ASA 8.X: Routing SSL VPN-verkeer door middel van een gekanaliseerde standaardgateway

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Achtergrondinformatie Configureren Netwerkdiagram ASA-configuratie met ASDM 6.1(5) Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u de adaptieve security applicatie (ASA) kunt configureren om het SSL VPN-verkeer via de getunneerde standaardgateway (TDG) te sturen. Wanneer u een standaardroute met de getunneerde optie maakt, wordt al verkeer van een tunnel die op de ASA eindigt die niet kan worden routed met geleerde of statische routes naar deze route verzonden. Voor verkeer dat uit een tunnel opkomt, overschrijdt deze route elke andere geconfigureerde of aangeleerde standaardroutes.

Voorwaarden

Vereisten

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

- ASA die op versie 8.x draait
- Cisco SSL VPN-client (SVC) 1.xOpmerking: Download het SSL VPN-clientpakket (slclientwin*.pkg) van <u>Cisco Software Download</u> (alleen geregistreerde klanten). Kopieert de SVC naar het flash-geheugen op de ASA. De SVC moet naar de externe gebruikerscomputers worden gedownload om de SSL VPN-verbinding met de ASA op te zetten.

Gebruikte componenten

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

- Cisco 5500 Series ASA-software met versie 8.x
- Cisco SSL VPN-clientversie voor Windows 1.1.4.17.9
- PC met Windows 2000 Professional of Windows XP
- Cisco Adaptieve Security Devices Manager (ASDM) versie 6.1(5)

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 geeft 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 de security applicatie.

In het huidige scenario, is er een SSL VPN client verbonden met de interne middelen achter de ASA door de SSL VPN-tunnel. De split-tunnel is niet ingeschakeld. Wanneer de SSL VPN-client is verbonden met de ASA, worden alle gegevens getunneld. Naast de toegang tot de interne bronnen is het belangrijkste criterium om dit getunnelde verkeer door de Default Tunneled Gateway (DTG) te leiden.

U kunt een afzonderlijke standaardroute voor getunneld verkeer definiëren samen met de standaardroute. Niet gecodeerd verkeer dat door ASA wordt ontvangen, waarvoor geen statische of aangeleerde route is, wordt door de standaard standaardroute geleid. Versleuteld verkeer dat door de ASA is ontvangen, waarvoor geen statische of aangeleerde route bestaat, zal worden doorgegeven aan de DTG die wordt gedefinieerd via de getunnelde standaardroute.

Om een getunnelde standaardroute te definiëren, gebruikt u deze opdracht:

route <if_name> 0.0.0.0 0.0.0.0 <gateway_ip> tunneled

Configureren

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

Opmerking: Gebruik het <u>Opname Gereedschap</u> (<u>alleen 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:



In dit voorbeeld, heeft de SSL VPN client toegang tot het binnennetwerk van de ASA door de tunnel. Het verkeer dat bestemd is voor andere bestemmingen dan het binnennetwerk, wordt ook getunneld omdat er geen gesplitste tunnel is ingesteld en wordt door de TDG geleid (192.168.100.20).

Nadat de pakketten aan TDG worden routed, dat in dit geval router 2 is, voert het adresvertaling uit om die pakketten naar Internet te leiden. Voor meer informatie bij het configureren van een router als een gateway voor internet, raadpleeg <u>hoe u een Cisco-router achter een niet-Cisco</u> <u>kabelmodem kunt configureren</u>.

ASA-configuratie met ASDM 6.1(5)

Dit document is gebaseerd op de basisconfiguraties, zoals de interfaceconfiguratie, zijn volledig en werken correct.

Opmerking: Raadpleeg <u>HTTPS Access voor ASDM</u> voor informatie over hoe de ASA door ASDM kan worden geconfigureerd.

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 van ASA</u> voor meer informatie.

Voltooi deze stappen om SSL VPN te configureren door de SSL VPN-wizard te gebruiken.

1. Kies in het menu Wizard de SSL VPN-

e View	Tools	Wizards	Window Help	
Home	Cor	Sta IPse SSL	rtup Wizard ec VP <u>N Wizard</u>	h Sack Forward ? Help
Dev	ice Info	Higi Pac	h Availability and Scalability Wizard ket Capture Wizard	

2. Klik op het vakje Cisco SSL VPN-client en klik op Volgende.



 Voer een naam in voor de verbinding in het veld Naam van de verbinding en kies vervolgens de interface die door de gebruiker wordt gebruikt om toegang te krijgen tot SSL VPN in de vervolgkeuzelijst SSL VPNinterface.

🖆 SSL VPN Wizard		×
SSL VPN Wizard	SSL ¥PN Interface (Step 2 of 6)	
	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 web brow	ser
-	to authenticate the ASA. Certificate: None ··	
A REAL PROPERTY	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	
	≤Back Next > Fylish Cancel Help	

- 4. Klik op Volgende.
- 5. Kies een authenticatiemodus en klik op **Volgende**. (Dit voorbeeld gebruikt lokale authenticatie.)

🖆 SSL VPN Wizard		X
SSL VPN Wizard	User Authentication (Step 3 of 6)	-
SSE VPM 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. At the security appliance authenticates users when they login. AAA Server Group Name: AAA Server Group Name: AAA Server Group Name: Carbine authenticate using the local user database User to be Added Usernone: Confirm Password: Confirm Password	
	Seck Next > Ginish Cancel He	þ

6. Maak een nieuw groepsbeleid anders dan het bestaande standaardgroepsbeleid.

📬 SSL VPN Wizard			X
SSL VPN Wizard	Group Policy (Step 4 of 6)		
12D	A group policy is a collection of user- policy, all users are members of the default group policy lets users inherit policy or username level.	oriented attribute/value default group policy (Dfl : attributes that you har	pairs. Unless assigned to a specific group tGrpPolicy). Therefore, configuring the re not configured at the individual group
6 6 6	Create new group policy	grppolicy	
	O Modify existing group policy	DRGrpPolicy	
E		≤Back	Next > nish Cancel Help

7. Maak een nieuwe pool van adressen die aan de SSL VPN client-PC's zal worden toegewezen zodra ze worden



Er is een pool van 192.168.10.40-192.168.10.50 aangemaakt door de naam

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

newpool.

8. Klik op Bladeren om de SSL VPN-clientafbeelding naar het flash-geheugen van de ASA te

kiezen en te uploaden.

🖆 SSL VPN Wizard					
SSL VPN Wizard	IP Address Pools and	Client Image - AnyO	onnect VPN C	ient Connections C	Inly (Step 5 of 6)
- Aller	The security appliano client self-installs, use to resources on a cor	e downloads the AnyCor is SSL or DTLS encryptio porate network. The ren	nect VPN Client n for the duratio note PC becomes	to remote users when n of the connection, a part of the corporati	n they connect. The and allows full access e network.
	IP Address Pool				
6.6	Create a new addre from the pool when	ess pool or select an exis they connect.	sting address poo	ol. Remote PCs are as	isigned addresses
and the second	IP Address Pool:	newpool	× (New	
and the second second	Address Pool Rang	: 192.168.10.40 - 19	2.168.10.50		
	AnyConnect VPN Clies	t Image Location			
-	Identify a file in fla the file and loads it	sh memory as an AnyCo Into cache memory for o	nnect VPN Client downloading to re	image. The security a	appliance expands
14	Location:			Browse	
	Download latest Av	wConnect VPN Client fro	om Cisco.com		
I-HULIMIN					
	1				
			≤ Back N	ext > Einish	Gancel Help

9. Klik op **Upload** om het bestandspad in de lokale map van de machine in te stellen.

🖆 Add SSL VPN Client I	mage			
AnyConnect Image:				Browse Flash
			-	Upload
	ок	Cancel	Help)

10. Klik op Local Files Bladeren om de map te selecteren waarin het bestand Sslclient.pkg bestaat.

📧 Upload Image	
Upload a file from local c few minutes. Please wail	omputer 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
(Upload File Close Help

11. Klik op **Upload File** om het geselecteerde bestand te uploaden naar de flitser van ASA.

🖆 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 Docum Browse Local Files
Flash File System Path: disk0:/sslclient-win-1.1.4.179.pkg Browse Flash
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.
ОК

12. Klik op **OK** om die taak te voltooien zodra het bestand op de flitser van ASA is geüpload.



13. Het toont het laatste bestand van willekeurige kg dat op de flitser van ASA is geüpload. Klik op

Volgende.

🖆 SSL VPN Wizard					
SSL VPN Wizard	IP Address Pools and	l Client Image - AnyConn	ect VPN Cli	ent Connec	tions Only (Step 5 of 6)
THE M	The security appliance client self-installs, use to resources on a cor	e downloads the AnyConnect is SSL or DTLS encryption for porate network. The remote I	VPN Client b the duration PC becomes	o remote use of the conn part of the c	rs when they connect. The ection, and allows full access orporate network.
6 A CH	Create a new addr from the pool when	ess pool or select an existing they connect.	address pool	. Remote PC	s are assigned addresses
and the second	IP Address Pool:	newpool	¥ [New	
1	Address Pool Rang	e: 192.168.10.40 - 192.16	68.10.50		-
a st	AnyConnect VPN Clie	nt Image Location			
- cette	Identify a file in fla the file and loads it	sh memory as an AnyConnect Into cache memory for down	t VPN Client i loading to rei	mage. The se mote users.	acurity appliance expands
-Ital	Location:	disk0:/sslclient-win-1.1.4.	179.pkg	Browse]
	Download latest Ar	nyConnect VPN Client from C	isco.com		
			s Back (at > DEnt	Cancel Help

14. De samenvatting van de SSL VPN clientconfiguratie wordt weergegeven. Klik op **Voltooien** om de wizard te voltooien.

			- Contraction of the local sector
SSL VPN Wizard	Summary (Step 6 of 6)		
	You have created a SSL VPN consected Features: SSL VP Connection Name: Test SSL VPN Interface: outsid User Authentication: LOCAL Group Policy: grppol IP Address Pool: newpo SSL VPN Client Location: disk0;	nnection with following attributes: PN Client le licy pol /ssiclient-win-1.1.4.179.pkg	
4.	й		

De configuratie die in ASDM wordt getoond, heeft voornamelijk betrekking op de SSL VPN client Wizard-configuratie.

In de CLI kan je wat extra configuratie observeren. De volledige CLI-configuratie wordt hieronder weergegeven en belangrijke opdrachten zijn gemarkeerd.

```
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
interface Ethernet0/4
shutdown
no nameif
no security-level
no ip address
1
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#
```

Verifiëren

De opdrachten in deze sectie kunnen worden gebruikt om deze configuratie te controleren.

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.
- Laat VPN-sessiondb svc-displays de informatie over de huidige SSL-verbindingen zien.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- <u>Cisco 5500 Series adaptieve security applicatie</u>
- PIX/ASA en VPN-client voor publiek internet VPN op een tick Configuration-voorbeeld
- <u>SSL VPN-client (SVC) op ASA met ASDM Configuratievoorbeeld</u>
- <u>Technische ondersteuning en documentatie Cisco Systems</u>