

Konfigurieren der statischen IP-Adressenzuweisung für sichere Client-VPN-Benutzer

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Remotezugriff-VPN-Benutzern statische IP-Adressen mithilfe einer LDAP-Attributzuordnung zugewiesen werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Active Directory (AD)
- Lightweight Directory Access Protocol (LDAP)
- Cisco Secure Firewall - Schutz vor Bedrohungen
- Cisco Secure Firewall Management Center

Verwendete Komponenten


Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Windows Server 2022
- FTD-Version 7.4.2
- FMC Version 7.4.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

 Hinweis: Die Option, einen Bereich für die IP-Adresszuweisung zu verwenden und LDAP-Attributzuordnungen zu konfigurieren, wird in der Version 6.7 oder höher von firepower unterstützt. Stellen Sie sicher, dass die Version 6.7 oder höher als die Firepower-Version installiert ist, bevor Sie fortfahren.

Konfigurieren

Schritt 1: Navigieren Sie zu Devices (Geräte) > Remote Access (Remote-Zugriff), und wählen Sie die gewünschte VPN-Richtlinie für den Remote-Zugriff aus. Wählen Sie das gewünschte Verbindungsprofil aus. Wählen Sie auf der Registerkarte AAA einen Bereich für den Authentifizierungsserver und den Autorisierungsserver aus.

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

Schritt 2: Navigieren Sie zu Devices (Geräte) > Remote Access (Remote-Zugriff), und wählen Sie die gewünschte Remote Access-VPN-Richtlinie aus. Navigieren Sie zu Erweitert > Adresszuweisungsrichtlinie, und stellen Sie sicher, dass die Option Autorisierungsserver verwenden (nur für RADIUS oder Bereich) aktiviert ist.

The screenshot shows the 'Address Assignment Policy' configuration page in the Firewall Management Center. The page is titled 'RAVPN_POLICY' and has a 'Save' button in the top right corner. The left sidebar contains a navigation menu with categories like 'Secure Client Images', 'Secure Client Customization', 'Address Assignment Policy', and 'IPsec'. The main content area is divided into 'IPv4 Policy' and 'IPv6 Policy' sections. Both sections have checkboxes for 'Use authorization server (Only for RADIUS or Realm)' and 'Use internal address pools'. The IPv4 section also includes a field for 'Allow reuse of IP address' set to '0' and a note 'minutes after it is released. (0 - 480 mins)'.

Schritt 3: Navigieren Sie zu Erweitert > LDAP-Attributzuordnung, und fügen Sie eine Namenszuordnung hinzu, deren LDAP-Attributname auf msRADIUSFramedIPAddress und Cisco Attributname auf IETF-Radius-Framed-IP-Address festgelegt ist.

The screenshot shows the 'LDAP Attribute Mapping' configuration page in the Firewall Management Center. The page is titled 'RAVPN_POLICY' and has a 'Save' button in the top right corner. The left sidebar contains a navigation menu with categories like 'Secure Client Images', 'Secure Client Customization', 'Address Assignment Policy', and 'IPsec'. The main content area is titled 'LDAP Attribute Mapping' and includes a table with columns 'Realm' and 'Map'. A row is visible with 'WINDOWS_2022_AD' in the 'Realm' column and 'msRADIUSFramedIPAddress -> IETF-Radius-Framed-IP-Address' in the 'Map' column. A 'Configure LDAP Attribute Map' dialog box is open, showing the 'Name Map' configuration. The 'Name Map' section has two dropdown menus: 'LDAP Attribute Name' set to 'msRADIUSFramedIPAddress' and 'Cisco Attribute Name' set to 'IETF-Radius-Framed-IP-Address'. The 'Value Maps' section is currently empty, with an 'Add Value Map' link. The dialog box has 'Cancel' and 'OK' buttons at the bottom.

Schritt 4: Öffnen Sie auf dem Windows AD-Server den Server-Manager, und navigieren Sie zu Extras > Active Directory-Benutzer und -Computer. Klicken Sie mit der rechten Maustaste auf einen Benutzer, wählen Sie Eigenschaften > Einwählen aus, und aktivieren Sie das Kontrollkästchen Statische IP-Adressen zuweisen.

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.

Schritt 5: Wählen Sie Statische IP-Adressen aus, und weisen Sie dem Benutzer eine statische IP-Adresse zu.

Static IP Addresses ✕

Assign a static IPv4 address: 172 . 16 . 20 . 73

Assign a static IPv6 address:

Prefix:

Interface ID:

OK
Cancel

Schritt 6: Stellen Sie eine Verbindung zum VPN-Gateway her, und melden Sie sich mit dem Cisco Secure Client an. Dem Benutzer wird die statische IP-Adresse zugewiesen, die Sie konfiguriert haben.

Cisco Secure Client
— □ ✕

Secure Client

ⓘ

General

Status Overview

AnyConnect VPN >

Zero Trust Access

Network

ISE Posture

Umbrella

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

Reset
Export Stats

Collect diagnostic information for all installed components.

Diagnostics

Überprüfung

Aktivieren Sie debug ldap 255, und stellen Sie sicher, dass das LDAP-Attribut msRADIUSFramedIPAddress abgerufen wird:

```
[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
```

Fehlerbehebung

Debug-Befehle:

```
debug webvpn 255
```

```
debug ldap
```

Befehl zur Validierung der statischen IP-Adresse, die dem gewünschten RA VPN-Benutzer zugewiesen ist:

```
show vpn-sessiondb anyconnect filtername <Benutzername>
```

```
<#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
```


Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.