# ASA 8.x : Exemple de configuration d'autorisation de la transmission tunnel partagée pour un client VPN AnyConnect sur le dispositif ASA

## Contenu

Introduction Conditions préalables Conditions requises Components Used Conventions Informations générales Configuration Diagramme du réseau Configuration d'ASA utilisant l'ASDM 6.0(2) Configuration de l'interface de ligne de commande ASA Établir la connexion VPN SSL avec SVC Vérification Dépannage Informations connexes

# **Introduction**

Ce document fournit des instructions pas à pas sur la façon de permettre l'accès de Cisco AnyConnect VPN Client à Internet tandis qu'ils sont reliés par tunnel à un appliance de sécurité adaptable Cisco (ASA) 8.0.2. Cette configuration permet l'accès client sécurisé aux ressources de l'entreprise par l'intermédiaire du SSL tout en donnant l'accès non sécurisé à Internet en utilisant le split tunnelling.

# **Conditions préalables**

#### **Conditions requises**

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

- L'appliance de sécurité ASA doit exécuter une version 8.x
- Cisco AnyConnect VPN Client 2.xRemarque : Téléchargez le package AnyConnect VPN Client (anyconnect-win\*.pkg) à partir du <u>téléchargement de logiciels</u> Cisco (clients <u>enregistrés</u> uniquement). Copiez le client VPN d'AnyConnect dans la mémoire flash de l'ASA qui doit être

téléchargée sur les ordinateurs des utilisateurs distants afin d'établir la connexion VPN SSL avec l'ASA. Référez-vous à la section <u>Installer le client d'AnyConnect du guide de</u> <u>configuration d'ASA pour plus d'informations.</u>

#### **Components Used**

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

- ASA de la gamme Cisco 5500 qui exécute le logiciel version 8.0(2)
- Client VPN SSL Cisco AnyConnect version pour Windows 2.0.0343
- PC qui exécute Microsoft Vista, Windows XP SP2 ou Windows 2000 Professionnel SP4 avec Microsoft Installer version 3.1
- Cisco Adaptive Security Device Manager (ASDM) version 6.0(2)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

#### **Conventions**

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

### Informations générales

Le Cisco AnyConnect VPN Client fournit les connexions sécurisées SSL au dispositif de sécurité pour des utilisateurs distants. Sans client installé précédemment, les utilisateurs distants saisissent dans leur navigateur l'adresse IP d'une interface configurée pour accepter les connexions VPN SSL. À moins que le dispositif de sécurité soit configuré pour rediriger des demandes de http:// à https://, les utilisateurs doivent saisir l'URL sous la forme https://<a href="https://sate-exact-sate-accepter-les-background-content-sa

Après avoir saisi l'URL, le navigateur se connecte à cette interface et affiche l'écran d'ouverture de connexion. Si la connexion et l'authentification de l'utilisateur sont acceptées, et que l'appliance de sécurité identifie que l'utilisateur demande le client, il télécharge le client correspondant au système d'exploitation de l'ordinateur distant. Après téléchargement, le client s'installe et se configure automatiquement, établit une connexion SSL sécurité et reste ou se désinstalle automatiquement (selon la configuration du dispositif de sécurité) quand la connexion se termine.

Avec un client installé précédemment, quand l'utilisateur s'authentifie, le dispositif de sécurité examine la révision du client et met à niveau le client selon les besoins.

Quand le client négocie une connexion VPN SSL avec le dispositif de sécurité, il se connecte en utilisant la Transport Layer Security (TLS), et sur option, la Datagram Transport Layer Security (DTLS). La DTLS permet d'éviter les problèmes de latence et de bande passante associés à certaines connexions SSL et d'améliorer les performances des applications en temps réel qui sont sensibles aux retards de paquet.

Le client d'AnyConnect peut être téléchargé depuis le dispositif de sécurité ou il peut être installé manuellement sur le PC distant par l'administrateur système. Référez-vous au <u>Guide</u> <u>d'administration du client VPN Cisco AnyConnect</u> pour plus d'informations sur l'installation manuelle du client.

Le dispositif de sécurité télécharge le client en fonction de la stratégie de groupe ou des attributs du nom d'utilisateur de l'utilisateur établissant la connexion. Vous pouvez configurer le dispositif de sécurité pour qu'il télécharge automatiquement le client ou vous pouvez le configurer pour qu'il demande à l'utilisateur distant s'il souhaite télécharger le client. Dans le dernier cas, si l'utilisateur ne répond pas, vous pouvez configurer le dispositif de sécurité pour qu'il télécharge le client après un délai d'attente ou qu'il présente la page de connexion.

### **Configuration**

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

**Remarque :** utilisez l'<u>outil de recherche de commandes</u> (clients <u>enregistrés</u> uniquement) 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 IP utilisés dans cette configuration ne sont pas routables légalement sur Internet. Ce sont des adresses <u>RFC 1918 qui ont été utilisés dans un</u> <u>environnement de laboratoire.</u>

#### Configuration d'ASA utilisant l'ASDM 6.0(2)

Ce document suppose que la configuration de base, telle que la configuration d'interface, est déjà faite et fonctionne correctement.

**Remarque :** référez-vous à <u>Autoriser l'accès HTTPS pour ASDM</u> afin de permettre à l'ASA d'être configuré par l'ASDM.

**Remarque :** WebVPN et ASDM ne peuvent pas être activés sur la même interface ASA, sauf si vous modifiez les numéros de port. Référez-vous à <u>ASDM et WebVPN activés sur la même</u> interface d'ASA pour plus d'informations.

Exécutez ces étapes afin de configurer le VPN SSL sur l'ASA avec le split tunneling :

1. Choisissez Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add pour créer un pool d'adresses IP

| Ĭ        | 🚰 Add IP Pool        |                |
|----------|----------------------|----------------|
|          |                      |                |
|          | Name:                | vpnpool        |
|          | Starting IP Address: | 192.168.10.1   |
|          | Ending IP Address:   | 192.168.10.254 |
|          | Subnet Mask:         | 255.255.255.0  |
|          |                      |                |
| vpnpool. | ок                   | Cancel Help    |

- 2. Cliquez sur Apply. Configuration CLI équivalente :
- 3. Activez WebVPN.Choisissez Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles et sous Access Interfaces, cliquez les cases à cocher Allow Access et Enable DTLS pour l'interface externe. En outre, cliquez la case à cocher Enable Cisco AnyConnect VPN Client ou legacy SSL VPN Client access on the interface selected in the table below afin d'activer le VPN SSL sur l'interface externe.

| ote Access VPN > Net  | work (Client) Access > SSL VPN   | Connection Profiles   |  |  |
|---|--|---|--|--|
| The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to<br>client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the<br>Layer Security (DTLS) tunneling options. |  |   |  |  |
| (More client-related parameters, such as client images and client profiles, can be found at <u>Client Settings</u>  |  |   |  |  |
|   |  |   |  |  |
| Connect VPN Client or le  | egacy SSL VPN Client access on the i   | interfaces selected in the  |  |  |
| Allow Access  | Require Client Certificate   | Enable DTLS   |  |  |
|   |  |   |  |  |
|   |  |   |  |  |
| Access Port: 443 DTLS Port: 443<br>Click here to Assign Certificate to Interface.   |  |   |  |  |
|   | te Access VPN > Net<br>e automatically deploys<br>puires end-user administ<br>) tunneling options.<br>parameters, such as clie<br>Connect VPN Client or le<br>Allow Access | ate Access VPN > Network (Client) Access > SSL VPN         e automatically deploys the Cisco AnyConnect VPN Client or         quires end-user administrative rights. The Cisco AnyConnect         ) tunneling options.         parameters, such as client images and client profiles, can be         Connect VPN Client or legacy SSL VPN Client access on the intervence         Allow Access       Require Client Certificate         V       Intervence         DTLS Port:       443 |  |  |

Cliquez sur Apply.Choisissez Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings > Add afin d'ajouter l'image de Cisco AnyConnect VPN Client depuis la mémoire flash de l'ASA comme indiqué.

| Flash SVC Image:       Upload         Upload       upload         OK       Cancel       Help         Image:       Files       Image:       Or/24/07 05:21:48         Image:       Orypto_archive       07/24/07 05:21:48       Or/24/07 05:21:48         Image:       Crypto_archive       07/24/07 05:21:48       Or/24/07 05:31:38         Image:       Crypto_archive       0.03:::::::::::::::::::::::::::::::::::  | 🕵 Add SSL VPN Client Image  |                                 | × SSL VPN > Clie    | ent Settings                 |                   |
|---|---|---------------------------------|---------------------|------------------------------|-------------------|
| OK       Cancel       Help         Image: Street of the street of   | Flash SVC Image:  | Browse Flash<br>Upload          |                     | ion system to the top of the |                   |
| © Browse Flash       ×         Folders       Files         Image: Size (bytes)       Date Modified         Image: Crypto_archive       O7/24/07 05:21:48         Image: Crypto_archive       O/2657,734         Image: Crypto_archive       O/2607,09141450         Image: Crypto_archive       O/212/07 09141450         Image: Crypto_archive       O/21007 09141450         Image: Crypto_archive       O/21007 09141450         Image: Crypto_archive       O/210/07 09141450         Image: Crypto_archive       O/210/07 09151:38         Image: Crypto_archive       O/200/07 09151:38         Image: Crypto_archive       O/200/07 09151:38      <  | ОК С  | ancel Help                      |                     |                              |                   |
| Folders       Files         Image: Size (bytes)       Date Modified         Image: Crypto_archive       07/24/07 05:21:36         Image: Crypto_archive       07/24/07 05:21:38         Image: Crypto_archive       07/24/07 05:31:38         Image: Crypto_archive       07/24/07 05:31:48         Image: Crypto_archive       0/20/07 09:51:38         Image: Crypto_archive       0/20/07 09:51:38         I   | 🔂 Browse Flash  |                                 |                     | ×                            |                   |
| FileName       Size (bytes)       Date Modified         Image: Crypto_archive       07/24/07 05:21:48       07/24/07 05:21:48         Image: Crypto_archive       0.46,851,212       01/04/06 18:07:02         Image: Crypto_archive       0.9/20/07 09:51:38       09/13/07 04:14:50         Image: Crypto_archive       0.9/20/07 09:51:38       09/13/07 04:14:50         Image: Crypto_archive       0.9/22-k8.bin       0.9/22,0/07 09:51:38         Image: Crypto_archive       0.9/22-k8.bin       14,524,416       01/03/08 21:38:26         Image: Crypto_archive       0.9/20,007 09:51:38       ssdClent-win-1.1.4.179       418,765       03/14/08 13:47:58         File Name: Image: Ct-win-2.0.0343-k9.pkg       Erowse Flash       03/14/08 13:47:58       Erowse Flash         Image: Ct-win-2.0.0343-k9.pkg       Erowse Flash       Upload       OK       Click OK         Click OK.       OK       Cancel       Help       Cliquez sur         Add.  | Folders   | Files                           |                     |                              |                   |
| File Name:       arcypto_archive       07/24/07 05:21:48         asdm-603.bin       6,851,212       01/04/06 18:07:02         asdm-603.bin       14,955,006       01/04/06 18:07:02         asdm-603.bin       14,955,006       01/04/06 18:07:02         asdm-602.bin       6,859,764       01/30/06 21:38:26         asdm-602.bin       6,859,764       01/30/08 21:38:26         asdm-522.bin       5,623,106       02/12/07 05:53:46         asa802-k8.bin       14,524,416       01/03/08 21:38:26         asa802-k8.bin       14,524,416       01/03/08 21:38:26         sslclient-win-1.1.4.179       418,765       03/14/08 13:47:58         Flex Name:       anyconnect-win-2.0.0343-k9.pkg       Erowsee Flash         Upload       OK       Cancel       Help         Click OK.       Cancel       Help       Cliquez sur         Add       Replace       Nove UP       Move Clien  | ⊟– 🥏 disk0:   | FileName 🔺                      | Size (bytes)        | Date Modified                |                   |
| Image: Image  | E-log   | crypto_archive                  |                     | 07/24/07 05:21:48            |                   |
| asdm-603.bin       6,851,212       01/04/08 18:07:02         asa803-k8.bin       14,635,008       01/04/08 17:49:50         admin.cfg       1,220       09/20/07 09:51:38         aryconnect-win-20.03       2,655,734       08/13/07 04:14:50         asdm-602.bin       6,889,764       01/03/08 21:38:26         asa72-k8.bin       8,312,832       02/13/07 04:16:30         asdm-602.bin       5,623,108       02/12/07 05:53:48         asa802-k8.bin       14,524,416       01/03/08 21:24:42         old_running.cfg       1,841       09/20/07 09:51:38         ssiclient-win-1.1.4.179       418,765       03/14/08 13:47:58         File Name:         aryconnect-win-2.0.0343-k9.pkg         File Name:         aryconnect-win-2.0.0343-k9.pkg         File Name:         aryconnect-win-2.0.0343-k9.pkg         File Name:         Click OK.         Cliquez sur         Add SSL VPN Client Image         File Name:         Click OK.         Click OK.         Click OK.         Click OK.         Click O   | <u> </u>  | 🔁 log                           |                     | 07/24/07 05:21:36            |                   |
| asa803-k8.bin       14,635,008       01/04/08 17:49:50         admin.cfg       1,220       09/20/07 09:51:38         admin.cfg       1,220       09/20/07 09:51:38         asdm-602.bin       6,889,764       01/03/08 21:38:26         asa722-k8.bin       8,312,832       02/13/07 04:16:30         asdm-522.bin       5,623,108       02/12/07 05:53:48         asa802-k8.bin       14,524,416       01/03/08 21:24:42         old_running.cfg       1,841       09/20/07 09:51:38         sslclient-win-1.1.4.179       148,765       03/14/08 13:47:58         File Name:         anyconnect-win-2.0.0343-k9.pkg         File Name:         anyconnect-win-2.0.0343-k9.pkg         Cliquez sur         Add SSL VPN Client Image         Flash SVC Image:       ct-win-2.0.0343-k9.pkg       Erowse Flash         Upload       Upload       Upload         OK       Cancel       Help       Cliquez sur         Add.       Configuration > Remote Access VPH > Network (Client) Access > Advanced > SSL VPN > Client Settings       Identify SSL VPN Client (SVC) related files.         SSL VPN Client (SVC) related files.         SSL VPN Client Images  |   | asdm-603.bin                    | 6,851,212           | 01/04/08 18:07:02            |                   |
| admin.ctg       1,220       09/20/07 09:51:38         anyconnect-win-2.0.03       2,635,734       08/13/07 04:14:50         asdm-602.bin       6,689,764       01/03/08 21:38:26         asadm-522.bin       5,623,108       02/12/07 05:53:48         asam-522.bin       5,623,108       02/12/07 05:53:48         asam-522.bin       5,623,108       02/12/07 05:53:48         asa802-48.bin       14,524,416       01/03/08 21:24:42         old_running.cfg       1,841       09/20/07 09:51:38         ssiclient-win-1.1.4.179       418,765       03/14/08 13:47:58         File Name:         anyconnect-win-2.0.0343-k9.pkg         Files SVC Image:       ct-win-2.0.0343-k9.pkg         Erowse Flash         Upload         OK         Click OK.         Click OK.         Cliquez sur         Add.         Configuration > Remote Access VPH > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client (SVC) related files.         SSL VPN Client (SVC) related files.         SSL VPN Client (SVC) related files. <td colspanyconnect-win-2.0.0<="" td=""><td></td><td>asa803-k8.bin</td><td>14,635,008</td><td>01/04/08 17:49:50</td></td>   | <td></td> <td>asa803-k8.bin</td> <td>14,635,008</td> <td>01/04/08 17:49:50</td> |                                 | asa803-k8.bin       | 14,635,008                   | 01/04/08 17:49:50 |
| anyconnect-win-2:0:03       2,639,73       08/13/07 04114:50         asdm-602.bin       6,889,764       01/03/08 21:38:26         asa722+48.bin       8,312,832       02/13/07 04:16:30         asa722+48.bin       14,524,416       01/03/08 21:24:42         old_running.cfg       1,841       09/20/07 09:51:38         asa802-k8.bin       14,524,416       01/03/08 21:24:42         old_running.cfg       1,841       09/20/07 09:51:38         sslcient-win-1.1.4.179       418,765       03/14/08 13:47:58         File Name:         anyconnect-win-2.0.0343-k9.pkg       Erowsee Flash         Upload         Upload         OK         Click OK.         Click OK.         Click OK.         OK         OK         OK         OK         OK         Olspan="2">OK         OK         Click OK.         Click OK         OK         OK         OK         Click OK         <  |   | admin.cfg                       | 1,220               | 09/20/07 09:51:38            |                   |
| asam=bu2.bin       6,889,74       01/03/08 21:33:26         asa722-k8.bin       6,312,832       02/13/07 04:16:30         asam522-k8.bin       5,623,108       02/12/07 05:53:48         asa802-k8.bin       14,524,416       01/03/08 21:24:42         old_running.cfg       1,841       09/20/07 09:51:38         sslclient-win-1.1.4.179       418,765       03/14/08 13:47:58         File Name:       anyconnect-win-2.0.0343-k9.pkg       03/14/08 13:47:58         Filesh SVC Image:       ct-win-2.0.0343-k9.pkg       Browsee Flash         Upload       OK       Cancel       Help         Click OK.       Cliquez sur       Add.         Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings       Identify SSL VPN Client (SVC) related files.         SSL VPN Client Images       Minimize connection setup time by moving the image used by the most commonly encountered operation system to 1         Minimize connection setup time by moving the image used by the most commonly encountered operation system to 1         Minimize connection setup time by moving the image used by the most commonly encountered operation system to 1         Minimize connection setup time by moving the image used by the most commonly encountered operation system to 1         Minimize connection setup time by moving the image used by the most commonly encountered operation system to 1  |   | anyconnect-win-2.0.03           | 2,635,734           | 08/13/07 04:14:50            |                   |
| asar22-ts.bin       5,012,000       02/12/07         asdm-522.bin       5,623,108       02/12/07         asa802-t8.bin       14,524,416       01/03/08         old_running.cfg       1,841       09/20/07         old_running.cfg       1,841       09/20/07         old_running.cfg       1,841       09/20/07         sslclient-win-1.1.4.179       418,765       03/14/08         File Name:       anyconnect-win-2.0.0343-k9.pkg         File Name:       envyconnect-win-2.0.0343-k9.pkg         Flash SVC Image:       ct-win-2.0.0343-k9.pkg         Browse Flash       Upload         OK       Cancel       Help         Cliquez sur       Add.         Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client (SVC) related files.         SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to 1         Add       Replace       Delete Move UP Move Down         disk0:/anyconnect-win-2.0.0343-k9.pkg       Move Down   |   | asdm-602.bin                    | 0,009,704           | 01/03/08 21:38:26            |                   |
| asa802-k8.bin       14,524,416       01/03/08 21:24:42         old_running.cfg       1,841       09/20/07 09:51:38         sslclient-win-1.1.4.179       418,765       03/14/08 13:47:58         File Name: anyconnect-win-2.0.0343-k9.pkg         File Name: anyconnect-win-2.0.0343-k9.pkg         File Name: anyconnect-win-2.0.0343-k9.pkg         File Name: C-win-2.0.0343-k9.pkg         Filesh SVC Image: ct-win-2.0.0343-k9.pkg         Cliquez sur         Add SSL VPN Client Image         Flash SVC Image: ct-win-2.0.0343-k9.pkg         Direct Cliquez sur         Add.         Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client (SVC) related files.         SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to the state of the setup of the prove Down         disk0://anyconnect-win-2.0.0343-k9.pkg  |   | asa/22-Ko.Din                   | 5 623 108           | 02/12/07 05:53:48            |                   |
| Image:       Image:       Image:       Image:         File Name:       anyconnect-win-2.0.0343-k9.pkg         File Name:       anyconnect-win-2.0.0343-k9.pkg         Image:       File Name:         Image:       Image:         Image:       Cliquez sur         OK       Cancel         Help       Cliquez sur         Add.       Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client Images       Move UP ✓ Move Down         Minimize connection setup time by moving the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the image uset the image used by the image used by the image used   |   | asa802-k8 bip                   | 14,524,416          | 01/03/08 21:24:42            |                   |
| Side Miningerg       1,01       01,01,01   |   | old rupping.cfg                 | 1.841               | 09/20/07 09:51:38            |                   |
| File Name:       anyconnect-win-2.0.0343-k9.pkg         File Name:       anyconnect-win-2.0.0343-k9.pkg         Browse Flash       Flash SVC Image:         Ct-win-2.0.0343-k9.pkg       Browse Flash         Upload       OK         Cancel       Help         Cliquez sur         Add.         Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client (SVC) related files.         SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to Image and Participation and Participation system to Image and Participation system to Image and Participation and Participation system to Image and Partipation system to Image and Partipation system to Ima   |   | sslclient-win-1.1.4.179         | 418,765             | 03/14/08 13:47:58            |                   |
| File Name:       anyconnect-win-2.0.0343-k9.pkg         Image:       Flash SVC Image:         Ct-win-2.0.0343-k9.pkg       Browse Flash         Upload       Upload         OK       Cancel         Help       Cliquez sur         Add.         Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client (SVC) related files.         SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the most commonly encountered operation system to the image used by the image used by the image used by the image  |   |                                 |                     |                              |                   |
| Image:       Add SSL VPN Client Image         Flash SVC Image:       ct-win-2.0.0343-k9.pkg         Browse Flash       Upload         Upload       OK         Cancel       Help         Click OK.       Cliquez sur         Add.         Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client (SVC) related files.         SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to Image and Prove Down         disk0:/anyconnect-win-2.0.0343-k9.pkg  | File Name:  | anyconnect-win-2.0.0343-k9.p    | ikg 🛛               |                              |                   |
| Flash SVC Image:       ct-win-2.0.0343-k9.pkg       Browse Flash         Upload       Upload         OK       Cancel       Help         Click OK.       Cliquez sur         Add.         Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client (SVC) related files.         SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to the files.         SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to the files.         Minimize connection setup time by moving the image used by the most commonly encountered operation system to the files.         Minimize connection setup time by moving the image used by the most commonly encountered operation system to the files.         Move UP       ✓ Move Down         disk0:/anyconnect-win-2.0.0343-k9.pkg  | 🔂 Add SSL VPN   | Client Image                    |                     | 2                            |                   |
| OK       Cancel       Help         Click OK.       Cliquez sur         Add.       Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client (SVC) related files.         SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to North and related files.         Generation         Identify SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to North and related files.         Idisk0://anyconnect-win-2.0.0343-k9.pkg   | Flash SVC Image:  | ct-win-2.0.0343-k9.pkg          | Browse Flash        |                              |                   |
| OK       Cancel       Help         Click OK.       Cliquez sur         Add.       Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client (SVC) related files.       SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to the Add  replace  Polete  Move UP  Move Down         disk0:/anyconnect-win-2.0.0343-k9.pkg   |   | ,                               | Upload              |                              |                   |
| OK       Cancel       Help         Click OK.       Cliquez sur         Add.       Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client (SVC) related files.       SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to the Add  related file for the Move UP  related for the Move Down         disk0:/anyconnect-win-2.0.0343-k9.pkg   |   |                                 |                     |                              |                   |
| Add.<br>Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings<br>Identify SSL VPN Client (SVC) related files.<br>SSL VPN Client Images<br>Minimize connection setup time by moving the image used by the most commonly encountered operation system to the<br>Add @ Replace @ Delete 	 Move UP 	 Move Down<br>disk0:/anyconnect-win-2.0.0343-k9.pkg  |   | Cancel                          | Help                |                              |                   |
| Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings         Identify SSL VPN Client (SVC) related files.         SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to the Add related file files.         Image: Provide the time of the time by moving the image used by the most commonly encountered operation system to the time of the time of the time operation system to the time operation system to the time operation to the time operation operation operation system to the time operation operation operation to the time operation operation operation operation to the time operation operation operation operation to the time operation ope  |   |                                 |                     | Cliquez sur                  |                   |
| Identify SSL VPN Client (SVC) related files.<br><b>SSL VPN Client Images</b><br>Minimize connection setup time by moving the image used by the most commonly encountered operation system to the setup of the set | Configuration > Remote Acces  | s VPN > Network (Client) Acce   | ess > Advanced > S  | SL VPN > Client Settings     |                   |
| SSL VPN Client Images         Minimize connection setup time by moving the image used by the most commonly encountered operation system to the Add  | Identify SSL VPN Client (SVC) re  | lated files.                    |                     |                              |                   |
| Add      Replace      P Delete      Move UP      ✓ Move Down     disk0:/anyconnect-win-2.0.0343-k9.pkg  | SSL VPN Client Images   | by moving the image used by the | most commonly encou | ntered operation system to t |                   |
| disk0:/anyconnect-win-2.0.0343-k9.pkg   | 🕹 Add 📝 Replace 📋 D   | velete 🛧 Move UP 🗲 Move         | Down                |                              |                   |
|   | disk0:/anyconnect-win-2.0.034   | 3-k9.pkg                        |                     |                              |                   |

Configuration CLI équivalente :

4. Configurez la stratégie de groupe.Choisissez Configuration > Remote Access VPN > Network (Client) Access > Group Policies afin de créer une stratégie de groupe interne clientgroup. Sous l'onglet General, sélectionnez la case à cocher SSL VPN Client afin d'activer le WebVPN comme protocole de

| tui | nellisation.<br>Add Internal Group Policy                                |  |
|-----|--|--|
|     | General<br>Servers<br>⊡-Advanced<br>Split Tunneling<br>—IE Browser Proxy | Name: Clientgroup Banner: I Inherit Address Pools: I Inherit |
|     |  | More Options   |
|     |  | Tunneling Protocols:   |

Dans l'onglet **Advanced > Split Tunneling**, décochez la case à cocher **Inherit** pour la stratégie de split tunneling et choisissez **Tunnel Network List Below** dans la liste déroulante.

| Ī | Add Internal Group Policy         |   | x                               |
|---|-----------------------------------|---|---------------------------------|
|   | General<br>Servers<br>-Advanced   | Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those<br>require tunneling. The security appliance makes split tunneling decisions on the basis of a network list.<br>ACL that consists of list of addresses on the private network. | se that do not<br>, which is an |
|   | IE Browser Proxy                  | DNS Names: 🔽 Inherit  |                                 |
|   | -SSL VPN Client    SSL VPN Client | Policy: Tunnel All Networks   |                                 |
|   |                                   | Natural Lists Toharth Tunnel Al Networks  | Manage                          |
|   |                                   | Tunnel Network List Below   | managerri                       |
|   |                                   | Exclude Network List Below  |                                 |

Décochez la case à cocher Inherit pour Split Tunnel Network List et cliquez ensuite sur Manage afin de lancer l'ACL Manager

| file Edit Internal Group Policy:                         | hivalleyvpn   |
|--|---|
| General<br>Servers                                       | Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not<br>require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an<br>ACL that consists of list of addresses on the private network. |
|  | DNS Names: 🔽 Inherit  |
| SSL VPN Client     IPsec Client                          | Policy: Tunnel Network List Below   |
| Client Access Rule<br>Client Firewall<br>Hardware Client | Network List: Inherit None  |

Dans le gestionnaire ACL, choisissez **Ajouter > Ajouter une ACL...** afin de créer une nouvelle liste

d'accès.

| <u>1</u> | ACL Manager  |            |         |             |  |
|----------|--|------------|---------|-------------|--|
| ſ        | Standard ACL Extended  | ACL        |         |             |  |
|          | 🔂 Add 🕞 📝 Edit 📋   | Delete 🛧 🗲 | * * * ® | *           |  |
|          |  |            |         |             |  |
|          | 🔂 Add ACL  | dress      | Action  | Description |  |
|          | <ul> <li>Add ACL</li> <li>Add ACE</li> </ul>                 | dress      | Action  | Description |  |
|          | <ul> <li>Add ACL</li> <li>Add ACE</li> <li>Insert</li> </ul> | dress      | Action  | Description |  |

Fournissez un nom pour l'ACL et cliquez sur

| OK       | •           |              |                   |         |   |             |
|----------|-------------|--------------|-------------------|---------|---|-------------|
| <b>1</b> | ACL Manag   | er           |                   |         |   |             |
| ſ        | Standard AC | L Extend     | ed ACL            |         |   |             |
|          | 💠 Add 🔸     | 📑 Edit       | <u>î</u> Delete 🔶 | 4 🕺 🖻 🛍 | - |             |
|          | No          |              | Address           | Action  |   | Description |
|          | 🔂 Add A     | ,<br>CL      |                   |         | × |             |
|          | ACL Nar     | me: split-tu | nnel              |         |   |             |
|          |             | ок           | Cancel            | Help    |   |             |

Une fois le nom de l'ACL créé, choisissez Add > Add ACE afin d'ajouter une entrée de contrôle d'accès (ACE).Définissez l'ACE qui correspond au LAN derrière l'ASA. Dans ce cas, le réseau est 10.77.241.128/26 et sélectionnez Permit comme action.Cliquez sur OK afin de quitter l'ACL

Manager.

| No          | Address              | Action | Description |          |
|-------------|----------------------|--------|-------------|----------|
| split-tunne | el                   |        |             |          |
| 🔄 Add AC    | E                    |        |             |          |
| Host/Ne     | stwork               |        |             |          |
| IP Ad       | dress: 10.77.241.128 |        |             | <b>_</b> |
| Netma       | ask: 255.255.255.192 |        |             | <b>•</b> |
|             |                      |        |             |          |

Assurez-vous que l'ACL que vous venez de créer est sélectionné pour la liste de réseaux à split tunneling. Cliquez sur **OK afin de retourner à la configuration de la stratégie de aroupe.** 

| grouper  |  |   |   |  |  |                                      |                                |                                   |
|--|--|---|---|--|--|--------------------------------------|--------------------------------|-----------------------------------|
| 🔂 Add Internal Group Policy  |  |   |   |  |  |                                      |                                | ×                                 |
| General<br>Servers<br>- Advanced<br>- IE Browser Proxy<br>- SSL VPN Client<br>+ IPsec Client | Split tunneling<br>require tunne<br>ACL that cons<br>DNS Names:<br>Policy: | ing. The sec<br>ling. The sec<br>sists of list of<br>Inherit<br>Inherit | s distinguish net<br>urity appliance r<br>addresses on th<br>Tunnel Netwo | works that re<br>nakes split tun<br>he private net<br>rrk List Below | quire traffic to g<br>ineling decisions<br>work. | go through the to<br>on the basis of | unnel and the<br>a network lis | ose that do not<br>t, which is an |
|  | Network List:  | 🕅 Inherit   | split-tunnel  |  |  |                                      |                                | Manage                            |
|  | Intercept  | DHCP Confi  | guration Mes  | sage from M  | licosoft Client                                  | s                                    |                                | ۲                                 |

Sur la page principale, cliquez sur **Apply, puis sur Send (s'il y a lieu) afin d'envoyer les commandes à l'ASA**.Configurez les paramètres de **VPN SSL en mode Stratégie de groupe**.Pour l'option Keep Installer on Client System, désélectionnez la case à cocher **Inherit, puis cliquez sur le bouton radio Yes**.Cette action permet au logiciel de SVC pour demeurer sur l'ordinateur client. Par conséquent, il n'est pas nécessaire que l'ASA télécharge le logiciel SVC sur le client chaque fois qu'une connexion est établie. Cette option est un bon choix pour les utilisateurs distants qui accèdent souvent au réseau de l'entreprise.

| 🧱 Ealt Internal Group Poli | cy: clientgroup                  |           |           |           |
|----------------------------|----------------------------------|-----------|-----------|-----------|
| General                    | Keep Installer on Client System: | 🔲 Inherit | • Yes     | C No      |
| -Servers                   | Compression:                     | 🔽 Inherit | C Enable  | C Disab   |
| Split Tunneling            | Datagram TLS:                    | 🔽 Inherit | C Enable  | C Disab   |
| Login Setting              | Keepalive Messages:              | 🔽 Inherit | 🗖 Disable | Interval: |

Cliquez sur Login Setting afin de paramétrer Post Login Setting et Default Post Login Selection comme indiqué.

| ndiqué.          |   |
|------------------|---|
| General          | After successfully logging in, user can have the choice to download the client software, or g |
| -Servers         | portal page. The following settings decides what will happen.                                 |
| E-Advanced       | 🔲 Inherit   |
| -Split Tunneling |   |
| IE Browser Proxy | Post Login Setting  |
| -SSL VPN Client  | Do not prompt user to choose  |
| Key Regeneration | C Prompt user to choose   |
| Customization    | User has seconds to choose, or Default Post Login Selection below is take                     |
|                  | Default Post Login Selection  |
|                  | C Go to Clientless SSL VPN portal   |
|                  | Download SSL VPN Client   |

Pour l'option Renegotiation Interval, décochez la case Inherit, décochez la case à cocher Unlimited et saisissez le nombre de minutes jusqu'à une nouvelle saisie. La sécurité est améliorée en fixant des limites à la durée de validité d'une clé. Pour l'option Renegotiation Method, décochez la case à cocher Inherit et cliquez sur la case d'option SSL. La renégociation peut utiliser le tunnel SSL actuel ou un nouveau tunnel créé expressément pour la

renégociation.

| General                           | Renegotiation Interval: | 🔲 Inherit | 🔲 Unlimited | 30    | minutes      |
|-----------------------------------|-------------------------|-----------|-------------|-------|--------------|
|                                   | Renegotiation Method:   | 🔲 Inherit | O None      | ⊙ SSL | O New Tunnel |
| -Split Tunneling                  |                         |           |             |       |              |
| -IE Browser Proxy                 |                         |           |             |       |              |
| 🖨 SSL VPN Client                  |                         |           |             |       |              |
| Login Setting<br>Key Regeneration | D                       |           |             |       |              |

Cliquez sur OK, puis sur Apply.

| Configuration > Remote Access VPN > N   | letwork (Client) Access   | > Group Policies   |                       |
|---|---|--|-----------------------|
| Manage VPN group policies. A VPN group (<br>externally on a RADIUS/LDAP server. The | policy is a collection of user-o<br>group policy information is r | priented attribute/value pairs that may be st<br>referenced by VPN tunnel groups and user ar | ored inter<br>counts. |
| 🔂 Add 🔻 📝 Edit 📋 Delete   |   |  |                       |
| Name  | Туре  | Tunneling Protocol   |                       |
| (clientgroup)   | Internal  | svc  | N/A -                 |
| DfltGrpPolicy (System Default)  | Internal  | L2TP-IPSec,IPSec,webvpn  | N/A -                 |

#### Configuration CLI équivalente :

5. Choisissez Configuration > Remote Access VPN > AAA Setup > Local Users > Add afin de créer un nouveau compte utilisateur ssluser1. Cliquez sur OK, puis sur

| Apply.<br>Add User Account |   |
|----------------------------|---|
|                            |   |
|                            | Username: ssluser1  |
|                            | Password: ******  |
|                            | Confirm Password: ******  |
|                            | User authenticated using MSCHAP   |
|                            | Member-of   |
|                            | Member-of: Add >> Delete  |
|                            | Access Restriction  |
|                            | Select one of the options below to restrict ASDM, SSH, Telnet and Console access. |
|                            | Note: All users have network access, regardless of these settings.                |
|                            | Full access(ASDM, SSH, Telnet and Console)  |
|                            | Privilege level is used with command authorization.                               |
|                            | Privilege Level: 2  |
|                            | CLI login prompt for SSH, Telnet and console (no ASDM access)                     |
|                            | This setting is effective only if AAA authenticate console command is configured. |
|                            | No ASDM, SSH, Telnet or Console access  |
|                            | This setting is effective only if AAA authenticate console command is configured. |

#### Configuration CLI équivalente :

 Choisissez Configuration > Remote Access VPN > AAA Setup > AAA Servers Groups > Edit afin de modifier le groupe de serveurs par défaut LOCAL en cochant la case à cocher Enable Local User Lockout avec comme valeur de tentatives maximale 16.

| Configurat | ion > Remote  | Access VPN > AA   | A Setup > AAA Serve  | r Groups  |   |
|------------|---|---|--|---|---|
| AAA Serve  | er Groups —   |   |  |   |   |
| Ser        | ver Group   | Protocol  | Accounting Mode  | Reactivation Mode   |   |
| LOCAL      |   | LOCAL   |  |   |   |
|            | Edit LOCA<br>This feature<br>before lockin<br>when the loc<br>Enable L<br>Maximum | AL Server Group<br>allows you to speci-<br>ig out and denying<br>al database is used<br>ocal User Lockout<br>Attempts: 16 | fy the maximum number<br>access to the user. This<br>I for authentication. | of failed attempts to allow<br>limit is applicable only<br>Help | ~ |
| •          |   | ОК  | Cancel   | Help  |   |

- 7. Cliquez sur OK, puis sur Apply.Configuration CLI équivalente :
- 8. Configurez le groupe de tunnels.Choisissez Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles Connection Profiles > Add afin de créer un nouveau groupe de tunnels sslgroup.Dans l'onglet Basic, vous pouvez exécuter la liste des configurations indiquée :Donnez au groupe de tunnels le nom sslgroup.Sous Client Address Assignment, choisir le pool d'adresses vpnpool dans la liste déroulante.Sous Default Group Policy, choisir la stratégie de groupe clientgroup dans la liste

| 1 | Add SSL VPN Connection             | Profile                |                                 |        |
|---|------------------------------------|------------------------|---------------------------------|--------|
|   | <mark>⊕Basic)</mark><br>⊕–Advanced | Name:<br>Aliases:      | ssigroup                        |        |
|   |                                    | Authentication ——      |                                 |        |
|   |                                    | Method:                | AAA C Certificate C Both        |        |
|   |                                    | AAA Server Group:      | LOCAL                           | Manag  |
|   |                                    |                        | Use LOCAL if Server Group fails |        |
|   |                                    | Client Address Assign  | nent                            |        |
|   |                                    | DHCP Servers:          |                                 |        |
|   |                                    | Client Address Pools:  | vpnpool                         | Select |
|   |                                    | Default Group Policy   |                                 |        |
|   |                                    | Group Policy:          | clientgroup                     | Manag  |
|   |                                    | SSL VPN Client Protoco | I: 🔽 Enabled                    |        |
|   |                                    | ОК                     | Cancel Help                     |        |

Sous l'onglet SSL VPN > Connection Aliases, spécifiez sslgroup\_users comme nom d'alias du groupe et cliquez sur

| Add SSL VPN Connection | Profile  |
|------------------------|--|
| Basic                  | Portal Page Customization: DfltCustomization       |
| -Advanced              |  |
| -General               | CSD Alternate Group Policy: [DritGrpPolicy         |
| -Client Addressing     | Enable the display of Radius Reject-Message on the |
| Authorization          |  |
| Accounting             | Connection Aliases                                 |
| SSL VPN                | 🔂 Add 🕽 📝 Delete                                   |
|                        |  |
|                        | 🔂 Add Connection Alias                             |
|                        |  |
|                        | Allas: [ssigroup_users                             |
|                        | Enabled  |
|                        |  |
|                        | G OK Cancel Help                                   |
|                        |  |
|                        | 🔁 Add 🛛 🖉 Delete                                   |

z sur OK, puis sur Apply.Configuration CLI équivalente :

9. Configurez NAT.Choisissez Configuration > Firewall > NAT Rules > Add Dynamic NAT Rule de façon à ce que le trafic venant de l'intérieur du réseau puisse être traduit avec l'adresse IP externe

| 2.16.1.5.<br>Add Dynam         | ic NAT Rule                      |                                     |
|--------------------------------|----------------------------------|-------------------------------------|
| Original —                     |                                  |                                     |
| Interface: in                  | side                             |                                     |
| Source:                        | ny                               |                                     |
| Translated —<br>Select a globa | al pool for dynamic translation. |                                     |
| Pool ID                        | Interface                        | Addresses Pool                      |
| 0                              | (outbound)                       | Same as original address (identity) |
| 0                              | (inbound)                        | Same as original address (identity) |
| 1                              | outside                          | 🖳 172.16.1.5                        |
|                                |                                  |                                     |

OK.Click OK.

| Co | onfigura   | tion > Firewall > NA | AT Rules   |             |             |                    |      |
|----|------------|----------------------|------------|-------------|-------------|--------------------|------|
|    | 🔂 Add      | 🝷 🗹 Edit ม De        | lete 🛧 🗲 👗 | 🖻 💼 🗉 🔍     | Find 🐏 Diag | gram 🛛 🥰 Packet Tr | race |
| Γ  | #          | Tupa                 |            | Original    |             |                    |      |
|    | *          | туре                 | Source     | Destination | Service     | Interface          |      |
|    | 🗄 inside i | (1 Dynamic rules)    |            |             |             |                    |      |
|    | 1          | <b>Dynamic</b>       | 🌍 any      |             |             | outside            |      |

Cliquez sur Apply. Configuration CLI équivalente :

10. Configurez l'exemption nat pour le trafic de retour du réseau interne vers le client VPN. ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0 ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0 ciscoasa(config)#nat (inside) 0 access-list nonat

#### Configuration de l'interface de ligne de commande ASA

| Cisco ASA 8.0(2)                             |
|--|
|  |
| ciscoasa(config)# <b>show running-config</b> |
| : Saved                                      |
| :  |
| ASA Version 8.0(2)                           |
| !  |
| hostname ciscoasa                            |
| domain-name default.domain.invalid           |
| enable password 8Ry2YjIyt7RRXU24 encrypted   |
| names  |
|  |
| interface Ethernet0/0                        |
| nameif inside                                |
| security-level 100                           |
| 1p address 10.//.241.142 255.255.255.192     |
| :<br>interface Ethernot(/1                   |
| nameif outside                               |
| security-level 0                             |
| ip address 172.16.1.1 255.255.255.0          |
|  |
| interface Ethernet0/2                        |
| shutdown                                     |
| no nameif                                    |
| no security-level                            |
| no ip address                                |
| !  |
| interface Ethernet0/3                        |
| shutdown                                     |
| no nameif                                    |
| no security-level                            |
| no ip address                                |
|  |
| interface ManagementU/U                      |
|  |
|  |
| no in address                                |
|  |
| passwd 2KFOnbNIdI.2KYOU encrypted            |
| boot system disk0:/asa802-k8.bin             |
|  |

ftp mode passive clock timezone IST 5 30 dns server-group DefaultDNS domain-name default.domain.invalid access-list split-tunnel standard permit 10.77.241.128 255.255.255.192 !--- ACL for Split Tunnel network list for encryption. access-list nonat permit ip 10.77.241.0 192.168.10.0 access-list nonat permit ip 192.168.10.0 10.77.241.0 !--- ACL to define the traffic to be exempted from NAT. pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0 !--- The address pool for the Cisco AnyConnect SSL VPN Clients no failover icmp unreachable rate-limit 1 burstsize 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400 global (outside) 1 172.16.1.5 !--- The global address for Internet access used by VPN Clients. !--- Note: Uses an RFC 1918 range for lab setup. !--- Apply an address from your public range provided by your ISP. nat (inside) 0 access-list nonat !--- The traffic permitted in "nonat" ACL is exempted from NAT. nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 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 no crypto isakmp nat-traversal telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list 1 class-map inspection\_default match default-inspection-traffic 1 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 esmtp  |
| inspect sqlnet   |
| inspect sunrpc   |
| inspect tftp   |
| inspect sip  |
| inspect xdmcp  |
| !  |
| service-policy global_policy global  |
| webvpn   |
| enable outside   |
| <pre>! Enable WebVPN on the outside interface svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1</pre>  |
| <pre>! Assign an order to the AnyConnect SSL VPN Client image svc enable</pre>   |
| <pre>! Enable the security appliance to download SVC<br/>images to remote computers tunnel-group-list enable</pre>   |
| ! Enable the display of the tunnel-group list on the<br>WebVPN Login page group-policy clientgroup internal  |
| <pre>! Create an internal group policy "clientgroup" group-policy clientgroup attributes vpn-tunnel-protocol svc</pre>   |
| <pre>! Specify SSL as a permitted VPN tunneling protocol split-tunnel-policy tunnelspecified</pre>   |
| split-tunnel-network-list value split-tunnel   |
| split-tunnel-network-list value split-tunnel   |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed</pre>   |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the stort of the log security with the veloce to be </pre>   |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place from 1 to 10000 (1 week) are prime articled.</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ' Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ' When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ' Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl</pre>   |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ' Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ' When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ' Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ' Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ' Create a user account "ssluser1" tunnel-group</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn     svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn    svc keep-installer installed ! When the security appliance and the SVC perform a   rekey, they renegotiate ! the crypto keys and   initialization vectors, increasing the security of the   connection. svc rekey time 30 ! Command that specifies the number of minutes from   the start of the ! session until the rekey takes   place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes   place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group   sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as   remote access tunnel-group sslgroup general-attributes</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes address-pool vpnpool</pre>  |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes address-pool vpnpool ! Associate the address pool vpnpool created default- group-policy clientgroup</pre> |
| <pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes address-pool vpnpool ! Associate the address pool vpnpool created default- group-policy clientgroup</pre> |

tunnel-group sslgroup webvpn-attributes



#### Établir la connexion VPN SSL avec SVC

Exécutez ces étapes afin d'établir une connexion VPN SSL avec l'ASA :

1. Saisissez l'URL ou l'adresse IP de l'interface WebVPN de l'ASA dans votre navigateur Web avec le format indiqué.

| OU   |  |
|--|--|
| https:// <ip address="" asa="" of="" the="" web<br="">WebVPN Service - Microsoft Inter-</ip> | bVPN interface><br>ernet Explorer  |
| File Edit View Favorites Tools   | Help   |
| 🕝 Back 🔹 🕥 🐇 📓 🔮   | 🏠 🔎 Search 🤺 Favorites 🤣 🎯 🖓 🔜 🦓   |
| Address ahttps://172.16.1.1/+webvpn-   | +/index.html   |
| CISCO SYSTEMS  | ervice   |
|  |  |
|  | Login  |
| P  | Login<br>Please enter your username and password.  |
| P  | Login<br>Please enter your username and password.<br>USERNAME:                                       |
| P  | Login Please enter your username and password. USERNAME: PASSWORD:                                   |
| P  | Login Please enter your username and password. USERNAME: PASSWORD: GROUP: sslgroup_users             |
| P  | Login Please enter your username and password. USERNAME: PASSWORD: GROUP: sslgroup_users Login Clear |

2. Saisissez votre nom d'utilisateur et votre mot de passe. En outre, choisissez votre groupe correspondant dans la liste déroulante comme

|          |                  | Login                    |                 |
|----------|------------------|--------------------------|-----------------|
|          | Please enter you | r username and password. |                 |
|          | USERNAME:        | ssluser1                 | ]               |
|          | PASSWORD:        | •••••                    |                 |
|          | GROUP:           | sslgroup_users 🛛 👻       |                 |
| indiqué. |                  | Login Clear              | ]<br>Cette fené |

apparaît avant que la connexion VPN SSL ne soit

établie.



**emarque :** le logiciel ActiveX doit être installé sur votre ordinateur avant de télécharger le SVC.Vous obtenez cette fenêtre une fois que la connexion est établie.



3. Cliquez sur le verrou qui apparaît dans la barre des tâches de votre

| 📲 Cisco AnyCo                 | nnect VPN Client     |   |                  |
|-------------------------------|----------------------|---|------------------|
| 🔌 Connection                  | 🚯 Statistics 🔒 About |   |                  |
|                               | cisco                |   |                  |
| Connect to:                   | 172.16.1.1           | * |                  |
|                               |                      |   |                  |
|                               |                      |   |                  |
|                               |                      |   |                  |
|                               |                      |   |                  |
|                               |                      |   |                  |
|                               |                      |   |                  |
|                               | Disconnect           |   |                  |
| linateur. (PN session establi | shed.                | С | ette fenêtre app |

et fournit des informations au sujet de la connexion SSL. Par exemple, **192.168.10.1 est** l'adresse IP attribuée par l'ASA,

|                 | 16           |
|-----------------|--------------|
| CISC            | 0            |
| Tunnel State:   | Connected    |
| Client Address: | 192.168.10.1 |
| Server Address: | 172.16.1.1   |
| Bytes Sent:     | 23461        |
| Bytes Received: | 1111         |
| Time Connected: | 00:04:51     |
|                 |              |
| Details         |              |

informations sur la version de Cisco AnyConnect VPN



#### Client. The ceccilin echanic

### **Vérification**

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

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

• show webvpn svc — Affiche les images de SVC enregistrées dans la mémoire flash de l'ASA.

```
1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1
CISCO STC win2k+
2,0,0343
Mon 04/23/2007 4:16:34.63
```

- 1 SSL VPN Client(s) installed
- show vpn-sessiondb svc Affiche les informations sur les connexions SSL actuelles. ciscoasa#show vpn-sessiondb svc

```
Session Type: SVC
```

```
Username : ssluser1
```

| Assigned IP  | : | 192.168.10.1           | Public IP    | : | 192.168.1.1 |  |  |
|--|---|------------------------|--------------|---|-------------|--|--|
| Protocol   | : | Clientless SSL-Tunnel  | DTLS-Tunnel  |   |             |  |  |
| Encryption   | : | RC4 AES128             | Hashing      | : | SHA1        |  |  |
| Bytes Tx   | : | 194118                 | Bytes Rx     | : | 197448      |  |  |
| Group Policy   | : | clientgroup            | Tunnel Group | : | sslgroup    |  |  |
| Login Time   | : | 17:12:23 IST Mon Mar 2 | 4 2008       |   |             |  |  |
| Duration   | : | 0h:12m:00s             |              |   |             |  |  |
| NAC Result   | : | Unknown                |              |   |             |  |  |
| VLAN Mapping   | : | N/A                    | VLAN         | : | none        |  |  |
| show webvpn group-alias — Affiche l'alias configuré pour différents groupes. |   |                        |              |   |             |  |  |

• Snow webvpn group-allas — Affiche l'allas configure pour differen ciscoasa#show webvpn group-alias

Tunnel Group: sslgroup Group Alias: sslgroup\_users enabled

 Dans l'ASDM, choisissez la Monitoring > VPN > VPN Statistics > Sessions afin de connaître les sessions WebVPN actuelles dans

| 17   | ЮЛ.                                       |                 |                        |  |                   |  |              |                   |    |
|--|---|-----------------|------------------------|--|-------------------|--|--------------|-------------------|----|
| 6  | onitoring > VF                            | YN > VPN S      | tatisti                | cs > Sessions                          | >                 |  |              |                   |    |
| F  | Sessions                                  |                 |                        |  |                   |  |              |                   |    |
|  | Remote<br>Access Site-to-Site             |                 | Site                   |  | SSL VPN           | SSL VPN                                      |              | UDM Load Palancia | ~  |
|  |   |                 | Site                   | Clientless                             | With Client       | Total  | E-mail Proxy | VPN LOad balanci  | ig |
|  | 0   | 0 0             |                        | 0                                      | 0                 | 0  | 0            | 0                 |    |
|  | Filter By: 55L                            | VPN Client      |                        | All Sessions                           |                   |  | Fil          | lter              |    |
| Username Group Policy<br>IP Address Connection |   | Proto<br>Encryp | Protocol<br>Encryption |  | in Time<br>ration | By<br>By                                     |              |                   |    |
|  | ssluser1 clientgr<br>192.168.10.1 sslgrou |                 | roup<br>Jp             | Clientless SSL-Tunnel DT<br>RC4 AES128 |                   | . 17:12:23 IST Mon Mar 24 2008<br>0h:03m:31s |              | 194118<br>192474  |    |

## **Dépannage**

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

1. vpn-sessiondb logoff name <username> — Commande pour fermer la session VPN SSL

```
pour le nom d'utilisateur particulier.
ciscoasa#vpn-sessiondb logoff name ssluser1
Do you want to logoff the VPN session(s)? [confirm] Y
INFO: Number of sessions with name "ssluser1" logged off : 1
ciscoasa#Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xB000)
```

De même, vous pouvez employer la commande **vpn-sessiondb logoff svc afin de terminer toutes les sessions SVC.** 

2. **Remarque :** si le PC passe en mode veille ou veille prolongée, la connexion VPN SSL peut être interrompue.

```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, e
tc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
```

ciscoasa#**show vpn-sessiondb svc** INFO: There are presently no active sessions

 debug webvpn svc <1-255> — Fournit les événements webvpn en temps réel afin d'établir la session.

Ciscoasa#debug webvpn svc 7

```
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343
Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B
7D75F4EDEF26'
Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8
625B92C1338D631B08B7D75F4EDEF26 '
Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B
08B7D75F4EDEF26'
WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7
5F4EDEF26'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
... input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40
642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693 '
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AE
BAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693 '
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3
-SHA:DES-CBC-SHA'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
```

| SVC: NP setup  |
|--|
| np_svc_create_session(0x3000, 0xD41611E8, TRUE)                    |
| webvpn_svc_np_setup  |
| SVC ACL Name: NULL   |
| SVC ACL ID: -1   |
| SVC ACL ID: -1   |
| <pre>vpn_put_uauth success!</pre>                                  |
| SVC IPv6 ACL Name: NULL  |
| SVC IPv6 ACL ID: -1  |
| SVC: adding to sessmgmt  |
| SVC: Sending response  |
| Unable to initiate NAC, NAC might not be enabled or invalid policy |
| CSTP state = CONNECTED   |
| webvpn_rx_data_cstp  |
| webvpn_rx_data_cstp: got internal message                          |
| Unable to initiate NAC, NAC might not be enabled or invalid policy |
|  |

4. Dans l'ASDM, choisissez Monitoring > Logging > Real-time Log Viewer > View afin de voir les événements en temps

| rée       |  |   |   |
|-----------|--|---|---|
| 1         | lisco ASDM 6.0 for ASA - 10.77.241                 |   |   |
| File      | <u>View T</u> ools Wi <u>z</u> ards <u>W</u> indow |   | Look For:   |
| C         | Home 🦓 Configuration 📴 Moni                        | 🔚 Save 🔇 Refresh 🔇 Back 🚫 F   | orward 🧳 Help   |
| 1         | Logging 🗇 🖓 🗙                                      | Monitoring > Logging > Real-Time Log View                                       | er  |
| wice List | Real-Time Log Viewer                               | Real-Time Log Viewer  |   |
| De        |  | Click the View button below to start d<br>desired logging level to see messages | isplaying syslog messages in real time. Select the<br>at that severity or higher. |
|           |  | Logging Level: Debu   | gging 💌   |
|           |  | Buffer Limit: 1000  |   |
|           |  |   |   |
|           |  |   | View  |

Cet exemple montre que la session SSL a été établie avec le périphérique de tête de réseau.

| 💼 Real-Time Log Viewer - 10.77.241.142   |             |          |           |              |                |  |  |  |
|--|-------------|----------|-----------|--------------|----------------|--|--|--|
| Ele Tools Window Help  |             |          |           |              |                |  |  |  |
| 🕕 Pause   🖹 Copy 🎧 Save 🆓 Clear   📅 Color Settings   🏠 Create Rule 📸 Show Rule   🙆 Show Details   🤗 Help   |             |          |           |              |                |  |  |  |
| Filter By: Filter I Show All Find:   |             |          |           |              |                |  |  |  |
| Severity   | Date        | Time     | Syslog ID | Source IP    | Destination IP |  |  |  |
| <u>4</u> 6   | Mar 21 2008 | 20:03:36 | 725007    | 10.77.233.74 |                | SSL session with client inside:10.77.233.74/1026 terminated.               |  |  |
| <u>4</u> 6   | Mar 21 2008 | 20:03:35 | 106015    | 10.77.233.74 | 10.77.241.142  | Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44        |  |  |
| <u>4</u> 6   | Mar 21 2008 | 20:03:35 | 302014    | 10.77.233.74 | 10.77.241.142  | Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Identii     |  |  |
| <u>4</u> 6   | Mar 21 2008 | 20:03:35 | 605005    | 0.0.0.0      | 0.0.0.0        | Login permitted from 0.0.0.0/1026 to inside:0.0.0.0/https for user "enable |  |  |
| A 6  | Mar 21 2008 | 20:03:35 | 725002    | 10.77.233.74 |                | Device completed SSL handshake with dient inside:10.77.233.74/1026         |  |  |
| <u>4</u> 6   | Mar 21 2008 | 20:03:35 | 725003    | 10.77.233.74 |                | SSL client inside:10.77.233.74/1026 request to resume previous session.    |  |  |
| <u>∔</u> 6   | Mar 21 2008 | 20:03:35 | 725001    | 10.77.233.74 |                | Starting SSL handshake with client inside:10.77.233.74/1026 for TLSv1 se   |  |  |
| <u>4</u> 6   | Mar 21 2008 | 20:03:35 | 302013    | 10.77.233.74 | 10.77.241.142  | Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.23    |  |  |
|  |             |          |           |              |                |  |  |  |
| %ASA-6 725002 Device completed SSL handshake with remote_device interface_name:IP_address/port<br>The SSL handshake has completed successfully with the remote device. |             |          |           |              |                |  |  |  |

## Informations connexes

- Page de support pour appliances de sécurité adaptables de la gamme Cisco 5500
- Notes de publication relatives au client VPN d'AnyConnect, Version 2.0
- ASA/PIX : Permettre le split tunneling pour des clients VPN sur l'exemple de configuration de l'ASA
- Exemple de configuration d'un routeur autorisant les clients VPN à se connecter à lPsec et à Internet via la transmission tunnel partagée
- PIX/ASA 7.x et client VPN pour le VPN d'Internet public sur un exemple de configuration de bâton
- Exemple de configuration d'un client VPN SSL (SVC) sur ASA avec ASDM
- <u>Support et documentation techniques Cisco Systems</u>