# Configureer AnyConnect Dynamic Split Tunnel op FTD die door FMC wordt beheerd

### Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie **Beperkingen** Configureren Stap 1. Het groepsbeleid bewerken voor gebruik van de dynamische splitstunnel Stap 2. De aangepaste AnyConnect-kenmerken configureren Stap 3. Controleer de configuratie, opslaan en implementeren Verifiëren Problemen oplossen Probleem Oplossing Gerelateerde informatie Inleiding

In dit document wordt beschreven hoe u AnyConnect Dynamic Split Tunnel kunt configureren bij Firepower Threat Defence (FTD), beheerd door Firepower Management Center (FMC).

### Voorwaarden

#### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco AnyConnect
- Basiskennis van het VCC

#### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- FMC versie 7.0
- FTD versie 7.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

AnyConnect Dynamic Split Tunnel configuratie op FTD beheerd door FMC is volledig beschikbaar op FMC versie 7.0 en nieuwer. Als u een oudere versie uitvoert, moet u deze via FlexConfig configureren zoals beschreven in de geavanceerde AnyConnect VPN-implementaties voor Firepower Threat Defence met FMC.

Met Dynamic Split Tunnel configuratie, kunt u gesplitste tunnelconfiguratie verfijnen op basis van DNS domeinnamen. Omdat de IP-adressen die gekoppeld zijn aan FQDN-domeinnamen (fullqualified domain) kunnen worden gewijzigd, biedt de gesplitste tunnelconfiguratie op basis van DNS-namen een dynamischer definitie van het verkeer dat al dan niet is opgenomen in de VPNtunnel (Virtual Private Network) voor externe toegang. Als er adressen worden teruggegeven voor uitgesloten domeinnamen binnen de adrespool die in de VPN is opgenomen, worden die adressen dan uitgesloten. Uitgesloten domeinen worden niet geblokkeerd. In plaats daarvan wordt het verkeer naar die domeinen buiten de VPN-tunnel gehouden.

Merk op dat u ook Dynamic Split Tunnel kunt configureren om domeinen te definiëren die in de tunnel moeten worden opgenomen en die anders op basis van IP-adres zouden worden uitgesloten.

#### Beperkingen

Op dit moment worden deze functies nog niet ondersteund:

- Dynamic Split Tunnel wordt niet ondersteund op iOS (Apple)-apparaten. Zie Cisco bug-id
   <u>CSCvr54798</u>
- Dynamic Split Tunnel wordt niet ondersteund op AnyConnect Linux-clients. Zie Cisco-bug IDCSCvt64988

### Configureren

In dit deel wordt beschreven hoe u AnyConnect Dynamic Split Tunnel kunt configureren op een FTD die wordt beheerd door FMC.

#### Stap 1. Het groepsbeleid bewerken voor gebruik van de dynamische splitstunnel

1. Navigeer in het VCC naar **Apparaten > VPN > Externe toegang** en selecteer vervolgens het **verbindingsprofiel** waarop u de configuratie wilt toepassen.

Overview Analysis Policies Devices Objects AMP Intelligence			0, Deploy System Help + admin +
Device Management Device Upgrade NAT VPN - Remote Access Q	oS Platform Settings FlexConfig Certificates		
SSL_AnyConnect			Save Cancel
		Local Realm: AnyConnect-Local-Aut	Policy Assignments (1) Dynamic Access Policy: angsanc2-test
Connection Profile Access Interfaces Advanced			
			0
Name	AAA	Group Policy	
DefaultWE8VPNGroup	Authentication: None Authentication: None Accounting: None	DttcGrpPolicy	/ 6
SSL_AnyConnect_LocalAuth	Authentication: LOCAL Authentication: None Accounting: None	AnyConnect_Local_Auth	/ 8
SSL_AnyConnect_LDAPAuth	Authentication: AnyConnect-LDAP-Auth (AD) Authentization: AnyConnect-LDAP-Auth (AD) Accounting: Informe	AnyConnect_LDAP_Auth	/ 6

2. Selecteer Groepsbeleid bewerken om een van de groepsbeleid te wijzigen dat al is gemaakt.

Overview Analysis Policies Devices Objects AMP Intelligence	e					🖲 Deploy System Help 🛛 admin
Device Management Device Upgrade NAT VPN > Remote Access	QoS PI	atform Settings Flex	Config Certificates			
SSL_AnyConnect						Save Save
						Policy Assignments (1)
					Local Realm: AnyConnect-Local-Aut	Dynamic Access Policy: angsanc2-test
Connection Reafile Access Interfaces Advanced						
Connection Prome Access Interfaces Advanced						
						0
Num						
Name Defended@URMCesse	AAA	Edit Connection P	rofile	? >	<	18
Descritesvinaroop	Authoriz					~ 0
CO AnsConnert Localisth	Authant	Connection Profile:*	SSL_AnyConnect_LocalAuth		Auth	28
and his connect from the	Authoriz	Group Policy:*	Edit Group Policy		/ Martin	¥ 0
SSL AnyConnect LDAPAuth	Authent				Auth	28
	Authoriz	Client Address Ass	Igniment Avia Aliases			
		IP Address for the re Configure the 'Client	mote clients can be assigned from local IP Address p Address Assignment Policy' in the Advanced tab to o	ools/DHCP Servers/AAA Servers. lefine the assignment criteria.		
		Address Pools:		0.		
		Name	IP Address Range			
		ftdv-dperezve-pool	172.16.13.1-172.16.13.254	/ 8		
		DHCP Servers:		0		
		Name	DHCP Server IP Address			
		Configure device ov	errides in the address pool object to avoid IP address con	flicts in case of object is shared across		
		multinla davinar		Save Cancel		
				(		

### Stap 2. De aangepaste AnyConnect-kenmerken configureren

1. Ga onder de configuratie Groepsbeleid naar **AnyConnect > Aangepaste kenmerken** en klik op de knop **Toevoegen (+)**:

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		E Save
		Policy Assignments (0) Local Realm: Local REALM1 Dynamic Access Policy: None
Connection Profile Access Interfaces Advanced	Edit Connection Profile ? X	
	Add Group Policy 7 ×	
	Name:* Anyconnect_Local_Auth	0
Name AAA	Description:	
DefaultWEBVPNGroup Authentic Authentic	General AnyConnect Advanced	/8
FTD_RAVPN_Policy13 Authoriti Authoriti	Profile AnyConnect Custon Attribute feature allows a more expedited way of configuring new Management Profile endpoint features on linewall Threat Defense. This feature is supported on Firewall Client Modules Threat Defense 7.0 onwards.	∕a
new-testo Authentic Authentic Autonetic	SSL Settings Control Attribute Name Content	<b>√</b> 8
	No records to display	

2. Selecteer de **Dynamic Split Tunneling** AnyConnect Attribute en klik op de knop **Add (+)** om een nieuw aangepast Attribute-object te maken:

Edit Connecti	ion Profile	? ×
Edit Group Po	licy	? ×
Name:*	Rogular_Users_GP1	
Description:		
General A	nyConnect Advanced	
Profile Management Pro	AnyConnect Custom Attribute feature allows a more office endpoint features on Firewall Threat Defense. This	e expedited way of configuring new feature is supported on Firewall
Client Modules	Add Custom Attribute	? ×
SSL Settings Connection Sett Custom Attribut	AnyConnect Attribute:* Dynamic Split Tunneling	
	Custom Attribute Object:*	
	Add	Cancel
		Save Cancel

3. Voer de **naam** van het **aangepaste AnyConnect-kenmerk in** en configureer de domeinen die dynamisch moeten worden opgenomen of uitgesloten.

Opmerking: u kunt alleen configureren of domeinen opnemen of domeinen uitsluiten.

	Overview Analysis Policies Devices Objects AMP Intelligence						₿ <sub>3</sub> De	sloy System Help <del>v</del> admin v
	Device Management Device Upgrade NAT VPN > Remote Access Q	os Pl	atform Settings FlexCo	Config Certificates				
	SSL_AnyConnect							Save Cancel
Name       Add         Default/REXVING/rup       Add         SSL, Any:Connect, Local-Auth       Add         SSL, Any:Connect, Local-Auth       Add         Management Horle       Addresse         Forter       Advacement         Default/REXVING/rup       Addresse         SSL, Any:Connect, Local-Auth       Addresse         Management Horle       Advacement         Partie       Advacement         Add Custom Attributes       Operante: Split Turneling         Concetton Stitl       Casem Attributes         Conceton Stitl       Ca	Connection Profile Access Interfaces Advanced					u	cal Realm: <u>AnvConnect-Local-Aut</u>	Policy Assignments (1) Synamic Access Policy: anssans2-test
Name     Add       Dordurd UNERPARTICIPUP     Add       SSL, Any Connect, LIXARACIN     Add       SSL, Any Connect, LIXARACIN     Add       SSL, Any Connect, LIXARACIN     Add       Add     Any Connect, Advanced       Profile     Any Connect, Advanced or PTD 2 Symmits       Connection Set     Any Connect Attribute       Connection Set     Any Connect Attribute       Connection Set     Connection Methode Status								0
DebularREEWINGroup Authors   SSL, Any Connect, Local Author   SSL, Any Connect, Local Author   Authors   SSL, Any Connect, Local Author Authors Solution Authors fabric fabrics a more segretated and in names that will Custom Attribute: Output and Top Link Educe is Split Tunnelling Add Custom Attribute: Output and Top Link Educe is Split Tunnelling Add Custom Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe in the Remote Access Vint Tunnelling Exclude domains: Configure genma separated domain names that will Exclude domains: Configure genma separated domain names that will Addition top Configure genma separ	Name	AAA	Edit Connection Pro	ofile		2 ×		
SSL, AnyConnect, LDAMuth SSL, AnyConnect, LDAMuth Access SSL, AnyConnect, Attribute SSL, An	DefaultWEBVPNGroup	Authent Authoria Account	Edit Group Policy	ane		? ×		/ 5
SSLAN/Connect_LDAMAUN       Autom       Autom       Add AnyConnect Custom Attribute       ? ×         Phale       Automatic Automatic Relative Release a more expedided way of control       Name:*       Description:         Content Modale       Add Custom Attribute Digect.*       •       Add AnyConnect Attribute.*       •         Custom Attribute Digect.*       •       •       •       •       •       •         Add       •	SSL_AnyConnect_LocalAuth	Authent Authoria Account	Name:* AnyCo Description:	onnect_Local_Auth		Auth		28
Profile       AnyConnect Custom Attribute       7 ×         SS. Settings       Add Custom Attribute       7 ×         Custom Attribute       0 ynamic Split Tunneling         AnyConnect Attribute       0 ynamic Split Tunneling         Custom Attribute       0 ynamic Split Tunneling         Exclude domains:       0 ynamic Split Tunneling         Exclude domains:       0 ynamic Split Tunneling         De excluded from the Remote Access VPH Tunnel       0 ynamic Split Tunneling         De exclude domains:       0 ynamic Split Tunneling         De exclude domains:       0 ynamic Split T	SSL_AnyConnect_LDAPAuch	Authent Authoria	General AnyConn	nect Advanced		Auth Add AnyConnect Cus	tom Attribute	2 S
Save and the second s		Account	Profile Management Profile Clarit Modules SG, Settings Connection Sett Custom Attribut Custom Attribut	AnyConnect Custom Attribute feature a endpoint features on FTD. This feature Connect Attribute Connect Attribute: Dynamic Solit Ture tom Attribute Object:*	lovs a more expedited way of configs supported on FTD 7.0 ensets. ? × elling v v Add Cancel Save	Name:* Description: AnyConnect.Attribute: Include domains: Exclude domains: Allow Overrides	Dynamic Split Tunneling     Configure comma separated domain names the     included in the Remote Access VHs Tunnel     Configure comma separated domain names the     be excluded from the Remote Access VHs Tunnel	

In dit voorbeeld hebben we **cisco.com** geconfigureerd als het uit te sluiten domein en de aangepaste kenmerken **Dynamic-Split-Tunnel** genoemd, zoals in de afbeelding:

Name:*	Dynamic-Split-Tunnel		
Description:			
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	1	

### Stap 3. Controleer de configuratie, opslaan en implementeren

Controleer of het ingestelde aangepaste kenmerk juist is, sla de configuratie op en implementeer de wijzigingen in het betreffende FTD.



### Verifiëren

U kunt deze opdrachten op de FTD uitvoeren via Command Line interface (CLI) om de configuratie van de Dynamic Split Tunnel te bevestigen:

- tonen in werking stellen-configuratiewebvpn
- toon in werking stelt -in werking stellen-configureren om het even welke verbinding-douanegegevens
- tonen het in werking stellen-Config groep-beleid <Naam van het groep-beleid>

In dit voorbeeld is de configuratie de volgende:

```
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-exclude-domains value cisco.com
```

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

Zo controleert u de geconfigureerde uitsluitingen van dynamische tunnels op de client:

1. Start de AnyConnect-software en klik op het pictogram van de versnelling, zoals in de afbeelding wordt weergegeven:

🕙 Cisco AnyO	Connect Secure Mobility Client	-	•	×	ļ
	VPN: Connected to 4	~ [	Disconnect	t	
00:04:22			1	IPv4	
<b>Ç</b> ()				iliilii cisco	

2. Navigeer naar VPN > Statistieken en bevestig de domeinen die worden weergegeven onder Dynamic Split Exclusion/Inclusion:

cisco	AnyConnect	Secure	e Mo	bility C	lien	t
Status Ove	rview	Virtual Pri	ivate Ne	twork (VPN	۱)	
VPN	>	Preferences	Statistics	Route Details	Firewall	Message His

/PN >			
etwork	Connection Information —		<b>^</b>
/stem Scan	State: Tunnel Mode (IPv4):	Connected Split Include	
aming Security	Tunnel Mode (IPv6): Dynamic Tunnel Exclusion:	Drop All Traffic cisco.com	
	Duration: Session Disconnect: Management Connection State: Address Information Client (IPv4): Client (IPv6):	00:00:25 None Disconnected (user tunnel active)	^
Collect diagnostic information for all installed components.	Server: Bytes		Reset Export Stats

### Problemen oplossen

U kunt de AnyConnect Diagnostics and Reporting Tool (DART) gebruiken om de gegevens te verzamelen die nuttig zijn voor het oplossen van installatie- en verbindingsproblemen met AnyConnect.

DART verzamelt de logboeken, status en diagnostische informatie voor analyse door de Cisco Technical Assistance Center (TAC) en heeft geen beheerdersbevoegdheden nodig om op het clientapparaat te werken.

#### Probleem

Als een jokerteken is geconfigureerd in de AnyConnect-aangepaste kenmerken, bijvoorbeeld **\*.cisco.com**, wordt de AnyConnect-sessie losgekoppeld.

#### Oplossing

U kunt de domeinwaarde van **cisco.com** gebruiken om de vervanging van de wildcard toe te staan. Met deze wijziging kunt u domeinen zoals **www, cisco.com** en **tools.cisco.com** opnemen of uitsluiten.

### Gerelateerde informatie

 Voor extra assistentie kunt u contact opnemen met het Technical Assistance Center (TAC). Een geldig ondersteuningscontract is vereist: <u>Cisco's wereldwijde contactgegevens voor</u> <u>ondersteuning.</u>

×

**(**)

• U kunt ook de Cisco VPN-community bezoeken hier.

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.