FlexVPN-implementaties: AnyConnect IKEv2 externe toegang met EAP-MD5

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie van hoe u Remote Access op IOS kunt instellen met behulp van de FlexVPN-toolkit.

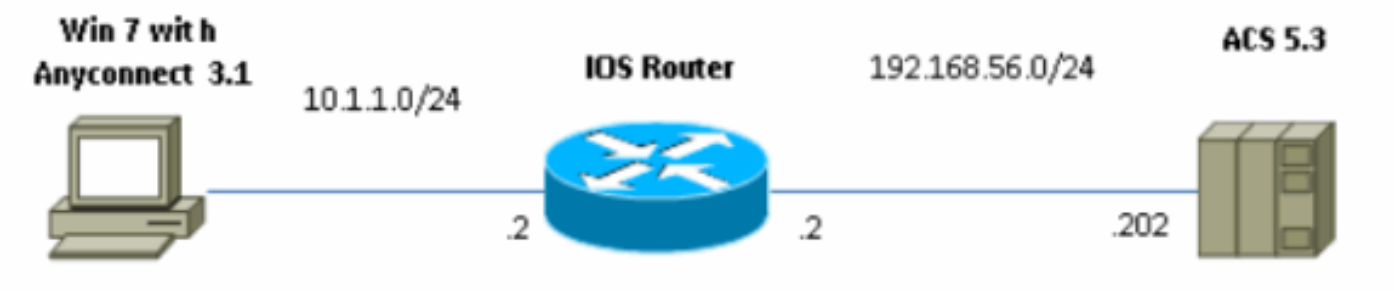
Op Remote Access VPN kunnen eindgebruikers met verschillende besturingssystemen op een veilige manier verbinding maken met hun bedrijfsnetwerk of thuisnetwerk via een niet-beveiligd medium, zoals internet. In het voorgelegde scenario wordt de tunnel van VPN op een Cisco IOS router beëindigd die IKEv2 protocol gebruikt.

Dit document toont aan hoe gebruikers met behulp van de EAP-MD5-methode kunnen worden geauthenticeerd en geautoriseerd.

Voorwaarden

Netwerkdiagram

Cisco IOS-router heeft twee interfaces - één voor ACS 5.3:



Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ACS 5.3 met pleister 6
- IOS-router met 15.2(4)M software
- Windows 7 PC met AnyConnect 3.1.01065

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrond

In IKEv1 XAUTH wordt gebruikt in fase 1.5, kunt u verificatie van gebruikers lokaal uitvoeren op een IOS-router en extern RADIUS/TACACS+ gebruiken. IKEv2 ondersteunt XAUTH en fase 1.5 niet langer. Het bevat ingebouwde EAP-ondersteuning, die wordt gedaan in fase IKE_AUTH. Het grootste voordeel hiervan is dat het IKEv2-ontwerp en EAP een bekende norm is.

EAP ondersteunt twee modi:

- Tunneling—EAP-TLS, EAP/PSK, EAP-PEAP enz.
- Niet-tunneling—EAP-MSCHAPv2, EAP-GTC, EAP-MD5 enz.

In dit voorbeeld wordt EAP-MD5 in een niet-tunneling-modus gebruikt omdat het een MAP-methode voor externe verificatie is die momenteel in ACS 5.3 wordt ondersteund.

EAP kan alleen worden gebruikt voor authenticatie initiator (client) om te reageren (IOS in dit geval).

IOS-initiële configuratie

IOS - CA

Eerst moet u certificaatinstantie (CA) creëren en een identiteitsbewijs voor de IOS-router maken. De klant zal de identiteit van de router op basis van dat Certificaat verifiëren.

De configuratie van CA op IOS ziet er zo uit:

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

U moet denken aan Extended Key Use (Server-Auth nodig voor EAP, voor RSA-SIG hebt u ook client-Auth nodig).

CA inschakelen met de opdracht **no shutdown** in crypto pki server CA.

IOS - identiteitsbewijs

Stel vervolgens Simple certificaatinschrijving Protocol (SCEP) in voor certificaat en stel vertrouwen in.

```
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
```

Verifieer en registreer het certificaat vervolgens:

```
(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
```

Als u geen vroege berichten in AnyConnect wilt hebben, vergeet dan dat de hostname/IP-adressen in het AnyConnect-profiel gelijk kunnen zijn.

In dit voorbeeld wordt cn=10.1.1.2. Daarom wordt in AnyConnect 10.1.1.2 het IP-adres van de server in het AnyConnect xml-profiel ingevoerd.

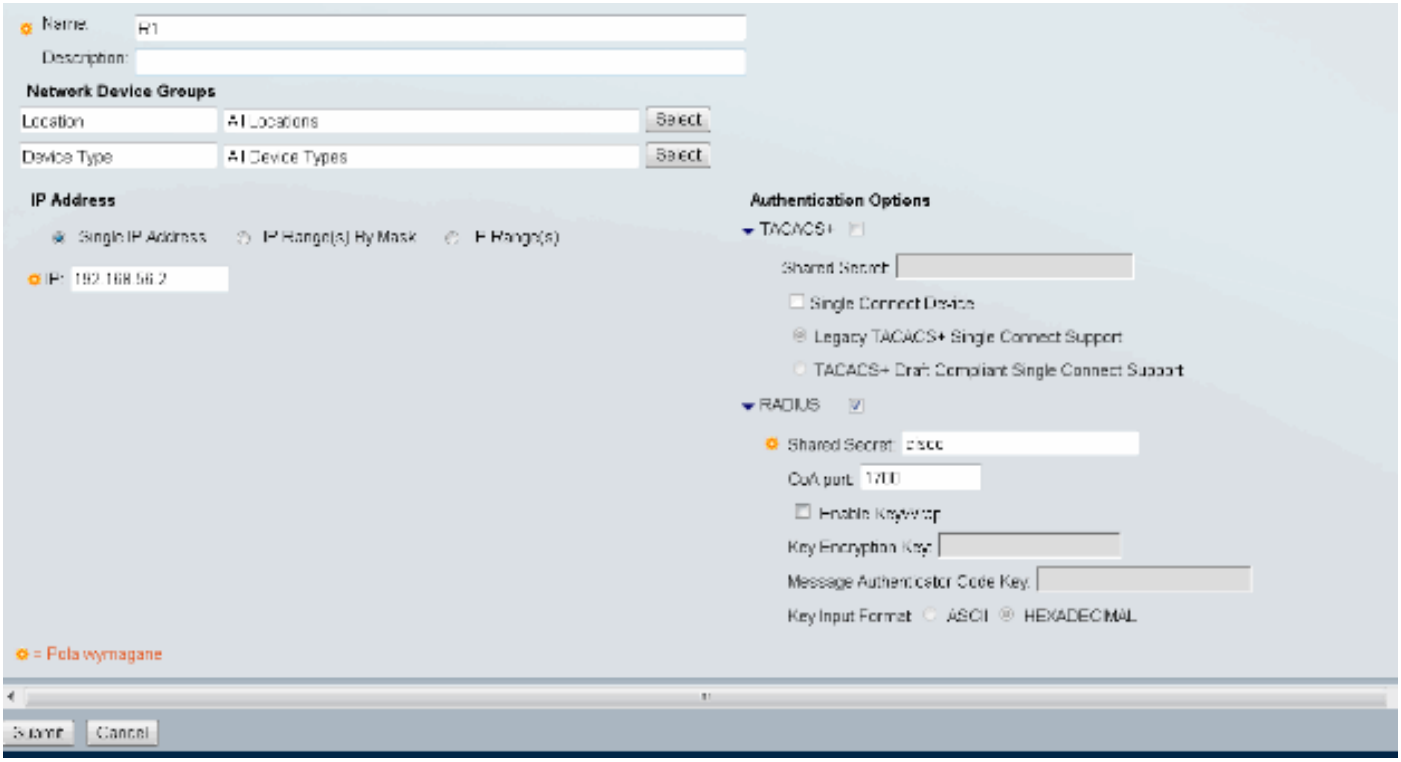
IOS - configuratie van AAA en RADIUS

U dient Radius en AAA-verificatie en -autorisatie te configureren:

```
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
```

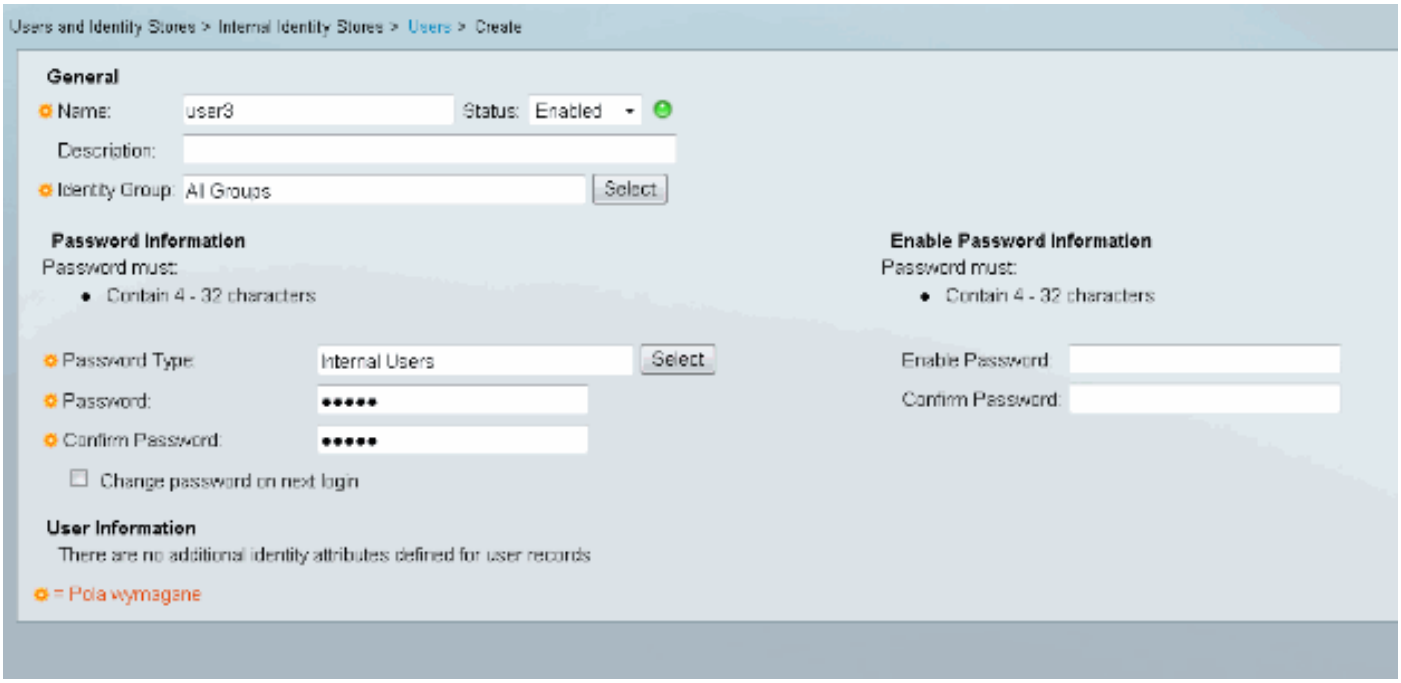
ACS Eerste configuratie

Voeg eerst het nieuwe netwerkapparaat toe in ACS (Netwerkbronnen > Netwerkapparaten en AAA-clients > Maken):

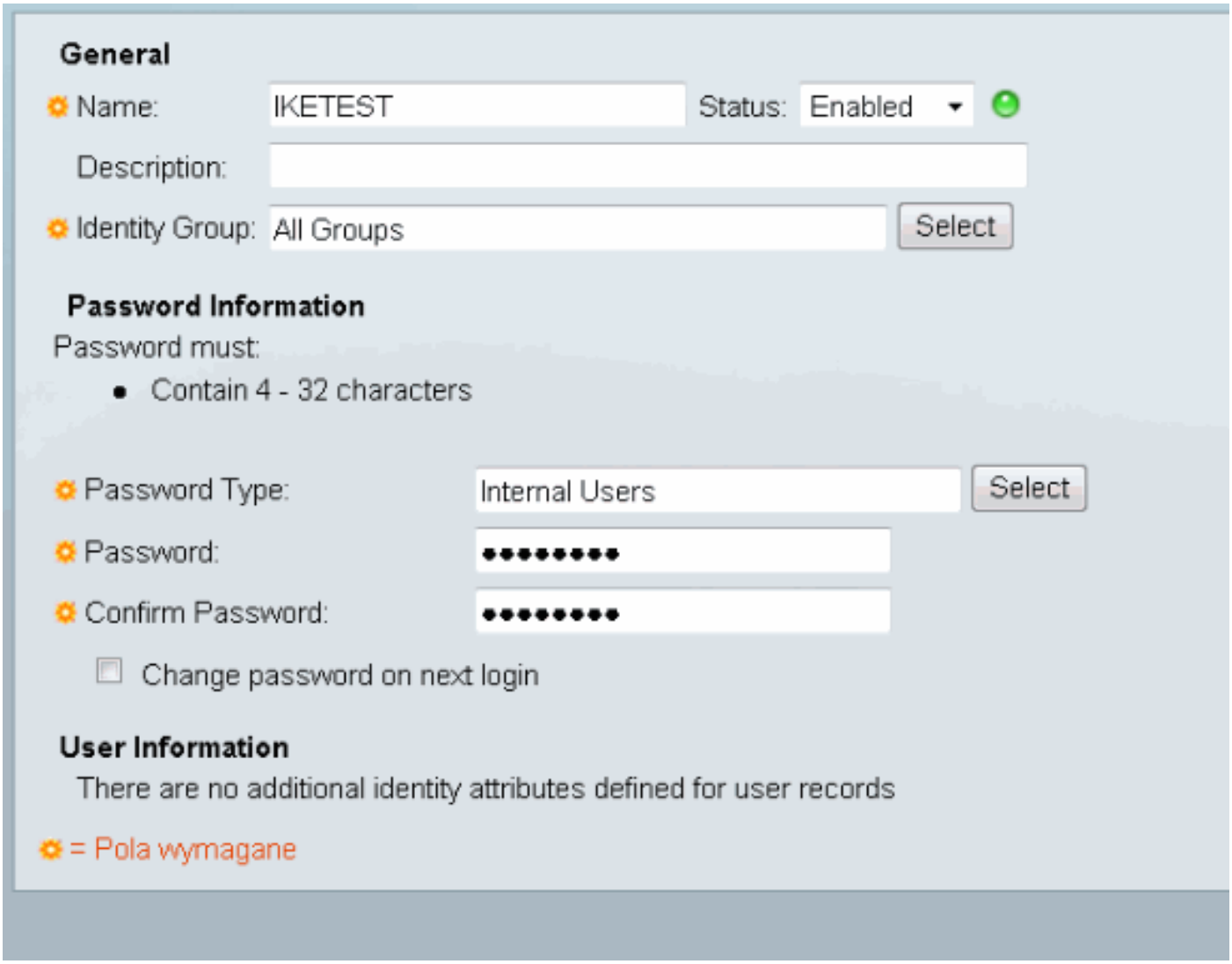


Voeg een gebruiker toe (gebruikers en identiteitsopslag > Interne identiteitsopslag > Gebruikers >

Maken):

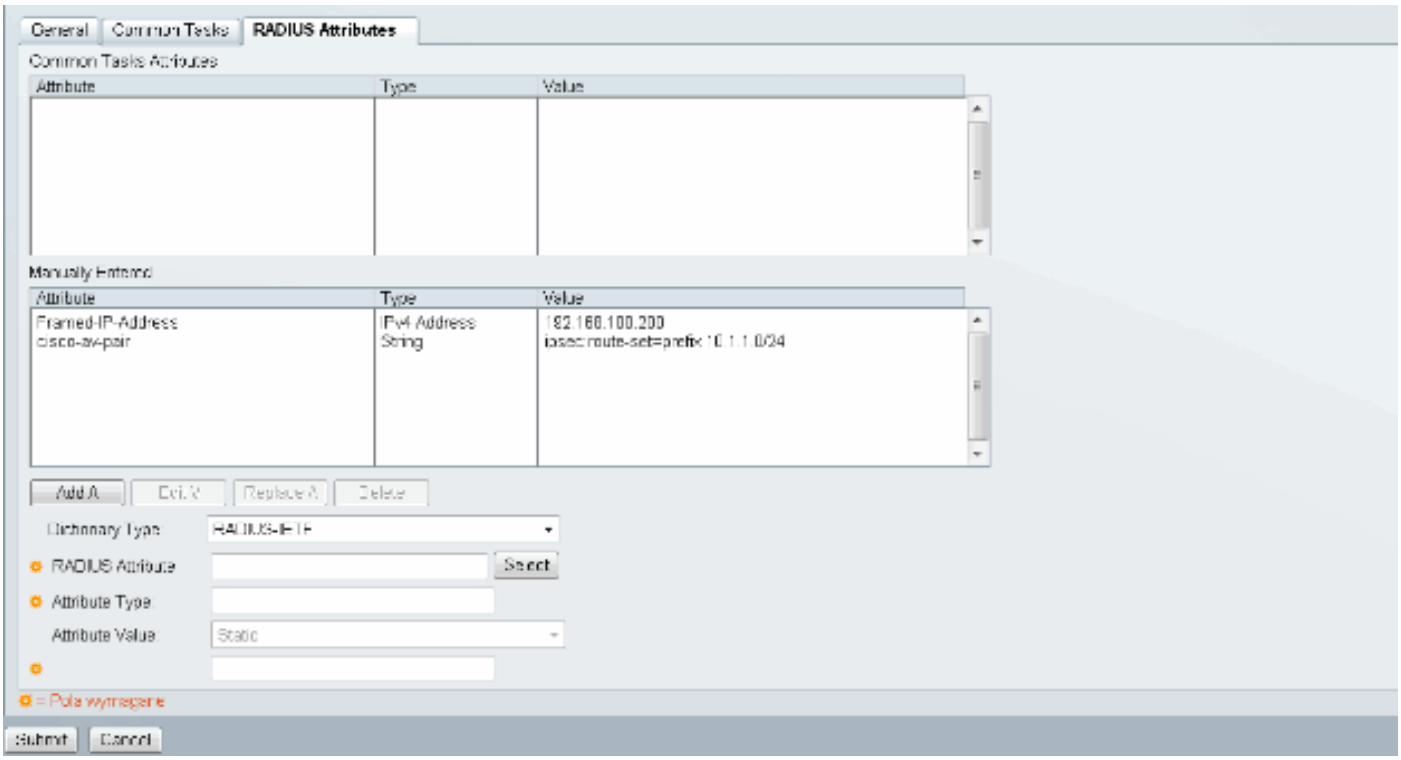


Voeg een gebruiker toe voor autorisatie. In dit voorbeeld is het IKETEST. Het wachtwoord moet "cisco" zijn omdat het de standaard is die door IOS wordt verzonden.

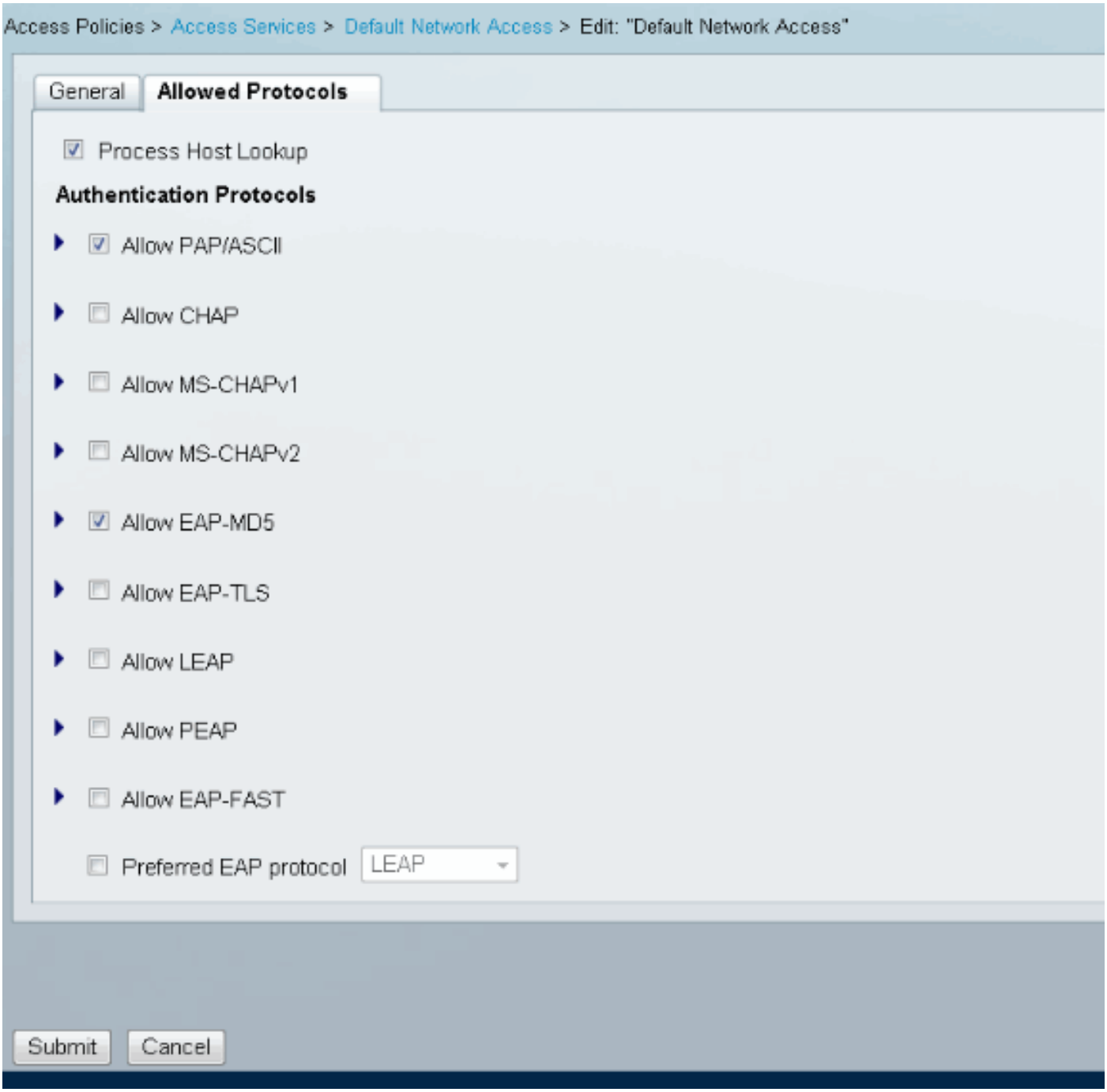


Creëer vervolgens een autorisatieprofiel voor de gebruikers (Beleidselementen > Vergunningen en toegangsrechten > Netwerktoegang > Verificatieprofielen > Maken).

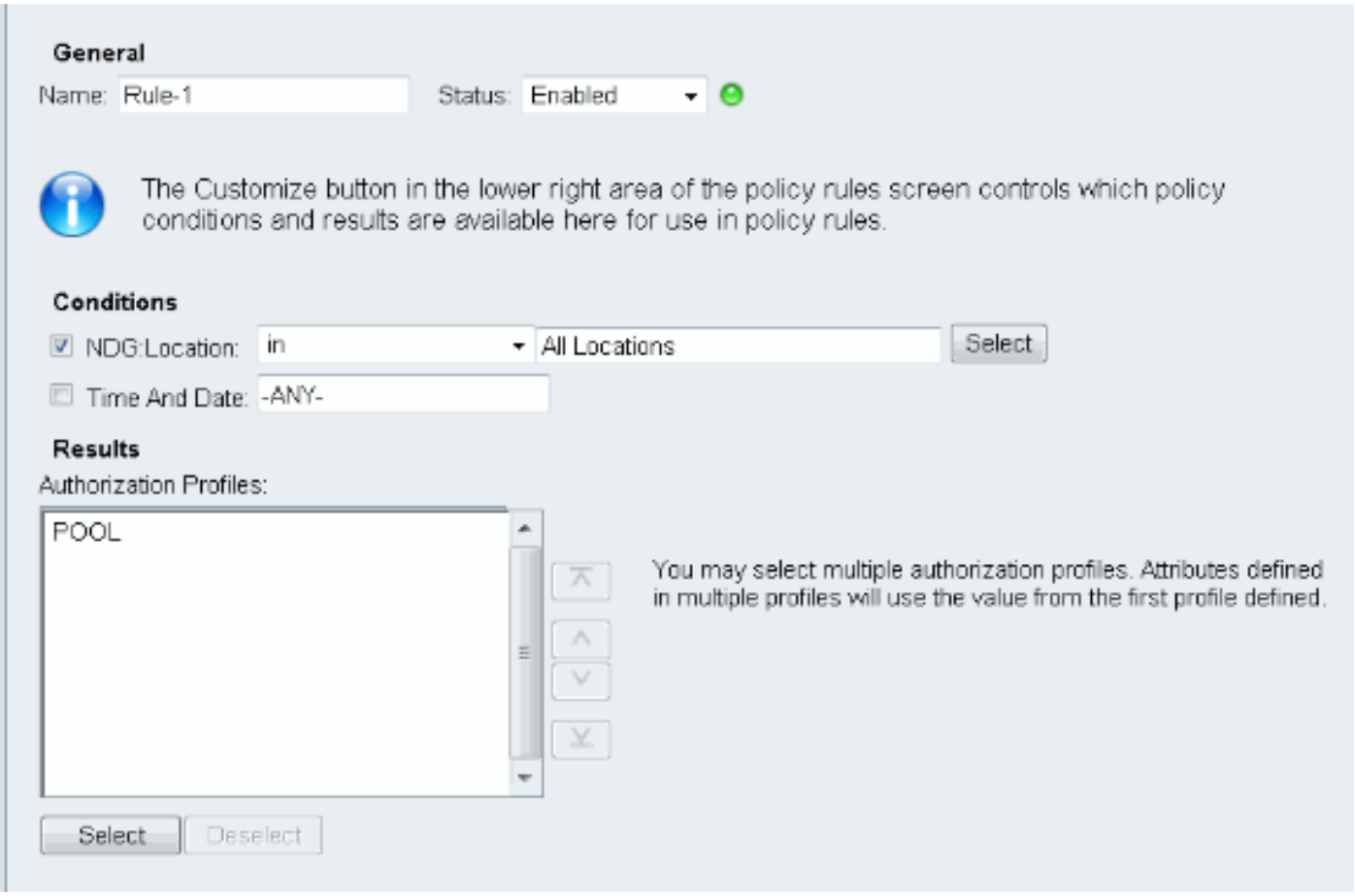
In dit voorbeeld heet het POOL. In dit voorbeeld wordt het paar Split-Tunnel AV (als voorvoegsel) ingevoerd en framed-IP-Address als IP-adres dat aan de verbonden client zal worden toegewezen. De lijst met alle ondersteunde AV-paren is hier te vinden: http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html



Vervolgens moet u de ondersteuning van EAP-MD5 (voor authenticatie) en PAP/ASCII (voor autorisatie) in het toegangsbeleid inschakelen. De standaardinstelling wordt in dit voorbeeld gebruikt (Toegangsbeleid > Standaardnetwerktoegang):



Maak een voorwaarde voor in het toegangsbeleid en verdeel het autorisatieprofiel dat is gemaakt. In dit geval wordt een voorwaarde voor NDG:Locatie in alle locaties gecreëerd, zodat in het geval van een aanvraag voor radiofrequenties een POOL-autorisatieprofiel beschikbaar is (Toegangsbeleid > Toegangsservices > Standaardnetwerktoegang):



U zou op een IOS router moeten kunnen testen als de gebruiker echt kan authenticeren:

```
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-configuratie

U moet IKEv2-voorstel en -beleid creëren (u hoeft dit misschien niet te doen, raadpleeg CSCtn59317). Het beleid wordt slechts voor één van de IP adressen (10.1.1.2) in dit voorbeeld gecreëerd.

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

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

Maak vervolgens een IKEV2-profiel en IPsec-profiel dat zich aan Virtual-sjabloon zal binden.

Zorg ervoor dat u de http-url cert uitschakelt, zoals geadviseerd in de configuratie gids.

```
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 dit voorbeeld wordt de vergunning ingesteld op basis van de door de gebruiker IKETEST gecreëerde IKETEST in de ACS-configuratie.

Windows-configuratie

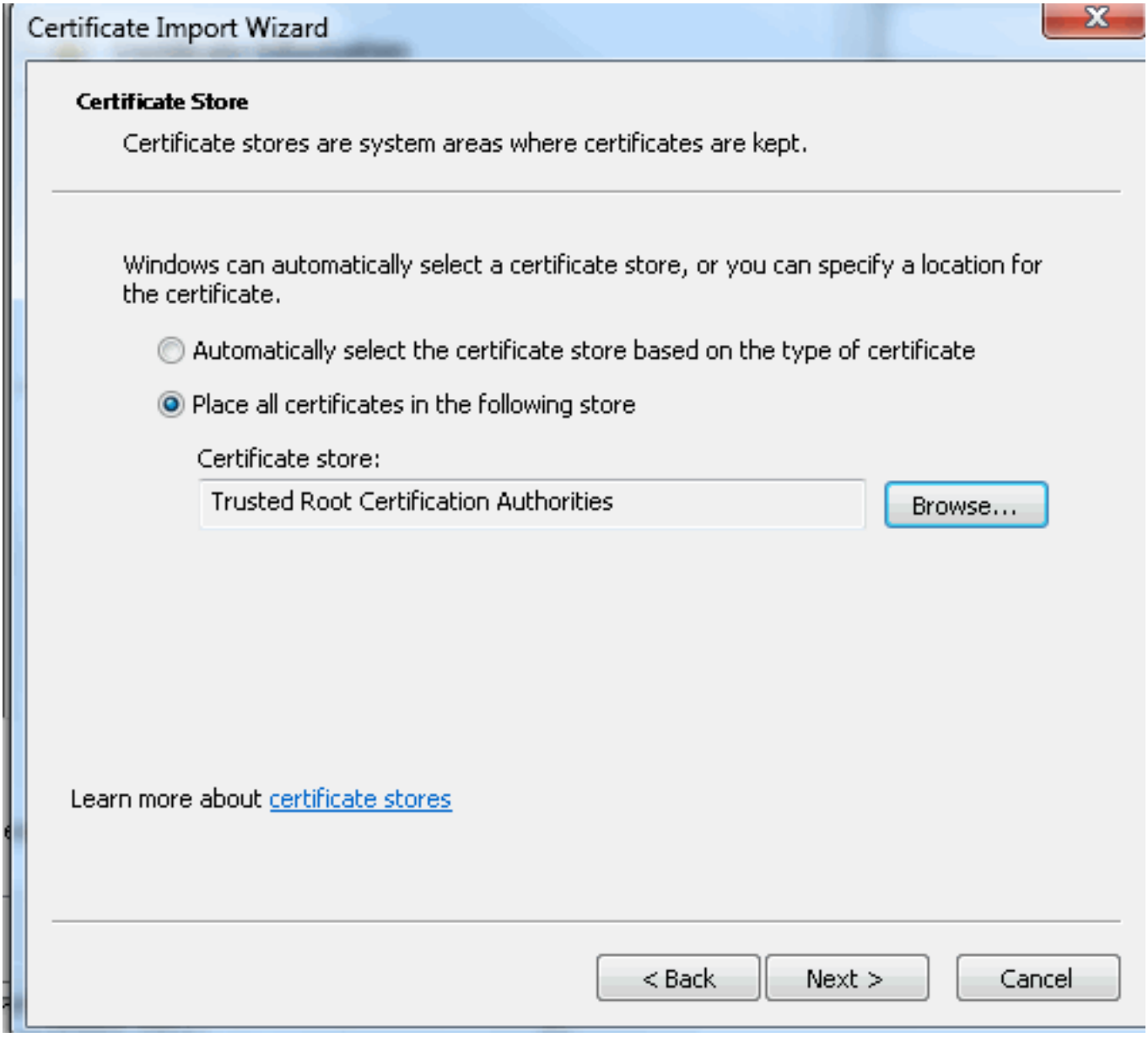
CA naar Windows Vertrouwen importeren

Exporteren van het CA-certificaat op IOS (controleer of u dit identiteitsbewijs wilt exporteren en neem alleen het eerste deel):

```
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-----
```

Kopieer het gedeelte tussen CERTIFICAAT BEGIN en EINDCERTIFICAAT en plak het naar Kladblok in Windows en slaat het op als bestand CA.crt.

U dient het te installeren zoals bij Trusted Root Authority (dubbelklik op bestand > Installeer certificaat > Plaats alle certificaten in de volgende winkel > Trusted Root Certified Services):



AnyConnect XML-profiel configureren

In C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile create a file "what.xml" en plak dit:

```
<?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>
```

Zorg ervoor dat de vermelding in 10.1.1.2 exact dezelfde is als GN=10.1.1.2 die voor het identiteitsbewijs is ingevoerd.

Testen

In dit scenario wordt SSL VPN niet gebruikt, dus zorg ervoor dat de HTTP server op IOS uitgeschakeld is (geen ip http server). Anders ontvangt u een foutbericht in AnyConnect waarin staat: "Gebruik een browser om toegang te krijgen".

Wanneer u een verbinding maakt in AnyConnect, wordt u om een wachtwoord gevraagd. In dit voorbeeld is het Gebruiker3 dat werd gemaakt

Daarna is de gebruiker verbonden.

Verificatie

IOS-router

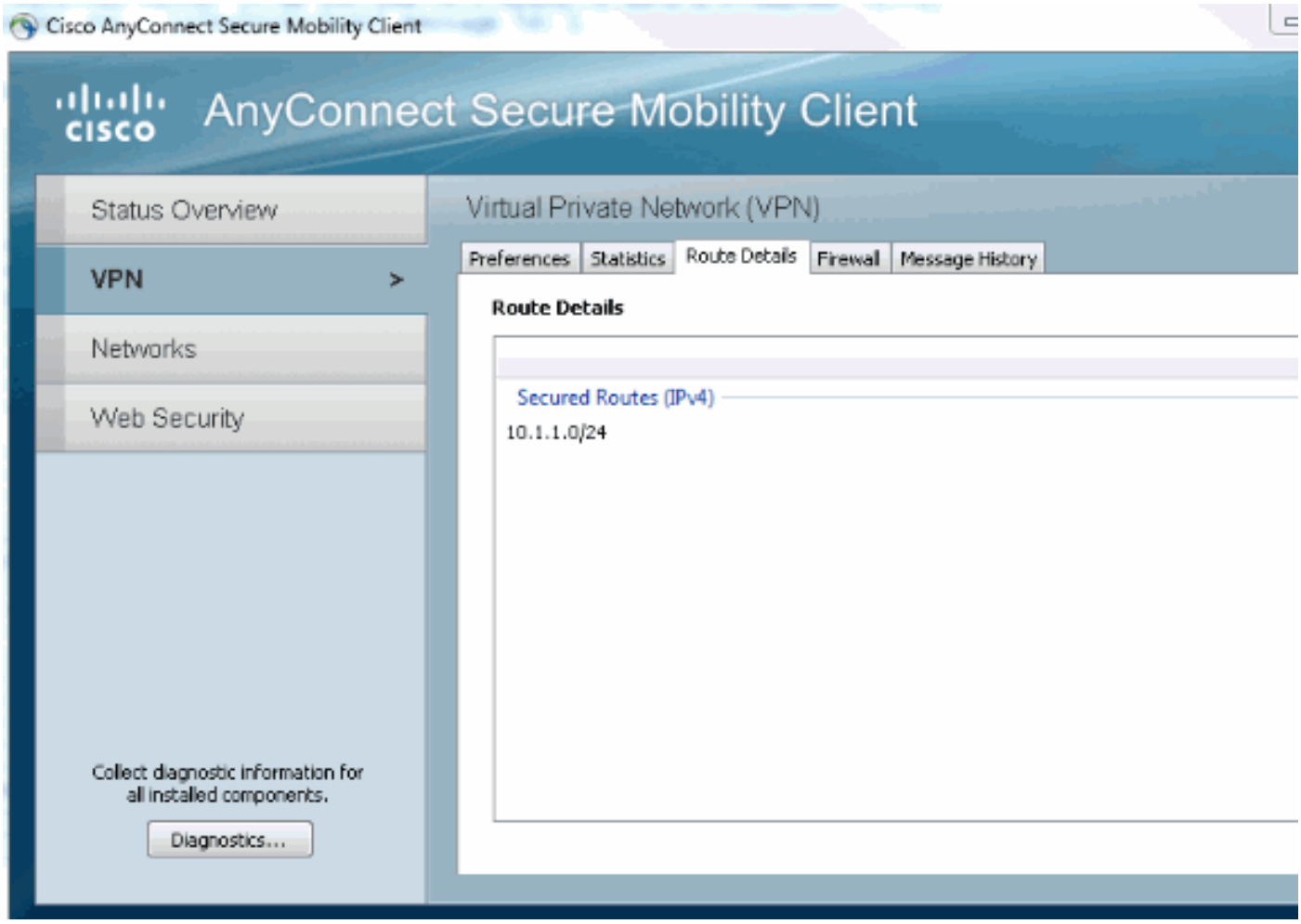
```
R1#show ip inter brief | i Virtual
Virtual-Access1    10.1.1.2  YES unset  up  up
Virtual-Template1  10.1.1.2  YES unset  up down
R1# show ip route 192.168.100.200
Routing entry for 192.168.100.200/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly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

U kunt een debug uitvoeren (debug crypto ikev2).

Windows

In de geavanceerde opties van AnyConnect in VPN kunt u Routedetails controleren om de netwerken voor splitsingen-tunneling te zien:



Bekende voorbehouden en kwesties

- Onthoud dat wanneer SHA1 een herkenningshash heeft en in het integriteitsbeleid in IKEv2 (raadpleeg Cisco bug ID CSCtn59317 (alleen geregistreerde klanten)).
- GN in IOS-identiteitsbewijs moet gelijk zijn aan hostname in het ACS XML-profiel.
- Als u Radius AV paren wilt gebruiken die zijn doorlopen tijdens de authenticatie en helemaal

geen toestemming van de groep gebruiken, kunt u dit in IKEv2-profiel gebruiken:
`aaa authorization user eap cached`

- De autorisatie wordt altijd gebruikt met het wachtwoord "cisco" voor de autorisatie van groepen en gebruikers. Dit kan verwarrend zijn bij gebruik
  `aaa authorization user eap list SERV (without any paramaters)`
  omdat het probeert om het gebruik van de gebruiker die in AnyConnect wordt doorgegeven als gebruiker en het wachtwoord "cisco" te autoriseren, wat waarschijnlijk niet het wachtwoord voor de gebruiker is.
- Bij problemen zijn dit outputs die u kunt analyseren en doorgeven aan Cisco TAC:debug van crypto ikev2debug van crypto ikev2 interneDART-uitgangen
- Als u SSL VPN niet gebruikt, vergeet dan ip http server (geen ip http server) uit te schakelen. Anders zal AnyConnect proberen verbinding te maken met de HTTP-server en het resultaat ontvangen, "Gebruik een browser om toegang te krijgen".

Cryptografie van de volgende generatie

De bovenstaande configuratie is voorzien voor een verwijzing naar een minimalistische werkconfiguratie.

Cisco raadt het gebruik van Next Generation Cryptografie (NGC) aan.

De huidige aanbevelingen voor migratie zijn hier te vinden:
http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Zorg er bij het kiezen van een NGC-configuratie voor dat zowel de clientsoftware als de head-end hardware deze ondersteunen. Routers voor ISR-generatie 2 en ASR 1000 worden aanbevolen als head-end vanwege hun hardwareondersteuning voor NGC.

Aan de AnyConnect-zijde wordt, zoals gebruikelijk van de AnyConnect 3.1 versie, de Suite B-algenreeks van de NSA ondersteund.

Gerelateerde informatie

- Cisco ASA IKEv2 PKI site-site VPN
- IKEv2 Site2-updates op IOS
- FlexVPN/IKEv2: Windows 7-client voor gebouwen: IOS-head-end: Deel I - certificaatverificatie
- Configuratie-gids voor FlexVPN en Internet Key Exchange, versie 2, Cisco IOS-softwarerelease 15.2M&T
- Technische ondersteuning en documentatie – Cisco Systems