

セキュアなクライアントVPNユーザに対するスタティックIPアドレス割り当ての設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、LDAP属性マップを使用してリモートアクセスVPNユーザにスタティックIPアドレスを割り当てる方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Active Directory (AD)
- Lightweight Directory Access Protocol(LDAP)
- Cisco Secure Firewall脅威対策
- Cisco Secureファイアウォール管理センター


使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Windows Server 2022
- FTDバージョン7.4.2
- FMCバージョン7.4.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

 注:IPアドレス割り当てにレルムを使用し、LDAP属性マップを設定するオプションは、firepowerバージョン6.7以降でサポートされています。先に進む前に、firepowerのバージョンが6.7以降であることを確認してください。

設定

ステップ 1 : Devices > Remote Accessに移動し、目的のRemote Access VPN Policyを選択します。目的の接続プロファイルを選択します。AAAタブで、Authentication ServerとAuthorization Serverのレルムを選択します。

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:

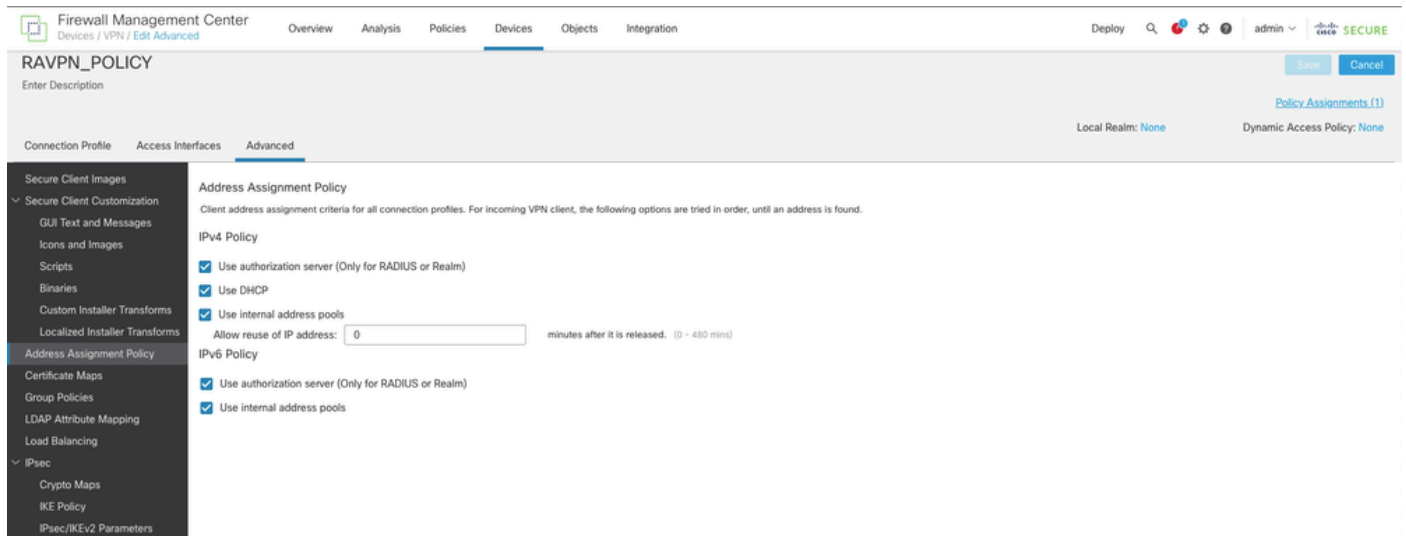
Allow connection only if user exists in authorization database
[Configure LDAP Attribute Map](#)

Accounting

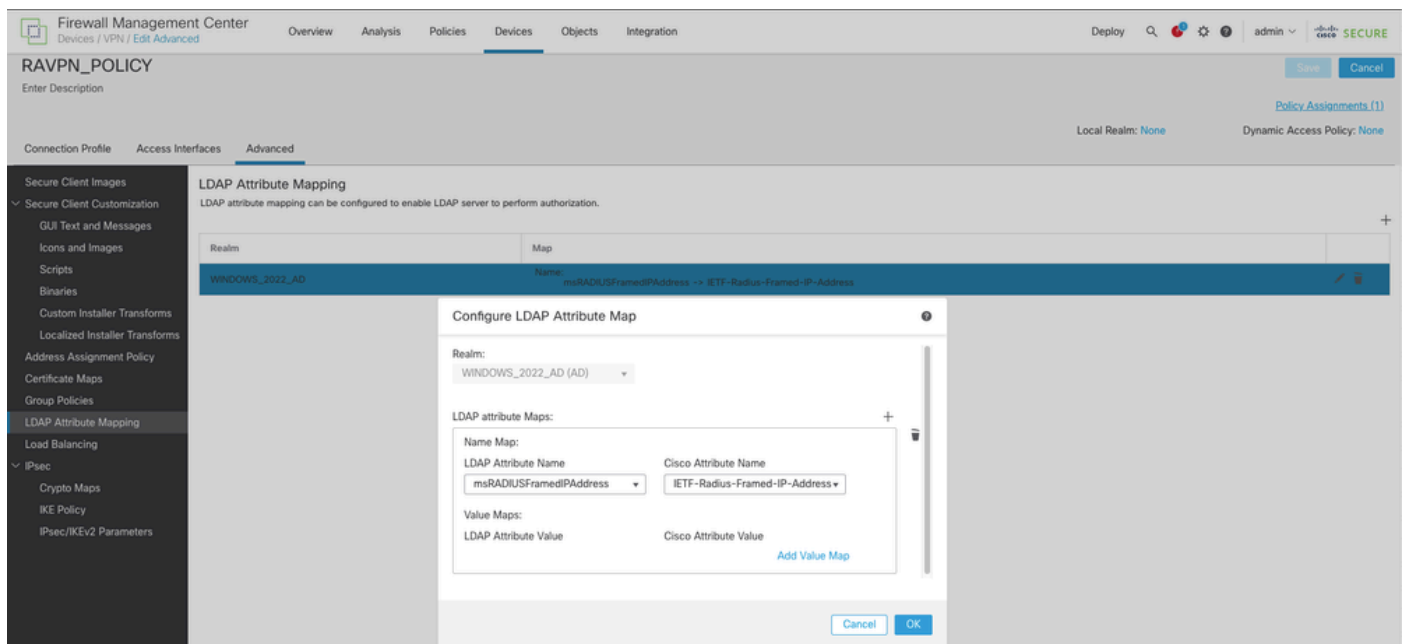
Accounting Server:

▶ Advanced Settings

ステップ 2 : Devices > Remote Accessに移動し、目的のリモートアクセスVPNポリシーを選択します。Advanced > Address Assignment Policyの順に選択し、Use authorization server (Only for RADIUS or Realm)オプションが有効になっていることを確認します。



ステップ 3 : Advanced > LDAP Attribute Mappingの順に移動し、LDAP Attribute NameがmsRADIUSFramedIPAddressに設定され、Cisco Attribute NameがIETF-Radius-Framed-IP-Addressに設定された名前マップを追加します。



ステップ 4 : Windows ADサーバでServer Managerを開き、Tools > Active Directory Users and Computersの順に移動します。userで右クリックして、Properties > Dial-inの順に選択し、Assign Static IP Addressesチェックボックスをオンにします。

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:

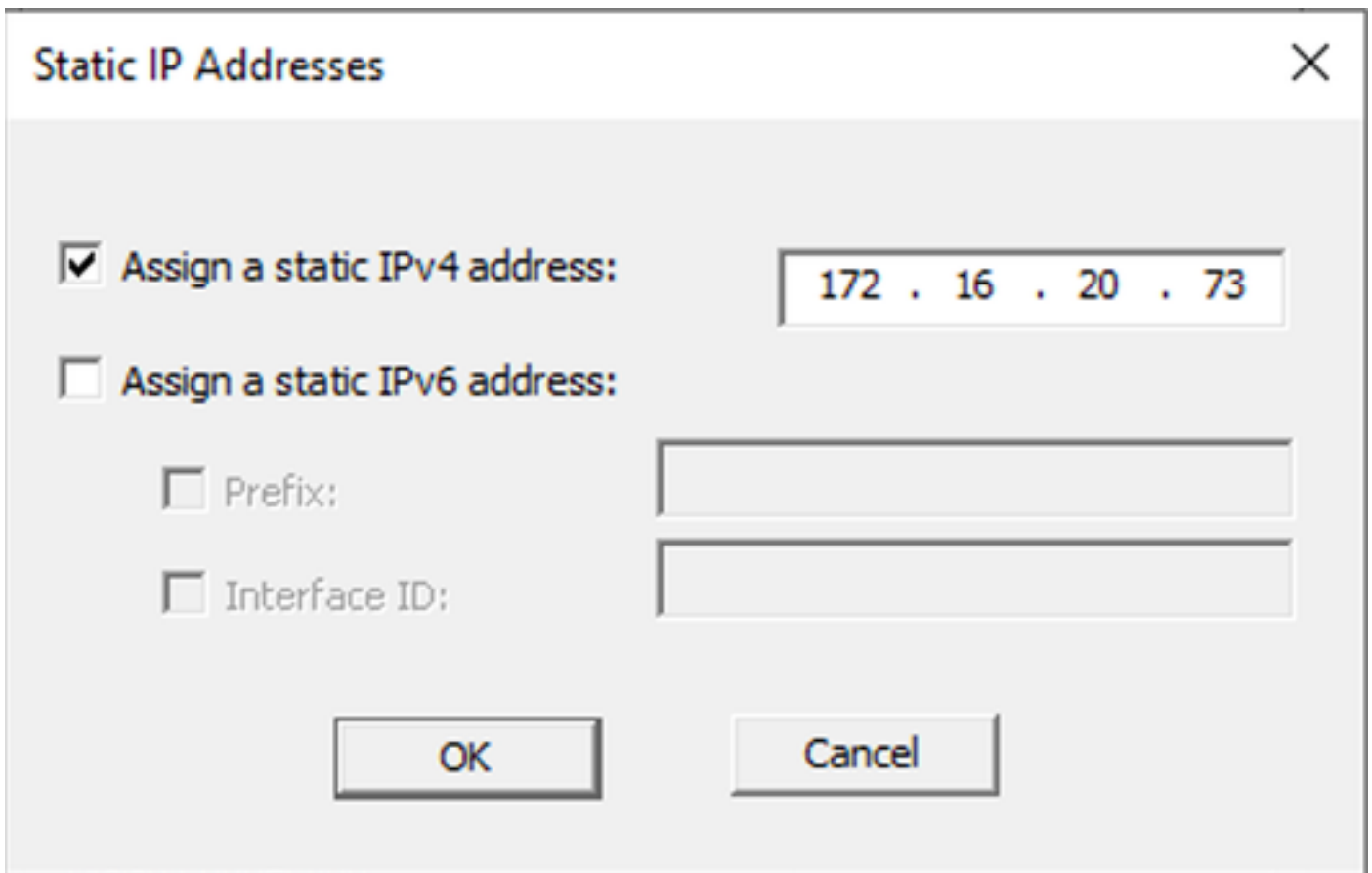
Assign Static IP Addresses

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

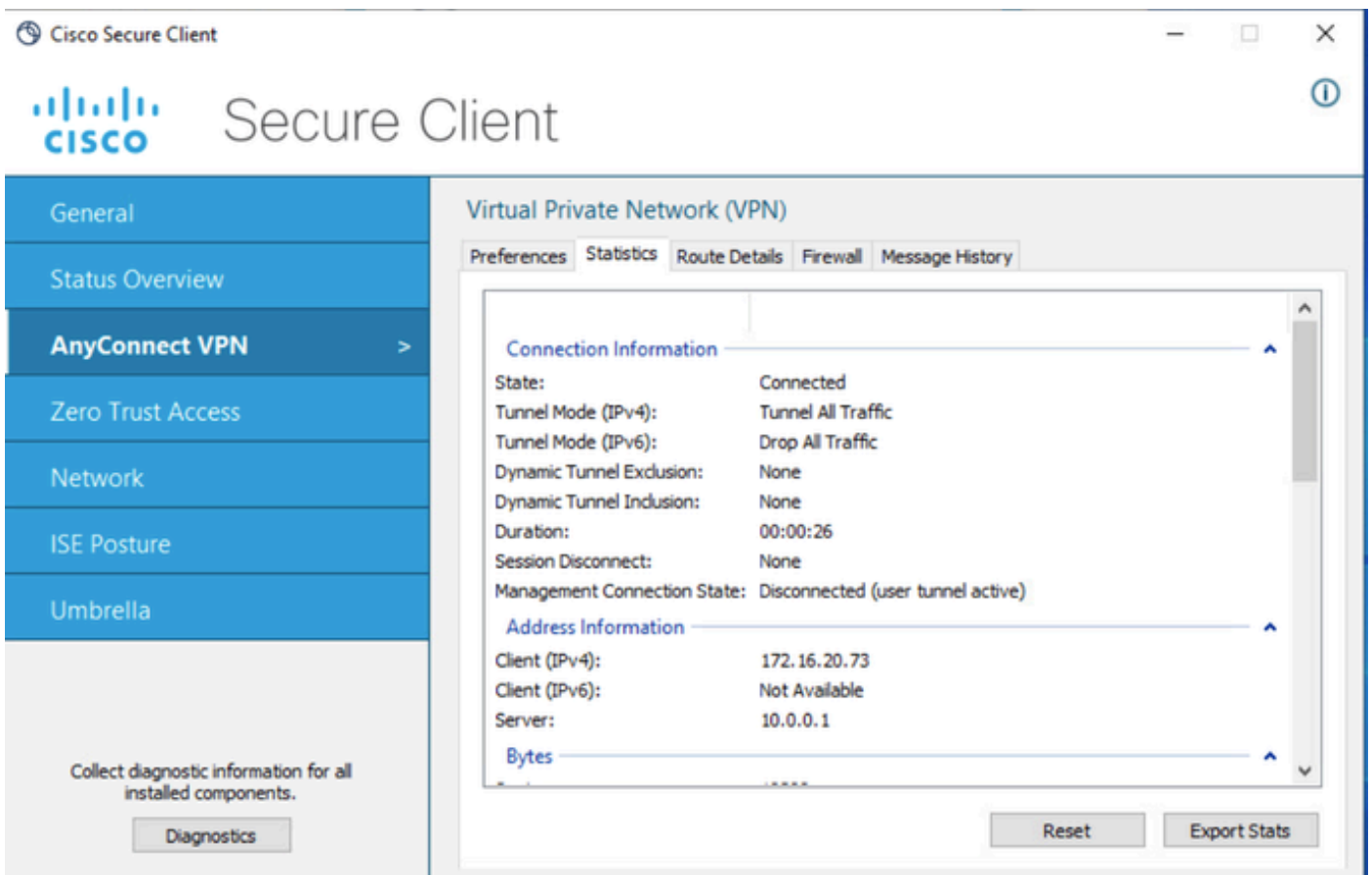
Apply Static Routes

Define routes to enable for this Dial-in connection.

ステップ 5 : Static IP Addressesを選択して、static IP addressをユーザに割り当てます。



手順 6 : VPNゲートウェイに接続し、Cisco Secure Clientを使用してログインします。設定した固定IPアドレスがユーザに割り当てられます。



確認

debug ldap 255を有効にして、msRADIUSFramedIPAddress LDAP属性が取得されることを確認します。

```
[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
```

トラブルシュート

debug コマンド :

```
debug webvpn 255
```

LDAPのデバッグ

目的のRA VPNユーザに割り当てられたスタティックIPアドレスを検証するコマンド :

```
show vpn-sessiondb anyconnect filter name <ユーザ名>
```

```
<#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
```

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。