Configure Secure Client VPN Management Tunnel on Secure Firewall

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Limitations
<u>Configure</u>
Configurations
Step 1. Create AnyConnect Management VPN Profile
Step 2. Create AnyConnect VPN Profile
Step 3. Upload AnyConnect Management VPN Profile and AnyConnect VPN Profile to FMC
Step 4. Create Group Policy
Step 5. Create New AnyConnect Configuration
Step 6. Create URL Object
Step 7. Define URL Alias
<u>Verify</u>
<u>Troubleshoot</u>

Introduction

This document describes how to configure a Secure Client VPN Management tunnel on a Secure Firewall Threat Defense that is managed by the Cisco FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco AnyConnect Profile Editor
- SSL AnyConnect configuration through Firewall Management Center (FMC)
- Client Certificate authentication

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Firewall Threat Defense (FTD) version 6.7.0 (Build 65)
- Cisco FMC version 6.7.0 (Build 65)
- Cisco AnyConnect 4.9.01095 installed on Windows 10 machine

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

In the example, Secure Sockets Layer (SSL) is used to create a Virtual Private Network (VPN) between FTD and a Windows 10 client.

From release 6.7, Cisco FTD supports configuration of AnyConnect Management tunnels. This fixes previously opened enhancement request Cisco bug ID <u>CSCvs78215</u>.

The AnyConnect Management feature allows you to create a VPN tunnel immediately after the endpoint finishes its startup. There is no need that the users manually launch the AnyConnect app. As soon as their system is powered up, the AnyConnect VPN agent service detects the Management VPN feature and initiates an AnyConnect session using theHost Entry defined in the Server List of the AnyConnect Management VPN Profile.

Limitations

- Only Client Certificate authentication is supported.
- Only Machine Certificate Store is supported for Windows clients.
- Not supported on Cisco Firepower Device Manager (FDM) Cisco bug ID <u>CSCvx90058</u>.
- Not supported on Linux clients.

Full limitations are described in the Cisco Secure Client Administrator Guide, Release 5.

Configure

Configurations

Step 1. Create AnyConnect Management VPN Profile

Open the AnyConnect Profile Editor to create AnyConnect Management VPN Profile. The Management Profile contains all the settings used to establish the VPN tunnel after the endpoint boots up.

In this example, a Server List entry that points to Fully Qualified Domain Name (FQDN) dperezve.jyoungta-labdomain.cisco.com is defined and SSL is selected as the primary protocol. To add a Server List, navigate to **Server List** and select **Add** button. Fill the required fields and save changes.

🐴 A	nyConnect	Profile	Editor -	VPN
-----	-----------	---------	----------	-----

VPN		× -
P Server Load Balancing Servers	SCEP Mobile Certificate Pinning	
B C Primary Server		Connection Information
Display Name (required)	AnyConnect_Management_Tunnel	Primary Protocol SSL 🗸
S FQDN or IP Address	User Group	ASA gateway
dperezve.jyoungta-labdom	nain.cisc / AnyConnect_Management_Tunnel	Auth Method During IKE Negotiation EAP-Ar
Group URL		IKE Identity (IOS gateway only)
dperezve.jyoungta-labdom	ain.cisco.com/AnyConnect_Management_Tunnel	
	Backup Servers	
	Host Address	Add
		Move Un
		more op
		Move Down
		Delete
	OK Cancel	
	Heln	

 \times

Besides the Server List, the Management VPN Profile must contain some mandatory preferences:

- AutomaticCertSelection must be set to true.
- AutoReconnect must be set to true.
- AutoReconnectBehavior must be configured for ReconnectAfterResume.
- AutoUpdate must be set to false.
- BlockUntrustedServers must be set to true.
- CertificateStore must be configured for MachineStore.
- CertificateStoreOverride must be set to true.
- EnableAutomaticServerSelection must be set to false.
- EnableScripting must be set to false.
- RetainVPNOnLogoff must be set to true.

In AnyConnect Profile Editor, navigate to Preferences (Part 1) and adjust settings as follows:



$ \Box$ $>$	X
-------------	---

VPN Preferences (Part 1) Preferences (Part 2)	Preferences (Part 1) Profile:nnect -FTD-Lab\.XML Profi	ile\AnyConnect_Management_Tunnel.xml	
Preferences (Part 2) 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 Auto Connect On Start	User Controllable	^
	 Minimize On Connect Local Lan Access Disable Captive Portal Detection Auto Reconnect Auto Reconnect Behavior ReconnectAfterResume 	User Controllable User Controllable User Controllable User Controllable User Controllable User Controllable	
	Auto Update RSA Secure ID Integration Automatic Vindows Logon Enforcement SingleLocalLogon Vindows VPN Establishment AllowRemoteUsers V	User Controllable	~

Then navigate to Preferences (Part 2) and uncheck the Disable Automatic Certificate Selection option.



$ \Box$ \rangle	×
-------------------	---

Disable Automatic Ce	ertificate Selection	User Controllable	^			
Proxy Settings	Native	✓ ✓ User Controllable				
Pu	blic Proxv Server Address:					
No	ote: Enter public Proxv Serve nnections	er address and Port here. Example:10.86.125.33:8080				
Enable Optimal Gate	way Selection	User Controllable				
Suspension Time T	hreshold (hours)	4				
Performance Impro	vement Threshold (%)	20				
Automatic VPN Policy Trusted Network Po	/ licy	Disconnect \lor				
Untrusted Network I	Policy	Connect \checkmark				
Trusted DNS Domai	ns					
Trusted DNS Server	'S					
Note: adding all DNS servers in use is recommended with Trusted Network Detection						
Trusted Servers @	https:// <server>[:<port>]</port></server>					
https://		Add				
		Delete				
			~			

Step 2. Create AnyConnect VPN Profile

As an addition to the Management VPN Profile, the regular AnyConnect VPN Profile needs to be configured. The AnyConnect VPN Profile is used in the first connection try. During this session, the Management VPN Profile is downloaded from FTD.

Use the AnyConnect Profile Editor to create the AnyConnect VPN Profile. In this case, both files contain the same settings so the same procedure can be follow.

Step 3. Upload AnyConnect Management VPN Profile and AnyConnect VPN Profile to FMC

Once the profiles are created, the next step is upload them to the FMC as AnyConnect File objects.

In order to upload the new AnyConnect Management VPN Profile to FMC, navigate to **Objects > Object Management** and choose **VPN** option from the table of contents, then select the **Add AnyConnect File** button.

Provide a name for the file. Choose **AnyConnect Management VPN Profile** as the file type and save the object.

Overview Analysis Policies	s Devices Objects	AMP Intelligen	ce				. Deploy System Help ▼	dperezve 🔻
Object Management Intrus	on Rules							
AnyConnect File File objects represent files used in cor	figurations, typically for remote	e access VPN policies.	They can contain AnyConnect Client Profile and	AnyConnect Clien	: Image	files.	Add AnyConnect File	
Security Group lag	Name			Value			Туре	
DNS Lists and Feeds	Anyconnect4.9_For_Windows	Edit AnyConnec	t File		? XI	9.01095-webd	AnyConnect Client Image	200
Network Lists and Feeds URL Lists and Feeds	AnyConnect_Management_Tu					gement_Tunne	AnyConnect Management VPN Profi	le 👲 🦉 🖬
Sinkhole	SSL_AnyConnect.xml	Name:*	AnyConnect_Management_Tunnel			cml	AnyConnect VPN Profile	2 🥒 🖯
SLA Monitor		File Name:*	AnyConnect_Management_Tunnel.xml	Browse				
Time Zone		File Type:*	AnyConnect Management VPN Profile	~				
Iunnei Zone		Description:	AnyConnect Client Image AnyConnect VPN Profile	^				
\$ Variable Set			AnyConnect Management VPN Profile					
			AMP Enabler Service Profile					
AnyConnect File			ISE Posture Profile	nce	el			
R Certificate Map			NAM Service Profile					
Group Policy			Network Visibility Service Profile					
KEv1 IPsec Proposal			Umbrella Roaming Security Profile					
IKEv1 Policy			Web Security Service Profile	~				
IKEv2 IPsec Proposal	<							>
SIKEv2 Policy						Displaying	1 - 3 of 3 rows 🛛 🕹 🕹 Page 🚺	of 1 > > C
Last login on Saturday, 2021-03-27 at 1	9:12:55 PM from rtp-vpn1-1115	.cisco.com	How To					

Now, in order to upload the AnyConnect VPN Profile navigate again to **Objects > Object Management** and choose **VPN** option from the table of contents, then select the **Add AnyConnect File** button.

Provide a name for the file but this time choose **AnyConnect VPN Profile** as the file type and save the new object.

Overview Analysis Policie	s 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 remot	te access VPN policies.	They can contain AnyConnect Client Profile and	AnyConnect Clier	nt Image	files.	Add AnyConnect File	
Security Group lag	Name			Value			Туре	
DNS Lists and Feeds	Anyconnect4.9_For_Windows	Edit AnyConnec	t File		? ×	.9.01095-webd	AnyConnect Client Image	200
Vetwork 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	205
Ga SLA Monitor		File Name:*	SSL_AnyConnect.xml	Browse				
💮 Time Zone		File Type:*	AnyConnect VPN Profile	~				
Tunnel Zone		Description:	AnyConnect Client Image	^				
\$ Variable Set		Description	AnyConnect VPN Profile AnyConnect Management VPN Profile					
📎 VLAN Tag			AMP Enabler Service Profile					
A BO VPN			Feedback Profile					
ManyConnect File			ISE Posture Profile					
R. Certificate Map			NAM Service Profile					
Group Policy			Network Visibility Service Profile					
REVI IPsec Proposal			Web Security Service Profile					
IKEV1 Policy			The second service frome	•				_
IKEV2 Policy v						Displaying	1 - 3 of 3 rows 🛛 🛠 Page 1 of 3	> > C
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115	5.cisco.com	How To	_				ululu cisco

Profiles must be added to the object list and marked as **AnyConnect Management VPN Profile** and **AnyConnect VPN Profile** respectively.

Overview Analysis Policie	s Devices Objects AMP Intelligence		● Deploy System Help v dp	erezve 🔻
Object Management Intrus	ion Rules			
AnyConnect File File objects represent files used in co	nfigurations, typically for remote access VPN policies. They can contain A	AnyConnect Client Profile and AnyConnect Client Image files.	Add AnyConnect File	
Security Group Tag	Name	Value	Туре	
DNS Lists and Feeds	Anyconnect4.9_For_Windows	anyconnect-win-4.9.0109	5-webd AnyConnect Client Image	2 🥒 🖯
Network Lists and Feeds URL Lists and Feeds	AnyConnect_Management_Tunnel	AnyConnect_Management	t_Tunne AnyConnect Management VPN Profile	2 🥒 🖯
Orice Source Construction Sinkhole SLA Monitor Time Range Time Zone Tunnel Zone URL VIAN Tag VIAN Tag VVN AnyConnect File Cretificate Map E Cretificate Map E Group Policy MEX-1 IPsec Proposal	SSL_AnyConnect.xml	SSL_AnyConnect.xml	AnyConnect VPN Profile	<u>ک</u> 🖉
 IKEv1 Policy IKEv2 IPsec Proposal IKEv2 Policy 	<	Dis	playing 1 - 3 of 3 rows 🛛 🕹 Page 🔟 of 1	>>\¢
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115.cisco.com	How To		cisco

Step 4. Create Group Policy

In order to create a new Group Policy navigate to **Objects > Object Management** and choose **VPN** option from the table of contents, then select **Group Policy** and clic on the **Add Group Policy** button.

Once the **Add Group Policy** window opens, assign a name, define an AnyConnect pool and open the **AnyConnect** tab. Navigate to **Profile** and select the object that represents the regular AnyConnect VPN Profile in the **Client Profile** drop down menu.



Then, navigate to **Management Profile** tab and select the object that contains the Management VPN Profile in the **Management Profile** drop down menu.



Save the changes to add the new object to the existing Group Policies.



Step 5. Create New AnyConnect Configuration

The configuration of SSL AnyConnect in FMC is composed of 4 different steps. To configure AnyConnect navigate to **Devices > VPN > Remote Access** and select the **Add** button. This must open the **Remote Access VPN Policy Wizard**.

On **Policy Assignment** tab, select the FTD device at hand, define a name for the Connection Profile, and check the SSL checkbox.

Overview Analysis Policies Devic Dashboards • Reporting Summary •	es Objects AMP Intelli	igence			€ ₁ Deploy Syste	em Help ▼	dperezve 🔻
Remote Access VPN Policy Wiz	zard						
1 Policy Assignment 2 Conn	ection Profile > 🌖 AnyC	onnect > 4	Access & Certificate	5 Summary			
Targeted Devic This wizard will gui a new user-defined Name:* Description: VPN Protocols: Targeted Devices:	AnyConnect_Management_Tunnel	Add	the Remote Access VPN policy with Selected Devices Rtdv-dperezve	Before You Star Before you start, ene configuration elements complete Remote Access Authentication Server Configure Realm or RAI or SSQ to authenticate AnyConnect Client Pa Make sure you have Ar for VPN Client downlo the relevant Cisco crede it during the wizard. Device Interface Interfaces should be ain targeted devices so tha as a security zone or enable VPN access.	t ure the following to be in place to s VPR Policy. r JUKS Server Group VPN clients. ckage aded or you have entials to download eady configured on t they can be used interface group to		
					Back	Next	Cancel
Last login on Thursday, 2021-03-25 at 17:01:05 PM	from rtp-vpn6-107.cisco.com		How To				

On **Connection Profile**, select **Client Certificate Only** as the authentication method. This is the only authentication supported for the feature.

Overview Analysis Policies Devices Objects AMP In	lligence	🖣 Deploy S	System Help 🔻	dperezve 🔻
Device Management NAT VPN > Remote Access QoS Pi	tform Settings FlexConfig Certificates			
Remote Access VPN Policy Wizard				
1 Policy Assignment 2 Connection Profile 3 Ar	Connect > ④ Access & Certificate > ⑤ Summary			
Connection Profile:				^
Connection Profiles specify the tunne accomplished and how addresses are	group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA i 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			
Authentication, Authorization & A Specify the method of authentication	counting (AAA): (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 SAMI			
Primary Field:	Client Certificate Only			
Secondary Field:	Client Certificate & AAA			
Authorization Server:	✓ (Realm or RADIUS)			
Accounting Server:	✓ (RADIUS)			
Client Address Assignment:				
Client IP address can be assigned fro assignment is tried in the order of AJ	AAA server, DHCP server and IP address pools. When multiple options are selected, IP address server, DHCP server and IP address pool.			
Use AAA Server (Realm or	ADIUS only) 🕕			
Use DHCP Servers				~
		Back	Next	Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com	How To			،رار،رار، cisco

Then select the Group Policy object created in step 3 in the Group Policy drop down.

				-		-
Overview Analysis Policies Devices Objects AMP	Intelligence		eploy	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 &	k Certificate > ち Summary				
Authorization Server:		▼ (Realm or RADIUS)				^
Accounting Server:		V (RADIUS)				
Client Address Assignment:						
Client IP address can be assigned assignment is tried in the order of	from AAA server, DHCP server and IP a AAA server, DHCP server and IP addre	ddress pools. When multiple options are selected, IP address ss pool.	i.			
Use AAA Server (Realm	or RADIUS only) 🕕					
Use DHCP Servers						
Use IP Address Pools						
IPv4 Address Pools	2: AnyConnect-Pool	la l				
IPv6 Address Pools	*	Ø				
Group Policy:						
A group policy is a collection of us or create a Group Policy object.	er-oriented session attributes which are	e assigned to client when a VPN connection is established. Se	lect			
Group Policy:*	AnyConnect_Management_Tunnel	× 0				
	AnyConnect_Management_Tun	nel <u></u>				
	DfltGrpPolicy					
			Back	Nex	t	Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com	How	То				որոր

On **AnyConnect** tab, select the **AnyConnect File Object** according to the Operating System (OS) on the endpoint.

Overview Analysis Policies	Devices Objects AMP Intel	lligence		. Deploy Syst	em Help v	dperezve 🔻
Device Management NAT V	/PN ► Remote Access QoS Plat	form Settings FlexConfig Certificates				
1) Policy Assignment	Connection Profile	Connect	S Summany			
1 Policy Assignment 2	S Any	Access & Certificate				^
	AnyConnect Client Image The VPN gateway can automatically downly initiated. Minimize connection setup time by	bad the latest AnyConnect package to the client choosing the appropriate OS for the selected pac	device when the VPN connection is kage.			
	Download AnyConnect Client packages from	Cisco Software Download Center.	Show Re-order buttons			
	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System			
	Anyconnect4.9_For_Windows	anyconnect-win-4.9.01095-webdeploy-k9.pkg	Windows 👻			
				Back	Next	Cancel
Last login on Saturday, 2021-03-27 at 19:	:12:55 PM from rtp-vpn1-1115.cisco.com	How To				

On Access & Certificate, specify the certificate that must be used by the FTD to probe its identity to the Windows client.

Note: Since users cannot interact with AnyConnect app when using the Management VPN feature, the certificate needs to be fully trusted and must not print any Warning message.

Note: In order to prevent certificate validation errors, the Common Name (CN) field included in the Subject Name of the certificate must match the FQDN defined in the Server List of XML profiles (Step 1 and Step 2).



Finally, select **Finish** button on the **Summary** tab to add the new AnyConnect Configuration.



Step 6. Create URL Object

Navigate to **Objects > Object Management** and select **URL** from the table of contents. Then select **Add Object** in the **Add URL** drop down.

Provide a name for the object and define the URL using the same FQDN/User Group specified in the Management VPN Profile Server List (Step 2). In this example, URL must be dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel.

Overview Analysis Policie	s Devices Objects	AMP Intelligence				tem Help v dperezve v
Object Management Intrus	ion Rules					
URL					Add URL •	Filter
URL object represents a single URL or	r IP address. You can use URL ob	ects and groups in variou	us places, including access control p	olicies and event searches. For exam	nple, you could write an access co	ntrol rule that blocks a specific
Security Group Tag	Name			Value		Override
 Security Intelligence 						
DNS Lists and Feeds			No reco	rds to display		
Network Lists and Feeds		New URL Object	s	? ×		
URL Lists and Feeds		Namo				
Sinkhole		Name	tanagement_Tunnel			
G SLA Monitor		Description				
Time Range						
🗑 Time Zone						
and Tunnel Zone		UKL h	ttps://dperezve.jyoungta-labdoma			
() URL		Allow Overrides]			
S Variable Set				Save Cancel		
A DuConnect Ello						
Certificate Man						
Group Policy						
M IKEV1 IPsec Proposal						
B IKEV1 Policy						
IKEv2 IPsec Proposal						
De treve Dollar					No data to display	< Page 1 of 1 > > C
						. de els
Last login on Monday, 2021-04-05 at 2	3:55:27 PM from rtp-vpn4-759.cise	o.com	How To			cisco

Save the changes to add the object to the object list.

Step 7. Define URL Alias

In order to enable the URL Alias in the AnyConnect configuration, navigate to **Devices** > **VPN** > **Remote Access** and click on the pencil icon to edit.

Then, on the **Connection Profile** tab, select the configuration at hand, navigate to **Aliases**, click on **Add** button, and select the **URL Object** in the **URL Alias** drop down . Ensure the **Enabled** check box is selected.

Overview Analysis Policies Device	Edit Connection Pro	file	? : >	🖣 Deploy System Help 🔻 dperezve 🔻
Device Management NAT VPN ▶ Rem AnyConnect_Management_	Connection Profile:*	AnyConnect_Management_Tunnel		Policy Assignments (1)
Connection Profile Access Interfaces Name DefaultWEBVPNGroup AnyConnect_Management_Tunnel	Alias Names: Incoming users can ch can be turned on or of Name	Add URL Aliases	? s configured on this device	nel 2 5
	URL Alias: Configure the list of URI system will automatical	L allas which your endpoints can select on web access. Iy log them in via this connection profile. Stat	If users choose the following URLs,	
			Save Cancel	
Last login on Monday, 2021-04-05 at 23:55:27 PM from	n rtp-vpn4-759.cisco.com	How To		cisco

Save changes and deploy configurations to FTD.

Verify

After the deployment finishes, a first manual AnyConnect connection with the AnyConnect VPN Profile is needed. During this connection the Management VPN Profile is downloaded from FTD and stored in C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun. From this point, subsequent connections must be initiated through the Management VPN profile without any user interaction.

Troubleshoot

For certificate validation errors:

- Ensure the root certificate for Certificate Authority (CA) is installed on the FTD.
- Ensure an identity certificate signed by the same CA is installed on Windows Machine Store.
- Ensure the CN field is included in the certificate and is the same as the FQDN defined in the Server List of the Management VPN Profile and FQDN defined in URL alias.

For Management tunnel not initiated:

- Ensure the Management VPN Profile has been downloaded and stored in C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun.
- Ensure the name for the Management VPN Profile is **VpnMgmtTunProfile.xml**.

For connectivity problems, collect DART bundle and contact Cisco TAC for further research.