مثال تكوين عميل FlexVPN و AnyConnect IKEv2

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين Cisco AnyConnect Secure Mobility Client لاستخدام خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS) وسمات التخويل المحلية للمصادقة مقابل Microsoft Active Directory.

ملاحظة: حاليا، لا يعمل إستخدام قاعدة بيانات المستخدم المحلي للمصادقة على أجهزة Cisco IOS®. وذلك لأن Cisco IOS لا يعمل كمصدق EAP. تم تصنيف طلب التحسين CSCui07025 لإضافة الدعم.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco IOS، الإصدار 15.2(T) أو إصدار أحدث
- Cisco AnyConnect Secure Mobility Client، الإصدار 3.0 أو إصدار أحدث
- Microsoft Active Directory

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

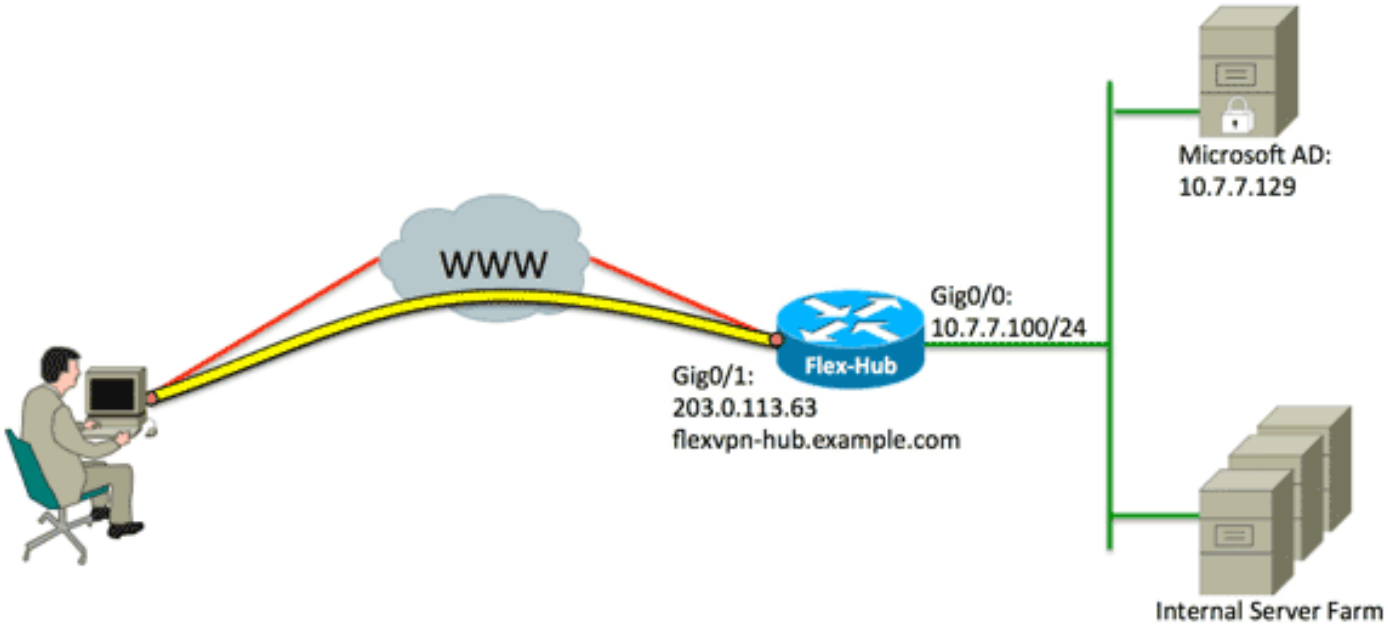
التكوين

في هذا القسم، تقدم لك المعلومات لتكوين الميزات الموضحة في هذا المستند.

استخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المُستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين الموزع
- تكوين خادم Microsoft Active Directory
- تكوين العميل

تكوين الموزع

1. قم بتكوين RADIUS للمصادقة فقط وحدد التفويض المحلي.

```
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
```

يشير أمر **قائمة تسجيل الدخول لمصادقة AAA** إلى مجموعة المصادقة والتخويل والمحاسبة (AAA) (التي تعرف خادم RADIUS). يشير الأمر **aaa authorization network list** إلى أنه يجب إستخدام المستخدمين/المجموعات المحددة محليا. يجب تغيير التكوين على خادم RADIUS للسماح بطلبات المصادقة من هذا الجهاز.

2. قم بتكوين نهج التخويل المحلي.

```
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
```

يتم إستخدام الأمر **ip local pool** لتحديد عناوين IP التي يتم تعيينها إلى العميل. يتم تحديد سياسة تفويض باسم مستخدم ل *FlexVPN-Local-Policy-1*، ويتم تكوين سمات العميل (خوادم DNS، و netmask، وقائمة التقسيم، واسم المجال، وما إلى ذلك) هنا.

3. تأكد من أن الخادم يستخدم شهادة (rsa-sig) لمصادقة نفسه.

يتطلب Cisco AnyConnect Secure Mobility Client أن يقوم الخادم بمصادقة نفسه باستخدام شهادة (rsa-sig). يجب أن يحتوي الموجه على شهادة *خادم ويب* (أي شهادة تحتوي على 'مصادقة الخادم' ضمن ملحق إستخدام المفتاح الموسع) من مرجع مصدق موثوق (CA).

ارجع إلى الخطوات من 1 إلى 4 في [ASA 8.x تثبيت شهادات مورد جهة خارجية يدويا للاستخدام مع مثال تكوين WebVPN](#)، وغير جميع مثيلات مرجع التشفير إلى *تشفير 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. تكوين إعدادات هذا الاتصال.

```
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
```

يحتوي ملف تعريف **crypto ikev2** على معظم الإعدادات ذات الصلة لهذا الاتصال: **مطابقة معرف المفتاح البعيد للهوية** - يشير إلى معرف IKE المستخدم من قبل العميل. يتم تكوين قيمة السلسلة هذه داخل ملف تعريف AnyConnect XML.**Identity Local dn** - يحدد هوية IKE المستخدمة من قبل موزع FlexVPN. تستخدم هذه القيمة القيمة من داخل الشهادة المستخدمة.**المصادقة عن بعد** - يحدد ضرورة إستخدام EAP لمصادقة العميل.**المصادقة المحلية** - يشير إلى أنه يجب إستخدام الشهادات للمصادقة المحلية.**AAA مصادقة** - EAP حالات لاستخدام قائمة تسجيل الدخول لمصادقة AAA FlexVPN-AuthC-List-1 عند إستخدام EAP للمصادقة.**قائمة EAP الخاصة بمجموعة تفويض AAA** - الحالات التي تستخدم قائمة تفويض شبكة AAA FlexVPN-AuthZ-List-1 باسم مستخدم *FlexVPN-Local-Policy-1* لسمات التفويض.**القالب الظاهري 10** - يحدد القالب الذي سيتم إستخدامه عند نسخ واجهة الوصول الظاهري.

5. قم بتكوين ملف تعريف IPsec الذي يرتبط مرة أخرى بملف تعريف IKEv2 المحدد في الخطوة 4.

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

ملاحظة: يستخدم Cisco IOS الإعدادات الافتراضية الذكية. ونتيجة لذلك، لا يلزم تعريف مجموعة تحويل بشكل صريح.

6. تكوين القالب الظاهري الذي يتم من خلاله نسخ واجهات الوصول الظاهري:
IP غير مرقم - إلغاء رقم الواجهة من واجهة *داخلية* حتى يمكن تمكين توجيه IPv4 على الواجهة.**IPv4 لوضع النفق -** يحدد الواجهة لتكون نفق نوع VTI.

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

7. قصر التفاوض على SHA-1. (إختياري)

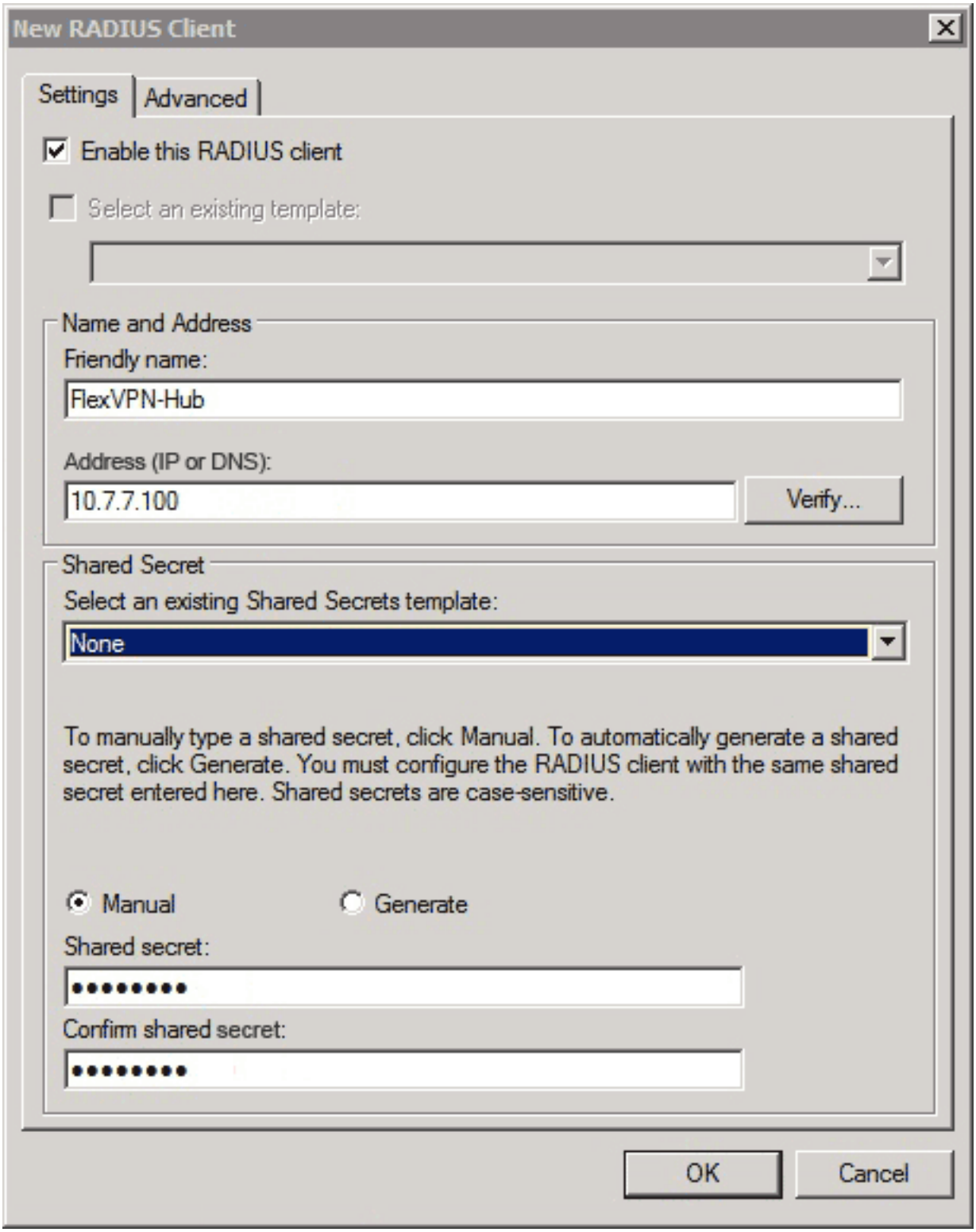
بسبب الخلل CSCud96246 (العملاء المسجلون فقط)، قد يفشل عميل AnyConnect في التحقق بشكل صحيح من صحة شهادة محور FlexVPN. ترجع هذه المشكلة إلى تفاوض IKEv2 على وظيفة SHA-2 للدالة شبه العشوائية (PRF) في حين تم توقيع شهادة FlexVPN-Hub باستخدام SHA-1. يحدد التكوين أدناه التفاوض على SHA-1:

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

تكوين خادم Microsoft Active Directory

في Windows Server Manager، قم بتوسيع **الأدوار > سياسة الشبكة وخادم الوصول > NMPS (محلي)** ⇐. **عملاء RADIUS وخوادم**، وانقر فوق **عملاء RADIUS**.

يظهر مربع الحوار عميل RADIUS الجديد.

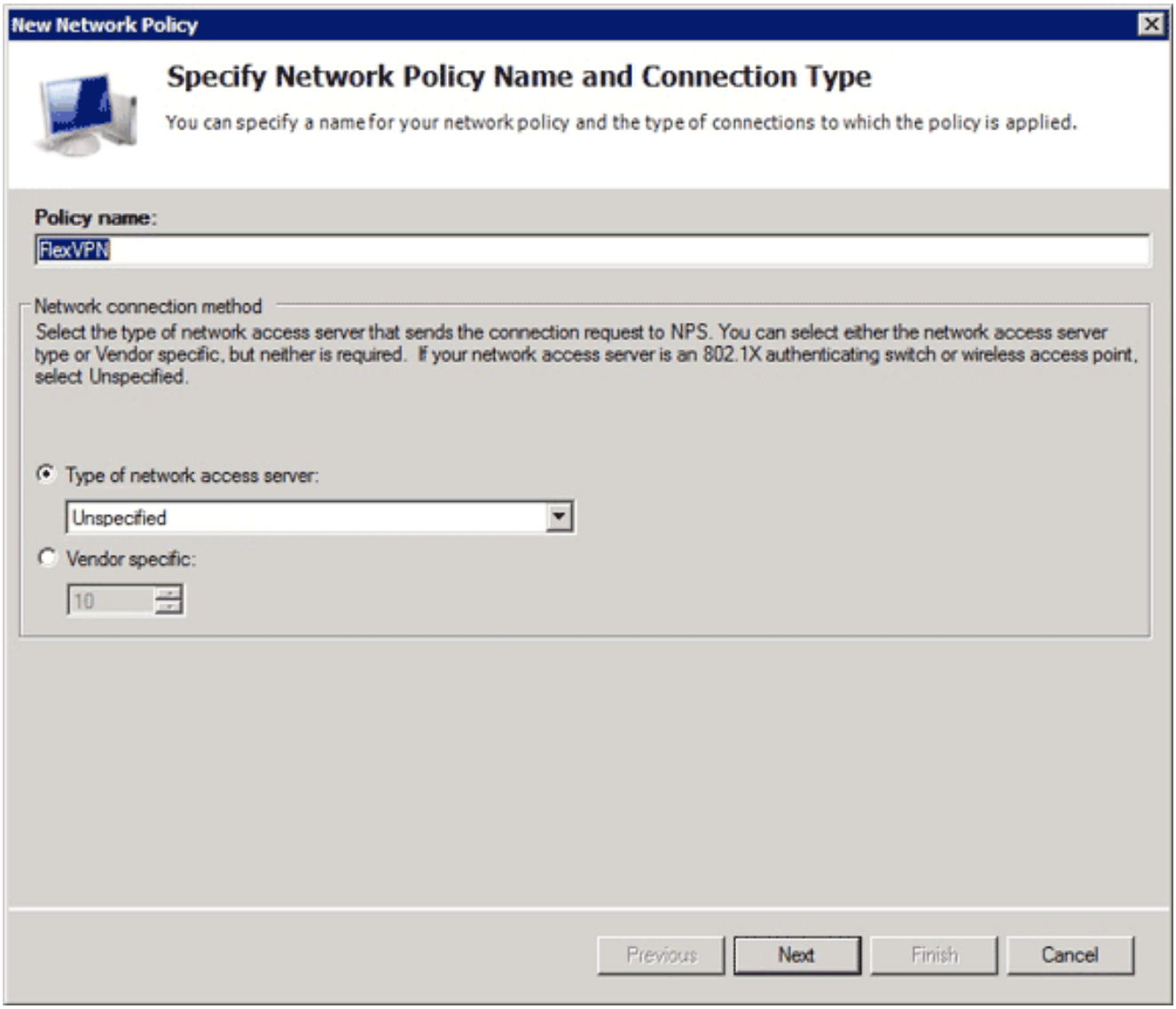


2. في شاشة عميل RADIUS الجديد، أضف موجه Cisco IOS كعميل RADIUS:
انقر فوق خانة الاختيار **تمكين عميل RADIUS هذا**.أدخل اسما في حقل الاسم المألوف. يستخدم هذا المثال *FlexVPN-Hub*.أدخل عنوان IP الخاص بالموجه في حقل العنوان.في منطقة "سر مشترك"، انقر زر **انتقاء**

يدوي، وأدخل السر المشترك في حقلي "سر مشترك" و"تأكيد سر مشترك".**ملاحظة:** يجب أن يتطابق السر المشترك مع السر المشترك الذي تم تكوينه على الموجه.وانقر فوق OK.

3. في واجهة "مدير الخادم"، قم بتوسيع **السياسات**، واختر **سياسات الشبكة**.

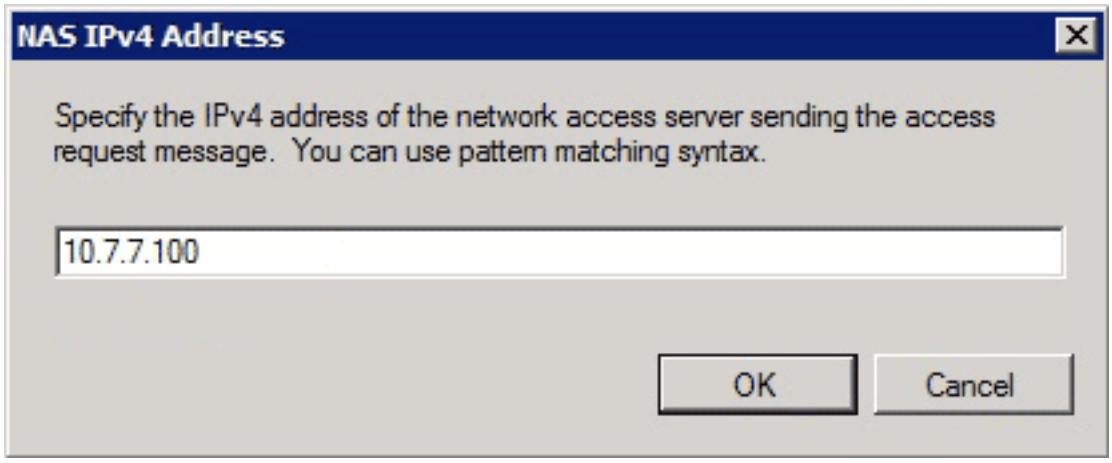
يظهر مربع الحوار "نهج الشبكة الجديد".



4. في شاشة نهج الشبكة الجديدة، أضف نهج شبكة جديد:

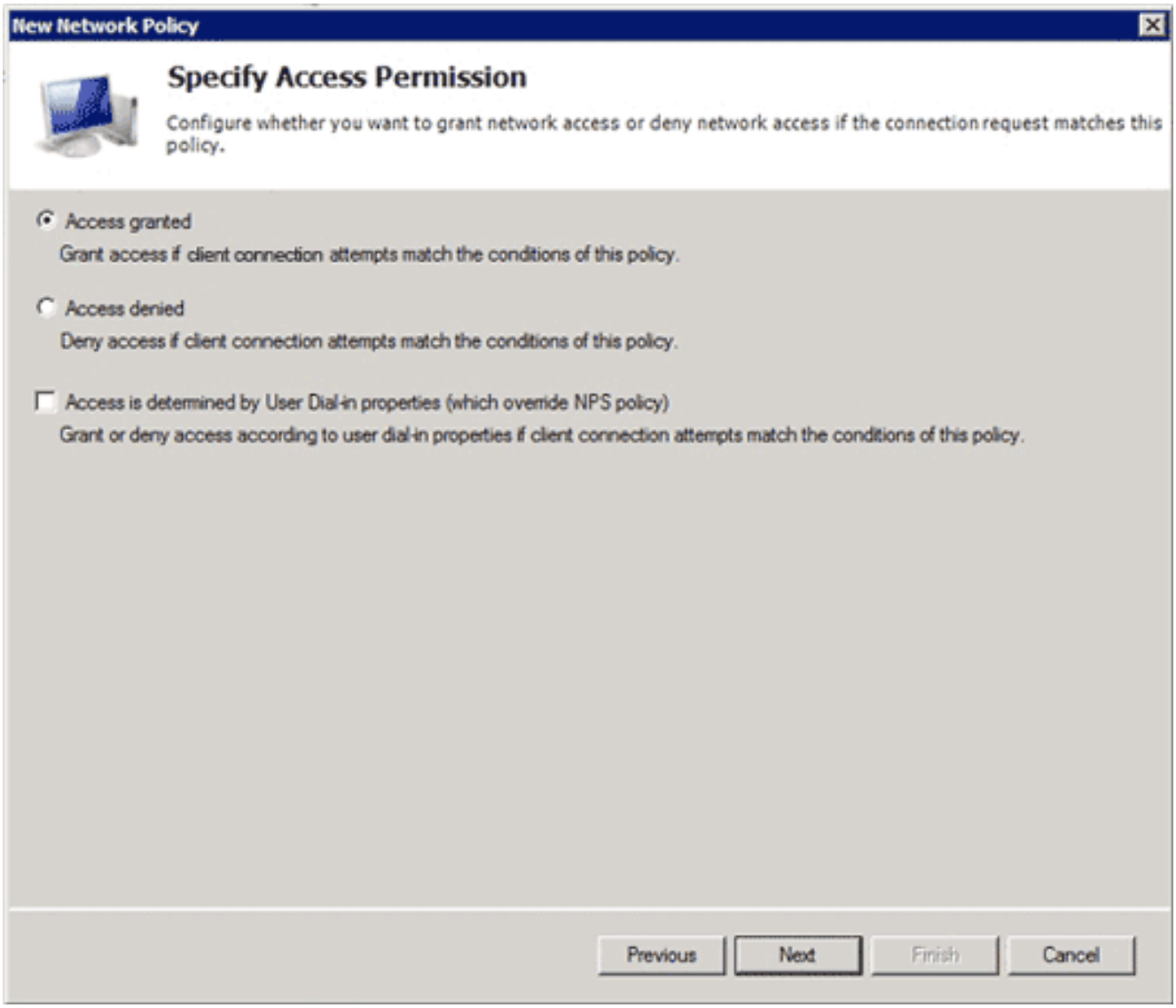
أدخل اسما في حقل اسم النهج. يستخدم هذا المثال *FlexVPN*.انقر فوق زر **نوع** راديو **خادم الوصول إلى الشبكة**، واختر **غير محدد** من القائمة المنسدلة.انقر فوق Next (التالي).في شاشة نهج الشبكة الجديدة، انقر فوق **إضافة** لإضافة شرط جديد.في شاشة تحديد شرط، حدد حالة **عنوان NAS IPv4**، وانقر **إضافة**.

يظهر مربع حوار عنوان NAS IPv4.

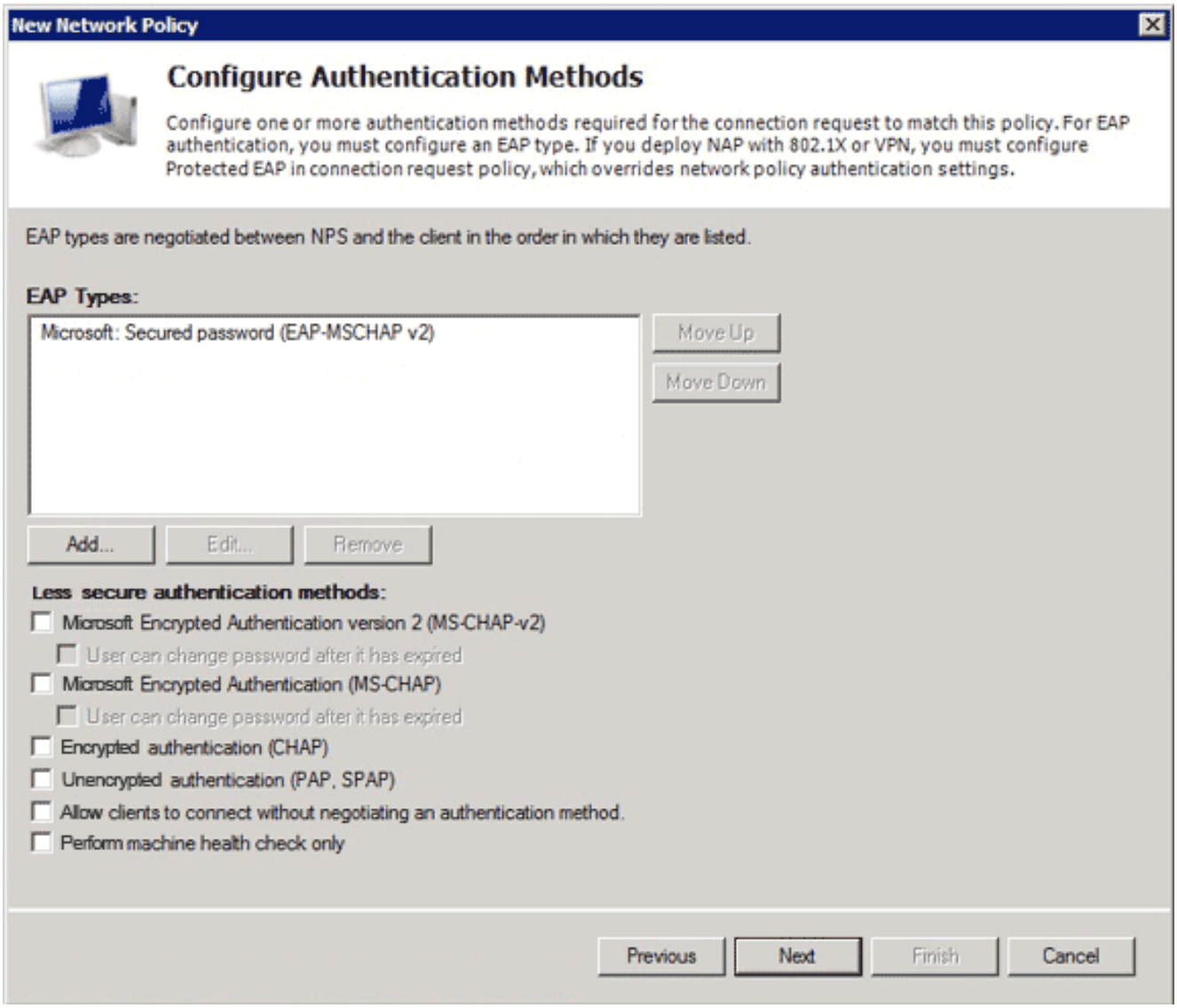


في مربع حوار عنوان NAS IPv4، أدخل عنوان IPv4 الخاص بخادم الوصول إلى الشبكة لتحديد سياسة الشبكة على الطلبات التي تنشأ من موجه Cisco IOS هذا فقط.

وانقر فوق OK.



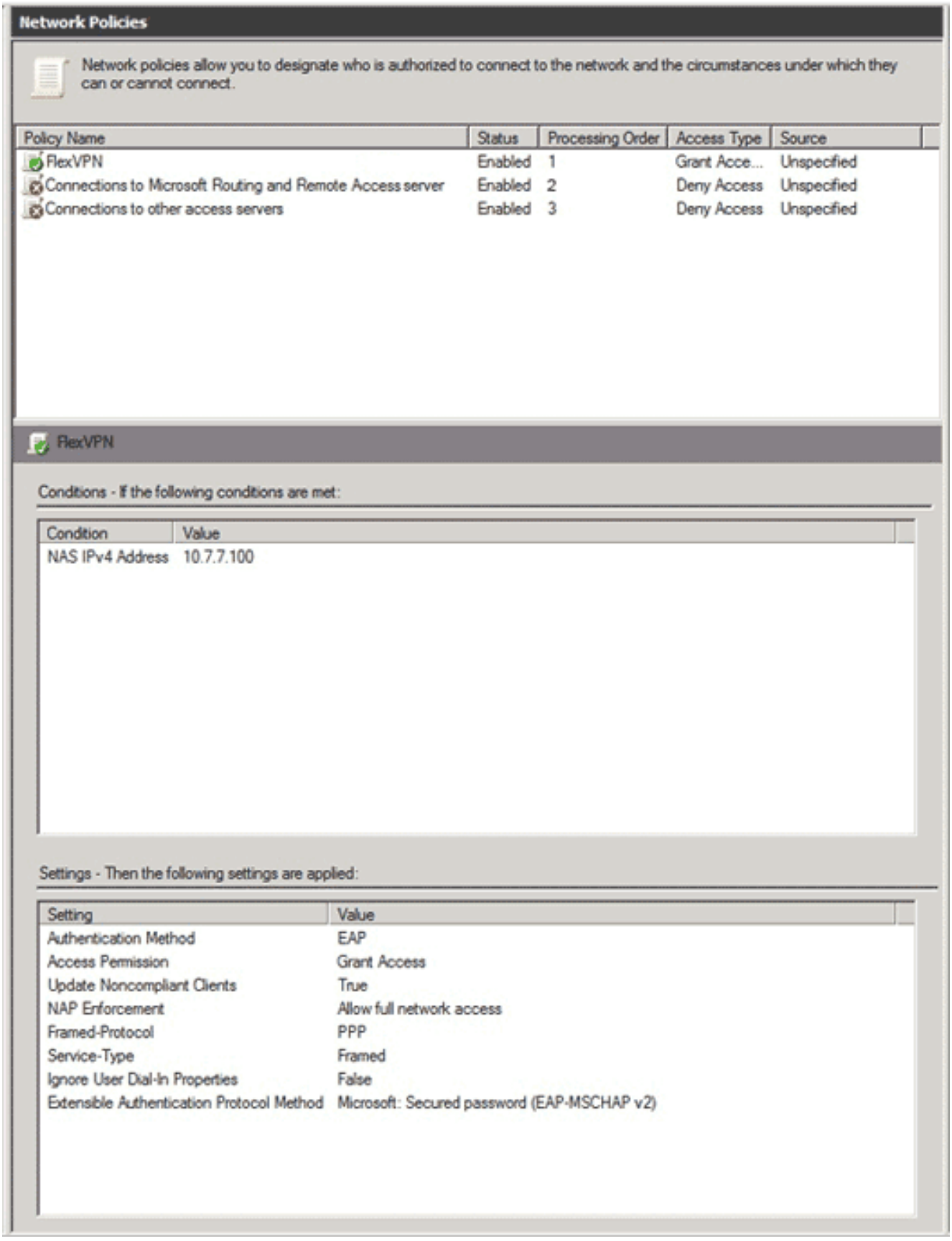
في مربع الحوار "نهج الشبكة" الجديد، انقر فوق الزر راديو **الوصول الممنوح** للسماح للعميل بالوصول إلى الشبكة (إذا كانت بيانات الاعتماد المقدمة من المستخدم صحيحة)، ثم انقر فوق **التالي**.



تأكد فقط من ظهور كلمة المرور الآمنة (EAP-MSCHAP v2) في منطقة أنواع EAP للسماح باستخدام EAP-MSCHAPv2 كطريقة اتصال بين جهاز Cisco IOS و Active Directory، وانقر **التالي**.

ملاحظة: أترك جميع خيارات "طرق المصادقة الأقل أمانا" دون تحديد.

تابع من خلال المعالج وقم بتطبيق أية قيود أو إعدادات إضافية كما هو محدد بواسطة نهج أمان مؤسستك.
بالإضافة إلى ذلك، تأكد من إدراج السياسة أولا في ترتيب المعالجة كما هو موضح في هذه الصورة:



تكوين العميل

1. قم بإنشاء ملف تعريف XML داخل محرر نصوص، وقم بتسميته *flexvpn.xml*.

يستخدم هذا المثال ملف تعريف XML هذا:

```
<?"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>
<"RSASecurIDIntegration UserControllable="false>
Automatic
<RSASecurIDIntegration/>
WindowsLogonEnforcement>SingleLocalLogon>
<WindowsLogonEnforcement/>
WindowsVPNEstablishment>LocalUsersOnly>
<WindowsVPNEstablishment/>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
PPPExclusion UserControllable="false">Disable>
<"PPPExclusionServerIP UserControllable="false>
<PPPExclusionServerIP/>
<PPPExclusion/>
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>
```

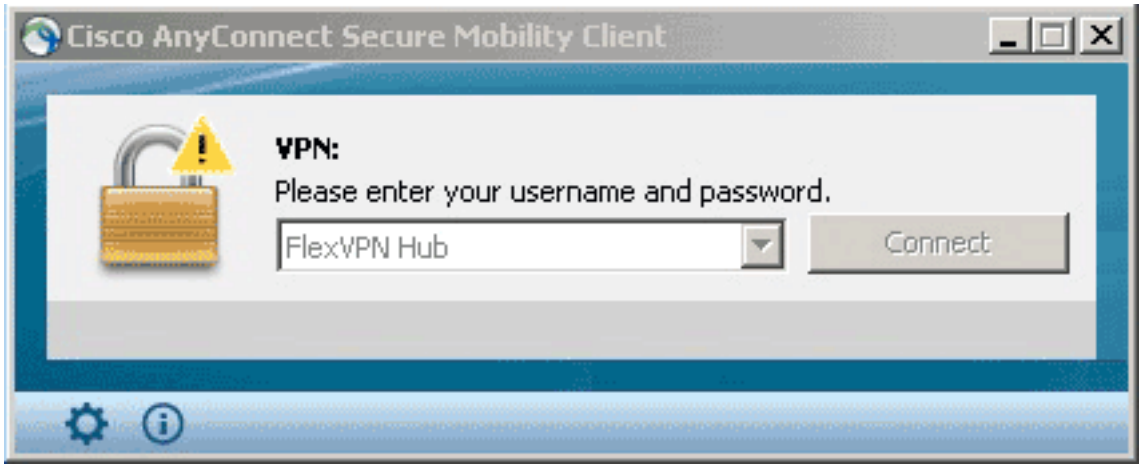
```
<HostName>FlexVPN Hub</HostName>
<HostAddress>flexvpn-hub.example.com</HostAddress>
PrimaryProtocol>IPsec>
StandardAuthenticationOnly>true>
<AuthMethodDuringIKENegotiation>EAP-MSCHAPv2</AuthMethodDuringIKENegotiation>
<IKEIdentity>example.com</IKEIdentity>
<StandardAuthenticationOnly/>
<PrimaryProtocol/>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

<HostName> عبارة عن سلسلة نصية تظهر في العميل.<HostAddress> هو اسم المجال المؤهل بالكامل (FQDN) لموزع FlexVPN.يقوم <primaryProtocol> بتكوين الاتصال لاستخدام IKEv2/IPsec بدلا من SSL (الافتراضي في AnyConnect).يقوم <AuthMethodDuringIKENegotiation> بتكوين الاتصال لاستخدام MSCHAPv2 داخل EAP. هذه القيمة مطلوبة للمصادقة مقابل Microsoft Active Directory.يحدد <IKEIdentity> قيمة السلسلة التي تطابق العميل بملف تعريف IKEv2 محدد على الموزع (راجع الخطوة 4 أعلاه).

ملاحظة: ملف تعريف العميل عبارة عن شيء لا يستخدمه العميل إلا. يوصى بأن يستخدم المسؤول محرر ملف تعريف AnyConnect لإنشاء ملف تعريف العميل.

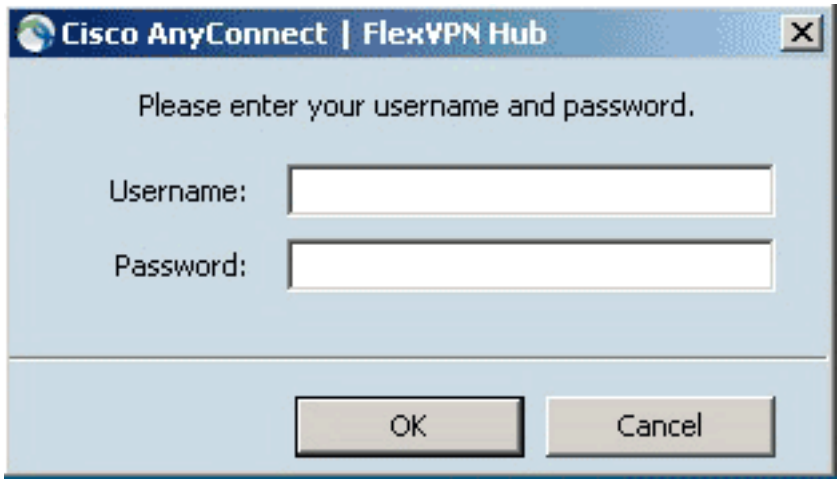
2. احفظ ملف FlexVPN.xml في الدليل المناسب كما هو مدرج في هذا الجدول:

3. قم بإغلاق عميل AnyConnect وإعادة تشغيله.



4. في شاشة Cisco AnyConnect Secure Mobility Client، أختر **موزع FlexVPN**، ثم انقر فوق **Connect**.

ال Cisco AnyConnect | يظهر مربع الحوار FlexVPN Hub.



5. دخلت username وكلمة، وطقطقة **ok**.

التحقق من الصحة

للتحقق من الاتصال، أستخدم الأمر **show crypto session detail remote client-ipaddress** . راجع عرض جلسة عمل التشفير للحصول على مزيد من المعلومات حول هذا الأمر.

ملاحظة: الإنتاج مترجم بِساند أداة (يسجل زبون فقط) (OIT) مؤكد **عرض** أمر. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

استكشاف الأخطاء وإصلاحها

لاستكشاف أخطاء الاتصال وإصلاحها، قم بجمع سجلات DART وتحليلها من العميل واستخدم أوامر تصحيح الأخطاء هذه على الموجه: **debug crypto ikev2 packet** و**debug crypto ikev2 internal**.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).