Déploiement FlexVPN : Accès à distance AnyConnect IKEv2 avec EAP-MD5

Contenu

Introduction

Ce document fournit un exemple de configuration de la configuration de l'accès à distance sur IOS à l'aide de la boîte à outils FlexVPN.

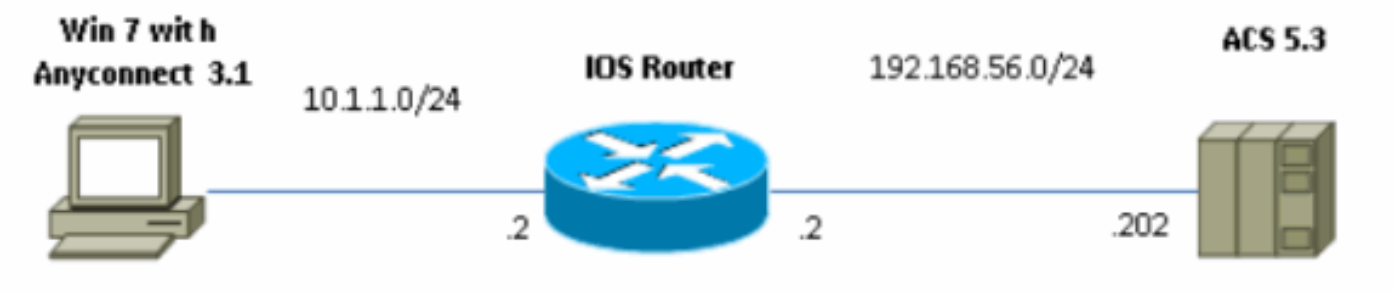
Le VPN d'accès à distance permet aux clients finaux utilisant divers systèmes d'exploitation de se connecter en toute sécurité à leurs réseaux d'entreprise ou domestiques via un support non sécurisé tel qu'Internet. Dans le scénario présenté, le tunnel VPN est interrompu sur un routeur Cisco IOS à l'aide du protocole IKEv2.

Ce document montre comment authentifier et autoriser les utilisateurs utilisant Access Control Server (ACS) via la méthode EAP-MD5.

Conditions préalables

Diagramme du réseau

Le routeur Cisco IOS comporte deux interfaces, une vers ACS 5.3 :



Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ACS 5.3 avec correctif 6
- Routeur IOS avec logiciel 15.2(4)M
- PC Windows 7 avec AnyConnect 3.1.01065

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Fond

Dans IKEv1 XAUTH est utilisé dans la phase 1.5, vous pouvez effectuer l'authentification des utilisateurs localement sur un routeur IOS et à distance à l'aide de RADIUS/TACACS+. IKEv2 ne prend plus en charge XAUTH et la phase 1.5. Il contient le support EAP intégré, qui est fait dans la phase IKE_AUTH. Le plus grand avantage de cela est dans la conception IKEv2 et EAP est une norme bien connue.

EAP prend en charge deux modes :

- Tunneling : EAP-TLS, EAP/PSK, EAP-PEAP, etc.
- Non-tunneling : EAP-MSCHAPv2, EAP-GTC, EAP-MD5, etc.

Dans cet exemple, EAP-MD5 en mode non-tunneling est utilisé car il s'agit de la méthode d'authentification externe EAP prise en charge actuellement dans ACS 5.3.

Le protocole EAP peut uniquement être utilisé pour l'authentification initiateur (client) au répondeur

(IOS dans ce cas).

Configuration initiale IOS

IOS - CA

Tout d'abord, vous devez créer une autorité de certification (CA) et un certificat d'identité pour le routeur IOS. Le client vérifie l'identité du routeur en fonction de ce certificat.

La configuration de CA sur IOS ressemble à :

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

Vous devez vous rappeler de l'utilisation étendue des clés (Server-Auth requise pour EAP, pour RSA-SIG, vous avez également besoin de Client-Auth).

Activez l'autorité de certification à l'aide de la commande **no shutdown** dans l'autorité de certification du serveur crypto pki.

IOS - Certificat d'identité

Ensuite, activez le protocole SCEP (Simple Certificate Enrollment Protocol) pour le certificat et configurez le point de confiance.

```
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
```

Ensuite, authentifiez et inscrivez le certificat :

```
(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 vous ne voulez pas que les messages d'invite soient affichés dans AnyConnect, n'oubliez pas que le nombre de messages peut être égal à celui des adresses IP/nom d'hôte configurées dans le profil AnyConnect.

Dans cet exemple, cn=10.1.1.2. Par conséquent, dans AnyConnect 10.1.1.2 est entré comme adresse IP du serveur dans le profil xml AnyConnect.

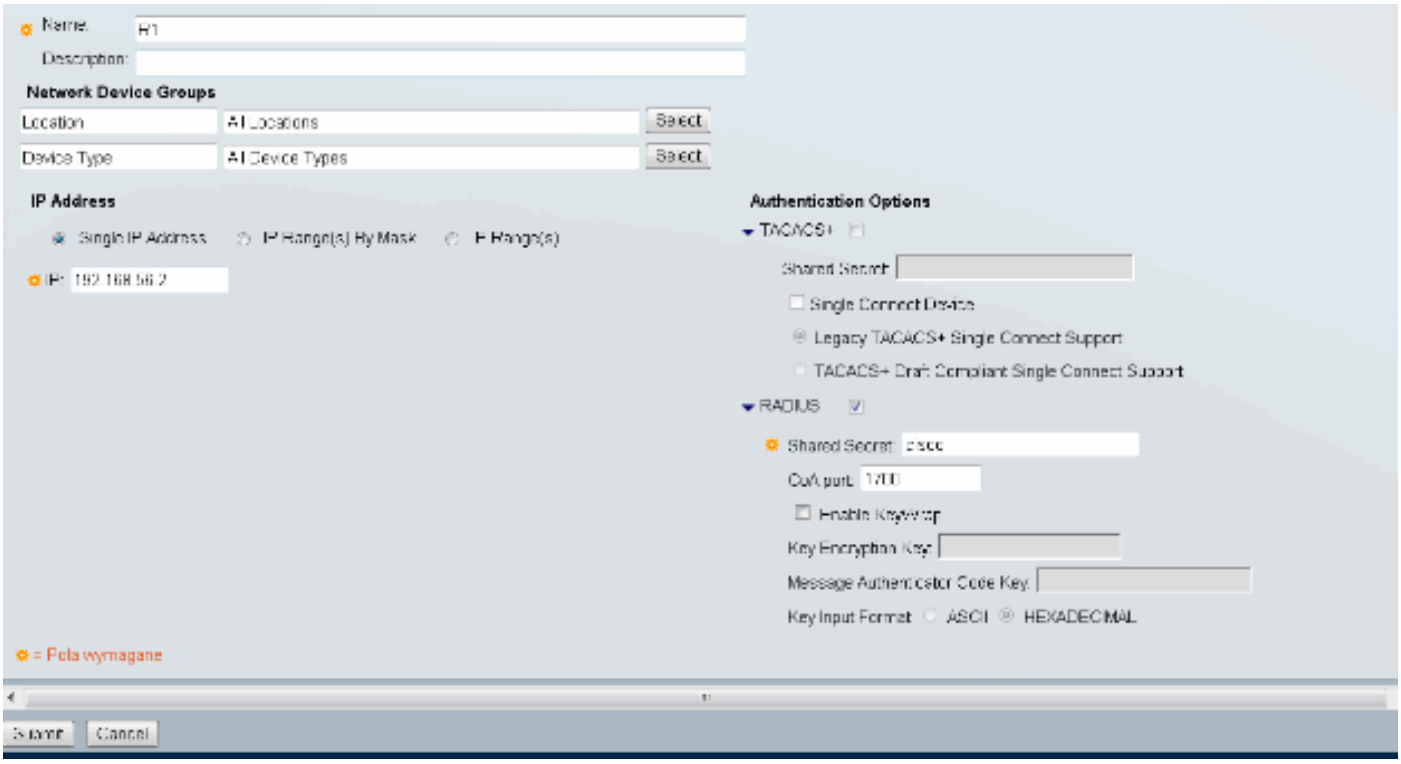
IOS - Configuration AAA et Radius

Vous devez configurer l'authentification et l'autorisation Radius et AAA :

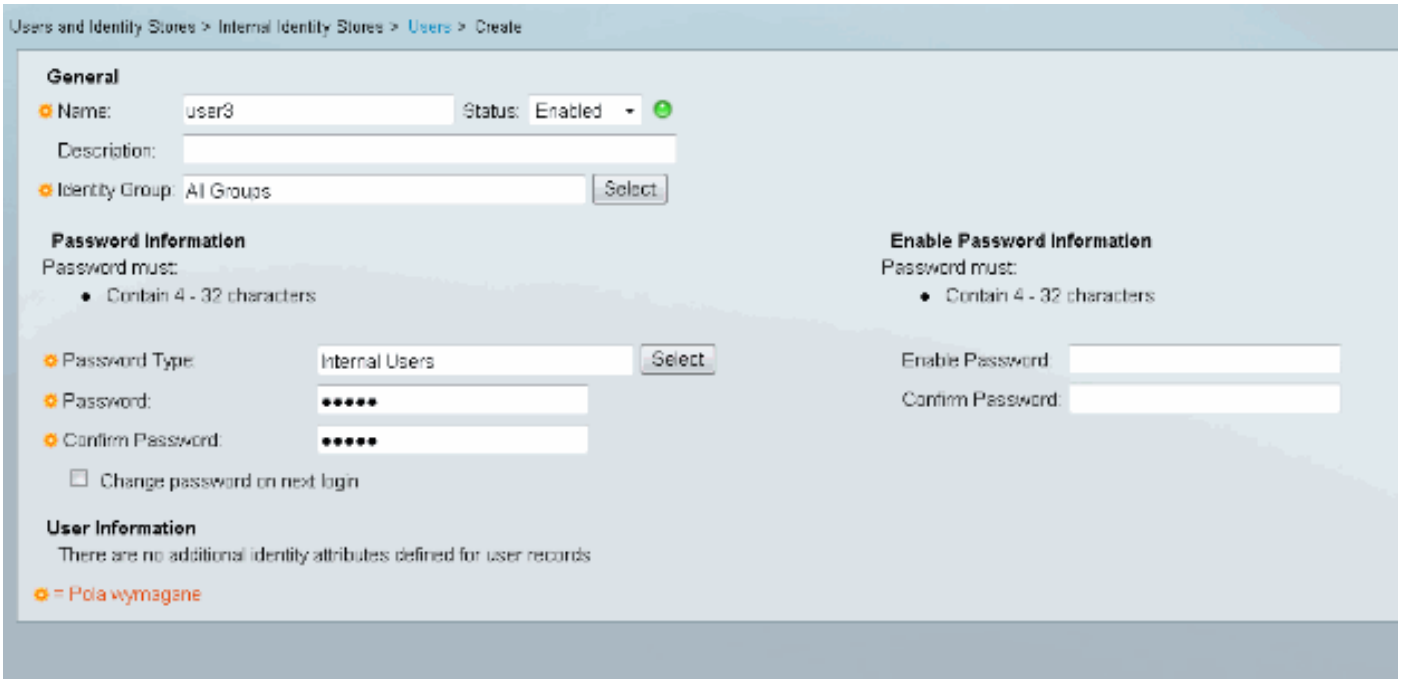
```
aaa new-model
radius-server host 192.168.56.202 key cisco
aaa group server radius SERV
server 192.168.56.202
aaa authentication login eap-list group SERV
aaa authorization network eap-list group SERV
```

Configuration initiale ACS

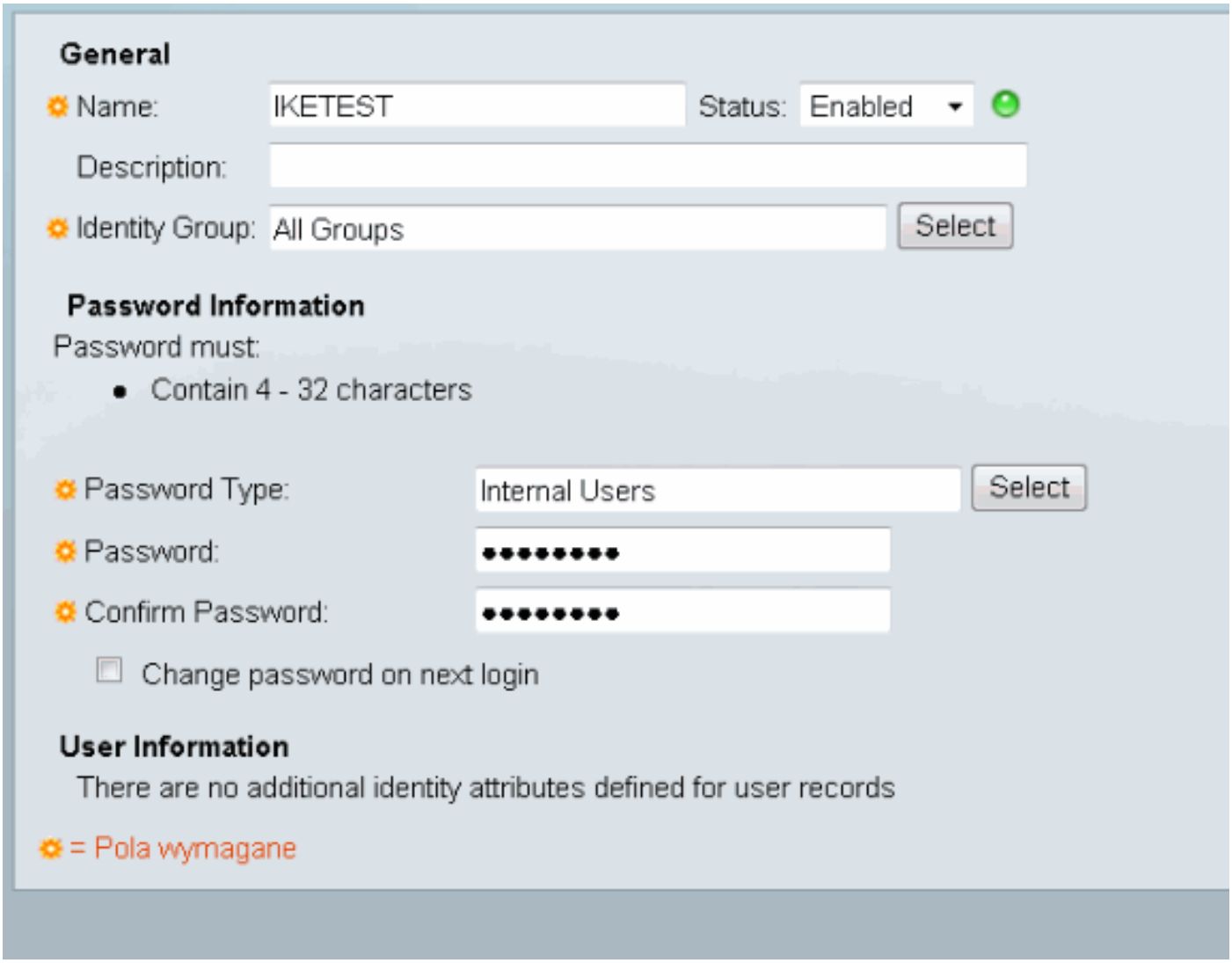
Tout d'abord, ajoutez le nouveau périphérique réseau dans ACS (Network Resources > Network Devices and AAA Clients > Create) :



Ajouter un utilisateur (Utilisateurs et magasins d'identités > Magasins d'identités internes > Utilisateurs > Créer) :

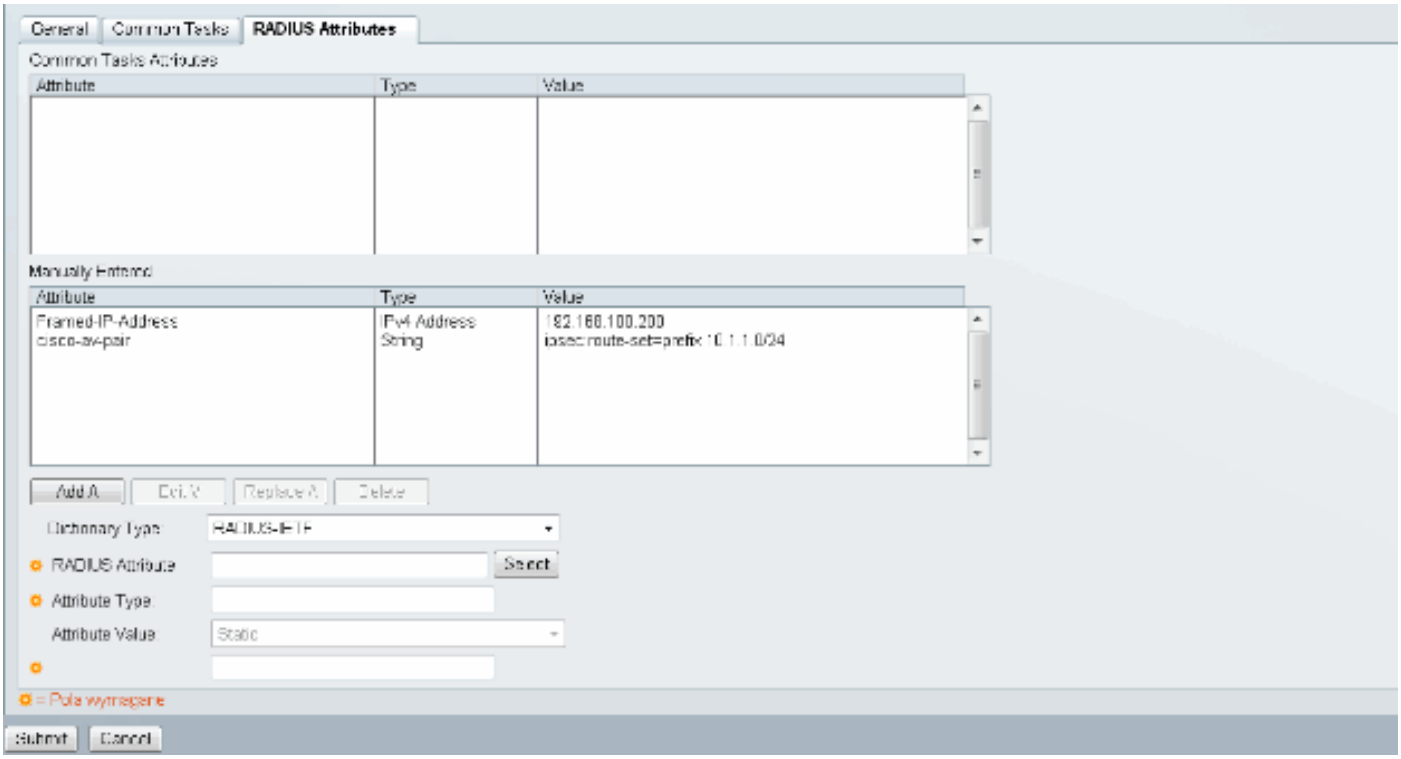


Ajoutez un utilisateur pour l'autorisation. Dans cet exemple, il s'agit de IKETEST. Le mot de passe doit être « cisco », car il s'agit de la valeur par défaut envoyée par IOS.

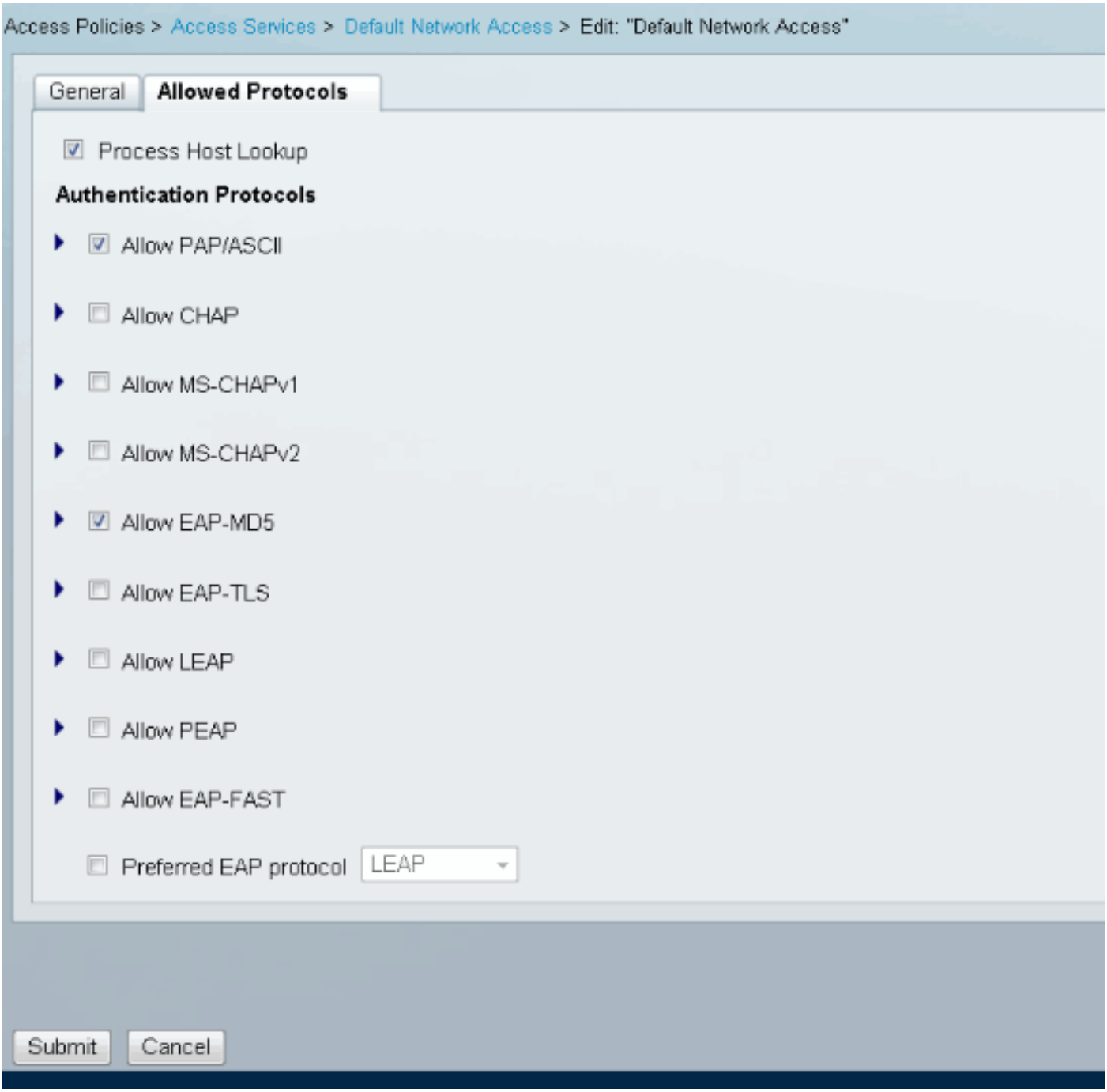


Ensuite, créez un profil d'autorisation pour les utilisateurs (éléments de stratégie > Autorisation et autorisations > Accès réseau > Profils d'autorisation > Créer).

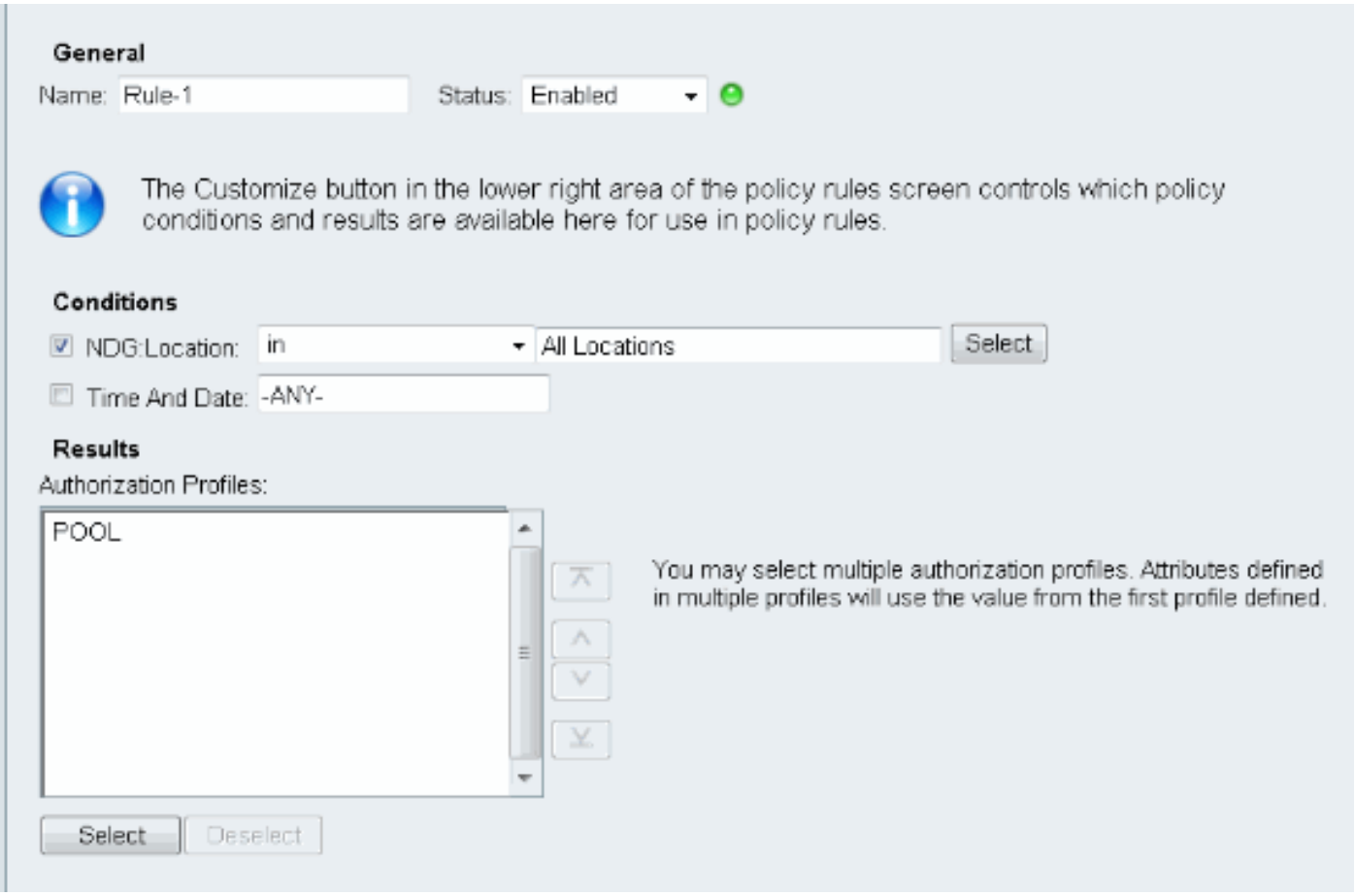
Dans cet exemple, il s'appelle POOL. Dans cet exemple, la paire AV de tunnel partagé (en tant que préfixe) est entrée et l'adresse IP de trame comme adresse IP qui sera attribuée au client connecté. La liste de toutes les paires AV prises en charge se trouve ici : http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html



Ensuite, vous devez activer la prise en charge d'EAP-MD5 (pour l'authentification) et PAP/ASCII (pour l'autorisation) dans la stratégie d'accès. La valeur par défaut est utilisée dans cet exemple (Access Policies > Default Network Access) :



Créez une condition pour dans la stratégie d'accès et affectez le profil d'autorisation qui a été créé. Dans ce cas, une condition pour NDG : Location in All Locations est créée. Par conséquent, pour toutes les demandes d'autorisation Radius, le profil d'autorisation POOL (Politiques d'accès > Services d'accès > Accès réseau par défaut) est fourni :



Vous devriez pouvoir tester sur un routeur IOS si l'utilisateur peut s'authentifier correctement :

```
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"
```

Configuration IOS FlexVPN

Vous devez créer une proposition et une stratégie IKEv2 (vous n'avez peut-être pas besoin de le faire, reportez-vous à CSCtn59317). La stratégie est créée uniquement pour l'une des adresses IP (10.1.1.2) dans cet exemple.

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

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

Ensuite, créez un profil IKEV2 et un profil IPsec qui seront liés à Virtual-Template.

Assurez-vous que vous désactivez http-url cert, comme indiqué dans le guide de configuration.

```
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
```

Dans cet exemple, l'autorisation est configurée en fonction de l'utilisateur IKETEST, qui a été créé dans la configuration ACS.

Configuration Windows

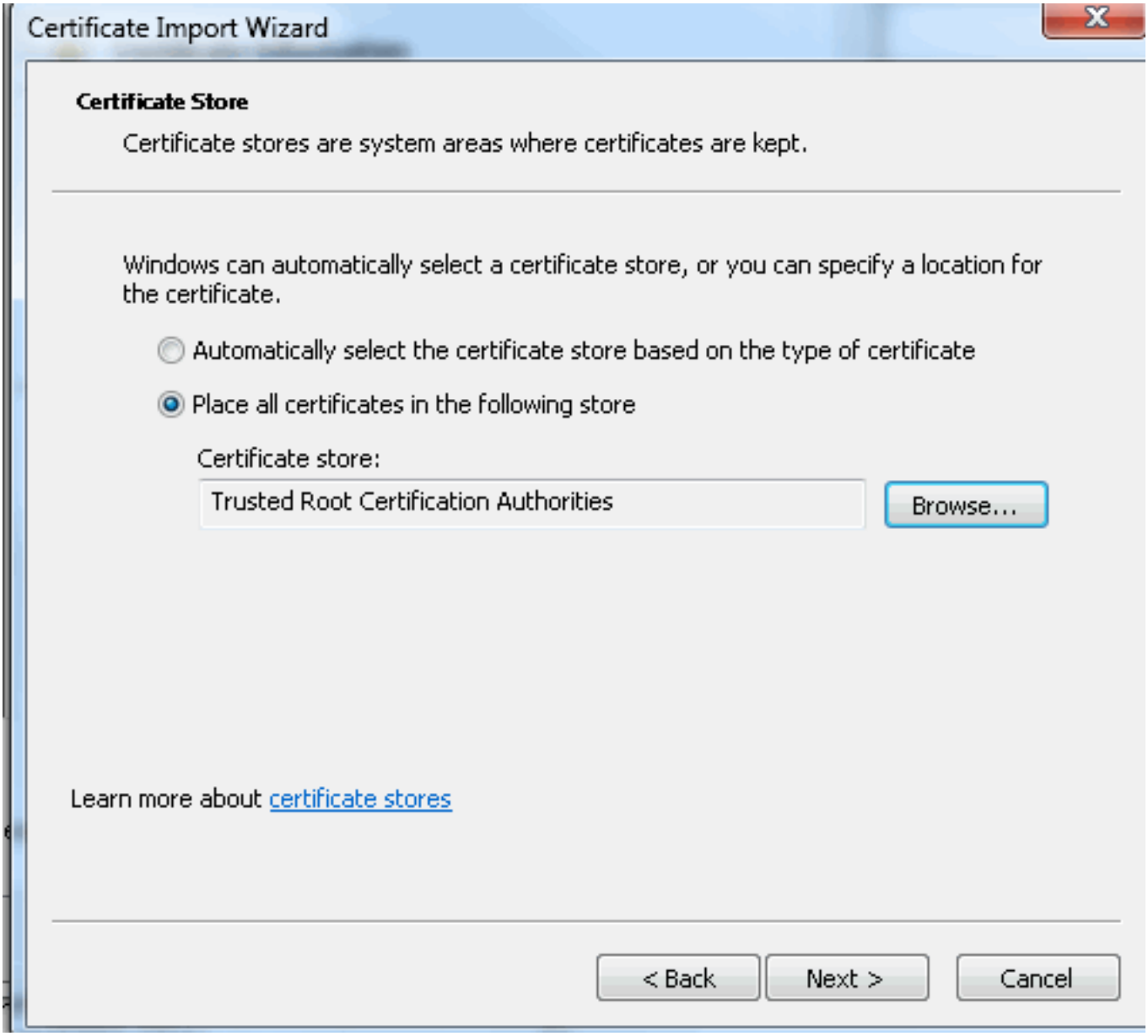
Importation de CA vers des approbations Windows

Exporter le certificat CA sur IOS (assurez-vous d'exporter le certificat d'identité et ne prendre que la première partie) :

```
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-----
```

Copiez la pièce entre DÉBUTER LE CERTIFICAT et FIN LE CERTIFICAT, puis collez-la dans le Bloc-notes de Windows et enregistrez-la sous forme de fichier CA.crt.

Vous devez l'installer comme dans Autorités racines de confiance (double-cliquez sur le fichier > Installer le certificat > Placer tous les certificats dans le magasin suivant > Autorités de certification racine de confiance) :



Configuration du profil XML AnyConnect

Dans C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile create a file « any.xml » et collez ceci :

```
<?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>
```

Assurez-vous que l'entrée 10.1.1.2 est exactement la même que CN=10.1.1.2 qui a été entrée pour le certificat d'identité.

Tests

Dans ce scénario, le VPN SSL n'est pas utilisé, alors assurez-vous que le serveur HTTP est désactivé sur IOS (pas de serveur ip http). Sinon, vous recevez un message d'erreur dans AnyConnect qui indique : « Utilisez un navigateur pour accéder à ».

Lorsque vous vous connectez à AnyConnect, vous devez être invité à fournir un mot de passe. Dans cet exemple, c'est l'utilisateur 3 qui a été créé

Après cela, l'utilisateur est connecté.

Vérification

Routeur IOS

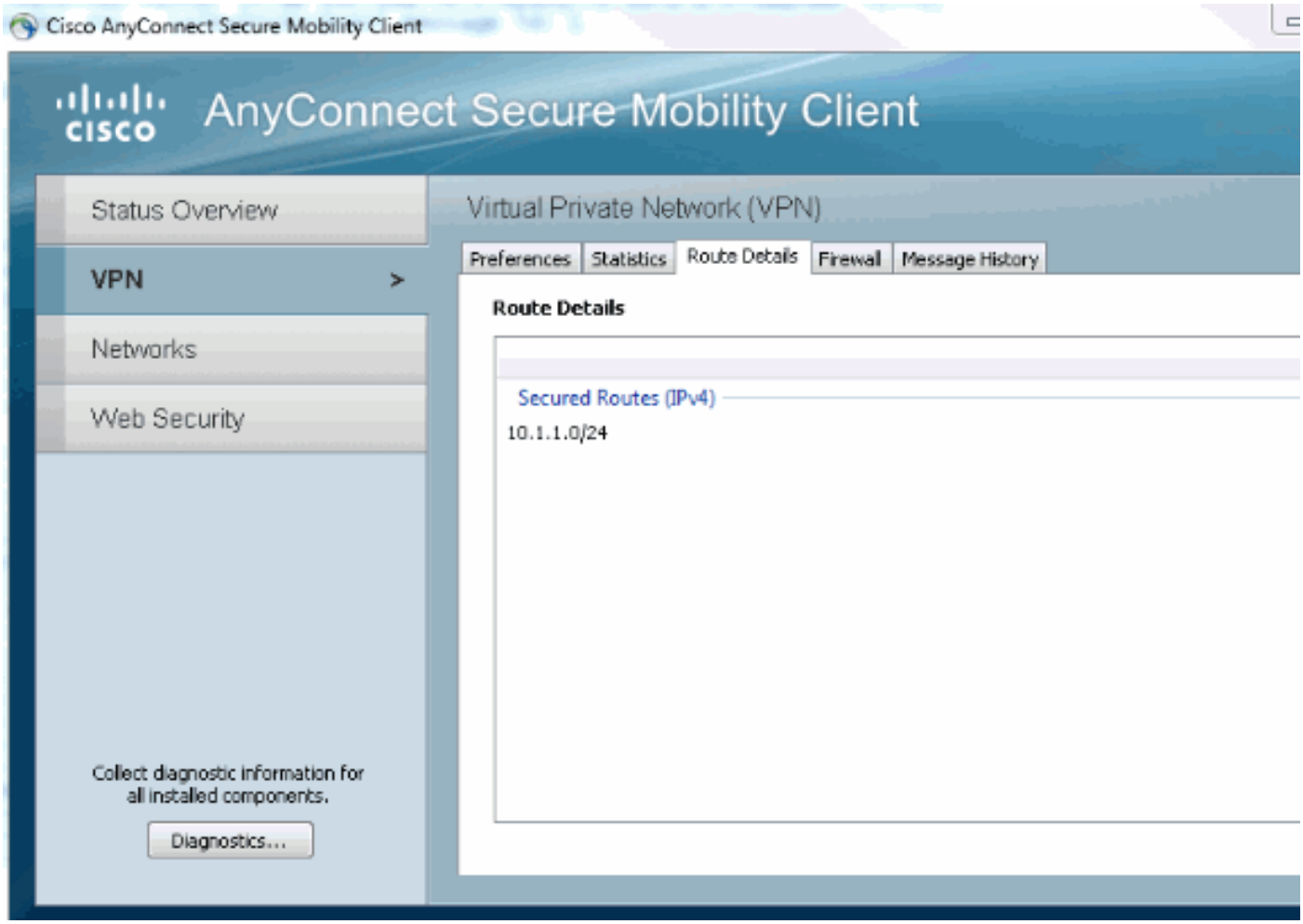
```
R1#show ip inter brief | i Virtual
Virtual-Access1    10.1.1.2  YES unset  up  up
Virtual-Template1  10.1.1.2  YES unset  up down
R1# show ip route 192.168.100.200
Routing entry for 192.168.100.200/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly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

Vous pouvez effectuer un débogage (debug crypto ikev2).

Fenêtres

Dans les options avancées d'AnyConnect dans VPN, vous pouvez vérifier les détails de route pour voir les réseaux de tunnellisation fractionnée :



Causes et problèmes connus

- N'oubliez pas d'avoir SHA1 dans le hachage de signature et dans la stratégie d'intégrité dans IKEv2 (reportez-vous à l'ID de bogue Cisco CSCtn59317 (clients enregistrés uniquement)).
- Le CN dans le certificat d'identité IOS doit être un nom d'hôte égal dans le profil XML ACS.
- Si vous voulez utiliser les paires AV Radius passées lors de l'authentification et ne pas utiliser

l'autorisation du groupe du tout, vous pouvez utiliser ceci dans le profil IKEv2 :
`aaa authorization user eap cached`

- L'autorisation utilise toujours le mot de passe « cisco » pour l'autorisation de groupe/utilisateurs. Cette opération peut être source de confusion lors de l'utilisation `aaa authorization user eap list SERV (without any paramaters)` car il tentera d'autoriser l'utilisation de l'utilisateur passé dans AnyConnect comme utilisateur et mot de passe « cisco », ce qui n'est probablement pas le mot de passe de l'utilisateur.
- En cas de problème, il s'agit de résultats que vous pouvez analyser et fournir au TAC Cisco :debug crypto ikev2debug crypto ikev2 internalSortie DART
- Si vous n'utilisez pas le VPN SSL, n'oubliez pas de désactiver le serveur ip http (pas de serveur ip http). Sinon, AnyConnect tentera de se connecter au serveur HTTP et recevra le résultat, « Utiliser un navigateur pour accéder ».

Cryptographie de nouvelle génération

La configuration ci-dessus est fournie à titre de référence pour montrer une configuration de travail minimaliste.

Cisco recommande d'utiliser la cryptographie nouvelle génération (NGC) si possible.

Les recommandations actuelles concernant la migration sont disponibles ici : http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Lors du choix de la configuration NGC, assurez-vous que le logiciel client et le matériel de tête de réseau le prennent en charge. Les routeurs ISR de 2e génération et ASR 1000 sont recommandés comme têtes de réseau en raison de leur prise en charge matérielle des NGC.

Du côté d'AnyConnect, depuis la version 3.1 d'AnyConnect, la suite d'algorithme Suite B de NSA est prise en charge.

Informations connexes

- VPN site-site PKI Cisco ASA IKEv2
- Débogues de site2 IKEv2 sur IOS
- FlexVPN / IKEv2 : Windows 7 Builtin-Client : Tête de réseau IOS : Partie I - Authentification par certificat
- Guide de configuration FlexVPN et Internet Key Exchange version 2, Cisco IOS version 15.2M&T
- Support et documentation techniques - Cisco Systems