# Configurar SSL Secure Client com autenticação local no FTD

# Contents

Introdução Pré-requisitos Requisitos Componentes Utilizados Informações de Apoio Configurar Configurações Etapa 1. Verificar licenciamento Etapa 2. Carregar o Cisco Secure Client Package no FMC Etapa 3. Gerar um certificado autoassinado Etapa 4. Criar território local no FMC Etapa 5. Configurar SSL Cisco Secure Client Verificar

### Introdução

Este documento descreve como configurar o Cisco Secure Client (inclui o Anyconnect) com autenticação local no Cisco FTD gerenciado pelo Cisco FMC.

### Pré-requisitos

#### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do SSL Secure Client através do Firepower Management Center (FMC)
- Configuração de objetos do Firepower por meio do FMC
- Certificados SSL no Firepower

#### **Componentes Utilizados**

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

- Cisco Firepower Threat Defense (FTD) versão 7.0.0 (Build 94)
- Cisco FMC versão 7.0.0 (Build 94)
- Cisco Secure Mobility Client 4.10.01075

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

#### Informações de Apoio

Neste exemplo, o Secure Sockets Layer (SSL) é usado para criar a Virtual Private Network (VPN) entre o FTD e um cliente Windows 10.

A partir da versão 7.0.0, o FTD gerenciado pelo FMC suporta autenticação local para Cisco Secure Clients. Isso pode ser definido como o método de autenticação principal ou como fallback, caso o método principal falhe. Neste exemplo, a autenticação local é configurada como a autenticação primária.

Antes desta versão de software, a autenticação local do Cisco Secure Client no FTD estava disponível apenas no Cisco Firepower Device Manager (FDM).

# Configurar

#### Configurações

Etapa 1. Verificar licenciamento

Antes de configurar o Cisco Secure Client, o FMC deve ser registrado e estar em conformidade com o Smart Licensing Portal. Você não pode implantar o Cisco Secure Client se o FTD não tiver uma licença Plus, Apex ou VPN Only válida.

Navegue até System > Licenses > Smart Licenses para garantir que o FMC esteja registrado e em conformidade com o Smart Licensing Portal:

Overview Analysis Policies	Devices Objects AMP Intelligence							0, De	oloy System	Help 🔻 dj	erezve 🔻
	Confi	uration Users	Domains	Integration	SecureX	Updates	Licenses + Smart Licenses	Logging •	Health 🔻	Monitoring •	Tools •
Smart License Status		Cisco Smart Softwar	e Manager	• 2							
Usage Authorization:	Authorized (Last Synchronized On Sep 04 2021)										
Product Registration:	Registered (Last Renewed On Sep 04 2021)										
Assigned Virtual Account:	SEC TAC										
Export-Controlled Features:	Enabled										
Cisco Success Network:	Enabled (1)										
Cisco Support Diagnostics:	Disabled 🕕										

Role para baixo na mesma página. Na parte inferior do gráfico Smart Licenses, você pode ver os diferentes tipos de licenças do Cisco Secure Client (AnyConnect) disponíveis e os dispositivos assinados para cada um. Assegurar que o DTF em questão está registrado em qualquer uma destas categorias:

Smart Licenses		Filter Devices	× Edit #	Performance Tier Edit Licenses
License Type/Device Name	License Status	Device Type	Domain	Group
🖻 📁 Firepower Management Center Virtual (2)	٢			
▷ 💋 Base (2)	0			
🖻 🥔 Malware (2)	0			
▷ 💋 Threat (2)	0			
> 💋 URL Filtering (2)	0			
a 🤪 AnyConnect Apex (2)	0			
ftdv-dperezve 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0	0	Cisco Firepower Threat Defense for VMWare	Global	N/A
ftdvha-dperezve (Performance Tier: FTDv50 - Tiered) 192.168.13.9 - Cisco Firepower Threat Defense for VMware - v7.0.0	0	Cisco Firepower Threat Defense for VMware	Global	N/A
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				
lote: Container Instances of same blade share feature licenses			Activate Win Go to System in G	dows Control Panel to activate Windows.
t login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2				ا،، د

#### Etapa 2. Carregar o pacote Cisco Secure Client no FMC

Faça o download do pacote de implantação de headend do Cisco Secure Client (AnyConnect) para Windows em <u>cisco.com:</u>

Application Programming Interface [API] (Windows) anyconnect-win-4.10.01075-vpnapi.zip Advisories	21-May-2021	141.72 MB	<u>+</u> \;
AnyConnect Headend Deployment Package (Windows) anyconnect-win-4.10.01075-webdeploy-k9.pkg Advisories	21-May-2021	77.81 MB	<u>+</u> \;
AnyConnect Pre-Deployment Package (Windows 10 ARM64) - includes individual MSI files anyconnect-win-arm64-4.10.01075-predeploy-k9.zip Advisories	21-May-2021	34.78 MB	<u>+</u> \;
AnyConnect Headend Deployment Package (Windows 10 ARM64) anyconnect-win-arm64-4.10.01075-webdeploy-k9.pkg Advisories	21-May-2021	44.76 MB	<u>+</u> \;
Profile Editor (Windows) tools-anyconnect-win-4.10.01075-profileeditor-k9.msi Advisories 📑	21-May-2021	10.90 MB	<u>+</u> \;
AnyConnect Installer Transforms (Windows) tools-anyconnect-win-4.10.01075-transforms.zip Advisories	21-May-2021	0.05 MB	±₩

Para carregar a imagem do Cisco Secure Client, navegue para Objects > Object Management e escolha Cisco Secure Client File na categoria VPN no sumário:



Escolha o botão Add AnyConnect File. Na janela Add AnyConnect Secure Client File, atribua um nome para o objeto e escolha Browse... para selecionar o pacote do Cisco Secure Client. Finalmente, escolha AnyConnect Client Image como o tipo de arquivo no menu suspenso:

Overview Analysis Polici	es Devices Objects AMP Intellige	nce		. @, Deploy System Help ▼ dperezve ▼
Object Management Intru	sion Rules			
AnyConnect File File objects represent files used in c	onfigurations, typically for remote access VPN policies	. They can contain AnyConnect Client Profile and AnyConnect Client Image files.		Add AnyConnect File
IPv6 Prefix List	Name		Value	Туре
Route Map				
<ul> <li>Security Intelligence</li> </ul>		No records to display	_	
DNS Lists and Feeds		Add AnyConnect File	7 ×	
Hetwork Lists and Feeds     URL Lists and Feeds     URL Lists and Feeds     StA Monitor     Time Range     Time Zone     URL     Vraible Set     VLAN Tag     Voi     AnyConnect File     Coston Attribute     Coston Attribute		Name:* AnyConnect_Win_4.10 File Name:* InyConnect_Win_4.10.01075-webdeploy-k9.p Browse File Type:* AnyConnect Client Image Description: Save C	ancet	
IKEV1 IPsec Proposal				
S IKEv1 Policy				
IKEv2 IPsec Proposal				
IKEv2 Policy				No data to display  < < Page 1 of 1 > >  C
				Go to system in Control Panel to activate Windows
Last login on Friday, 2021-09-03 at 12				CISCO

Escolha o botão Salvar. O objeto deve ser adicionado à lista de objetos:



Etapa 3. Gerar um certificado autoassinado

O SSL Cisco Secure Client (AnyConnect) requer um certificado válido para ser usado no handshake SSL entre o headend da VPN e o cliente.

Observação: neste exemplo, um certificado autoassinado é gerado para essa finalidade. Além disso, além dos certificados autoassinados, é possível carregar um certificado assinado por uma CA (Certificate Authority, Autoridade de Certificação) interna ou também por uma CA conhecida.

. @ Deploy System Help ▼ dperezve ▼

Para criar o certificado autoassinado, navegue para Dispositivos > Certificados.

 Overview
 Analysis
 Policies
 Devices
 Objects
 AMP
 Intelligence

 Device
 Management
 Device Upgrade
 NAT
 VPN •
 QoS
 Platform Settings
 FlexConfig
 Certificates

Escolha o botão Adicionar. Em seguida, escolha o FTD listado no menu suspenso Device na janela Add New Certificate.

Overview Analysis Policies Devices Objects AMP	Intelligence	. Ø <sub>4</sub> Deploy System Help ▼ dperezve ▼
Device Management Device Upgrade NAT VPN • Qo	Platform Settings FlexConfig Certificates	
		O Add
Name Domain	Enrollment Type Status	
	No certificates Ad	dd Certificates
	Add New Certificate	? ×
	Add a new certificate to the device using cert enroll identify certificate.	illment object which is used to generate CA and
	Device*: ftdvha-dperezve	
	Cert Enrollment*: Select a certificate entro	rollment object 🔽 🖸
		Add Cancel
		Activate Windows
Last login on Saturday. 2021-09-04 at 14:26:07 PM from 192.168.13.2		د مایران

Escolha o botão Add Cert Enrollment (verde + símbolo) para criar um novo objeto de inscrição. Agora, na janela Add Cert Enrollment, atribua um nome ao objeto e escolha Self Signed Certificate no menu suspenso Enrollment Type.

Overview Analysis Policies Devices Obje	ects AMP	Intelligence					. Q Deploy System Help ▼ dperezve ▼
Device Management Device Upgrade NAT	VPN VQoS	Platform Settings	FlexConfig Certificates			_	
		Add Cert Enrollment				? ×	Com Add
Name	Domain	Name*	SSL_SelfSigned				
		Description					
			Cardellanda Davarandara - Marci	Deveration			
		CAInformation	Certificate Parameters Key	Revocation			
		Common Name (Chi)	Self Signed Certificate	Forto that is used in Report	Y		
		Common Name (CN)	is mandatory for self-signed certi to 'Certificate Parameters' tab.	ncate that is used in Remoti	e Access VPN. To configure		
		Allow Overrides	0				
					Save Cance		Activate Windows
							Go to System in Control Panel to activate Windows
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.16							

Por fim, para certificados autoassinados, é obrigatório ter um nome comum (CN). Navegue até a guia Parâmetros do Certificado para definir um CN:

Overview Analysis Policies	Devices Objects AMP	Intelligence			0 <sub>4</sub> Deploy System Help ▼ dperezve ▼
Device Management Device Upg	grade NAT VPN • QoS	Platform Settings Fl	exConfig Certificates		
		Add Cert Enrollment		? ×	Add Add
Name	Domain	Name*	SSL_SelfSigned		
		Description			
		CA Information Cert	ificate Parameters Key Revocation		
		Include FQDN:	Don't use FQDN in certificate	*	
		Include Device's IP Address	s:		
		Common Name (CN):	dperezve.local		
		Organization Unit (OU):			
		Organization (O):			
		Locality (L):			
		State (ST):			
		Country Code (C):	Comma separated country codes		
		Email (E):			
		Include Device's Serial N	lumber		
		Nieu Oueridee	0		
		Allow Overrides	0		
				Save Cancel	
					Activate Windows

Clique nos botões Salvar e Adicionar. Após alguns segundos, o novo certificado deve ser adicionado à lista de certificados:



Etapa 4. Criar território local no FMC

O banco de dados de usuário local e as respectivas senhas são armazenados em um realm local. Para criar o território local, navegue para Sistema > Integração > Territórios:



Escolha o botão Add Realm. Na janela Add New Realm, atribua um nome e escolha a opção LOCAL no menu suspenso Type:

Quanties Analysis Policies Devices Objects AMP Tr	telligence			Deploy System Help * depender *
Overview Analysis Policies Devices Objects Arm	Add New Realm		θ×	Lisses a Lassing a Halling Menitoria Talan
Cloud Services Realms Identity Sources High Av Realms Realm Sequences Sync Results	AnyConnect-Local-Auth Type Local Local User Configuration Username Password Add another local user	Description	Save	
Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2				alialia

As contas de usuário e senhas são criadas na seção Configuração de usuário local.

Observação: as senhas devem ter pelo menos uma letra maiúscula, uma letra minúscula, um número e um caractere especial.

Overview Analysis Policies Devices Objects AMP	atelligence				0. Dep	ov System	Help 🔻 d	perezve 🔻
	Add New Realm		θ×	Licenses 🔻	Logging V	Health •	Monitoring *	Tools •
Cloud Services Realms Identity Sources High A Realms Realm Sequences Sync Results	Add New Realm Name* AnyConnect-Local-Auth Type LoCAL V Local User Configuration  deprezve Username deprezve Password	Confirm Password	• ×	Licenses •	Logging •	Compare	e Realms	It Realm
		Cancel	Save					
Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2								ahaha

Salve as alterações e clique em Adicionar território para adicionar um novo território à lista de territórios existente.

Overview Analysis Policies Devices Objects	AMP Intelligence									€ Deg	oloy System	Help 🔻	dperezve +
			Configuration	Users	Domains	Integration	SecureX	Updates	Licenses ¥	Logging •	Health •	Monitoring	<ul> <li>Tools •</li> </ul>
Cloud Services Realms Identity Sources	High Availability eStreamer	Host Input Client	Smart Software Ma	nager On	Prem								
Realms Realm Sequences Sync Results													
											Compar	e Realms	Add Realm
Name - Description	Туре	Domain	AD Primary	Domain		B	ise DN				State		
AnyConnect-Local-Auth	LOCAL	Global									C Enable	d ∳	/ % 🗑

Etapa 5. Configurar SSL Cisco Secure Client

Para configurar o SSL Cisco Secure Client, navegue para Devices > VPN > Remote Access:

 Overview
 Analysis
 Policies
 Devices
 Objects
 AMP
 Intelligence
 Operazive ▼

 Device
 Management
 Device Upgrade
 NAT
 VPN ▶ Remote Access
 QoS
 Platform Settings
 FlexConfig
 Certificates

Clique no botão Add para criar uma nova política de VPN. Defina um nome para o perfil de conexão, marque a caixa de seleção SSL e escolha o FTD listado como o dispositivo de destino. Tudo deve ser configurado na seção Atribuição de política no Assistente de política de VPN de acesso remoto:



Escolha Next para ir para a configuração Connection Profile. Defina um nome para o perfil de conexão e escolha AAA Only como o método de autenticação. Em seguida, no menu suspenso Authentication Server, escolha LOCAL e, finalmente, escolha o território local criado na Etapa 4 no menu suspenso Território local:



Role para baixo na mesma página e clique no ícone do lápis na seção IPv4 Address Pool para definir o pool de IP usado pelos Cisco Secure Clients:

Overview Analysis Policies Devices Objects AMP Inte	lligence	🦺 Deploy System Help 🕶 dperezve 🕶
Device Management Device Upgrade NAT VPN • Remote Acc	ess QoS Platform Settings FlexConfig Certificates	
Remote Access VPN Policy Wizard		
Policy Assignment     O Connection Profile     Any	Connect > 4 Access & Certificate > 5 Summary	
Authent	ication Server:* LOCAL V (LOCAL or Realm or RADIUS)	1
	Address Pools ? ×	
Author	Available IPv4 Pools	
Accour	Search	
Client Addres	Ttdv-dperezve-pool	
assignment is	1994	
Use		
Sector Use		
Group Policy A group policy	ed. Select	
or create a Gr		
Group	OK Cancel	
		Back Next Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2		-iltili. cisco

Clique em Next para ir para a seção AnyConnect . Agora, selecione a imagem do Cisco Secure Client carregada na Etapa 2:

Overview Analysis Policies Devices Objects AMP Intelligence	\rm 04 Deploy	System Help 🔻	dperezve *
Device Management Device Upgrade NAT VPN > Remote Access QoS Platform Settings FlexConfig Certificates			
Remote Access VPN Policy Wizard			
Policy Assignment 2 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary			
Remote User AnyConnect Client Duternet Outside VPN Device Inside Corporate Resources			Î
AAA AnyConnect Client Image The VPM gateway can automatically download the latest AnyConnect package to the client device when the VPM connection is			
initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.			
Downiolad AnyConnect Client packages from <u>Clico Software Download Center</u> . Show Re-order buttons			
AnyConnect File Object Name AnyConnect Client Package Name Operating System			
AnyConnect_Win_4.10 anyconnect-win-4.10.01075-webdeploy-k9.pkg Windows			
Act Got	i (ate Backdov)	Next	Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2			ahaha

Clique em Avançar para ir para a seção Acesso e certificado. No menu suspenso Interface group/Security Zone, escolha a interface em que o Cisco Secure Client (AnyConnect) precisa ser habilitado. Em seguida, no menu suspenso Certificate Enrollment, escolha o certificado criado na Etapa 3:

Overview Analysis Policies Devices Objects AMP Intelligence	🧕 Deploy System H	elp 🔻 dperezve 🔻
Device Management Device Upgrade NAT VPN • Remote Access QoS Platform Settings FlexConfig Certificates		
Remote Access VPN Policy Wizard		
Policy Assignment     2 Connection Profile     3 AnyConnect     4 Access & Certificate     5 Summary		
Remote User AnyConnect Client Internet Outside User Corporate Resources		ĺ
AAA Notwork Teterford for Tecorolog VIDN Assocs		
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:* VLAN232		
Enable DTLS on member interfaces		
$\underline{\mathbb{A}}$ 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:* SSL_SelfSigned 🗸 🕤		
	Activate Backdows Next Go to System Control Parter to act	Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192:168.13.2		 cisco

Finalmente, clique em Avançar para ver um resumo da configuração do Cisco Secure Client:



Se todas as configurações estiverem corretas, clique em Concluir e implante as alterações no FTD.

Overview	N /	Analysis Policies Devices Objects AMP Intelligen	ce						0 <sub>4</sub> Deploy System Help ▼ dperezve ▼
									Deployment Deployment History
									1 device selected Deploy time: Estimate Deploy
<b>T</b> ( °	S	Search using device name, user name, type, group or status							
	•	Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
> 3		ftdvha-dperezve	dperezve		FTD		Sep 7, 2021 2:44 PM	B.	Pending
								Activate W	/indows

### Verificar

Depois que a implantação tiver sido bem-sucedida, inicie uma conexão do Cisco AnyConnect Secure Mobility Client do cliente Windows para o FTD. O nome de usuário e a senha usados no prompt de autenticação devem ser iguais aos criados na Etapa 4:

dute

	VPN:
	S Cisco AnyConnect   10.31.124.25 ×
	Group: SSL_AnyConnect_LocalAuth ~
<b>\$</b> (i)	Username: dperezve
	Password: *********

Quando as credenciais forem aprovadas pelo FTD, o aplicativo Cisco AnyConnect Secure Mobility

Client deverá exibir o estado conectado:

🕥 Cisco AnyC	Connect Secure Mobility Client		—		×
	VPN: Connected to 10.31.124.25. 10.31.124.25	~	Dì	sconnec	t
00:00:49					IPv4
<b>Ö</b> (i)					ahaha

No FTD, você pode executar o comando show vpn-sessiondb anyconnect para exibir as sessões do Cisco Secure Client atualmente ativas no Firewall:

firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect Username : dperezve Index : 8 Public IP : 10.31.124.34 Assigned IP : 172.16.13.1 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Bytes Tx : 15756 Bytes Rx : 14606 Group Policy : DfltGrpPolicy Tunnel Group : SSL\_AnyConnect\_LocalAuth Login Time : 21:42:33 UTC Tue Sep 7 2021 : Oh:00m:30s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0000000000080006137dcc9 Tunnel Zone : 0 Security Grp : none

#### Troubleshooting

Execute o comando debug webvpn anyconnect 255 no FTD para ver o fluxo de conexão SSL no FTD:

Além das depurações do Cisco Secure Client, o fluxo de conexão também pode ser observado com capturas de pacotes TCP. Este é um exemplo de uma conexão bem-sucedida, um handshake triplo regular entre o cliente Windows e o FTD é concluído, seguido por um handshake SSL usado para concordar com cifras.

Ethernet1					- a ×
File Edit View Go	Capture Analyze St.	stistics Telephony Wirele	ss Tools Hel	,	
🖌 🔳 🏾 🔍 🔜 🛤	X	a T 4 🗖 🔳 Q G			
ip.addr == 10.31.124.2	5				X - +
Ale North		Contraction .	lower la	and tak	
13 3 331622	10 31 124 34	10 31 124 25	TCR	66 51388 a 443 [SVII] Secul Mine64348 Lenve MCSe1468 MSe256 SALV PERMIT	
14 3.332733	10.31.124.25	10.31.124.34	TCP	60 443 a 51300 [SVII. ACK] Secol Ackal Mina32268 Lene0 MSSa1460	
15 3, 332833	10,31,124,34	10.31.124.25	TCP	54 51300 + 443 [ACK] Seg=1 Ack=1 Win=64240 Len=0	
16 3.338665	10.31.124.34	10.31.124.25	TLSv1.2	247 Client Hello	-
17 3.341963	10.31.124.25	10.31.124.34	TCP	60 443 + 51300 [ACK] Seg=1 Ack=194 Win=32768 Len=0	
18 3.341963	10.31.124.25	10.31.124.34	TLSv1.2	1171 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
21 3.390864	10.31.124.34	10.31.124.25	TCP	54 51300 + 443 [ACK] Seq=194 Ack=1118 Win=63123 Len=0	
29 5.494978	10.31.124.34	10.31.124.25	TLSv1.2	147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
30 5.496969	10.31.124.25	10.31.124.34	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message	
31 5.497482	10.31.124.34	10.31.124.25	TLSv1.2	1299 Application Data	
32 5.498069	10.31.124.25	10.31.124.34	TCP	60 443 → 51300 [ACK] Seq=1169 Ack=1532 Win=32768 Len=0	
33 5,500054	10.31.124.25	10.31.124.34	TLSv1.2	594 Application Data	
34 5.500054	10.31.124.25	10.31.124.34	TLSv1.2	797 Application Data	
35 5.500054	10.31.124.25	10.31.124.34	TLSv1.2	90 Application Data	
36 5.500158	10.31.124.34	10.31.124.25	TCP	54 51300 + 443 [ACK] Seq=1532 Ack=2488 Win=64240 Len=0	
66 12.255091	10.31.124.34	10.31.124.25	TL5v1.2	1524 Application Data	
67 12.269297	10.31.124.25	10.31.124.34	TCP	60 443 + 51500 [ACK] Seq=2488 Ack=2992 Win=32768 Len=0	
68 12.269297	10.31.124.25	10.31.124.34	TICH	60 443 + 51300 [ACK] Seq=2488 ACK=3002 H1n=32/68 Len=0	
70 12 269297	10.31.124.25	10.31.124.34	TLSV1.2	1411 Application Data	
70 12.209297	10 31 124 25	10 31 124 34	TI Sv1 2	1433 Application Data	
72 12 269518	10.31.124.34	10.31.124.25	TCP	54 51388 a 443 [AFV] Sena3883 Arba5784 Wina64348 Lena8	
73 12.278473	10.31.124.25	10.31.124.34	TLSv1.2	1514 Application Data	
74 12.278473	10.31.124.25	10.31.124.34	TLSv1.2	1514 Application Data [TCP segment of a reassembled PDU]	
75 12.278473	10.31.124.25	10.31.124.34	TLSv1.2	1271 Application Data	
> Frame 13: 66 byte	s on wire (528 bits	), 66 bytes cantured (	528 bits) on	interface \Device\NPF (0C14AC43-8A81-4ACC-AB5E-84CFC2FFC8C9), id 0	
> Ethernet II. Scc	Whare 96:c6:e8 (0	0:50:56:96:c6:e8), Dst	: Where b3:8	4:a7 (00:50:56:b3:84:a7)	
> Internet Protocol	Version 4, Src: 10	.31.124.34, Dst: 10.31	.124.25	····· • • ····························	
> Transmission Cont	trol Protocol, Src P	ort: 51300, Dst Port:	443, Seq: 0,	Len: 0	
0000 00 50 56 b3 8	4 a7 00 50 56 96 c	5 e8 08 00 45 00 PV	P VE		
0010 00 34 70 8f 4	0 00 50 05 00 00 0	a 1f 7c 22 0a 1f .4p			
0020 7c 19 c8 64 0	1 bb 94 5b 21 b4 0	0 00 00 00 50 02	q[ 1		
0030 Ta TO OC 80 0	0 00 02 04 05 04 0.				
0000 00 0A					

Após handshakes de protocolo, o FTD deve validar as credenciais com as informações armazenadas no território local.

Colete o pacote DART e entre em contato com o TAC da Cisco para pesquisa adicional.

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.