Configurazione di AAA e Cert Auth per Secure Client su FTD tramite FDM

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Secure Client over SSL su FTD gestito da FDM con AAA e autenticazione dei certificati.

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

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

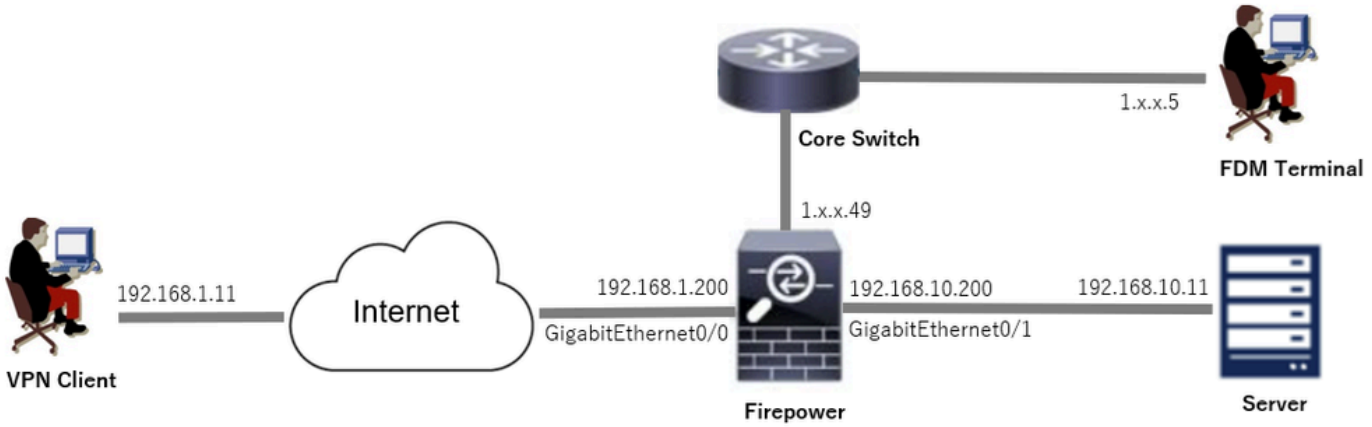
Firepower Device Manager (FDM) è un'interfaccia di gestione semplificata e basata su Web utilizzata per la gestione dei dispositivi Cisco Firepower Threat Defense (FTD). Firepower Device Manager consente agli amministratori di rete di configurare e gestire i dispositivi FTD senza utilizzare il più complesso Firepower Management Center (FMC). FDM fornisce un'interfaccia utente intuitiva per le operazioni di base, ad esempio la configurazione di interfacce di rete, aree di sicurezza, policy di controllo dell'accesso e VPN, nonché per il monitoraggio delle prestazioni dei dispositivi e degli eventi di sicurezza. È adatto per installazioni di piccole e medie dimensioni in cui è necessaria una gestione semplificata.
Questo documento descrive come integrare nomi utente precompilati con Cisco Secure Client su FTD gestito da FDM.
Se si gestisce FTD con FMC, consultare la guida Configure AAA and Cert Auth for Secure Client on FTD via FMC.

Catena di certificati con il nome comune di ogni certificato utilizzato nel documento.

- CA: ftd-ra-ca-nome comune
- Certificato client: sslVPNClientCN
- 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

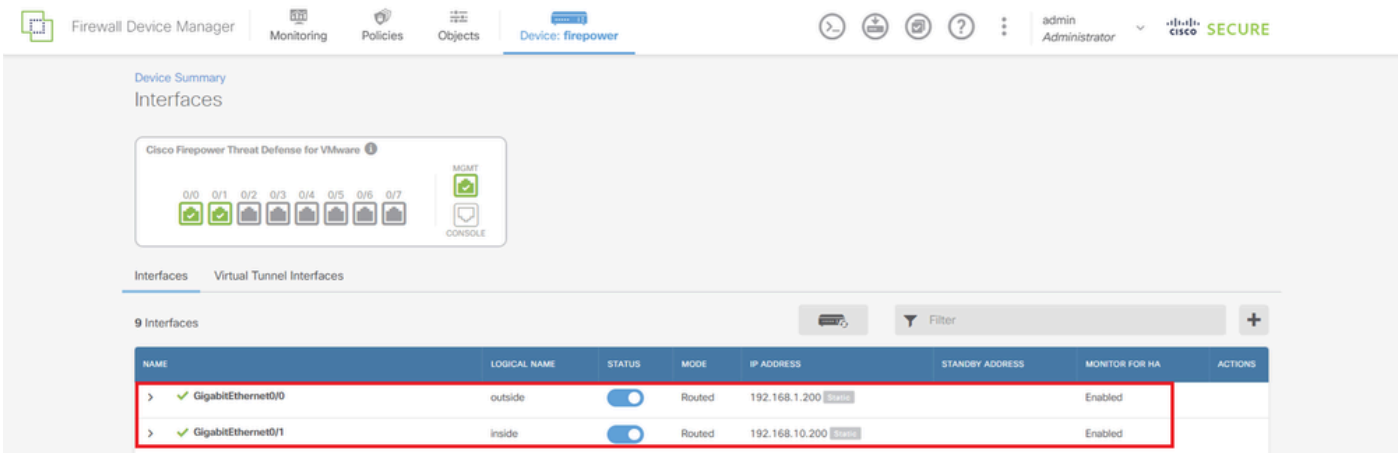
Selezionare Dispositivo > Interfacce > Visualizza tutte le interfacce, configurare l'interfaccia interna ed esterna per FTD nella scheda Interfacce.

Per Gigabit Ethernet0/0,

- Nome: esterno
- Indirizzo IP: 192.168.1.200/24

Per Gigabit Ethernet0/1,

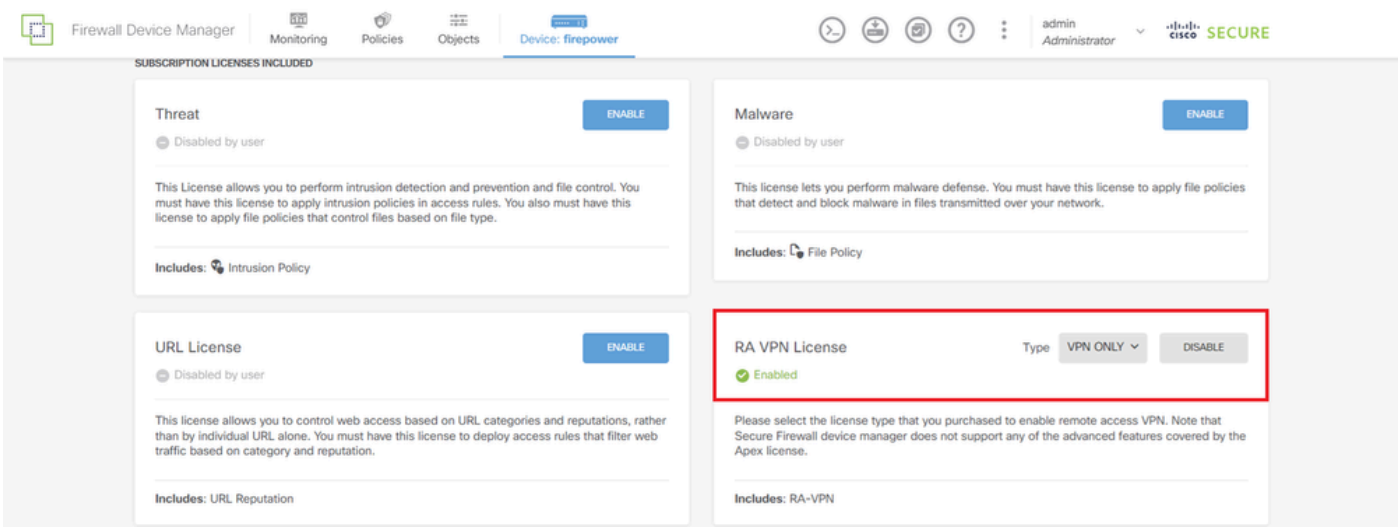
- Nome: interno
- Indirizzo IP: 192.168.10.200/24



Interfaccia FTD

Passaggio 2. Conferma licenza Cisco Secure Client

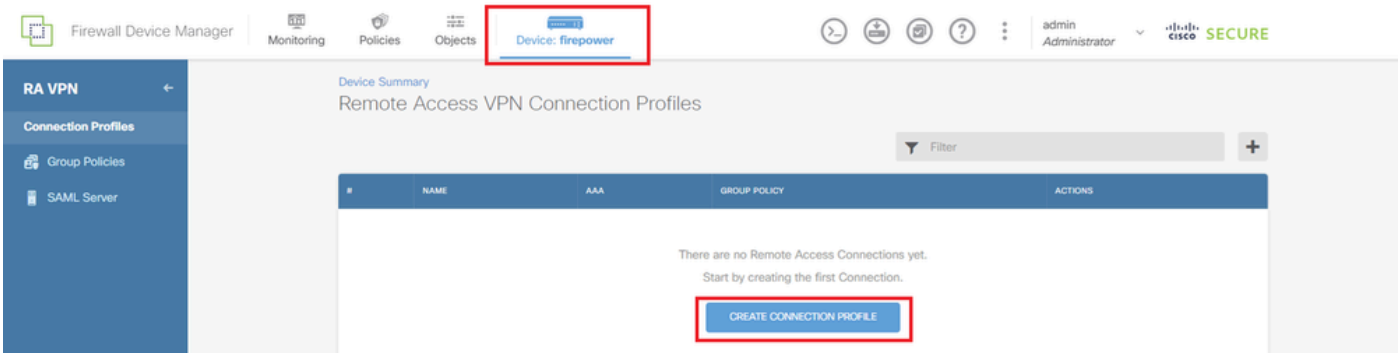
Selezionare Device > Smart License > View Configuration, quindi confermare la licenza Cisco Secure Client in RA VPN Licenseitem.



Licenza Secure Client

Passaggio 3. Aggiungi profilo di connessione VPN di Accesso remoto

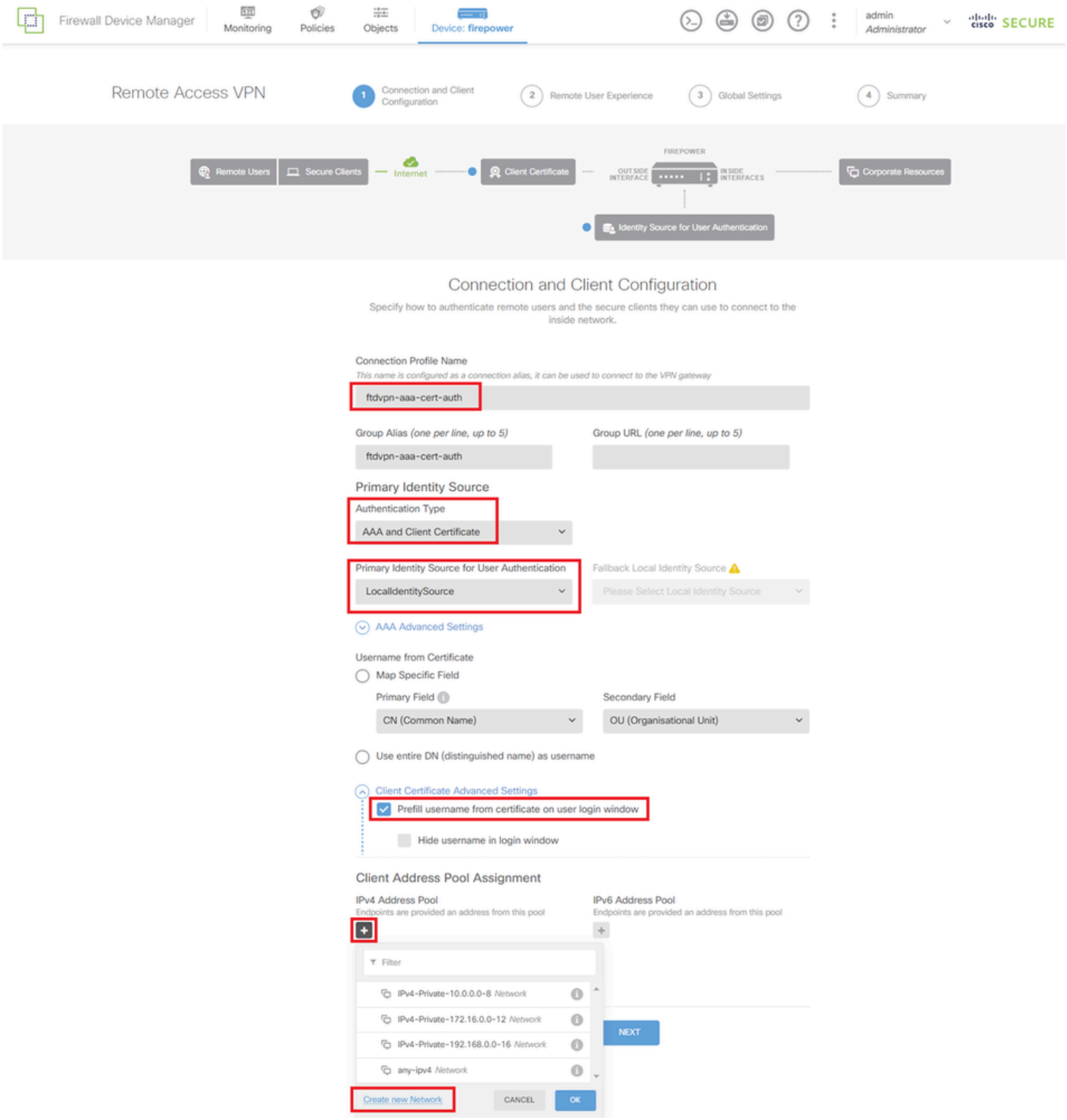
Selezionare Dispositivo > VPN ad accesso remoto > Visualizza configurazione, quindi fare clic sul pulsante CREA PROFILO DI CONNESSIONE.



Aggiungi profilo di connessione VPN di Accesso remoto

Immettere le informazioni necessarie per il profilo di connessione e fare clic sul pulsante Crea nuova rete nell'elemento Pool di indirizzi IPv4.

- Nome profilo connessione: ftdvpn-aaa-cert-auth
- Tipo di autenticazione: AAA e certificato client
- Origine identità primaria per autenticazione utente: LocalIdentitySource
- Impostazioni avanzate certificato client: Precompila il nome utente dal certificato nella finestra di accesso dell'utente

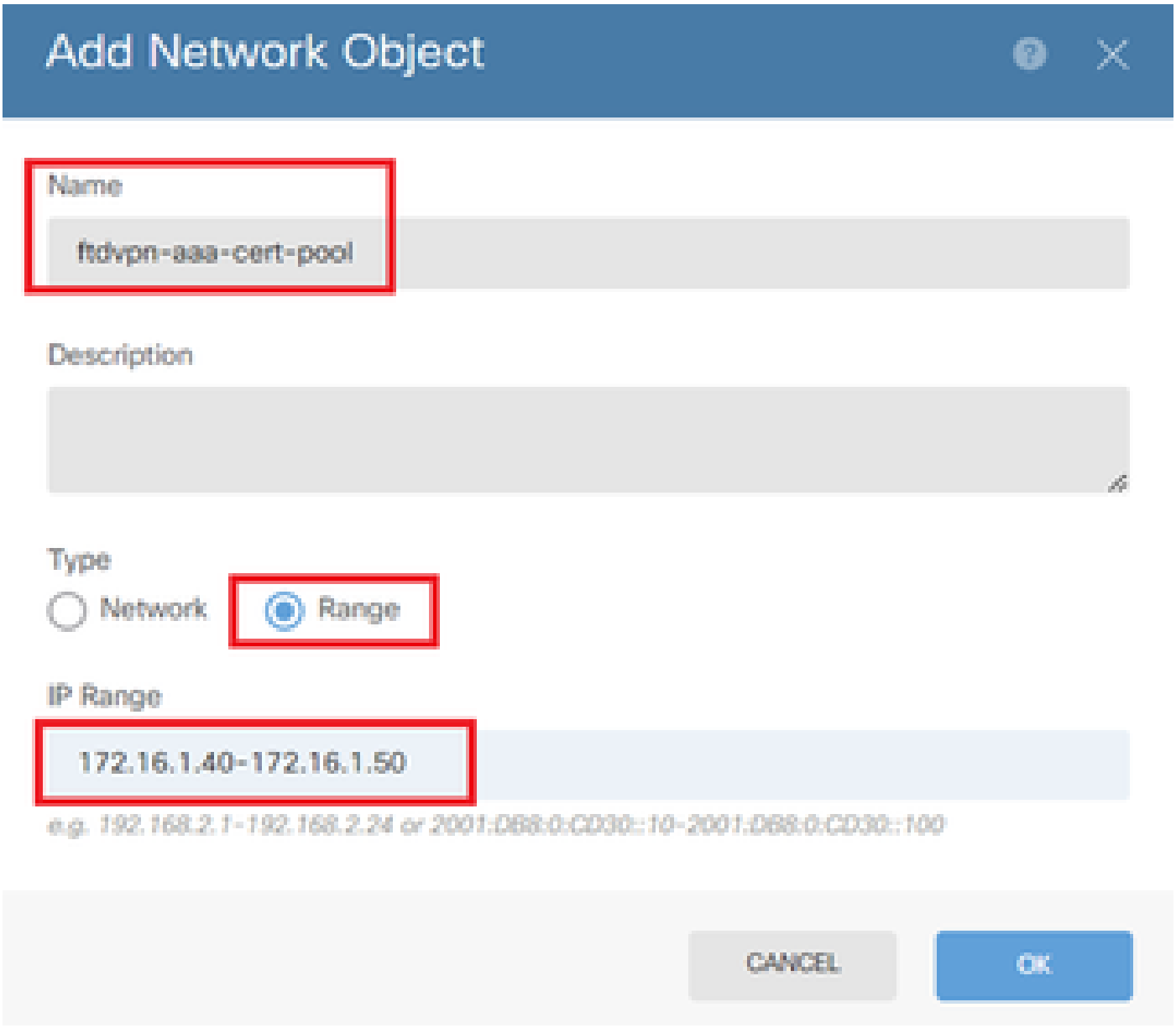


Dettagli del profilo di connessione VPN

Passaggio 4. Aggiungi pool di indirizzi per profilo di connessione

Immettere le informazioni necessarie per aggiungere un nuovo pool di indirizzi IPv4. Selezionare il nuovo pool di indirizzi IPv4 aggiunto per il profilo di connessione e fare clic sul pulsante Avanti.

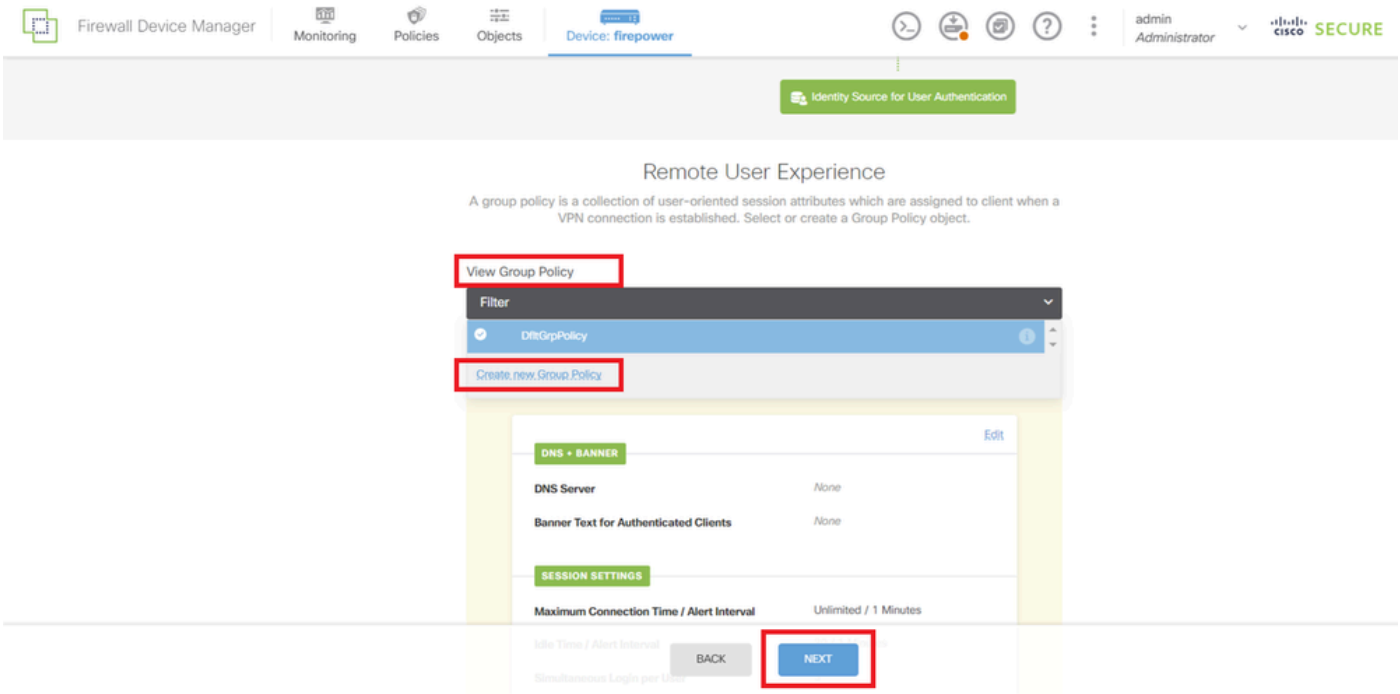
- Nome: ftdvpn-aaa-cert-pool
- Tipo: intervallo
- Range IP: 172.16.1.40-172.16.1.50



Dettagli del pool di indirizzi IPv4

Passaggio 5. Aggiungi Criteri di gruppo per il profilo di connessione

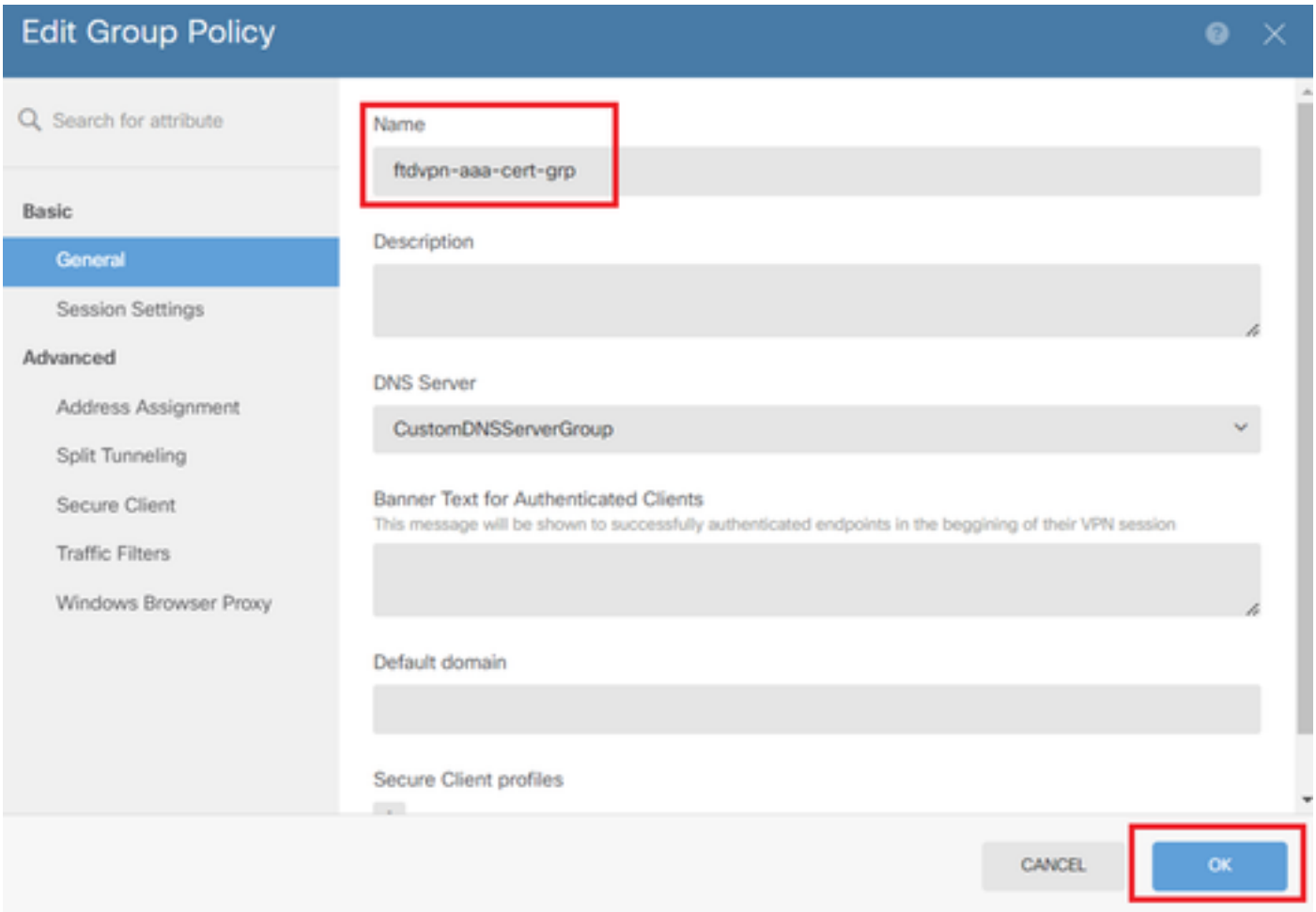
Fare clic su Crea nuovi Criteri di gruppo nell'elemento Visualizza Criteri di gruppo.



Aggiungi Criteri di gruppo

Immettere le informazioni necessarie per aggiungere un nuovo criterio di gruppo e fare clic su OK pulsante. Selezionare nuovi criteri di gruppo aggiunti per il profilo di connessione.

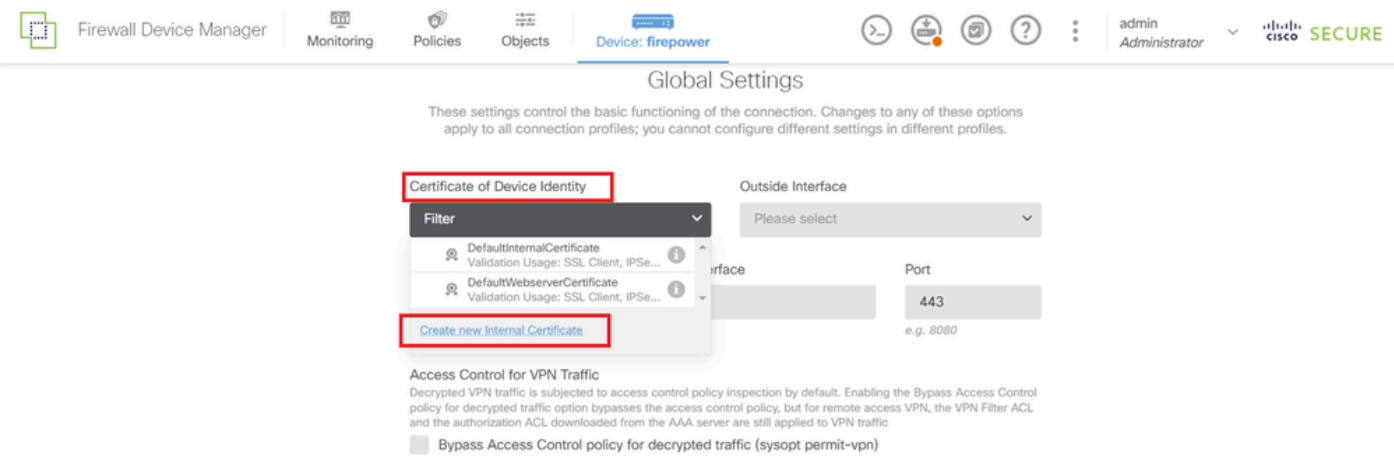
- Nome: ftdvpn-aaa-cert-grp



Dettagli di Criteri di gruppo

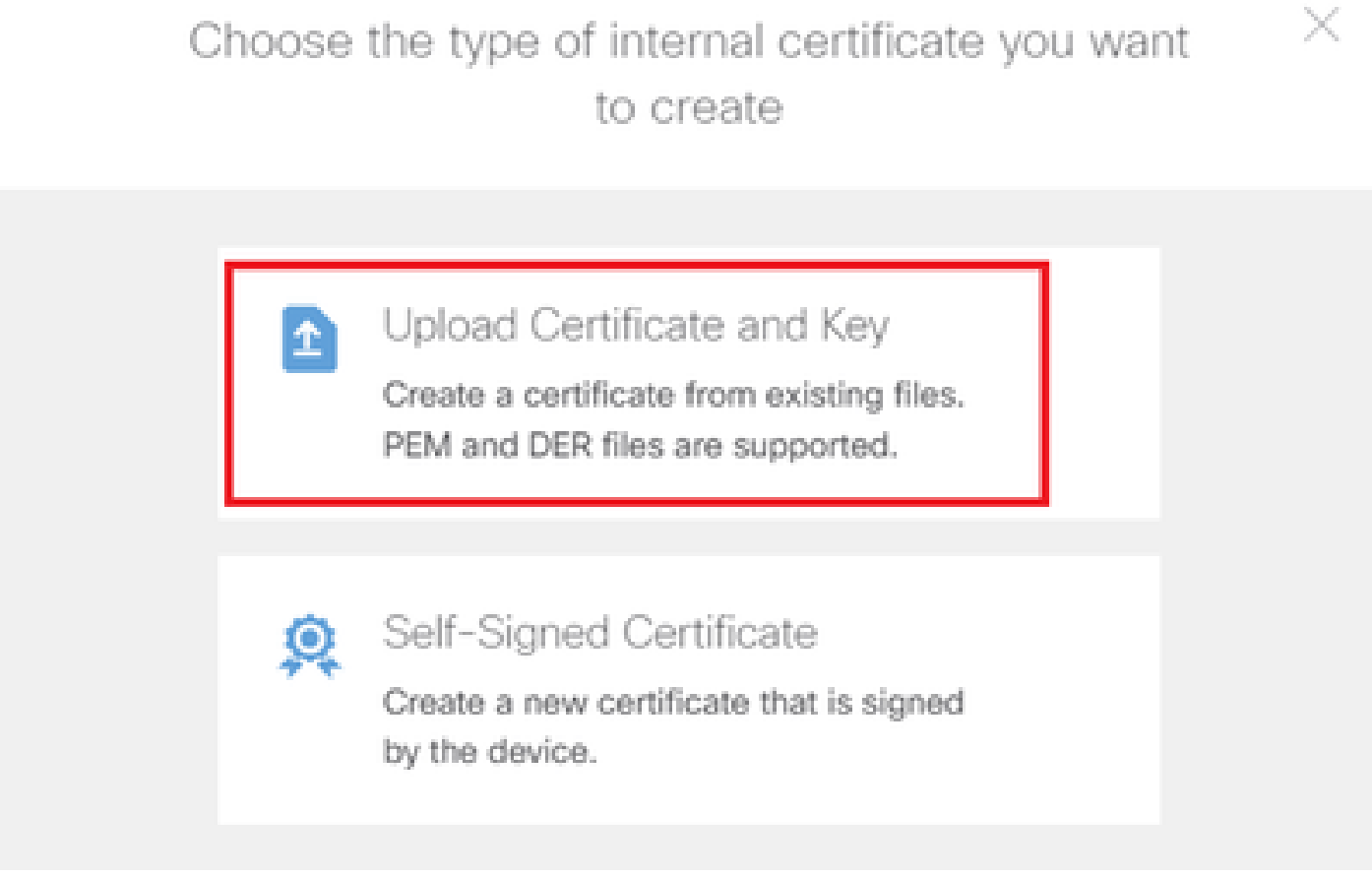
Passaggio 6. Configura certificato di identità del dispositivo e interfaccia esterna per il profilo di connessione

Fare clic su Crea nuovo certificato interno nella voce Certificato di identità del dispositivo.



Aggiungi certificato interno

Fare clic su Carica certificato e chiave.

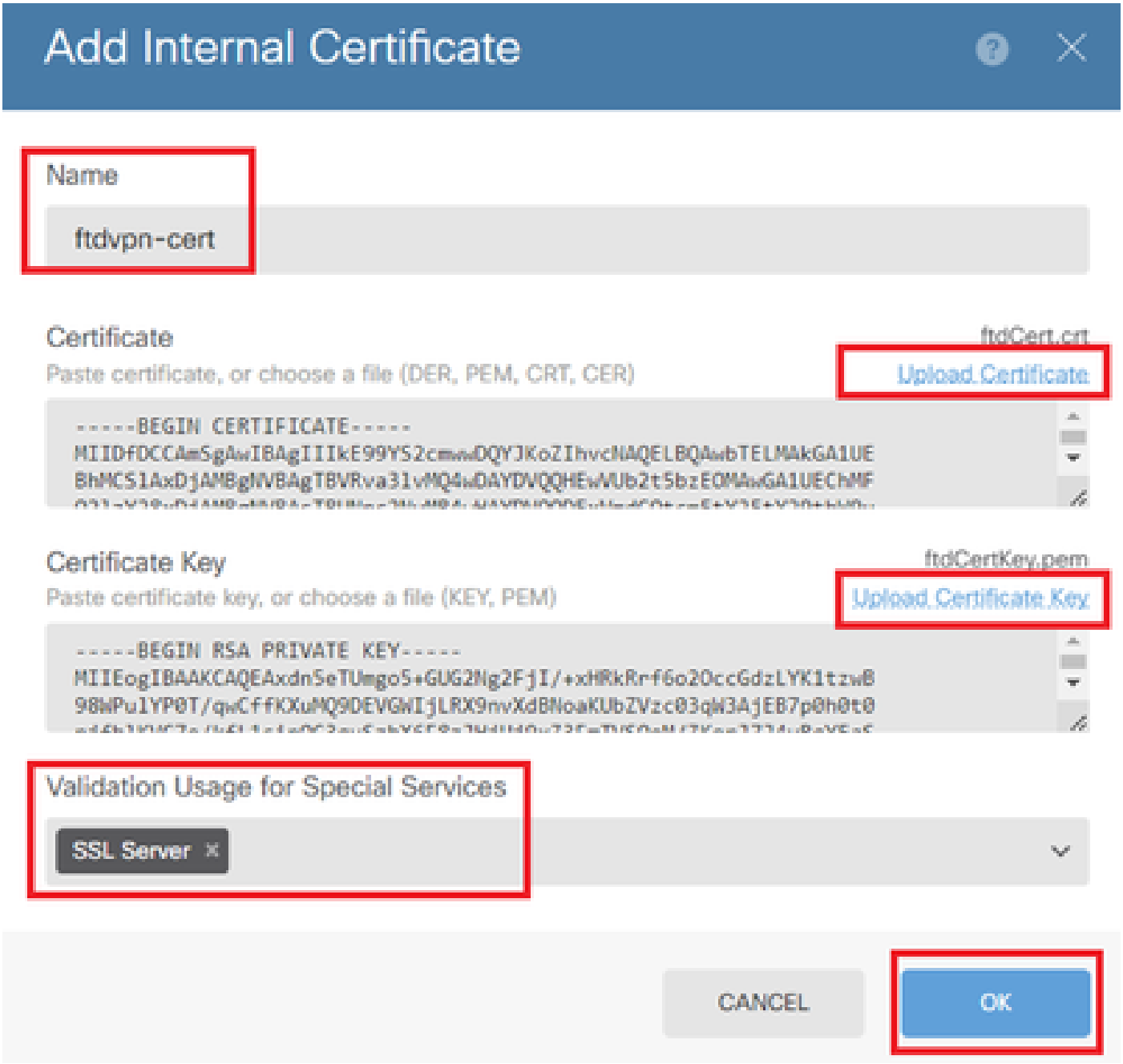


Carica certificato e chiave

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.

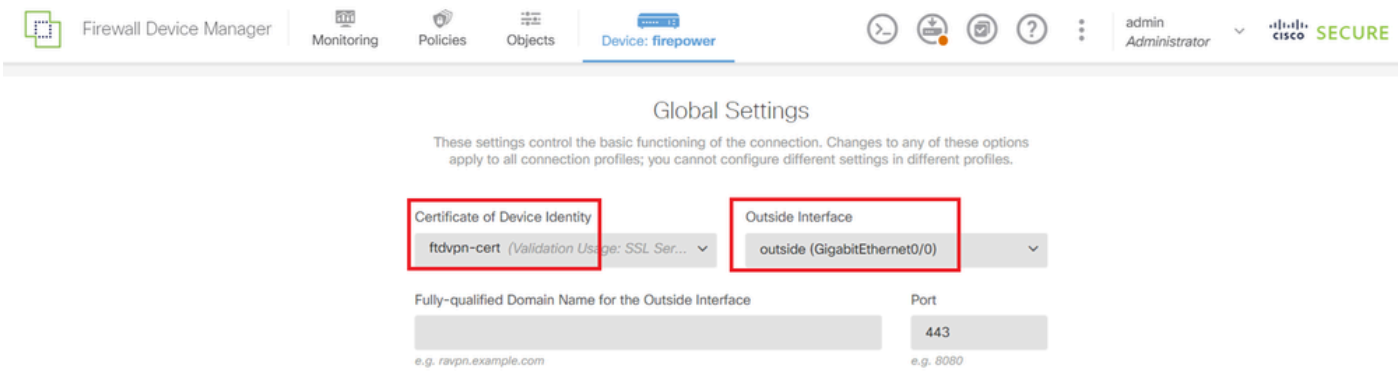
- Nome: ftdvpn-cert
- Utilizzo convalida per servizi speciali: server SSL



Dettagli del certificato interno

Selezionare Certificato di identità del dispositivo e Interfaccia esterna per la connessione VPN.

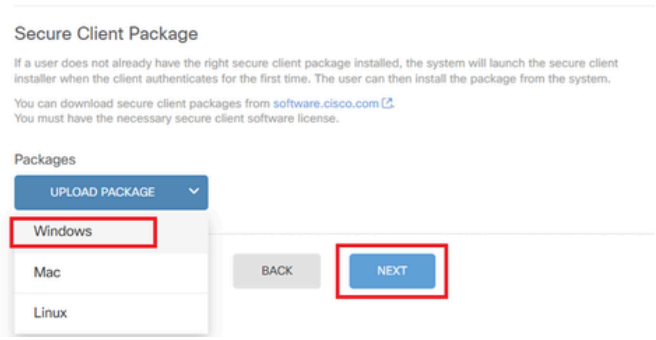
- Certificato di identità del dispositivo: ftdvpn-cert
- Interfaccia esterna: esterna (Gigabit Ethernet0/0)



Dettagli delle impostazioni globali

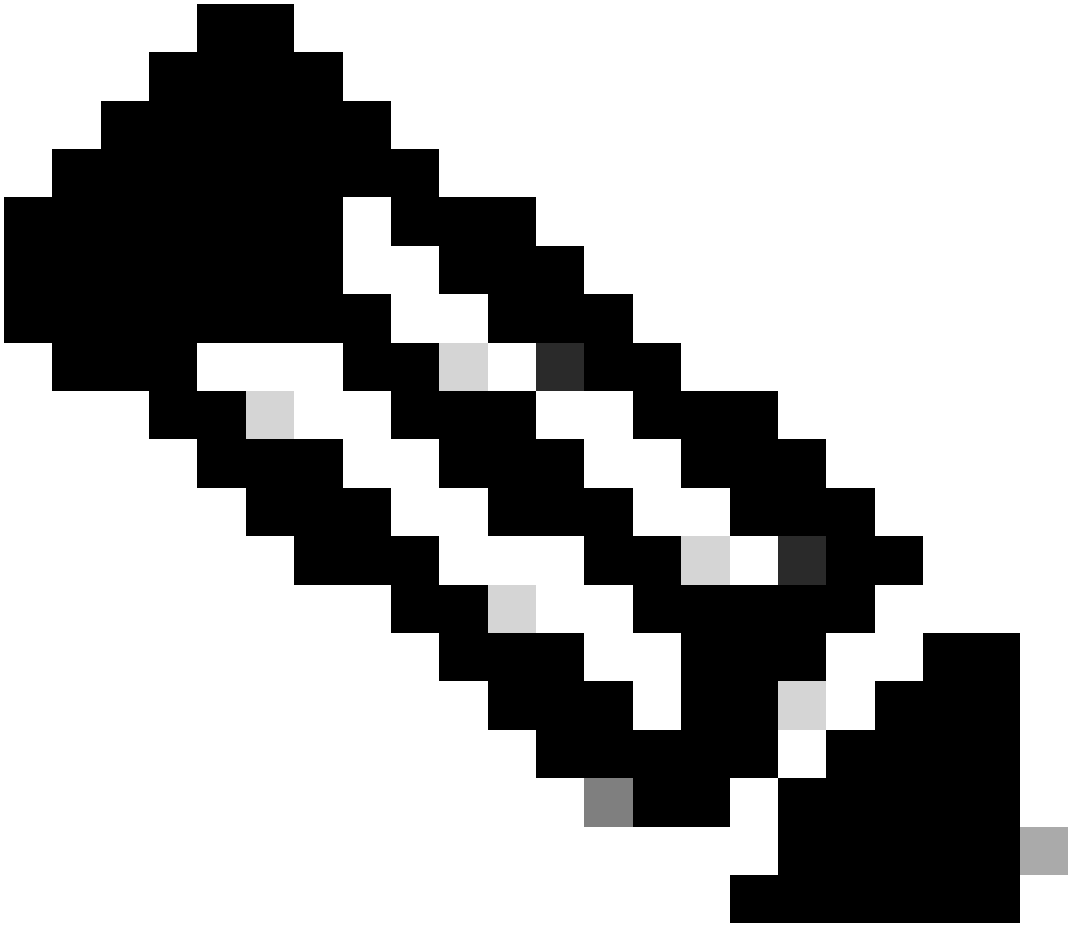
Passaggio 7. Configura immagine client sicura per il profilo di connessione

Seleziona Windows nell'elemento Pacchetti

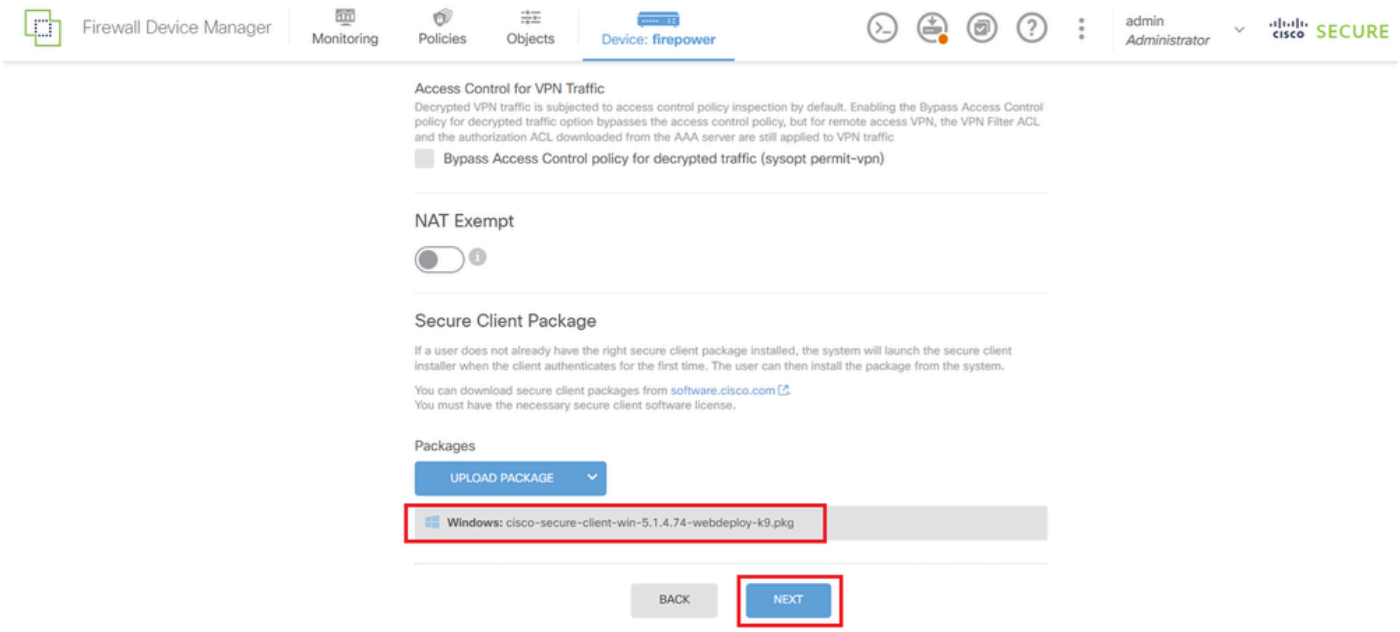


Carica pacchetto immagine client sicura

Caricare il file di immagine client protetta dal computer locale e fare clic su NextButton.



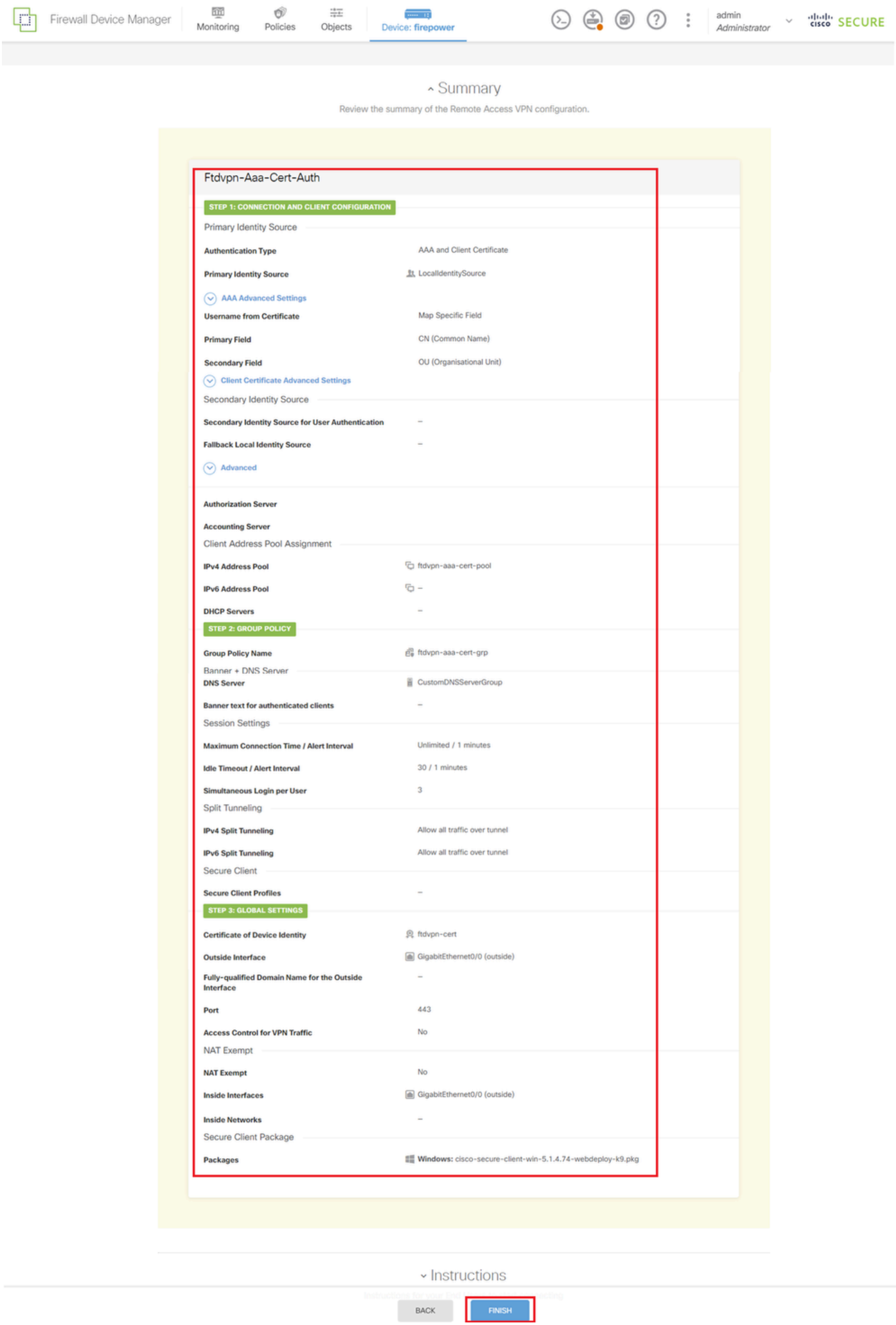
Nota: la funzione NAT Exempt (Esente NAT) è disabilitata in questo documento. Per impostazione predefinita, l'opzione Ignora il criterio di controllo di accesso per il traffico decrittografato (syspot allow-vpn) è disabilitata, quindi il traffico VPN decrittografato viene sottoposto all'ispezione dei criteri di controllo di accesso.



Seleziona pacchetto immagine client sicura

Passaggio 8. Conferma riepilogo per il profilo di connessione

Confermare le informazioni immesse per la connessione VPN e fare clic su FINISHbutton.



Conferma impostazioni per profilo connessione

```
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
!
interface GigabitEthernet0/1
speed auto
nameif inside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.10.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50

// Defines a local user
username sslVPNClientCN password ***** pbkdf2

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
enrollment terminal
keypair ftdvpn-cert
validation-usage ssl-server
crl configure

// Server Certificate
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
......
quit

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client ssl-server
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 enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
dns-server value 64.x.x.245 64.x.x.184
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 none
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

// Configures the tunnel-group to use the aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
authentication-server-group LOCAL
secondary-authentication-server-group none
no accounting-server-group
default-group-policy ftdvpn-aaa-cert-grp
username-from-certificate CN OU
secondary-username-from-certificate CN OU
authentication-attr-from-server primary
authenticated-session-username primary
username-from-certificate-choice second-certificate
```

```
secondary-username-from-certificate-choice second-certificate
// These settings are displayed in the 'show run all' command output. End
tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes
authentication aaa certificate
pre-fill-username client
group-alias ftdvpn-aaa-cert-auth enable
```

Conferma in client VPN

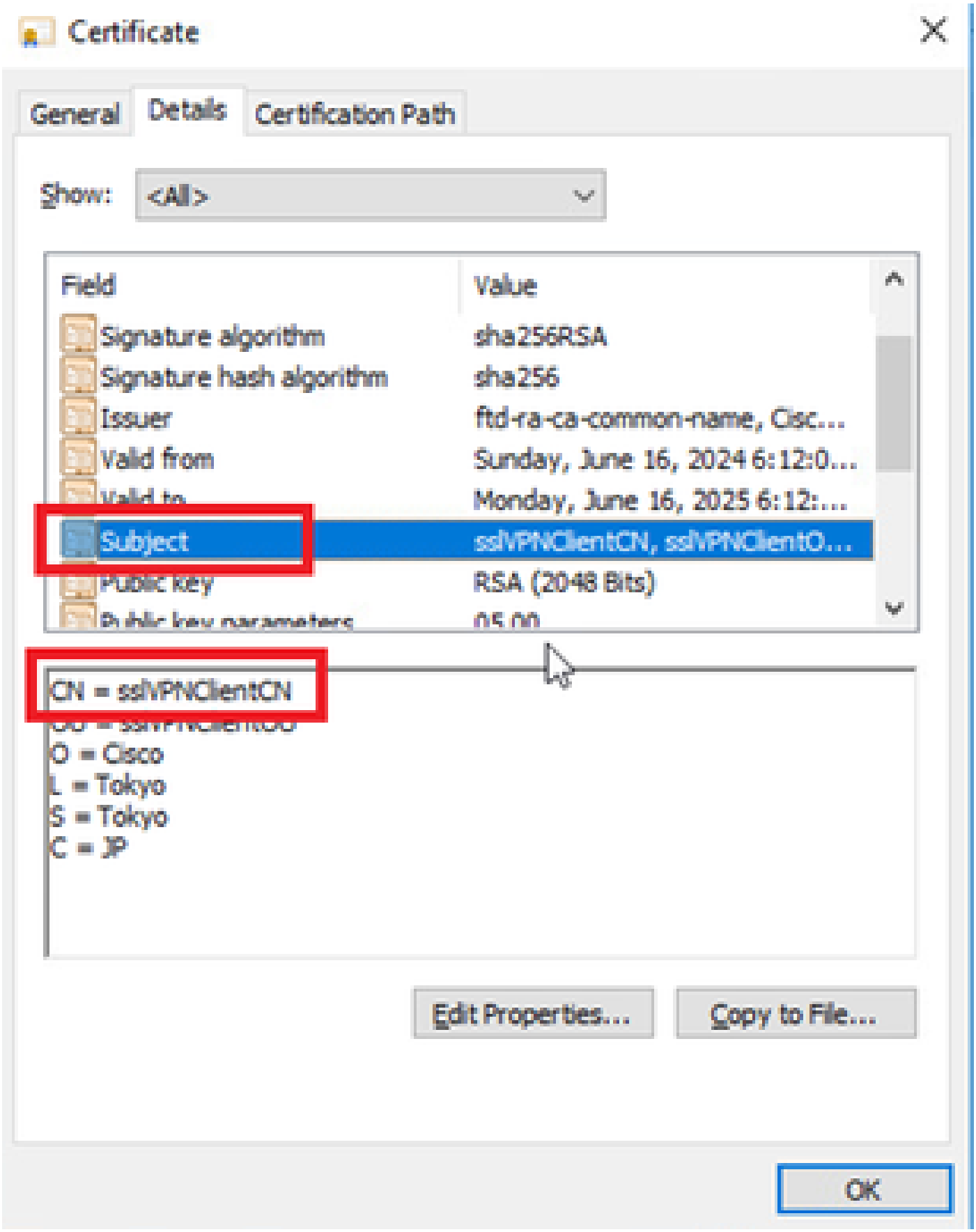
Passaggio 1. Conferma certificato client

Passare a Certificati - Utente corrente > Personale > Certificati, verificare il certificato client utilizzato per l'autenticazione.

Conferma certificato client

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

- Oggetto: CN = sslVPNClientCN



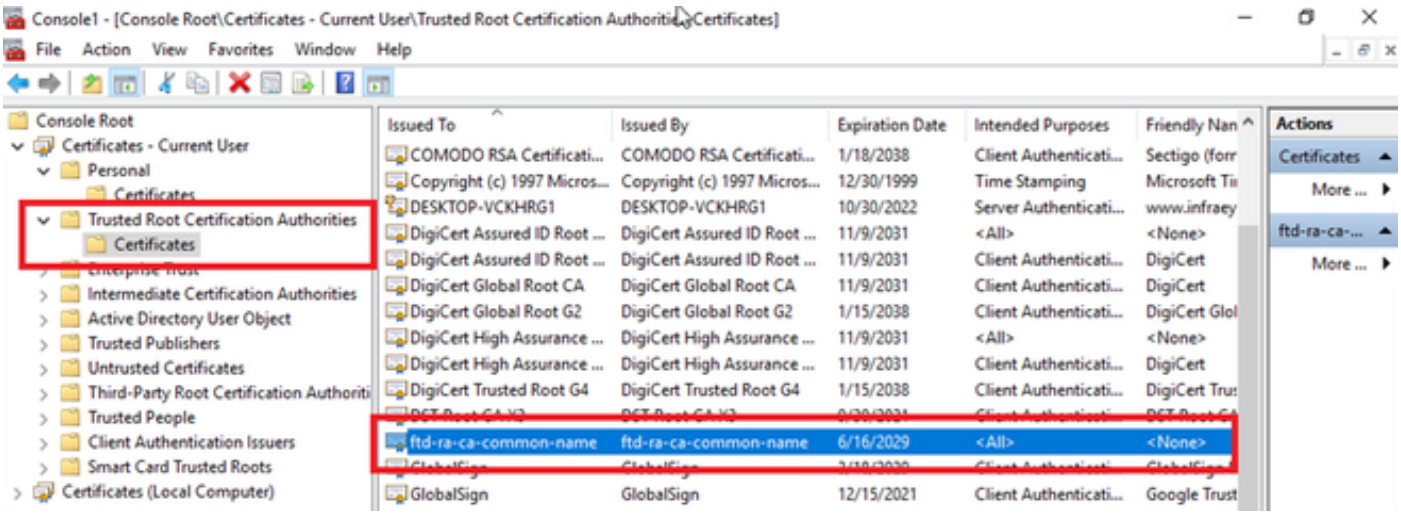
Dettagli del certificato client

Passaggio 2. Conferma CA

Passare a Certificati - Utente corrente > Autorità di certificazione radice attendibili > Certificati,

quindi verificare la CA utilizzata per l'autenticazione.

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

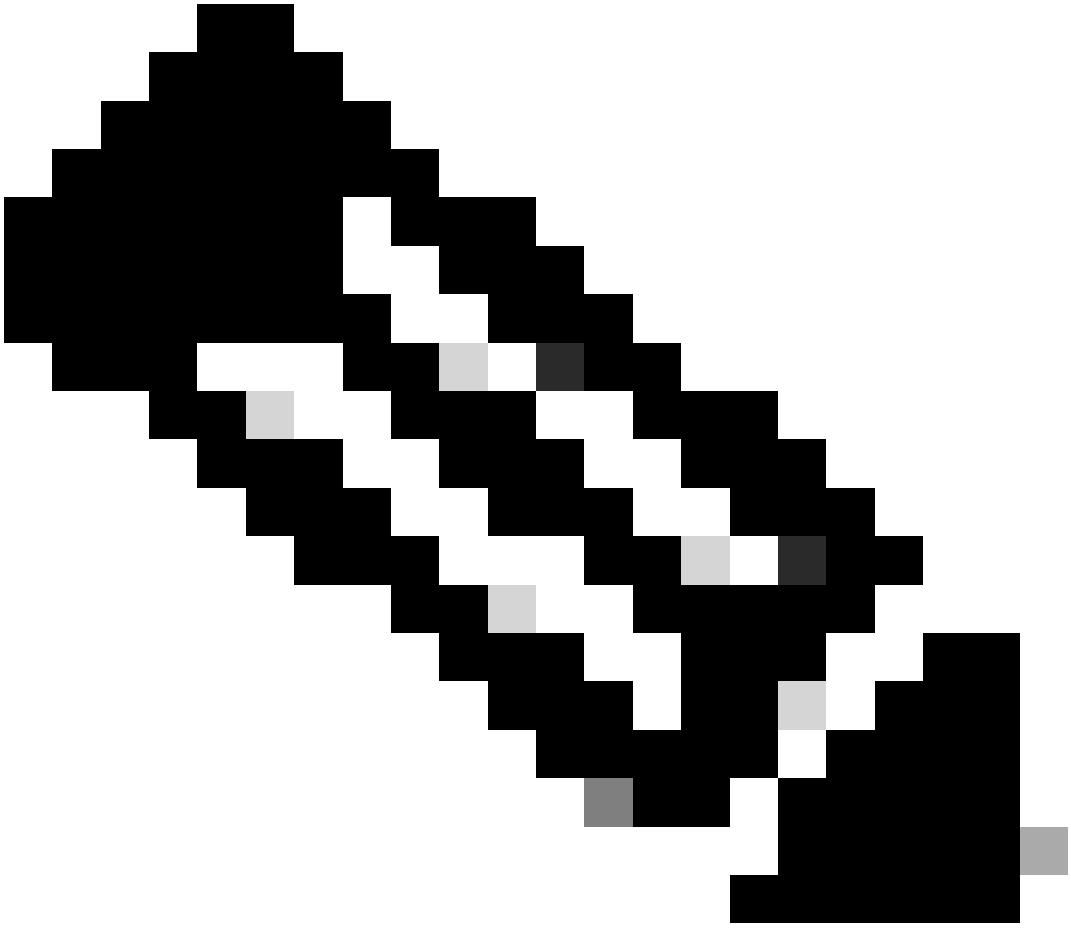


Conferma CA

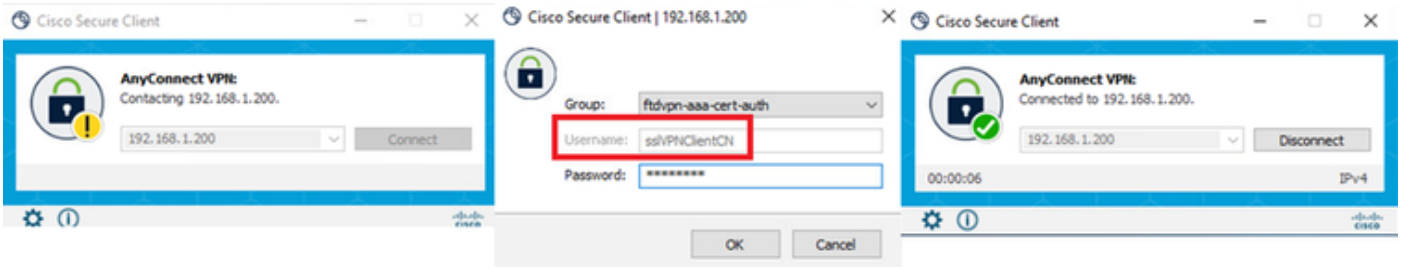
Verifica

Passaggio 1. Avvia connessione VPN

Sull'endpoint, avviare la connessione Cisco Secure Client. Il nome utente viene estratto dal certificato client. È necessario immettere la password per l'autenticazione VPN.



Nota: il nome utente viene estratto dal campo Nome comune (CN) del certificato client in questo documento.



Avvia connessione VPN

Passaggio 2. Conferma sessione VPN nella CLI FTD

Eseguireshow vpn-sessiondb detail anyconnect il comando nella CLI FTD (Lina) per confermare la sessione VPN.

```
firepower# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 4
Assigned IP : 172.16.1.40 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 : 29072 Bytes Rx : 44412
Pkts Tx : 10 Pkts Rx : 442
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 11:47:42 UTC Sat Jun 29 2024
Duration : 1h:09m:30s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 000000000004000667ff45e
Security Grp : none Tunnel Zone : 0

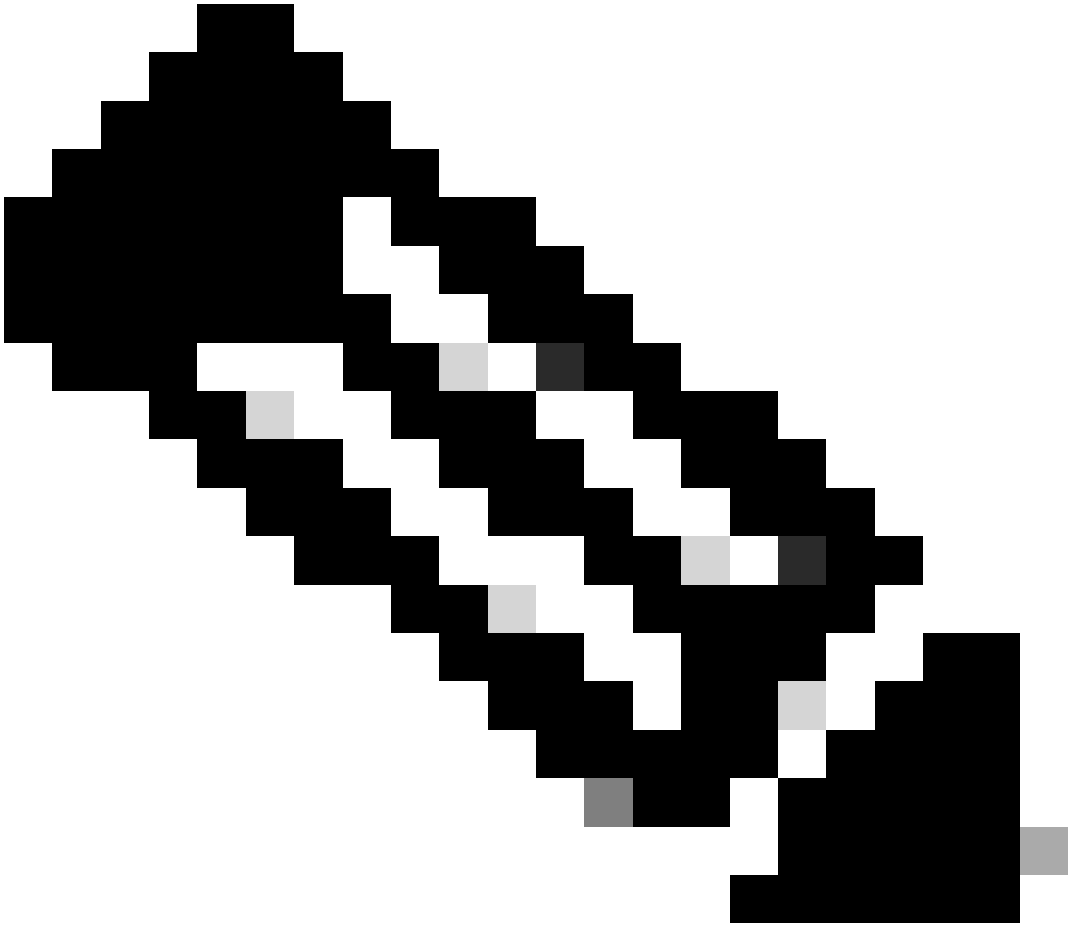
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 4.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 49779 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 7 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 : 14356 Bytes Rx : 0
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

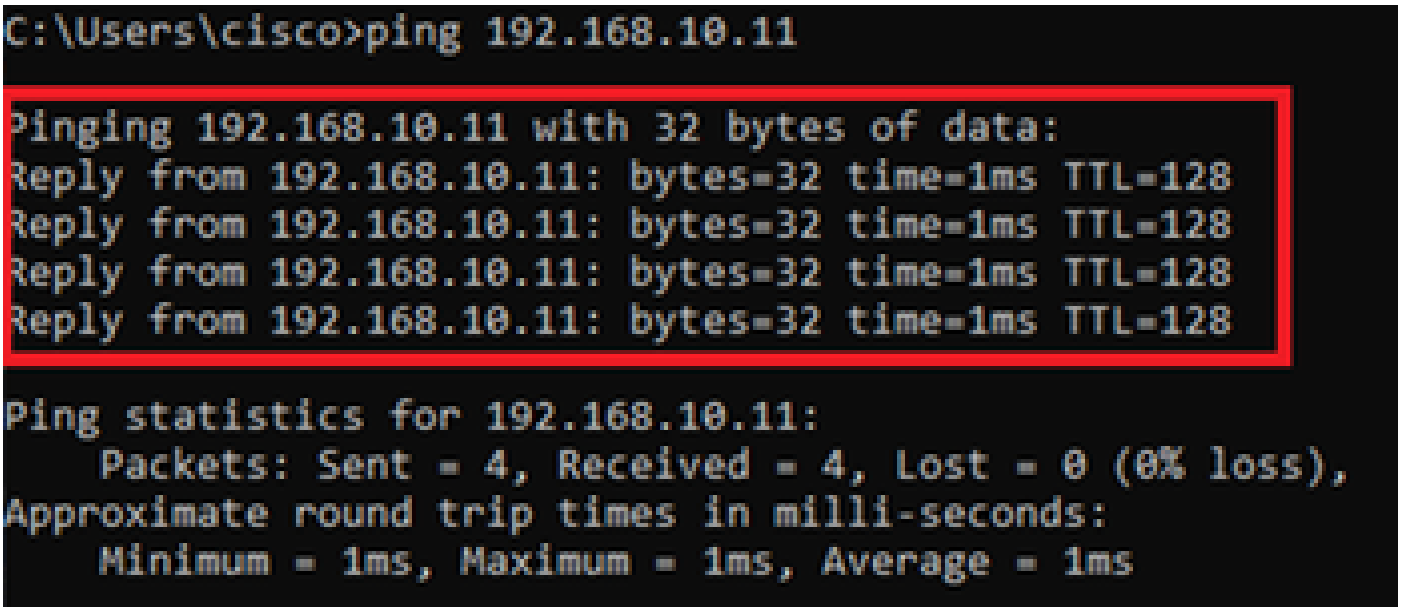
SSL-Tunnel:
Tunnel ID : 4.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 49788
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7178 Bytes Rx : 10358
Pkts Tx : 1 Pkts Rx : 118
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Passaggio 3. Conferma comunicazione con il server

Eseguire il ping tra il client VPN e il server e verificare che la comunicazione tra il client VPN e il server sia riuscita.



Nota: poiché l'opzione Ignora i criteri di controllo di accesso per il traffico decrittografato (syspot allow-vpn) è disabilitata nel passaggio 7, è necessario creare regole di controllo di accesso che consentano al pool di indirizzi IPv4 di accedere al server.



Ping riuscito

capture in interface inside real-timeEseguire il comando nella CLI FTD (Lina) per confermare l'acquisizione dei pacchetti.

firepower# capture in interface inside real-time

Warning: using this option with a slow console connection may
result in an excessive amount of non-displayed packets
due to performance limitations.

Use ctrl-c to terminate real-time capture

1: 12:03:26.626691 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 12:03:26.627134 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 12:03:27.634641 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 12:03:27.635144 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 12:03:28.650189 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 12:03:28.650601 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 12:03:29.665813 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 12:03:29.666332 192.168.10.11 > 172.16.1.40 icmp: echo reply

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.

// Certificate Authentication
Jun 29 2024 11:29:37: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 29 2024 11:29:37: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
Jun 29 2024 11:29:37: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=sslVPNClientCN

// Extract username from the CN (Common Name) field

Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 3]
Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 3]

// AAA Authentication
Jun 29 2024 11:29:53: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 29 2024 11:29:53: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 29 2024 11:29:53: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN

Questi debug possono essere eseguiti dalla CLI diagnostica dell'FTD, che fornisce le informazioni da usare per risolvere i problemi relativi alla configurazione.

- debug crypto ca 14
- debug webvpn anyconnect 255
- debug crypto ike-common 255

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).