Configurez le VPN SSL sans client (webvpn) sur l'ASA

Contenu

Introduction

Ce document fournit une configuration simple pour la gamme 5500 de l'appliance de sécurité adaptable Cisco (ASA) afin de permettre l'accès VPN sans client de Secure Sockets Layer (SSL) aux ressources en réseau interne. Le réseau privé virtuel sans client SSL (webvpn) tient compte de limité, mais de l'objet de valeur, accès sécurisé au réseau d'entreprise de n'importe quel emplacement. Les utilisateurs peuvent réaliser l'accès basé sur navigateur sécurisé aux ressources de l'entreprise à tout moment. Aucun client supplémentaire n'est nécessaire afin d'accéder aux ressources internes. L'accès est fourni utilisant un hypertexte Transfer Protocol au-dessus de la connexion SSL.

Le VPN SSL sans client fournit sécurisé et facile d'accès à une large gamme de ressources web et des applications Web-activées et existantes à partir de presque n'importe quel ordinateur qui peut atteindre des sites d'Internet de Transfer Protocol d'hypertexte (HTTP). Ceci inclut :

- Sites Web internes
- SharePoint de Microsoft 2003, 2007, et 2010

- Accès au Web de Microsoft Outlook 2003, 2007, et 2013
- Microsoft Outlook Web App 2010
- Accès au Web de domino (DWA) 8.5 et 8.5.1
- Serveur 4.x de présentation de Citrix Metaframe
- Versions 5 à 6.5 de Citrix XenApp
- Versions 5 à 5.6 de Citrix XenDesktop, et 7.5
- Vue 4 de VMware

Une liste de logiciel pris en charge peut être trouvée dans des Plateformes prises en charge VPN, gamme de Cisco ASA 5500.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- navigateur SSL-activé
- ASA avec la version 7.1 ou supérieure
- Certificat X.509 fourni au nom de domaine ASA
- Port TCP 443, qui ne doit pas être bloqué le long du chemin entre le client et l'ASA

La liste complète de conditions requises peut être trouvée dans des Plateformes prises en charge VPN, gamme de Cisco ASA 5500.

Composants utilisés

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

- Version 9.4(1) ASA
- Version 7.4(2) d'Adaptive Security Device Manager (ASDM)
- ASA 5515-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 commencé par une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

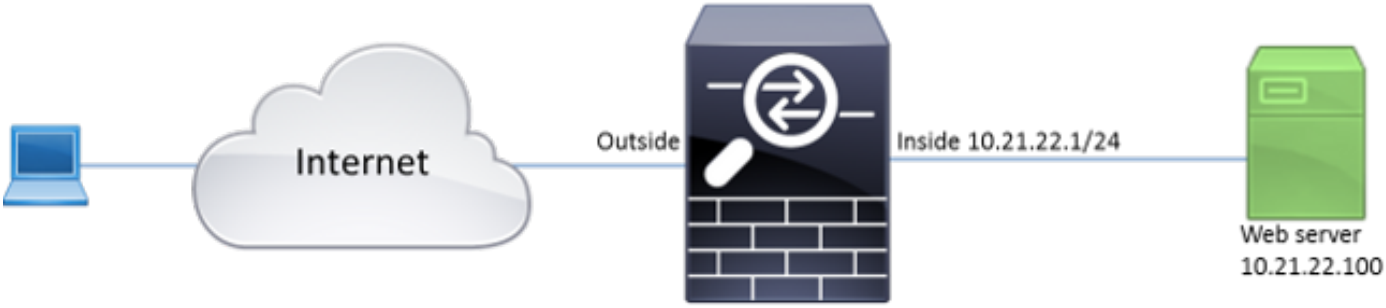
Configurez

Cet article décrit le processus de configuration pour l'ASDM et le CLI. Vous pouvez choisir de suivre l'un ou l'autre des outils afin de configurer le webvpn, mais certaines des étapes de configuration peuvent seulement être réalisées avec l'ASDM.

> **Note**: Utilisez l'outil Command Lookup Tool (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 :



Informations générales

Le webvpn emploie le protocole SSL afin de sécuriser les données transférées entre le client et le serveur. Quand le navigateur initie une connexion à l'ASA, l'ASA présente son certificat pour s'authentifier au navigateur. Afin de s'assurer que la connexion entre le client et l'ASA est sécurisée, vous devez fournir à l'ASA le certificat qui est signé par l'autorité de certification cette les confiances de client déjà. Autrement le client n'aura pas les moyens de vérifier l'authenticité de l'ASA qui a comme conséquence la possibilité de l'attaque homme-dans-le-moyenne et de l'expérience utilisateur pauvre, parce que le navigateur produit un avertissement que la connexion n'est pas faite confiance.

> **Note**: Par défaut, l'ASA génère un certificat X.509 auto-signé sur le startup. Ce certificat est utilisé afin de servir des connexions client par défaut. Il n'est pas recommandé pour utiliser ce certificat parce que son authenticité ne peut pas être vérifiée par le navigateur. En outre, ce certificat est régénéré sur chaque réinitialisation ainsi il change après chaque réinitialisation.

L'installation de certificat est hors de portée de ce document.

Configuration

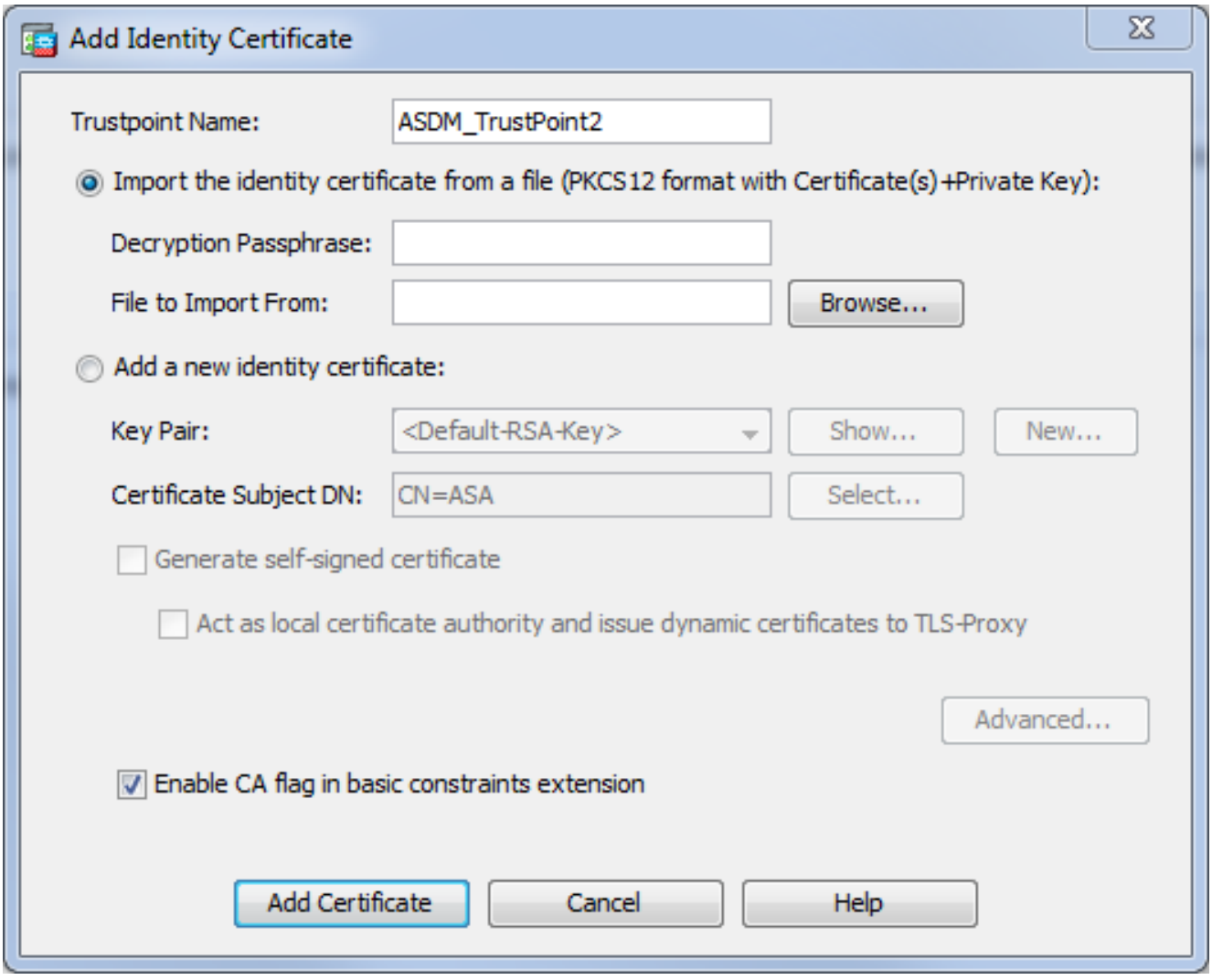
Configurez le webvpn sur l'ASA avec cinq étapes principales :

- Configurez le certificat qui sera utilisé par l'ASA.
- Activez le WebVPN sur une interface ASA.
- Créez une liste des serveurs et/ou de l'uniform resource locator (URL) pour l'accès de webvpn.
- Créez une stratégie de groupe pour les utilisateurs de WebVPN.
- Appliquez la nouvelle stratégie de groupe à un groupe de tunnels.

> **Note**: Dans des versions ASA plus tard que la version 9.4, l'algorithme utilisé pour choisir des chiffrements SSL a été changé (voir les notes en version pour la gamme de Cisco ASA, 9.4(x)).If seulement des clients curve-capables qu'elliptiques seront utilisés, puis il est sûr d'utiliser la clé privée de curve elliptique pour le certificat. Autrement la suite faite sur

commande de chiffrement devrait être utilisée afin d'éviter d'avoir le présent ASA un certificat provisoire auto-signé. Vous pouvez configurer l'ASA pour utiliser seulement des chiffrements basés sur RSA avec la commande "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-sha:des-**CBC-SHA:RC4-SHA:RC4-Md5" faite sur commande du chiffrement tlsv1.2 SSL**.

1. **Option 1** - Importez le certificat avec le fichier pkcs12.Choisissez la **configuration > le Pare-feu > a avancé > Gestion > certificats d'identité de certificat > ajoutent**. Vous pouvez l'installer avec le fichier pkcs12 ou coller le contenu dans le Privacy Enhanced Mail (PEM) formatez.

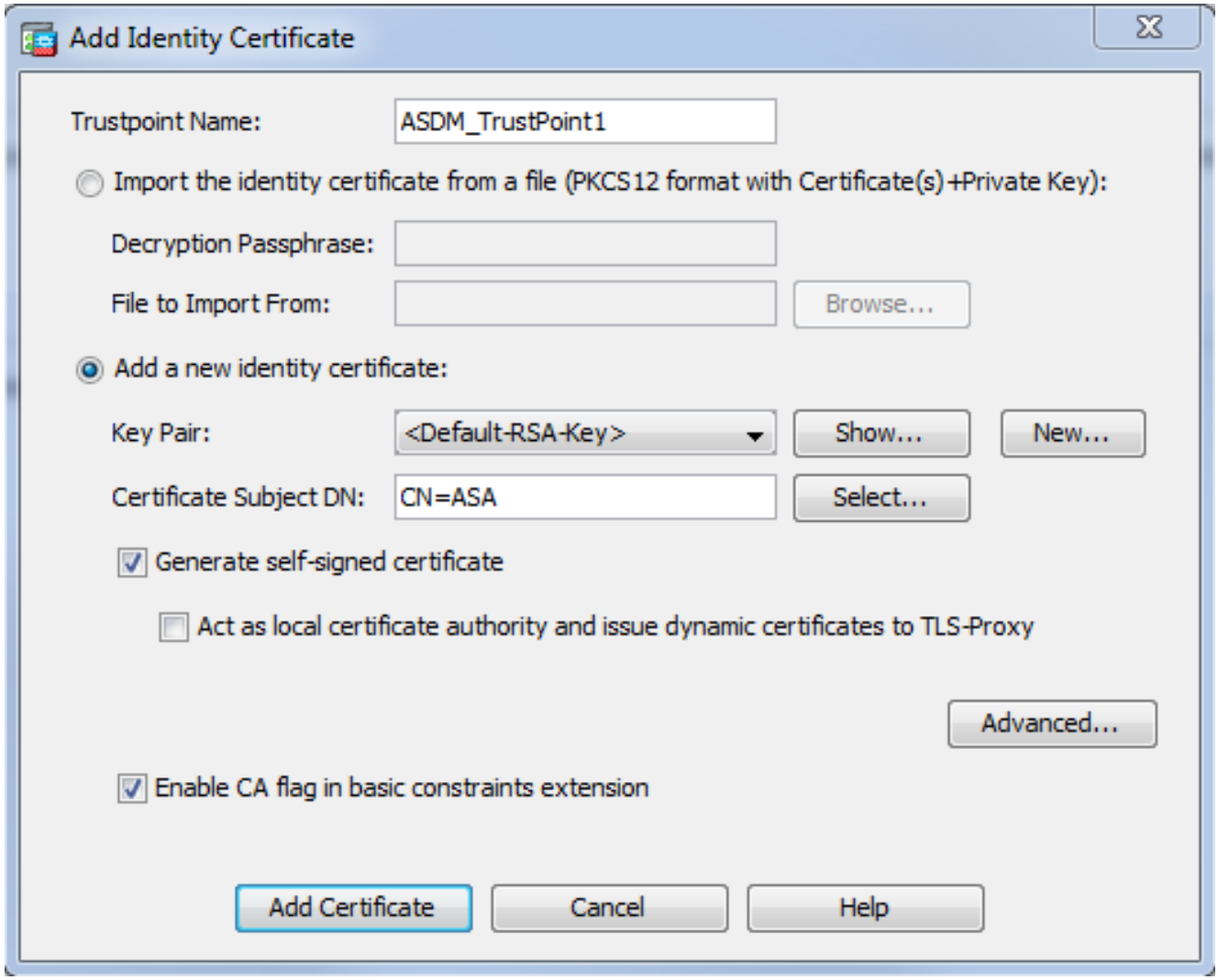


CLI :

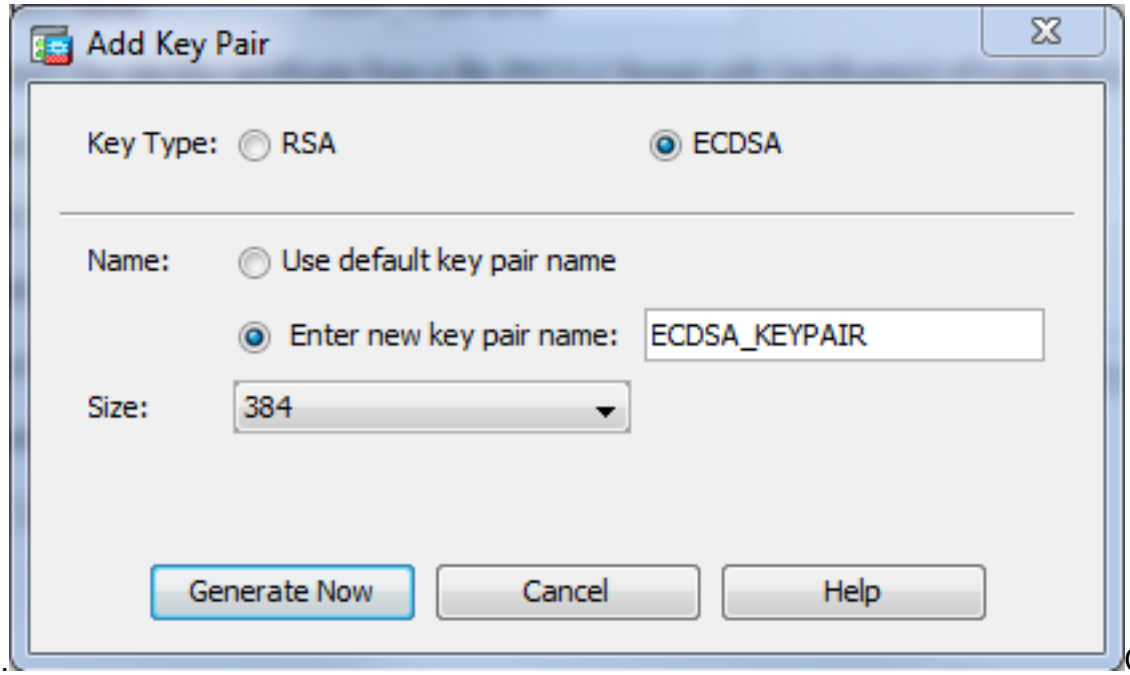
```
ASA(config)# crypto ca import TrustPoint-name pkcs12 "password"


Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCAggAgIIFuHFrV6enVflNv3sBByB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh0O7No4Ycx75Y5sOhyuQGPhLJRdionbi1s1ioe4Dplx1b


--- output ommited ---
```

```
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCAggAgIIFuHFrV6enVflNv3sBByB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh0O7No4Ycx75Y5sOhyuQGPhLJRdionbi1s1ioe4Dplx1b

quit


INFO: Import PKCS12 operation completed successfully
```

Option 2 - Créez un certificat auto-signé.Choisissez la **configuration > le Pare-feu > a avancé > Gestion > certificats d'identité de certificat > ajoutent**.Cliquez sur la case d'option **Add a new identity certificate**. Cochez la **case de certificat auto-signée Generate**. Choisissez un nom commun (NC) ce nom de domaine de correspondances de l'ASA.



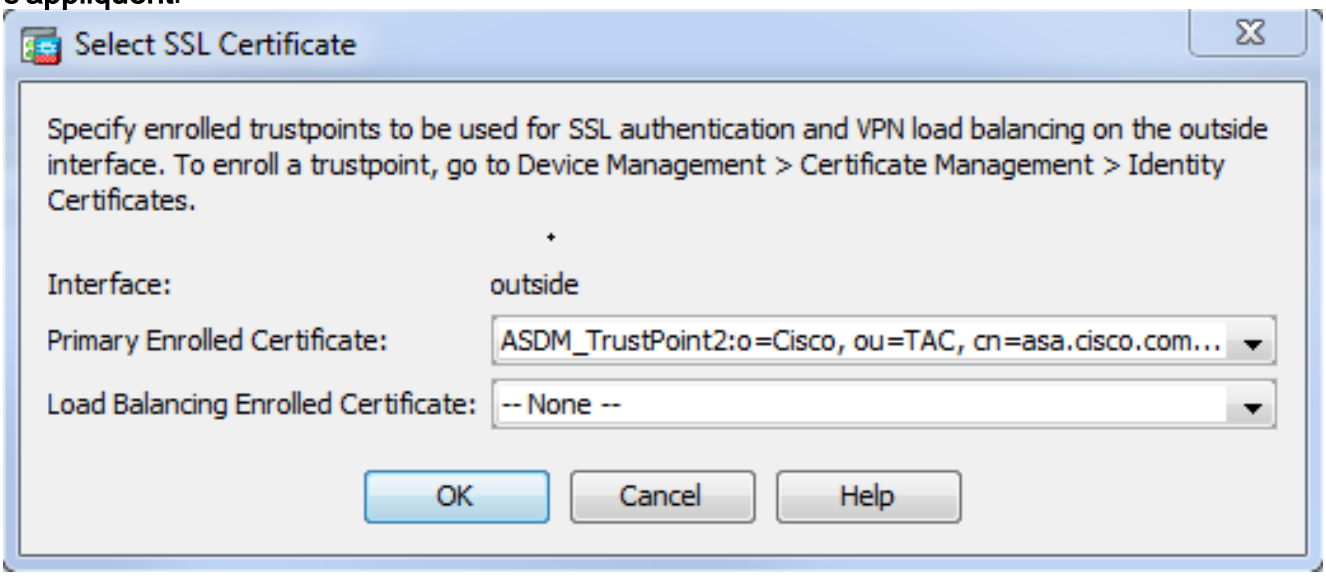
Cliquez sur New afin de créer le keypair pour le certificat. Choisissez le type, le nom, et la taille



principaux. CLI :

```
ASA(config)# crypto key generate ecdsa label ECDSA_KEYPAIR noconfirm

ASA(config)# crypto ca trustpoint TrustPoint1
ASA(config-ca-trustpoint)# revocation-check none
ASA(config-ca-trustpoint)# id-usage ssl-ipsec
ASA(config-ca-trustpoint)# no fqdn
ASA(config-ca-trustpoint)# subject-name CN=ASA
ASA(config-ca-trustpoint)# enrollment self
ASA(config-ca-trustpoint)# keypair ECDSA_KEYPAIR
ASA(config-ca-trustpoint)# exit
ASA(config)# crypto ca enroll TrustPoint1 noconfirm
```

2. Choisissez le certificat qui sera utilisé pour servir des connexions de webvpn.Choisissez la **configuration > l'Accès à distance VPN > a avancé > des configurations SSL**. Du menu de Certificats, choisissez le point de confiance associé avec le certificat désiré pour l'interface extérieure. Le clic **s'appliquent**.

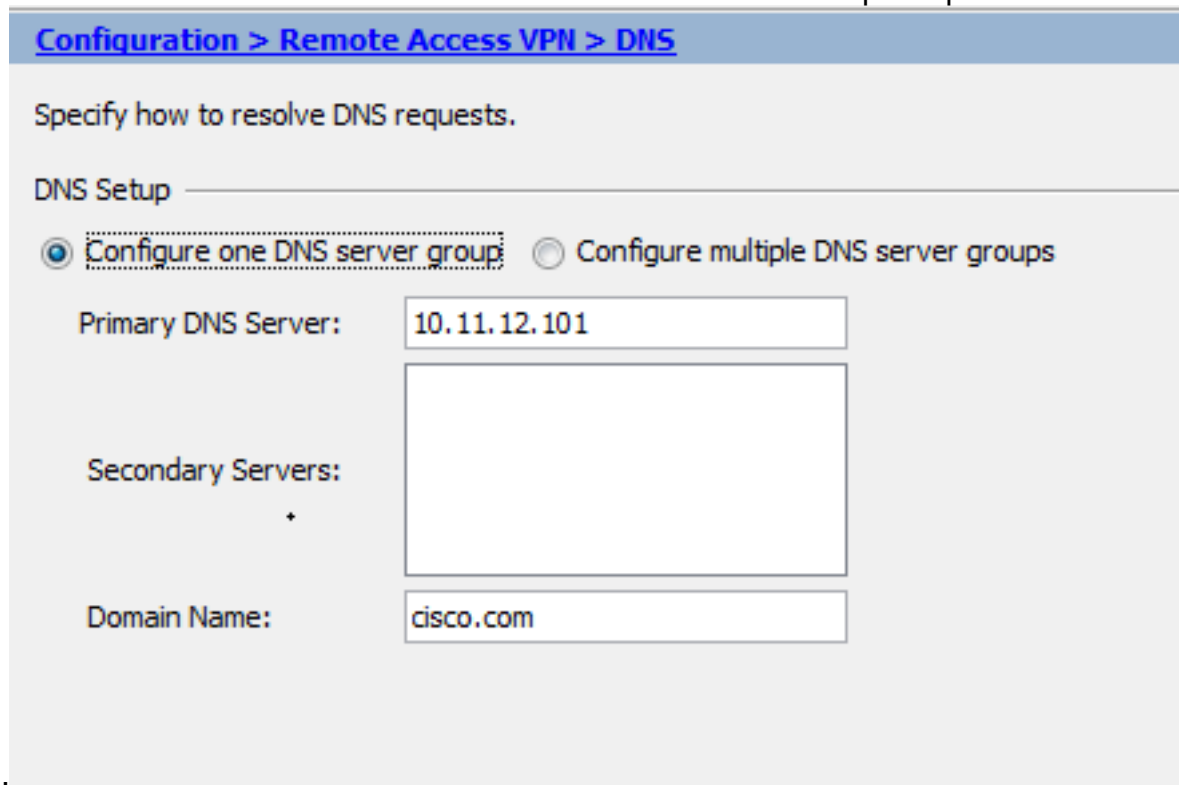


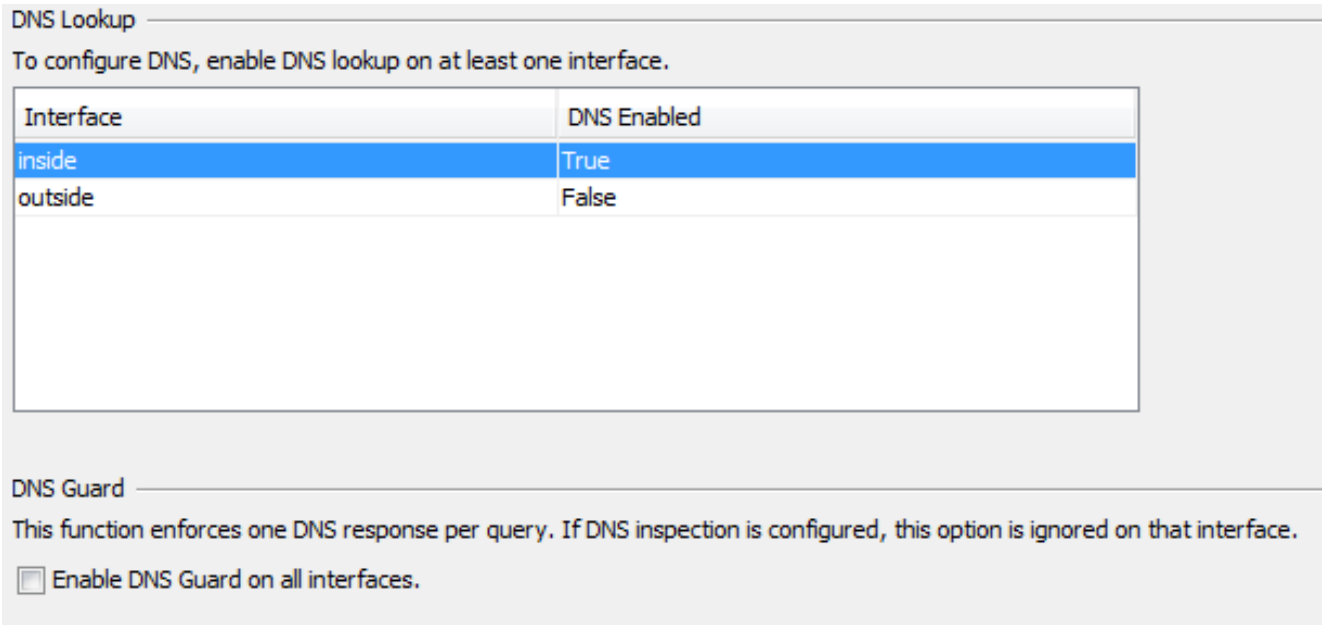
Configuration équivalente CLI :

```
ASA(config)# ssl trust-point <trustpoint-name> outside
```

3. Consultations (facultatives) de Domain Name Server d'enable (DN).Le serveur de webvpn agit en tant que proxy pour des connexions client. Il signifie que l'ASA crée des connexions aux ressources au nom du client. Si les clients ont besoin des connexions aux ressources

qui utilisent des noms de domaine, alors l'ASA doit exécuter la consultation de DN.Choisissez la **configuration > l'Accès à distance VPN > DN**.Configurez au moins les consultations de DN d'un serveur DNS et d'enable sur l'interface qui se pose au serveur DNS.

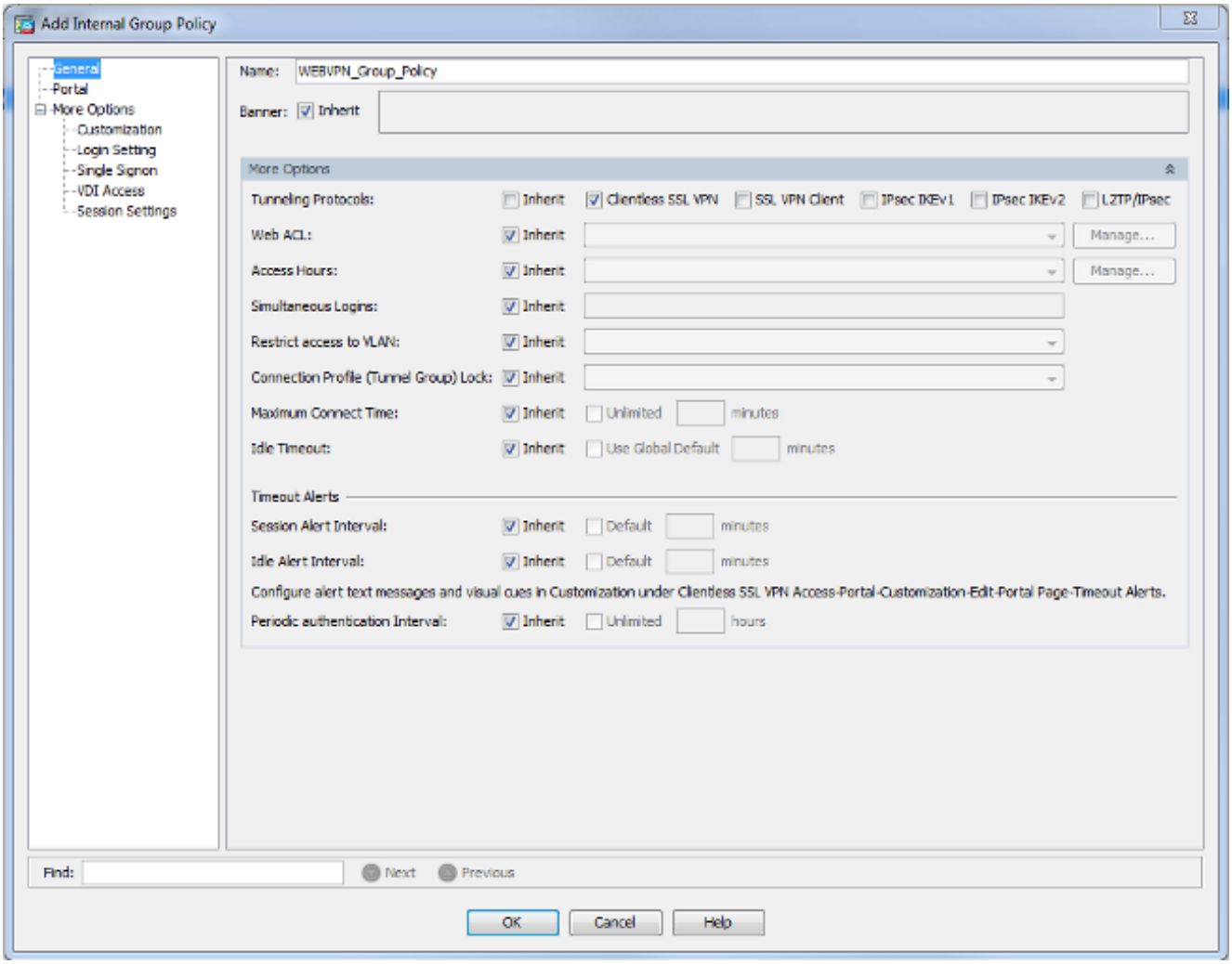




CLI :

```
ASA(config)# dns domain-lookup inside
ASA(config)# dns server-group DefaultDNS
ASA(config-dns-server-group)# name-server 10.11.12.101
```

4. (Facultatif) créez la stratégie de groupe pour des connexions de WEBVPN.Choisissez la **configuration > l'Accès à distance VPN > VPN SSL sans client Access > stratégies de groupe > Add Internal Group Policy**.Sous des options générales changez la valeur de protocoles de Tunelling « au VPN SSL sans client ».



CLI :

```
ASA(config)# group-policy WEBVPN_Group_Policy internal
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# vpn-tunnel-protocol ssl-clientless
```

5. Configurez le profil de connexion.Dans l'ASDM, choisissez la **configuration > l'Accès à distance VPN > VPN SSL sans client Access > profils de connexion**.
Pour un aperçu des profils de connexion et des stratégies de groupe, consultez le guide de configuration de la gamme VPN CLI de Cisco ASA, 9.4 - des profils de connexion, les stratégies de groupe, et les utilisateurs.Par défaut, les connexions de webvpn utilisent le profil de DefaultWEBVPNGroup. Vous pouvez créer des profils supplémentaires.**Note**: Il y a de diverses manières d'affecter des utilisateurs à d'autres profils.

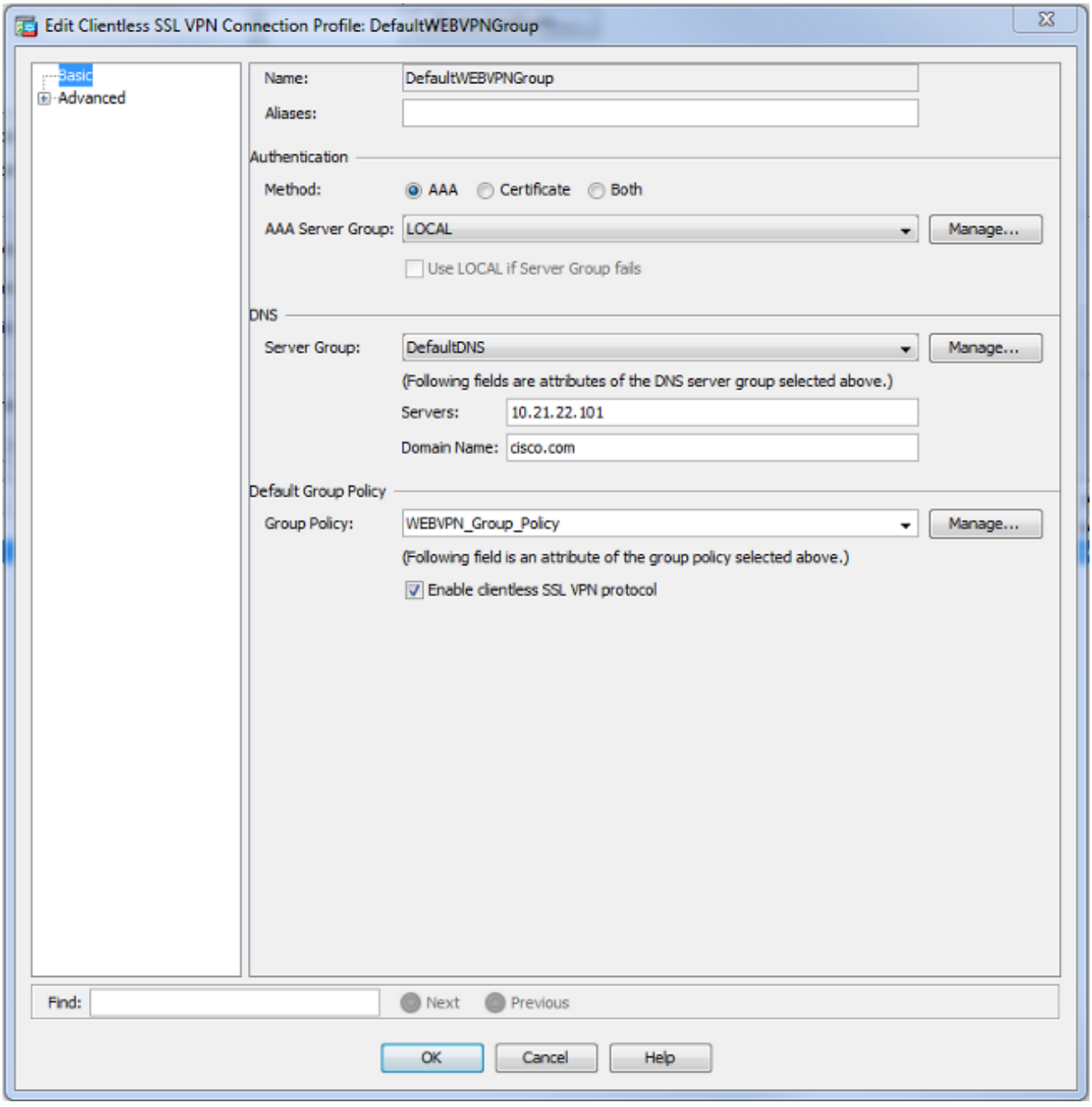
- Les utilisateurs peuvent manuellement sélectionner le profil de connexion de la liste déroulante ou avec un URL de particularité. Voir l'ASA 8.x : Permettez aux utilisateurs pour sélectionner un groupe à la procédure de connexion de webvpn par l'intermédiaire du Group-Alias et de la méthode de Group-URL.

- Quand vous utilisez un serveur LDAP, vous pouvez assigner le profil utilisateur basé sur les attributs reçus du serveur LDAP, voyez l'utilisation ASA de l'exemple de configuration de cartes d'attribut de LDAP.

- Quand vous utilisez l'authentification basée sur certificat des clients, vous pouvez tracer l'utilisateur aux profils basés sur les champs contenus dans le certificat, voyez le guide de configuration de la gamme VPN CLI de Cisco ASA, 9.4 - configurez le groupe de certificat

s'assortissant pour IKEv1.

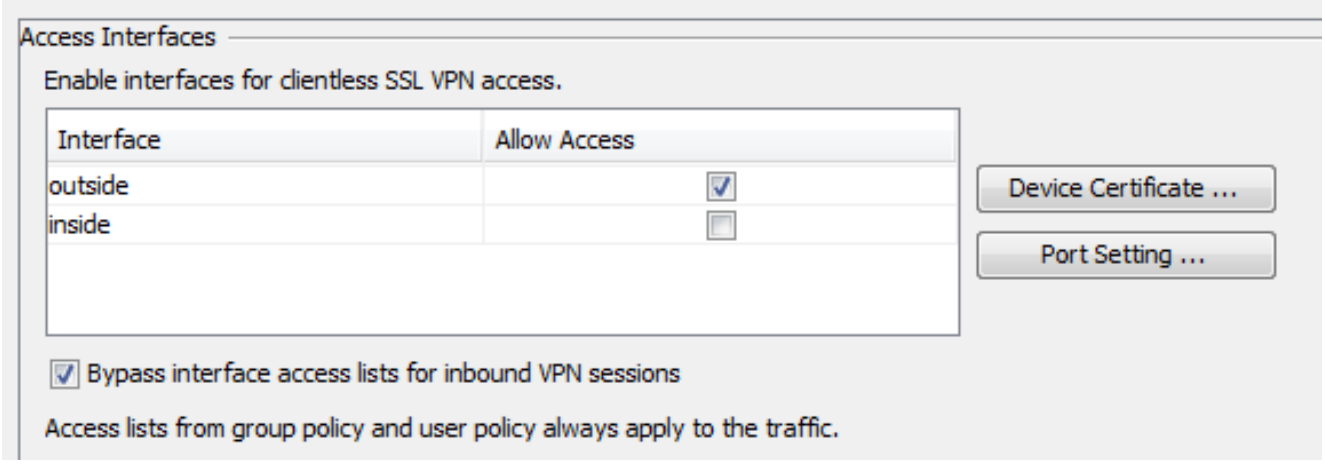
- Afin d'affecter les utilisateurs manuellement à la stratégie de groupe, voir le guide de configuration de la gamme VPN CLI de Cisco ASA, 9.4 - configurer des attributs pour des utilisateurs individuelsÉditez le profil de DefaultWEBVPNGroup et choisissez le WEBVPN_Group_Policy dans le cadre de la stratégie de groupe par défaut.



CLI :

```
ASA(config)# tunnel-group DefaultWEBVPNGroup general-attributes
ASA(config-tunnel-general)# default-group-policy WEBVPN_Group_Policy
```

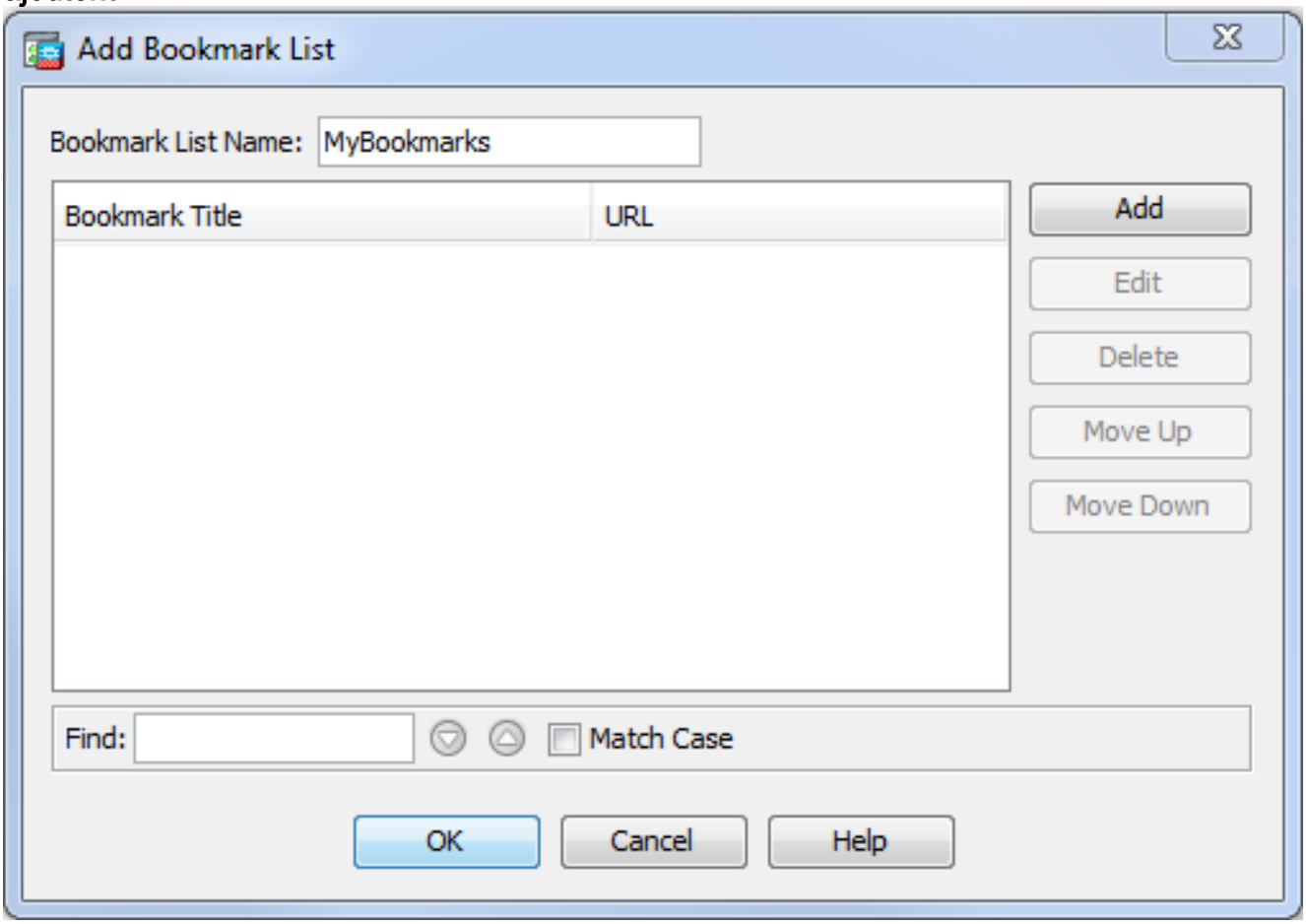
6. Afin d'activer le webvpn sur l'interface extérieure, choisissez la **configuration > l'Accès à distance VPN > VPN SSL sans client Access > profils de connexion**.Vérifiez la case à cocher d'**Access d'autoriser** à côté de l'interface extérieure.



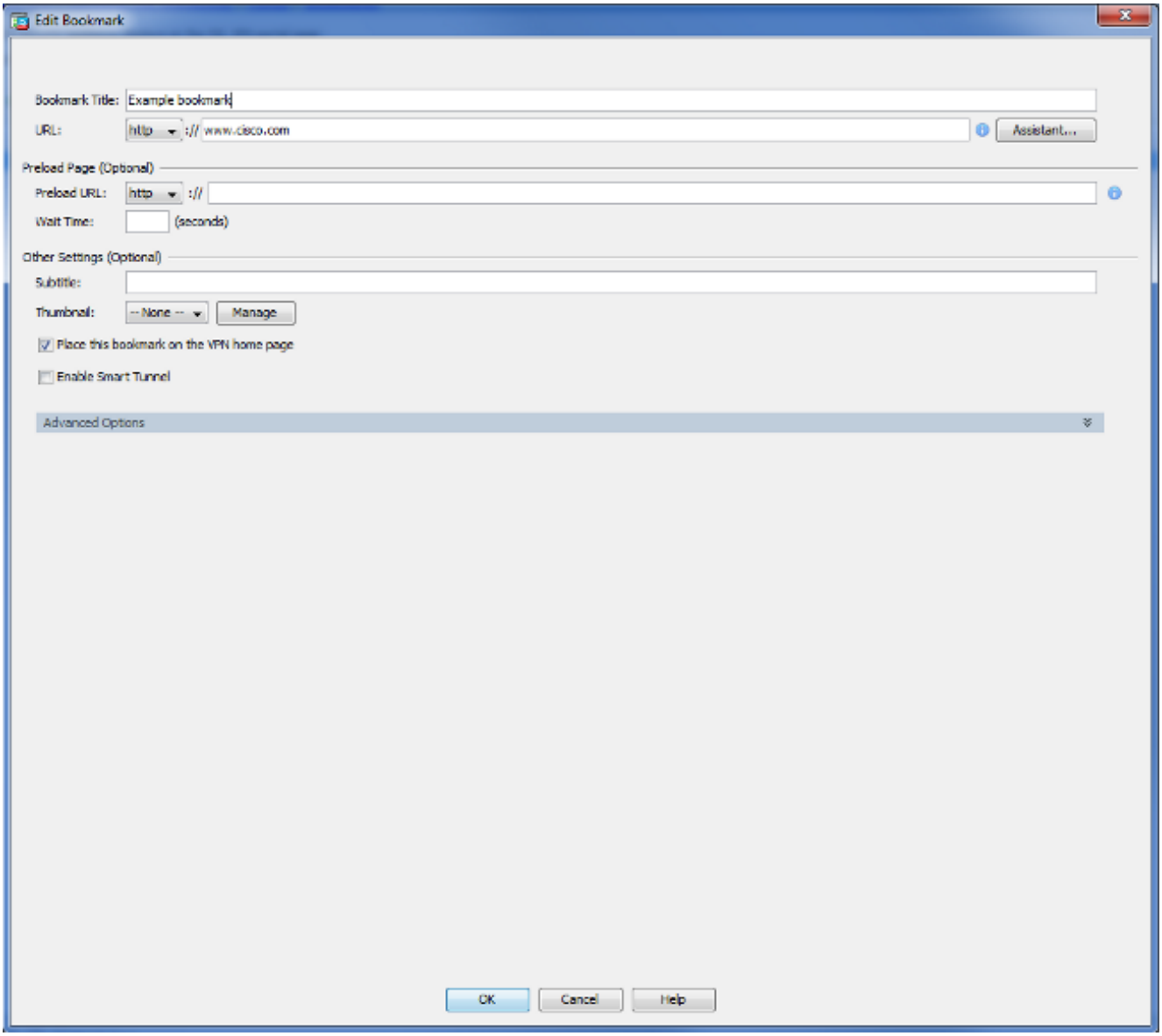
CLI :

```
ASA(config)# webvpn
ASA(config-webvpn)# enable outside
```

7. (Facultatif) créez les signets pour le contenu.Les signets permettent à l'utilisateur pour parcourir facilement les ressources internes sans devoir se souvenir l'URLs.Afin de créer un signet, choisissez la **configuration > l'Accès à distance VPN > VPN SSL sans client Access > portail > signets > ajoutent**.

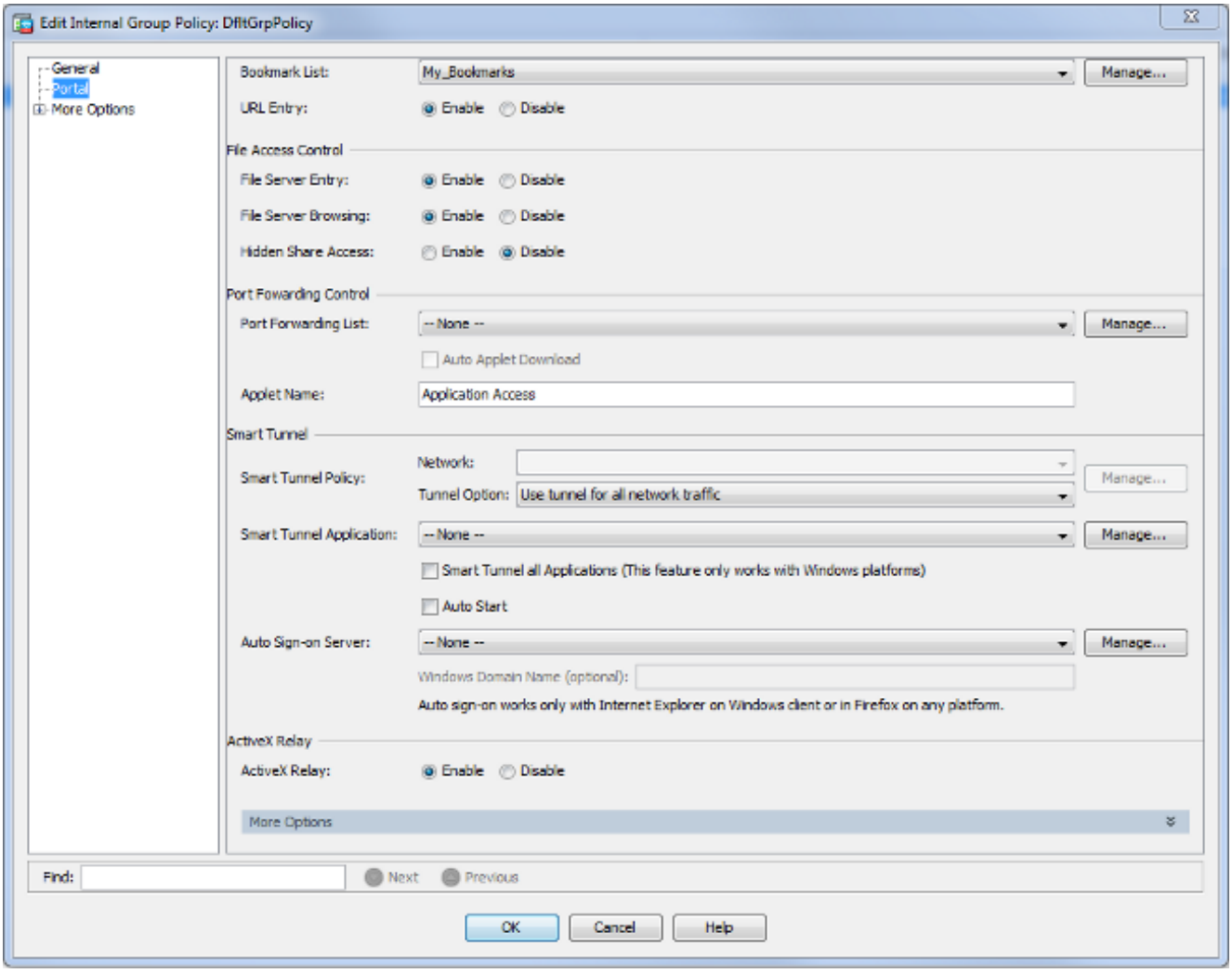


Choisissez **ajoutent** afin d'ajouter un signet spécifique.



CLI :Il est impossible de créer des signets par l'intermédiaire du CLI parce qu'ils sont créés comme fichiers XML.

8. (Facultatif) assignez les signets à une stratégie de groupe spécifique.Choisissez la **configuration > l'Accès à distance VPN > VPN SSL sans client Access > stratégies de groupe > éditent > liste de portail > de signet**.

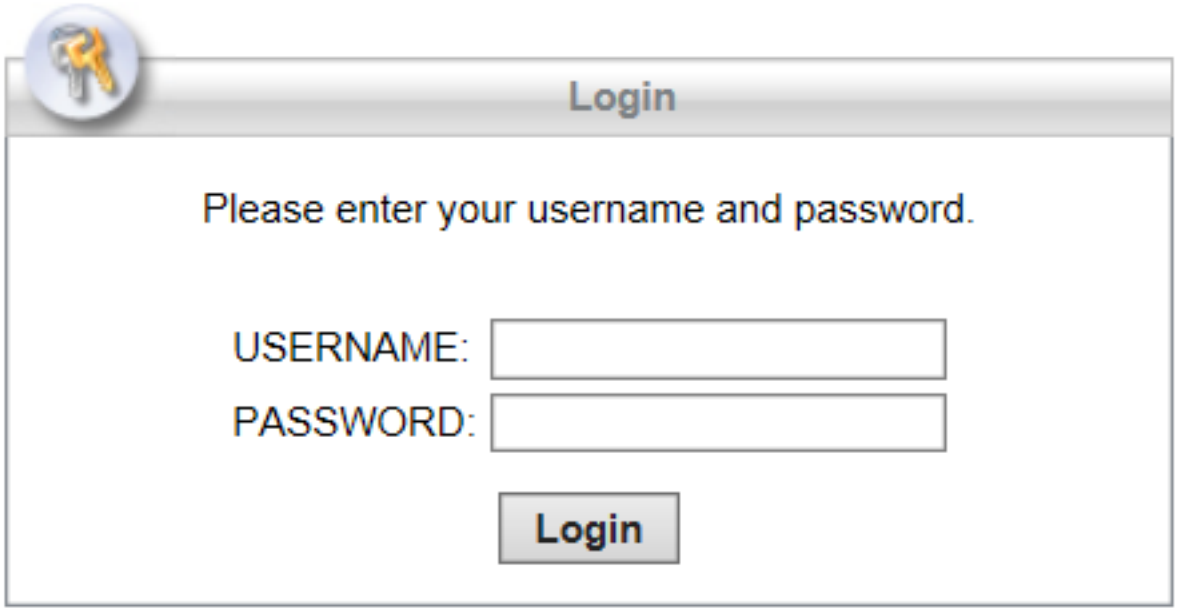


CLI :

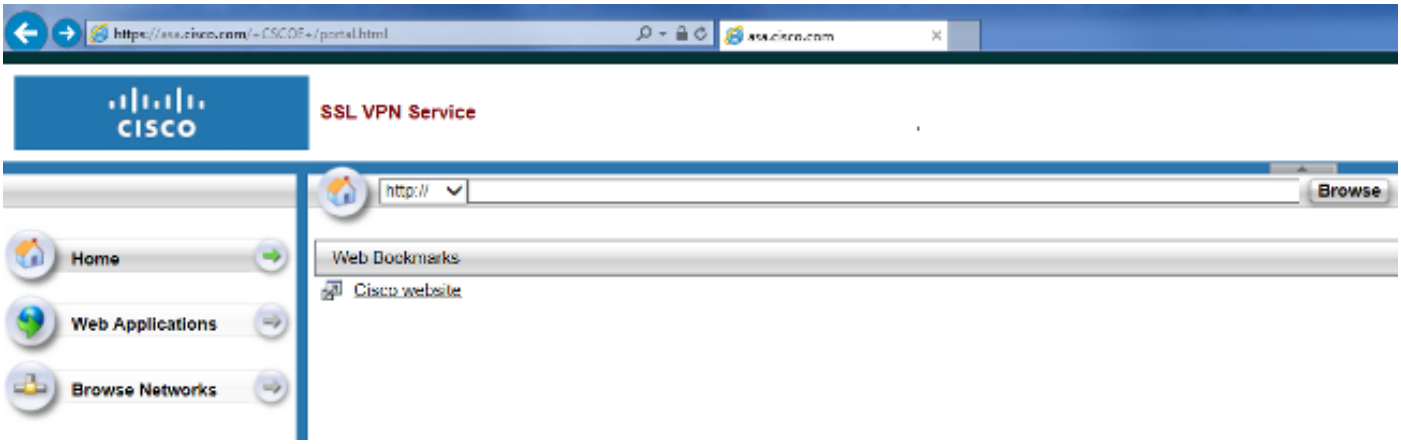
```
ASA(config)# group-policy DfltGrpPolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

Vérifiez

Une fois que le webvpn a été configuré, utilisez l'adresse https:// <FQDN de l'*ASA*> dans le navigateur.



Après que vous ouvrir une session devrait pouvoir voir la barre d'adresses utilisée pour naviguer vers des sites Web et les signets.



Dépannez

Procédures utilisées pour dépanner

Suivez ces instructions afin de dépanner votre configuration.

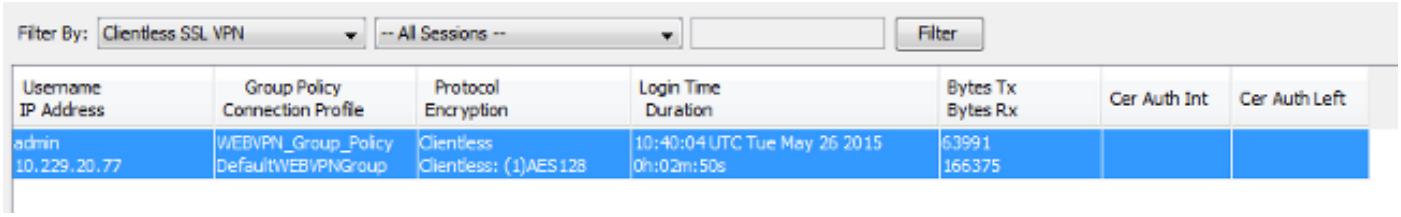
Dans l'ASDM, choisissez **Monitoring > logging > Real-time Log Viewer > View**. Quand un client se connecte à l'ASA, notez l'établissement de la session de TLS, la sélection de la stratégie de groupe, et l'authentification réussie de l'utilisateur.

```
Device completed SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLSv1.2 session
SSL client outside:10.229.20.77/61307 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLS session
SSL client outside:10.229.20.77/61306 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLS session
Built inbound TCP connection 107 for outside:10.229.20.77/61307 (10.229.20.77/61307) to identity:10.48.66.179/443 (10.48.66.179/443)
Built inbound TCP connection 106 for outside:10.229.20.77/61306 (10.229.20.77/61306) to identity:10.48.66.179/443 (10.48.66.179/443)
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> Authentication: successful, Session Type: WebVPN.
Device selects trust-point ASA-self-signed for client outside:10.229.20.77/53047 to 10.48.66.179/443
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> WebVPN session started.
DAP: User admin, Addr 10.229.20.77, Connection Clientless: The following DAP records were selected for this connection: DfltAccessPolicy
AAA transaction status ACCEPT : user = admin
AAA retrieved default group policy (WEBVPN_Group_Policy) for user = admin
AAA user authentication Successful : local database : user = admin
Device completed SSL handshake with client outside:10.229.20.77/61304 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61303 to 10.48.66.179/443 for TLSv1.2 session
```

CLI :

```
ASA(config)# logging buffered debugging
ASA(config)# show logging
```

Dans l'ASDM, choisissez le **Monitoring > VPN > VPN Statistics > Sessions > le filtre par : VPN SSL sans client.** Recherchez la nouvelle session WebVPN. Soyez sûr de choisir le filtre WebVPN et cliquez sur **Filter**. Si un problème se pose, contournez temporairement le périphérique ASA pour vous assurer que les clients peuvent accéder aux ressources réseau désirées. Passez en revue les étapes de configuration énumérées dans ce document.



CLI :

```
ASA(config)# show vpn-sessiondb webvpn

Session Type: WebVPN

Username : admin Index : 3
Public IP : 10.229.20.77
Protocol : Clientless
License : AnyConnect Premium
Encryption : Clientless: (1)AES128 Hashing : Clientless: (1)SHA256
Bytes Tx : 72214 Bytes Rx : 270241
Group Policy : WEBVPN_Group_Policy Tunnel Group : DefaultWEBVPNGroup
Login Time : 10:40:04 UTC Tue May 26 2015
Duration : 0h:05m:21s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a1516010000300055644d84
Security Grp : none
```

Commandes utilisées pour dépanner

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** .

> **Note**: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **webvpn d'exposition** - Il y a beaucoup de **commandes show** associées avec le webvpn. Afin de voir l'utilisation des **commandes show** en détail, voyez la section de référence de commandes de l'appliance de sécurité Cisco.
- **debug webvpn -** L'utilisation des commandes de **débogage** peut défavorablement affecter l'ASA. Afin de voir l'utilisation des commandes de **débogage** plus en détail, voyez la section de référence de commandes de l'appliance de sécurité Cisco.

Problèmes courants

L'utilisateur ne peut pas ouvrir une session

Problème

On ne permet pas le message « l'accès sans client de VPN SSL (de navigateur). » apparaît dans le navigateur après qu'une tentative infructueuse de procédure de connexion. La licence premium d'AnyConnect n'est pas installée sur l'ASA ou elle est non utilisable comme affiché par « le permis de la meilleure qualité d'AnyConnect n'est pas activé sur l'ASA. »

Solution

Activez le permis de la meilleure qualité d'AnyConnect avec ces commandes :

```
ASA(config)# webvpn
ASA(config-webvpn)# no anyconnect-essentials
```

Problème

Le message « échec de connexion » apparaît dans le navigateur après qu'une tentative infructueuse de procédure de connexion. La limite de permis d'AnyConnect a été dépassée.

Solution

Recherchez ce message dans les logs :

```
ASA(config)# webvpn
ASA(config-webvpn)# no anyconnect-essentials
```

En outre, vérifiez votre limite de permis :

```
ASA(config)# show version | include Premium
AnyConnect Premium Peers : 2 perpetual
```

Problème

Le message « AnyConnect n'est pas activé sur le serveur VPN » apparaît dans le navigateur après qu'une tentative infructueuse de procédure de connexion. Le protocole VPN sans client n'est pas activé dans la stratégie de groupe.

Solution

Recherchez ce message dans les logs :

```
ASA(config)# show version | include Premium
AnyConnect Premium Peers : 2 perpetual
```

Assurez-vous que le protocole VPN sans client est activé pour la stratégie de groupe désirée :

```
ASA(config)# show version | include Premium
AnyConnect Premium Peers : 2 perpetual
```

Incapable de connecter plus de trois utilisateurs WebVPN à l'ASA

Problème

Seulement trois clients de webvpn peuvent se connecter à l'ASA. La connexion pour le quatrième client échoue.

Solution

Dans la plupart des cas, ce problème est lié à un paramètre de connexion simultanée dans la stratégie de groupe. Employez cette illustration afin de configurer le nombre désiré de procédures de connexion simultanées. Dans cet exemple, la valeur désirée est 20.

```
ASA(config)# group-policy Cisco attributes
ASA(config-group-policy)# vpn-simultaneous-logins 20
```

Les clients de webvpn ne peuvent pas frapper des signets et sont grisés

Problème

Si ces signets étaient configurés pour que des utilisateurs se connectent au VPN sans client, mais sur l'écran d'accueil sous des « applications Web » ils apparaissent comme grisé, comment est-ce que je peux activer ces liens de HTTP de sorte que les utilisateurs puissent les cliquer sur et entrer dans l'URL particulier ?

Solution

Vous devriez d'abord vous assurer que ASA peut résoudre les sites Web à travers le DNS. Essayez d'envoyer un ping aux sites Web par nom. Si ASA ne peut pas résoudre le nom, le lien est grisé. Si les serveurs DNS sont internes à votre réseau, configurez l'interface privée de recherche de domaine DNS.

Connexion de Citrix par le webvpn

Problème

Le message d'erreur « **the ica client received a corrupt ica file.** » se produit pour Citrix au-dessus de webvpn.

Solution

Si vous utilisez le mode *secure gateway* pour la connexion Citrix via WebVPN, le fichier ICA peut être endommagé. Puisque ASA n'est pas compatible avec ce mode de fonctionnement, créez un nouveau fichier ICA en mode direct (mode non sécurisé).

Comment éviter le besoin de deuxième authentification pour les utilisateurs

Problème

Quand vous accédez à des liens de protocole CIFS sur le portail sans client de webvpn, vous êtes incité pour des qualifications après que vous cliquiez sur le signet. Le Protocole LDAP (Lightweight Directory Access Protocol) est utilisé afin d'authentifier les ressources et les utilisateurs sont déjà entrés dans des qualifications de LDAP pour ouvrir une session à la session VPN.

Solution

Vous pouvez utiliser la caractéristique d'automatique-ouverture de session dans ce cas. Dans le cadre de la stratégie de groupe spécifique étant utilisée et sous ses attributs de webvpn, configurez ceci :

```
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri cifs://X.X.X.X/* auth-type all
```

là où `X.X.X.X=IP du` serveur et du `*=restof de` protocole CIFS le `chemin pour atteindre le` fichier partagé/répertoire en question.

Un extrait d'exemple de configuration est affiché ici :

```
ASA(config)# group-policy ExamplePolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri
https://*.example.com/* auth-type all
```

Pour plus d'informations sur ceci, voyez configurer SSO avec le HTTP de base ou authentification NTLM.

Informations connexes

- ASA : Exemple de configuration de tunnel SMART avec ASDM
- Support et documentation techniques - Cisco Systems