

# Déploiement de FlexVPN : Accès à distance d'AnyConnect IKEv2 avec EAP-MD5

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Diagramme du réseau](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Fond](#)

[Configuration initiale IOS](#)

[IOS - CA](#)

[IOS - Certificat d'identité](#)

[IOS - AAA et configuration RADIUS](#)

[Configuration initiale ACS](#)

[Configuration IOS FlexVPN](#)

[Configuration de Windows](#)

[Importer le CA aux confiances de Windows](#)

[Configurer le profil d'AnyConnect XML](#)

[Tests](#)

[Vérification](#)

[Routeur IOS](#)

[Windows](#)

[Mises en garde et questions connues](#)

[Chiffrement de nouvelle génération](#)

[Informations connexes](#)

## [Introduction](#)

Ce document fournit une configuration d'échantillon de la façon d'installer l'Accès à distance sur l'IOS utilisant la boîte à outils de FlexVPN.

L'Accès à distance VPN permet des fin-clients à l'aide de divers systèmes d'exploitation pour se connecter sécurisé à leurs entreprise ou réseaux domestiques par le support non-sécurisé tel que l'Internet. Dans le scénario présenté, le tunnel VPN est terminé sur un routeur Cisco IOS utilisant le protocole IKEv2.

Ce document affiche comment authentifier et autoriser des utilisateurs à l'aide du serveur de contrôle d'accès (ACS) par la méthode EAP-MD5.

# Conditions préalables

## Diagramme du réseau

Le routeur Cisco IOS a deux interfaces - une vers ACS 5.3 :



## Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

## Composants utilisés

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

- ACS 5.3 avec le correctif 6
- Routeur IOS avec le logiciel de 15.2(4)M
- PC de 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 le XAUTH est utilisé dans la phase 1.5, vous pouvez faire l'authentification des utilisateurs localement sur un routeur IOS et à distance utilisant RADIUS/TACACS+. IKEv2 ne prend en charge plus le XAUTH et la phase 1.5. Il contient le support intégré d'EAP, qui est fait dans la phase IKE\_AUTH. Le plus grand avantage de ceci est dans la conception IKEv2 et l'EAP est une norme réputée.

L'EAP prend en charge deux modes :

- Perçage d'un tunnel — EAP-TLS, EAP/PSK, EAP-PEAP etc.
- Non-Tunnellisation — EAP-MSCHAPv2, EAP-GTC, EAP-MD5 etc.

Dans cet exemple, EAP-MD5 en mode de non-Tunnellisation est utilisé parce que c'est méthode d'authentification externe d'EAP prise en charge actuellement dans ACS 5.3.

L'EAP peut être seulement utilisé au demandeur d'authentification (client) au responder (IOS dans

ce cas).

## Configuration initiale IOS

### IOS - CA

D'abord de tous vous devez créer l'Autorité de certification (CA) et créer un certificat d'identité pour le routeur IOS. Le client vérifiera l'identité du routeur basée sur ce certificat.

La configuration du CA sur l'IOS ressemble à :

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

Vous devez se souvenir au sujet de l'utilisation principale étendue (serveur-Auth requis pour l'EAP, parce que au sujet du RSA-SIG vous avez besoin également de client-Auth).

Activez le CA utilisant l'aucune commande **shutdown** dans le crypto pki server CA.

### IOS - Certificat d'identité

Ensuite, activez l'inscription de certificat simple Protocol (SCEP) 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
```

Puis, authentifiez et inscrivez-vous 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 faire se souvenir les messages prompts en AnyConnect que la NC doit être égale à l'adresse Internet/aux adresses IP configurées dans le profil d'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 de xml d'AnyConnect.

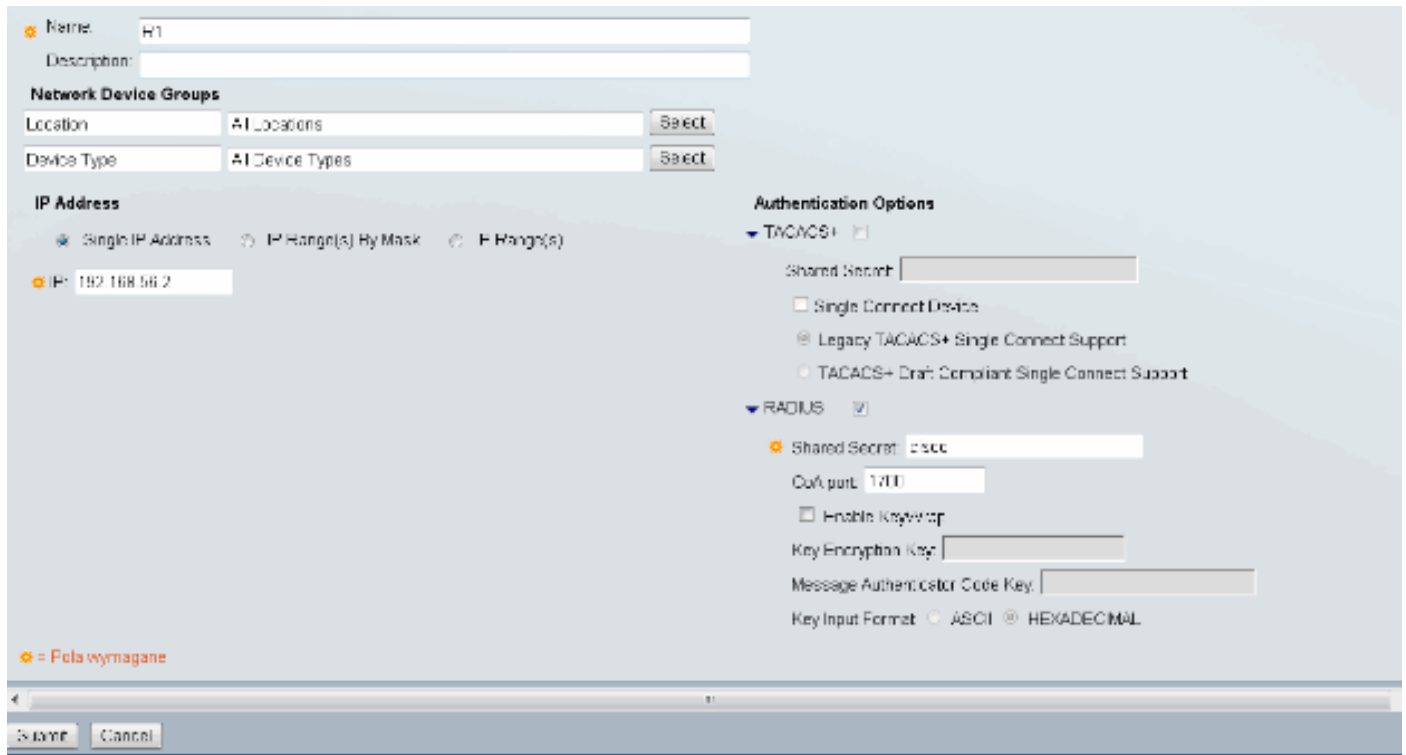
## IOS - AAA et configuration RADIUS

Vous devez configurer le rayon et l'authentification et l'autorisation d'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

D'abord, ajoutez le nouveau périphérique de réseau dans ACS (les ressources de réseau > les périphériques de réseau et les clients d'AAA > créent) :



The screenshot shows the configuration page for a new network device in ACS. The device name is 'R1'. The IP address is set to '192.168.56.2'. The authentication options are configured for RADIUS with a shared secret of 'cisco' and a port of '1711'. The key input format is set to 'HEXADECIMAL'.

**Network Device Groups**

Location: All Locations

Device Type: All Device Types

**IP Address**

Single IP Address  IP Range(s) By Mask  IP Range(s)

IP: 192.168.56.2

**Authentication Options**

**TACACS+**

Shared Secret:

Single Connect Disable

Legacy TACACS+ Single Connect Support

TACACS+ Draft Compliant Single Connect Support

**RADIUS**

Shared Secret: cisco

CoA port: 1711

Enable Keyvector

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format:  ASCII  HEXADECIMAL

Ajoutez un utilisateur (les utilisateurs et l'identité enregistré > identité interne enregistré > des utilisateurs > créent) :

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:

Ajoutez un utilisateur pour l'autorisation. Dans cet exemple, c'est IKETEST. Le mot de passe doit être « Cisco » parce que c'est le par défaut envoyé par l'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

Ensuite, créez un profil d'autorisation pour les utilisateurs (les éléments de stratégie > l'autorisation et les autorisations > les profils d'accès au réseau > d'autorisation > créent).

Dans cet exemple, ce s'appelle le GROUPE. Dans cet exemple, la paire AV de tunnel partagé (comme préfixe) est écrite et Encadrer-IP-adresse comme adresse IP qui va être assignée au client connecté. La liste de toutes les paires AV prises en charge peut être trouvée ici : [http://www.cisco.com/en/US/docs/ios-xml/ios/sec\\_conn\\_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html](http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html)

The screenshot displays the 'RADIUS Attributes' configuration page. It features two tables for managing attributes:

Attribute	Type	Value
Common Tasks Attributes		

Attribute	Type	Value
Manually Entered		
Framed-IP-Address cisco-av-pair	IPv4 Address String	192.168.100.200 iossec route-set=prefix 10.1.1.0/24

Below the tables, there are control buttons: 'Add A', 'Del A', 'Rebuild A', and 'Delete'. A 'Dictionary Type' dropdown is set to 'RADIUS-IP-IP'. There are also input fields for 'RADIUS Attribute', 'Attribute Type', and 'Attribute Value', with a 'Select' button next to the first field. A legend at the bottom left indicates that an orange dot represents a 'Pole wymagane' (required field). At the bottom of the interface are 'Submit' and 'Cancel' buttons.

Puis, vous devez activer le support d'EAP-MD5 (pour l'authentification) et de PAP/ASCII (pour l'autorisation) dans la stratégie d'Access. Le par défaut est utilisé dans cet exemple (stratégies d'Access > accès au réseau de par défaut) :

**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

Créez une condition pour dans la stratégie d'Access et assignez le profil d'autorisation qui a été créé. Dans ce cas une condition pour NDG : L'emplacement dans tous les emplacements est créé, ainsi pour toute la demande d'autorisations RADIUS fournira le profil d'autorisation de GROUPE (stratégies d'Access > services d'accès > accès au réseau de par défaut) :

**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.

Vous devriez pouvoir tester sur un routeur IOS si l'utilisateur peut 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 la proposition IKEv2 et la stratégie (vous ne pourriez pas devez, se rapporter à CSCtn59317). La stratégie est créée seulement pour 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
```

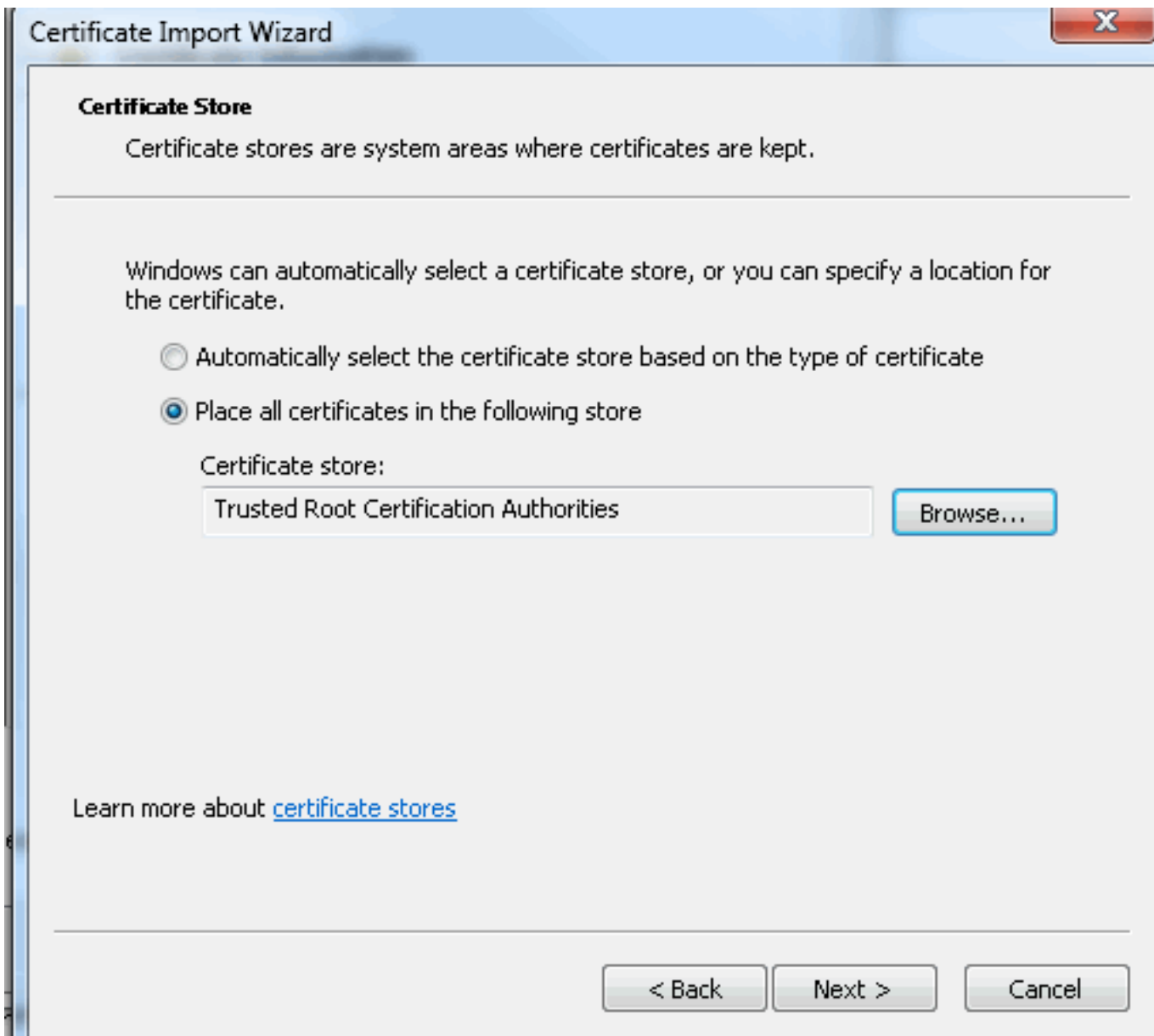
Puis, créez un profil IKEV2 et un profil IPsec qui lieront au virtual-template.

Assurez-vous que vous arrêtez le CERT HTTP-URL, comme informé 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
```







## [Configurer le profil d'AnyConnect XML](#)

Dans le client sécurisé \ profil de mobilité de C:\ProgramData\Cisco\Cisco AnyConnect créez un fichier « whatever.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>
  </ClientInitialization>
</AnyConnectProfile>
```

```

<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>

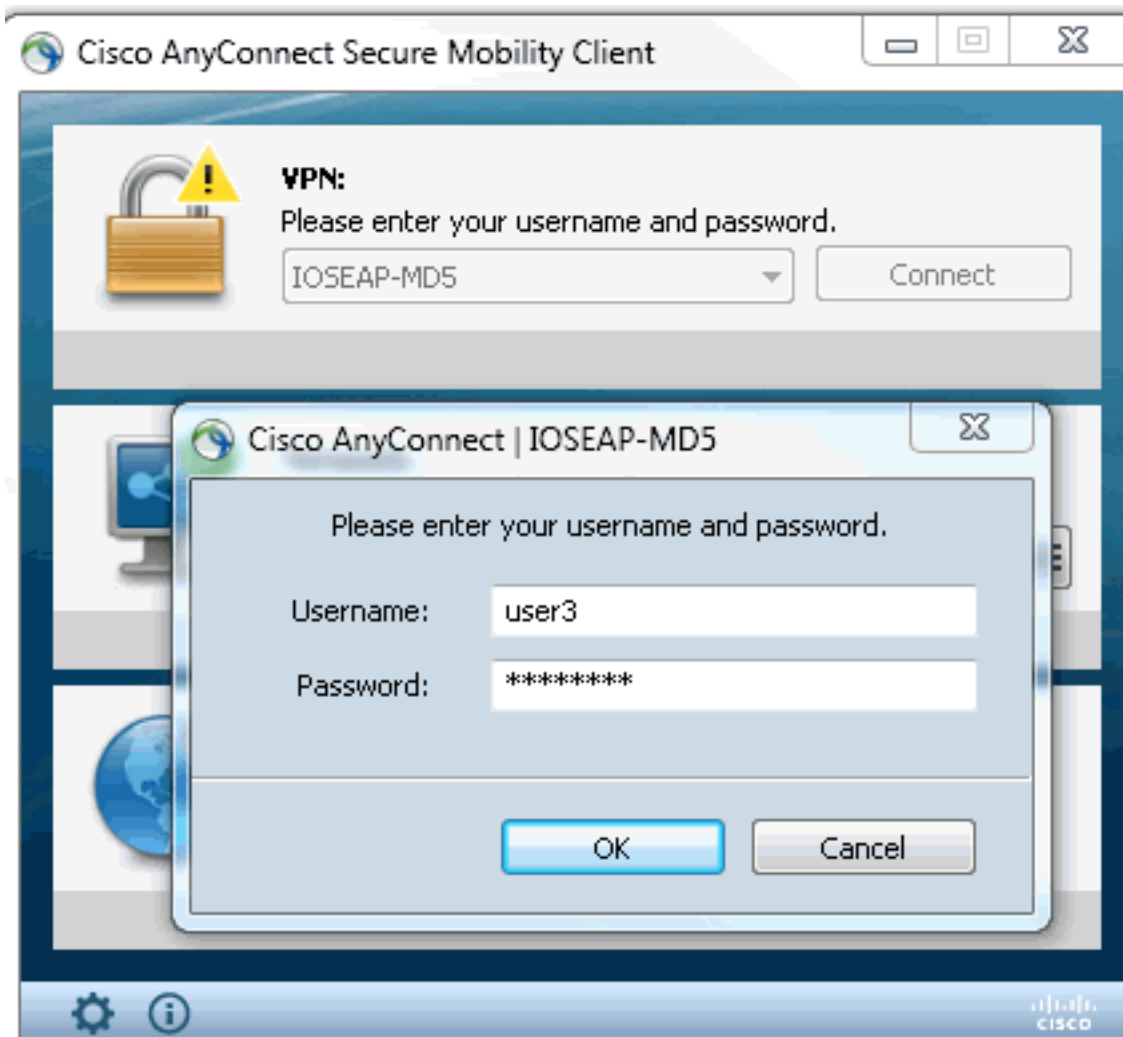
```

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

## Tests

Dans ce scénario le VPN SSL n'est pas utilisé, ainsi assurez-vous que le serveur HTTP est désactivé sur IOS (aucun ip http server). Autrement, vous recevez un message d'erreur dans AnyConnect qui énonce, « utilisez un navigateur pour accéder ».

En se connectant dans AnyConnect, vous devriez être incité pour un mot de passe. Dans cet exemple, c'est User3 qui a été créé



Après ce, l'utilisateur est connecté.

## Vérification

### Routeur IOS

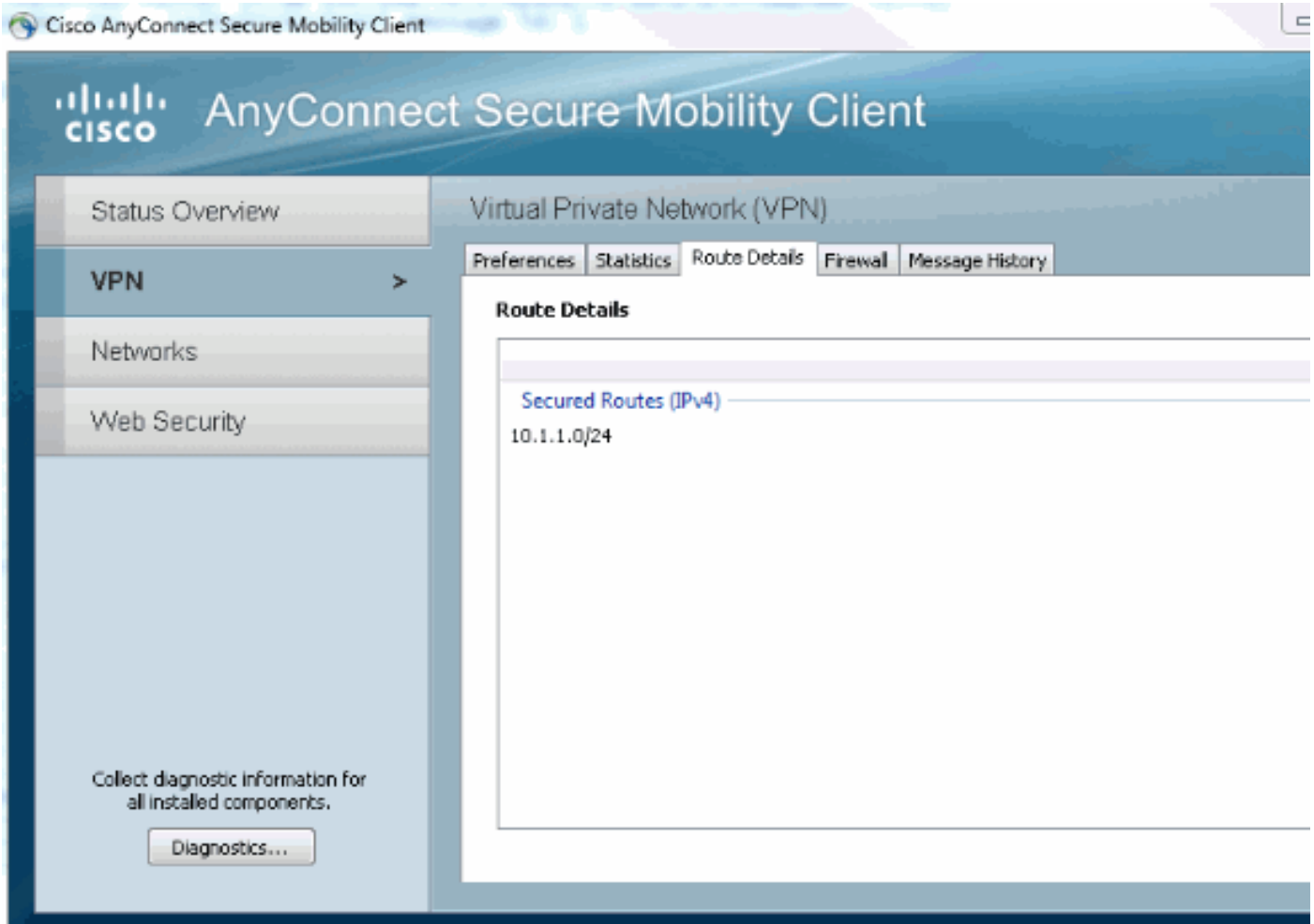
```
R1#show ip inter brief | i Virtual Virtual-Access1 10.1.1.2 YES unset up up Virtual-Templatel
10.1.1.2 YES unset up down R1# show ip route 192.168.100.200 Routing entry for
192.168.100.200/32 Known via "static", distance 1, metric 0 (connected) Routing Descriptor
Blocks: * directly connected, via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

Vous pouvez exécuter un débogage (debug crypto ikev2).

### Windows

Dans les options avancées d'AnyConnect dans le VPN vous pouvez vérifier des détails d'artère

pour voir les réseaux de Segmentation de tunnel :



## Mises en garde et questions connues

- Souvenez-vous en ayant SHA1 en informations parasites de signature et dans la stratégie d'intégrité dans IKEv2 (référez-vous à l'ID de bogue Cisco [CSCtn59317](#) (clients [enregistrés](#) seulement)).
- La NC dans le certificat d'identité IOS doit être adresse Internet égale dans le profil ACS XML.
- Si vous voulez utiliser des paires AV de rayon passées pendant l'authentification et pas l'autorisation d'utilisation 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. Ceci pourrait être embrouillant tout en utilisant 

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

 parce qu'il essaiera d'autoriser utilisant l'utilisateur passé dans AnyConnect comme utilisateur et mot de passe « Cisco », qui n'est probablement pas le mot de passe pour l'utilisateur.
- En cas de toutes les questions ce sont des sorties que vous pouvez analyser et fournir à Cisco TAC :

```
debug crypto ikev2debug crypto ikev2 interne
```

Sorties de DART
- Sinon utilisant le VPN SSL souvenez-vous pour désactiver l'ip http server (aucun ip http server). Autrement, AnyConnect essaiera de se connecter au serveur HTTP et recevoir le résultat, « utilisez un navigateur pour accéder ».

## Chiffrement de nouvelle génération

La configuration ci-dessus est donnée pour la référence pour afficher une configuration en cours minimalistic.

Cisco recommande utilisant le chiffrement de nouvelle génération (NGC) si possible.

Des recommandations en cours pour le transfert peuvent être trouvées ici :

[http://www.cisco.com/web/about/security/intelligence/nextgen\\_crypto.html](http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html)

En choisissant la configuration NGC, assurez-vous que logiciel client et support matériel de headend il. Les Routeurs 2 et ASR 1000 de génération ISR sont recommandés comme headends en raison de leur support matériel pour NGC.

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

## [Informations connexes](#)

- [Site-site VPN de PKI de Cisco ASA IKEv2](#)
- [IKEv2 Site2-Site met au point sur l'IOS](#)
- [FlexVPN/IKEv2 : Élément de Windows 7 - Client : Headend IOS : Partie I - Authentification de certificat](#)
- [FlexVPN et guide de configuration de version 2 d'échange de clés Internet \(IKE\), version de Cisco IOS 15.2M&T](#)
- [Support et documentation techniques - Cisco Systems](#)