# ASA 8.X: 터널링된 기본 게이트웨이 구성을 통해 SSL VPN 트래픽 라우팅 예

### 목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 표기 규칙 배경 정보 구성 네트워크 다이어그램 ASDM 6.1(5)을 사용하는 ASA 컨피그레이션 다음을 확인합니다. 문제 해결 관련 정보

### <u>소개</u>

이 문서에서는 터널링된 기본 게이트웨이(TDG)를 통해 SSL VPN 트래픽을 라우팅하도록 ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다. tunneled 옵션을 사용하여 기본 경로를 생성하면 학습된 경로 또는 고정 경로를 사용하여 라우팅할 수 없는 ASA에서 종료되 는 터널의 모든 트래픽이 이 경로로 전송됩니다. 터널에서 발생하는 트래픽의 경우 이 경로는 다른 구성 또는 학습된 기본 경로를 재정의합니다.

# <u>사전 요구 사항</u>

#### <u>요구 사항</u>

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 버전 8.x에서 실행되는 ASA
- Cisco SSL VPN Client(SVC) 1.x**참고:** <u>Cisco 소프트웨어 다운로드(등록된</u> 고객만 해당)에서 SSL VPN 클라이언트 패키지(sslclient-win\*.pkg)를 다운로드합니다. ASA의 플래시 메모리에 SVC를 복사합니다. ASA와의 SSL VPN 연결을 설정하려면 SVC를 원격 사용자 컴퓨터로 다운 로드해야 합니다.

#### <u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.x를 실행하는 Cisco 5500 Series ASA
- Windows 1.1.4.179용 Cisco SSL VPN Client 버전
- Windows 2000 Professional 또는 Windows XP를 실행하는 PC
- Cisco ASDM(Adaptive Security Device Manager) 버전 6.1(5)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

#### <u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 규칙</u>을 참조하십시오.

### <u>배경 정보</u>

SVC(SSL VPN Client)는 원격 사용자에게 IPSec VPN 클라이언트를 설치 및 구성할 필요 없이 IPSec VPN 클라이언트의 이점을 제공하는 VPN 터널링 기술입니다. SVC는 원격 컴퓨터에 이미 있 는 SSL 암호화와 보안 어플라이언스의 WebVPN 로그인 및 인증을 사용합니다.

현재 시나리오에서는 SSL VPN 터널을 통해 ASA 뒤의 내부 리소스에 연결하는 SSL VPN 클라이언 트가 있습니다. 스플릿 터널이 활성화되지 않았습니다. SSL VPN 클라이언트가 ASA에 연결되면 모 든 데이터가 터널링됩니다. 내부 리소스에 액세스하는 것 외에도, 주요 기준은 이 터널링된 트래픽 을 DTG(Default Tunneled Gateway)를 통해 라우팅하는 것입니다.

표준 기본 경로와 함께 터널링된 트래픽에 대해 별도의 기본 경로를 정의할 수 있습니다. 고정 경로 또는 학습된 경로가 없는 ASA에서 수신한 암호화되지 않은 트래픽은 표준 기본 경로를 통해 라우 팅됩니다. 고정 경로 또는 학습 경로가 없는 ASA에서 수신한 암호화된 트래픽은 터널링된 기본 경 로를 통해 정의된 DTG로 전달됩니다.

터널링된 기본 경로를 정의하려면 다음 명령을 사용합니다.

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

### <u>구성</u>

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** <u>명령 조회 도구(등록된</u> 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

#### <u>네트워크 다이어그램</u>

이 문서에서는 다음 네트워크 설정을 사용합니다.



이 예에서 SSL VPN 클라이언트는 터널을 통해 ASA의 내부 네트워크에 액세스합니다. 내부 네트워 크 이외의 목적지를 위한 트래픽도 터널링됩니다. 스플릿 터널이 구성되지 않고 TDG(192.168.100.20)을 통해 라우팅되기 때문입니다.

패킷이 라우터 2인 TDG로 라우팅되면 주소 변환을 수행하여 해당 패킷을 인터넷에 미리 라우팅합 니다. 라우터를 인터넷 게이트웨이로 구성하는 방법에 대한 자세한 내용은 <u>Cisco 이외의 케이블 모</u> <u>뎀 뒤에 Cisco 라우터를 구성하는 방법을 참조하십시오</u>.

#### ASDM 6.1(5)을 사용하는 ASA 컨피그레이션

이 문서에서는 인터페이스 컨피그레이션과 같은 기본 컨피그레이션이 완료되었으며 제대로 작동한 다고 가정합니다.

**참고:** ASDM에서 ASA를 <u>구성하는</u> 방법에 대한 자세한 내용은 ASDM에 대한 HTTPS 액세스 허용 을 참조하십시오.

**참고:** 포트 번호를 변경하지 않으면 동일한 ASA 인터페이스에서 WebVPN 및 ASDM을 활성화할 수 없습니다. 자세한 내용은 <u>ASA의 동일한 인터페이스에서 ASDM 및 WebVPN 활성화</u>를 참조하십 시오.

SSL VPN 마법사를 사용하여 SSL VPN을 구성하려면 다음 단계를 완료합니다.

ile View Tools V	zards Window Help
Home Cor Home Device	Startup Wizard     I Startup Wizard       IPsec VPN Wizard     Back Fernand Provided Provi
General Lice	Packet Capture Wizard

1. Wizards(마법사) 메뉴에서 SSL VPN Wizard(SSL VPN 마법사)를 선택합니다

2. Cisco SSL VPN Client(Cisco SSL VPN 클라이언트) 확인란을 클릭하고 Next(다음)를 클릭합 니다



3. Connection Name(연결 이름) 필드에 연결 이름을 입력한 다음 SSL VPN Interface(SSL VPN 인터페이스) 드롭다운 목록에서 사용자가 SSL VPN에 액세스하는 데 사용할 인터페이스를 선 택합니다

🖆 SSL VPN Wizard	
SSL VPN Wizard	SSL VPN 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: Oligital Certificate When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA. Certificate: None
- Alle	Connection Group Settings 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
£	Sack Next > Fish Cancel Help

- 4. Next(**다음)를 클릭합니다**.
- 5. 인증 모드를 선택하고 Next(**다음**)를 클릭합니다. (이 예에서는 로컬 인증을 사용합니다 .)

🖆 SSL VPN Wizard		×
SSL VPN Wizard	User Authentication (Step 3 of 6)	
SSL VPN WIZARD	The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login. Authenticate using a AAA server group AAA Server Group Name: Authenticate using the local user database User to be Added Usersname: Cisco Password: Delete Confirm Password: Delete	
	Sack Next > Einish Cancel Help	

6. 기존 기본 그룹 정책 이외의 새 그룹 정책을 생성합니다

CCL VDN Wizard	Group Policy (Step 4 of 6)			
SSE VPN Wizard	A group policy is a collection of user- policy, all users are members of the default group policy lets users inheri policy or username level.	oriented attribute/v default group policy t attributes that you	alue pairs. Unless assigned to a specif (DfltGrpPolicy). Therefore, configurin have not configured at the individual	fic group g the group
610	O Create new group policy	grppolicy	$\supset$	
	Modify existing group policy	DRGrpPolicy		
		Sack	Next > Brish Cancel	Help

7. SSL VPN 클라이언트 PC가 연결되면 SSL VPN 클라이언트 PC에 할당할 새 주소 풀을 생성 합니다



8. SSL VPN 클라이언트 이미지를 선택하고 ASA의 플래시 메모리에 업로드하려면 Browse를 클

#### 릭합니다

.

🖆 SSL VPN Wizard					
SSL VPN Wizard	IP Address Pools and	Client Image - Any	Connect VPN C	ient Connections	Only (Step 5 of 6)
	The security appliance client self-instals, use to resources on a corp IP Address Pool Create a new addre from the pool when	e downloads the AnyCo s SSL or DTLS encrypti porate network. The re ess pool or select an ex they connect.	onnect VPN Client on for the duratio mote PC becomes isting address poo	to remote users wh n of the connection part of the corpor ol. Remote PCs are	en they connect. The n, and allows full access ate network. assigned addresses
and the second	IP Address Pool:	newpool	× (	New	
	Address Pool Range	: 192.168.10.40 - 1	92.168.10.50		
	AnyConnect VPN Clier	t Image Location			
Territe	Identify a file in fla: the file and loads it	h memory as an AnyO into cache memory for	onnect VPN Client downloading to re	image. The securit	y appliance expands
	Location: Download latest Ar	wConnect VPN Client f	rom Cisco.com	Browse	
			<u>≤</u> Back	ext > Einish	Cancel Help

9. 시스템**의** 로컬 디렉토리에서 파일 경로를 설정하려면 Upload를 클릭합니다

📬 Add SSL VPN C	lient Image			
AnyConnect Image:				Browse Flash
				Upload
	ОК	Cancel	Help	1
3.				J

10. sslclient.pkg 파일이 있는 디렉토리를 선택하려면 Browse Local Files를 클릭합니다

储 Upload Image	
Upload a file from local c few minutes. Please wai	omputer to flash file system on the device. The upload process might take a t for the operation to finish.
Local File Path:	Browse Local Files
Flash File System Path:	Browse Flash
	Upload File Close Help

11. 선택한 파일을 ASA 플래시에 업로드하려면 Upload File을 클릭합니다

.

•

🕵 Upload I	mage 🛛 🛛
Upload a file few minutes.	from local computer to flash file system on the device. The upload process might take a Please wait for the operation to finish.
Local File Pat	h: C:\Documents and Settings\jtammera\My Documi Browse Local Files
Flash File Sy:	tem Path: disk0:/sslclient-win-1.1.4.179.pkg Browse Flash
15	Upload File Close Help
🔂 Status	
	Please wait while ASDM is uploading the file. The upload process may take a few minutes.
🖆 Informa	tion 🛛 🕅
4	File has been uploaded to flash successfully.
	ок
파일이 ASA의	│플래시에 업로드되면 OK를 클릭하여 해당 작업을 완료합니다

🖆 Add SSL VPN C	lient Image	
AnyConnect Image:	disk0:/sslclient-win-1.1.4.179.pkg	Browse Flash
		Upload
	OK Cancel Help	

13. 이제 ASA의 플래시에 업로드된 최신 anyconnect pkg 파일이 표시됩니다. Next(**다음)를 클릭** 

#### 합니다

.

🖆 SSL VPN Wizard					
SSL VPN Wizard	<b>IP Address Pools and</b>	Client Image - Any	Connect VPN Cl	ient Connecti	ons Only (Step 5 of 6)
	The security appliance client self-instals, use to resources on a corp IP Address Pool Create a new addre from the pool when	e downloads the AnyCo s SSL or DTLS encrypti porate network. The re ess pool or select an ex- they connect.	rnect VPN Client i on for the duratio mote PC becomes sting address poo	to remote users n of the connec part of the cor ol. Remote PCs	s when they connect. The tion, and allows full access porate network. are assigned addresses
	IP Address Pool:	newpool	¥ [	New	
	Address Pool Range	: 192.168.10.40 - 1	92.168.10.50		·
	AnyConnect VPN Clier	t Image Location			
cinta in	Identify a file in flas the file and loads it	sh memory as an AnyCo Into cache memory for	nnect VPN Client downloading to re	image. The sec smote users.	urity appliance expands
-It	Location:	disk0:/sslclient-win-	.1.4.179.pkg	Browse	
	Download latest Ar	wConnect VPN Client fr	om Cisco.com		
	<u>8</u>		≤ Back (	ext > DEnio	Gancel Help

14. SSL VPN 클라이언트 컨피그레이션의 요약이 표시됩니다. **마침**을 클릭하여 마법사를 완료 합니다

	I construction of the second second		
SSL VPN Wizard	Summary (Step 6 of	6)	
	You have created a SS Selected Features: Connection Name: SSL VPN Interface: User Authentication: Group Policy: IP Address Pool: SSL VPN Client Locatio	SL VPN connection with following attributes: SSL VPN Client Test outside LOCAL grppolicy newpool m:disk0:/sslclient-win-1.1.4.179.pkg	
		Seck Next > (Firsh) Cancel H	de

ASDM에 표시된 컨피그레이션은 주로 SSL VPN 클라이언트 마법사 컨피그레이션과 관련이 있습니다.

CLI에서 몇 가지 추가 컨피그레이션을 관찰할 수 있습니다. 전체 CLI 컨피그레이션이 아래에 표시 되고 중요한 명령이 강조 표시됩니다.

ciscoasa
ciscoasa# <b>show running-config</b>
: Saved
:
ASA Version 8.0(4)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 209.165.201.2 255.255.255.224
interface Ethernet0/1
namelf inside
security-level 100
1p address 192.168.100.2 255.255.255.0
!
interiace Ethernetu/2
nameli manage
security-ievel U
Th address In.1.1.1 522.522.5220

```
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#
```

# <u>다음을 확인합니다.</u>

이 섹션에 제공된 명령을 사용하여 이 컨피그레이션을 확인할 수 있습니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 show 명령을 지원합니다. OIT를 사용하여 show 명령 출력의 분석을 봅니다.

- show webvpn svc ASA 플래시 메모리에 저장된 SVC 이미지를 표시합니다.
- show VPN-sessiondb svc 현재 SSL 연결에 대한 정보를 표시합니다.

### <u>문제 해결</u>

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

# <u>관련 정보</u>

- <u>Cisco 5500 Series Adaptive Security Appliance 지원</u>
- <u>스틱 컨피그레이션의 공용 인터넷 VPN용 PIX/ASA 및 VPN 클라이언트 예</u>
- ASA의 SVC(SSL VPN Client) with ASDM 컨피그레이션 예
- <u>기술 지원 및 문서 Cisco Systems</u>