# ASA 8.x: ASA 컨피그레이션의 AnyConnect VPN 클라이언트에 대해 스플릿 터널링 허용 예

### 목차

소개 <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>표기 규칙</u> <u>배경 정보</u> 구성 <u>네트워크 다이어그램</u> <u>ASDM 6.0(2)을 사용하는 ASA 컨피그레이션</u> <u>ASA CLI 컨피그레이션</u> <u>SVC와 SSL VPN 연결 설정</u> <u>다음을 확인합니다.</u> <u>문제 해결</u> <u>관련 정보</u>

### <u>소개</u>

이 문서에서는 Cisco AnyConnect VPN 클라이언트가 Cisco ASA(Adaptive Security Appliance) 8.0.2으로 터널링되는 동안 인터넷에 액세스할 수 있도록 허용하는 방법에 대한 단계별 지침을 제공 합니다. 이 구성을 통해 클라이언트는 스플릿 터널링을 사용하여 인터넷에 비보안 액세스를 제공하 는 동시에 SSL을 통해 기업 리소스에 안전하게 액세스할 수 있습니다.

### <u>사전 요구 사항</u>

#### <u>요구 사항</u>

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- ASA Security Appliance는 버전 8.x를 실행해야 함
- Cisco AnyConnect VPN Client 2.x**참고:** Cisco <u>소프트웨어 다운로드(등록된</u> 고객만 해당)에서 AnyConnect VPN 클라이언트 패키지(anyconnect-win\*.pkg)를 다운로드합니다. ASA와의 SSL VPN 연결을 설정하기 위해 원격 사용자 컴퓨터에 다운로드될 ASA의 플래시 메모리에 AnyConnect VPN 클라이언트를 복사합니다. 자세한 <u>내용은</u> ASA 컨피그레이션 가이드<u>의</u> AnyConnect 클라이언트 설치 섹션을 참조하십시오.

#### <u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.0(2)을 실행하는 Cisco 5500 Series ASA
- Windows 2.0.0343용 Cisco AnyConnect SSL VPN Client 버전
- Microsoft Visa, Windows XP SP2 또는 Windows 2000 Professional SP4(Microsoft Installer 버 전 3.1 포함)를 실행하는 PC
- Cisco ASDM(Adaptive Security Device Manager) 버전 6.0(2)

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>

Cisco AnyConnect VPN Client는 원격 사용자를 위해 보안 어플라이언스에 보안 SSL 연결을 제공 합니다. 이전에 설치된 클라이언트가 없는 경우 원격 사용자는 SSL VPN 연결을 허용하도록 구성된 인터페이스의 브라우저에 IP 주소를 입력합니다. 보안 어플라이언스가 http:// 요청을 https://으로 리 디렉션하도록 구성되어 있지 않은 경우 사용자는 https://<address> 형식으로 URL을 입력해야 합니 다.

URL을 입력하면 브라우저가 해당 인터페이스에 연결되고 로그인 화면이 표시됩니다. 사용자가 로 그인 및 인증을 충족하고 보안 어플라이언스가 사용자가 클라이언트를 필요로 한다고 식별하면 원 격 컴퓨터의 운영 체제와 일치하는 클라이언트를 다운로드합니다. 다운로드 후 클라이언트는 자신 을 설치 및 구성하고, 보안 SSL 연결을 설정하며, 연결이 종료되면 (보안 어플라이언스 구성에 따라 ) 그대로 유지하거나 제거합니다.

이전에 설치된 클라이언트의 경우 사용자가 인증하면 보안 어플라이언스는 클라이언트의 수정 버 전을 검사하고 필요에 따라 클라이언트를 업그레이드합니다.

클라이언트가 보안 어플라이언스와 SSL VPN 연결을 협상할 때 TLS(Transport Layer Security) 및 선택적으로 DTLS(Datagram Transport Layer Security)를 사용하여 연결합니다. DTLS는 일부 SSL 연결과 관련된 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성 능을 향상시킵니다.

AnyConnect 클라이언트는 보안 어플라이언스에서 다운로드하거나 시스템 관리자가 원격 PC에 수 동으로 설치할 수 있습니다. 클라이언트를 수동으로 설치하는 방법에 대한 자세한 내용은 <u>Cisco</u> AnyConnect VPN 클라이언트 관리자 설명서를 참조하십시오.

보안 어플라이언스는 연결을 설정하는 사용자의 그룹 정책 또는 사용자 이름 특성에 따라 클라이언 트를 다운로드합니다. 클라이언트를 자동으로 다운로드하도록 보안 어플라이언스를 구성하거나, 원격 사용자에게 클라이언트 다운로드 여부를 묻는 메시지를 표시하도록 구성할 수 있습니다. 후자 의 경우 사용자가 응답하지 않을 경우 시간 초과 기간 후에 클라이언트를 다운로드하거나 로그인 페이지를 표시하도록 보안 어플라이언스를 구성할 수 있습니다.

### <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.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



**참고:** 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 이는 <u>실</u> <u>습</u> 환경에서 사용된 RFC <u>1918</u> 주소입니다.

#### ASDM 6.0(2)을 사용하는 ASA 컨피그레이션

이 문서에서는 인터페이스 컨피그레이션과 같은 기본 컨피그레이션이 이미 만들어졌으며 제대로 작동한다고 가정합니다.

**참고:** ASDM에서 ASA를 <u>구성할 수 있도록</u> 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조 하십시오.

**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.

스플릿 터널링을 사용하여 ASA에서 SSL VPN을 구성하려면 다음 단계를 완료합니다.

1. IP 주소 **풀 vpnpool을** 생성하려면 Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add를 선택합니다

🔂 Add IP Pool	
Name:	vpnpool
Starting IP Address:	192.168.10.1
Ending IP Address:	192.168.10.254
Subnet Mask:	255.255.255.0
ок	Cancel Help
Starting IP Address: Ending IP Address: Subnet Mask: OK	192.168.10.1       192.168.10.254       255.255.255.0       Cancel       Help

- 2. Apply를 클릭합니다.동일한 CLI 구성:
- 3. WebVPN을 활성화합니다.Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > SSL VPN Connection Profiles(SSL VPN 연결 프로파일)를 선택하고 Access Interfaces(액세스 인터페이스)에서 Allow Access(액세스 허용) 및 Enable DTLS for the outside interface(외부 인터페이스에 대해 DTLS 활성화)를 클릭합니다. 또한 외부 인터페이스에서 SSL VPN을 활성화하려면 Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interface(아래 표에서 선택한 인터페이 스에서 Cisco AnyConnect VPN 클라이언트 또는 레거시 SSL VPN 클라이언트 액세스 활성화 ) 확인란을 선택합니다

configuration / Remote Recease and / Recease and Recease and Recease and Recease and Recease and Recease and Re	LESS / JOE VEN CONNECTION FLORIES
---	-----------------------------------

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at <u>Client Settings</u>

A	Access Interfaces								
	🔽 Enable Cisco Any	Connect VPN Client or le	egacy SSL VPN Client access on the i	nterfaces selected in the					
	Interface	Allow Access	Require Client Certificate	Enable DTLS					
(	outside								
	inside								
(	Access Port: 443 DTLS Port: 443								
	Click here to Assign	Certificate to Interface.							

Apply를 클릭합니다.Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > SSL VPN > Client Settings(클라이언트 설정) > Add(추가)를 선택하여 ASA의 플래시 메모리에서 Cisco AnyConnect VPN 클라이언트 이미지를 추가합니다

🕵 Add SSL VPN Client Ir	mage	X SSL VPN > Clie	nt Settings
Flash SVC Image:	Browse Flash	2	
	Upload	buntered operation	on system to the top of the
OK	Cancel Help		
薩 Browse Flash			×
Folders	Files		
⊟– 🥏 disk0:	FileName 🔬	Size (bytes)	Date Modified
🔁 🔁 log	crypto_archive		07/24/07 05:21:48
🗄 🔁 crypto_archi	ve 🔁 log		07/24/07 05:21:36
	asdm-603.bin	6,851,212	01/04/08 18:07:02
	asa803-k8.bin	14,635,008	01/04/08 17:49:50
	admin.cfg	1,220	09/20/07 09:51:38
	anyconnect-win-2.0.03	2,635,734	08/13/07 04:14:50
	asdm-602.bin	6,889,764	01/03/08 21:38:26
	asa722-k8.bin	8,312,832	02/13/07 04:16:30
	asdm-522.bin	5,623,108	02/12/07 05:53:48
	asa802-k8.bin	14,524,416	01/03/08 21:24:42
	old_running.cfg	1,841	09/20/07 09:51:38
	sslclient-win-1.1.4.179	418,765	03/14/08 13:47:58
File N	Jame: anyconnect-win-2.0.0343-k9.pl		
		9	-
J.	Add SSL VPN Client Image		1
F	ilash SVC Image: ct-win-2.0.0343	-k9.pkg Browse	Flash
		Uplo	pad
	OK Cance	Help	
확인을 클릭합니다. )를 클릭합니다			Add(추가

Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings
Identify SSL VPN Client (SVC) related files.
SSL VPN Client Images
Minimize connection setup time by moving the image used by the most commonly encountered operation system to t
🕈 Add 📝 Replace 前 Delete 🛧 Move UP 🗲 Move Down
disk0:/anyconnect-win-2.0.0343-k9.pkg

#### 동일한 CLI 구성:

4. 그룹 정책을 구성합니다.내부 그룹 정책 **클라이언트 그룹을** 생성하려면 Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액 세스) > Group Policies(그룹 정책)를 선택합니다. WebVPN을 터널링 프로토콜로 활성화하려 면 General(일반) 탭에서 SSL VPN Client(SSL VPN 클라이언트) 확인란을 선택합니다

I	Add Internal Group Policy	
	General	Name: Clientgroup
	-Advanced	Banner: 🔽 Inherit
		Address Pools: 🔽 Inherit
		More Options
		Tunneling Protocols: 📃 Inherit 🔲 Clientless SSL VPN 🛛 🔽 SSL VPN Client 🗍 IPsec

Advanced(**고급) > Split Tunneling(스플릿 터널링**) 탭에서 Split Tunnel Policy(터널 정책 분할 )에 **Inherit(상속**) 확인란의 선택을 취소하고 드롭다운 목록에서 Tunnel Network List Below(아 래 터널 네트워크 목록)를 선택합니다



Split Tunnel **Network List(터널 네트워크 목록** 분할)에 대한 Inherit(상속) 확인란을 선택 취소 한 다음 **Manage(관리**)를 클릭하여 ACL Manager를 시작합니다

General Servers	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do n require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL behavior of the decision of the security appliance makes split tunneling decisions on the basis of a network list, which is an
- Advanced	ACL that consists or list of addresses on the private network.
Split Tunneling	
IE Browser Proxy	DNS Names: 🔽 Inherit
SSL VPN Client	
E IPsec Client	Policy: Inherit Tunnel Network List Below
Client Access Rule	Network List: Topare
Client Access Rule	Network List: Inherit None
Hardware Cleat	

ACL Manager(ACL 관리자)에서 **Add(추가) > Add ACL...을** 선택하여 새 액세스 목록을 생성합 니다

🎼 ACL Manager					
Standard ACL Extended	ACL				
🔂 Add 🔻 📝 Edit 📋	Delete 🛧 🗲	3 B B	*		
🔂 Add ACL	dress	Action		Description	
Add ACL Add ACL	dress	Action		Description	
Add ACL Add ACE Add ACE	dress	Action		Description	

#### ACL의 이름을 입력하고 OK를 **클릭합니다**

<b>1</b>	ACL Manag	jer				
	Standard A	CL Extend	ded ACL			
	🔂 Add 🚽	📑 Edit	📋 Delete 🛉 🛧 🕤	€   % <b>™ ®</b>	*	
	No		Address	Action		Description
	🔂 Add A	CL			×	
	Add A	CL me: split-tu	unnel		×	

ACL 이름이 생성되면 Add > Add ACE를 선택하여 ACE(Access Control Entry)를 추가합니다 .ASA 뒤의 LAN에 해당하는 ACE를 정의합니다. 이 경우 네트워크는 10.77.241.128/26이고 Permit을 Action으로 선택합니다.ACL Manager를 종료하려면 OK를 클릭합니다

No	Address	Action	Descriptio	n
split-tunnel				
Add ACE				
Action				
Action:	🖌 Permit 🔄			
Host/Netwo	ork			
IP Addres	ss: 10.77.241.128			<b>~</b>
Netmask:	255.255.255.192			-
Description:				
Description.				

방금 생성한 ACL이 스플릿 터널 네트워크 목록에 대해 선택되었는지 확인합니다. 그룹 정책 컨피그레이션으로 돌아가려면 **OK**(확인)를 클릭합니다

ø	Add Internal Group Policy									×
	General Servers -Advanced -IE Browser Proxy -SSL VPN Client -IPsec Client	Split tunnelin; require tunne ACL that con DNS Names: Policy:	ing. The sect sists of list of Inherit	s distinguish netv urity appliance m addresses on th Tunnel Netwo	works that req nakes split turn ne private netw rk List Below	uire traffic to g neling decisions vork.	to through the tur on the basis of a	nel and the network lis	ose that do noi t, which is an	t
		Network List:	🕅 Inherit	split-tunnel					Manage	
		Intercept	DHCP Confi	guration Mess	age from Mi	icosoft Client	5		*	

기본 페이지에서 Apply를 클릭한 다음 Send(필요 시)를 클릭하여 명령을 ASA로 전송합니다 .그룹 정책 모드에서 SSL VPN 설정을 구성합니다.Keep Installer on Client System(클라이언 트 시스템에서 설치 프로그램 유지) 옵션에서 Inherit(상속) 확인란의 선택을 취소하고 Yes(예) 라디오 버튼을 클릭합니다.이 작업을 수행하면 SVC 소프트웨어가 클라이언트 시스템에 남아 있게 됩니다. 따라서 연결이 이루어질 때마다 SVC 소프트웨어를 클라이언트에 다운로드할 필 요가 없습니다. 이 옵션은 기업 네트워크에 자주 액세스하는 원격 사용자에게 적합합니다

2	Edic Incernal Group Policy	/: cilencgroup			
	General	Koop Tostallar op Cliept Sustemu	- Inhorit	@ ¥23	C No.
	-Servers	(Keep Installer on Client System:	j Innenc	( Tes	O NO
	-Advanced	Compression:	🔽 Inherit	C Enable	C Disab
	-Split Tunneling - IE Browser Proxy	Datagram TLS:	🔽 Inherit	C Enable	C Disab
	SSL VPN Client	Keepalive Messages:	🔽 Inherit	🗖 Disable	Interval:

Login Setting(로그인 설정)을 클릭하여 표시된 대로 Post Login Setting(사후 로그인 설정) 및 Default Post Login Selection(기본 사후 로그인 선택)을 설정합니다

General	<ul> <li>After successfully logging in, user can have the choice to download the client software, or g participants. The following estimate desides what will be page.</li> </ul>
-Servers	portal page. The following settings decides what will happen.
-Advanced	🔲 Inherit
—Split Tunneling	
—IE Browser Proxy	Post Login Setting
Login Setting	Do not prompt user to choose
Key Regeneration	
—Dead Peer Detecti	
Customization	User has seconds to choose, or Default Post Login Selection below is take
i — IPsec Client	
	Default Post Login Selection
	C Go to Clientless SSL VPN portal
	Download SSL VPN Client
	General Servers Advanced JE Browser Proxy Solit Tunneling JE Browser Proxy SE VPN Client Cogin Setting Key Regeneration Dead Peer Detecti Customization +IPsec Client

Renegotiation Interval(재협상 간격) 옵션에서 Inherit(상속) 상자의 **선택을** 취소하고 Unlimited(무제한) 확인란의 선택을 취소하고 다시 키를 누를 때까지 분 수를 입력합니다.키가 유효한 시간에 대한 제한을 설정하여 보안이 강화됩니다.Renegotiation Method(재협상 방법) 옵션에서 Inherit(상속) 확인란의 선택을 취소하고 **SSL** 라디오 버튼을 클릭합니다.재협상에서 는 재협상용으로 명시적으로 생성된 현재 SSL 터널 또는 새 터널을 사용할 수 있습니다

General	Renegotiation Interval:	🔲 Inherit	🔲 Unlimited	30	minutes
-Servers -Advanced	Renegotiation Method:	🔲 Inherit	O None	⊙ SSL	C New Tunnel
-Split Tunneling					
IE Browser Proxy					
Login Setting Key Regeneration	)				
OK( <b>확인)</b> 를 클릭한 다음 Apply(적용)를 <b>클릭합니다</b>					

Ca	nfiguration > Remote Access VPN >	> Net	work (Client) Access	Group Policies		
	Manage VPN group policies. A VPN grou externally on a RADIUS/LDAP server. T	p poli he gr	cy is a collection of user-c oup policy information is r	priented attribute/val eferenced by VPN tu	ue pairs that may be sto nnel groups and user acc	red inter counts.
	🛧 Add 🝷 🗹 Edit 📋 Delete					
	Name		Туре	Tunnel	ng Protocol	
- (	clientgroup	)	Internal	svc		N/A -
	DfltGrpPolicy (System Default)		Internal	L2TP-IPSec, IPSec, w	ebvpn	N/A -

동일한 CLI 구성:

5. 새 사용자 계정 ssluser**1을** 생성하려면 **구성 > 원격 액세스 VPN > AAA 설정 > 로컬 사용자 > 추가**를 선택합니다. 확인을 클릭한 다음 **적용**을 **클릭합니다** 

🔄 Add User Account	
Identity -VPN Policy	Username: ssluser1
	Password: ******
	Confirm Password: ******
	User authenticated using MSCHAP
	Member-of
	Member-of: Add >> Delete
	Access Restriction
	Select one of the options below to restrict ASUM, SSH, Teinet and Console access. Note: All users have betwork access, regardless of these settings
	Eull access(ASDM_SSH_Telpet and Console)
	Drivilege level is used with compand authorization
	Privilege Level: 2
	C CLUppin prompt for SSH. Telpet and console (no ASDM access)
	This setting is effective only if 0.0.0 authenticate console command is configured
	C No ASDM SSH. Tablet or Copcole access
	This setting is effective only if AAA authenticate console command is configured.

#### 동일한 CLI 구성:

.

6. Enable Local User Lockout(로컬 사용자 잠금 활성화) 확인란을 선택하여 기본 서버 그룹 LOCAL을 수정하려면 Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > AAA Setup(AAA 설정) > AAA Servers Groups(AAA 서버 그룹) > Edit(수정)를 16으로 선택 합니다

Co	Configuration > Remote Access VPN > AAA Setup > AAA Server Groups					
AP	AA Server Groups —					
	Server Group	Protocol	Accounting Mode	Reactivation Mode		
	LOCAL	LOCAL				
	🕵 Edit LOCA	L Server Group			×	
	This feature allows you to specify the maximum number of failed attempts to allow before locking out and denying access to the user. This limit is applicable only when the local database is used for authentication.		v			
	Enable Local User Lockout					
	Maximun	Attempts: 16				
	•	ОК	Cancel	Help		

- 7. OK(**확인)**를 클릭한 다음 Apply(적용)를 **클릭합니다.동일한 CLI 구성**:
- 8. 터널 그룹을 구성합니다.새 터널 그룹 sslgroup을 생성하려면 Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > SSL VPN Connection Profiles(SSL VPN 연결 프로파일) Connection Profiles(연결 프로파일) > Add(추가)를 선택합니다.Basic(기본) 탭에서 다음과 같이 구성 목록을 수행할 수 있습니다 .터널 그룹의 이름을 sslgroup으로 지정합니다.Client Address Assignment(클라이언트 주소 할당)의 드롭다운 목록에서 주소 풀 vpnpool을 선택합니다.Default Group Policy(기본 그룹 정 책)의 드롭다운 목록에서 그룹 정책 클라이언트 그룹을 선택합니다

Ī	Add SSL VPN Connection	Profile		
	- Basic) ⊕-Advanced	Name:	ssigroup	
		Authentication —		
		Method:	AAA C Certificate C Both	
		AAA Server Group:	LOCAL	Manag
			Use LOCAL if Server Group fails	
		Client Address Assign	nent	
		DHCP Servers:		
		Client Address Pools:	vpnpool	Select
		Default Group Policy		
		Group Policy:	clientgroup	Manag
		SSL VPN Client Protoco	l: 🔽 Enabled	
		OK	Cancel Help	

SSL VPN > Connection Aliases 탭에서 그룹 별칭 이름을 sslgroup\_users로 지정하고 OK를 클릭합니다

🚰 Add SSL VPN Connection Profile	
Basic Advanced General Client Addressing Authentication Authorization Accounting SSL VPN SSL VPN G Connection Aliases Add Connection Alias Alias: [sslgroup_users] Connection Aliases Connection Alias Connection Alias	
이번     이번       )를 클릭한 다음 Apply(적용)를 클릭합니다.동일한 CLI 구성:     이번       9. NAT를 구성합니다.Configuration > Firewall > NAT Rules > Add Dynamic NAT Rule을	<( <b>확인</b> 선택하
Add Dynamic NAT Rule	
Interface: inside  Source: any	
Translated Select a global pool for dynamic translation.	İ.
Deal ID Television Addresses Deal	

	Pool ID	Interface	Addresses Pool	
	0	(outbound)	Same as original address (identity)	
	<del>_0</del>	(inbound)	<del>Same as origin</del> a <mark>,</mark> address (identity)	
	1	outside	🖳 172.16.1.5 화이	으
- 1				:2

#### 클릭합니다.확인을 클릭합니다

Configuration > Firewall > NAT Rules						
dd	🝷 📝 Edit   🃋 De	lete 🛧 🗲 👗	🖻 🛍 🗉 🔍 Q	Find 🔛 Diag	gram 🛛 🥰 Packet Ti	race
Turce			Original			
	туре	Source	Destination	Service	Interface	
🖂 inside (1 Dynamic rules)						
	🙀 Dynamic	🌍 any			outside	
	JULA dd ;ide (	Iuration > Firewall > NA dd • 2 Edit 1 De Type ide (1 Dynamic rules)	dd ▼ 2 Edit 1 Delete + ↓ ↓ Type Source ide (1 Dynamic rules) 1 Dynamic @ any	uration > Firewall > NAT Rules         dd       ✓       ☑       Edit       Î       Delete       I       I       I       Q         Image: Type       Image: Type       Image: Original       Image: Original	uration > Firewall > NAT Rules         dd       ✓       ☑       Edit       Î       Delete       I       I       I       Q       Find       Image: Diagonal         Type       Image: Diagonal       Image:	uration > Firewall > NAT Rules         dd ▼ I Colspan       Q Find Provide Diagram I Packet T         dd       Type       Original       Original       Interface         Type       Source       Destination       Service       Interface         ide (1 Dynamic rules)       Interface       Interface       Interface

Apply를 클릭합니다.동일한 CLI 구성:

10. 내부 네트워크에서 VPN 클라이언트로의 반환 트래픽에 대한 nat-exemption을 구성합니다. 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

#### <u>ASA CLI 컨피그레이션</u>

```
Cisco ASA 8.0(2)
ciscoasa(config)#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
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
!
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
!
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
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 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 burstsize 1 asdm image disk0:/asdm-602.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 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 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
<pre>! Enable WebVPN on the outside interface svc image</pre>
disk0:/anyconnect-win-2.0.0343-k9.pkg 1
I Assign an order to the AnyConnect SSL VPN Client
imago sug enable
<i>! Enable the security appliance to download SVC</i>
images to remote computers tunnel-group-list enable
I Enable the display of the tunnel-group list on the
Wohl/PN Login page group-poligy glientgroup internal
Webvin hegin page group poincy citencyroup incernar
<pre>! Create an internal group policy "clientgroup"</pre>
group-policy clientgroup attributes
vpn-tunnel-protocol svc
I Specify SSL as a permitted VPN tunneling protocol
anlit turnel neligy turnelgregified
spiit-tunnei-poilty tunneispetilled
split-tunnel-network-list value split-tunnel
<i>! Encrypt the traffic specified in the split tunnel</i>
ACL only webvpn
svc keen-installer installed
Sto hoop installer installed
! When the security appliance and the SVC perform a
rekey, they renegotiate ! the crypto keys and
initialization vectors, increasing the security of the
connection. svc rekey time 30
-
I Command that specifies the number of minutes from
command that specifies the number of minutes from
the start of the ! session until the rekey takes
place, from 1 to 10080 (1 week). svc rekey method ssl
<i>! Command that specifies that SSL renegotiation takes</i>
place during SVC rekey. svc ask none default svc
username ssluser1 password ZRhW85jZgEaVd5P, encrypted
less Croate a user account "selucer1" tunnel-group
ssigroup type remote-access
<pre>! Create a tunnel group "sslgroup" with type as</pre>
remote access tunnel-group sslgroup general-attributes
address-pool vpnpool
Accordiate the address need impress greated default
Associate the address poor vphpoor created deladit-
group-policy clientgroup
<pre>! Associate the group policy "clientgroup" created</pre>
tunnel-group sslgroup webvpn-attributes
group-alias sslgroup users enable
I Configure the group alian an galaroun waara recent
configure the group arras as ssigroup-users prompt
nostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end
ciscoasa(config)#

<u>SVC와 SSL VPN 연결 설정</u>

ASA와 SSL VPN 연결을 설정하려면 다음 단계를 완료하십시오.

1. 웹 브라우저에 표시된 형식으로 ASA WebVPN 인터페이스의 URL 또는 IP 주소를 입력합니다

h	https://url
ם - ב	또는 https:// <ip address="" asa="" interface="" of="" the="" webvpn=""></ip>
4	WebVPN Service - Microsoft Internet Explorer
	File Edit View Favorites Tools Help
	🚱 Back 🔹 🕥 🔹 🛃 🌮 Search 🤺 Favorites 🤣 🎯 🍓 🔜 🦓
	Address 🕘 https://172.16.1.1/+webvpn+/index.html
	Cisco Systems willingentillinge WebVPN Service
	Login
	Please enter your username and password.
	USERNAME:
	PASSWORD:
	GROUP: sslgroup_users
	Login Clear
 2. /	사용자 이름과 비밀번호를 입력합니다. 또한 드롭다운 목록에서 해당 그룹을 선택합니다
	Login
	Please enter your username and password.
	USERNAME: ssluser1
	PASSWORD: ••••••
	GROUP: sslgroup_users
	Login Clear 이 창은 SSL VPN 연

결이 설정되기 전에 나타납니다

Cisco	AnyConnect VPN Client
Please   -   -	der vait while the VPN connection is established. to Cancel
<ul> <li>Microsoft Java</li> <li>- Sun Java</li> <li>- Download</li> <li>- Connected</li> </ul>	Help Cancel

**참고:** SVC를 다운로드하려면 컴퓨터에 ActiveX 소프트웨어를 설치해야 합니다.연결이 설정되 면 이 창이 표시됩니다

.



3. 컴퓨터의 작업 표시줄에 나타나는 잠금을 클릭합니다

🗿 Cisco AnyCo	onnect VPN Client			
K Connection	) 🕕 Statistics 🔒 About			
	ahaha			
	CISCO			
Connect to:	172.16.1.1	*		
	Disconnect			
PN session establi	shed.		이 창이 나타나고 SS	SL 연결에 대
한 정보를 제공합니	니다. 예를 들어 <b>192.168.10.</b> 1	I은 ASA 등에	의해 할당된 IP입니[	<b>가</b>

Cisco AnyConnect VPN Client		<
🔌 Connection 📵 Statistics 릚 About		
cisco		
Tunnel State:	Connected	
Client Address: Server Address:	192.168.10.1 172.16.1.1	
Bytes Sent:	23461	
Bytes Received:	1111	
Time Connected:	00:04:51	
Details		
VPN session established.		이 창

VPN 클라이언트 버전 정보가 표시됩니다



# <u>다음을 확인합니다.</u>

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

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.
  - ciscoasa#**show webvpn svc** 1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1 CISCO STC win2k+ 2,0,0343 Mon 04/23/2007 4:16:34.63
  - 1 SSL VPN Client(s) installed
- show vpn-sessiondb svc 현재 SSL 연결에 대한 정보를 표시합니다. ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username : **ssluser1** 

Assigned IP	:	192.168.10.1	Public IP	:	192.168.1.1
Protocol	:	Clientless SSL-Tunnel	DTLS-Tunnel		
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 2	4 2008		
Duration	:	0h:12m:00s			
NAC Result	:	Unknown			
VLAN Mapping	:	N/A	VLAN	:	none
show webvpn group-alias - 다양한 그룹에 대해 구성된 별칭을 표시합니다.					
ciscoasa# <b>show webvpn group-alias</b>					

Tunnel Group: sslgroup Group Alias: sslgroup\_users enabled

• ASDM에서 현재 WebVPN 세션을 확인하려면 ASA에서 Monitoring > VPN > VPN Statistics > Sessions를 선택합니다

1	nitoring > VP	'N > VPN S	tatistio	s > Sessions	)				
-	essions								
Remote Site to Site		SSL VPN			E-mail Prove	VDN Load Palancin			
	Access		Clientless		With Client	Total	E-mail Proxy	VPIN LUGU Dalah Cir	' <sup>y</sup>
	0	0		0	0	0	0	0	
	Filter By: SSL	VPN Client		All Sessions			Fi	ter	
	Username IP Address		Group Policy Connection	Proto Encryp	icol ation	Login Time Duration		Byt Byt	
	ssluser1 clientgrou 192.168.10.1 sslgroup		roup Ip	Clientless SSL RC4 AES128	Tunnel DT	17:12:23 IST Mor 0h:03m:31s	Mar 24 2008	194118 192474	

### <u>문제 해결</u>

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

1. **vpn-sessiondb logoff name** *<username>*—특정 사용자 이름에 대한 SSL VPN 세션을 로그오 프하는 명령입니다.

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)

마찬가지로 vpn-sessiondb logoff svc 명령을 사용하여 모든 SVC 세션을 종료할 수 있습니다. 2. **참고:** PC가 대기 모드 또는 최대 절전 모드로 전환되면 SSL VPN 연결을 종료할 수 있습니다.

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, e tc) Called vpn\_remove\_uauth: success! webvpn\_svc\_np\_tear\_down: no ACL webvpn\_svc\_np\_tear\_down: no IPv6 ACL np\_svc\_destroy\_session(0xA000) ciscoasa#**show vpn-sessiondb svc** INFO: There are presently no active sessions

3. debug webvpn svc <1-255>—세션을 설정하기 위한 실시간 webvpn 이벤트를 제공합니다. Ciscoasa#debug webvpn svc 7

```
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 AnyConnect VPN Client 2, 0, 0343'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343
Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B
7D75F4EDEF26'
Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8
625B92C1338D631B08B7D75F4EDEF26'
Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B
08B7D75F4EDEF26'
WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7
5F4EDEF26'
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: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40
642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693 '
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AE
BAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693 '
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'
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
np_svc_create_session(0x3000, 0xD41611E8, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
```

```
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
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
```

.

4. ASDM에서 실시간 이벤트를 보려면 Monitoring > Logging > Real-time Log Viewer > View를 선택합니다

🚰 Cisco ASDM 6.0 for ASA - 10.77.241.142						
File	View Tools Wizards Window He	þ	Look For:			
G	Home 🦓 Configuration 🔯 Monitori	g 🔚 Save 🔇 Refresh 🔇 Back 🕥 Forward 🢡 Help				
	Logging 🗗 🕂 🕹	Monitoring > Logging > Real-Time Log Viewer				
evice List	Real-Time Log Viewer	Real-Time Log Viewer				
		Click the View button below to start displaying syslog messages in re desired logging level to see messages at that severity or higher.	eal time. Select the			
		Logging Level: Debugging				
		Buffer Limit: 1000				
		View				

이 예에서는 SSL 세션이 헤드 엔드 디바이스로 설정되었음을 보여줍니다

Real-	Time Log View	er - 10 77 2	241.142				
File To	Fie Topis Window Help						
0 Paus	III Pause   🖹 Copy 🎧 Save 🆓 Clear   📸 Color Settings   🜓 Create Rule 取 Show Rule   🕼 Show Details   🦿 Help						
Filter By:		•	Filter	🗐 Show All 🖪	ind:	0,	
Severity	Date	Time	Syslog ID	Source IP	Destination IP		
<u>4</u> 6	Mar 21 2008	20:03:36	725007	10.77.233.74		SSL session with client inside:10.77.233.74/1026 terminated.	
A 6	Mar 21 2008	20:03:35	106015	10.77.233.74	10.77.241.142	Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44	
<u>4</u> 6	Mar 21 2008	20:03:35	302014	10.77.233.74	10.77.241.142	Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Identii	
A 6	Mar 21 2008	20:03:35	605005	0.0.0.0	0.0.0.0	Login permitteri from 0.0.0.0/1026 to inside:0.0.0.0/https for user "enable	
<u>A</u> 6	Mar 21 2006	20:03:35	725002	10.77.233.74		Device completed SSL handshake with dient inside:10.77.233.74/1026	
🔺 6	Mar 21 2008	20:03:35	725003	10.77.233.74		S5L client inside:10.77.233.74/1026 request to resume previous session.	
A 6	Mar 21 2008	20:03:35	725001	10.77.233.74		Starting SSL handshake with client inside: 10.77.233.74/1026 for TLSv1 se	
<u>4</u> 6	Mar 21 2008	20:03:35	302013	10.77.233.74	10.77.241.142	Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.23	
%ASA-6-725002 Device completed SSL handshake with remote_device interface_name:IP_address/port The SSL handshake has completed successfully with the remote device.							

## <u>관련 정보</u>

- <u>Cisco 5500 Series Adaptive Security Appliance 지원 페이지</u>
- <u>AnyConnect VPN 클라이언트 릴리스 정보, 릴리스 2.0</u>
- ASA/PIX: ASA 컨피그레이션의 VPN 클라이언트에 대해 스플릿 터널링 허용 예
- <u>라우터를 통해 VPN 클라이언트가 스플릿 터널링 컨피그레이션을 사용하여 IPsec 및 인터넷에</u> <u>연결할 수 있음 예</u>
- <u>스틱 컨피그레이션의 공용 인터넷 VPN용 PIX/ASA 7.x 및 VPN 클라이언트 예</u>
- ASA의 SVC(SSL VPN Client) with ASDM 컨피그레이션 예
- <u>기술 지원 및 문서 Cisco Systems</u>