FMC에서 관리하는 FTD에 AnyConnect 동적 스 플릿 터널 구성

목차

<u>소개</u> 사전 요구 사항 요구 사항 사용되는 구성 요소 배경 정보 제한 사항 구성 1단계. 동적 스플릿 터널을 사용하도록 그룹 정책 편집 2단계. AnyConnect 사용자 지정 특성 구성 3단계. 컨피그레이션 확인, 저장 및 구축 다음을 확인합니다. 문제 해결 문제 솔루션 관련 정보 소개

이 문서에서는 FMC(Firepower Management Center)에서 관리하는 FTD(Firepower Threat Defense)에서 AnyConnect 동적 스플릿 터널을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco AnyConnect
- FMC에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- FMC 버전 7.0
- FTD 버전 7.0

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

FMC에서 관리하는 FTD의 AnyConnect 동적 스플릿 터널 컨피그레이션은 FMC 버전 7.0 이상에서 완전히 사용할 수 있습니다. 이전 버전을 실행하는 경우 FMC를 사용하는 Firepower <u>Threat</u> <u>Defense</u>용 <u>Advanced AnyConnect VPN Deployments</u>의 지침에 따라 FlexConfig를 통해 <u>구성해야</u> 합니다.

동적 스플릿 터널 컨피그레이션을 사용하면 DNS 도메인 이름을 기반으로 스플릿 터널 컨피그레이 션을 세부적으로 조정할 수 있습니다. FQDN(Full-Qualified Domain Name)과 연결된 IP 주소가 변 경될 수 있으므로 DNS 이름을 기반으로 하는 스플릿 터널 컨피그레이션을 통해 원격 액세스 VPN(Virtual Private Network) 터널에 어떤 트래픽이 포함되는지 또는 포함되지 않는지 좀 더 동적 으로 정의할 수 있습니다. 제외된 도메인 이름에 대해 반환된 주소가 VPN에 포함된 주소 풀 내에 있 는 경우 해당 주소는 제외됩니다. 제외된 도메인은 차단되지 않습니다. 대신 이러한 도메인에 대한 트래픽은 VPN 터널 외부에 유지됩니다.

동적 스플릿 터널도 구성할 수 있습니다 IP 주소를 기반으로 제외되는 터널을 포함할 도메인을 정의 합니다.

제한 사항

현재 이러한 기능은 여전히 지원되지 않습니다.

- 동적 스플릿 터널은 iOS(Apple) 디바이스에서 지원되지 않습니다. Cisco 버그 ID CSCvr<u>을 참조</u> 하십시오54798
- 동적 스플릿 터널은 Anyconnect Linux 클라이언트에서 지원되지 않습니다. Cisco 버그 IDCSCvt를 참조하십시오64988

구성

이 섹션에서는 FMC에서 관리하는 FTD에서 AnyConnect 동적 스플릿 터널을 구성하는 방법에 대해 설명합니다.

1단계. 동적 스플릿 터널을 사용하도록 그룹 정책 편집

1. FMC에서 Devices(**디바이스) > VPN > Remote Access(원격 액세스)**로 이동한 다음 컨피그레이 션을 적용할 **연결** 프로필을 선택합니다.

Overview Analysis Policies Devices Objects AMP Intelligence	1		\rm 0, Deploy System Help + admin +
Device Management Device Upgrade NAT VPN + Remote Access 0	QoS Platform Settings FlexConfig Certificates		
SSL_AnyConnect			Save Cancel
			Policy Assignments (1)
		Local Realm: AnyConnect-Local-Aut	Dynamic Access Policy: angsanc2-test
Connection Profile Access Interfaces Advanced			
			0
Name	AAA	Group Policy	
DefaultWE8VPNGroup	Authentication: None Authorization: None Accounting: None	DftGrpPolicy	/ 5
SSL_AnyConnect_LocalAuth	Authentication: LOCAL Authorization: None Accounting: None	AnyConnect_Local_Auth	/ 8
SSL_AnyConnect_LDAPAuth	Authentication: AnyConnect-LDAP-Auth (AD) Authorization: AnyConnect-LDAP-Auth (AD) Accounting: Anne	AnyConnect_LDAP_Auth	/8

2. 이미 생성된 그룹 정책 중 하나를 수정하려면 그룹 정책 편집을 선택합니다.

Overview Analysis Policies Devices Objects A	MP Intelligence					0 ₃ Deploy System Help v admin √
Device Management Device Upgrade NAT VPN + Rer	mote Access QoS Pla	tform Settings Flex	Config Certificates			
SSL_AnyConnect						Save Cancel
						Policy Assignments (1)
					Local Realm: Am/Connect-Local-Aut	Dynamic Access Policy: angsanc2-test
Connection Profile Access Interfaces Advanced						
						0
Name						
DefaultWEBVPNGroup	Authent	Edit Connection P	rofile	? ×		19
Design a cover workey	Authoriz Account					~ 0
SSL AnyConnect LocalAuth	Authent	Connection Profile:*	SSL_AnyConnect_LocalAuth		Auth	28
and the second	Authoriz	Group Policy:*	Edit Group Policy		,	<i>.</i> .
SSL AnyConnect LDAPAuth	Authent				Auth	18
	Authoriz	Client Address Ass	Ignment AAA Allases			- 0
		IP Address for the re Configure the 'Client	mote clients can be assigned from local IP Address pool Address Assignment Policy' in the Advanced tab to defi	Is/DHCP Servers/AAA Servers. ne the assignment criteria.		
		Address Pools:		0.		
		Name	IP Address Range			
		ftdv-dperezve-pool	172.16.13.1-172.16.13.254	/8		
		DHCP Servers:		0		
		Name	DHCP Server IP Address			
		Configure device ov multinla davicar	errides in the address pool object to avoid IP address conflic	ts in case of object is shared across		
				Save Cancel		

2단계. AnyConnect 사용자 지정 특성 구성

1. Group Policy(그룹 정책) 컨피그레이션에서 Anyconnect > Custom Attributes(사용자 지정 특성)로 이동하고 Add(+) 버튼을 클릭합니다.

Overview Analysis Policies Devices Objects Integration Device Management Device Upgrade NAT QoS Platform Settings Fiex	nfig Certificates VPN > Rem	note Access Troubleshoot •	Desiloy 🧌 🏤 System Help v admin v
FTD_RAVPN_Policy1			Save Cancel
	Edit Connection Profile	**	Policy Assignments (0) Local Realm: Local. REALM1 Dynamic Access Policy: <u>Bone</u>
Connection Profile Access Interfaces Advanced	Add Group Policy	? ×	
	Name:* Anyconnect,	Llocal Auth	0
Name	Description:		
DefaultWEBVINGroup	General AnyConnect	Advanced	/8
FTD_RAVPN_Policy11	ventor Ve	AryConnect Custom Attribute feature allows a more expedited way of configuring new endpoint features on Firewall Threat Defense. This feature is supported on Firewall Threat Defense 7.0 onwards.	28
new-testo	SSL Settings Senter Senter Custom Attributes	Attribute Name Content	∕8
		No records to display	

2. **동적 스플릿 터널링 AnyConnect 특성**을 선택하고 **추가(+) 버튼**을 클릭하여 새 사용자 지정 특성 개체를 만듭니다.

Edit Connecti	ion Profile	? ×
Edit Group Po	blicy	? ×
Name:*	Regular_Users_GP1	
Description:		
General A	nyConnect Advanced	
Profile Management Pro	AnyConnect Custom Attribute feature allows a more expedited way of configuring new office endopint features on Firewall Threat Defense. This feature is supported on Firewall	,
Client Modules	Add Custom Attribute ? ×	0
Connection Set	AnyConnect Attribute:* Dynamic Split Tunneling	
Custom Attriout	Custom Attribute Object:*	
	Add Cancel	
	Save Car	cel

3. AnyConnect 사용자 **지정** 특성의 **이름**을 입력하고 동적으로 포함하거나 제외할 도메인을 구성합 니다.

참고: Include domains(도메인 포함) 또는 **Exclude domains(도메인** 제외)**만** 구성할 수 있습니 다.

Overview Analysis Policies Devices Objects AMP Intelligence	1						Q, Deploy	System Help v admin v
Device Management Device Upgrade NAT VPN - Remote Access	QoS Pl	atform Settings FlexCo	onfig Certificates					
SSL_AnyConnect								
								Policy Assignments (1)
						Lo	cal Realm: AnyConnect-Local-Aut Dyna	mic Access Policy: angsanc2-test
Connection Profile Access Interfaces Advanced								
								0
Name	AAA	Edit Connection Pro	file			7 ×		
DefaultWEBVPNGroup	Authent Authoria Account	Edit Group Policy				? ×		/8
SSL_AnyConnect_LocalAuth	Authent	Name:* AnyCo	onnect_Local_Auth			Auth		Ø 6
	Account	Description:						
SSL_AnyConnect_LDAPAUth	Authent	General AnyConne	ect Advanced			Add AnyConnect Cus	tom Attribute	? ×
	M600905	Profile Management Profile Clinit Modules Add C SSL Settings Conrection Set Custom Attribut Custom Attribut	AnyConnect Custom Attribue ustoom Attribute Connect Attribute Connect Attribute.* Dynam tom Attribute Object.*	ute feature allows a more This feature is supported mic Split Tunneling	e expedited very of configu on TID 7.0 ensered. ? × V Cancel Save	Name:* Description: AnyConnect Attribute:* Include domains: Exclude domains: Allow Overrides	Dynamic Split Tunneling Configure comma separated domain names that will be included in the Remote Access VPN Tunnel. Configure comma separated domain names that will be excluded from the Remote Access VPN Tunnel.	
					Save		Save	Cancel

이 예에서는 cisco.com을 제외할 도메인으로 구성하고 이미지에 표시된 대로 사용자 지정 특성 Dynamic-Split-Tunnel을 명명했습니다.

Add AnyConnect Custor	m Attribute		? ×
Name:*	Dynamic-Split-Tunnel		
AnyConnect Attribute:* Include domains:	Dynamic Split Tunneling Configure comma separated domain names that will included in the Remote Access VPN Tunnel	► be	
Exclude domains:	cisco.com		
Allow Overrides			
	Save	Car	ncel

3단계. 컨피그레이션 확인, 저장 및 구축

구성된 사용자 지정 특성이 올바른지 확인하고 컨피그레이션을 저장하고 변경 사항을 문제의 FTD에 배포합니다.

dd Group Policy				?
lame:*	nyconnect_Local_Auth			
escription:				
General AnyCo	Advanced	0		
hofile Nanagement Profile Slient Modules	AnyConnect (endpoint feat	Custom Attribute featu ures on FTD. This feat	re allows a more expedited way of are is supported on FTD 7.0 onward	configuring new ds.
SL Settings	Attribute	Name	Content	
Sustom Attributes	Dynamic Sp Tunneling	lit Dynamic-Split.	Include domains: None Exclude domains: cisco.com	18
			6	>
			Save	Cancel

다음을 확인합니다.

CLI(Command Line Interface)를 통해 FTD에서 다음 명령을 실행하여 동적 스플릿 터널 컨피그레 이션을 확인할 수 있습니다.

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy <그룹 정책의 이름>

이 예에서 컨피그레이션은 다음과 같습니다.

ftd# show run group-policy Anyconnect_Local_Auth group-policy Anyconnect_Local_Auth attributes vpn-idle-timeout 30 vpn-simultaneous-logins 3 vpn-session-timeout none vpn-filter none vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelspecified ipv6-split-tunnel-policy-tunnelall split-tunnel-network-list value AC_networks Default-domain none split-dns none address-pools value AC_pool anyconnect-custom dynamic-split-exclude-domains value cisco.com anyconnect-custom dynamic-split-include-domains none ftd# show run webvpn webvpn enable outside anyconnect-custom-attr dynamic-split-exclude-domains anyconnect-custom-attr dynamic-split-include-domains http-headers hsts-server enable max-age 31536000 include-sub-domains no preload hsts-client enable content-security-policy anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows" anyconnect profiles xmltest disk0:/csm/xmltest.xml anyconnect enable tunnel-group-list enable cache disable certificate-group-map cert_map_test 10 cert_auth error-recovery disable 클라이언트에서 구성된 동적 터널 제외를 확인하려면 다음을 수행합니다.

1. AnyConnect 소프트웨어를 실행하고 그림과 같이 톱니바퀴 모양 아이콘을 클릭합니다.



2. VPN > Statistics(통계)로 이동하여 Dynamic Split Exclusion/Inclusion(동적 분할 제외/포함) 아래 에 표시된 도메인을 확인합니다.

🚳 Cisco AnyConnect Secure Mobility Client			×
cisco AnyConnect	Secure Mobility Client		()
Status Overview	Virtual Private Network (VPN)		
VPN >	Preferences Statistics Route Details Firewall Message History		
Network	Connection Information	^	^
System Scan	Tunnel Mode (IPv4): Split Include		
Roaming Security	Tunnel Mode (IPv6): Drop All Traffic Dynamic Tunnel Exclusion: cisco.com Dynamic Tunnel Inclusion: Nene		
	Duration: 00:00:25 Session Disconnect: None Management Connection State: Disconnected (user tunnel active) Address Information Client (IPv4): Client (IPv6): Server:	~	
Collect diagnostic information for all installed components.	Bytes Reset	Export Stats.	•

문제 해결

AnyConnect Diagnostics and Reporting Tool(DART)을 사용하여 AnyConnect 설치 및 연결 문제를 해결하는 데 유용한 데이터를 수집할 수 있습니다.

DART는 Cisco TAC(Technical Assistance Center) 분석을 위해 로그, 상태 및 진단 정보를 취합하며 클라이언트 시스템에서 실행하는 데 관리자 권한이 필요하지 않습니다.

와일드카드가 AnyConnect 사용자 지정 특성(예: ***.cisco.com)**에 구성된 경우 AnyConnect 세션의 연결이 끊어집니다.

솔루션

cisco.com 도메인 값을 사용하여 와일드카드 대체를 허용할 수 있습니다. 이 변경을 통해 www,cisco.com 및 tools.cisco.com과 같은 도메인을 포함하거나 제외할 수 있습니다.

관련 정보

- 추가 지원이 필요한 경우 TAC(Technical Assistance Center)에 문의하십시오. 유효한 지원 계 약이 필요합니다. <u>Cisco 전 세계 지원 문의처.</u>
- 또한 Cisco VPN Community를 방문하여 <u>여기</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.