

Konfigurieren von RA VPN mit LDAP-Authentifizierung und -Autorisierung für FTD

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Hintergrundinformationen](#)
- [Lizenzanforderungen](#)
- [Konfigurationsschritte auf FMC](#)
- [Konfiguration des REALM-/LDAP-Servers](#)
- [RA VPN-Konfiguration](#)
- [Überprüfung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Remote Access VPN mit LDAP AA auf einem von einem FirePOWER Management Center verwalteten FirePOWER Threat Defense (FTD) konfiguriert wird.

Voraussetzungen

Anforderungen

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

- Grundkenntnisse der Funktionsweise von Remote Access VPN (RA VPN)
- Navigation durch das FirePOWER Management Center (FMC)
- Konfiguration von LDAP-Diensten (Lightweight Directory Access Protocol) unter Microsoft Windows Server

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco FirePOWER Management Center Version 7.3.0
- Cisco Firepower Threat Defense Version 7.3.0
- Microsoft Windows Server 2016, konfiguriert als LDAP-Server

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

In diesem Dokument wird die Konfiguration von Remote Access VPN (RA VPN) mit LDAP-Authentifizierung und -Autorisierung (Lightweight Directory Access Protocol) auf einer von einem

FirePOWER Management Center (FMC) verwalteten FirePOWER Threat Defense (FTD) beschrieben.

LDAP ist ein offenes, herstellerneutrales, branchenübliches Anwendungsprotokoll für den Zugriff auf und die Verwaltung verteilter Verzeichnisinformationsdienste.

Eine LDAP-Attributzuordnung gleicht Attribute, die im Active Directory (AD)- oder LDAP-Server vorhanden sind, mit Cisco Attributnamen aus. Wenn dann der AD- oder LDAP-Server Authentifizierungsantworten an das FTD-Gerät während des Aufbaus einer VPN-Verbindung für den Fernzugriff zurückgibt, kann das FTD-Gerät anhand dieser Informationen einstellen, wie der AnyConnect-Client die Verbindung abschließt.

RA VPN mit LDAP-Authentifizierung wird auf dem FMC seit Version 6.2.1 unterstützt, und die LDAP-Autorisierung vor FMC Version 6.7.0 wurde über FlexConfig angewiesen, die LDAP Attribute Map zu konfigurieren und mit dem Realm Server zu verknüpfen. Diese Funktion der Version 6.7.0 wurde nun in den RA VPN Configuration Wizard des FMC integriert und erfordert keinen Einsatz von FlexConfig mehr.

Hinweis: Diese Funktion setzt voraus, dass das FMC auf Version 6.7.0 installiert ist, während das verwaltete FTD auf jeder höheren Version als 6.3.0 installiert werden kann.

Lizenzanforderungen

Erfordert AnyConnect Apex-, AnyConnect Plus- oder AnyConnect VPN Only-Lizenzen mit aktivierter exportgesteuerter Funktionalität.

Um die Lizenz zu überprüfen, navigieren Sie zu **System > Licenses > Smart Licenses**.

The screenshot shows the Cisco Smart License Status page. At the top right, it says "Cisco Smart Software Manager" with a red 'x' and a refresh icon. Below this is a table with the following data:

Usage Authorization:	✓	Authorized (Last Synchronized On May 18 2023)
Product Registration:	✓	Registered (Last Renewed On May 18 2023)
Assigned Virtual Account:		SEC TAC
Export-Controlled Features:		Enabled

Below the table is the "Edit Licenses" section. It has a search bar and an "Add" button. There are two columns: "Devices without license" and "Devices with license (1)". The "Devices with license" column contains one entry: "FTD73". At the bottom right, there are "Cancel" and "Apply" buttons.

Konfigurationsschritte auf FMC

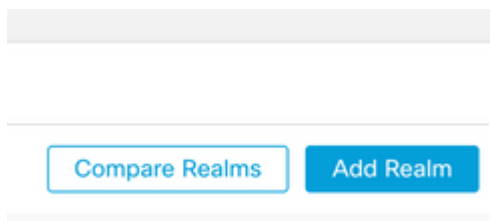
Konfiguration des REALM-/LDAP-Servers

Hinweis: Die aufgeführten Schritte sind nur erforderlich, wenn sie für die Konfiguration eines neuen REALM-/LDAP-Servers erforderlich sind. Wenn Sie über einen vorkonfigurierten Server verfügen, der zur Authentifizierung in RA VPN verwendet werden kann, navigieren Sie zu [RA VPN Configuration](#).

Schritt 1: Navigieren Sie zu System > Other Integrations > Realms, wie in diesem Bild dargestellt.



Schritt 2: Klicken Sie wie in der Abbildung dargestellt auf **Add a new realm**.



Schritt 3: Geben Sie die Details des AD-Servers und des AD-Verzeichnisses an. Klicken Sie auf OK.

Für diese Demonstration gilt Folgendes:

Name: LDAP

Typ: AD

Primäre AD-Domäne: test.com

Verzeichnis-Benutzername: CN=Administrator,CN=Users,DC=test,DC=com

Verzeichniskennwort: <Ausgeblendet>

Basis-DN: DC=test,DC=com

Gruppen-DN: DC=test,DC=com

Add New Realm



Name*	Description
<input type="text"/>	<input type="text"/>
Type	AD Primary Domain
AD	<input type="text"/>
	<small>E.g. domain.com</small>
Directory Username*	Directory Password*
<input type="text"/>	<input type="password"/>
<small>E.g. user@domain.com</small>	
Base DN	Group DN
<input type="text"/>	<input type="text"/>
<small>E.g. ou=group,dc=cisco,dc=com</small>	<small>E.g. ou=group,dc=cisco,dc=com</small>

Directory Server Configuration

^ New Configuration

Hostname/IP Address*	Port*
<input type="text"/>	636
Encryption	CA Certificate*
LDAPS	Select certificate

Interface used to connect to Directory server ⓘ

Resolve via route lookup

Choose an interface

Default: Management/Diagnostic Interface

Test

[Add another directory](#)

Cancel

Configure Groups and Users

Schritt 4: Klicken Sie auf **Save**, um die Realm-/Verzeichnisänderungen zu speichern, wie in diesem Bild dargestellt.

Cancel Save

Schritt 5: Schalten Sie um **State**-Taste, um den Status des Servers in Enabled (Aktiviert) zu ändern, wie in diesem Bild dargestellt.

State

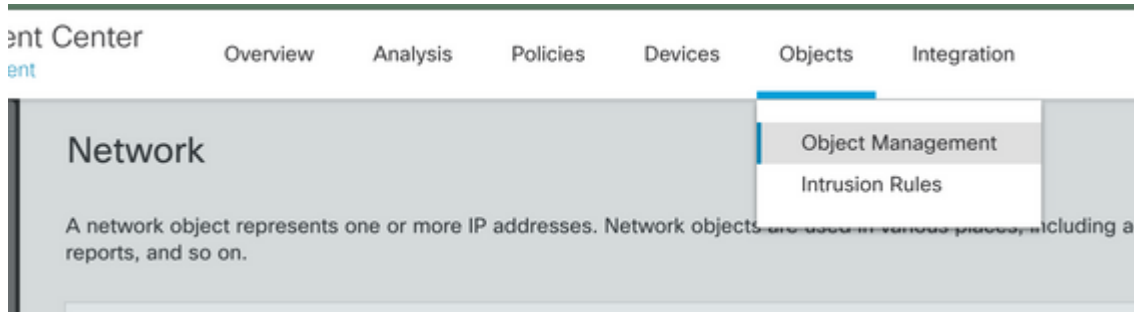
Enabled



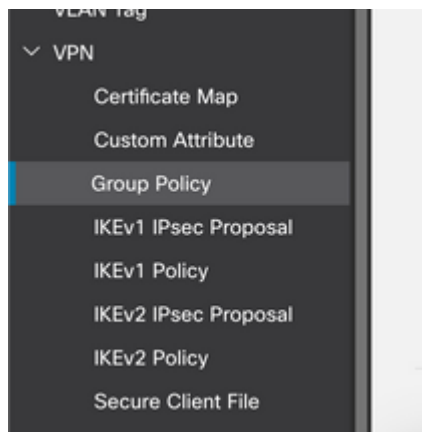
RA VPN-Konfiguration

Diese Schritte sind erforderlich, um die Gruppenrichtlinie zu konfigurieren, die autorisierten VPN-Benutzern zugewiesen wird. Wenn die Gruppenrichtlinie bereits definiert ist, fahren Sie mit [Schritt 5 fort](#).

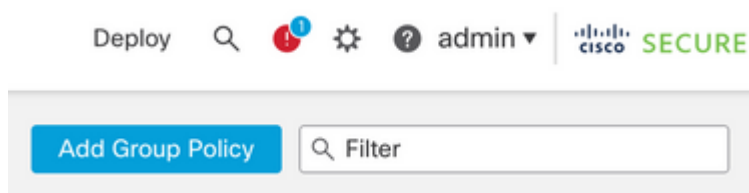
Schritt 1: Navigieren Sie zu Objects > Object Management.



Schritt 2: Navigieren Sie im linken Bereich zu VPN > Group Policy.



Schritt 3: Klicken Add Group Policy.



Schritt 4: Geben Sie die Gruppenrichtlinienwerte an.

Für diese Demonstration gilt Folgendes:

Name: RA-VPN

Banner: ! Willkommen bei VPN!

Gleichzeitige Anmeldung pro Benutzer: 3 (Standard)

Add Group Policy

Name:*

Description:

General Secure Client **Advanced**

VPN Protocols
 IP Address Pools
Banner
 DNS/WINS
 Split Tunneling

Banner:
 Maximum total size: 3999, Maximum characters in a line : 497.
 In case of a line spanning more than 497 characters, split the line into multiple lines.
 ** Only plain text is supported (symbols "<" and ">" are not allowed)

Add Group Policy

Name:*

Description:

General Secure Client **Advanced**

Traffic Filter
Session Settings

Access Hours:
 +

Simultaneous Login Per User:
 (Range 0-2147483647)

Schritt 5: Navigieren Sie zu Devices > VPN > Remote Access.

Devices	Objects	Integration
Device Management	VPN	Troubleshoot
Device Upgrade	Site To Site	File Download
NAT	Remote Access	Threat Defense CLI
QoS	Dynamic Access Policy	Packet Tracer
Platform Settings	Troubleshooting	Packet Capture
FlexConfig		
Certificates		

Schritt 6: Klicken Sie auf Add a new configuration.

Status	Last Modified
No configuration available Add a new configuration	

Schritt 7. Bieten Sie Name für die RA VPN Policy. Auswählen VPN Protocols und wählen Targeted Devices. Klicken Sie auf Next.

Für diese Demonstration gilt Folgendes:

Name: RA-VPN

VPN-Protokolle: SSL

Zielgeräte: FTD

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*
RA-VPN

Description:

VPN Protocols:

SSL
 IPsec-IKEv2

Targeted Devices:

Available Devices
Q Search
FTD73

Selected Devices
FTD73

Add

Schritt 8: Für die Authentication Method, wählen **AAA Only**. Wählen Sie den REALM-/LDAP-Server für die Authentication Server. **Klicken Sie auf [Configure LDAP Attribute Map](#)** (zum Konfigurieren der LDAP-Autorisierung).

AAA

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:* RA-VPN

i This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: AAA Only

Authentication Server:* AD +
(LOCAL or Realm or RADIUS)
 Fallback to LOCAL Authentication

Authorization Server: Use same authentication server +
(Realm or RADIUS)

[Configure LDAP Attribute Map](#)

Schritt 9. Stellen Sie die LDAP Attribute Name und Cisco Attribute Name. **Klicken Sie auf [Add Value Map](#)**.


Für diese Demonstration gilt Folgendes:

LDAP-Attributname: memberOfI

Cisco-Attributname: Gruppenrichtlinie

Configure LDAP Attribute Map ?

Realm:
AD (AD) ▼

LDAP attribute Maps: + 

Name Map:

LDAP Attribute Name	Cisco Attribute Name
memberOf ▼	Group-Policy ▼

Value Maps:

LDAP Attribute Value	Cisco Attribute Value
	Add Value Map


Cancel OK

Schritt 10. Stellen Sie die LDAP Attribute Value und Cisco Attribute Value. Klicken Sie auf **OK**.

Für diese Demonstration gilt Folgendes:

LDAP-Attributwert: DC=tlalocan,DC=sec


Cisco Attributwert: RA-VPN

LDAP attribute Maps: + 

Name Map:

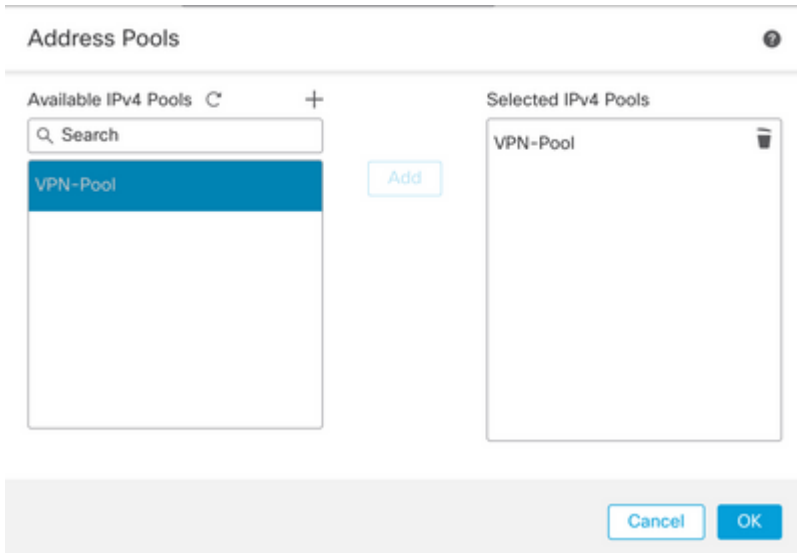
LDAP Attribute Name	Cisco Attribute Name
memberOf ▼	Group-Policy ▼

Value Maps:

LDAP Attribute Value	Cisco Attribute Value
dc=tlalocan,dc=sec	RA-VPN ▼ + 

Hinweis: Sie können weitere Value Maps je nach Anforderung hinzufügen.

Schritt 11. Fügen Sie Address Pool für die lokale Adresszuweisung. Klicken Sie auf **OK**.



Schritt 12: Stellen Sie die **Connection Profile Name** und Group-Policy. Klicken Sie auf Next.

Für diese Demonstration gilt Folgendes:

Name des Verbindungsprofils: RA-VPN

Authentifizierungsmethode: nur AAA

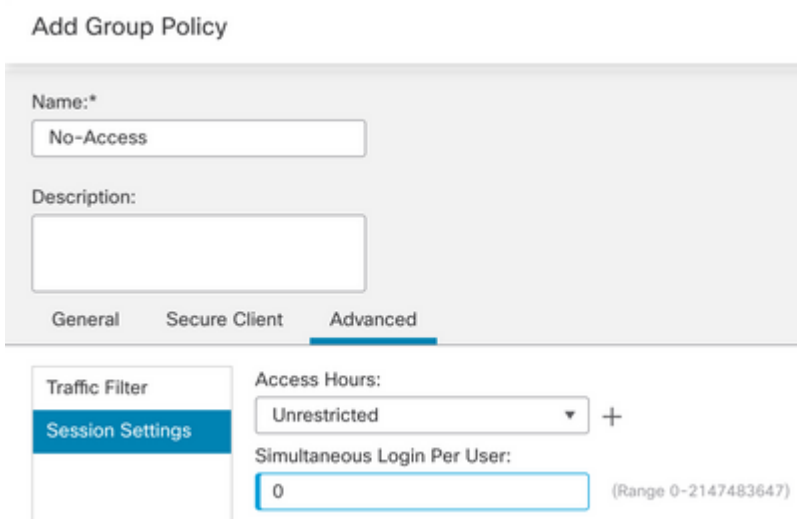
Authentifizierungsserver: LDAP

IPv4-Adresspool: VPN-Pool

Gruppenrichtlinie: Kein Zugriff

Hinweis: Die **Authentifizierungsmethode**, der **Authentifizierungsserver** und der IPV4-Adresspool wurden in den vorherigen Schritten konfiguriert.

Die Gruppenrichtlinie "Kein Zugriff" enthält die Simultaneous Login Per User -Parameter auf 0 gesetzt (um Benutzern nicht die Möglichkeit zu geben, sich anzumelden, wenn sie die Standard-Gruppenrichtlinie "Kein Zugriff" erhalten).



Schritt 13: Klicken Sie auf **Add new AnyConnect Image** um eine **AnyConnect Client Image** an die FTD.

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Select at least one Secure Client image [Show Re-order buttons](#) +

<input checked="" type="checkbox"/> Secure Client File Object Name	Secure Client Package Name	Operating System
No Secure Client Images configured Add new Secure Client Image		

Schritt 14: Bieten Sie Name um das hochgeladene Bild anzuzeigen und im lokalen Speicher zu suchen, um das Bild hochzuladen. Klicken Sie auf Save.

Add Secure Client File ?

Name:*

File Name:*

File Type:*

Description:

Schritt 15: Klicken Sie auf das Kontrollkästchen neben dem Bild, um es zu aktivieren. Klicken Sie auf Next.

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

[Show Re-order buttons](#) +

<input checked="" type="checkbox"/> Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/> Mac	anyconnect-macos-4.10.07061-webdeploy...	Mac OS

Schritt 16: Wählen Sie Interface group/Security Zone und Device Certificate. Klicken Sie auf Next.

Für diese Demonstration gilt Folgendes:

Schnittstellengruppe/Sicherheitszone: Out-Zone

Gerätezertifikat: selbstsigniert

Hinweis: Sie können die Richtlinienoption "Zugriffskontrolle umgehen" aktivieren, um die Zugriffskontrolle für verschlüsselten (VPN) Datenverkehr zu umgehen (standardmäßig deaktiviert).



Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +
 Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +
 Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

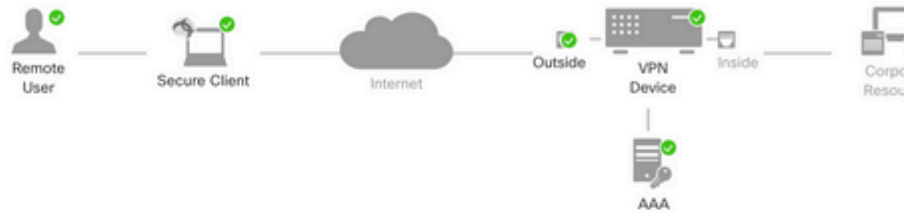
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Schritt 17: Überblick über die RA VPN-Konfiguration anzeigen. Klicken Sie auf **Finish** um zu speichern, wie im Bild gezeigt.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary



Remote Access VPN Policy Configuration

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RA-VPN
Device Targets:	FTD73
Connection Profile:	RA-VPN
Connection Alias:	RA-VPN
AAA:	
Authentication Method:	AAA Only
Authentication Server:	AD (AD)
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	VPN-Pool
Address Pools (IPv6):	-
Group Policy:	No-Access
Secure Client Images:	Mac
Interface Objects:	InZone

Additional Configuration Required

After the wizard completes, the following configuration needs to be completed on all device targets.

- 1 Access Control Policy Update
An Access Control rule must be defined to allow VPN traffic on all targeted devices.
- 1 NAT Exemption
If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.
- 1 DNS Configuration
To resolve hostname specified in the Access Control rule or CA Servers, configure DNS using a DNS Policy on the targeted devices.
- 1 Port Configuration
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and 4500. NAT-Traversal will be enabled on port 443 for image download.

Schritt 18: Navigieren Sie zu Deploy > Deployment. Wählen Sie den FTD aus, auf dem die Konfiguration bereitgestellt werden soll. Klicken Sie auf Deploy.

Die Konfiguration wird nach der erfolgreichen Bereitstellung an die FTD-CLI weitergeleitet:

```
<#root>
```

```
!--- LDAP Server Configuration ---!
```

```
ldap attribute-map LDAP
```

```
map-name memberOf Group-Policy
map-value memberOf DC=tlalocan,DC=sec RA-VPN
```

```
aaa-server LDAP protocol ldap
max-failed-attempts 4
realm-id 2
aaa-server LDAP host 10.106.56.137
server-port 389
ldap-base-dn DC=tlalocan,DC=sec
ldap-group-base-dn DC=tlalocan,DC=sec
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password *****
ldap-login-dn CN=Administrator,CN=Users,DC=test,DC=com
server-type microsoft
```

ldap-attribute-map LDAP

!--- RA VPN Configuration ---!

```
webvpn
enable Outside
anyconnect image disk0:/csm/anyconnect-win-4.10.07061-webdeploy-k9.pkg 1 regex "Mac"
anyconnect enable
tunnel-group-list enable
error-recovery disable
```

```
ssl trust-point Self-Signed
```

```
group-policy No-Access internal
```

```
group-policy No-Access attributes
```

```
vpn-simultaneous-logins 0
```

```
vpn-idle-timeout 30
```

!--- Output Omitted ---!

```
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
```

```
group-policy RA-VPN internal
```

```
group-policy RA-VPN attributes
```

```
banner value ! Welcome to VPN !
```

```
vpn-simultaneous-logins 3
```

```
vpn-idle-timeout 30
```

!--- Output Omitted ---!

```
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list non
```

```
ip local pool VPN-Pool 10.72.1.1-10.72.1.150 mask 255.255.255.0
```

```
tunnel-group RA-VPN type remote-access
```

```
tunnel-group RA-VPN general-attributes
```

```
address-pool VPN-Pool
```

authentication-server-group LDAP

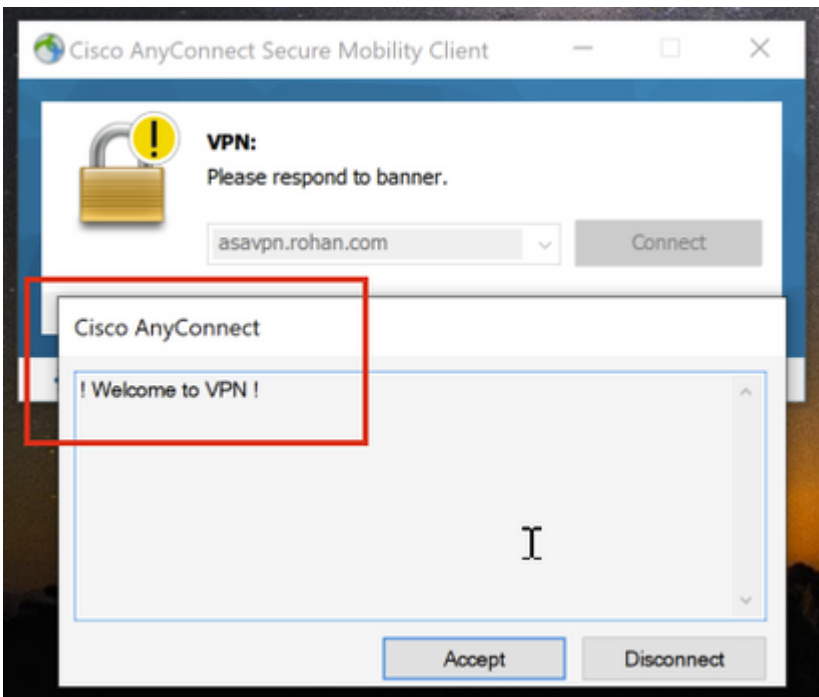
default-group-policy No-Access

tunnel-group RA-VPN webvpn-attributes

group-alias RA-VPN enable

Überprüfung

Melden Sie sich auf dem AnyConnect-Client mit gültigen Anmeldeinformationen für VPN-Benutzergruppen an, und Sie erhalten die richtige Gruppenrichtlinie, die von der LDAP-Attributzuordnung zugewiesen wird:



Im LDAP-Debugausschnitt (debug ldap 255) wird eine Übereinstimmung in der LDAP-Attributzuordnung angezeigt:

```
<#root>
```

```
Authentication successful for test to 10.106.56.137
```

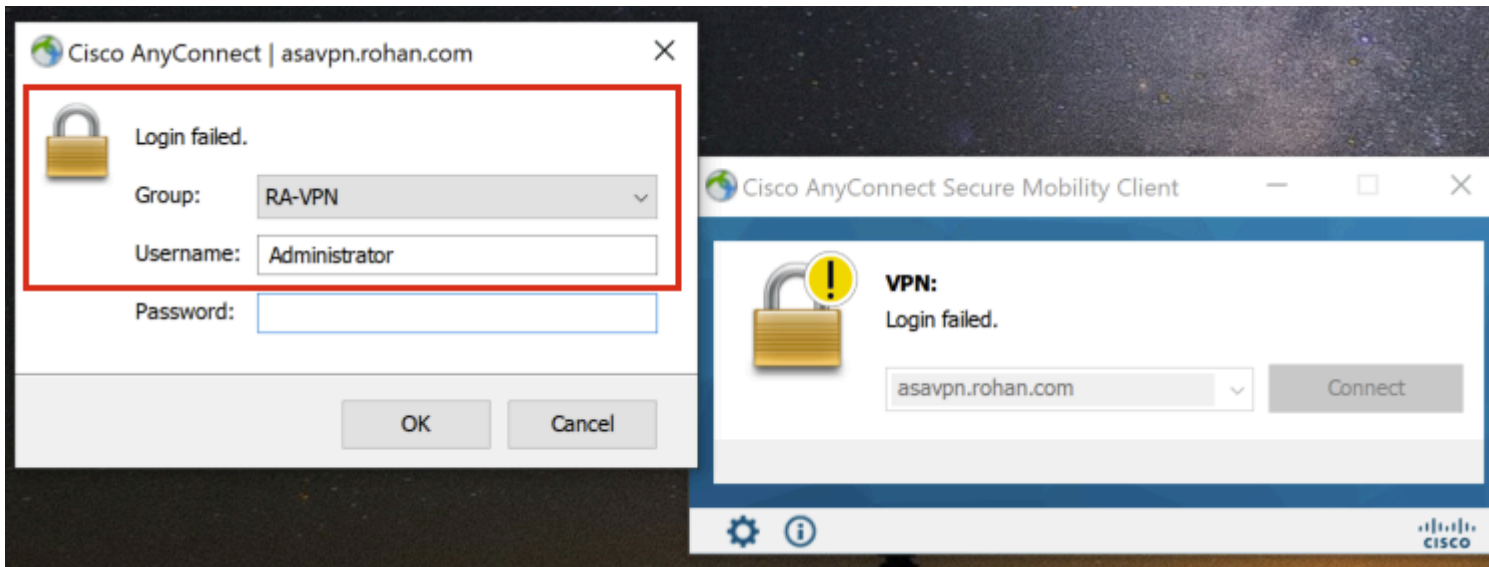
```
memberOf: value = DC=tlalocan,DC=sec
```

```
mapped to Group-Policy: value = RA-VPN
```

```
mapped to LDAP-Class: value = RA-VPN
```

Melden Sie sich auf dem AnyConnect-Client mit ungültigen VPN-Benutzergruppenanmeldeinformationen

an, und Sie erhalten die Gruppenrichtlinie "Kein Zugriff".



```
<#root>
```

```
%FTD-6-113004: AAA user authentication Successful : server = 10.106.56.137 : user = Administrator
```

```
%FTD-6-113009: AAA retrieved default group policy (No-Access) for user = Administrator
```

```
%FTD-6-113013: AAA unable to complete the request Error : reason =
```

```
Simultaneous logins exceeded for user : user = Administrator
```

In LDAP Debug Snippet (debug ldap 255) wird keine Übereinstimmung in der LDAP-Attributzuordnung angezeigt:

```
<#root>
```

```
Authentication successful for Administrator to 10.106.56.137
```

```
memberOf: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec  
  mapped to Group-Policy: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec  
  mapped to LDAP-Class: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec  
memberOf: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec  
  mapped to Group-Policy: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec  
  mapped to LDAP-Class: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec  
memberOf: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec  
  mapped to Group-Policy: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec  
  mapped to LDAP-Class: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec  
memberOf: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec  
  mapped to Group-Policy: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec  
  mapped to LDAP-Class: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec  
memberOf: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec  
  mapped to Group-Policy: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec  
  mapped to LDAP-Class: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec  
memberOf: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec  
  mapped to Group-Policy: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec
```

mapped to LDAP-Class: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec

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.