Implementación de FlexVPN: Acceso remoto AnyConnect IKEv2 con EAP-MD5

Contenido

Introducción

Este documento proporciona una configuración de ejemplo de cómo configurar el acceso remoto en IOS usando el kit de herramientas FlexVPN.

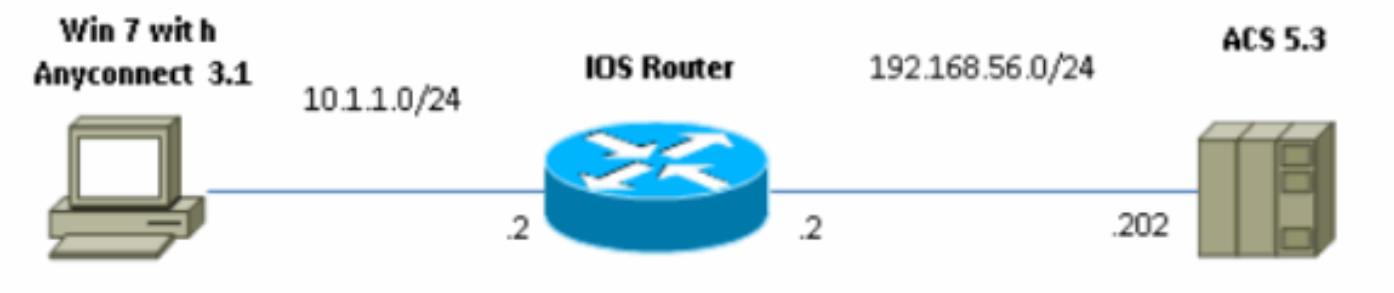
La VPN de acceso remoto permite a los clientes finales que utilizan varios sistemas operativos conectarse de forma segura a sus redes corporativas o domésticas a través de medios no seguros como Internet. En el escenario presentado, se está terminando el túnel VPN en un router Cisco IOS mediante el protocolo IKEv2.

Este documento muestra cómo autenticar y autorizar a los usuarios mediante Access Control Server (ACS) a través del método EAP-MD5.

Prerequisites

Diagrama de la red

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



Requirements

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

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Background

En IKEv1 XAUTH se utiliza en la fase 1.5, puede realizar la autenticación de usuarios localmente en un router IOS y de forma remota mediante RADIUS/TACACS+. IKEv2 ya no admite XAUTH y la fase 1.5. Contiene soporte EAP integrado, que se realiza en la fase IKE_AUTH. La mayor ventaja de esto es en el diseño de IKEv2 y EAP es un estándar bien conocido.

EAP admite dos modos:

- Tunelización: EAP-TLS, EAP/PSK, EAP-PEAP, etc.
- Sin tunelización: EAP-MSCHAPv2, EAP-GTC, EAP-MD5, etc.

En este ejemplo, se utiliza EAP-MD5 en modo no tunelizado porque es el método de autenticación externa EAP admitido actualmente en ACS 5.3.

EAP sólo se puede utilizar para el iniciador de autenticación (cliente) al respondedor (IOS en este caso).

Configuración inicial de IOS

IOS - CA

En primer lugar, debe crear la autoridad de certificación (CA) y un certificado de identidad para el router IOS. El cliente verificará la identidad del router basándose en ese certificado.

La configuración de CA en IOS es similar a:

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

Debe recordar el uso de clave extendida (Server-Auth se necesita para EAP, para RSA-SIG también necesita Client-Auth).

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

IOS - Certificado de identidad

A continuación, active el protocolo simple de inscripción de certificados (SCEP) para el certificado y configure el punto de confianza.

```
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
```

Luego, autentique e inscríbase 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 no desea tener mensajes de solicitud en AnyConnect, recuerde que puede ser igual a nombre de host/direcciones IP configuradas 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 dirección IP del servidor en el perfil xml de AnyConnect.

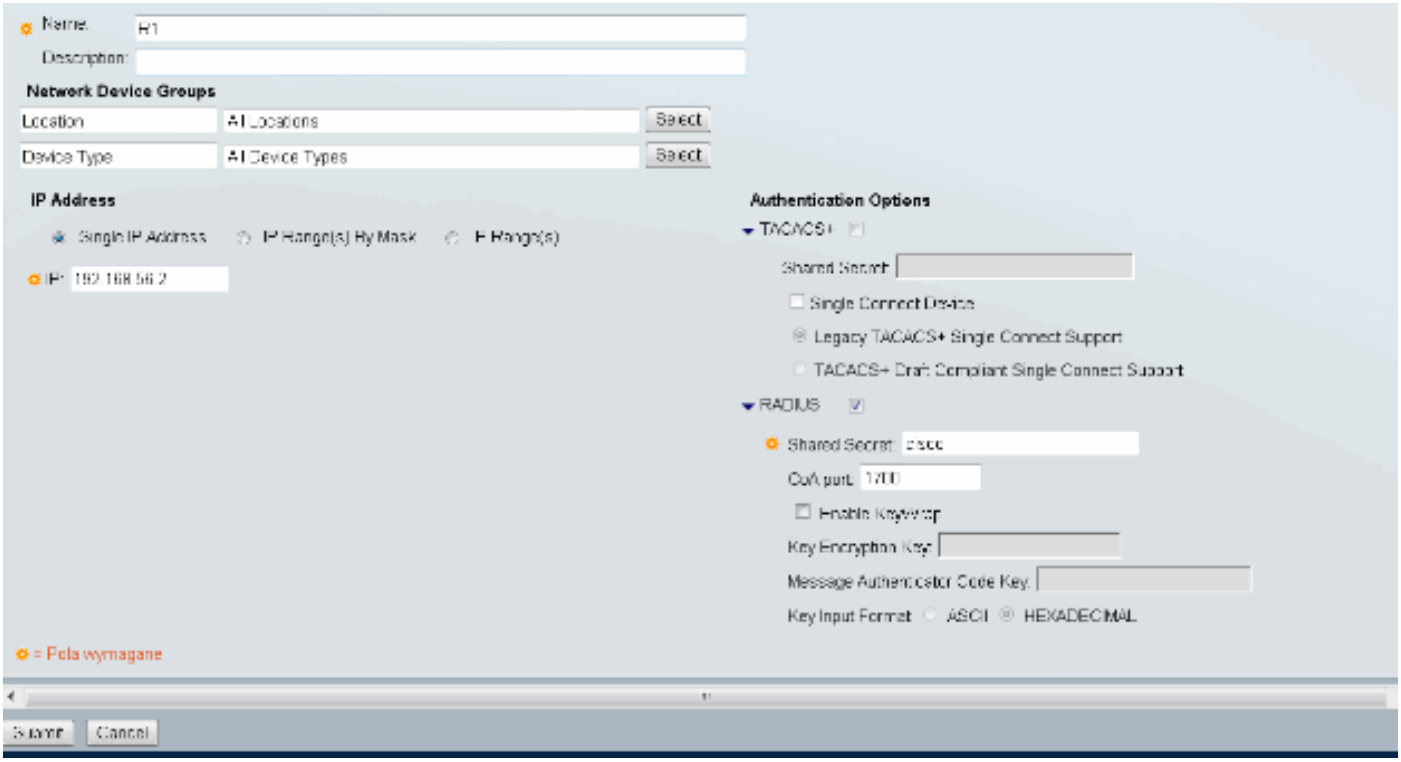
IOS - configuración AAA y Radius

Debe configurar la autenticación y autorización de RADIUS y 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
```

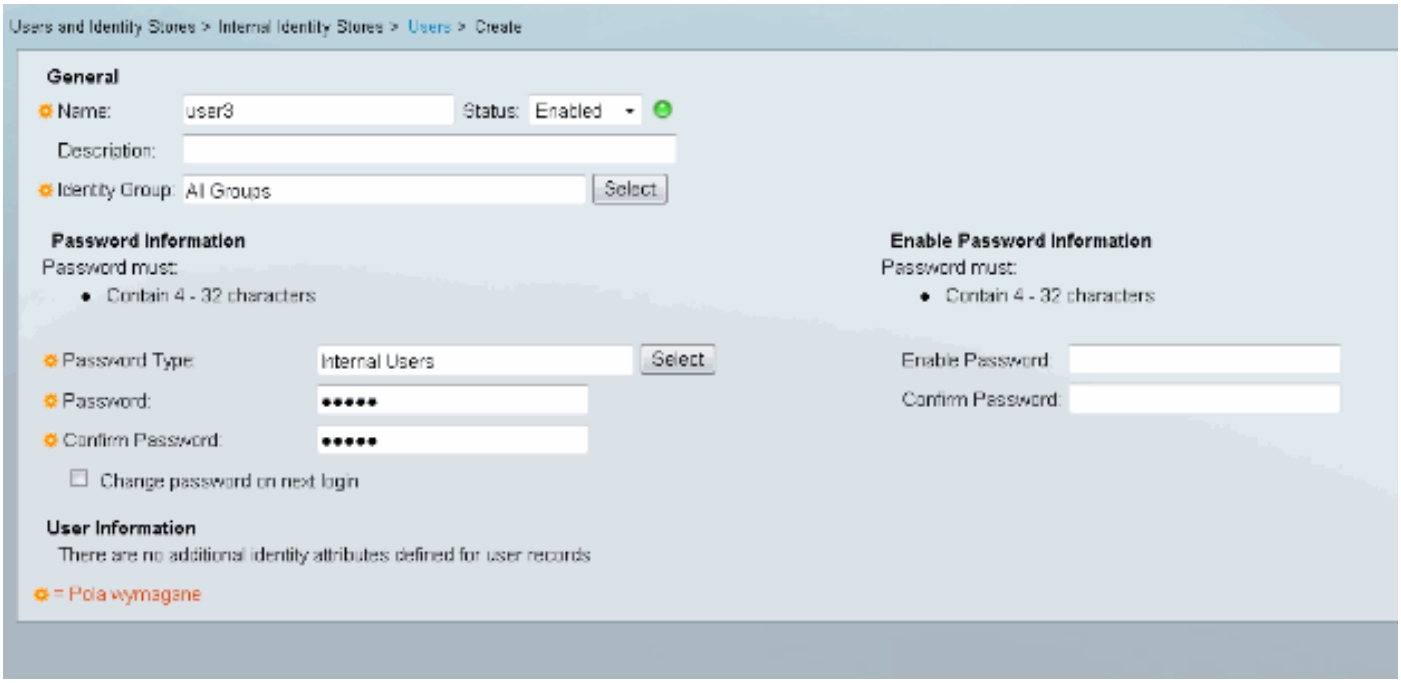
configuración inicial de ACS

Primero, agregue el nuevo dispositivo de red en ACS (Recursos de red > Dispositivos de red y Clientes AAA > Crear):

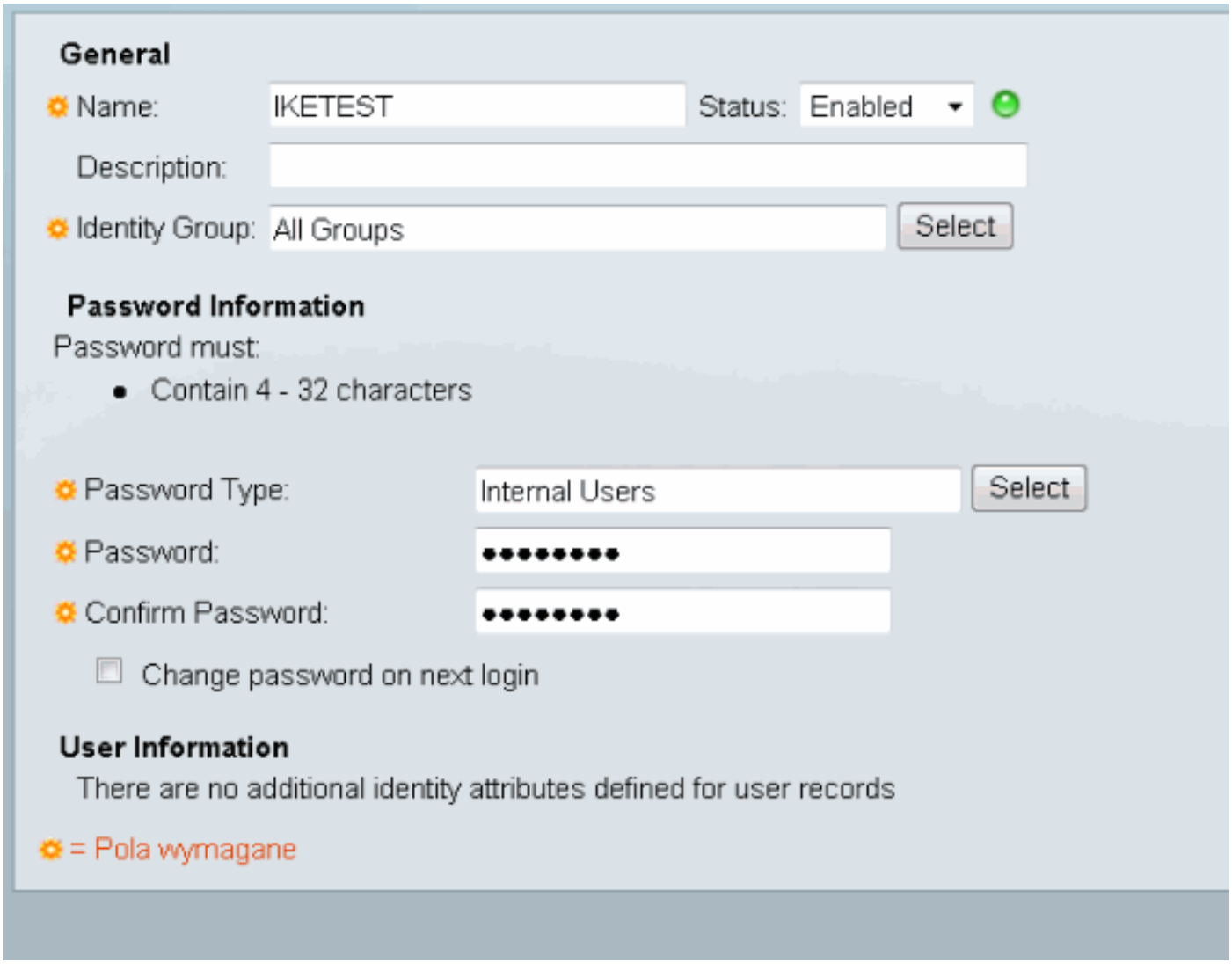


Agregue un usuario (Usuarios y almacenes de identidad > Almacenes de identidad internos >

Usuarios > Crear):

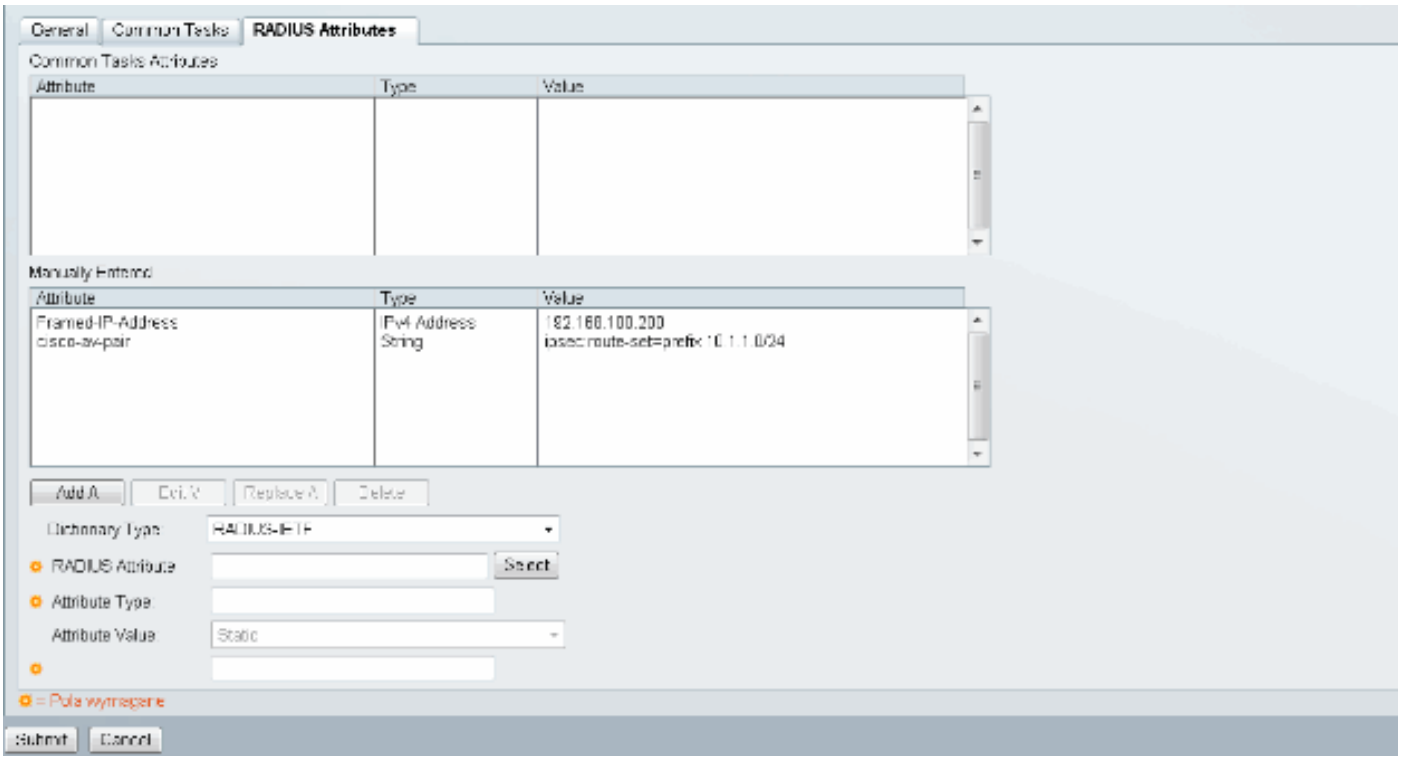


Agregue un usuario para la autorización. En este ejemplo, es IKETEST. La contraseña debe ser "cisco" porque es el valor predeterminado enviado por IOS.

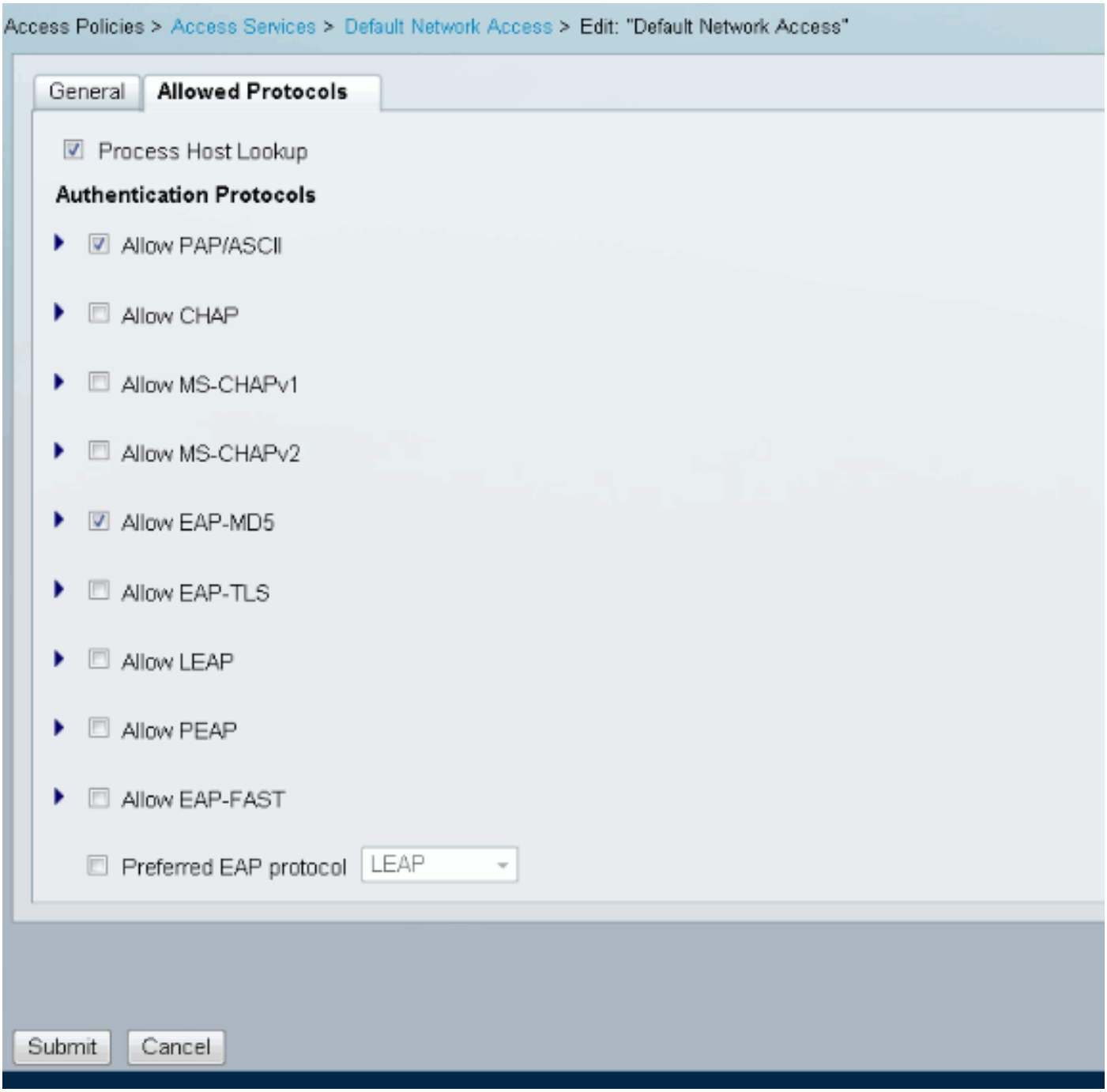


A continuación, cree un perfil de autorización para los usuarios (elementos de política > Autorización y permisos > Acceso a red > Perfiles de autorización > Crear).

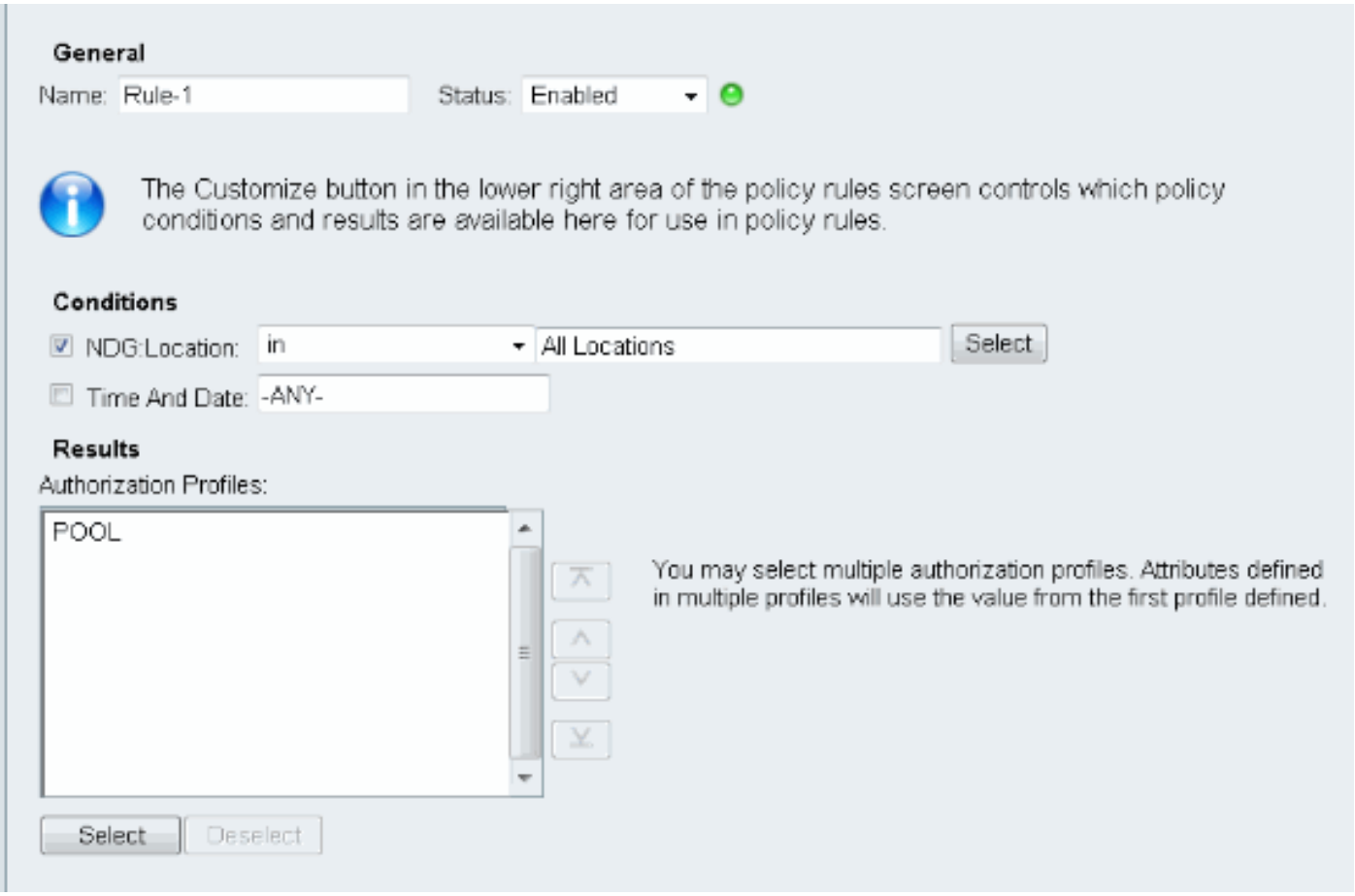
En este ejemplo, se denomina POOL. En este ejemplo, se ingresa el par AV de túnel dividido (como prefijo) y la dirección IP entramada como dirección IP que se va a asignar al cliente conectado. La lista de todos los pares AV admitidos se puede encontrar aquí: http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html



A continuación, debe activar el soporte de EAP-MD5 (para autenticación) y PAP/ASCII (para autorización) en la política de acceso. El valor predeterminado se utiliza en este ejemplo (Políticas de acceso > Acceso de red predeterminado):



Cree una condición para en Access Policy y asigne el perfil de autorización que se creó. En este caso, se crea una condición para NDG:Location in All Locations (Ubicación en todas las ubicaciones), por lo tanto, para todas las solicitudes de autorización de RADIUS se proporcionará el perfil de autorización de POOL (Políticas de acceso > Servicios de acceso > Acceso de red predeterminado):



Debería poder probar en un router IOS si el usuario puede autenticarse 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 de FlexVPN de IOS

Debe crear una propuesta y una política IKEv2 (es posible que no tenga que hacerlo, consulte CSCtn59317). La política se crea sólo para una de las direcciones IP (10.1.1.2) en este ejemplo.

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

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

A continuación, cree un perfil IKEV2 y un perfil IPsec que se enlazarán a Virtual-Template.

Asegúrese de desactivar el certificado http-url, como se indica en la guía de configuración.

```
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
```

En este ejemplo, la autorización se configura en función del usuario IKETEST, que se creó en la configuración ACS.

configuración de Windows

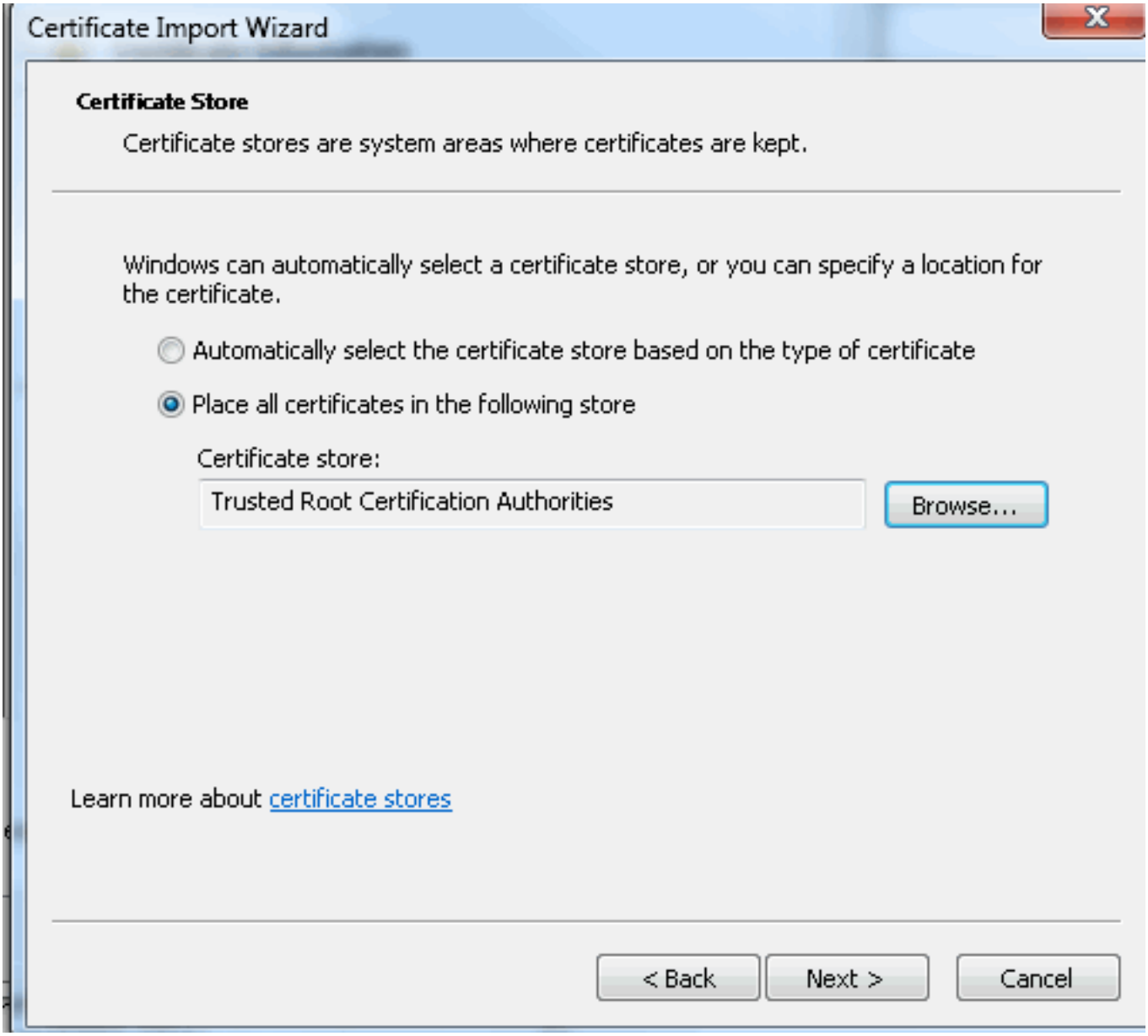
Importación de CA a confianzas de Windows

Exportar el certificado de CA en IOS (asegúrese de exportar el certificado de identidad y tomar sólo la primera parte):

```
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-----
```

Copie la pieza entre CERTIFICADO DE INICIO y CERTIFICADO FINAL y péguela en el Bloc de notas en Windows y guárdela como archivo CA.crt.

Debe instalarlo como en Autoridades raíz de confianza (haga doble clic en Archivo > Instalar certificado > Colocar todos los certificados en el siguiente almacén > Autoridades de certificación raíz de confianza):



Configuración del perfil XML de AnyConnect

En C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile create a file "any.xml" y pegue esto:

```
<?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>
```

Asegúrese de que la entrada 10.1.1.2 es exactamente la misma que CN=10.1.1.2 que se introdujo para el certificado de identidad.

Pruebas

En este escenario, no se utiliza SSL VPN, por lo que asegúrese de que el servidor HTTP esté inhabilitado en IOS (sin servidor ip http). De lo contrario, recibirá un mensaje de error en AnyConnect que indica "Utilice un explorador para obtener acceso".

Al conectarse a AnyConnect, se le solicitará una contraseña. En este ejemplo, se creó User3

Después, el usuario se conecta.

Verificación

Router IOS

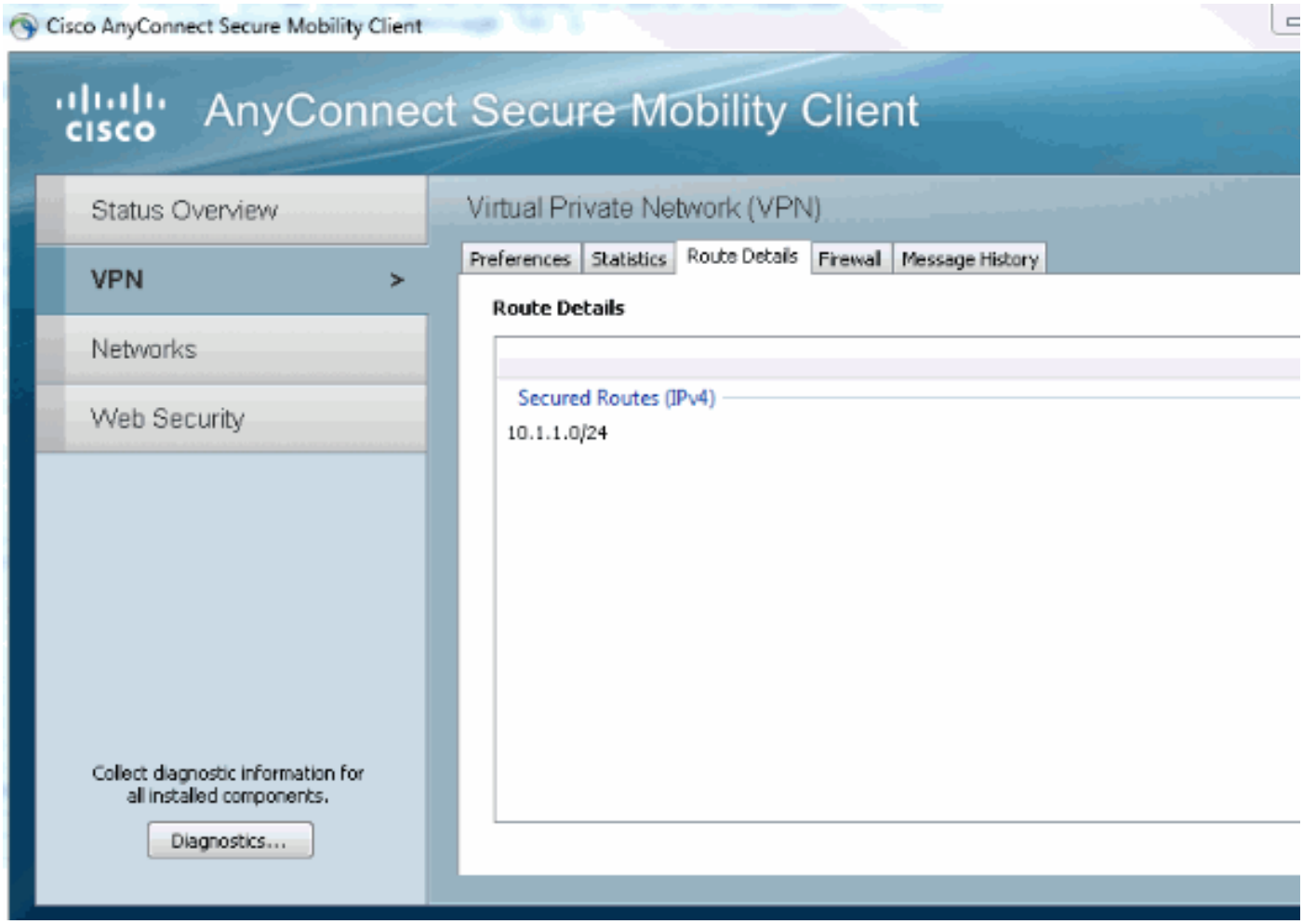
```
R1#show ip inter brief | i Virtual
Virtual-Access1    10.1.1.2  YES unset  up  up
Virtual-Template1  10.1.1.2  YES unset  up down
R1# show ip route 192.168.100.200
Routing entry for 192.168.100.200/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly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

Puede realizar un debug (debug crypto ikev2).

Windows:

En las opciones avanzadas de AnyConnect en VPN, puede comprobar los detalles de la ruta para ver las redes de tunelización divididas:



Advertencias y problemas conocidos

- Recuerde que cuando SHA1 esté en el hash de firma y en la política de integridad en IKEv2 (consulte Cisco bug ID CSCtn59317 (sólo clientes registrados)).
- El CN en el certificado de identidad del IOS debe ser igual nombre de host en el perfil XML de ACS.

- Si desea utilizar pares AV de RADIUS pasados durante la autenticación y no utilizar la autorización del grupo en absoluto, puede utilizar esto en el perfil IKEv2:
  `aaa authorization user eap cached`
- La autorización siempre utiliza la contraseña "cisco" para la autorización de grupo/usuarios. Esto podría ser confuso mientras se utiliza
  `aaa authorization user eap list SERV (without any paramaters)`
  porque intentará autorizar el uso del usuario pasado en AnyConnect como usuario y contraseña "cisco", que probablemente no sea la contraseña del usuario.
- En caso de que surja algún problema, se trata de salidas que puede analizar y proporcionar al TAC de Cisco:debug crypto ikev2debug crypto ikev2 internalSalidas DART
- Si no utiliza SSL VPN, recuerde desactivar ip http server (sin ip http server). De lo contrario, AnyConnect intentará conectarse al servidor HTTP y recibirá el resultado: "Use un navegador para obtener acceso".

Criptografía de última generación

La configuración anterior se proporciona como referencia para mostrar una configuración de funcionamiento minimalista.

Cisco recomienda utilizar la criptografía de última generación (NGC) siempre que sea 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 de NGC, asegúrese de que tanto el software del cliente como el hardware de cabecera lo admitan. Los routers ISR de segunda generación y ASR 1000 se recomiendan como cabeceras debido a su soporte de hardware para NGC.

En el lado de AnyConnect, desde la versión AnyConnect 3.1, se admite el conjunto de algoritmos Suite B de la NSA.

Información Relacionada

- VPN de sitio PKI Cisco ASA IKEv2 PKI
- Depuraciones del Sitio 2 de IKEv2 en IOS
- FlexVPN / IKEv2: Cliente de compilación de Windows 7: Encabezado IOS: Parte I - Autenticación de certificado
- Guía de Configuración de FlexVPN e Internet Key Exchange Versión 2, Cisco IOS Release 15.2M&T
- Soporte Técnico y Documentación - Cisco Systems