# Exemple de configuration d'un VPN SSL client léger (WebVPN) sur ASA avec ASDM

## Contenu

Introduction Conditions préalables **Conditions requises Components Used** Diagramme du réseau Conventions Informations générales Configuration VPN SSL client léger à l'aide d'ASDM Étape 1. Activer WebVPN sur l'ASA Étape 2. Configuration des caractéristiques de transfert de port Étape 3. Créer une stratégie de groupe et la lier à la liste de transfert de port Étape 4. Créer un groupe de tunnels et le lier à la stratégie de groupe Étape 5. Créer un utilisateur et ajouter cet utilisateur à la stratégie de groupe Configuration VPN SSL client léger à l'aide de l'interface de ligne de commande Vérification Pro<u>cédure</u> Commandes Dépannage Le processus de connexion SSL est-il terminé ? Le client léger VPN SSL est-il fonctionnel ? Commandes Informations connexes

## **Introduction**

La technologie Thin-Client VPN SSL permet l'accès sécurisé pour certaines applications dotées de ports statiques, telles que Telnet(23), SSH(22), POP3(110), IMAP4(143) et SMTP(25). Vous pouvez utiliser Thin-Client VPN SSL en tant qu'application déterminée axée sur l'utilisateur, axée sur la politique, ou les deux à la fois. C'est-à-dire que vous pouvez configurer l'accès selon chaque utilisateur, ou que vous pouvez créer des Politiques collectives auxquelles vous ajoutez un ou plusieurs utilisateurs.

 VPN SSL sans client (WebVPN) - Fournit un client distant nécessitant un navigateur Web compatible SSL pour accéder à des serveurs Web HTTP ou HTTPS sur un réseau local d'entreprise (LAN). En outre, le VPN SSL sans client permet l'exploration de fichiers Windows via le protocole Common Internet File System (CIFS). Outlook Web Access (OWA) est un exemple d'accès HTTP.Consultez l'Exemple de configuration d'un VPN SSL sans client

#### (WebVPN) sur une ASA afin d'en savoir plus sur le VPN SSL sans client.

- VPN SSL client léger (redirection de port) Fournit un client distant qui télécharge un petit applet basé sur Java et permet l'accès sécurisé aux applications de Protocole de contrôle de transmissions (TCP) qui utilisent des numéros de port statiques. Le Post Office Protocol (POP3), le Simple Mail Transfer Protocol (SMTP), le Protocole de messagerie IMAP, le Secure shell (SSH) et le telnet sont des exemples d'accès sécurisé. Puisque les fichiers sur l'ordinateur local changent, les utilisateurs doivent avoir des privilèges d'administrateur locaux pour utiliser cette méthode. Cette méthode de VPN SSL ne fonctionne pas avec les applications qui utilisent des affectations de ports dynamiques, telles que certaines applications de protocole de transfert de fichiers (FTP).Remarque : le protocole UDP (User Datagram Protocol) n'est pas pris en charge.
- Client VPN SSL (Mode Tunnel) Télécharge un petit client sur le poste de travail distant et permet un accès entièrement sécurisé aux ressources d'un réseau d'entreprise interne. Vous pouvez télécharger de manière permanente le client VPN SSL (SVC) sur une station de travail distante ou supprimer le client une fois la session sécurisée fermée.Référez-vous à <u>Exemple de configuration du client VPN SSL (SVC) sur ASA avec ASDM</u> afin d'en savoir plus sur le client VPN SSL.

Ce document présente une configuration simple pour le VPN SSL client léger sur l'appareil de sécurité adaptatif (ASA). La configuration permet à un utilisateur d'établir une connexion Telnet sécurisée à un routeur situé à l'intérieur de l'ASA. La configuration de ce document est prise en charge pour ASA version 7.x et ultérieure.

## **Conditions préalables**

#### **Conditions requises**

Avant de tenter cette configuration, assurez-vous de respecter les conditions suivantes pour les stations clientes distantes :

- Navigateur Web compatible SSL
- SUN Java JRE version 1.4 ou ultérieure
- Cookies activés
- Bloqueurs de fenêtres publicitaires intempestives désactivés
- Privilèges administratifs locaux (non requis mais fortement suggéré)

**Note :** La dernière version de SUN Java JRE est disponible en téléchargement gratuit sur le <u>site</u> <u>Java</u>.

#### **Components Used**

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

- Dispositif de sécurité adaptatif de la gamme Cisco 5510
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1)Remarque : référez-vous à <u>Autoriser</u> <u>l'accès HTTPS pour ASDM</u> afin de permettre à l'ASA d'être configuré par l'ASDM.
- Logiciel Cisco Adaptive Security Appliance Version 7.2(1)
- Client distant Microsoft Windows XP Professionnel (SP 2)

Les informations de ce document ont été élaborées dans un environnement de laboratoire. Tous

les périphériques utilisés dans ce document ont été réinitialisés à leur configuration par défaut. Si votre réseau est opérationnel, assurez-vous que vous comprenez l'impact potentiel de toute commande. Toutes les adresses IP utilisées dans cette configuration ont été sélectionnées à partir d'adresses RFC 1918 dans un environnement de laboratoire ; ces adresses IP ne sont pas routables sur Internet et sont utilisées à des fins de test uniquement.

#### Diagramme du réseau

Ce document utilise la configuration réseau décrite dans cette section.

Lorsqu'un client distant lance une session avec l'ASA, le client télécharge une petite applet Java sur la station de travail. Une liste des ressources préconfigurées est présentée au client.



#### **Conventions**

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## Informations générales

Afin de démarrer une session, le client distant ouvre un navigateur SSL à l'interface externe de l'ASA. Une fois la session établie, l'utilisateur peut utiliser les paramètres configurés sur l'ASA pour appeler n'importe quel accès Telnet ou d'application. L'ASA proxie la connexion sécurisée et permet à l'utilisateur d'accéder au périphérique.

**Remarque :** Les listes d'accès entrantes ne sont pas nécessaires pour ces connexions car l'ASA est déjà conscient de ce qui constitue une session juridique.

## Configuration VPN SSL client léger à l'aide d'ASDM

Afin de configurer le VPN SSL client léger sur l'ASA, procédez comme suit :

- 1. Activer WebVPN sur l'ASA
- 2. Configuration des caractéristiques de transfert de port
- 3. Créer une stratégie de groupe et la lier à la liste de transfert de port (créée à l'étape 2)
- 4. Créer un groupe de tunnels et le lier à la stratégie de groupe (créé à l'étape 3)
- 5. Créer un utilisateur et ajouter cet utilisateur à la stratégie de groupe (créée à l'étape 3)

#### Étape 1. Activer WebVPN sur l'ASA

Pour activer WebVPN sur l'ASA, procédez comme suit :

- 1. Dans l'application ASDM, cliquez sur Configuration, puis cliquez sur VPN.
- 2. Développez WebVPN, puis sélectionnez WebVPN
  - Access.

File Option Tools Warnets Help Seech Prod -   Hore Configuration Modebring Back Provad Refresh Save Help	📫 Cisco ASD	4 5.2 for ASA	10.2.2.1								🔳 🗆 🔀
Kore Correspondence   Kore Reference   Kore </td <td>File Options</td> <td>Tools Wizards</td> <td>Help</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>Search</td> <td>Find •</td>	File Options	Tools Wizards	Help							Search	Find •
Configure access parameters for Web/PNL         Web/PNLogn Page	S Home	Configuration	Monitoring	Back	Forward Pac	cket Tracer   F	<b>Q</b> lefresh	<b>Save</b>	? Help		Cesco Systems
cisco 15 Mar 6/27/06 7:01:44 AM UTC 7	Interfaces Security Policy NAT Security Policy	Contaurento VPNU Contaurento Contaurento Contaurento Contaurento Contaurento Contaurento Contaurento Pose NAC Contaurento NACONTAURENTO NACIONACIONACIONACIONACIONACIONACIONACIO	MicroPhysics Micro Areas Manager Areas Manager Areas Manager Areas	LS Interest	INTERVENT Access etv/PN Access Configure access para Interface Inside outside Port Number: Defauit Idle Timeout: Max. Sessions Limit: WebVPN Memory Size Enable Tunnel Geo	ameters for WebV 443 1800 2 : 50 sup Drop-down Li	/PN.	ebVPN Enable onds (total physica /PN Login Pa	ed No Yes al memory ge Reset		Enable Disable

- 3. Mettez l'interface en surbrillance, puis cliquez sur Enable.
- 4. Cliquez sur **Apply**, sur **Save**, puis sur **Yes** pour accepter les modifications.

Étape 2. Configuration des caractéristiques de transfert de port

Afin de configurer les caractéristiques de transfert de port, procédez comme suit :

1. Développez WebVPN, puis choisissez Port Forwarding.



2. Cliquez sur le bouton Add.

File Options T	ools Wizards	Help							Search		Find •
Some Home	oggi Configuration	Monitoring	Back	Forward	Packet Tracer	Refresh	Save	<b>?</b> Нер			Cisco Systems
Interfaces	Configuration	on × VPN × We Wizard eral VPN System Opt Client Update Tunnel Group Policy Users Default Tunnel G Zone Labs Integr	oven > Pro ions ateway ity Server	Post Forwardin	Configure port for This parameter	warding lists fo is enforced in Local TCP P	r application n either a V ort Rem	access over PN <u>user</u> or ote Server	WebVPN. group policy cor Remote TCP	figuration.	Add
VPN PS		c ddress Manager Assignment IP Pools ; ;vVPN	- LU	st Name:	Routers						
CSD Manager		WebVPN Access Proxies APCF Auto Signon Cache Content Rewrite Java Trustpoint Proxy Bypass Servers and URI Ront Followending Webpage Custor ACLs	5 	Local TCP Por	t Remote Ser	ver Remot	e TCP Port	Description	n		Add Edit Delete
rigeneo	8 🥞 E-ma	Encoding SSL VPN Client SSO Servers all Proxy				ок	Car	ncel	Help	 @ @,	/18/06 12:40:29 PM UTC

3. Dans la boîte de dialogue Ajouter une liste de transfert de port, entrez un nom de liste, puis cliquez sur **Ajouter**.La boîte de dialogue Ajouter une entrée de transfert de port s'affiche.

😼 Add Port Forwarding	Entry	×
Local TCP Port:	3044	
Remote Server:	10.2.2.2	
Remote TCP Port:	23	
Description:	Telnet to R1	
ок	Cancel Help	

4. Dans la boîte de dialogue Ajouter une entrée de transfert de port, entrez les options suivantes :Dans le champ Local TCP Port, saisissez un numéro de port ou acceptez la valeur par défaut.La valeur que vous entrez peut être n'importe quel nombre compris entre 1024 et 65535.Dans le champ Remote Server, saisissez une adresse IP.Cet exemple utilise l'adresse du routeur.Dans le champ Remote TCP Port, saisissez un numéro de port.Cet exemple utilise le port 23.Dans le champ Description, saisissez une description, puis cliquez sur **OK**.

- 5. Cliquez sur OK, puis sur Apply.
- 6. Cliquez sur Save, puis sur Yes pour accepter les modifications.

#### Étape 3. Créer une stratégie de groupe et la lier à la liste de transfert de port

Afin de créer une stratégie de groupe et de la lier à la liste de transfert de port, procédez comme suit :

1. Développez General, puis choisissez Group



 Cliquez sur Add, puis sélectionnez Internal Group Policy.La boîte de dialogue Ajouter une stratégie de groupe interne s'affiche.

Tunneling Protocols:	🔲 Inherit	VIPSec VWebVPN VL2TP over IPSec
Filter:	🗹 Inherit	Manage
Connection Settings		
Access Hours:	🗹 Inherit	Manage
Simultaneous Logins:	🗹 Inherit	
Maximum Connect Time:	🗹 Inherit	Unlimited minutes
Idle Timeout:	🗹 Inherit	Unlimited minutes
Servers		
DNS Servers:	🗹 Inherit	Primary: Secondary:
WINS Servers:	🗹 Inherit	Primary: Secondary:
DHCP Scope:	🔽 Inherit	

- 3. Entrez un nom ou acceptez le nom de stratégie de groupe par défaut.
- 4. Décochez la case Tunneling Protocols Inherit et cochez la case WebVPN.
- 5. Cliquez sur l'onglet **WebVPN** situé en haut de la boîte de dialogue, puis cliquez sur l'onglet **Fonctions**.
- 6. Décochez la case Hériter et cochez les cases Activer le téléchargement automatique des applets et Activer le transfert de port comme indiqué dans cette image
   :

<b>1</b>	dd Internal	Group Policy						X
	Name:	NetAdmins		1				
	reality.			1				
	General IPS	ec Client Configu	ration Clien	t Firewall Hardv	/are Clier	nt NAC WebVF	PN	
	Configure V	∕eb∨PN attributes u	sing the follo	wing tabs .				
	Check an Ini	nerit checkbox to le	t the corresp	onding setting tak	e its valu	e from the defau	t group policy.	
	Functions	Content Filtering	Homepage	Port Forwarding	Other	SSL VPN Client	Auto Signon	
	Inhe	rit						
	E	nable URL entry		E	nable por	t forwarding		
	E	nable file server ac	cess	E	nable Out	tlook/Exchange pr	оху	
	E 6	hable file server en	try		pply Wet	p-type ACL		
		nable file server bri nable auto applet d	owsing ownload		nable rittş nable Citr	ix MetaFrame		
								1
			OK		-al	Hale		_
			UN			rieip		

 Également dans l'onglet WebVPN, cliquez sur l'onglet Port Forwarding et décochez la case Port Forwarding List Inherit.

🖾 Add Internal Group Policy
Name: NetAdmins
General IPSec Client Configuration Client Firewall Hardware Client NAC WebVPN
Configure WebVPN attributes using the following tabs .
Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.
Functions Content Filtering Homepage Port Forwarding Other SSL VPN Client Auto Signon
Port Forwarding List: Inherit Routers New
Applet Name: Inherit Secure Router Access
Cancer I neip

- 8. Cliquez sur la flèche de la liste déroulante **Port Forwarding List**, puis sélectionnez la liste de transfert de port que vous avez créée à l'<u>étape 2</u>.
- 9. Décochez la case **Hériter** le nom de l'applet et modifiez le nom dans le champ de texte.Le client affiche le nom de l'applet lors de la connexion.
- 10. Cliquez sur **OK**, puis sur **Apply**.
- 11. Cliquez sur Save, puis sur Yes pour accepter les modifications.

#### Étape 4. Créer un groupe de tunnels et le lier à la stratégie de groupe

Vous pouvez modifier le groupe de tunnels *DefaultWebVPNroup* par défaut ou créer un nouveau groupe de tunnels.

Pour créer un nouveau groupe de tunnels, procédez comme suit :

1. Développez **General**, puis sélectionnez **Tunnel Group**.



 Cliquez sur Add, puis sélectionnez WebVPN Access.La boîte de dialogue Ajouter un groupe de tunnels s'affiche.

Name: General	NetGroup							
General		5		Type:	webypn			
	WebVPN							
L	THE THE							
Configu	re general acce	ss attributes fro	om the followi	ng sub-ta	abs.			
Basic	Authentication	Authorization	Accounting	Client A	ddress Assignm	ent Advanc	ed	
Grou	up Policy:	NetAdmins	~	•				
	Strip the realm f	rom username k	efore passing	g it on to	the AAA server			
	Strip the group t	rom username l	pefore passin	ig it on to	the AAA server			
Pas	sword Manager	nent						
l L	Epable potific	ount-disabled in	dication from	i AAA se	rver			
	Enable	notification prior	to expiration	uon to air	Notify	davs pri	or to expiration	n
		OK		Cano		Help	1	

- 3. Saisissez un nom dans le champ Nom.
- 4. Cliquez sur la flèche de la liste déroulante **Stratégie de groupe**, puis sélectionnez la stratégie de groupe que vous avez créée à l'<u>étape 3</u>.
- 5. Cliquez sur **OK**, puis sur **Apply**.
- 6. Cliquez sur **Save**, puis sur **Yes pour accepter les modifications.**Le groupe de tunnels, la stratégie de groupe et les caractéristiques de transfert de port sont maintenant liés.

#### Étape 5. Créer un utilisateur et ajouter cet utilisateur à la stratégie de groupe

Pour créer un utilisateur et l'ajouter à la stratégie de groupe, procédez comme suit :

1. Développez **General**, puis choisissez **Users**.

File Options To	ols Wizards	Help							Search		Find •
Home .	oggi Configuration	Monitoring	O Back	Forward	Recket Tracer	Q Refresh	Save	? Help			Cisco Systems
Home	Configuration	Monitoring Monitoring Mizard real VPN System Option Clent Update Funnel Group Group Policy Sector Conce Labos Integrity C PSec Rules Fransform Sets Yre-Fragmentation kiress Management Assignment P Pools VPN AboVPN Access	Back ral > User s S S	Forward Forward Create entries the user acco User Name mable 15 clsco wommi railes1	Packet Tracer	Refresh user datab be enforced Level (Role)	Save ase. Comman. To enable co VPN Group Po NA DitGrpPolicy DitGrpPolicy SalesGroupPoli	d author mmand licy cy	rization must be en authorization, go to VPN Group Lock NA Inherit Group Polic. Inherit Group Polic. Inherit Group Polic.	abled in order for	
Routing Global Objects Properties		Incodes APCF Auto Signon Content Rewrits Iover Trustpoint Incory Bypass Servers and URLs Servers and URLs ACLS Incoding SSL VPN Client SSO Servers al Proxy	at				Apply		Reset		

2. Cliquez sur le bouton **Add.**La boîte de dialogue Ajouter un compte d'utilisateur s'affiche.

🖆 Add User Account	
Identity VPN Palicy WebVPN	
The set of	
Username:	user1
Password:	*****
Confirm Password:	*****
User authenticate	ed using MSCHAP
Privilege level is used with	h command authorization
Privilege Level:	2
OK R	Cancel Help

3. Entrez les valeurs du nom d'utilisateur, du mot de passe et des informations de privilège, puis cliquez sur l'onglet **Stratégie VPN**.

Check an Inherit checkbox to let the co	prresponding setti	ing take its value from the gro	up policy.
Tunneling Protocols:	🗹 Inherit	IPSec WebVPN	L2TP over IPSec
Filter:	🗹 Inherit		Manage
Tunnel Group Lock:	🗹 Inherit		~
Store Password on Client System:	🗹 Inherit	⊖Yes ⊖No	
Connection Settings			
Access Hours:	🗹 Inherit		New
Simultaneous Logins:	🗹 Inherit		
Maximum Connect Time:	🗹 Inherit	Unlimited	minutes
Idle Timeout:	🔽 Inherit	Unlimited	minutes
Dedicated IP Address (Optional)			
IP Address:	Subr	net Mask:	~

- 4. Cliquez sur la flèche de la liste déroulante Stratégie de groupe, puis sélectionnez la stratégie de groupe que vous avez créée à l'étape 3. Cet utilisateur hérite des caractéristiques et des stratégies WebVPN de la stratégie de groupe sélectionnée.
- 5. Cliquez sur OK, puis sur Apply.
- 6. Cliquez sur Enregistrer, puis Oui pour accepter les modifications.

## Configuration VPN SSL client léger à l'aide de l'interface de ligne de commande

ASA	
	ſ
ASA Version 7.2(1)	
1	
hostname ciscoasa	
domain-name default.domain.invalid	
enable password 8Ry2YjIyt7RRXU24 encrypted	
names	
!	
interface Ethernet0/0	

```
nameif inside
 security-level 100
ip address 10.1.1.1 255.255.255.0
!--- Output truncated port-forward portforward 3044
10.2.2.2 telnet Telnet to R1
!--- Configure the set of applications that WebVPN
users !--- can access over forwarded TCP ports group-
policy NetAdmins internal
!--- Create a new group policy for enabling WebVPN
access group-policy NetAdmins attributes
vpn-tunnel-protocol IPSec 12tp-ipsec webvpn
!--- Configure group policy attributes webvpn
 functions port-forward auto-download
!--- Configure group policies for WebVPN
                                           port-forward
value portforward
!--- Configure port-forward to enable WebVPN
application access !--- for the new group policy port-
forward-name value Secure Router Access
!--- Configure the display name that identifies TCP
port !--- forwarding to end users username user1
password tJsDL6po9m1UFs.h encrypted
username user1 attributes
vpn-group-policy NetAdmins
!--- Create and add User(s) to the new group policy
http server enable http 0.0.0.0 0.0.0.0 DMZ no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart tunnel-group NetGroup type webvpn
tunnel-group NetGroup general-attributes
default-group-policy NetAdmins
!--- Create a new tunnel group and link it to the group
policy telnet timeout 5 ssh timeout 5 console timeout 0
! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect
sqlnet inspect sunrpc inspect tftp inspect sip inspect
xdmcp ! service-policy global_policy global webvpn
enable outside
!--- Enable Web VPN on Outside interface port-forward
portforward 3044 10.2.2.2 telnet Telnet to R1 prompt
hostname context
```

## **Vérification**

Utilisez cette section pour vérifier que votre configuration fonctionne correctement.

#### **Procédure**

Cette procédure décrit comment déterminer la validité de la configuration et comment la tester.

 Àpartir d'une station de travail client, saisissez https:// outside\_ASA\_IP Address ; où outside\_ASA\_IPAddress est l'URL SSL de l'ASA.Une fois le certificat numérique accepté et l'utilisateur authentifié, la page Web du service Web WebVPN s'affiche.

	vorites Tools Help					1
🚱 Back 🔹 🕥 -	🖹 🛢 🏠 🍃	🔎 Search 🛛 🔶 Fa	vorites 🔗	Ø• 🕹	w •	, »
Address 🙆 https://172	.22.1.160/+webvpn+/p	ortal.html		•	🖌 🄁 Go	Links »
Google -	~ G	Search 🔹 🧭 🗄	💋 🛃 Popu	ps okay »	SnagI 😌	t 🛃
Cisco Systems willingentillingen W	/ebVPN Servi	ce		2		
Start Application (	UTER Client Go	outer Access - M	icrosoft Int	ernet Ex		
			nor obvit mit			
Close this wi Please wait f If you shut de later have pr <u>details.</u>	ndow when you fir for the table to be own your compute oblems running th	nish using Appli displayed befor er without closin re applications l	cation Acc e starting : g this wind isted below	ess. applications ow, you mig v. <u>Click her</u> o	;ht <u>e for</u>	112
Close this wi Please wait f If you shut d later have pr <u>details.</u> Name Telnet to R1 SSH to R1	ndow when you fir for the table to be own your compute roblems running th Local 127.0.0.1:3044 127.0.0.1:3255	nish using Appli displayed befor er without closin te applications l Remote 10.2.2.2:23 10.2.2.2:22	cation Acc re starting : g this wind isted below Bytes Out 0 0	ess. applications ow, you mig v. <u>Click hero</u> Bytes In So 0	sht <u>e for</u> ockets 0 0	

L'adresse et les informations de port nécessaires pour accéder à l'application apparaissent dans la colonne locale. Les colonnes Octets sortants et Octets entrants n'affichent aucune activité car l'application n'a pas été appelée pour le moment.

- 2. Utilisez l'invite DOS ou une autre application Telnet pour démarrer une session Telnet.
- 3. Àl'invite de commandes, entrez telnet 127.0.0.1 3044.Remarque : cette commande fournit un exemple de la façon d'accéder au port local affiché dans l'image de page Web du service Web Web WebVPN de ce document. La commande n'inclut pas de deux-points (:). Tapez la commande comme décrit dans ce document.L'ASA reçoit la commande sur la session sécurisée, et comme il stocke une carte des informations, l'ASA sait immédiatement ouvrir la session Telnet sécurisée sur le périphérique mappé.



Une fois que vous avez entré votre nom d'utilisateur et votre mot de passe, l'accès au périphérique est terminé.

4. Afin de vérifier l'accès au périphérique, vérifiez les colonnes Octets sortants et Octets entrants, comme indiqué dans cette image

<ul> <li>https://172.22.1.160 - Secure Router Access - Microsoft Internet Ex</li> <li>Close this window when you finish using Application Access. Please wait for the table to be displayed before starting applications.</li> <li>If you shut down your computer without closing this window, you might later have problems running the applications listed below. <u>Click here for details.</u></li> </ul>										
Name	Local	Remote	Bytes Out	Bytes In	Sockets					
Telnet to R1	127.0.0.1:3044	10.2.2.2:23	56	127	1					
SSH to R1	127.0.0.1:3255	10.2.2.2:22	0	0	0					
🕘 https://172.22.1.160/+webvpn+/help/warning.ht 🔒 🥶 Internet										

#### **Commandes**

Plusieurs **commandes show sont associées à WebVPN.** Vous pouvez exécuter ces commandes dans l'interface de ligne de commande (CLI) afin d'afficher les statistiques et autres informations. Pour obtenir des informations détaillées à propos des commandes **show, reportez-vous à** <u>Vérification de la configuration de WebVPN</u>.

Note : 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**.

## **Dépannage**

Utilisez cette section pour dépanner votre configuration.

#### Le processus de connexion SSL est-il terminé ?

Une fois que vous vous connectez à l'ASA, vérifiez si le journal en temps réel indique la fin de la connexion SSL.

🌃 Real-time Log Viewer									
0 Pause	в 📭 Сору 🕻	🚽 Save 🖣	Clear 📅	Color Settings	🔁 Create Rule	Show Rule 🔘 Show Details 🦩 Help			
Filter By:			Filter	Show Al Fin	vet:	9			
Severity	Date	Time	Syslog	Source IP	Destination IP	Description			
<b>@</b> 2	Jun 27 2006	11:40:42	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172 22.1 203/3102 to 216 239.53.			
<b>Ø</b> 2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.70.157.215	Deny inbound UDP from 172.22.1.203/3101 to 171.70.157.215/1029 on			
<b>Ø</b> 2	Jun 27 2006	11:40:34	106006	172.22.1.203	64.101.176.170	Deny inbound UDP from 172.22.1.203/3101 to 64.101.176.170/1029 on			
<b>@</b> 2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.68.222.149	Deny inbound UDP from 172.22.1.203/3101 to 171.68.222.149/1029 on			
2	Jun 27 2006	11:40:32	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3100 to 216.239.53.			
2	Jun 27 2006	11:40:24	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.239.53.			
2	Jun 27 2006	11:40:22	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.239.53.			
4.6	Jun 27 2006	11:40:18	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.203/309			
A 6	Jun 27 2006	11:40:18	725003	172.22.1.203		SSL client outside:172.22.1.203/3097 request to resume previous sess			
<b>A</b> 6	Jun 27 2006	11:40:18	725001	172.22.1.203		Starting SSL handshake with client outside:172.22.1.203/3097 for TLSV			
<b>A</b> 6	Jun 27 2006	11:40:18	302013	172.22.1.203	172.22.1.160	Built inbound TCP connection 3711 for outside:172.22.1.203/3097 (172.			
<b>A</b> 6	Jun 27 2006	11:40:18	725007	172.22.1.203		SSL session with client outside:172.22.1.203/3096 terminated.			
<b>▲</b> 6	Jun 27 2006	11:40:17	302014	172.22.1.203	172.22.1.160	Teardown TCP connection 3710 for outside:172.22.1.203/3096 to NP ld			
<b>▲</b> 6	Jun 27 2006	11:40:17	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.203/309			
A 6	Jun 27 2006	11:40:17	725001	172.22.1.203		Starting SSL handshake with client outside:172.22.1.203/3096 for TLSV			
A 6	Jun 27 2006	11:40:17	302013	172.22.1.203	172.22.1.160	Built inbound TCP connection 3710 for outside:172.22.1.203/3096 (172.			
G 3	Jun 27 2006	11:40:16	305005	64.101.176.170		No translation group found for udp src inside:10.2.2.4/1830 dst outside			
G 3	Jun 27 2006	11:40:16	305005	171.70.157.215		No translation group found for udp src inside:10.2.2.4/1830 dst outside			
6 3	Jun 27 2006	11:40:16	305005	171.68.222.149		No translation group found for udp src inside:10.2.2.4/1830 dst outside			
<b>0</b> 2	Jun 27 2006	11:40:15	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3095 to 216.239.53.			
<b>Ø</b> 2	Jun 27 2006	11:40:12	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3095 to 216.239.53.			
<			щ.,,			>			
Please select a syslog entry to see the explanation ×									
Explanation Recommended Action Details									
🔾 Emergencies 🔇 Alerts 🐵 Critical 🔒 Errors 🗼 Warnings 🔺 Notifications 🔺 Informational 🛞 Debugging									

#### Le client léger VPN SSL est-il fonctionnel ?

Afin de vérifier que le client léger VPN SSL fonctionne, procédez comme suit :

- 1. Cliquez sur Surveillance, puis sur VPN.
- 2. Développez VPN Statistics, puis cliquez sur Sessions. Votre session client léger VPN SSL doit apparaître dans la liste des sessions. Assurez-vous de filtrer par WebVPN comme indiqué dans cette image



#### **Commandes**

Plusieurs commandes **debug sont associées à WebVPN.** Pour obtenir des informations détaillées à propos de ces commandes, reportez-vous à <u>Utilisation des commandes Debug WebVPN</u>.

**Remarque :** l'utilisation des commandes **debug** peut avoir un impact négatif sur votre périphérique Cisco. Avant d'utiliser les commandes **debug , référez-vous à la section** <u>Informations importantes</u> <u>sur les commandes Debug</u>.

## Informations connexes

- Exemple de configuration d'un VPN SSL sans client (WebVPN) sur ASA
- Exemple de configuration d'un client VPN SSL (SVC) sur ASA avec ASDM
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Exemple de configuration d'ASA avec WebVPN et authentification unique à l'aide d'ASDM et de NTLMv1

Support et documentation techniques - Cisco Systems