

ASA/PIX 8.x : Autorisation RADIUS (ACS 4.x) pour l'accès VPN utilisant l'ACL téléchargeable avec l'exemple de configuration CLI et ASDM

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Produits connexes](#)

[Conventions](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurez l'Accès à distance VPN \(IPSec\)](#)

[Configurer ASA/PIX avec CLI](#)

[Configuration de Client VPN Cisco](#)

[Configurez ACS pour l'ACL téléchargeable pour l'utilisateur individuel](#)

[Configurez ACS pour l'ACL téléchargeable pour le groupe](#)

[Configurez les configurations de RAYON IETF pour un groupe d'utilisateurs](#)

[Vérifiez](#)

[Affichez les cryptos commandes](#)

[ACL téléchargeable pour l'utilisateur/groupe](#)

[ACL de Filtre-id](#)

[Dépannez](#)

[Suppression des associations de sécurité](#)

[Dépannage des commandes](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment configurer l'apppliance de sécurité pour authentifier des utilisateurs pour l'accès au réseau. Puisque vous pouvez implicitement activer des autorisations RADIUS, cette section ne contient aucun renseignement sur la configuration de l'autorisation RADIUS sur l'apppliance de sécurité. Elle fournit néanmoins des renseignements sur la façon dont l'apppliance de sécurité gère les renseignements de liste d'accès reçus des serveurs RADIUS.

Vous pouvez configurer un serveur de RAYON pour télécharger une liste d'accès aux dispositifs de sécurité ou un nom de liste d'accès au moment de l'authentification. L'utilisateur est autorisé à faire seulement ce qui est permis dans la liste d'accès d'utilisateur-particularité.

Les Listes d'accès téléchargeables sont les moyens les plus extensibles quand vous employez le Cisco Secure ACS pour fournir les Listes d'accès appropriées pour chaque utilisateur. Pour plus d'informations sur les caractéristiques téléchargeables de liste d'accès et le Cisco Secure ACS, référez-vous à [configurer un serveur de RAYON pour envoyer les listes de contrôle d'accès téléchargeables](#) et l'[IP téléchargeable ACLs](#).

Référez-vous à [ASA 8.3 et plus tard : Autorisation RADIUS \(ACS 5.x\) pour l'accès VPN utilisant l'ACL téléchargeable avec l'exemple de configuration CLI et ASDM](#) pour la configuration identique sur Cisco ASA avec des versions 8.3 et ultérieures.

[Conditions préalables](#)

[Conditions requises](#)

Ce document suppose que l'ASA est complètement opérationnel et configuré pour permettre au Cisco ASDM ou CLI d'apporter des modifications de configuration.

Remarque: Référez-vous à [Permettre l'accès HTTPS pour l'ASDM](#) ou [PIX/ASA 7.x : SSH dans l'exemple de configuration d'interface interne et externe](#) pour permettre au périphérique d'être configuré à distance par l'ASDM ou Secure Shell (SSH).

[Composants utilisés](#)

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

- Logiciel Cisco Adaptive Security Appliance versions 7.x et ultérieures
- Version 5.x et ultérieures de Cisco Adaptive Security Device Manager
- Client VPN Cisco Versions 4.x et ultérieures
- Cisco Secure Access Control Server 4.x

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

[Produits connexes](#)

Vous pouvez également utiliser cette configuration avec le dispositif de sécurité Cisco PIX Versions 7.x et ultérieures.

[Conventions](#)

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

[Informations générales](#)

Vous pouvez employer IP téléchargeable ACLs pour créer des ensembles de définitions d'ACL

que vous pouvez s'appliquer à beaucoup d'utilisateurs ou de groupes d'utilisateurs. Ces ensembles de définitions d'ACL s'appellent le contenu d'ACL. En outre, quand vous incorporez NAFs, vous contrôlez le contenu d'ACL qui sont envoyés au client d'AAA duquel un utilisateur recherche l'accès. C'est-à-dire, un ACL IP téléchargeable comporte un ou plusieurs définitions de contenu d'ACL, qui est associé avec NAF ou (par défaut) associé à tout l'AAA des clients. NAF contrôle l'applicabilité du contenu spécifié d'ACL selon l'adresse IP du client d'AAA. Pour plus d'informations sur NAFs et comment ils règlent IP téléchargeable ACLs, voyez [au sujet des filtres d'accès au réseau](#).

IP téléchargeable ACLs actionnent de cette façon :

1. Quand ACS accorde un accès client au réseau, ACS détermine si un ACL IP téléchargeable est assigné à cet utilisateur ou au groupe de l'utilisateur.
2. Si ACS localise un ACL IP téléchargeable qui est assigné à l'utilisateur ou au groupe de l'utilisateur, il détermine si une entrée de contenu d'ACL est associée avec le client d'AAA qui a envoyé la demande d'authentification de RAYON.
3. ACS envoie, en tant qu'élément de la session d'utilisateur, d'un paquet d'acceptation d'accès de RAYON, d'un attribut qui spécifie ACL Désigné, et de la version d'ACL Désigné.
4. Si le client d'AAA répond qu'il n'a pas la version en cours de l'ACL dans son cache, c.-à-d., l'ACL est nouveau ou a changé, ACS envoie l'ACL (nouveau ou mis à jour) au périphérique.

IP téléchargeable ACLs sont une alternative à la configuration d'ACLs dans l'attribut [26/9/1] de Cisco-poids du commerce-paires de Cisco de RAYON de chaque utilisateur ou groupe d'utilisateurs. Vous pouvez créer un ACL IP téléchargeable une fois, lui donnez un nom, et puis assignez l'ACL IP téléchargeable à chaque utilisateur ou groupe d'utilisateurs applicable si vous mettez en référence son nom. Cette méthode est plus efficace que si vous configurez l'attribut de Cisco-poids du commerce-paires de Cisco de RAYON pour chaque utilisateur ou groupe d'utilisateurs.

De plus, quand vous utilisez NAFs, vous pouvez s'appliquer le contenu différent d'ACL au même utilisateur ou groupe d'utilisateurs en vue de le client d'AAA qu'ils utilisent. Aucune configuration supplémentaire du client d'AAA n'est nécessaire après que vous ayez configuré le client d'AAA pour utiliser IP téléchargeable ACLs d'ACS. ACLs téléchargeable sont protégés par le régime de sauvegarde ou de réplication que vous avez établi.

Quand vous écrivez les définitions d'ACL dans l'interface web ACS, n'utilisez pas les entrées de mot clé ou de nom ; en outre, utilisez la syntaxe de commande d'ACL et la sémantique standard pour le client d'AAA sur lequel vous avez l'intention d'appliquer l'ACL IP téléchargeable. Les définitions d'ACL que vous écrivez dans ACS comportent un ou plusieurs commandes d'ACL. Chaque commande d'ACL doit être sur une ligne distincte.

Vous pouvez ajouter un ou plusieurs contenu Désigné d'ACL à un ACL IP téléchargeable. Par défaut, chaque contenu d'ACL applique à tout l'AAA des clients, mais, si vous avez défini NAFs, vous pouvez limiter l'applicabilité de chaque contenu d'ACL aux clients d'AAA qui sont répertoriés dans NAF que vous associez à elle. C'est-à-dire, quand vous utilisez NAFs, vous pouvez faire chaque contenu d'ACL, dans un ACL IP téléchargeable simple, applicable à de plusieurs différents périphériques ou à groupes de périphériques réseau de réseau selon votre stratégie de sécurité des réseaux.

En outre, vous pouvez changer la commande du contenu d'ACL dans un ACL IP téléchargeable. ACS examine le contenu d'ACL, à partir du dessus de la table, et télécharge le premier contenu d'ACL qu'elle trouve avec NAF qui inclut le client d'AAA qui est utilisé. Quand vous placez la commande, vous pouvez assurer l'efficacité de système si vous placez le plus largement le

contenu applicable d'ACL plus élevé sur la liste. Vous devez vous rendre compte que, si vos NAFs incluent des populations de clients d'AAA qui se chevauchent, vous devez procéder à partir du plus spécifique au plus général. Par exemple, ACS en téléchargement n'importe quel contenu d'ACL avec les Tout-AAA-clients NAF plaçant et ne considère pas qui sont inférieurs sur la liste.

Afin d'utiliser un ACL IP téléchargeable sur un client particulier d'AAA, le client d'AAA doit suivre ces directions :

- RAYON d'utilisation pour l'authentification
- IP téléchargeable ACLs de support

Ce sont des exemples des périphériques de Cisco qui prennent en charge IP téléchargeable ACLs :

- ASA et périphériques PIX
- Concentrateurs VPN série 3000
- Périphériques de Cisco qui exécutent la version IOS 12.3(8)T ou plus tard

C'est un exemple du format que vous devez employer pour écrire VPN 3000/ASA/PIX 7.x+ ACLs dans la case de définitions d'ACL :

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

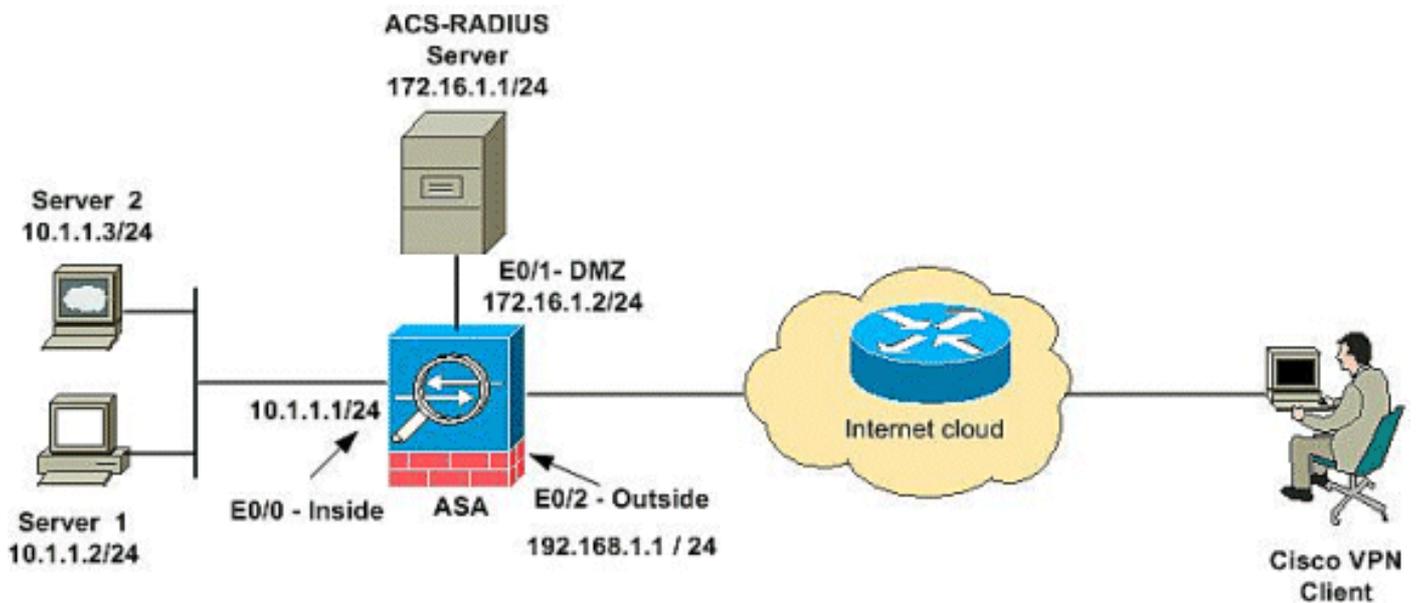
[Configurez](#)

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'[Outil de recherche de commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

[Diagramme du réseau](#)

Ce document utilise la configuration réseau suivante :



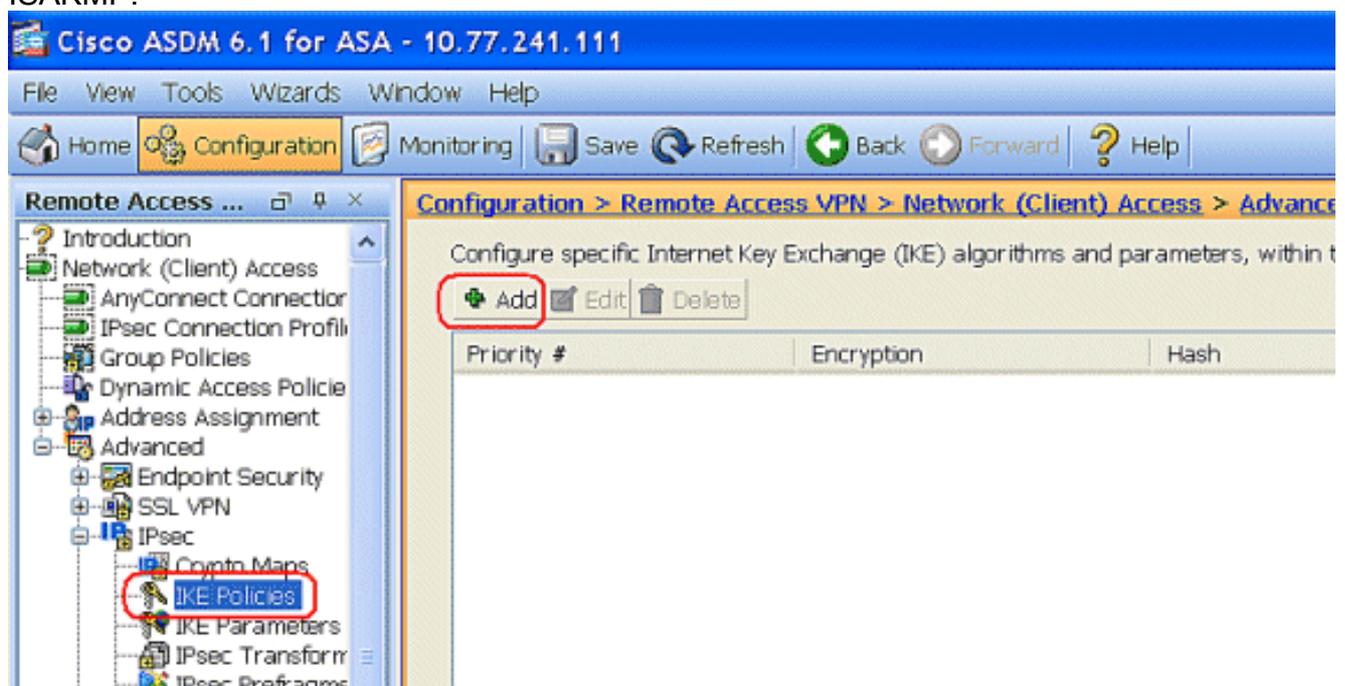
Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

[Configurez l'Accès à distance VPN \(IPSec\)](#)

Procédure ASDM

Complétez ces étapes afin de configurer le VPN d'accès à distance :

1. Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > a avancé > IPSec > IKE Policies> ajoutent** afin de créer une stratégie ISAKMP.

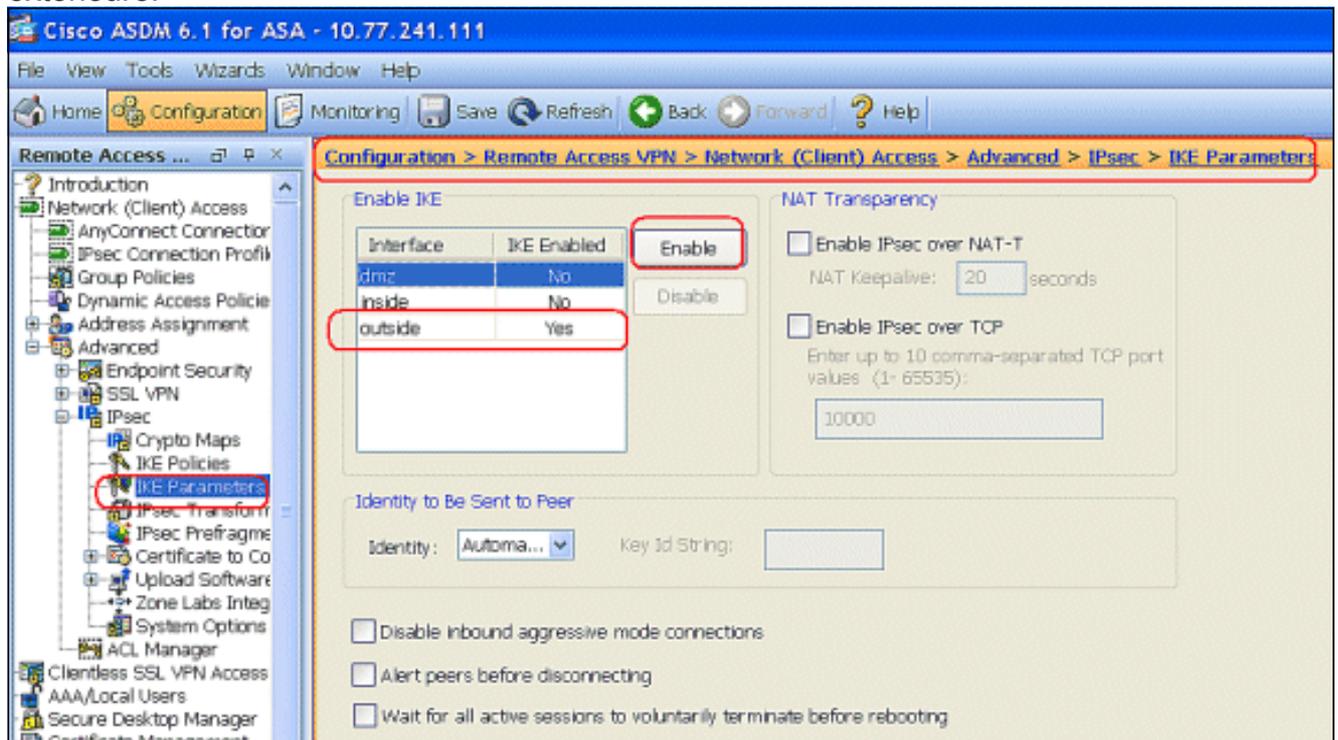


2. Fournissez les détails de stratégie ISAKMP comme affichés.



Cliquez sur **OK** et sur **Apply**.

3. Choisissez la configuration > l'Accès à distance VPN > réseau (client) Access > a avancé > IPsec > paramètres d'IKE pour activer l'IKE sur l'interface extérieure.



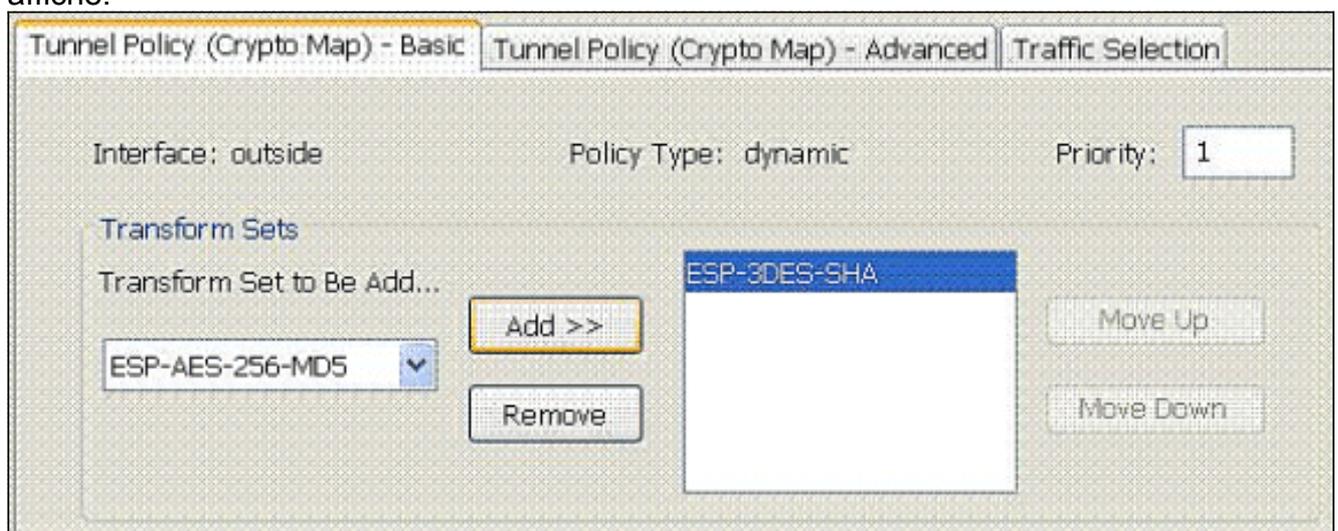
4. Choisissez la configuration > l'Accès à distance VPN > réseau (client) Access > a avancé > IPsec > jeux de transformations d'IPsec > ajoutent afin de créer le jeu de transformations ESP-3DES-SHA, comme



affiché.

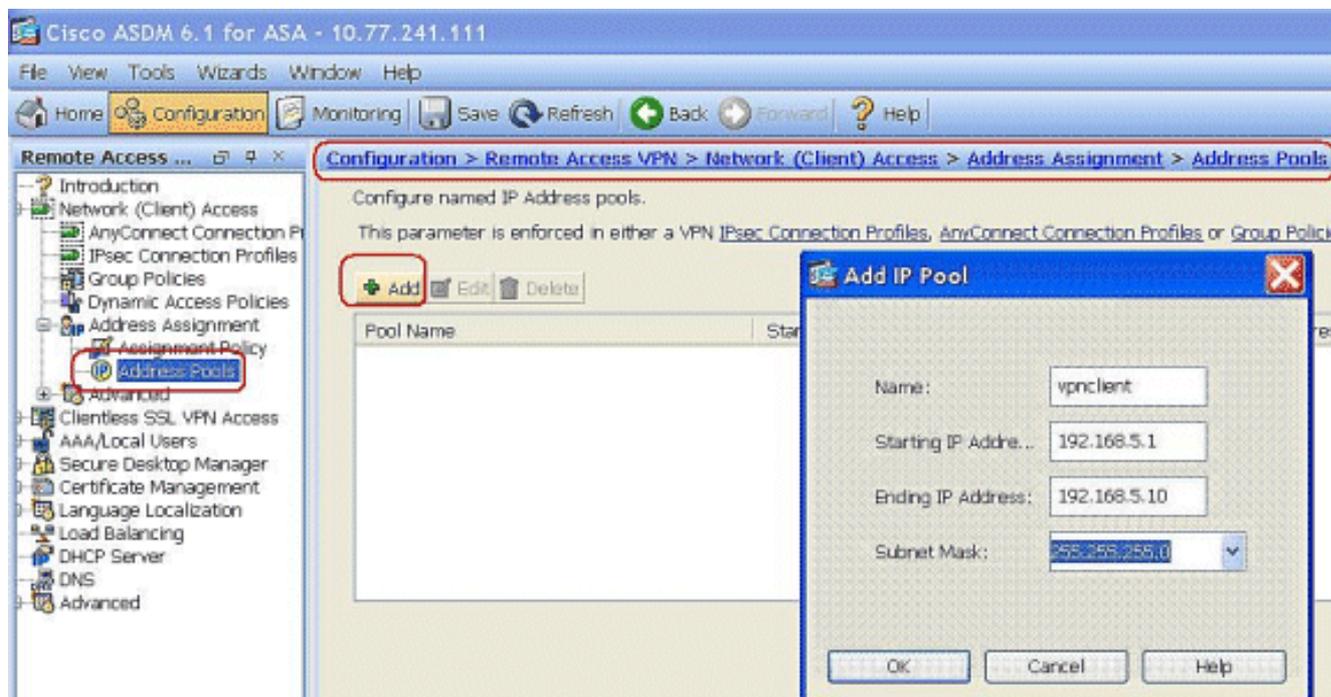
Cliquez sur **OK** et sur **Apply**.

5. Choisissez la configuration > l'Accès à distance VPN > réseau (client) Access > a avancé > IPsec > crypto map > ajoutent afin de créer un crypto map avec la stratégie dynamique de la priorité 1, comme affiché.

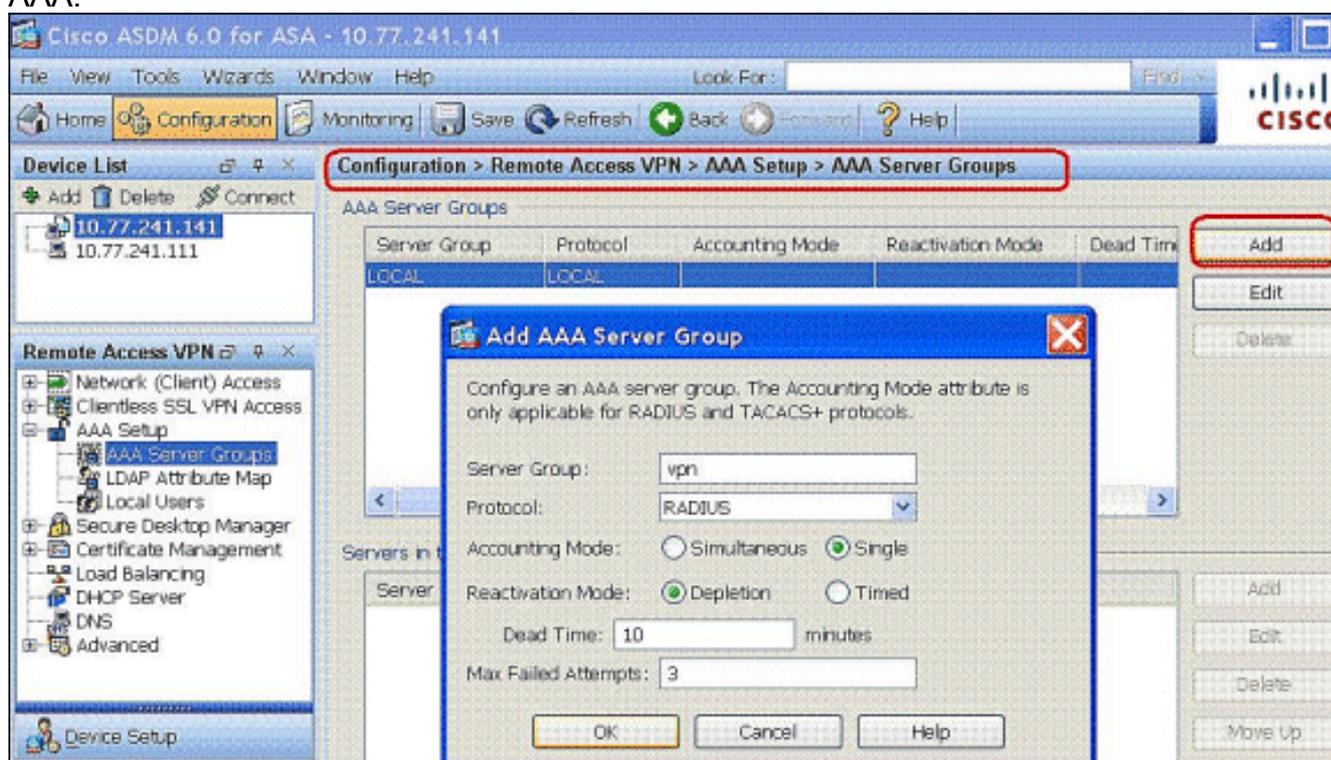


Cliquez sur **OK** et sur **Apply**.

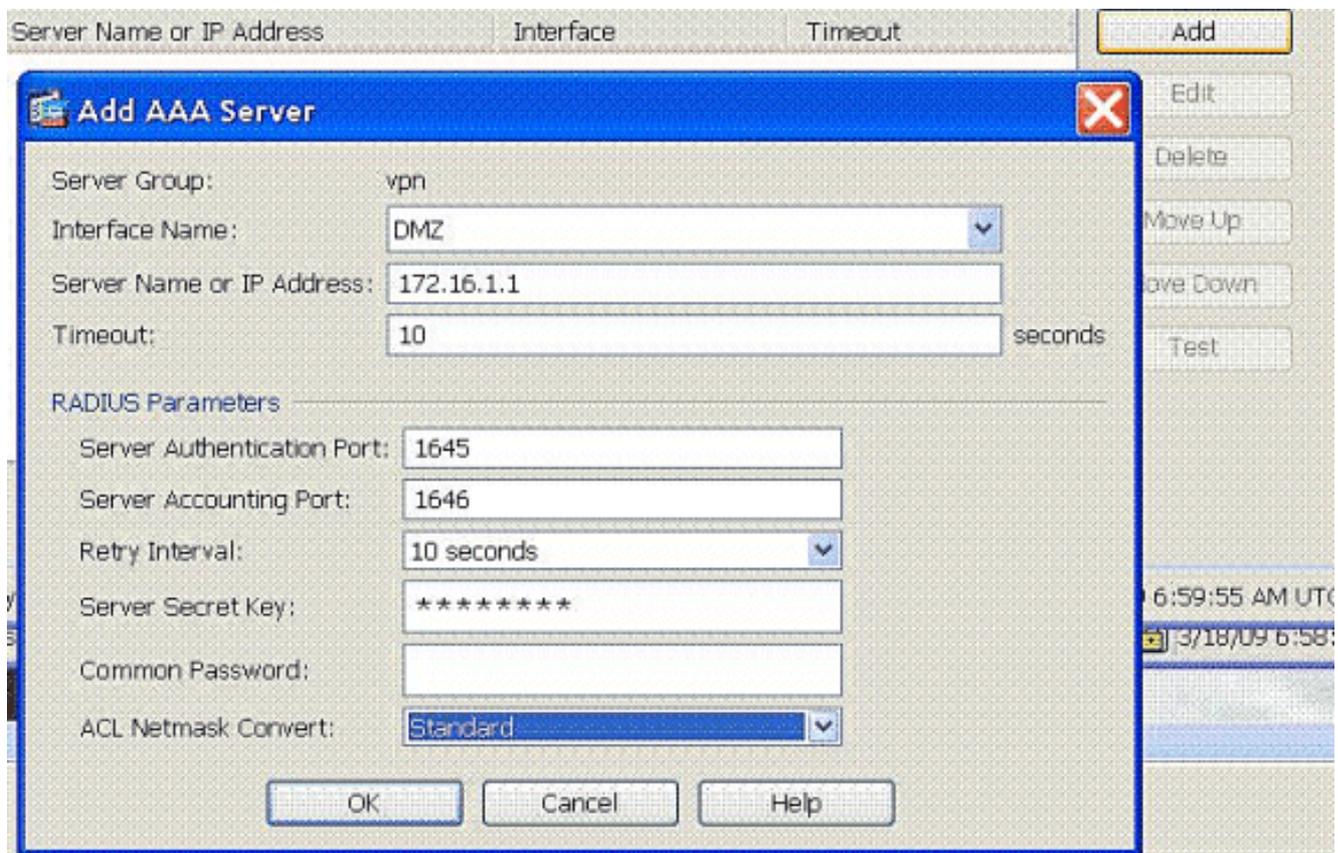
6. Choisissez la configuration > l'Accès à distance VPN > réseau (client) Access > affectation d'adresses > pools d'adresses et cliquez sur Add pour ajouter le client vpn pour les utilisateurs de client vpn.



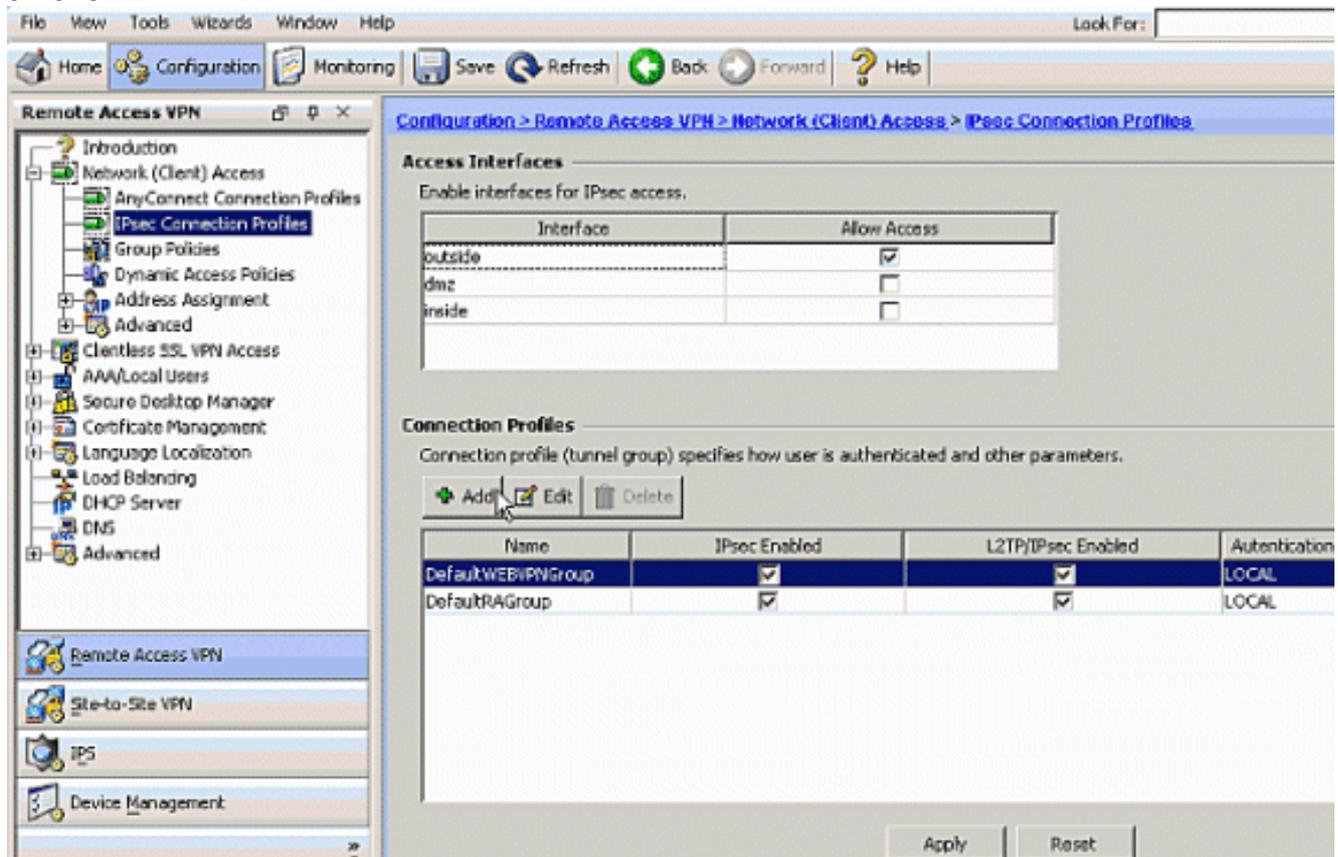
7. Choisissez la configuration > l'Accès à distance VPN > AAA installé > des Groupes de serveurs AAA et cliquez sur Add pour ajouter le nom et Protocol de Groupe de serveurs AAA.



Ajoutez l'adresse IP du serveur d'AAA (ACS) et l'interface qu'elle connecte. Ajoutez également la clé secrète de serveur dans la région de paramètres de RAYON. Cliquez sur OK.

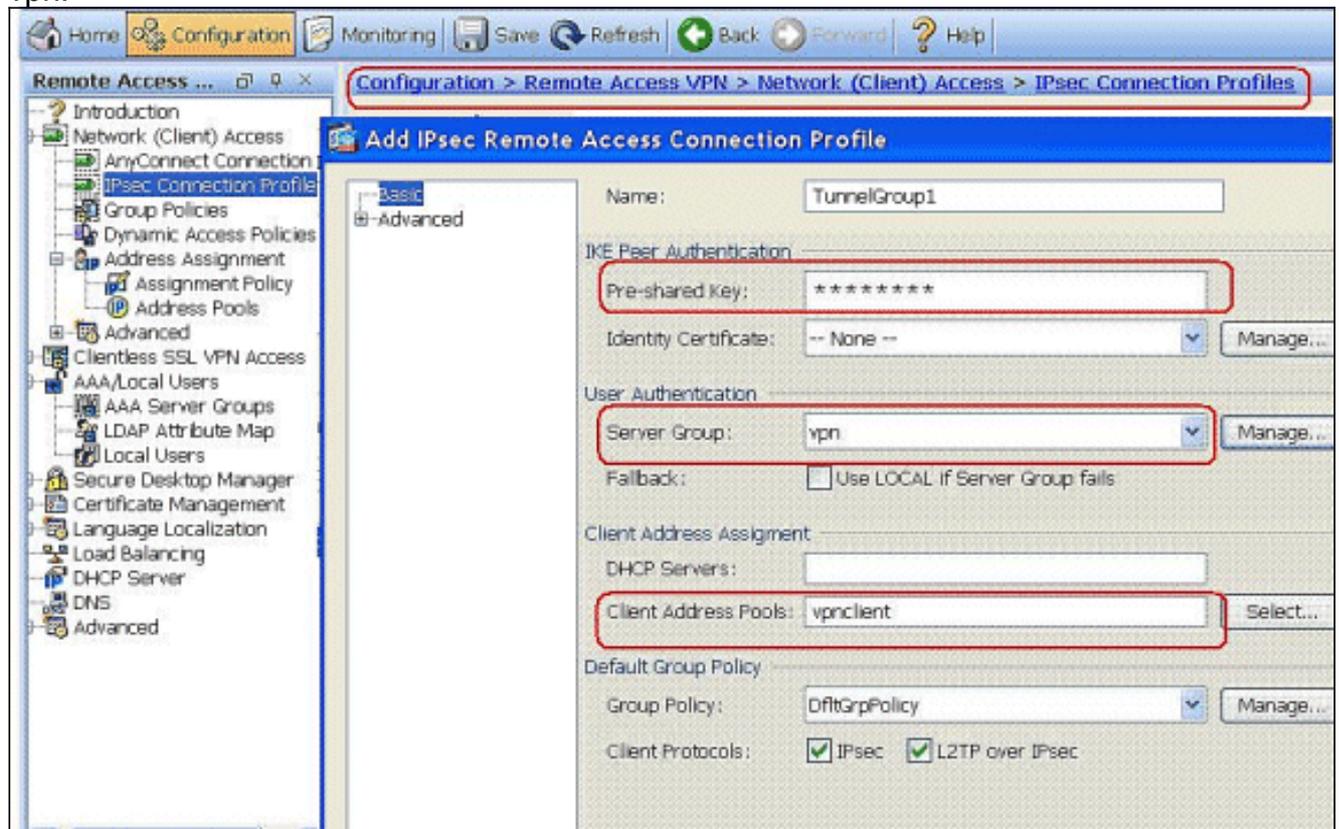


8. Choisissez la configuration > l'Accès à distance VPN > réseau (client) Access > des profils de connexion d'IPSec > ajoutent afin d'ajouter un groupe de tunnel, par exemple, TunnelGroup1 et la clé pré-partagée comme cisco123, comme affiché.



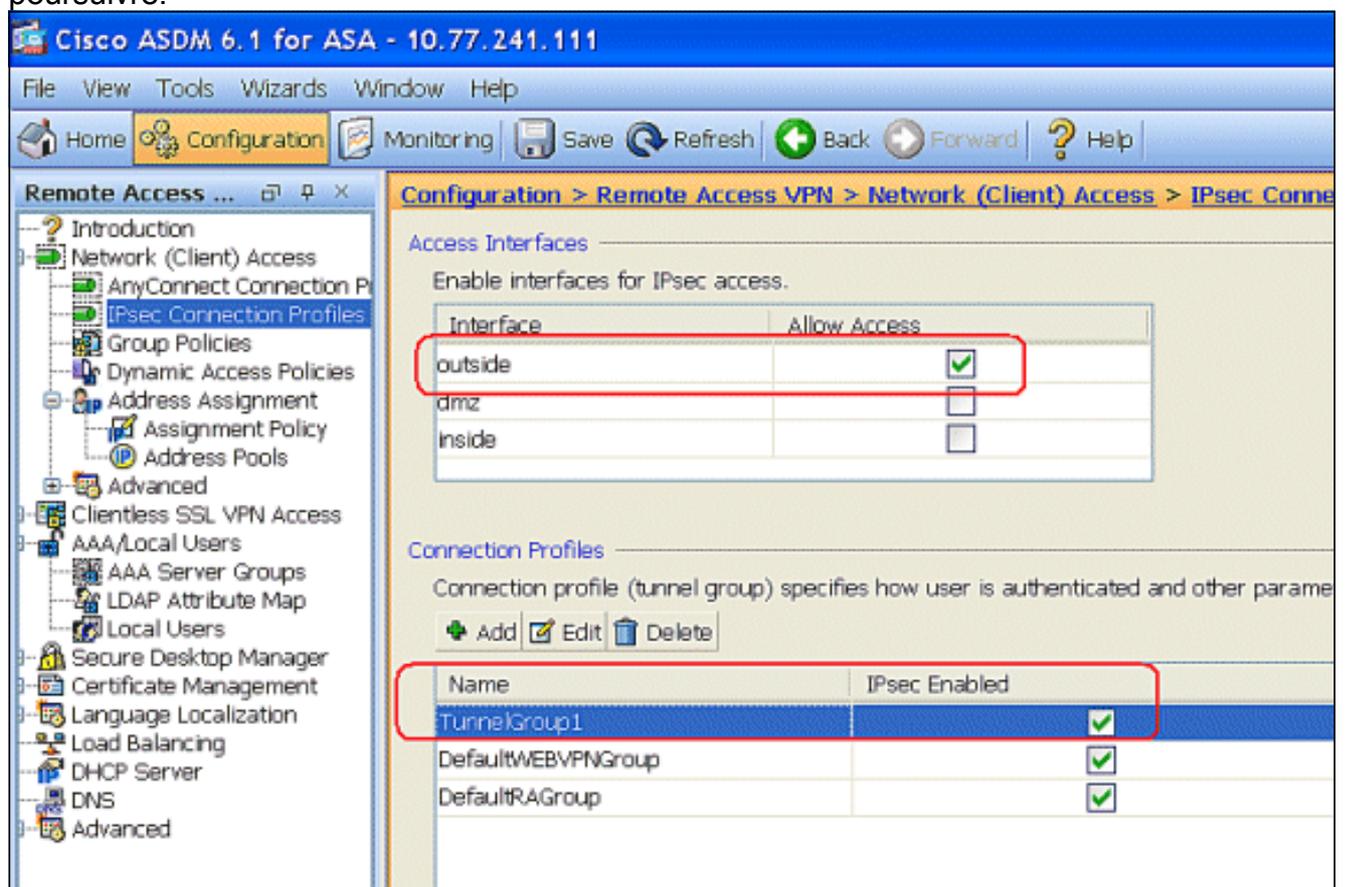
Sous l'onglet de base, choisissez le groupe de serveurs comme **vpn** pour le champ d'authentification de l'utilisateur. Choisissez **vpnclient** en tant que groupes d'adresse du client pour les utilisateurs de client

vpn.



Cliquez sur OK.

9. Activez l'interface extérieure pour IPsec Access. Cliquez sur Apply pour poursuivre.



[Configurer ASA/PIX avec CLI](#)

Terminez-vous ces étapes afin de configurer le serveur DHCP pour fournir des adresses IP aux clients vpn de la ligne de commande. Référez-vous à [Configurer les vpn d'accès à distance](#) ou [Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5505-Références de commande](#) pour plus d'informations sur chaque commande qui est utilisée.

Configuration en cours sur le périphérique ASA

```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif DMZ security-level 100 ip
address 172.16.1.2 255.255.255.0 ! interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.1
255.255.255.0 !--- Output is suppressed. passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa802-
k8.bin ftp mode passive access-list 101 extended permit
ip 10.1.1.0 255.255.255.0 192.168.5.0 255.255.255.0 !---
Radius Attribute Filter access-list new extended deny ip
any host 10.1.1.2 access-list new extended permit ip any
any pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.1-192.168.5.10
mask 255.255.255.0 no failover icmp unreachable rate-
limit 1 burst-size 1 !--- Specify the location of the
ASDM image for ASA to fetch the image for ASDM access.
asdm image disk0:/asdm-613.bin no asdm history enable
arp timeout 14400 global (outside) 1 192.168.1.5 nat
(outside) 0 access-list 101 nat (inside) 1 0.0.0.0
0.0.0.0 route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy !---
Create the AAA server group "vpn" and specify the
protocol as RADIUS. !--- Specify the CSACS server as a
member of the "vpn" group and provide the !--- location
and key. aaa-server vpn protocol radius max-failed-
attempts 5 aaa-server vpn (DMZ) host 172.16.1.1 retry-
interval 1 timeout 30 key cisco123 http server enable
http 0.0.0.0 0.0.0.0 inside no snmp-server location no
snmp-server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart !--- PHASE 2
CONFIGURATION ---! !--- The encryption types for Phase 2
are defined here. !--- A Triple DES encryption with !---
the sha hash algorithm is used. crypto ipsec transform-
set ESP-3DES-SHA esp-3des esp-sha-hmac !--- Defines a
dynamic crypto map with !--- the specified encryption
settings. crypto dynamic-map outside_dyn_map 1 set
transform-set ESP-3DES-SHA !--- Binds the dynamic map to
the IPsec/ISAKMP process. crypto map outside_map 1
ipsec-isakmp dynamic outside_dyn_map !--- Specifies the
interface to be used with !--- the settings defined in
this configuration. crypto map outside_map interface
outside !--- PHASE 1 CONFIGURATION ---! !--- This
configuration uses ISAKMP policy 2. !--- The
```

```

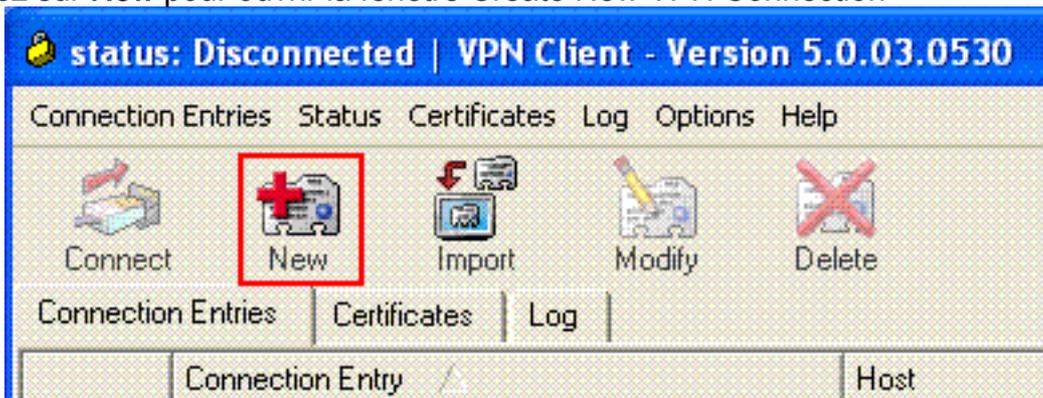
configuration commands here define the Phase !--- 1
policy parameters that are used. crypto isakmp enable
outside crypto isakmp policy 2 authentication pre-share
encryption 3des hash sha group 2 lifetime 86400 no
crypto isakmp nat-traversal telnet timeout 5 ssh timeout
5 console timeout 0 threat-detection basic-threat
threat-detection statistics access-list ! class-map
inspection_default match default-inspection-traffic !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtip inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
! group-policy DfltGrpPolicy attributes vpn-tunnel-
protocol IPsec webvpn group-policy GroupPolicy1 internal
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (VPN) with the tunnel group. tunnel-group
TunnelGroup1 type remote-access tunnel-group
TunnelGroup1 general-attributes address-pool vpnclient
authentication-server-group vpn !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#

```

Configuration de Client VPN Cisco

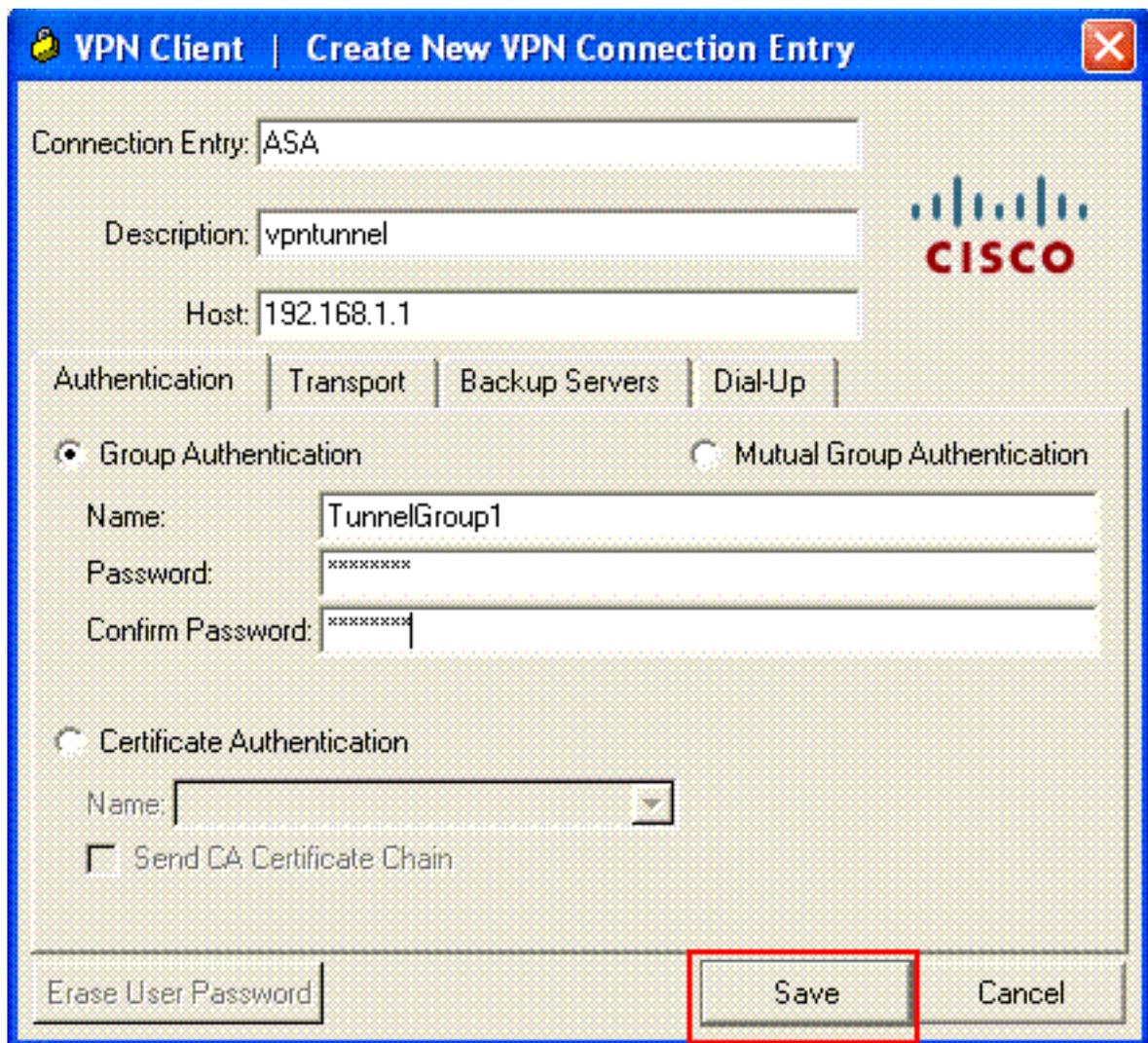
Tentez de se connecter à Cisco ASA au Client VPN Cisco afin de vérifier que l'ASA est avec succès configurée.

1. Choisissez le **début > les programmes > le client vpn de Cisco Systems > le client vpn.**
2. Cliquez sur **New** pour ouvrir la fenêtre Create New VPN Connection



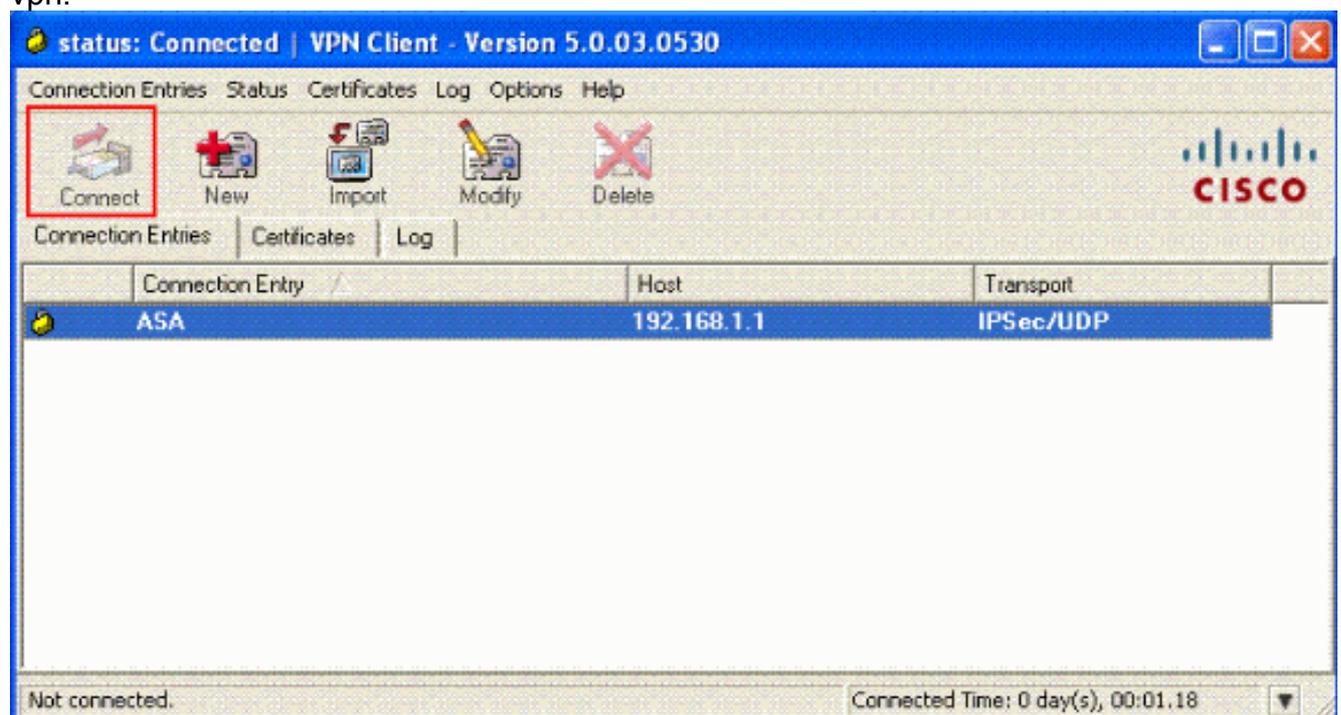
Entry.

3. Complétez les détails de votre nouvelle connexion. Entrez le nom de l'entrée de connexion avec une description. Écrivez l'**adresse IP extérieure de l'ASA** dans la case d'hôte. Entrez alors le nom de groupe de tunnel VPN (TunnelGroup1) et le mot de passe (clé pré-partagée - cisco123) comme configuré dans l'ASA. Cliquez sur

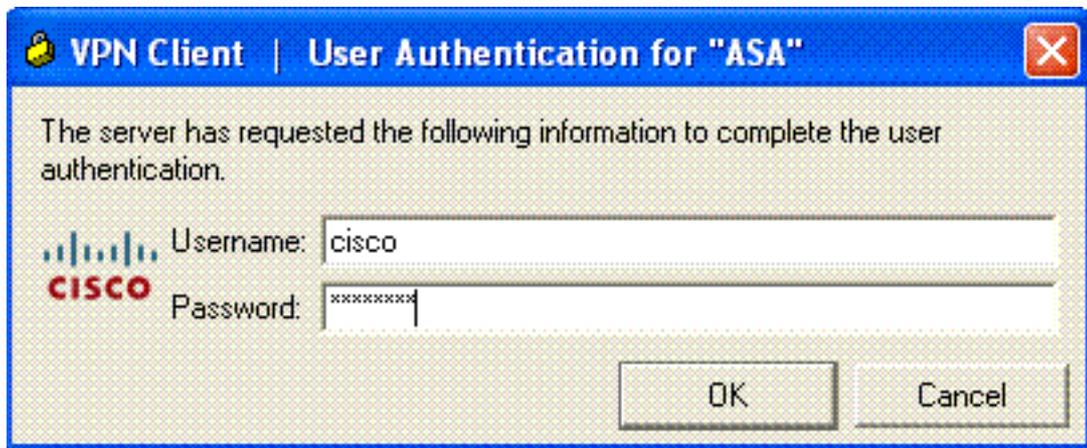


Save.

4. Cliquez sur la connexion que vous voulez utiliser, et le clic **se connectent de la fenêtre principale de client vpn.**

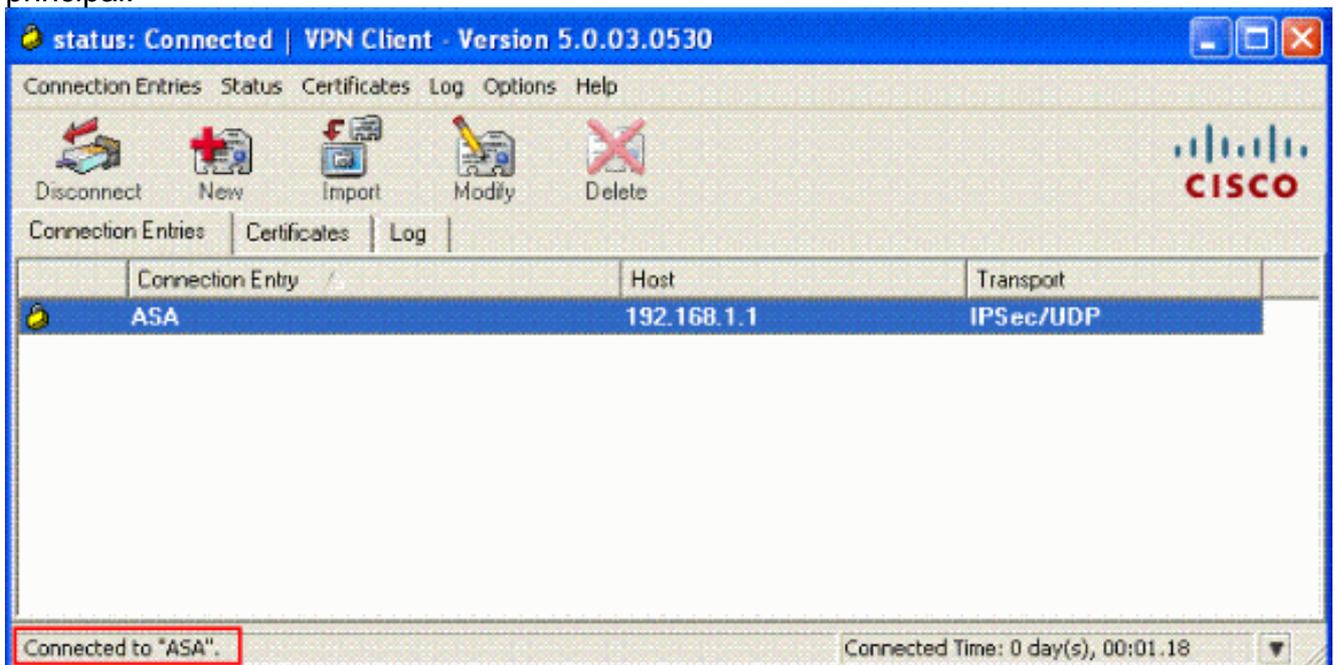


5. Une fois incité, écrivez le **nom d'utilisateur : Cisco** et **mot de passe : password1** comme configurés dans l'ASA pour le Xauth, et cliquent sur OK pour se connecter au réseau

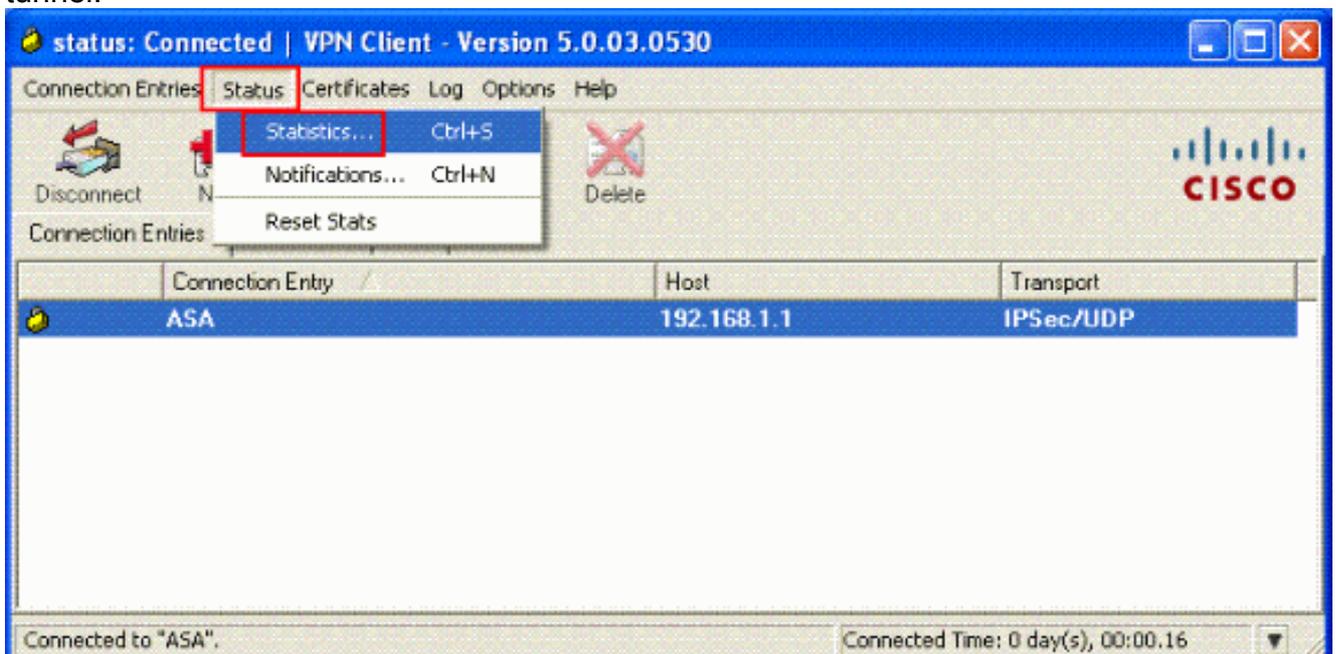


distant.

6. Le client vpn est connecté à l'ASA au lieu d'exploitation principal.



7. Une fois que la connexion est avec succès établie, choisissez les **statistiques** du menu d'état pour vérifier les détails du tunnel.



[Configurez ACS pour l'ACL téléchargeable pour l'utilisateur individuel](#)

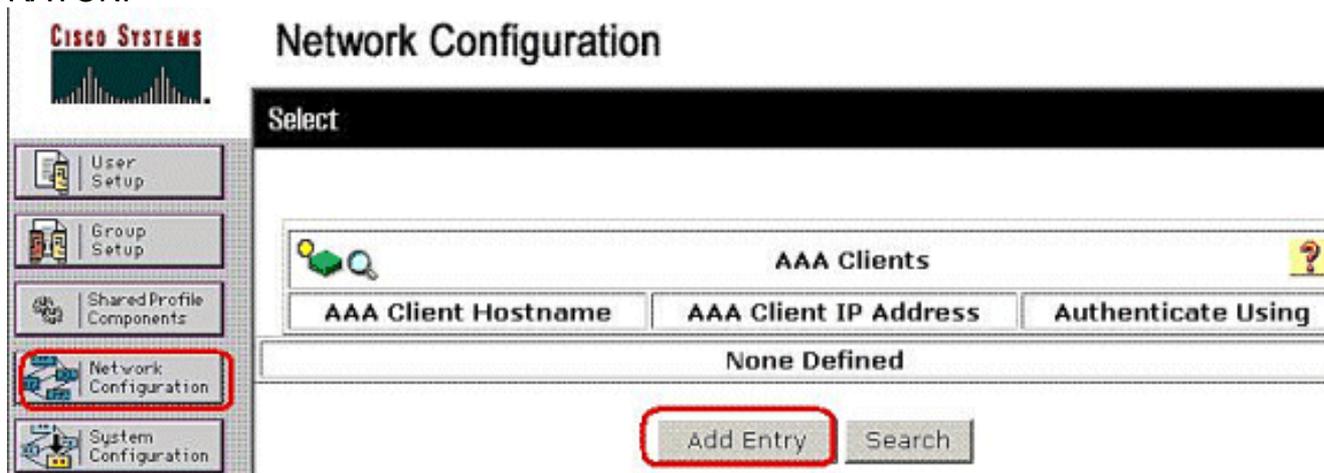
Vous pouvez configurer les Listes d'accès téléchargeables sur le Cisco Secure ACS comme un composant partagé de profil et puis assignez la liste d'accès à un groupe ou à un utilisateur individuel.

Afin d'implémenter des listes d'accès dynamique, vous devez configurer le serveur de RAYON pour le prendre en charge. Quand l'utilisateur authentifie, le serveur de RAYON envoie une liste d'accès ou un nom téléchargeable de liste d'accès aux dispositifs de sécurité. Access à un service donné est permis ou refusé à la liste d'accès. Les dispositifs de sécurité suppriment la liste d'accès quand la session d'authentification expire.

Dans cet exemple, l'utilisateur « Cisco » d'IPSec VPN authentifie avec succès, et le serveur de RAYON envoie une liste d'accès téléchargeable aux dispositifs de sécurité. L'utilisateur « Cisco » peut accéder à seulement le serveur de 10.1.1.2 et refuse tout autre accès. Afin de vérifier l'ACL, voyez l'[ACL téléchargeable pour la section d'utilisateur/groupe](#).

Terminez-vous ces étapes afin de configurer le RAYON dans un Cisco Secure ACS.

1. Choisissez la **configuration réseau** du côté gauche, et cliquez sur Add l'entrée pour ajouter une entrée pour l'ASA dans la base de données du serveur de RAYON.



2. Entrez dans 172.16.1.2 dans le domaine d'adresse IP de client, et écrivez "cisco123" pour la zone de tri secrète partagée. Choisissez le RAYON (Cisco VPN 3000/ASA/PIX 7.x+) dans l'authentifieur utilisant la liste déroulante. Cliquez sur Submit.



Network Configuration

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Add AAA Client

AAA Client Hostname

AAA Client IP Address

Shared Secret

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format

ASCII Hexadecimal

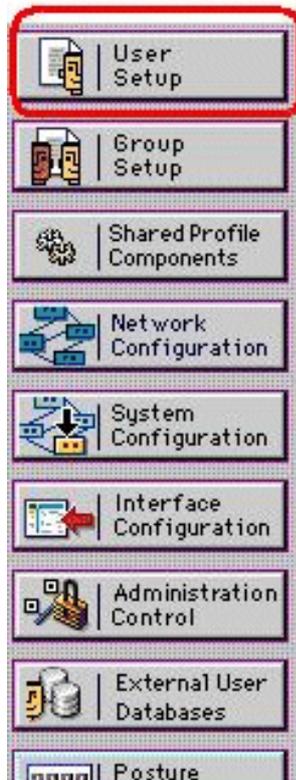
Authenticate Using

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

- Écrivez le nom d'utilisateur dans le domaine d'utilisateur dans la base de données Cisco Secure, et cliquez sur Add/l'éditez. Dans cet exemple, le nom d'utilisateur est Cisco.



User Setup



Select

User:

List users beginning with letter/number:

<u>A</u>	<u>B</u>	<u>C</u>	<u>D</u>	<u>E</u>	<u>F</u>	<u>G</u>	<u>H</u>	<u>I</u>	<u>J</u>	<u>K</u>	<u>L</u>	<u>M</u>
<u>N</u>	<u>O</u>	<u>P</u>	<u>Q</u>	<u>R</u>	<u>S</u>	<u>T</u>	<u>U</u>	<u>V</u>	<u>W</u>	<u>X</u>	<u>Y</u>	<u>Z</u>
<u>0</u>	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	<u>7</u>	<u>8</u>	<u>9</u>			

4. Dans la prochaine fenêtre, entrez le mot de passe pour « Cisco ». Dans cet exemple, le mot de passe est également **password1**. Quand vous terminez, cliquez sur Submit.



User Setup

User: cisco

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Account Disabled

Supplementary User Info 

Real Name

Description

User Setup 

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

5. Vous employez la page options avancée pour déterminer quelles options avancées l'ACS présente. Vous pouvez simplifier les pages qui paraissent dans d'autres zones de l'interface web ACS si vous masquez les options avancées que vous n'utilisez pas. Cliquez sur la **configuration d'interface**, et puis cliquez sur les **options avancées** d'ouvrir la page options avancée.



Interface Configuration

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Advanced Options ?

Note: Only the selected options will appear in the user interface.

- Per-user TACACS+/RADIUS Attributes
- User-Level Shared Network Access Restrictions
- User-Level Network Access Restrictions
- User-Level Downloadable ACLs
- Default Time-of-Day / Day-of-Week Specification
- Group-Level Shared Network Access Restrictions
- Group-Level Network Access Restrictions
- Group-Level Downloadable ACLs
- Group-Level Password Aging

Cochez la case pour le **niveau utilisateur ACLs téléchargeable** et le **niveau du groupe ACLs téléchargeable**. Niveau utilisateur ACLs téléchargeable - Une fois choisie, cette option active la section téléchargeable d'ACLs (listes de contrôle d'accès) à la page d'installation utilisateur. Niveau du groupe ACLs téléchargeable - Une fois choisie, cette option active la section téléchargeable d'ACLs à la page de Group Setup.

6. Dans la barre de navigation, cliquez sur les **composants partagés de profil**, et cliquez sur **IP téléchargeable ACLs**. Remarque: Si *IP téléchargeable ACLs* n'apparaît pas sur les composants partagés page de profil, vous devez activer le niveau utilisateur ACLs téléchargeable, l'option téléchargeable d'ACLs de niveau du groupe, ou chacun des deux sur la page options avancée de la section de configuration d'interface.



Shared Profile Components

User Setup

Group Setup

Shared Profile Components

Network Configuration

Select

- [Downloadable IP ACLs](#)
- [Network Access Filtering](#)
- [RADIUS Authorization Components](#)
- [Shell Command Authorization Sets](#)
- [PIX/ASA Command Authorization Sets](#)

7. Cliquez sur **Add**. La page téléchargeable IP ACLs

Shared Profile Components

Select

Downloadable IP ACLs	
Name	Description
None Defined	

Add

Cancel

paraît.

8. Dans la case de nom, introduisez le nom du nouvel ACL IP. **Remarque:** Le nom d'un ACL IP peut contenir jusqu'à 27 caractères. Le nom ne doit pas contenir les espaces ou l'un de ces caractères : trait d'union (-), crochet de gauche ([), crochet droit (]), slash (/), barre oblique inverse (\), devis ("), chevron gauche (<), crochet à angle droit (>), ou tiret (-). Dans la case de description, tapez une description du nouvel ACL IP. La description peut être jusqu'à 1,000

Shared Profile Components

Edit

Downloadable IP ACLs

Name:	<input type="text" value="VPN_Access"/>
Description:	<input type="text" value="Cisco VPN Client Access"/>

ACL Contents	Network Access Filtering
No ACLs	
<input type="button" value="Add"/> <input type="button" value="Up"/> <input type="button" value="Down"/>	
<input type="button" value="Back to Help"/>	

<input type="button" value="Submit"/>	<input type="button" value="Cancel"/>
---------------------------------------	---------------------------------------

caractères.

Afin d'ajouter un contenu d'ACL au nouvel ACL IP, cliquez sur Add.

9. Dans la case de nom, introduisez le nom du nouveau contenu d'ACL. **Remarque:** Le nom d'un contenu d'ACL peut contenir jusqu'à 27 caractères. Le nom ne doit pas contenir les espaces ou l'un de ces caractères : trait d'union (-), crochet de gauche ([), crochet droit (]), slash (/), barre oblique inverse (\), devis ("), chevron gauche (<), crochet à angle droit (>), ou tiret (-). Dans l'ACL les définitions enferment dans une boîte, tapent la nouvelle définition d'ACL. **Remarque:** Quand vous écrivez les définitions d'ACL dans l'interface web ACS, n'utilisez pas les entrées de mot clé ou de nom ; en revanche, commencez par une autorisation ou refusez le mot clé. Afin de sauvegarder le contenu d'ACL, cliquez sur

Shared Profile Components

Edit

Downloadable IP ACL Content

Name:

VPN_Client

ACL Definitions

```
permit ip any host 10.1.1.2  
deny ip any any
```



Back to Help

Submit

Cancel

Submit.

10. La page téléchargeable IP ACLs paraît avec le nouveau contenu d'ACL répertorié de nom dans la colonne de contenu d'ACL. Afin d'associer NAF au contenu d'ACL, choisissez NAF de la case de filtrage d'accès au réseau à la droite du nouveau contenu d'ACL. Par défaut, NAF est (des Tout-AAA-clients). Si vous n'assignez pas NAF, ACS associe le contenu d'ACL à tous les périphériques de réseau, qui est le par

Shared Profile Components

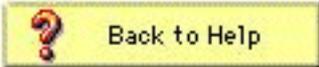
Edit

Downloadable IP ACLs

Name:

Description:

	ACL Contents	Network Access Filtering
<input checked="" type="radio"/>	VPN_Client	(All-AAA-Clients) ▼

 Back to Help

défait.

A

fin de placer la commande du contenu d'ACL, cliquez sur la case d'option pour une définition d'ACL, et puis cliquez sur **en haut ou en bas** pour la replacer dans la liste. Afin de sauvegarder l'ACL IP, cliquez sur **Submit**. **Remarque:** La commande du contenu d'ACL est significative. De haut en bas, ACS télécharge seulement la première définition d'ACL qui a NAF applicable plaçant, qui inclut la valeur par défaut de Tout-AAA-clients, si utilisé. Typiquement, votre liste de contenu d'ACL se poursuit de celui avec la plupart de NAF (le plus étroit) spécifique à celui par la plupart (des Tout-AAA-clients) de NAF général. **Remarque:** ACS entre dans le nouvel ACL IP, qui le prend effet immédiatement. Par exemple, si l'ACL IP sert avec des Pare-feu PIX, il est disponible d'être envoyé à n'importe quel Pare-feu PIX qui tente l'authentification d'un utilisateur qui a cet ACL IP téléchargeable assigné à son profil d'utilisateur ou de groupe.

11. Allez à la page d'installation utilisateur et éditez la page utilisateur. Sous la section téléchargeable d'ACLs, cliquez sur l'**ACL IP d'assigner** : case. Choisissez un ACL IP de la liste. Si vous terminez la configuration des options de compte utilisateur, cliquez sur **Submit** pour enregistrer les

User Setup

Account Disable

Never

Disable account if:

Date exceeds: Apr 15 2009

Failed attempts exceed:

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

Downloadable ACLs

Assign IP ACL: VPN_Access

options.

[Configure ACS for the downloadable ACL for the group](#)

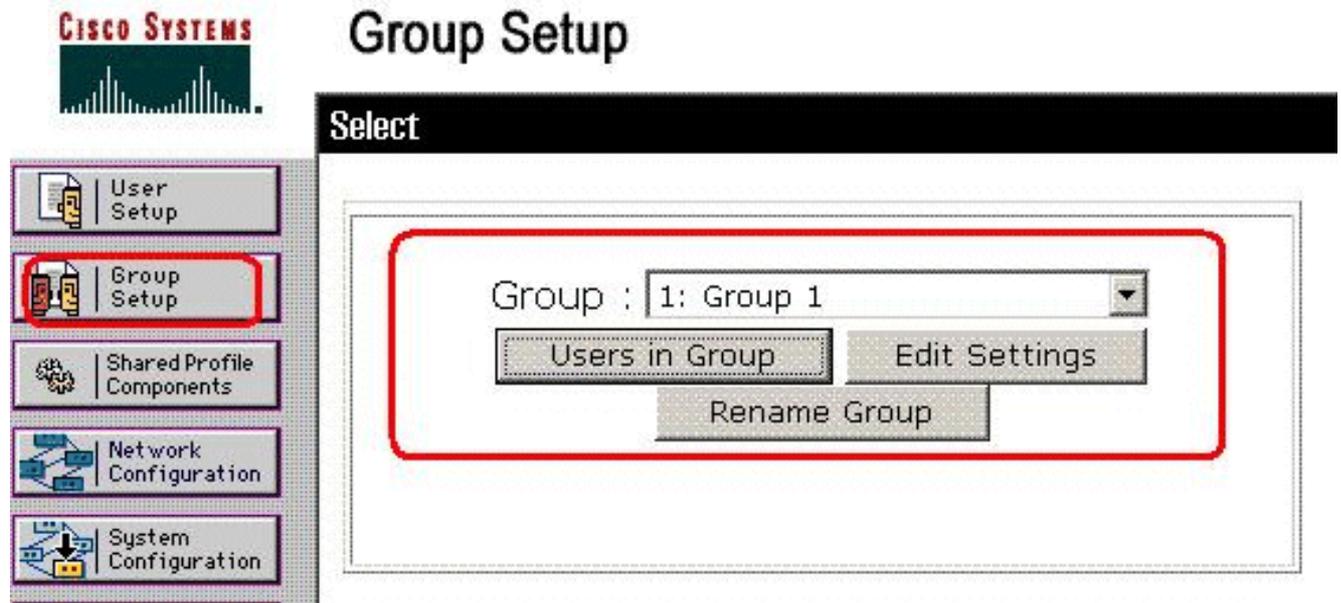
Étapes complètes 1 à 9 du [configurer ACS pour l'ACL téléchargeable pour l'utilisateur individuel](#) et suivent ces étapes afin de configurer l'ACL téléchargeable pour le groupe dans un Cisco Secure ACS.

Dans cet exemple, l'utilisateur « Cisco » d'IPSec VPN appartient aux groupes VPN. Les stratégies de groupe VPN sont appliquées pour tous les utilisateurs dans le groupe.

L'utilisateur " Cisco » de groupe VPN authentifie avec succès, et le serveur de RAYON envoie une liste d'accès téléchargeable aux dispositifs de sécurité. L'utilisateur « Cisco » peut accéder à seulement le serveur de 10.1.1.2 et refuse tout autre accès. Afin de vérifier l'ACL, référez-vous à [l'ACL téléchargeable pour la](#) section d'[utilisateur/groupe](#).

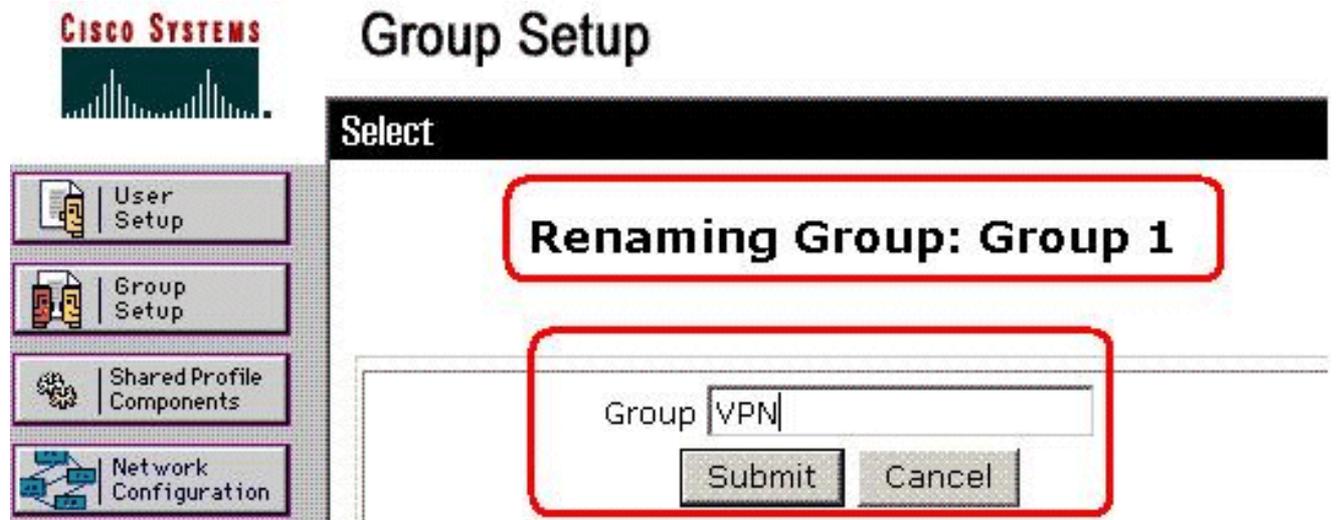
1. Dans la barre de navigation, **Group Setup** de clic. La page choisie de Group Setup

s'ouvre.



The screenshot shows the Cisco Systems logo at the top left. Below it is a navigation menu with five items: 'User Setup', 'Group Setup' (highlighted with a red box), 'Shared Profile Components', 'Network Configuration', and 'System Configuration'. The main content area is titled 'Group Setup' and contains a 'Select' header. Below the header is a form with a dropdown menu showing '1: Group 1'. Below the dropdown are three buttons: 'Users in Group', 'Edit Settings', and 'Rename Group'. A red box highlights the dropdown menu and the 'Edit Settings' button.

2. Renommez le groupe 1 au VPN, et cliquez sur Submit.

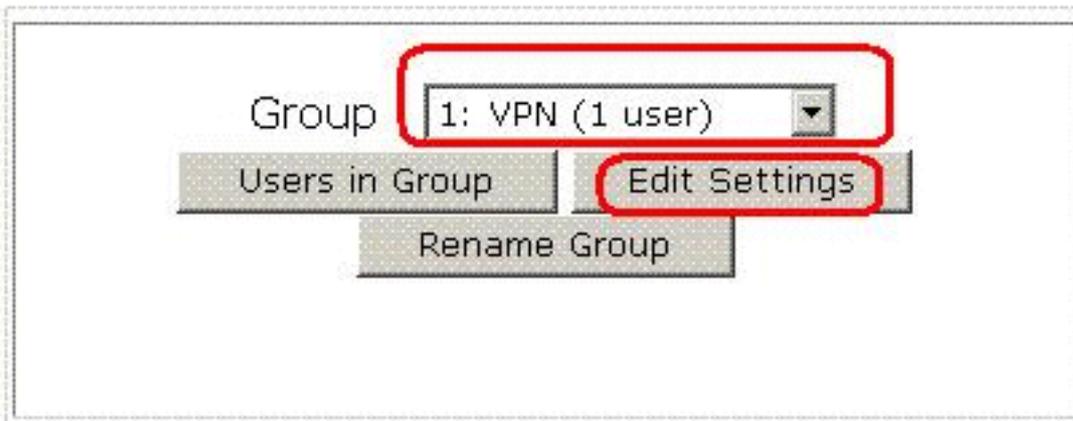


The screenshot shows the same Cisco Systems logo and navigation menu as the previous screenshot. The main content area is titled 'Group Setup' and contains a 'Select' header. Below the header is a dialog box titled 'Renaming Group: Group 1'. The dialog box has a text input field containing 'VPN' and two buttons: 'Submit' and 'Cancel'. A red box highlights the dialog box title and the input field and buttons.

3. De la liste de groupe, choisissez un groupe, et puis cliquez sur Edit les configurations.

Group Setup

Select



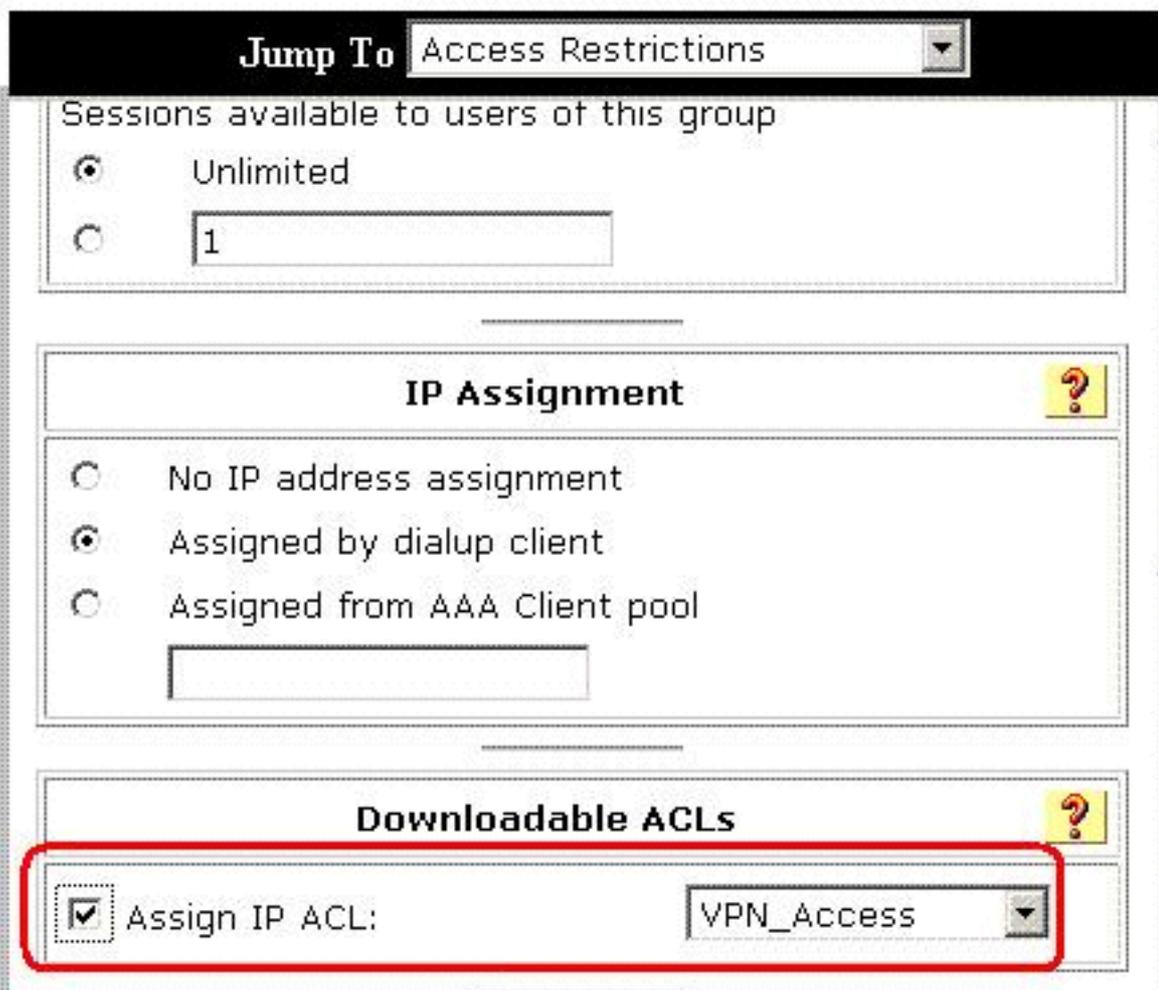
Group 1: VPN (1 user) ▼

Users in Group Edit Settings

Rename Group

4. Sous la section téléchargeable d'ACLs, cliquez sur la case d'ACL IP d'assigner. Choisissez un ACL IP de la

Group Setup



Jump To Access Restrictions ▼

Sessions available to users of this group

Unlimited

1

IP Assignment ?

No IP address assignment

Assigned by dialup client

Assigned from AAA Client pool

Downloadable ACLs ?

Assign IP ACL: VPN_Access ▼

liste.

5. Afin de sauvegarder les configurations de groupe que vous avez juste faites, cliquez sur Submit.
6. Allez à l'installation utilisateur et éditez l'utilisateur que vous voudriez ajouter dedans au

groupe : VPN. Quand vous terminez, cliquez sur Submit.

The screenshot shows the Cisco User Setup configuration interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, and External User Databases. The main area is titled 'User Setup' and contains the following fields and options:

- Password: [Redacted]
- Confirm Password: [Redacted]
- Separate (CHAP/MS-CHAP/ARAP)
- Password: [Redacted]
- Confirm Password: [Redacted]
- Text: When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.
- Group to which the user is assigned: [VPN]

Maintenant l'ACL téléchargeable configuré pour le groupe VPN est appliqué pour cet utilisateur.

7. Afin de continuer à spécifier d'autres configurations de groupe, exécutez d'autres procédures en ce chapitre, comme applicable

[Configurez les configurations de RAYON IETF pour un groupe d'utilisateurs](#)

Afin de télécharger un nom pour une liste d'accès que vous avez déjà créée sur les dispositifs de sécurité du serveur de RAYON quand un utilisateur authentifie, configurez l'attribut de filtre-id de RAYON IETF (attribut numéro 11) comme suit :

```
filter-id=acl_name
```

L'utilisateur " Cisco » de groupe VPN authentifie avec succès, et le serveur de RAYON télécharge un nom d'ACL (nouveau) pour une liste d'accès que vous avez déjà créée sur les dispositifs de sécurité. L'utilisateur « Cisco » peut accéder à tous les périphériques qui sont réseau intérieur de l'ASA **excepté le** serveur de 10.1.1.2. Afin de vérifier l'ACL, voyez la section d'[ACL de Filtre-id](#).

Selon l'exemple, l'ACL nommé **nouveau** est configuré pour filtrer dans l'ASA.

```
access-list new extended deny ip any host 10.1.1.2 access-list new extended permit ip any any
```

Ces paramètres apparaissent seulement quand ce sont vrais. Vous avez configuré

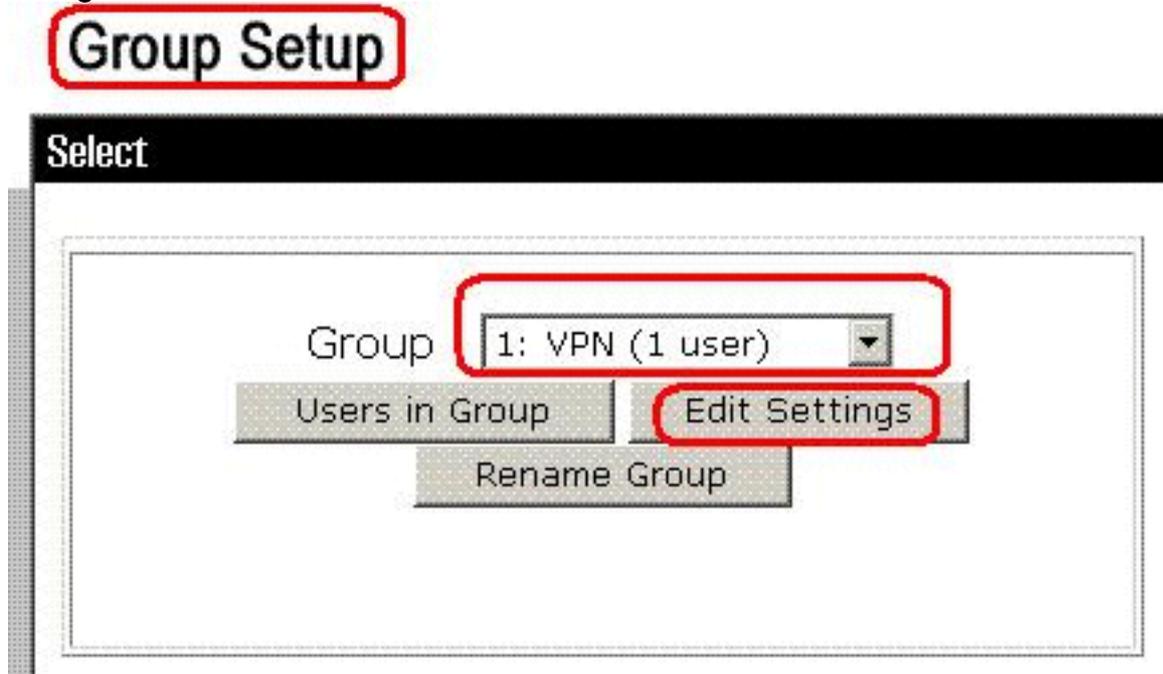
- Client d'AAA pour utiliser un des protocoles RADIUS en configuration réseau
- Attributs RADIUS de niveau du groupe à la page du RAYON (IETF) dans la section de

configuration d'interface de l'interface web

Des attributs RADIUS sont envoyés comme profil pour chaque utilisateur d'ACS au client de demande d'AAA.

Afin de configurer des configurations d'attribut RADIUS IETF pour s'appliquer comme autorisation pour chaque utilisateur dans le groupe en cours, exécutez ces actions :

1. Dans la barre de navigation, **Group Setup** de clic. La page choisie de Group Setup s'ouvre.
2. De la liste de groupe, choisissez un groupe, et puis cliquez sur Edit les configurations.



Le nom du

groupe apparaît en haut de la page Settings de groupe.

3. Défilement aux attributs RADIUS IETF. Pour chaque attribut RADIUS IETF, vous devez autoriser le groupe en cours. Cochez la case de l'attribut de Filtre-id [011], et puis ajoutez le name(new) d'ACL défini par ASA dans l'autorisation pour l'attribut dans le domaine. Référez-vous à la sortie de *configuration en cours d'exposition*

Group Setup

Jump To Access Restrictions

IETF RADIUS Attributes

[006] Service-Type

Authenticate only

[007] Framed-Protocol

Ascend MPP

[009] Framed-IP-Netmask

0.0.0.0

[010] Framed-Routing

None

[011] Filter-Id

new

[012] Framed-MTU (64..65535)

ASA.

4. Afin de sauvegarder les configurations de groupe que vous avez juste faites et les appliquer immédiatement, cliquez sur Submit et **appliquez**. **Remarque:** Afin de sauvegarder vos configurations de groupe et les appliquer plus tard, cliquez sur Submit. Quand vous êtes prêt à implémenter les modifications, choisissez la **configuration système > le contrôle des services**. Choisissez alors la **reprise**.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Affichez les cryptos commandes

- **show crypto isakmp sa** — Affiche toutes les associations de sécurité actuelles IKE (SA) sur un homologue.

```
ciscoasa# sh crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 192.168.10.2 Type : user Role : responder Rekey : no State : AM_ACTIVE ciscoasa#
```
- **show crypto ipsec sa** — Affiche les paramètres utilisés par les SA en cours.

```
ciscoasa# sh crypto ipsec sa interface: outside Crypto map tag: outside_dyn_map, seq num: 1, local addr: 192.168.1.1 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.5.1/255.255.255.255/0/0) current_peer: 192.168.10.2, username: cisco dynamic allocated peer ip: 192.168.5.1 #pkts encaps: 65, #pkts encrypt: 65, #pkts digest: 65 #pkts decaps: 65, #pkts decrypt: 65, #pkts verify: 65 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.10.2 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: EEF0EC32 inbound esp sas: spi: 0xA6F92298 (2801345176) transform: esp-3des esp-sha-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 86016, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 28647 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xEEF0EC32 (4008766514) transform: esp-3des esp-sha-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 86016, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 28647 IV size: 8 bytes replay detection support: Y
```

[ACL téléchargeable pour l'utilisateur/groupe](#)

Vérifiez l'ACL téléchargeable pour l'utilisateur Cisco. ACLs obtient téléchargé du CSACS.

```
ciscoasa(config)# sh access-list access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300 access-list 101; 1 elements access-list 101 line 1 extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0 255.255.255.0 (hitcnt=0) 0x8719a411 access-list #ACSACL#-IP-VPN_Access-49bf68ad; 2 elements (dynamic) access-list #ACSACL#-IP-VPN_Access-49bf68ad line 1 extended permit ip any host 10.1.1.2 (hitcnt=2) 0x334915fe access-list #ACSACL#-IP-VPN_Access-49bf68ad line 2 extended deny ip any any (hitcnt=40) 0x7c718bd1
```

[ACL de Filtre-id](#)

Le Filtre-id [011] s'est appliqué pour le groupe - le VPN, et les utilisateurs du groupe sont filtrés selon l'ACL (nouveau) défini dans l'ASA.

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0,
  denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0
  255.255.255.0 192.168.5.0 255.255.255.0
  (hitcnt=0) 0x8719a411
access-list new; 2 elements
access-list new line 1 extended deny ip any host 10.1.1.2 (hitcnt=4) 0xb247fec8 access-list new
line 2 extended permit ip any any (hitcnt=39) 0x40e5d57c
```

[Dépannez](#)

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration. L'exemple de sortie Debug est également affiché.

Remarque: Pour plus d'informations sur l'Accès à distance IPsec VPN de dépannage, référez-vous à [la plupart des solutions communes de dépannage VPN d'IPsec L2L et d'Accès à distance](#).

Suppression des associations de sécurité

Quand vous dépannez, veillez à autoriser les associations de sécurité existantes après que vous apportiez une modification. En mode privilégiée du PIX, utilisez les commandes suivantes :

- **clear [crypto] ipsec sa** - Supprime les SA IPsec actives. Le mot clé crypto est facultatif.
- **clear [crypto] isakmp sa** — supprime les SA IKE actives. Le mot clé crypto est facultatif.

Dépannage des commandes

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

- **debug crypto ipsec 7** — Affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp 7** — Affiche les négociations ISAKMP de la phase 1.

Informations connexes

- [Page d'assistance des appliances de sécurité adaptables de la gamme Cisco ASA 5500](#)
- [Références de commandes de Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500](#)
- [Page de support pour serveurs de sécurité de la gamme Cisco PIX 500](#)
- [Cisco Adaptive Security Device Manager](#)
- [Page de support de la négociation IPsec/des protocoles IKE](#)
- [Cisco VPN Client Support Page](#)
- [Cisco Secure Access Control Server pour Windows](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)