Esempio di configurazione del client FlexVPN e Anyconnect IKEv2

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco AnyConnect Secure Mobility Client in modo che utilizzi RADIUS (Remote Authentication Dial-In User Service) e gli attributi di autorizzazione locale per l'autenticazione in Microsoft Active Directory.

> **Nota:** Al momento, l'uso del database degli utenti locale per l'autenticazione non funziona sui dispositivi Cisco IOS®. Infatti Cisco IOS non funziona come autenticatore EAP. Richiesta di miglioramento CSCui07025 non riuscita per aggiungere supporto.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS versione 15.2(T) o successive
- Cisco AnyConnect Secure Mobility Client versione 3.0 o successiva
- Microsoft Active Directory

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

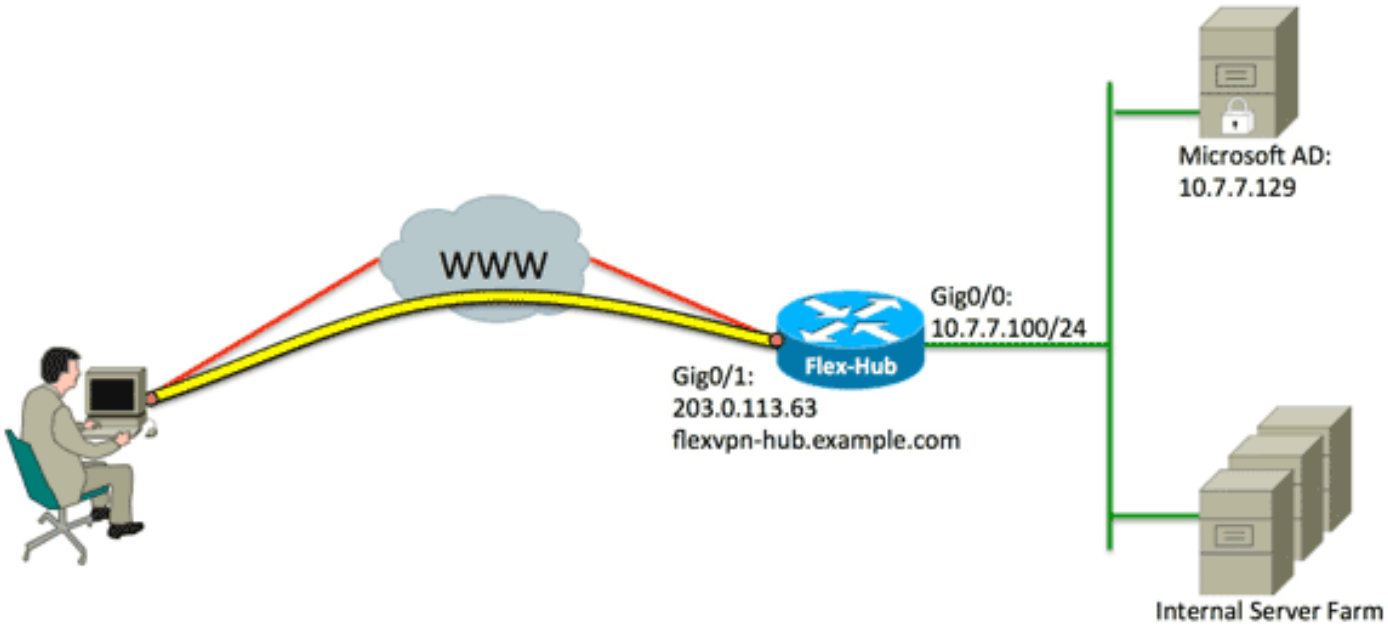
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- Configurazione hub
- Configurazione server Microsoft Active Directory
- Configurazione client

Configurazione hub

1. Configurare RADIUS solo per l'autenticazione e definire l'autorizzazione locale.

```
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
```

   Il comando **aaa authentication login list** fa riferimento al gruppo authentication, authorization, and accounting (AAA) (che definisce il server RADIUS). Il comando **aaa authorization network list** indica che devono essere utilizzati gli utenti/gruppi definiti localmente. È necessario modificare la configurazione nel server RADIUS per consentire le richieste di autenticazione da questo dispositivo.

2. Configurare il criterio di autorizzazione locale.

```
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
```

   Il comando **ip local pool** viene usato per definire gli indirizzi IP assegnati al client. I criteri di autorizzazione vengono definiti con il nome utente *FlexVPN-Local-Policy-1* e gli attributi per il client (server DNS, netmask, elenco di divisione, nome di dominio e così via) vengono configurati qui.

3. Accertarsi che il server utilizzi un certificato (rsa-sig) per autenticarsi.

   Cisco AnyConnect Secure Mobility Client richiede che il server si autentichi utilizzando un certificato (rsa-sig). Il router deve disporre di un certificato del *server Web* (ovvero un certificato con 'autenticazione server' nell'estensione di utilizzo chiavi esteso) rilasciato da un'Autorità di certificazione (CA) attendibile.

   Fare riferimento ai passaggi da 1 a 4 in ASA 8.x Installazione manuale dei certificati dei fornitori di terze parti da utilizzare con l'esempio di configurazione di WebVPN e modificare tutte le istanze della *CA crittografica* in *pki crittografica*.

```
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. Configurare le impostazioni per questa connessione.

```
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
```

Il profilo **crypto ikev2** contiene la maggior parte delle impostazioni rilevanti per questa connessione: **match identity id-chiave remota**: fa riferimento all'identità IKE utilizzata dal client. Questo valore stringa è configurato nel profilo XML AnyConnect.**dn locale identità**: definisce l'identità IKE utilizzata dall'hub FlexVPN. Questo valore utilizza il valore contenuto nel certificato utilizzato.**authentication remote** - Indica che EAP deve essere utilizzato per l'autenticazione del client.**authentication local**: indica che i certificati devono essere utilizzati per l'autenticazione locale.**aaa authentication eap** - Indica di utilizzare l'elenco di accesso con autenticazione aaa FlexVPN-AuthC-List-1 quando EAP viene utilizzato per l'autenticazione.**aaa authorization group eap list** - Stati di usare un elenco di reti di autorizzazione aaa FlexVPN-AuthZ-List-1 con nome utente *FlexVPN-Local-Policy-1* per gli attributi di autorizzazione.**virtual-template 10**: definisce il modello da utilizzare quando viene duplicata un'interfaccia di accesso virtuale.

5. Configurare un profilo IPsec che rimandi al profilo IKEv2 definito nel passaggio 4.

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

Nota: Cisco IOS utilizza Smart Default. Di conseguenza, un set di trasformazioni non deve essere definito in modo esplicito.

6. Configurare il modello virtuale da cui vengono clonate le interfacce di accesso virtuale:
ip senza numero: annullare la numerazione dell'interfaccia da un'interfaccia *interna in* modo che il routing IPv4 possa essere abilitato sull'interfaccia.**tunnel mode ipsec ipv4**: definisce l'interfaccia come tunnel di tipo VTI.

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

7. Limitare la negoziazione a SHA-1 (facoltativo).

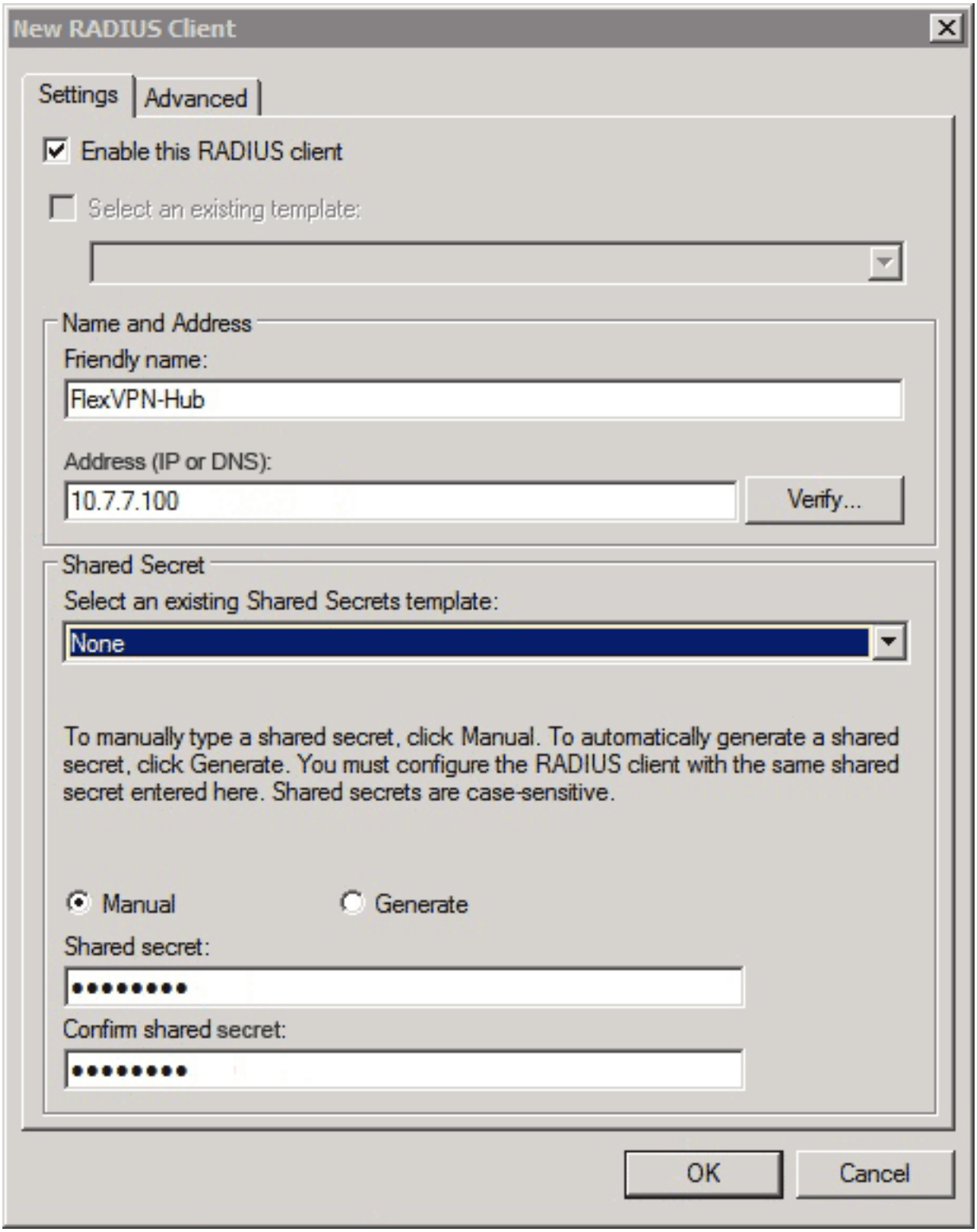
   A causa del problema CSCud96246 (solo utenti registrati), il client AnyConnect potrebbe non convalidare correttamente il certificato dell'hub FlexVPN. Questo problema è dovuto alla negoziazione da parte di IKEv2 di una funzione SHA-2 per una funzione pseudo-casuale (PRF), mentre il certificato FlexVPN-Hub è stato firmato utilizzando SHA-1. La configurazione seguente limita la negoziazione a 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
```

Configurazione server Microsoft Active Directory

1. In Windows Server Manager espandere **Ruoli > Server dei criteri di rete e di accesso > Server dei criteri di rete (locale) > Client e server RADIUS** e fare clic su **Client RADIUS**.

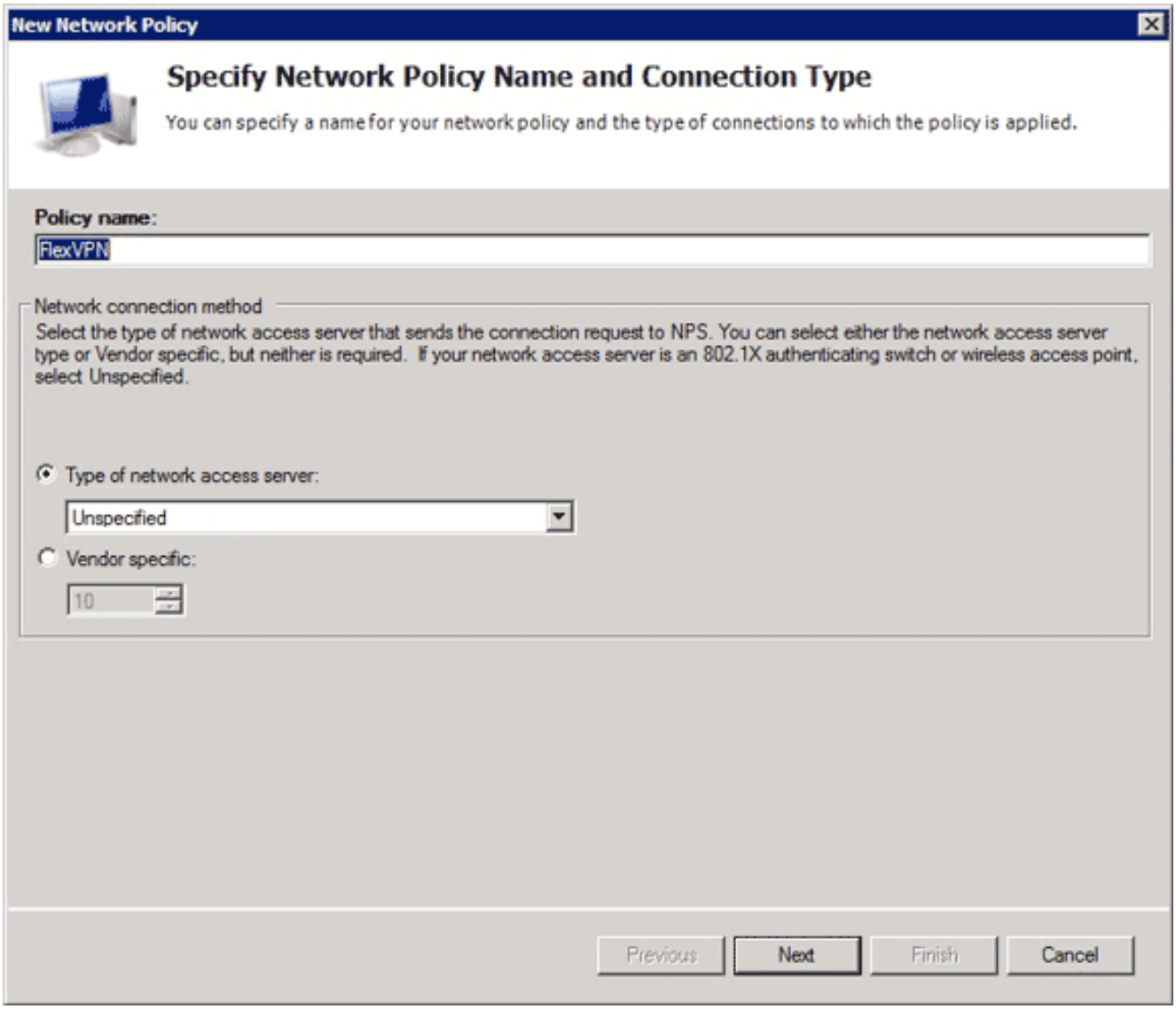
   Viene visualizzata la finestra di dialogo Nuovo client RADIUS.



2. Nella finestra di dialogo Nuovo client RADIUS aggiungere il router Cisco IOS come client RADIUS:
   Selezionare la casella di controllo **Abilita questo client RADIUS**.Immettere un nome nel campo Nome descrittivo. In questo esempio viene utilizzato *FlexVPN-Hub*.Immettere l'indirizzo IP del router nel campo Indirizzo.Nell'area Segreto condiviso fare clic sul pulsante di opzione **Manuale** e immettere il segreto condiviso nei campi Segreto condiviso e Conferma segreto condiviso.**Nota:** il segreto condiviso deve corrispondere al segreto condiviso configurato sul router.Fare clic su OK.

3. Nell'interfaccia di Server Manager, espandere **Criteri** e scegliere **Criteri di rete**.

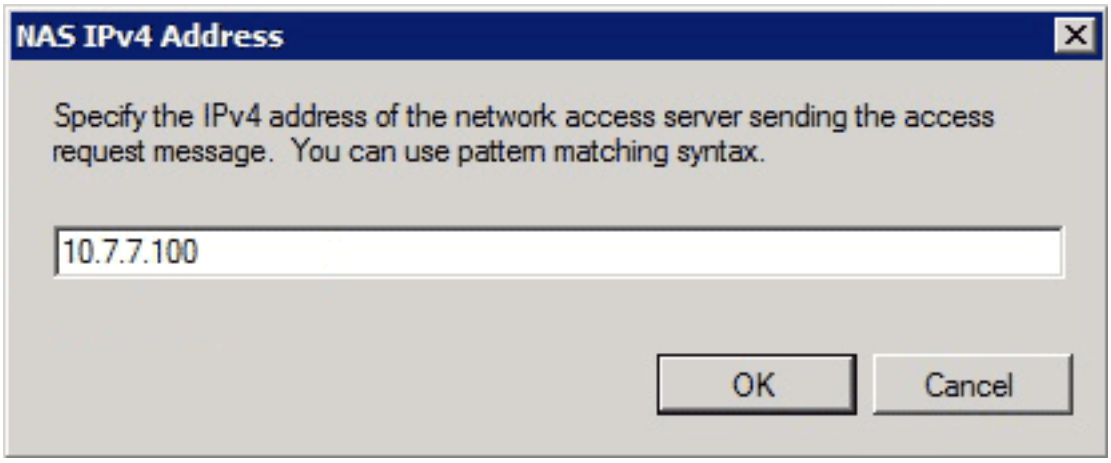
Verrà visualizzata la finestra di dialogo Nuovo criterio di rete.



4. Nella finestra di dialogo Nuovo criterio di rete aggiungere un nuovo criterio di rete:

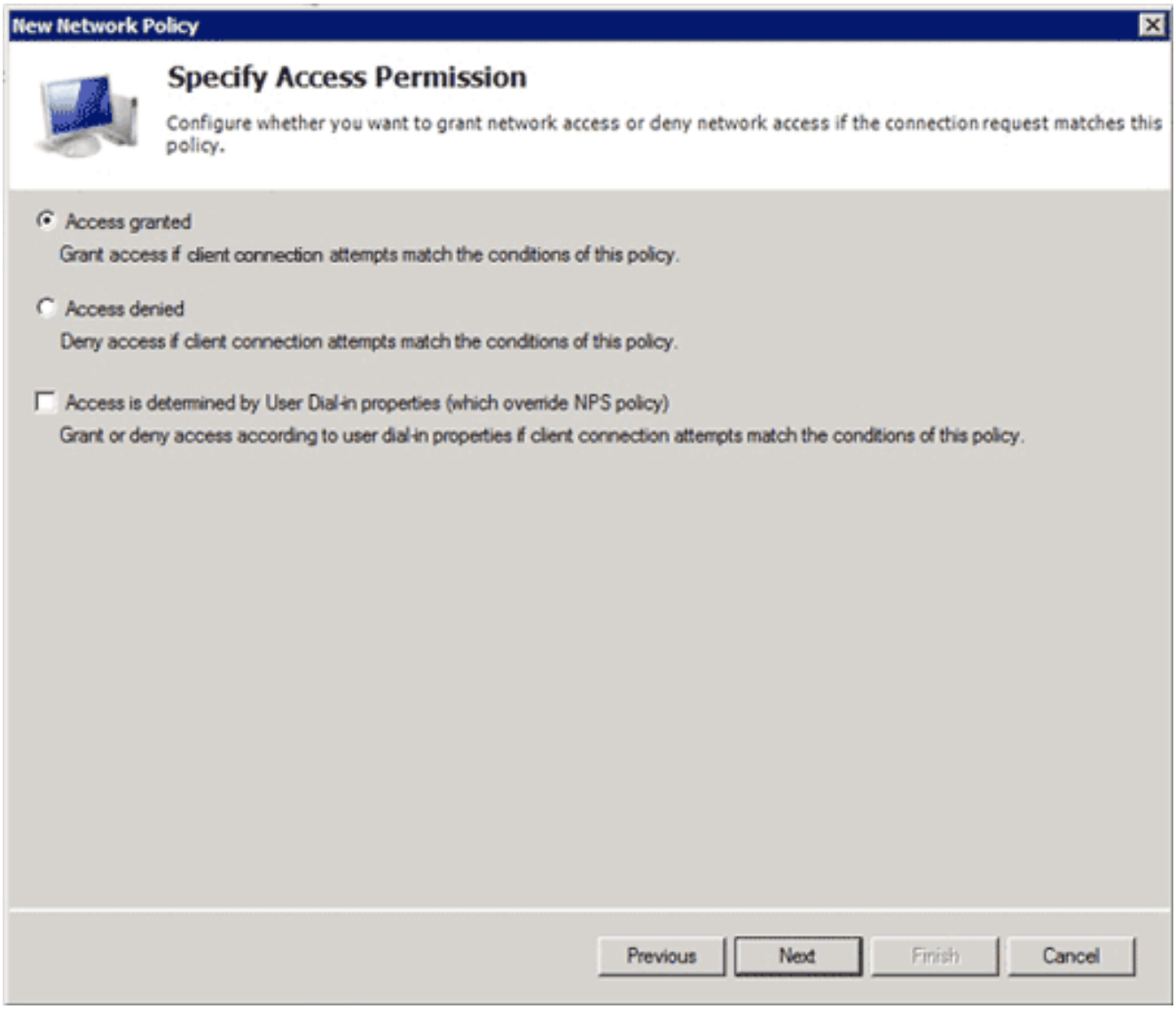
   Immettere un nome nel campo Nome criterio. In questo esempio viene utilizzato *FlexVPN*.Fare clic sul pulsante di scelta **Tipo di server di accesso alla rete** e scegliere **Non specificato** dall'elenco a discesa.Fare clic su Next (Avanti).Nella finestra di dialogo Nuovo criterio di rete fare clic su **Aggiungi** per aggiungere una nuova condizione.Nella finestra di dialogo Seleziona condizione selezionare la condizione **Indirizzo IPv4 NAS** e fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo Indirizzo IPv4 NAS.



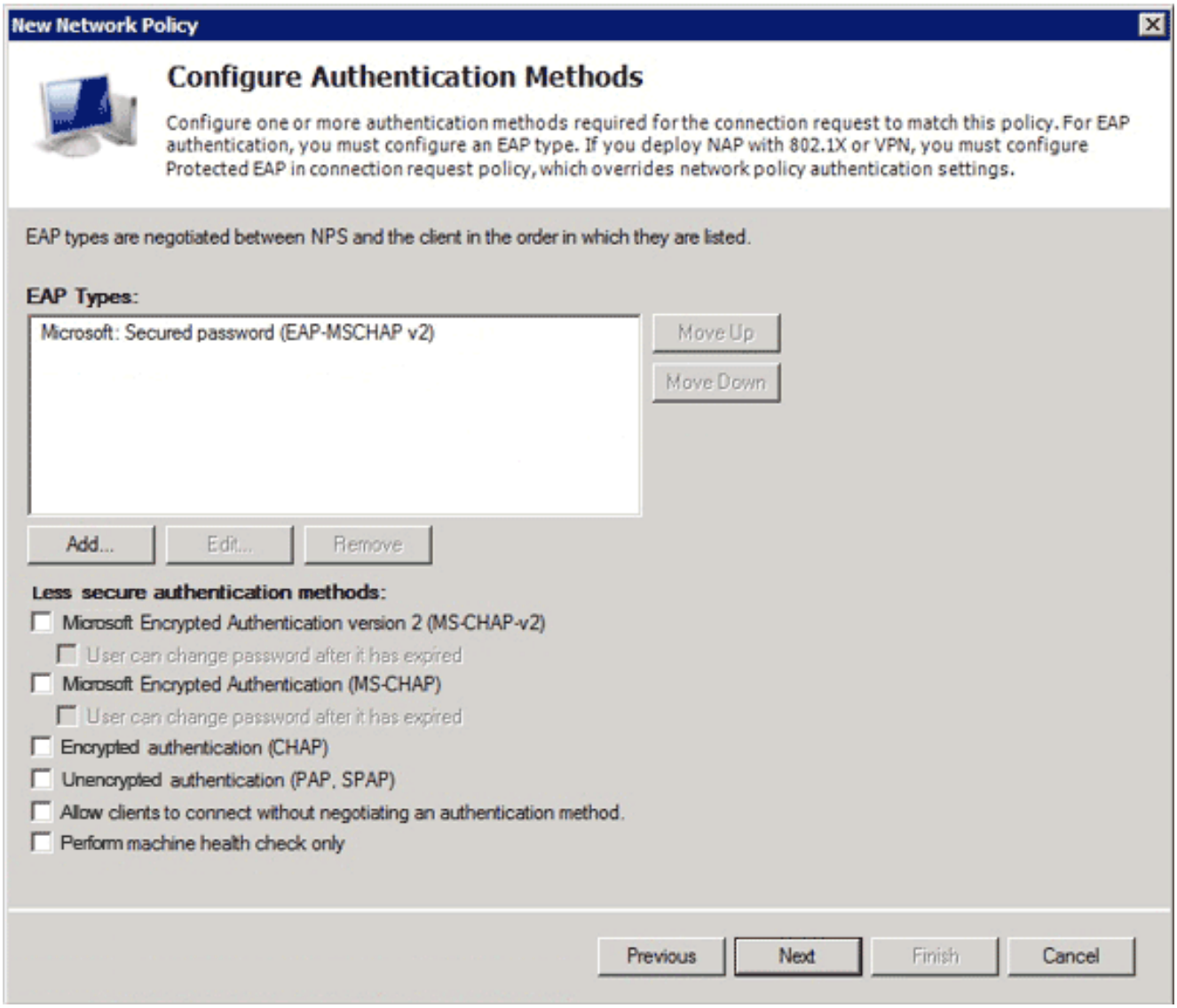
Nella finestra di dialogo Indirizzo IPv4 NAS immettere l'indirizzo IPv4 del server di accesso alla rete per limitare il criterio di rete alle sole richieste provenienti da questo router Cisco IOS.

Fare clic su OK.



Nella finestra di dialogo Nuovo criterio di rete fare clic sul pulsante di opzione **Accesso concesso** per consentire al client di accedere alla rete (se le credenziali fornite dall'utente

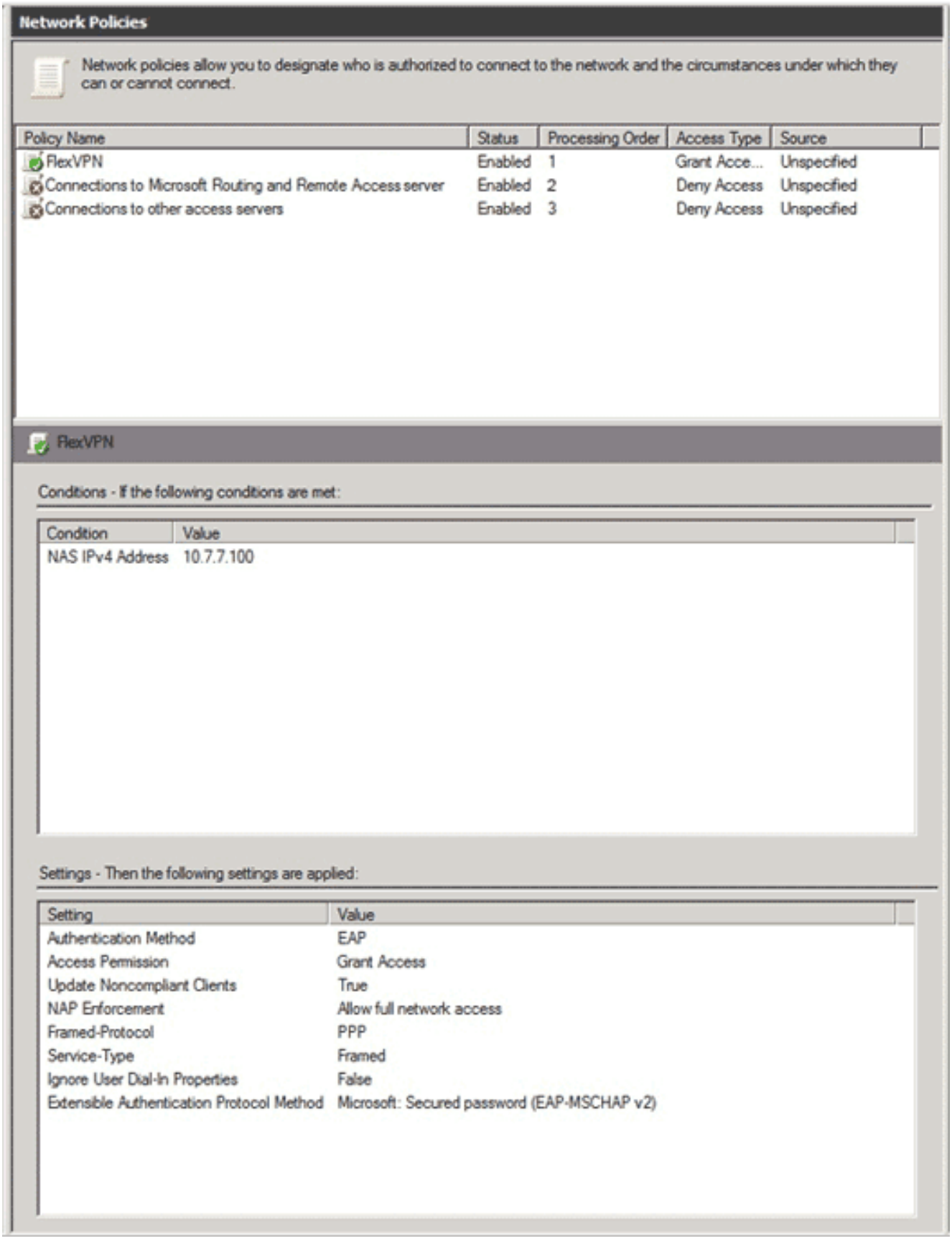
sono valide) e quindi fare clic su **Avanti**.



Assicurarsi che solo Microsoft: Nell'area Tipi EAP viene visualizzata la password di protezione (EAP-MSCHAP v2) per consentire l'utilizzo di EAP-MSCHAPv2 come metodo di comunicazione tra il dispositivo Cisco IOS e Active Directory, quindi fare clic su **Avanti**.

Nota: Lasciare deselezionate tutte le opzioni 'Metodi di autenticazione meno sicuri'.

Continuare la procedura guidata e applicare eventuali vincoli o impostazioni aggiuntivi definiti dai criteri di sicurezza dell'organizzazione. Verificare inoltre che il criterio sia elencato per primo nell'ordine di elaborazione, come illustrato nella seguente immagine:



Configurazione client

1. Creare un profilo XML all'interno di un editor di testo e denominarlo *flexvpn.xml*.

In questo esempio viene utilizzato il seguente profilo XML:

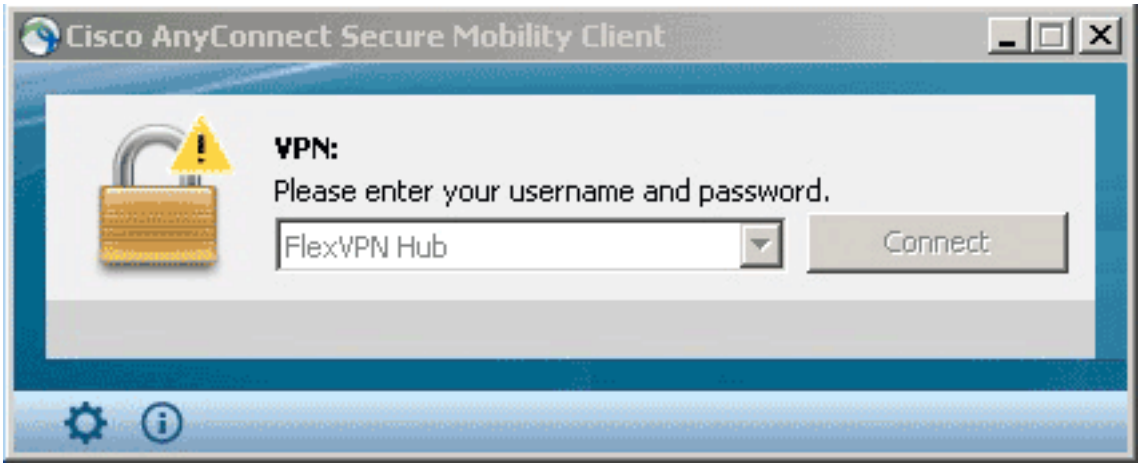
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false
</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>
```

<NomeHost> è una stringa di testo visualizzata nel client.<IndirizzoHost> è il nome di dominio completo (FQDN) dell'hub FlexVPN.<PrimaryProtocol> configura la connessione in modo che utilizzi IKEv2/IPsec anziché SSL (impostazione predefinita in AnyConnect).<AuthMethodDuringIKENegotiation> configura la connessione per l'utilizzo di MSCHAPv2 in EAP. Questo valore è necessario per l'autenticazione con Microsoft Active Directory.<IKEIdentity> definisce il valore stringa che corrisponde al client a un profilo IKEv2 specifico sull'hub (vedere il passaggio 4 riportato sopra).
Nota: Il profilo client è utilizzato solo dal client. Per creare il profilo client, si consiglia all'amministratore di usare l'editor di profili Anyconnect.

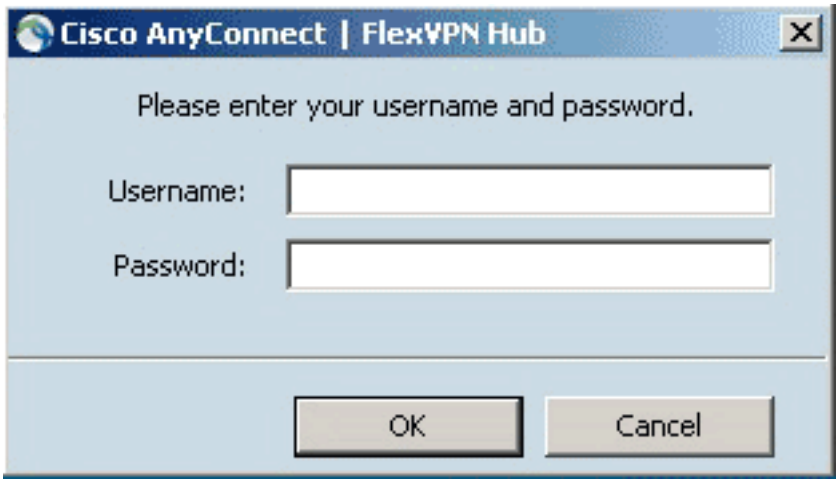
2. Salvare il file flexvpn.xml nella directory appropriata, come indicato nella seguente tabella:

3. Chiudere e riavviare il client AnyConnect.



4. Nella finestra di dialogo Cisco AnyConnect Secure Mobility Client, selezionare **FlexVPN Hub**, quindi fare clic su **Connect**.

   Cisco AnyConnect | FlexVPN Hub.



5. Immettere un nome utente e una password e fare clic su **OK**.

Verifica

Per verificare la connessione, utilizzare il comando **show crypto session detail remote client-ip address**. Per ulteriori informazioni sul comando show crypto session, consultare il documento.

> **Nota:** Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Per risolvere i problemi di connessione, raccogliere e analizzare i log DART dal client e usare i seguenti comandi di debug sul router: **debug crypto ikev2 packet** ed **debug crypto ikev2 internal**.

> **Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di debug.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems