# ASA 8.X : Exemple de configuration de routage du trafic VPN SSL via la passerelle par défaut tunnelisée

### Contenu

Introduction Conditions préalables Conditions requises Components Used Conventions Informations générales Configuration Diagramme du réseau Configuration d'ASA utilisant l'ASDM 6.1(5) Vérification Dépannage Informations connexes

# **Introduction**

Ce document décrit comment configurer l'appliance de sécurité adaptable (ASA) pour router le trafic VPN SSL via la passerelle tunnelisée par défaut (TDG). Lorsque vous créez une route par défaut avec l'option tunnel, tout le trafic d'un tunnel se terminant sur l'ASA qui ne peut pas être routé à l'aide de routes apprises ou statiques est envoyé à cette route. Pour le trafic sortant d'un tunnel, cette route remplace toute autre route par défaut configurée ou apprise.

# **Conditions préalables**

### **Conditions requises**

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

- ASA qui s'exécute sur la version 8.x
- Client VPN SSL Cisco (SVC) 1.xRemarque : Téléchargez le package client VPN SSL (sslclient-win\*.pkg) à partir du <u>téléchargement de logiciels Cisco</u> (clients <u>enregistrés</u> uniquement). Copiez le SVC dans la mémoire flash de l'ASA. Le SVC doit être téléchargé sur les ordinateurs des utilisateurs distants afin d'établir la connexion VPN SSL avec l'ASA.

#### **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 la version logicielle 8.x
- Version du client VPN SSL Cisco pour Windows 1.1.4.179
- PC exécutant Windows 2000 Professionnel ou Windows XP
- Cisco Adaptive Security Device Manager (ASDM) version 6.1(5)

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 client VPN SSL (SVC) est une technologie de tunnellisation VPN qui offre aux utilisateurs distants les avantages d'un client VPN IPSec sans que les administrateurs réseau aient besoin d'installer et de configurer des clients VPN IPSec sur des ordinateurs distants. Le SVC utilise le chiffrement SSL qui est déjà présent sur l'ordinateur distant, ainsi que la connexion WebVPN et l'authentification de l'appliance de sécurité.

Dans le scénario actuel, un client VPN SSL se connecte aux ressources internes derrière l'ASA via le tunnel VPN SSL. Le split-tunnel n'est pas activé. Lorsque le client VPN SSL est connecté à l'ASA, toutes les données sont tunnellisées. Outre l'accès aux ressources internes, le principal critère est d'acheminer ce trafic tunnelisé via la passerelle tunnelée par défaut (DTG).

Vous pouvez définir une route par défaut distincte pour le trafic tunnelisé avec la route par défaut standard. Le trafic non chiffré reçu par l'ASA, pour lequel il n'existe aucune route statique ou apprise, est acheminé par la route par défaut standard. Le trafic crypté reçu par l'ASA, pour lequel il n'existe aucune route statique ou apprise, sera transmis au DTG défini par la route par défaut tunnelisée.

Afin de définir une route par défaut avec tunnel, utilisez cette commande :

route <if\_name> 0.0.0.0 0.0.0.0 <gateway\_ip> tunneled

### **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 :



Dans cet exemple, le client VPN SSL accède au réseau interne de l'ASA via le tunnel. Le trafic destiné à des destinations autres que le réseau interne est également tunnelisé, car aucun tunnel partagé n'est configuré et est acheminé via le TDG (192.168.100.20).

Une fois que les paquets sont routés vers le TDG, qui est le routeur 2 dans ce cas, il effectue la traduction d'adresses pour acheminer ces paquets vers Internet. Pour plus d'informations sur la configuration d'un routeur en tant que passerelle Internet, référez-vous à <u>Comment configurer un</u> routeur Cisco derrière un modem câble non Cisco.

#### Configuration d'ASA utilisant l'ASDM 6.1(5)

Ce document suppose que les configurations de base, telles que la configuration d'interface, sont complètes et fonctionnent correctement.

**Remarque :** référez-vous à <u>Autoriser l'accès HTTPS pour ASDM</u> pour plus d'informations sur la façon 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> <u>interface d'ASA pour plus d'informations.</u>

Complétez ces étapes afin de configurer le VPN SSL à l'aide de l'Assistant VPN SSL.

#### 1. Dans le menu Assistants, sélectionnez Assistant VPN

e View Tools	Wizards Window Help	
Home	Startup Wizard IPsec VPN Wizard SSL VPN Wizard	n Sack Forward ? Help
Device Info	High Availability and Scalability Wizard Packet Capture Wizard	

2. Cochez la case Client VPN SSL Cisco, puis cliquez sur Suivant.



3. Entrez un nom pour la connexion dans le champ Nom de la connexion, puis choisissez l'interface utilisée par l'utilisateur pour accéder au VPN SSL dans la liste déroulante Interface VPN

SSL.

🚳 SSL VPN Wizard		
SSL VPN Wizard	SSL VPN Interface (Step 2 of 6)	
SSL VPN WIZaid	Provide a connection name and the interface that SSL VPN users connect to. Connection Name: Test The interface users access for SSL VPN connections. SSL VPN Interface: Outside Digital Certificate When users connect, the security appliance sends this digital certificate to the remote w to authenticate the ASA. Certificate: None Concerting Course Settinger	eb browser
	Connection Group Alias/URU Connection Group Alias/URU Display Group Alias list at the login page Information URL to access SSL VPN Service: https://209.165.201.2 URL to access ASDM: https://209.165.201.2(admin)	
£-,	<u>≤Back(Next</u> > F)/sh ⊆ancel	Help

- 4. Cliquez sur Next (Suivant).
- 5. Choisissez un mode d'authentification, puis cliquez sur **Suivant**. (Cet exemple utilise l'authentification

locale.)

🖆 SSL VPN Wizard		X
SSL VPN Wizard	User Authentication (Step 3 of 6)	
SSL VPN WIZARD	The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login.  AAA Server Group Name:  Cordiant Server Group Name:  Add >>  Delete  Confirm Password:  Delete  Delete Delete Delete Delete Delete Delete Delete Delete Delete Delete Delete Delete Delete Delete Delete Delete Delete Delete Delete De	
	Sack Next > Deinish Sancel B	elp

6. Créez une nouvelle stratégie de groupe autre que la stratégie de groupe par défaut existante.

📬 SSL VPN Wizard				
SSL VPN Wizard	Group Policy (Step 4 of 6)			
12 M	A group policy is a collection of user-oriented attribute/value pairs. Unless assigned to a specific policy, all users are members of the default group policy (DftGrpPolicy). Therefore, configuring default group policy lets users inherit attributes that you have not configured at the individual g policy or username level.			
66	Create new group policy	grppolicy	$\triangleright$	
	O Modify existing group policy	DitGepPolicy	1	
California de la del				
			xt > )nish Cancel Help	

7. Créez un nouveau pool d'adresses qui sera attribué aux PC clients VPN SSL une fois qu'ils seront



Un pool de plage 192.168.10.40-192.168.10.50 a été créé par le nom

Name:	newpool
Starting IP Address:	192.168.10.40
Ending IP Address:	192.168.10.50
Subnet Mask:	255.255.255.0

newpool.

8. Cliquez sur Parcourir afin de choisir et de télécharger l'image du client VPN SSL dans la

# mémoire flash de l'ASA.

Dancilli IADN 182					
COL UDAL WIZELU	TP Address Pools and	Elient Imane - Any	Connect VPN Fil	ent Conor	ctions Only (Sten 5 of 6)
	The security appliance client self-instals, use to resources on a corp IP Address Pool Create a new addre from the pool when	downloads the AnyCo s SSL or DTLS encrypti lorate network. The re ess pool or select an ex they connect.	onnect VPN Client t on for the duration mote PC becomes isting address poo	o remote us of the con part of the I. Remote P	sers when they connect. The nection, and allows full access corporate network. 'Cs are assigned addresses
	IP Address Pool:	newpool	V [	New	7
and the second second	Address Pool Range	: 192.168.10.40 - 1	92.168.10.50		_
a.	AnyConnect VPN Clien	t Image Location			
SULTE . Y	Identify a file in flas the file and loads it	h memory as an AnyC into cache memory for	onnect VPN Client downloading to re	mage. The mote users	security appliance expands
	Location: Download latest Ar	ryConnect VPN Clent f	ram Cisco.com	Browse	
			≤ Back	exit > Ei	nish Cancel Help

9. Cliquez sur **Upload** afin de définir le chemin d'accès au fichier à partir du répertoire local de l'ordinateur.

🖆 Add SSL VPN Cli	ent Image			
AnyConnect Image:				Browse Flash
	ок	Cancel	Help	]

10. Cliquez sur **Parcourir les fichiers locaux** afin de sélectionner le répertoire dans lequel le fichier sslclient.pkg existe.

🕵 Upload Image	
Upload a file from local co few minutes. Please wait	mputer to flash file system on the device. The upload process might take a for the operation to finish.
Local File Path:	Browse Local Files
Flash File System Path:	Browse Flash
C	Upload File Close Help

11. Cliquez sur **Upload File** afin de télécharger le fichier sélectionné dans la mémoire flash <u>d'ASA</u>.

🛍 Upload Image 🛛 🛛 🛛
Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.
Local File Path:       C:\Documents and Settings\jtammera\My Documy       Browse Local Files         Elash File System Path:       disk0:/cslclient-win-1       1       4       179 pkg       Browse Elash
Upload File Close Help
🖆 Status 🛛 🕅
Please wait while ASDM is uploading the file. The upload process may take a few minutes.         77%         Completed transfer of 360,448 bytes out of 418,765 bytes
🖆 Information
File has been uploaded to flash successfully.
ΟΚ

12. Une fois le fichier téléchargé sur la mémoire flash d'ASA, cliquez sur **OK** pour terminer cette tâche.

Browse Flash
Upload
]

 Il affiche maintenant le dernier fichier pkg anyconnect téléchargé sur la mémoire flash d'ASA. Cliquez sur Next (Suivant).

SSL WON Witzard					
SSI VPN Wizard	IP Address Pools an	d Client Image - AnyConr	nect VPN Cli	ent Connec	tions Only (Step 5 of 6)
	The security appliance client self-installs, us to resources on a con IP Address Pool Create a new addre from the pool when	e downloads the AnyConnect es SSL or DTLS encryption for porate network. The remote ess pool or select an existing h they connect.	t VPN Client t r the duration PC becomes address poo	o remote use of the conn part of the c I. Remote PC	rs when they connect. The action, and allows full access orporate network. s are assigned addresses
Sec. Marco	IP Address Pool:	newpool	~	New	1
	Address Pool Rang	e: 192.168.10.40 - 192.10	68.10.50		-
a.	AnyConnect VPN Clie	nt Image Location			
	Identify a file in fla the file and loads it	sh memory as an AnyConnec into cache memory for dowr	t VPN Client i Noading to re	mage. The se mote users.	curity appliance expands
14	Location:	disk0:/sslclient-win-1.1.4	.179.pkg	Browse	]
	Download latest A	nyConnect VPN Client from C	<u>lsco.com</u>		
			≤ Back ( N	ext > DEM	a Cancel Help

 Le résumé de la configuration du client VPN SSL est affiché. Cliquez sur Terminer pour terminer l'Assistant.

La configuration présentée dans ASDM concerne principalement la configuration de l'assistant client VPN SSL.

Dans l'interface de ligne de commande, vous pouvez observer une configuration supplémentaire. La configuration complète de l'interface de ligne de commande est présentée ci-dessous et des commandes importantes ont été mises en surbrillance.

ciscosa
ciscoasa# <b>show running-config</b>
: Saved
:
ASA Version 8.0(4)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
namelf outside
security-level U
1p address 209.165.201.2 255.255.255.224
: interface Ethernot(/1
nameif incide
security-level 100
in address 192 168 100 2 255 255 255 0
!
interface Ethernet0/2
nameif manage
security-level 0

```
ip address 10.1.1.1 255.255.255.0
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
interface Ethernet0/4
shutdown
no nameif
no security-level
no ip address
interface Ethernet0/5
shutdown
no nameif
no security-level
no ip address
1
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list nonat extended permit ip 192.168.100.0
255.255.255.0 192.168.10.0 255.255.255.0
access-list nonat extended permit ip 192.168.10.0
255.255.255.0 192.168.100.0 255.255.255.0
!--- ACL to define the traffic to be exempted from NAT.
no pager logging enable logging asdm informational mtu
outside 1500 mtu inside 1500 mtu manage 1500 !---
Creating IP address block to be assigned for the VPN
clients ip local pool newpool 192.168.10.40-
192.168.10.50 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-615.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 192.168.100.0 255.255.255.0
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
!--- Default route is configured through "inside"
interface for normal traffic. route inside 0.0.0.0
0.0.0.0 192.168.100.20 tunneled
!--- Tunneled Default route is configured through
"inside" interface for encrypted traffic ! 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
!--- Configuring the ASA as HTTP server. http 10.1.1.0
255.255.255.0 manage
!--- Configuring the network to be allowed for ASDM
access. ! !--- Output is suppressed ! telnet timeout 5
ssh timeout 5 console timeout 0 threat-detection basic-
threat threat-detection statistics access-list ! class-
map inspection_default match default-inspection-traffic
! ! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map
```

global\_policy class inspection\_default inspect dns

```
preset_dns_map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global ! !--- Output suppressed !
webvpn
enable outside
!--- Enable WebVPN on the outside interface svc image
disk0:/sslclient-win-1.1.4.179.pkg 1
!--- Assign the AnyConnect SSL VPN Client image to be
used svc enable
!--- Enable the ASA to download SVC images to remote
computers group-policy grppolicy internal
!--- Create an internal group policy "grppolicy" group-
policy grppolicy attributes
VPN-tunnel-protocol svc
!--- Specify SSL as a permitted VPN tunneling protocol !
username cisco password ffIRPGpDS0Jh9YLq encrypted
privilege 15
!--- Create a user account "cisco" tunnel-group Test
type remote-access
!--- Create a tunnel group "Test" with type as remote
access tunnel-group Test general-attributes
address-pool newpool
!--- Associate the address pool vpnpool created default-
group-policy grppolicy
!--- Associate the group policy "clientgroup" created
prompt hostname context
Cryptochecksum:1b247197c8ff70ee4432c13fb037854e : end
ciscoasa#
```

# **Vérification**

Les commandes indiquées dans cette section peuvent être utilisées pour vérifier cette 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 SVC stockées dans la mémoire flash ASA.
- show vpn-sessiondb svc Affiche les informations sur les connexions SSL actuelles.

# **Dépannage**

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

### Informations connexes

- Prise en charge des appareils de sécurité adaptatifs de la gamme Cisco 5500
- Exemple de configuration de PIX/ASA et d'un client VPN pour un VPN Internet public sur un stick
- Exemple de configuration d'un client VPN SSL (SVC) sur ASA avec ASDM
- Support et documentation techniques Cisco Systems