

Konfigurationsbeispiel für FlexVPN- und AnyConnect IKEv2-Client

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Hub-Konfiguration](#)

[Microsoft Active Directory-Serverkonfiguration](#)

[Client-Konfiguration](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie der Cisco AnyConnect Secure Mobility Client so konfiguriert wird, dass er den Remote Authentication Dial-In User Service (RADIUS) und lokale Autorisierungsattribute verwendet, um sich mit Microsoft Active Directory zu authentifizieren.

Hinweis: Derzeit funktioniert die Verwendung der lokalen Benutzerdatenbank für die Authentifizierung auf Cisco IOS[®] Geräten nicht. Das liegt daran, dass Cisco IOS nicht als EAP-Authentifizierer fungiert. Die [CSCui07025-Anfrage](#) wurde eingereicht, um Unterstützung hinzuzufügen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS Version 15.2(T) oder höher
- Cisco AnyConnect Secure Mobility Client Version 3.0 oder höher
- Microsoft Active Directory

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

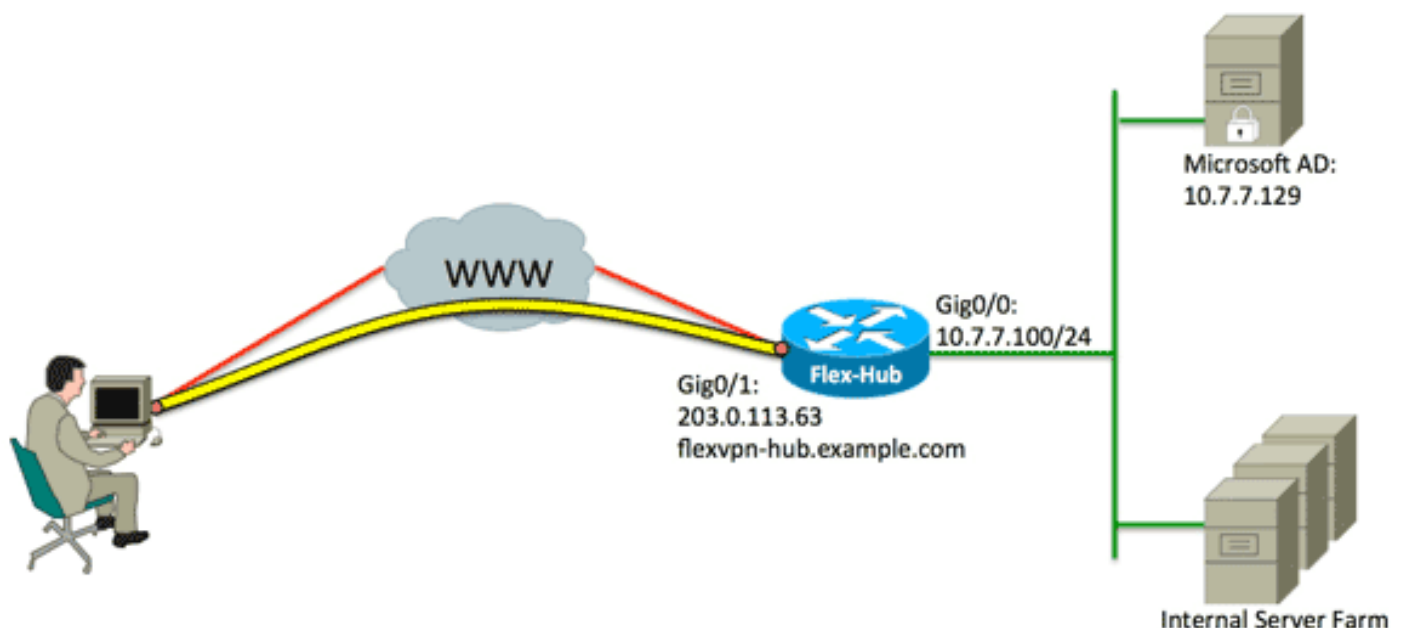
Konfigurieren

In diesem Abschnitt werden die Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen angezeigt.

Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- [Hub-Konfiguration](#)
- [Microsoft Active Directory-Serverkonfiguration](#)
- [Client-Konfiguration](#)

Hub-Konfiguration

1. Konfigurieren Sie RADIUS nur für die Authentifizierung und definieren Sie die lokale Autorisierung.

```
aaa new-model
aaa group server radius FlexVPN-AuthC-Server-Group-1
server-private 10.7.7.129 key Cisco123
aaa authentication login FlexVPN-AuthC-List-1 group
FlexVPN-AuthC-Server-Group-1
aaa authorization network FlexVPN-AuthZ-List-1 local
```

Der Befehl **aaa authentication login list** bezieht sich auf die AAA-Gruppe (Authentication, Authorization, Accounting) (die den RADIUS-Server definiert). Der Befehl **aaa authorized network list** gibt an, dass lokal definierte Benutzer/Gruppen verwendet werden sollen. Die Konfiguration auf dem RADIUS-Server muss geändert werden, um Authentifizierungsanforderungen von diesem Gerät zuzulassen.

2. Konfigurieren Sie die lokale Autorisierungsrichtlinie.

```
ip local pool FlexVPN-Pool-1 10.8.8.100 10.8.8.200
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
pool FlexVPN-Pool-1
dns 10.7.7.129
netmask 255.255.255.0
def-domain example.com
```

Mit dem Befehl **ip local pool** werden die dem Client zugewiesenen IP-Adressen definiert. Eine Autorisierungsrichtlinie wird mit einem Benutzernamen von *FlexVPN-Local-Policy-1* definiert, und hier werden Attribute für den Client (DNS-Server, Netzmaske, Split List, Domänenname usw.) konfiguriert.

3. Stellen Sie sicher, dass der Server zur Selbstauthentifizierung ein Zertifikat (rsa-sig) verwendet.

Für den Cisco AnyConnect Secure Mobility Client muss der Server sich mithilfe eines Zertifikats (rsa-sig) authentifizieren. Der Router muss über ein *Webserver*-Zertifikat (d. h. ein Zertifikat mit 'Serverauthentifizierung' innerhalb der Durchwahl für die erweiterte Schlüsselnutzung) von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) verfügen.

Weitere Informationen finden Sie in den Schritten 1 bis 4 in [ASA 8.x. Installieren Sie die Lizenzzertifikate von Drittanbietern für die Verwendung mit dem WebVPN-Konfigurationsbeispiel manuell](#), und ändern Sie alle Instanzen von *crypto ca* in *crypto pki*.

```
crypto pki trustpoint FlexVPN-TP-1
enrollment url
serial-number none
fqdn flex-hub.example.com
ip-address none
subject-name cn=flex-hub.example.com
revocation-check crl
rsakeypair FlexVPN-TP-1-Key 2048
```

4. Konfigurieren Sie die Einstellungen für diese Verbindung.

```
crypto ikev2 profile FlexVPN-IKEv2-Profile-1
match identity remote key-id example.com
identity local dn
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint FlexVPN-TP-1
dpd 60 2 on-demand
aaa authentication eap FlexVPN-AuthC-List-1
aaa authorization group eap list FlexVPN-AuthZ-List-1
FlexVPN-Local-Policy-1
virtual-template 10
```

Das **crypto ikev2**-Profil enthält die meisten relevanten Einstellungen für diese Verbindung:

- match identity remote key-ID** - Bezieht sich auf die vom Client verwendete IKE-Identität. Dieser Zeichenfolgenwert wird im AnyConnect-XML-Profil konfiguriert.
- identity local dn** - Definiert die IKE-Identität, die vom FlexVPN-Hub verwendet wird. Dieser Wert verwendet den Wert aus dem verwendeten Zertifikat.
- Authentication Remote** - Gibt an, dass EAP für die Client-Authentifizierung verwendet werden soll.
- Authentifizierung lokal** - Staaten, in denen Zertifikate für die lokale Authentifizierung verwendet werden sollen.
- aaa authentication eap**: Gibt an, dass eine Authentifizierungs-Anmeldeleiste FlexVPN-AuthC-List-1 verwendet wird, wenn EAP für die Authentifizierung verwendet wird.
- aaa authorized group eap list** - Staaten, die eine Autorisierungsnetzwerkliste FlexVPN-AuthZ-List-1 mit dem Benutzernamen *FlexVPN-Local-Policy-1* für Autorisierungsattribute verwenden.
- virtual-template 10** - Definiert, welche Vorlage beim Klonen einer virtuellen Zugriffsschnittstelle verwendet werden soll.

5. Konfigurieren Sie ein IPsec-Profil, das wieder mit dem in Schritt 4 definierten IKEv2-Profil verbunden ist.

```
crypto ipsec profile FlexVPN-IPsec-Profile-1
set ikev2-profile FlexVPN-IKEv2-Profile-1
```

Hinweis: Cisco IOS verwendet Smart Defaults. Daher muss ein Transformationssatz nicht explizit definiert werden.

6. Konfigurieren Sie die virtuelle Vorlage, aus der die virtuellen Zugriffsschnittstellen geklont werden:

ip unnumbered (nicht nummerierte IP) - Unnumber the interface from an *Inside* interface,

sodass IPv4-Routing auf der Schnittstelle aktiviert werden kann. **tunnel mode ipsec ipv4** -
Definiert die Schnittstelle als VTI-Typtunnel.

```
interface Virtual-Template10 type tunnel
ip unnumbered GigabitEthernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

7. Beschränken Sie die Aushandlung auf SHA-1. (Optional)

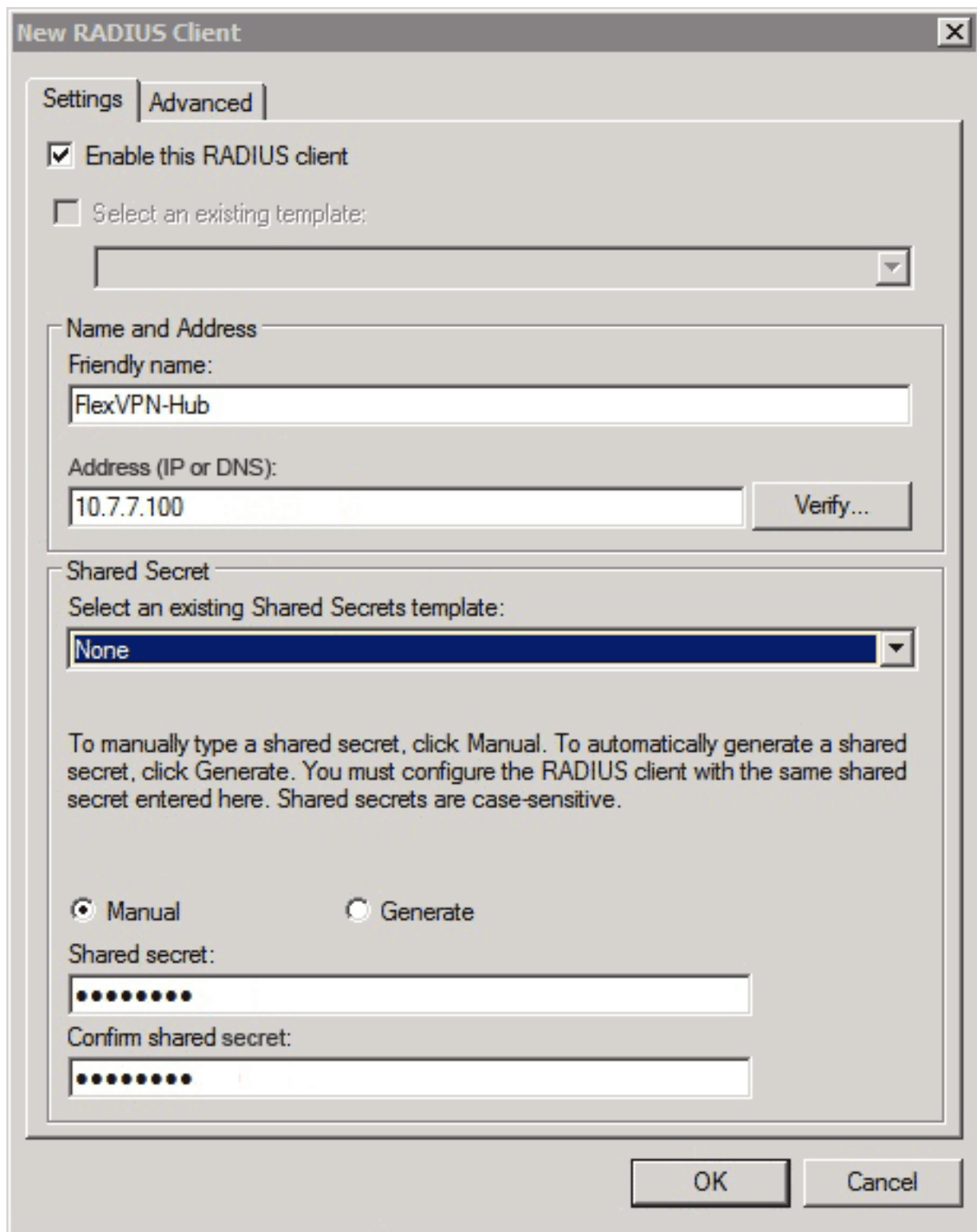
Aufgrund des Defekts [CSCud96246](#) (nur [registrierte](#) Kunden) kann es vorkommen, dass der AnyConnect-Client das FlexVPN Hub-Zertifikat nicht korrekt validiert. Dieses Problem ist darauf zurückzuführen, dass IKEv2 eine SHA-2-Funktion für Pseudo-Random Function (PRF) aushandelt, während das FlexVPN-Hub-Zertifikat mit SHA-1 signiert wurde. Die nachfolgende Konfiguration beschränkt die Aushandlung auf SHA-1:

```
crypto ikev2 proposal SHA1-only
encryption aes-cbc-256
integrity sha1
group 5
crypto ikev2 policy SHA1-only
match fvrf any
proposal SHA1-only
```

Microsoft Active Directory-Serverkonfiguration

1. Erweitern Sie in Windows Server Manager die Optionen **Roles > Network Policy and Access Server > NMPS (Local) > RADIUS Clients and Servers**, und klicken Sie auf **RADIUS Clients**.

Das Dialogfeld Neuer RADIUS-Client wird angezeigt.



2. Fügen Sie im Dialogfeld Neuer RADIUS-Client den Cisco IOS-Router als RADIUS-Client hinzu:

Klicken Sie auf das Kontrollkästchen **Diesen RADIUS-Client aktivieren**. Geben Sie im Feld Freundlicher Name einen Namen ein. In diesem Beispiel wird *FlexVPN-Hub* verwendet. Geben Sie die IP-Adresse des Routers im Feld Adresse ein. Klicken Sie im Bereich "Freier geheimer Schlüssel" auf das Optionsfeld **Manuell**, und geben Sie den freigegebenen geheimen Schlüssel in die Felder "Freier geheim" und "Freigegebene geheime Schlüssel bestätigen" ein. **Hinweis:** Der gemeinsam verwendete geheime Schlüssel muss mit dem auf dem Router konfigurierten gemeinsamen geheimen Schlüssel übereinstimmen. Klicken Sie auf **OK**.

- Erweitern Sie in der Server Manager-Oberfläche **Richtlinien**, und wählen Sie **Netzwerkrichtlinien** aus.

Das Dialogfeld Neue Netzwerkrichtlinie wird angezeigt.

New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:
FlexVPN

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:
Unspecified

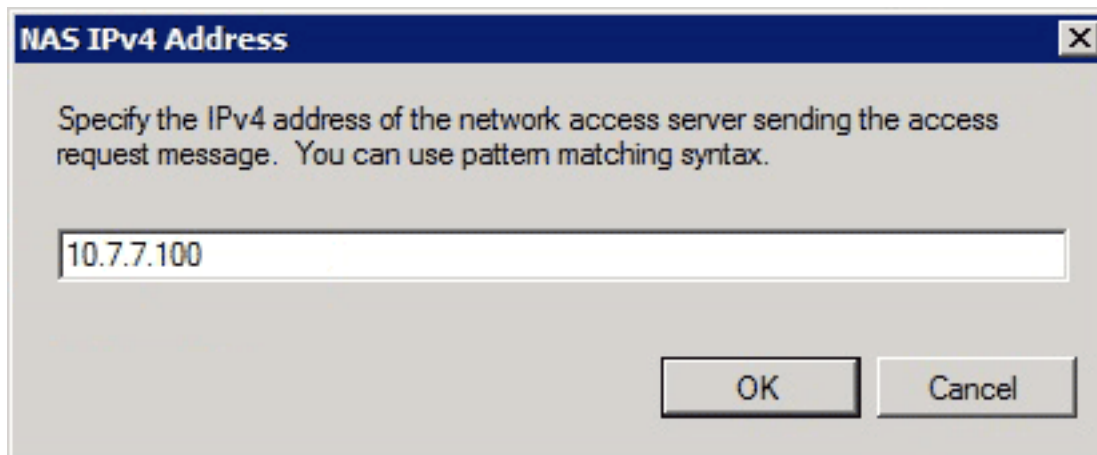
Vendor specific:
10

Previous Next Finish Cancel

- Fügen Sie im Dialogfeld Neue Netzwerkrichtlinie eine neue Netzwerkrichtlinie hinzu:

Geben Sie im Feld Policy name (Richtliniennamen) einen Namen ein. In diesem Beispiel wird *FlexVPN* verwendet. Klicken Sie auf das Optionsfeld **Typ des Netzwerkzugriffsservers**, und wählen Sie **Unspecified (Nicht festgelegt)** aus der Dropdown-Liste aus. Klicken Sie auf **Weiter**. Klicken Sie im Dialogfeld Neue Netzwerkrichtlinie auf **Hinzufügen**, um eine neue Bedingung hinzuzufügen. Wählen Sie im Dialogfeld Select condition (Bedingung auswählen) die Bedingung **NAS IPv4 Address (NAS-IPv4-Adresse)** aus, und klicken Sie auf **Add (Hinzufügen)**.

Das Dialogfeld "NAS-IPv4-Adresse" wird angezeigt.



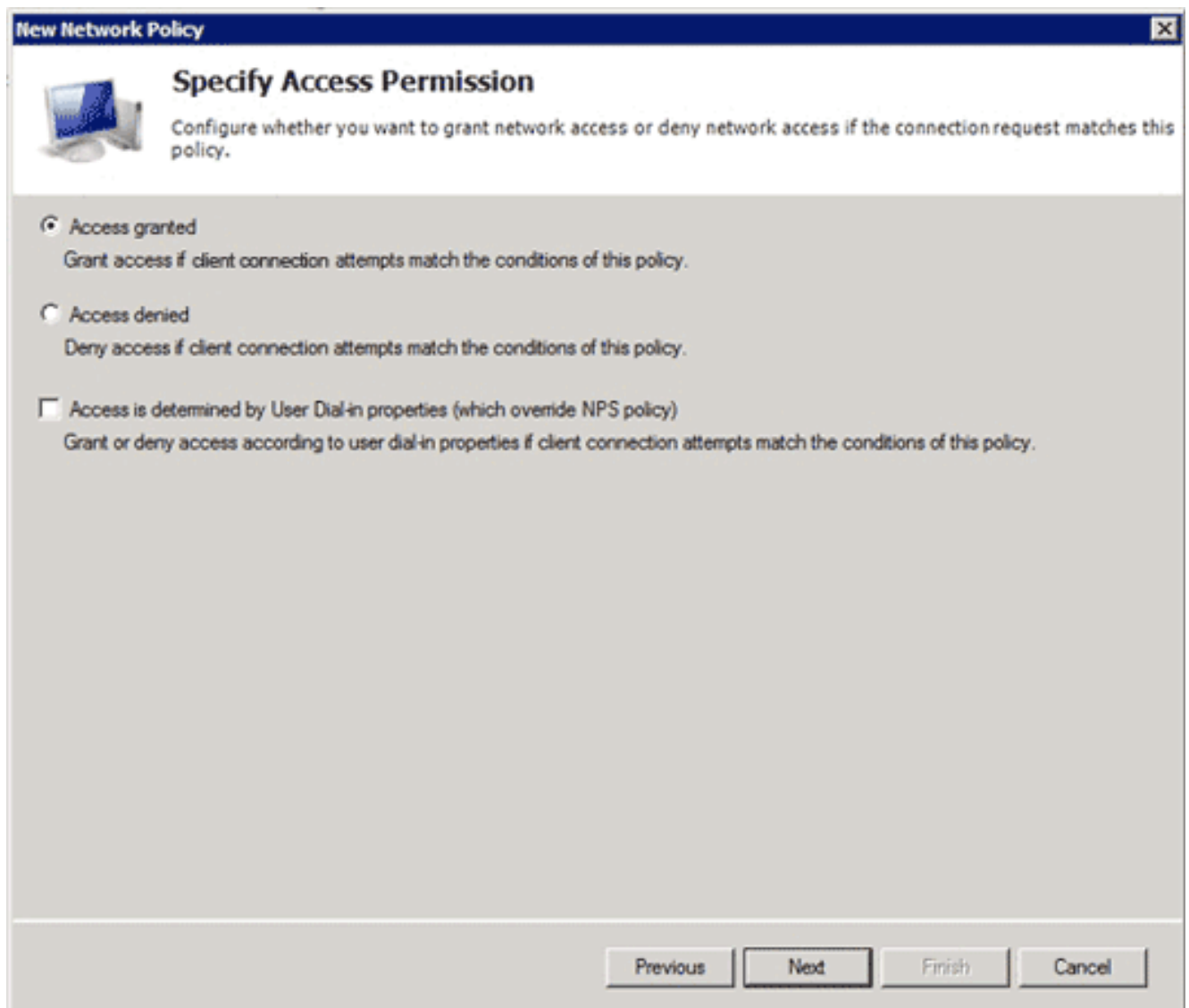
NAS IPv4 Address [X]

Specify the IPv4 address of the network access server sending the access request message. You can use pattern matching syntax.


OK Cancel

Geben Sie im Dialogfeld NAS IPv4 Address (NAS-IPv4-Adresse) die IPv4-Adresse des Netzwerkzugriffsservers ein, um die Netzwerkrichtlinie auf Anfragen zu beschränken, die von diesem Cisco IOS-Router stammen.

Klicken Sie auf **OK**.



New Network Policy [X]

 **Specify Access Permission**

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

Access granted
Grant access if client connection attempts match the conditions of this policy.

Access denied
Deny access if client connection attempts match the conditions of this policy.

Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

Klicken Sie im neuen Dialogfeld Netzwerkrichtlinie auf das Optionsfeld **Access (Zugriff gewährt)**, um dem Client den Zugriff auf das Netzwerk zu ermöglichen (wenn die vom

Benutzer angegebenen Anmeldeinformationen gültig sind), und klicken Sie auf **Next (Weiter)**.

New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

- Microsoft: Secured password (EAP-MSCHAP v2)

Move Up
Move Down

Add... Edit... Remove

Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
 - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method.
- Perform machine health check only

Previous Next Finish Cancel

Nur Microsoft sicherstellen: Im Bereich EAP-Typen wird ein sicheres Kennwort (EAP-MSCHAP v2) angezeigt, damit EAP-MSCHAPv2 als Kommunikationsmethode zwischen dem Cisco IOS-Gerät und Active Directory verwendet werden kann, und klicken Sie auf **Weiter**.

Hinweis: Lassen Sie alle Optionen für 'Weniger sichere Authentifizierungsmethoden' deaktiviert.

Fahren Sie mit dem Assistenten fort, und wenden Sie alle zusätzlichen Einschränkungen oder Einstellungen an, die in den Sicherheitsrichtlinien Ihrer Organisation festgelegt sind. Stellen Sie außerdem sicher, dass die Richtlinie zuerst in der Verarbeitungsreihenfolge aufgeführt wird, wie in diesem Bild gezeigt:

Network Policies



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
FlexVPN	Enabled	1	Grant Acce...	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	2	Deny Access	Unspecified
Connections to other access servers	Enabled	3	Deny Access	Unspecified

FlexVPN

Conditions - If the following conditions are met:

Condition	Value
NAS IPv4 Address	10.7.7.100

Settings - Then the following settings are applied:

Setting	Value
Authentication Method	EAP
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False
Extensible Authentication Protocol Method	Microsoft: Secured password (EAP-MSCHAP v2)

Client-Konfiguration

1. Erstellen Sie ein XML-Profil in einem Text-Editor, und nennen Sie es *flexvpn.xml*.

In diesem Beispiel wird dieses XML-Profil verwendet:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">>false
</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">>true
</AutomaticCertSelection>
<ShowPreConnectMessage>>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>>true
</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">>false
</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">>true
</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">>false
</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">>false
</ClearSmartcardPin>
<AutoReconnect UserControllable="false">>true
<AutoReconnectBehavior UserControllable="false">
DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="true">>false</AutoUpdate>
<RSA SecurIDIntegration UserControllable="false">
Automatic
</RSA SecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon
</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly
</WindowsVPNEstablishment>
<AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
<PPPEExclusion UserControllable="false">Disable
<PPPEExclusionServerIP UserControllable="false">
</PPPEExclusionServerIP>
</PPPEExclusion>
<EnableScripting UserControllable="true">>true
<TerminateScriptOnNextEvent>true
</TerminateScriptOnNextEvent>
<EnablePostSBLOnConnectScript>true
</EnablePostSBLOnConnectScript>
</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">>false
<AutoServerSelectionImprovement>20
</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4
</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
<HostEntry>
```

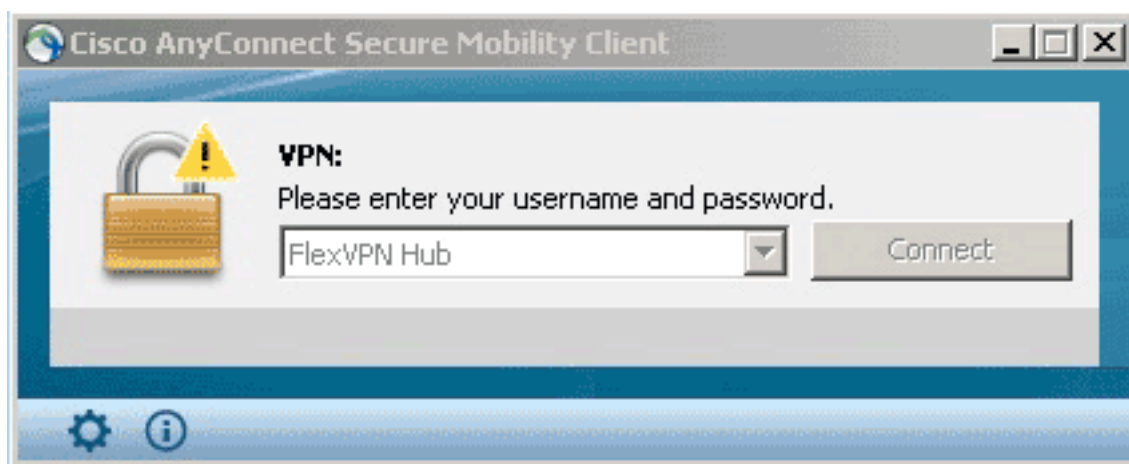
```
<HostName>FlexVPN Hub</HostName>
<HostAddress>flexvpn-hub.example.com</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>EAP-MSCHAPv2</AuthMethodDuringIKENegotiation>
<IKEIdentity>example.com</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

<HostName> ist eine Zeichenfolge, die im Client angezeigt wird.<HostAddress> ist der vollqualifizierte Domänenname (FQDN) des FlexVPN-Hub.<PrimaryProtocol> konfiguriert die Verbindung so, dass sie IKEv2/IPsec anstelle von SSL (der Standardwert in AnyConnect) verwendet.<AuthMethodWährendIKENegotiation> konfiguriert die Verbindung für die Verwendung von MSCHAPv2 innerhalb des EAP. Dieser Wert ist für die Authentifizierung mit Microsoft Active Directory erforderlich.<IKEIdentity> definiert den Zeichenfolgenwert, der dem Client mit einem bestimmten IKEv2-Profil auf dem Hub übereinstimmt (siehe Schritt 4 oben).

Hinweis: Das Clientprofil wird nur vom Client verwendet. Es wird empfohlen, dass ein Administrator den AnyConnect-Profil-Editor verwendet, um das Clientprofil zu erstellen.

2. Speichern Sie die Datei "flexvpn.xml" im entsprechenden Verzeichnis, wie in dieser Tabelle aufgeführt:

3. Schließen und starten Sie den AnyConnect-Client neu.



4. Wählen Sie im Dialogfeld Cisco AnyConnect Secure Mobility Client die Option **FlexVPN Hub**, und klicken Sie auf **Verbinden**.

Cisco AnyConnect | Das Dialogfeld FlexVPN Hub wird angezeigt.



5. Geben Sie einen Benutzernamen und ein Kennwort ein, und klicken Sie auf **OK**.

Überprüfen

Um die Verbindung zu überprüfen, verwenden Sie den Befehl **show crypto session detail remote client-ipaddress**. Weitere Informationen zu diesem Befehl finden Sie unter [show crypto session](#).

Hinweis: Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

Fehlerbehebung

Um die Verbindungsprobleme zu beheben, sammeln und analysieren Sie die DART-Protokolle des Clients und verwenden Sie diese Debug-Befehle auf dem Router: **Debuggen des Crypto iKev2-Pakets** und **Debuggen des Crypto iKev2 intern**.

Hinweis: Weitere Informationen [zu Debug-Befehlen](#) vor der Verwendung von **Debug**-Befehlen finden Sie unter [Wichtige Informationen](#).

Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)