Configurazione della corrispondenza del certificato per l'autenticazione client sicura su FTD tramite FDM

Sommario

Introduzione

Questo documento descrive come configurare Cisco Secure Client con SSL su FTD tramite FDM utilizzando la corrispondenza dei certificati per l'autenticazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Virtual Cisco Firepower Device Manager (FDM)
- Virtual Firewall Threat Defense (FTD)
- Flusso di autenticazione VPN

Componenti usati

- Cisco Firepower Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defense Virtual 7.2.8

- Cisco Secure Client 5.1.4.74
- Editor di profili (Windows) 5.1.4.74

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 funzionalità CertificateMatch consente agli amministratori di configurare i criteri che il client deve utilizzare per selezionare un certificato client per l'autenticazione con il server VPN. Questa configurazione viene specificata nel profilo client, ovvero un file XML che può essere gestito utilizzando l'Editor di profili o modificato manualmente. La funzionalità CertificateMatch può essere utilizzata per migliorare la sicurezza delle connessioni VPN garantendo che per la connessione VPN venga utilizzato solo un certificato con attributi specifici.

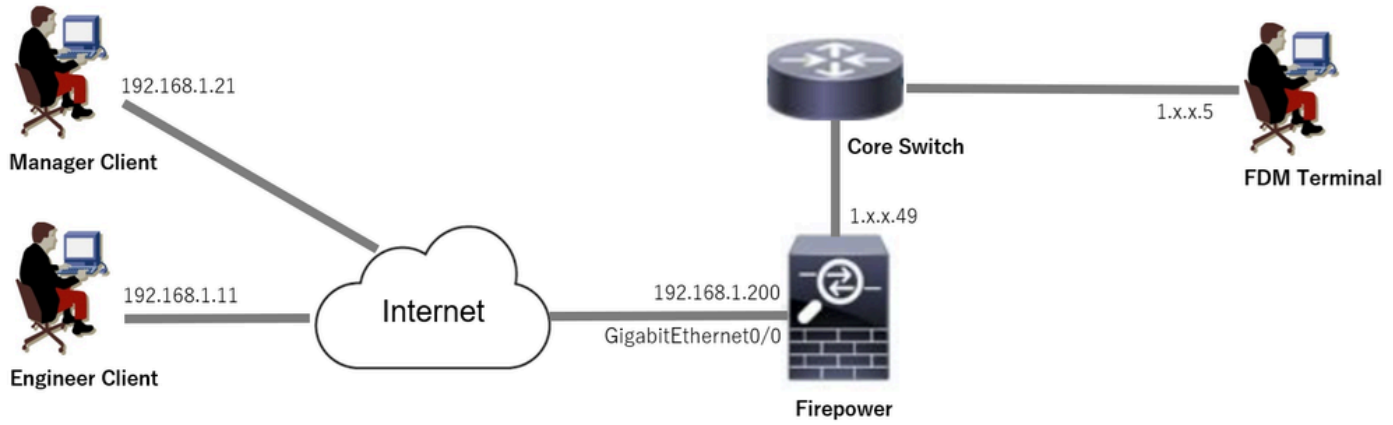
In questo documento viene descritto come autenticare Cisco Secure Client utilizzando il nome comune tratto da un certificato SSL.

Questi certificati contengono un nome comune, utilizzato ai fini dell'autorizzazione.

- CA: ftd-ra-ca-nome comune
- Certificato client VPN del tecnico: vpnEngineerClientCN
- Certificato client VPN Manager: vpnManagerClientCN
- Certificato server: 192.168.1.200

Esempio di rete

Nell'immagine è illustrata la topologia utilizzata per l'esempio del documento.



Esempio di rete

Configurazioni

Configurazione in FDM

Passaggio 1. Configura interfaccia FTD

Selezionare Dispositivo > Interfacce > Visualizza tutte le interfacce, configurare l'interfaccia interna ed esterna per FTD nella scheda Interfacce.

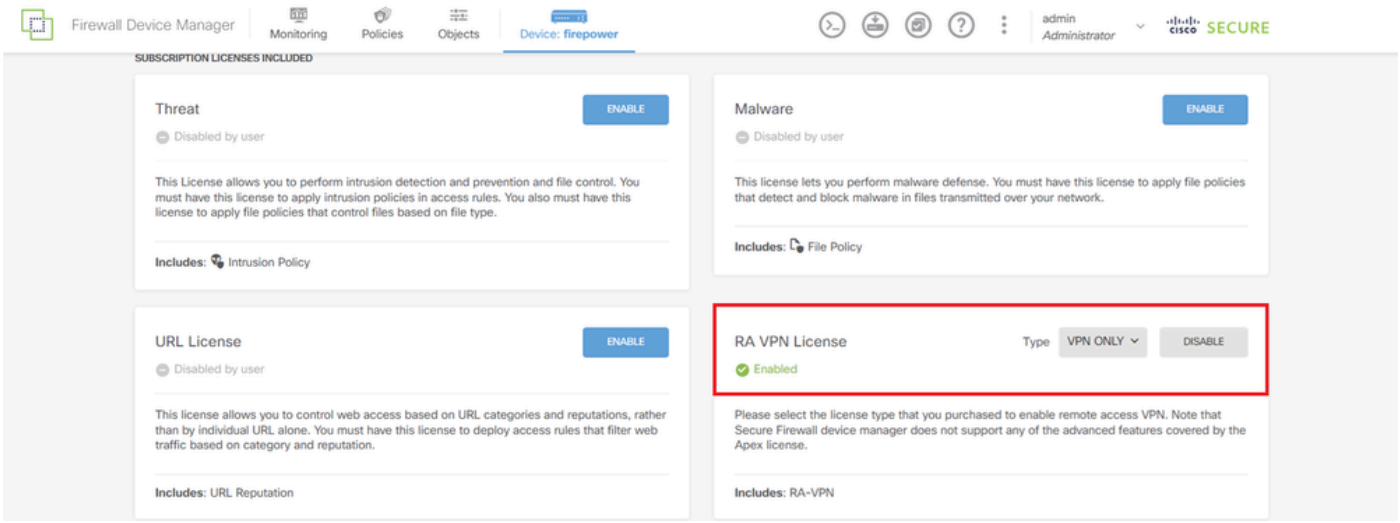
Per Gigabit Ethernet0/0,

- Nome: esterno
- Indirizzo IP: 192.168.1.200/24

Interfaccia FTD

Passaggio 2. Conferma licenza Cisco Secure Client

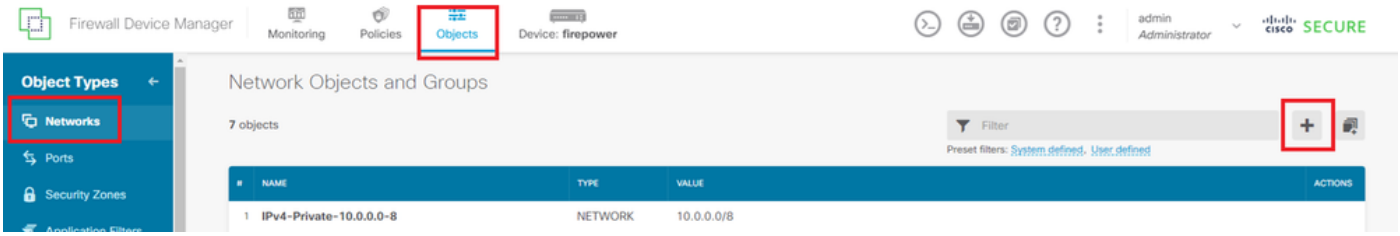
Selezionare Device > Smart License > View Configuration, quindi confermare la licenza Cisco Secure Client in RSA VPN License.



Licenza Secure Client

Passaggio 3. Aggiungi pool di indirizzi

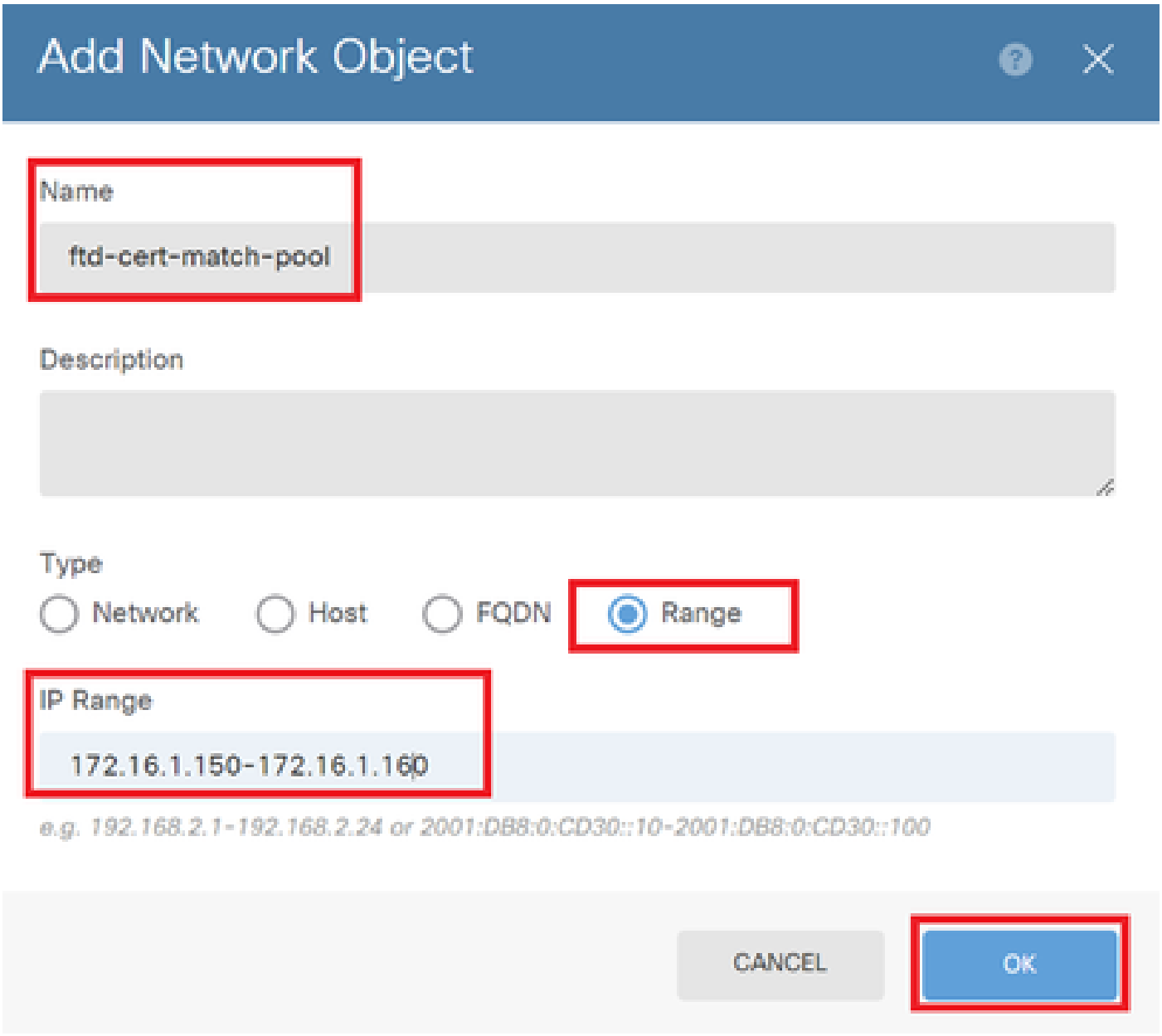
Passare a Oggetti > Reti, fare clic + pulsante.



Aggiungi pool di indirizzi

Immettere le informazioni necessarie per aggiungere un nuovo pool di indirizzi IPv4. fare clic sul pulsante OK.

- Nome: ftd-cert-match-pool
- Tipo: intervallo
- Range IP: 172.16.1.150-172.16.1.160

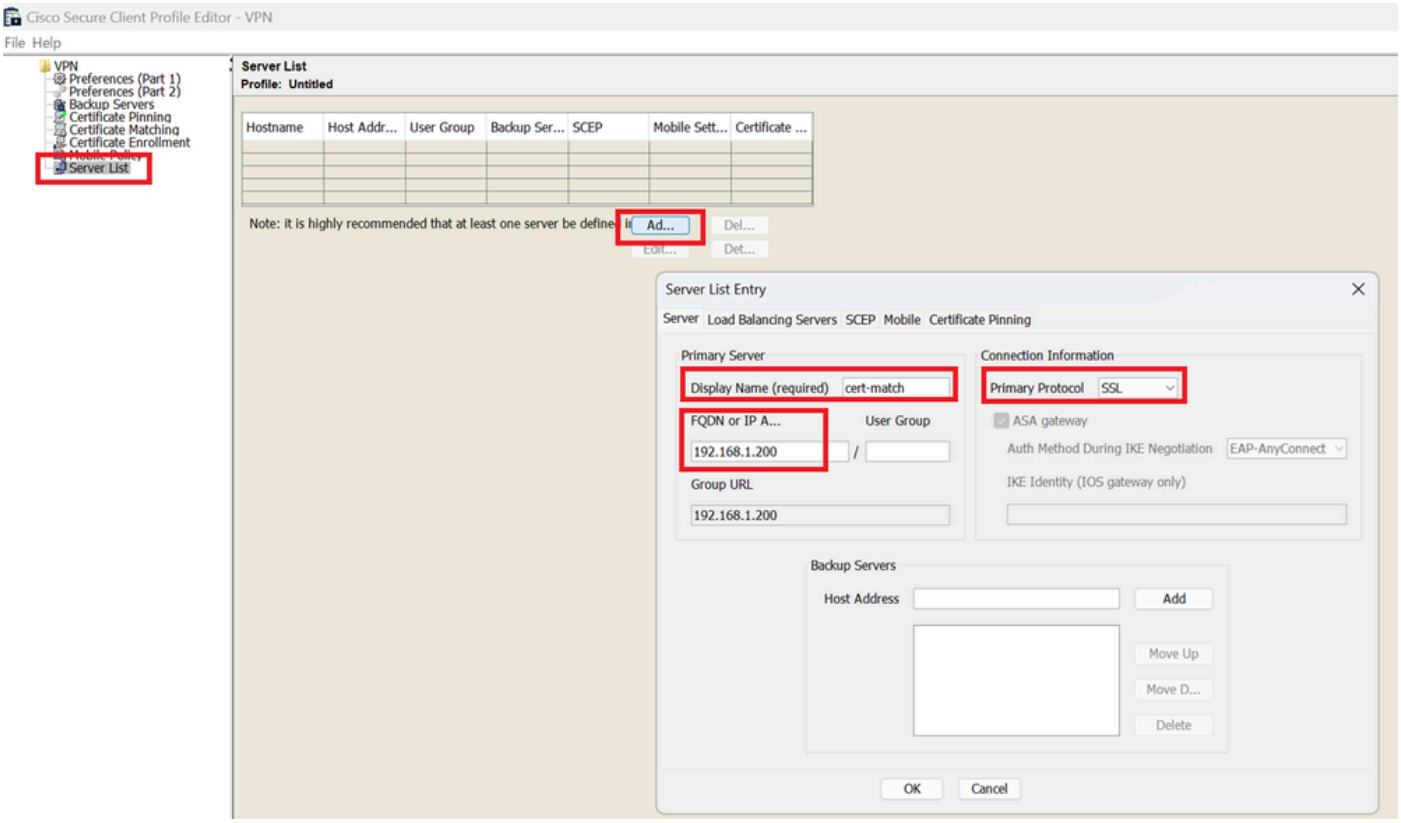


Dettagli pool di indirizzi IPv4

Passaggio 4. Crea profilo client protetto

Scaricare e installare Secure Client Profile Editor dal sito software Cisco. Passare a Elenco server, quindi fare clic su Aggiungi pulsante. Immettere le informazioni necessarie per aggiungere una voce dell'elenco dei server e fare clic su pulsante OK.

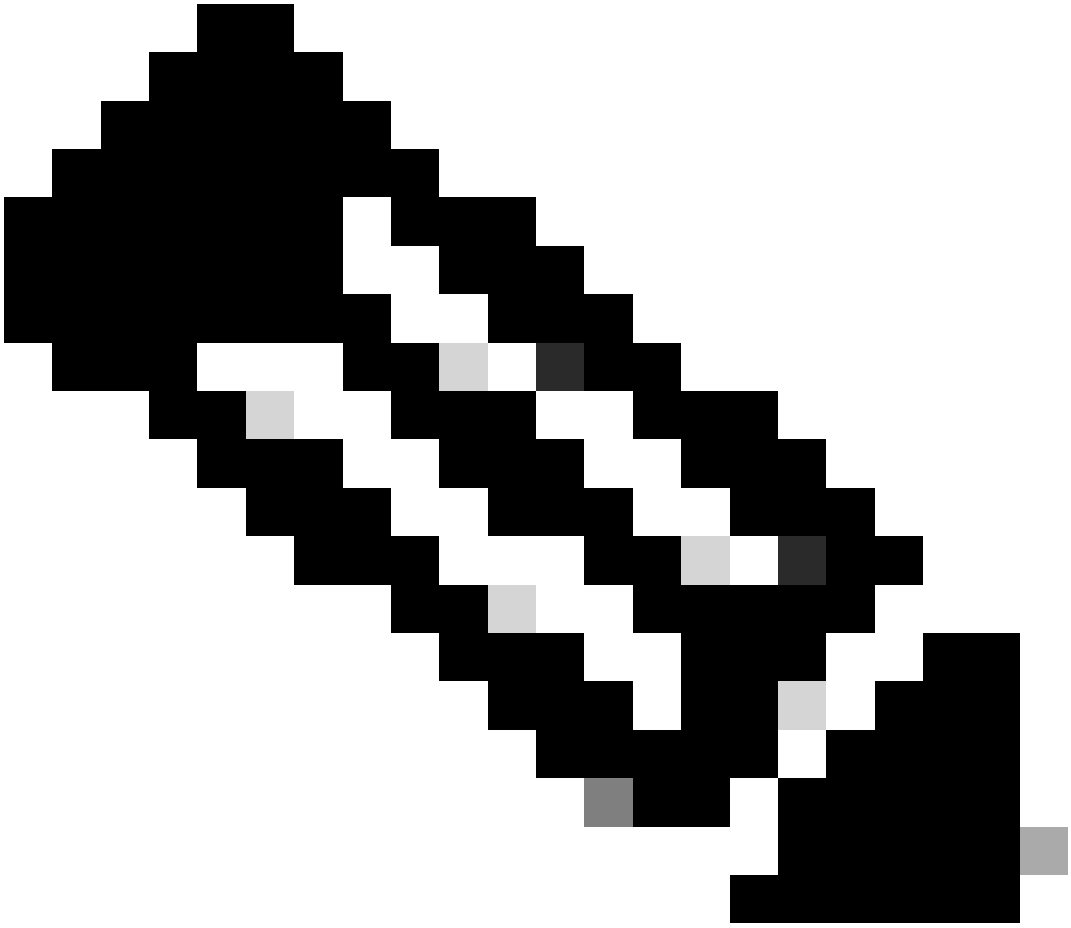
- Nome visualizzato: cert-match
- FQDN o indirizzo IP: 192.168.1.200
- Protocollo primario: SSL



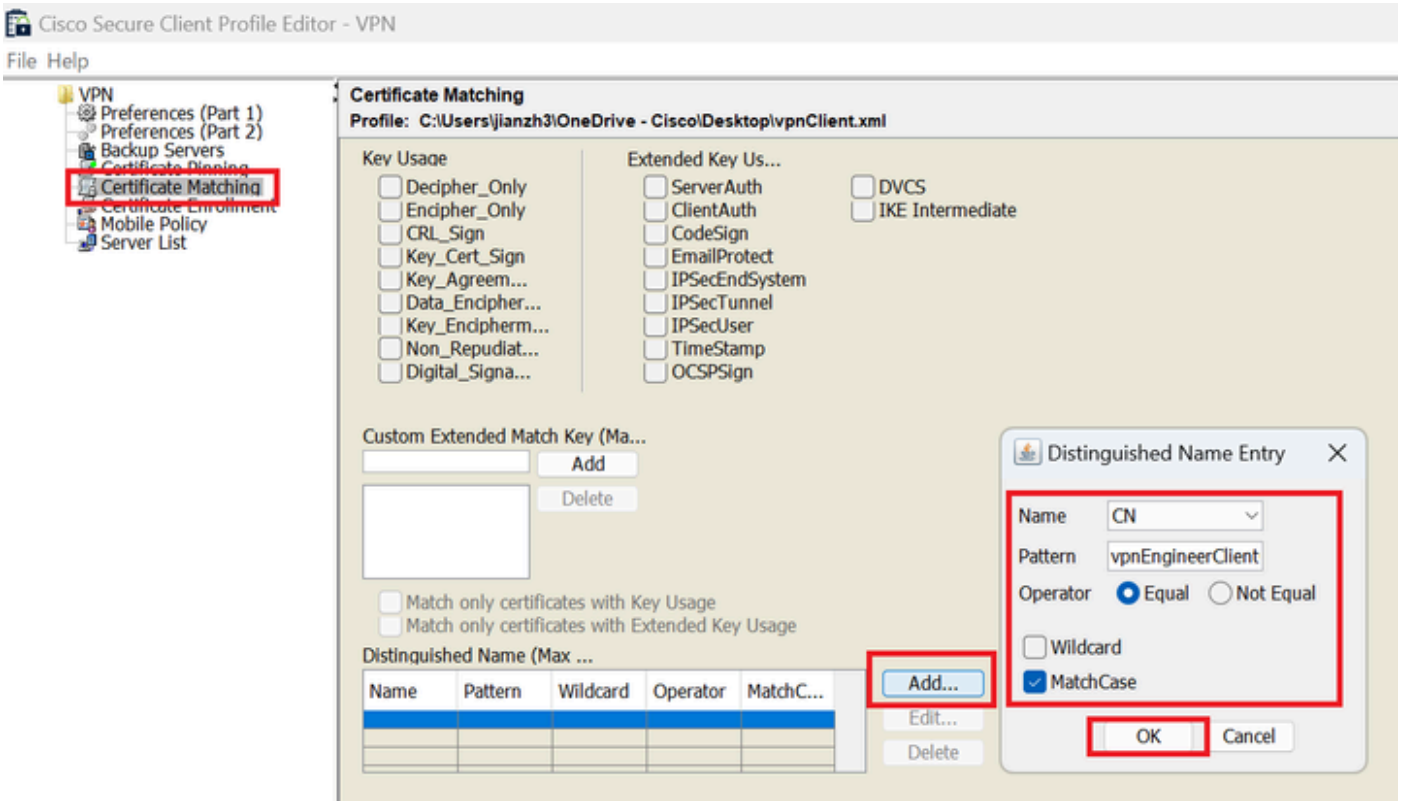
Voce elenco server

Passare a Corrispondenza certificato, fare clic su Aggiungi pulsante. Immettere le informazioni necessarie per aggiungere una voce nome distinto e fare clic su pulsante OK.

- Nome: CN
- Modello: vpnEngineerClientCN
- Operatore: Uguale



Nota: selezionare l'opzione Maiuscole/minuscole in questo documento.



Voce nome distinto

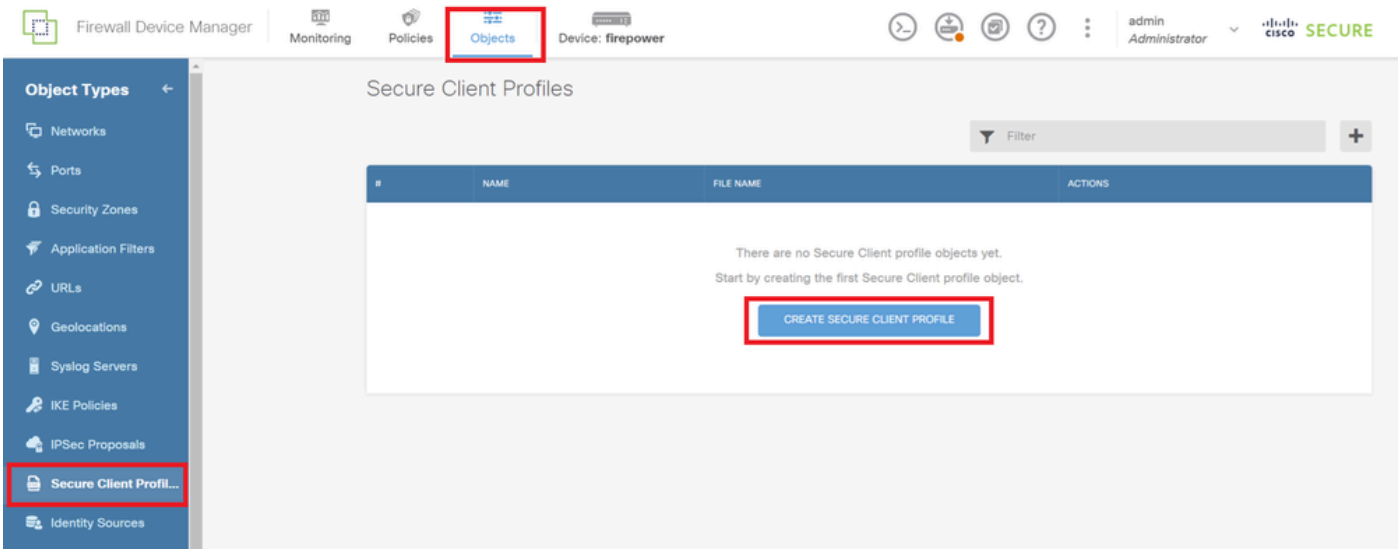
Salvare il profilo client sicuro nel computer locale e confermare i dettagli del profilo.

```
▼<CertificateMatch>
  <MatchOnlyCertsWithKU>false</MatchOnlyCertsWithKU>
  ▼<DistinguishedName>
    ▼<DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled" MatchCase="Enabled">
      <Name>CN</Name>
      <Pattern>vpnEngineerClientCN</Pattern>
    </DistinguishedNameDefinition>
  </DistinguishedName>
</CertificateMatch>
▼<EnableAutomaticServerSelection UserControllable="false">
  false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false </RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
▼<ServerList>
  ▼<HostEntry>
    <HostName>cert-match</HostName>
    <HostAddress>192.168.1.200</HostAddress>
  </HostEntry>
</ServerList>
</AnyConnectProfile>
```

Secure Client Profile

Passaggio 5. Carica profilo client sicuro in FDM

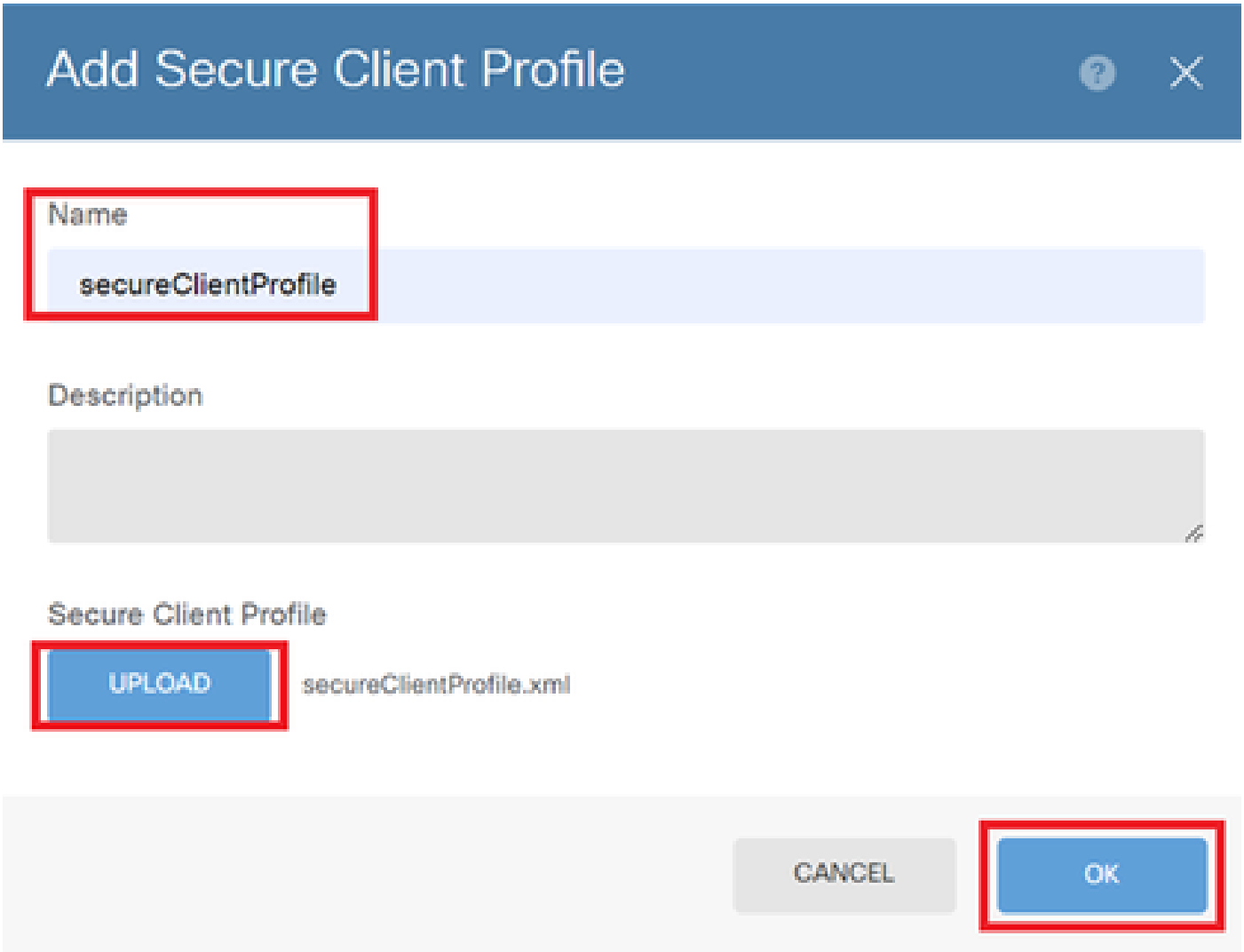
Selezionare Oggetti > Profilo client sicuro, quindi fare clic sul pulsante CREA PROFILO CLIENT SICURO.



Crea profilo client protetto

Immettere le informazioni necessarie per aggiungere un profilo client sicuro e fare clic su OK pulsante.

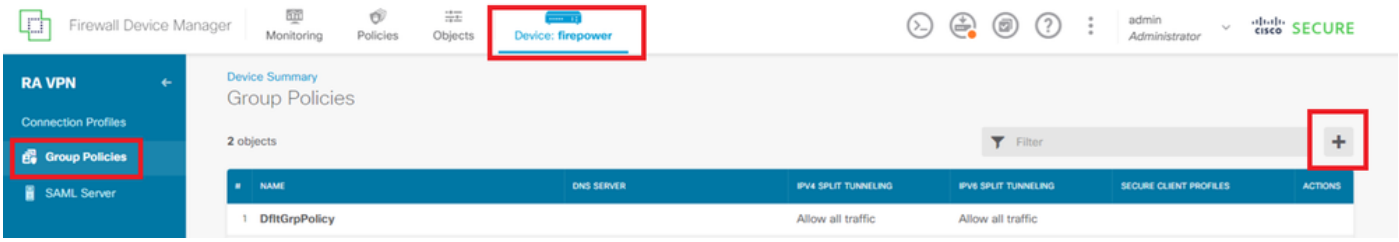
- Nome: secureClientProfile
- Profilo client sicuro: secureClientProfile.xml (caricamento dal computer locale)



Aggiungi profilo client sicuro

Passaggio 6. Aggiungi Criteri di gruppo

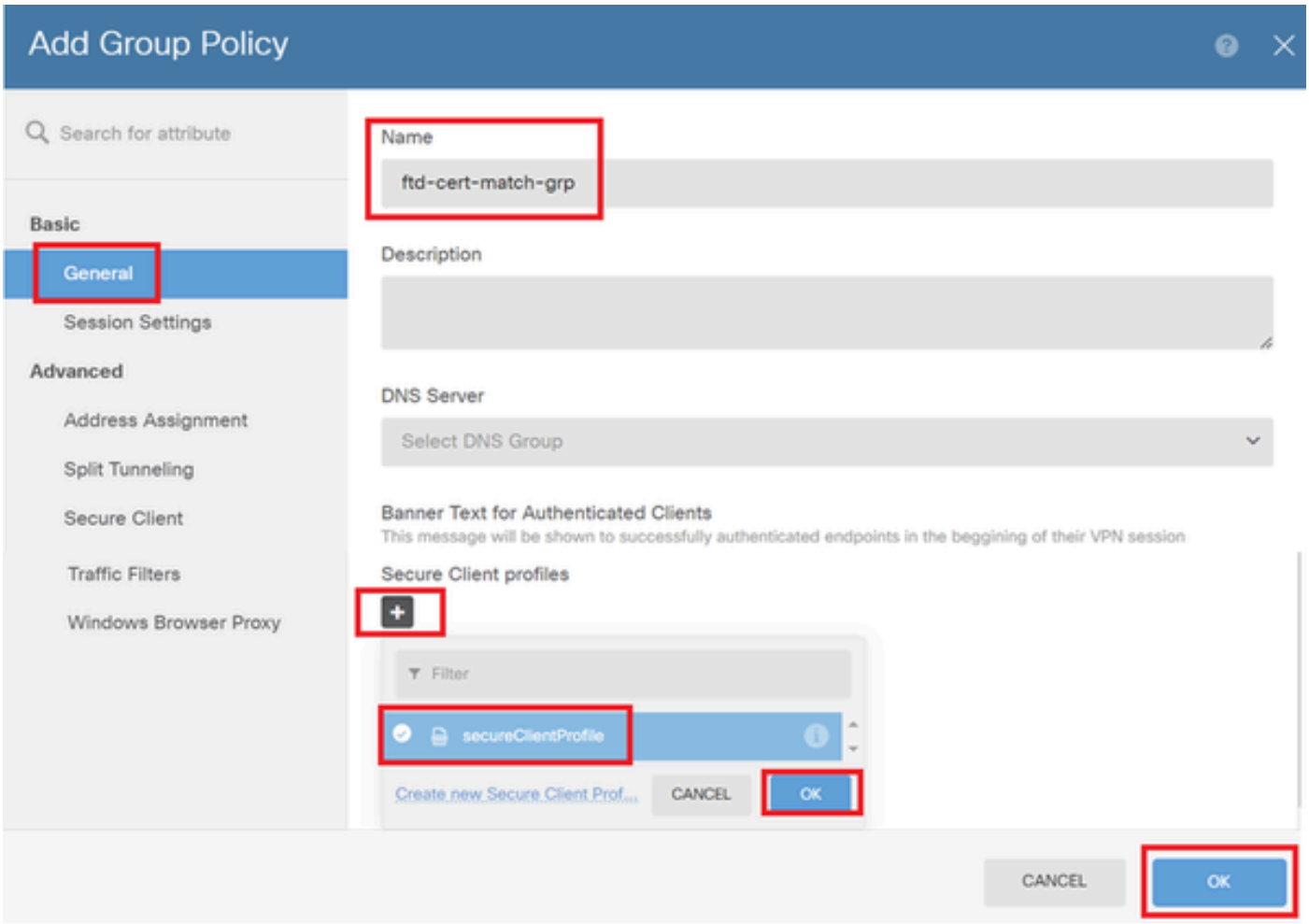
Selezionare Dispositivo > VPN ad accesso remoto > Visualizza configurazione > Criteri di gruppo, quindi fare clic sul pulsante +.



Aggiungi Criteri di gruppo

Immettere le informazioni necessarie per aggiungere un criterio di gruppo e fare clic sul pulsante OK.

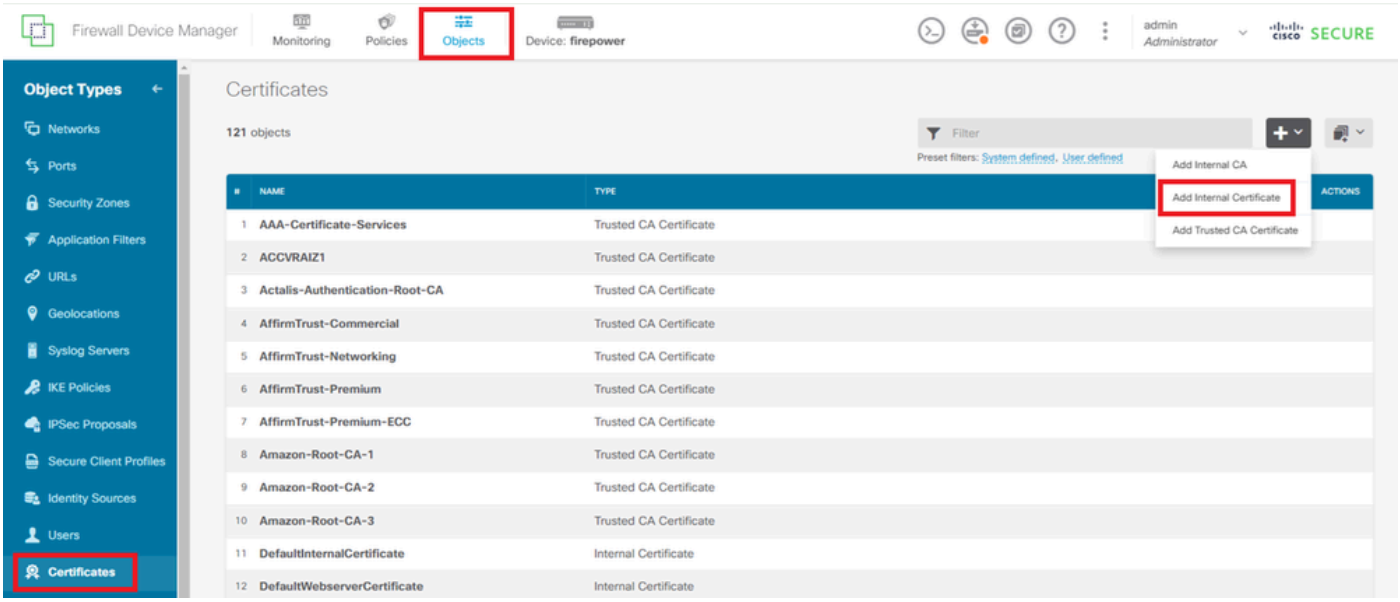
- Nome: ftd-cert-match-grp
- Profili client sicuri: secureClientProfile



Dettagli di Criteri di gruppo

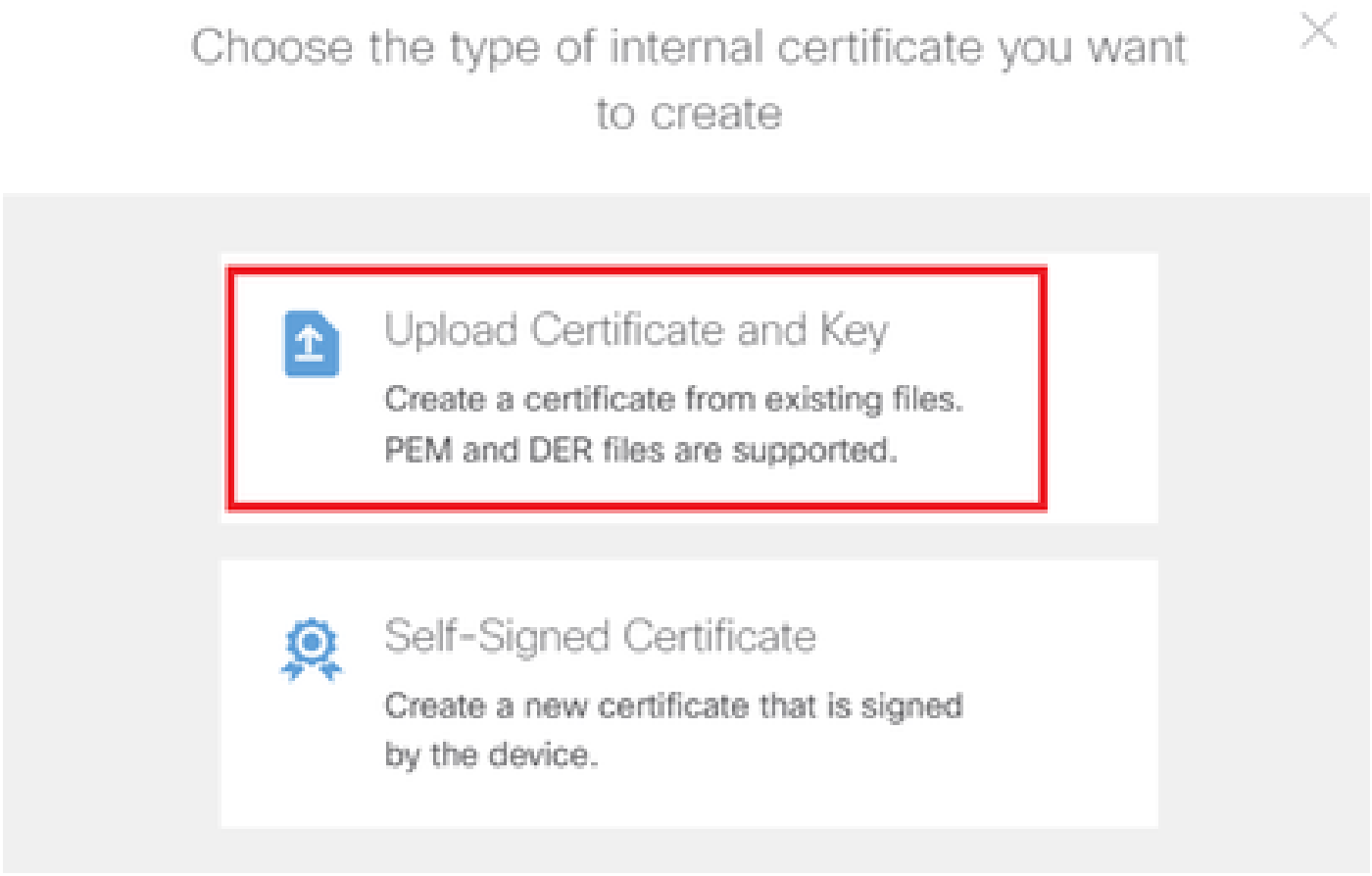
Passaggio 7. Aggiungi certificato FTD

Passare a Oggetti > Certificati, quindi fare clic su Aggiungi certificato interno da + elemento.



Aggiungi certificato interno

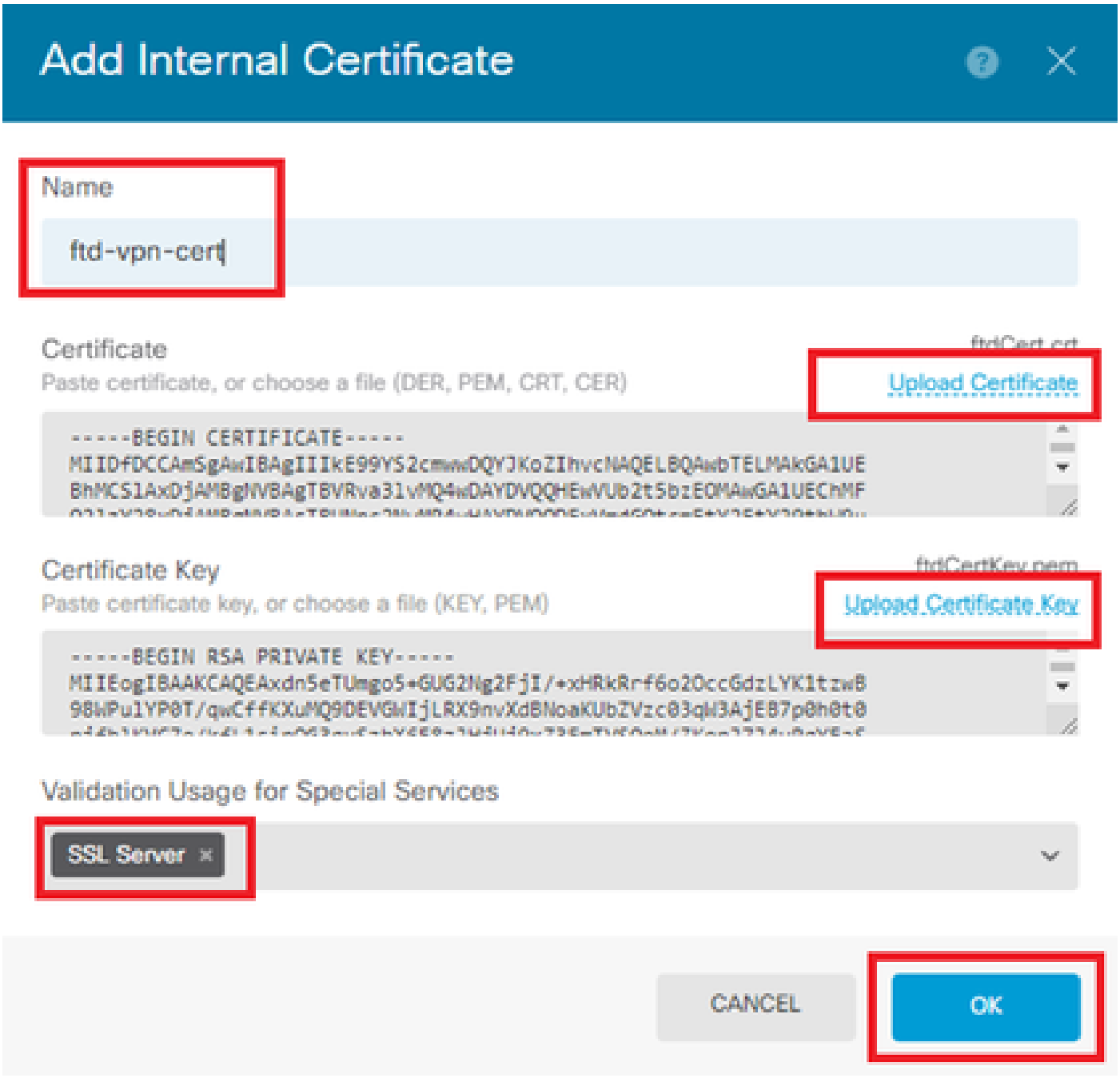
Fare clic su Carica certificato e chiave.



Carica certificato e chiave

Immettere le informazioni necessarie per il certificato FTD, importare un certificato e una chiave di certificato dal computer locale e quindi fare clic su OK pulsante.

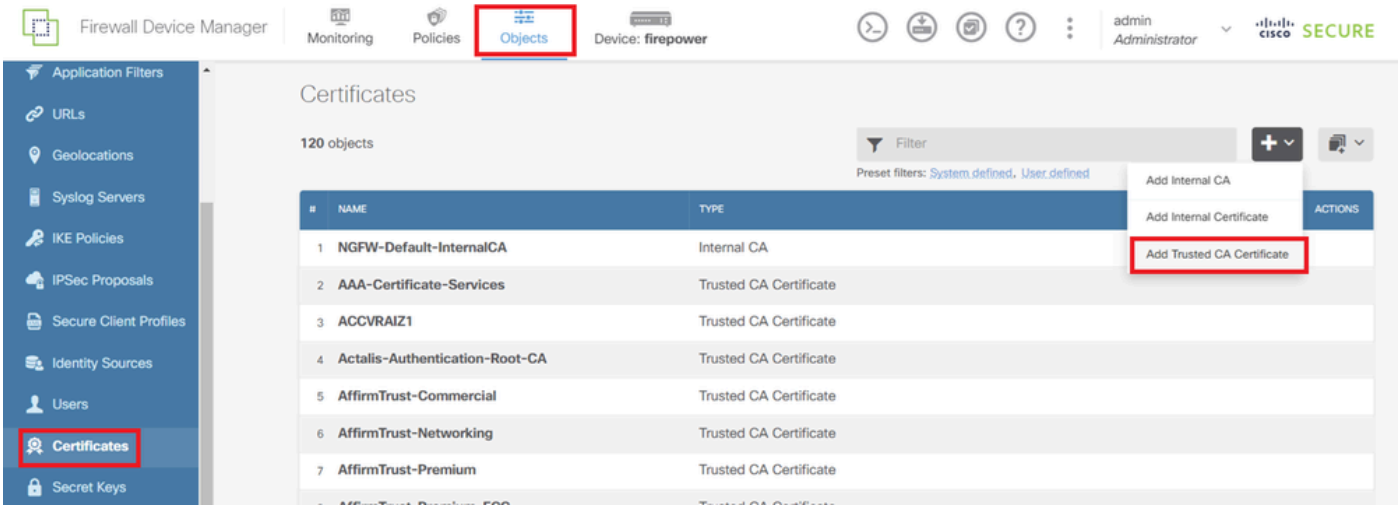
- Nome: ftd-vpn-cert
- Utilizzo convalida per servizi speciali: server SSL



Dettagli del certificato interno

Passaggio 8. Aggiungi CA a FTD

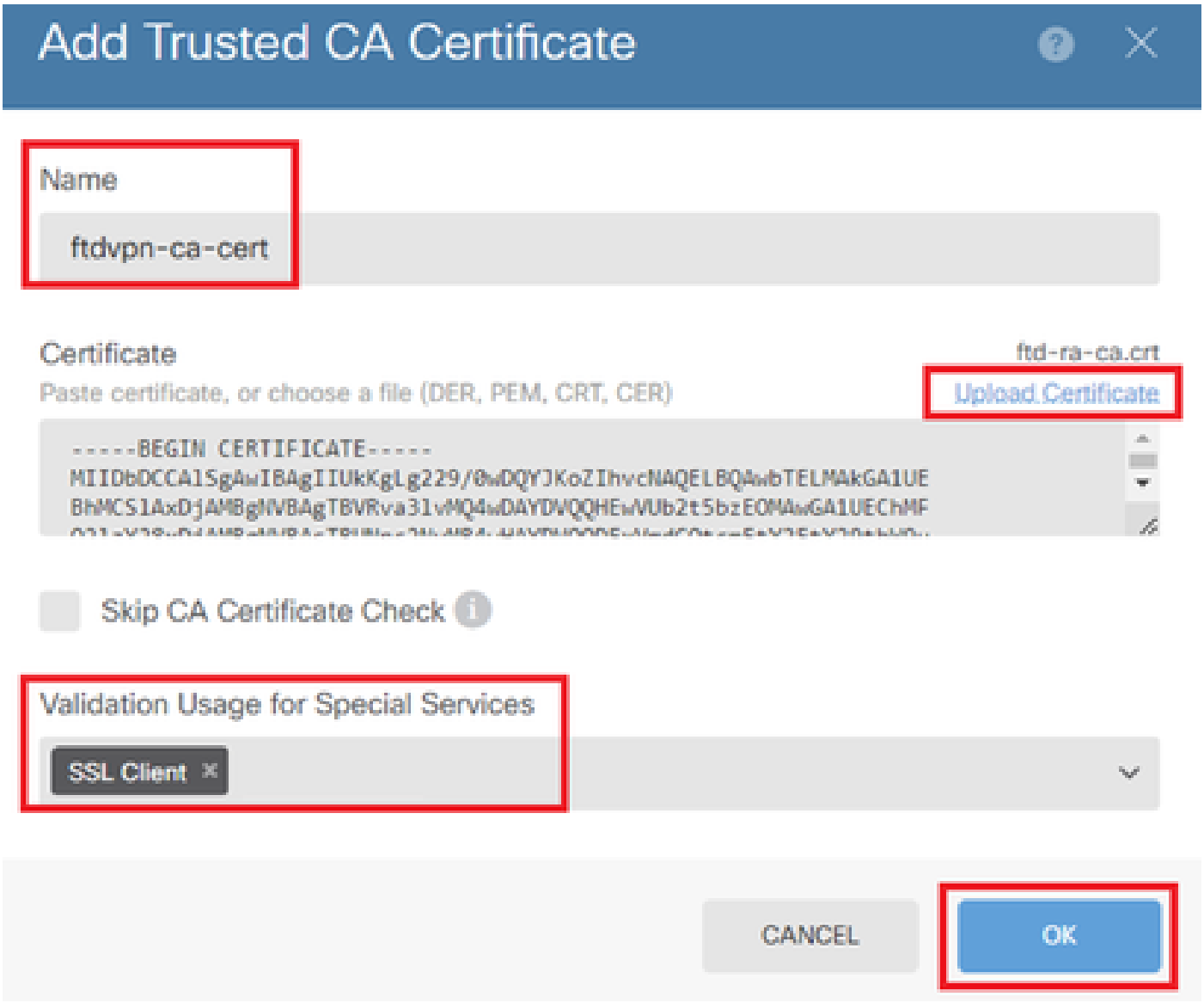
Passare a Oggetti > Certificati, quindi fare clic su Aggiungi certificato CA attendibile da + elemento.



Aggiungi certificato CA attendibile

Immettere le informazioni necessarie per la CA, importare un certificato dal computer locale.

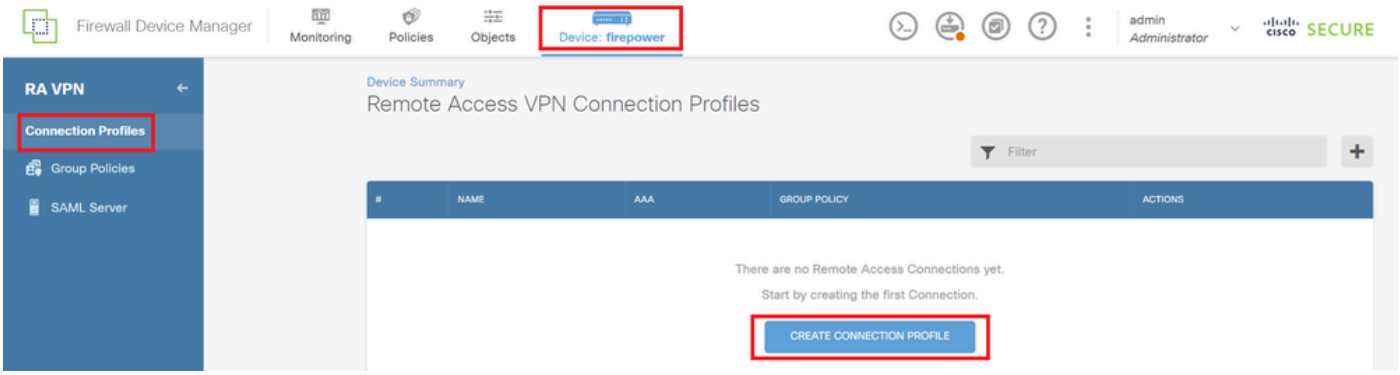
- Nome: ftdvpn-ca-cert
- Utilizzo convalida per servizi speciali: client SSL



Dettagli del certificato CA attendibile

Passaggio 9. Aggiungi profilo di connessione VPN di Accesso remoto

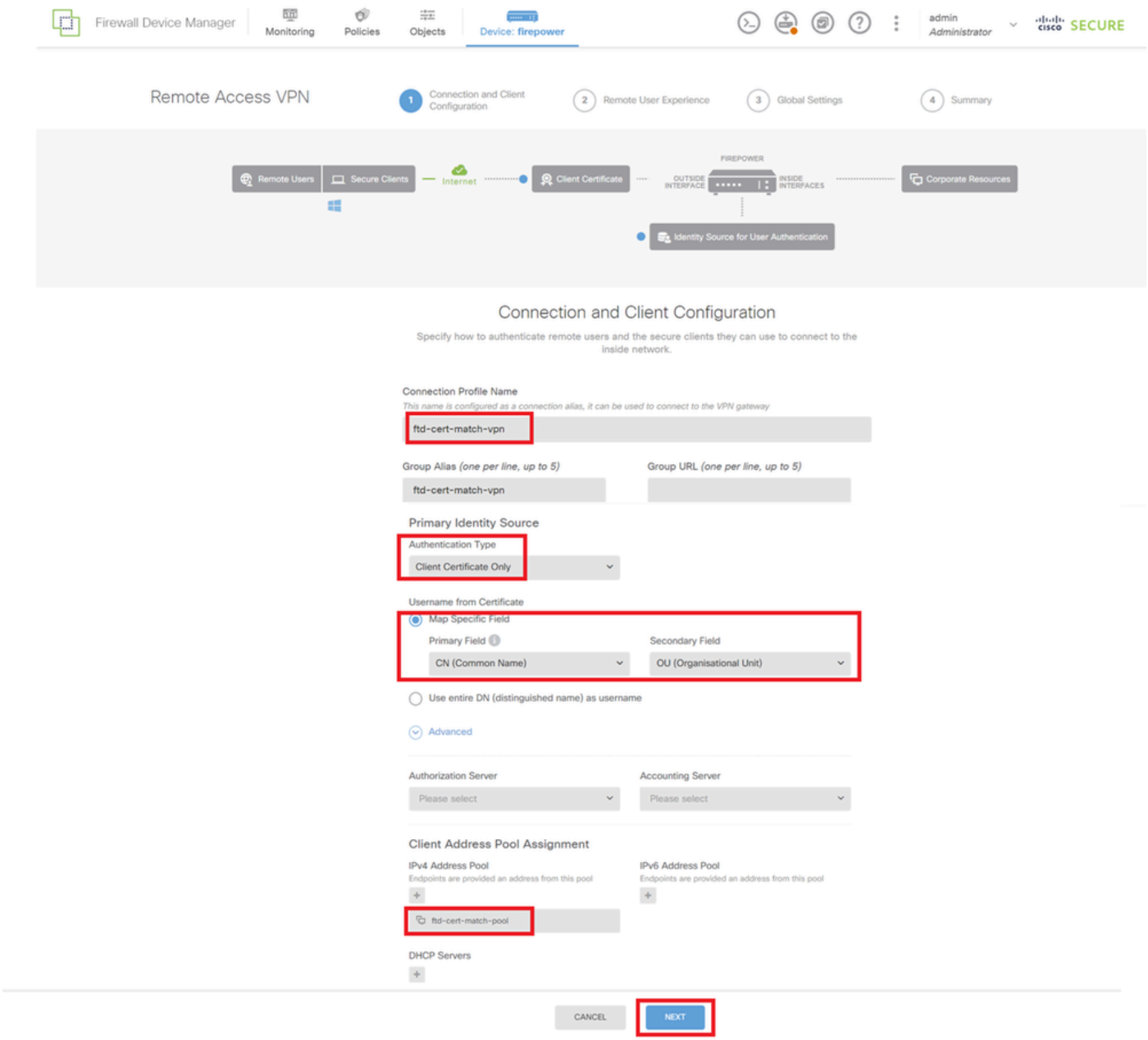
Selezionare Dispositivo > VPN ad accesso remoto > Visualizza configurazione > Profili di connessione, quindi fare clic sul pulsante CREA PROFILO DI CONNESSIONE.



Aggiungi profilo di connessione VPN di Accesso remoto

Immettere le informazioni necessarie per il profilo di connessione e fare clic sul pulsante Avanti.

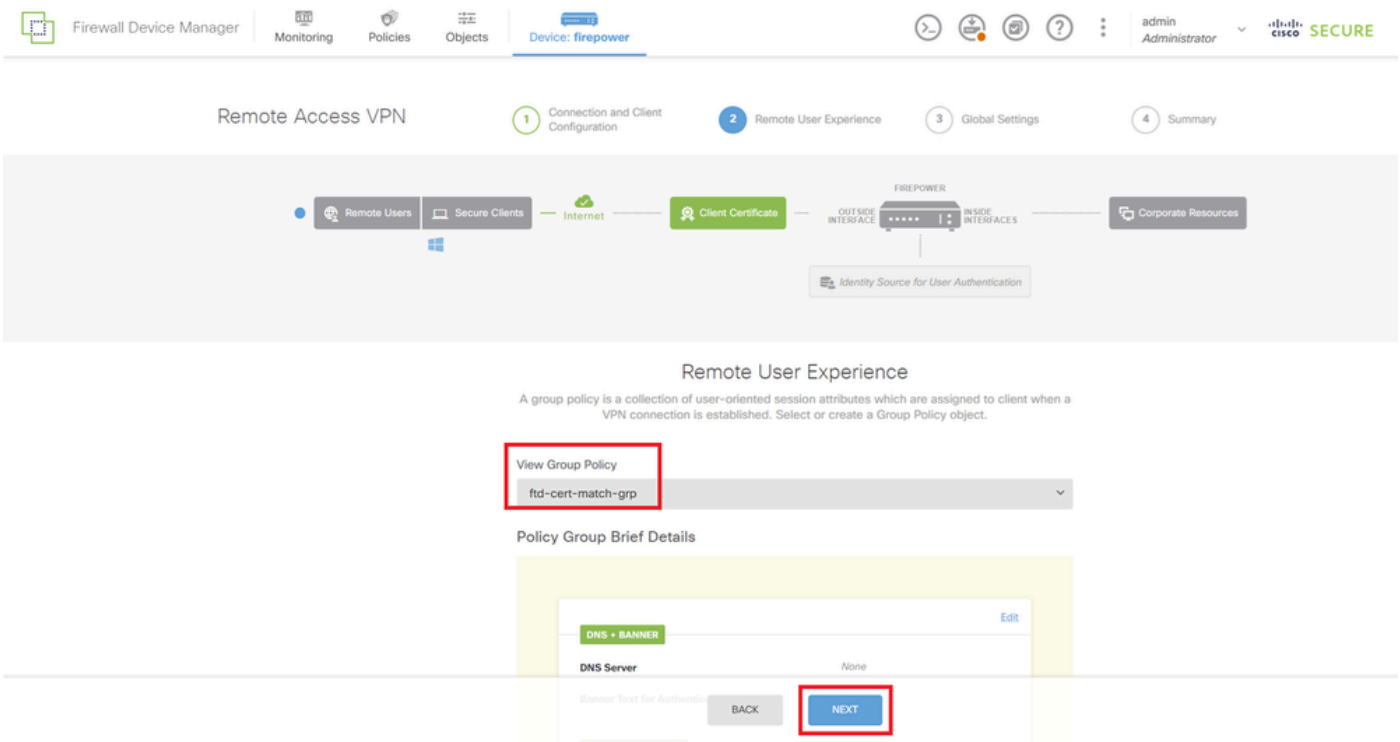
- Nome profilo connessione: ftd-cert-match-vpn
- Tipo di autenticazione: solo certificato client
- Nome utente da certificato: campo specifico della mappa
- Campo principale: CN (nome comune)
- Campo secondario: unità organizzativa
- Pool di indirizzi IPv4: ftd-cert-match-pool



Dettagli del profilo di connessione VPN

Immettere le informazioni necessarie per Criteri di gruppo e fare clic su Pulsante Avanti.

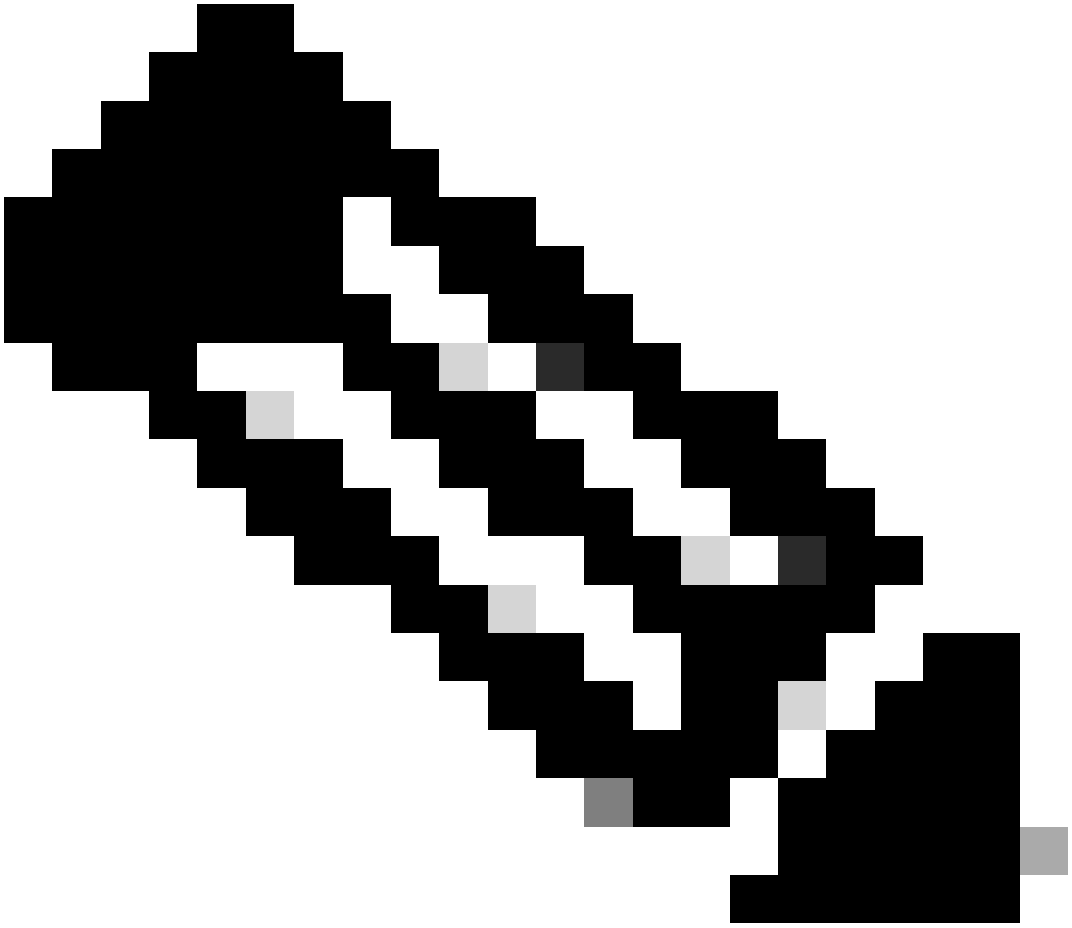
- Visualizza Criteri di gruppo: ftd-cert-match-grp



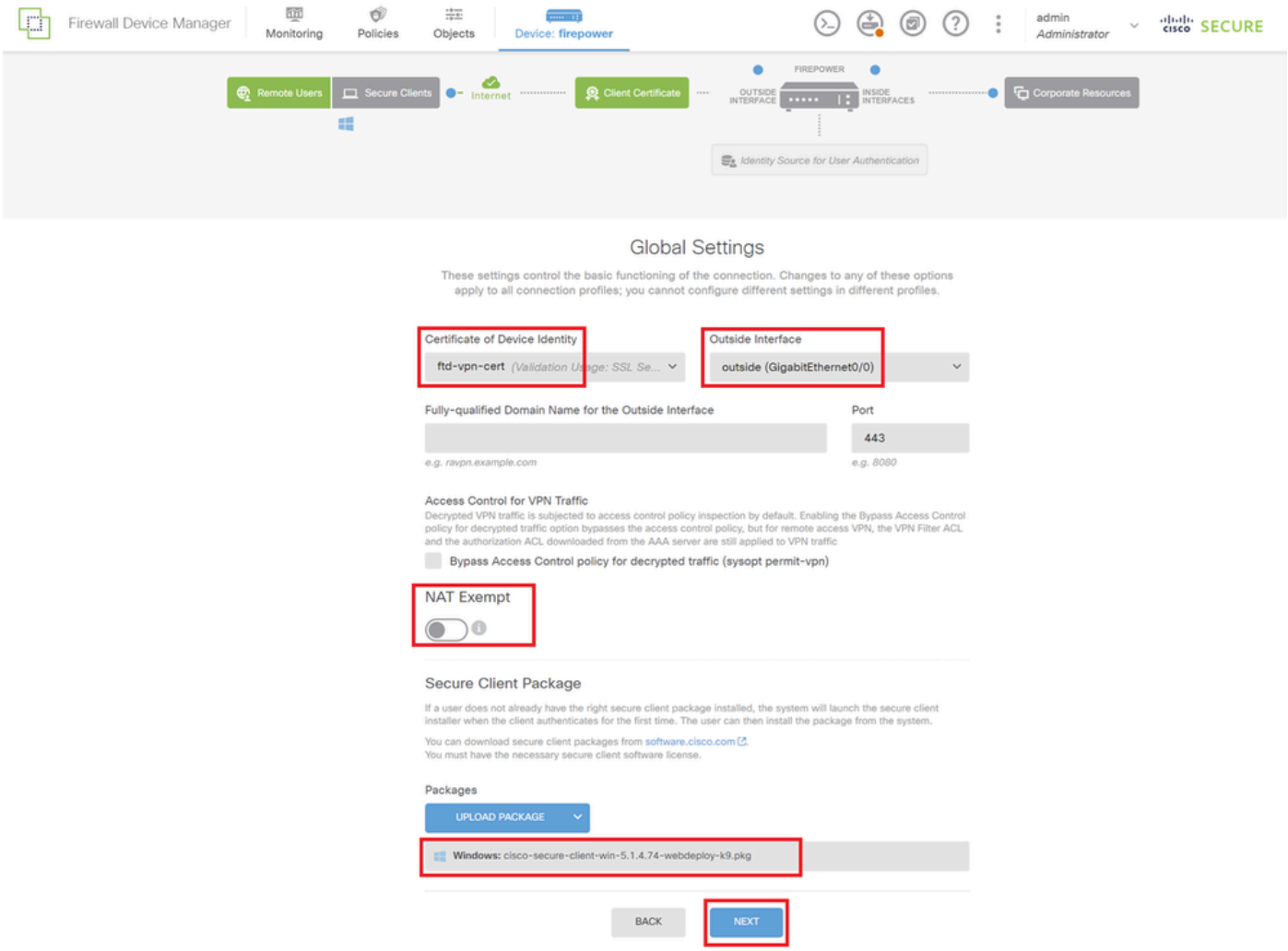
Seleziona Criteri di gruppo

Selezionare Certificato di identità del dispositivo, Interfaccia esterna, Pacchetto client sicuro per la connessione VPN.

- Certificato di identità del dispositivo: ftd-vpn-cert
- Interfaccia esterna: esterna (Gigabit Ethernet0/0)
- Pacchetto Secure Client: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



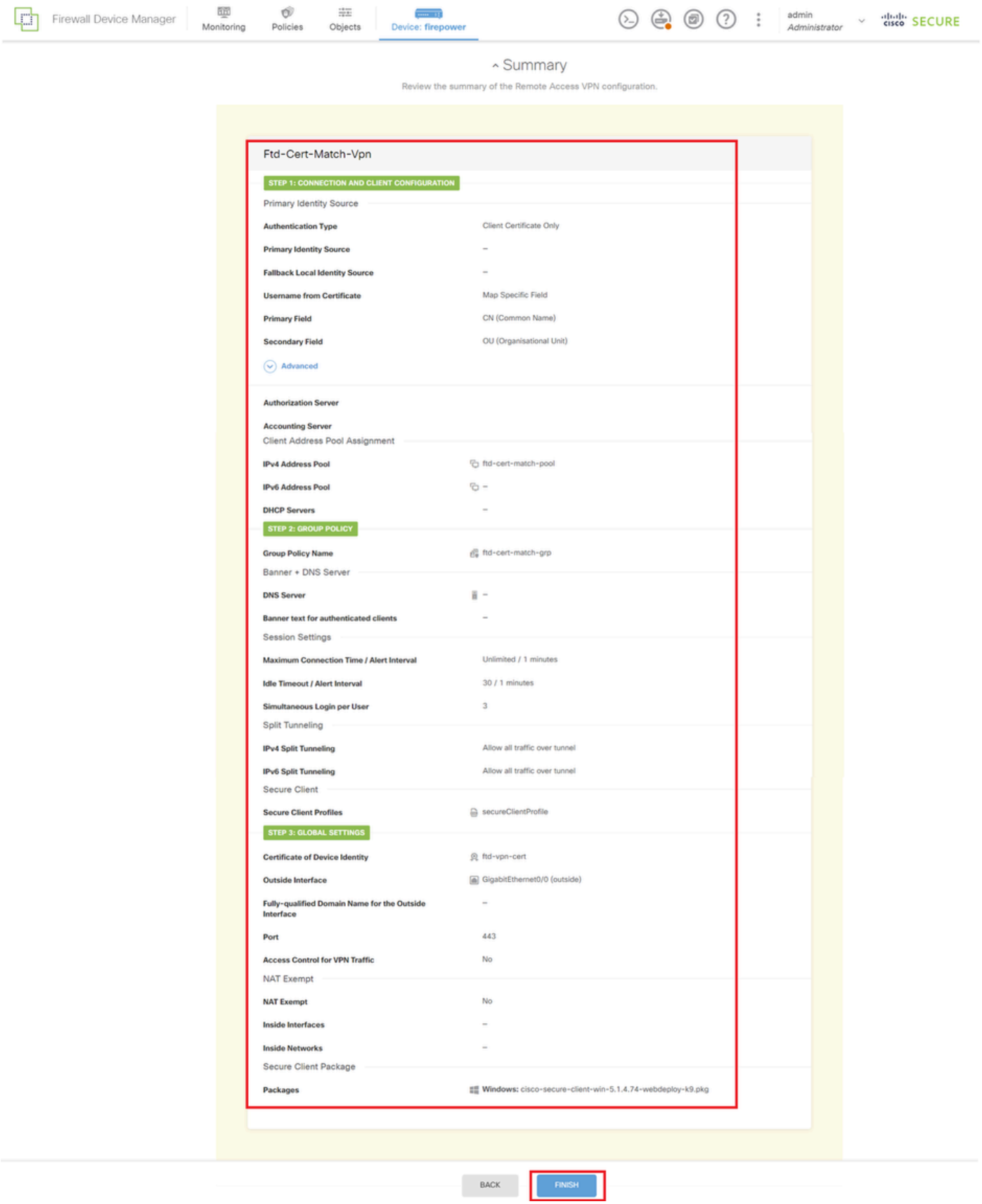
Nota: la funzionalità Esente da NAT di questo documento è disabilitata.



Dettagli delle impostazioni globali

Passaggio 10. Conferma riepilogo per il profilo di connessione

Confermare le informazioni immesse per la connessione VPN e fare clic sul pulsante FINE.



Conferma riepilogo per il profilo di connessione

Conferma nella CLI FTD

Confermare le impostazioni della connessione VPN nella CLI FTD dopo la distribuzione da FDM.

```
// Defines IP of interface
interface GigabitEthernet0/0
speed auto
nameif outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftd-vpn-cert
enrollment terminal
keypair ftd-vpn-cert
crl configure

// Server Certificate
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client
crl configure

// CA
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2
anyconnect profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
```

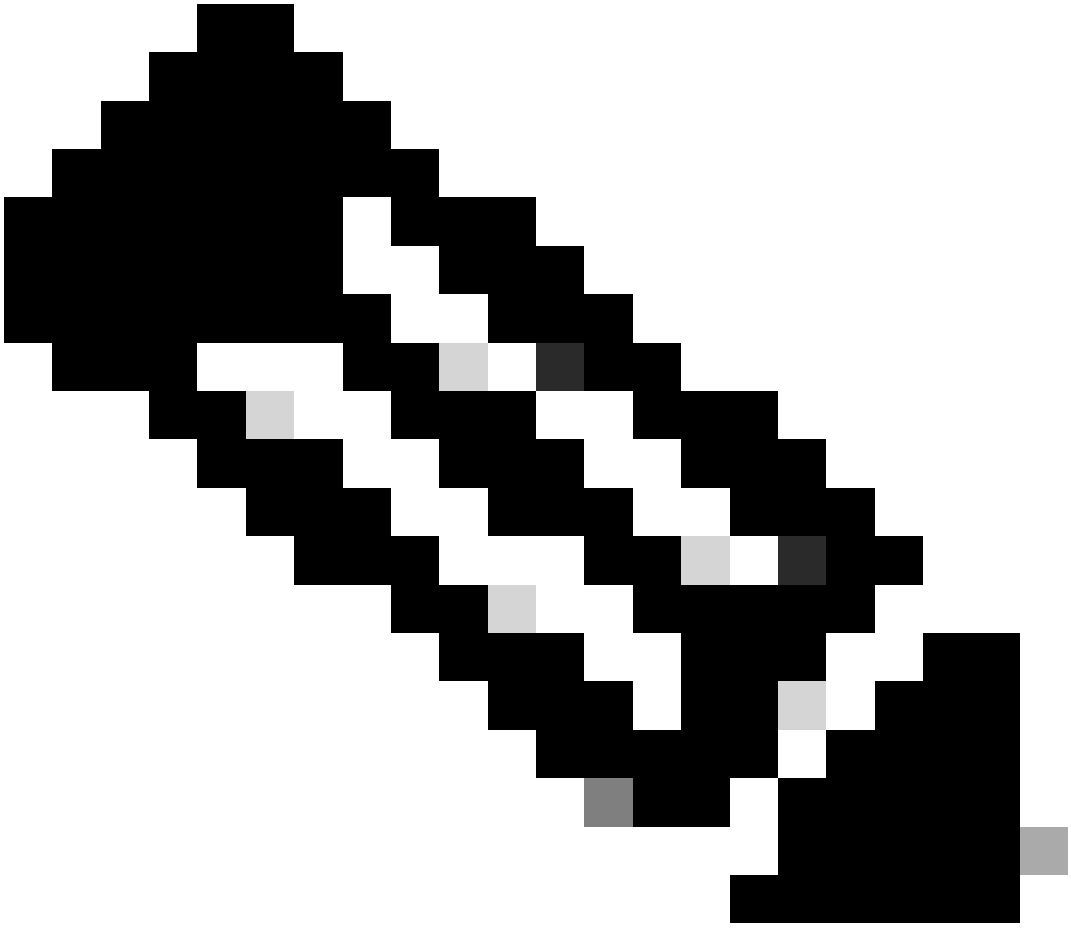
```
group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
anyconnect ssl dtls none
anyconnect mtu 1406
anyconnect ssl keepalive none
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client none
anyconnect dpd-interval gateway none
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules none
anyconnect profiles value secureClientProfile type user
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

// Configures the tunnel-group to use the certificate authentication
tunnel-group ftd-cert-match-vpn type remote-access
tunnel-group ftd-cert-match-vpn general-attributes
address-pool ftd-cert-match-pool
default-group-policy ftd-cert-match-grp
tunnel-group ftd-cert-match-vpn webvpn-attributes
authentication certificate
group-alias ftd-cert-match-vpn enable
```

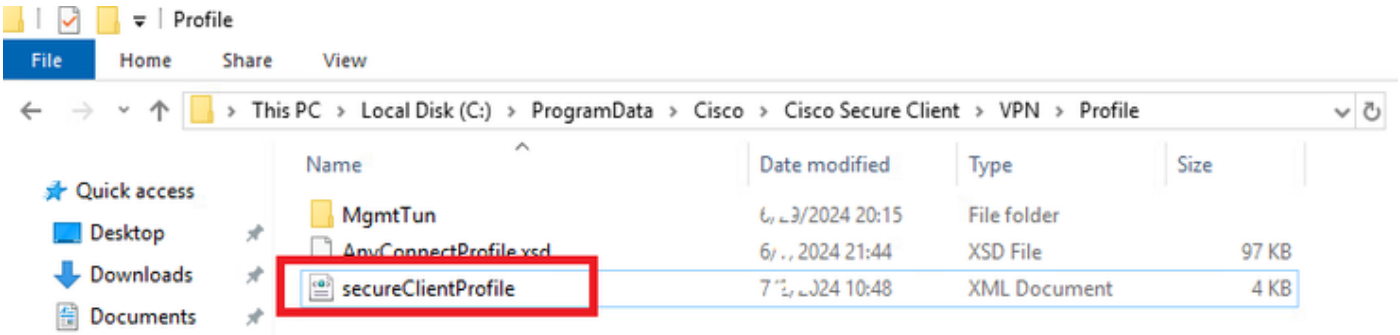
Conferma in client VPN

Passaggio 1. Copia profilo client sicuro su client VPN

Copiare il profilo client sicuro sul client VPN di progettazione e sul client VPN di gestione.



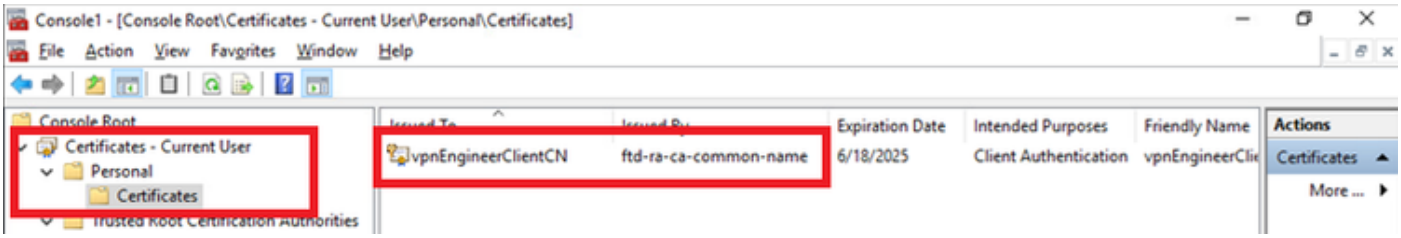
Nota: la directory del profilo client sicuro nel computer Windows: C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



Copia profilo client sicuro su client VPN

Passaggio 2. Conferma certificato client

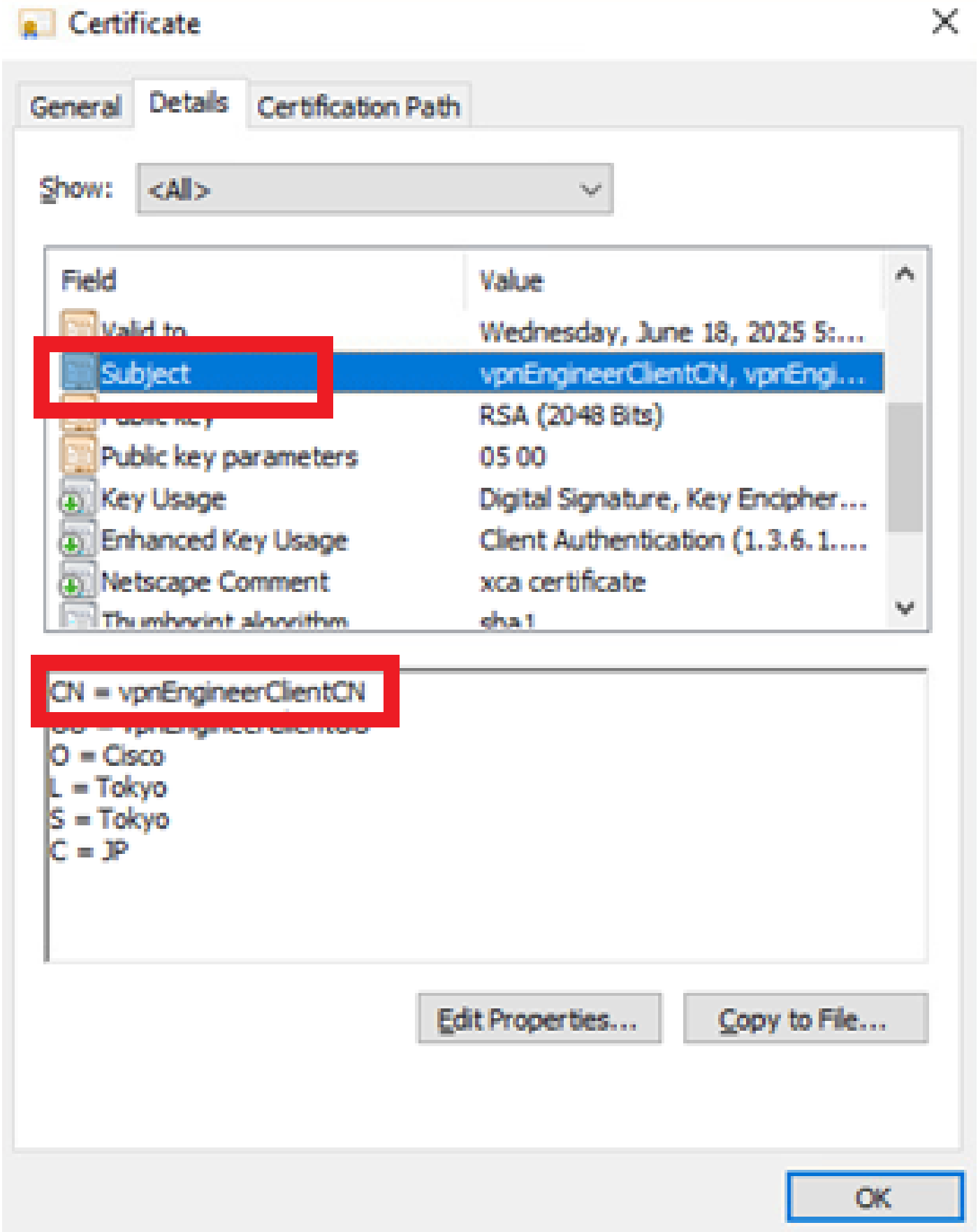
In Engineer VPN client, passare a Certificati - Utente corrente > Personale > Certificati, quindi controllare il certificato client utilizzato per l'autenticazione.



Conferma certificato per il client VPN del tecnico

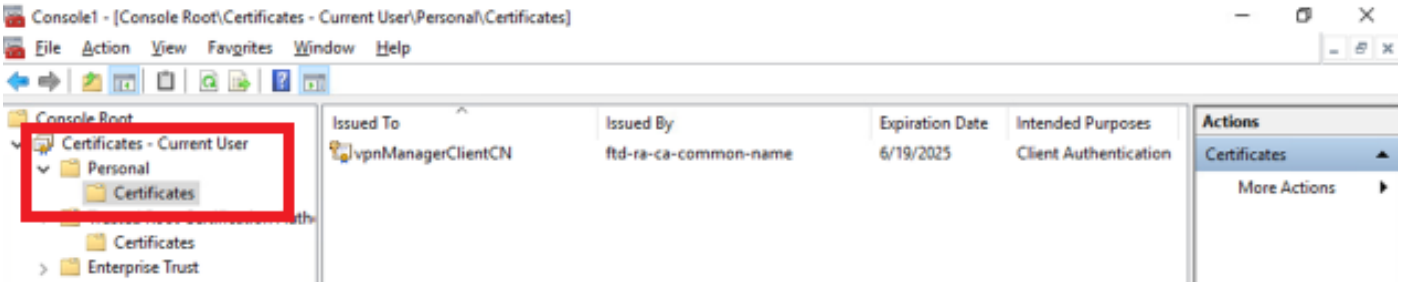
Fare doppio clic sul certificato client, passare a Dettagli, controllare i dettagli di Oggetto.

- Oggetto: CN = vpnEngineerClientCN



Dettagli del certificato client del tecnico

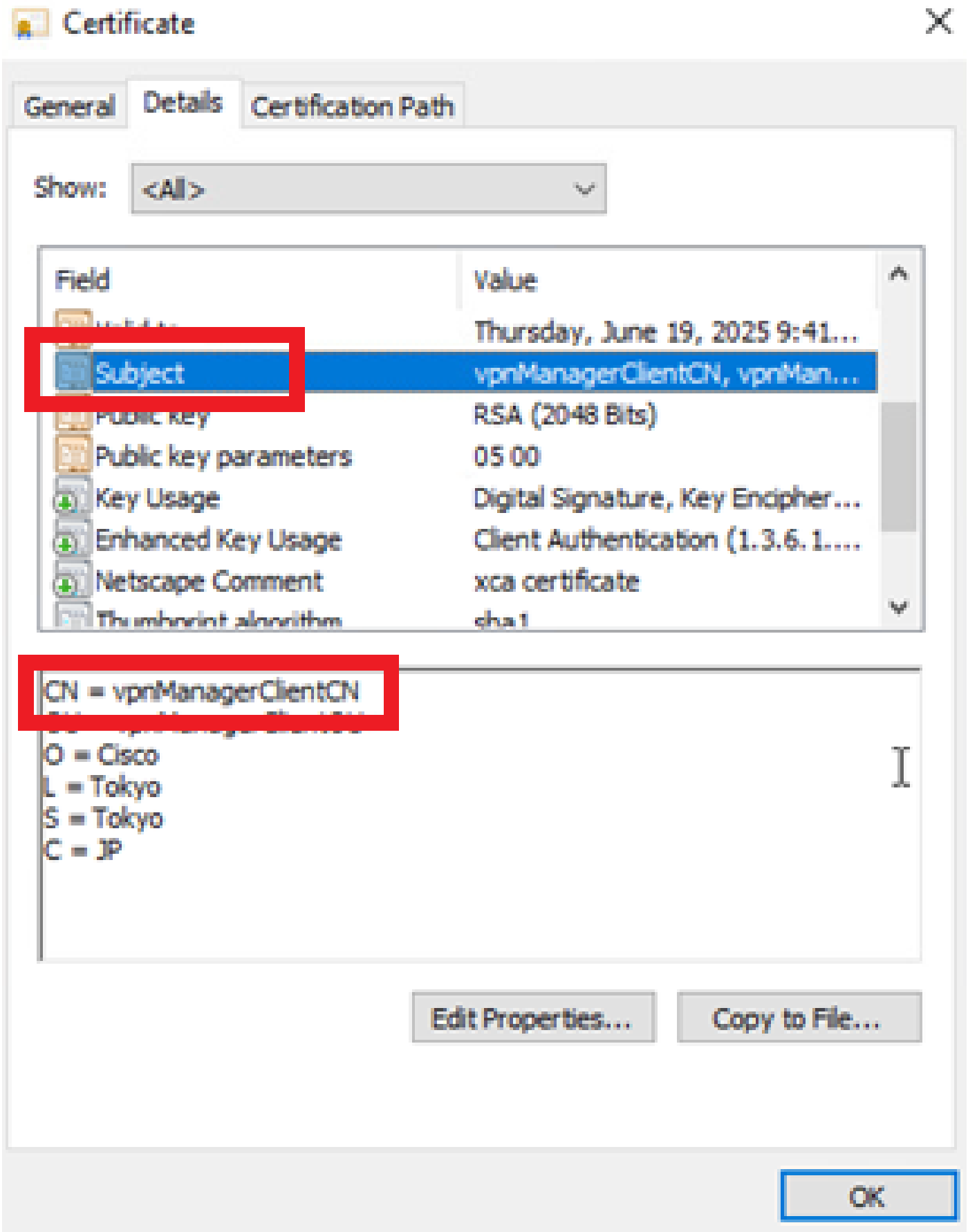
In Manager VPN Client, passare a Certificati - Utente corrente > Personale > Certificati, verificare il certificato client utilizzato per l'autenticazione.



Conferma certificato per client VPN di gestione

Fare doppio clic sul certificato client, passare a Dettagli, controllare i dettagli di Oggetto.

- Oggetto: CN = vpnManagerClientCN

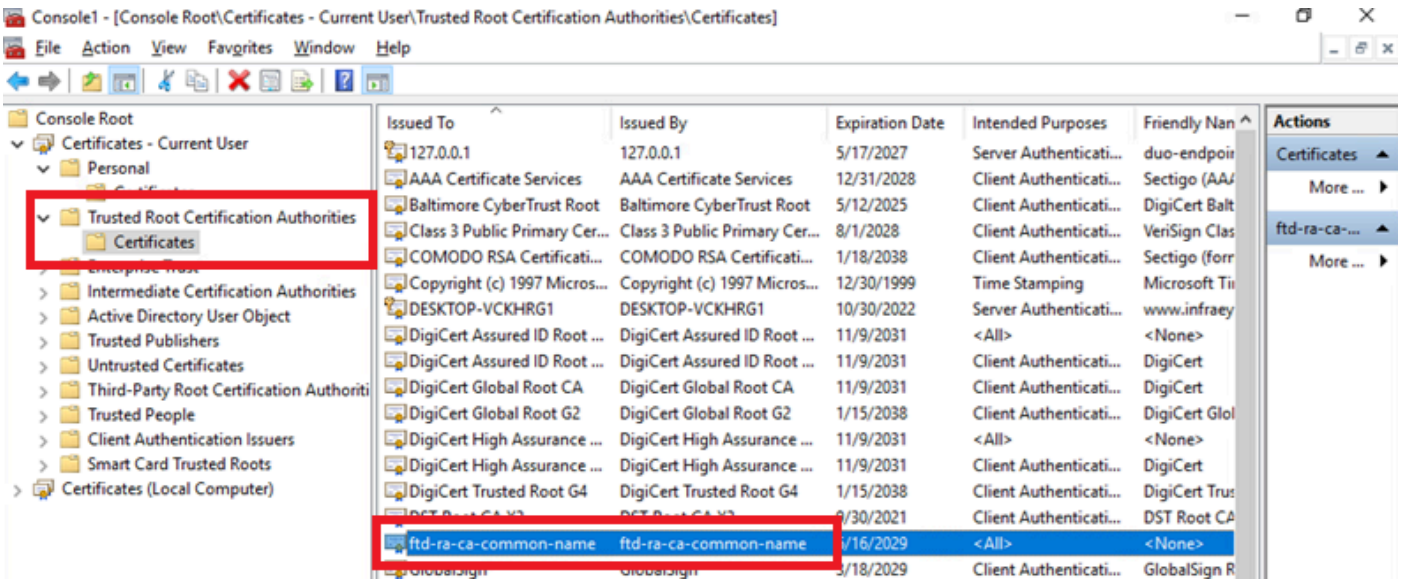


Dettagli del certificato client del gestore

Passaggio 3. Conferma CA

In Engineer VPN Client e Manager VPN Client, passare a Certificati - Utente corrente > Autorità di certificazione radice attendibili > Certificati, quindi controllare la CA utilizzata per l'autenticazione.

- Rilasciato da: ftd-ra-ca-common-name



Conferma CA

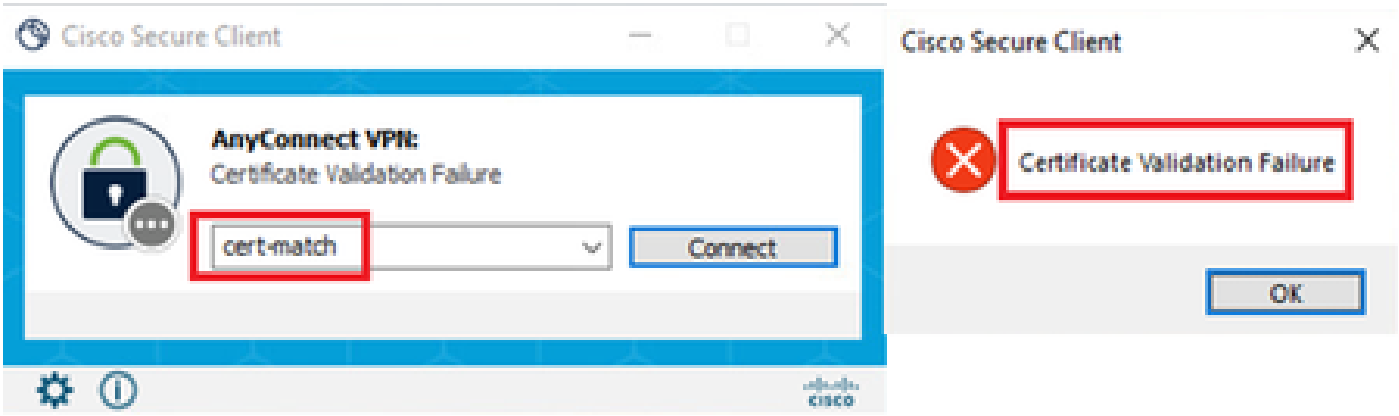
Verifica

Passaggio 1. Avvia connessione VPN

In Engineer VPN Client, avviare la connessione Cisco Secure Client. Non è necessario immettere il nome utente e la password. La VPN è stata connessa correttamente.

Connessione VPN riuscita per il client VPN del tecnico

Nel client VPN di gestione, avviare la connessione Cisco Secure Client. Connessione VPN non riuscita a causa di un errore di convalida del certificato.



Connessione VPN non riuscita per il client VPN di gestione

Passaggio 2. Conferma sessioni VPN nella CLI FTD

Eseguire show vpn-sessiondb detail anyconnect il comando nella CLI di FTD (Lina) per confermare le sessioni VPN del tecnico.

```
firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 32
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11
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 : 14718 Bytes Rx : 12919
Pkts Tx : 2 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn
Login Time : 05:42:03 UTC Tue Jul 2 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 000000000002000006683932b
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 32.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50170 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.17763
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7359 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
```

Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 32.2
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 50177
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7359 Bytes Rx : 12919
Pkts Tx : 1 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Risoluzione dei problemi

Per informazioni sull'autenticazione VPN, vedere il syslog di debug del motore Lina e il file DART nel computer Windows.

Questo è un esempio di log di debug nel motore Lina durante la connessione VPN da un client di progettazione.

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn
Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClie
Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN
Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 sessi

Informazioni correlate

Configurazione del servizio di gestione integrata di FDM per Firepower 2100

Configura VPN ad accesso remoto su FTD Gestito da FDM

Configurazione e verifica di Syslog in Gestione periferiche di Firepower

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).