모바일 액세스를 위한 Anyconnect 인증서 기반 인증 구성

목차

<u>문제 해결</u>

<u>디버그</u>

소개

이 문서에서는 모바일 디바이스에서 인증서 기반 인증을 구현하는 예를 설명합니다.

사전 요구 사항

이 가이드에서 사용하는 도구 및 장치는 다음과 같습니다.

- Cisco FTD(Firepower 위협 방어)
- FMC(Firepower Management Center)
- Apple iOS 장치(iPhone, iPad)
- CA(인증 기관)
- Cisco Anyconnect 클라이언트 소프트웨어

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 VPN
- SSL/TLS
- 공개 키 인프라
- FMC 경험
- OpenSSL

Cisco Anyconnect

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD
- Cisco FMC
- Microsoft CA 서버
- XCA
- Cisco Anyconnect
- 애플 아이패드

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.

FTD에서 Cisco Anyconnect 구성

이 섹션에서는 FMC를 통해 Anyconnect를 구성하는 단계를 설명합니다. 시작하기 전에 모든 컨피 그레이션을 구축해야 합니다.

네트워크 다이어그램



FTD에 인증서 추가

1단계. FMC 어플라이언스에서 FTD에 대한 인증서를 생성합니다. 다음 이미지에 표시된 대로 Devices > Certificate(디바이스 > 인증서)로 이동하고 Add(추가)를 선택합니다.

Firepower Management Center Devices / Certificates	Overview Ar	nalysis Policies	Devices Objects	AMP	Intelligence		Q D	eploy 🚱	🗘 🛛 adn	nin •
	-									80
Name	Domain	Enrollment Type	Status							
V=FTD1										
FTD	Global	Manual (CA & ID)	CA LD					G	2 C 🗑	
✓ I Tcoutrie-FTD2										
ftd2	Global	PKCS12 file	CA ID					G	• 🕑 C 🗑	
					How To					

2단계. VPN 연결에 필요한 FTD를 선택합니다. 디바이스 드롭다운에서 FTD 어플라이언스를 선택 합니다. 다음 이미지에 표시된 것처럼 새 인증서 등록 방법을 추가하려면 + 아이콘을 클릭합니다.

← → C @ O A https:	//tcoutrie-fmc.tcoutrie-	security301.com/ddd/#P	KiCerificate	☆	© <u>±</u> ⊫		B 0	= 🐮 =
Octing Started C School C Work							(Other Bookmarks
CISCO Devices / Certificates	Overview Ar	nalysis Policies	Devices Objects AMP Intelligence		٩	Deploy	ې 🍪	🕒 admin 🕶
								Add
Name	Domain	Enrollment Type	Status					
~ ➡ FTD1								
FTD	Global	Manual (CA & ID)	(s_CA) (s_10)				B• 💰	2 C T
V Tcoutrie-FTD2								
ftd2	Global	PKCS12 file	Add New Certificate				G• 💰	2 C 🗑
			Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.					
			How To					

3단계. 디바이스에 인증서를 추가합니다. 환경에서 인증서를 얻기 위해 선호하는 방법인 옵션을 선 택합니다. ✔ 팁: 사용 가능한 옵션은 다음과 같습니다. Self Signed Certificate - Generate a new certificate locally(자체 서명 인증서 - 로컬에서 새 인증서 생성), SCEP - Use Simple Certificate Enrollment Protocol to obtain a certificate from a CA(SCEP(단순 인증서 등록 프로토콜 사용), Manual(수동) - Root and Identity certificate(루트 및 ID 인증서) 수동 설치, PKCS12 - Upload encrypted certificate bundle with root(루트, ID 및 개인 키로 암호화된 인증서 번들 업 로드)

4단계. FTD 디바이스에 인증서를 업로드합니다. 다음 이미지에 표시된 대로 암호(PKCS12에만 해 당)를 입력하고 Save(저장)를 클릭합니다.

Add Cert Enrollme	ent	?
Name* ftdcert Description		
CA Information	Certificate Parameters Key Revocation	
Enrollment Type:	PKCS12 File	
PKCS12 File*:	Tcoutrie-ftd2.p12 Browse PKCS12 File	
Passphrase:	······ (C)	
	Skip Check for CA flag in basic constraints of the CA Certifi	icate
	Cancel	Save

참고: 파일을 저장하면 인증서 구축이 즉시 수행됩니다. 인증서 세부사항을 보려면 ID를 선택 합니다.

Cisco Anyconnect 구성

원격 액세스 마법사로 FMC를 통해 Anyconnect를 구성합니다.

1단계. 원격 액세스 VPN 정책 마법사를 시작하여 Anyconnect를 구성합니다.

Devices(디바이스) > Remote Access(원격 액세스)로 이동하고 Add(추가)를 선택합니다.

tice: Firepower Management Center Overview Analys	is Policies Devices	Objects AMP	Intelligence		Q	Deploy	6° ¢ (admin •
							-	Add
Name	Status			Last Modified				
RAVPN	Targeting 1 device Up-to-date on all	es targeted devices		2021-07-09 17:10:31 Modified by "admin"		/ 1		
			How To					

2단계. 정책 할당.

정책 할당을 완료합니다. a. 정책의 이름을 지정합니다.

b. 원하는 VPN 프로토콜을 선택합니다.

c. 컨피그레이션을 적용할 대상 디바이스를 선택합니다.

Remote Access VPN Policy Wizard Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary	ary
Targeted Devices and Protocols This withard will guide you through the required minimal steps to Access VPH policy with a new user-defined connection profile. This This Description: Description:	Image: Second
	How To

3단계. 연결 프로파일.

a. 연결 프로파일의 이름을 지정합니다. b. 인증 방법을 클라이언트 인증서 전용으로 설정합니다.

c. IP 주소 풀을 할당하고, 필요한 경우 새 그룹 정책을 생성합니다.

d. 다음을 클릭합니다.

Remote Access VPN Policy Wizard	
1 Policy Assignment 2 Connection Profile 3	An/Contect 0 Access & Carthoute 5 Summary
	Synthesis Prome
	Connection Profile search products acceled products and a VM connection. These applicies partners to creating the turner attack two and As a concentration and the addresses are assessed.
	This name is configured as a connection alias, it can be used to connect to the VPN gateway
	Authentication, Authoritation & Accounting (AAA):
	Specify the method of authentication (AAA, conflicters or both), and the AAA servers that will be used for VPN connections.
	Automication Memoria Clavet Centralization Only *
	Username Finn 🔹 Map specific field 🔿 Use entrie DN (Distriguished Yame) as username
	Primary Fluid: (CN ICommon Name) •
	Secondary Field: None +
	Authorization Server:
	Accounting Server:
	Client Address Assignment:
	Client IP address can be assigned from AAA server, CHCP server and IP address pools. When multiple options are selected, IP address assignment to tried in the order of AAA server, CHCP server and IP address pool.
	🕑 Uxe IP Address Pools
	Bud Address Prote: RWIN
	Bv4 Address Peole
	Group Policy:
	A group policy is a collection of user-viented sexion attributes which are assigned to client when a VPN connection is established. Series of our dept.
	Group Policy* (Ethologiabeley +) +
	Edit Group Policy

✤ 참고: 인증 세션의 사용자 이름을 입력하는 데 사용할 기본 필드를 선택합니다. 이 설명서에서 는 인증서의 CN을 사용합니다.

4단계. AnyConnect.

어플라이언스에 Anyconnect 이미지를 추가합니다. Anyconnect의 기본 버전을 업로드하고 Next(다음)를 클릭합니다.

≫ 참고: Cisco Anyconnect 패키지는 Software.Cisco.com에서 다운로드할 수 있습니다.

5단계. 액세스 및 인증서.

이 이미지에 표시된 대로 인터페이스에 인증서를 적용하고 인터페이스 레벨에서 Anyconnect를 활성화하고 Next(다음)를 클릭합니다.

📫 Firefox File Edit View History Bookmarks Tools Window Help			0 0 6 6 6 0 0	💰 📷 🖙 💿 🍳 📰 🤌 Fri Jul 30 10:40 AM
● ● ●				
← → C @ D https://tcoutrie-fmc.tcoutrie-security301.co	n/ddd/#RAVpnSetupWizard		☆	S 7 W E 8 S 9 = 1 =
Getting Started D School D Work				C Other Bookmarks
CISCO Devices / VPN / Setup Wizard Overview Analysis Pr	licies Devices Objects AMP Intelligence			् Deploy 💕 🌣 🕼 admin 🕶
Remote Access VPN Policy Wizard				
Policy Assignment 2 Connection Profile 3 AnyConnect	Access & Certificate 5 Summary			
Remote User	AnyConnect Client	e vpn Inside	Corporate Resources	
	Network Interface for Incoming VPN Access			
	Select or create an Interface Group or a Security Zone that con will access for VPN connections.	tains the network interfaces users		
	Interface group/Security Zone:" outside	+ +		
	All the devices must have interfaces as part of the Interface	e Group/Security Zone selected.		
	Device Certificates			
	Device certificate (also called identity certificate) identifies the clients. Select a certificate which is used to authenticate the VP	/PN gateway to the remote access N gateway.		
	Certificate Enrollment:* ftd2	• +		
	Enroll the selected cert	ficate object on the target devices		
	Access Control for VPN Traffic			
	All decrypted traffic in the VPN tunnel is subjected to the Acces this option to bypass decrypted traffic from the Access Control	s Control Policy by default. Select Policy.		
			How To	Cancel

6단계. 요약.

구성을 검토합니다. 모두 체크 아웃한 경우 마침을 클릭한 다음 구축합니다.

모바일 사용자를 위한 인증서 만들기

연결에 사용되는 모바일 디바이스에 추가할 인증서를 만듭니다.

1단계. XCA.

a. XCA 열기

b. 새 데이터베이스 시작

2단계. CSR을 생성합니다.

a. CSR(Certificate Signing Request)을 선택합니다.

b. 신규 요청을 선택합니다

c. 인증서에 필요한 모든 정보가 포함된 값을 입력합니다

d. 새 키 생성

e. 완료되면 OK(확인)를 클릭합니다.

	💞 X Certificate and Key	/ management		
Create Certificate signing request				3 Deriver
Source	Extensions Key u	usage Netscape	Advanced	
Distinguished name				
Internal name	organ	nizationName		
countryName	orgar	nizationalUnitName		
stateOrProvinceName	comr	nonName	Cisco_Test	
localityName	email	Address		
Туре		Content		Add
				Delete
Private key				
Cisco Test 1 (PSA:2048 bit)			too Genera	te a new key
			Genera	te a new key
			С	ancel OK

참고: 이 문서에서는 인증서의 CN을 사용합니다.

3단계. CSR을 제출합니다.

a. CSR 내보내기

b. CA에 CSR을 제출하여 새 인증서 받기

•	• •	I	X Certificate and Key management	
		Private Keys	Certificates Templates Revocation lists	
	Internal name A commonName Signed			New Request
				Export
				Import
				Show Details
				Delete
				D Forminecta Dividence Time
Da	tabase: /Users/tcoutrie/cisco.xdb		Search	

참고: CSR의 PEM 형식을 사용합니다.

모바일 장치에 설치

1단계. 모바일 디바이스에 디바이스 인증서를 추가합니다. 2단계. Anyconnect 애플리케이션과 인증서를 공유하여 새 인증서 애플리케이션을 추가합니다.

⚠️ 주의: 수동으로 설치하려면 사용자가 인증서를 응용 프로그램과 공유해야 합니다. MDM을 통 해 푸시되는 인증서에는 적용되지 않습니다.

C Documents		certs	Ē	9 🔡 Select
Q Search				Ŷ
Cisco_Test.p1	DMChain.p7b	DMS	Certificate Personal Control	Certificate Personal
Сору	Ф	4/25/21, 1:50 1 KB	driod.p12 5/13/21, 7:04	driod_1.p12 5/13/21, 7:05
Duplicate	æ		4 ND	4 ND
Move		Certificate	Certificate	Certificate
Delete	觉	Personal	Personal 🚇	Personal 💕
t Info		Noblesse_IPA D_2.p12	Noblesse_IPh one.p12	Noblesse_IPh one_1.p12
Quick Look	۲	4/25/21, 11:18 4 KB	4/25/21, 10:31 3 KB	4/25/21, 11:01 4 KB
Tags	0			
Rename	1	Certificate Perional	Certificate Personal	Certificate Personal
, Share	Û	Noblesse_MA	Noblesse_Wi	Noblesse_Wi
Compress		C_2.p12 4/25/21, 11:19 4 KB	ndows.p12 4/25/21, 12:56 3 KB	ndowsIKE.p12 5/12/21, 12:42 4 KB

3단계. PKCS12 파일의 인증서 비밀번호를 입력합니다.

4단계. Anyconnect에서 새 연결을 생성합니다.

5단계. Connections(연결) > Add VPN Connection(VPN 연결 추가)으로 이동합니다.

AnyConnect	VPN Connections
PRIMARY VIRTUAL PRIVATE NETWORK	
AnyConnect VPN	CALO Enabled
Connections CALO >	HOMEIKE
Details Disconnected >	HOMEIKE-IN
GENERAL	HOMESSL-IN
Settings >	HomelPEC-IN
Diagnostics >	HomelPSEC
About >	HomeSSL
	rtp-vpn-cluster.cisco.com
	Add VPN Connection
cisco	

6단계. 새 연결에 대한 정보를 입력합니다.

설명: 연결의 이름

서버 주소: FTD의 IP 주소 또는 FQDN

고급: 추가 구성

7단계. 고급을 선택합니다.

8단계. Certificate(인증서)를 선택하고 새로 추가한 인증서를 선택합니다.

Any	Connect	VPN	VPN Connections			
PRIMARY VIRTUA	L PRIVATE NETWOR	rk l				
AnyConnect V	PN (Advanced Select Certificate		i		
Connections	FT			(j)		
Details	Disconnecte	Disabled		0		
		Selecting this option will disable certificate authentication	on.	i		
		Automatic		í		
GENERAL		This will automatically select a certificate for authentica	tion.			
Settings		Noblesse_IPAD		(1)		
Diagnostics		Issuer: DMsliders-TCOUTRIE-SRV-CA		i		
		Cisco_Test		(i)		
About		Issuer: DMsliders-TCOUTRIE-SRV-CA	(i) >	0		
		Expiration Date: Aug 02, 2022 08:12:47		(i)		
		Issuer: DMsliders-TCOUTRIE-SRV-CA	(i) >	i		
		Expiration Date: Apr 25, 2022 11:04:38				
		Noblesse_IPAD	(i) >			
		Expiration Date: Apr 25, 2022 00:42:05				
	nd n					
CI	sco					

9단계. 다시 Connections and test(연결 및 테스트)로 이동합니다.

성공하면 토글이 계속 켜져 있으며 세부 정보가 연결된 상태로 표시됩니다.



다음을 확인합니다.

show vpn-sessiondb detail Anyconnect 명령은 연결된 호스트에 대한 모든 정보를 표시합니다.

🔎 팁: 이 명령을 추가로 필터링하는 옵션은 명령에 추가된 'filter' 또는 'sort' 키워드입니다.

예를 들면 다음과 같습니다.

Tcoutrie-FTD3# show vpn-sessiondb detail Anyconnect

Username : Cisco_Test Index : 23 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Protocol : Anyconnect-Parent SSL-Tunnel DTLS-Tunnel License : Anyconnect Premium, Anyconnect for Mobile Encryption : Anyconnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hash : Anyconnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Bytes Tx : 8627 Bytes Rx : 220 Pkts Tx : 4 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : SSL Tunnel Group : SSL Login Time : 13:03:28 UTC Mon Aug 2 2021 Duration : 0h:01m:49s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a7aa95d000170006107ed20 Security Grp : none Tunnel Zone : 0 Anyconnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 Anyconnect-Parent: Tunnel ID : 23.1 Public IP : 10.118.18.168 Encryption : none Hashing : none TCP Src Port : 64983 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : apple-ios Client OS Ver: 14.6 Client Type : Anyconnect Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 6299 Bytes Rx : 220 Pkts Tx : 2 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 23.2 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 64985 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Apple iOS Client Type : SSL VPN Client Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 2328 Bytes Rx : 0 Pkts Tx : 2 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 23.3 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 51003 UDP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Apple iOS Client Type : DTLS VPN Client Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 0 Bytes Rx : 0 Pkts Tx : 0 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

문제 해결

디버그

이 문제를 해결하는 데 필요한 디버깅은 다음과 같습니다.

Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255

연결이 SSL이 아닌 IPSEC인 경우:

Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14

Anyconnect 모바일 애플리케이션의 로그:

Diagnostic(진단) > VPN Debug Logs(VPN 디버그 로그) > Share logs(로그 공유)로 이동합니다.

AnyConnect	Diagnostics
PRIMARY VIRTUAL PRIVATE NETWORK	
AnyConnect VPN	VPN Debug Logs
Connections Asa1 >	Logs
Details Disconnected >	System Information >
	Share Logs
GENERAL	Customize Debug Logs
Settings >	
Diagnostics	Certificates
About >	Profile
	Localization
11 11 11	
CISCO	

다음 정보를 입력합니다.

- 문제
- 재현 단계

그런 다음 Send(보내기) > Share with(공유)로 이동합니다.

3:49 PM Wed Sep 29		•••		奈 47% ■
AnyConnect			Diagnostics	
	DRK			
AnyConnect VPN	Canc	el Share Logs	Send	
Connections As	e Please follow	e describe the problem and steps to r ing fields.	Email logs to	>
Details Disconnecte	PROBL	EM	Administrator	>
GENERAL	Test		Cisco	
Settings	STEPS	TO REPRODUCE	Share with	,
Diagnostics	Test			>
About				>
				>
	The da about addres addres purpos	ata sent is for diagnostic purposes only and configured connections, as well as server a sses, and username. This data will appear to as you specify and will not be used for mark ses.	may contain information nd endpoint identities, IP o come from the email eting or advertising	
cisco				

그러면 이메일 클라이언트를 사용하여 로그를 전송하는 옵션이 표시됩니다.

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.