

Installazione di FlexVPN: Accesso remoto AnyConnect IKEv2 con EAP-MD5

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Esempio di rete](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Sfondo](#)

[Configurazione iniziale di IOS](#)

[IOS - CA](#)

[IOS - Certificato di identità](#)

[IOS - Configurazione AAA e Radius](#)

[Configurazione iniziale ACS](#)

[Configurazione IOS FlexVPN](#)

[configurazione di Windows](#)

[Importazione di CA in trust Windows](#)

[Configurazione del profilo XML AnyConnect](#)

[Test](#)

[Verifica](#)

[IOS Router](#)

[Windows](#)

[Avvertenze e problemi noti](#)

[Crittografia di nuova generazione](#)

[Informazioni correlate](#)

[Introduzione](#)

Questo documento fornisce una configurazione di esempio di come configurare Accesso remoto su IOS utilizzando il toolkit FlexVPN.

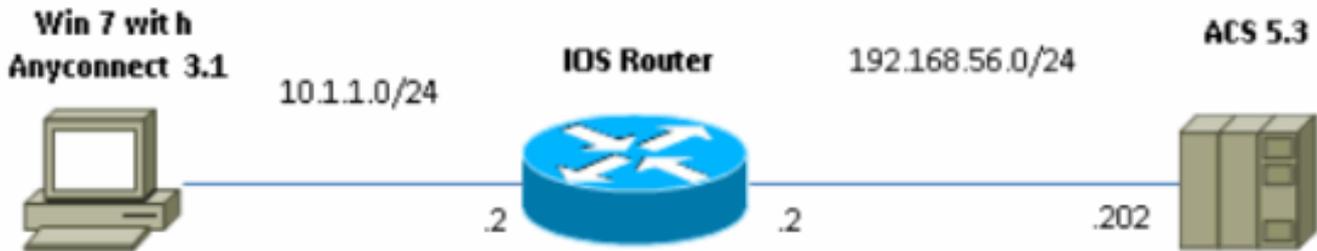
La VPN ad accesso remoto consente ai client finali che utilizzano vari sistemi operativi di connettersi in modo sicuro alle reti aziendali o domestiche tramite un supporto non sicuro, ad esempio Internet. Nello scenario illustrato, il tunnel VPN viene terminato su un router Cisco IOS con protocollo IKEv2.

In questo documento viene illustrato come autenticare e autorizzare gli utenti tramite Access Control Server (ACS) con il metodo EAP-MD5.

Prerequisiti

Esempio di rete

Il router Cisco IOS ha due interfacce, una verso ACS 5.3:



Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- ACS 5.3 con patch 6
- Router IOS con software 15.2(4)M
- PC con Windows 7 con AnyConnect 3.1.01065

Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.](#)

Sfondo

In IKEv1 XAUTH viene utilizzato nella fase 1.5, è possibile eseguire l'autenticazione degli utenti in locale su un router IOS e in remoto utilizzando RADIUS/TACACS+. IKEv2 non supporta più XAUTH e la fase 1.5. Contiene il supporto EAP incorporato, eseguito nella fase IKE_AUTH. Il vantaggio più grande è la progettazione IKEv2 e EAP è uno standard conosciuto.

EAP supporta due modalità:

- Tunneling: EAP-TLS, EAP/PSK, EAP-PEAP, ecc.
- Non tunneling: EAP-MSCHAPv2, EAP-GTC, EAP-MD5 ecc.

Nell'esempio, viene usato EAP-MD5 in modalità non tunneling perché è il metodo di autenticazione esterna EAP supportato attualmente in ACS 5.3.

EAP può essere utilizzato solo per l'iniziatore di autenticazione (client) al risponditore (IOS in questo caso).

Configurazione iniziale di IOS

IOS - CA

Innanzitutto è necessario creare un'Autorità di certificazione (CA) e un certificato di identità per il router IOS. Il client verificherà l'identità del router in base a tale certificato.

La configurazione di CA su IOS è simile alla seguente:

```
crypto pki server CA
grant auto
hash sha1
eku server-auth client-auth
```

È necessario ricordare l'utilizzo esteso delle chiavi (Server-Auth necessario per EAP, per RSA-SIG è necessario anche Client-Auth).

Abilitare la CA utilizzando il comando **no shutdown** nella CA del server PKI crittografica.

IOS - Certificato di identità

Quindi, abilitare SCEP (Simple Certificate Enrollment Protocol) per il certificato e configurare il trust point.

```
ip http server
crypto pki trustpoint CA-self
enrollment url http://10.1.1.2:80
fqdn 10.1.1.2
ip-address 10.1.1.2
subject-name cn=10.1.1.2,ou=TAC
revocation-check none
eku request server-auth client-auth
```

Quindi, autenticare e registrare il certificato:

```
(config)#crypto pki authenticate CA-self
Certificate has the following attributes:
    Fingerprint MD5: 741C671C 3202B3AE 6E05161C 694CA53E
    Fingerprint SHA1: 8C99513C 2198470F 7CB58FA2 32D8AA8D FC31D1ED
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

```
R1(config)#crypto pki enroll CA-self
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: cn=10.1.1.2,ou=TAC
% The subject name in the certificate will include: 10.1.1.2
% Include the router serial number in the subject name? [yes/no]: no
% The IP address in the certificate is 10.1.1.2
Request certificate from CA? [yes/no]: yes
```

```

% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CA-self' command
will show the fingerprint.
R1(config)#
*Dec 2 10:57:44.141: CRYPTO_PKI: Certificate Request Fingerprint MD5:
BF8EF4B6 87FA8162 9079F917 698A5F36
*Dec 2 10:57:44.141: CRYPTO_PKI: Certificate Request Fingerprint SHA1:
AC13FEA3 295F7AE6 7014EF60 784E33AF FD94C41D
R1(config)#
*Dec 2 10:57:44.198: %PKI-6-CERTRET: Certificate received from
Certificate Authority

```

Se non si desidera che i messaggi di richiesta in AnyConnect siano presenti, ricordare che può essere necessario usare lo stesso nome host o indirizzo IP configurato nel profilo AnyConnect.

Nell'esempio, cn=10.1.1.2. Pertanto, in AnyConnect 10.1.1.2 viene immesso come indirizzo IP del server nel profilo xml di AnyConnect.

[IOS - Configurazione AAA e Radius](#)

È necessario configurare l'autenticazione e l'autorizzazione Radius e AAA:

```

aaa new-model
radius-server host 192.168.56.202 key cisco
aaa group server radius SERV
server 192.168.56.202
aaa authentication login eap-list group SERV
aaa authorization network eap-list group SERV

```

[Configurazione iniziale ACS](#)

Innanzitutto, aggiungere il nuovo dispositivo di rete in ACS (Risorse di rete > Dispositivi di rete e client AAA > Crea):

The screenshot shows the 'Add New Device' configuration page in ACS. The 'Name' field is set to 'H1'. Under 'Network Device Groups', 'Location' is set to 'All Locations' and 'Device Type' is set to 'All Device Types'. In the 'IP Address' section, 'Single IP Address' is selected with the value '192.168.56.2'. The 'Authentication Options' section is expanded to show 'TACACS+' and 'RADIUS' options. Under 'RADIUS', 'Shared Secret' is set to 'cisco', 'Auth port' is '1812', and 'Key Input Format' is set to 'HEXADECIMAL'. A legend at the bottom left indicates that orange dots represent required fields.

Aggiungere un utente (Utenti e archivi identità > Archivi identità interni > Utenti > Crea):

Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: user3 Status: Enabled

Description:

Identity Group: All Groups

Password Information

Password must:

- Contain 4 - 32 characters

Password Type: Internal Users

Password: ●●●●●●

Confirm Password: ●●●●●●

Change password on next login

User Information

There are no additional identity attributes defined for user records

= Pola wymagane

Enable Password Information

Password must:

- Contain 4 - 32 characters

Enable Password:

Confirm Password:

Aggiungere un utente per l'autorizzazione. In questo esempio, questo valore è IKETEST. La password deve essere "cisco" perché è l'impostazione predefinita inviata da IOS.

General

Name: IKETEST Status: Enabled

Description:

Identity Group: All Groups

Password Information

Password must:

- Contain 4 - 32 characters

Password Type: Internal Users

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

Change password on next login

User Information

There are no additional identity attributes defined for user records

= Pola wymagane

Creare quindi un profilo di autorizzazione per gli utenti (Elementi criteri > Autorizzazioni e autorizzazioni > Accesso alla rete > Profili di autorizzazione > Crea).

In questo esempio viene denominato POOL. Nell'esempio, viene immesso un doppio AV a tunnel diviso (come prefisso) e l'indirizzo IP con frame viene assegnato al client connesso come indirizzo IP. L'elenco di tutte le coppie AV supportate è disponibile qui:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html

The screenshot shows the 'RADIUS Attributes' configuration page. It features two tables and a form below them.

Common Tasks Attributes

Attribute	Type	Value
-----------	------	-------

Manually Entered

Attribute	Type	Value
Framed-IP-Address cisco-av-pair	IPv4 Address String	192.168.100.200 isec route-set=prefix 10.1.1.0/24

Buttons: Add A, Del A, Replace A, Delete

Dictionary Type: RADIUS-IF-IF

RADIUS Attribute: Select

Attribute Type:

Attribute Value: Static

= Pola wyłączone

Submit Cancel

Quindi, è necessario attivare il supporto di EAP-MD5 (per l'autenticazione) e PAP/ASCII (per l'autorizzazione) nei criteri di accesso. L'impostazione predefinita viene utilizzata in questo esempio (Criteri di accesso > Accesso di rete predefinito):

General **Allowed Protocols**

Process Host Lookup

Authentication Protocols

- ▶ Allow PAP/ASCII
- ▶ Allow CHAP
- ▶ Allow MS-CHAPv1
- ▶ Allow MS-CHAPv2
- ▶ Allow EAP-MD5
- ▶ Allow EAP-TLS
- ▶ Allow LEAP
- ▶ Allow PEAP
- ▶ Allow EAP-FAST

Preferred EAP protocol

Creare una condizione per in Criteri di accesso e assegnare il profilo di autorizzazione creato. In questo caso viene creata una condizione per NDG:Posizione in tutte le posizioni, pertanto per tutte le richieste di autorizzazioni Radius verrà fornito il profilo di autorizzazione del pool (Criteri di accesso > Servizi di accesso > Accesso di rete predefinito):

General
 Name: Rule-1 Status: Enabled 

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions
 NDG:Location: in
 Time And Date:

Results
 Authorization Profiles:

POOL

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

Dovrebbe essere possibile eseguire il test su un router IOS se l'utente può autenticarsi correttamente:

```
R1#test aaa group SERV user3 Cisco123 new-code
User successfully authenticated

USER ATTRIBUTES
username      0  "user3"
addr          0  192.168.100.200
route-set     0  "prefix 10.1.1.0/24"
```

[Configurazione IOS FlexVPN](#)

È necessario creare la proposta e il criterio IKEv2. Potrebbe non essere necessario fare riferimento a CSCtn59317. In questo esempio, i criteri vengono creati solo per uno degli indirizzi IP (10.1.1.2).

```
crypto ikev2 proposal PROP
encryption 3des
integrity sha1
group 2

crypto ikev2 policy 5
match address local 10.1.1.2
proposal PROP
```

Creare quindi un profilo IKEV2 e un profilo IPsec da associare a Virtual-Template.

Assicurarsi di disattivare il certificato http-url, come indicato nella guida alla configurazione.

```
crypto ikev2 profile PROF
match identity remote address 0.0.0.0
match identity remote key-id IKETEST
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint CA-self
aaa authentication eap eap-list
aaa authorization user eap list eap-list IKETEST
virtual-template 1
```

```
no crypto ikev2 http-url cert
crypto ipsec transform-set transform1 esp-3des esp-sha-hmac
crypto ipsec profile PROF
set transform-set transform1
set ikev2-profile PROF
interface Virtual-Template1 type tunnel
ip unnumbered Ethernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
```

In questo esempio, l'autorizzazione viene impostata in base all'utente IKETEST, creato nella configurazione ACS.

configurazione di Windows

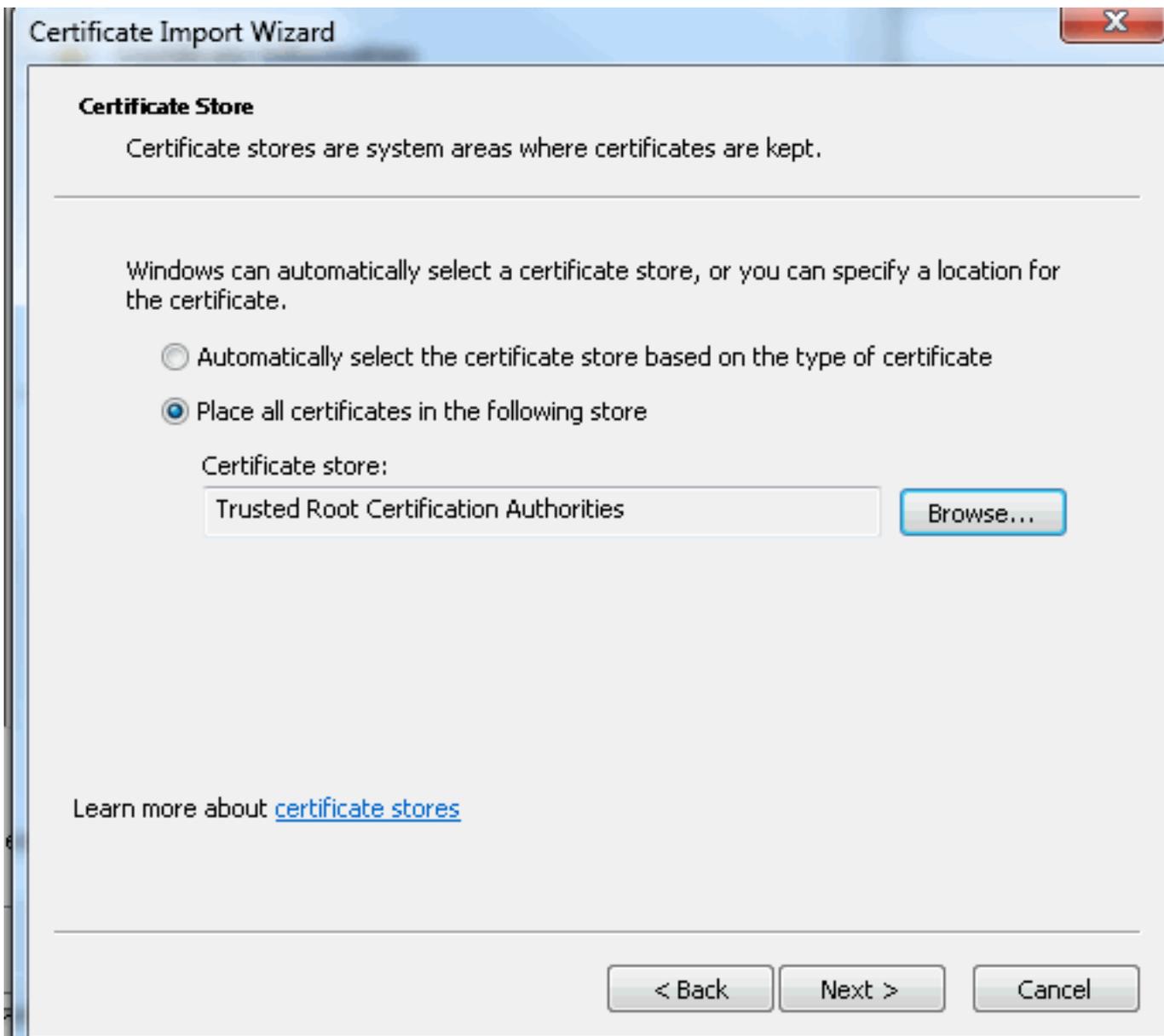
Importazione di CA in trust Windows

Esportare il certificato CA in IOS (accertarsi di esportare il certificato di identità e di ricevere solo la prima parte):

```
R1(config)#crypto pki export CA-self pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB8zCCAVygAwIBAgIBATANBgkqhkiG9w0BAQUFADANMQswCQYDVQQDEwJDQTAE
Fw0xMjExMjYxNzZmMzlaFw0xNTEExMjYxNzZmMzlaMA0xCzAJBgNVBAMTAkNBMI
GfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvDR4lH0crj42QfHpRuNu4EyFrLR8H
TbPanXYV+GdCBmu53pDILE00ASEHByD6DYBx01EZuDsioLJ7t2MPTguB+YZe6V40
JbtayxtZGmF7+eDqRegQHHC394adQQWl2ojgQiuThERDTqDJR8i5gN2Ee+K0sr3
+OjnHjUmXb/I6QIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQE
AwIBhjAfBgNVHSMEGDAWgBTH5Sdh69q4HAJulLQYLbYH0Nk9zzAdBgNVHQ4EFgQU
x+UnYevauBwCbP50GC22B9DZPc8wDQYJKoZIhvcNAQEFBQADgYEADtBLiNXnl+LC
PIgJ0nl/jH5p2IwVlzwBpbZcOsZ9mn54QaqrhmhbHnmqKQJl/20+JPE6p+4noICq
VBrxoiX2KYQ1OwmEScPpQ2XJ9vhGqtQ4Xcx3g20HhxxFDfp2XuW7hwU0W8dTCmZw
4vodj47qEXKI6pGuzauw9MN1xhkNarc=
-----END CERTIFICATE-----
```

Copiare la parte tra BEGIN CERTIFICATE ed END CERTIFICATE e incollarla in Blocco note in Windows e salvarla come file CA.crt.

È necessario installarlo come in Autorità principali attendibili (fare doppio clic su file > Installa certificato > Archivia tutti i certificati nel seguente archivio > Autorità di certificazione principali attendibili):



[Configurazione del profilo XML AnyConnect](#)

In C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile creare un file "any.xml" e incollare quanto segue:

```
<?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">
      false</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">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
  <AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
  </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</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="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
  <HostEntry>
    <HostName>IOSEAP-MD5</HostName>
    <HostAddress>10.1.1.2</HostAddress>
    <PrimaryProtocol>IPsec
      <StandardAuthenticationOnly>true
        <AuthMethodDuringIKENegotiation>EAP-MD5</AuthMethodDuringIKENegotiation>
        <IKEIdentity>IKETEST</IKEIdentity>
      </StandardAuthenticationOnly>
    </PrimaryProtocol>
  </HostEntry>
</ServerList>
</AnyConnectProfile>

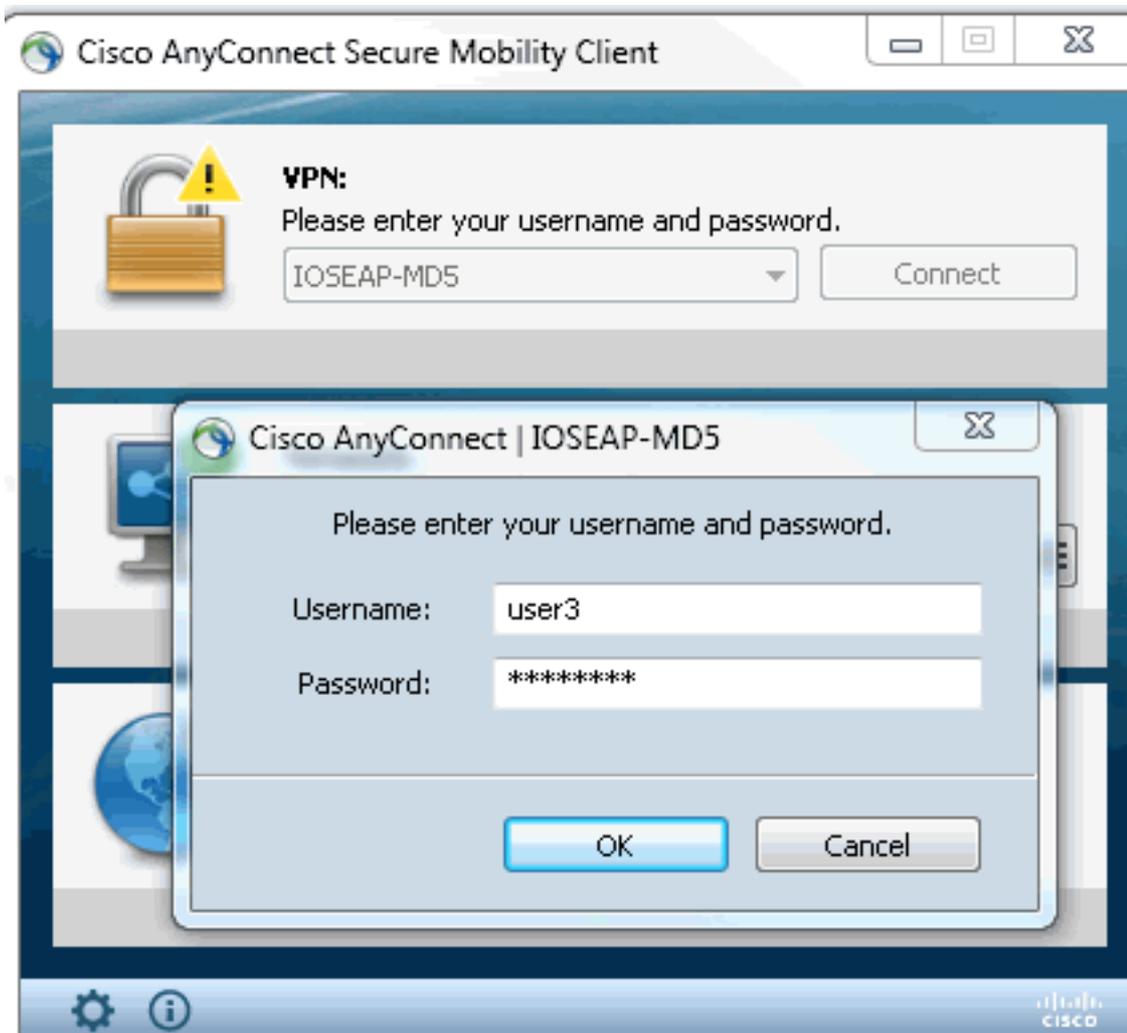
```

Assicurarsi che la voce 10.1.1.2 sia esattamente la stessa di CN=10.1.1.2 inserita per il certificato di identità.

Test

Poiché in questo scenario non viene utilizzata la VPN SSL, verificare che il server HTTP sia disabilitato in IOS (nessun server HTTP ip). In caso contrario, viene visualizzato un messaggio di errore in AnyConnect che dice "Usare un browser per ottenere l'accesso".

Quando ci si connette in AnyConnect, viene richiesta una password. In questo esempio, è stato creato User3



In seguito, l'utente viene connesso.

Verifica

IOS Router

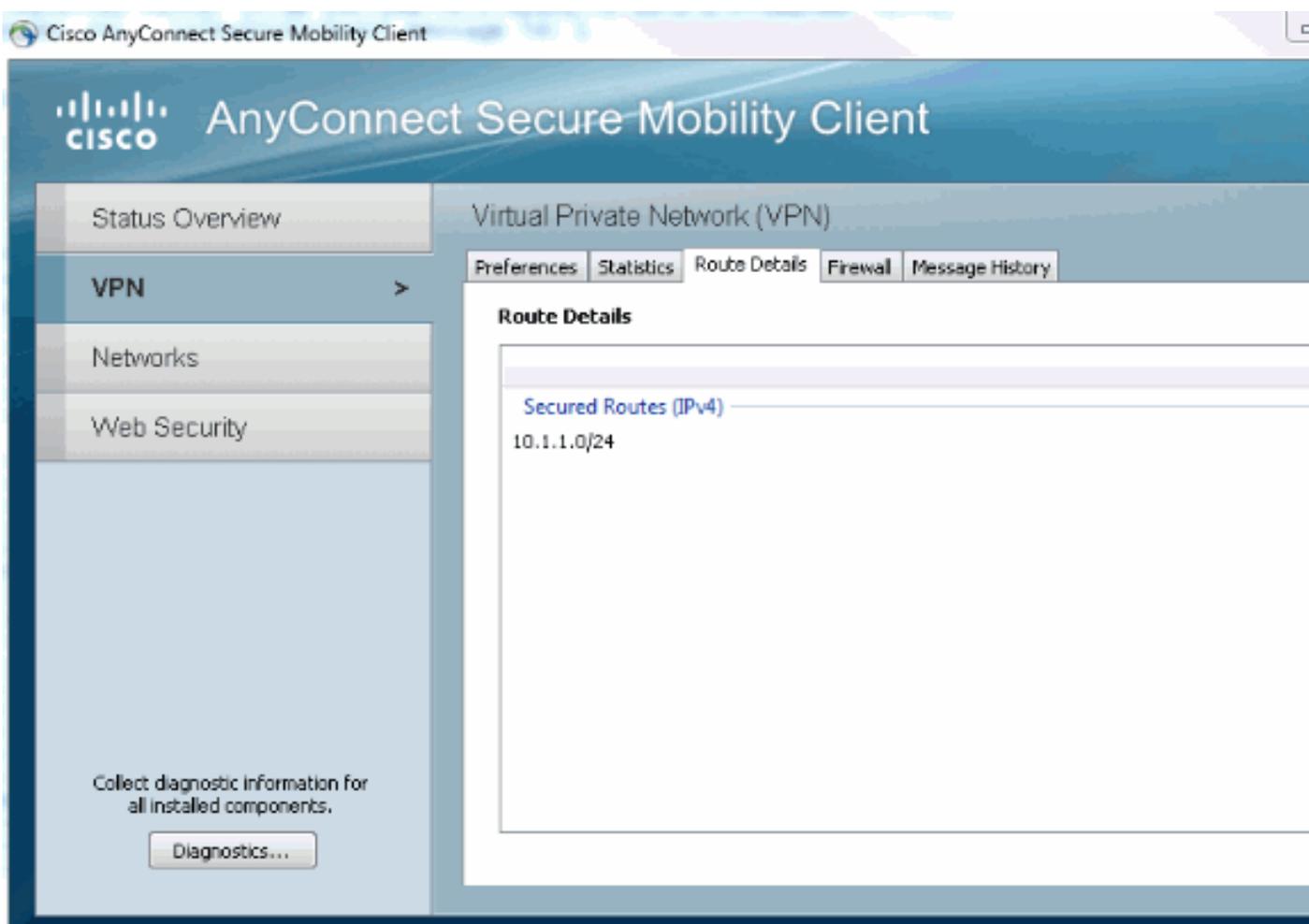
```
R1#show ip inter brief | i Virtual
Virtual-Access1    10.1.1.2  YES unset  up  up
Virtual-Templatel 10.1.1.2  YES unset  up  down
R1# show ip route 192.168.100.200
Routing entry for 192.168.100.200/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Virtual-Access1
    Route metric is 0, traffic share count is 1
R1#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA
Tunnel-id Local Remote fvrf/ivrf Status
1 10.1.1.2/4500 110.1.1.100/61021 none/none READY
  Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: RSA, Auth verify: EAP
  Life/Active Time: 86400/94 sec
IPv6 Crypto IKEv2 SA
R1#show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
```

```
X - IKE Extended Authentication, F - IKE Fragmentation
Interface: Virtual-Access1
Uptime: 00:04:06
Session status: UP-ACTIVE
Peer: 192.168.56.1 port 61021 fvrf: (none) ivrf: (none)
  Phase1_id: IKETEST
  Desc: (none)
IKEv2 SA: local 10.1.1.2/4500 remote 10.1.1.100/61021 Active
  Capabilities:(none) connid:1 lifetime:23:55:54
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.100.200
  Active SAs: 2, origin: crypto map
  Inbound: #pkts dec'ed 1 drop 0 life (KB/Sec) 4160122/3353
  Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4160123/3353
```

È possibile eseguire un debug (debug crypto ikev2).

Windows

Nelle opzioni avanzate di AnyConnect in VPN, è possibile controllare i dettagli della route per visualizzare le reti di tunneling suddivise:



Avvertenze e problemi noti

- Tenere presente quando SHA1 è presente nell'hash della firma e nei criteri di integrità in IKEv2 (fare riferimento all'ID bug Cisco [CSCtn59317](#) (solo utenti [registrati](#))).
- Il CN nel certificato di identità IOS deve essere uguale al nome host nel profilo XML ACS.
- Se si desidera utilizzare coppie Radius AV passate durante l'autenticazione e non utilizzare

l'autorizzazione del gruppo, è possibile utilizzare questo nel profilo IKEv2:

```
aaa authorization user eap cached
```

- L'autorizzazione utilizza sempre la password "cisco" per l'autorizzazione di gruppi o utenti. Ciò potrebbe creare confusione durante l'utilizzo

```
aaa authorization user eap list SERV (without any paramaters)
```

perché proverà ad autorizzare l'uso dell'utente passato in AnyConnect come utente e della password "cisco", che probabilmente non è la password dell'utente.

- In caso di problemi, si tratta di output che è possibile analizzare e fornire a Cisco TAC:debug crypto ikev2debug crypto ikev2 internalUscite DART
- Se non si utilizza la VPN SSL, ricordare di disabilitare il server http ip (nessun server http ip). In caso contrario, AnyConnect tenterà di connettersi al server HTTP e riceverà il risultato, "Utilizzare un browser per ottenere l'accesso".

Crittografia di nuova generazione

La configurazione precedente viene fornita come riferimento per mostrare una configurazione di lavoro minima.

Cisco consiglia di utilizzare la crittografia di nuova generazione (NGC), ove possibile.

Le raccomandazioni correnti per la migrazione sono disponibili all'indirizzo:

http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Quando si sceglie la configurazione NGC, accertarsi che sia il software client che l'hardware headend la supportino. Si consiglia l'uso di router ISR generazione 2 e ASR 1000 come headend perché supportano NGC.

Sul lato AnyConnect, a partire dalla versione 3.1 di AnyConnect, è supportata la suite di algoritmi NSA Suite B.

Informazioni correlate

- [Cisco ASA IKEv2 PKI Site-Site VPN](#)
- [Debug di siti IKEv2 su IOS](#)
- [FlexVPN/IKEv2: Client integrato di Windows 7: Headend IOS: Parte I - Autenticazione certificato](#)
- [Guida alla configurazione di FlexVPN e Internet Key Exchange versione 2, Cisco IOS release 15.2M&T](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)