Konfigurieren von SSL AnyConnect Management VPN auf FTD

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Einschränkungen Konfiguration Konfigurationen Schritt 1: AnyConnect Management VPN-Profil erstellen Schritt 2: AnyConnect VPN-Profil erstellen Schritt 3: Laden Sie das AnyConnect Management VPN-Profil und das AnyConnect VPN-Profil auf FMC hoch. Schritt 4: Gruppenrichtlinie erstellen Schritt 5: Neue AnyConnect-Konfiguration erstellen Schritt 6: URL-Objekt erstellen Schritt 7: URL-Alias definieren Überprüfung Fehlerbehebung

Einführung

Dieses Dokument beschreibt die Konfiguration eines Cisco AnyConnect Management-Tunnels auf einer Cisco FirePOWER Threat Defense (FTD), die vom Cisco FirePOWER Management Center (FMC) verwaltet wird. Im Beispiel unten wird Secure Sockets Layer (SSL) zum Erstellen eines Virtual Private Network (VPN) zwischen FTD und einem Windows 10-Client verwendet.

Mitarbeiter: Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco AnyConnect Profile Editor
- SSL AnyConnect-Konfiguration über FMC
- Client-Zertifikatsauthentifizierung

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FTD Version 6.7.0 (Build 65)
- Cisco FMC Version 6.7.0 (Build 65)
- Auf dem Windows 10-Computer installierter Cisco AnyConnect 4.9.01095

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Ab Version 6.7 unterstützt Cisco FTD die Konfiguration von AnyConnect Management-Tunneln. Dadurch wird der zuvor geöffnete Verbesserungsantrag <u>CSCvs78215</u> behoben.

Die AnyConnect Management-Funktion ermöglicht die Erstellung eines VPN-Tunnels unmittelbar nach dem Start des Endpunkts. Die Benutzer müssen die AnyConnect-App nicht manuell starten, sobald ihr System hochgefahren ist. Der AnyConnect VPN-Agent-Dienst erkennt die Management-VPN-Funktion und initiiert eine AnyConnect-Sitzung mithilfe des in der Serverliste des AnyConnect Management VPN-Profils definierten Host Entry.

Einschränkungen

- Es wird nur die Client-Zertifikatsauthentifizierung unterstützt.
- Für Windows-Clients wird nur der Machine Certificate Store unterstützt.
- Wird vom Cisco FirePOWER Device Manager (FDM) <u>CSCvx90058</u> nicht unterstützt.
- Nicht unterstützt auf Linux-Clients.

Konfiguration

Konfigurationen

Schritt 1: AnyConnect Management VPN-Profil erstellen

Öffnen Sie den AnyConnect Profile Editor, um ein AnyConnect Management VPN-Profil zu erstellen. Das Verwaltungsprofil enthält alle Einstellungen, die zum Einrichten des VPN-Tunnels nach dem Hochfahren des Endpunkts verwendet werden.

In diesem Beispiel wird ein Server List-Eintrag definiert, der auf Fully Qualified Domain Name (FQDN) dperezve.jyoungta-labdomain.cisco.com zeigt, und SSL wird als primäres Protokoll ausgewählt. Um eine Serverliste hinzuzufügen, navigieren Sie zur **Serverliste**, und wählen Sie die Schaltfläche **Hinzufügen aus**, füllen Sie die erforderlichen Felder aus, und speichern Sie die Änderungen.

- an	AnyConnect	Profile	Editor -	VPN
------	------------	---------	----------	-----

le He	Serve	er List Entry				×
ି କୁ ଜୁନ	Serv	Load Balancing Servers	SCEP Mobile Cert	tificate Pinning		
B 一屋 C	F	Primary Server			Connection Information	ate Pin
g		Display Name (required)	AnyConnect_Manag	gement_Tunnel	Primary Protocol SSL ~	
<u>∎</u> 9 N		FQDN or IP Address	User Grou	qı	ASA gateway	
		dperezve.jyoungta-labdom	nain.cisc / AnyConne	ect_Management_Tunnel	Auth Method During IKE Negotiation	EAP-Ar
		Group URL			IKE Identity (IOS gateway only)	
		dperezve.jyoungta-labdom	nain.cisco.com/AnyCo	onnect_Management_Tunnel		
			Backup Servers			
			Host Address		Add	
					Move Up	
					Maria Davia	
					Move Down	
					Delete	
				L		
				OK Cancel		
	_					
				👔 Help		

Neben der Serverliste muss das Management-VPN-Profil einige erforderliche Voreinstellungen enthalten:

- AutomaticCertSelection muss auf true festgelegt werden.
- AutoReconnect muss auf true eingestellt sein.
- AutoReconnectBehavior muss für ReconnectAfterResume konfiguriert werden.
- AutoUpdate muss auf false eingestellt sein.
- BlockUntrustedServers muss auf true festgelegt werden.
- CertificateStore muss für MachineStore konfiguriert werden.
- CertificateStoreOverride muss auf true festgelegt werden.
- EnableAutomaticServerSelection muss auf false festgelegt werden.
- EnableScripting muss auf false festgelegt werden.
- RetainVPNOnLogoff muss auf true eingestellt sein.

Navigieren Sie im AnyConnect Profile Editor zu Voreinstellungen (Teil 1) und passen Sie die Einstellungen wie folgt an:

 \times

File Help

VPN Preferences (Part 1) Preferences (Part 2)	Preferences (Part 1) Profile:nnect -FTD-Lab\.XML Prof	Preferences (Part 1) Profile:nnect -FTD-Lab\.XML Profile\AnyConnect_Management_Tunnel.xml							
Backup Servers Certificate Pinning Certificate Matching Certificate Enrollment Mobile Policy Server List	□ Use Start Before Logon □ Show Pre-Connect Message Certificate Store Windows Machine ~ macOS All ~ Certificate Store Override	User Controllable	^						
	Auto Connect On Start	User Controllable							
		User Controllable							
	Disable Captive Portal Detection	User Controllable							
	🔽 Auto Reconnect	User Controllable							
	Auto Reconnect Behavior ReconnectAfterResume	User Controllable							
	🖂 Auto Update	User Controllable							
	RSA Secure ID Integration	User Controllable							
	Windows Logon Enforcement								
	SingleLocalLogon 🗸								
	Windows VPN Establishment								
	AllowRemoteUsers		~						
	6	Help							

Navigieren Sie dann zu Voreinstellungen (Teil 2), und deaktivieren Sie die Option Automatische Zertifikatauswahl deaktivieren.

 \Box \times

_

File Help

Backup Servers Certificate Pinning Gertificate Matching Certificate Enrollment	Disable Automatic C	ertificate Selection	User Controllable	^				
	Proxy Settings	Native	✓ User Controllable					
	Pt	ublic Proxv Server Address:						
	Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080 Allow Local Proxy Connections							
	Enable Optimal Gate	way Selection	User Controllable					
	Suspension Time T	hreshold (hours)	4					
	Performance Impro	ovement Threshold (%)	20					
	Automatic VPN Polic Trusted Network Po	y blicy	Disconnect ~					
	Untrusted Network	Policy	Connect \lor					
	Trusted DNS Doma	ins						
	Trusted DNS Servers Note: adding all DNS servers in use is recommended with Trusted Network Detection							
	Trusted Servers @	https:// <server>[:<port>]</port></server>						
	https://		Add					
			Delete					
				~				

Schritt 2: AnyConnect VPN-Profil erstellen

Zusätzlich zum Management-VPN-Profil muss das reguläre AnyConnect VPN-Profil konfiguriert werden. Das AnyConnect VPN-Profil wird beim ersten Verbindungsversuch verwendet. Während dieser Sitzung wird das Management-VPN-Profil von FTD heruntergeladen.

Erstellen Sie das AnyConnect VPN-Profil mit dem AnyConnect Profile Editor. In diesem Fall enthalten beide Dateien die gleichen Einstellungen, sodass das gleiche Verfahren ausgeführt werden kann.

Schritt 3: Laden Sie das AnyConnect Management VPN-Profil und das AnyConnect VPN-Profil auf FMC hoch.

Nachdem die Profile erstellt wurden, werden sie als AnyConnect-Dateiobjekte in das FMC hochgeladen.

Um das neue AnyConnect Management VPN-Profil in FMC hochzuladen, navigieren Sie zu **Objects > Object Management** und wählen Sie die **VPN-**Option aus dem Inhaltsverzeichnis aus, und wählen Sie dann die Schaltfläche **AnyConnect-Datei hinzufügen aus**.

Geben Sie einen Namen für die Datei an, wählen Sie **AnyConnect Management VPN Profile** als Dateityp aus, und speichern Sie das Objekt.

 \times



Um das AnyConnect VPN-Profil hochzuladen, navigieren Sie erneut zu **Objects > Object Management** und wählen Sie die **VPN-**Option aus dem Inhaltsverzeichnis aus, und wählen Sie dann die Schaltfläche **AnyConnect-Datei hinzufügen aus**.

Geben Sie einen Namen für die Datei an, wählen Sie jedoch dieses Mal **AnyConnect VPN Profile** als Dateityp aus, und speichern Sie das neue Objekt.

Overview Analysis Policie	es Devices Objects	AMP Intelligen	ce				. Deploy System Help ▼ d	perezve 🔻
Object Management Intrus	sion Rules							
AnyConnect File File objects represent files used in co	nfigurations, typically for remo	te access VPN policies.	They can contain AnyConnect Client Profile and A	nyConnect Clie	nt Image	e files.	Add AnyConnect File	
Security Group lag	Name			Value			Туре	
Security Intelligence DNS Lists and Feeds	Anyconnect4.9_For_Windows	Edit AnyConnec	t File		? ×	.9.01095-webd	AnyConnect Client Image	200
Network Lists and Feeds IIII Lists and Feeds	AnyConnect_Management_Tu					gement_Tunne	AnyConnect Management VPN Profile	2 🖉 🖯
Sinkhole	SSL_AnyConnect.xml	Name:*	SSL_AnyConnect.xml			cml	AnyConnect VPN Profile	200
G SLA Monitor		File Name:*	SSL_AnyConnect.xml	Browse				
Time Zone		File Type:*	AnyConnect VPN Profile	~				
URL		Description:	AnyConnect Client Image AnyConnect VPN Profile	Î				
S Variable Set			AnyConnect Management VPN Profile AMP Enabler Service Profile					
4 😥 VPN			Feedback Profile					
ManyConnect File			ISE Posture Profile		ļ			
8, Certificate Map			NAM Service Profile					
Group Policy			Network Visibility Service Profile	- 1				
IKEv1 IPsec Proposal			Umbrella Roaming Security Profile	- 1				
IKEv1 Policy			web security service Profile	~				
IKEV2 IPsec Proposal	<					Disalaulaa		
V IKEVZ POlicy						Displaying	1 - 5 or 5 rows in a Page 1 or :	1 1 0
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-111	5.cisco.com	How To					uluilu cisco

Profile müssen der Objektliste hinzugefügt und als AnyConnect Management VPN Profile und AnyConnect VPN Profile markiert werden.

Overview Analysis Policie	es Devices Objects	AMP Intelligence			. Peploy System Help ▼	dperezve 🔻
Object Management Intrus	sion Rules					
AnyConnect File File objects represent files used in co	onfigurations, typically for remote	access VPN policies. They can contain	AnyConnect Client Profile and AnyCo	onnect Client Image files.	Add AnyConnect File	
Security Group lag	Name			Value	Туре	
 Security Intelligence DNS Lists and Feeds 	Anyconnect4.9_For_Windows			anyconnect-win-4.9.01095-wel	od AnyConnect Client Image	2 🥒 🖯
Network Lists and Feeds	AnyConnect_Management_Tun	nel		AnyConnect_Management_Tun	ne AnyConnect Management VPN Profil	200
Sinkhole	SSL_AnyConnect.xml			SSL_AnyConnect.xml	AnyConnect VPN Profile	2 🥒 🖯
SLA Monitor						
Time Zone						
Contraction and the second sec						
\$ Variable Set						
📎 VLAN Tag						
A DVPN						
ManyConnect File						
R. Certificate Map						
Group Policy						
REVI IPSec Proposal						
IVENT POlicy	,					
REV2 IPSet Proposal				Displayir	ng 1 - 3 of 3 rows K < Page 1	of 1 > > C
La nate toney				0 opid jii	a contract to the toge	
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115.c	isco.com	How To			uluilu cisco

Schritt 4: Gruppenrichtlinie erstellen

Um eine neue Gruppenrichtlinie zu erstellen, navigieren Sie zu **Objects > Object Management** und wählen Sie im Inhaltsverzeichnis die **VPN-**Option aus, wählen Sie dann **Gruppenrichtlinie aus** und klicken Sie auf die Schaltfläche **Gruppenrichtlinie hinzufügen**.

Wenn das Fenster **Gruppenrichtlinie hinzufügen** geöffnet wird, weisen Sie einen Namen zu, definieren Sie einen AnyConnect-Pool, und öffnen Sie die Registerkarte **AnyConnect**. Navigieren Sie zu **Profile**, und wählen Sie im Dropdown-Menü **Client Profile** das Objekt aus, das das reguläre AnyConnect VPN-Profil darstellt.



Navigieren Sie anschließend zur Registerkarte **Management Profile** (Verwaltungsprofil), und wählen Sie im Dropdown-Menü für das Verwaltungsprofil das Objekt aus, das das Management-VPN-Profil enthält.



Speichern Sie die Änderungen, um das neue Objekt den vorhandenen Gruppenrichtlinien hinzuzufügen.



Schritt 5: Neue AnyConnect-Konfiguration erstellen

Die Konfiguration von SSL AnyConnect in FMC umfasst vier verschiedene Schritte. Um AnyConnect zu konfigurieren, navigieren Sie zu **Devices > VPN > Remote Access** und wählen die Schaltfläche **Add (Hinzufügen)** aus. Hiermit muss der **Remote Access VPN Policy Wizard** geöffnet **werden**.

Wählen Sie auf der Registerkarte "**Richtlinienzuweisung**" das jeweilige FTD-Gerät aus, legen Sie einen Namen für das Verbindungsprofil fest, und aktivieren Sie das Kontrollkästchen SSL.

Overview Analysis Policies Devic	es Objects AMP Intellig	jence			$oldsymbol{\theta}_{1}$ Deploy Syst	em Help 🔻	dperezve 🔻
Remote Access VPN Policy Wiz	ard						
1 Policy Assignment 2 Conne	ection Profile 🔰 3 AnyCo	nnect 🔰 4	Access & Certificate > 🤅	5 Summary			
Targeted Devic This wizard will gui a new user-defined Name:* Description: VPN Protocols: Targeted Devices:	es and Protocols de you through the required minimal : connection profile. AnyConnect_Management_Tunnel SSL IPSec-IKEv2 Available Devices Search Michael Content fidv-fejimene	steps to configure th	e Remote Access VPN policy with Selected Devices	Before Y Before you s configuration complete Rem Authenticati Configure Res or SSO to auti AnyConnect Make sure yo for VPN Cleft the relevant C it during the w Device Inter Interfaces sho targeted devia as a security enable VPN ac	You Start start, ensure the following elements to be in place to ote Access VPN Policy. on Server im or RADIUS Server Group henticate VPN clients. Client Package u have AnyConnect package ti downloaded or you have isco credentials to download vizard. face uld be already configured on cess of that they can be used zone or interface group to cess.		
Last loon on Thursday, 2021-03-25 at 12-01-05 DM	from the units 107 circo com		How To		Back	Next	Cancel

Wählen Sie im Verbindungsprofil Client Certificate Only als Authentifizierungsmethode aus. Dies ist die einzige für die Funktion unterstützte Authentifizierung.

Overview Analysis Policies Devices Objects AMP Intelligence	$igoplus_1$ Deplo	y System	Help 🔻	dperezve 🔻
Device Management NAT VPN > Remote Access QoS Platform Settings FlexConfig Certificates				
Remote Access VPN Policy Wizard				
1 Policy Assignment 2 Connection Profile 3 AnyConnect 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 accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies. Connection Profile Name: AnyConnect_Management_Profile This name is configured as a connection alias, it can be used to connect to the VPN gateway	AAA is			^
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 Only				
Username From Certificate: AAA Only istinguished Name) as username				
Primary Field: SAPL Client Certificate Only				
Secondary Field: Client Certificate & AAA 🗸				
Authorization Server: 🗸 🗸 (Realm or RADIUS)				
Accounting Server:				
Client Address Assignment: Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP ad assignment is tried in the order of AAA server, DHCP server and IP address pool.	fress			
Use AAA Server (Realm or RADIUS only) ()				
	Back	Next		Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To				.1/1.1/1. cisco

Wählen Sie anschließend im Dropdown-Menü **Gruppenrichtlinie** das in Schritt 3 erstellte Gruppenrichtlinienobjekt aus.

Overview Analysis Policies Devices Objects AMP Intell	igence	. Deploy	System	Help 🔻	dperezve	•
Device Management NAT VPN > Remote Access QoS Platfe	orm Settings FlexConfig Certificates					
Remote Access VPN Policy Wizard						
1 Policy Assignment 2 Connection Profile 3 AnyC	connect $>$ 4 Access & Certificate $>$ 5 Summary					
Authorization Server:	(Realm or RADIUS)					^
Accounting Server:	V (RADIUS)					
Client Address Assignment: Client IP address can be assigned from A assignment is tried in the order of AAA s	WAA server, DHCP server and IP address pools. When multiple options are selected, IP addre erver, DHCP server and IP address pool.	is				
Use AAA Server (Realm or RAD Use DHCP Servers Use IP Address Pools	DIUS only) 🕕					
IPv4 Address Pools: A	nyConnect-Pool 🥜					
IPv6 Address Pools:	Ø					
Group Policy:						
A group policy is a collection of user-orie or create a Group Policy object.	ented session attributes which are assigned to client when a VPN connection is established.	elect				
Group Policy:*	nyConnect_Management_Tunnel 🔽 📀					
	AnyConnect_Management_Tunnel					
E	DfltGrpPolicy v					
						~
		Back	Nex	t	Cancel	
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com	How To				սիսի	

Wählen Sie auf der Registerkarte **AnyConnect** das **AnyConnect-Dateiobjekt** entsprechend dem Betriebssystem auf dem Endgerät aus.

Overview Analysis Policies	Devices Objects	AMP Inte	elligence							. Deploy	System	Help 🔻	dperezve 🔻
Device Management NAT V	/PN ► Remote Access	QoS Pla	tform Settings	FlexConfig	Certificates								
Relicy Assignment	Connection Profile		Connect	Access 8	Cortificato		ummany						
Policy Assignment / 2	Connection Prome	3 Any	yconnect	Access o	x certificate	/ 3 5	unninary						
	AnyConnect Client I The VPN gateway can aut initiated. Minimize connect	mage tomatically down tion setup time b	nload the latest Ar by choosing the ap	nyConnect packag propriate OS for t	ge to the client the selected paci	device when t	the VPN cor	nection is	5				
	Download AnyConnect Clie	ent packages from	m Cisco Software I	Download Center.		Show Re-order	r buttons	C					
	AnyConnect File 0	bject Name	AnyConnect C	lient Package N	lame	Operating 9	System						
	Anyconnect4.9_For_	Windows	anyconnect-wir	n-4.9.01095-web	deploy-k9.pkg	Windows		~					
													~
										Back	Nex	t	Cancel
Last login on Saturday, 2021-03-27 at 19	12:55 PM from rtp-vpn1-11	15.cisco.com		How	То								uluilu cisco

Geben Sie unter **Zugriff und Zertifikat** das Zertifikat an, das von der FTD verwendet werden muss, um seine Identität an den Windows-Client zu überprüfen.

Hinweis: Da Benutzer bei Verwendung der Management-VPN-Funktion nicht mit der AnyConnect-App interagieren sollten, muss das Zertifikat voll vertrauenswürdig sein und darf keine Warnmeldung ausdrucken.

Hinweis: Um Fehler bei der Zertifikatsvalidierung zu vermeiden, muss das Feld Common Name (CN) im Betreffnamen des Zertifikats mit dem in der Serverliste der XML-Profile definierten FQDN übereinstimmen (Schritt 1 und Schritt 2).

Overview Analysis Policies Devices Objects AMP Intelligence			System Help	ø dperezve ♥
Device Management NAT VPN • Remote Access QoS Platform Settle	ings FlexConfig Certificates			
Remote Access VPN Policy Wizard				
1 Policy Assignment $>$ 2 Connection Profile $>$ 3 AnyConnect	Access & Certificate 5 Summary			
Interface group/Security Zone:* 0	utside 🗸 🖓			-
V	Enable DTLS on member interfaces			
_				
Device Certificates	rtificate) identifies the VDN estauray to the remote access clients. Select a			
certificate which is used to authenticate to	the VPN gateway.			
Certificate Enrollment:* S	SL_AnyConnect 🗸 🛇			
	Enroll the selected certificate object on the target devices			
Access Control for VPN Traffic				
All decrypted traffic in the VPN tunnel is bypass decrypted traffic from the Access	subjected to the Access Control Policy by default. Select this option to Control Policy.			
Bypass Access Control policy for decr This option bypasses the Access Contr AAA server are still applied to VPN traff	<pre>ypted traffic (sysopt permit-vpn) rol Policy inspection, but VPN filter ACL and authorization ACL downloaded from ic.</pre>			
		Back	Next	Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com	How To			،۱۱،۱۱، cisco

Wählen Sie abschließend auf der Registerkarte **Zusammenfassung die** Schaltfläche **Beenden**, um die neue AnyConnect-Konfiguration hinzuzufügen.



Schritt 6: URL-Objekt erstellen

Navigieren Sie zu **Objekte > Objektverwaltung**, und wählen Sie **URL** aus dem Inhaltsverzeichnis aus. Wählen Sie dann **Objekt hinzufügen** im Dropdown-Menü **URL hinzufügen aus**.

Geben Sie einen Namen für das Objekt ein, und definieren Sie die URL mithilfe desselben FQDN/Benutzergruppen, der in der Liste der Management-VPN-Profilserver (Schritt 2) angegeben ist. In diesem Beispiel muss die URL dperezve.jyoungtalabdomain.cisco.com/AnyConnect_Management_Tunnel lauten.

Overview Analysis Policies	s Devices Objects	AMP Intelligence			$oldsymbol{ extsf{0}}_1$ Deploy	System Help 🔻 dperezve 🔻
Object Management Intrus	ion Rules					
URL	IP address. You can use IIP1 oh	lierts and groups in vario	us places including access control o	vilicies and event searches. For	Add URL	Filter Show Unused Objects
ushelts	None	jeces and groups in vario	us places, including access control p	sides and event searches. For	example, you could inter an acc	cost control rate char blocks a specific
Security Group Tag	Name			van	ue	Overnide
Security Intelligence			No rece	rda ta dianlari		
Notwork Lists and Feeds		New URL Object	INO FECO	ras to display		
IIPL Liete and Foode		New URL Object	S	? X		
Sinkhole		Name N	Management_Tunnel			
SLA Monitor		Description				
Time Range						
Time Zone						
Tunnel Zone		URL	https://dperezve.jyoungta-labdoma			
G URL		Allow Overrides	1			
\$ Variable Set						
💊 VLAN Tag				Save Cancel		
- 🕑 VPN						
🎽 AnyConnect File						
R. Certificate Map						
Croup Policy						
IKEv1 IPsec Proposal						
DIKEv1 Policy						
(A) IKEv2 IPsec Proposal					No data to display	
De TVEvo Dellev					No data to display	or regulation of the second
Last login on Monday, 2021-04-05 at 23	3:55:27 PM from rtp-vpn4-759.cis	co.com	How To			iliili cisco

Speichern Sie die Änderungen, um das Objekt der Objektliste hinzuzufügen.

Schritt 7: URL-Alias definieren

Um die URL-Alias in der AnyConnect-Konfiguration zu aktivieren, navigieren Sie zu **Devices > VPN > Remote Access** und klicken Sie auf das Bleistiftsymbol, um die Alias zu bearbeiten.

Wählen Sie dann auf der Registerkarte Verbindungsprofil die aktuelle Konfiguration aus, navigieren Sie zu Aliases, klicken Sie auf die Schaltfläche Hinzufügen, und wählen Sie das URL-Objekt im Dropdown-Menü URL-Alias aus. Stellen Sie sicher, dass das Kontrollkästchen Aktiviert aktiviert aktiviert ist.

Device Management NAT VPN > Rem AnyConnect_Management_Management_Tunnel Connection Profile:* AnyConnect_Management_Tunnel Enter Description Group Policy:* AnyConnect_Management_Tunnel	Cancel
Connection Profile Access Interfaces	gnments (1)
Alias Names: Add URL Alias ? Incoming users can chan burned on or of URL Alias: Incoming users can chan burned on or of Name: URL Alias: Incoming users can chan burned on or of VEL Alias: Incoming users can chan burned on or of VEL Alias: Incoming users can chan burned on or of VEL Alias: Incoming users can chan burned on or of	0
DefaultWEBVPNGroup OK Cancel	J 🛛
AnyConnect_Management_Tunnel and	6
URL Alias: Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.	
URL Status	
Last login on Monday, 2021-04-05 at 23:55:27 PM from rtp-vpn4-759.cisco.com	սիսիս

Speichern von Änderungen und Bereitstellen von Konfigurationen in FTD

Überprüfung

Nach Abschluss der Bereitstellung ist eine erste manuelle AnyConnect-Verbindung mit dem AnyConnect VPN-Profil erforderlich. Während dieser Verbindung wird das Management-VPN-Profil von FTD heruntergeladen und in C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun gespeichert. Von diesem Zeitpunkt an müssen nachfolgende Verbindungen über das Management-VPN-Profil ohne Benutzerinteraktion initiiert werden.

Fehlerbehebung

Bei Zertifikatsvalidierungsfehlern:

- Stellen Sie sicher, dass das Stammzertifikat der Zertifizierungsstelle (Certificate Authority, CA) in der FTD installiert ist.
- Stellen Sie sicher, dass ein Identitätszertifikat, das von derselben Zertifizierungsstelle signiert wurde, im Windows Machine Store installiert ist.
- Stellen Sie sicher, dass das CN-Feld im Zertifikat enthalten ist und mit dem in der Serverliste des Management-VPN-Profils definierten FQDN und dem in URL-Alias definierten FQDN übereinstimmt.

Für Management-Tunnel nicht initiiert:

- Stellen Sie sicher, dass das Management-VPN-Profil heruntergeladen und in C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun gespeichert wurde.
- Stellen Sie sicher, dass der Name für das Management-VPN-Profil VpnMgmtTunProfile.xml lautet.

Bei Verbindungsproblemen können Sie das DART-Paket sammeln und das Cisco TAC um weitere Informationen bitten.