Configurar Autenticação Baseada em Certificado do Anyconnect para Acesso Móvel

Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar o Cisco Anyconnect no FTD Diagrama de Rede Adicionar certificado ao FTD Configurar o Cisco Anyconnect Criar certificado para usuários móveis Instalar no Dispositivo Móvel Verificar Troubleshoot Debugs

Introduction

Este documento descreve um exemplo da implementação da autenticação baseada em certificado em dispositivos móveis.

Prerequisites

As ferramentas e dispositivos usados no guia são:

- Defesa contra ameaças (FTD) do Cisco Firepower
- Firepower Management Center (FMC)
- Dispositivo Apple iOS (iPhone, iPad)
- autoridade de certificado (CA)
- Software Cisco Anyconnect Client

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VPN básica,
- SSL/TLS
- Infraestrutura de chave pública
- Experiência com o FMC
- OpenSSL
- Cisco Anyconnect

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FTD da Cisco
- FMC da Cisco
- Servidor de CA da Microsoft
- XCA
- Cisco Anyconnect
- Ipad da Apple

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar o Cisco Anyconnect no FTD

Esta seção descreve as etapas para configurar o Anyconnect via FMC. Antes de começar, implante todas as configurações.

Diagrama de Rede



Adicionar certificado ao FTD

Etapa 1. Criar um certificado para o FTD no dispositivo FMC. Navegue até **Devices > Certificate** e escolha **Add**, como mostrado nesta imagem:

Firepower Management Center Overview Ana Devices / Certificates	lysis Policies Devices Objects AMP Int	telligence	Q. Deploy 💕	🔅 🕒 admin 🕶
			\rightarrow	Add
Name Domain	Enrollment Type Status			
V=FTD1				
FTD Global	Manual (CA & ID)			₽₽C₽
✓				
ftd2 Global	PKCS12 file CA ID			₽ ₽ C ∎
	_	_		
	Но	w To		

Etapa 2. Escolha o FTD desejado para a conexão VPN. Escolha o **dispositivo FTD** no menu suspenso de dispositivos. Clique no ícone + para adicionar um novo método de registro de certificado, como mostrado nesta imagem:

← → C @ O A https://to	coutrie-fmc.tcoutrie-se	ecurity301.com/ddd/#P	acerificate 🏠 😌 🖢 İn, 60 💽 I	8 0		* ≡
Getting Started C School C Work					C) 0%	er Bookmarks
Firepower Management Center Devices / Certificates	Overview Ana	alysis Policies	Devices Objects AMP Intelligence Q Deploy (\$	0	admin 🕶
						Add
Name	Domain	Enrollment Type	Status			
V == FTD1						
FTD	Global	Manual (CA & ID)		B• (₽ C	¥
V m Tcoutrie-FTD2						
ftxd2	Global	PKCS12 file	Add New Certificate	B+ (C C	Ì
			Add a new certificate to the device using cert enrollment object which is used to enroll to certificate certificate certificate entrollment object Cent Enrollment*: Select a certificate entrollment object Cancel Add			
			How To			

Etapa 3. Adicione os certificados ao dispositivo. Escolha a opção que é o método preferido para obter certificados no ambiente.

Tip: As opções disponíveis são: **Certificado Autoassinado** - Gere um novo certificado localmente, **SCEP** - Use o Simple Certificate Enrollment Protocol para obter um certificado de uma CA, **Manual** - Instale manualmente o certificado Raiz e Identidade, **PKCS12** - Carregue o pacote de certificado criptografado com raiz, identidade e chave privada.

Etapa 4. Carregue o certificado no dispositivo FTD. Insira a senha (somente PKCS12) e clique em **Save**, como mostrado nesta imagem:

Add Cert Enrollment	9
Name* ftdcert Description	
Enrollment Type: PKCS12 File PKCS12 File*: Tcoutrie-ftd2.p12 Passphrase: Skip Check for CA flag in basic constraints of the CA Certificate	
Cancel	ave

Note: Depois de salvar o arquivo, a implantação dos certificados ocorre imediatamente. Para ver detalhes do certificado, escolha a ID.

Configurar o Cisco Anyconnect

Configure o Anyconnect via FMC com o assistente de acesso remoto.

Procedimento:

Etapa 1. Inicie o assistente de política de VPN de acesso remoto para configurar o Anyconnect.

Navegue até Devices > Remote Access e escolha Add.

Firepower Management Center Overview Analysis Policies	Devices Objects AMP Intelligence		् Deploy 💕 🌣 🛭 admin 🔻
Name	Status	Last Modified	
RAVPN	Targeting 1 devices Up-to-date on all targeted devices	2021-07-09 17:10:31 Modified by "admin"	/ 1
	How To		

Etapa 2. Atribuição de políticas.

Conclua a atribuição de política: a. Nomear a política

- b. Escolha os protocolos VPN desejados
- c. Escolha o dispositivo de destino para aplicar a configuração

Remote Access VPN Policy Wizard Policy Assignment ? Connection Profile ? AnyConnect Access & Certificate Summary	
• Oncy assignment • Andreetion Hode Calculate • Automation Produces 	Centre You Start Mater you start, ensuin the following configuration dements to be in place to complete Remote Access Authentication Server Configure Realm of RADIUS Server Group of SSO to authenticate VPN element. AryConnect Client Package Mater sure you have AnyConnect package for VPN Client Gowindadd of you have the relevant Clico condentists to dowinded the durps the webant. Device Interface Index Server
How To	Cancel Back Next

Etapa 3. Perfil de Conexão.

- a. Nomear o Perfil de Conexão
- b. Definir o método de autenticação como Somente Certificado do Cliente

- c. Atribua um pool de endereços IP e, se necessário, crie uma nova Política de Grupo
- d. Clique em Next

Remote Access VPN Policy Wizard	
Precy Assignment Connection Prome Anglummet Anglummet	(ummary
And	
Connection Prolian search the turned entrop anticipa for a	a MNI consection. These policies posts to constant the
turnel Tasti, New AAA is accomplished and how addresse are defined in group peldes. Connection Public Immes. ¹ (RAMM)	as are analyzed. They also include user ambuses, which
This name is confoured as a connection alian. It can	are be used to correct to the VPN outreese.
Authoritation Restanciation R Association (ARR)	
Facility the method of authorities (AAA) configuration	n en stad i mel dan data annan data all'han anna ha 1980.
connections.	
Authentication Mathod. Client Certificate Only	•
Usemane From Map specific field Contricate:) Upo entire DN (Distinguished Name) as usertaine
Primory Field: CN (Common Name)	•
Secondary Pielo: None	
Authorization Server: (Nation of NUTUD)	* +
Accounting Server:	• +
Client Address Adsignment:	
Client IP address can be assigned from AAA server, DHCP selected, IP address assignment is triad in the order of AA	29 server and 19 address pools. When multiple options are MA server, DHCD server and 19 address pool.
Use AAA Server (Realm or RADIUS only)	
Use DHOP Servers	
Use IP Address Poors	
IPv4 Address Pools	
Group Policy:	
A group policy is a collection of user-oriented session attr	Abbutes which are assigned to clear when a VIW
connection is established. Select or create a Group Policy	y edget.
UtilityPoley *	17
tet disp rate)	

Note: Escolha o Campo Primário a ser usado para inserir o nome de usuário para sessões de autenticação. O CN do certificado é usado neste guia.

Etapa 4. Anyconnect.

Adicione uma imagem do Anyconnect ao equipamento. Carregue a versão preferencial do Anyconnect e clique em **Avançar**.

Note: Os pacotes do Cisco Anyconnect podem ser baixados em Software.Cisco.com.

Etapa 5. Acesso e certificado.

Aplique o certificado a uma interface e ative o Anyconnect no nível da interface, como mostrado nesta imagem, e clique em **Avançar**.



Etapa 6. Resumo.

Revise as configurações. Se todos fizerem check-out, clique em concluir e em implantar.

Criar certificado para usuários móveis

Crie um certificado a ser adicionado ao dispositivo móvel usado na conexão.

Etapa 1. XCA.

a. Abrir XCA

b. Iniciar um novo Banco de Dados

Etapa 2. Criar CSR.

- a. Escolha Solicitação de Assinatura de Certificado (CSR)
- b. Escolher Nova Solicitação
- c. Insira o valor com todas as informações necessárias para o certificado
- d. Gerar uma nova chave
- e. Ao terminar, clique em OK

● ● ●	💞 X Certificate and Key management
Create Certificate signing request	3) Promised Thickey The
Source	Extensions Key usage Netscape Advanced
Distinguished name	
Internal name	organizationName
countryName	organizationalUnitName
stateOrProvinceName	commonName Cisco_Test
localityName	emailAddress
Туре	Content Add
	Delete
Private kev	
Ciase Test 1 (DSA:2049 bit)	
CISCO_TEST_T (RSA-2048 DIL)	Used keys too Generate a new key
	Cancel

Note: Este documento usa o CN do certificado.

Etapa 3. Enviar CSR.

- a. Exportar o CSR
- b. Enviar CSR para CA para obter um novo certificado

	I.	X Certificate and Key management	
	Private Keys	Certificates Templates Revocation lists	
Internal name A commonName Signed			New Request
			Export
			Import
			Show Details
			Delete
1			
			2 Divernoe Time
Database: /Users/tcoutrie/cisco.xdb		Search	

Note: Use o formato PEM do CSR.

Instalar no Dispositivo Móvel

Etapa 1. Adicione o certificado do dispositivo ao dispositivo móvel.

Etapa 2. Compartilhe o certificado com o aplicativo Anyconnect para adicionar o novo aplicativo de certificado.

Caution: A instalação manual exige que o usuário compartilhe o certificado com o aplicativo. Isso não se aplica a certificados enviados via MDMs.

Contents		certs	Ē	Select
Q Search				Ŷ
Cisco_Test.p1	DMChain.p7b	DMS	Certificate Percente Noblesse_An	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	Œ		4 KB	4 KB
Move	8	(P	(A A	(A A
Delete	创	Certificate Perional	Certificate Perional	Certificate Perional
t Info	i	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 Perional	Certificate Perional
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

- Etapa 3. Insira a senha do certificado para o arquivo **PKCS12**.
- Etapa 4. Criar uma nova conexão no Anyconnect.
- Etapa 5. Navegar até novas conexões; Conexões > Adicionar conexão VPN.

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

Etapa 6. Digite as informações para a nova conexão.

Descrição: Nomear a conexão

Endereço do servidor: Endereço IP ou FQDN do FTD

Avançado: Configurações adicionais

Etapa 7. Escolha Avançado.

Etapa 8. Selecione Certificate e escolha o certificado recém-adicionado.

AnyConnect	VPN Connections	
PRIMARY VIRTUAL PRIVATE NETWO	RK	
AnyConnect VPN	Advanced Select Certificate	(j)
Connections FT		(i)
Details Disconnecte	Disabled	
Dottino Discontinuotto	Selecting this option will disable certificate authentication.	í
	Automatic	(i)
GENERAL	This will automatically select a certificate for authentication.	\odot
Settings	Noblesse_IPAD	(i)
	Issuer: DMsliders-TCOUTRIE-SRV-CA	(i)
Diagnostics	Expiration Date: Apr 25, 2022 11:00:36	Ŭ
About	Cisco_Test	í
	Issuer: DMsliders-TCOUTRIE-SRV-CA Eveloptics Date: Aug 02, 2022 09:12:47	()
	Noblesse IPAD	
	Issuer: DMsliders-TCOUTRIE-SRV-CA	i
	Expiration Date: Apr 25, 2022 11:04:38	
	Noblesse_IPAD	
	Issuer: DMsliders-TCOUTRIE-SRV-CA	
	Expiration Date: Apr 25, 2022 00:42:05	
CISCO		
CISCO		

Etapa 9. Navegue de volta para **Conexões** e teste.

Uma vez bem-sucedida, a alternância permanece ativa e os detalhes mostram conectado no status.



Verificar

O comando **show vpn-sessiondb detail Anyconnect** mostra todas as informações sobre o host conectado.

Tip: A opção para filtrar ainda mais esse comando são as palavras-chave 'filter' ou 'sort' adicionadas ao comando.

Por exemplo:

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

Troubleshoot

Debugs

As depurações que devem ser exigidas para solucionar esse problema são:

Debug crypto ca 14 Debug webvpn 255 Debug webvpn Anyconnect 255 **Se a conexão for IPSEC e não SSL:**

Debug crypto ikev2 platform 255 Debug crypto ikev2 protocol 255 debug crypto CA 14 Logs do aplicativo móvel Anyconnect:

Navegue até Diagnostic > VPN Debug Logs > Share logs.

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

Digite as informações:

- Problema
- Etapas para reprodução

Em seguida, navegue até Enviar > Compartilhar com.

3:49 PM Wed Sep 29		•••		奈 47% ■
AnyConnect		Diagnostics		
AnyConnect VPN	Car	ncel Share Logs	Send	
Connections Asa	Plea follo	ase describe the problem and steps to r owing fields.	Email logs to	>
Details Disconnecte	PRO	BLEM	Administrator	>
GENERAL	Test		Cisco	
Settings	STEPS TO REPRODUCE			>
Diagnostics	Test			>
About				>
				>
սիսիս	The data sent is for diagnostic purposes only and may contain information about configured connections, as well as server and endpoint identities, IP addresses, and username. This data will appear to come from the email address you specify and will not be used for marketing or advertising purposes.			
CISCO				

Isso apresenta a opção de usar um cliente de e-mail para enviar os logs.