# Configuration du trafic U-turn du client VPN AnyConnect sur ASA 9.X

## Contenu

Introduction Conditions préalables **Conditions requises Components Used** Informations générales Configuration du trafic d'accès à distance U-turn Exemple de configuration d'un client VPN AnyConnect pour un VPN Internet public sur un stick Diagramme du réseau Configurations ASA version 9.1(2) avec ASDM version 7.1(6) Configuration ASA version 9.1(2) dans la CLI Autoriser la communication entre les clients VPN AnyConnect avec la configuration TunnelAll en place Diagramme du réseau Configurations ASA version 9.1(2) avec ASDM version 7.1(6) Configuration ASA version 9.1(2) dans la CLI Autoriser la communication entre les clients VPN AnyConnect avec split-tunnel Diagramme du réseau Configurations ASA version 9.1(2) avec ASDM version 7.1(6) Configuration ASA version 9.1(2) dans la CLI Vérification Dépannage Informations connexes

## Introduction

Ce document décrit comment configurer un dispositif de sécurité adaptatif Cisco (ASA) version 9.X pour lui permettre de réactiver le trafic VPN. Il couvre ce scénario de configuration : Détourner le trafic des clients d'accès à distance.

**Note**: Afin d'éviter un chevauchement d'adresses IP dans le réseau, affectez un pool d'adresses IP complètement différent au client VPN (par exemple, 10.x.x.x, 172.16.x.x et 192.168.x.x). Ce schéma d'adresses IP est utile pour dépanner votre réseau.

#### Cheveux en épingle ou demi-tour

Cette fonctionnalité est utile pour le trafic VPN qui entre dans une interface, mais qui est ensuite acheminé hors de cette même interface. Par exemple, si vous avez un réseau VPN Hub and Spoke où l'appliance de sécurité est le concentrateur et les réseaux VPN distants sont des rayons, pour qu'un rayon communique avec un autre, le trafic doit aller à l'appliance de sécurité, puis de

nouveau à l'autre rayon.

Saisissez le same-security-traffic afin de permettre au trafic d'entrer et de sortir de la même interface.

ciscoasa(config)#same-security-traffic permit intra-interface

## Conditions préalables

### **Conditions requises**

Cisco vous recommande de respecter les conditions suivantes avant de tenter cette configuration :

- L'appliance de sécurité ASA du concentrateur doit exécuter la version 9.x.
- Client VPN Cisco AnyConnect 3.xNote: Téléchargez le package AnyConnect VPN Client (anyconnect-win\*.pkg) à partir du <u>téléchargement de logiciels</u> Cisco (clients enregistrés uniquement). Copiez le client VPN AnyConnect dans la mémoire flash Cisco 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>Connexions client VPN AnyConnect</u> du guide de configuration ASA pour plus d'informations.

### **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 9.1(2)
- Client VPN SSL Cisco AnyConnect version pour Windows 3.1.05152
- PC qui exécute un système d'exploitation pris en charge par les <u>plates-formes VPN prises en</u> <u>charge, gamme Cisco ASA</u>.
- Cisco Adaptive Security Device Manager (ASDM) version 7.1(6)

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## 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. Sauf si l'appliance de sécurité est configurée pour rediriger http:// demandes à https://, les utilisateurs doivent saisir l'URL dans le formulaire https://

.Une fois l'URL saisie, le navigateur se connecte à cette interface et affiche l'écran de connexion. Si l'utilisateur satisfait aux conditions de connexion et d'authentification et que l'appliance de sécurité identifie l'utilisateur comme ayant besoin du client, il télécharge le client correspondant au système d'exploitation de l'ordinateur distant. Après le téléchargement, le client s'installe et se configure, établit une connexion SSL sécurisée et reste ou se désinstalle (cela dépend de la configuration de l'appliance de sécurité) lorsque 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.Lorsque le client négocie une connexion VPN SSL avec l'appliance de sécurité, il se connecte avec TLS (Transport Layer Security) et utilise également DTLS (Datagram Transport Layer Security). DTLS évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore les performances des applications en temps réel sensibles aux retards de paquets.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. Pour plus d'informations sur la façon d'installer le client manuellement, référez-vous au Guide d'administration du client Cisco AnyConnect Secure Mobility. L'appliance de sécurité télécharge le client en fonction de la stratégie de groupe ou des attributs de nom d'utilisateur de l'utilisateur qui établit 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. Note: Les exemples utilisés dans ce document utilisent IPv4. Pour le trafic de demi-tour IPv6, les étapes sont les mêmes, mais

### utilisent les adresses IPv6 au lieu d'IPv4. Configuration du trafic d'accès à

**distance U-turn**Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.Note: Utilisez les guides <u>Références aux commandes</u> afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.Exemple de configuration d'un client VPN AnyConnect pour un VPN Internet public sur un stickDiagramme du réseauCe document utilise la configuration réseau suivante :



Configurations ASA version 9.1(2) avec ASDM version 7.1(6)Ce document suppose que la configuration de base, telle que la configuration d'interface, est déjà terminée et fonctionne correctement.Note: Référez-vous à <u>Configuration de l'accès à la gestion</u> afin de permettre à l'ASA d'être configuré par l'ASDM.Note: Dans les versions 8.0(2) et ultérieures, l'ASA prend en charge simultanément les sessions VPN SSL (WebVPN) sans client et les sessions d'administration ASDM sur le port 443 de l'interface externe. Dans les versions antérieures à la version 8.0(2), WebVPN et ASDM ne peuvent pas être activés sur la même interface ASA à moins que vous ne changiez les numéros de port. Référez-vous à <u>ASDM et WebVPN activé sur la même interface de l'ASA</u> pour plus d'informations.Complétez ces étapes afin de configurer le VPN SSL sur une clé dans ASA :

1. Choisir Configuration > Device Setup > Interfaces *et vérifiez la* Enable traffic between two or more hosts connected to the same interface *afin d'autoriser le trafic VPN SSL à entrer et sortir de la même interface. Cliquer* Apply.

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Туре [	Add 🔻
igabitEthemet0/0	outside	Enabled	0	172.16.1.1	255,255,255.0		Hardware	Edit
igabitEthernet0/1	inside	Enabled	100	10.77.241.142	255.255.255.192		Hardware	
igabitEthernet0/2		Disabled					Hardware	Delete
igabitEthernet0/3		Disabled					Hardware	
anagement0/0	mgmt	Disabled	0				Hardware/Ma	
	m						8	

#### Configuration CLI équivalente :

ciscoasa(config)#same-security-traffic permit intra-interface

2. Choisir Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add afin de créer un pool d'adresses IP vpnpool.

Name:	vpnpool
Starting IP Address:	192.168.10.1
Ending IP Address:	192.168.10.254
Subnet Mask:	255.255.255.0

- 3. Cliquer Apply. Configuration CLI équivalente :
- ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
- 4. Activez WebVPN. Choisir Configuration > Remote Access VPN > Network (Client) Access > SSL VPN

Connection Profiles *et* Access Interfaces, *cliquez sur les cases à cocher* Allow Access *et* Enable DTLS *pour l'interface externe.* Vérifiez également la Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below *afin d'activer le VPN SSL sur l'interface externe.* 

administrative r options. cess Interfaces Ø Enable Oso	ights. The Cisco AnyCon	nect VPN Client support	es selected in the table l	s well as SSL tunnel with Datagram	Transport Layer Security (DTLS) turnelin
SL access mus	t be enabled if you allow	AnyConnect client to b	e launched from a brows	er (Web Launch) .	
55L access mus	t be enabled if you allow SSL Access	AnyConnect client to b	e launched from a brows IPsec (IKEv2) Acco	er (Web Launch) . 85	
55L access mus Interface	t be enabled if you allow SSL Access Allow Access	AnyConnect client to b Enable DTLS	e launched from a brows IPsec (IKEv2) Acco Allow Access	er (Web Launch) . iss Enable Client Services	Device Certificate
SSL access mus Interface outside	t be enabled if you allow SSL Access Allow Access	Enable DTLS	e launched from a brows IPsec (IKEv2) Acco Allow Access	er (Web Launch) . sss Enable Client Services	Device Certificate

*Cliquer* Apply.*Choisir* Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add afin d'ajouter l'image du client VPN Cisco AnyConnect à partir de la mémoire flash de l'ASA comme indiqué.

and the second second second		
Local File Path:	C:\Users\josemed\Desktop\anyconnect-win-3.1.05152-k9.pkg	Browse Local Files
Flash File System Path:	disk0:/anyconnect-win-3.1.05152-k9.pkg	Browse Flash
Add AnyConne	ct Client Image	X
AnyConnect Image	anyconnect-win-3.1.05152-k9.pkg	Browse Flash
	(	Upload

#### Configuration CLI équivalente :

ciscoasa(config)#**webvpn** 

ciscoasa(config-webvpn)#**enable outside** 

ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable

5. Configurez la stratégie de groupe. Choisir Configuration > Remote Access VPN > Network (Client) Access > Group Policies afin de créer une politique de groupe interne clientgroup. Sous la General, sélectionnez l'option SSL VPN Client afin d'activer le WebVPN comme protocole de tunnel.

1	10.	. 1		9 11
Jarvara	Farm:	yatorb _		
Advance:	Advance: Barner:	nher:		
	SCEP forwarding URL	inte-it		
	Activess Pools	nhe-t		Ereck
	3Pv6 Address Pools	mer:	1	Seet
	More Options			*
	Tunneling Protocols	📃 Sherik 🔄 Clenifess SS, WPV 📝 SS, WPA C and 📄 (Psec SIEV). 🔄 (Psec Si	EV2 🔲 L2754Fsec	

Dans la Advanced > Split Tunneling, sélectionnez Tunnel All Networks de la liste déroulante Policy de la Policy afin de faire passer tous les paquets du PC distant par un tunnel sécurisé.

910113	
deanced DNs Nancer (#) Infent	
BORGETTURY Public:    Infant    Infa	1.

#### Configuration CLI équivalente :

ciscoasa(config)#group-policy clientgroup internal ciscoasa(config)#group-policyclientgroup attributes ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client ciscoasa(config-group-policy)#split-tunnel-policy tunnelall

6. Choisir Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add afin de créer un

nouveau compte d'utilisateur ssluser1. Cliquer OK et ensuite Apply.

Policy					
	Linertwarks: entangel				
	Partment management				
	Confine Password: *******				
	F (Ger aufenhaded using MSCHAP				
	Auca Kalnibur				
	Selections of the optimor below to reduct ACTIVE, STUL Televisient Constributions				
	Note: Alloces have relevant access, regardless of these settings.				
	(ii) Full-access(JSDN, 75H, Teltet and Console)				
	Philage wells used with command authoritation.				
	Privlege (avv): 2				
	C. Llogin prompt for 53H, Telnet and console (no ASDH access)				
	This setting is effective only it "area authentication http: console LOCIA." command is configured.				
	() No ANDA, 334, Talant or Consola access				
	The setting is offsetive only 6" and authentication bits coreade LOCAL" and "asse adherization eres" commands are configured.				

#### Configuration CLI équivalente :

ciscoasa(config)#username ssluser1 password asdmASA@

7. Configurez le groupe de tunnels. Choisir Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add afin de créer un nouveau groupe de tunnels ssigroup.Dans la Basic , vous pouvez exécuter la liste des configurations comme indiqué : Nommez le groupe de tunnels ssigroup.Sous Client Address Assignment, choisissez le pool d'adresses vpnpool a partir des versions Client Address Pools liste déroulante.Sous Default Group Policy, choisissez la stratégie de groupe clientgroup a partir des versions Group Policy liste déroulante.

Name:	ssigroup	
Aliases:		
Authentication		
Method:	💿 AAA 💿 Certificate 💿 Both	
AAA Server Group:	LOCAL	Manage
	Use LOCAL if Server Group fails	
Client Address Assignment		
DHCP Servers:		
	💿 None 💿 DHCP Link 💿 DHCP Subnet	
Client Address Pools:	vpnpool	Select
Client IPv6 Address Pool	s:	Select
	IPv6 address pool is only supported for SSL.	
Default Group Policy		- 222
Group Policy:	clientgroup	Manage
	Aliases: Authentication Method: AAA Server Group: Client Address Assignment DHCP Servers: Client Address Pools: Client IPv6 Address Pool Default Group Policy Group Policy:	Aliases: Authentication Method:

Sous la Advanced > Group Alias/Group URL , spécifiez le nom d'alias du groupe comme ssigroup\_users et cliquez sur ok. Configuration CLI équivalente :

ssigloup\_users et cirquez sur ok. Coringulation of requivalence. ciscoasa(config)#tunnel-group sslgroup type remote-access ciscoasa(config)#tunnel-group sslgroup general-attributes ciscoasa(config-tunnel-general)#address-pool vpnpool ciscoasa(config-tunnel-general)#default-group-policy clientgroup ciscoasa(config-tunnel-general)#exit ciscoasa(config)#tunnel-group sslgroup webvpn-attributes ciscoasa(config-tunnel-webvpn)#group-alias sslgroup\_users enable

8. Configurer NAT Choisir Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule Ainsi, le trafic provenant du réseau interne peut être traduit avec l'adresse IP externe 172.16.1.1.

File View Tools Wizards Wind	low Help							
Home 🆧 Configuration 🔯 Mc	nitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦿 🖓 H	de						
Device List 🗗 🕂 🛪	Configuration > Firewall > NAT Rules				[			
Add 📋 Delete 🖉 Cornect	🗣 Add - 📝 Edit 👔 Delete   🛧 🎸 🐰 📴 🛄 -   Q. Find 🖽 Diagram 📿 Paduet Trace							
50 50 50 50 50 50 50 50 50 50 50 50 50 5	Add NAT Rule Before "Network Object" NAT Rules		Action: Transk	sted Packet				
- 🔐 localhost:55000	Add NAT Rule After "Network Object" NAT Rules	Service	Source	Destination	Service			
	🔹 Insert	any 🕹	Original (5)	Original	Original			
irewall 🗗 🖓 🖓	🐺 Insert After	11						
Public Servers     URL Filtering Servers     Threat Detection     Dotnet Traffic Filter     Objects     Objects     Objects     Objects     Objects								
B Device Setup								

lame:	obj-inside	
Гуре:	Network	•]
P Address:	10.77.241.128	
Vetmask:	255.255.255.192	-
Description:		
NAT		*
NAT Add Auto Type:	omatic Address Translation Rules Dynamic 👻	*
NAT Add Auto Type: Translated	omatic Address Translation Rules Dynamic <b>+</b> I Addr: outside	*

*Choisir* Configuration >

Firewall > NAT Rules > Add "Network Object" NAT Rule Ainsi, le trafic VPN provenant du réseau externe peut être traduit avec l'adresse IP externe 172.16.1.1.

Jame: ob	j-AnyconnectPool	
Type: Ne	twork	•]
P Address: 19	2.168.10.0	
Jetmask: 25	5.255.255.0	-
Description:		
NAT		۲
NAT Add Automatic Type:	Address Translation Rules Dynamic PAT (Hide) 👻	*
NAT Add Automatic Type: Translated Addr:	Address Translation Rules Dynamic PAT (Hide) 👻 outside	*

#### équivalente :

```
ciscoasa(config)# object network obj-inside
ciscoasa(config-network-object)# subnet 10.77.241.128 255.255.255.192
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
ciscoasa(config)# object network obj-AnyconnectPool
ciscoasa(config-network-object)# subnet 192.168.10.0 255.255.255.0
ciscoasa(config-network-object)# nat (outside,outside) dynamic interface
```

#### Configuration ASA version 9.1(2) dans la CLI

```
ciscoasa(config)#show running-config
```

```
: Saved
.
ASA Version 9.1(2)
1
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
1
interface GigabitEthernet0/1
nameif inside
```

security-level 100
ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address

#### !

passwd 2KFQnbNIdI.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 same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool subnet 192.168.10.0 255.255.255.0 object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

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 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

nat (inside, outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated when going to the Anyconnect Pool.

object network obj-AnyconnectPool nat (outside,outside) dynamic interface object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and Anyconnect Clients. !--- Note: Uses an RFC 1918 range for lab setup.

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 class-map inspection\_default match default-inspection-traffic 1 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

!--- Enable WebVPN on the outside interface

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

anyconnect enable

!--- Enable the security appliance to download SVC images to remote computers

tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the WebVPN Login page

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

split-tunnel-policy tunnelall

!--- Encrypt all the traffic from the SSL VPN Clients.

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

!--- Associate the group policy "clientgroup" created

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup\_users enable

!--- Configure the group alias as sslgroup-users

prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#

Autoriser la communication entre les clients VPN AnyConnect avec la configuration TunnelAll en placeDiagramme du réseau



Si la communication entre les clients Anyconnect est requise et que la fonction NAT pour Internet public sur un Stick est en place ; une NAT manuelle est également nécessaire pour permettre la communication bidirectionnelle.II s'agit d'un scénario courant dans lequel les clients Anyconnect utilisent des services téléphoniques et doivent pouvoir s'appeler mutuellement.Configurations ASA version 9.1(2) avec ASDM version 7.1(6)Choisir Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules Ainsi, le trafic provenant du réseau externe (Anyconnect Pool) et destiné à un autre client Anyconnect du même pool n'est pas traduit avec l'adresse IP externe 172.16.1.1.

File View Tools Wizards Windo	ow Help nitoring 🔲 Save 🔿 Refresh 🧑 Back 🔿 Forward 🦻 Hel	P			
Device List an 9 ×	Configuration > Firewall > NAT Rules				
🌩 Add 📋 Delete 🚿 Connect	🗣 Add - 🖪 Edt 🗻 Delete 🕈 🗲 👗 🗞 🛍 - 🔍 Find	🖭 Diagram 🏹	Packet Trace		
Find: Go	Add NAT Rule Before "Network Object" NAT Rules	Action: Translated Packet			
	Add "Network Object" NAT Rule	Service	Source	Destination	Service
	Add NAT Rule After "Network Object" NAT Rules	any	Original (S)	Original	Original
· · · · · · · · · · · · · · · · · · ·	👷 Insert	any	Original (5)	Original	Original
Firewall -7 -P	🐺 Insert After	, 🦃 any	Original (5)	- Original	- Original

Source Interface:	outside	Destination Interface:	outside	+
Source Address:	obj-AnyconnectPool (	Destination Address:	obj-AnyconnectPool	[
		Service:	any	
Action: Translated	Packet		2	
Source NAT Type:	Static	•		
5ource Address:	obj-AnyconnectPool (		obj-AnyconnectPool	
Fall through to	interface PAT	Service:	Original	
Options				
📝 Enable rule				
Translate DNS	replies that match this rule			
Direction: Both				
	· · ·			

#### Configuration CLI équivalente :

```
nat (outside, outside) source static obj-AnyconnectPool obj-AnyconnectPool destination
static obj-AnyconnectPool obj-AnyconnectPool
Configuration ASA version 9.1(2) dans la CLI
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
```

```
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
shutdown
no nameif
no security-level
```

no ip address

passwd 2KFQnbNIdI.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 same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool subnet 192.168.10.0 255.255.255.0 object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

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 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT statements used so that traffic from the inside network destined to the Anyconnect Pool and traffic from the Anyconnect Pool destined to another Client within the same pool does not get translated.

object network obj-AnyconnectPool nat (outside,outside) dynamic interface object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and Anyconnect Clients. !--- Note: Uses an RFC 1918 range for lab setup.

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
1
service-policy global_policy global
webvpn
enable outside
```

```
!--- Enable WebVPN on the outside interface
```

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

anyconnect enable

!--- Enable the security appliance to download SVC images to remote computers

tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the WebVPN Login page

```
group-policy clientgroup internal
```

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

split-tunnel-policy tunnelall

!--- Encrypt all the traffic from the SSL VPN Clients. 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

!--- Associate the group policy "clientgroup" created

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup\_users enable

!--- Configure the group alias as sslgroup-users

prompt hostname context Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end ciscoasa(config)# Autoriser la communication entre les clients VPN AnyConnect avec splittunnelDiagramme du réseau



Si la communication entre clients Anyconnect est requise et que le Split-Tunnel est utilisé ; aucune fonction NAT manuelle n'est requise pour autoriser la communication bidirectionnelle, sauf si une règle NAT affecte ce trafic configuré. Cependant, le pool VPN Anyconnect doit être inclus dans la liste de contrôle d'accès Split-Tunnel.II s'agit d'un scénario courant dans lequel les clients Anyconnect utilisent des services téléphoniques et doivent pouvoir s'appeler mutuellement.Configurations ASA version 9.1(2) avec ASDM version 7.1(6)

1. Choisir Configuration > Remote Access VPN > Network (Client) Access > Address Assignment> Address Pools > Add afin de créer un pool d'adresses IP vpnpool.

Name:	vpnpool	
Starting IP Address:	192.168.10.1	
Ending IP Address:	192.168.10.254	
Subnet Mask:	255.255.255.0	•

- 2. Cliquer Apply. Configuration CLI équivalente :
- ciscoasa (config) #ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0 3. Activez WebVPN. Choisir Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles *et* Access Interfaces, *cliquez sur les cases à cocher* Allow Access *et* Enable DTLS pour l'interface externe. Vérifiez également la Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below *afin d'activer le VPN SSL sur l'interface externe*.

The security ap administrative r options. cess Interfaces Ø Enable Oso	plance automatically dep ights. The Cisco AnyCon : 	loys the Cisco AnyCom nect VPN Client support	ect VPN Client to remot s IPsec (IKEv2) tunnel a es selected in the table l	e users upon connection. The initia s well as SSL tunnel with Datagram	l dient deployment requires end-user Transport Layer Security (DTLS) tunnelin
SL access mus	t be enabled if you allow	AnyConnect client to b	e launched from a brows	er (Web Launch) .	
55L access mus	t be enabled if you allow SSL Access	AnyConnect client to b	IPsec (IKEv2) Acc	ser (Web Launch) , SSS	
55L access mus Interface	t be enabled if you allow SSL Access Allow Access	AnyConnect client to b Enable DTLS	e launched from a brows IPsec (IKEv2) Acco Allow Access	er (Web Launch) . sss Enable Client Services	Device Certificate
Interface	t be enabled if you allow SSL Access Allow Access	AnyConnect client to b Enable DTLS	IPsec (JKEv2) Acco Allow Access	Enable Client Services	Device Certificate Port Settings

*Cliquer* Apply.*Choisir* Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add afin d'ajouter l'image du client VPN Cisco AnyConnect à partir de la mémoire flash de l'ASA comme indiqué.

Upload a file from local o Please wait for the oper	computer to flash file system on the device. The upload process mi ation to finish.	ght take a few minutes.	
Local File Path:	C:\Users\josemed\Desktop\anyconnect-win-3.1.05152-k9.pkg	Browse Local Files	
Flash File System Path:	disk0:/anyconnect-win-3.1.05152-k9.pkg	Browse Flash	

AnyConnect Image:	anyconnect-win	Browse Flash		
				Upload
Regular express	ion to match u	ser-agent		*

#### Configuration CLI équivalente :

ciscoasa(config)# <b>webvpn</b>
ciscoasa(config-webvpn)# <b>enable outside</b>
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)# <b>tunnel-group-list enable</b>
ciscoasa(config-webvpn)# <b>anyconnect enable</b>

4. Configurez la stratégie de groupe. Choisir Configuration > Remote Access VPN > Network (Client) Access > Group Policies afin de créer une politique de groupe interne clientgroup. Sous la General, sélectionnez l'option SSL VPN Client afin d'activer le WebVPN en tant que protocole de tunnel autorisé.

	flars:	intgroup	
<b>FK</b> 12	Barrer:	(imen	
	SCEP forwarding URL:	(Ime:	
	Address Pools	gene:	Eest
	3PV6 Address Pools	()mex	 Seet

Dans la Advanced > Split Tunneling , sélectionnez Tunnel Network List Below dans la liste déroulante Policy afin de faire passer tous les paquets du PC distant par un tunnel sécurisé.

anved	965Nenes: 💽 Prest				
Roweser Proof	Entry Trans Kesses Let Below				
*yConnect Client Sco(IREv1) Client	Network Lists     Inner (: SPLID-ACL		<ul> <li>Mana</li> </ul>		
	Pressing Unstatuter to set up split of Law	🖬 ACI Manager 👘			
	Set up Split Cudie on the Web Security	Furnland Acc. ] Extended Act.			
	Intercept DHCP Configuration Mex	♥ Add + III Dakte			
		No Address Action Secretation			
		Image: Second			

#### Configuration CLI équivalente :

ciscoasa(config)#access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0 ciscoasa(config)#access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

ciscoasa(config)#group-policy clientgroup internal ciscoasa(config)#group-policy clientgroup attributes ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified ciscoasa(config-group-policy)#split-tunnel-network-list SPLIt-ACL

5. Choisir Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add afin de créer un

nouveau compte d'utilisateur ssluser1. Cliquer OK et ensuite Apply.

VPN Policy						
	LIGHTINER, COLORY L					
	Paeswork measure					
	Confine Possenda *******					
	F   Corr addictioned asing PSCH9*					
	Access Madrathan					
	Select one of the optimic below to reduct ASDM, SSU, Telline and Concole enters.					
	Note: All users have indowed access, repardless of these sectory.					
	Tull-americ/2014, 531, Tethel and Console)					
	Privilege invalidued with command authorization.					
	Privlege lovel: 2 -					
	🗇 0.1 login prompt for SSH, Teltret and console (on ASSM acress)					
	This setting is effective only #"ase authentication http: console LOCAL" command is configured.					
	🕐 No ARIAN, SIPI, Televit or Consele access					
	This setting is effective only 6" and authentication http conside LOCHL" and "ana authentication uses" converses are configured.					

#### Configuration CLI équivalente :

ciscoasa(config)#username ssluser1 password asdmASA@

6. Configurez le groupe de tunnels. Choisir Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add afin de créer un nouveau groupe de tunnels ssigroup.Dans la Basic , vous pouvez exécuter la liste des configurations comme indiqué : Nommez le groupe de tunnels ssigroup.Sous Client Address Assignment, choisissez le pool d'adresses vpnpool a partir des versions Client Address Pools liste déroulante.Sous Default Group Policy, choisissez la stratégie de groupe clientgroup a partir des versions Group Policy liste déroulante.

Basic	Name:	ssigroup	
Advanced	Aliases:		Ì
	Authentication		59 
	Method:	💿 AAA 💿 Certificate 💿 Both	
	AAA Server Group:	LOCAL	Manage
		Use LOCAL if Server Group fails	
	Client Address Assignment		2
	DHCP Servers:		
		None O DHCP Link O DHCP Subnet	
	Client Address Pools:	vpnpcol	Select
	Client IPv6 Address Pool	s:	Select
		IPv6 address pool is only supported for SSL.	
	Default Group Policy		
	Crown Dollary	[clieptoroup]	Manage

Sous la Advanced > Group Alias/Group URL , spécifiez le nom d'alias du groupe comme

```
sslgroup_users et cliquez sur ok. Configuration CLI équivalente :
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

#### Configuration ASA version 9.1(2) dans la CLI ciscoasa (config) #show running-config

```
: Saved
ASA Version 9.1(2)
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
interface Management0/0
shutdown
no nameif
no security-level
no ip address
```

#### ! passwd 2KFQnbNIdI.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 same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0 access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

*!--- Standard Split-Tunnel ACL that determines the networks that should travel the Anyconnect tunnel.* 

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 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

*nat (inside, outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool* 

!--- The Manual NAT that prevents the inside network from getting translated when going to the Anyconnect Pool

object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users.
!--- Note: Uses an RFC 1918 range for lab setup.

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 ! ! 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 WebVPN on the outside interface

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

anyconnect enable

!--- Enable the security appliance to download SVC images to remote computers

tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the WebVPN Login page

group-policy clientgroup internal

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

!--- Encrypt only traffic specified on the split-tunnel ACL coming from the SSL VPN Clients.

split-tunnel-network-list value SPLIt-ACL

!--- Defines the previosly configured ACL to the split-tunnel policy.

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

Session Type: SVC

!--- Associate the group policy "clientgroup" created

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup\_users enable

!--- Configure the group alias as sslgroup-users

```
prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#
```

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

• show vpn-sessiondb svc - Affiche les informations sur les connexions SSL actuelles. ciscoasa#show vpn-sessiondb anyconnect

```
Username : ssluser1 Index : 12
Assigned IP : 192.168.10.1 Public IP : 192.168.1.1
Protocol : Clientless SSL-Tunnel DTLS-Tunne1
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 24 2008
```

Duration : 0h:12m:00s NAC Result : Unknown VLAN Mapping : N/A VLAN : none

- show webvpn group-alias Affiche l'alias configuré pour divers groupes. ciscoasa#show webvpn group-alias Tunnel Group: sslgroup Group Alias: sslgroup\_users enabled
- Dans ASDM, sélectionnez Monitoring > VPN > VPN Statistics > Sessions afin de connaître les sessions actuelles dans l'ASA.



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

• vpn-sessiondb logoff name - 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 Utiliser la vpn-sessiondb logoff anyconnect afin de mettre fin à toutes les

sessions AnyConnect.

Ciscoasa#debug webvpn anyconnect 7

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

CSTP state = HEADER PROCESSING http\_parse\_cstp\_method() ...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1' webvpn\_cstp\_parse\_request\_field() ...input: 'Host: 10.198.16.132' Processing CSTP header line: 'Host: 10.198.16.132' webvpn\_cstp\_parse\_request\_field() ...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.05152' Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.05152' Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.1.05152' webvpn\_cstp\_parse\_request\_field() ...input: 'Cookie: webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60' Processing CSTP header line: 'Cookie: webvpn= 146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60' Found WebVPN cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60' WebVPN Cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60' 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: WCRSJOW7Pnbc038' Processing CSTP header line: 'X-CSTP-Hostname: WCRSJOW7Pnbc038' Setting hostname to: 'WCRSJOW7Pnbc038' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-MTU: 1280' Processing CSTP header line: 'X-CSTP-MTU: 1280' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-Address-Type: IPv6, IPv4' Processing CSTP header line: 'X-CSTP-Address-Type: IPv6, IPv4' webvpn\_cstp\_parse\_request\_field() webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-Base-MTU: 1300' Processing CSTP header line: 'X-CSTP-Base-MTU: 1300' webvpn\_cstp\_parse\_request\_field() webvpn\_cstp\_parse\_request\_field() ... input: 'X-CSTP-Full-IPv6-Capability: true' Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true' webvpn\_cstp\_parse\_request\_field() ...input: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0A602CF075972F91EAD1 9BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D' Processing CSTP header line: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0 A602CF075972F91EAD19BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D' 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' webvpn\_cstp\_parse\_request\_field() ...input: 'X-DTLS-Accept-Encoding: lzs' Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'

```
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/255.255.255.0
webvpn_cstp_accept_ipv6_address: No IPv6 Address
CSTP state = HAVE_ADDRESS
SVC: Sent gratuitous ARP for 192.168.10.1.
SVC: NP setup
np_svc_create_session(0x5000, 0xa930a180, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.1!
NO SVC ACL
Iphdr=20 base-mtu=1300 def-mtu=1500 conf-mtu=1406
tcp-mss = 1260
path-mtu = 1260 (mss)
mtu = 1260(path-mtu) - 0(opts) - 5(ssl) - 8(cstp) = 1247
tls-mtu = 1247(mtu) - 20(mac) = 1227
DTLS Block size = 16
mtu = 1300(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1243
mod-mtu = 1243(mtu) & 0xfff0(complement) = 1232
dtls-mtu = 1232(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1210
computed tls-mtu=1227 dtls-mtu=1210 conf-mtu=1406
DTLS enabled for intf=2 (outside)
tls-mtu=1227 dtls-mtu=1210
SVC: adding to sessmgmt
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
```

 Dans ASDM, sélectionnez Monitoring > Logging > Real-time Log Viewer > View afin de voir les événements en temps réel. Cet exemple montre les informations de session entre AnyConnect 192.168.10.1 et le serveur Telnet 10.2.2.2 sur Internet via ASA 172.16.1.1

	0						
Real-Ti	ime Log View	425 -					
Lie 10	ols <u>Window</u>	e <u>H</u> elp					
þ. Rægr	· Rt Copy	See By d	we i 😰 Calor S	ertings   🚉 Cons	w Rule 🎆 Shon Ri	🕼 🖗 Shon Details	2 telo
Hilua Bys	2000 - E-F			- Spritz	및 subhite 웹 :	how All Ands	u,
Time	Syring ID	Source IP	Source Port	Destination IP	Destination Port	Description	
22:03:02	302013	292.368.30.1	51050	30.2.2.2	50	Built rissund TCP com	rector 103 for outside: 592.388.10.1/8/050 (172.16.1.1/8/050)(JCCAC) soluter 1) to outside: 10.2.2.2/80 (10.2.2.2/80) (soluter 1)
22103402	305011	192.363.30.3	64059	172.35.4.1	64059	Built dynamic TCP trans	wishon from outside: 192, 168, 10, 1,64039), OCAL (soluser j) to outside: 172, 35, 1, 1,64059

### Informations connexes

- Pare-feu Cisco ASA 5500-X
- <u>Exemple de configuration de PIX/ASA et d'un client VPN pour un VPN Internet public sur</u> <u>un stick</u>
- Exemple de configuration d'un client VPN SSL (SVC) sur ASA avec ASDM
- <u>Support et documentation techniques Cisco Systems</u>

#### À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.