

Despliegue de FlexVPN: Acceso Remoto de AnyConnect IKEv2 con el EAP-MD5

Contenido

[Introducción](#)

[prerrequisitos](#)

[Diagrama de la red](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedente](#)

[Configuración inicial IOS](#)

[IOS - CA](#)

[IOS - Certificado de identidad](#)

[IOS - AAA y configuración de RADIUS](#)

[Configuración inicial ACS](#)

[Configuración IOS FlexVPN](#)

[Configuración de Windows](#)

[Importación de CA a las confianzas de Windows](#)

[Configurar el perfil de AnyConnect XML](#)

[Pruebas](#)

[Verificación](#)

[Router IOS](#)

[Windows:](#)

[Advertencias conocidas y problemas](#)

[Criptografía de la última generación](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una configuración de muestra de cómo configurar el Acceso Remoto en el IOS usando el juego de herramientas de FlexVPN.

El VPN de acceso remoto permite a los fin-clientes que usan los diversos sistemas operativos para conectar con seguridad con su corporativo o redes domésticas con el media NON-seguro tal como Internet. En el actual escenario, el túnel VPN se está terminando en un router del Cisco IOS que usa el protocolo IKEv2.

Este documento muestra cómo autenticar y autorizar a los usuarios que usan el Access Control Server (ACS) con el método del EAP-MD5.

prerrequisitos

Diagrama de la red

El router del Cisco IOS tiene dos interfaces - una hacia ACS 5.3:



Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ACS 5.3 con la corrección 6
- Router IOS con el software del 15.2(4)M
- Windows 7 PC con AnyConnect 3.1.01065

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Antecedente

En IKEv1 el XAUTH se utiliza en la fase 1.5, usted puede hacer la autenticación de los usuarios localmente en un router IOS y remotamente usando el RADIUS/TACACS+. IKEv2 no soporta el XAUTH y la fase 1.5 más. Contiene el soporte del accesorio EAP, que se hace en la fase IKE_AUTH. La ventaja más grande de esto está en el diseño IKEv2 y el EAP es un estándar bien conocido.

El EAP soporta dos modos:

- El hacer un túnel — EAP-TLS, EAP/PSK, EAP-PEAP etc.
- NON-Tunelización — EAP MSCHAPv2, EAP-GTC, EAP-MD5 etc.

En este ejemplo, el EAP-MD5 en el modo del NON-Tunelización se utiliza porque es método de autenticación externo EAP soportado actualmente en ACS 5.3.

El EAP se puede utilizar solamente al iniciador de la autenticación (cliente) al respondedor (IOS

en este caso).

Configuración inicial IOS

IOS - CA

En primer lugar usted necesita crear el Certificate Authority (CA) y crear un certificado de identidad para el router IOS. El cliente verificará la identidad del router basada en ese certificado.

La configuración de CA en el IOS parece:

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

Usted necesita recordar sobre el uso dominante extendido (Servidor-auth necesario para el EAP, porque RSA-SIG usted también necesita el Cliente-auth).

Habilite el CA usando el **comando no shutdown** en el servidor pki crypto CA.

IOS - Certificado de identidad

Después, protocolo simple certificate enrollment del permiso (SCEP) para el certificado y trustpoint de la configuración.

```
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
```

Entonces, autentique y aliste el certificado:

```
(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

```

Si usted no quiere hacer que los prompts de petición en AnyConnect recuerden que el cn necesita ser igual al nombre de host/a los IP Addresses configurados en el perfil de AnyConnect.

En este ejemplo, cn=10.1.1.2. Por lo tanto, en AnyConnect 10.1.1.2 se ingresa como IP Address del servidor en el perfil del xml de AnyConnect.

[IOS - AAA y configuración de RADIUS](#)

Usted necesita configurar el radio y autenticación AAA y autorización:

```

(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

```

[Configuración inicial ACS](#)

Primero, agregue el nuevo dispositivo de red en el ACS (los recursos de red > los dispositivos de red y los clientes AAA > crean):

The screenshot shows the configuration page for a new network device in Cisco ACS. The form includes the following sections:

- Name:** H1
- Description:** (empty)
- Network Device Groups:**
 - Location:** All Locations
 - Device Type:** All Device Types
- IP Address:**
 - Single IP Address (selected)
 - IP Range(s) By Mask
 - IP Range(s)
 - IP:** 192.168.56.2
- Authentication Options:**
 - TACACS+:**
 - Shared Secret: (empty)
 - Single Connect Device: (unchecked)
 - Legacy TACACS+ Single Connect Support: (checked)
 - TACACS+ Draft Compliant Single Connect Support: (unchecked)
 - RADIUS:**
 - Shared Secret: cisco
 - Out port: 1812
 - Enable Keywrap: (unchecked)
 - Key Encryption Key: (empty)
 - Message Authenticator Code Key: (empty)
 - Key Input Format: ASCII (unchecked), HEXADECIMAL (checked)

At the bottom left, there is a legend: **⊙ = Pola wymagane**. At the bottom, there are buttons for "Save" and "Cancel".

Agregue a un usuario (los usuarios y la identidad salva > los almacenes internos de la identidad > Users > crean):


The screenshot shows the configuration page for a new user in Cisco ACS. The form includes the following sections:

- General:**
 - Name:** user3
 - Status:** Enabled
 - Description:** (empty)
 - Identity Group:** All Groups
- Password Information:**
 - Password must:
 - Contain 4 - 32 characters
 - Password Type:** Internal Users
 - Password:** (masked with dots)
 - Confirm Password:** (masked with dots)
 - Change password on next login: (unchecked)
- Enable Password Information:**
 - Password must:
 - Contain 4 - 32 characters
 - Enable Password:** (empty)
 - Confirm Password:** (empty)
- User Information:**
 - There are no additional identity attributes defined for user records

At the bottom left, there is a legend: **⊙ = Pola wymagane**.

Agregue a un usuario para la autorización. En este ejemplo, es IKETEST. La contraseña necesita ser "Cisco" porque es el valor por defecto enviado por el 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

Después, cree un perfil de la autorización para los usuarios (los elementos de la directiva > la autorización y los permisos > los perfiles del acceso a la red > de la autorización > crean).

En este ejemplo, se llama POOL. En este ejemplo, el par AV del túnel dividido (como prefijo) se ingresa y Framed-IP-direccionamiento como IP Address que vaya a ser asignado al cliente conectado. La lista de todos los pares AV soportados se puede encontrar aquí:

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

General Common Tasks **RADIUS Attributes**

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
Framed-IP-Address	IPv4 Address	192.168.100.200
isco-sw-pair	String	isco:route-set=prefix:10.1.1.0/24

Dictionary Type:

RADIUS Attribute

Attribute Type

Attribute Value

= Pola wyłączone

Entonces, usted necesita girar el soporte del EAP-MD5 (para la autenticación) y de PAP/ASCII (para la autorización) en política de acceso. El valor por defecto se utiliza en este ejemplo (políticas de acceso > acceso de red predeterminada):

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

Cree una condición para en política de acceso y asigne el perfil de la autorización que fue creado. En este caso una condición para NDG: La ubicación en todas las ubicaciones se crea, así para toda la petición de las autorizaciones de RADIUS proporcionará el perfil de la autorización del POOL (las políticas de acceso > el acceso mantiene > acceso de red predeterminada):

General
 Name: Status:

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:
 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.

Usted debe poder probar en un router IOS si el usuario puede autenticar correctamente:

```
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"
```

[Configuración IOS FlexVPN](#)

Usted necesita crear la oferta IKEv2 y la directiva (usted no pudo tuvo que, referir a CSCtn59317). La directiva se crea solamente para uno de los IP Addresses (10.1.1.2) en este ejemplo.

```
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"
```

Entonces, cree un perfil IKEV2 y un perfil de ipsec que aten a la Virtual-plantilla.

Asegurese le están apagando HTTP URL el CERT, según lo aconsejado en la guía de configuración.

```
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"
```

En este ejemplo, se configura la autorización basó en el usuario IKETEST, que fue creado en la configuración de ACS.

Configuración de Windows

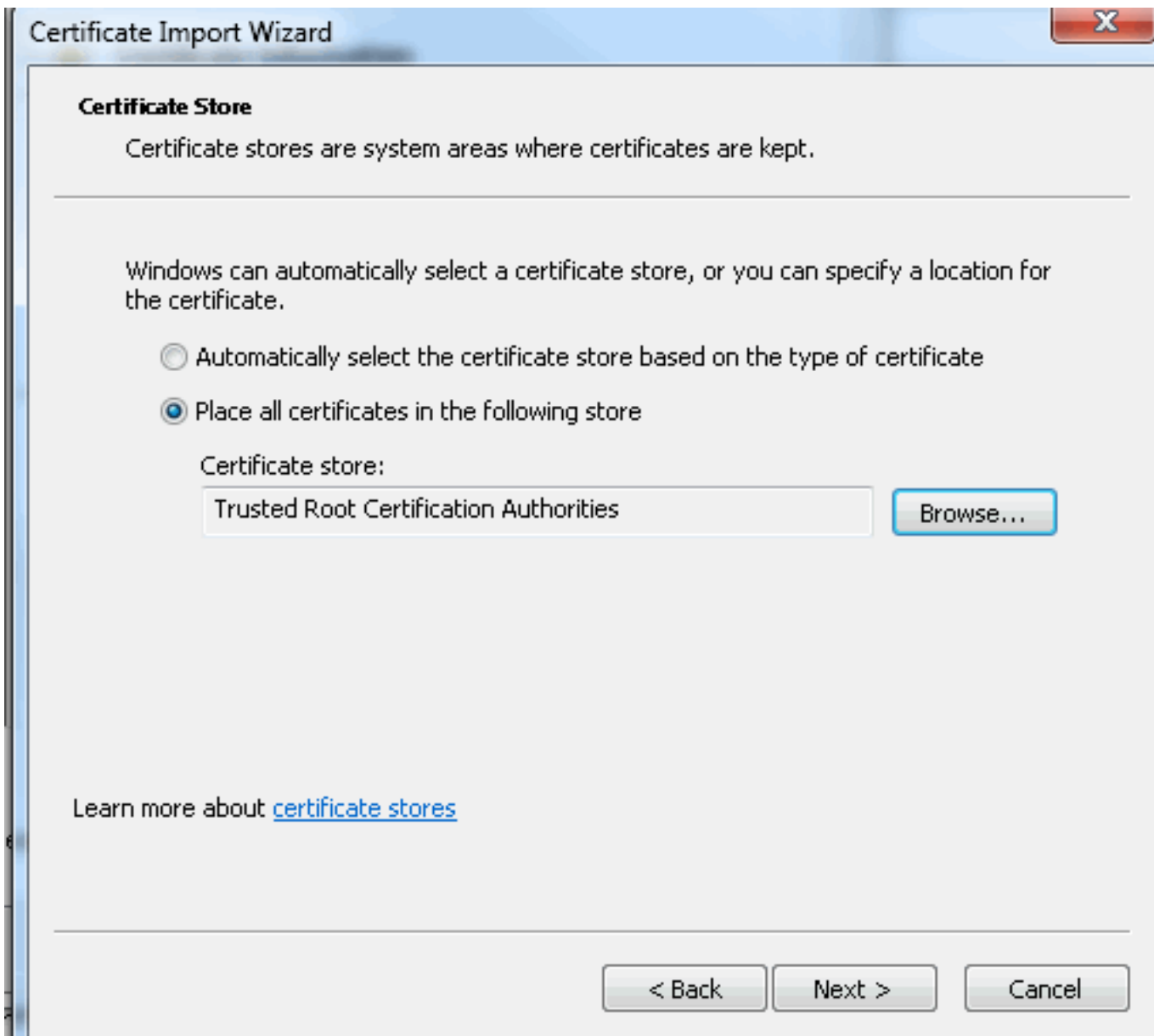
Importación de CA a las confianzas de Windows

Exporte el certificado de CA en el IOS (asegurese exportar el certificado de identidad y tomar solamente la primera parte):

```
R1(config)#crypto pki export CA-self pem terminal  
% CA certificate:  
-----BEGIN CERTIFICATE-----  
MIIB8zCCAbygAwIBAgIBATANBgkqhkiG9w0BAQUFADANMQswCQYDVQQDEwJDQTAe  
Fw0xMjExMjYxNzZmZmlaFw0xNTEyMjYxNzZmZmlaMA0xCzAJBgNVBAMTAkNBMIgf  
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvDR4lHOcrj42QfHpRuNu4EyFrLR8H  
TbPanXYV+GdCBmu53pDILE00ASEHByD6DYBx01EZuDsioLJ7t2MPTguB+YZe6V4O  
JbtayyxtZGmF7+eDqRegQHHC394adQQWl2ojgQiuTHERDTqDJR8i5gN2Ee+K0sr3  
+OjnHjUmXb/I6QIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQE  
AwIBhjAfBgNVHSMEGDAwBTH5Sdh69q4HAJulLQYLbYH0Nk9zzAdBgNVHQ4EFgQU  
x+UnYevauBwCbPpS0GC22B9DZPc8wDQYJKoZIhvcNAQEFBQADgYEADtBLiNXnl+LC  
PIgJ0nl/jH5p2IwVlzwBpbZc0sZ9mn54QaqrhmhbHnmqKQJl/20+JPE6p+4noICq  
VBrxoiX2KYQ10wmeScPpQ2XJ9vhGqtQ4Xcx3g20HhxxFDfp2XuW7hwU0W8dTcmZw  
4vodj47qEXKI6pGuzauw9MN1xhkNarc=  
-----END CERTIFICATE-----
```

Copie la pieza en medio COMIENZAN EL CERTIFICADO y el CERTIFICADO del EXTREMO y lo pegan a la libreta en Windows y lo salvan como archivo CA.crt.

Usted necesita instalarlo como en las autoridades de la Raíz confiable (el doble hace clic en el archivo > instala el certificado > el lugar todos los Certificados en el almacén > los Trusted Root Certification Authority siguientes):



[Configurar el perfil de AnyConnect XML](#)

En el cliente seguro \ el perfil de la movilidad de C:\ProgramData\Cisco\Cisco AnyConnect cree un archivo "whatever.xml" y pegue esto:

```
R1(config)#crypto pki export CA-self pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB8zCCABygAwIBAgIBATANBgkqhkiG9w0BAQUFADANMQswCQYDVQQDEwJDQTAe
Fw0xMjExMjYxNzZmZmZlaFw0xNTEyMjYxNzZmZmZlaMA0xCzAJBgNVBAMTAkNBMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvDR4lHOcrj42QfHpRuNu4EYFrLR8H
TbPanXYV+GdCBmu53pDILE00ASEHByD6DYBx01EZuDsio1J7t2MPTguB+YZe6V4O
JbtayxtZGmF7+eDqRegQHHC394adQQWl2ojgQiuTHERDTqDJR8i5gN2Ee+KOs3
+OjnHjUmXb/I6QIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQE
AwIBhjAfBgNVHSMEGDAWgBTH5Sdh69q4HAJulLQYLbYH0Nk9zzAdBgNVHQ4EFgQU
x+UnYevauBwCbP50GC22B9DZPc8wDQYJKoZIhvcNAQEFBQADgYEADtBLiNXnl+LC
PIgJ0nl/jH5p2IwV1zwbPbZcOsZ9mn54QaqrhmhbHnmqKQJl/20+JPE6p+4noICq
VBrxoiX2KYQ10wmeScPpQ2XJ9vhGqtQ4Xcx3g20HhxxFDfp2XuW7hwU0W8dTCmZw
4vodj47qEXKI6pGuzauw9MN1xhkNarc=
-----END CERTIFICATE-----
```

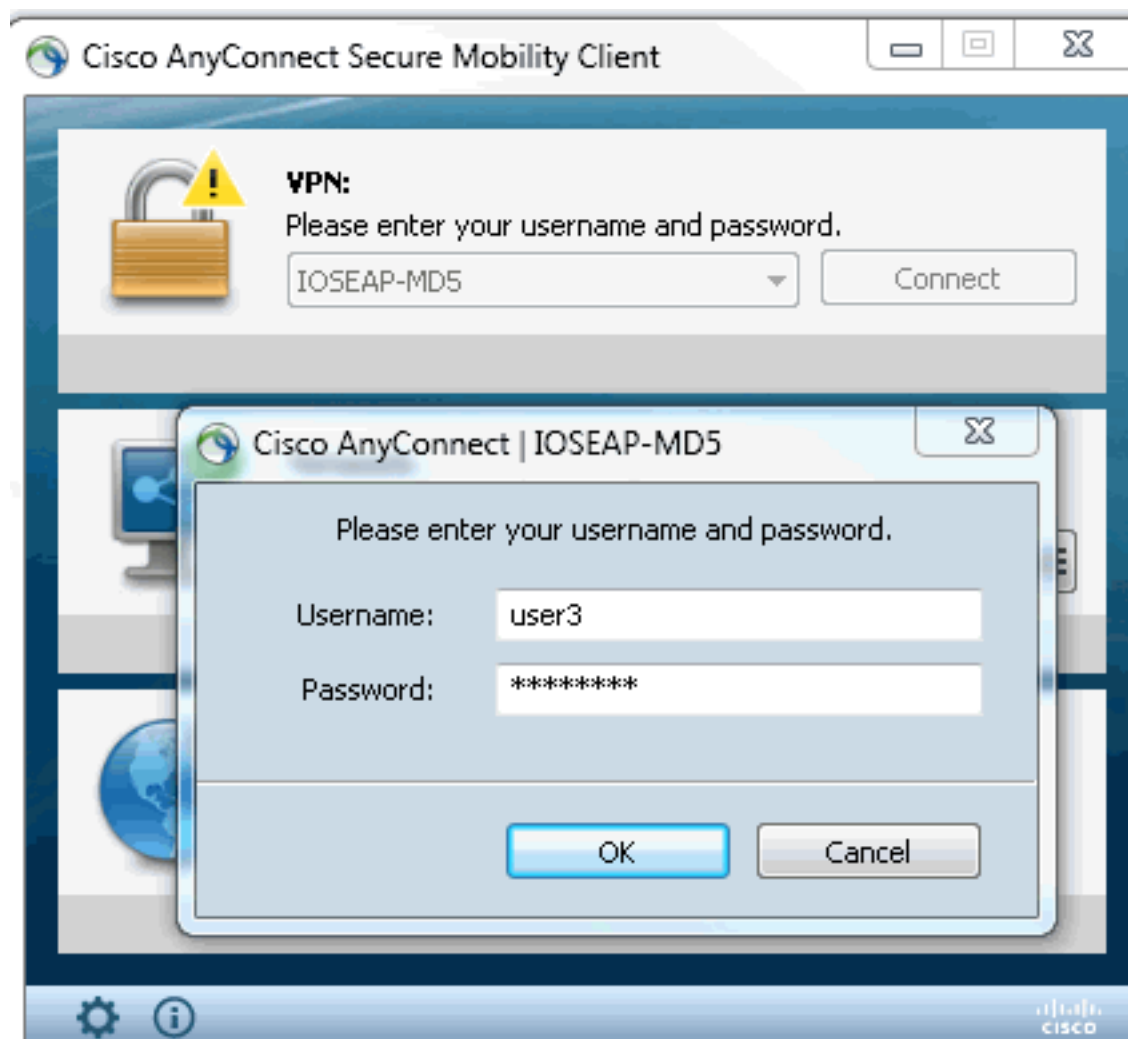
Asegurese que la entrada de 10.1.1.2 es exactamente lo mismo que CN=10.1.1.2 que fue

ingresado para el certificado de identidad.

Pruebas

En este escenario SSL EL VPN no se utiliza, así que asegúrese al servidor HTTP se inhabilita en IOS (ningún ip http servidor). Si no, usted recibe un mensaje de error en AnyConnect que estado, "utiliza a un navegador para acceder".

Al conectar en AnyConnect, usted debe ser indicado para una contraseña. En este ejemplo, es User3 que fue creado



Después de ese, el usuario está conectado.

Verificación

Router IOS

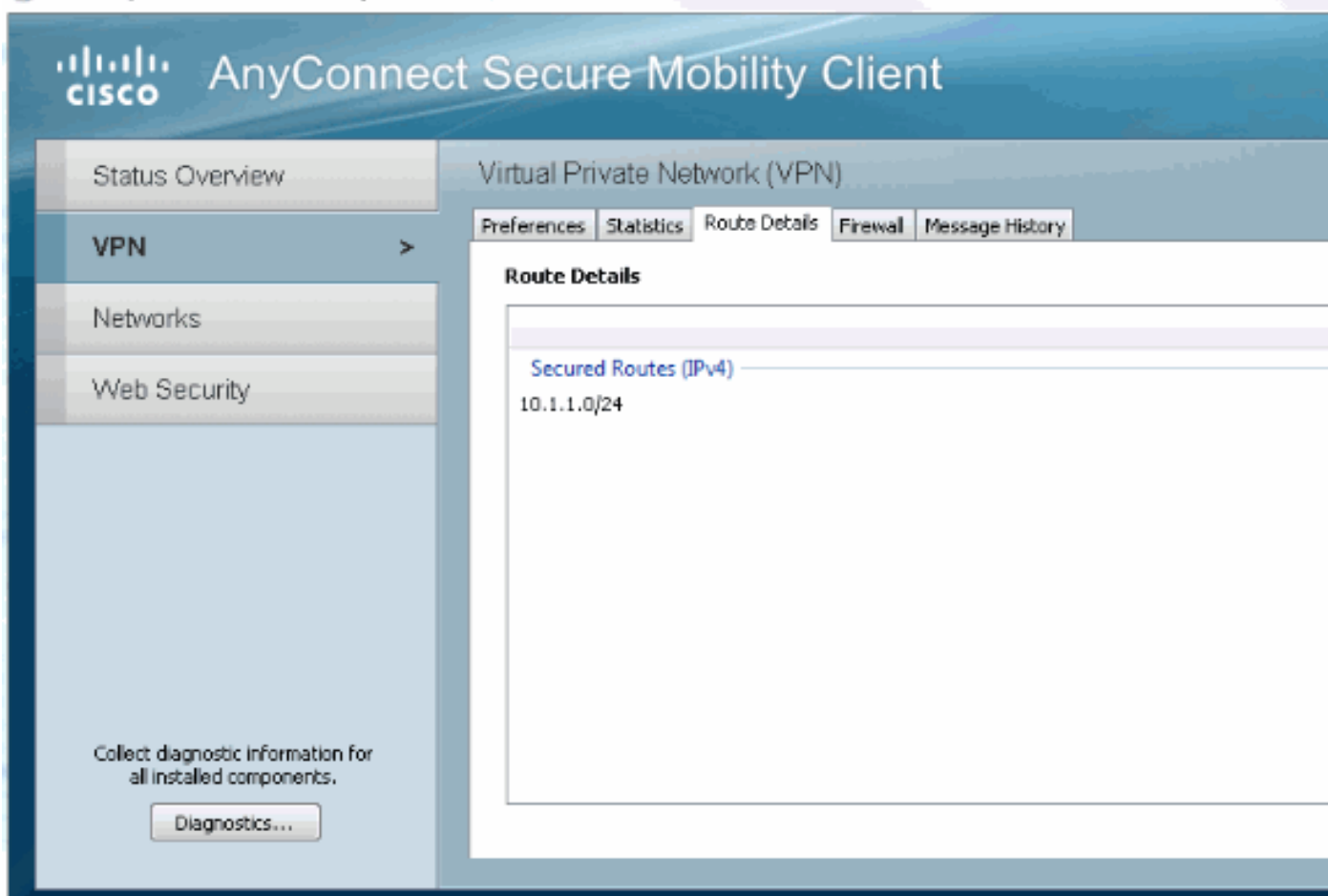
```
R1#show ip inter brief | i Virtual
Virtual-Access1  10.1.1.2  YES unset  up  up
Virtual-Templatel 10.1.1.2  YES unset  up  down
R1# show ip route 192.168.100.200
Routing entry for 192.168.100.200/32
  Known via "static", distance 1, metric 0 (connected)
```

```
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
```

Usted puede realizar un debug (debug crypto ikev2).

Windows:

En las opciones avanzadas de AnyConnect en el VPN usted puede marcar los detalles de la ruta para ver las redes del Túnel dividido:



Advertencias conocidas y problemas

- Recuerde al tener SHA1 en el hash de la firma y en la directiva de la integridad en IKEv2 (refiera al Id. de bug Cisco [CSCtn59317](#) (clientes registrados solamente)).
- El CN en el certificado de identidad IOS tiene que ser nombre de host igual en el perfil ACS XML.
- Si usted quiere utilizar los pares AV del radio pasajeros durante la autenticación y no la autorización del uso del grupo en absoluto, usted puede utilizar esto en el perfil IKEv2:

```
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)
  Phasel_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

```

- La autorización está utilizando siempre la contraseña “Cisco” para la autorización del grupo/de los usuarios. Esto pudo ser confuso mientras que usaba

```

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)
  Phasel_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

```

porque intentará autorizar usando el usuario pasajero en AnyConnect como el usuario y contraseña “Cisco”, que no es probablemente la contraseña para el usuario.

- En caso de cualquier problema éstas son las salidas que usted puede analizar y proporcionar al TAC de Cisco: debug crypto ikev2 debug crypto ikev2 interno Salidas del DARDO
- Si no usando SSL VPN recuerde inhabilitar ip http el servidor (ningún ip http servidor). Si no, AnyConnect intentará conectar con el servidor HTTP y recibir el resultado, “utiliza a un navegador para acceder”.

[Criptografía de la última generación](#)

La configuración antedicha se proporciona para que la referencia muestre una configuración en

funcionamiento minimalistic.

Cisco recomienda usando la criptografía de la última generación (NGC) en lo posible.

Las recomendaciones actuales para la migración se pueden encontrar aquí:

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

Al elegir la configuración NGC, asegúrese que software de cliente y soporte del hardware del headend él. Recomiendan la generación 2 ISR y los 1000 Router ASR como headends debido a su soporte del hardware para NGC.

En el lado de AnyConnect, a partir de la versión de AnyConnect 3.1, se soporta la habitación del algorithm de la habitación B NSA.

[Información Relacionada](#)

- [Sitio-sitio VPN de Cisco ASA IKEv2 PKI](#)
- [Debugs IKEv2 Site2-Site en el IOS](#)
- [FlexVPN/IKEv2: Accesorio de Windows 7 - Cliente: Headend IOS: Parte I - Autenticación certificada](#)
- [FlexVPN y guía de configuración de la versión 2 del intercambio de claves de Internet, Cisco IOS Release 15.2M&T](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)