

Configurazione dell'assegnazione degli indirizzi IP statici per gli utenti VPN client sicuri

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come assegnare indirizzi IP statici agli utenti VPN di Accesso remoto utilizzando una mappa di attributi LDAP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Active Directory (AD)
- Protocollo LDAP (Lightweight Directory Access Protocol)
- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center

Componenti usati

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

- Windows Server 2022
- FTD versione 7.4.2
- FMC versione 7.4.2

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

 Nota: l'opzione per utilizzare un realm per l'assegnazione degli indirizzi IP e per configurare le mappe di attributi LDAP è supportata in firepower versione 6.7 o successiva. Prima di procedere, verificare che la versione di firepower sia 6.7 o successiva.

Configurazione

Passaggio 1. Passare a Dispositivi > Accesso remoto e selezionare il criterio VPN di Accesso remoto desiderato. Selezionare il profilo di connessione desiderato. Nella scheda AAA, selezionare un realm per il server di autenticazione e il server di autorizzazione.

Edit Connection Profile

Connection Profile:*

Group Policy:* +

[Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method:

Authentication Server:

Fallback to LOCAL Authentication

Use secondary authentication

Authorization

Authorization Server:

Allow connection only if user exists in authorization database
[Configure LDAP Attribute Map](#)

Accounting

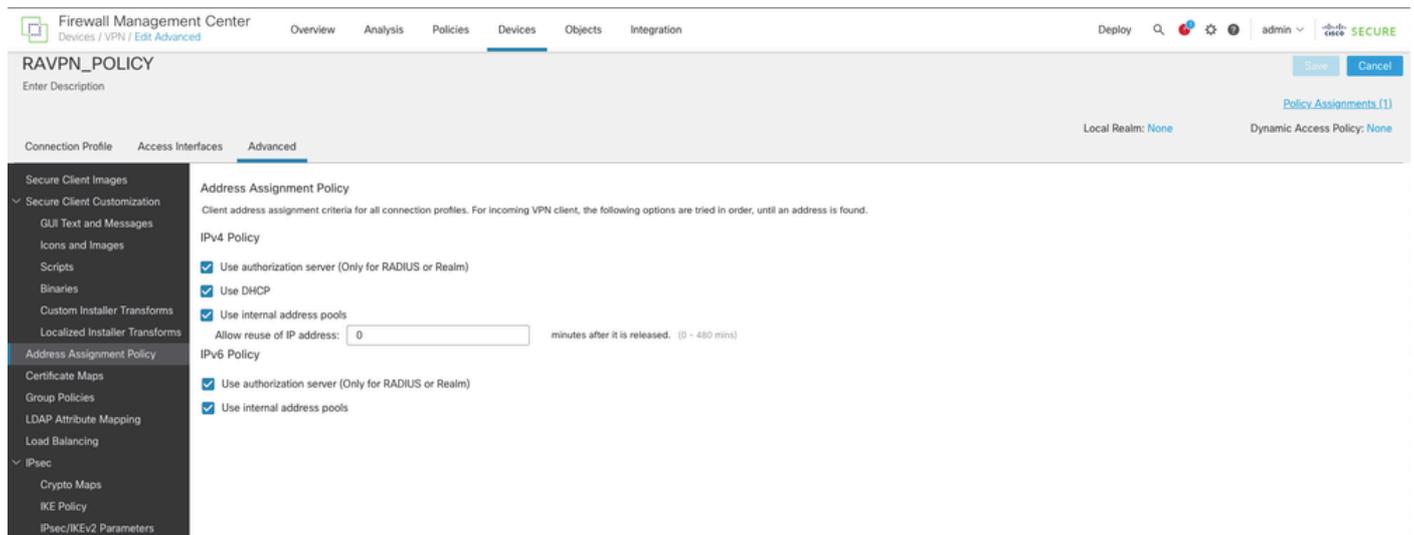
Accounting Server:

▶ Advanced Settings

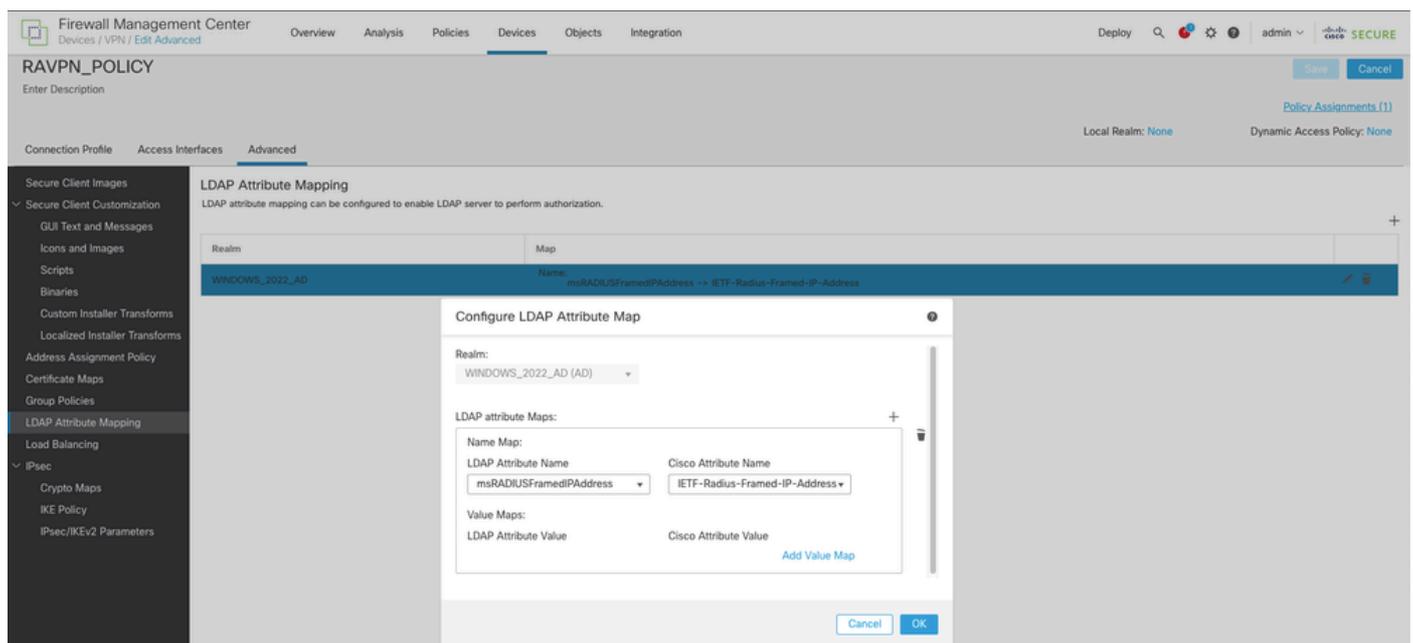
Cancel

Save

Passaggio 2. Passare a Dispositivi > Accesso remoto e selezionare il criterio VPN di Accesso remoto desiderato. Passare a Avanzate > Criterio di assegnazione degli indirizzi e verificare che l'opzione Usa server di autorizzazione (solo per RADIUS o realm) sia abilitata.



Passaggio 3. Selezionare Avanzate > Mappatura attributi LDAP e aggiungere una mappa dei nomi con Nome attributo LDAP impostato su msRADIUSFramedIPAddress e Nome attributo Cisco impostato su IETF-Radius-Framed-IP-Address.



Passaggio 4. Sul server AD di Windows, aprire Server Manager e selezionare Strumenti > Utenti e computer di Active Directory. Fare clic con il pulsante destro del mouse su un utente, selezionare Proprietà > Chiamate in ingresso e selezionare la casella denominata Assegna indirizzi IP statici.

John Doe Properties



Remote control		Remote Desktop Services Profile			COM+
General	Address	Account	Profile	Telephones	Organization
Member Of		Dial-in	Environment		Sessions

Network Access Permission

Allow access

Deny access

Control access through NPS Network Policy

Verify Caller-ID:

Callback Options

No Callback

Set by Caller (Routing and Remote Access Service only)

Always Callback to:

Assign Static IP Addresses

Define IP addresses to enable for this Dial-in connection.

Apply Static Routes

Define routes to enable for this Dial-in connection.

Passaggio 5. Selezionare Indirizzi IP statici e assegnare un indirizzo IP statico all'utente.

Static IP Addresses

Assign a static IPv4 address:

Assign a static IPv6 address:

Prefix:

Interface ID:

Passaggio 6. Connettersi al gateway VPN e accedere utilizzando Cisco Secure Client. All'utente viene assegnato l'indirizzo IP statico configurato.

Cisco Secure Client

Secure Client

- General
- Status Overview
- AnyConnect VPN**
- Zero Trust Access
- Network
- ISE Posture
- Umbrella

Collect diagnostic information for all installed components.

Virtual Private Network (VPN)

Preferences | Statistics | Route Details | Firewall | Message History

Connection Information

State:	Connected
Tunnel Mode (IPv4):	Tunnel All Traffic
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:00:26
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)

Address Information

Client (IPv4):	172.16.20.73
Client (IPv6):	Not Available
Server:	10.0.0.1

Bytes

Verifica

Abilitare debug ldap 255 e verificare che l'attributo LDAP msRADIUSFramedIPAddress sia stato recuperato:

```
[13] Session Start
[13] New request Session, context 0x000015371bf7a628, reqType = Authentication
[13] Fiber started
[13] Creating LDAP context with uri=ldap://192.168.2.101:389
[13] Connection to LDAP server: ldap://192.168.2.101:389, status = Successful
[13] supportedLDAPVersion: value = 3
[13] supportedLDAPVersion: value = 2
[13] Binding as (Administrator@test.example) [Administrator@test.example]
[13] Performing Simple authentication for Administrator@test.example to 192.168.2.101
[13] LDAP Search:
Base DN = [CN=Users,DC=test,DC=example]
Filter = [sAMAccountName=jdoe]
Scope = [SUBTREE]
[13] User DN = [CN=John Doe,CN=Users,DC=test,DC=example]
[13] Talking to Active Directory server 192.168.2.101
[13] Reading password policy for jdoe, dn:CN=John Doe,CN=Users,DC=test,DC=example
[13] Read bad password count 0
[13] Binding as (jdoe) [CN=John Doe,CN=Users,DC=test,DC=example]
[13] Performing Simple authentication for jdoe to 192.168.2.101
[13] Processing LDAP response for user jdoe
[13] Message (jdoe):
[13] Authentication successful for jdoe to 192.168.2.101
[13] Retrieved User Attributes:
[13] objectClass: value = top
[13] objectClass: value = person
[13] objectClass: value = organizationalPerson
[13] objectClass: value = user
[13] cn: value = John Doe
[13] sn: value = Doe
[13] givenName: value = John
[13] distinguishedName: value = CN=John Doe,CN=Users,DC=test,DC=example
[13] instanceType: value = 4
[13] whenCreated: value = 20240928142334.0Z
[13] whenChanged: value = 20240928152553.0Z
[13] displayName: value = John Doe
[13] uSNCreated: value = 12801
[13] uSNChanged: value = 12826
[13] name: value = John Doe
[13] objectGUID: value = .....fA.f...;,
[13] userAccountControl: value = 66048
[13] badPwdCount: value = 0
[13] codePage: value = 0
[13] countryCode: value = 0
[13] badPasswordTime: value = 0
[13] lastLogoff: value = 0
[13] lastLogon: value = 0
[13] pwdLastSet: value = 133720070153887755
[13] primaryGroupID: value = 513
[13] userParameters: value = m: d.
[13] objectSid: value = .....Q=.S....=...Q...
[13] accountExpires: value = 9223372036854775807
[13] logonCount: value = 0
[13] sAMAccountName: value = jdoe
```

```
[13] sAMAccountType: value = 805306368
[13] userPrincipalName: value = jdoe@test.example
[13] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=test,DC=example
[13] msRADIUSFramedIPAddress: value = -1408232375
[13] mapped to IETF-Radius-Framed-IP-Address: value = -1408232375
[13] msRASSavedFramedIPAddress: value = -1408232375
[13] dScorePropagationData: value = 16010101000000.0Z
[13] lastLogonTimestamp: value = 133720093118057231
[13] Fiber exit Tx=522 bytes Rx=2492 bytes, status=1
[13] Session End
```

Risoluzione dei problemi

Comandi debug:

```
debug webvpn 255
```

```
debug ldap
```

Comando per convalidare l'indirizzo IP statico assegnato all'utente RSA VPN desiderato:

```
show vpn-sessiondb anyconnect filter name <nome utente>
```

```
<#root>
```

```
firepower#
```

```
show vpn-sessiondb anyconnect filter name jdoe
```

Session Type: AnyConnect

```
Username : jdoe Index : 7
Assigned IP : 172.16.20.73 Public IP : 10.0.0.10
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14664 Bytes Rx : 26949
Group Policy : DfltGrpPolicy Tunnel Group : RAVPN_PROFILE
Login Time : 11:45:48 UTC Sun Sep 29 2024
Duration : 0h:38m:59s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000700066f93dec
Security Grp : none Tunnel Zone : 0
```

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).