Configurazione di AAA e Cert Auth per Secure Client su FTD tramite FMC

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Esempio di rete
Configurazioni
Configurazione in FMC
Passaggio 1. Configura interfaccia FTD
Passaggio 2. Conferma licenza Cisco Secure Client
Passaggio 3. Aggiungi assegnazione criteri
Passaggio 4. Dettagli configurazione per profilo connessione
Passaggio 5. Aggiungi pool di indirizzi per profilo di connessione
Passaggio 6. Aggiungi Criteri di gruppo per il profilo di connessione
Passaggio 7. Configura immagine client sicura per il profilo di connessione
Passaggio 8. Configura accesso e certificato per profilo di connessione
Passaggio 9. Conferma riepilogo per il profilo di connessione
Conferma nella CLI FTD
Conferma in client VPN
Passaggio 1. Conferma certificato client
Passaggio 2. Conferma CA
<u>Verifica</u>
Passaggio 1. Avvia connessione VPN
Passaggio 2. Conferma sessioni attive in FMC
Passaggio 3. Conferma sessione VPN nella CLI FTD
Passaggio 4. Conferma comunicazione con il server
Risoluzione dei problemi
Riferimento

Introduzione

In questo documento viene descritto come configurare Cisco Secure Client over SSL su FTD gestito da FMC con AAA e autenticazione dei certificati.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defense Virtual (FTD)
- Flusso di autenticazione VPN

Componenti usati

- Cisco Firepower Management Center per VMWare 7.4.1
- Cisco Firewall Threat Defense Virtual 7.4.1
- Cisco Secure Client 5.1.3.62

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Con l'adozione di misure di sicurezza più rigorose da parte delle aziende, la combinazione dell'autenticazione a due fattori (2FA) con l'autenticazione basata su certificati è diventata una pratica comune per migliorare la sicurezza e la protezione contro l'accesso non autorizzato. Una delle funzionalità che possono migliorare significativamente l'esperienza e la sicurezza dell'utente è la capacità di precompilare il nome utente in Cisco Secure Client. Questa funzionalità semplifica il processo di accesso e migliora l'efficienza complessiva dell'accesso remoto. Questo documento descrive come integrare un nome utente precompilato con Cisco Secure Client su FTD, garantendo che gli utenti possano connettersi alla rete in modo rapido e sicuro.

Questi certificati contengono un nome comune, utilizzato ai fini dell'autorizzazione.

- CA: ftd-ra-ca-nome-comune
- Certificato client : sslVPNClientCN
- Certificato server : 192.168.1.200

Esempio di rete

Nell'immagine è illustrata la topologia utilizzata per l'esempio del documento.



Esempio di rete

Configurazioni

Configurazione in FMC

Passaggio 1. Configura interfaccia FTD

Selezionare Dispositivi > Gestione dispositivi, modificare il dispositivo FTD di destinazione, configurare l'interfaccia interna ed esterna per FTD nella scheda Interfacce.

Per Gigabit Ethernet0/0,

- Nome : esterno
- Area di sicurezza: outsideZone
- Indirizzo IP: 192.168.1.200/24

Per Gigabit Ethernet0/1,

- Nome : Inside
- Area di sicurezza : insideZone
- Indirizzo IP: 192.168.10.200/24

Firewall Management Center Devices / Secure Firewall Interfaces	Overview	Analysis	Policies Devices	Objects Integration	De	play Q 🚱 🌣	Ø admin ∽ dual cose	SECURE	
1									
All Interfaces Virtual Tunnels					Q, Search by name	s	iync Device Add Int	erfaces ¥	
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router		
Management0/0	management	Physical				Disabled	Global	۹.4	
GigabitEthernet0/0	outside	Physical	outsideZone		192.168.1.200/24(Static)	Disabled	Global	/	
GigabitEthernet0/1	inside	Physical	insideZone		192.168.10.200/24(Static)	Disabled	Global	/	
GigabitEthernet0/2		Physical				Disabled		/	
GigabitEthernet0/3		Physical				Disabled		/	

Interfaccia FTD

Passaggio 2. Conferma licenza Cisco Secure Client

Selezionare Dispositivi > Gestione dispositivi, modificare il dispositivo FTD di destinazione, confermare la licenza Cisco Secure Client nella scheda Dispositivo.

Devices / Secure Firewall Device S	ænter Overview Analy Summary	sis Policies Devices	Objects Integration		Depl	oy Q 💕 🌣 🔕 admin 🗸 "tieste St
sco Firepower Threat Defense for VMv	ware	License			0	
Device Routing Interfaces	Inline Sets DHCP VTEP	License Types				
		Performance Tier:	FTDv5 - 100 Mbps	*		
General	1.4	Essentials:			m	© G
Name:	1.7644.4	Export-Controlled Features:			:	Cisco Firepower Threat Defense for VMware
Transfer Packets:	Ye	Malware Defense:	-			9A33F35ANSU
Troubleshoot:	Logs CLI Download	IPS:				2024-06-14 07:38:47
Mode:	Route	Carrier .			Zone:	UTC (UTC+0:00)
Compliance Mode:	None	Carrier.			n:	7.4.1
Performance Profile:	Defaul	URL:			Zone setting for	UTC (UTC+0:00)
TLS Crypto Acceleration:	Disable	Secure Client Premier:			Jased Rules.	
		Secure Client Advantage:				
Device Configuration:	Import Export Download	Secure Client VPN Only:				
OnBoarding Method:	Registration Ke	If a device already has Secure Client VP	N Only they cannot have			
		Secure Client Premier or Secure Client A has Secure Client Premier or Secure Client	Advantage. If a device ent Advantage it cannot			
Inspection Engine		have Secure Client VPN Only			gement	/ 🜑
Inspection Engine:	Snort				e Host Address:	1.175
Revert to Snort 2				Cancel Save	dary Address:	

Licenza Secure Client

Passaggio 3. Aggiungi assegnazione criteri

Selezionare Dispositivi > VPN > Accesso remoto, quindi fare clic su Aggiungi pulsante.

Firewall Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	¢	° 0	admin	cisco SECURE
													Add
Name				Status			Last Modified						
No configuration available Add a new configuration													

Aggiungi VPN di accesso remoto

Inserire le informazioni necessarie e fare clic su Avanti pulsante.

- Nome : ftdvpn-aaa-cert-auth
- Protocolli VPN: SSL
- Dispositivi di destinazione : 1.x.x.49

Firewall Management Center Overview Analysis Policies Devices Objects Integration		Deploy	۹	¢ 🕹	o adm	in v state S	ECURE
Remote Access VPN Policy Wizard Policy Assignment ② Connection Profile ③ Secure Client ④ Access & Certificate ⑤ Summary Targeted Devices and Protocols This wizard will quide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile. Name*	 Before You Start Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy. 						ĺ
tdvpn-aaa-cert-auth Description: VPN Protocols: SSL IPsec-IKEV2	Authentication Server Configure LOCAL or Realm or RADIUS Server Group or SS0 to authenticate VPN clients. Secure Client Package Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Clico credentials to download it during the wizard. Device Interface						
Targeted Devices:	Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.						
				Ci	incel	Back	

```
Assegnazione criteri
```

Passaggio 4. Dettagli configurazione per profilo connessione

Immettere le informazioni necessarie per il profilo di connessione e fare clic sul pulsante + accanto all'elemento Realm locale.

- Metodo di autenticazione: certificato client e AAA
- Server di autenticazione : LOCAL
- · Nome utente da certificato : Campo specifico del mapping
- Campo primario : CN (nome comune)
- Campo secondario: unità organizzativa

Firewall Management Center Overview Analysis	Policies Devices Objects Integration	Deploy	٩	¢	° 0	admin ~	cisco SECURE
Remote Access VPN Policy Wizard							
1 Policy Assignment 2 Connection Profile 3 Secu	e Client (4) Access & Certificate (5) Summary						
	Connection Profile:						
	Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.						
	Connection Profile Name:* ftdvpn-aaa-cert-auth						
	This name is configured as a connection alias, it can be used to connect to the VPN gateway						
	Authentication, Authorization & Accounting (AAA):						
	Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.						
	Authentication Method: Client Certificate & AAA						
	Authentication Server.* LOCAL + +						
	Local Realm.*						
	Prefil username from certificate on user login window						
	Username From Certificate: Map specific field Use entire DN (Distinguished Name) as username						
	Primary Field: CN (Common Name)						
	Secondary Field: OU (Organisational Unit)						

Dettagli profilo connessione

Fare clic su Locale dall'elenco a discesa Aggiungi realm per aggiungere un nuovo realm locale.

Firewall Management Center Integration / Other Integrations / Realms	Overview Analysis Policies Devices	Objects Integration			Deploy Q 🧬 🌣 🛛 admin - 👘 SECURE
Cloud Services Realms Identity Sources	High Availability eStreamer Host Input Client	Smart Software Manager On-Prem			
Realms Realm Sequences Sync Result	9				
					Compare Realms Add Realm 🗸
Name * Type	Description		Status O	Value	State
LocalRealmTest Local					Enabled Active Directory/LDAP

Aggiungi area di autenticazione locale

Immettere le informazioni necessarie per il realm locale e fare clic su Salva pulsante.

- Nome : LocalRealmTest
- Nome utente : ssIVPNClientCN



Nota: il nome utente è uguale al nome comune nel certificato client

Name* LocalRealmTest	Description
Local User Configuration	
∧ ssIVPNClientCN	
Username sslVPNClientCN	
Password	Confirm Password

0 X

Add another local user

	Cancel Save	1
--	-------------	---

Dettagli del realm locale

Passaggio 5. Aggiungi pool di indirizzi per profilo di connessione

Fare clic sul pulsante Modifica accanto alla voce Pool di indirizzi IPv4.

Client Address Assignment:
Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.
Use AAA Server (Realm or RADIUS only)
Use DHCP Servers
Jse IP Address Pools
IPv4 Address Pools:
IPv6 Address Pools:

Aggiungi pool di indirizzi IPv4

Immettere le informazioni necessarie per aggiungere un nuovo pool di indirizzi IPv4. Selezionare il nuovo pool di indirizzi IPv4 per il profilo di connessione.

- Nome : ftdvpn-aaa-cert-pool
- Intervallo di indirizzi IPv4 : 172.16.1.40-172.16.1.50

•	Maschera:	255	.255	.255.0
---	-----------	-----	------	--------

Add IPv4 Pool

Name* ftdvpn-aaa-cert-pool Description		
IPv4 Address Range* 172.16.1.40-172.16.1.50 Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150		
Mask* 255.255.255.0 Allow Overrides		
 Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices Override (0) 		
	Cancel	Save
Dettagli del pool di indirizzi IPv4 Passaggio 6. Aggiungi Criteri di gruppo per il profilo di connessione		
Fare clic sul pulsante + accanto all'elemento Criteri di gruppo. Group Policy: A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object. Group Policy: Edit Group Policy		
	Cancel	Back Next

Ø

Aggiungi Criteri di gruppo

Immettere le informazioni necessarie per aggiungere un nuovo criterio di gruppo. Selezionare il

nuovo criterio di gruppo per il profilo di connessione.

- Nome : ftdvpn-aaa-cert-grp
- Protocolli VPN: SSL

Add Group Policy

Name:* ftdvpn-aaa-cert-grp	
Description:	
General Secure	Client Advanced
VPN Protocols IP Address Pools Banner DNS/WINS Split Tunneling	VPN Tunnel Protocol: Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel. SSL I Psec-IKEv2

0

Cancel

Save

Dettagli di Criteri di gruppo

Passaggio 7. Configura immagine client sicura per il profilo di connessione

Selezionare il file immagine client sicuro e fare clic su Avanti pulsante.



Seleziona immagine client sicura

Passaggio 8. Configura accesso e certificato per profilo di connessione

Selezionare Area di sicurezza per la connessione VPN e fare clic sul pulsante + accanto all'elemento Registrazione certificato.

· Gruppo di interfacce/Zona di sicurezza : outsideZone

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧬 🌣 🙆 admin ~ 讨 🐝 SECURE
Remote Access VPN Policy Wizard	
1) Policy Assignment (2) Connection Profile (3) Secure Client (4) Access & Certificate (5) Summary	
Remote Secure Client Internet Outside Upp Inside Corporate Resources	
Network Interface for Incoming VPN Access	
Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPM connections.	
Interface group/Security Zone:* outsideZone +	
Enable DTLS on member interfaces	
▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.	
Device Certificates	
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.	
Certificate Enrollment.*	



Immettere le informazioni necessarie per il certificato FTD e importare un file PKCS12 dal computer locale.

- Nome : ftdvpn-cert
- Tipo di registrazione : File PKCS12

Add Cert Enrollment

Name*				-
Description				
CA Information	Certificate Paramet	ers Key Revo	cation	
Eacollmost Tupo:	DVOC10 File			
PKCS12 File*:	ftdCert.ofx	¥	Browse PKCS12 File	
Passphrase*:				
Validation Usage:	IPsec Client	SSL Client 🗌 SS	SL Server	
	Skip Check for	or CA flag in basic con:	straints of the CA Certificate	
			Cancel	
			Gancer	

Aggiungi certificato FTD

Confermare le informazioni immesse nella procedura guidata Accesso e certificati e fare clic su Pulsante Avanti.

3



Nota: abilitare i criteri di controllo di accesso da ignorare per il traffico decrittografato (syspot allow-vpn), in modo che il traffico VPN decrittografato non venga sottoposto all'ispezione dei criteri di controllo di accesso.

Firewall Management Center Overview Analysis Polic Devices / VPN / Setup Wizard Overview	es Devices Objects Integration	Deploy Q 🗳 🌣 🛛 admin 🗸 🕬 SECURE
Remote Access VPN Policy Wizard		
Onnection Profile 3 Secure Client 3	Access & Certificate S Summary	
Remote User	Secure Client Internet Cutation United Composition Produces	
	Network Interface for Incoming VPN Access	
	Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections	
	Interface group/Security Zone:* outsideZone +	
	Enable DTLS on member interfaces	
	All the devices must have interfaces as part of the Interface Group/Security Zone selected.	
	Device Certificates	
	Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.	
	Certificate Enrollment.*	
	Enroll the selected certificate object on the target devices	
	Access Control for VPN Traffic	
	All decrypted trame in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.	
	Physics Access Control policy for decrypted traffic (sysopt permit-ypn) This option bypasses the Access: Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.	
4		·
		Cancel Back Next

Conferma impostazioni in Accesso e certificato

Passaggio 9. Conferma riepilogo per il profilo di connessione

Confermare le informazioni immesse per la connessione VPN e fare clic sul pulsante Fine.



Conferma impostazioni connessione VPN

Confermare il riepilogo dei criteri VPN di accesso remoto e distribuire le impostazioni in FTD.

Cancel
(1)
cy: None
+
/1
/1
cy.

Riepilogo dei criteri VPN di Accesso remoto

Conferma nella CLI FTD

Confermare le impostazioni della connessione VPN nella CLI FTD dopo la distribuzione dal FMC.

// Defines IP of interface interface GigabitEthernet0/0 nameif outside security-level 0 ip address 192.168.1.200 255.255.255.0 interface GigabitEthernet0/1 nameif inside security-level 0 ip address 192.168.10.200 255.255.255.0 // Defines a pool of addresses ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50 mask 255.255.255.0 // Defines a local user username sslVPNClientCN password ***** encrypted // Defines Trustpoint for Server Certificate crypto ca trustpoint ftdvpn-cert keypair ftdvpn-cert crl configure // Server Certificate Chain crypto ca certificate chain ftdvpn-cert certificate 22413df584b6726c 3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7 quit certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 quit // Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images webvpn enable outside http-headers hsts-server enable max-age 31536000 include-sub-domains no preload hsts-client

enable x-content-type-options x-xss-protection content-security-policy anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows" anyconnect enable tunnel-group-list enable cache disable error-recovery disable // Bypass Access Control policy for decrypted traffic // This setting is displayed in the 'show run all' command output sysopt connection permit-vpn // Configures the group-policy to allow SSL connections group-policy ftdvpn-aaa-cert-grp internal group-policy ftdvpn-aaa-cert-grp attributes banner none 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 ssl-client split-tunnel-policy tunnelall ipv6-split-tunnel-policy tunnelall split-tunnel-network-list none default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools none 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 // Configures the tunnel-group to use the aaa & certificate authentication tunnel-group ftdvpn-aaa-cert-auth type remote-access tunnel-group ftdvpn-aaa-cert-auth general-attributes address-pool ftdvpn-aaa-cert-pool default-group-policy ftdvpn-aaa-cert-grp // These settings are displayed in the 'show run all' command output. Start authentication-server-group LOCAL secondary-authentication-server-group none

no accounting-server-group default-group-policy ftdvpn-aaa-cert-grp username-from-certificate CN OU secondary-username-from-certificate CN OU authentication-attr-from-server primary authenticated-session-username primary username-from-certificate-choice second-certificate secondary-username-from-certificate-choice second-certificate // These settings are displayed in the 'show run all' command output. End tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes authentication aaa certificate pre-fill-username client group-alias ftdvpn-aaa-cert-auth enable

Conferma in client VPN

Passaggio 1. Conferma certificato client

Passare a Certificati - Utente corrente > Personale > Certificati, verificare il certificato client utilizzato per l'autenticazione.



Conferma certificato client

Fare doppio clic sul certificato client, passare a Dettagli, controllare i dettagli di Oggetto.

• Oggetto: CN = sslVPNClientCN

💼 Certificate

General	Details	Certification Pa	ath	
Show:	<al></al>		\sim	
Field Sig Sig Sig Val	nature al nature hi uer id from id to bject	gorithm ash algorithm	Value sha256RSA sha256 ftd-ra-ca-common-name, Cisc Sunday, June 16, 2024 6:12:0 Monday, June 16, 2025 6:12: ssiVPNClientCN, ssiVPNClientO	^
Pu	blic key blic key n	arameterc	RSA (2048 Bits)	~
CN = s O = Cis L = Tok S = Tok C = JP	sivervelier co cyo cyo	ntCN	6	
			Edit Properties Copy to File	

X

Dettagli del certificato client

Passaggio 2. Conferma CA

Passare a Certificati - Utente corrente > Autorità di certificazione radice attendibili > Certificati,

quindi verificare la CA utilizzata per l'autenticazione.

• Rilasciato da: ftd-ra-ca-common-name

Console1 - [Console Root\Certificates - Curren	t User\Trusted Root Certification A	Authoritie (Certificates)			-	ø	×	<
File Action View Favorites Window	Help						- 8	×
🗢 🏟 🖄 🚾 🐇 🗞 🗙 🔛 📓								
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Action	5	
Certificates - Current User	COMODO RSA Certificati	COMODO RSA Certificati	1/18/2038	Client Authenticati	Sectigo (forr	Certific	ates	•
Certificates	Copyright (c) 1997 Micros	Copyright (c) 1997 Micros	12/30/1999	Time Stamping	Microsoft Til	M	ore	۲
Trusted Root Certification Authorities	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2022	<all></all>	<none></none>	ftd-ra-	ca	
Certificates	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	Client Authenticati	DigiCert	M	ore	•
> Intermediate Certification Authorities	DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati	DigiCert			
> Active Directory User Object	DigiCert Global Root G2	DigiCert Global Root G2 DigiCert High Assurance	1/15/2038	Client Authenticati	DigiCert Glol			
Invited Publishers	DigiCert High Assurance	DigiCert High Assurance	11/9/2031	Client Authenticati	DigiCert			
> Third-Party Root Certification Authoriti	DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati	DigiCert Tru:			
> iii Trusted People	DOT Det CA X3	OCT Durin CA X2	0/20/2021	Client Authorities	OCT Out C			
> Client Authentication Issuers	🙀 ftd-ra-ca-common-name	ftd-ra-ca-common-name	6/16/2029	<all></all>	<none></none>			
> Smart Card Trusted Roots	- ClobalEign	ClabelCige	2/10/2020	Clinet Authoriticati	ClobalCign 1			
> Grtificates (Local Computer)	🔄 GlobalSign	GlobalSign	12/15/2021	Client Authenticati	Google Trust			

Conferma CA

Verifica

Passaggio 1. Avvia connessione VPN

Sull'endpoint, avviare la connessione Cisco Secure Client. Il nome utente viene estratto dal certificato client. È necessario immettere la password per l'autenticazione VPN.



Nota: il nome utente viene estratto dal campo CN (Nome comune) del certificato client in questo documento.

Sisco Secure Client	- 0	×	Sisco Secure Client 192.168.1.200	×	Sisco Secure Client	- 🗆 X
AnyConnect VPII: Contacting 192.168.1.200. 192.168.1.200	✓ Connect	_	Group: ftdvpn-aaa-cert-auth Username: sslVPNClientCN	~	AnyConnect VPII: Connected to 192. 168. 1. 200. 192. 168. 1. 200	V Disconnect
			Password:		00:00:07	IPv4
☆ ①		-10-10-10-10-10-10-10-10-10-10-10-10-10-			\$	aliada CISCO
			OK Cancel			

Avvia connessione VPN

Passaggio 2. Conferma sessioni attive in FMC

Passare ad Analisi > Utenti > Sessioni attive, quindi controllare la sessione attiva per l'autenticazione VPN.

ę	Firewall Management Center Overview Analysis / Desires Devices Objects Integration Deploy Q, C O O admin / the SECURI											ECURE					
	Switch to legacy U										egacy UI						
T	Select														× Ref	resh L	g Out
Ø	Showing the 1 and only session	<u>E</u>			_											15	
C	Looin.Time	Realm/Username	Last.Seen 4	Authentication.Type	Current IP	Basics	Usemane	Eixt.Name	Last.Name	Email	Department	Phone Number	Discovery Application	Device			^
	2024-06-17 11:38:22	LocalRealmTest(ssIVPNClientCN	2024-06-17 11:38:22	VPN Authentication	172.16.1.40	LocalRealmTest	ssIVPNClientCN						LDAP	1	9		

Conferma sessione attiva

Passaggio 3. Conferma sessione VPN nella CLI FTD

Eseguireshow vpn-sessiondb detail anyconnect il comando nella CLI FTD (Lina) per confermare la sessione VPN.

ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7 Assigned IP: 172.16.1.40 Public IP: 192.168.1.11 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384 Bytes Tx : 14780 Bytes Rx : 15386 Pkts Tx: 2 Pkts Rx: 37 Pkts Tx Drop: 0 Pkts Rx Drop: 0 Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth Login Time : 02:38:22 UTC Mon Jun 17 2024 Duration: 0h:01m:22s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : cb00718200007000666fa19e Security Grp: none Tunnel Zone: 0

AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1

AnyConnect-Parent: Tunnel ID : 7.1 Public IP : 192.168.1.11 Encryption : none Hashing : none TCP Src Port : 50035 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : win Client OS ver: 10.0.15063 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 7390 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel: Tunnel ID : 7.2 Assigned IP : 172.16.1.40 Public IP : 192.168.1.11 Encryption : AES-GCM-128 Hashing : SHA256 Ciphersuite : TLS_AES_128_GCM_SHA256 Encapsulation: TLSv1.3 TCP Src Port : 50042 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 7390 Bytes Rx : 2292 Pkts Tx : 1 Pkts Rx : 3 Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel: Tunnel ID : 7.3 Assigned IP : 172.16.1.40 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 56382 UDP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 0 Bytes Rx : 13094 Pkts Tx : 0 Pkts Rx : 34 Pkts Tx Drop : 0 Pkts Rx Drop : 0

Passaggio 4. Conferma comunicazione con il server

Eseguire il ping tra il client VPN e il server e verificare che la comunicazione tra il client VPN e il server sia riuscita.

C:\Users\CALO>ping 192.168.10.11
Pinging 192.168.10.11 with 32 bytes of data: Reply from 192.168.10.11: bytes=32 time=12ms TTL=128 Reply from 192.168.10.11: bytes=32 time=87ms TTL=128 Reply from 192.168.10.11: bytes=32 time=3ms TTL=128 Reply from 192.168.10.11: bytes=32 time=3ms TTL=128
Ping statistics for 192.168.10.11: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 3ms, Maximum = 87ms, Average = 26ms

Ping riuscito

Eseguire capture in interface inside real-time il comando nella CLI FTD (Lina) per confermare l'acquisizione dei pacchetti.

<#root>

```
ftd702#
```

capture in interface inside real-time

Use ctrl-c to terminate real-time capture

1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request 2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply 3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request 4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply 5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request 6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply 7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request 8: 03:39:28.808399 192.168.10.11 > 172.16.1.40 icmp: echo request

Risoluzione dei problemi

Per informazioni sull'autenticazione VPN, vedere il syslog di debug del motore Lina e il file DART nel computer Windows.

Questo è un esempio di log di debug nel motore Lina.

// Certificate Authentication

Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=ssIV Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked. Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=ssIVPNClientCl

// Extract username from the CN (Common Name) field

Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 5] Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 5]

// AAA Authentication

Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN Jun 17 2024 02:38:22: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN

Questi debug possono essere eseguiti dalla CLI diagnostica dell'FTD, che fornisce le informazioni da usare per risolvere i problemi relativi alla configurazione.

- debug crypto ca 14
- debug webvpn anyconnect 255
- debug crypto ike-common 255

Riferimento

Configurazione dell'autenticazione basata sul certificato Anyconnect per l'accesso mobile

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).