透過FMC為FTD上的安全使用者端設定AAA和憑 證驗證

目錄
<u>必要條件</u>
採用元件
· · · · · · · · · · · · · · · · · · ·
<u>四小天的</u> 细败图主
<u> </u>
<u>少乘之班的心代女主音广调副问题</u> 先聽 3. 貸加策略分配
步驟 4.連線配置檔案的配置詳細資訊
步驟 6.新增連線設定檔的群組原則
步驟 7.設定連線設定檔的安全使用者端映像
步驟 8.設定連線設定檔的存取與憑證
步驟 9.確認連線設定檔摘要
在FTD CLI中確認
在VPN客戶端中確認
步驟 1.確認使用者端憑證
步驟 2.確認CA
<u>驗證</u>
步驟 1.啟動VPN連線
步驟 2.確認FMC中的活動會話
<u> 步驟 3.在FTD CLI中確認VPN作業階段</u>
步驟 4.確認與伺服器的通訊
<u>疑難排解</u>
參考

簡介

本檔案介紹在由FMC管理的FTD上透過SSL設定Cisco Secure Client,並使用AAA和憑證驗證的步驟。

必要條件

需求

思科建議您瞭解以下主題:

- Cisco Firepower管理中心(FMC)
- 防火牆威脅防禦虛擬(FTD)
- VPN身份驗證流程

採用元件

- 適用於VMWare的Cisco Firepower管理中心7.4.1
- 思科防火牆威脅防禦虛擬7.4.1
- 思科安全使用者端5.1.3.62

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

隨著組織採取更嚴格的安全措施,將雙因素身份驗證(2FA)與基於證書的身份驗證相結合已成為一種 常見做法,可增強安全性並防止未經授權的訪問。 可以顯著改善使用者體驗和安全性的功能之一是 能夠預填充Cisco Secure Client中的使用者名稱。此功能簡化了登入過程,並提高了遠端訪問的整 體效率。

本檔案介紹如何將預先填入的使用者名稱與FTD上的Cisco Secure Client整合,以確保使用者可以 快速安全地連線到網路。

這些憑證中包含用於授權目的的通用名稱。

- CA : ftd-ra-ca-common-name
- 客戶端證書:sslVPNClientCN
- 伺服器證書: 192.168.1.200

網路圖表

下圖顯示本文檔示例中使用的拓撲。



組態

FMC中的配置

步驟 1.設定FTD介面

導覽至Devices > Device Management,在Interfaces索引標籤中編輯目標FTD裝置、設定FTD的內 部和外部介面。

對於GigabitEthernet0/0,

- 名稱 : outside
- 安全區域: outsideZone
- IP地址: 192.168.1.200/24

對於GigabitEthernet0/1,

- 名稱: inside
- 安全區域: insideZone
- IP地址: 192.168.10.200/24

Firewall Management Center Devices / Secure Firewall Interfaces	Overview Overview	Analysis	Policies Devices	Objects Integration	D	eploy Q 🚱 🌣	admin 🗸 🖏	SECURE
149 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Initia	ne Sets DHCP	VTEP						Cancel
All Interfaces Virtual Tunnels					Q. Search by name	9 S	Sync 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.⊄
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		/

FTD介面

步驟 2.確認思科安全客戶端許可證

導覽至Devices > Device Management,編輯目標FTD裝置,在Device索引標籤中確認Cisco Secure Client授權。

Firewall Management Center Devices / Secure Firewall Device Summary	Overview Analys	sis Policies Devices	Objects Integration		Deploy	९ 💕 🌣 🎯	admin ~ "	SECURE
1.5.49 Gisco Firepower Threat Defense for VMware		License		0				
Device Routing Interfaces Inline	Sets DHCP VTEP	License Types Performance Tier:	FTDv5 - 100 Mbps	•				
General	1±	Essentials:		n	n			G
Name:	1.78643.4	Export-Controlled Features:				Cisco Firepower Threa	t Defense for VMw	are
Transfer Packets: Troubleshoot:	Logs CLI Download	Malware Defense:					9A33F35AM 2024-06-14 07:38	ISU 3:47
Mode:	Router	IPS:		Zo	one:		UTC (UTC+0	:00)
Compliance Mode:	None	Carrier:		n			7	.4.1
Performance Profile:	Defaul	URL: Secure Client Premier:		2c 30	one setting for ased Rules:		UTC (UTC+0	.00)
TES Grypto Acceleration.	Disablet	Secure Client Advantage:						
Device Configuration:	Import Export Download	Secure Client VPN Only:	0					
OnBoarding Method:	Registration Ke	If a device already has Secure Client VPN Secure Client Premier or Secure Client A	N Only they cannot have idvantage. If a device					
Inspection Engine		has Secure Client Premier or Secure Clie have Secure Client VPN Only	ent Advantage it cannot	g	gement		1	
Inspection Engine:	Snort			Cancel Save	Host Address:		1.100	.49
				d	lary Address:			



步驟 3.增加策略分配

導航到Devices > VPN > Remote Access,按一下Add按鈕。

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

增加遠端訪問VPN

輸入必要資訊,然後按一下Next按鈕。

- 名稱: ftdvpn-aaa-cert-auth
- VPN協定:SSL
- 目標裝置:1.x.x.49

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 🔕 admin ~ 🖓 🐯 SECURE
Firewall Management Center Overview Analysis Policies Objects Integration Perices / VPN / Setup Weard Overview Analysis Policies Objects Integration	Deploy Q Q admin Item SECURE
Add	
	Cancel Back Next

策略分配

步驟 4.連線配置檔案的配置詳細資訊

輸入連線配置檔案的必要資訊,然後按一下本地領域項旁邊的+按鈕。

- 身份驗證方法:客戶端證書和AAA
- 身份驗證伺服器:本地
- 證書使用者名稱:對映特定欄位
- 主欄位:CN(公用名)
- 輔助欄位:OU(組織單位)

Firewall Management Center Overview Analysis	Policies Devices Objects Integration	Deploy Q 🧬 🌣 🔕 admin 🗸 🕬 SECURE
Remote Access VPN Policy Wizard		
1 Policy Assignment 2 Connection Profile 3 Sect	rre Client	
	Connection Profile:	
	Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accompliabled 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 LOCAL or Reatm or RADIUS +	
	Local Realm." +	
	Prefill 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)	

連線設定檔的詳細資訊

從增加領域下拉選單中按一下本地,以增加新的本地領域。

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

新增本機範圍

輸入本地領域所需的資訊,然後按一下Save按鈕。

- 名稱:LocalRealmTest
- 使用者名稱:sslVPNClientCN



注意:使用者名稱與客戶端證書中的公用名相同

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

Add another local user

Cancel Save		
	Save	Cancel

本機範圍詳細資訊

步驟 5.為連線配置檔案增加地址池

按一下IPv4地址池專案旁邊的edit按鈕。

Cilent Address Assignment	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:	1
IPv6 Address Pools:	1

增加IPv4地址池

輸入必要的資訊以新增新的IPv4位址集區。為連線配置檔案選擇新的IPv4地址池。

- 名稱: ftdvpn-aaa-cert-pool
- IPv4地址範圍: 172.16.1.40-172.16.1.50
- 掩碼: 255.255.255.0

 $\mathbf{0} \times$

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
IPv4地址池的詳細資訊		
步驟 6.新增連線設定檔的群組原則		
點選組策略專案旁邊的+按鈕。		
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

0

增加組策略

輸入必要的資訊以新增群組原則。為連線配置檔案選擇新的組策略。

• 名稱: ftdvpn-aaa-cert-grp

• VPN協定: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 IPsec-IKEv2

0



步驟 7.設定連線設定檔的安全使用者端映像

選擇secure client image file並按一下Next按鈕。



Cancel Back Next

選擇安全客戶端映像

步驟 8.設定連線設定檔的存取與憑證

為VPN連線選擇Security Zone,然後按一下Certificate Enrollment專案旁邊的+按鈕。

• 介面組/安全區域:outsideZone

Firewall Management Center Overview Anal Devices / VPN / Setup Wizard Overview	lysis Policies Devices Objects Integration	Deploy Q 🧳 🌣 🙆 admin ~ 📫 🕯 SECURE
Remote Access VPN Policy Wizard		
Policy Assignment 2) Connection Profile (3) 3	Secure client Access & Certificate S Summary	
	Remote Secure Client Internet Outside User 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 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.*	

選擇安全區域

輸入FTD憑證的必要資訊,並從本機電腦匯入PKCS12檔案。

- 名稱: ftdvpn-cert
- 註冊型別: PKCS12檔案

Add Cert Enrollment

Name*				
Description				
CA Information C	ertificate Paramet	ers Key Revo	ocation	
Enrollment Type:	PKCS12 File	•		
PKCS12 File*:	ftdCert.pfx		Browse PKCS12 File	
Passphrase*:				
Validation Usage:	Skip Check fr	SSL Client S	SL Server	
		a overlag in basic cor	istuints of the overortheore	
				ľ
				•
			Cancel Save	

新增FTD憑證

確認在Access & Certificate嚮導中輸入的資訊,然後按一下Next按鈕。

0



注意:為解密的流量啟用繞過訪問控制策略(sysopt permit-vpn),以便解密VPN流量不會受 到訪問控制策略檢查。

Firewall Management Center Overview Analysis Polic	Lies Devices Objects Integration	Deploy Q 🥩 🌣 🔕 admin 🖞
Remote Access VPN Policy Wizard		
Policy Assignment (2) Connection Profile (3) Secure Client (3)	Access & Certificate 5 Summary	
Remote	Secure Client Internet Outside Unice 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 VPN connections. Interface group/Security Zone:* outsideZone • +	
	▲ 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.* ftdvpn-cert 💌 +	
	Enroll the selected certificate object on the target devices	
	Access Control for VPN Traffic	
	All decrypted traffic 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.	
	Bypass Access Control policy for decrypted traffic (syspet permit-type) This option bypasses the Access Control Policy impection, but VPW filter ACL and authorization ACL downloaded from AAA server are still applied to VPW traffic.	
<		
		Cancel Back Next



步驟 9.確認連線設定檔摘要

確認輸入的VPN連線資訊,然後按一下Finish按鈕。

Firewall Management Center Overview Devices / VPN / Setup Wizard	Analysis Policies Device	s Objects Integration		Deploy Q 💕 🌣 🌒	admin v dealer SECURE
Remote Access VPN Policy Wizard 1 Policy Assignment (2) Connection Profile	(3) Secure Client (4) A	Access & Certificate 5 Summary			
	Remote Access VPN Policy C	onfiguration	Additional Configuration Requirements		
	Firewall Management Center will cont Name: Device Targets: Connection Polifie: Connection Alias: AAA: Authentication Method: Username From Certificate: Authentication Server: Accounting Server: Accounting Server: Address Assignment: Address from AAA:	gure an RA VPN Policy with the following settings Rdvpn-aaa-cert-auth 1.1,1,2,3,249 Rdvpn-aaa-cert-auth Rdvpn-aaa-cert-auth Cleint Certificate & AAA CN (Common Name) & OU (Organisational Unit) LocalReahmTest (Local) -	After the vicand completed the receptor internal configuration needs to be completed for VPN to work on all device targets. • Access Control Policy Update An Access Control rule must be defined to allow VPN traffic on all targeted devices. • NAT Exemption If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic. • DNS Configuration To resolve hostname specified in AAA Servers or CA. Servers, configure DNS using FierConfig		
	DHCP Servers: Address Pools (IPv4):	- ftdvpn-aaa-cert-pool	Port Configuration		
	Address Pools (IPv6): Group Policy: Secure Client Images:	- Rdvpn-aaa-cert-grp cisco-secure-client-win-5.1.3.62+webdeploy+k9.pk n	SSL will be enabled on port 443. Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.		
	Interface Objects:	outsideZone	A Network Interface Configuration		
L	Device Certificates:	novpri-cert	Make sure to add interface from targeted devices to SecurityZone object 'outsideZone'		
	Device Identity Certificate Enrollmer	nt			
	Certificate enrollment object 'ftdypn-cert' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the <u>certificates</u> page to check the status of the installation.				
4				Cancel	Back Einish

確認VPN連線的設定

確認遠端存取VPN原則的摘要並將設定部署到FTD。

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects I	Integration	Deploy Q 💕 🌣 (admin ~ whether SECURE
ftdvpn-aaa-cert-auth				Save Cancel
Enter Description				
				Policy Assignments (1)
Connection Profile Access Interfaces Advanced			Local Realm: LocalRealmTest	Dynamic Access Policy: None
				+
Name	ААА	Group Policy		
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	E Dft0rpPolicy		/1
ftdvpn-aaa-cert-auth	Authentication: Client Certificate & LOCAL Authorization: None Accounting: None	Patricia fidvpn-aaa-cert-grp		/1
			1	

遠端訪問VPN策略摘要

在FTD CLI中確認

從FMC部署後,在FTD CLI中確認VPN連線設定。

// 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

在VPN客戶端中確認

步驟 1.確認使用者端憑證

導航到證書- Current User > Personal > Certificates, 檢查用於身份驗證的客戶端證書。



確認使用者端憑證

按兩下客戶端證書,導航到Details,檢查Subject的詳細資訊。

• 主題:CN = sslVPNClientCN

🕵 Certificate

General	Details	Certification P	Path	
Show:	<al></al>		\sim	
Field			Value	^
Sk	nature al	gorithm	sha256RSA	12
Sk	nature h	ash algorithm	sha256	
E Is	suer		ftd-ra-ca-common-name, Cisc	
🔄 Va	lid from		Sunday, June 16, 2024 6:12:0	
- No	id to		Monday, June 16, 2025 6:12:	
🗐 Su	bject		sslVPNClientCN, sslVPNClientO	
PU	blic key		RSA (2048 Bits)	
- Ph	hlic key n	arameterc	05.00	v
O = Cr L = To S = To C = JP	sco kyo kyo			
			Edit Properties Copy to File.	

X

步驟 2.確認CA

導航到證書- Current User > Trusted Root Certification Authorities > Certificates,檢查用於身份驗

• 頒發者: ftd-ra-ca-common-name

 Console1 - [Console Root\Certificates - Current File Action View Favorites Window 	t User\Trusted Root Certification A Help	Authoritie Certificates]			-	5 ×
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Actions
Certificates - Current User	COMODO RSA Certificati	COMODO RSA Certificati	1/18/2038	Client Authenticati	Sectigo (forr	Certificates 🔺
Certificates	Copyright (c) 1997 Micros	Copyright (c) 1997 Micros	12/30/1999	Time Stamping	Microsoft Tii	More >
 Trusted Root Certification Authorities Certificates 	DESKTOP-VCKHRG1	DESKTOP-VCKHRG1 DigiCert Assured ID Root DigiCert Assured ID Root	10/30/2022 11/9/2031	Server Authenticati <all></all>	<none> DigiCart</none>	ftd-ra-ca 🔺
Concerprise Trusc Concerprise Trusc Concerprise Trusc Concerprise Trusc Concerprise Truscond Concerprise Concerprise Trusted Publishers Concerprise Contificates	DigiCert Assured D Rode DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance DigiCert High Assurance	DigiCert Assured to Noot DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance DigiCert High Assurance	11/9/2031 1/15/2038 11/9/2031 11/9/2031	Client Authenticati Client Authenticati <all> Client Authenticati</all>	DigiCert DigiCert Glol <none> DigiCert</none>	More 🕨
 Third-Party Root Certification Authoriti Trusted People 	DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati	DigiCert Tru:	
 Client Authentication Issuers Smart Card Trusted Roots 	td-ra-ca-common-name	ftd-ra-ca-common-name ClabalCige	6/16/2029	<all></all>	<none></none>	
> 🗊 Certificates (Local Computer)	📮 GlobalSign	GlobalSign	12/15/2021	Client Authenticati	Google Trust	

確認CA

驗證

步驟 1.啟動VPN連線

在終端上,啟動Cisco Secure Client連線。使用者名稱從客戶端證書中提取,您需要輸入密碼進行 VPN身份驗證。



注意:使用者名稱擷取自本檔案中使用者端憑證的CN (一般名稱)欄位。

AnyConnect VPH: Contacting 192.168.1.200. 192.168.1.200 Connect Username: ssVPNCientCN Password: ******** Connect Username: ssVPNCientCN Password: ******* Connect Con	S Cisco Secure Client —	- ×	S Cisco Secure Client 192.168.1.200 X	Sisco Secure Client	×
Password: Password: Contraction Contractio	AnyConnect VPH: Contacting 192.168.1.200. 192.168.1.200	Connect	Group: ftdvpn-aaa-cert-auth ~ Username: sslvPNClentCN	AnyConnect VPH: Connected to 192.168.1.200. 192.168.1.200	Disconnect IPv4
	☆ ①	սիսիս ՀՅՏԵԹ	Password:	\$	altada. cisco

啟動VPN連線

步驟 2.確認FMC中的活動會話

導航到分析>使用者>活動會話,檢查活動會話以進行VPN身份驗證。

þ	Errevall Management Center Avalysis Policies Devices Objects Integration Depiny Q 💞 O 🕒 admin V														
	Settich to legacy UI														
T	Y Select X Referent Log Cod									efresh Log Out					
0	🖉 Drowing the 1 and only session 🛓 💦 🛼									E					
	LosinTime	Realm/Username	Last.Seen 4	Authentication Type	Current.IP	Baales	Usemane	Exxt.Name	Last Name	Email	Department	Phone Number	Discovery. Application	Device	-
	2024-06-17 11:38:22	LocalRealmTest(ssIVPNCIentCN	2024-06-17 11:38:22	VPN Authentication	172.16.1.40	LocalRealmTest	ss/VPNC/ientCN						LDAP	1	

確認活動會話

步驟 3.在FTD CLI中確認VPN作業階段

在FTD (Lina) CLI中執行show vpn-sessiondb detail anyconnect命令以確認VPN作業階段。

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

步驟 4.確認與伺服器的通訊

從VPN客戶端向伺服器發出ping命令,確認VPN客戶端與伺服器之間的通訊成功。

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 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成功

在FTD (Lina) CLI中執行capture in interface inside real-time命令以確認封包擷取。

```
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

疑難排解

您可以期待在Lina引擎的調試系統日誌和Windows PC上的DART檔案中找到有關VPN身份驗證的資訊。

以下是Lina引擎中的偵錯日誌範例。

// 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

您可以從FTD的診斷CLI執行這些偵錯,提供的資訊可用於排除組態故障。

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

參考

<u>為行動存取配置基於Anyconnect證書的身份驗證</u>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。