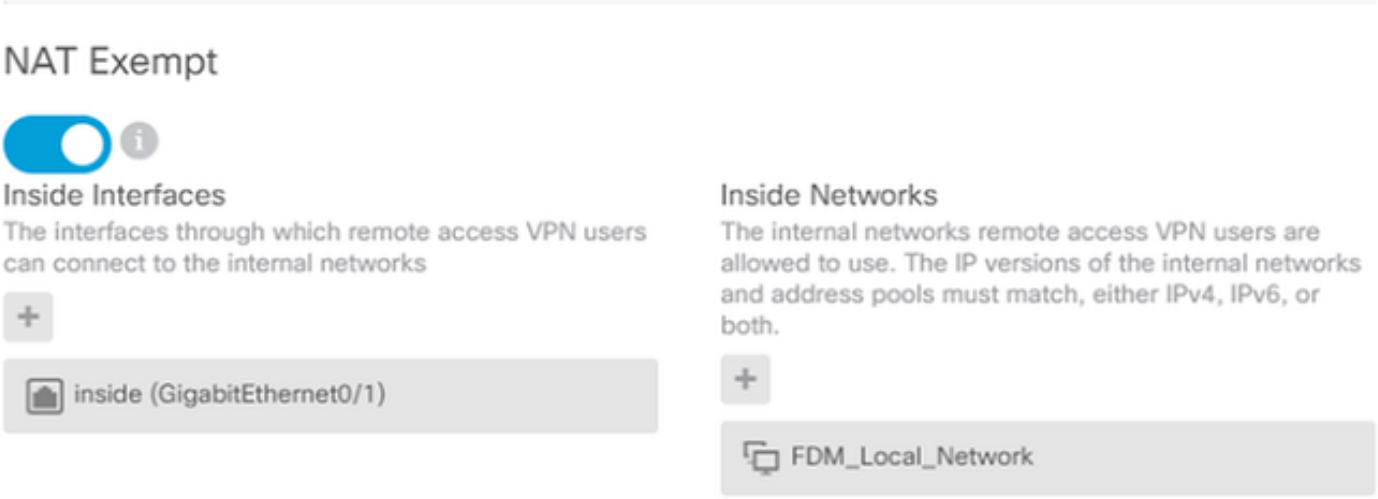


Nei Criteri di gruppo, aggiungere il tunneling suddiviso in modo che gli utenti connessi a Anyconnect inviino solo il traffico destinato alla rete FTD interna sul client Anyconnect, mentre tutto il resto del traffico esce dalla connessione ISP dell'utente, come mostrato nell'immagine:

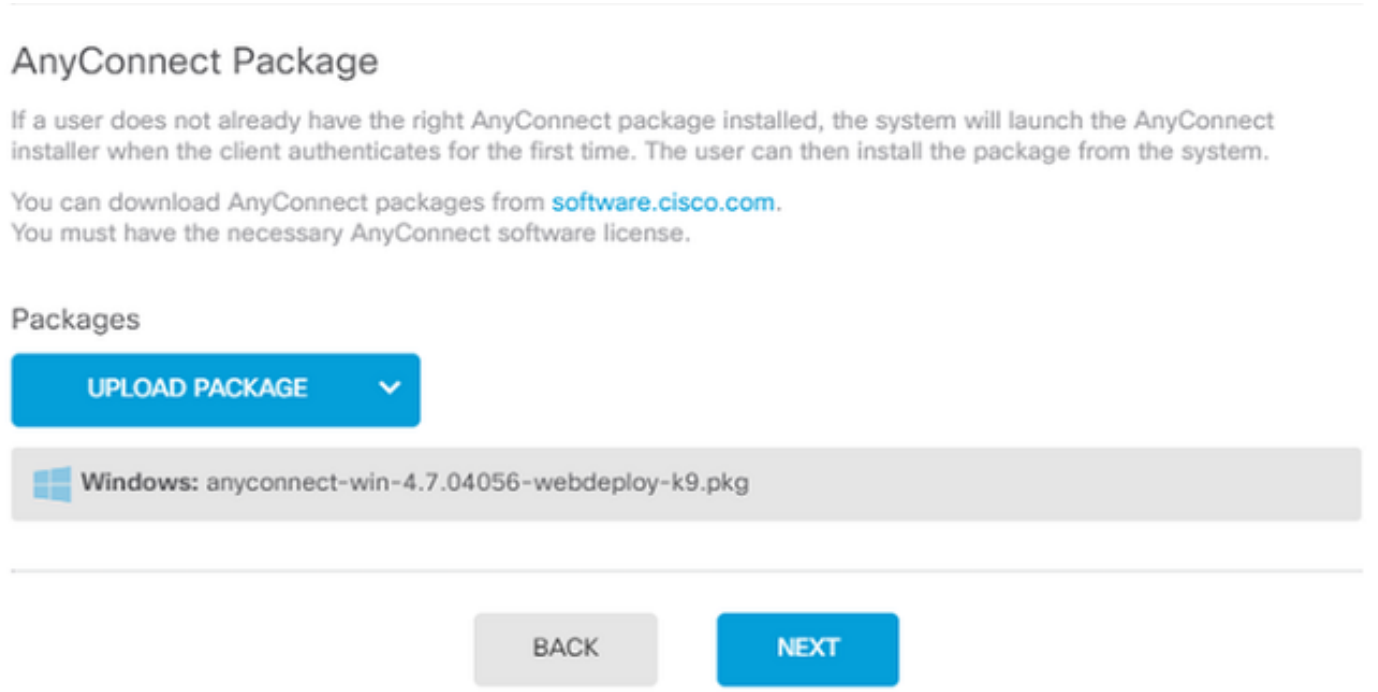
Nella pagina successiva scegliere il pulsante Anyconnect_Certificate aggiunto nella sezione certificato. Quindi, scegliere l'interfaccia su cui l'FTD resta in ascolto delle connessioni AnyConnect. Scegliere il criterio Ignora controllo di accesso per il traffico decrittografato (sysopt permit-vpn). Si 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:



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.



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



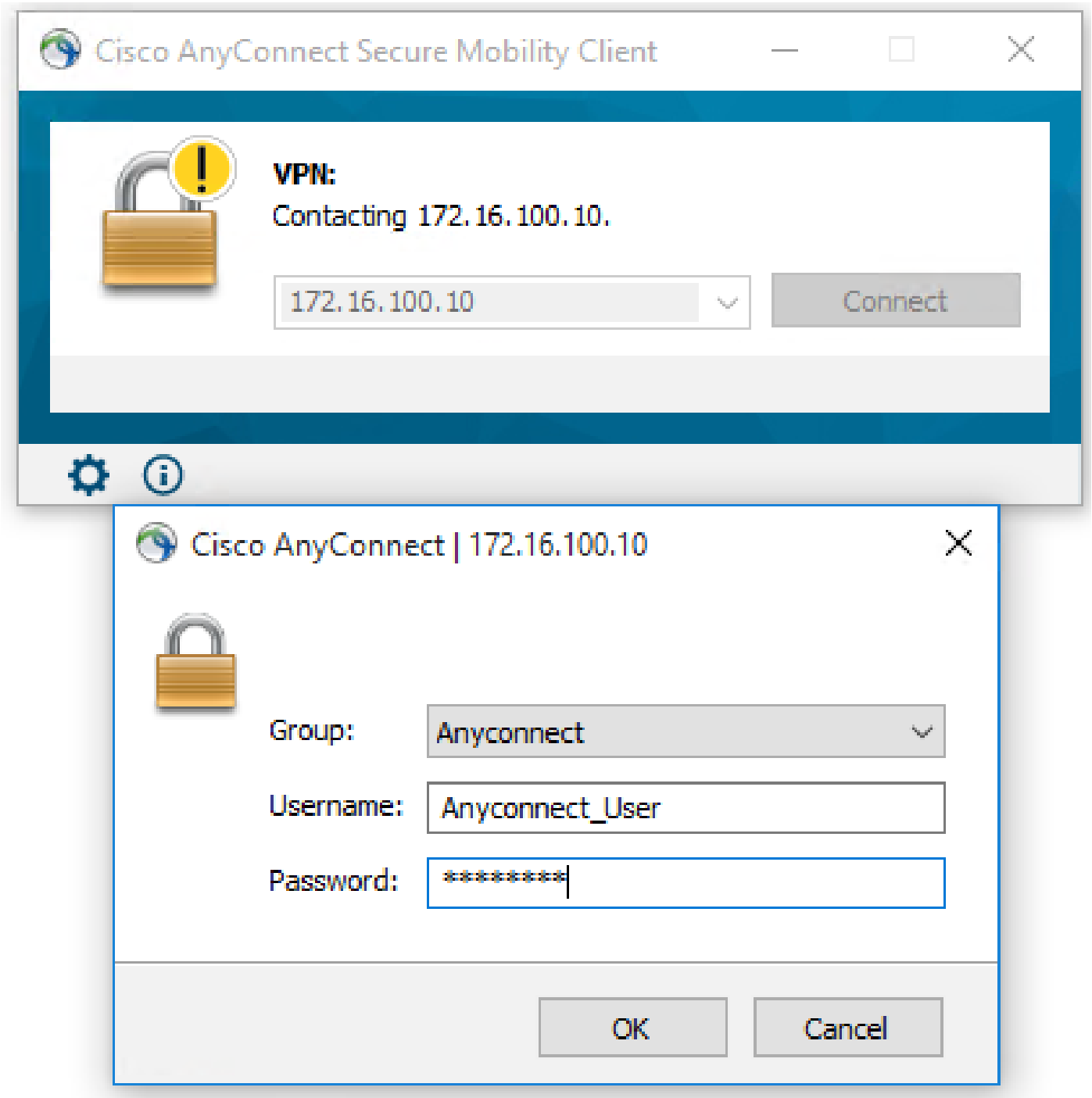
L'ultima pagina fornisce un riepilogo dell'intera configurazione. Verificare che siano stati impostati i parametri corretti, fare clic sul pulsante Fine e distribuire la nuova configurazione.

Verifica

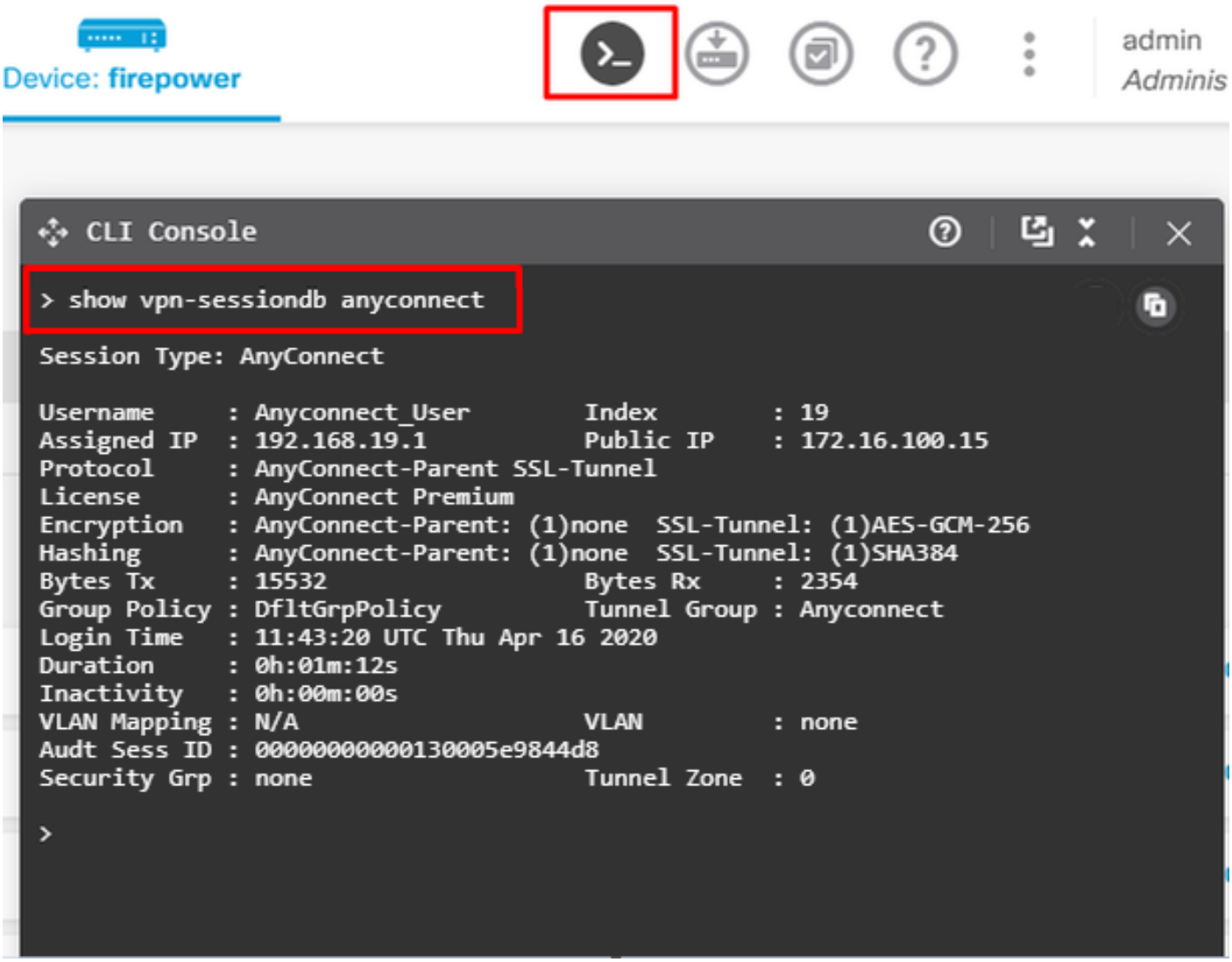
Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

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).