# FMCによって管理されるFTDでのAnyConnectダ イナミックスプリットトンネルの設定

## 内容

概要
前提条件
要件
使用するコンポーネント
背景説明
制限
設定
ステップ1:ダイナミックスプリットトンネルを使用するためのグループポリシーの編集
ステップ2:AnyConnectカスタム属性の設定
ステップ3:設定の確認、保存と展開
確認
トラブルシュート
問題
解決方法
関連情報

### 概要

このドキュメントでは、Firepower Management Center(FMC)によって管理されるFirepower Threat Defense(FTD)でAnyConnectダイナミックスプリットトンネル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。

- Cisco AnyConnect
- FMCの基礎知識

#### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

• FMCバージョン7.0

• FTDバージョン7.0

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、初期(デフォルト)設定の状態から起動しています 。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

FMCによって管理されるFTDのAnyConnectダイナミックスプリットトンネル設定は、FMCバー ジョン7.0以降で完全に使用できます。古いバージョンを実行している場合は、『<u>FMCを使用した</u> <u>Firepower Threat Defenseのための高度なAnyConnect VPN導入</u>』の指示に従って、FlexConfigを 使用して設定する必要があります。

ダイナミックスプリットトンネル設定を使用すると、DNSドメイン名に基づいてスプリットトン ネル設定を微調整できます。完全修飾ドメイン名(FQDN)に関連付けられたIPアドレスは変更され る可能性があるため、DNS名に基づくスプリットトンネルの設定では、リモートアクセス仮想プ ライベートネットワーク(VPN)トンネルに含まれるトラフィックと含まれないトラフィックをよ り動的に定義できます。除外されたドメイン名に対して返されたアドレスがVPNに含まれるアド レスプール内にある場合、それらのアドレスは除外されます。除外されたドメインはブロックさ れません。代わりに、これらのドメインへのトラフィックはVPNトンネルの外部に保持されます 。

ダイナミックスプリットトンネルを設定することもできます IPアドレスに基づいて除外されるド メインをトンネルに含めるように定義します。

#### 制限

現在のところ、次の機能はまだサポートされていません。

- ダイナミックスプリットトンネルは、iOS(Apple)デバイスではサポートされていません。
   Cisco Bug ID <u>CSCvr54798</u>
- ダイナミックスプリットトンネルは、Anyconnect Linuxクライアントではサポートされていません。 Cisco Bug ID CSCvt64988を参照してください。

### 設定

このセクションでは、FMCによって管理されるFTDにAnyConnectダイナミックスプリットトンネ ルを設定する方法について説明します。

#### ステップ 1 : ダイナミックスプリットトンネルを使用するためのグループポリシー の編集

1. FMCで、[Devices] > [VPN] > [Remote Access] に移動し、設定を適用する**接続プロファイル**を 選択します。

Device Management Device Upgrade NAT VPN > Remote Access QoS Platform Settings FlexConfig Certificates	
SSL_AnyConnect	Save Cancel
Local Realm: AnyConnect-Local-Aut	Policy Assignments (1) Dynamic Access Policy: anosanc2-test
Connection Profile Access Interfaces Advanced	
	0
Name AAA Group Policy	
DefaultWEBVPNGroup Authentication: None DtRGrpPolicy Authorization: None Accounting: None	/ 9
SSL_AnyConnect_LocalAuth Authentication: LOCAL AnyConnect_Local_Auth Authentication: None Accounting: None	/ 5
SSL_AmyConnect_LDAPAuth Authentication: AmyConnect_LDAPAuth (Ab)  Authentication: AmyConnect_LDAP_Auth (Ab)  Authorities: AmyConnect_LDAP_Auth (Ab)  Accounting: mixing	/ 5

2. [Edit Group Policy] を選択して、作成済みのグループポリシーの1つを変更します。

	Overview Analysis Policies Devices Objects AMP Intellige	ence					0, Deploy System Help v admin
	Device Management Device Upgrade NAT VPN + Remote Access	QoS PI	atform Settings Flex	xConfig Certificates			
	SSL_AnyConnect						Save Cancel
							Policy Assignments (1)
Contextite Profile       Access Taterface       Adverse         Name       Market       Adverse       Adverse         Status       Adverse       Adverse       Adverse         Paddress for the method clents and he assignment Adverse in the adverse pool adverse in the ad						Local Realm: AnyConnect-Local-Aut	Dynamic Access Policy: angsanc2-test
Nome       Add         Polkurdettrynkleine       Address         Str., AngeGeneett, LosalAda       Construction Profile         Address for the memotic clients can be assignment from Local IP Address straightment from Local IP Addresstraightment from Local IP Address straightment from Local IP Addre	Connection Profile Access Interfaces Advanced						
New     Autom       Detworte: Ubdature:     I Cit Connection Profile     1 x x       SSL_ArqConnect_Locabiluti     Autom     I Cit Connection Profile     1 x x       SSL_ArqConnect_Locabiluti     Autom     I Cit Connection Profile     1 x x       SSL_ArqConnect_Locabiluti     Autom     I Cit Connection Profile     1 x x       SSL_ArqConnect_Locabiluti     Autom     I Cit Connection Profile     1 x x       SSL_ArqConnect_Locabiluti     Autom     I Cit Connection Profile     1 x x       P Address Assignment     M x xx     I Cit Connection Profile     1 x x       P Address Assignment     M x xx     I Cit Connection Profile     1 x x       P Address Assignment     M x xx     I Cit Connection Profile     1 x x       P Address Assignment     M x x     I Cit Connection Profile     1 x x       P Address Assignment     M x x     I Cit Connection Profile     1 x x       P Address Assignment Profile     N x x     I T X x     I T X x       Neme     DHCP Server IP Address     I T X x x x     I T X x x x       P Configure device overrides in the address pool adject to avoid IP address conficts in case of adject is shared across     I x x x							0
Defunctions Address   SGS, Any-Connect, LoadAuth Conserts   SGS, Any-Connect, LoadAuth Address   SGS, Any-Connect, LoadAuth Conserts   Connect Internet Conserts   Conserts Conserts  <	Name	AAA	Edit Connection P	rofile	? ×		
SR_AryConnect_LDAMAuh     SR_AryConnect_LDAMAuh     SR_AryConnect_LDAMAuh     Auth     China Address Assignment Aulor in beat IP Address pools/DHCP Servers/AAA. Servers.     China Address Assignment Aulor in the Address Assignment Aulor in the Address Social/DHCP Servers/AAA. Servers.     DHCP Servers:     DHCP Ser	DefaultWEBVFNGroup	Authent Authoria Account	Connection Profile:*	SSL AnyConnect LocalAuth			/ 8
SSL, AnyConnect, LDAMAUN     Clinch Address Assignment (Andres)     Address for the rendo leading of clines can be assignment of notal IP Address gool/DHCP Servers/AAA Servers.   Address For the rendo leading of clines can be assignment of notal IP Address gool/DHCP Servers/AAA Servers.   Address For the rendo leading of clines can be assignment of notal IP Address gool/DHCP Servers/AAA Servers.   Address For the rendo leading of clines can be assignment of notal IP Address gool/DHCP Servers/AAA Servers.   Address For the rendo leading of clines can be assignment of notal IP Address for the rendo leading of clines the assignment of notal IP Address for the rendo leading of clines the assignment of notal IP Address for the rendo leading of clines f	SSL_AnyConnect_LocalAuth	Authent Authoriz Account	Group Policy:*	Edit Group Policy		Auth	08
P Address for the remet clients can be assigned from local IP Address pools/DPC Servers/AAA Servers. Configure device overnides in the address pool abject to avoid IP address conflicts in case of object is shared across           DHCP Servers:	SSL_AnyConnect_LDAPAuth	Authent Authoria Account	Client Address Ass	ilgnment AAA Aliases		Auth	/8
Address Pool:   Name   Indr- dperezve-pool   172.16.13.1-172.16.13.254     DHCP Servers:     DHCP Servers:     Name   DHCP Servers:     Configure device overrides in the address pool adject to avoid IP address conflicts in case of object is shared accres     Store     Case			IP Address for the re Configure the 'Client	mote clients can be assigned from local IP Address pool: Address Assignment Policy' in the Advanced tab to defin	s/DHCP Servers/AAA Servers. ne the assignment criteria.		
Name IP Address Range   fide-dpertare-gool 172.16.13.1-172.16.13.254   DHCP Server: Image: Configure device overrides in the address pool adject to avoid IP address   Image: Configure device overrides in the address pool adject to avoid IP address conflicts in case of object is shared across			Address Pools:		0-		
hdi-deerezve-pool 122.16.13.254			Name	IP Address Range			
DHCP Servers: Name DHCP Server IP Address DHCP Server IP Address DHCP Server IP Address DHCP Server IP Address DHCP Server IP Address Server Server Cancel			ftdv-dperezve-pool	172.16.13.1-172.16.13.254	/ 8		
DHCP Servers:   Mame DHCP Server IP Address  Configure device overnides in the address pool object to avoid IP address conflicts in case of object is shared across  Serve Cancel							
DHCP Servers:							
DHCP Servers:							
Name     DHCP Server IP Address       Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across			DHCP Servers:		0		
Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across			Name	DHCP Server IP Address			
Oconfigure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across seventiate devices Seven Cancel							
Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across environs devices  State Cancel							
Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across sendence devices Save Cancel							
and the factors Stree Cancel			Configure device ov	errides in the address paol object to avoid IP address conflict	is in case of object is shared across		
			multinla devices		Sava Cancel		
					und Carco		

## ステップ2: AnyConnectカスタム属性の設定

1.グループポリシー設定で、[Anyconnect] > [Custom Attributes] に移動し、[Add (+)] ボタンをク リックします。

Overview Analysis Policies Devices Objects Integration		Deploy 🧛 System Help 🔻 admin 🔻
Device Management Device Upgrade NAT QoS Platform Settings FlexConfig	Certificates VPN + Remote Access Troubleshoot +	
FTD_RAVPN_Policy1		Save Carcel
		Policy Assignments (0) Local Realm: Local REALM1 Dynamic Access Policy: None
Connection Profile Access Interfaces Advanced	Edit Connection Profile ? X	
	Add Group Policy ? ×	
	Name:* Anyconnect_Local_Auth	0
Name AAA	Description:	
DefaultWEBVPNGroup Authen Author Account	General AnyConnect Advanced	/8
FTD_RAVPN_Policy11 Authors Authors Account	Profile AnyConnect Custon Attribute feature allows a more expedited way of configuring new Management Profile endpoint features on linewal Threat Defense. This feature is supported on Firewal Client Modules Threat Defense 7.0 onwards.	∕a
new-testo Authen Authen Authori	SSL Settings Cuttom Attribute Attribute Name Centent	28
	No records to display	

2. [Dynamic Split Tunneling] の[AnyConnect Attribute]を選択し、[Add (+)] ボタンをクリックして 新しいカスタム属性オブジェクトを作成します。

Edit Connecti	ion Profile	? ×
Edit Group Po	licy	? ×
Name:*	Regular_Users_GP1	
Description:		
General Ar	nyConnect Advanced	
Profile Management Pro	AnyConnect Custom Attribute feature allows a more expedited way of co office endpoint features on Firewall Threat Defense. This feature is supported of	nfiguring new on Firewall
Client Modules	Add Custom Attribute ?	×
Connection Set	AnyConnect Attribute:* Dynamic Split Tunneling	42
	Custom Attribute Object:*	
	Add Cancel	
		Carrel
	Sere	Cance

3. [AnyConnect Custom Attribute] の[Name] を入力し、ドメインを動的に含めるか除外するかを 設定します。

注:設定できるのは、[Include domains] または[Exclude domains] だけです。

Overview Analysis Policies Devices Objects AMP Intelligence					oy System Help <del>v</del> admin v
Device Management Device Upgrade NAT VPN + Remote Access	QoS P	atform Settings FlexConfig Certificates			
SSL_AnyConnect					Save Cancel
Connection Profile Access Interfaces Advanced				Local Realm: <u>AnvConnect-Local-Aut</u> D	Policy Assignments (1) mamic Access Policy: <u>angsanc2-test</u>
					0
Name	AAA	Edit Connection Profile	7 X		
DefaultWE8VPNGroup	Authent Authoria Account	Edit Group Policy	? ×		/ 5
SSL_AnyConnect_LocalAuth	Authent Authoria Account	Name:* AnyConnect_Local_Auth Description:	Auth		Ø 6
SSL_AnyConnect_LDAPAuth	Authent Authoris Account	General AnyConnect Advanced	Auth Add AnyConnect	Custom Attribute	2 × 0
		Profile Management Profile Any-Connect Custom Attribute feature allows a more expedient easy of con motions flavoure as PTD: This feature is supported on PTD 30 markets SSS Settings Custom Attribute Any-Connect Attribute:* Dynamic Split Turneling Custom Attribute Add Canced	Name:* Description: AnyConnect Attrib Include domains: Exclude domains: Allow Overrides	vite:*	
		Save		Save	Cancel

この例では、図に示すように、除外するドメインとしてcisco.comを設定し、カスタム属性に Dynamic-Split-Tunnelという名前を付けています。

Name:*	Dynamic-Split-Tunnel		
Description:		1	
AnyConnect Attribute:*	Dynamic Split Tunneling	~	
Include domains:	Configure comma separated domain names that will included in the Remote Access VPN Tunnel	be	
Exclude domains:	cisco.com		

## ステップ3:設定の確認、保存と展開

設定したカスタム属性が正しいことを確認し、設定を保存して、問題のFTDに変更を適用します。



## 確認

Command Line Interface(CLI;コマンドラインインターフェイス)を使用してFTDで次のコマンドを実行し、ダイナミックスプリットトンネルの設定を確認できます。

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy <グループポリシーの名前>

この例では、設定は次のようになります。

```
ftd# show run group-policy Anyconnect_Local_Auth
group-policy Anyconnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list value AC_networks
Default-domain none
split-dns none
address-pools value AC_pool
anyconnect-custom dynamic-split-include-domains none
```

ftd# show run webvpn
webvpn
enable outside
anyconnect-custom-attr dynamic-split-exclude-domains

anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert_map_test 10 cert_auth
error-recovery disable
クライアントで設定されているダイナミックトンネル除外を確認するには、次の手順を実行しま
<b>व</b> 。

1. AnyConnectソフトウェアを起動し、次の図に示すように歯車アイコンをクリックします。

🕙 Cisco AnyC	onnect Secure Mobility Client	-	- 🗆	×	l,
	VPN: Connected to 4	V [	Disconne	ct	
00:04:22				IPv4	
<b>Ç</b> ()				ululu cisco	

2. [VPN] > [Statistics] に移動し、[Dynamic Split Exclusion/Inclusion] に表示されるドメインを確認 します。

cisco	AnyConnect	Secure Mobility Client	
01-1	- ÷	Virtual Driveta Naturals (V(DN)	

Status Overview	Virtual Private Network (VPN)
VPN >	Preferences Statistics Route Details Firewall Message History
Network	Connection Information
System Scan	State:     Connected       Tunnel Mode (IPv4):     Split Include       Tunnel Mode (IPv6):     Drop All Tapfin
Roaming Security	Dynamic Tunnel Exclusion: cisco.com
	Duration:       00:00:25         Session Disconnect:       None         Management Connection State:       Disconnected (user tunnel active)         Address Information <ul> <li>Cleab (Thurth):</li> <li>Cleab (Thurth):</li> </ul>
Collect diagnostic information for all	Client (IPV+): Client (IPV6): Server: Bytes
Diagnostics	Reset Export Stats

## トラブルシュート

AnyConnect Diagnostics and Reporting Tool(DART)を使用して、AnyConnectのインストールおよび接続の問題のトラブルシューティングに役立つデータを収集できます。

DART によってログ、ステータス、および診断情報が収集され、それを Cisco Technical Assistance Center(TAC)での分析に使用できます。クライアントマシンで実行するために管理 者権限は不要です。

#### 問題

AnyConnectカスタム属性(\*.cisco.comなど)にワイルドカードが設定されている場合、 AnyConnectセッションは切断されます。

#### 解決方法

cisco.comドメイン値を使用して、ワイルドカードを置き換えることができます。この変更により、www,cisco.comやtools.cisco.comなどのドメインを含めるか除外するかを選択できます。

## 関連情報

- 詳細については、Technical Assistance center(TAC)にお問い合わせください。有効なサポート契約が必要です。
   各国のシスコ サポートの連絡先。
- ・また、Cisco VPN Community <u>here</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。