보안 클라이언트에 대한 로컬 LAN 액세스 구성

목차

소개 <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>배경 정보</u> <u>구성</u> <u>FMC 컨피그레이션</u> <u>보안 클라이언트 컨피그레이션</u> <u>다음을 확인합니다.</u> <u>보안 클라이언트</u> <u>FTD CLI</u> <u>문제 해결</u>

소개

이 문서에서는 Cisco Secure Client가 로컬 LAN에 액세스하고 헤드엔드에 대한 보안 연결을 계속 유지하도록 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco FMC(Secure Firewall Management Center)
- Cisco FTD(Firepower 위협 방어)
- CSC(Cisco Secure Client)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Firewall Management Center Virtual Appliance 버전 7.3
- Cisco Firepower Threat Defense Virtual Appliance 버전 7.3
- Cisco Secure Client 버전 5.0.02075

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

이 문서에 설명된 컨피그레이션을 통해 Cisco Secure Client는 로컬 LAN에 대한 모든 액세스 권한 을 가지면서 헤드엔드 및 기업 리소스에 대한 보안 연결을 유지할 수 있습니다. 클라이언트가 NAS(Network Access Server)를 인쇄하거나 액세스할 수 있도록 하는 데 사용할 수 있습니다.

구성

FMC 컨피그레이션

이 문서에서는 이미 작동하는 원격 액세스 VPN 컨피그레이션이 있는 것으로 가정합니다.

로컬 LAN 액세스 기능을 추가하려면 Devices(디바이스) > Remote Access(원격 액세스)로 이동하고 적절한 원격 액세스 정책에서 Edit(수정) 버튼을 클릭합니다.

	Firewall Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹	•	° 0	admin ~	cisco SECURE
													Add
Nar	ne		Status				Last Modified						
AC	Policy		Targeting Up-to-dat	1 devices te on all targe			2023-07-18 11:55:56 Modified by "admin"					· · ·	ì

그런 다음 Advanced(고급) > Group Policies(그룹 정책)로 이동합니다.

Firewall Managemen Devices / VPN / Edit Advance	nt Center	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹ (¢ ۹	ŧ 0	admin ~	cisco	SECURE
AC-Policy													Save	Cancel
Enter Description														
												Polic	cy Assignm	ients (1)
								Local Realm: L	OCAL			Dynamic Ar	ccess Polic	sy: None
Connection Profile Access Inte	rfaces Advand	ced												
Secure Client Images	Group Policie	s												
✓ Secure Client Customization	Group policy can	be assigned to	VPN user throug	gh connection	profile or by RA	ADIUS server d	uring authentication.							
GUI Text and Messages	Following are the	group policies t	hat are associa	ted with this R	emote Access	VPN configurat	ion. Add a group pol	licy if it is required to	be assig	ned by	RADIUS	S server durin	ig authentic	ation.
Icons and Images														+
Scripts	Name		F	Protocol			DNS Servers		VPN	Filter				
Binaries														
Custom Installer Transforms	LocalLAN		S	SL,IKEV2										/ •
Localized Installer Transforms	BlueGP		s	SL,IKEV2										11
Address Assignment Policy	RedGP		s	SL.IKEV2										13
Certificate Maps														
Group Policies														
LDAP Attribute Mapping														
Load Balancing														

로컬 LAN 액세스를 구성하려는 그룹 정책에서 Edit(편집) 버튼을 클릭하고 Split Tunneling(스플릿 터널링) 탭으로 이동합니다.

Edit Group Policy

Name:*	
LocalLAN	
Description:	
General Secure (Client Advanced
VPN Protocols	IPv4 Split Tunneling:
IP Address Pools	Allow all traffic over tunnel
Banner	IPv6 Split Tunneling:
DNS/WINS	Allow all traffic over tunnel
Split Tunneling	Split Tunnel Network List Type: Standard Access List Extended Access List
	Standard Access List:
	• +
	DNS Request Split Tunneling
	DNS Requests:
	Send DNS requests as per split t▼
	Domain List:
	Cancel
	Cancer

IPv4 Split Tunneling(IPv4 스플릿 터널링) 섹션에서 Exclude networks specified below(아래에 지정 된 네트워크 제외) 옵션을 선택합니다. Standard Access List(표준 액세스 목록) 선택을 묻는 메시지 가 표시됩니다.

8

Edit Group Policy

Name:*	
LocalLAN	
Description:	
General Secu	ure Client Advanced
VPN Protocols	IPv4 Split Tunneling:
IP Address Pools	Exclude networks specified belo
Banner	IPv6 Split Tunneling:
DNS/WINS	Allow all traffic over tunnel
Split Tunneling 🏮	Split Tunnel Network List Type: Standard Access List Extended Access List
	Standard Access List:
	• +
	DNS Request Split Tunneling
	DNS Requests:
	Send DNS requests as per split t▼
	Domain List:
L	
	Cancel

새 표준 액세스 목록을 만들려면 + 버튼을 클릭합니다.

Edit Standard Acces	s List Object			0
Name LocalLAN-Access				
▼ Entries (0)				
				Add
Sequence No	Action	Network		
	No record	ls to display		
Allow Overrides				
			Cancel	Save

Add(추가) 버튼을 클릭하여 Standard Access List Entry(표준 액세스 목록 항목)를 생성합니다. 이 항목의 Action(작업)을 Allow(허용)로 설정해야 합니다.

Add Standard Access List Ent	ry		0
Action: Allow ▼ Network: Available Network C ↓ Q Search PC2828 Router-1 Router-2 Routersub10 Sub1 Sub2 Sub3 Subi3 Subit50	Add	Selected Network	Add
		Cancel	Add

새 네트워크 객체를 추가하려면+ 버튼을 클릭합니다. 이 객체가 Network(네트워크) 섹션에서 Host(호스트)로 설정되어 있는지 확인하고 상자에 0.0.0.0을 입력합니다.

Edit Network Object		?
Name LocalLAN Description Network O.0.0.0) FQDN	
Allow Overrides		
	Cancel	Save

저장 버튼을 클릭하고 새로 만든 개체를 선택합니다.

Add Standard Access List Ent	ry		0
Action: Allow Allow Action: Network: Available Network C Available Network C Available Network C Action NS-GW NS-GW NS1 NS2 NS3 PC2828 Router-1	Add	Selected Network	
Router-2 Routersub10		Enter an IP address	Add
		Cancel	Add

Add(추가) 버튼을 클릭하여 Standard Access List(표준 액세스 목록) 항목을 저장합니다.

Edit Standard Acces	s List Object			0
Name LocalLAN-Access				
▼ Entries (1)				
				Add
Sequence No	Action	Network		
1	🚭 Allow	LocalLAN		11
Allow Overrides				
			Cancel	Save

Save(저장) 버튼을 클릭하면 새로 생성된 표준 액세스 목록이 자동으로 선택됩니다.

Edit Group Policy

Name:*	
LocalLAN	
Description:	
General Secure	Client Advanced
VPN Protocols	IPv4 Split Tunneling:
IP Address Pools	Exclude networks specified belo [,] ▼
Banner	IPv6 Split Tunneling:
DNS/WINS	Allow all traffic over tunnel
Split Tunneling	Split Tunnel Network List Type:
	Standard Access List
	LocalLAN-Access +
	DNS Request Split Tunneling
	DNS Requests:
	Send DNS requests as per split t▼
	Domain List:
	Cancel

Save(저장) 버튼을 클릭하고 변경 사항을 구축합니다.

보안 클라이언트 컨피그레이션

기본적으로 Local LAN Access(로컬 LAN 액세스) 옵션은 User Controllable(사용자 제어 가능)으로 설정됩니다. 옵션을 활성화하려면 Secure Client GUI에서 Gear(기어) 아이콘을 클릭합니다.

8

S Cisco Secu	re Client	_		\times
	AnyConnect VPN: Ready to connect. Testing-Deploy	×	Connect	
\$ ①				-ili-ili- cisco

Preferences(기본 설정)로 이동하고 Allow local (LAN) access when using VPN (if configured)(VPN 사용 시 로컬(LAN) 액세스 허용(구성된 경우)) 옵션이 활성화되었는지 확인합니다.



다음을 확인합니다.

보안 클라이언트

보안 클라이언트를 사용하여 헤드엔드에 연결합니다.

🕲 Cisco Secu	re Client	-	
	AnyConnect VPN: Connected to FTD FTD		Disconnect
00:00:20			IPv4
\$ ()			clisco

기어 아이콘을 클릭하고 Route Details(경로 세부사항)로 이동합니다. 여기서 로컬 LAN이 자동으로 탐지되고 터널에서 제외됨을 확인할 수 있습니다.

S Cisco Secure Client		-	\times
cisco	Secure Client		0
Virtual Private Network (VPN) Preferences Statistics Route Details Firewall Message History			
	The walk Pressage Thistory		٦
Non-Secured Routes (IPv4)			 •
10.28.28.0/24			
Secured Routes (IPv4)			`
0.0.0/0			

FTD CLI

컨피그레이션이 성공적으로 적용되었는지 확인하려면 FTD의 CLI를 사용할 수 있습니다.

<#root>

firepower#

show running-config group-policy LocalLAN

group-policy LocalLAN internal group-policy LocalLAN attributes banner value Local LAN Access is allowed wins-server none dns-server none dhcp-network-scope none vpn-simultaneous-logins 3 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ikev2 ssl-client split-tunnel-policy excludespecified ipv6-split-tunnel-policy tunnelall split-tunnel-network-list value LocalLAN-Access default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools value AC_Pool webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20 anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value none anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable

문제 해결

로컬 LAN 액세스 기능이 적용되었는지 확인하려면 다음 디버그를 활성화할 수 있습니다.

debug webvpn anyconnect 255

다음은 성공적인 디버그 출력의 예입니다.

<#root>

firepower# debug webvpn anyconnect 255 Validating the session cookie... Processing CSTP header line: 'webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05' Found WebVPN cookie: 'webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05' WebVPN Cookie: 'webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05' Cookie validation successfull, session authenticated http_parse_cstp_method() ...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1' webvpn_cstp_parse_request_field() ...input: 'Host: ftdv-cehidalg.cisco.com' Processing CSTP header line: 'Host: ftdv-cehidalg.cisco.com' webvpn_cstp_parse_request_field() ...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 5.0.02075' Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 5.0.02075' Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 5.0.02075' webvpn_cstp_parse_request_field() ...input: 'Cookie: webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05' Processing CSTP header line: 'Cookie: webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31B Session already authenticated, skip cookie validation webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Version: 1' Processing CSTP header line: 'X-CSTP-Version: 1' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Hostname: DESKTOP-LPMOG6M' Processing CSTP header line: 'X-CSTP-Hostname: DESKTOP-LPMOG6M' Setting hostname to: 'DESKTOP-LPMOG6M' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-MTU: 1399' Processing CSTP header line: 'X-CSTP-MTU: 1399' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Address-Type: IPv6, IPv4' Processing CSTP header line: 'X-CSTP-Address-Type: IPv6, IPv4' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Local-Address-IP4: 10.28.28.7' Processing CSTP header line: 'X-CSTP-Local-Address-IP4: 10.28.28.7' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Base-MTU: 1500' Processing CSTP header line: 'X-CSTP-Base-MTU: 1500' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Remote-Address-IP4: 10.28.28.10' Processing CSTP header line: 'X-CSTP-Remote-Address-IP4: 10.28.28.10' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Full-IPv6-Capability: true' Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true' webvpn_cstp_parse_request_field() ...input: 'X-AnyConnect-STRAP-Pubkey: MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEkzG6nj9HDKz/zLa3Yz+QJDHOYWfT6 Processing CSTP header line: 'X-AnyConnect-STRAP-Pubkey: MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEkzG6nj9HDK Setting Anyconnect STRAP rekey public key(len: 124): MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEkzG6nj9HDKz/zL webvpn_cstp_parse_request_field() ...input: 'X-AnyConnect-STRAP-Verify: MEQCICzX1yDWLXQHnl0hOXV+/0I1/0lLjBic/Nu/K2+N6E5GAiA5CLAF6Bt0tcxhj Processing CSTP header line: 'X-AnyConnect-STRAP-Verify: MEQCICzX1yDWLXQHn10h0XV+/0I1/01LjBic/Nu/K2+N6E Setting Anyconnect STRAP client signature(len: 96): MEQCICzX1yDWLXQHnl0h0XV+/0I1/0lLjBic/Nu/K2+N6E5GAiA webvpn_cstp_parse_request_field() ...input: 'X-DTLS-Master-Secret: 0224D83639071BBF29E2D77B15B762FE85BD50D1F0EF9758942B75DF9A97C709325C3E Processing CSTP header line: 'X-DTLS-Master-Secret: 0224D83639071BBF29E2D77B15B762FE85BD50D1F0EF9758942 webvpn_cstp_parse_request_field() ...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-GCM-SHA25 Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-R Skipping cipher selection using DTLSv1 since a higher version is set in ssl configuration webvpn_cstp_parse_request_field() ...input: 'X-DTLS12-CipherSuite: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AE Processing CSTP header line: 'X-DTLS12-CipherSuite: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM- Selecting cipher using DTLSv1.2 webvpn_cstp_parse_request_field() ...input: 'X-DTLS-Accept-Encoding: lzs' Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs' webvpn_cstp_parse_request_field() ... input: 'X-DTLS-Header-Pad-Length: 0' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Accept-Encoding: lzs,deflate' Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.' Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.' cstp_util_address_ipv4_accept: address asigned: 172.16.28.15 cstp_util_address_ipv6_accept: No IPv6 Address np_svc_create_session(0xF36000, 0x000014d37b17c080, TRUE) webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 No SVC ACL Iphdr=20 base-mtu=1500 def-mtu=1500 conf-mtu=1406 tcp-mss = 1460path-mtu = 1460(mss)TLS Block size = 16, version = 0x304mtu = 1460(path-mtu) - 0(opts) - 5(ssl) = 1455mod-mtu = 1455(mtu) & 0xfff0(complement) = 1440 tls-mtu = 1440(mod-mtu) - 8(cstp) - 32(mac) - 1(pad) = 1399 DTLS Block size = 16 mtu = 1500(base-mtu) - 20(ip) - 8(udp) - 13(dt]shdr) - 16(dt]siv) = 1443 mod-mtu = 1443(mtu) & 0xfff0(complement) = 1440 dtls-mtu = 1440(mod-mtu) - 1(cdtp) - 48(mac) - 1(pad) = 1390 computed tls-mtu=1399 dtls-mtu=1390 conf-mtu=1406 DTLS enabled for intf=2 (outside) tls-mtu=1399 dtls-mtu=1390 SVC: adding to sessmgmt Sending X-CSTP-Split-Exclude msgs: for ACL - LocalLAN-Access: Start Sending X-CSTP-Split-Exclude: 0.0.0.0/255.255.255.255 Sending X-CSTP-MTU: 1399 Sending X-DTLS-MTU: 1390 Sending X-DTLS12-CipherSuite: ECDHE-ECDSA-AES256-GCM-SHA384 Sending X-CSTP-FW-RULE msgs: Start Sending X-CSTP-FW-RULE msgs: Done Sending X-CSTP-Quarantine: false Sending X-CSTP-Disable-Always-On-VPN: false Sending X-CSTP-Client-Bypass-Protocol: false

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.