ASA 7.1/7.2: Split-tunneling voor SVC toestaan op het ASA Configuration-voorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Achtergrondinformatie Configureren Netwerkdiagram ASA-configuraties met ASDM 5.2(2) ASA 7.2(2) Configuratie met CLI Instellen van de SSL VPN-verbinding met SVC Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document bevat stap-voor-stap instructies over hoe u Secure Socket Layer (SSL) VPN-clients (SVC) toegang tot het internet kunt verlenen terwijl ze in een Cisco adaptieve security applicatie (ASA) zijn getunneld. Deze configuratie maakt SVC een veilige toegang tot bedrijfsmiddelen via SSL mogelijk en geeft onbeveiligde toegang tot het internet door het gebruik van gesplitste tunneling.

De mogelijkheid om zowel beveiligd als onbeveiligd verkeer op dezelfde interface te verzenden is bekend als gesplitste tunneling. Split-tunneling vereist dat u precies specificeert welk verkeer beveiligd is en wat de bestemming van dat verkeer is, zodat alleen het gespecificeerde verkeer de tunnel ingaat, terwijl de rest niet gecodeerd wordt door het openbare netwerk (Internet).

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Lokale beheerrechten op alle externe werkstations
- Java en ActiveX controleren het externe werkstation
- Port 443 (SSL) is nergens langs het verbindingspad geblokkeerd

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5500 Series adaptieve security applicatie (ASA) met softwareversie 7.2(2)
- Cisco SSL VPN-clientversie voor Windows 1.1.4.17.9Opmerking: Download het SSL VPN-clientpakket (slclient-win*.pkg) van de <u>Cisco Software Download</u> (alleen geregistreerde klanten). Kopieer de SVC naar het flash-geheugen van de ASA, dat gedownload moet worden naar de externe gebruikerscomputers om de SSL VPN-verbinding met ASA op te zetten. Raadpleeg het gedeelte <u>SVC-software installeren</u> van de ASA-configuratiegids voor meer informatie.
- PC die Windows 2000 Professional SP4 of Windows XP SP2 uitvoert
- Cisco Adaptieve Security Devices Manager (ASDM) versie 5.2(2)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

De SSL VPN Client (SVC) is een VPN-tunneling-technologie die externe gebruikers de voordelen van een IPsec VPN-client biedt zonder dat netwerkbeheerders IPsec VPN-clients op externe computers moeten installeren en configureren. SVC gebruikt de SSL-encryptie die reeds op de externe computer aanwezig is, evenals de inlognaam en verificatie van WebeVPN van het security apparaat.

Om een SVC-sessie te kunnen opzetten, gaat de externe gebruiker het IP-adres in van een WebVPN-interface van het security apparaat in de browser, en de browser sluit zich aan op die interface en geeft het inlogscherm van WebVPN weer. Als u voldoet aan de inlognaam en de verificatie en het beveiligingsapparaat u identificeert dat u de SVC nodig hebt, wordt de SVC op de externe computer gedownloads. Als het beveiligingsapparaat u identificeert met de optie om de SVC te gebruiken, wordt de SVC-installatie door het beveiligingsapparaat gedownload naar de externe computer terwijl er een link in het venster verschijnt om de SVC-installatie te overslaan.

Nadat u het downloaden, installeert en vormt SVC zichzelf, en dan blijft of oninstalleert de SVC, wat van de configuratie afhangt, van de afstandscomputer wanneer de verbinding wordt beëindigd.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het <u>Opdrachtupgereedschap</u> (alleen<u>geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn <u>RFC 1918</u> adressen die in een labomgeving gebruikt zijn.

ASA-configuraties met ASDM 5.2(2)

Voltooi deze stappen om SSL VPN op ASA met Split Tunneling zoals aangegeven te configureren:

- Het document gaat uit van de basisconfiguratie, zoals de configuratie van de interface, enzovoort, die al gemaakt is en naar behoren werkt. Opmerking: Raadpleeg <u>HTTPS-toegang</u> <u>voor ASDM</u> om de ASA te kunnen configureren door de ASDM.Opmerking: WebVPN en ASDM kunnen niet op dezelfde ASA-interface worden ingeschakeld tenzij u de poortnummers wijzigt. Raadpleeg <u>ASDM en WebVPN ingeschakeld op dezelfde interface</u> <u>van ASA</u> voor meer informatie.
- 2. Kies Configuration > VPN > IP-adresbeheer > IP-pools om een IP-adrespool te maken: VPN-

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

3. WebVPN inschakelenKies Configuration > VPN > WebeVPN > WebeVPN Access en licht de externe interface met muis toe en klik op Enable. Selecteer de vervolgkeuzelijst Tunnel groep inschakelen in het dialoogvenster Pagina voor vastlegging van WebVPN om de uitrollijst in de inlogpagina voor gebruikers in staat te stellen hun respectievelijke groepen te

op Apply (Toepassen).

kiezen.			
Configuration > VPN > WebVPN	> WebVPN Access		
VPN Wizard	WebVPN Access		
🕀 🚰 General			
Ē-∱ KE	Configure access parameters for WebV	PN.	
🖲 📲 IPSec			
E Sp IP Address Management			
Assignment			
P Pools	Interface	WebVPN Enabled	Ensble
1 NAC	inside	No	
	outside	Ves	Disable
WebVPN Access			Disable
Proxies			
Auto Simon			
- Cache			
Content Rewrite			
Java Trustpoint	· · · · · · · · · · · · · · · · · · ·	_	
Proxy Bypass	Port Number: 443		
- Tig Servers and URLs	· · · · · · · · · · · · · · · · · · ·	<u> </u>	
Port Forwarding	Default Idle Timeout: 1800	seconds	
		<u> </u>	
ACLs	Max. Sessions Limit: 2		
-16 Encoding	a second and a second		
SSL VPN Client	WebVPN Memory Size: 50	% of total physical memory	
SSO Servers	(many and a star		
🕑 🚟 E-mail Proxy	M Enable Tunnel Group Drop-down Lis	t on WebVPN Login Page	
		(Accily) Reset	
-d thread			

Klik op **Apply** (Toepassen).Kies **Configuratie > VPN > WebVPN > SSL VPN-client > Add** om het SSL VPN-clientbeeld uit het flash-geheugen van ASA zoals weergegeven toe te voegen.

			sh
		Upload	
ОК	Cancel	Help	
owse Flash Dialog			
Folders	Files		
🖃 🥏 disk0:	FileName 🔺	Size (bytes)	
0			
	asdm-603.bin	6,851,212	
	asdm-603.bin asa803-k8.bin	6,851,212 14,635,008	
	asdm-603.bin asa803-k8.bin admin.cfg	6,851,212 14,635,008 1,220	
	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0	6,851,212 14,635,008 1,220 2,635,734	
⊕–͡⊒ log 迚–͡⊒ crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin	6,851,212 14,635,008 1,220 2,635,734 6,889,764	
⊕– ີ log ⊞– ີ crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin	6,851,212 14,635,008 1,220 2,635,734 6,889,764 8,312,832	
ug ⊡-⊡ crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin asdm-522.bin	6,851,212 14,635,008 1,220 2,635,734 6,889,764 8,312,832 5,623,108	
ug ⊡-⊡ crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin asadm-522.bin asa802-k8.bin	6,851,212 14,635,008 1,220 2,635,734 6,889,764 8,312,832 5,623,108 14,524,416	
ug ⊡ - i crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin asam-522.bin asa802-k8.bin old_running.cfg	6,851,212 14,635,008 1,220 2,635,734 6,889,764 8,312,832 5,623,108 14,524,416 1,841	

Klik op

🎼 Add SSL VPN Client	Image	
Flash SVC Image	disk0:/sslclient-win-1.1.4.179.pkg	Browse Fla
		Upload.
	OK Cancel	Help

op OK.Klik op SSL VPN-client

vakje.

Configuration > VPN > WebVPN	I > SSL VPN Client	
VPN Wizard General KE P Rec P Address Management Assignment IP Pools NAC ViebVPN ViebVPN Access	SSL VPN Client Configure SSL VPN Client parameters. ✓ Enable SSL VPN Client SSL VPN Client Images disk0:/sslclient-win-1.1.4.179.pkg	

Klik op Apply (Toepassen).Compatibele CLI-configuratie:

4. Groepsbeleid configurerenKies Configuratie > VPN > Algemeen > Groepsbeleid > Toevoegen (Intern Groepsbeleid) om een interne clientgroep voor groepsbeleid te creëren. Selecteer onder General het aankruisvakje WebVPN om WebVPN in te schakelen als een tunneling-

protocol.

🚰 Add Internal Group Policy		
Name: Clientgroup		
General IPSec Client Conf	iguration Client Fir	ewall Hardware Client NAC WebVPN
Check an Inherit checkbox	to let the correspo	nding setting take its value from the default group policy.
Tunneling Protocols:	🗖 Inherit	IPSec WebVPN L2TP over IPSec
Filter:	🔽 Inherit	Manage

In het tabblad **Clientconfiguratie > Algemene clientparameters**, schakelt u het vakje **Inherit** uit voor Split-tunnelbeleid en kiest u **de onderstaande** lijst met **tunnelnetwerkbestanden** in de vervolgkeuzelijst.Schakel het vakje **Inherit** uit voor de **netwerklijst van splitter** en klik

vervolgens op **Bewerken** om de ACL-Manager te starten.

Edit Internal Group Policy: clientgroup		
Name: clientgroup		
General IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
General Client Parameters Cisco Client Parameter	s Microsoft Client	Parameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🔲 Inherit	Tunnel Network List Below
Split Tunnel Network List:	🗆 Inherit	None Manage
Address pools		
🔽 Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	Add⊳>	8
	< <remove< td=""><td></td></remove<>	
2		
ок	Cancel	Help

Kies in de ACL Manager **Add > Add ACL...** om een nieuwe toegangslijst te maken.

CL Manager	-d ACI]		
🔂 Add 👻 🛒 Edit (🗊 Delete 🛧 🧃	- X = a -	1
🔂 Add ACL	dress	Action	Description
🖨 Add ACE		de construction de	
🔹 Insert			
insert After			

Typ een naam voor ACL en klik op

Add 👻 🗹	Edit <u>î</u> Delete 🛧	* * * * * *	
No	Address	Action	Description
Add ACL			×

Zodra de ACL-naam is gemaakt, kiest u Add > Add ACE om een Access Control Entry (ACE) toe te voegen.Defineer de ACE die overeenkomt met het LAN achter de ASA. In dit geval is het netwerk 10.77.241.128/26 en kiest u Vergunning.Klik op OK om de ACL-Manager te verlaten.

No	Address	Action	Description	
split-tunnel				
Add ACE				
Action				
Action:	Permit 💌			
1000000				
-Host/Netv	work			
IP Addr	ess: 10.77.241.128			-
Notmoo	h DEE DEE DEE 100			-
Netmas	k.			
Description	,			
Description	•			

Verzeker u dat ACL die u zojuist hebt gemaakt, is geselecteerd voor Split Tunnel Network List.Klik op **OK** om naar de configuratie van het groepsbeleid terug te keren.

撞 Edit Internal Group Policy: clientgroup		
Name: clientgroup		¥
General IPSec Client Configuration Client Firewa	I Hardware Client	NAC VVebVPN
Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
General Client Parameters Cisco Client Parameter	rs Microsoft Client	Parameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🗖 Inherit	Tunnel Network List Below
Split Tunnel Network List:	🗖 Inherit	split-tunnel Manage
⊂ Address pools		
I Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	Add⊳>	
	< <remove< td=""><td></td></remove<>	
2		
	Cancel	Help
ок	Cancel	Help

Klik in de hoofdpagina op **Toepassen** en **Verzend** (indien nodig) om de opdrachten naar de ASA te verzenden.Schakel voor de optie SSL VPN-client in het vakje Inherit uit en klik op het **optionele** radioknop.Met deze keuze kunt de externe client kiezen of u op het tabblad **WebVPN > SLB** klikt, en deze opties kiezen:Download de SVC niet. Kies altijd een optie die garandeert dat de SVC wordt gedownload naar het externe werkstation tijdens elke SSL VPN-verbinding.Schakel het vakje **Inherit uit** voor de optie Installeren bij clientsysteem en klik vervolgens op het radioknop **Ja**.Met deze actie kan de SVC-software op de clientmachine blijven staan; Daarom is de ASA niet verplicht de SVC-software aan de client te downloaden telkens wanneer een verbinding wordt gemaakt. Deze optie is een goede keuze voor externe gebruikers die vaak toegang hebben tot het bedrijfsnetwerk.Schakel het vakje **Inherit** uit, trek voor de optie Interval heronderhandelingen uit en geef het aantal minuten op tot het vakje

Onbeperkt is.De beveiliging wordt verbeterd wanneer u de limieten instelt op de tijdsduur die een toets geldig is.Schakel het vakje **Inherit uit** voor de optie Heronderhandelingsmethode en klik op de radioknop **SSL**. Heronderhandeling kan gebruik maken van de huidige SSL-tunnel of een nieuwe tunnel die uitdrukkelijk is gemaakt voor heronderhandeling.Uw SSL VPN-clienteigenschappen moeten worden geconfigureerd zoals in deze afbeelding:

Name: clientgroup				
,	-	. 6		
eneral IPSec Client Configuration C	lient Firewall Hardw	vare Client NAC 🔱	VebVPN	
Configure WebVPN attributes using the f	ollowing tabs .			
Check an Inherit checkbox to let the corr	esponding setting tak	e its value from the	default group polic	су.
Functions Content Filtering Homepa	ge Port Forwarding	Other SSL VPN	Client) Auto Signo	on
Use SSL VPN Client:	🗌 Inherit	C Always	© Optional	C Never
Keep Installer on Client System:	🗖 Inherit	(Yes	C No	
Compression:	🔽 Inherit	C Enable	$oldsymbol{C}$ Disable	
Keepalive Messages:	🔽 Inherit	F Enable	Interval:	secor
Key Renegotiation Settings				
Renegotiation Interval:	🗌 Inherit	🗌 Unlimited	30	minutes
Renegotiation Method:	🗖 inherit	C None	(ISSL	C New tunn
Dead Peer Detection				
Gateway Side Detection:	🔽 Inherit	F Enable	Interval:	seco
Client Side Detection:	🔽 Inherit	🗖 Enable	Interval:	seco

Klik op **OK** en vervolgens **op Toepassen**.



Compatibele CLI-configuratie:

5. Kies Configuratie > VPN > Algemeen > Gebruikers > Toevoegen om een nieuwe gebruikersaccount te maken1. Klik op OK en

Identity VPN Policy	Web∨PN		
	Username:	ssluser1	
	Password:	******	
	Confirm Password:	******	
	🔲 User authentio	cated using MSCHAP	
	Privilege level is used v	with command authorization.	
	Privilege Level:	2	<u>·</u>
	OK	Cancel	Heln

ompatibele CLI-configuratie:

6. Kies Configuratie > Eigenschappen > AAA Instellingen > AAA-servers > Bewerken om de standaardinstelling van de servergroep LOCAL te wijzigen en kies het aanvinkvakje Local User Lockout inschakelen met maximale probewaarde 16.

Configuration > Properties > A	AA Setup > AAA Server Gro	ups			
Startup Wizard	AAA Server Groups	_			
🕀 🚽 AAA Setup	1				
AAA Server Groups	AAA server groups				
Auth. Prompt	Server Group	Destand	Accounting Mode	Readination Mode	
LDAP Attribute Map	Server oroup	Protocol	Accounting mode	Reactivation mode	Add
Anti-Spoofing	LOCAL	LOCAL			Edd.
E-B ARP	🐋 Edit LOCAL Server Gro	oup		×	
Auto Update	Sector and the sector of the s			-	Delete
Client Update					-
Certificate	I his feature allows to	specify the maxim	um number of falled attem	ipts to allow before	
E price Access	detabase is used for a	access to in a therefication	e user. This limit is applici	able only when local	
AAA Access	ualabase is used for a	autrenucation.			
	E Emiliaria				
Secure Shell	Enable Local Use	Lockout;			-
Teinet					Add
Virtual Access	Maximum Attempt	s: (16)			-
Device Administration		1.00			Ealt
P DHCP Services					
E DNS					Delete
High Availability and Scal					1 10 19
Failover	0		Cancel H	aln	move.u
Fragment				alp	Mose Dry

Compatibele CLI-configuratie:

7. Tunnelgroep configurerenKies Configuration > VPN > General > Tunnel Group > Add (WebVPN-toegang) om een nieuwe groep voor tunnelgroepen te maken. In het tabblad Algemeen > Basis kiest u het groepsbeleid als clientgroep uit de vervolgkeuzelijst.

🚰 Add Tunnel (Group			_	<u></u>	
Name:	sslgroup)	T	ype:	ebvpn	
General 🛛	VebVPN					
Configure	e general acci	ess attributes fro	om the followir	ng sub-tab	s.	
Basic A	uthentication	Authorization	Accounting	Client Ad	dress Assignment	Advanced
Group	Policy:	clientgroup	×]		
⊏ s	trip the realm t	rom username l	pefore passing	it on to th	e AAA server	

In **het** tabblad **Toewijzing van** clientadres, klikt u onder Adres Pools op **Add** >> om het beschikbare **VPN-adrespool** toe te wijzen.

rianic.	Jasigroup	k (rype. Jv	repupit	
General	WebVPN				
Configu	re general access attributes	s from the followir	ng sub-tai	os.	
Basic	Authentication Authorizati	on Accounting	Client Ac	ldress Assignment	Advanced
т	o specify whether to use D	HCP or address p	ools for a	address assignment	t, go to Configurati
Ż	IP Address Management >	Assignment.		-	
	DHCP Servers				
				14	
	IP Address:		Add >>		
	IP Address:		Add >> Delete		
	IP Address:		Add >> Delete		
	IP Address:		Add >> Delete		
	IP Address:		Add >> Delete		
	IP Address:	pecific address po	Add >> Delete	the Advanced tab.	
	IP Address: Address Pools To configure interface-sp Available Pools	pecific address po	Add >> Delete	the Advanced tab.	ools

In het tabblad **WebVPN > Group Aliases en URL**'s typt u de naam van het alias in het dialoogvenster parameter en klikt u op **Add >>** om dit in de lijst met groepsnamen in de logpagina te laten

verschijnen.

onfigure \A/eh\/PN access attrik	utes from the following sub	tabs	
	Alieses and LIPLs Lucks		
ISIC NetBIUS Servers (0100)	Allases and UKES Web F	'age	
Group Aliases			- 1
		Alias	Statu
Alias:	Add >>	sslgroup_users	enable

Klik op OK en vervolgens op Toepassen.Compatibele CLI-configuratie:

8. NAT configurerenKies Configuration > NAT > Add > Add > Dynamic NAT Rule voor het

verkeer dat v	an het b	oinnennetwer	rk komt di	e met ex	ctern IP	adres	172.16	.1.5 kan w	orden
per P	dd Dyn	amic NAT R	ule						

-Real Address				
Interface:	inside			I
IP Address:	0.0.0.0].
Netmask:	0.0.0.0			1
Dynamic Tran	slation			
Interface:	outside			
🔂 Add 🗗	🖌 Edit	<u> Delete</u>		
Select	Pooi ID	Addre	sses Pool	
		🚇 172.16.1.5		
			-1:	
NAT Options				

Klik op **OK** en klik op

Toepassen in de hoofdpagina.Compatibele CLI-configuratie:

9. Configureer de nat-vrijstelling voor het retourverkeer van binnen het netwerk naar de VPNclient.

```
ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0
ciscoasa(config)#nat (inside) 0 access-list nonat
```

ASA 7.2(2) Configuratie met CLI

Cisco ASA 7.2(2)
ciscoasa# show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!

```
interface Ethernet0/1
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
1
interface Management0/0
shutdown
no nameif
no security-level
no ip address
1
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list split-tunnel standard permit 10.77.241.128
255.255.255.192
!--- ACL for Split Tunnel network list for encryption.
access-list nonat permit ip 10.77.241.0 192.168.10.0
access-list nonat permit ip 192.168.10.0 10.77.241.0 !--
- ACL to define the traffic to be exempted from NAT.
pager lines 24 mtu inside 1500 mtu outside 1500 ip local
pool vpnpool 192.168.10.1-192.168.10.254
!--- The address pool for the SSL VPN Clients no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-522.bin no asdm history enable arp
timeout 14400 global (outside) 1 172.16.1.5
!--- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP. nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 0.0.0.0 0.0.0.0
access-group 100 in interface outside
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 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal
!--- Create an internal group policy "clientgroup".
group-policy clientgroup attributes
vpn-tunnel-protocol webvpn
```

! Enable webvpn as tunneling protocol. split-tunnel-
policy tunnelspecified
split-tunnel-network-list value split-tunnel
! Encrypt the traffic specified in the split tunnel
ACL only. webvpn
svc required
! Activate the SVC under webvpn mode. svc keep-
installer installed
! When the security appliance and the SVC perform a
rekey. ! they renegotiate the crypto keys and
initialization vectors I and increase the security
of the connection syc rekey time 30
of the connection. By creater of
I Command that specifies the number of minutes I
from the stort of the socier until the velocitation
from the start of the session until the rekey takes
place, ! from 1 to 10080 (1 week). svc rekey method
ssl
<pre>! Command that specifies that SSL renegotiation !</pre>
takes place during SVC rekey. username ssluser1 password
ZRhW85jZqEaVd5P. encrypted
! Create an user account "ssluser1". aaa local
authentication attempts max-fail 16
• • • • • • • • • • • • • • • • • • • •
I Enable the AAA local authentication http server
onable http 0.0.0.0.0.0.0.0 ingide no grmp gerver
leasting as any source source hour sump-server
iocación no simp-server contact simp-server enable traps
snmp authentication linkup linkdown coldstart tunnel-
group sslgroup type webvpn
<i>! Create a tunnel group "sslgroup" with type as</i>
WebVPN. tunnel-group sslgroup general-attributes
address-pool vpnpool
<pre>! Associate the address pool vpnpool created.</pre>
default-group-policy clientgroup
<i>! Associate the group policy "clientgroup" created.</i>
tunnel-group sslgroup webvon-attributes
aroun-alias selaroun users enable
gloup allas ssigloup_usels enable
Configure the group plice of galaroup years tolet
configure the group arias as ssigroup-users, ternet
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
esmtn inspect salnet inspect suproc inspect tftn inspect
sin inspect where I service-policy global policy global
sip inspect xamep : service poincy global_poincy global
enable outside
Enable WebVPN on the outside interface. svc image
disk0:/sslclient-win-1.1.4.179.pkg 1

!--- Assign an order to the SVC image. svc enable



Instellen van de SSL VPN-verbinding met SVC

Voltooi deze stappen om een SSL VPN-verbinding met ASA op te zetten.

1. Typ het URL- of IP-adres van de WebVPN-interface van de ASA in uw webbrowser in het formaat zoals weergegeven.

https:// <ip address="" asa="" interface="" of="" the="" webvpn=""></ip>	
File Edit View Favorites Tools Help	
🔇 Back 🔹 🕥 - 💽 😰 🚮 🔎 Search 🤺 Favorites 🤣 🎯 - 🖕 🖼 🖄	
Address 🕘 https://172.16.1.1/+webvpn+/index.html	
CISCO SYSTEMS WebVPN Service	
Login	
Please enter your username and password.	
USERNAME:	
PASSWORD:	
CROUR	
GROOP: ssigroup_users	
Login Clear	
	and the second sec

2. Voer uw gebruikersnaam en wachtwoord in en kies vervolgens uw respectievelijke groep in de vervolgkeuzelijst zoals

	Login	
Please enter you	r username and pas	sword.
USERNAME:	ssluser1	
PASSWORD:	•••••	
GROUP:	sslgroup_users	~
	Login	Clear

weergegeven.l
3. ActiveX-software moet in uw computer geïnstalleerd zijn voordat u de SVC downloaden.

File Edit View Favorites Tools Help
🚱 Back 🔹 🕥 - 💽 🛃 🏹 🔎 Search 🤶 Favorites 🧭
Address Status://172.16.1.1/CACHE/stc/1/index.html
CISCO SYSTEMS SSL VPN CLIENT for WEBVPN
The installer is downloading the ActiveX. Please wait
<u>Useful Tips</u>

4. Deze vensters verschijnen voordat de SSL VPN-verbinding tot stand is



5. U kunt deze vensters verkrijgen zodra de verbinding tot stand is

gebracht.



6. Klik op de gele toets die in de taakbalk van uw computer verschijnt. Deze vensters worden weergegeven die informatie geven over de SSL-verbinding. Bijvoorbeeld, 192.168.10.1 is de toegewezen IP voor client en server IP adres is 172.16.1.1, Split tunneling is ingeschakeld,

allo SSLV	PIN CLIENT for	WEBVPIN	
Statistics Boute D	etails About		
Address Informa	tion	SSL Information	
Server:	172.16.1.1	Cipher:	3DES SHA-1
Client:	192.168.10.1	Version:	TLSv1
Bytes		Transport Informat	ion
Sent:	2887	Local LAN:	Disabled
Received:	940	Split Tunneling:	Enabled
Frames		Connection Inform	ation
Sent:	35	Time:	00:00:24
Received:	12		

enzovoort.

kunt ook het beveiligde netwerk controleren dat door SSL moet worden versleuteld, de netwerklijst wordt gedownload van de gesplitste tunneltoegangslijst in ASA.In dit voorbeeld, waarborgt de SSL VPN client toegang tot 10.77.241.128/24 terwijl al het andere verkeer niet versleuteld en niet over de tunnel verzonden

0	Cisco Syste	ms SSL VPN Client		
	CISCO SYSTEMS	SLVPN CLIENT F	or WEBVPN	
	Statistics Bo	ute Details About		
	Local LAN	Routes	Secure Routes	
	Network	Subnet Mask	Network 10.77.241.128	Subnet Mask 255.255.255
wordt.	2	Close	Disconnect	
🥑 Ciso	co Systems SS	iL VPN Client		E
Cisco Sys	SSLV	PN CLIENT for W	ebvpn	
Stati	istics Route De	tails (About)		
C	ISCO SYSTEMS Illiumiillius	SSL VPN CLIE for WEBVPN	NT Version	1.1.4.179
1		Create a full anywhere an	y secure connectivitime	tion
0.0	Copyright 2004-200	6 Cisco Systems Inc. Al	rights reserved. Cisco. Cis	co Systems
and its a	the Cisco System affiliates in the Unit	s Logo are registered tra ed States and certain oth	demarks of Cisco Systems, her countries.	Inc. and/or
		Close	Disconnect	

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

• toon WebVPN svc-Toont de SVC beelden die in het ASA flash geheugen zijn opgeslagen.

```
1. disk0:/sslclient-win-1.1.4.179.pkg 1
CISCO STC win2k+ 1.0.0
1,1,4,179
Fri 01/18/2008 15:19:49.43
```

- 1 SSL VPN Client(s) installed
- toon vpn-sessiondb svc-Toont de informatie over de huidige SSL verbindingen.

```
Session Type: SVC
```

```
Username : ssluser1
Index
           : 1
Assigned IP : 192.168.10.1 Public IP : 192.168.1.1
Protocol : SVC
                                Encryption : 3DES
Hashing
          : SHA1
Bytes Tx : 131813
                                Bytes Rx : 5082
Client Type : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Client Ver : Cisco Systems SSL VPN Client 1, 1, 4, 179
Group Policy : clientgroup
Tunnel Group : sslgroup
Login Time : 12:38:47 UTC Mon Mar 17 2008
Duration : 0h:00m:53s
Filter Name :
```

• Laat website-groep-alias-displays de geconfigureerde alias voor verschillende groepen zien.

Tunnel Group: sslgroup Group Alias: sslgroup_users enabled

 In ASDM, kies Bewaking > VPN > Statistieken > Sessies om over de huidige WebVPN sessies in de ASA te weten te

Very Connection Graphs	Sessions		-				
PSec Tunnels	Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
VPN Statistics	0	0	1	0	0	1 1	12
Global IND/PSec Stat NAC Session Summe Protocol Statistics	Usernam	e G	roup Policy	Protocol		Login Time	Detai
- Canadana	achusert	clientar	nner Group	WebVPN	08 49 5	2 UTC Thu Mar 20	2 Loog

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

1. **vpn-sessiondb naam <gebruikersnaam>**- Opdracht om de SSL VPN-sessie voor de specifieke gebruikersnaam op te starten.

```
ciscoasa#vpn-sessiondb logoff name ssluser1
Called vpn_remove_uauIth: success!
webvpn_svc_np_tear_down: no ACL
NFO: Number of sessions with name "ssluser1" logged off : 1
```

Evenzo kunt u de **vpn-sessiondb logoff svc** opdracht gebruiken om alle SVC-sessies te beëindigen.

 N.B.: Als de PC naar de stand-by of de hibernate modus gaat, kan de SSL VPN-verbinding worden afgesloten.

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

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

Debug WebVPN svc <1-255>—Biedt de real-time webgebeurtenissen om de sessie te

kunnen opzetten. Ciscoasa#debug webvpn svc 7

```
ATTR_CISCO_AV_PAIR: got SVC ACL: -1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179'
Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4,
179'
Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
webvpn_cstp_parse_request_field()
... input: 'X-CSTP-Accept-Encoding: deflate; q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2 '
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2 '
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2 '
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
```

SVC: NP setup
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC: adding to sessmgmt
SVC: Sending response
CSTP state = CONNECTED

4. Kies in ASDM Bewaking > Vastlegging > Realtime logvenster > Weergave om de gebeurtenissen in realtime te kunnen zien. Dit voorbeeld toont de sessieinformatie tussen SVC 192.168.10.1 en Webserver 10.2.2.2 in het internet via ASA

0 S 192.10 10.77	ource IP	Destination P	Description
192.16	68.10.255		
10.77	the second second second second		No translation group found for up are outside:192.168.10.1/138 dist inside:192.168.10.255/138
	244,193		Notranslation group found for udp arc outside:192,168,18.17/027 dat inside:10.77.244.193/53
10.77	244,193		No transistion group found for udp are outside:192.168.10.17.028 dat inside:10.77.244.19363
192.16	68.10.1	10.2.2.2	Built inbound TCP connection 1902 for outside:192.168.10.1/1100 (172.16.1.5/1025) to outside:10.2.2.260 (10.2.2.260) (soluser1)
192.16	68.10.1	172,16.1.5	Built dynamic TCP translation from outside:192.158.10.1/1100 to outside:172.16.1.5/1025
192.18	66.10.255		No translation group Yound for upp arc outside 192,168,10,1/138 dist inside:192,168,10,255/138
10.77	244.193		No translation group found for upp and outside: 192.168.10.1/1027 dat inside: 10.77.244.193/53
10:77.	244.193		No translation group found for upp and outside: 192.168.10.1/1028.dst.inside:10.77.244.193/53
10.77	244 193		No transistion group found for upla and outside 192.168.10.1/1027 dat inside:10.77.244.193/53
1.000			

Gerelateerde informatie

- Cisco 5500 Series adaptieve security applicatie, productondersteuning
- ASA/PIX: Split-tunneling voor VPN-clients toestaan in het ASA Configuration-voorbeeld
- De router staat VPN-clients toe om IPsec en internet te verbinden met behulp van het configuratievoorbeeld voor splitter-tunneling
- PIX/ASA 7.x en VPN-client voor publiek internet VPN op een tick Configuration Voorbeeld
- SSL VPN-client (SVC) op ASA met ASDM Configuratievoorbeeld
- <u>Technische ondersteuning en documentatie Cisco Systems</u>