

FlexVPN 구축:EAP-MD5를 사용한 AnyConnect IKEv2 원격 액세스

목차

[소개](#)

[사전 요구 사항](#)

[네트워크 다이어그램](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경](#)

[IOS 초기 컨피그레이션](#)

[IOS - CA](#)

[IOS - ID 인증서](#)

[IOS - AAA 및 Radius 컨피그레이션](#)

[ACS 초기 컨피그레이션](#)

[IOS FlexVPN 컨피그레이션](#)

[Windows 구성](#)

[Windows 트러스트로 CA 가져오기](#)

[AnyConnect XML 프로파일 구성](#)

[테스트](#)

[확인](#)

[IOS 라우터](#)

[윈도우](#)

[알려진 주의 사항 및 문제](#)

[차세대 암호화](#)

[관련 정보](#)

소개

이 문서에서는 FlexVPN 툴킷을 사용하여 IOS에서 원격 액세스를 설정하는 방법에 대한 샘플 컨피그레이션을 제공합니다.

원격 액세스 VPN을 사용하면 다양한 운영 체제를 사용하는 최종 클라이언트가 인터넷과 같은 비보안 매체를 통해 회사 또는 홈 네트워크에 안전하게 연결할 수 있습니다. 제시된 시나리오에서 IKEv2 프로토콜을 사용하여 Cisco IOS 라우터에서 VPN 터널이 종료됩니다.

이 문서는 EAP-MD5 방법을 통해 ACS(Access Control Server)를 사용하여 사용자를 인증하고 권한을 부여하는 방법을 보여줍니다.

사전 요구 사항

네트워크 다이어그램

Cisco IOS Router에는 ACS 5.3을 향한 2개의 인터페이스가 있습니다.



요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ACS 5.3(패치 6 포함)
- 15.2(4)M 소프트웨어가 포함된 IOS 라우터
- Windows 7 PC with AnyConnect 3.1.01065

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

배경

IKEv1 XAUTH는 1.5단계에서 사용되며 IOS 라우터에서 로컬로 그리고 RADIUS/TACACS+를 사용하여 원격으로 사용자를 인증할 수 있습니다. IKEv2는 XAUTH 및 1.5단계를 더 이상 지원하지 않습니다. IKE_AUTH 단계에서 수행되는 내장 EAP 지원을 포함합니다. IKEv2 설계에서 가장 큰 장점이 있으며 EAP는 잘 알려진 표준입니다.

EAP는 두 가지 모드를 지원합니다.

- 터널링 - EAP-TLS, EAP/PSK, EAP-PEAP 등
- 비 터널링 - EAP-MSCHAPv2, EAP-GTC, EAP-MD5 등

이 예에서는 비 터널링 모드의 EAP-MD5가 현재 ACS 5.3에서 지원되는 EAP 외부 인증 방법이므로 사용됩니다.

EAP는 인증 개시자(클라이언트)에서 responder(이 경우 IOS)에만 사용할 수 있습니다.

IOS 초기 컨피그레이션

IOS - CA

먼저 CA(Certificate Authority)를 생성하고 IOS 라우터에 대한 ID 인증서를 생성해야 합니다.클라이언트는 해당 인증서를 기반으로 라우터의 ID를 확인합니다.

IOS에서 CA의 구성은 다음과 같습니다.

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

확장 키 사용(EAP에 필요한 서버-인증, RSA-SIG에 클라이언트 인증 필요)에 대해 기억해야 합니다

crypto pki 서버 CA에서 **no shutdown** 명령을 사용하여 CA를 활성화합니다.

IOS - ID 인증서

그런 다음 인증서에 대해 SCEP(Simple Certificate Enrollment Protocol)를 활성화하고 신뢰 지점을 구성합니다.

```
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
```

그런 다음 인증서를 인증하고 등록합니다.

```
(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
```

AnyConnect에서 프롬프트 메시지를 표시하지 않으려면 AnyConnect 프로파일에 구성된 호스트 이름/IP 주소와 동일해야 합니다.

이 예에서는 cn=10.1.1.2입니다. 따라서 AnyConnect 10.1.1.2에서 AnyConnect xml 프로파일에 서버의 IP 주소로 입력됩니다.

IOS - AAA 및 Radius 컨피그레이션

Radius 및 AAA 인증 및 권한 부여를 구성해야 합니다.

```
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 초기 컨피그레이션

먼저 ACS에 새 네트워크 디바이스를 추가합니다(Network Resources(네트워크 리소스) > Network Devices and AAA Clients(네트워크 디바이스 및 AAA 클라이언트) > Create(생성).

The screenshot shows the configuration page for a new network device in ACS. The 'Name' field contains 'H1'. The 'Network Device Groups' section has 'Location' set to 'All Locations' and 'Device Type' set to 'All Device Types'. The 'IP Address' section has 'Single IP Address' selected with the IP address '192.168.56.2'. The 'Authentication Options' section has 'TACACS+' disabled and 'RADIUS' selected. Under 'RADIUS', the 'Shared Secret' is 'cisco', 'Auth port' is '1812', and 'Key Input Format' is 'HEXADECIMAL'. There are also fields for 'Key Encryption Key' and 'Message Authenticator Code Key'.

사용자 추가(Users and Identity Stores > Internal Identity Stores > Users > Create):

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:

권한 부여를 위해 사용자를 추가합니다. 이 예에서는 IKEST입니다. 비밀번호는 IOS에서 전송하는 기본값이므로 "cisco"여야 합니다.

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

그런 다음 사용자에게 대한 권한 부여 프로파일을 만듭니다(Policy elements(정책 요소) > Authorization and Permissions(권한 부여 및 권한) > Network Access(네트워크 액세스) >

Authorization Profiles(권한 부여 프로파일) > Create(생성).

이 예에서는 POOL이라고 합니다.이 예에서는 Split-Tunnel AV Pair(접두사로) 를 입력하고 연결된 클라이언트에 할당할 IP 주소로 Framed-IP-Address를 입력합니다.지원되는 모든 AV 쌍의 목록은 여기에서 확인할 수 있습니다.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: 'Common Tasks Attributes' (empty) and 'Manually Entered' (containing one entry). Below the tables are buttons for 'Add A', 'Edit A', 'Replace A', and 'Delete'. A 'Dictionary Type' dropdown is set to 'RADIUS-IP'. There are also fields for 'RADIUS Attribute', 'Attribute Type', and 'Attribute Value' with a 'Select' button. At the bottom, there are 'Submit' and 'Cancel' buttons.

Attribute	Type	Value
Framed-IP-Address cisco-av-pair	IPv4 Address String	182.168.100.200 iossec:route-set=prefix:10.1.1.0/24

그런 다음 액세스 정책에서 EAP-MD5(인증) 및 PAP/ASCII(권한 부여용) 지원을 켜야 합니다.기본 값은 다음 예에서 사용됩니다(Access Policies(액세스 정책) > Default Network Access(기본 네트워크 액세스)).

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

Access Policy(액세스 정책)에 대한 조건을 생성하고 생성된 권한 부여 프로파일을 할당합니다.이 경우 NDG:Location in All Locations(모든 위치의 위치)에 대한 조건이 생성되므로 모든 RADIUS 권한 부여 요청에 대해 POOL 권한 부여 프로파일(액세스 정책 > 액세스 서비스 > 기본 네트워크 액세스)이 제공됩니다.

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
 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.

사용자가 올바르게 인증할 수 있는 경우 IOS 라우터에서 테스트할 수 있어야 합니다.

```
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 컨피그레이션](#)

IKEv2 제안서 및 정책을 생성해야 합니다(CSCtn59317 참조). 이 예에서는 IP 주소(10.1.1.2) 중 하나에 대해서만 정책이 생성됩니다.

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

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

그런 다음 가상 템플릿에 바인딩할 IKEV2 프로파일 및 IPsec 프로파일 만듭니다.

컨피그레이션 가이드에서 권장하는 대로 http-url 인증서를 꺼야 합니다.

```
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-Templatel type tunnel
ip unnumbered Ethernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF

```

이 예에서는 ACS 컨피그레이션에서 생성된 사용자 IKEST를 기반으로 권한 부여가 설정됩니다.

Windows 구성

Windows 트러스트로 CA 가져오기

IOS에서 CA 인증서를 내보냅니다(ID 인증서를 내보내고 첫 번째 부분만 가져와야 함).

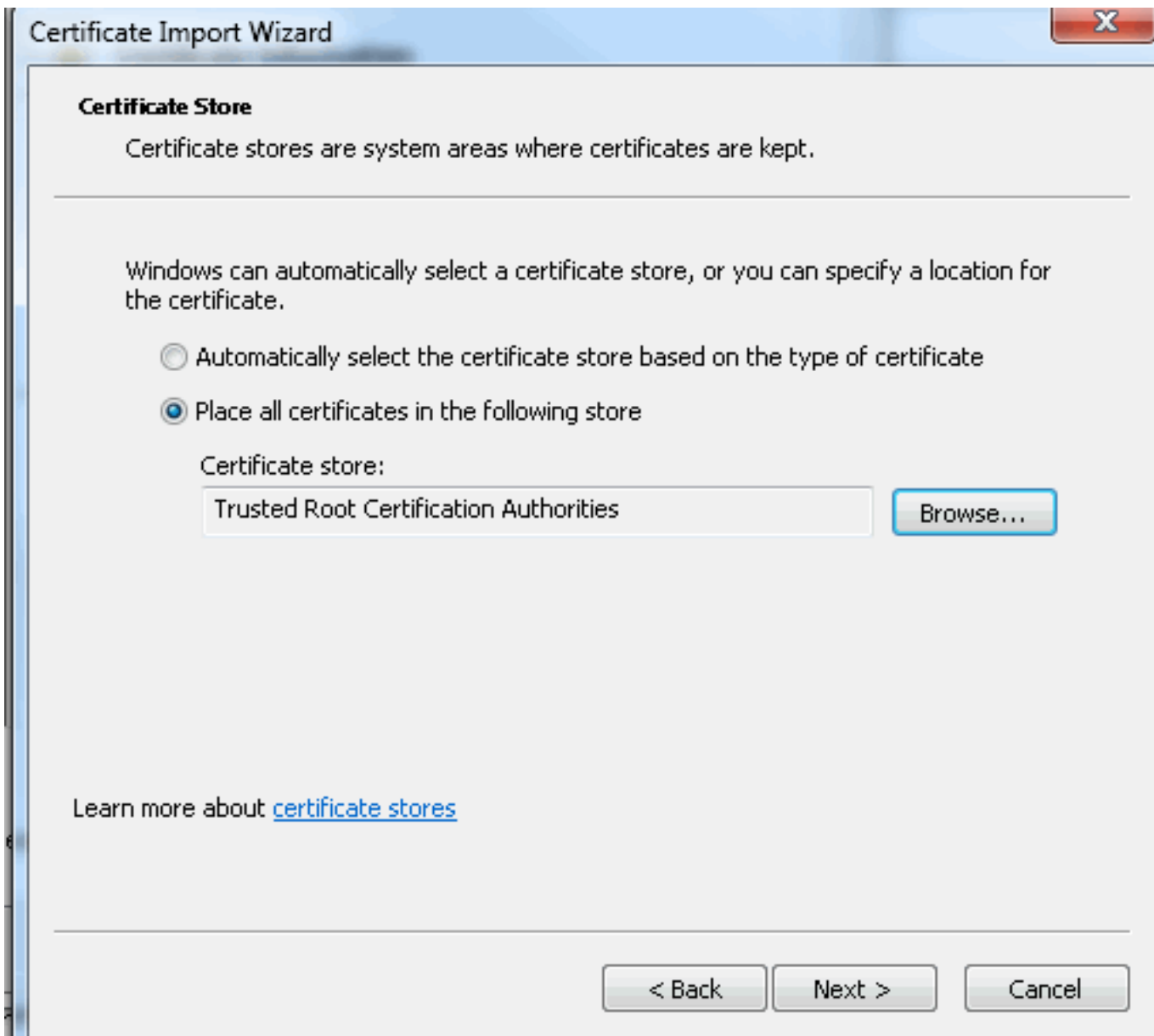
```

R1(config)#crypto pki export CA-self pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB8zCCAIVygAwIBAgIBATANBgkqhkiG9w0BAQUFADANMQswCQYDVQQDEwJDQTAE
Fw0xMjExMjYxNzZmZmlaFw0xNTEyMjYxNzZmZmlaMA0xCzAJBgNVBAMTAKNBMIGF
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvDR4lHOcrj42QfHpRuNu4EyFrLR8H
TbPanXYV+GdCBmu53pDILE00ASEHByD6DYBx01EZuDsioLJ7t2MPTguB+YZe6V4O
JbtayyxtZGmF7+eDqRegQHHC394adQQWl2ojgQiuThERDTqDJR8i5gN2Ee+K0sr3
+OjnHjUmXb/I6QIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQE
AwIBhjAfBgNVHSMEGDAWgBTH5Sdh69q4HAJulLQYLbYH0Nk9zzAdBgNVHQ4EFgQU
x+UnYevauBwCbPpS0GC22B9DZPc8wDQYJKoZIhvcNAQEFBQADgYEADtBLiNXnl+LC
PIgJ0nl/jH5p2IwVlzwPbZcOsZ9mn54QaqrhmhbHnmqKQJl/20+JPE6p+4noICq
VBrxoiX2KYQ1OwmEScPpQ2XJ9vhGqtQ4Xcx3g20HhxxFDfp2XuW7hwU0W8dTCmZw
4vodj47qEXKI6pGuzauw9MN1xhkNarc=
-----END CERTIFICATE-----

```

BEGIN CERTIFICATE와 END CERTIFICATE 사이에 부품을 복사하여 Windows의 메모장에 붙여 넣고 CA.crt 파일로 저장합니다.

신뢰할 수 있는 루트 권한(file > Install Certificate > Place all certificates in the following store > Trusted Root Certification Authorities)을 두 번 클릭하여 이 인증서를 신뢰할 수 있는 루트 인증 기관(Trusted Root Authorities)에 설치해야 합니다.



[AnyConnect XML 프로파일 구성](#)

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile create a file "whether.xml"에서 다음을 붙여넣습니다.

```
<?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>

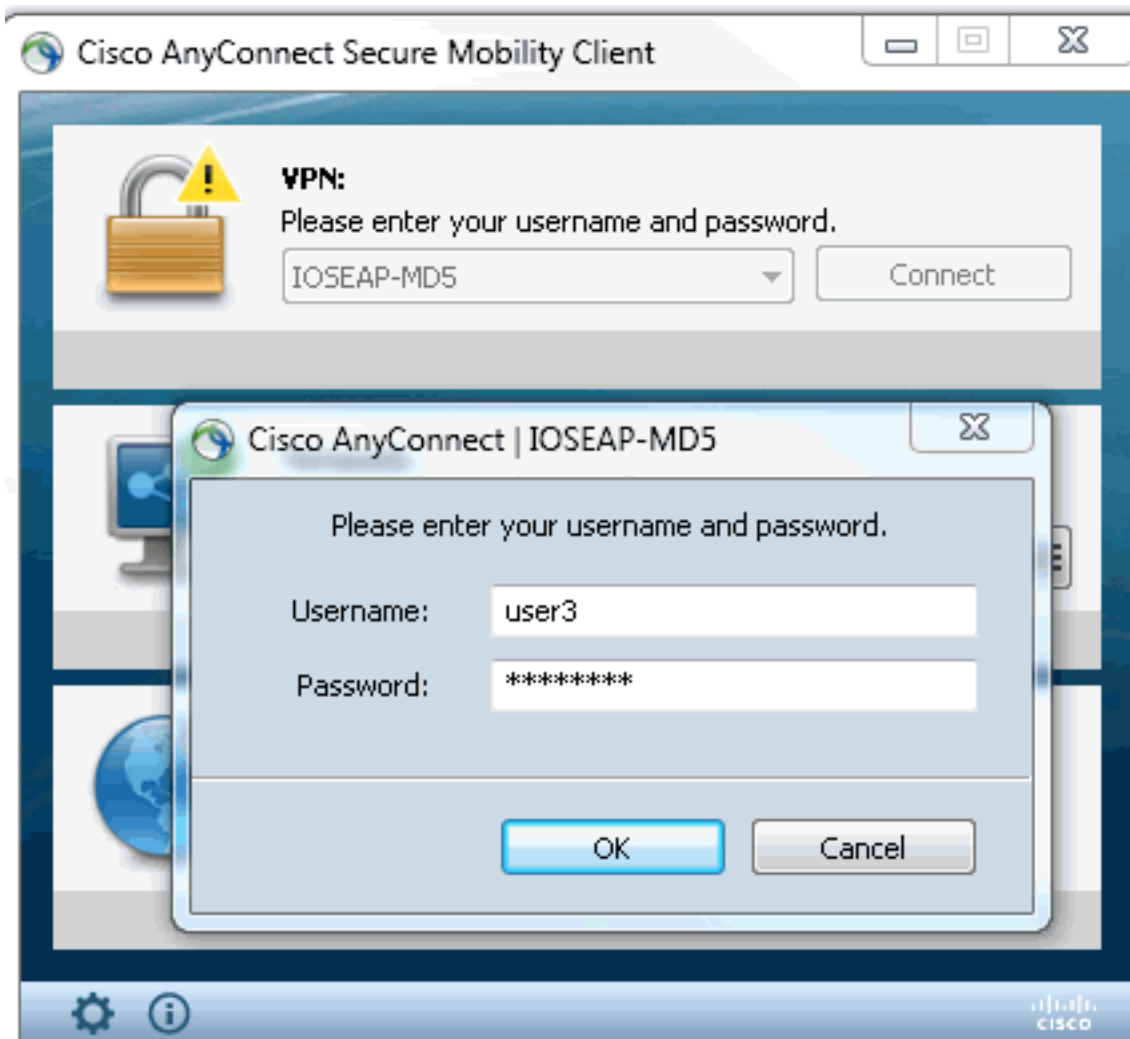
```

10.1.1.2 항목이 ID 인증서에 대해 입력된 CN=10.1.1.2과 정확히 같은지 확인합니다.

테스트

이 시나리오에서는 SSL VPN이 사용되지 않으므로 IOS에서 HTTP 서버가 비활성화되었는지 확인합니다(ip http 서버 없음). 그렇지 않으면 AnyConnect에서 "Use a browser to gain access"라는 오류 메시지가 표시됩니다.

AnyConnect에서 연결할 때 암호를 입력하라는 메시지가 표시됩니다.이 예에서는 생성된 User3입니다.



그 후에는 사용자가 연결됩니다.

확인

IOS 라우터

```
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
```

```

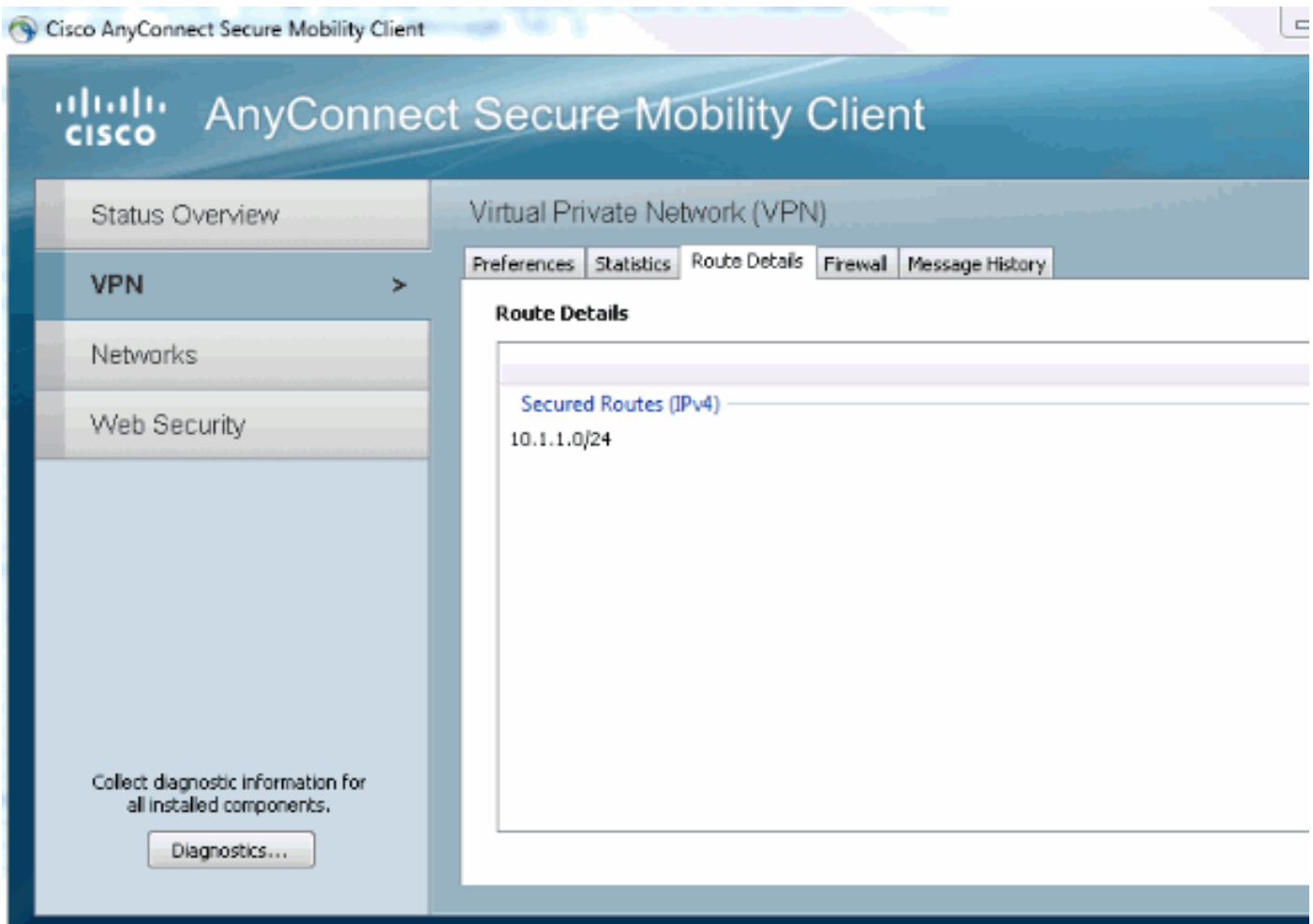
X - IKE Extended Authentication, F - IKE Fragmentation
Interface: Virtual-Access1
Uptime: 00:04:06
Session status: UP-ACTIVE
Peer: 192.168.56.1 port 61021 fvrf: (none) ivrf: (none)
  Phase1_id: IKETEST
  Desc: (none)
  IKEv2 SA: local 10.1.1.2/4500 remote 10.1.1.100/61021 Active
    Capabilities:(none) 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

```

디버그(debug crypto ikev2)를 수행할 수 있습니다.

원도우

VPN에서 AnyConnect의 고급 옵션에서 Route Details를 선택하여 스플릿 터널링 네트워크를 확인할 수 있습니다.



알려진 주의 사항 및 문제

- IKEv2의 서명 해시 및 무결성 정책에 SHA1을 사용하는 경우(Cisco 버그 ID [CSCtn59317](#) 참조 (등록된 고객만 해당)).
- IOS ID 인증서의 CN은 ACS XML 프로파일의 호스트 이름과 같아야 합니다.
- 인증 중에 전달된 Radius AV 쌍을 사용하고 그룹의 권한 부여를 전혀 사용하지 않으려면

IKEv2 프로파일에서 이 기능을 사용할 수 있습니다.

```
aaa authorization user eap cached
```

- 권한 부여는 항상 그룹/사용자 권한 부여에 비밀번호 "cisco"를 사용합니다.사용 중에 혼동될 수 있습니다.

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

AnyConnect에서 사용자 및 비밀번호 "cisco"로 전달된 사용자를 사용하여 권한을 부여하려고 합니다. 이는 사용자의 비밀번호가 아닐 수 있습니다.

- 문제가 발생할 경우 이러한 결과는 분석 및 Cisco TAC에 제공할 수 있는 출력입니다.디버그 암호화 ikev2디버그 암호화 ikev2 내부DART 출력
- SSL VPN을 사용하지 않는 경우 ip http 서버(ip http 서버 없음)를 비활성화하십시오. 그렇지 않으면 AnyConnect는 HTTP 서버에 연결을 시도하여 "Use a browser to gain access(브라우저를 사용하여 액세스를 얻음)"라는 결과를 수신합니다.

차세대 암호화

위의 컨피그레이션은 최소한의 작업 컨피그레이션을 표시하기 위한 참조를 위해 제공됩니다.

가능한 경우 NGC(Next Generation Cryptography)를 사용하는 것이 좋습니다.

마이그레이션에 대한 현재 권장 사항은 여기에서 확인할 수 있습니다

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

NGC 컨피그레이션을 선택할 때 클라이언트 소프트웨어와 헤드엔드 하드웨어 모두 이를 지원하는지 확인합니다.ISR 2세대 및 ASR 1000 라우터는 NGC에 대한 하드웨어 지원 때문에 헤드엔드로 권장됩니다.

AnyConnect에서는 AnyConnect 3.1 버전부터 NSA의 Suite B 알고리즘 스위트가 지원됩니다.

관련 정보

- [Cisco ASA IKEv2 PKI 사이트 사이트 VPN](#)
- [IOS의 IKEv2 Site2-Site 디버깅](#)
- [FlexVPN/IKEv2:Windows 7 기본 제공 클라이언트:IOS 헤드엔드:Part I - 인증서 인증](#)
- [FlexVPN 및 Internet Key Exchange 버전 2 컨피그레이션 가이드, Cisco IOS 릴리스 15.2M&T](#)
- [기술 지원 및 문서 - Cisco Systems](#)