

Configurer le VPN SSL sans client (WebVPN) sur l'ASA

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Informations générales](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

[Procédures utilisées pour dépanner](#)

[Commandes utilisées pour dépanner](#)

[Problèmes courants](#)

[L'utilisateur ne peut pas se connecter](#)

[Impossible de connecter plus de trois utilisateurs WebVPN à l'ASA](#)

[Les clients WebVPN ne peuvent pas accéder aux signets et sont grisés](#)

[Connexion Citrix via WebVPN](#)

[Comment éviter la nécessité d'une deuxième authentification pour les utilisateurs](#)

[Informations connexes](#)

Introduction

Ce document fournit une configuration simple pour la gamme Cisco ASA 5500 afin de permettre l'accès VPN SSL (Secure Sockets Layer) sans client aux ressources réseau internes. Le réseau privé virtuel SSL sans client (WebVPN) permet un accès limité mais précieux et sécurisé au réseau de l'entreprise depuis n'importe quel emplacement. Les utilisateurs peuvent accéder aux ressources de l'entreprise à tout moment via un navigateur sécurisé. Aucun client supplémentaire n'est nécessaire pour accéder aux ressources internes. L'accès est fourni à l'aide d'un protocole de transfert hypertexte sur une connexion SSL.

Le VPN SSL sans client fournit un accès sécurisé et facile à un large éventail de ressources Web et d'applications Web et héritées à partir de presque tous les ordinateurs pouvant accéder aux sites HTTP (Hypertext Transfer Protocol Internet). Cela inclut :

- Sites Web internes
- Microsoft SharePoint 2003, 2007 et 2010
- Microsoft Outlook Web Access 2003, 2007 et 2013

- Microsoft Outlook Web App 2010
- Accès Web Domino (DWA) 8.5 et 8.5.1
- Serveur de présentation Citrix Metaframe 4.x
- Citrix XenApp version 5 à 6.5
- Citrix XenDesktop version 5 à 5.6 et 7.5
- VMware View 4

Une liste des logiciels pris en charge se trouve dans les [plates-formes VPN prises en charge de la gamme Cisco ASA 5500](#).

Conditions préalables

Conditions requises

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

- Navigateur compatible SSL
- ASA avec la version 7.1 ou supérieure
- Certificat X.509 délivré 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 des conditions requises se trouve dans les [plates-formes VPN prises en charge de la gamme Cisco ASA 5500](#).

Components Used

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

- ASA version 9.4(1)
- Adaptive Security Device Manager (ASDM) version 7.4(2)
- ASA 5515-X

The information in this document was created from the devices in a specific lab environment. Tous les périphériques utilisés dans ce document ont commencé par une configuration effacée (par défaut). If your network is live, make sure that you understand the potential impact of any command.

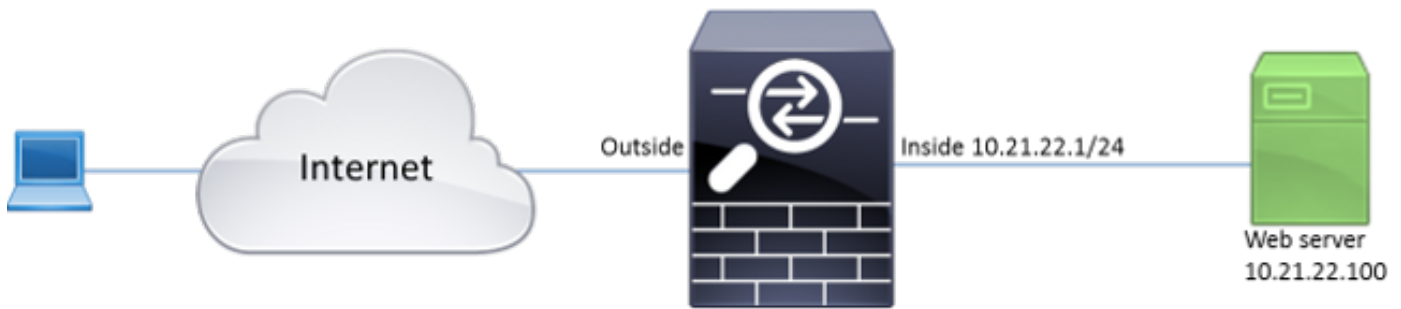
Configuration

Cet article décrit le processus de configuration de l'ASDM et de l'interface de ligne de commande. Vous pouvez choisir de suivre l'un ou l'autre des outils afin de configurer le WebVPN, mais certaines étapes de configuration ne peuvent être réalisées qu'avec l'ASDM.

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Informations générales

WebVPN utilise le protocole SSL afin de sécuriser les données transférées entre le client et le serveur. Lorsque le navigateur initie une connexion à l'ASA, l'ASA présente son certificat pour s'authentifier auprès du navigateur. Afin de vous assurer que la connexion entre le client et l'ASA est sécurisée, vous devez fournir à l'ASA le certificat signé par l'autorité de certification que le client a déjà confiance. Sinon, le client n'aura pas les moyens de vérifier l'authenticité de l'ASA, ce qui entraîne la possibilité d'une attaque de l'homme du milieu et une mauvaise expérience de l'utilisateur, parce que le navigateur produit un avertissement que la connexion n'est pas fiable.

Note: Par défaut, l'ASA génère un certificat X.509 autosigné au démarrage. Ce certificat est utilisé afin de servir les connexions client par défaut. Il n'est pas recommandé d'utiliser ce certificat car son authenticité ne peut pas être vérifiée par le navigateur. En outre, ce certificat est régénéré à chaque redémarrage, de sorte qu'il change après chaque redémarrage.

L'installation du certificat n'entre pas dans le cadre de ce document.

Configuration

Configurez le WebVPN sur l'ASA en cinq étapes principales :

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

Note: Dans les versions d'ASA ultérieures à la version 9.4, l'algorithme utilisé pour choisir les algorithmes de chiffrement SSL a été modifié (voir [Notes de version pour la gamme Cisco ASA, 9.4\(x\)](#)). Si seuls des clients capables de courbes elliptiques sont utilisés, il est possible d'utiliser la clé privée de courbe elliptique pour le certificat. Sinon, la suite de chiffrement personnalisée doit être utilisée afin d'éviter que l'ASA présente un certificat temporaire autosigné. Vous pouvez configurer l'ASA pour qu'il n'utilise que des algorithmes de chiffrement RSA avec `ssl cipher tls1.2 personnalisé « AES256-SHA:AES128-SHA:DHE-`

RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:A DES-CBC-SHA:RC4-SHA:RC4-MD5 ».

1. **Option 1** - Importez le certificat avec le fichier pkcs12. Choisissez **Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Add**. Vous pouvez l'installer avec le fichier pkcs12 ou coller le contenu au format PEM (Privacy Enhanced Mail).

Trustpoint Name: ASDM_TrustPoint2

Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):

Decryption Passphrase:

File to Import From: Browse...

Add a new identity certificate:

Key Pair: <Default-RSA-Key> Show... New...

Certificate Subject DN: CN=ASA Select...

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Advanced...

Enable CA flag in basic constraints extension

Add Certificate Cancel Help

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  
+vkvjUgCaggAgIIFuHFrV6enVf1Nv3sBByB/yZswHELY5KpeALbXhfrFDpLNncAB  
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/  
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5sOhyuQGPhLJRdionbil1sioe4Dplx1b
```

--- output ommited ---

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

MI IJUQIBAzCCCRcGCSqGS Ib3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGS Ib3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGS Ib3DQEMAQYwDgQI8F3N
+vkvjUgCaggAgIIFuHFrv6enVflNv3sBBYB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5s0hyuQGPhLJRdionbi1s1ioe4Dplx1b

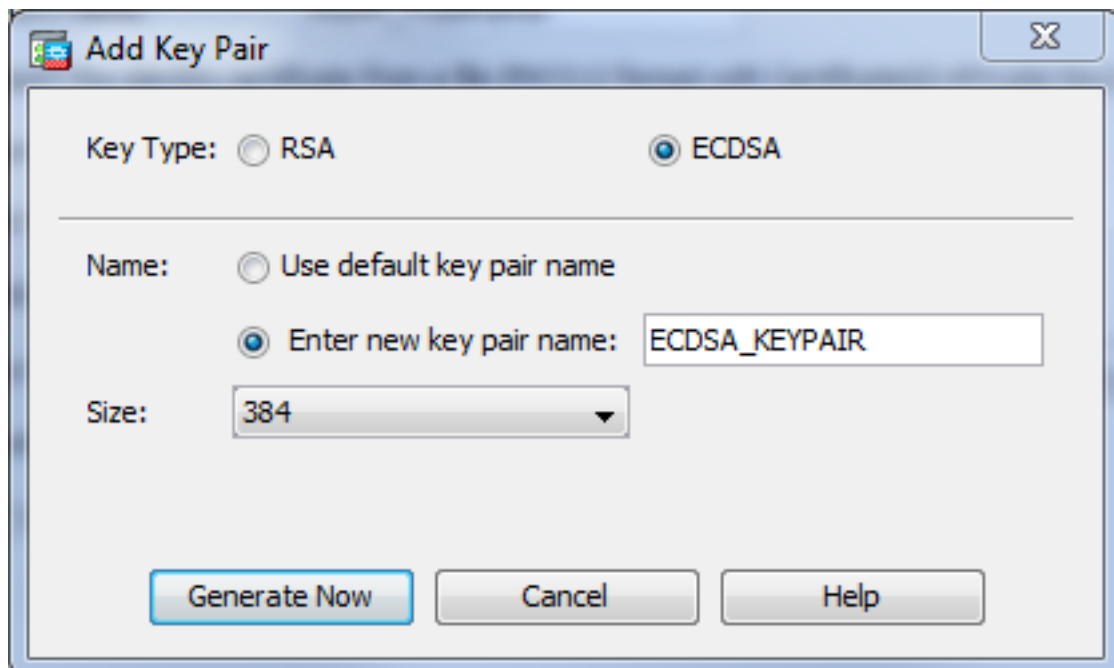
quit

INFO: Import PKCS12 operation completed successfully

Option 2 - Créer un certificat auto-signé. Choisissez **Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Add**. Cliquez sur la case d'option **Add a new identity certificate**. Cochez la case **Générer un certificat auto-signé**. Choisissez un nom commun (CN) correspondant au nom de domaine de l'ASA.

The screenshot shows the 'Add Identity Certificate' dialog box. The 'Trustpoint Name' field contains 'ASDM_TrustPoint1'. There are two radio button options: 'Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):' (unselected) and 'Add a new identity certificate:' (selected). Under the first option, there are fields for 'Decryption Passphrase:' and 'File to Import From:' with a 'Browse...' button. Under the second option, there is a 'Key Pair:' dropdown menu set to '<Default-RSA-Key>' with 'Show...' and 'New...' buttons. Below that is a 'Certificate Subject DN:' field containing 'CN=ASA' with a 'Select...' button. There are two checkboxes: 'Generate self-signed certificate' (checked) and 'Act as local certificate authority and issue dynamic certificates to TLS-Proxy' (unchecked). An 'Advanced...' button is located at the bottom right. At the very bottom, there are three buttons: 'Add Certificate', 'Cancel', and 'Help'.

Cliquez sur **Nouveau** afin de créer la paire de clés pour le certificat. Sélectionnez le type de clé, le nom et la



taille.

CLI :

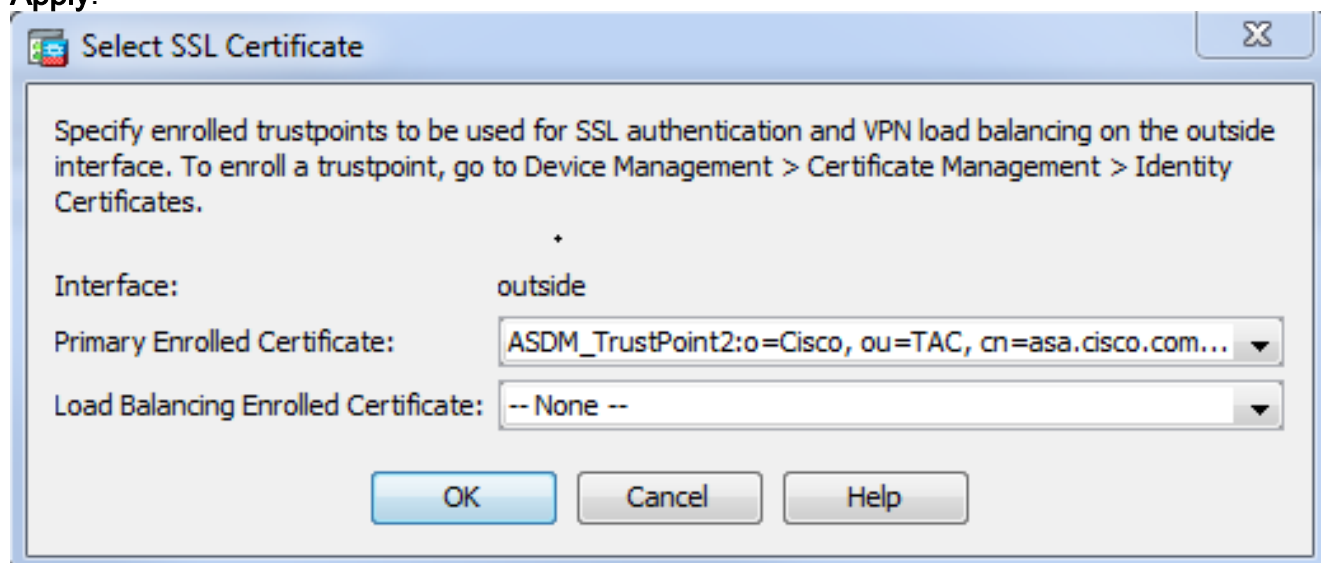
```
ASA(config)# crypto key generate ecdsa label ECDSA_KEYPAIR noconfirm
```

```
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. Sélectionnez le certificat qui sera utilisé pour les connexions WebVPN. Choisissez **Configuration > Remote Access VPN > Advanced > SSL Settings**. Dans le menu Certificats, sélectionnez le point de confiance associé au certificat souhaité pour l'interface externe.

Cliquez sur

Apply.



Configuration CLI équivalente :

```
ASA(config)# ssl trust-point
```

3. (Facultatif) Activez les recherches DNS (Domain Name Server). Le serveur WebVPN agit en tant que proxy pour les connexions client. Cela signifie que l'ASA crée des connexions aux ressources pour le compte du client. Si les clients ont besoin de connexions aux ressources qui utilisent des noms de domaine, l'ASA doit effectuer la recherche DNS. Choisissez **Configuration > Remote Access VPN > DNS**. Configurez au moins un serveur DNS et activez les recherches DNS sur l'interface qui fait face au serveur

Configuration > Remote Access VPN > DNS

Specify how to resolve DNS requests.

DNS Setup

Configure one DNS server group Configure multiple DNS server groups

Primary DNS Server:

Secondary Servers:

Domain Name:

DNS.

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
inside	True
outside	False

DNS Guard

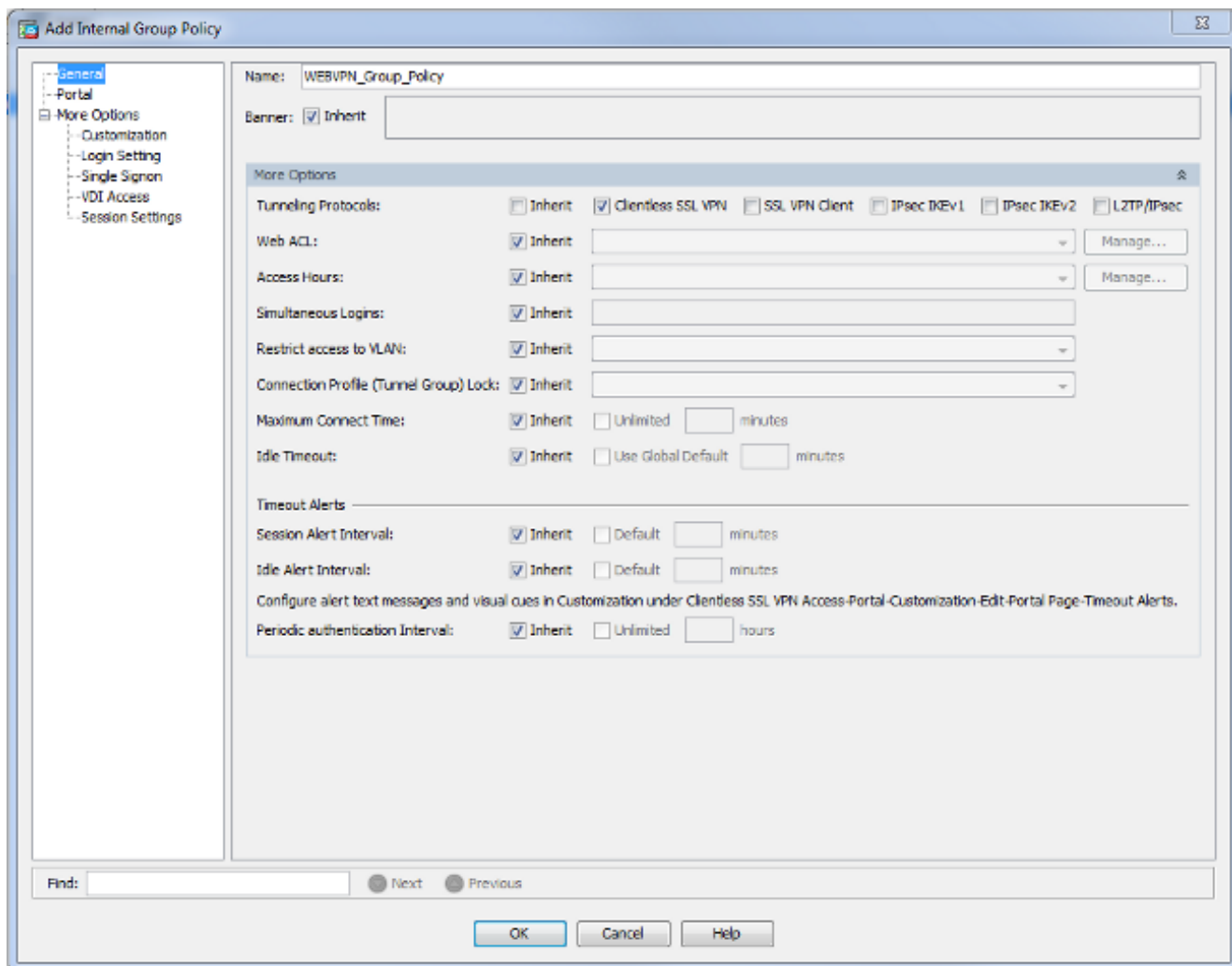
This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface.

Enable DNS Guard on all interfaces.

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 une stratégie de groupe pour les connexions WEBVPN. Choisissez **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add Internal Group Policy**. Sous Options générales, modifiez la valeur des protocoles de tunelling en 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 ASDM, sélectionnez **Configuration > Remote Access VPN > Client SSL VPN Access > Connection Profiles**.

Pour obtenir une vue d'ensemble des profils de connexion et des stratégies de groupe, consultez le [Guide de configuration de l'interface de ligne de commande VPN de la gamme Cisco ASA, 9.4 - Profils de connexion, Stratégies de groupe et Utilisateurs](#). Par défaut, les connexions WebVPN utilisent le profil DefaultWEBVPNGroup. Vous pouvez créer des profils supplémentaires. **Note:** Il existe différentes façons d'affecter des utilisateurs à d'autres profils.

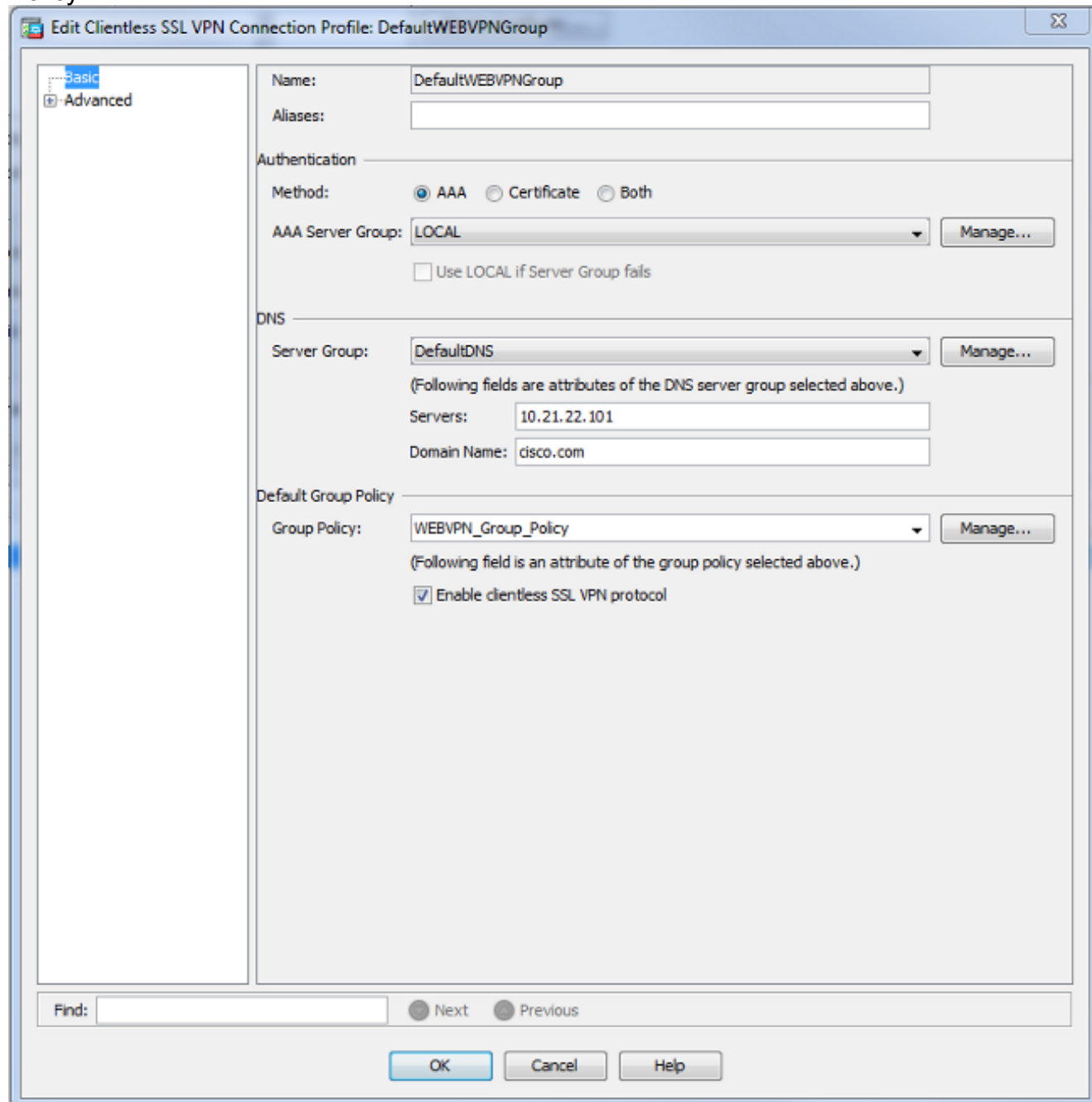
- Les utilisateurs peuvent sélectionner manuellement le profil de connexion dans la liste déroulante ou avec une URL spécifique. Voir [ASA 8.x : Autoriser les utilisateurs à sélectionner un groupe au niveau de la connexion WebVPN via la méthode Group-Alias et Group-URL](#).

- Lorsque vous utilisez un serveur LDAP, vous pouvez affecter le profil utilisateur en fonction des attributs reçus du serveur LDAP, voir [Exemple de configuration de l'utilisation ASA des mappages d'attributs LDAP](#).

- Lorsque vous utilisez l'authentification basée sur les certificats des clients, vous pouvez mapper l'utilisateur aux profils en fonction des champs contenus dans le certificat, voir [Guide de configuration CLI VPN de la gamme Cisco ASA, 9.4 - Configurer la correspondance de](#)

[groupe de certificats pour IKEv1.](#)

- Afin d'affecter manuellement les utilisateurs à la stratégie de groupe, reportez-vous au [Guide de configuration CLI VPN de la gamme Cisco ASA, 9.4 - Configuration des attributs pour les utilisateurs individuels](#) Modifiez le profil DefaultWEBVPNGroup et choisissez WEBVPN_Group_Policy sous Default Group Policy.



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 externe, choisissez **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**. Cochez la case **Autoriser l'accès** en regard de l'interface externe.

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Device Certificate ...

Port Setting ...

CLI :

```
ASA(config)# webvpn
```

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

7. (Facultatif) Créez des signets pour le contenu. Les signets permettent à l'utilisateur de naviguer facilement dans les ressources internes sans avoir à mémoriser les URL. Afin de créer un signet, choisissez **Configuration > Remote Access VPN > Client SSL VPN Access > Portal > Bookmarks > Add**.

Add Bookmark List

Bookmark List Name:

Bookmark Title	URL
----------------	-----

Add

Edit

Delete

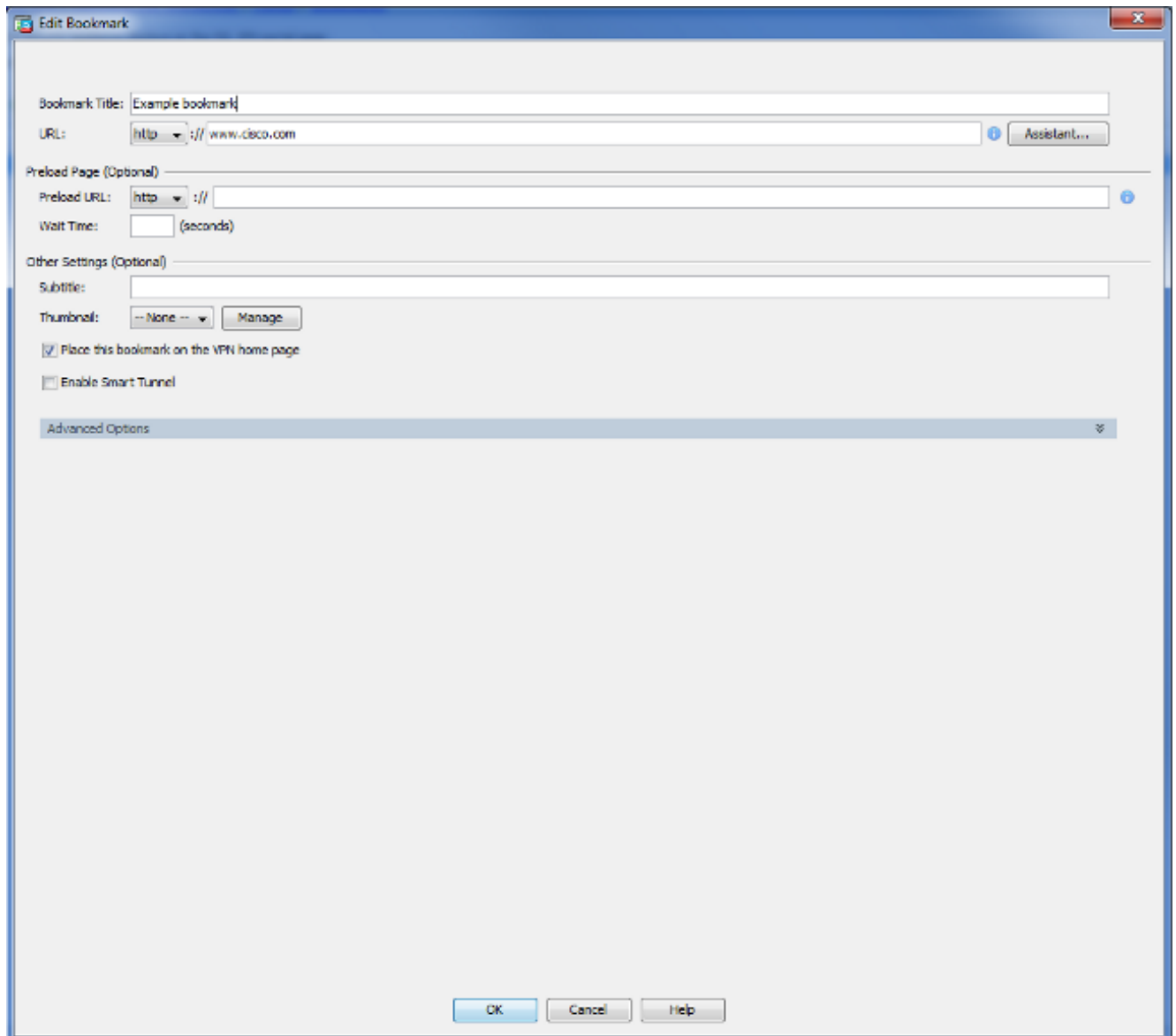
Move Up

Move Down

Find: Match Case

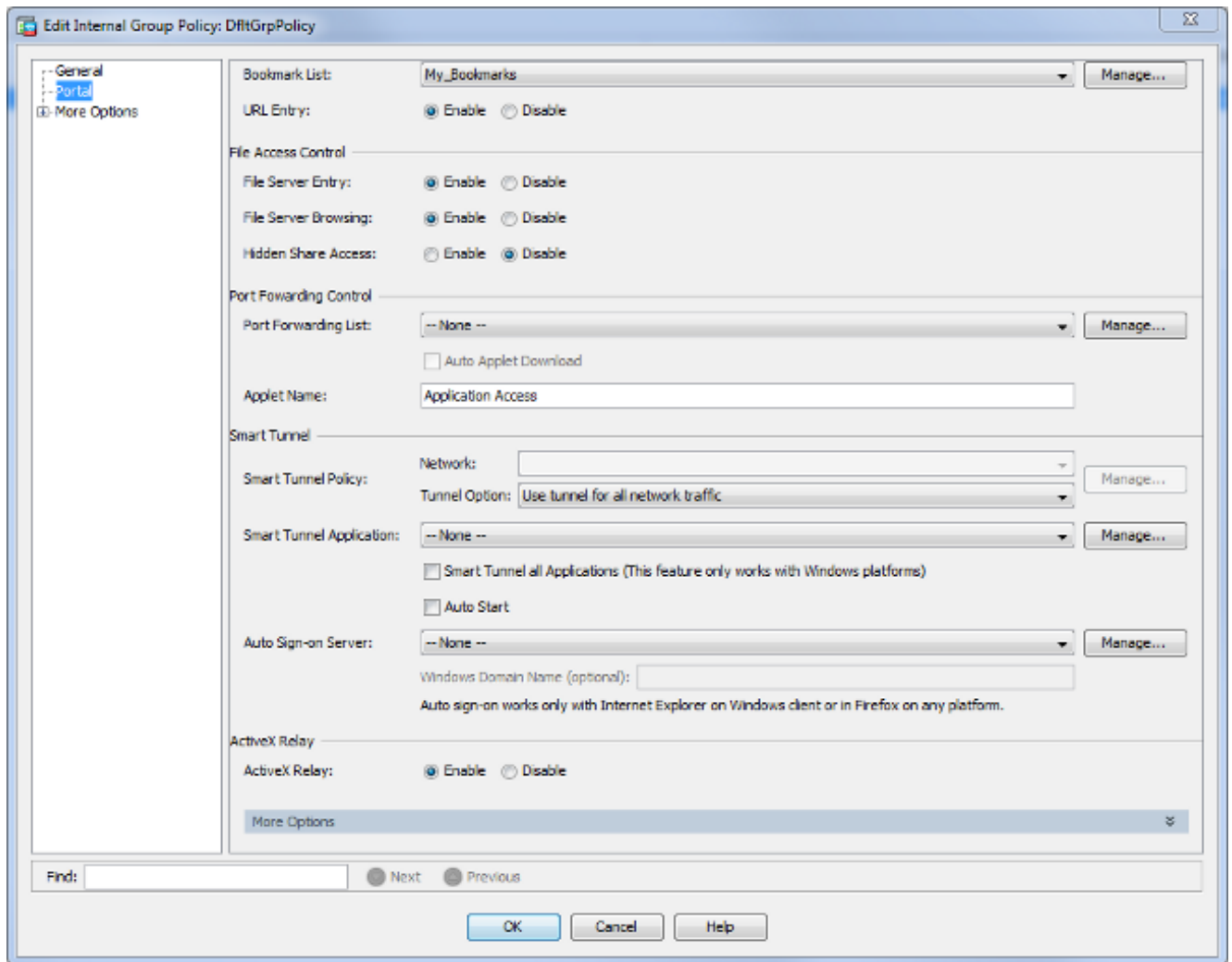
OK Cancel Help

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



CLI :Il est impossible de créer des signets via l'interface de ligne de commande, car ils sont créés en tant que fichiers XML.

8. (Facultatif) Affectez des signets à une stratégie de groupe spécifique. Choisissez **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Portal > Bookmark List**.

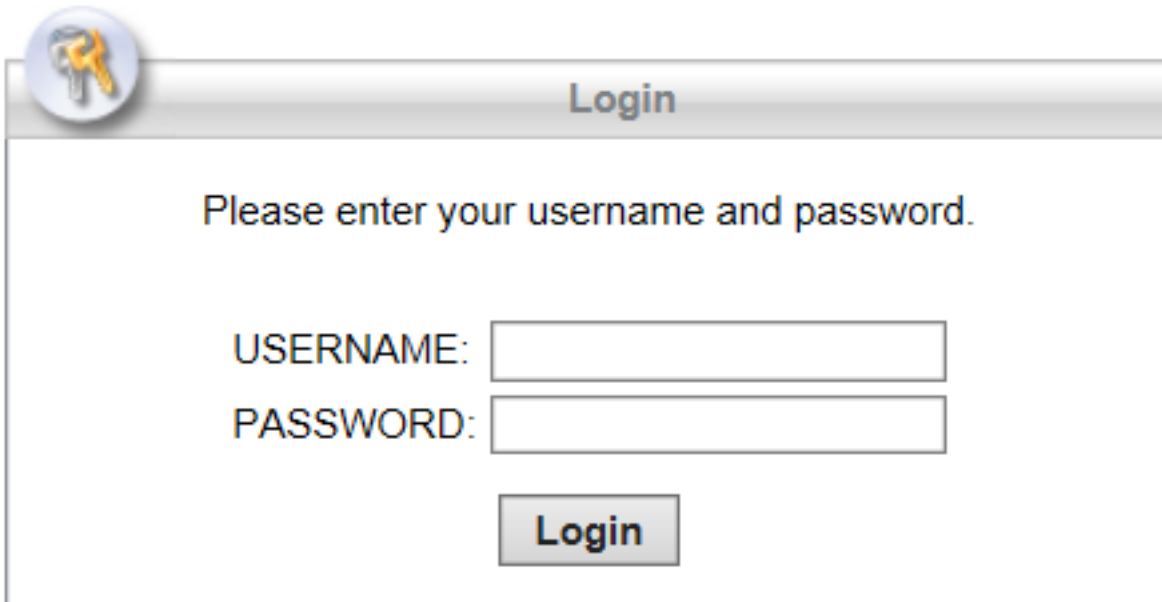


CLI :

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

Vérification

Une fois le WebVPN configuré, utilisez l'adresse `https://<FQDN de l'ASA>` dans le navigateur.



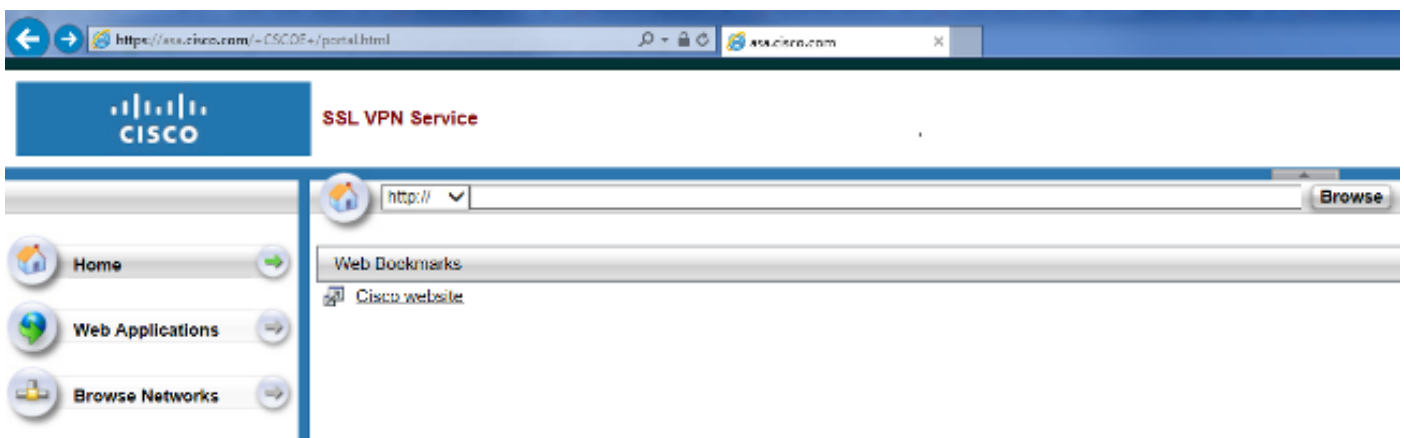
Login

Please enter your username and password.

USERNAME:

PASSWORD:

Après vous être connecté, vous devriez voir la barre d'adresse utilisée pour naviguer vers les sites Web et les signets.



Dépannage

Procédures utilisées pour dépanner

Suivez ces instructions afin de faire le dépannage de votre configuration .

Dans l'ASDM, choisissez **Monitoring > logging > Real-time Log Viewer > View**. Lorsqu'un client se connecte à l'ASA, notez l'établissement de la session 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 ASDM, choisissez **Monitoring > VPN > VPN Statistics > Sessions > Filter by : 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.

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Cer Auth Int	Cer Auth Left
admin 10.229.20.77	WEBVPN_Group_Policy DefaultWEBVPNGroup	Clientless Clientless: (1)AES128	10:40:04 UTC Tue May 26 2015 0h:02m:50s	63991 166375		

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.

- **show webvpn** - Il existe de nombreuses commandes **show** associées à WebVPN. Afin de voir l'utilisation des commandes **show** en détail, consultez la section [référence de commande](#) de l'appliance de sécurité Cisco.
- **debug webvpn** - L'utilisation des commandes **debug** peut avoir un impact négatif sur l'ASA. Afin de voir l'utilisation des commandes **debug** plus en détail, consultez la section [référence de commande](#) de l'appliance de sécurité Cisco.

Problèmes courants

L'utilisateur ne peut pas se connecter

Problème

Le message « Accès VPN SSL sans client (navigateur) n'est pas autorisé. » apparaît dans le navigateur après une tentative de connexion infructueuse. La licence AnyConnect Premium n'est pas installée sur l'ASA ou elle n'est pas utilisée comme indiqué par « La licence Premium AnyConnect n'est pas activée sur l'ASA. »

Solution

Activez la licence Premium AnyConnect avec les commandes suivantes :

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

Problème

Le message « Échec de la connexion » apparaît dans le navigateur après une tentative de connexion infructueuse. La limite de licence AnyConnect a été dépassée.

Solution

Recherchez ce message dans les journaux :

```
%ASA-4-716023: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>
Session could not be established: session limit of 2 reached.
```

Vérifiez également votre limite de licence :

```
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 une tentative de connexion infructueuse. Le protocole VPN sans client n'est pas activé dans la stratégie de groupe.

Solution

Recherchez ce message dans les journaux :

```
%ASA-6-716002: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>  
WebVPN session terminated: Client type not supported.
```

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

```
ASA(config)# show run all group-policy | include vpn-tunnel-protocol  
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-clientless
```

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

Problème

Seuls trois clients 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. Utilisez cette illustration afin de configurer le nombre souhaité de connexions simultanées. Dans cet exemple, la valeur souhaitée est 20.

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

Les clients WebVPN ne peuvent pas accéder aux signets et sont grisés

Problème

Si ces signets ont été configurés pour que les utilisateurs se connectent au VPN sans client, mais sur l'écran d'accueil sous « Applications Web » ils apparaissent grisés, comment puis-je activer ces liens HTTP pour que les utilisateurs puissent les cliquer et aller dans l'URL particulière ?

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 Citrix via 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 la nécessité d'une deuxième authentification pour les utilisateurs

Problème

Lorsque vous accédez aux liens CIFS sur le portail WebVPN sans client, vous êtes invité à fournir des informations d'identification après avoir cliqué sur le signet. Le protocole LDAP (Lightweight Directory Access Protocol) est utilisé afin d'authentifier les ressources et les utilisateurs qui ont déjà entré des informations d'identification LDAP pour se connecter à la session VPN.

Solution

Vous pouvez utiliser la fonctionnalité de connexion automatique dans ce cas. Sous la stratégie de groupe spécifique utilisée et sous ses attributs 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
```

où X.X.X.X=IP du serveur CIFS et *=reste du chemin pour atteindre le fichier/dossier de partage en question.

Un exemple d'extrait de configuration est présenté 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 à ce sujet, consultez [Configuration de SSO avec l'authentification HTTP Basic ou NTLM](#).

Informations connexes

- [ASA : Exemple de configuration de tunnel SMART avec ASDM](#)
- [Support et documentation techniques - Cisco Systems](#)