ASA での AnyConnect 管理 VPN トンネルの設 定

内容 <u>はじめに</u> 前提条件 要件 <u>使用するコンポーネント</u> 背景説明 管理トンネルの動作 制限事項 設定 <u>ASDM/CLIを使用したASAでの設定</u> AnyConnect管理VPNプロファイルの作成 AnyConnect管理VPNプロファイルの展開方法 <u>(オプション)Tunnel-All設定をサポートするカスタム属性を設定します</u> 確認 <u>トラブルシュート</u> 関連情報

はじめに

このドキュメントでは、VPNゲートウェイが管理VPNトンネルを介してAnyConnectセキュアモビ リティクライアントからの接続を受け入れるようにASAを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ Adaptive Security Device Manager(ASDM)によるVPN設定
- ・基本的な適応型セキュリティアプライアンス(ASA)のCLI設定
- X509証明書

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ Cisco ASAソフトウェアバージョン9.12(3)9
- ・ Cisco ASDMソフトウェアバージョン7.12.2

Cisco AnyConnectセキュアモビリティクライアントバージョン4.8.03036がインストールされたWindows 10

◆ 注: AnyConnect VPN Web deployパッケージ(anyconnect-win*.pkg or anyconnect-macos*.pkg)は、Cisco Software Download(登録ユーザ専用)からダウンロードします。リモートユーザコンピュ ータにダウンロードされるASAのフラッシュメモリにAnyConnect VPNクライアントをコピ ーし、ASAとのSSL VPN接続を確立します。詳細については、ASAコンフィギュレーショ ンガイドの「AnyConnectクライアントのインストール」セクションを参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

管理VPNトンネルは、エンドユーザによってVPN接続が確立される場合だけでなく、クライアン トシステムの電源が投入されるたびに企業ネットワークへの接続を保証します。オフィス外のエ ンドポイント、特にユーザがVPN経由でオフィスのネットワークにほとんど接続していないデバ イスに対して、パッチ管理を実行できます。企業ネットワーク接続を必要とするエンドポイント OSログインスクリプトでも、この機能を利用できます。

AnyConnect管理トンネルを使用すると、管理者はユーザがログインする前に、ユーザの介入なし でAnyConnectを接続できます。AnyConnect管理トンネルはTrusted Network Detection(TND)と組 み合わせて動作できるため、エンドポイントがオフプレミスで、ユーザが開始したVPNから切断 された場合にのみトリガーされます。AnyConnect管理トンネルはエンドユーザに対して透過的で 、ユーザがVPNを開始すると自動的に切断されます。

OS/アプリケーション	最小バージョン要件
ASA	9.0.1
ASDM	7.10.1
Windows AnyConnectバージョン	4.7.00136
macOS AnyConnectバージョン	4.7.01076
Linux	サポートされていない

管理トンネルの動作

AnyConnect VPNエージェントサービスは、システムの起動時に自動的に開始されます。管理ト ンネル機能が(管理VPNプロファイルを介して)有効になっていることが検出されるため、管理 クライアントアプリケーションが起動されて管理トンネル接続が開始されます。管理クライアン トアプリケーションは、管理VPNプロファイルからのホストエントリを使用して接続を開始しま す。次に、VPNトンネルは通常どおり確立されますが、例外が1つあります。管理トンネルはユ ーザに対して透過的に動作するように意図されているため、管理トンネルの接続中にソフトウェ アの更新は行われません。

ユーザはAnyConnect UIを使用してVPNトンネルを開始し、これにより管理トンネルの終端がト リガーされます。管理トンネルが終端すると、ユーザトンネルの確立は通常どおり継続されます 。

ユーザがVPNトンネルの接続を解除すると、管理トンネルの自動再確立がトリガーされます。

制限事項

- ユーザーの操作はサポートされていません
- ・ マシン証明書ストア(Windows)による証明書ベースの認証のみがサポートされます
- 厳密なサーバ証明書チェックが適用される
- プライベートプロキシはサポートされていません
- パブリックプロキシはサポートされていません(ネイティブプロキシ設定がブラウザから取 得されないプラットフォームでは、ProxyNative値がサポートされています)
- AnyConnectカスタマイズスクリプトはサポートされていません

SV 注:詳細については、「<u>管理VPNトンネルについて</u>」を参照してください<u>。</u>

設定

このセクションでは、Cisco ASAをVPNゲートウェイとして設定し、管理VPNトンネル経由で AnyConnectクライアントからの接続を受け入れる方法について説明します。

ASDM/CLIを使用したASAでの設定

ステップ 1: AnyConnectグループポリシーを作成します。に移動しConfiguration > Remote Access VPN > Network (Client) Access > Group Policiesます。をクリックします。Add

✤ 注:新しいAnyConnectグループポリシーを作成することをお勧めします。このポリシーは、AnyConnect管理トンネルのみに使用されます。



ステップ2:グループポリシーのName「」を指定します。を割り当て/作成しAddress Poolます。次の 図に示すように、Tunneling Protocols **as**SSL VPN Client **and/or**IPsec IKEv2を選択します。

		Edit Internal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers	Name: AnyConnect_MGMT_	Tunnel	
► Advanced	Banner: 🗹 Inherit		
	SCEP forwarding URL: 🗹 Inherit		
	Address Pools: Inherit VPN_Po	ool	Select
	IPv6 Address Pools: 🗹 Inherit		Select
	More Options		*
	Tunneling Protocols:	Inherit Clientless SSL VPN 🗹 SSL VPN Client IPsec IKEv1 🗹 IPsec IKEv2 L2TP/IPsec IKEv2	sec
	Filter:	☑ Inherit	Manage
	Access Hours:	✓ Inherit	Manage
	Simultaneous Logins:	✓ Inherit	
	Restrict access to VLAN:	✓ Inherit	
	Connection Profile (Tunnel Group) Lock:	✓ Inherit	
	Maximum Connect Time:	✓ Inherit Unlimited minutes	
	Idle Timeout:	✓ Inherit None minutes	
	Security Group Tag (SGT):	✓ Inherit None (2 – 65519)	
	On smart card removal:	✓ Inherit Oisconnect Keep the connection	
	Timeout Alerts		
	Maximum Connect Time Alert Interval:	✓ Inherit Default minutes	
	Periodic Certificate Authentication Interval	I: 🗹 Inherit 🗌 Unlimited hours	
Find:	Next	Previous	
		Help Cancel OK	

ステップ3: に移動しAdvanced > Split Tunnelingます。図に示すようにPolicy、を設定しTunnel Network List Below、Network Listを選択します。

• • •		Edit Internal G	I Group Policy: AnyConnect_MGMT_Tunnel	
General Servers Advanced Split Tunneling Browser Proxy b AnyConnect Client	The VPN client makes split tunneling der fields. DNS Names: Send All DNS Lookups Through Tunnel:	isions on the Inherit	the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'N	etworl
▶ IPsec(IKEv1) Client	Policy: IPv6 Policy:	🗌 Inherit 🗹	Tunnel Network List Below	
•	Network List: Pressing this button to set up split exlus Set up Split Exclusion for Web Securi Intercept DHCP Configuration Message	Inherit	VPN-Split C b Security proxies. psoft Clients	Manag
Find:	Next G	Previous		
		Help	elp Cancel OK	

注:クライアントアドレスが両方のIPプロトコル(IPv4とIPv6)に対してプッシュされてい ない場合、対応するトラフィックが管理トンネルによって中断されないようにClient Bypass Protocol設定する必要がありますenabled。設定するには、「ステップ4」を参照してください。

ステップ4: に移動しAdvanced > AnyConnect Clientます。 に設定Client Bypass Protocol し Enableます。 図に示す ように、OK[Save]をクリックします。

•		Add Internal Group Policy	
General	Keep Installer on Client System:	🗹 Inherit 🔿 Yes 💿 No	
Servers Advanced	Datagram Transport Layer Security (DTLS):	✓ Inherit	
Split Tunneling	DTLS Compression:	🗹 Inherit 🔷 Enable 🔷 Disable	
Browser Proxy AnyConnect Client	SSL Compression:	☑ Inherit O Deflate O LZS O Disable	
▶ IPsec(IKEv1) Client	Ignore Don't Fragment(DF) Bit:	☑ Inherit 🔹 Enable 🔹 Disable	
	Client Bypass Protocol:	Inherit O Enable	
	FQDN of This Device:	V FQDN	
	MTU:	🗹 Inherit	
	Keepalive Messages:	☑ Inherit Disable Interval: seconds	
	Optional Client Modules to Download:	🗹 Inherit	
	Always-On VPN:	☑ Inherit O Disable O Use AnyConnect Profile setting 0	
	Client Profiles to Download:	🗹 Inherit	
		Add 1 Delete	
		Profile Name Profile Usage/Type	
ind:	💿 Next 💿	Previous	

ステップ5:次の図に示すように、をクリックしてApply、設定をASAにプッシュします。

🔥 Home 🔩 Configuration 📴 Monitoring 🔚	🕽 Save 🔇 Refresh 🔇 Back 🔘 Forw	rard ? Help Type topic Go			diada
000 Remote Access VPN	Configuration > Remote Acc	cess VPN > Network (Client) Acce	ss > Group Policies		
Introduction Introduction AnyConnect Connection Profiles AnyConnect Customization/Localizati AnyConnect Client Profile AnyConnect Client Profile	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes f Add - If Edit Delete As	roup is a collection of user-oriente VPN connection profiles and user a from an LDAP server you must use sign	ed authorizzation attribute/value pairs that may be stored i ccounts. an <u>LDAP attribute map</u> .	nternally on the device or externally on a RADIUS/LDAP server. The group	
Dynamic Access Policies	Name	Type	Turneling Protocol	Connection Profiles/Users	
S Group Policies	American	Internal	ed dies	Assigned To	_
IPsec(IKEv1) Connection Profiles	DftCrnPolicy (System Default)	Internal	ikev1:ikev2:12tn_insec	DefaultRACrown: DefaultI 21 Grown: DefaultADMINGrown: DefaultR	Æ
Psec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel	
 Address Assignment Advanced Clientiss SSL VPN Access An/Local Users An/Local Users DAP Attribute Map					
Firewall Remote Access VPN					
Site-to-Site VPN	Find:	Match Case			
Device Management			Reset		

グループポリシーのCLI設定:

<#root>

ip local pool

VPN_Pool

192.168.10.1-192.168.10.100 mask 255.255.255.0 !

access-list

VPN-Split

standard permit 172.16.0.0 255.255.0.0 !

group-policy

AnyConnect_MGMT_Tunnel

internal group-policy

AnyConnect_MGMT_Tunnel

attributes vpn-tunnel-protocol

ikev2 ssl-client

split-tunnel-network-list value

VPN-Split

address-pools value

VPN_Pool

手順 6: AnyConnect接続プロファイルを作成します。に移動しConfiguration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profileます。 をクリックします。Add

✤ 注:新しいAnyConnect接続プロファイルを作成することをお勧めします。このプロファイ ルは、AnyConnect管理トンネルのみで使用されます。



手順7: Connection ProfileにNameを指定し、として設定Authentication MethodCertificate onlyします。ス<u>テッ</u> <u>プ1</u>で作成したとしてGroup Policy、を選択します。

Basic Adversed	Name:	AnyConnect_MGMT_Tunnel	
Advanced	Aliases:		
	Authentication		
	Method:	Certificate only	
	AAA Server Group:	LOCAL	ᅌ Manage
		Use LOCAL if Server Group fails	
	SAML Identity Provider		
	SAML Server :	None	S Manage
	Client Address Assignmen	it —	
	DHCP Servers:		
		• None OHCP Link OHCP Subnet	
	Client Address Pools:		Select
	Client IPv6 Address Poo	ls:	Select
	Default Group Policy		
	Group Policy:	AnyConnect_MGMT_Tunnel	Manage
	(Following fields are lin	ked to attribute of the group policy selected above.)	
	✓ Enable SSL VPN cl	ient protocol	
	Enable IPsec(IKEv)	2) client protocol	
	DNS Servers:		
	WINS Servers:		
	Domain Name:		
Find:		Next Previous	

◆ 注:ローカルCAからのルート証明書がASAに存在することを確認します。 証明書を追加または表示するには、Configuration > Remote Access VPN > Certificate Management > CA Certificatesに移動します。

◆ 注:同じローカルCAによって発行されたID証明書が、マシン証明書ストア(Windowsの場合)またはシステムキーチェーン(macOSの場合)に存在することを確認してください。

ステップ 8:に移動しAdvanced > Group Alias/Group URLます。のAdd下をクリックしGroup URLs、を追加し URLます。がオンになっていることを確認しますEnabled。図に示すように、OK[Save]をクリックし ます。 Add AnyConnect Connection Profile

Basic Advanced Ceneral Client Addressing Authentication Secondary Authentication Authorization Accounting Group Alias/Group URL	 Enable the display of Radius Reject-Message on the login screen when authentication is rejected Enable the display of Securld messages on the login screen Connection Aliases This SSL VPN access method will present a list of aliases configured for all connection profiles. You r the Login Page Setting in the main panel to complete the configuration. Add Delete (The table is in-line editable.) Alias
	Group URLs This SSL VPN access method will automatically select the connection profile, without the need for use Add Delete (The table is in-line editable.) URL Enabled URL: https://asa.example.com/AnyConnect_MGMT_Tunnel I Enabled Help Cancel OK
Find:	Next Previous Help Cancel OK

IKEv2を使用する場合は、AnyConnectに使用するインターフェイスでIPsec (IKEv2) Access、が有効になっていることを確認します。

○ ○ ○ Remote Access VPN	Config	uration > Remot	e Access VPN > N	Network (Client) A	ccess > AnyConnect Co	Inection Profiles
Introduction Network (Client) Access AnyConnect Connection Profiles	The security Client suppo	appliance automa rts IPsec (IKEv2) tu	tically deploys the unnel as well as SS	e Cisco AnyConnec SL tunnel with Data	t VPN Client to remote us gram Transport Layer Sec	rs upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN urity (DTLS) tunneling options.
AnyConnect Customization/Local AnyConnect Client Profile AnyConnect Client Software	Enable C SSL access r	isco AnyConnect nust be enabled if	VPN Client access you allow AnyCon	on the interfaces :	selected in the table below wurched from a browser ((eb Launch) .
Group Policies	Interface	SSL Access Allow Access	Enable DTLS	IPsec (IKEv2) Acce Allow Access	Enable Client Services	Device Certificate
Secure Mobility Solution	outside inside					Port Settings

ステップ9:をクリック_{Apply}して、設定をASAにプッシュします。



接続プロファイル(トンネルグループ)のCLI設定:

<#root>

tunnel-group

AnyConnect_MGMT_Tunnel

type remote-access
tunnel-group

AnyConnect_MGMT_Tunnel

general-attributes

default-group-policy AnyConnect_MGMT_Tunnel

tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes

authentication certificate group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable

ステップ 10:信頼できる証明書がASAにインストールされ、AnyConnect接続に使用されるイン ターフェイスにバインドされていることを確認します。に移動してConfiguration > Remote Access VPN > Advanced > SSL Settings、この設定を追加または表示します。

注:「<u>ASAへのID証明書のインストール</u>」を参照してください。

Remote Access VPN	○ ○ ○ Configuration > Remote Acce	ess VPN > Advanced > SSL Settings				
Introduction	r					
Network (Client) Access	Configure SSL parameters. These pa	rameters affect both ASDM and SSL VPN acc	ess.			
AnyConnect Customization AnyConnect Client Profile	The minimum SSL version for the se	curity appliance to negotiate as a "server":	TLS V1	0	OTLSV1 OTLSV1.2	
AnyConnect Client Softwar	The minimum SSL version for the se	curity appliance to negotiate as a "client":	TLS V1	C		
Group Policies	Diffie-Hellman group to be used with	th SSL:	Group2 - 1024-bit modulus	C		
IPsec(IKEv1) Connection P IPsec(IKEv2) Connection P	ECDH group to be used with SSL:		Group19 - 256-bit EC	S		
Secure Mobility Solution	Encountion					
Address Assignment	Encryption					_
Advanced	Cipher Version	Cipher Security Level		Cipher Algorithm	is/ Custom String	Edit
Clientless SSI VPN Access	Default	Medium		DES-CBC3-SHA	AES128-SHA DHE-RSA-AES128-SHA AES256-SHA DHE-RSA	
AA II ogst Urger	TLSV1	Medium		DHE-RSA-AES2	56-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
www.cocar osers	TLSV1.1	Medium		DHE-RSA-AES2	56-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
AAA Server Groups	TLSV1.2	Medium		ECDHE-ECDSA-	AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D	
CDAP Attribute Map	DTLSV1	Medium		DHE-RSA-AES2	56-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
🗊 Local Users	DTLSV1.2	Medium		ECDHE-ECDSA-	AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D	
Secure Desktop Manager						
Certificate Management						
Language Localization						
load Balancing						
DHCP Server	Server Name Indication (SNI)					
DNS	Domain		Certificate			Add
Advanced						E-dia
SSL Settings						Edit
Reference Identity						Delet
Certificate to AnyConnect						
HTTP Redirect						
Maximum VPN Sessions						
Crypto Engine						
	Cartificatos					
	Constitution and first of	should be used for ffit with only of	ab landars. The follows a set	will be used as 1 and	and and an an allowed with a second finance of shares	
	specity which certificates, if any,	should be used for SSL authentication on ea	ich interrace. The failback certificate	will be used on interra	ces not associated with a certificate of their own.	
	Interface	Primary Certificate	Load Balancing Certificate		Key-Type	Edit
evice Setup	inside		-			Lon
	management					
rewall	outside	ROOT_CA:bostname=ASA_example	(0)		Primary: RSA (2048 hits) Load Balancing: pope	
emote Access VPN		proof eventstaame=Asktexample	icon i		change to the oney, court takening, none	
te-to-Site VPN						
evice Management						

SSLトラストポイントのCLI設定:

<#root>

ssl trust-point ROOT-CA outside

AnyConnect管理VPNプロファイルの作成

ステップ1: AnyConnectクライアントプロファイルを作成します。に移動しConfiguration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profileます。図に示すように、をクリックしますAdd。

ổ H	lome 🖏 Configuration 📴 Monitor	ing 🔚 Save 🔇 Refresh 🔇 Back (Sorward ? Help Type topic Go			cisco
	Remote Access VPN	O O O Configuration > Remote Ac	cess VPN > Network (Client) Access > AnyCon	nect Client Profile		
Boolmarks Device Lis	Inroduction Inroduction Monoret Connection Profil AnyConnect Customization/Lc AnyConnect Clustomization/Lc AnyConnect Client Profile AnyConnect Client Software Pynamic Access Policies Group Policies	This panel is used to manage AnyC button to add a new profile. Pressin The profile Usage field is introduce HostScan configuration can be perf	onnect Client Profiles and perform group assignn ng the Import or Export button is for upload and a d with the Secure Mobility Solution. This field con formed by going to Secure Desktop Manager/Hos Policy Delete The Import Secure Cashed	nent for AnyConnect version 2.5 or later.You can select lownload of client profiles between local machine and ntains different profile usage in AnyConnect version 3. IScan. If 'HostScan' is not visible under 'Secure Deskto	: a profile to edit, change group or to delete. You can select the 'Add' device. 0 and later. Manager', you will need to restart ASDM.	
	IPsec(IKEv1) Connection Profil	Profile Name	Profile Usage	Group Policy	Profile Location	
	Plexc(KEV2) Connection Profil Psec(KEV2) Connection Profil Advanced Advanced Advanced Advanced AAA.cocal Users AAA.cocal Users AAA.cocal Users Call Charl Xethoute Map Call Cocal Users Call Charl Attribute Map Call Charl Matching Call Charl Attribute Map Call Charl Matching Call Charl Attribute Map Call Charl Matching Charl Matc		i tonin Suga			
	Reference Identity					
	HTTP Redirect MATTP Redirect Maximum VPN Sessions					
	-					
	Device Setup					
	🚰 Firewall					
	Remote Access VPN					
	🚰 Site-to-Site VPN					
	Device Management					
	20 *			Reset Apply		

ステップ 2:Profile Nameを指定します。asを選択しProfile UsageAnyConnect Management VPN profileます。ステ <u>ップ1</u>で作成したGroup Policyを選択します。図に示すように、をクリックしますOK。

le Name		Profile Usage	Group Policy	Profile Location
	• • •	Add AnyConnect Client R	Profile	
	Profile Name	AnyConnect_MGMT_Profile		
	Profile Usage	AnyConnect Management VPN Profile	.	
	Enter a device f created if it doo	' ile path for an xml file, ie. disk0:/ac_profile. The file es not exist.	will be automatically	
	Profile Location	disk0:/anyconnect_mgmt_profile.vpnm	Browse Flash	
			Upload	
	Group Policy	AnyConnect_MGMT_Tunnel	0	
	,	Enable 'Always On VPN' for selected group		
		Help Cancel	ОК	
			Reset Apply	

ステップ3:作成したプロファイルを選択し、図に示すようにEditをクリックします。

Name	Profile Usage	Group Policy	Profile Location
onnect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm

ステップ4:に移動しServer Listます。クリックAdd して、図に示すように、新しいサーバリストエントリを追加します。

VPN Preferences (Part 1) Preferences (Part 2)	Server List				
() · · · · · · · · · · · · · · · · · · ·					
Certificate Matching	Hostname	Host Address	User Group	Backup Server List	Certificate Pins
	Note: at most o	one server can be define	d in a management VP	N profile. Add Edit	Delete Details
•					

ステップ 5: Display Nameを指定します。ASAのFQDN/IP addressを追加します。をトンネルグループ名として指定しますUser Group。はGroup URL、FQDN andで自動的に設定されますUser Group。をクリックします。OK

Primary Server Display Name (required) AnyConnect_MGMT_Tunnel FQDN or IP Addr User Group (required) asa.example.com / AnyConnect_MGMT. Group URL asa.example.com/AnyConnect_MGMT_Tunnel Backup Servers Host Address	Connection Information Primary Protocol SSL ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect IKE Identity (IOS gateway only) Add
ОК	Move Up Move Down Delete

Ŷ 注:FQDN/IPアドレス+ユーザグループは、ステップ8でAnyConnect接続プロファイルを設定するときに指定したグループURLと同じである必要があります。

◆ 注:プロトコルとしてIKEv2を使用するAnyConnectは、ASAへの管理VPNを確立するためにも使用できます。ステップ5でPrimary Protocol、がに設定されていることを確認しますIPsec。

手順6:図に示すように、クリックしてок[保存]をクリックします。

8 🗍 🖶	AnyCor	nnect Client Profile Edit	or - AnyConnect_MGM	T_Profile	
Profile: AnyConnect_MG	GMT_Profile				Abou
VPN Preferences (Part 1) Preferences (Part 2)	Server List				
Backup Servers Certificate Pinning Certificate Matching Server List	Hostname AnyConnect_MGMT_T	Host Address	User Group AnyConnect_MGMT_	Backup Server List T Inherited	Certificate Pins
	Note: at most one	server can be defined	in a management VPN	profile. Add Edit	Delete Details
		Help Ca	ncel OK]	

手順7:図Applyに示すように、をクリックして設定をASAにプッシュします。



AnyConnect管理VPNプロファイル追加後のCLI設定

<#root> webvpn enable outside hsts enable max-age 31536000 include-sub-domains no preload no anyconnect-essentials anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm anyconnect enable tunnel-group-list enable cache disable error-recovery disable group-policy AnyConnect_MGMT_Tunnel internal group-policy AnyConnect_MGMT_Tunnel attributes vpn-tunnel-protocol ikev2 ssl-client split-tunnel-network-list value VPN-Split client-bypass-protocol enable address-pools value VPN_Pool

webvpn

ļ

AnyConnectクライアントマシンのAnyConnect管理VPNプロファイル:

<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSc
<ClientInitialization>
<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>
```

true

<ShowPreConnectMessage>false</ShowPreConnectMessage>

Machine

System

true

<ProxySettings>IgnoreProxy</ProxySettings> <AllowLocalProxyConnections>true</AllowLocalProxyConnections> <AuthenticationTimeout>30</AuthenticationTimeout>

--- Output Omitted ---

<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover> <AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>

AnyConnect_MGMT_Tunnel

asa.example.com

</AnyConnectProfile>



注:エンドユーザPCでは、管理VPNプロファイルでTND設定が有効になっており、ユーザ VPNプロファイルがない場合、ユーザVPNプロファイルがない代わりに、TNDのデフォル ト設定(ACクライアントアプリケーションのデフォルト設定で無効)が考慮されます。こ の不一致により、予期しない動作や未定義の動作が発生する可能性があります。 デフォルトでは、TND設定はデフォルト設定で無効になっています。 AnyConnect Clientアプリケーションのデフォルト設定ハードコード設定を克服するには、 エンドユーザPCに2つのVPNプロファイル(ユーザVPNプロファイルとAC管理VPNプロフ ァイル)が必要で、両方に同じTND設定が必要です。 管理VPNトンネルの接続および切断のロジックは、管理VPNトンネルを確立するために、 ACエージェントはユーザVPNプロファイルTND設定を使用し、管理VPNトンネルの切断に は、管理VPNプロファイルTND設定を確認することです。

AnyConnect管理VPNプロファイルの展開方法

VPNゲートウェイからAnyConnect管理VPNプロファイルをダウンロードするには、ASA接続プロファイルを使用してユーザVPN接続が正常に完了します。

✤ 注:管理VPNトンネルに使用されるプロトコルがIKEv2の場合、最初の接続は(ASAから AnyConnect管理VPNプロファイルをダウンロードするために)SSLを介して確立する必要 があります。

• AnyConnect管理VPNプロファイルは、GPOプッシュまたは手動インストール(プロファイル

の名前がVpnMgmtTunProfile.xmlであることを確認)によってクライアントマシンに手動でアップロードできます。

プロファイルを追加する必要があるフォルダの場所:

Windows : C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun macOS: /opt/cisco/anyconnect/profile/mgmttun/

(オプション)Tunnel-All設定をサポートするカスタム属性を設定します

管理VPNトンネルでは、ユーザが開始するネットワーク通信に影響を与えないように、デフォル トでトンネリング設定を含むスプリットが必要です。これは、管理トンネル接続で使用されるグ ループポリシーでカスタム属性を設定する場合に上書きできます。

ステップ1:に移動しConfiguration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributesます。図に示すように、をクリックします。



ステップ2.カスタム属性タイプをに設定ManagementTunnelAllAllowed し、を指定Descriptionします。図に示すように、をクリックしますOK。

O O O Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes

	Description
• • •	Create Custom Attribute Type
• • • Type:	Create Custom Attribute Type ManagementTunnelAllAllowed
• • • Type:	Create Custom Attribute Type ManagementTunnelAllAllowed ManagementTunnelAllAllowed
Type: Description	Create Custom Attribute Type ManagementTunnelAllAllowed ManagementTunnelAllAllowed
Type: Description	Create Custom Attribute Type ManagementTunnelAllAllowed .

ステップ3: に移動しConfiguration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Namesます。図に示すように、をクリックします。



ステップ4:タイプとしてManagementTunnelAllAllowedを選択します。名前をに設定しtrueます。クリックAddして、図に示すようにカスタム属性値を指定します。

○ ○ ○ Configuration > Remo	te Access VPN > Network (Client) Acce	ess > Advanced > AnyConnect Custo	<u>m Attribute Names</u>
Declarations of custom attrib	ute names and these attributes are enfor	ced in <u>AnyConnect group policy</u> and <u>An</u>	<u>yConnect dynamic access policy</u>
🕈 Add 🗹 Edit 📋 Delete			
Type Name Values			
	Create Custom A	ttribute Name	
Time	ManagementTunnelAllAllowed		Managa
Type:	Management runnerAnAnowed		Manage
Name:	true		
	Value	Add	
		Edit	
		Delete	
Configure Values:			
	Help Canc	el OK	

ステップ 5:値をに設定しtrueます。図に示すように、をクリックしますOK。

	Management i unne	elAllAllowed		\$	Manage
Name:	true				
	Value			Add	
				e 15	
•		Add Value	9		
true					
lue:					
ue:					

手順 6:に移動しConfiguration > Remote Access VPN > Network (Client) Access > Group Policies ます。グループポリシーを選択します。 図に示すように、をEditクリックします。

đ) Home 🍫 Configuration 📴 Monitoring 冒	🕽 Save 🔇 Refresh 🔇 Back 🔘 Fo	orward 🧳 Help Type topic G	0		cisco
	O O O Remote Access VPN	Configuration > Remote A	Access VPN > Network (Client)	Access > Group Policies		
arks	? Introduction ▶ Introduction ▶ Introduction Profiles ▶ AnyConnect Consection Profiles ▷ AnyConnect Customization/Localization ◎ AnyConnect Clent Profile ◎ AnyConnect Clent Profile	Manage VPN group policies.A VPN server. The group policy informat To enforce authorization attribute Add C Edit Delete	I group is a collection of user-o ion is referenced by VPN connec es from an LDAP server you mus Assign	iented authorization attribute/value pairs that m tion profiles and user accounts. use an <u>LDAP attribute map</u> .	ay be stored internally on the device or externally on a RADIUS/I	.DAP
km	P Dynamic Access Policies	Name	Туре	Tunneling Protocol	Connection Profiles/Users	
Boc	Group Policies	AnyConnect	Internal	ssl-client	AnyConnect	
	IPsec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup	p;Def
	IPsec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel	
	Secure Mobility Solution					
	 Advanced Advanced Advanced AnyConnect Essentials AnyConnect Custom Attributes AnyConnect Custom Attribute Names Perce ACL Manager Clenthess SSL VPN Access AAA/Local Users AAA Server Groups LDAP Attribute Map Clocal Users Certificate Management Language Localization Lad Balancing DHCP Server DNS 					
	3 Advanced					
	Device Setup Firewall Senecte Access VPN Setup to Setup					
	2ite-to-site VPN	Find:	🔘 🔘 🗌 Match Case			
	Device Management			Reset Apply		

手順7:次の図に示すように、に移動しAdvanced > Split Tunnelingます。ポリシーをに設定しTunnel All Networksます。

• •		Edit Intern	nal Group Policy: AnyConnect_MGMT_Tunnel
General Servers	The VPN client makes split tunneling de fields.	cisions on the	e basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network Lis
Servers Advanced Split Tunneling Browser Proxy AnyConnect Client IPsec(IKEv1) Client	Treids. DNS Names: Send All DNS Lookups Through Tunnel: Policy: IPv6 Policy: Network List: Pressing this button to set up split exlu Set up Split Exclusion for Web Securi Intercept DHCP Configuration Message	Inherit Inher	Yes Tunnel All Networks C Manage Security proxies. oft Clients
Find:	Next	Previous	
			Help Cancel OK

ステップ8:に移動しAdvanced > Anyconnect Client > Custom Attributesます。図に示すように、をクリックし

ますAdd。

• •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel
General Servers ▼ Advanced Split Tunneling Browser Proxy ▼ AnyConnect Client Login Setting Client Firewall Key Regeneration Dead Peer Detection Customization Custom Attributes ► IPsec(IKEv1) Client	Configuration of custom policy attributes. Image: Configuration of custom policy attributes. Type Name of Value
Find:	Next Previous
	Help Cancel OK

ステップ9: 属性タイプとしてを選択ManagementTunnelAllAllowed し、値としてを選択し trueます。図 に示すように OK、をクリックします。

Add 🗹 Edit 📋	Delete		
pe		Name of V	/alue
•		Create Custom Attribute	
	Attribute type:	ManagementTunnelAllAllowed	Manage
	Omit the value		
	Select Value:	true 🗘	Manage
		Help Cancel OK	

ステップ 10 : クリックするとApply、図に示すように、設定がASAにプッシュされます。



カスタム属性を追加した後のCLI設定ManagementTunnelAllAllowed:

<#root>

```
webvpn
```

```
enable outside
```

```
anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
```

```
enable
 max-age 31536000
 include-sub-domains
 no preload
no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
I
anyconnect-custom-data ManagementTunnelAllAllowed true true
I
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
```

```
split-tunnel-policy tunnelall
```

client-bypass-protocol enable address-pools value VPN_Pool

anyconnect-custom ManagementTunnelAllAllowed value true

webvpn

anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt

確認

コマshow vpn-sessiondb detail anyconnect ンドを使用して、ASA CLIの管理VPNトンネル接続を確認します。

<#root>

ASA#

show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

:

Username

vpnuser

Index : 10 Assigned IP :

192.168.10.1

Public IP : 10.65.84.175 Protocol :

AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

```
: AnyConnect Premium
License
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
            : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Hashing
                                                 : 1988
Bytes Tx
            : 17238
                                     Bytes Rx
                                                  : 13
            : 12
                                     Pkts Rx
Pkts Tx
Pkts Tx Drop : 0
                                     Pkts Rx Drop : 0
Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel
Login Time : 01:23:55 UTC Tue Apr 14 2020
Duration
            : 0h:11m:36s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                     VLAN
                                                 : none
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

DTLS-Tunnel: Tunnel ID : 10.3
 Assigned IP
 : 192.168.10.1
 Public IP
 : 10.65.84.175

 Encryption
 : AES-GCM-256
 Hashing
 : SHA384
 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 57053 UDP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 18 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03036 Bytes Tx : 17238 Bytes Rx : 1988 Pkts Tx : 12 : 13 Pkts Rx Pkts Tx Drop : 0 Pkts Rx Drop : 0

ASDMで管理VPNトンネル接続を確認します。

--- Output Omitted ---

[モニタリング(Monitoring)] > [VPN] > [VPN 統計情報(VPN Statistics)] > [セッション (Sessions)] の順に移動します。クライアントセッションを表示するには、AnyConnect Clientでフィルタリングします。

🚮 Home 🦓 Configuration 🗾 Mo	onitoring 🔚 Save 🌘	🔇 Refresh 🔇 Ba	ck 🔘 Forward 💡	Help Type topic Go					cisco
Device List Bookmarks	OOO Monitoring	> VPN > VPN Stati	stics > Sessions						
OOO Device List									
🕈 Add 📲 Delete 🔉 Connect	Туре	Active	C	umulative	Peak Concurrent		Inactive		
Go Go	AnyConnect Client		1		19		1		0
₫ 10.106.39.196	SSL/TLS/DTLS		1		19		1		0
10.106.64.230									
10.197.227.47									
10.106.51.99:444									
COO VPN			_	_					
VPN Statistics	Filter By AnyCo	nnect Client	🗧 🛛 –– All Se	ssions ᅌ	Filte	r			
Sessions	Usersen	Group Policy	Assigned IP Address	Protocol	Login Time	Bytes Tx	In a set size of	Audias	Details
	Osername	Connection Profile	Public IP Address	Encryption	Duration	Bytes Ra	inactivity	Audit :	Details
Compression Statistics	vpnuser	AnyConnect_MGMT.		AnyConnect-Parent (1)	none 0h:01m:31s	34688	0h:00m:00s	c0a80	Logout
Encryption Statistics		party connection and		rangeonneet rarenti (a)					
Global IKE/IPsec Statistics									Ping
Protocol Statistics									
VLAN Mapping Sessions									
Clientless SSL VPN									
Shared SSL VPN									
WSA Sessions									
VPN									
A Routing	To sort VPN session	is, right-click on th	e above table and se	lect Table Sort Order fre	om popup menu.				
Reperties	Logout By: A	ll Sessio ᅌ		Logout Sessions					

クライアントマシンでの管理VPNトンネル接続の確認:

Sisco AnyConnect Secure Mobil	ity Client	- 🗆 🗙	
cisco AnyCon	nect Secure Mobility Clie	ent	
Virtual Private Network (VPI	۷)	Diagnostics	
Preferences Statistics Route Detail	Is Firewall Message History		
Connection Information State: Tunnel Mode (IPv4):	Disconnected Not Available	Sisco AnyConnect Secure Mobility Client –	×
Tunnel Mode (IPv6): Dynamic Tunnel Exclusion: Dynamic Tunnel Inclusion: Duration: Session Disconnect: Management Connection State:	Not Available Not Available Not Available 00:00:00 None Connected (asa.example.com)	VPN: Ready to connect.	inect
Address Information	Not Available		
Client (IPv6): Server:	Not Available Not Available	\$ ()	ululu cisco
Bytes		^ ~	
	Reset	Export Stats	

トラブルシュート

新しいUI統計行(管理接続状態)は、管理トンネルの接続問題のトラブルシューティングに使用 できます。一般的に見られるエラー状態を次に示します。

切断(無効):

- この機能は無効になっています。
- 管理VPNプロファイルが、ユーザトンネル接続(ユーザトンネルグループポリシーに管理 VPNプロファイルを追加する必要がある)を介して、またはプロファイルの手動アップロー ドによってアウトオブバンドで、クライアントに展開されていることを確認します。
- 管理VPNプロファイルが、トンネルグループを含む単一のホストエントリで設定されている ことを確認します。

切断(信頼できるネットワーク):

• TNDが信頼できるネットワークを検出したため、管理トンネルが確立されません。

切断 (ユーザトンネルがアクティブ):

• ユーザVPNトンネルが現在アクティブである。

切断(プロセスの起動に失敗):

• 管理トンネル接続の試行中にプロセスの起動エラーが発生しました。

切断(接続に失敗しました):

- 管理トンネルの確立時に接続エラーが発生しました。
- 証明書認証がトンネルグループに設定されていること、グループポリシーにバナーが存在しないこと、およびサーバ証明書が信頼されていることを確認します。

切断(無効なVPN構成):

- 無効なスプリットトンネリング構成またはクライアントバイパスプロトコル構成をVPNサー バーから受信しました。
- 管理トンネルグループポリシーの設定をドキュメントと照合します。

切断(ソフトウェアの更新が保留中):

• AnyConnectソフトウェアのアップデートは現在保留中です。

切断されました:

• 管理トンネルを確立しようとしているか、または他の理由で確立できません。

さらにトラブルシューティングを行うために<u>DART</u>を<u>収集</u>します。

関連情報

- <u>管理VPNトンネルの設定</u>
- <u>管理VPNトンネルのトラブルシューティング</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。