ASA에서 AnyConnect 관리 VPN 터널 설정

목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 배경 정보 관리 터널 작업 제한 사항 구성 ASDM/CLI를 통한 ASA 컨피그레이션 AnyConnect 관리 VPN 프로파일 생성 AnyConnect 관리 VPN 프로파일의 구축 방법 (선택 사항) Tunnel-All 컨피그레이션을 지원하도록 사용자 지정 특성을 구성합니다 다음을 확인합니다. 문제 해결 관련 정보

소개

이 문서에서는 VPN 게이트웨이가 Cisco AnyConnect Secure Mobility Client에서 관리 VPN 터널을 통한 연결을 수락할 때 ASA를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASDM(Adaptive Security Device Manager)을 통한 VPN 구성
- 기본 ASA(Adaptive Security Appliance) CLI 컨피그레이션
- X509 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 소프트웨어 버전 9.12(3)9
- Cisco ASDM 소프트웨어 버전 7.12.2
- Windows 10(Cisco AnyConnect Secure Mobility Client 버전 4.8.03036)

참고: AnyConnect VPN 웹 배포 패키지(anyconnect-win*.pkg or anyconnect-macos*.pkg) Cisco <u>Software</u> <u>Download</u>(등록된 고객만 해당) AnyConnect VPN 클라이언트를 원격 사용자 컴퓨터에 다운 로드할 ASA의 플래시 메모리에 복사하여 ASA와의 SSL VPN 연결을 설정합니다. 자세한 내 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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

관리 VPN 터널은 최종 사용자가 VPN 연결을 설정하는 경우뿐만 아니라 클라이언트 시스템의 전원 이 켜질 때마다 기업 네트워크에 대한 연결을 보장합니다. 사무실 외부 엔드포인트, 특히 사용자가 VPN을 통해 사무실 네트워크에 연결하는 빈도가 낮은 디바이스에 대해 패치 관리를 수행할 수 있 습니다. 회사 네트워크 연결이 필요한 엔드포인트 OS 로그인 스크립트도 이 기능을 활용할 수 있습 니다.

관리자는 AnyConnect 관리 터널을 사용하여 사용자가 로그인하기 전에 사용자 작업 없이 AnyConnect를 연결할 수 있습니다. AnyConnect 관리 터널은 신뢰할 수 있는 네트워크 탐지와 함께 작동할 수 있으므로 엔드포인트가 오프프레미스 상태이고 사용자가 시작한 VPN에서 연결이 끊어 진 경우에만 트리거됩니다. AnyConnect 관리 터널은 엔드 유저에게 투명하며, 사용자가 VPN을 시 작하면 자동으로 연결이 끊깁니다.

OS/애플리케이션 ASA ASDM Windows AnyConnect 버전 macOS AnyConnect 버전 Linux **최소 버전 요구 사항** 9.0.1 7.10.1 4.7.00136 4.7.01076 지원되지 않음

관리 터널 작업

AnyConnect VPN 에이전트 서비스는 시스템 부팅 시 자동으로 시작됩니다. 관리 터널 기능이 (관리 VPN 프로필을 통해) 활성화된 것을 탐지하므로 관리 클라이언트 애플리케이션을 시작하여 관리 터 널 연결을 시작합니다. 관리 클라이언트 애플리케이션은 관리 VPN 프로필의 호스트 항목을 사용하 여 연결을 시작합니다. 그런 다음 VPN 터널이 평소와 같이 설정됩니다. 단, 관리 터널은 사용자에게 투명하게 설정되므로 관리 터널 연결 중에 소프트웨어 업데이트가 수행되지 않습니다.

사용자는 AnyConnect UI를 통해 VPN 터널을 시작하며, 이는 관리 터널 종료를 트리거합니다. 관리 터널이 종료되면 사용자 터널 설정이 평소와 같이 계속됩니다.

사용자가 VPN 터널을 연결 해제하면 관리 터널의 자동 재설정이 트리거됩니다.

제한 사항

- 사용자 상호 작용이 지원되지 않습니다.
- 머신 인증서 저장소(Windows)를 통한 인증서 기반 인증만 지원됩니다.
- 엄격한 서버 인증서 검사가 시행됩니다.
- 개인 프록시는 지원되지 않습니다.
- 공용 프록시가 지원되지 않습니다. ProxyNative 값은 기본 프록시 설정이 브라우저에서 검색되 지 않는 플랫폼에서 지원됩니다.

• AnyConnect 사용자 지정 스크립트는 지원되지 않습니다.

참고: 자세한 내용은 관리 VPN 터널 정보를 참조하십시오.

구성

이 섹션에서는 Cisco ASA를 VPN 게이트웨이로 구성하여 AnyConnect 클라이언트에서 관리 VPN 터널을 통해 연결을 수락하는 방법에 대해 설명합니다.

ASDM/CLI를 통한 ASA 컨피그레이션

1단계. AnyConnect 그룹 정책을 생성합니다. 탐색 Configuration > Remote Access VPN > Network (Client) Access > Group Policies. 클릭 Add.

참고: AnyConnect 관리 터널에만 사용되는 새 AnyConnect 그룹 정책을 생성하는 것이 좋습 니다.

1	Home 🦓 Configuration 📴 Monitoring 🔚	Save 🔇 Refresh 🔇 Back 🔘 Forv	vard ? Help Type topic Go		cisco
	O O Remote Access VPN	Configuration > Remote Ac	cess VPN > Network (Client) Acces	s > Group Policies	
G Device List	Introduction Introduction AnyConnect Connection Profiles AnyConnect Customization/Localizati AnyConnect Client Profile	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes	roup is a collection of user-oriente VPN connection profiles and user ac from an LDAP server you must use a sign	d authorization attribute/value pairs that may be stored i counts. In <u>LDAP attribute map</u> .	nternally on the device or externally on a RADIUS/LDAP server. The group
a l	AnyConnect Client Software				Connection Profiles (Ilsers
lok	Dynamic Access Policies	Name	Туре	Tunneling Protocol	Assigned To
8	Group Policies	AnyConnect	Internal	ssl-client	AnyConnect
	IPsec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;DefaultWE
	Psec(IKEV2) Connection Profiles				
	Secure Mobility Solution				
	Address Assignment				
	Giantiare SELVEN Accord				
	AAA Server Grouns				
	Se LDAP Attribute Map				
	Cocal Users				
	A Secure Desktop Manager				
	E Certificate Management				
	S Language Localization				
	St Load Balancing				
	P DHCP Server				
	A DNS				
	Advanced				
	-				
	A Device Setup				
	A firmell				
	Big Firewall				
	Kemote Access VPN				
	Site-to-Site VPN	Find:	Match Case		
	Device Management				
				Reset Apply	
	÷			invest Chippin	

2단계. 제공: Name 그룹 정책. 할당/생성 Address Pool. 선택 Tunneling Protocols 다음으로 SSL VPN Client 및 /또는 IPsec IKEv2에 나와 있는 것처럼.

General Servers	Name: AnyConnect_MGMT_	Tunnel	
Advanced	Banner: 🔽 Inherit		
	SCEP forwarding URL: 🗹 Inherit		
	Address Pools: Inherit VPN_Po	ol	Select.
	IPv6 Address Pools: 🗹 Inherit		Select.
	More Options		_
	Tunneling Protocols:	Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/I	'sec
	Filter:	✓ Inherit 0	Manage
	Access Hours:	☑ Inherit ○	Manage
0	Simultaneous Logins:	🕑 Inherit	
	Restrict access to VLAN:	☑ Inherit 0	
	Connection Profile (Tunnel Group) Lock:	☑ Inherit 0	
	Maximum Connect Time:	✓ Inherit Unlimited minutes	
	Idle Timeout:	Inherit None minutes	
	Security Group Tag (SGT):	✓ Inherit None (2 – 65519)	
	On smart card removal:	✓ Inherit Disconnect Keep the connection	
	Timeout Alerts		
	Maximum Connect Time Alert Interval:	✓ Inherit Default minutes	
	Periodic Certificate Authentication Interval	Inherit Unlimited hours	
lindi	Nevt	C Provinus	

3단계. 탐색 Advanced > Split Tunneling. 구성 Policy 다음으로 Tunnel Network List Below Firepower Threat Defense Network List에 나와 있는 것처럼.

• • •		Edit Internal G	Froup Policy: AnyConnect_MGMT_	Tunnel	
General Servers Advanced Split Tunneling Browser Proxy AnyConnect Client IPsec(IKEv1) Client	The VPN client makes split tunneling de fields. DNS Names: Send All DNS Lookups Through Tunnel: Policy: IPv6 Policy:	Edit Internal G cisions on the government Inherit Inherit government Inherit	Broup Policy: AnyConnect_MGMT_ e basis of a network list that can Yes No Tunnel Network List Below	Funnel be specified below by providing the proper parameters to 'Policy' and	'Networl
Find:	Network List: Pressing this button to set up split exlu Set up Split Exclusion for Web Securi Intercept DHCP Configuration Message	Inherit sion for Web S ty from Microso	VPN-Split Security proxies.		Manag
		Help	Cancel OK		

참고: 두 IP 프로토콜(IPv4 및 IPv6) 모두에 대해 클라이언트 주소가 푸시되지 않으면 Client Bypass Protocol 설정은 다음과 같아야 합니다 enabled 해당 트래픽이 관리 터널에 의해 중단되지 않도록 합니다. 구성하려면 <u>4</u>단계를 <u>참조하십시오</u>.

에 표시된 대로 저장합니다.

• • •		Add Internal Group Policy	
General	Keep Installer on Client System:	☑ Inherit O Yes O No	
Servers Advanced	Datagram Transport Layer Security (DTLS):	🗹 Inherit 🔿 Enable 🔿 Disable	
Split Tunneling	DTLS Compression:	🗹 Inherit 🔿 Enable 🔿 Disable	
Browser Proxy AnyConnect Client	SSL Compression:	☑ Inherit O Deflate O LZS O Disable	
▶ IPsec(IKEv1) Client	Ignore Don't Fragment(DF) Bit:	Inherit Enable Disable	
	Client Bypass Protocol:	Inherit O Enable Disable	ш
	FQDN of This Device:	V FQDN	
	MTU:	🗹 Inherit	
	Keepalive Messages:	☑ Inherit Disable Interval: seconds	
	Optional Client Modules to Download:	🛛 Inherit	
0	Always-On VPN:	☑ Inherit O Disable O Use AnyConnect Profile setting ●	Ш
	Client Profiles to Download:	🗹 Inherit	
		Add 💼 Delete	
		Profile Name Profile Usage/Type	
			Ш
			Ш
			Ш
Find:	🔘 Next 🔘	Previous	Ĭ
		Help Cancel OK	

5단계. 이 그림과 같이 Apply ASA에 컨피그레이션을 푸시합니다.

Iome 🏹 Configuration 🔯 Monitoring 🔓	J Save 🔇 Refresh 🔇 Back 🔘 Forw	rard 7 Help Type topic Go			c
O O Remote Access VPN	Configuration > Remote Acc	cess VPN > Network (Client) Access	i > Group Policies		
 ? Introduction ? Network (Client) Access ≥ AnyConnect Connection Profiles > S AnyConnect Customization/Localizati 3 AnyConnect Client Profile 	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes	roup is a collection of user-oriented VPN connection profiles and user acc from an LDAP server you must use ar	authorization attribute/value pairs that may be stored ounts. h LDAP attribute map.	internally on the device or externally on a RADIUS/LDAP server. The g	roup
AnyConnect Client Software	Add Belete Sc As	sign			
Popularic Access Policies	Name	Туре	Tunneling Protocol	Assigned To	
Group Policies	AnyConnect	Internal	ssl-client	AnyConnect	
IPsec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;D	Default
IPsec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel	
Secure Mobility Solution		,			
 ▷ Advanced ▷ Clendes SSL VPN Access ▷ Advanced ▷ Advanced ▷ Advanced ▷ Advanced ▷ Cartificate Management ○ Cartificat					
Bervice Setup Firewall Generate Access VPN Stencto Access VPN Device Management	Find:	Match Case			
*			Reset Apply		

그룹 정책에 대한 CLI 구성:

```
! group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-network-list value VPN-Split
client-bypass-protocol enable
address-pools value VPN_Pool
```

6단계. AnyConnect 연결 프로파일을 생성합니다. 탐색 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. 클릭 Add.

참고: AnyConnect 관리 터널에만 사용되는 새 AnyConnect 연결 프로파일을 생성하는 것이 좋습니다.



7단계. 제공: Name Connection Profile에 대해 Authentication Method 다음으로 Certificate only. 다음을 선택 합니다. Group Policy <u>1단계</u>에서 생성한<u>것입니다</u>.

Basic Advanced	Name:	AnyConnect_MGMT_Tunnel		
Advanced	Aliases:			
	Authentication			
	Method:	Certificate only		
	AAA Server Group:	LOCAL	2	Manage
		Use LOCAL if Server Group fails		
	SAML Identity Provider			
	SAML Server :	None	0	Manage
	Client Address Assignment			
	DHCP Servers:			
		• None OHCP Link OHCP Subnet		
	Client Address Pools:			Select
	Client IPv6 Address Pools:			Select
	Default Group Policy			
	Group Policy:	AnyConnect_MGMT_Tunnel	٥	Manage
	(Following fields are linked	t to attribute of the group policy selected above.)		
	Enable SSL VPN clier	nt protocol		
	Enable IPsec(IKEv2) of the sec (IKEv2) of the se	client protocol		
	DNS Servers:			
	WINS Servers:			
	Domain Name:			
Find:		Next Previous		

참고: 로컬 CA의 루트 인증서가 ASA에 있어야 합니다. 탐색 Configuration > Remote Access VPN > Certificate Management > CA Certificates 인증서를 추가/봅니다.

참고: 동일한 로컬 CA에서 발급한 ID 인증서가 머신 인증서 저장소(Windows용) 및/또는 시스 템 키 체인(macOS용)에 있는지 확인하십시오.

8단계. 탐색 Advanced > Group Alias/Group URL. 클릭 Add 의 밑에 Group URLs 및 URL. 확인 Enabled 이(가) 선택되어 있습니다. 클릭 OK 을 눌러 이미지에 표시된 대로 저장합니다. Add AnyConnect Connection Profile

Basic Advanced General Client Addressing Authentication Secondary Authentication Authorization Accounting Group Alias/Group URL	 Enable the display of Radius Reject-Message on the login screen when authentication is rejected Enable the display of Securid messages on the login screen Connection Aliases This SSL VPN access method will present a list of aliases configured for all connection profiles. You r the Login Page Setting in the main panel to complete the configuration. Add Delete (The table is in-line editable.) Alias Enabled
	Group URLs This SSL VPN access method will automatically select the connection profile, without the need for use Add Delete (The table is in-line editable.) URL Enabled URL: https://asa.example.com/AnyConnect_MGMT_Tunnel Cancel OK
Find:	Next Previous Help Cancel OK

IKEv2를 사용하는 경우 IPsec (IKEv2) Access AnyConnect에 사용되는 인터페이스에서 활성화됩니다.

O O Remote Access VPN	Config	uration > Remot	e Access VPN > N	Network (Client) A	Access > AnyConnect Co	nnection Profiles
Introduction Network (Client) Access AnyConnect Connection Profiles	The security Client suppo	appliance automa orts IPsec (IKEv2) tu	tically deploys the unnel as well as SS	e Cisco AnyConnec SL tunnel with Data	ct VPN Client to remote us agram Transport Layer Sec	sers upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN unity (DTLS) tunneling options.
S AnyConnect Customization/Local Access Interfaces						
🛐 AnyConnect Client Profile 🛛 🛛 🔁 Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below						N
SSL access must be enabled if you allow AnyCongect client to be launched from	aunched from a browser 0	Web Launch).				
Population of the second secon		SSL Access		IPsec (IKEv2) Acc		
Group Policies	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate
Psec(IKEv1) Connection Profiles	outside	Image: A start and a start	Sec.	Image: A start and a start	Image: A start and a start	Derice Certificate
Secure Mehility Solution	inside			0	0	Port Settings
Address Assignment						

9단계. 클릭 Apply ASA에 컨피그레이션을 푸시합니다.



연결 프로파일(터널 그룹)에 대한 CLI 컨피그레이션:

tunnel-group AnyConnect_MGMT_Tunnel type remote-access tunnel-group AnyConnect_MGMT_Tunnel general-attributes default-group-policy AnyConnect_MGMT_Tunnel tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes authentication certificate group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable

10단계. 신뢰할 수 있는 인증서가 ASA에 설치되어 있고 AnyConnect 연결에 사용되는 인터페이스에 바인딩되어 있는지 확인합니다. 탐색 Configuration > Remote Access VPN > Advanced > SSL Settings 을 클릭하면 이 설정을 추가/볼 수 있습니다.

참고: <u>ASA에 ID 인증서 설치를</u> 참조하십시오.

Remote Access VPN	○ ○ ○ Configuration > Remote Access	VPN > Advanced > SSL Settings				
Introduction	(
Network (Client) Access	Configure SSL parameters. These param	eters affect both ASDM and SSL VPN acc	ess.			
AnyConnect Customization	The minimum SSL version for the secur	ity appliance to negotiate as a "server":	TLS V1	2	OTLSV1 OTLSV1.2	
AnyConnect Client Softwar	The minimum SSL version for the secur	ity appliance to negotiate as a "client":	TLS V1	0		
Group Policies	Diffie-Hellman group to be used with S	SL:	Group2 - 1024-bit modulus	0		
IPsec(IKEv1) Connection P IPsec(IKEv2) Connection P	ECDH group to be used with SSL:		Group19 - 256-bit EC	0		
Secure Mobility Solution	Encountion					
Address Assignment	cheryption				10	
Advanced	Cipher version	Cipher Security Level		Cipher Algorithm	s/ Custom String	Edit
Clientless SSL VPN Access	Default	Medium		DES-CBC3-SHA	AES128-SHA DHE-RSA-AES128-SHA AES256-SHA DHE-RSA	
AAA/Local Urerr	TLSV1	Medium		DHE-RSA-AES25	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
We and Comments	TLSV1.1	Medium		DHE-RSA-AES25	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
And Server Groups	TLSV1.2	Medium		ECDHE-ECDSA-/	AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D	
CDAP Attribute Map	DTLSV1	Medium		DHE-RSA-AES25	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
🕼 Local Users	DTLSV1.2	Medium		ECDHE-ECDSA-/	AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D	
Secure Desktop Manager						
Certificate Management						
Language Localization						
Load Balancing						
DHCP Server	Server Name Indication (SNI)					
DNS	Domain		Certificate			
Advanced						Add
Advanced						Edit
22 SCL Sattinger						Cont
te sst seconds						Delete
La Reference Identity						
Certificate to AnyConnect						
HTTP Redirect						
Maximum VPN Sessions						
Crypto Engine						
	Castificator					
	Certificates					
	Specify which certificates, if any, sho	uld be used for SSL authentication on ea	ich interface. The fallback certificate	will be used on interfa-	ces not associated with a certificate of their own.	
	Interface	Primary Certificate	Load Balancing Certificate		Key-Type	T-dia -
evice Setup	inside	i i i i i i i i i i i i i i i i i i i			and the	Edit
	management					
rewall	management.	DOOT CHANNEL ICI AND TO			Delevera DCA (2010 bits) Lond Delevelars area	
	outside	IKOOT-CA:hostname=ASA.example	.co		Primary: KSA (2048 bits), Load Balancing: none	
emote Access VPN						
ite-to-Site VPN						
evice Management						
evice management						
			Reset Ann	ly l		

SSL 신뢰 지점에 대한 CLI 구성:

ssl trust-point ROOT-CA outside

AnyConnect 관리 VPN 프로파일 생성

1단계. AnyConnect 클라이언트 프로파일을 생성합니다. 탐색 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. 클릭 Add에 나와 있는 것처럼.

ổ I	lome 🔏 Configuration 📴 Monitor	ing 🔚 Save 🔇 Refresh 🔇 Bac	🖈 🔘 Forward 🧳 Help Type topic Go			cisco
	O O O Remote Access VPN	○ ○ ○ Configuration > Remote	Access VPN > Network (Client) Access > AnyCon	nect Client Profile		
ookmarks Device List	Introduction Introduction Introduction Introduction AnyConnect Connection Profil AnyConnect Clustomization/Lc AnyConnect Clustomization/Lc AnyConnect Clust Profile AnyConnect Clust Profile AnyConnect Clust Profile AnyConnect Clust Profile AnyConnect Cluster AnyConnect AnyConnect AnyConnect AnyConnect	This panel is used to manage A button to add a new profile. Pre The profile Usage field is introd HostScan configuration can be	nyConnect Client Profiles and perform group assign ssing the Import or Export button is for upload and a luced with the Secure Mobility Solution. This field cor performed by going to Secure Desktop Manager/Hos sup Policy III. Deleter III. Import S. Export III Validat	nent for AnyConnect version 2.5 or later You can select lownload of client profiles between local machine and tains different profile usage in AnyConnect version 3.0 Scan. If 'HostScan' is not visible under 'Secure Desktop	a profile to edit, change group or to delete. You can select the 'Add' Jevice. and later. Manager', you will need to restart ASDM.	
	IPser(IKEv1) Connection Profil	- rise a completered		•		
	Precisition of the set of th	Profile Name	Profile Usage	Group Policy	Profile Location	
	SS. Settings Reference identity Certificate to AnyConnect and HTTP Redirect Maximum VPN Sessions Crypto Engine Crypto Engine Composition Comp			Reset Apply		

2단계. 제공: Profile Name. 다음을 선택합니다. Profile Usage 다음으로 AnyConnect Management VPN profile. 다 음을 선택합니다. Group Policy <u>1</u>단계에서 <u>생성됩니다</u>. 클릭 OK 에 나와 있는 것처럼.

ie Name		Profile Usage	Group Policy	Profile Location
	• • •	Add AnyConnect Client Pro	ofile	
	Profile Name	AnyConnect_MGMT_Profile		
	Profile Usage	AnyConnect Management VPN Profile	0	
	Enter a device f created if it doe	ile path for an xml file, ie. disk0:/ac_profile. The file w es not exist.	ill be automatically	
	Profile Location	disk0:/anyconnect_mgmt_profile.vpnm	Brow	vse Flash
			U	pload
	Group Policy	AnyConnect_MGMT_Tunnel	0	
		Enable 'Always On VPN' for selected group		
		Help Cancel	ОК	
	1			
			Reset Apply	

3단계. 생성된 프로필을 선택하고 Edit에 나와 있는 것처럼.



4단계. 탐색 Server List. 클릭 Add 새 서버 목록 항목을 추가합니다(이미지 참조).

	4				710
PN Preferences (Part 1)	Server List				
Preferences (Part 2)					
Backup Servers	Hostname	Host Address	User Group	Backup Server List	Certificate Pins
Certificate Pinning					
Server List					
	Note: at most o	one server can be define	d in a management VP	N profile. Add	Delete
				Edit	Details
	•				

5단계. 제공: Display Name. 추가 FQDN/IP address ASA를 구성합니다 제공: User Group 를 터널 그룹 이름 으로 사용합니다. Group URL 자동으로 채워집니다 FQDN 및 User Group. 클릭 OK.

Sen	ver Certificate Pinning					
Primary Server Display Name (required) AnyConnect_MGMT_Tunr FQDN or IP Addr User Group (requir asa.example.com / AnyConnect_MGM Group URL asa.example.com/AnyConnect_MGMT_Tunnel	Connection Information Primary Protocol SSL ed) ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect IKE Identity (IOS gateway only)					
Backup Servers Host Address	Add Move Up Move Down Delete					
OK Cancel						

참고: FQDN/IP 주소 + 사용자 그룹은 <u>8단계</u>에서 AnyConnect 연결 프로파일 컨피그레이션 중 에 언급된 그룹 URL과 동일해야<u>합니다</u>.

참고: IKEv2를 프로토콜로 사용하는 AnyConnect를 사용하여 ASA에 대한 관리 VPN을 설정 할 수도 있습니다. 확인 Primary Protocol 다음으로 설정됨 IPsec <u>5</u>단계.

6단계. 그림에 표시된 대로 ок 저장하십시오.

file: AnyConnect_M	GMT_Profile				Abo
VPN	Server List				
Preferences (Part 1)					
Backup Servers	Hostnamo	Host Address	llsor Croup	Packup Conver List	Cortificato Dinc
🖉 Certificate Pinning	AnyConnect_MGM	T_T asa.example.com	AnyConnect_MGMT	_T Inherited	Certificate Fins
Certificate Matching					
Server List					
	Note: at most o	one server can be defined	in a management VPN	I profile. Add	Delete
	note. at most c		in a management mit		Delete
				Edit	Details
	•				
	×				

7단계. 클릭 Apply t을 눌러 그림과 같이 ASA에 컨피그레이션을 푸시합니다.

1	Home 🍕 Configuration 👰 Monito	ing 調 Save 💽 Refresh 🔇 Back 🔘 Forv	vard 💡 Help Type topic Go			cisco
	O O O Remote Access VPN	○ ○ ○ Configuration > Remote Access Vi	PN > Network (Client) Access > AnyConnect Client	nt Profile		
Ĕ	Introduction					
S	V Network (Client) Access					
8	AnyConnect Connection Profil	This panel is used to manage AnyConnect	Client Profiles and perform group assignment for A	nyConnect version 2.5 or later.You can select a profi	le to edit, change group or to delete. You can select the 'Add'	
n.	h AmConnect Customization/L	The profile Usage field is introduced with	he forum Mehility Solution. This field contains diff	or client profiles between local machine and device.		
	Am Connect Client Profile	The prome usage neid is introduced with t	the secure mobility solution. This neid contains unit	erent prome usage in Anyconnect version 5.0 and ia	ter.	
2	Am Connect Client Software	HostScan configuration can be performed	by going to Secure Desktop Manager/HostScan. If '	HostScan' is not visible under 'Secure Desktop Manag	er', you will need to restart ASDM.	
2	Demonsis Assess Balisias					
ð.	Craw Palisias	Add 17 Edit 22 Change Crown Policy	Delete Tilmport 🖡 Export 🖓 Validate			
8	Billion (Kful) Connection Profil	* Add Care 25 change Group Foncy	Belete a import a cxport gy vandate			
	Psec(KEVI) Connection Profil	Profile Name	Profile Usage	Group Policy	Profile Location	
	Psec(ikev2) Connection Profil	AnyConnect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm	
	Secure Mobility Solution					
	Address Assignment					
	P W Advanced					
	P Chendess SSL VPN Access					
	REF AAA Correct Correct					
	AAA Server Groups					
	EDAF Attribute Map					
	B Cocura Dachter Manager					
	Gertificate Management					
	Ceronicate Management					
	8.8 Load Palancing					
	Coad balancing					
	B DNS					
	T T Advanted					
	the Connection Category					
	SEL Satting					
	Reference Identify					
	Cartificate to AmConnect and					
	WITTP Redirect					
	Maximum VPN Services					
	Comto Engine					
	Ba Crypto Engine					
	Q Davidas Satura					
	Bevice Setup					
	Firewall					
	Remote Access VPN					
	Site-to-Site VPN					
	Device Management					
	No overce management			Devel Australia		
	2 T			Appry		

AnyConnect 관리 VPN 프로파일 추가 후 CLI 구성

webvpn enable outside hsts enable max-age 31536000 include-sub-domains no preload no anyconnect-essentials anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm anyconnect enable tunnel-group-list enable cache disable error-recovery disable 1 group-policy AnyConnect_MGMT_Tunnel internal group-policy AnyConnect_MGMT_Tunnel attributes vpn-tunnel-protocol ikev2 ssl-client split-tunnel-network-list value VPN-Split client-bypass-protocol enable address-pools value VPN_Pool webvpn anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt

AnyConnect 클라이언트 머신의 AnyConnect 관리 VPN 프로파일:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<UseStartBeforeLogon UserControllable="false">false"/schemas.xmlsoap.org/encoding/
```

<ShowPreConnectMessage>false</ShowPreConnectMessage>

```
<ProxySettings>IgnoreProxy</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>
```

--- Output Omitted ---

```
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>
```

참고: 사용자 AnyConnect VPN 프로파일에서 TND(Trusted Network Detection)를 사용하는 경우 일관된 사용자 환경을 위해 관리 VPN 프로파일에서 동일한 설정을 확인하는 것이 좋습 니다. 관리 VPN 터널은 사용자 VPN 터널 프로파일에 적용된 TND 설정에 따라 트리거됩니다 . 또한 관리 VPN 프로파일의 TND 연결 작업(관리 VPN 터널이 활성 상태일 때만 시행됨)은 관 리 VPN 터널이 최종 사용자에게 투명하게 유지되도록 항상 사용자 VPN 터널에 적용됩니다.

참고: 모든 최종 사용자 PC에서 Management VPN 프로필에 TND 설정이 활성화되어 있고 사 용자 VPN 프로필이 누락된 경우, 누락된 사용자 VPN 프로필 대신 TND에 대한 기본 환경 설 정(AC 클라이언트 애플리케이션의 기본 환경 설정에서 비활성화됨)을 고려합니다. 이러한 불 일치는 예기치 않은/정의되지 않은 동작으로 이어질 수 있습니다.

기본적으로 TND 설정은 기본 환경 설정에서 비활성화되어 있습니다.

AnyConnect 클라이언트 애플리케이션에서 기본 환경 설정 하드코딩된 설정을 극복하려면 최 종 사용자 PC에 두 개의 VPN 프로파일, 즉 사용자 VPN 프로파일과 AC 관리 VPN 프로파일 이 있어야 하며 두 프로파일 모두 동일한 TND 설정이 있어야 합니다.

관리 VPN 터널 연결 및 연결 해제의 논리는 AC 에이전트가 관리 VPN 터널을 설정하기 위해 사용자 VPN 프로필 TND 설정을 사용하고 관리 VPN 터널의 연결을 해제하려면 관리 VPN 프 로필 TND 설정을 확인하는 것입니다.

AnyConnect 관리 VPN 프로파일의 구축 방법

• VPN 게이트웨이에서 AnyConnect 관리 VPN 프로파일을 다운로드하기 위해 ASA 연결 프로파 일을 사용하여 성공한 사용자 VPN 연결이 완료되었습니다.

참고: 관리 VPN 터널에 사용된 프로토콜이 IKEv2인 경우 SSL을 통해 첫 번째 연결을 설정해 야 합니다(ASA에서 AnyConnect 관리 VPN 프로파일을 다운로드하려면).

• AnyConnect 관리 VPN 프로필은 GPO 푸시를 통해 또는 수동 설치를 통해 클라이언트 머신에 수동으로 업로드할 수 있습니다(프로필의 이름이 VpnMgmtTunProfile.xml).

프로필을 추가해야 하는 폴더의 위치:

창: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun

맥OS: /opt/cisco/anyconnect/profile/mgmttun/

(선택 사항) Tunnel-All 컨피그레이션을 지원하도록 사용자 지정 특성을 구성합니다

사용자가 시작한 네트워크 통신에 영향을 주지 않으려면 관리 VPN 터널에는 기본적으로 터널링 컨 피그레이션이 포함된 분할이 필요합니다. 관리 터널 연결에서 사용하는 그룹 정책에서 사용자 지정 특성을 구성할 때 이를 무시할 수 있습니다.

1단계. 탐색Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. 클 릭 Add에 나와 있는 것처럼.



2단계. 사용자 지정 특성 유형 설정 ManagementTunnelAllAllowed Cisco의 Description. 클릭 OK에 나와 있 는 것처럼.

	Delete						
e				Description	1		
	•••	Create Cu	ustom Attribute	Туре			
	• • •	Create Cu	ustom Attribute	Туре			
	• • Type:	Create Cu ManagementTunnelAllAllou	ustom Attribute	Туре			
	Type:	Create Cu ManagementTunnelAllAllov ManagementTunnelAllAllov	wed	Туре			
	Type: Descriptio	Create Cu ManagementTunnelAllAllov ManagementTunnelAllAllov 1:	wed	Туре	=		
	Type: Descriptio	Create Cu ManagementTunnelAllAllov ManagementTunnelAllAllov 1:	wed	Туре			
	Type: Descriptio	Create Cu ManagementTunnelAllAllov ManagementTunnelAllAllov 1:	wed wed	Туре			

3단계. 탐색 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. 클릭 Add에 나와 있는 것처럼.



4단계. Type(유형)을 ManagementTunnelAllAllowed . Name(이름)을 true. 클릭 Add- 이미지에 표시된 대로 사용자 지정 특성 값을 제공합니다.

Add Edit Delete		
• • •	Create Custom Attribut	e Name
Type: Name: Configure Value	ManagementTunnelAllAllowed true Value	Contraction Manage
	Help Cancel	ОК

5단계. 값 설정 true. 클릭 oK에 나와 있는 것처럼.

	Create Custo	om Attribute Name			
Type:	ManagementTunnelAllAllowed		\$	Manage	
Name:	true				
	Value		Add		
		Add Value	e.0.		
true					
Value.					
value.					

6단계. 탐색 Configuration > Remote Access VPN > Network (Client) Access > Group Policies. 그룹 정책을 선택합니 다. 클릭 Edit 에 나와 있는 것처럼.

ổ н	ome 🍫 Configuration 📴 Monitoring 🚛	Save 💽 Refresh 🔇 Back 🔘 Fo	rward ? Help Type topic Go			cisco
	COO Remote Access VPN	O O Configuration > Remote A	ccess VPN > Network (Client) Access	> Group Policies		
rks 📑 Device List	Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Connection Profiles AnyConnect Client Profile TomyConnect Client Profile	Manage VPN group policies.A VPN server. The group policy informati To enforce authorization attribute	group is a collection of user-oriented a on is referenced by VPN connection pro s from an LDAP server you must use an Assign	uthorization attribute/value pairs that may be : files and user accounts. LDAP attribute map.	stored internally on the device or externally on a RADIUS/L	DAP
okma	Dynamic Access Policies	Name	Туре	Tunneling Protocol	Connection Profiles/Users	
ă	Group Policies	AmConnect	Internal	ssl-client	AmConnect	_
	Psec(IKEv1) Connection Profiles	DftCroBolicy (System Default)	Internal	ikend ikend (2)	DefaultRACroup: DefaultI 21 Croup: DefaultADMINCroup	Dof
	IPsec(IKEv2) Connection Profiles	Am Copport MCMT Tuppel	Internal	ikev2,iztp=ipsec	Am Connect MCMT Tunnel	p,Dei
	Secure Mobility Solution	Priyoonnect_wowr_runner	internal	ikevz,ssi-cient	Partyconnect_wowr_runner	
	Address Assignment Advanced AryConnect Essentials AryConnect Custom Attributes AryConnect Custom Attribute AryConnect Custom Advanced					
	-					
	Device Setup					
1	Firewall					
	Remote Access VPN					
	🚰 Site-to-Site VPN	Find:	Match Case			
1	Device Management					
	*			Reset Apply		

7단계. 이 이미지에 표시된 대로 Advanced > Split Tunneling. 정책 구성 Tunnel All Networks.

• •		Edit Interr	nal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers	The VPN client makes split tunneling de fields.	cisions on the	e basis of a network list that can be specified below by providing the proper parameters to 'Policy	/' and 'Network Li:
General Servers Advanced Split Tunneling Browser Proxy AnyConnect Client IPsec(IKEv1) Client	The VPN client makes split tunneling de fields. DNS Names: Send All DNS Lookups Through Tunnel: Policy: IPv6 Policy: Network List: Pressing this button to set up split exlu Set up Split Exclusion for Web Securi Intercept DHCP Configuration Message	Inherit Inherit	e basis of a network list that can be specified below by providing the proper parameters to 'Policy Yes No Tunnel All Networks Security proxies.	 And 'Network Lit Manage
Find:	Next	Previous		
			Help Cancel OK	

8단계. 탐색 Advanced > Anyconnect Client > Custom Attributes. 클릭 Add에 나와 있는 것처럼.

• • •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel
General Servers V Advanced Split Tunneling Browser Proxy V AnyConnect Client Login Setting Client Firewall Key Regeneration Dead Peer Detection Customization Custom Attributes V IPsec(IKEV1) Client	Configuration of custom policy attributes. Image: Configuration of custom policy attributes. Type Name of Value
Find:	Next Previous Help Cancel OK

9단계. 특성 유형을 다음과 같이 선택합니다. ManagementTunnelAllAllowed Value as(값)를 true. 클릭 ок에 나와 있는 것처럼.

	Name	of Value
	Create Custom Attribute	
Attribute type:	ManagementTunnelAllAllowed	Manage
Omit the value		_
Select Value:	true	Manage

10단계. 클릭 Apply 를 클릭하면 그림과 같이 ASA에 컨피그레이션을 푸시합니다.

🔥 Home 🍕 Configuration 📴 Monitoring 🔚	🕽 Save 🔇 Refresh 🔇 Back 🔘 Forw	ard 💡 Help Type topic Go		aludu cisco
000 Remote Access VPN	O O Configuration > Remote Acc	ess VPN > Network (Client) Acce	ss > Group Policies	
Introduction I	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes f Add - @ Edit 1 Delete As:	oup is a collection of user-oriente /PN connection profiles and user a from an LDAP server you must use sign	d authorization attribute/value pairs that may be stored in ccounts. an LDAP attribute map.	tternally on the device or externally on a RADIUS/LDAP server. The group
E Dunamic Access Policies	Mama	Tune	Turnaling Bratesol	Connection Profiles/Users
9 ST Group Policies	Name	Type	Tunneing Protocol	Assigned To
Psec(IKEv1) Connection Profiles	AnyConnect	Internal	ssi-client	AnyConnect
IPsec(IKEv2) Connection Profiles	DritGrpPolicy (system Default)	internal	ikev2;iztp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;DefaultWE
Secure Mobility Solution	Milyconnect_MGM1_1unnet	insernal	ikevz,ssi+cilerik	AnyConnect_MGM1_10nnet
Address Assignment				
Advanced				
Clientless SSL VPN Access				
🔻 🖬 AAA/Local Users				
M AAA Server Groups				
See LDAP Attribute Map				
😥 Local Users				
Manager				
Certificate Management				
Language Localization				
Load Balancing				
p DHCP Server				
J DNS				
Advanced				
Device Setup				
Firewall				
Remote Access VPN				
Site-to-Site VPN	Find:	Match Case		
Device Management				
			Reset Apply	
¢ .				

다음 이후의 CLI 컨피그레이션 ManagementTunnelAllAllowed 사용자 지정 특성이 추가되었습니다.

webvpn

enable outside

anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed hsts enable

max-age 31536000

```
include-sub-domains
 no preload
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
anyconnect enable
tunnel-group-list enable
cache
 disable
 error-recovery disable
1
anyconnect-custom-data ManagementTunnelAllAllowed true true
1
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelall
client-bypass-protocol enable
address-pools value VPN_Pool
anyconnect-custom ManagementTunnelAllAllowed value true
webvpn
 anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

다음을 확인합니다.

ASA CLI에서 관리 VPN 터널 연결을 show vpn-sessiondb detail anyconnect 명령을 실행합니다.

```
ASA# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

```
Username
           : vpnuser
                                    Index
                                                : 10
                                    Public IP
Assigned IP : 192.168.10.1
                                                 : 10.65.84.175
           : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
License
           : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-
256
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Hashing
            : 17238
Bytes Tx
                                    Bytes Rx
                                              : 1988
            : 12
Pkts Tx
                                    Pkts Rx
                                                 : 13
Pkts Tx Drop : 0
                                    Pkts Rx Drop : 0
Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel
Login Time : 01:23:55 UTC Tue Apr 14 2020
Duration
           : 0h:11m:36s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                    VLAN
                                                : none
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
--- Output Omitted ---
DTLS-Tunnel:
 Tunnel ID
             : 10.3
                                      Public IP : 10.65.84.175
 Assigned IP : 192.168.10.1
 Encryption : AES-GCM-256
                                      Hashing
                                                  : SHA384
 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
 Encapsulation: DTLSv1.2
                                      UDP Src Port : 57053
```

UDP Dst Port :	443 Au	th Mode :	Certificate
Idle Time Out:	30 Minutes Id	le TO Left :	18 Minutes
Client OS :	Windows		
Client Type :	DTLS VPN Client		
Client Ver :	Cisco AnyConnect VPN Agen	t for Windows	s 4.8.03036
Bytes Tx :	17238	Bytes Rx	: 1988
Pkts Tx :	12	Pkts Rx	: 13
Pkts Tx Drop :	0	Pkts Rx Dro	op : 0

ASDM에서 관리 VPN 터널 연결을 확인합니다.

Monitoring(**모니터링) > VPN > VPN Statistics(VPN 통계) > Sessions(세션)로 이동합니다**. 클라이 언트 세션**을** 보려면 AnyConnect 클라이언트로 필터링합니다.

🚮 Home 🔩 Configuration [🦉 Mo	onitoring 🔚 Save 🔇	Refresh 🔇 Back	Forward ?	Help Type topic Go					cisco
Device List Bookmarks	0 0 0 Monitoring >	VPN > VPN Statistic	cs > <u>Sessions</u>						
O O O Device List									
🕈 Add 📋 Delete 🚿 Connect	Туре	Active	c	umulative	Peak Concurren	t	Inactive		
ind: Go	AnyConnect Client		1		19		1		0
A 10.106.39.196	SSL/TLS/DTLS		1		19		1		0
A 10.106.64.230									
A 10.197.227.47									
10.106.51.99:444									
OOO VPN									
 VPN Statistics Sessions 	Filter By AnyConn	ect Client	All Se	ssions ᅌ	Filt	er			
VPN Cluster Loads	Username	Group Policy A:	ssigned IP Address	Protocol	Login Time	Bytes Tx	Inactivity	Audit !	Details
Crypto Statistics	vpnuser Ar	nvConnect MGMT19	92.168.10.1	AnvConnect-Parent	10:52:25 UTC		0h:00m:00s	c0a80	
Compression Statistics	A	nyConnect_MGMT 10	0.65.84.175	AnyConnect-Parent: (1)nor	ne Oh:01m:31s	33954			Logout
Encryption Statistics	L								-
GIODAI IKE/IPSec Statistics									Ping
VI AN Manning Sessions									
Clientless SSL VPN									
Shared SSL VPN									
VPN Connection Graphs									
SA Sessions									
Interfaces									
C VPN									
	To sort VPN sessions	right-click on the a	hove table and sel	ect Table Sort Order from	popup menu				
Area Routing	to sole the sessions,	ingite circk on the a	above table and set	cer ruble borr order from	popup menu.				
Sam Properties	Logout By: All S	Sessio ᅌ		Logout Sessions					

클라이언트 컴퓨터에서 관리 VPN 터널 연결 확인:

Sisco AnyConnect Secure Mobil	ity Client	- 🗆 X
cisco AnyCon	nect Secure Mobility	Client
Virtual Private Network (VPI	۷)	Diagnostics
Preferences Statistics Route Detail	s Firewall Message History	
Connection Information State: Tunnel Mode (IPv4):	Disconnected Not Available	Cisco AnyConnect Secure Mobility Client — X
Tunnel Mode (IPv6): Dynamic Tunnel Exclusion: Dynamic Tunnel Inclusion: Duration: Session Disconnect: Management Connection State:	Not Available Not Available Not Available 00:00:00 None Connected (asa.example.com)	VPN: Ready to connect.
Address Information Client (IPv4):	Not Available	
Client (IPv6): Server:	Not Available Not Available	
Bytes		• •
		Reset Export Stats

문제 해결

새 UI Statistics 라인(Management Connection State(관리 연결 상태))을 사용하여 관리 터널 연결 문제를 해결할 수 있습니다. 일반적으로 나타나는 오류 상태입니다.

연결 끊김(사용 안 함):

- 기능이 비활성화되어 있습니다.
- 사용자 터널 연결(사용자 터널 그룹 정책에 관리 VPN 프로파일을 추가해야 함)을 통해 관리 VPN 프로파일이 클라이언트에 배포되었거나 프로파일 수동 업로드를 통해 대역 외 상태인지 확인합니다.
- 관리 VPN 프로필이 터널 그룹을 포함하는 단일 호스트 항목으로 구성되어 있는지 확인합니다.

연결 끊김(신뢰할 수 있는 네트워크):

• TND가 트러스트된 네트워크를 탐지하여 관리 터널이 설정되지 않았습니다.

연결 끊김(사용자 터널 활성):

• 사용자 VPN 터널이 현재 활성 상태입니다.

연결 끊김(프로세스 시작 실패):

• 관리 터널 연결을 시도하는 동안 프로세스 시작 오류가 발생했습니다.

연결 끊김(연결 실패):

- 관리 터널을 설정하는 동안 연결 오류가 발생했습니다.
- 인증서 인증이 터널 그룹에 구성되어 있고 그룹 정책에 배너가 없으며 서버 인증서를 신뢰할 수 있어야 합니다.

연결 끊김(잘못된 VPN 구성):

- VPN 서버에서 잘못된 스플릿 터널링 구성을 받았습니다.
- 관리 터널 그룹 정책에서 스플릿 터널링 컨피그레이션을 확인합니다.

연결 끊김(소프트웨어 업데이트 보류 중):

• AnyConnect 소프트웨어 업데이트가 현재 보류 중입니다.

연결 끊김:

• 관리 터널이 설치되려고 하거나 다른 이유로 설치할 수 없습니다.

<u>추가 트러블슈팅</u>을 위해 DART를 수집합니다.

관련 정보

- <u>관리 VPN 터널 구성</u>
- <u>관리 VPN 터널 문제 해결</u>
- <u>기술 지원 및 문서 Cisco Systems</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.