Konfiguration eines dynamischen AnyConnect Split-Tunnels auf einem von FMC verwalteten FTD

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Einschränkungen Konfigurieren Schritt 1: Bearbeiten der Gruppenrichtlinie zur Verwendung von dynamischem Split-Tunnel Schritt 2: Konfigurieren des benutzerdefinierten AnyConnect-Attributs Schritt 3: Überprüfen der Konfiguration, Speichern und Bereitstellen Überprüfung Fehlerbehebung Problem Lösung Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie Sie den dynamischen AnyConnect Split-Tunnel auf dem vom FirePOWER Management Center (FMC) verwalteten FirePOWER Threat Defense (FTD) konfigurieren.

Voraussetzungen

Anforderungen

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

- Cisco AnyConnect
- Grundkenntnisse von FMC

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- FMC Version 7.0
- FTD Version 7.0

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 möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Die AnyConnect Dynamic Split Tunnel-Konfiguration auf FTD, die von FMC verwaltet wird, ist ab FMC-Version 7.0 vollständig verfügbar. Wenn Sie eine ältere Version ausführen, müssen Sie diese über FlexConfig konfigurieren, wie in <u>Advanced AnyConnect VPN Deployments for</u> <u>Firepower Threat Defense with FMC</u> beschrieben.

Mit der Konfiguration des Dynamic Split Tunnels können Sie die Split-Tunnel-Konfiguration basierend auf DNS-Domänennamen optimieren. Da sich die IP-Adressen ändern können, die mit vollqualifizierten Domänennamen (FQDN) verknüpft sind, bietet die Konfiguration von Split-Tunneln auf Basis von DNS-Namen eine dynamischere Definition, welcher Datenverkehr im Virtual Private Network (VPN)-Tunnel für den Remote-Zugriff enthalten ist oder nicht. Wenn Adressen, die für ausgeschlossene Domänennamen zurückgegeben werden, innerhalb des im VPN enthaltenen Adresspools liegen, werden diese Adressen dann ausgeschlossen. Ausgeschlossene Domänen werden nicht blockiert. Stattdessen wird der Datenverkehr zu diesen Domänen außerhalb des VPN-Tunnels gehalten.

Beachten Sie, dass Sie auch Dynamic Split Tunnel konfigurieren können. Domänen definieren, die in den Tunnel aufgenommen werden sollen und andernfalls basierend auf der IP-Adresse ausgeschlossen würden.

Einschränkungen

Diese Funktionen werden derzeit noch nicht unterstützt:

- Dynamic Split Tunnel wird auf iOS-Geräten (Apple) nicht unterstützt. Siehe Cisco Bug-ID
 <u>CSCvr54798</u>
- Dynamic Split Tunnel wird auf AnyConnect Linux Clients nicht unterstützt. Siehe Cisco Bug <u>IDCSCvt64988</u>

Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie einen dynamischen AnyConnect Split Tunnel auf einem von FMC verwalteten FTD konfigurieren.

Schritt 1: Bearbeiten der Gruppenrichtlinie zur Verwendung von dynamischem Split-Tunnel

1. Navigieren Sie auf dem FMC zu **Devices > VPN > Remote Access**, und wählen Sie dann das **Verbindungsprofil aus,** auf das die Konfiguration angewendet werden soll.

Overview Analysis Policies Devices Objects AMP Intelligence			\varTheta Deploy System Help 🕶 admin 🕶
Device Management Device Upgrade NAT VPN > Remote Access C	QoS 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	
DefaultWEBVPNGroup	Authentication: None Authentication: None Accounting: None	E DftGrpPolicy	/ 5
SSL_AnyConnect_LocalAuth	Authentication: LOCAL Authentication: Increa Accounting: Increa	AnyConnect_Local_Auth	/ 9
SSL_AnyConnect_LDAPAuth	Authentication: AnyConnect-LDAP-Auth (AD) Authentication: AnyConnect-LDAP-Auth (AD) Accounting: Anne	AnyConnect_LDAP_Auth	/ 5

2. Wählen Sie **Gruppenrichtlinie bearbeiten**, um eine der bereits erstellten Gruppenrichtlinien zu ändern.

Overview Analysis Policies Devices Objects AMP Intelligence	DoS PI	form Settions ElexConfin Certificates	0 ₃ Deploy System Help v admin
SSL_AnyConnect	200 F	ann acungs reaconny countaits	Save Cancel
Connection Profile Access Interfaces Advanced			Policy Assignments (1) Local Realm: <u>AnsCannect-Local-Aut</u> Dynamic Access Policy: <u>anosanc2-test</u>
			0
Name	AAA	Edit Connection Profile ?	×
DefaultWEBVPWGroup	Authent Authoriz Account	Connection Profile:* \$SL_AnyConnect_LocalAuth	/ 6
SSL_AnyConnect_LocalAuth	Authent Authoriz Account	Group Policy: * Auth * O	Auth 🖉 🕄
SSL_AnyConnect_LDAPAuth	Authent Authoriz Account	Client Address Assignment AAA Aliases	Auth 28
		IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria. Address Pools:	
		Name IP Address Range	
		ftóv-óperezve-pool 172.16.13.1-172.16.13.254 🥜 🗒	
		DHCP Servers: G	
		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 mathematicate devices.	

Schritt 2: Konfigurieren des benutzerdefinierten AnyConnect-Attributs

1. Navigieren Sie unter der Gruppenrichtlinienkonfiguration zu **AnyConnect > Benutzerdefinierte Attribute,** und klicken Sie auf die Schaltfläche **Hinzufügen (+)**:

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 Cancel
	Local Resim: Local REAM	Policy Assignments (0) 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 Authentic Authentic Account	General AnyConnect Advanced	/8
FTD_RAVPN_Policy11 Authority Authority Accountin	Profile Profile AnyConnect Custom Attribute feature allows a more expedited way of configuring new Management Features on Financial Threat Defense. This feature is supported on Financial Client Modules Threat Defense 7.0 onwards.	<i>2</i> ti
new-testo Authentic Authentic Accounti	SS, Settops Carterio Settops Cutom Attribute Name Centent	/8
	No records to display	

2. Wählen Sie das **Dynamic Split Tunneling** AnyConnect-Attribut, und klicken Sie auf die Schaltfläche **Hinzufügen (+)**, um ein neues benutzerdefiniertes Attributobjekt zu erstellen:

Edit Connecti	ion Profile	۶×
Edit Group Po	blicy	? ×
Name:*	Regular_Users_GP1	
Description:		
General A	nyConnect Advanced	
Profile Management Pro	AnyConnect Custom Attribute feature allows a more expedited way of configuring new endpoint features on Firewall Threat Defense. This feature is supported on Firewall Add Custom Attribute	
SSL Settings Connection Sett	AnyConnect Attribute:* Dynamic Split Tunneling	
	Custom Attribute Object:*	
	Add Cancel	
	Save Cano	el

3. Geben Sie den **Namen** des **benutzerdefinierten AnyConnect-Attributs ein**, und konfigurieren Sie die Domänen so, dass sie dynamisch ein- oder ausgeschlossen werden.

Hinweis: Sie können nur Domänen einschließen oder ausschließen konfigurieren.

Overview Analysis Policies Devices Objects AMP Intelligence	æ			0 3	Deploy System Help v admin v
Device Management Device Upgrade NAT VPN > Remote Access	QoS PI	latform Settings FlexConfig Certificates			
SSL_AnyConnect					Save Cancel
Connection Profile Access Interfaces Advanced				Local Realm: <u>AnvConnect-Local-Aut</u>	Policy Assignments (1) Dynamic Access Policy: <u>anssanc2-test</u>
					0
Name	AAA	Edit Connection Profile	2 ×		
DefaultWEBVPNGroup	Authent Authoria Account	Edit Group Policy	? ×		Ø 9
SSL_AnyConnect_LocalAuth	Authent Authoria Account	Name:* AnyConnect_Local_Auth Description:		Auth	28
SSL_AnyConnect_LDAPAuth	Authent Authoria	General AnyConnect Advanced	Add AnyCo	Auth onnect Custom Attribute	? ×
	Account	Profile AnyConnect Outforn Attribute fee endpoint Hastman en PTD. This fe Context Module Add Custom Attribute SS, Settings Custom Attribute AnyConnect Attribute.* Dynamic Sp Custom Attribute Outform O	thre allows a more expedited way of configuration is supported on FTD 7.9 conserved.	on: ect Attribute:* Dynamic Split Turnsling semains: Configure comma separated domain names be included in the Remote Access VPH Turns domains: Configure comma separated domain names be excluded from the Remote Access VPH Turns emides	That will and a set of the set of
			Save	Sav	e Cancel

In diesem Beispiel haben wir **cisco.com** als auszuschließende Domäne konfiguriert und das benutzerdefinierte Attribut **Dynamic-Split-Tunnel** benannt, wie im Bild gezeigt:

	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		

Schritt 3: Überprüfen der Konfiguration, Speichern und Bereitstellen

Überprüfen Sie, ob das konfigurierte benutzerdefinierte Attribut korrekt ist, speichern Sie die Konfiguration, und stellen Sie die Änderungen im betreffenden FTD bereit.



Überprüfung

Sie können diese Befehle über die FTD-Befehlszeilenschnittstelle (CLI) ausführen, um die Konfiguration des Dynamic Split Tunnels zu bestätigen:

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy <Name der Gruppenrichtlinie>

In diesem Beispiel ist die Konfiguration die nächste:

```
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-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
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
So überprüfen Sie die konfigurierten dynamischen Tunnelausschlüsse auf dem Client:

1. Starten Sie die AnyConnect-Software und klicken Sie auf das Zahnrad-Symbol, wie im Bild gezeigt:

🚳 Cisco AnyC	Connect Secure Mobility Client	-	- 🗆	×	k
	VPN: Connected to 4	V [Disconne	ct	
00:04:22				IPv4	
۞				cisco	

2. Navigieren Sie zu **VPN > Statistics**, und bestätigen Sie die unter "**Dynamic Split Exclusion/Inclusion**" angezeigten Domänen:

cisco	AnyConnect	Secure	e Mo	bility C	lien	t
Status Ove	rview	Virtual Pr	ivate Ne	twork (VPN	1)	
VPN	>	Preferences	Statistics	Route Details	Firewall	Message Hi

VPN >		
Network	Connection Information	^
System Scan	State: Connected Tunnel Mode (IPv4): Split Include	
Roaming Security	Tunnel Mode (IPv6): Drop All Traffic Dynamic Tunnel Exclusion: cisco.com	
	Duration: 00:00:25 Session Disconnect: None Management Connection State: Disconnected (user tunnel active)	
	Address Information Client (IPv4):	^
	Client (IPv6): Server:	
Collect diagnostic information for all installed components.	Bytes	· · ·
Diagnostics	Reset	Export Stats

Fehlerbehebung

Sie können das AnyConnect Diagnostics and Reporting Tool (DART) verwenden, um die Daten zu erfassen, die zur Behebung von AnyConnect-Installations- und Verbindungsproblemen nützlich sind.

DART stellt die Protokolle, Status und Diagnoseinformationen für die Analyse durch das Cisco Technical Assistance Center (TAC) zusammen. Für die Ausführung von DART auf dem Client-Computer sind keine Administratorrechte erforderlich.

Problem

Wenn ein Platzhalter in den benutzerdefinierten AnyConnect-Attributen konfiguriert ist, z. B. ***.cisco.com**, wird die Verbindung zur AnyConnect-Sitzung getrennt.

Lösung

Sie können den **cisco.com**-Domänenwert verwenden, um den Ersatz des Platzhalters zu ermöglichen. Mit dieser Änderung können Sie Domänen wie **www,cisco.com** und **tools.cisco.com** ein- oder ausschließen.

Zugehörige Informationen

- Wenden Sie sich für weitere Unterstützung an das Technical Assistance Center (TAC). Ein gültiger Supportvertrag ist erforderlich: <u>Weltweiter Kontakt zum Cisco Support.</u>
- Besuchen Sie auch die Cisco VPN Community. <u>hier</u>.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.