# FlexVPN部署：採用EAP-MD5的AnyConnect IKEv2遠端存取

## 目錄

## 簡介

本文檔提供如何使用FlexVPN工具包在IOS上設定遠端訪問的示例配置。

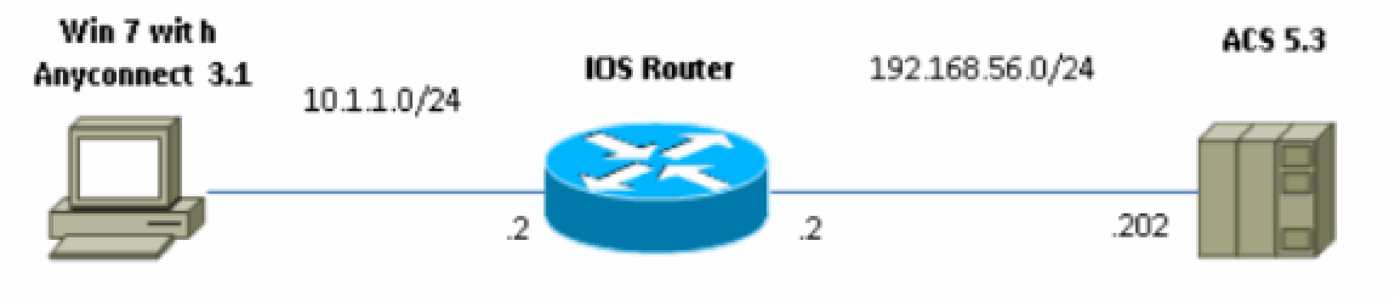
遠端訪問VPN允許使用各種作業系統的終端客戶端通過不安全介質（例如網際網路）安全地連線到公司或家庭網路。在所顯示的場景中，VPN隧道在使用IKEv2協定的Cisco IOS路由器上終止。

本檔案介紹如何透過EAP-MD5方法使用存取控制伺服器(ACS)對使用者進行驗證和授權。

## 必要條件

### 網路圖表

Cisco IOS路由器有兩個介面 — 一個指向ACS 5.3:



## 需求

本文件沒有特定需求。

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ACS 5.3，帶補丁6
- 採用15.2(4)M軟體的IOS路由器
- 採用AnyConnect 3.1.01065的Windows 7 PC

## 慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

# 背景

在IKEv1中，XAUTH用於第1.5階段，您可以在IOS路由器本機上以及使用RADIUS/TACACS+遠端執行使用者驗證。IKEv2不再支援XAUTH和1.5階段。它包含內建EAP支援，在IKE_AUTH階段完成。最大的優勢在於IKEv2設計，而EAP是眾所周知的標準。

EAP支援兩種模式：

- 通道 — EAP-TLS、EAP/PSK、EAP-PEAP等
- 非隧道 — EAP-MSCHAPv2、EAP-GTC、EAP-MD5等

在本示例中，使用非隧道模式中的EAP-MD5，因為它是當前在ACS 5.3中支援的EAP外部身份驗證方法。

EAP只能用於驗證啟動器（客戶端）到響應方（本例中為IOS）。

# IOS初始配置

## IOS - CA

首先，您需要建立憑證授權單位(CA)並為IOS路由器建立身分憑證。使用者端會根據該憑證驗證路由器的身分。

IOS上的CA配置如下所示：

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

您需要記住擴展金鑰用法（EAP需要Server-Auth，對於RSA-SIG，也需要客戶端 — Auth）。

在加密pki伺服器CA中使用**no shutdown**命令啟用CA。

## IOS — 身份證書

接下來，為證書啟用簡單證書註冊協定(SCEP)並配置信任點。

```
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
```

然後驗證並註冊憑證：

```
(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
```

如果不想在AnyConnect中包含提示消息，請記住cn需要等於AnyConnect配置檔案中配置的主機名/IP地址。

在本示例中，cn=10.1.1.2。因此，在AnyConnect中，10.1.1.2在AnyConnect xml配置檔案中輸入為伺服器的IP地址。

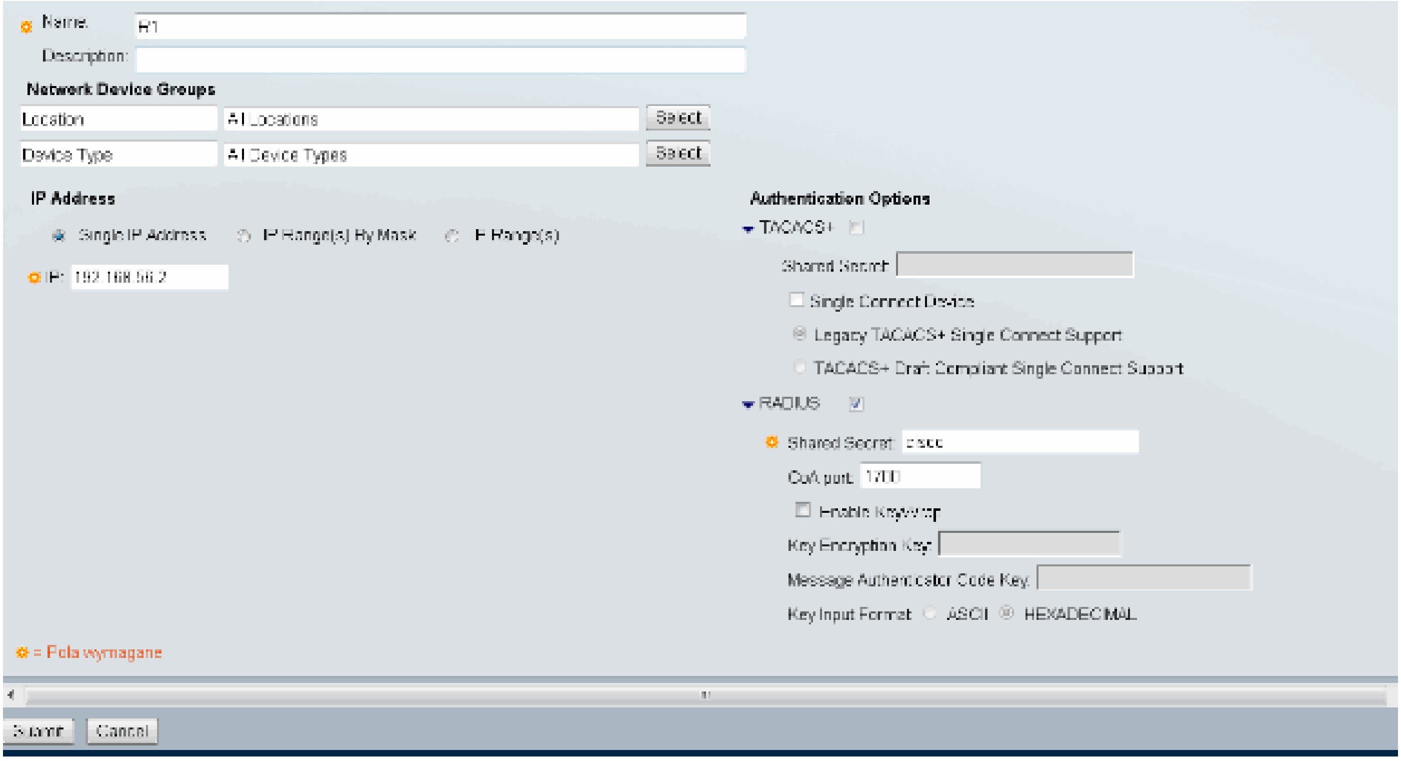
## IOS - AAA和Radius配置

您需要設定Radius和AAA驗證與授權：

```
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
```

# ACS初始配置

首先，在ACS中新增新的網路裝置(Network Resources > Network Devices and AAA Clients > Create):



Name: R1

Description:

Network Device Groups

| | | |
|---|---|---|
| Location | All Locations | Select |
| Device Type | All Device Types | Select |

IP Address

● Single IP Address ○ IP Range(s) By Mask ○ IP Range(s)

IP: 192.168.56.2

Authentication Options

TACACS+ □

Shared Secret:

□ Single Connect Device

● Legacy TACACS+ Single Connect Support

○ TACACS+ Draft Compliant Single Connect Support

RADIUS ☑

Shared Secret: cisco

CoA port: 1700

□ Enable KeyWrap

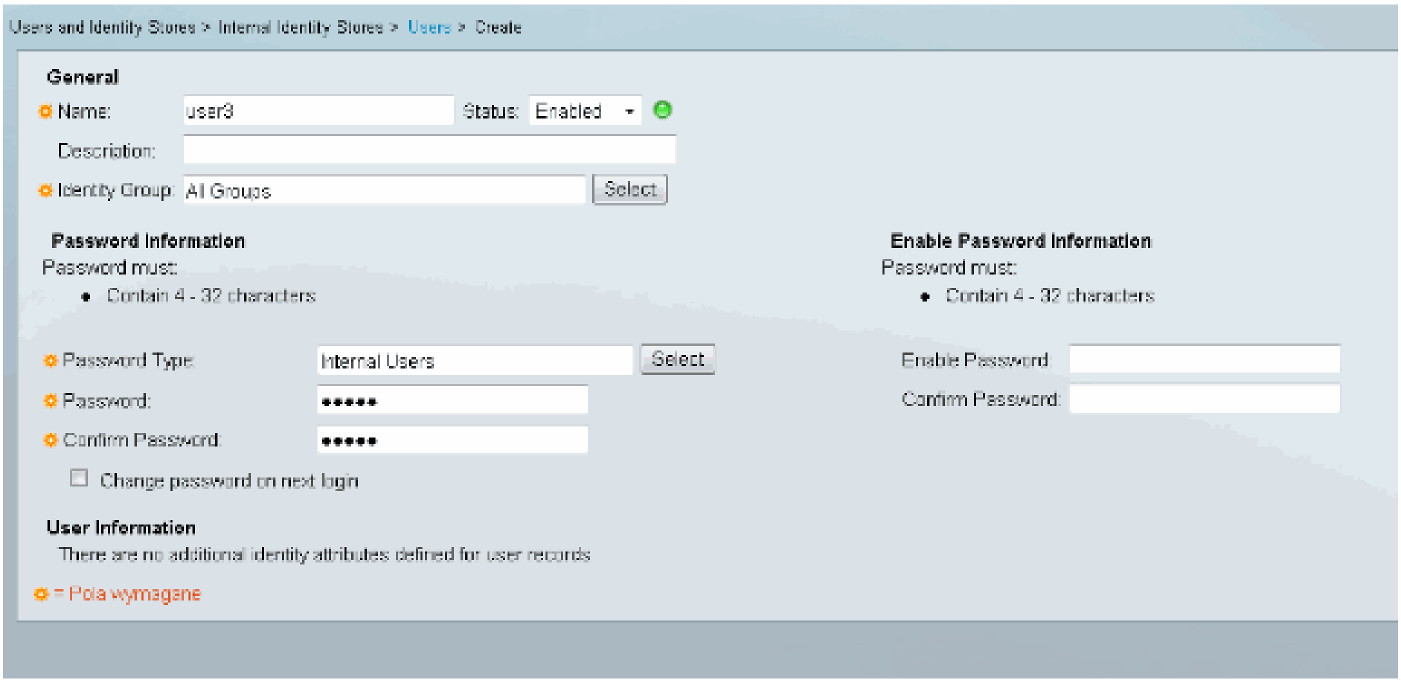
Key Encryption Key:

Message Authenticator Code Key:

Key Input Format ○ ASCII ● HEXADECIMAL

= Pola wymagane

新增使用者（使用者和身份庫>內部身份庫>使用者>建立）：



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

Enable Password Information

Password must:

- Contain 4 - 32 characters

Enable Password:

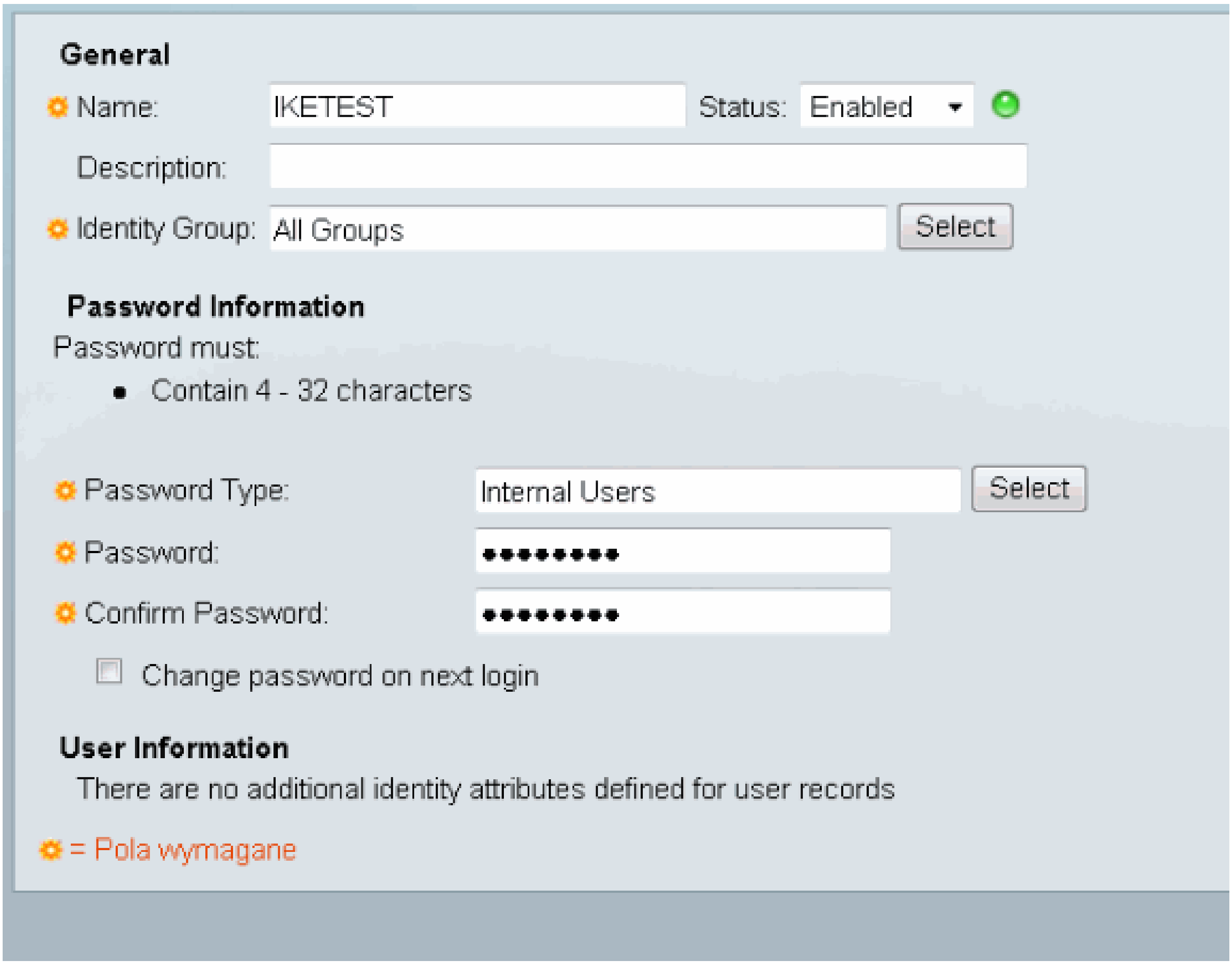
Confirm Password:

User Information

There are no additional identity attributes defined for user records

= Pola wymagane

新增使用者以進行授權。在本示例中，它是IKETEST。密碼必須為「cisco」，因為它是IOS傳送的預設密碼。



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

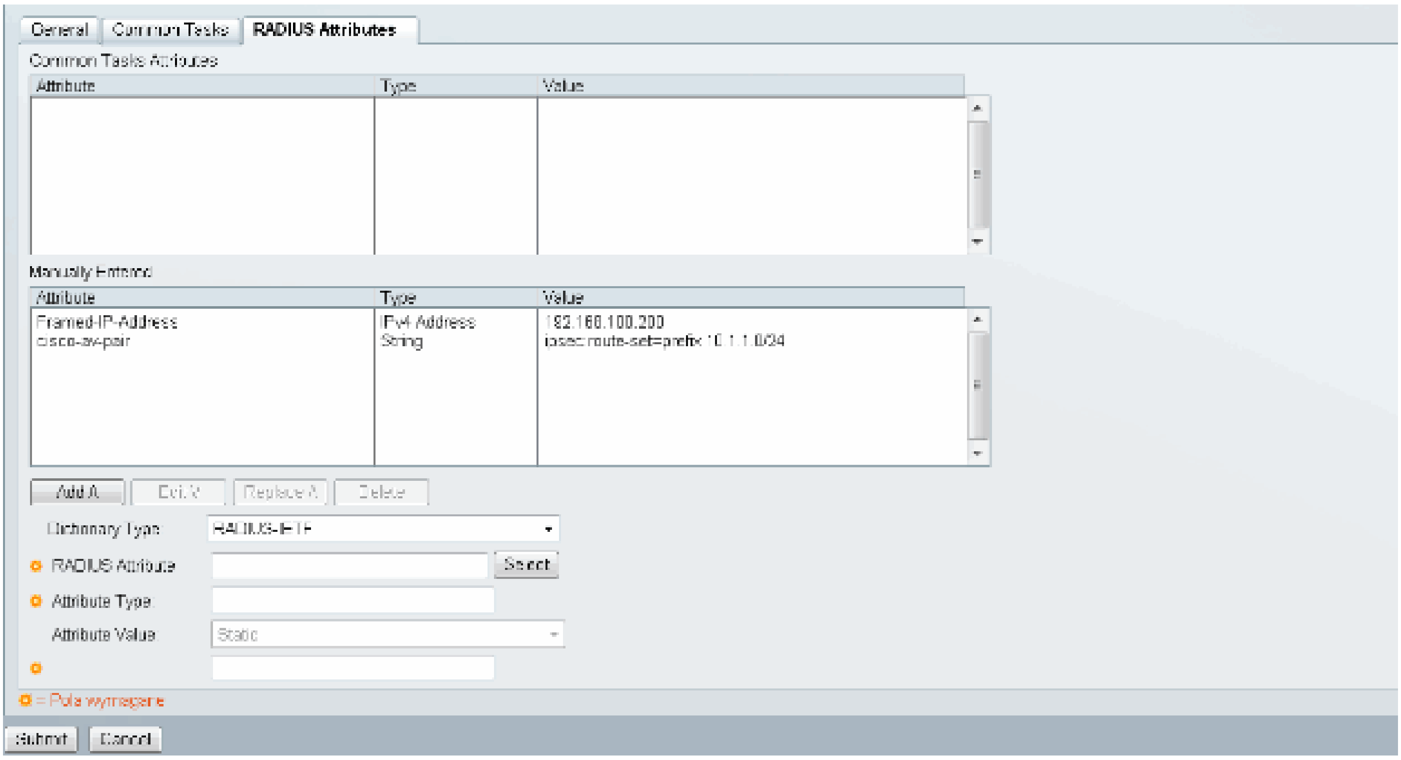
User Information

There are no additional identity attributes defined for user records

= Pola wymagane

接下來，為使用者建立授權配置檔案(Policy elements > Authorization and Permissions > Network Access > Authorization Profiles > Create)。

在本示例中，它稱為POOL。在本示例中，輸入拆分隧道AV對（作為字首），並將Framed-IP-Address作為要分配給所連線客戶端的IP地址。所有支援的AV對清單可在此處找到：http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html



Common Tasks Attributes

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

Manually Entered

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

Dictionary Type: RADIUS-IETF

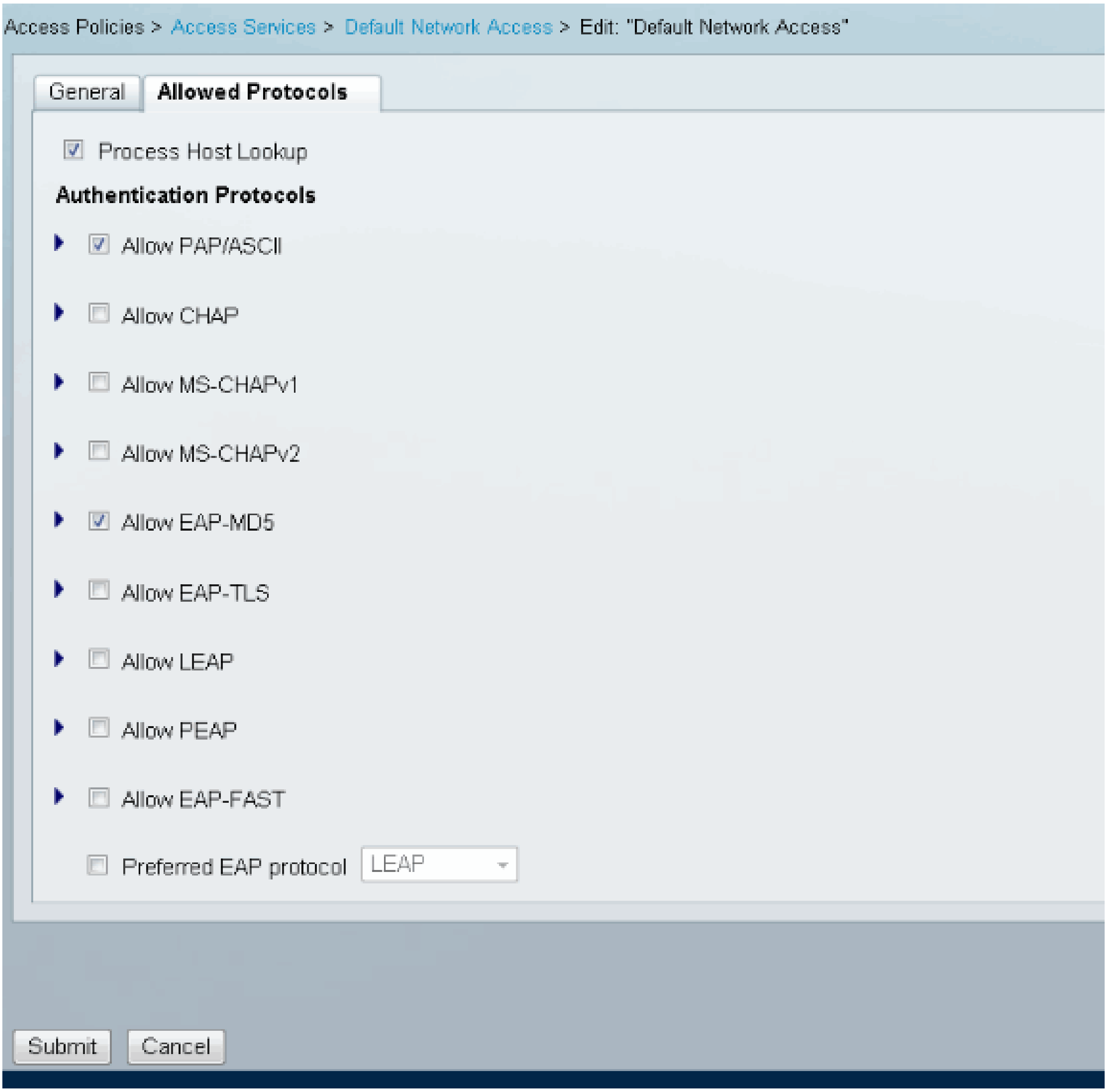
RADIUS Attribute:

Attribute Type:

Attribute Value: Static

= Pola wymagane

然後，您需要在「訪問策略」中啟用EAP-MD5（用於身份驗證）和PAP/ASCII（用於授權）支援。本示例中使用的是預設值(Access Policies > Default Network Access):



Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"

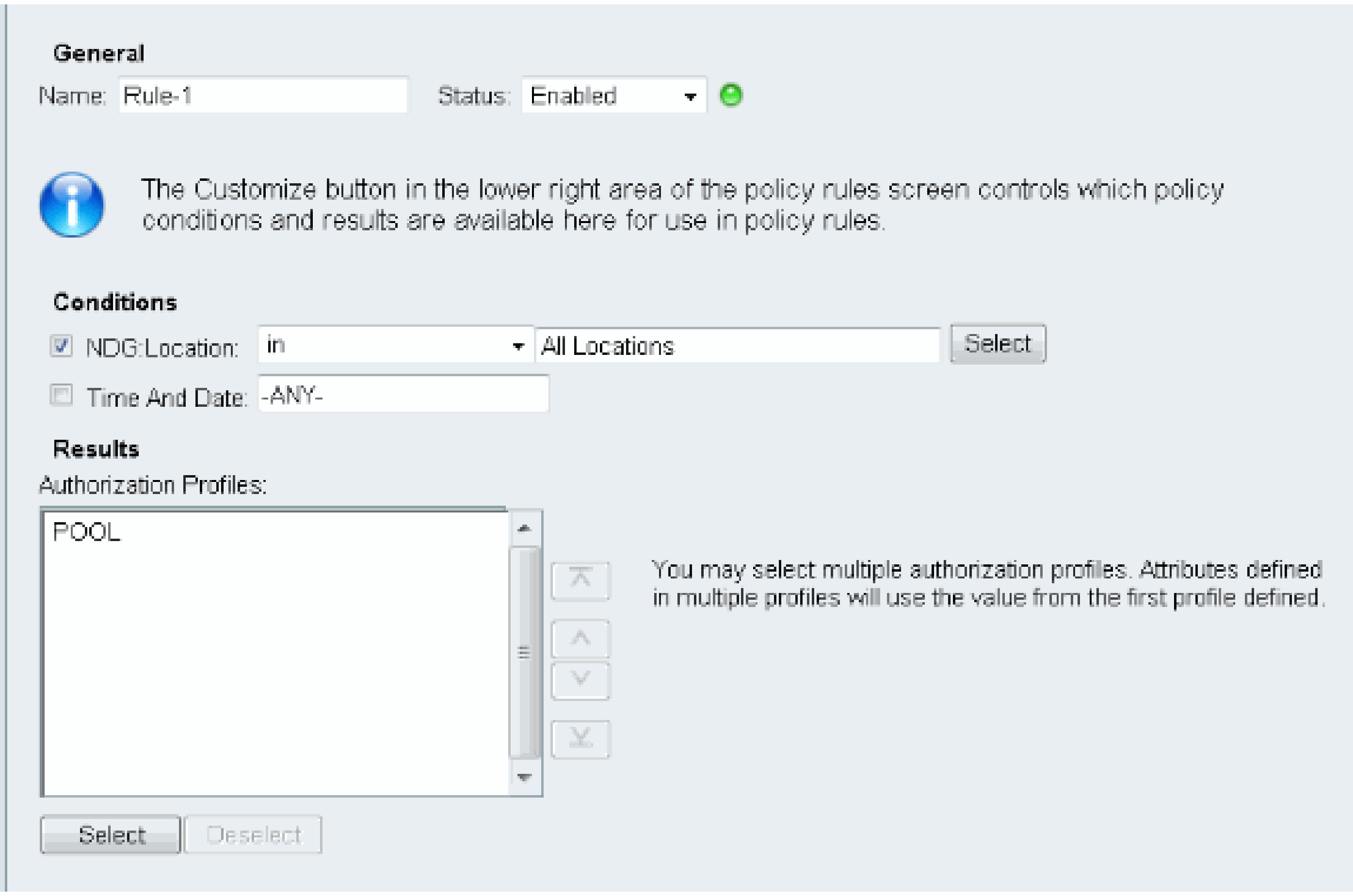
☑ Process Host Lookup

**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 LEAP

在訪問策略中為建立條件並分配已建立的授權配置檔案。在這種情況下，將建立NDG:Location in All Locations的條件，因此對於所有Radius授權請求，將提供POOL授權配置檔案（訪問策略>訪問服務>預設網路訪問）：



**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 All Locations Select

□ Time And Date: -ANY-

**Results**

Authorization Profiles:

POOL

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

如果使用者可以正確進行驗證，您應該能夠在IOS路由器上進行測試：

```
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"
```

# IOS FlexVPN配置

您需要建立IKEv2建議和策略(您可能不需要建立，請參閱CSCtn59317)。 在本例中，只為其中一個IP地址(10.1.1.2)建立策略。

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

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

然後，建立將繫結到虛擬模板的IKEV2配置檔案和IPsec配置檔案。

確保按照配置指南中的建議關閉http-url cert。

```
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
```

在本示例中，根據在ACS配置中建立的使用者IKETEST設定授權。

# Windows配置

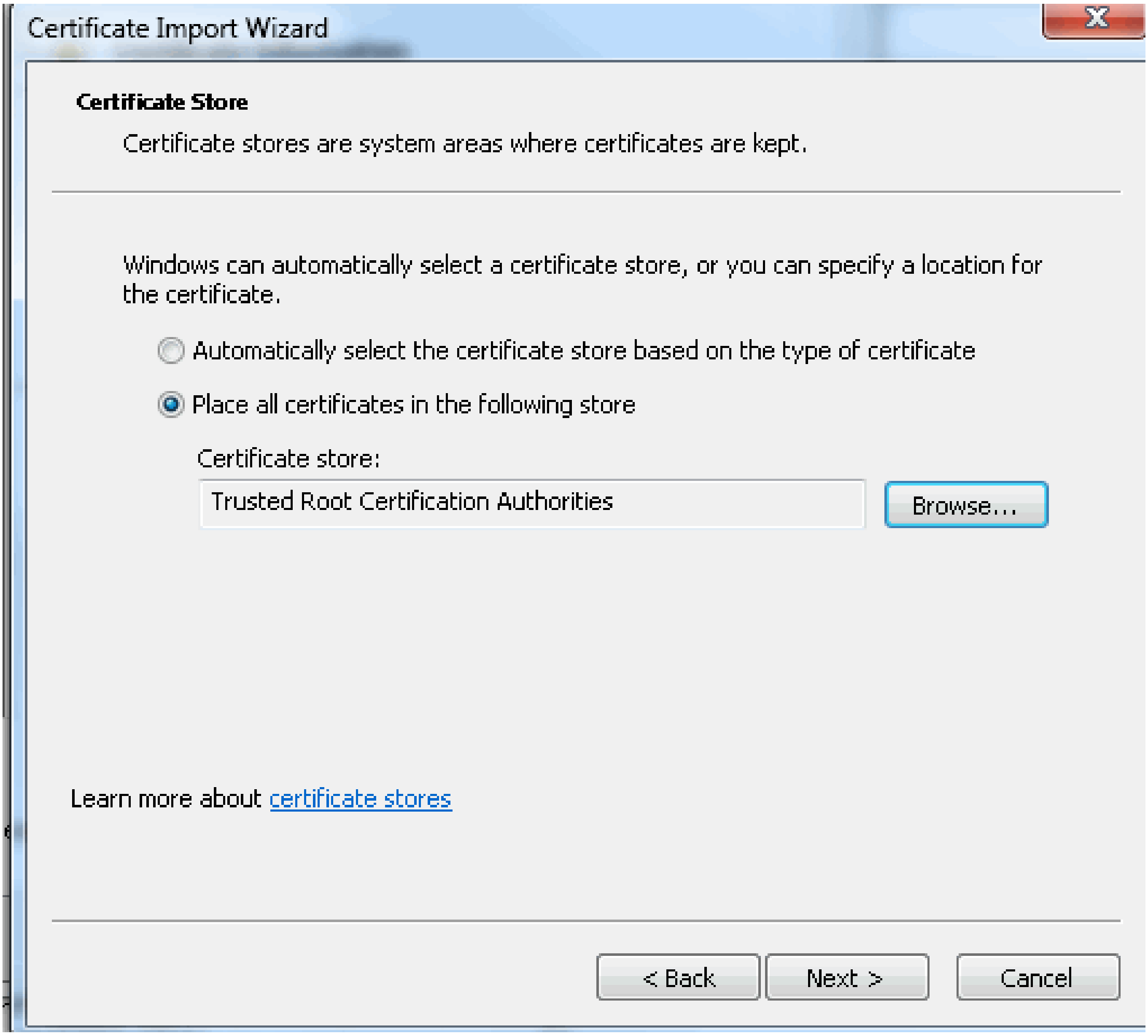
## 將CA匯入Windows信任

匯出IOS上的CA證書（確保匯出身份證書並只參加第一部分）：

```
R1(config)#crypto pki export CA-self pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB8zCCAVygAwIBAgIBATANBgkqhkiG9w0BAQUFADANMQswCQYDVQQDEwJDQTAe
Fw0xMjExMjYxNzMzMzlaFw0xNTExMjYxNzMzMzlaMA0xCzAJBgNVBAMTAkNBMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvDR4lHOcrj42QfHpRuNu4EyFrLR8H
TbPanXYV+GdCBmu53pDILE00ASEHByD6DYBx01EZuDsiolJ7t2MPTguB+YZe6V4O
JbtayyxtZGmF7+eDqRegQHHC394adQQWl2ojgQiuTHeRDTqDJR8i5gN2Ee+KOsr3
+OjnHjUmXb/I6QIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQE
AwIBhjAfBgNVHSMEGDAWgBTH5Sdh69q4HAJulLQYLbYH0Nk9zzAdBgNVHQ4EFgQU
x+UnYevauBwCbpS0GC22B9DZPc8wDQYJKoZIhvcNAQEFBQADgYEADtBLiNXnl+LC
PIgJ0nl/jH5p2IwVlzwbPbZcOsZ9mn54QaqrhmhbHnmqKQJl/20+JPE6p+4noICq
VBrxoiX2KYQ1OwmEScPpQ2XJ9vhGqtQ4Xcx3g20HhxxFDfp2XuW7hwU0W8dTCmZw
4vodj47qEXKI6pGuzauw9MN1xhkNarc=
-----END CERTIFICATE-----
```

將BEGIN CERTIFICATE和END CERTIFICATE之間的部分複製並貼上到Windows中的記事本中，然後儲存為檔案CA.crt。

您需要將其安裝為受信任的根證書頒發機構（按兩下檔案>安裝證書>將所有證書放入以下儲存>受信任的根證書頒發機構）：



Certificate Import Wizard

**Certificate Store**

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Learn more about certificate stores

## 配置AnyConnect XML配置檔案

在C:\ProgramData\Cisco\Cisco中，AnyConnect Secure Mobility Client\Profile建立檔案「whatever.xml」並貼上以下內容：

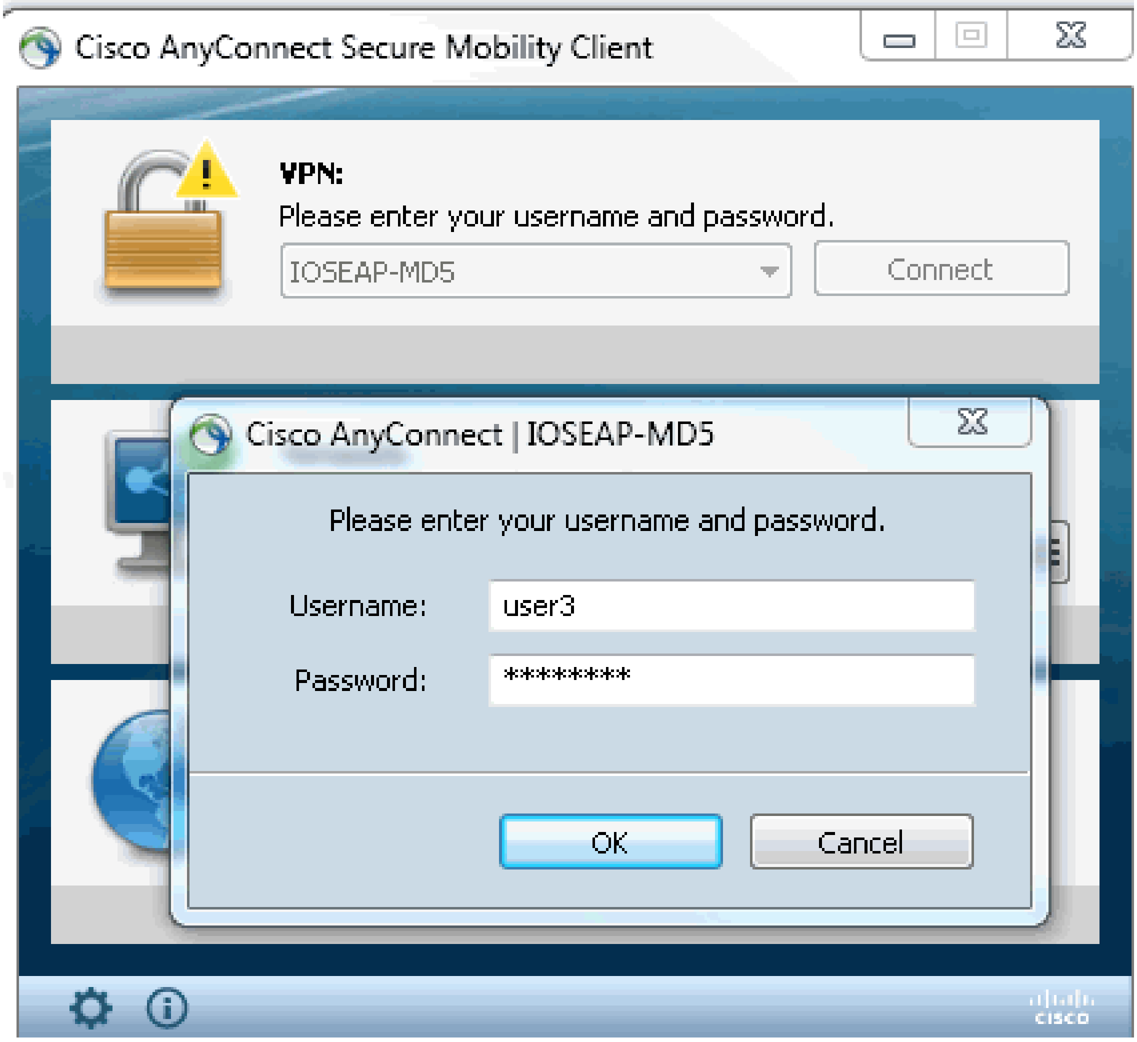
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
    <ClientInitialization>
        <UseStartBeforeLogon UserControllable="true">false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

確保10.1.1.2條目與為身份證書輸入的CN=10.1.1.2完全相同。

# 測試

在此情況中，未使用SSL VPN，因此請確保在IOS上禁用了HTTP伺服器(no ip http server)。 否則，您會收到AnyConnect中的錯誤消息「Use a browser to gain access（使用瀏覽器獲取訪問許可權）」。

在AnyConnect中連線時，應提示您輸入密碼。在本示例中，建立的是User3



Cisco AnyConnect Secure Mobility Client

VPN:
Please enter your username and password.

IOSEAP-MD5

Cisco AnyConnect | IOSEAP-MD5

Please enter your username and password.

Username: user3

Password: ********

之後，使用者會連線。

# 驗證

## IOS路由器

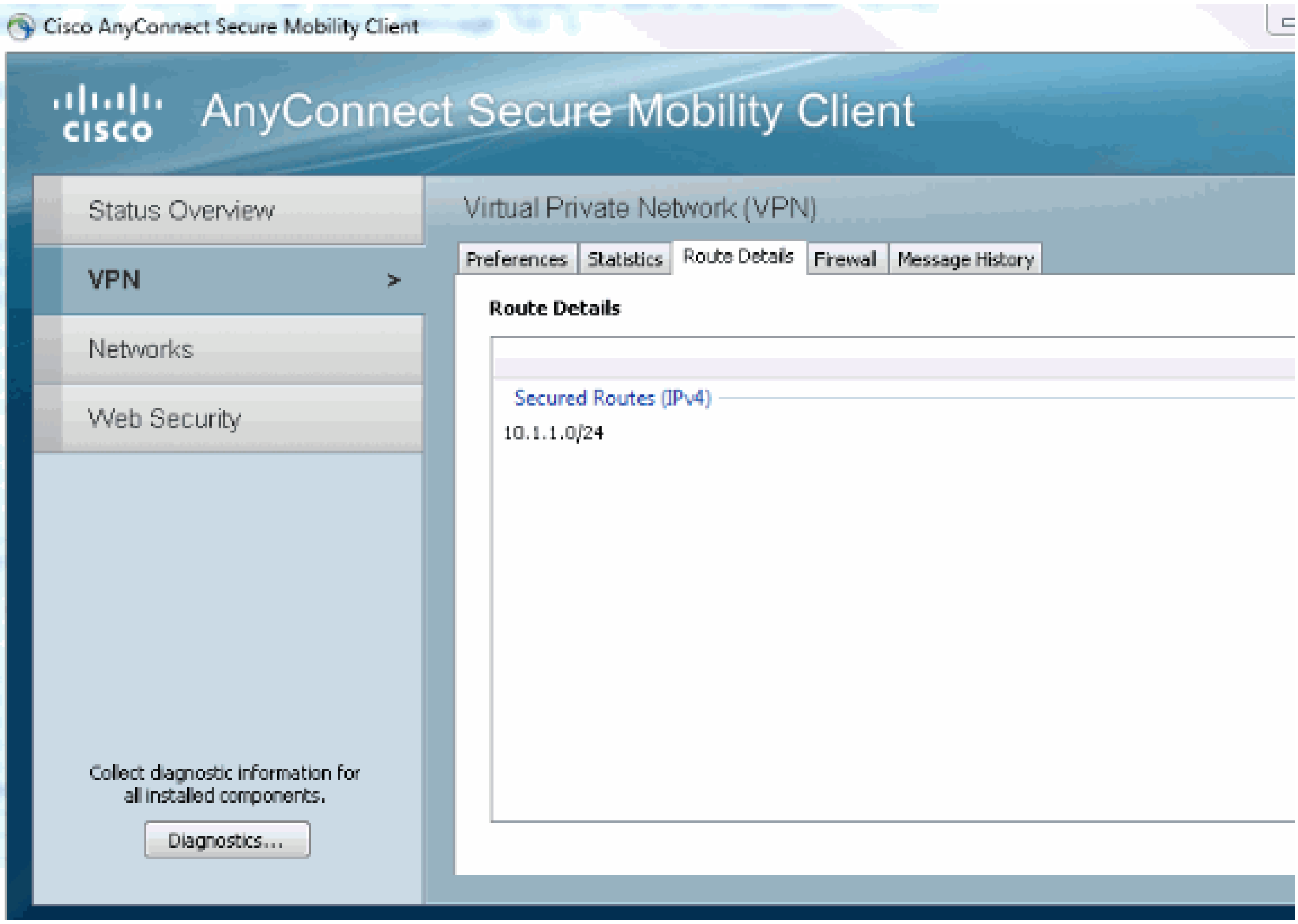
```
R1#show ip inter brief | i Virtual
Virtual-Access1    10.1.1.2  YES unset  up  up
Virtual-Template1  10.1.1.2  YES unset  up down
R1# show ip route 192.168.100.200
Routing entry for 192.168.100.200/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly 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
```

您可以執行調試(debug crypto ikev2)。

## Windows

在VPN中AnyConnect的Advanced選項中，可以檢查Route Details以檢視分割隧道網路：


Cisco AnyConnect Secure Mobility Client
cisco
AnyConnect Secure Mobility Client
Status Overview
VPN
Networks
Web Security
Virtual Private Network (VPN)
Preferences
Statistics
Route Details
Firewall
Message History
Collect diagnostic information for all installed components.
Diagnostics...

Route Details

Secured Routes (IPv4)

10.1.1.0/24

# 已知警告和問題

- 請記得，在IKEv2中，將SHA1放在簽名雜湊和完整性策略中時(請參閱思科錯誤ID CSCtn59317(僅限註冊客戶))。
- IOS身份證書中的CN必須等於ACS XML配置檔案中的主機名。
- 如果要在身份驗證期間使用傳遞的Radius AV對，而完全不使用組的授權，可以在IKEv2配置檔案中使用以下命令：
  ```
  aaa authorization user eap cached
  ```

- 授權始終使用密碼「cisco」進行組/使用者授權。在使用時可能會造成混淆
  `aaa authorization user eap list SERV (without any paramaters)`
  因為它將嘗試使用作為使用者和密碼「cisco」傳遞到AnyConnect中的使用者進行授權，該密碼可能不是該使用者的密碼。
- 如果發生任何問題，您可以分析以下輸出並將其提供給Cisco TAC:debug crypto ikev2debug crypto ikev2 internalDART輸出
- 如果未使用SSL VPN，請記住禁用ip http伺服器(no ip http server)。 否則，AnyConnect將嘗試連線到HTTP伺服器並接收結果「使用瀏覽器獲取訪問許可權」。

## 下一代加密技術

上述結構可供參考，以展示最小的工作結構。

思科建議儘可能使用下一代加密技術(NGC)。

有關遷移的最新建議，請訪問以下網站：http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

選擇NGC配置時，請確保客戶端軟體和頭端硬體都支援它。建議使用ISR第2代路由器和ASR 1000路由器作為前端，因為它們支援NGC。

在AnyConnect端，自AnyConnect 3.1版本起，支援NSA的Suite B演算法套件。

# 相關資訊

- Cisco ASA IKEv2 PKI站點到站點VPN
- IOS上的IKEv2 Site2-Site調試
- FlexVPN/IKEv2:Windows 7內建客戶端：IOS頭端：第I部分 — 證書身份驗證
- FlexVPN和Internet金鑰交換版本2配置指南，Cisco IOS版本15.2M&T
- 技術支援與文件 - Cisco Systems