Configurazione di Secure Client IKEv2/ASA in ASDM con AAA & Cert Auth

Sommario

Introduzione

In questo documento viene descritto come configurare un client sicuro su IKEv2 su un'appliance ASA usando ASDM con AAA e autenticazione dei certificati.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco Identity Services Engine (ISE)
- Configurazione di Cisco Adaptive Security Virtual Appliance (ASAv)
- Configurazione di Cisco Adaptive Security Device Manager (ASDM)
- Flusso di autenticazione VPN

Componenti usati

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

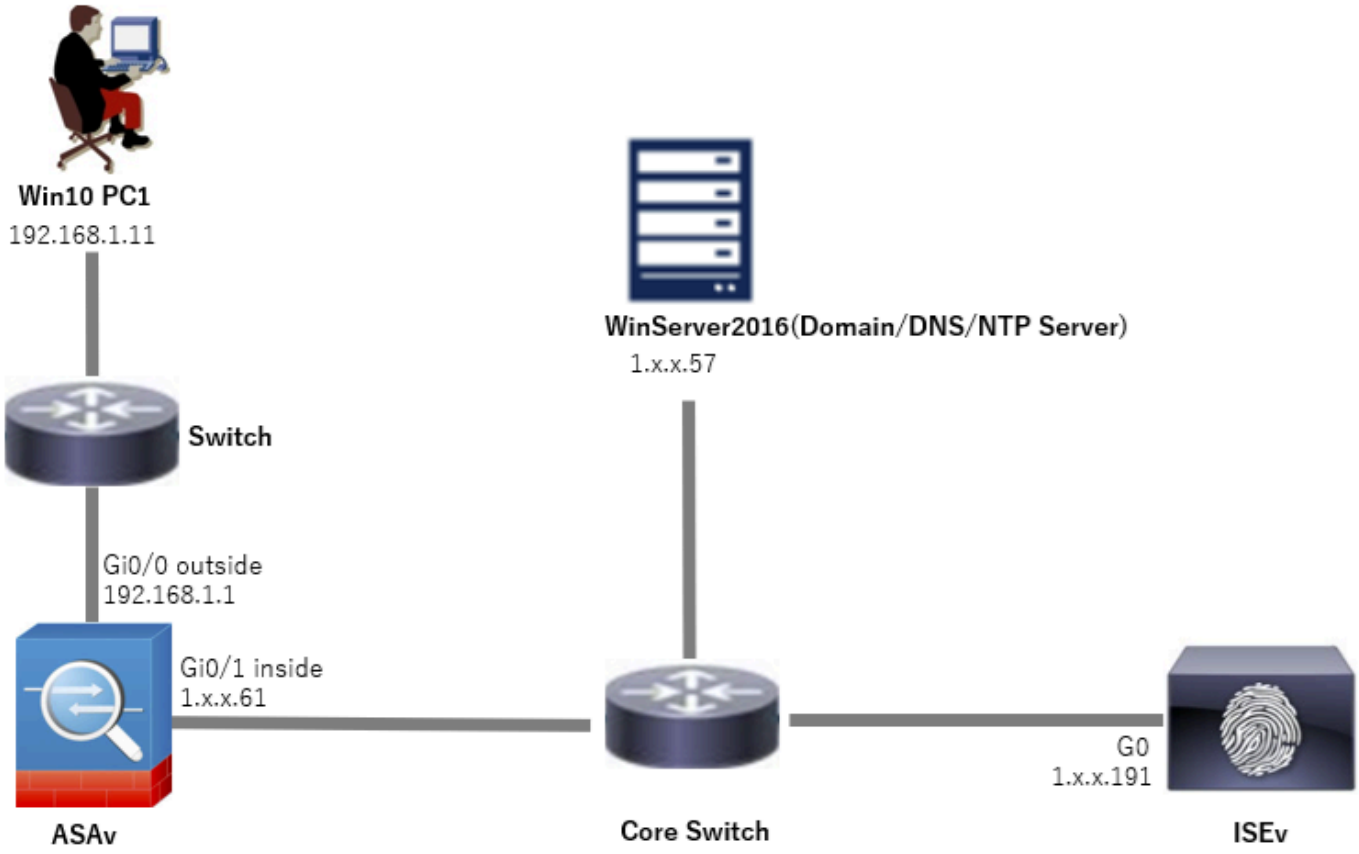
- Patch 1 di Identity Services Engine Virtual 3.3
- Adaptive Security Virtual Appliance 9.20(2)21
- Adaptive Security Device Manager 7.20(2)
- Cisco Secure Client 5.1.3.62
- Windows Server 2016
- Windows 10

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.

Esempio di rete

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

Il nome di dominio configurato in Windows Server 2016 è ad.rem-system.com, utilizzato come esempio in questo documento.



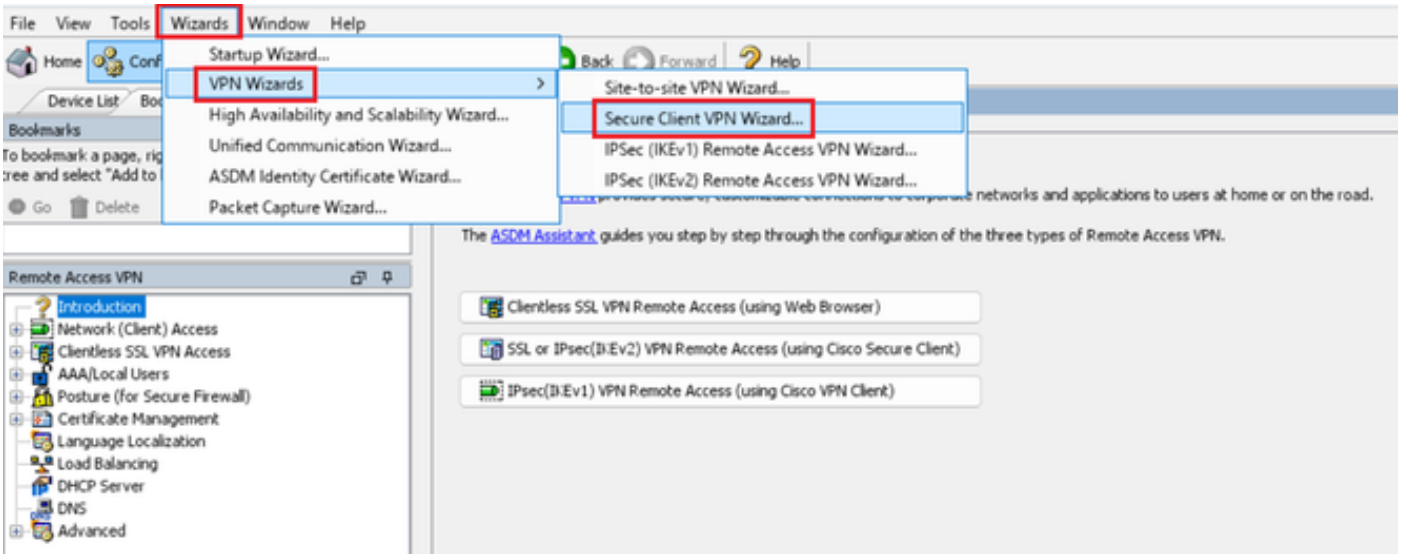
Esempio di rete

Configurazioni

Configurazione in ASDM

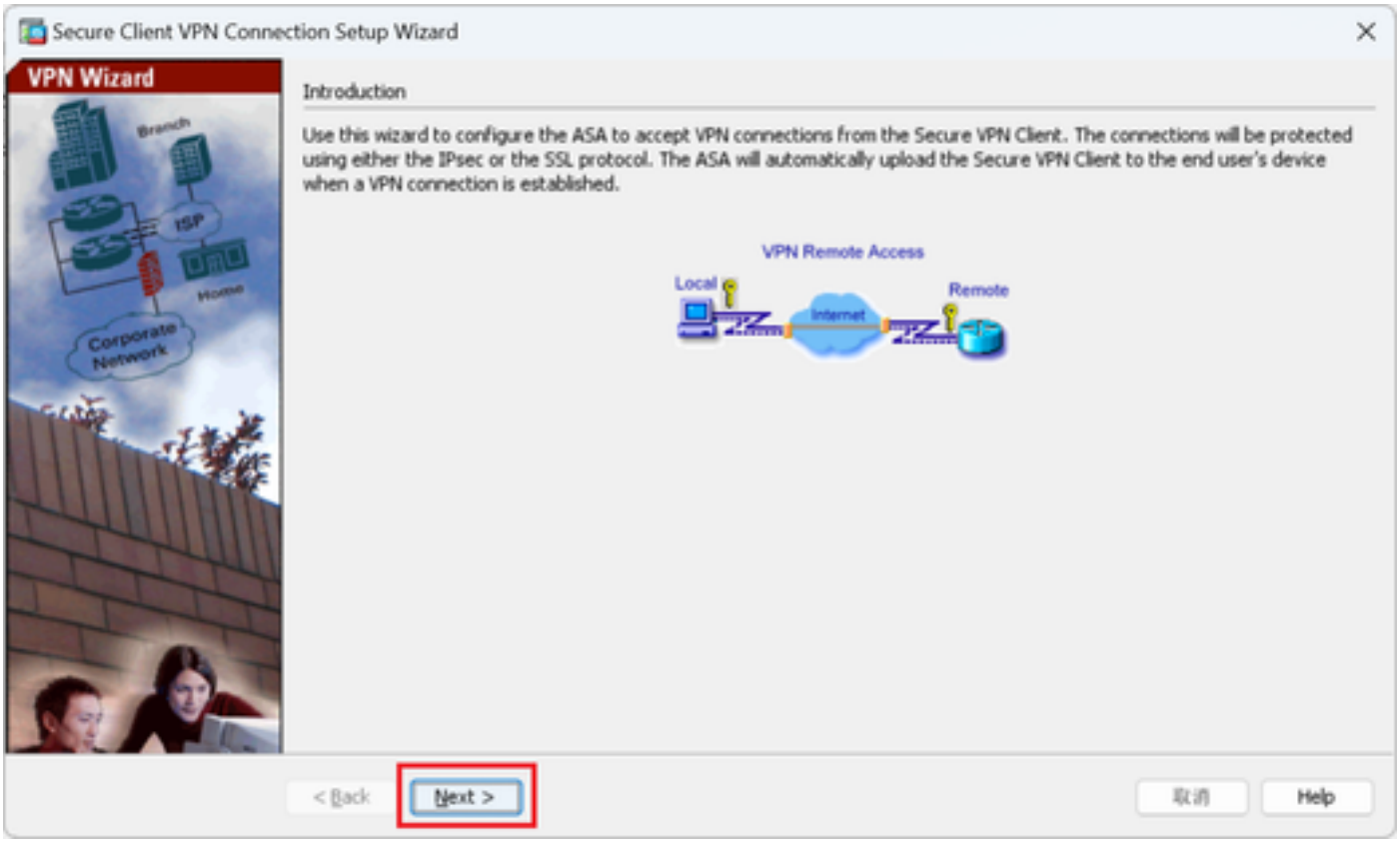
Passaggio 1. Apri procedure guidate VPN

Passare a Creazioni guidate > Creazioni guidate VPN, fare clic su Creazione guidata VPN client sicura.



Apri procedure guidate VPN

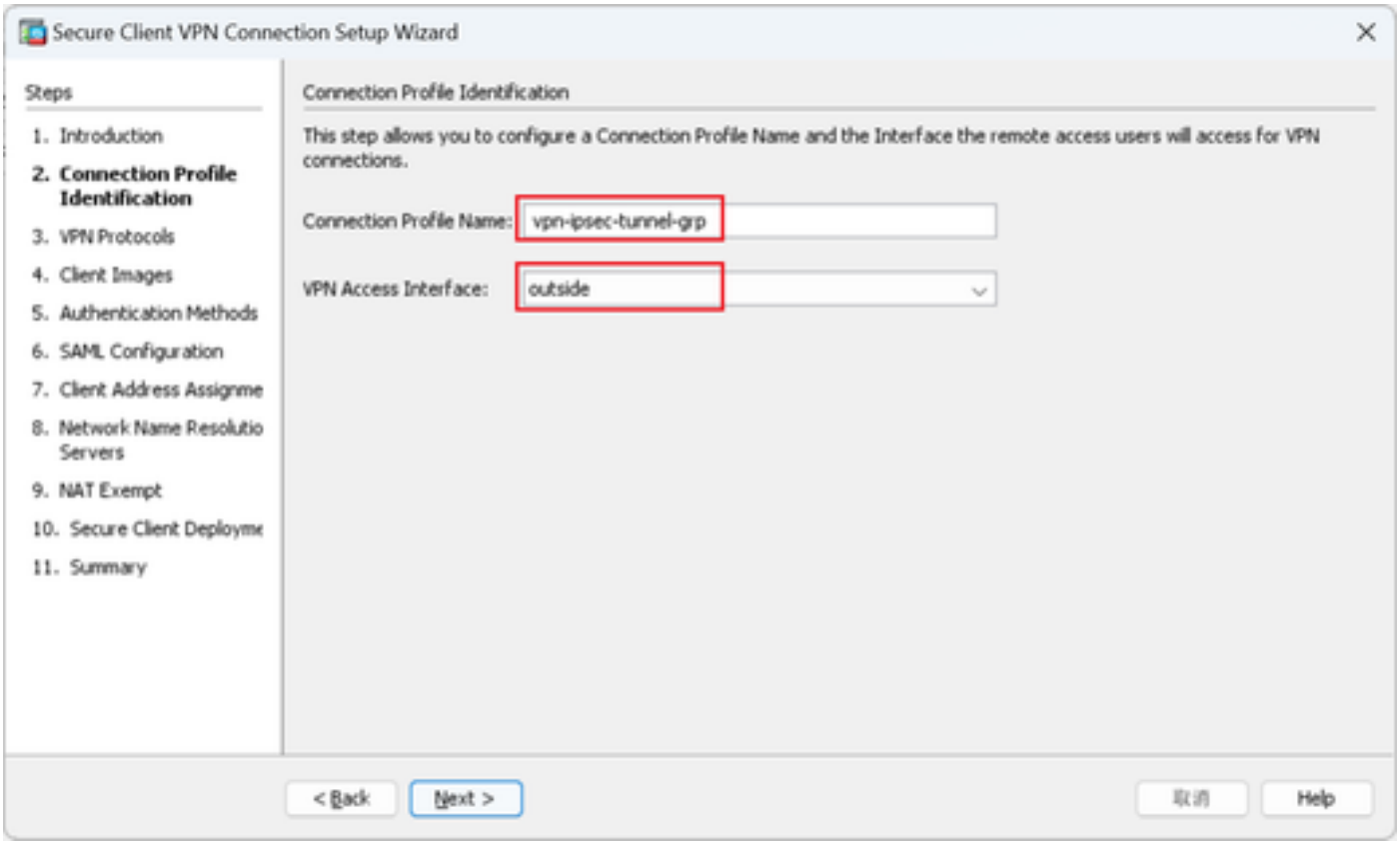
Fare clic su Next (Avanti).



Fare clic sul pulsante Avanti

Passaggio 2. Identificazione profilo di connessione

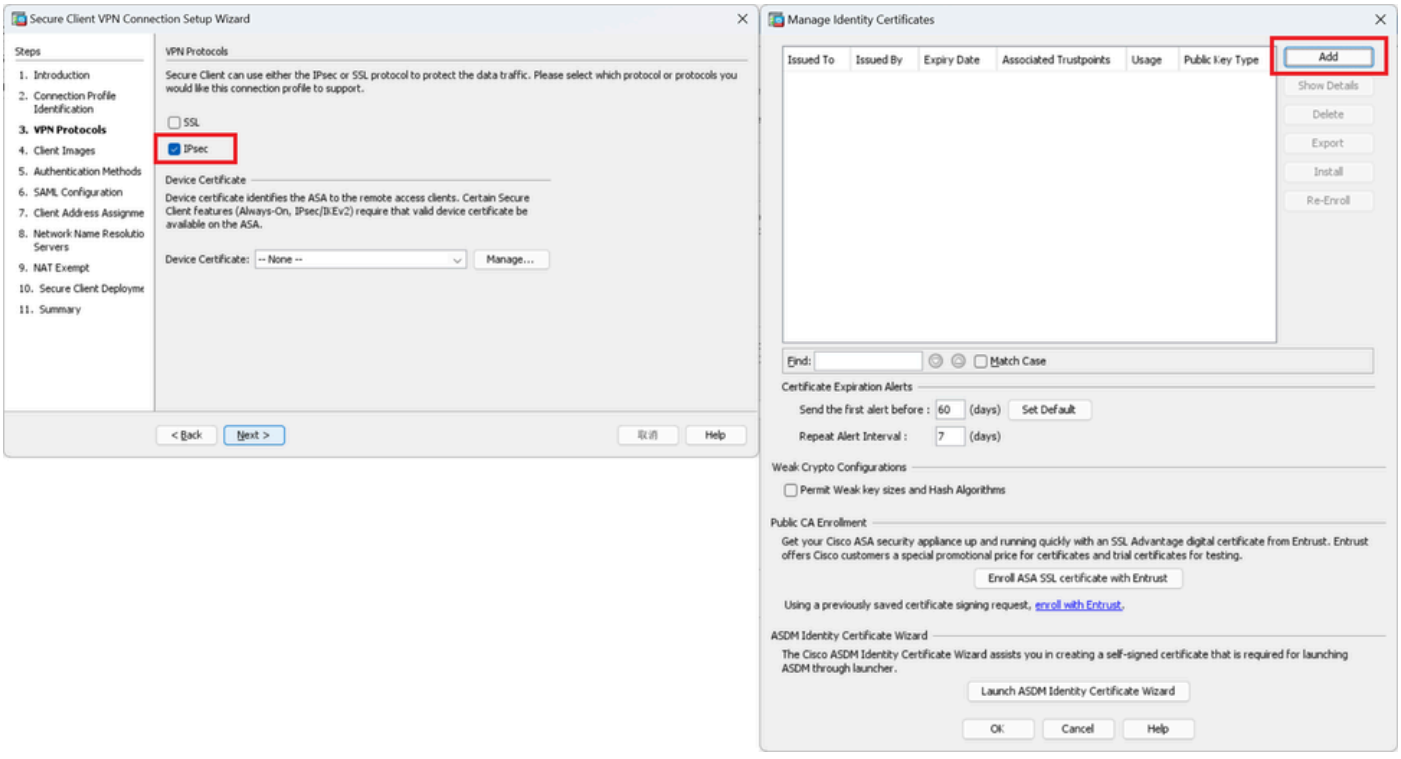
Immettere le informazioni per il profilo di connessione.
Nome profilo connessione : vpn-ipsec-tunnel-grp
Interfaccia di accesso VPN : esterna



Identificazione profilo di connessione

Passaggio 3. Protocolli VPN

Selezionare IPsec, fare clic su Aggiungi pulsante per aggiungere un nuovo certificato autofirmato.

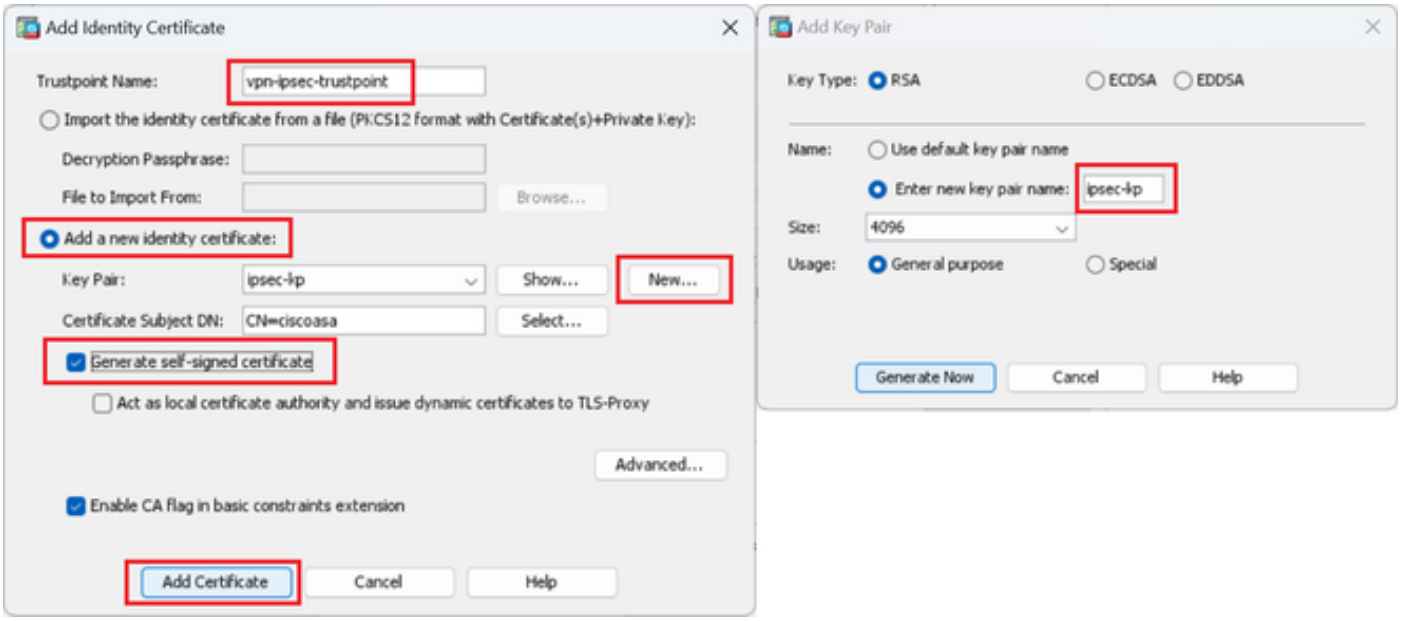


Protocolli VPN

Immettere le informazioni per il certificato autofirmato.

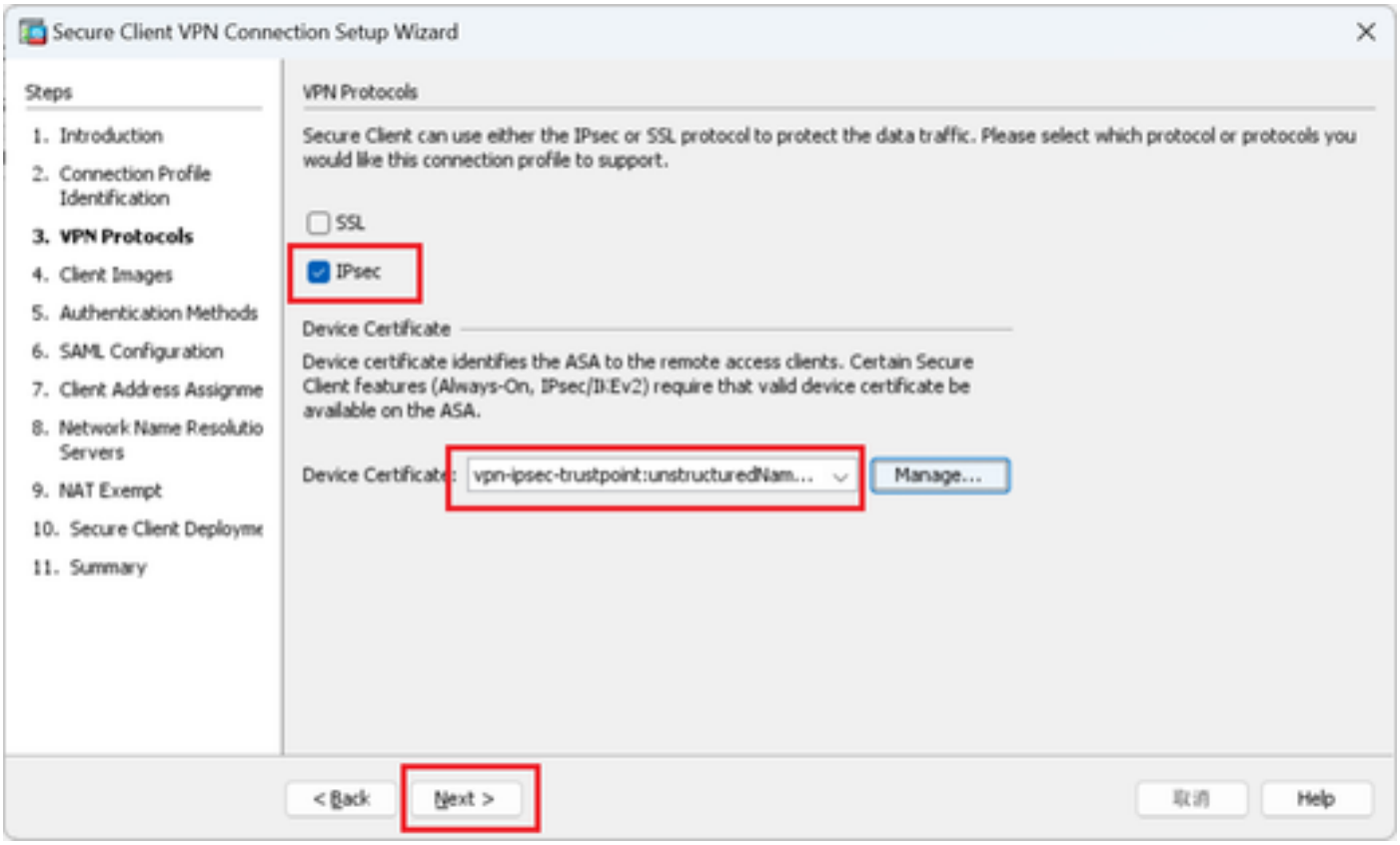
Nome punto di fiducia : vpn-ipsec-trustpoint

Coppia di chiavi: ipsec-kp



Dettagli del certificato autofirmato

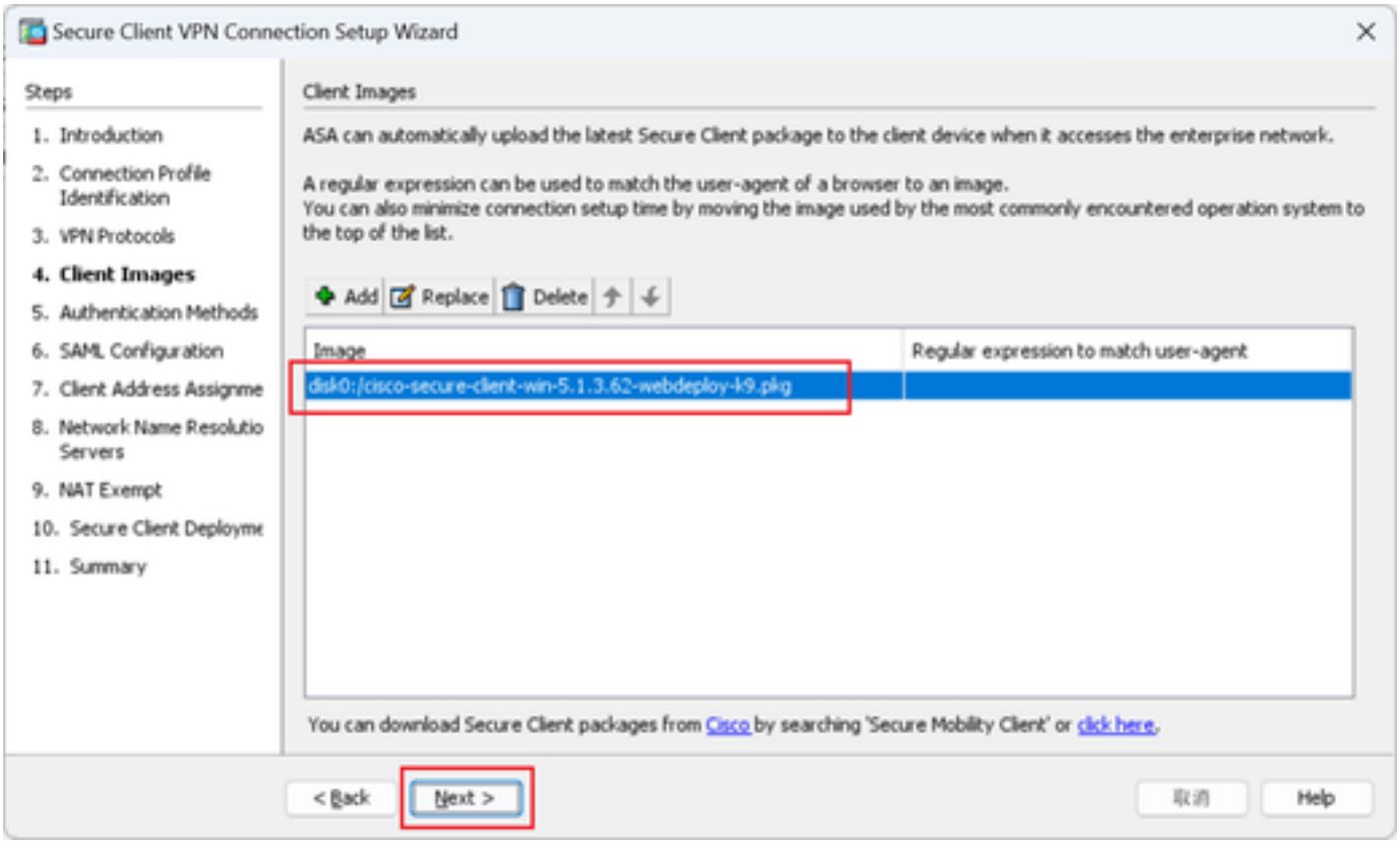
Confermare le impostazioni dei protocolli VPN, quindi fare clic su Next button.



Conferma impostazioni protocollo VPN

Passaggio 4. Immagini client

Fare clic su Add button per aggiungere un'immagine client sicura, quindi fare clic su Next button.



Immagini client

Passaggio 5. Metodi di autenticazione

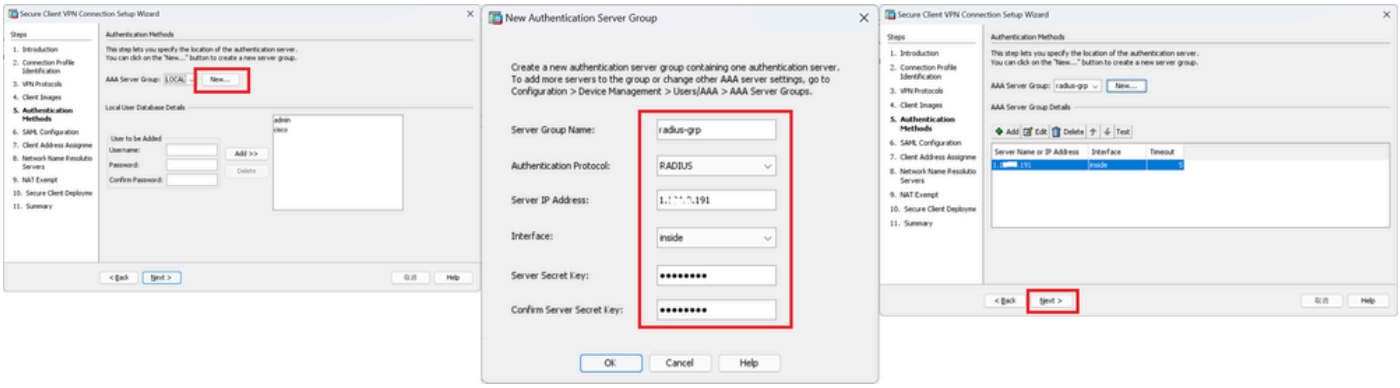
Fare clic su Nuovo pulsante per aggiungere un nuovo server aaa, fare clic su Avanti pulsante.

Nome gruppo server : radius-grp

Protocollo di autenticazione : RADIUS

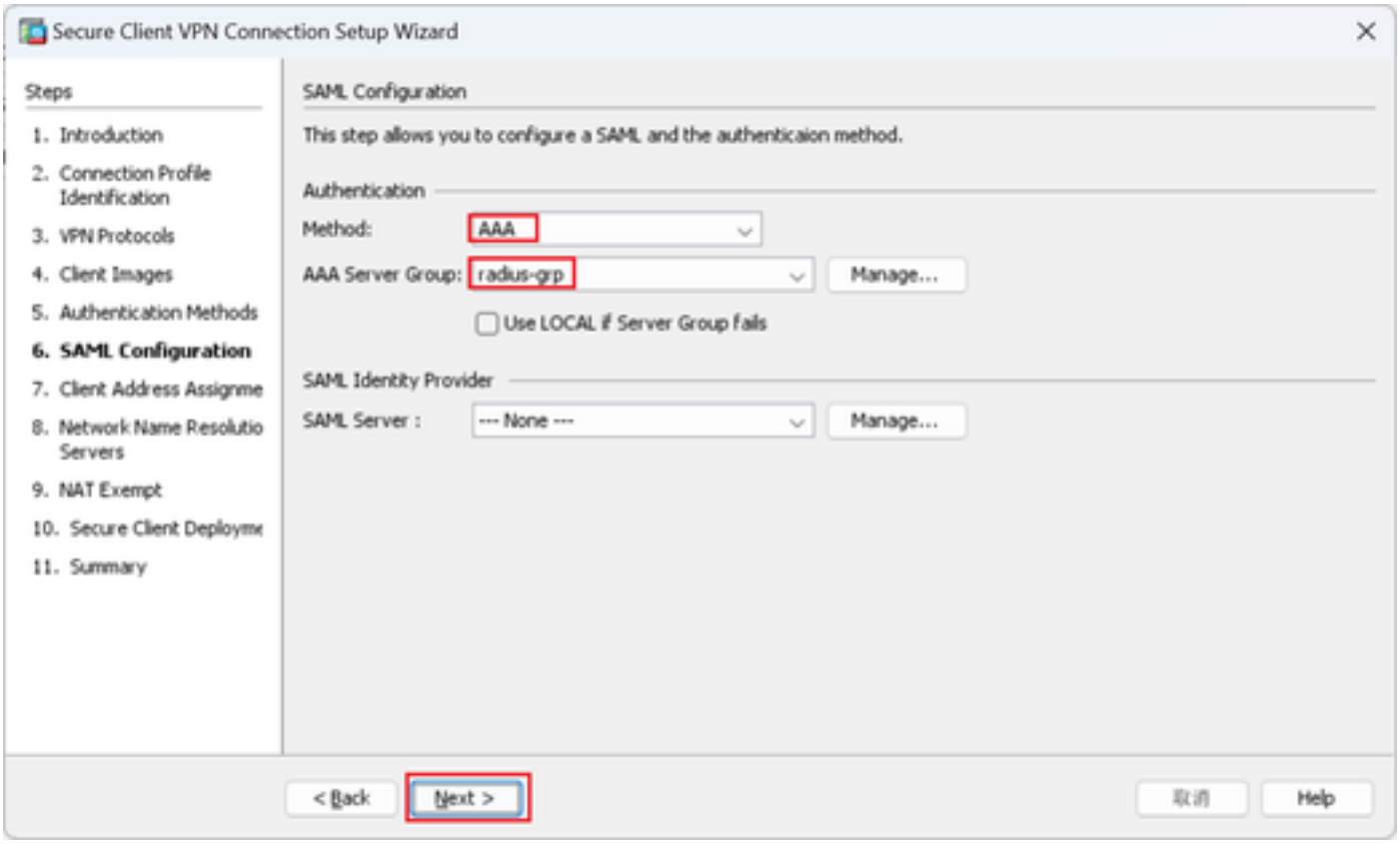
Indirizzo IP server : 1.x.x.191

Interfaccia : interna



Passaggio 6. Configurazione SAML

Fare clic sul pulsante Avanti.



Configurazione SAML

Passaggio 7. Assegnazione indirizzo client

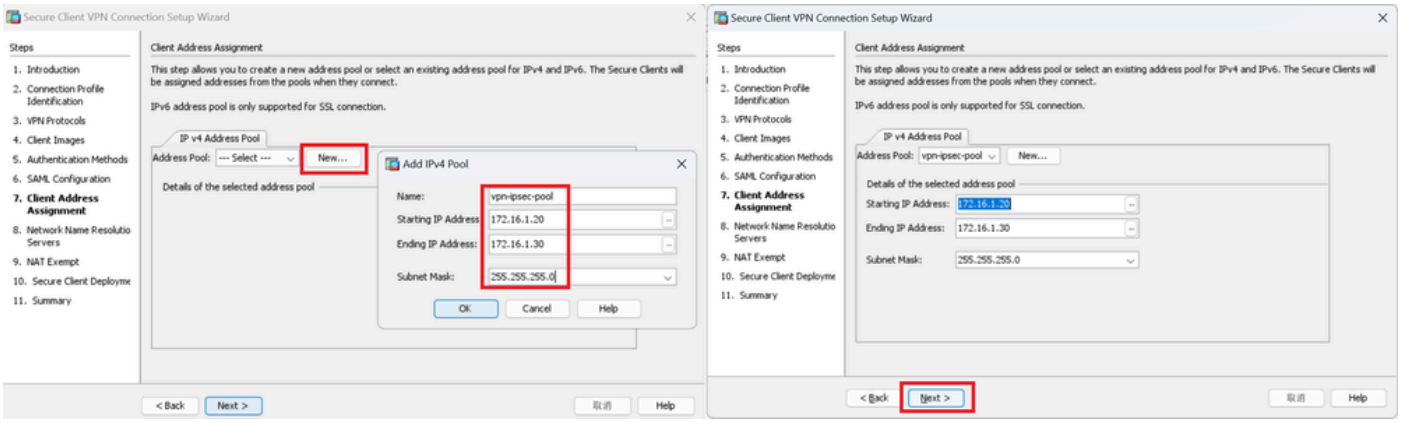
Fare clic sul pulsante New (Nuovo) per aggiungere un nuovo pool IPv4, fare clic sul pulsante Next (Avanti).

Nome : vpn-ipsec-pool

Indirizzo IP iniziale: 172.16.1.20

Indirizzo IP finale : 172.16.1.30

Subnet mask: 255.255.255.0



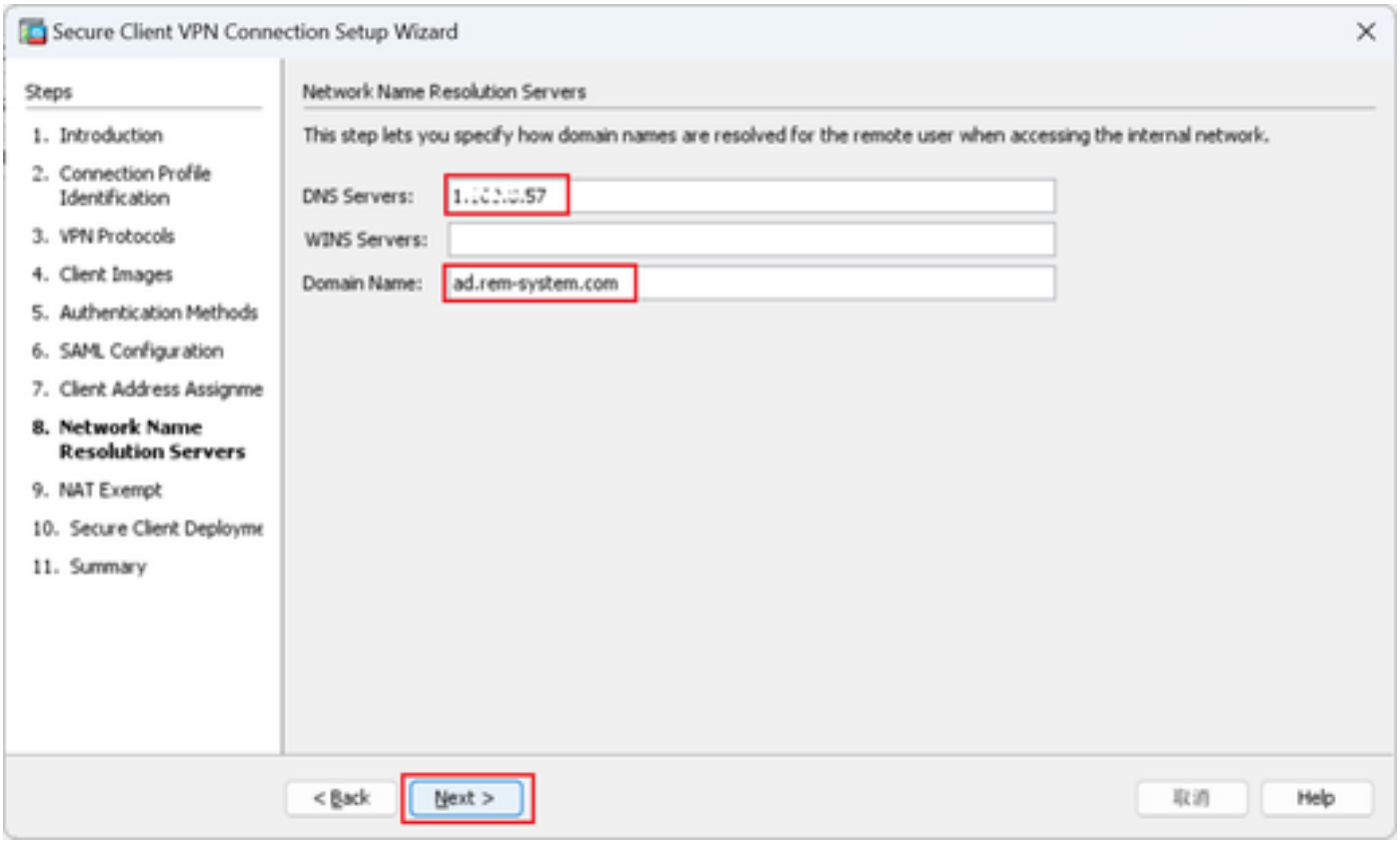
Assegnazione indirizzo client

Passaggio 8. Server di risoluzione dei nomi di rete

Immettere le informazioni per il DNS e il dominio, fare clic su Avanti pulsante.

Server DNS : 1.x.x.57

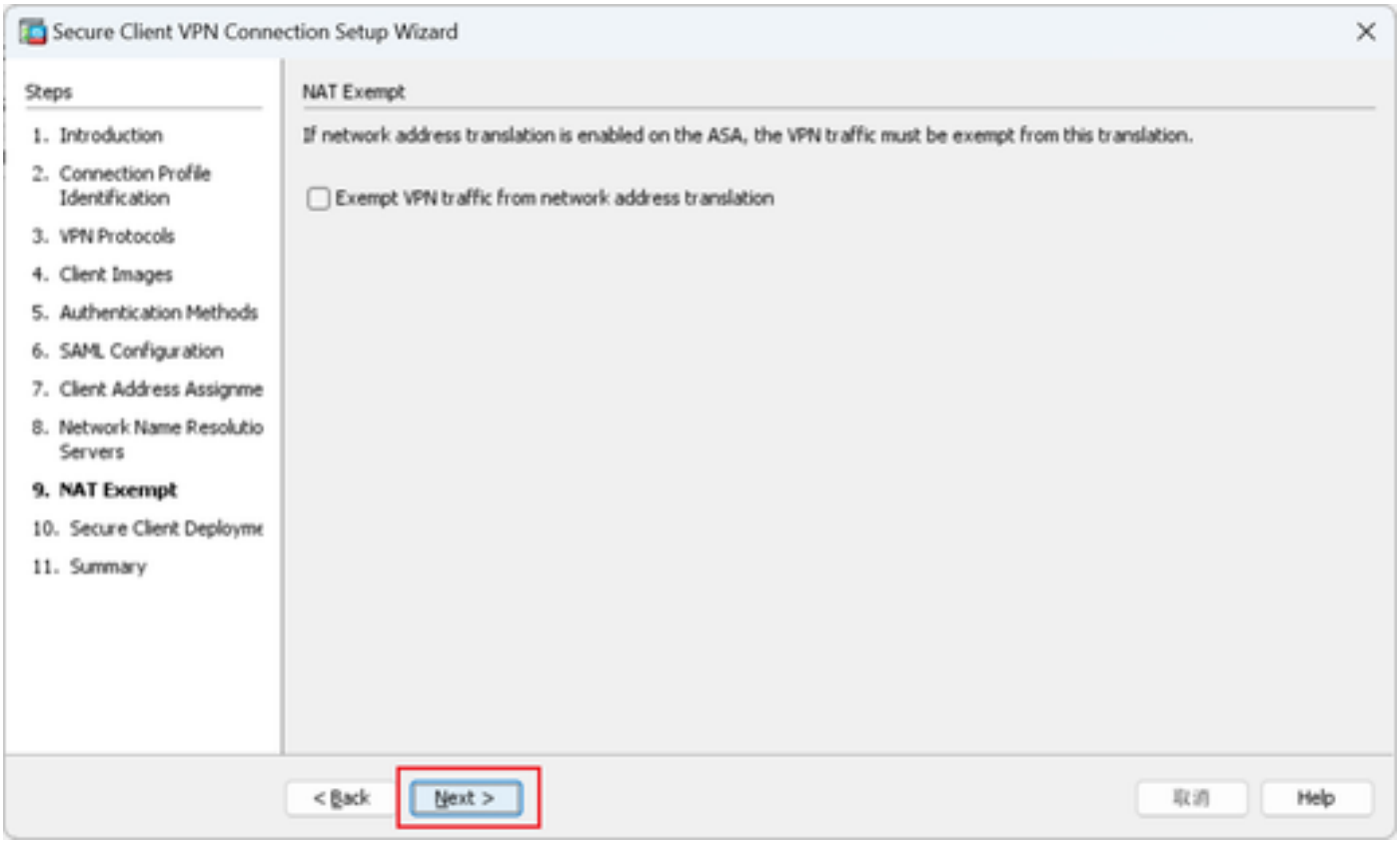
Nome dominio: ad.rem-system.com



Server di risoluzione dei nomi di rete

Passaggio 9. Esente da NAT

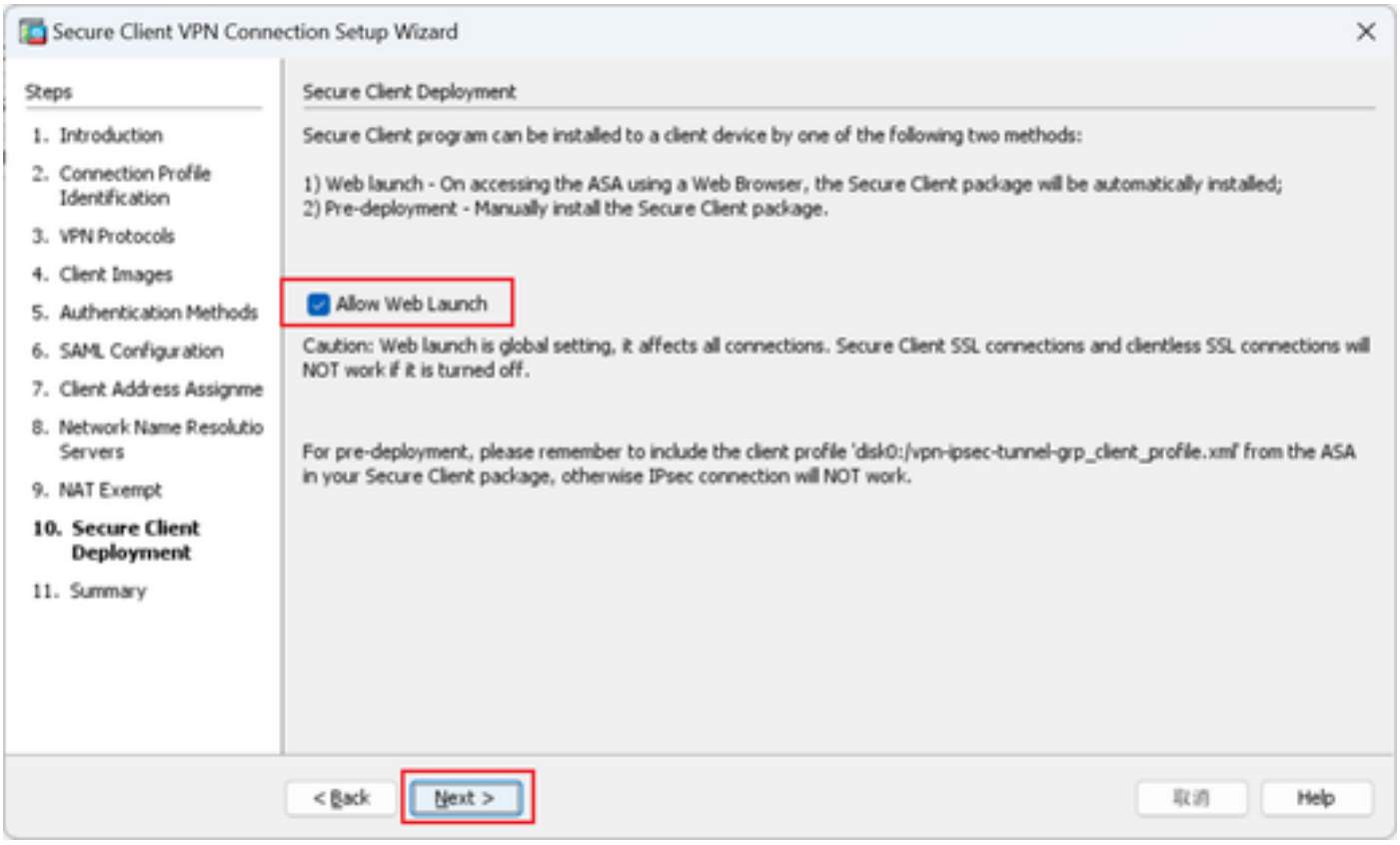
Fare clic sul pulsante Avanti.



Esente da NAT

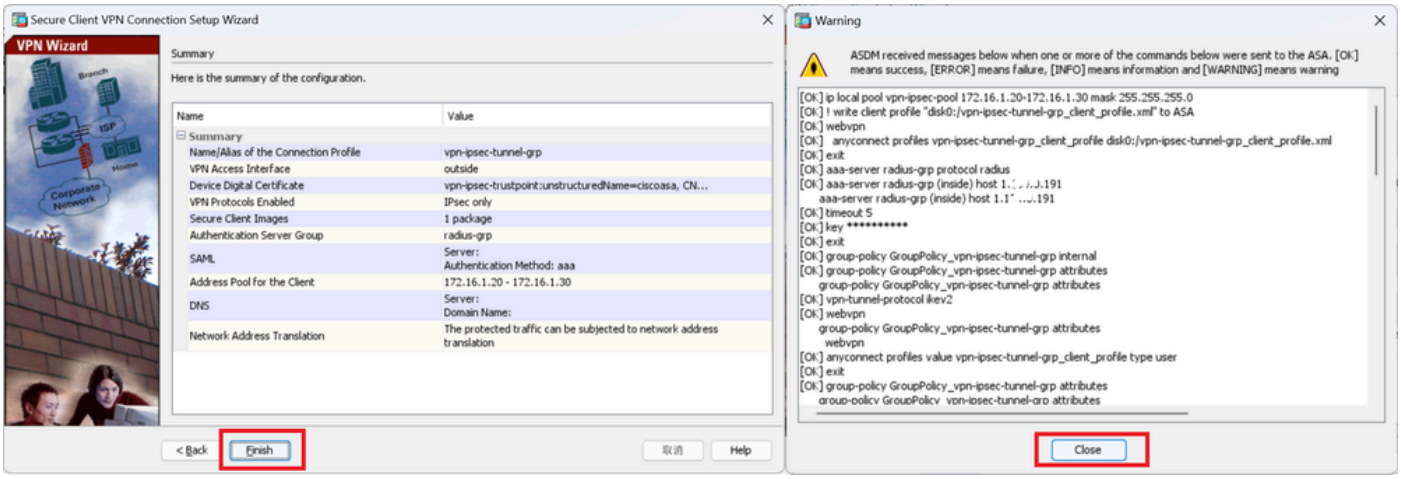
Passaggio 10. Installazione client sicura

Selezionare Consenti avvio Web, quindi fare clic su Pulsante Avanti.



Passaggio 11. Salva impostazioni

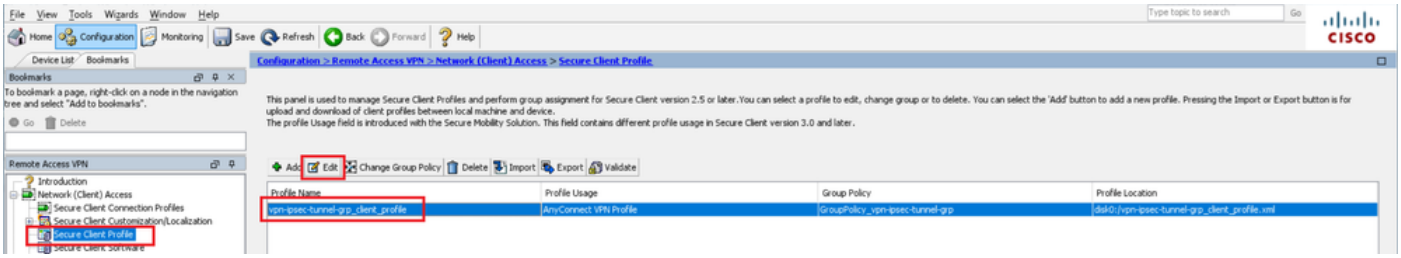
Fare clic su Fine per salvare le impostazioni.



Salva impostazioni

Passaggio 12. Conferma ed esporta profilo client protetto

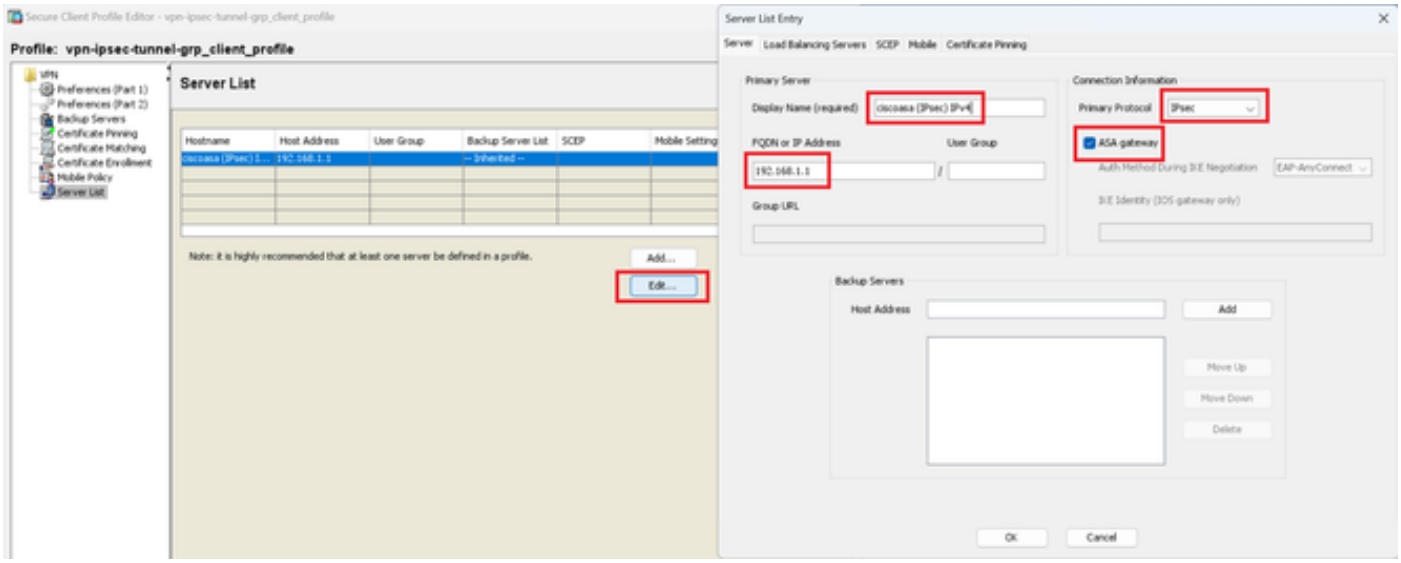
Selezionare Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profilo client protetto, quindi fare clic sul pulsante Modifica.



Modifica profilo client protetto

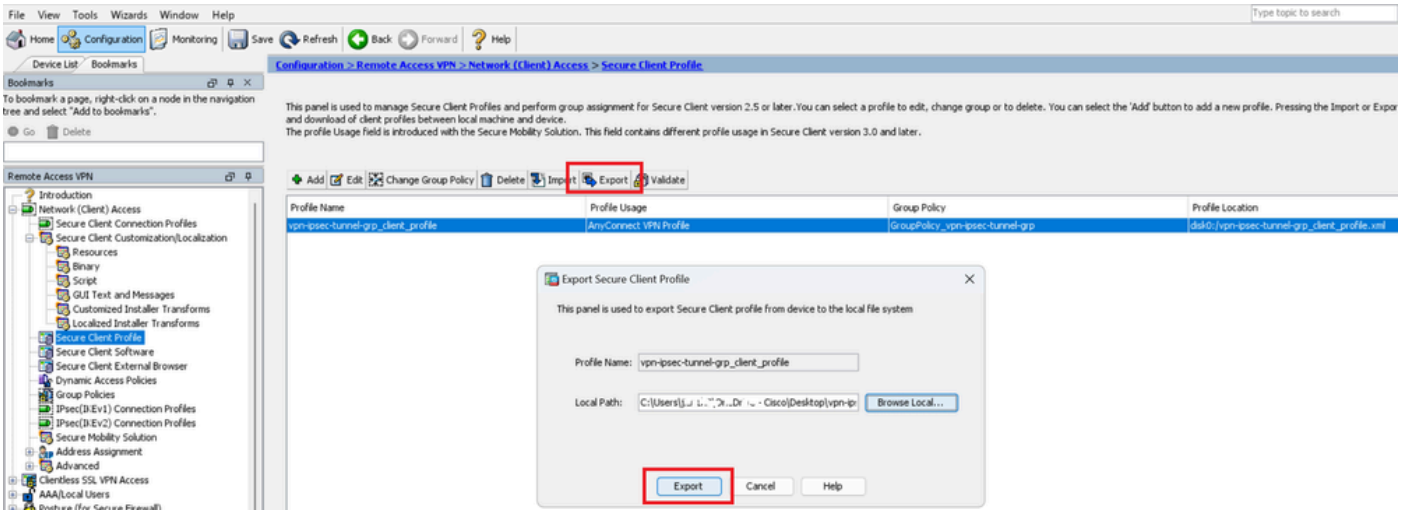
Confermare il dettaglio del profilo.

- Nome visualizzato (obbligatorio) : ciscoasa (IPsec) IPv4
- FQDN o indirizzo IP : 192.168.1.1
- Protocollo primario: IPsec



Conferma profilo client protetto

Fare clic sul pulsante Esporta per esportare il profilo sul PC locale.



Esporta profilo client protetto

Passaggio 13. Conferma dettagli profilo client protetto

Aprire Secure Client Profile tramite browser, verificare che il protocollo primario per l'host sia IPsec.

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/">
  <ServerList>
    <HostEntry>
      <HostName>ciscoasa (IPsec) IPv4</HostName>
      <HostAddress>192.168.1.1</HostAddress>
      <PrimaryProtocol>IPsec</PrimaryProtocol>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>
```

Passaggio 14. Conferma impostazioni nella CLI di ASA

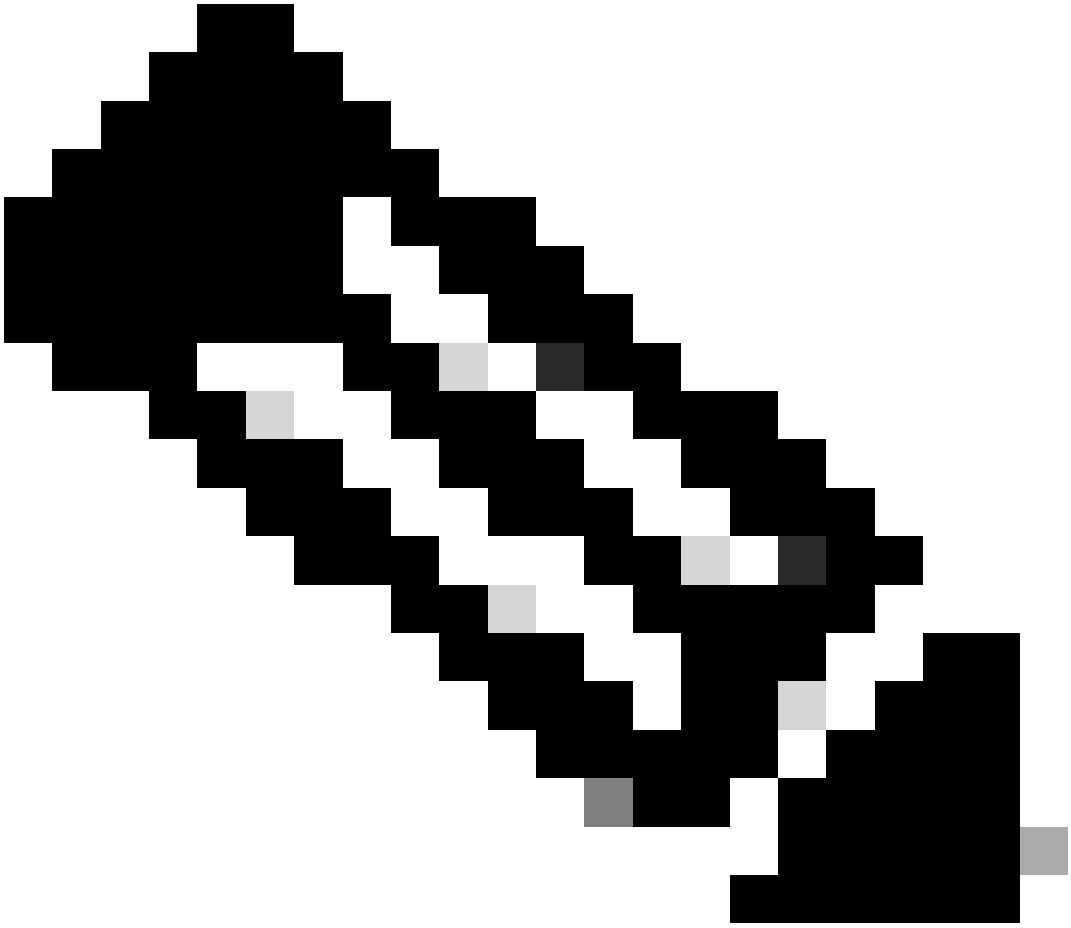
Confermare le impostazioni IPsec create da ASDM nella CLI dell'ASA.

```
// Defines a pool of addresses
ip local pool vpn-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.0

// Defines radius server
aaa-server radius-grp protocol radius
aaa-server radius-grp (inside) host 1.x.x.191
timeout 5

// Define the transform sets that IKEv2 can use
crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES192
protocol esp encryption aes-192
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal 3DES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal DES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1

// Configures the crypto map to use the IKEv2 transform-sets
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside

// Defines trustpoint
crypto ca trustpoint vpn-ipsec-trustpoint
enrollment self
subject-name CN=ciscoasa
keypair ipsec-kp
crl configure

// Defines self-signed certificate
crypto ca certificate chain vpn-ipsec-trustpoint
certificate 6651a2a2
308204ed 308202d5 a0030201 02020466 51a2a230 0d06092a 864886f7 0d01010b
......
ac76f984 efd41d13 073d0be6 f923a9c6 7b
quit

// IKEv2 Policies
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 10
```

```
encryption aes-192
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 20
encryption aes
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 40
encryption aes
integrity sha256
group 5
prf sha256
lifetime seconds 86400

// Enabling client-services on the outside interface
crypto ikev2 enable outside client-services port 443

// Specifiies the certificate the ASA uses for IKEv2
crypto ikev2 remote-access trustpoint vpn-ipsec-trustpoint

// Configures the ASA to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
enable
anyconnect image disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1
anyconnect profiles vpn-ipsec-tunnel-grp_client_profile disk0:/vpn-ipsec-tunnel-grp_client_profile.xml
anyconnect enable
tunnel-group-list enable

// Configures the group-policy to allow IKEv2 connections and defines which Cisco Secure Client profile
group-policy GroupPolicy_vpn-ipsec-tunnel-grp internal
group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
wins-server none
dns-server value 1.x.x.57
vpn-tunnel-protocol ikev2
default-domain value ad.rem-system.com
webvpn
anyconnect profiles value vpn-ipsec-tunnel-grp_client_profile type user

// Ties the pool of addressess to the vpn connection
tunnel-group vpn-ipsec-tunnel-grp type remote-access
tunnel-group vpn-ipsec-tunnel-grp general-attributes
address-pool vpn-ipsec-pool
authentication-server-group radius-grp
default-group-policy GroupPolicy_vpn-ipsec-tunnel-grp
tunnel-group vpn-ipsec-tunnel-grp webvpn-attributes
group-alias vpn-ipsec-tunnel-grp enable
```

Passaggio 15. Aggiungi algoritmo di crittografia

Nella CLI di ASA, aggiungere il gruppo 19 ai criteri IKEv2.

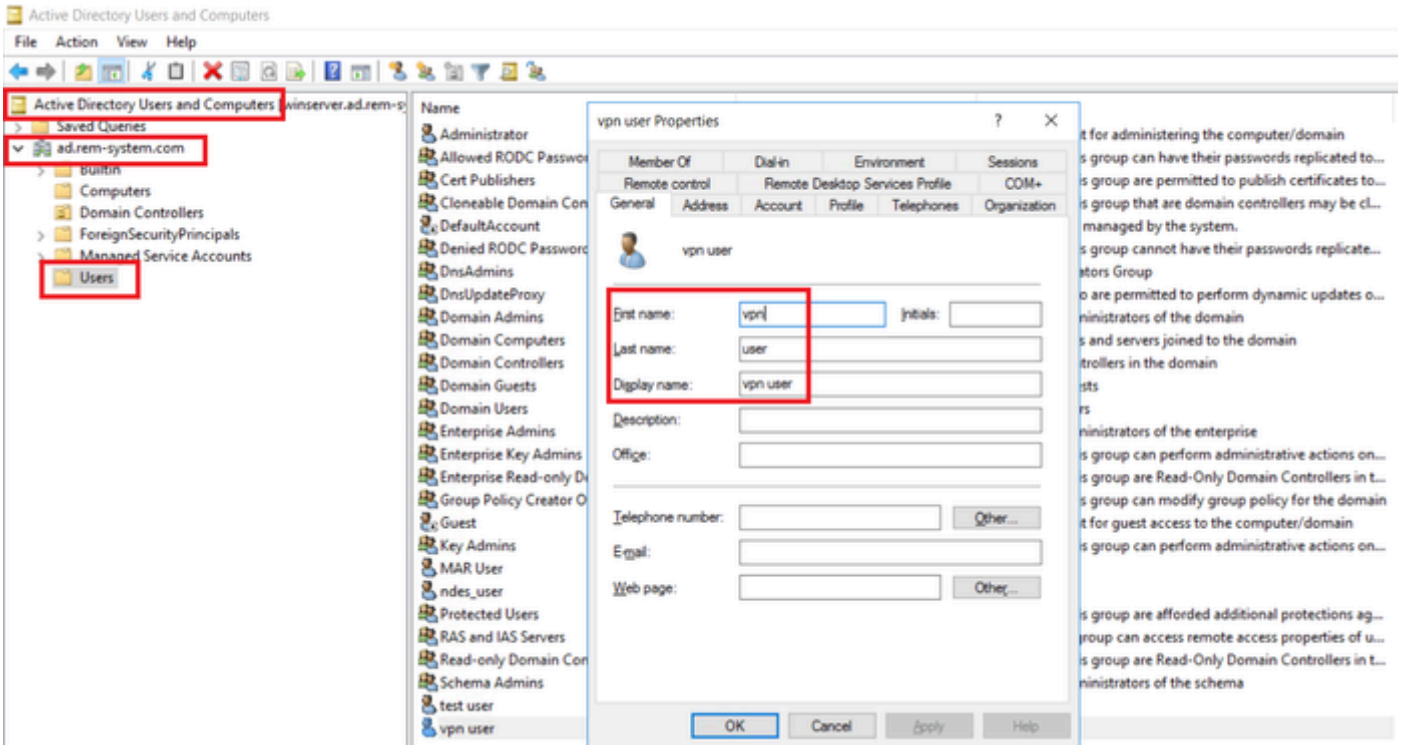


Nota: per le connessioni IKEv2/IPsec, Cisco Secure Client non supporta più i gruppi Diffie-Hellman (DH) 2, 5, 14 e 24 alla versione 4.9.00086. Questa modifica può causare errori di connessione dovuti a mancata corrispondenza dell'algoritmo di crittografia.

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 19
ciscoasa(config-ikev2-policy)#
```

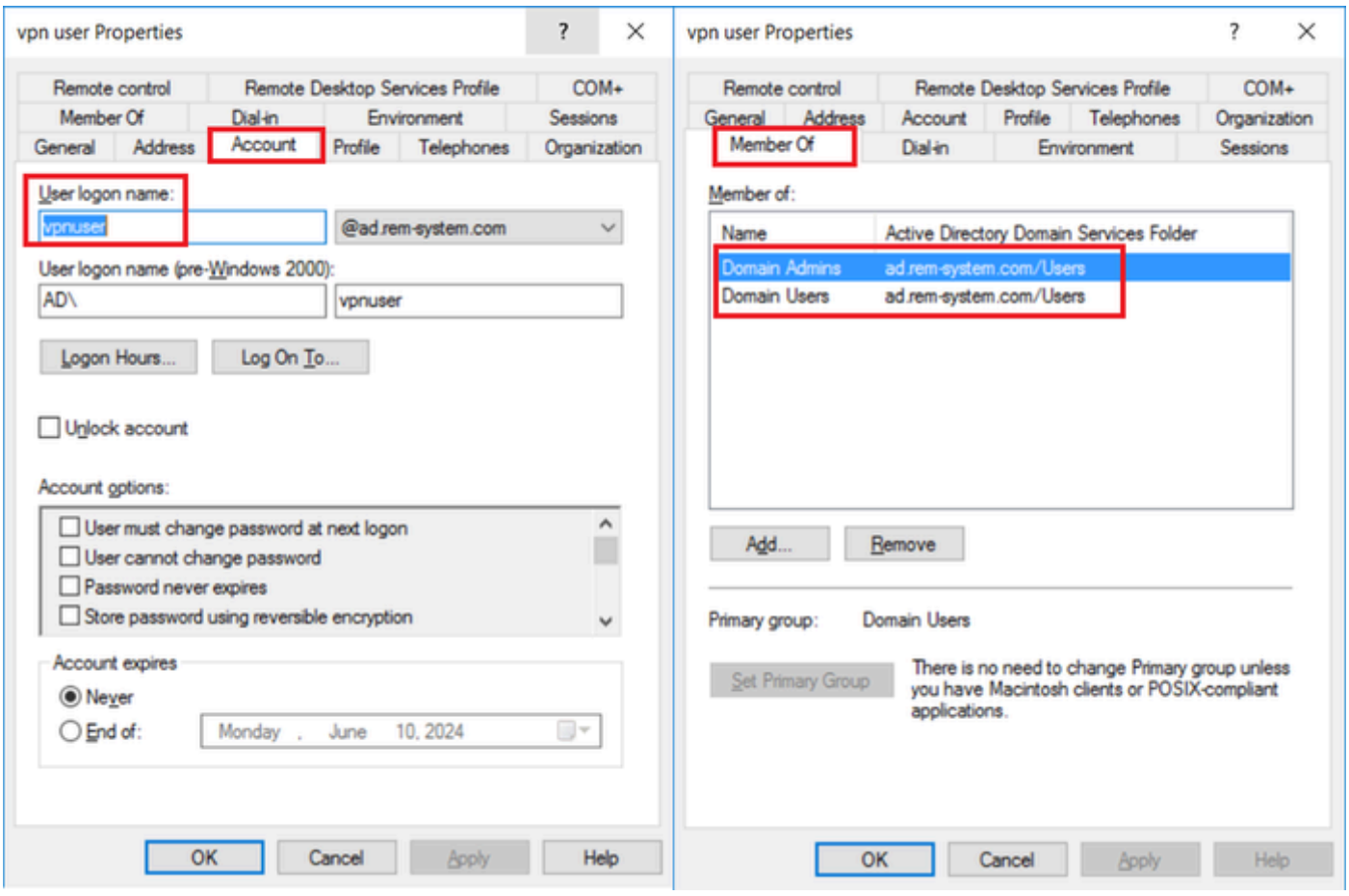
Configurazione in Windows Server

È necessario aggiungere un utente di dominio per la connessione VPN. Passare a Utenti e computer di Active Directory, quindi fare clic su Utenti. Aggiungere vpnuser come utente di dominio.



Aggiungi utente di dominio

Aggiungere l'utente di dominio al membro di Domain Admins e Domain Users.

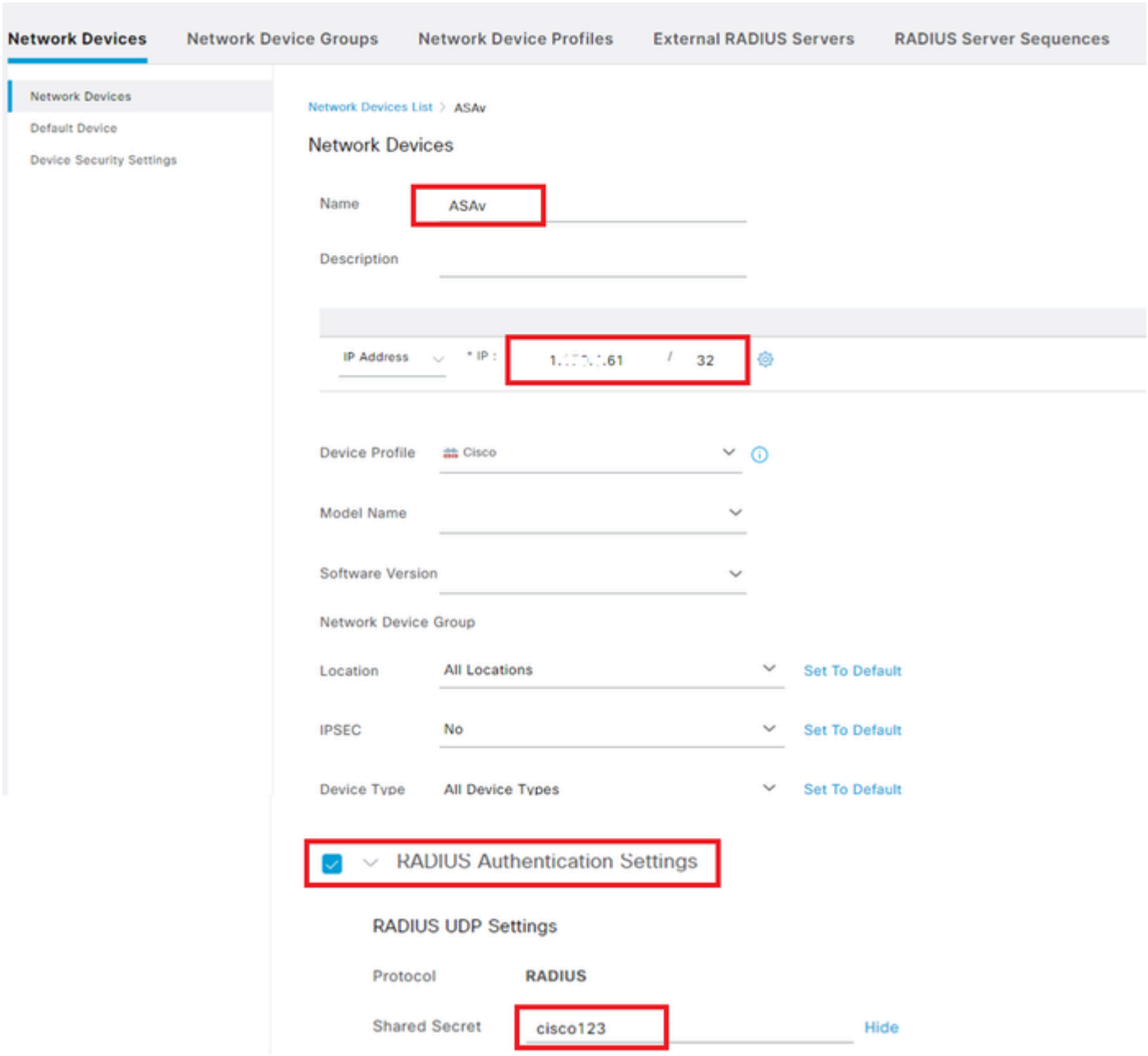


Domain Admins e Domain Users

Configurazione in ISE

Passaggio 1. Aggiungi dispositivo

Selezionare Amministrazione > Dispositivi di rete, quindi fare clic su Aggiungi per aggiungere un dispositivo ASAv.

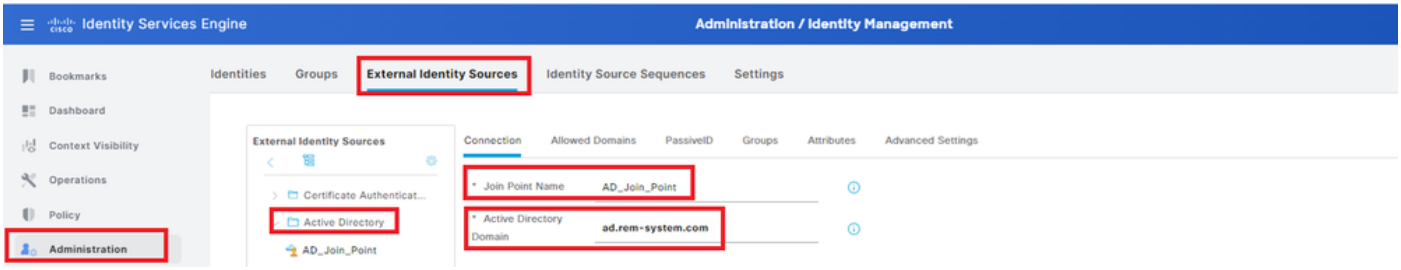


Aggiungi dispositivo

Passaggio 2. Aggiungi Active Directory

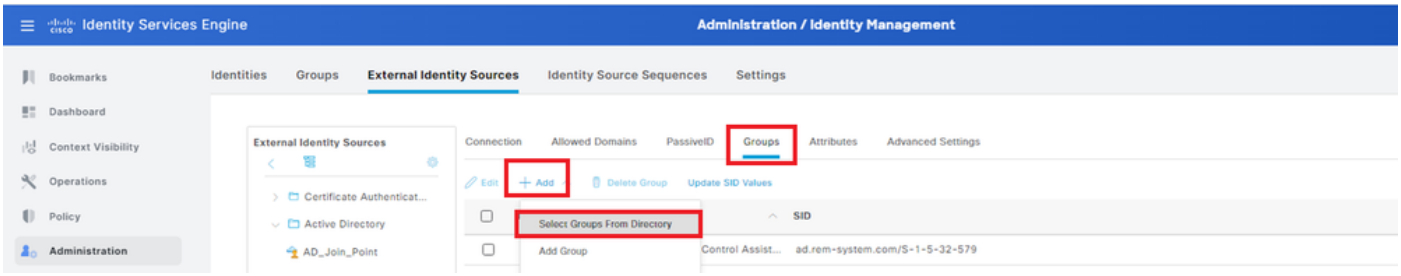
Selezionare Amministrazione > Origini identità esterne > Active Directory, fare clic sulla scheda Connessione, quindi aggiungere Active Directory ad ISE.

- Nome punto di join: AD_Join_Point
- Dominio Active Directory: ad.rem-system.com



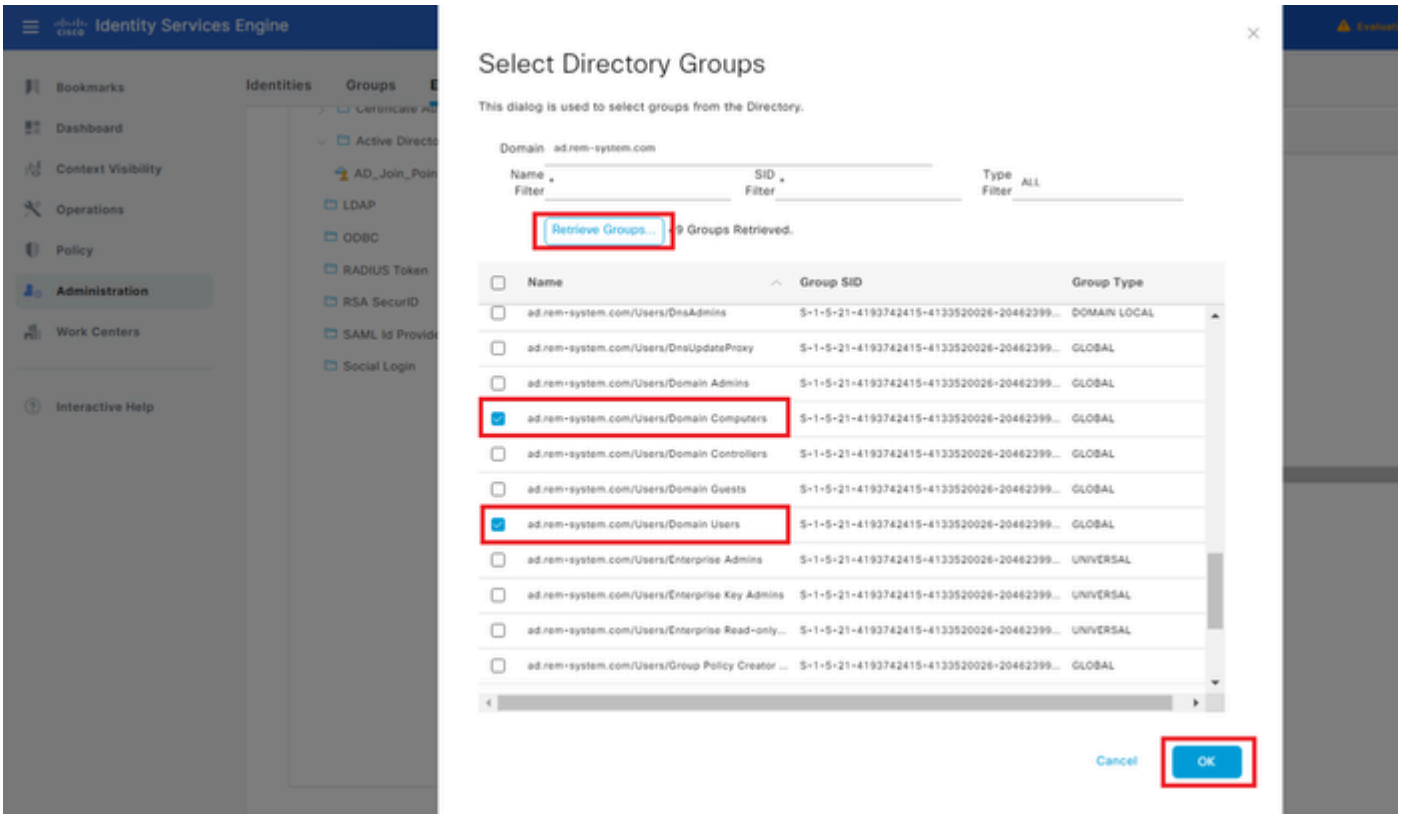
Aggiungi Active Directory

Passare alla scheda Gruppi, selezionare Seleziona gruppi dalla directory dall'elenco a discesa.



Seleziona gruppi dalla directory

Selezionate Recupera gruppi (Retrieve Groups) dall'elenco a discesa. Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain Utenti e fare clic su OK.



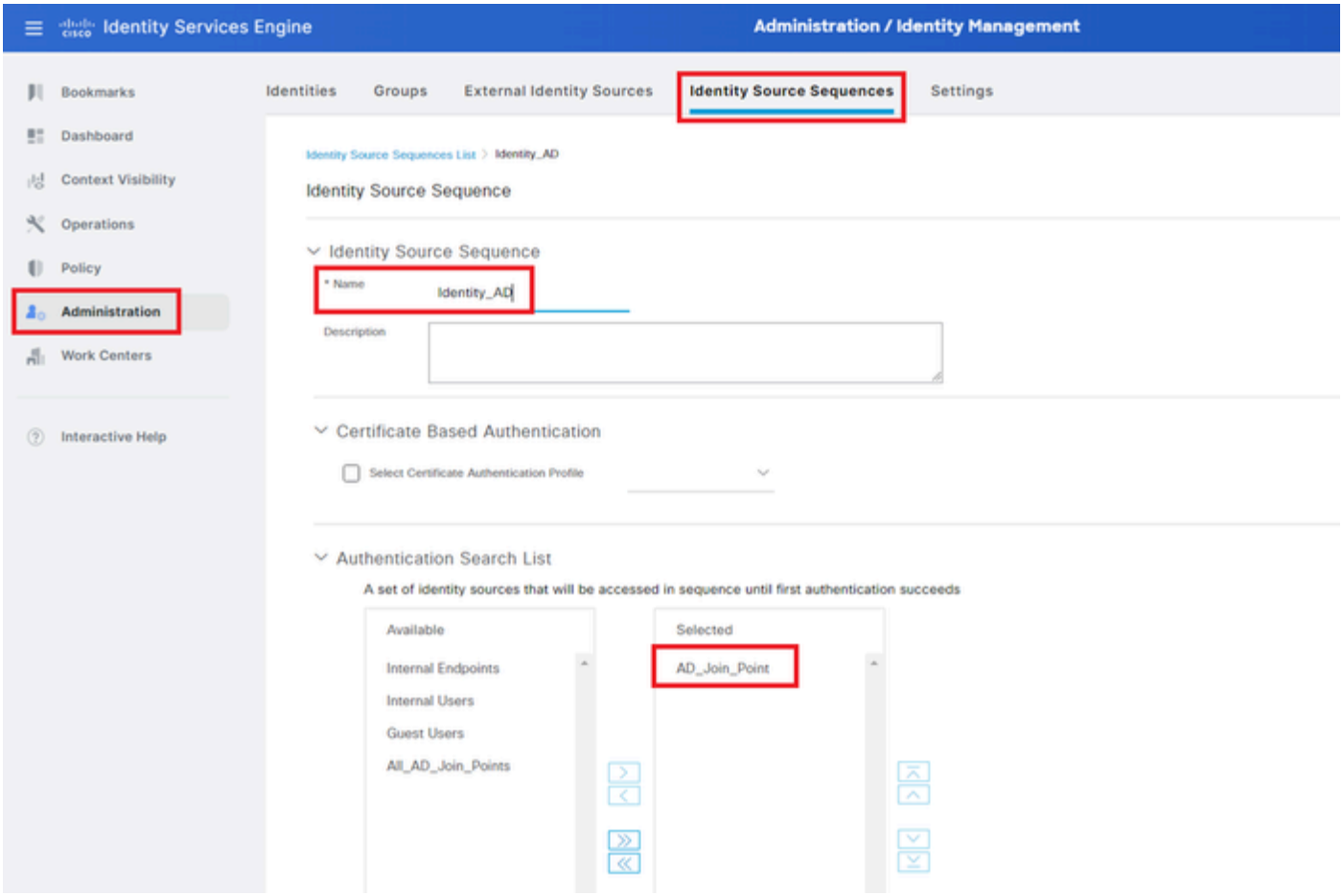
Aggiungi computer e utenti del dominio

Passaggio 3. Aggiungi sequenza di origine identità

Passare ad Amministrazione > Sequenze origine identità, quindi aggiungere una sequenza origine

identità.

- Nome: Identity_AD
- Elenco di ricerca autenticazione: AD_Join_Point

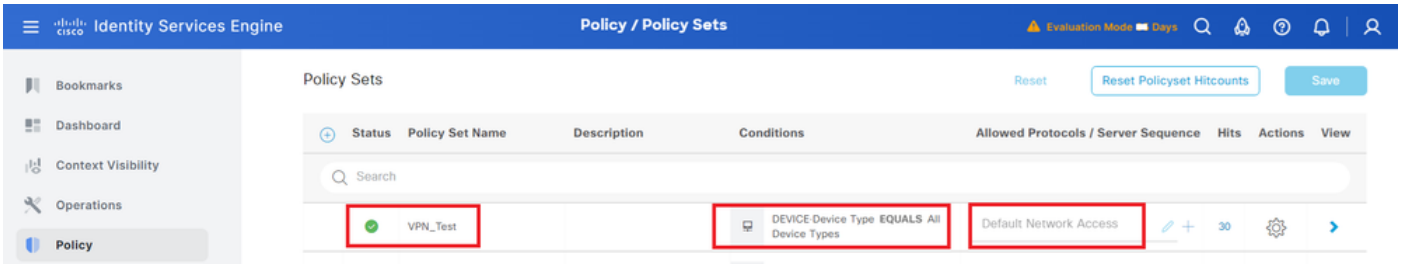


Aggiungi sequenze origine identità

Passaggio 4. Aggiungi set di criteri

Passare a Criterio > Set di criteri, fare clic su + per aggiungere un set di criteri.

- Nome set di criteri : VPN_Test
- Condizioni : Tipo di dispositivo dispositivo uguale a Tutti i tipi di dispositivo
- Protocolli consentiti/sequenza server: accesso alla rete predefinito

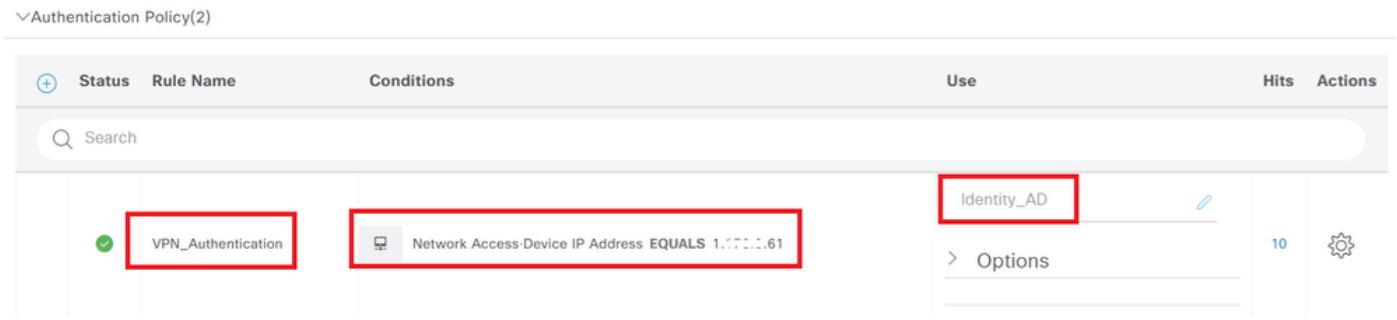


Aggiungi set di criteri

Passaggio 5. Aggiungi criterio di autenticazione

Passare a Set di criteri e fare clic su VPN_Test per aggiungere un criterio di autenticazione.

- Nome regola : VPN_Authentication
- Condizioni : Indirizzo IP dispositivo di accesso alla rete UGUALE A 1.x.x.61
- Usa: Identity_AD

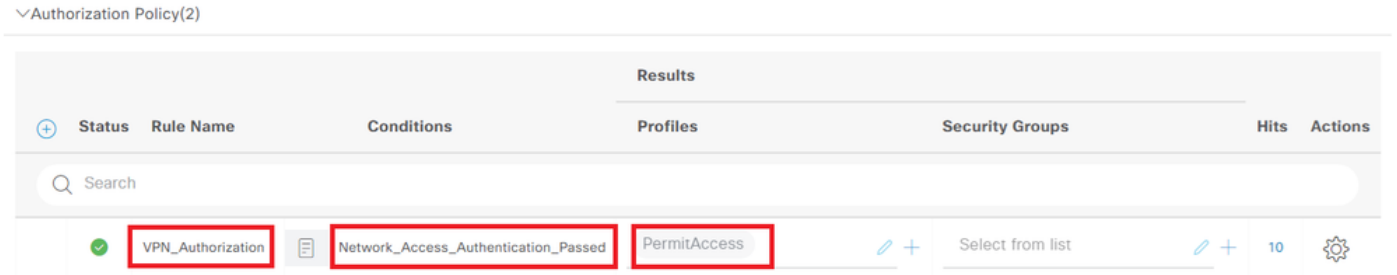


Aggiungi criterio di autenticazione

Passaggio 6. Aggiungi criterio di autorizzazione

Passare a Set di criteri e fare clic su VPN_Test per aggiungere un criterio di autorizzazione.

- Nome regola : VPN_Authorization
- Condizioni : Network_Access_Authentication_Passed
- Risultati : PermitAccess

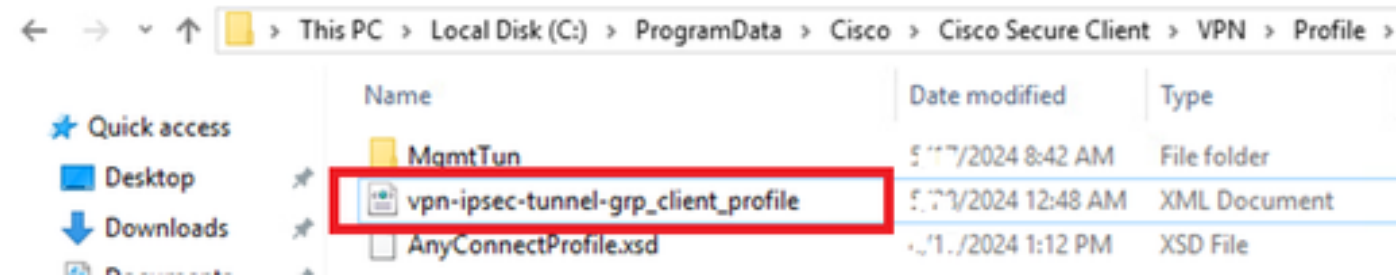


Aggiungi criterio di autorizzazione

Verifica

Passaggio 1. Copia profilo client sicuro in Win10 PC1

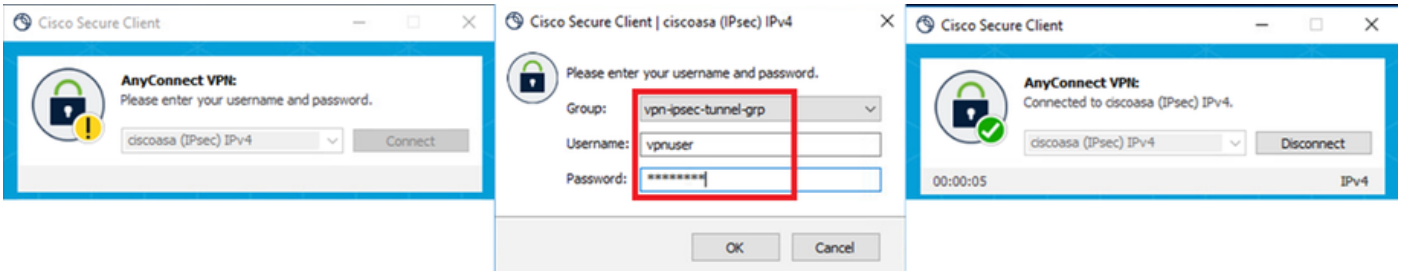
Copiare il profilo client sicuro nella directory C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile.



Copia profilo su PC

Passaggio 2. Avvia connessione VPN

Sull'endpoint, eseguire Cisco Secure Client e immettere il nome utente e la password, quindi verificare che Cisco Secure Client si connetta correttamente.



Connessione riuscita

Passaggio 3. Conferma syslog su ASA

Nel syslog, verificare che la connessione IKEv2 sia riuscita.

<#root>

```
May 28 20xx 08:xx:20: %ASA-5-750006: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser
```

New Connection Established

```
May 28 20xx 08:xx:20: %ASA-6-751026: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser
```

Passaggio 4. Conferma sessione IPsec su ASA

eseguire show vpn-sessiondb detail anyconnect il comando per confermare la sessione IKEv2/IPsec sull'appliance ASA.

<#root>

ciscoasa#

show vpn-sessiondb detail anyconnect

```
Session Type: AnyConnect Detailed

Username : vpnuser Index : 23
Assigned IP : 172.16.1.20 Public IP : 192.168.1.11
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : IKEv2: (1)AES256 IPsecOverNatT: (1)AES256 AnyConnect-Parent: (1)none
Hashing : IKEv2: (1)SHA256 IPsecOverNatT: (1)SHA256 AnyConnect-Parent: (1)none
Bytes Tx : 840 Bytes Rx : 52408
Pkts Tx : 21 Pkts Rx : 307
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_vpn-ipsec-tunnel-grp
Tunnel Group : vpn-ipsec-tunnel-grp
```

```
Login Time : 08:13:20 UTC Tue May 28 2024
Duration : 0h:10m:10s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 01aa003d0001700066559220
Security Grp : none
```

IKEv2 Tunnels: 1

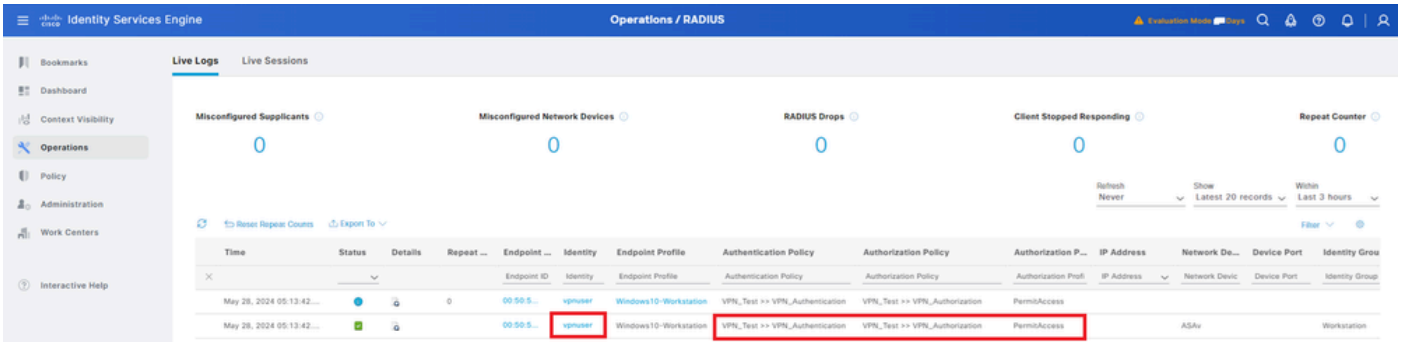
IPsecOverNatT Tunnels: 1

AnyConnect-Parent Tunnels: 1

```
AnyConnect-Parent:
Tunnel ID : 23.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 19 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : 5.1.3.62

IKEv2:
Tunnel ID : 23.2
UDP Src Port : 50982 UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption : AES256 Hashing : SHA256
Rekey Int (T): 86400 Seconds Rekey Left(T): 85790 Seconds
PRF : SHA256 D/H Group : 19
Filter Name :
Client OS : Windows Client Type : AnyConnect

IPsecOverNatT:
Tunnel ID : 23.3
Local Addr : 0.0.0.0/0.0.0.0/0/0
Remote Addr : 172.16.1.20/255.255.255.255/0/0
Encryption : AES256 Hashing : SHA256
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 28190 Seconds
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 840 Bytes Rx : 52408
Pkts Tx : 21 Pkts Rx : 307
```

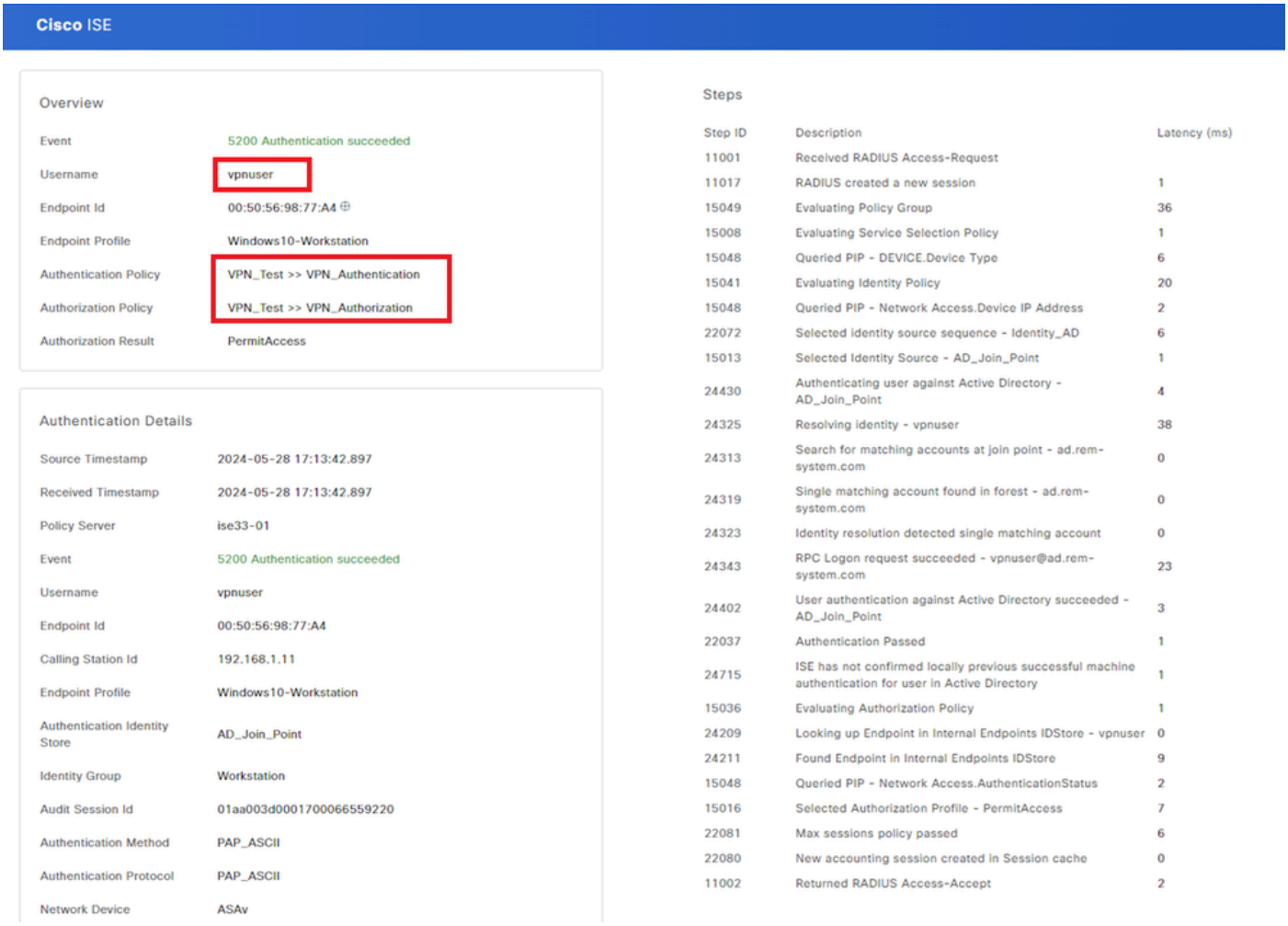
Passaggio 5. Conferma registro dinamico Radius

Selezionare **Operations** > **RADIUS** > **Live** Login nell'interfaccia utente di ISE, quindi confermare il log attivo per l'autenticazione VPN.



Registro Radius Live

Fare clic su Stato per confermare i dettagli del registro attivo.



Dettagli del registro attivo

Risoluzione dei problemi

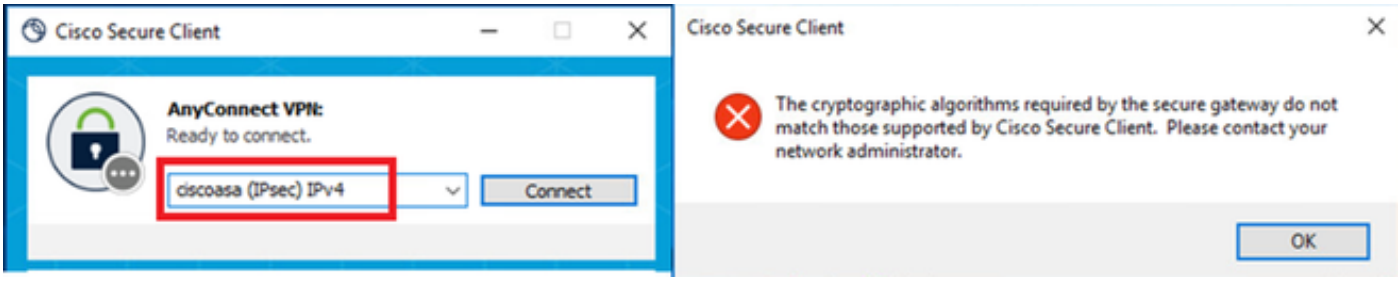
La mancata corrispondenza degli algoritmi di crittografia può causare errori di connessione. Questo è un esempio di quando si verifica un problema di mancata corrispondenza degli algoritmi. Per risolvere il problema, eseguire il passo 15 della sezione Configurazione in ASDM.

Passaggio 1. Avvia connessione VPN

Sull'endpoint, eseguire Cisco Secure Client e confermare che la connessione non è riuscita a causa di una mancata corrispondenza degli

algoritmi di crittografia.

The cryptographic algorithms required by the secure gateway do not match those supported by AnyConnect.Please contact your network administrator.



Connessione non riuscita

Passaggio 2. Conferma syslog nella CLI

Nel syslog, confermare che la negoziazione IKEv2 non è riuscita.

<#root>

May 28 20xx 08:xx:29: %ASA-5-750002: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Received a IKE_INIT_SA requ
May 28 20xx 08:xx:29: %ASA-4-750003: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Negotiation aborted due to ERR

Failed to find a matching policy

Riferimento

AnyConnect over IKEv2 su ASA con autenticazione AAA e certificato

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).