

配置安全客户端VPN用户的静态IP地址分配

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何使用LDAP属性映射为远程访问VPN用户分配静态IP地址。

先决条件

要求

Cisco 建议您了解以下主题：

- Active Directory (AD)
- 轻量级目录访问协议(LDAP)
- 思科安全防火墙威胁防御
- 思科安全防火墙管理中心


使用的组件

本文档中的信息基于以下软件和硬件版本：

- Windows Server 2022
- FTD版本7.4.2
- FMC版本7.4.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

 **注意：** Firepower 6.7或更高版本支持使用领域进行IP地址分配并配置LDAP属性映射的选项。在继续之前，请确保firepower版本为6.7或更高版本。

配置

步骤1:导航到Devices > Remote Access，然后选择所需的Remote Access VPN Policy。选择所需的Connection Profile。在AAA选项卡下，选择Authentication Server和Authorization Server的领域。

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:

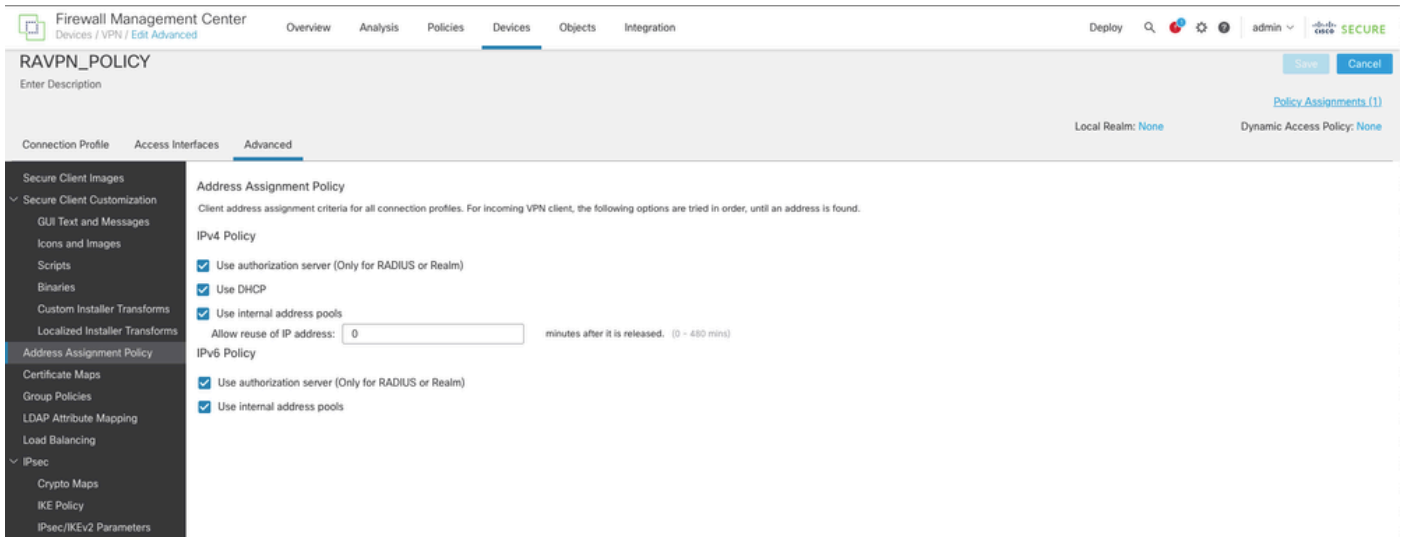
Allow connection only if user exists in authorization database
[Configure LDAP Attribute Map](#)

Accounting

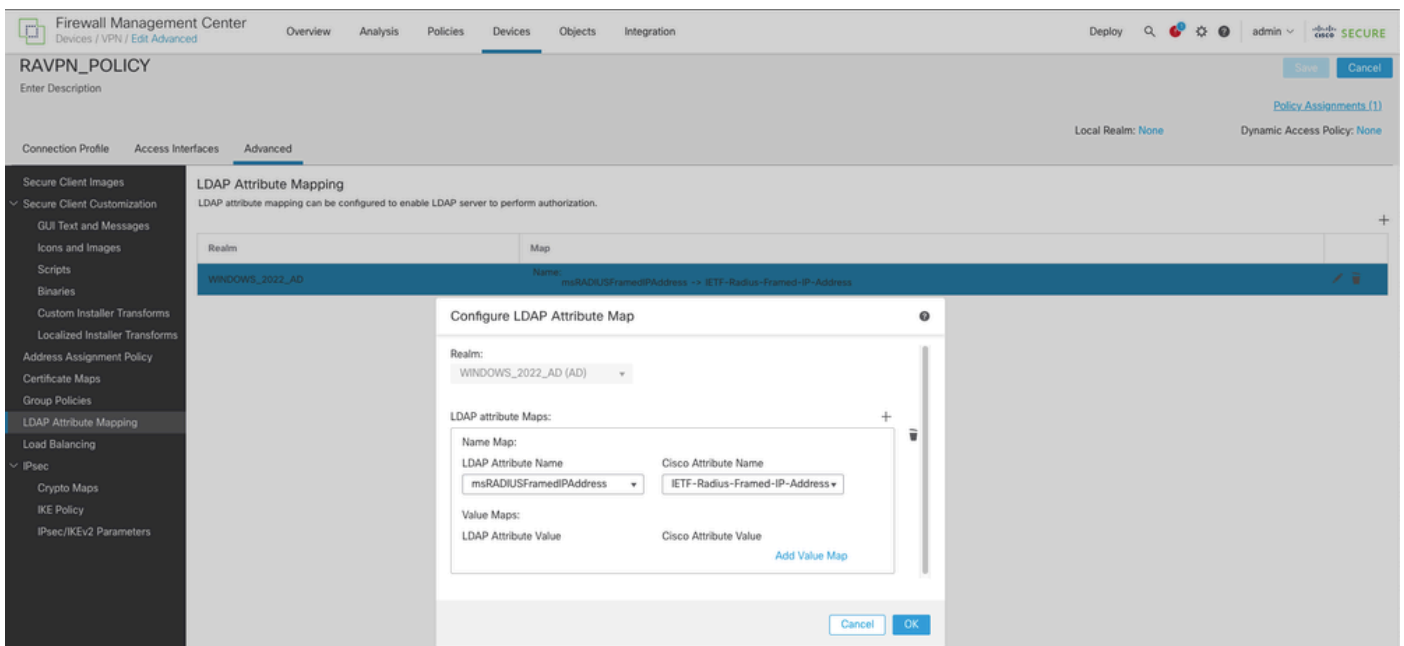
Accounting Server:

▶ Advanced Settings

第二步：导航到Devices > Remote Access，然后选择所需的远程访问VPN策略。导航到高级>地址分配策略，确保启用选项使用授权服务器（仅适用于RADIUS或领域）。



第三步：导航到Advanced > LDAP Attribute Mapping并添加Name Map，其中LDAP Attribute Name set to msRADIUSFramedIPAddress and Cisco Attribute Name set to IETF-Radius-Framed-IP-Address。



第四步：在Windows AD服务器上，打开服务器管理器，然后导航到工具> Active Directory用户和计算机。右键单击用户，选择属性>拨入，然后选中名为分配静态IP地址的框。

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:

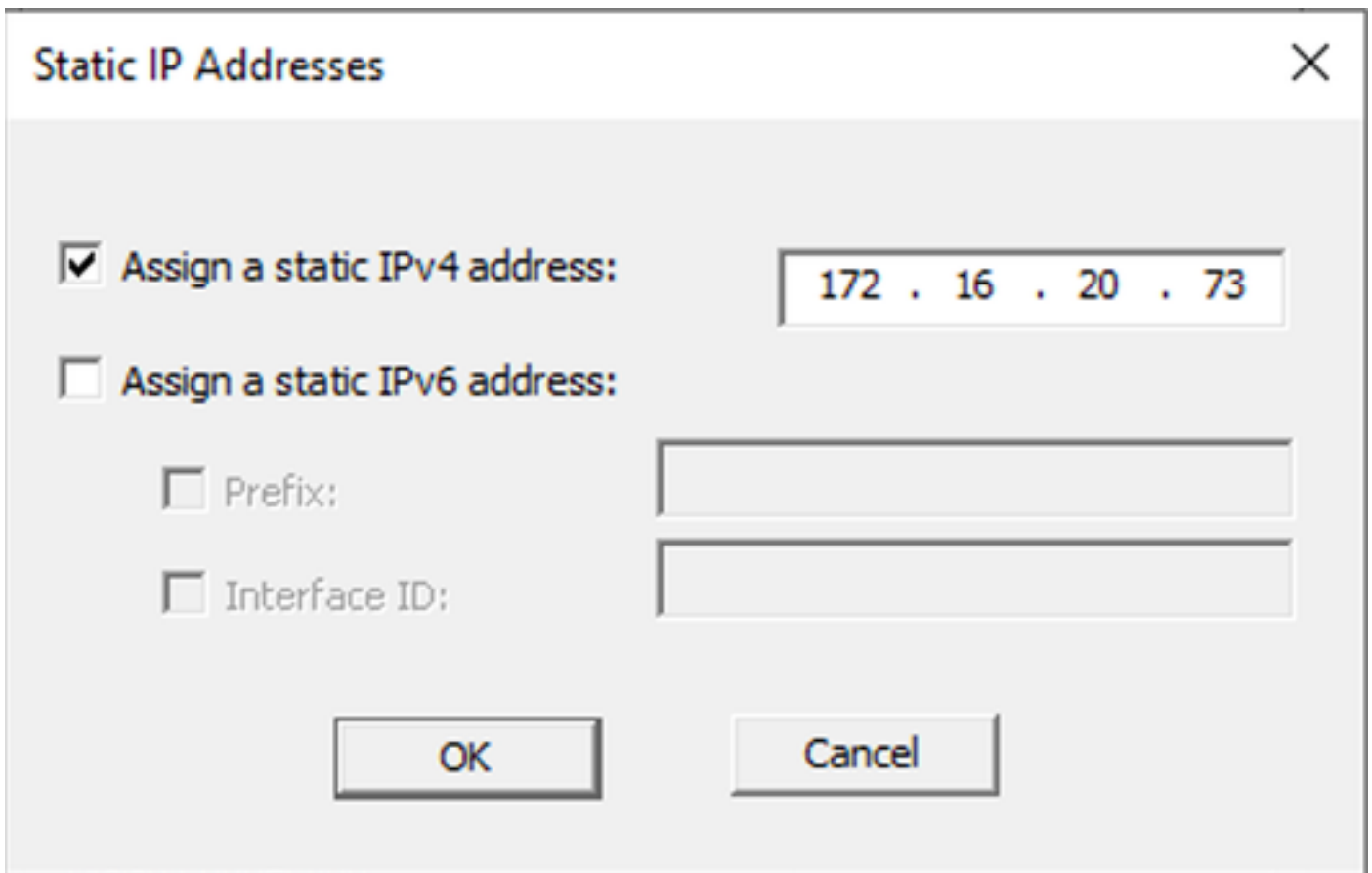
Assign Static IP Addresses

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

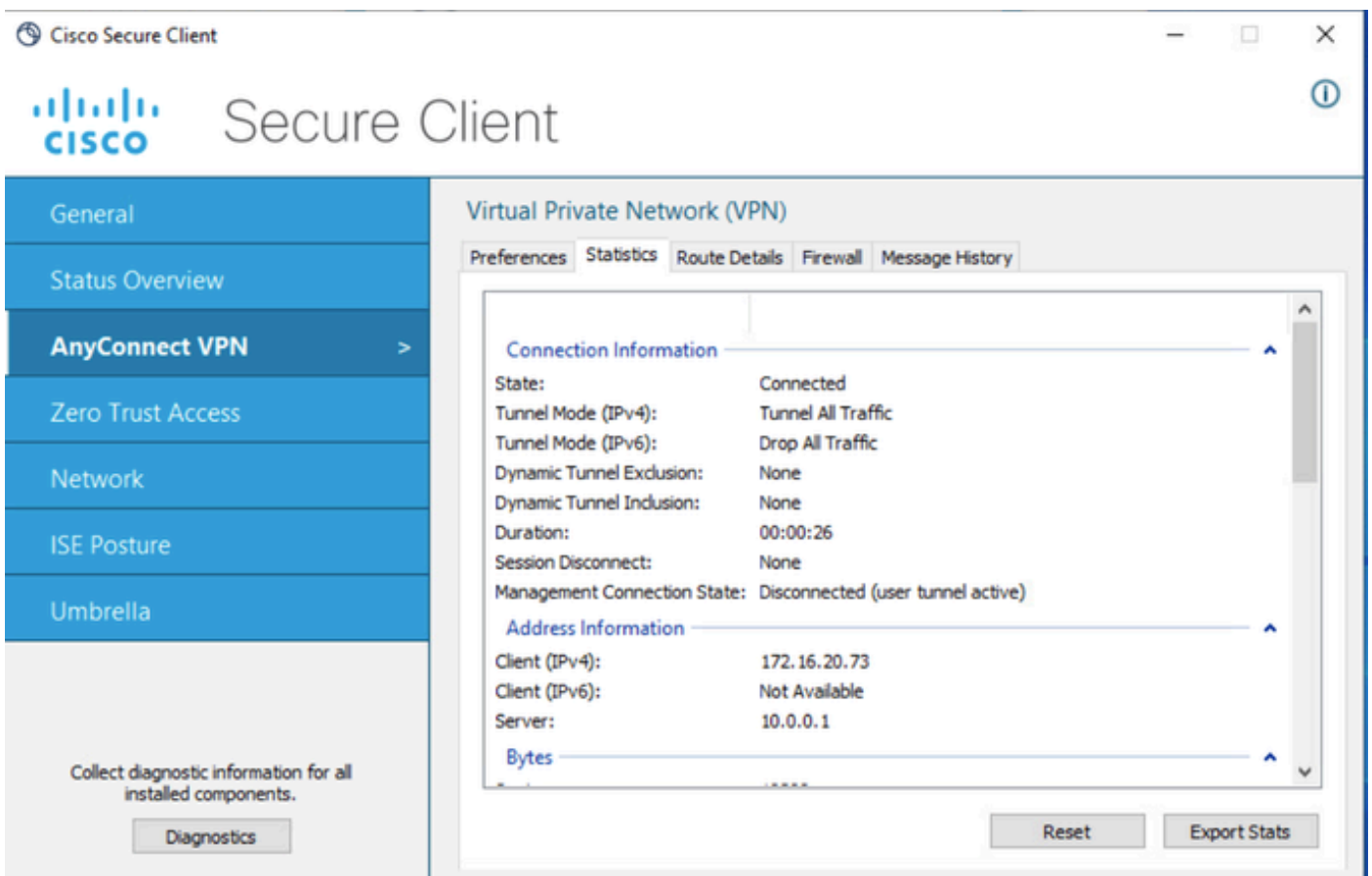
Apply Static Routes

Define routes to enable for this Dial-in connection.

第五步：选择Static IP Addresses并向用户分配静态IP地址。



第六步：连接到VPN网关并使用Cisco安全客户端登录。系统将为用户分配您配置的静态IP地址。



验证

启用debug ldap 255并确保检索到msRADIUSFramedIPAddress LDAP属性：

```
[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] msRASavedFramedIPAddress: 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
```

故障排除

调试命令：

```
debug webvpn 255
```

```
debug ldap
```

用于验证分配给所需RA VPN用户的静态IP地址的命令：

```
show vpn-sessiondb anyconnect filter name <username>
```

```
<#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
```

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。