# Configurer les politiques de contrôle d'accès au plan de contrôle pour Secure Firewall Threat Defense et ASA

# Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configurer
Configurations
Configurer une liste de contrôle d'accès du plan de contrôle pour FTD géré par FMC
Configurer une liste de contrôle d'accès du plan de contrôle pour FTD géré par FDM
Configurer une ACL de plan de contrôle pour ASA à l'aide de CLI
Configuration alternative pour bloquer les attaques du pare-feu sécurisé à l'aide de la commande « shun »
<u>Vérifier</u>
Boques associés

# Introduction

Ce document décrit le processus de configuration des règles d'accès au plan de contrôle pour Secure Firewall Threat Defense et Adaptive Security Appliance (ASA).

# Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protection pare-feu contre les menaces (FTD)
- Gestionnaire de périphériques de pare-feu sécurisé (FDM)
- Centre de gestion du pare-feu sécurisé (FMC)
- Pare-feu sécurisé ASA
- Liste de contrôle d'accès (ACL)
- FlexConfig

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Protection pare-feu sécurisée version 7.2.5
- Secure Firewall Manager Center version 7.2.5
- Secure Firewall Device Manager version 7.2.5
- Pare-feu sécurisé ASA version 9.18.3

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Informations générales

Le trafic traverse généralement un pare-feu et est acheminé entre des interfaces de données ; dans certaines circonstances, il est préférable de refuser le trafic destiné au pare-feu sécurisé. Le pare-feu sécurisé Cisco peut utiliser une liste de contrôle d'accès (ACL) du plan de contrôle pour restreindre le trafic prêt à l'emploi. Par exemple, lorsqu'une liste de contrôle d'accès du plan de contrôle peut être utile, il est possible de contrôler quels homologues peuvent établir un tunnel VPN (site à site ou accès à distance VPN) vers le pare-feu sécurisé.

Trafic prêt à l'emploi du pare-feu sécurisé

Le trafic traverse normalement les pare-feu d'une interface (entrante) à une autre (sortante), c'est ce qu'on appelle le trafic « tout-en-un » et il est géré à la fois par les politiques de contrôle d'accès (ACP) et les règles de pré-filtrage.



Image 1. Exemple de trafic prêt à l'emploi

Trafic prêt à l'emploi du pare-feu sécurisé

Dans d'autres cas, le trafic est directement destiné à une interface FTD (VPN de site à site ou d'accès à distance). Il s'agit du trafic « prêt à l'emploi », géré par le plan de contrôle de cette interface spécifique.



Image 2. Exemple de trafic prêt à l'emploi

Considérations importantes concernant les ACL du plan de contrôle

- À partir de la version 7.0 de FMC/FTD, une liste de contrôle d'accès du plan de contrôle doit être configurée à l'aide de FlexConfig, en utilisant la même syntaxe de commande que celle utilisée sur l'ASA.
- Le mot clé control-plane est ajouté à la configuration access-group, qui appliquera le trafic 'vers' l'interface de pare-feu sécurisée. Sans le mot de plan de contrôle ajouté à la commande, la liste de contrôle d'accès restreindrait le trafic « à travers » le pare-feu sécurisé.
- Une liste de contrôle d'accès du plan de contrôle ne restreint pas les connexions entrantes SSH, ICMP ou TELNET à une interface de pare-feu sécurisée. Elles sont traitées (autorisées/refusées) conformément aux stratégies des paramètres de la plate-forme et ont une priorité plus élevée.
- Une liste de contrôle d'accès du plan de contrôle restreint le trafic 'vers' le pare-feu sécurisé lui-même, alors que la politique de contrôle d'accès pour le FTD ou les listes de contrôle d'accès normales pour l'ASA, contrôle le trafic 'à travers' le pare-feu sécurisé.
- Contrairement à une liste de contrôle d'accès normale, il n'y a pas de « deny » implicite à la fin de la liste.
- Au moment de la création de ce document, la fonction de géolocalisation du FTD ne peut pas être utilisée pour restreindre l'accès au FTD.

# Configurer

Dans l'exemple suivant, un ensemble d'adresses IP d'un pays donné tente de forcer le VPN dans le réseau en essayant de se connecter au RAVPN FTD. La meilleure option pour protéger le FTD contre ces attaques de force brute VPN est de configurer une ACL de plan de contrôle pour bloquer ces connexions à l'interface FTD externe.

### Configurations

Configurer une liste de contrôle d'accès du plan de contrôle pour FTD géré par FMC

Voici la procédure que vous devez suivre dans un FMC pour configurer une ACL de plan de contrôle pour bloquer les attaques en force entrantes de VPN vers l'interface FTD externe :

Étape 1. Ouvrez l'interface utilisateur graphique FMC via HTTPS et connectez-vous avec vos informations d'identification.

cisco SECURE	
Secure Firewall	
Management	
Center	
Username	
Password	
Log In	NI COTTA
	And Destroyed and the second second

Image 3. Page de connexion FMC

Étape 2. Vous devez créer une liste de contrôle d'accès étendue. Pour cela, accédez à Objets > Gestion des objets.

Firewall Management Center Overview / Dashboards / Dashboard	Overview Analy	vsis Policies	Devices	Objects	Integration	Deploy Q 🔮 🌣 💡 a	dmin • ••••••• SECURE
Summary Dashboard (switch.slatzboard) Provides a summary of activity on the appliance				Object M Intrusion	lanagement Rules		Reporting
Network × Threats Intrusion Events	Status Geolocati	on QoS				Show the Last 1 hour	• 11
Unique Applications over Time		<ul> <li>Top Web App</li> </ul>	lications Seen			Top Client Applications Seen	
No Data			N	lo Data		No Data	
Last updated 2 minutes ago							
Traffic by Application Risk		► Top Server A	pplications See	n		Top Operating Systems Seen	

Image 4. Gestion des objets

Étape 2.1. Dans le volet de gauche, accédez à Access List > Extended pour créer une liste de contrôle d'accès étendue.

Firewall Management	t Center <sub>Overview</sub>	Analysis I	Policies Devices	Objects	Integration		Deploy Q 🧬	🌣 🕜 admin 🕇 🏻	SECURE
> AAA Server <ul> <li>Access List</li> <li>Extended</li> <li>Standard</li> </ul>	Network A network object represent network discovery rules, ev	s one or more IP ad ent searches, repor	idresses. Network object ts, and so on.	ts are used in v	arious places, ir	Add Network	Cies, network variables,	Filter Show Unused Object intrusion rules, identity	s rules,
> Address Pools	Name				N N	Value	Туре	Override	
Application Filters AS Path	any				(	0.0.0/0 ::/0	Group		ୟ 🗑 👪
Cipher Suite List	any-ipv4				(	0.0.0.0/0	Network		ୟ 🗑 👪
> Community List	any-ipv6					::/0	Host		۵ 🗎 🛤
<ul> <li>Distinguished Name</li> <li>DNS Server Group</li> </ul>	IPv4-Benchmark-Tests				1	198.18.0.0/15	Network		९ ≣ ₿
> External Attributes	IPv4-Link-Local				1	169.254.0.0/16	Network		ର ≣ ଲ
File List	IPv4-Multicast				:	224.0.0.0/4	Network		ୟ 🗑 👪
Geolocation	IPv4-Private-10.0.0.0-8				1	10.0.0/8	Network		ର ≣ ଈ
Interface	IPv4-Private-172.16.0.0-12				1	172.16.0.0/12	Network		ୟ 🗑 👪
Key Chain	IPv4-Private-192.168.0.0-1	6			1	192.168.0.0/16	Network		् 🗑 👪
> PKI	IPv4-Private-All-RFC1918					10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group		ୟ ≣ ୫୫
Port							Displaying 1 - 14 of 14 ro	ws K < Page 1	of 1 > >  C

Image 5. Menu ACL étendue

### Étape 2.2. Sélectionnez ensuite Ajouter une liste d'accès étendue.

Cipiects / Object Management	Center	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	, Q ,	<b>\$</b> \$	🗿 admin 🕶 🛛	cisco SECURE
> AAA Server	Extended							Add Extended Acc	ess List	् Filter		
✓ Access List	An oppose list of	biest sles kno		ee eestrol lie		a tha traffic to	utich a condec udl contro G	Standard Identifian traffic	based on	dectinatio	addraaa aabr	Identifies
Extended	traffic based on	source and de	stination addr	ess and ports	s. Supports IPv	4 and IPv6 ad	dresses. You use these obje	cts when configuring par	ticular fea	tures, such	as route map	s.
Standard												
> Address Pools	Name							Value			Override	
Application Filters												
AS Path							records to display					
Cipher Suite List												
> Community List												
> Distinguished Name												
DNS Server Group												
> External Attributes												
File List												
> FlexConfig												
Geolocation												
Interface												
Key Chain												
Network												
> ркі												
Policy List												
Port									No data to	display  <	< Page 1	of 1 > > C
> Prefix List												

Image 6. Ajouter une liste de contrôle étendue

Étape 2.3. Tapez un nom pour la liste de contrôle d'accès étendue, puis cliquez sur le bouton Ajouter pour créer une entrée de contrôle d'accès :

AAA Server Access List Object	Firewall Man Objects / Object N	agement Cer Management	nter	Overview	Analysis	Policies	Device	s Objects	Integ	ration		Deploy	٩	¢	🕜 admin 🔻	cisco SECURE	
Access List   Extended Name   Standard ACL-UNWANTED-COUNTRY     Address Pools ACL-UNWANTED-COUNTRY     Address Pools ACL-UNWANTED-COUNTRY     Address Pools Action Source     Application Filters   AS Path   Cipher Suite List   Sequence Action Source   Source Port   Destination Port   Application     No records to display        No records to display        No records to display        Pietural Attributes   File List   Pietural Attributes   File List   Pietural Attributes	> AAA Server	New Exter	nded Acc	ess List Ob	ject												
Standard ACL-UNWANTED-COUNTRY     A Address Pools     Application Filters     AS Path     Cipher Suite List     Sequence   Action   Source Port      Source Port   Destination Port        Add     Source Port     Destination Port     Application     No records to display     Vertices     Piet List     Piet	<ul> <li>Access List</li> <li>Extended</li> </ul>	Name													dress on oute ma	y. Identifies os.	
Application Filters         Application Filters         As Path         Cipher Suite List         Source Management         Action         Source Port         Destination Port         Application         No records to display         Vorecords         File List         Peternal Attributes         File List         Geolocation         Interface	Standard  Address Pools	ACL-UNWA	ANTED-CO	UNTRY											Override		
Sequence       Action       Source Port       Destination       Destination Port       Application         > Community List       No records to display       No records to display       Image: Community List       Image: Community List	Application Filters	Entries (0)												Add			
> Community List     No records to display       > Distinguished Name     DNS Server Group       > External Attributes     File List       > FlexConfig     Allow Overrides       Interface     Allow Overrides	Cipher Suite List	Sequence	Action	Source		Source Port		Destination		Destination Port	Applicatio	'n					
DNS Server Group   > External Attributes   File List   > FlexConfig   Geolocation   Interface	Distinguished Name																
File List       > FlexConfig       Geolocation       Interface	DNS Server Group > External Attributes																
Geolocation Allow Overrides	File List																
	Geolocation	Allow Ove	errides														
Key Chain	Key Chain													Save			
	> ркі																
Policy List       Port       No data to display       I       of 1	Policy List Port											No	o data to	o display	< Page 1	of 1 $>$ > C	

Image 7. Entrées ACL étendues

Étape 2.4. Remplacez l'action ACE par Block (Bloquer), puis ajoutez le réseau source pour qu'il corresponde au trafic devant être refusé au FTD, conservez le réseau de destination sur Any (Tous) et cliquez sur le bouton Add (Ajouter) pour terminer l'entrée ACE :

- Dans cet exemple, l'entrée ACE configurée bloquera les attaques en force de VPN provenant du sous-réseau 192.168.1.0/24.

Firewa Objects /	Action: Block			cisco SECURE
> AAA Server	Logging: Default			
Extended Standard	Log Level:			Identifies ;.
> Address Pools	Log Interval:			
Application Filt	300 Sec.			1 1 8
AS Path	Network Port   Application			
Community List	Available Networks C +	Source Networks (1)	Destination Networks (0)	
> Distinguished N	Q Search by name or value	192.168.1.0/24	any	
DNS Server Gre	any Add to Source			
> External Attribu	any-ipv4 Add to Destination			
File List	any-ipv6			
> FlexConfig	IPv4-Benchmark-Tests			
Geolocation	IPv4-Link-Local			
Interface	IPv4-Multicast			
Key Chain	IPv4-Private-10.0.0.0-8			
Network	IPv4-Private-172.16.0.0-12	Enter an IP address Add	Enter an IP address Add	
2 PKI Dollow List				
Policy List				of 1 >>  C
> Prefix List			Cancel Add	

Image 8. Réseaux refusés

Étape 2.5. Si vous devez ajouter d'autres entrées ACE, cliquez à nouveau sur le bouton Add et répétez l'étape 2.4. Ensuite, cliquez sur le bouton Save (Enregistrer) pour terminer la configuration de la liste de contrôle d'accès.

Firewall Managemen Objects / Object Management	Edit Extend	ded Acc	ess List Object					0	cisco SECURE
> AAA Server	Name ACL-UNWA	NTED-CO	UNTRY						
Extended	Entries (1)								Identifies
Standard								Add	
> Address Pools								_	
Application Filters	Sequence	Action	Source	Source Port	Destination	Destination Port	Application		之言从
AS Path	1 (	Block	192.168.1.0/24					11	2 00
Cipher Suite List									
> Community List									
> Distinguished Name									
DNS Server Group									
> External Attributes									
File List	Allow Ove	errides							
> FlexConfig									
Geolocation								Save	
Interface									
Key Chain									
Network									
> ркі									
Policy List									
Port							Displaying 1 - 1 of 1 rows	K < Page 1	of 1 > >  C
> Prefix List									

Image 9. Entrées ACL étendues terminées

Étape 3. Vous devez ensuite configurer un objet Flex-Config pour appliquer la liste de contrôle d'accès du plan de contrôle à l'interface FTD externe. Pour cela, accédez au panneau de gauche et sélectionnez l'option FlexConfig > FlexConfig Object.

Ð	Firewall Management Objects / Object Management	Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy Q	¢ 🗘	🕜 admin 🕶 🛛	cisco SECURE
> AAA	Server	Extended	d						Add Extende	ed Access Lis	it Q Filte	r	
✓ Acc	ess List					. (							
	Extended	An access list of traffic based or	object, also kno n source and d	own as an acce estination addr	ess control list ess and ports	t (ACL), select s. Supports IPv	ts the traffic to 4 and IPv6 ad	which a service will apply. dresses. You use these obje	Standard-Identifies ects when configuri	ng particular	on destination features, suc	h as route maps	. Identifies s.
	Standard												
> Add	ress Pools	Name							Value			Override	
Арр	lication Filters	ACL-UNWANT	ED-COUNTRY										1 1 8
AS F	Path												
Ciph	ner Suite List												
> Com	nmunity List												
> Disti	inguished Name												
DNS	Server Group												
> Exte	rnal Attributes												
File	List												
~ Flex	Config												
	FlexConfig Object												
	Text Object												
Geo	location												
Inter	face												
Key	Chain												
Netv	work												
> ркі									C	Displaying 1 - 1	lof1 rows 🕸	C < Page 1	of 1 > >  C
Polic	nv Liet												



Étape 3.1. Cliquez sur Ajouter un objet FlexConfig.

Firewall Manageme	nt Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧳 🌣 🕜 admin 🕶 🖓 SECURE
<ul> <li>&gt; AAA Server</li> <li>&gt; Access List</li> <li>Extended</li> <li>Standard</li> </ul>	FlexConfig Object FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is	Add FlexConfig Object Q. Filter
> Address Pools	Name	Description
Application Filters AS Path	Default_DNS_Configure	Configure Default DNS with the help of TextObj $has a c = 0$
Cipher Suite List	Default_Inspection_Protocol_Disable	Disable Default Inspection.
> Community List	Default_Inspection_Protocol_Enable	Enable Default Inspection. 📲 Q 👕
> Distinguished Name	DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one insid 📲 Q 🍵
DNS Server Group	DHCPv6 Prefix Delegation UnConfigure	Remove configuration of one outside (PD client 🖬 Q 📄
File List		
✓ FlexConfig	DNS_Configure	Configure DNS with the help of TextObjects an • 2 🔍
FlexConfig Object	DNS_UnConfigure	Remove the DNS configurations. For Q 🦷
Text Object	Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. co 📲 Q 🍵
Geolocation	Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. C 📲 Q 🥛
Interface	Fiaro UnConfigure	Clears eigro configuration for an AS
Key Chain		
> PKI	Eigrp_Unconfigure_All	Clears eigrp configuration. Fig. Q Displaying 1 - 20 of 48 rows I < < Page 1 of 3 > > C

Image 11. Ajouter un objet Flexconfig

Étape 3.2. Ajoutez un nom pour l'objet FlexConfig, puis insérez un objet de stratégie ACL. Pour cela, sélectionnez Insert > Insert Policy Object > Extended ACL Object.

Firewall Manageme	Name:							⊱ 🕜 admin 🕶 🗄	dualia SECURE
Objects / Object Managemen	OBJ-FC-CONTROL-PLANE								
> AAA Server	Description:							Filter	
✓ Access List									
Extended	Copy-pasting any rich te	ext might introduce line break	s while generating CLI.	Please verify the	CLI before deploy	ment.			
Standard	Insert - Pi f	Peployment: Once		Type:	Append		•		
> Address Pools	Insert Policy Object	Text Object			Append				
Application Filters	Insert System Variable >	Network						the help of TextObj	¶a Q
AS Path	Insert Secret Key	Security Zones							Ra a ⊒
Cipher Suite List		Standard ACL Object							
Community List     Distinguished Name		Extended ACL Object							¶ <u>a</u> ⊂ <sub>  </sub>
DNS Server Group		Route Map						lient) and one insid	¶∎ Q
> External Attributes								e outside (PD client	¶a ⊂, 🗑
								of TextObjects dn	R∎ Q T
✓ FlexConfig	▼ Variables								
	Name	Dimension	Default Value	Property	Override	Description		ions.	
Text Object			Nie recente te di	(Type:Name)				res next hop. 2. co	¶∎ Q
Geolocation			No records to di	spiay				ters for eigrp. 1. C	<b>팀</b> Q 🗍
Interface								ar an AS	Fa o, 🗑
Key Chain									
Network									
2 PK							Save		

Image 12. Variable objet FlexConfig

Étape 3.3. Ajoutez un nom pour la variable d'objet ACL, puis sélectionnez la liste de contrôle d'accès étendue créée à l'étape 2.3. Ensuite, cliquez sur le bouton Enregistrer.

Firewall Managemen	Name: OBJ-FC-CONTROL-PLANE	:			⊁ 🥝 admin ▾ 🏻 🤚	sco SECURE
> AAA Server ~ Access List	Description:	Insert Extended Access List Object Var	iable Ø		Filter	
Extended Standard > Address Pools Application Filters AS Path Cipher Suite List > Community List > Distinguished Name DNS Server Group > External Attributes	Copy-pasting any rich	Variable Name: VAR-ACL-UNWANTED-COUNTRY Description: Available Objects C Q. Search C. Search C. DRWANTED COUNTRY Add	Selected Object		the help of TextObj the help of TextObj lient) and one insid o outside (PD client	
✓ FlexConfig	▼ Variables				of TextObjects dn	
FlexConfig Object Text Object Geolocation Interface Key Chain	Name		Cancel	ription	res next hop. 2. co eters for eigrp. 1. C or an AS	
Network > PKI Policy List				Cancel Save	s I< < Page 1	¶∎ Q, of3>> C

Image 13. FlexConfig, variable d'objet attribution ACL

Étape 3.4. Configurez ensuite la liste de contrôle d'accès du plan de contrôle comme entrante pour l'interface externe comme suit.

Syntaxe de ligne de commande :

```
access-group "variable name starting with $ symbol" in interface "interface-name" control-plane
```

Ceci se traduit par l'exemple de commande suivant, qui utilise la variable ACL créée à l'étape 2.3 ci-dessus 'VAR-ACL-UNWANTED-COUNTRY' comme suit :

```
access-group $VAR-ACL-UNWANTED-COUNTRY in interface outside control-plane
```

C'est ainsi qu'il doit être configuré dans la fenêtre d'objet FlexConfig, après quoi, sélectionnez le bouton Enregistrer pour terminer l'objet FlexConfig.

Firewall Manageme	Name: OBJ-FC-CONTROL-PLANE						≵ @ admin <del>v</del>   "≵	secure
> AAA Server	Description:						Filter	
✓ Access List								
Extended	A Copy-pasting any rich text might in	troduce line breaks	s while generating CLI.	Please verify the	CLI before deploy	ment.		
Standard								
> Address Pools	Insert V 🔢 Deployment	Once		Type:	Append	•		
Application Filters	access-group \$VAR-ACL-UNWANTED-COUN	TRY in interface outsid	e control-plane				the help of TextObj	<b>₽</b> _ 0, ]
AS Path								Bo =
Cipher Suite List								
> Community List								¶∎ Q
> Distinguished Name							lient) and one insid	Ela Q ≣
DNS Server Group								
> External Attributes							e outside (PD client	<b>Г</b> а ( )
							of TextObjects dn	<b>₽</b> a ⊂
✓ FlexConfig	▼ Variables							B. A. E
	Name	Dimension	Default Value	Property	Override	Description	lons.	
Text Object				(Type:Name)			ires next hop. 2. co	¶∎ Q
Geolocation	VAR-ACL-UNWANTED-COUNTRY	SINGLE	ACL-UNWANTED	EXD_ACL:A	false		eters for eigro. 1. C	En α ⊒
Interface								
Key Chain							or an AS	Fi Q 📄
Network								¶a q =
> ркі							s IK < Page 1	of 3 > >  C
Policy List						Cancel Save		



Étape 4. Vous devez appliquer la configuration de l'objet FlexConfig au FTD. Pour cela, accédez à Périphériques > FlexConfig.

Cipiects / Object Management	t Center <sub>Overview</sub> Analysis Policies	Devices Objects	Integration	Deploy Q 🧬 🔒	🗱 🕜 admin <del>v</del> 🏻 🖞	SECURE	
<ul> <li>&gt; AAA Server</li> <li>&gt; Access List</li> <li>Extended</li> <li>Standard</li> <li>&gt; Address Pools</li> <li>Application Filters</li> </ul>	FlexConfig Object FlexConfig Object include device configuration commande Name Defaul	Device Management Device Upgrade NAT QoS Platform Settings FlexConfig Certificates	VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting Site to Site Monitoring	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture	ilter he help of TextObj		
AS Path Cipher Suite List	Default_Inspo	action_Protocol_Disable		Disable Default Inspection.		<b>₽</b> 0 =	
Distinguished Name     DNS Server Group	Detaul_Inspi	ix_Delegation_Configure		Configure one outside (PD client			
<ul> <li>External Attributes</li> <li>File List</li> <li>FlexConfig</li> </ul>	DHCPv6_Prefix	_Delegation_UnConfigure		Configure DNS with the help of T			
FlexConfig Object Text Object	Eig	S_UnConfigure		Remove the DNS configurat	ions. ures next hop. 2. co	α α Π	
Geolocation Interface Key Chain	Eigrp_In Eigr	nterface_Configure		Configures interface parame	eters for eigrp. 1. C or an AS	Ω α Π	
Network > PKI	Eigrp	Unconfigure_All		Clears eigrp configuration. Displaying 1 - 20 of 49 row	rs I< < Page 1	na_Q or3>>\C	

Image 15. Menu FlexConfig Policy

Étape 4.1. Cliquez ensuite sur New Policy (Nouvelle stratégie) si aucun FlexConfig n'a déjà été créé pour votre FTD, ou modifiez la stratégie FlexConfig existante.

Ę	Firewall Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🕯	•	🕜 admin <del>-</del>	cisco SECURE
													New Policy
	FlexConfig Policy			Status				Last Modified					
						created. Add	a new policy						

Image 16. Création de stratégie FlexConfig

Étape 4.2. Ajoutez un nom pour la nouvelle stratégie FlexConfig et sélectionnez le FTD auquel vous souhaitez appliquer la liste de contrôle d'accès du plan de contrôle créée.

Firewall Management Center	Overview Analysis Policies Devices Objects Integration	Deptoy Q 🥔 🌣 🕜 admin 🕶 🖓 secure
FlexConfig Policy	New Policy	0
	Name:         FLEXCONFIG-POLICY         Description:         Targeted Devices         Select devices to which you want to apply this policy.         Available Devices         Q. Search by name or value         FTD-CONTROL-PLANE         Add to Policy	

Image 17. Affectation de périphérique FlexConfig Policy

Étape 4.3. Dans le volet de gauche, recherchez l'objet FlexConfig créé à l'étape 3.2 ci-dessus, puis ajoutez-le à la stratégie FlexConfig en cliquant sur la flèche droite située au milieu de la fenêtre. Ensuite, cliquez sur le bouton Enregistrer.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	م	🥐 🌣	❷ admin •   ;	SECURE
FLEXCONFIG-POLICY										v Config Save	Cancel
										Policy As	ssignments (1)
	"3 Solooto	d Dropond F	lovConfigs								
Available FlexConfig	Selecte	a Prepena P	lexconligs								
	# Nan	10		C	Description						
V User Defined											
OBJ-FC-CONTROL-PLANE											
✓ System Defined											
Topfault_DNS_Configure											
Default_Inspection_Protocol_Disable											
Contemporary Conte	_ Selecte	d Append F	lexConfigs								
Therefix_Delegation_Configure											
DHCPv6_Prefix_Delegation_UnConfigure	# Nan	ne		C	Description						
TDNS_Configure	1 овј	-FC-CONTROL	-PLANE								۹ 🖥
DNS_UnConfigure	ц										
"B Eigrp_Configure											
B Eigrp_Interface_Configure											
_9 Eigrp_UnConfigure											

Image 18. Attribution d'objet Stratégie FlexConfig

Étape 5. Poursuivez le déploiement de la modification de configuration sur le FTD. Pour cela, accédez à Déployer > Déploiement avancé.

Overview	Analysis	Policies	Devices	Objects	Integration	Deploy C	ર 🔮 🌣	🕜 admi	n 🕶 🔤 diadia SE	CURE
							Advance	ed Deploy	Deploy All	ncel
					FTD-CONTROL-PLANE		Ready for	r Deployment	é	:s (1)
3 Select	ed Prepend F	lexConfigs								
# Na	me			Description						
					<ol> <li>1 device is available for deployment</li> </ol>				₿ •9	
Select	ed Append Fl	exConfigs								
# Na	me			Description						
1 08	I-EC-CONTROL	-PI ANF								a 🖬
		- CPUTL								
	Overview	Overview     Analysis       Image: Selected Prepend F       Image: Selected Append FI       Image: Selected Append FI<	Overview     Analysis     Policies       *     Selected Prepend FlexConfigs       #     Name       •     Selected Append FlexConfigs       #     Name	Overview     Analysis     Policies     Devices       **     Selected     Prepend FlexConfigs	Overview     Analysis     Policies     Devices     Objects       * Selected Prepend FlexConfigs      Description       * Name      Description	Overview     Analysis     Policies     Devices     Objects     Integration       Q     FTD-CONTROL-PLANE     FTD-CONTROL-PLANE     FTD-CONTROL-PLANE       #     Name     Description       #     Name     Description       •     1 device is available for deployment       1     OBJ-FC-CONTROL-PLANE	Overview Analysis Policies Devices Objects Integration Deploy O   Q FTD-CONTROL-PLANE PTD-CONTROL-PLANE PTD-CONTROL-PL	Overview Analysis Policies Devices Objects Integration Deploy Q Image: Confige Conf	Overview Analysis Policies Devices Objects Integration Deploy Q Image: Configs   Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs   Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs   Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs   Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs   Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs   Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs   Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs   Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs   Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs   Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs Image: Configs   Image: Configs Image: Configs Im	Overview Analysis Policies Devices Objects Integration Deploy Q Image: Control - PLANE Advanced Deploy Deploy All   Image: Control - PLANE   Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE   Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE   Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE   Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE Image: Control - PLANE

Image 19. Déploiement avancé FTD

Étape 5.1. Sélectionnez ensuite le FTD auquel vous souhaitez appliquer la stratégie FlexConfig. Si tout est correct, cliquez sur Déployer.

þ	Fi	rewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🇳	🌣 😧 admin 🕶	cisco SECURE
1 devic	ce sele Q	ected Search using device name, user name, type,	, group or statu	15								Deploy time: Estime	te Deploy
	2	Device	Modified by		Inspect Inte	rruption	Туре	Group	Last Deploy Time		Preview	Status	
×		FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12:0	5 PM	B	Ready for Deployme	ant
:: •		Flex Configuration     Template Policy: FLEXCONFIG-POLICY											
https://10	RR 243	R 5R43013/ddd/IIC ontworksmicroen											
												-	

Image 20. Validation du déploiement FTD

Étape 5.2. Ensuite, une fenêtre de confirmation du déploiement s'affiche, ajoute un commentaire pour suivre le déploiement et passe à Déployer.

Firewall Management Center	Overview	Analysis P	Policies	Devices	Objects	Integration		De	ploy Q 🤞	🔅 🕝 admin 🕶 🔤	SECURE
1 device selected           Image: The selected           Image: The selected selected           Image: The selected s											
Device	Modified by										
V 🛃 FTD-CONTROL-PLANE	admin						Sep	5, 2023 12:05 PM		Ready for Deployment	
<ul> <li>Flex Configuration</li> <li>Template Policy: FLEXCONFIG-POLICY</li> </ul>		Deployme	ent Conf	irmation			×				
		You have sel	lected 1 d	evice to deple	v						
		Deployment	Notes:								
		You can opt	tionally ad	d notes abou	t the configur	ation changes					
							Deploy				

Image 21. Commentaires sur le déploiement FTD

Étape 5.3. Un message d'avertissement peut s'afficher lors du déploiement des modifications FlexConfig. Cliquez sur Déployer uniquement si vous êtes entièrement certain que la configuration de la stratégie est correcte.



Image 22. Avertissement FTD Deployment Flexconfig

#### Étape 5.4. Vérifiez que le déploiement de la stratégie a réussi pour le FTD.

Ð	Fi De	rewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy Q	. 🧳	🌣 🕜 admi	n ▼ disabi SECURE
<b>T</b>	۹	Search using device name, user name, type,	, group or statu	IS									Deploy
		Device	Modified by		Inspect Inte	rruption	Туре	Group	Last Deploy Time	Previ	ew	Status	
~		FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12:0	5 PM	B.	Completed	
*= •		<ul> <li>Flex Configuration</li> <li>Template Policy; FLEXCONFIG-POLICY</li> </ul>									I		

Image 23. Déploiement FTD réussi

Étape 6. Si vous créez une nouvelle liste de contrôle d'accès de plan de contrôle pour votre FTD ou si vous avez modifié une liste existante en cours d'utilisation, il est important de souligner que les modifications de configuration apportées ne s'appliquent pas aux connexions déjà établies au FTD. Par conséquent, vous devez effacer manuellement les tentatives de connexion actives au FTD. Pour cela, connectez-vous à l'interface de ligne de commande du FTD et effacez les connexions actives comme suit.

Pour effacer la connexion active d'une adresse IP d'hôte spécifique :

> clear conn address 192.168.1.10 all

Pour effacer les connexions actives d'un réseau de sous-réseau entier :

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

Pour effacer les connexions actives d'une plage d'adresses IP :

> clear conn address 192.168.1.1-192.168.1.10 all

Remarque : il est fortement recommandé d'utiliser le mot clé « all » à la fin de la commande clear conn address pour forcer l'effacement des tentatives de connexion en force brute VPN actives vers le pare-feu sécurisé, principalement lorsque la nature de l'attaque en force brute VPN lance une rafale de tentatives de connexion constantes.

Configurer une liste de contrôle d'accès du plan de contrôle pour FTD géré par FDM

Voici la procédure que vous devez suivre dans un FDM pour configurer une ACL de plan de contrôle pour bloquer les attaques en force entrantes de VPN vers l'interface FTD externe :

Étape 1. Ouvrez l'interface utilisateur graphique de FDM via HTTPS et connectez-vous avec vos informations d'identification.



cisco SECURE

Cisco Secure Firewall Device Manager

Username	
Password	
	•
	LOG IN

© 2015-2023 Clisco Systems, Inc. Clisco, Clisco Systems and Clisco Systems logo are registered trademarks of Clisco Systems, Inc. This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2, 1 and 3" provided with ABSOLUTEUX NO WARRANTV under the terms of "GNU Lesser General Public License, versions 2, 2, 2, 1 and 3" provided with

Firewall Device Manager Monitoring	Image: Policies         Image: Policies         Device: firepower	> 🖨 @ ?	admin Administrator
Model Cisco Firepower Threat Defen	Software VDB Intrusion R se for VMwa 7.2.5-208 353.0 20220511	tule Update Cloud Services High Av. -1540 Not Registered   Register Not Cor	ailability 🕜 CONFIGURE
r Inside Net	0/1 Cisco Firepower Threat Defense for VMware 0/0 0/1 € € 0/0	MGMT MGMT CONSOLE ISP/WAN/Gateway CONSOLE	Mit DNS Server
Interfaces Connected Enabled 3 of 3 View All Interfaces	Routing There are no static routes yet View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service DNS Server
Smart License Evaluation expires in 89 days	Backup and Restore	Troubleshoot No files created yet	Management Interface Hostname Time Services

Étape 2. Vous devez créer un réseau d'objets. Pour cela, accédez à Objets :

Image 25. Tableau de bord principal FDM

Étape 2.1. Dans le volet de gauche, sélectionnez Réseaux, puis cliquez sur le bouton « + » pour créer un nouvel objet réseau.

+ 🔍
ACTIONS
te-

Image 26. Création d'objets

Étape 2.2. Ajoutez un nom pour l'objet réseau, sélectionnez le type de réseau pour l'objet, ajoutez l'adresse IP, l'adresse réseau ou la plage d'adresses IP pour faire correspondre le trafic qui doit être refusé au FTD. Cliquez ensuite sur le bouton Ok pour terminer le réseau d'objets.

- Dans cet exemple, le réseau objet configuré est destiné à bloquer les attaques en force de VPN provenant du sous-réseau 192.168.1.0/24.

Firewall Device Manager	Monitoring Police			admin
Object Types ←	Network Obje		V ×	
C Networks	6 objects	OBJ-NET-UNWANTED-COUNTRY		+ 🕫
S Ports				defined. User defined
G Security Zones	N NAME	Description		ACTIONS
F Application Filters	1 IPv4-Private-A		1.	e-172.16.0.0-12, IPv4-Private-
🖉 URLs	2 IPv4-Private-10	Туре		
Geolocations	3 IPv4-Private-1	Network Host FQDN Rang	l6	
Syslog Servers	4 IPv4-Private-19	Network		
	5 any-ipv4	192.168.1.0/24		
IPSec Proposals	6 any-ipv6	e.g. raz.rooz.o/z+ or zoor.boo.o.boo		
Secure Client Profiles			CANCEL OK	
🚉 Identity Sources				
1 Users				
🙊 Certificates				
🔒 Secret Keys				

Image 27. Ajouter un objet réseau

Étape 3. Ensuite, vous devez créer une liste de contrôle d'accès étendue. Pour cela, accédez à l'onglet Device du menu supérieur.

Firewall Device Manager	Monitoring Policies Objects Device: firepow	er	cisco SECURE
Object Types ←	Network Objects and Groups		
C Networks	7 objects	<b>T</b> Filter	+ 👰
S Ports		Preset filters: System defined, User defined	
Security Zones	# NAME	TYPE VALUE	ACTIONS
Application Filters	1 IPv4-Private-AlI-RFC1918	Group IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private- 192.168.0.0-16	
🖉 URLs	2 IPv4-Private-10.0.0-8	NETWORK 10.0.0/8	
Geolocations	3 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0/12	
Svslog Servers	4 IPv4-Private-192.168.0.0-16	NETWORK 192.168.0.0/16	
	5 any-ipv4	NETWORK 0.0.0.0/0	
TKE Policies	6 any-ipv6	NETWORK ::/0	
🛶 IPSec Proposals	7 OBJ-NET-UNWANTED-COUNTRY	NETWORK 192.168.1.0/24	
Secure Client Profiles			
Sal Identity Sources			
1 Users			
🙊 Certificates			
🔒 Secret Keys			

Image 28. Page Paramètres du périphérique

Étape 3.1. Faites défiler vers le bas et sélectionnez Afficher la configuration dans le carré Configuration avancée comme suit.

Firewall Device Manager Monitoring	Policies Objects Device: firepower	> 🚔 💿 ?	admin Administrator
	070 		
Interfaces	Routing	Updates	System Settings
Connected Enabled 3 of 3 View All Interfaces	There are no static routes yet View Configuration	Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	DNS Service
Smart License	Backup and Restore	Troubleshoot No files created yet	DNS Server Management Interface Hostname Time Services
View Configuration	View Configuration	REQUEST FILE TO BE CREATED	See more
Site-to-Site VPN There are no connections yet	Remote Access VPN Requires RA VPN license No connections   1 Group Policy	Advanced Configuration Includes: FlexConfig, Smart CLI	Device Administration Audit Events, Deployment History, Download Configuration
View Configuration	Configure >	View Configuration	View Configuration

Image 29. Configuration avancée de FDM

Étape 3.2. Dans le volet de gauche, accédez à Smart CLI > Objects, puis cliquez sur CREATE SMART CLI OBJECT.

Firewall Device Manager	题 Monitoring F	© Policies Ot	bjects Device:	: firepower				?:	admin Administrator	<ul> <li>diale SECURE</li> </ul>	
Advanced ← Configuration	Device Summary Objects										
Smart CLI										+	
Objects	# N	AME	TYPE		DESCRIPTION				ACTIONS		
FlexConfig				Cta	There are no Sma	art CLI objects y	et.				
FlexConfig Objects				Sta	int by creating the	first Smart GLI	oject.				
FlexConfig Policy				L	CREATE SMA	RT CLI OBJECT					

Image 30. Objets Smart CLI

Étape 3.3. Ajoutez un nom à la liste de contrôle d'accès étendue à créer, sélectionnez Liste d'accès étendue dans le menu déroulant du modèle CLI, puis configurez les ACE requises à l'aide de l'objet réseau créé à l'étape 2.2 ci-dessus, puis cliquez sur le bouton OK pour terminer la liste de contrôle d'accès.

Firewall Devic	Edit Smart CLI Object	admin that SE	CURE
Advanced Configuration	Name	Description	
Smart CLI	ACL-UNWANTED-COUNTRY CLI Template		+ CTIONS
Objects	Extended Access List ~		
FlexConfig	Template	Show disabled \$\overline\$ Reset	
	<ul> <li>1 access-list ACL-UMANITED-COUNTRY extended</li> <li>2 configure access-list-entry demy ~</li> <li>3 demy network source [00]-hef-UMANITED-COUNTRY ~ &gt;] destin</li> <li>4 configure demy port any ~</li> <li>5 demy port source ANY destination ANY</li> <li>6 configure logging default ~</li> <li>7 default log set log-level INFORMATIONAL log-interval</li> </ul>	ation [ <u>my-ipvf X</u> ~ ] 300	
		CANCEL	

Image 31. Création ACL étendue

Remarque : si vous devez ajouter d'autres ACE pour la liste de contrôle d'accès, vous pouvez le faire en plaçant le curseur de la souris sur la gauche de l'ACE actuelle ; trois points cliquables s'affichent alors. Cliquez dessus et sélectionnez Dupliquer pour ajouter d'autres ACE.

Étape 4. Ensuite, vous devez créer un objet FlexConfig, pour cela, naviguez vers le panneau de gauche et sélectionnez FlexConfig > Objets FlexConfig, puis cliquez sur CREATE FLEXCONFIG OBJECT.

Firewall Device Mana	iger Monitoring	Policies Object	cts Device: firepower	۵. 🚔 (	adi	imin v their SECURE
Advanced ← Configuration	Device Summ FlexCont	ary fig Objects				
Smart CLI				۲	Filter	+
Objects		NAME	DESCRIPTION		ACTIONS	
FlexConfig			There Start by c	are no FlexConfig objects yet. reating the first FlexConfig objec	ct.	
FlexConfig Objects				CREATE FLEXCONFIG OBJECT		

Image 32. Objets FlexConfig

Étape 4.1. Ajoutez un nom à l'objet FlexConfig pour créer et configurer la liste de contrôle d'accès

du plan de contrôle comme entrant pour l'interface externe comme suit.

Syntaxe de ligne de commande :

```
access-group "ACL-name" in interface "interface-name" control-plane
```

Cela se traduit par l'exemple de commande suivant, qui utilise la liste de contrôle d'accès étendue créée à l'étape 3.3 ci-dessus « ACL-UNWANTED-COUNTRY » comme suit :

```
access-group \ \ ACL-UNWANTED-COUNTRY \ in \ interface \ outside \ \ control-plane
```

C'est ainsi qu'il doit être configuré dans la fenêtre d'objet FlexConfig, après quoi, sélectionnez le bouton OK pour terminer l'objet FlexConfig.

Firewall Device Ma	nager Monitoring	Ø #2			admin Administrator
	Davice Sur	Create FlexConfig Object			
Advanced ← Configuration	FlexCo	Name			
		OBJ-FC-CONTROL-PLANE			+
Smart CLI		Description			ctows
Objects				11.	
FlexConfig		Variables			
FlexConfig Objects		There are no variables yet. Start with adding a new variable.			
FlexConfig Policy		+ ADD VARIABLE			
		Template	Expand	🗘 Reset	
		1 access-group ACL-UNWANTED-COUN	ITRY in interface outside control-plane		
		Negate Template 🛆	Expand	🗘 Reset	
		1 no access-group ACL-UNMANTED-0	COUNTRY in interface outside control-plane		
			CANCEL	ОК	

Image 33. Création d'objet FlexConfig

Étape 5. Continuez à créer une politique FlexConfig, pour cela, accédez à Flexconfig > FlexConfig Policy, cliquez sur le bouton '+', et sélectionnez l'objet FlexConfig qui a été créé à l'étape 4.1 cidessus.



Image 34. Politique FlexConfig

Étape 5.1. Vérifiez que l'aperçu de FlexConfig affiche la configuration correcte pour la liste de contrôle d'accès du plan de contrôle créée et cliquez sur le bouton Save (Enregistrer).

Firewall Device Mana	Iger Monitoring Policies Objects Device: firepower	(c)	
Advanced ← Configuration	Device Summary FlexConfig Policy		
Smart CLI	Group List	Preview	
Objects	OBJ-FC-CONTROL-PLANE	1 access-group ACL-UNMANTED-COUNTRY in interface outside control-plane	
FlexConfig			
FlexConfig Objects			
FlexConfig Policy			
	SAVE		

Image 35. Aperçu de la stratégie FlexConfig

Étape 6. Déployez les modifications de configuration sur le FTD que vous souhaitez protéger contre les attaques en force VPN. Pour cela, cliquez sur le bouton Déploiement dans le menu supérieur, vérifiez que les modifications de configuration à déployer sont correctes, puis cliquez sur DÉPLOYER MAINTENANT.

Firewall Device Manager		istrator v ulturle SECURE	
Advanced ← Configuration	Pending Changes     Last Deployment Completed Successfully     05 Sep 2023 02:27 PM. See Deployment History	• ×	
Smart CLI	Deployed Version (05 Sep 2023 02:27 PM)	Pending Version C LEGEND	
Objects	Network Object Added: OBJ-NET-UNWANTED-COUNTRY		
FlexConfig		subType: Network CLAND value: 2.2.2.0/24 isSystemDefined: false dmsResolution: IPV4_ND_IPV6 description:	
FlexConfig Objects	-	name: 083-NET-UNMANTED-COUNTRY	
FlexConfig Policy	SelexConfig Policy Edited: default-group		
	flexConfigObjects: -	083-FC-CONTROL-PLANE	
	Extended Access List Added: ACL-UNWANTED-COUNTRY		
	- - - entries[0].sourceNetworks:	entries[0].logging: DEFAULT entries[0].action: DENY name: ACL-UNWANTED-COUNTRY	
	MORE ACTIONS V	CANCEL DEPLOY NOW	

Image 36. Déploiement en attente

Firewall Device Mar	anager Pending Changes	ator 🐣 就 SECURE
Advanced Configuration Configuration	There are no Pending Changes yet.	↔ Expand
FlexConfig FlexConfig Objects FlexConfig Policy	Last successful deployment was on <b>05 Sep 2023 11:09 AM</b> . You can see what was deployed in previous jobs in the Deployment History.	interface outside
	SAVE	

Image 37. Déploiement réussi

Étape 7. Si vous créez une nouvelle liste de contrôle d'accès de plan de contrôle pour votre FTD ou si vous avez modifié une liste existante en cours d'utilisation, il est important de souligner que les modifications de configuration apportées ne s'appliquent pas aux connexions déjà établies au FTD. Par conséquent, vous devez effacer manuellement les tentatives de connexion actives au FTD. Pour cela, connectez-vous à l'interface de ligne de commande du FTD et effacez les connexions actives comme suit.

Pour effacer la connexion active d'une adresse IP d'hôte spécifique :

> clear conn address 192.168.1.10 all

Pour effacer les connexions actives d'un réseau de sous-réseau entier :

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

Pour effacer les connexions actives d'une plage d'adresses IP :

> clear conn address 192.168.1.1-192.168.1.10 all

Remarque : il est fortement recommandé d'utiliser le mot clé « all » à la fin de la commande clear conn address pour forcer l'effacement des tentatives de connexion en force brute VPN actives vers le pare-feu sécurisé, principalement lorsque la nature de l'attaque en force brute VPN lance une rafale de tentatives de connexion constantes.

Configurer une ACL de plan de contrôle pour ASA à l'aide de CLI

Voici la procédure à suivre dans une interface de ligne de commande ASA pour configurer une liste de contrôle d'accès du plan de contrôle pour bloquer les attaques en force entrantes du VPN vers l'interface externe :

Étape 1. Connectez-vous au pare-feu sécurisé ASA via l'interface de ligne de commande et accédez au « terminal de configuration » comme suit.

asa# configure terminal

Étape 2. Utilisez la commande suivante pour configurer une liste de contrôle d'accès étendue afin de bloquer une adresse IP hôte ou une adresse réseau pour le trafic qui doit être bloqué vers l'ASA.

 Dans cet exemple, vous créez une nouvelle liste de contrôle d'accès appelée « ACL-UNWANTED-COUNTRY » et l'entrée ACE configurée bloque les attaques en force brute VPN provenant du sous-réseau 192.168.1.0/24. Étape 3. Utilisez la commande next access-group pour configurer la liste de contrôle d'accès « ACL-UNWANTED-COUNTRY » en tant que liste de contrôle d'accès du plan de contrôle pour l'interface ASA externe.

asa(config)# access-group ACL-UNWANTED-COUNTRY in interface outside control-plane

Étape 4. Si vous créez une nouvelle liste de contrôle d'accès de plan de contrôle ou si vous avez modifié une liste existante qui est activement utilisée, alors il est important de souligner que les modifications de configuration apportées ne s'appliquent pas aux connexions déjà établies à l'ASA, par conséquent, vous devez effacer manuellement les tentatives de connexion active à l'ASA. Pour cela, effacez les connexions actives comme suit.

Pour effacer la connexion active d'une adresse IP d'hôte spécifique :

```
asa# clear conn address 192.168.1.10 all
```

Pour effacer les connexions actives d'un réseau de sous-réseau entier :

asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all

Pour effacer les connexions actives d'une plage d'adresses IP :

asa# clear conn address 192.168.1.1-192.168.1.10 all

Remarque : il est fortement recommandé d'utiliser le mot clé « all » à la fin de la commande clear conn address pour forcer l'effacement des tentatives de connexion en force brute VPN actives vers le pare-feu sécurisé, principalement lorsque la nature de l'attaque en force brute VPN lance une rafale de tentatives de connexion constantes.

Configuration alternative pour bloquer les attaques du pare-feu sécurisé à l'aide de la commande « shun »

En cas d'option immédiate de blocage des attaques pour le pare-feu sécurisé, vous pouvez alors

utiliser la commande « shun ». La commande hunvous permet de bloquer les connexions d'un hôte attaquant.

- Une fois l'adresse IP désactivée, toutes les connexions futures à partir de l'adresse IP source sont abandonnées et consignées jusqu'à ce que la fonction de blocage soit supprimée manuellement.

- La fonction de blocage de la commande hunest appliquée qu'une connexion avec l'adresse hôte spécifiée soit active ou non.

- Si vous spécifiez l'adresse de destination, les ports source et de destination, ainsi que le protocole, vous supprimez la connexion correspondante et vous placez un shun sur toutes les futures connexions à partir de l'IP source

; toutes les connexions futures sont rejetées, pas seulement celles qui correspondent à ces paramètres de connexion spécifiques.

- Vous ne pouvez avoir qu'une seule commande hunpar adresse IP source.

- Comme la commande hunest utilisée pour bloquer les attaques de manière dynamique, elle n'est pas affichée dans la configuration du périphérique de défense contre les menaces.

- Chaque fois qu'une configuration d'interface est supprimée, tous les shuns qui sont reliés à cette interface sont également supprimés.

- Syntaxe de la commande Shun :

```
shun source_ip [ dest_ip source_port dest_port [ protocol]] [ vlan vlan_id]
```

- Pour désactiver un shun, utilisez la forme no de cette commande :

```
no shun source_ip [ vlan vlan_id]
```

Pour désactiver une adresse IP d'hôte, procédez comme suit pour le pare-feu sécurisé. Dans cet exemple, la commande « shun » est utilisée pour bloquer les attaques de force brute VPN provenant de l'adresse IP source 192.168.1.10.

Exemple de configuration pour FTD.

Étape 1. Connectez-vous au FTD via l'interface de ligne de commande et appliquez la commande shun comme suit.

#### <#root>

```
> shum 192.168.1.10
Shun 192.168.1.10 added in context: single_vf
```

Shun 192.168.1.10 successful

Étape 2. Vous pouvez utiliser les commandes show suivantes pour confirmer les adresses IP de shun dans le FTD et pour surveiller le nombre d'occurrences de shun par adresse IP :

#### <#root>

>

show shun

shun (outside) 192.168.1.10 0.0.0.0 0 0

>

show shun statistics

diagnostic=OFF, cnt=0
outside=ON, cnt=0

Shun 192.168.1.10 cnt=0, time=(0:00:28)

Exemple de configuration pour ASA

Étape 1. Connectez-vous à l'ASA via l'interface de ligne de commande et appliquez la commande shun comme suit.

#### <#root>

asa#

shun 192.168.1.10

Shun 192.168.1.10 added in context: single\_vf

Shun 192.168.1.10 successful

Étape 2. Vous pouvez utiliser les commandes show suivantes pour confirmer les adresses IP de shun dans l'ASA et pour surveiller le nombre d'occurrences de shun par adresse IP :

#### <#root>

asa#
show shun
shun (outside) 192.168.1.10 0.0.0 0 0 0
asa#
show shun statistics
outside=ON, cnt=0
inside=OFF, cnt=0
dmz=OFF, cnt=0
outside1=OFF, cnt=0
Shun 192.168.1.10 cnt=0, time=(0:01:39)

Remarque : pour plus d'informations sur la commande secure firewall shun, consultez le document <u>Cisco Secure Firewall Threat Defense Command Reference</u>

### Vérifier

Pour confirmer que la configuration de la liste de contrôle d'accès du plan de contrôle est en place pour le pare-feu sécurisé, procédez comme suit :

Étape 1. Connectez-vous au pare-feu sécurisé via l'interface de ligne de commande et exécutez les commandes suivantes pour confirmer que la configuration de la liste de contrôle d'accès du plan de contrôle est appliquée.

Exemple de résultat pour le FTD géré par FMC :

<#root>

>

show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

>

show running-config access-group

```
***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Exemple de résultat pour le FTD géré par FDM :

#### <#root>

```
> show running-config object id OBJ-NET-UNWANTED-COUNTRY
```

object network OBJ-NET-UNWANTED-COUNTRY subnet 192.168.1.0 255.255.255.0

>

```
show running-config access-list ACL-UNWANTED-COUNTRY
```

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any4 log default

> show running-config access-group

```
***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Exemple de résultat pour ASA :

```
<#root>
```

asa#

show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

asa#

show running-config access-group

\*\*\*OUTPUT OMITTED FOR BREVITY\*\*\* access-group ACL-UNWANTED-COUNTRY in interface outside control-plane

Étape 2. Pour confirmer que la liste de contrôle d'accès du plan de contrôle bloque le trafic requis, utilisez la commande packet-tracer pour simuler une connexion TCP 443 entrante à l'interface externe du pare-feu sécurisé, puis utilisez la commande show access-list <acl-name> , le nombre d'occurrences de la liste de contrôle d'accès doit s'incrémenter chaque fois qu'une connexion VPN en force brute au pare-feu sécurisé est bloquée par la liste de contrôle d'accès du plan de contrôle :

 Dans cet exemple, la commande packet-tracer simule une connexion TCP 443 entrante provenant de l'hôte 192.168.1.10 et destinée à l'adresse IP externe de notre pare-feu sécurisé. Le résultat « packet-tracer » confirme que le trafic est abandonné et le résultat « show access-list » affiche les incréments du nombre de succès pour notre ACL de plan de contrôle en place :

Exemple de résultat pour FTD

<#root>

> packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.251 443 Phase: 1 Type: ACCESS-LIST Subtype: log Result: DROP Elapsed time: 21700 ns Config: Additional Information: Result: input-interface: outside(vrfid:0) input-status: up input-line-status: up Action: drop Time Taken: 21700 ns Drop-reason: (acl-drop) Flow is denied by configured rule , Drop-location: frame 0x00005623c7f324e7 flow (NA)/NA > show access-list ACL-UNWANTED-COUNTRY

```
access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any (
```

hitcnt=1

) 0x142f69bf

Exemple de résultat pour ASA

#### <#root>

asa#

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.5 443

Phase: 1 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 19688 ns Config: Implicit Rule Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: log Result: DROP Elapsed time: 17833 ns Config: Additional Information: Result: input-interface: outside input-status: up input-line-status: up Action: drop Time Taken: 37521 ns Drop-reason: (acl-drop) Flow is denied by configured rule , Drop-location: frame 0x0000556e6808cac8 flow (NA)/NA asa# show access-list ACL-UNWANTED-COUNTRY access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any (hitcnt=1) 0x9b4d26ac

Remarque : si une solution RAVPN telle que Cisco Secure Client VPN est implémentée dans le pare-feu sécurisé, une tentative de connexion réelle au pare-feu sécurisé peut être effectuée pour confirmer que la liste de contrôle d'accès du plan de contrôle fonctionne comme prévu pour bloquer le trafic requis.

## Bogues associés

 ENH | Connexions AnyConnect Client basées sur la géolocalisation : ID de bogue Cisco CSCvs65322

### À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.