# セキュアなファイアウォール脅威対策とASAの ためのコントロールプレーンアクセスコントロ ールポリシーの設定

内容
<u>はじめに</u>
前提条件
要件
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設定</u>
<u>コンフィギュレーション</u>
<u>FMCによって管理されるFTDのコントロールプレーンACLの設定</u>
<u>FDMによって管理されるFTDのコントロールプレーンACLの設定</u>
<u>CLIを使用したASAのコントロールプレーンACLの設定</u>
<u>「shun」コマンドを使用してセキュアファイアウォールの攻撃をブロックする代替設定</u>
関連バグ

# はじめに

このドキュメントでは、セキュアファイアウォール脅威対策および適応型セキュリティアプライ アンス(ASA)のコントロールプレーンアクセスルールを設定するプロセス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。

- セキュアファイアウォール脅威対策(FTD)
- Secure Firewall Device Manager(FDM)
- ・ セキュアファイアウォール管理センター(FMC)
- セキュアなファイアウォールASA
- Access Control List (ACL; アクセス コントロール リスト)
- FlexConfig

使用するコンポーネント

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

- Secure Firewall Threat Defense  $\mathcal{N} = \mathcal{V}7.2.5$
- Secure Firewall Manager Centerバージョン7.2.5
- Secure Firewall Device Managerバージョン7.2.5
- ・ セキュアファイアウォールASAバージョン9.18.3

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

# 背景説明

通常、トラフィックはファイアウォールを通過し、データインターフェイス間でルーティングさ れます。状況によっては、セキュアなファイアウォール宛てのトラフィックを拒否することが有 益です。シスコのセキュアファイアウォールでは、コントロールプレーンアクセスコントロール リスト(ACL)を使用して、「to-the-box」トラフィックを制限できます。コントロールプレーン ACLが役立つ例としては、セキュアファイアウォールへのVPN(サイト間またはリモートアクセ スVPN)トンネルを確立できるピアを制御する場合があります。

ファイアウォールの「through-the-box」トラフィックの保護

トラフィックは通常、1つのインターフェイス(インバウンド)から別のインターフェイス(アウ トバウンド)にファイアウォールを通過します。これは「through-the-box」トラフィックと呼ば れ、アクセスコントロールポリシー(ACP)とプレフィルタルールの両方で管理されます。



画像 1.through-the-boxトラフィックの例

ファイアウォールの「to-the-box」トラフィックの保護

トラフィックがFTDインターフェイス(サイト間またはリモートアクセスVPN)に直接送信され る別のケースもあります。これは「to-the-box」トラフィックと呼ばれ、その特定のインターフェ イスのコントロールプレーンによって管理されます。



画像 2.To-the-boxトラフィックの例

#### コントロールプレーンACLに関する重要な考慮事項

- FMC/FTDバージョン7.0以降では、ASAで使用されるのと同じコマンド構文を使用して、 FlexConfigを使用してコントロールプレーンACLを設定する必要があります。
- キーワードcontrol-planeがaccess-group設定に追加され、セキュアなファイアウォールイン ターフェイスに対してトラフィックを「強制」します。コマンドにコントロールプレーンワ ードが追加されないと、ACLはセキュアファイアウォールを「通過する」トラフィックを制 限します。
- コントロールプレーンACLは、セキュアなファイアウォールインターフェイスへのSSH、 ICMP、またはTELNET着信を制限しません。これらはプラットフォーム設定ポリシーに従って処理(許可/拒否)され、より高い優先順位を持ちます。
- コントロールプレーンACLはトラフィックをセキュアファイアウォール自体に「制限」しますが、FTDのアクセスコントロールポリシーまたはASAの通常のACLはセキュアファイアウォールを「通過」するトラフィックを制御します。
- 通常のACLとは異なり、ACLの最後には暗黙の「deny」は存在しません。
- このドキュメントの作成時点では、FTDの位置情報機能を使用してFTDへのアクセスを制限 することはできません。

# 設定

次の例では、特定の国からのIPアドレスのセットが、FTD RAVPNへのログインを試みることに より、VPNへのブルートフォースを試みます。これらのVPNの総当たり攻撃からFTDを保護する 最良のオプションは、外部FTDインターフェイスへの接続をブロックするようにコントロールプ レーンACLを設定することです。

コンフィギュレーション

FMCによって管理されるFTDのコントロールプレーンACLの設定

外部FTDインターフェイスへの着信VPNブルートフォース攻撃をブロックするようにコントロー ルプレーンACLを設定するには、FMCで次の手順を実行する必要があります。 ステップ1:HTTPS経由でFMCグラフィックユーザインターフェイス(GUI)を開き、クレデンシャルでログインします。



画像 3.FMCログインページ

ステップ2:拡張ACLを作成する必要があります。このためには、「オブジェクト」>「オブジェ クト管理」に移動します。

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy Q 🤞	📍 🌣 🕜 adm	in ▼ death SECURE
Summary Dashboard (mitch databased)					Object N Intrusion	Management NRules				Reporting
Network × Threats Intrusion Events	Status	Geolocation	QoS					Show the Last	1 hour	• II
Unique Applications over Time		-× •	Top Web App	lications Seen				Top Client Applications Seen		
No Data Last updated 2 minutes ago				utes ago	No Data			N Last updated 2 minutes ago	No Data	
Traffic by Application Risk		-× 🕨	Top Server Ap	plications See	n		- ×	Top Operating Systems Seer		– ×

図 4.オブジェクト管理

ステップ 2.1:左側のパネルから、Access List > Extendedの順に移動して、拡張ACLを作成します。

Firewall Managemen	t Center <sub>Overview</sub>	Analysis	Policies Devices	Objects	Integration	Depl	loy Q <mark>6</mark> 🌣	admin
AAA Server     Access List     Extended     Standard	Network A network object represer network discovery rules, e	its one or more IP a vent searches, repo	ddresses. Network objec rts, and so on.	ts are used in v	arious places, inclu	Add Network	C Filt     C Filt     She etwork variables, intru	er ww Unused Objects sion rules, identity rules,
> Address Pools	Name				Valu	Je	Туре	Override
Application Filters AS Path	any				0.0. ::/0	.0.0/0	Group	Q ≣ ₿
Cipher Suite List	any-ipv4				0.0	.0.0/0	Network	ୟ ≣ #
> Community List	any-ipv6				::/0		Host	Q ≣ #
Distinguished Name DNS Server Group	IPv4-Benchmark-Tests				198	8.18.0.0/15	Network	Q ≣ 88
> External Attributes	IPv4-Link-Local				169	9.254.0.0/16	Network	ୟ 🗑 👪
File List	IPv4-Multicast				224	1.0.0.0/4	Network	Q ≣ ₿
Geolocation	IPv4-Private-10.0.0.0-8				10.	0.0.0/8	Network	Q ≣ 8
Interface	IPv4-Private-172.16.0.0-1	2			172	2.16.0.0/12	Network	Q ≣ ₿
Key Chain	IPv4-Private-192.168.0.0-	16			192	2.168.0.0/16	Network	Q ≣ ₿
> PKI	IPv4-Private-All-RFC1918				10. 172 192	0.0.0/8 2.16.0.0/12 2.168.0.0/16	Group	ର ≣ ଲ
Port						Displayir	ng 1 - 14 of 14 rows	< Page 1 of 1 > > C

図 5.拡張ACLメニュー

# ステップ 2.2 : 次に、Add Extended Access Listを選択します。

Firewall Managemen	t Center <sub>ove</sub>	rview Analysis	Policies	Devices	Objects	Integration	Deploy	۹ 🕯	₽ \$ (	🗿 admin 🕶 🛛	cisco SECURE
> AAA Server	Extended						Add Extended Acce	ss List	् Filter		
Access List     Extended	An access list object traffic based on sour	t, also known as an ac rce and destination ad	cess control lis dress and ports	at (ACL), selec s. Supports IP	ts the traffic to v4 and IPv6 ad	which a service will apply. Si dresses. You use these object	tandard-Identifies traffic t cts when configuring parti	based on c	destination ures, such	address only. as route maps	Identifies
Standard											
> Address Pools	Name						Value			Override	
Application Filters AS Path											
Cipher Suite List											
> Community List											
> Distinguished Name											
DNS Server Group											
> External Attributes											
File List											
> FlexConfig											
Geolocation											
Interface											
Key Chain											
Network											
> ркі											
Policy List											
Port							N	o data to d	fisplay I<	< Page 1	of1>>C
> Prefix List											

図 6.拡張ACLの追加

ステップ 2.3:拡張ACLの名前を入力し、Addボタンをクリックしてアクセスコントロールエント リ(ACE)を作成します。

Firewall Mana Objects / Object Ma	agement Ce	nter	Overview	Analysis Policies	Devices Obj	ects Integration		Deploy Q	e o	admin 🔻	cisco SECURE
> AAA Server	New Exter	nded Acc	cess List Obj	ect							
Extended	Name ACL-UNW/	ANTED-CO	UNTRY							dress only. oute maps	Identifies 3.
> Address Pools Application Filters	Entries (0)								_	Override	
AS Path Cipher Suite List	Sequence	Action	Source	Source Port	Destinati	on Destinati	ion Port Applicatio	n	Add		
Community List     Distinguished Name	No record										
DNS Server Group											
File List											
Geolocation	Allow Ov	errides									
Key Chain Network									Save		
> PKI Policy List											
Port								No data t	o display 🛛 🕹	< Page 1	of 1 > >  C

図 7.拡張ACLエントリ

ステップ 2.4: ACEのアクションをBlockに変更し、FTDに対して拒否する必要があるトラフィックと一致するように送信元ネットワークを追加し、宛先ネットワークをAnyのままにして、AddボタンをクリックしてACEエントリを完了します。

– この例では、設定されたACEエントリにより、192.168.1.0/24サブネットからのVPNブルートフ ォース攻撃がブロックされます。

Chiects /	Action: Block		cisco SECURE
> AAA Server <ul> <li>Access List</li> </ul>	Logging: Default •		Identifies
Extended Standard > Address Pools	Log Level: Informational		3.
Application Filt AS Path	300 Sec.		/ ₹ 8
Cipher Suite Lit	Available Networks C + Sou	urce Networks (1) Destination Networks (0)	
Distinguished N DNS Server Green	Q Search by name or value     15       any     Add to Source	22.168.1.0/24	
External Attribu     File List     ElexConfig	any-ipv4 Add to Destination any-ipv6 Up 1 Destination		
Geolocation	IPv4-Benchmark-Lests IPv4-Link-Local IPv4-Multicast		
Key Chain Network	IPv4-Private-10.0.0.0-8	nter an IP address Add Enter an IP address Add	
> PKI Policy List			
Port		Cancel	of 1 > >  C

図 8.拒否されたネットワーク

ステップ 2.5:さらにACEエントリを追加する必要がある場合は、もう一度Addボタンをクリック して、ステップ2.4を繰り返します。その後、Saveボタンをクリックして、ACLの設定を完了し ます。

Firewall Managemen Objects / Object Management	Edit Exten	nded Acc	ess List Object					0	cisco SECURE	
> AAA Server ~ Access List	Name ACL-UNW	ANTED-CC	PUNTRY							
Extended	Entries (1)	Entries (1)								
Standard								Add		
> Address Pools										
Application Filters	Sequence	Action	Source	Source Port	Destination	Destination Port	Application		2 E M	
AS Path	1	Block	192.168.1.0/24					11	<b>00</b>	
Cipher Suite List										
> Community List										
> Distinguished Name										
DNS Server Group										
> External Attributes										
File List	Allow Ov	verrides								
> FlexConfig										
Geolocation								Saus		
Interface								Save		
Key Chain										
Network										
> ркі										
Policy List										
Port							Displaying 1 - 1 of 1 rows	K < Page 1	of 1 > >  C	
> Prefix List										

#### 図 9.完成した拡張ACLエントリ

ステップ 3:次に、コントロールプレーンACLを外部FTDインターフェイスに適用するように Flex-Configオブジェクトを設定する必要があります。このためには、左側のパネルに移動し、オ プションFlexConfig > FlexConfig Objectを選択します。

Cipects / Object Management	t Center c	Overview Analys	sis Policies	Devices	Objects	Integration	Deploy	۹ 🧬	🗘 🕜 ad	imin 🕶 🏻	cisco SECURE
> AAA Server	Extended						Add Extended Acc	ess List	Filter		
✓ Access List											
Extended	An access list obj traffic based on se	ect, also known as a ource and destination	n access control I n address and por	ist (ACL), selec ts. Supports IP	ts the traffic to v4 and IPv6 ac	which a service will apply. Idresses. You use these ob	Standard-Identifies traffic piects when configuring part	based on dest icular features	ination addr	ess only. I ute maps.	dentifies
Standard			rodonooc ana por	an ooppond n			Joons mineri se mga mg pan		,	are maps.	
> Address Pools	Name						Value			Override	
Application Filters	ACL-UNWANTED	-COUNTRY									1 1 8
AS Path											
Cipher Suite List											
> Community List											
> Distinguished Name											
DNS Server Group											
> External Attributes											
File List											
✓ FlexConfig											
FlexConfig Object											
Text Object											
Geolocation											
Interface											
Key Chain											
Network											
> ркі							Displayir	g 1 - 1 of 1 rov	vs I< < Pa	ige 1	of 1 > >  C
Policy Liet											

図 10.FlexConfigオブジェクトメニュー

ステップ 3.1 : [FlexConfigオブジェクトの追加]をクリックします。

Firewall Management	Center Overview Analysis Policies Devices Obj	ects Integration C	eploy Q 🤩 🌣 🕜 admin 🕶 🖓 thether SECUR	RE
AAA Server     Access List     Extended     Standard	FlexConfig Object FlexConfig Object include device configuration commands, variables, and scrip	Add Flext	Q. Filter	
> Address Pools	Name	Desc	ription	
Application Filters AS Path	Default_DNS_Configure	Con	igure Default DNS with the help of TextObj 🖣 🛱 ର୍ 🗑	
Cipher Suite List	Default_Inspection_Protocol_Disable	Disa	ble Default Inspection. 📲 Q 🚆	
> Community List	Default_Inspection_Protocol_Enable	Enab	le Default Inspection. 📲 Q 🚆	
Distinguished Name     DNS Server Group	DHCPv6_Prefix_Delegation_Configure	Cont	igure one outside (PD client) and one insid 🛛 🖷 Q  🗑	
> External Attributes	DHCPv6_Prefix_Delegation_UnConfigure	Rem	ove configuration of one outside (PD client 🛚 🖷 Q 🗎	
File List	DNS_Configure	Con	igure DNS with the help of TextObjects dn 📲 🍳 🗎	
<ul> <li>FlexConfig</li> <li>FlexConfig Object</li> </ul>	DNS_UnConfigure	Rem	ove the DNS configurations. ${\bf F}_{\rm III}$ Q, ${\bf C}_{\rm IIII}$	
Text Object	Eigrp_Configure	Con	lgures eigrp. 1. Configures next hop. 2. co 📲 🭳 🗎	
Geolocation	Eigrp_Interface_Configure	Conl	igures interface parameters for eigrp. 1. C 📲 오 冒	
Interface Key Chain	Eigrp_UnConfigure	Cies	rs eigrp configuration for an AS 📲 ର୍ 📄	
Network	Eigrp_Unconfigure_All	Clea	rs eigrp configuration. 🖬 Q 🗎	
> ркі		Disp	aying 1 - 20 of 48 rows I< < Page 1 of 3 > >  C	*

図 11.Flexconfigオブジェクトの追加

ステップ 3.2 : FlexConfigオブジェクトの名前を追加し、ACLポリシーオブジェクトを挿入します。このためには、Insert > Insert Policy Object > Extended ACL Objectの順に選択します。

Firewall Manageme	Name:							
	OBJ-FC-CONTROL-PLAN	E					admin v ∣	CISCO SECURI
> AAA Server	Description:						Filter	
Extended	Copy-pasting any rich	text might introduce line break	s while generating CLI	. Please verify the	CLI before deploy	ment.		
Standard	Insert v 🛤	Deployment: Once		Type:	Append	-		
> Address Pools	Insert Policy Object	Taxt Object			oppoint			
Application Filters	Insert System Variable >	Network					the help of TextObj	¶∎ Q 🗑
AS Path	Insert Secret Key	Security Zones						Faq ⊒
Cipher Suite List		Standard ACL Object						
> Community List		Extended ACL Object						<b>『</b> 월 Q
> Distinguished Name		Route Map					lient) and one insid	Pa Q 🗑
External Attributes							e outside (PD client	¶a q ≣
							of TextObjects dn	Pa Q 🗑
✓ FlexConfig	▼ Variables							Bo =
	Name	Dimension	Default Value	Property	Override	Description	Uns.	
Text Object				(Type:wame)			ires next hop. 2. co	¶∎ Q
Geolocation			No records to d	isplay			ters for eigrp. 1. C	<b>唱</b> Q 🗑
Interface							1 an AS	ELO =
Key Chain							ar an AS	- <b>U</b> ( )
Network								<b>₽</b> Q =
> ркі							* K < Page 1	of 3 > >  C
The second se							Save	

図 12.FlexConfigオブジェクト変数

ステップ 3.3: ACLオブジェクト変数の名前を追加してから、ステップ2.3で作成した拡張ACLを 選択します。その後、Saveボタンをクリックします。

Firewall Managemer	Name: OBJ-FC-CONTROL-PLANE		נוגנייט admin ד מוליגניי secure ליגניי
> AAA Server > Access List	Description:	Insert Extended Access List Object Variable	Filter
Extended Standard > Address Pools	Copy-pasting any rich	Variable Name: VAR-ACL-UNWANTED-COUNTRY	
Application Filters AS Path Cipher Suite List > Community List > Distinguished Name	acces-group	Description:         Available Objects C         Q. Search         B. CLOWWAPTED-COUNTRY	the help of TextObj Pa Q = Pa Q = Pa Q = stient) and one insid Pa Q =
DNS Server Group External Attributes File List FilexConfig		Add	e outside (PD client 🖥 Q 📄
FlexConfig Object Text Object	Name	ription	ions. 📲 Q 📄 res next hop. 2. co 📲 Q
Interface Key Chain		Cancel	iters for eigrp. 1. C № Q
> PKI			s I< < Page 1 of 3 > >  C

図 13.FlexConfigオブジェクト変数ACL割り当て

ステップ 3.4:次に、コントロールプレーンACLを外部インターフェイスのインバウンドとして 次のように設定します。

コマンドライン構文:

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

これは、次のコマンド例に変換されます。この例では、上記のステップ2.3で作成したACL変数「 VAR-ACL-UNWANTED-COUNTRY」を次のように使用しています。

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

FlexConfigオブジェクトウィンドウで設定する方法は次のとおりです。その後、Saveボタンを選択してFlexConfigオブジェクトを完了します。

Firewall Manageme	Name: OBJ-FC-CONTROL-PLANE						⊁ 🕜 admin <del>v</del>   🖞	sco SECURE
> AAA Server	Description:						Filter	
✓ Access List								
Extended	Copy-pasting any rich text might in	troduce line breaks wi	hile generating CLI. Pl	ease verify the	CLI before deployr	nent.		
Standard					A			
> Address Pools	Insert V 👪 Deploymen	Once		• Type:	Append	¥		
Application Filters	access-group \$VAR-ACL-UNWANTED-COUN	TRY in interface outside cor	ntrol-plane				the help of TextOhi	
AS Path								
Cipher Suite List								<b>팀</b> Q 📄
> Community List								<b>₽</b> q =
> Distinguished Name							Foot) and one insid	B o E
DNS Server Group							litent) and one insid	
> External Attributes							e outside (PD client	<b>唱</b> Q 🗑
							of TextObjects dn	<b>₽</b> _a ⊂ =
✓ FlexConfig	▼ Variables							
	Name	Dimension D	efault Value	Property	Override	Description	ions.	19 Q
Text Object		Dimension		(Type:Name)	overnue	beachpiton	ires next hop. 2. co	¶a Q 🗑
Geolocation	VAR-ACL-UNWANTED-COUNTRY	SINGLE A	ACL-UNWANTED	EXD_ACL:A	false		iters for eigro. 1. C	Fa α ⊒
Interface								
Key Chain							or an AS	¶∎ <
Network								<b>⊑</b> q =
> ркі							s IC < Page 1	of 3 > >  C
Policy List						Cancel Save		

図 14.Flexconfig Object completeコマンドライン

# ステップ 4 : FlexConfigオブジェクトの設定をFTDに適用する必要があります。そのためには、 Devices > FlexConfigの順に選択します。

Firewall Management	Center Overview Analysis Policies	Devices Objects	Integration	Deploy Q 🤩 🕂	🔅 🕜 admin 🕶 🏻 🖞	SECURE
AAA Server     Access List     Extended     Standard     Address Pools	FlexConfig Object FlexConfig Object include device configuration comma	Device Management Device Upgrade nd: NAT QoS Platform Settings	VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture	ilter	
Application Filters AS Path	Def	FlexConfig faul Certificates	Site to Site Monitoring		he help of TextObj	<b>₽</b> q
Cipher Suite List Community List	Default_Ir Default_I	spection_Protocol_Disable		Disable Default Inspection.		■  ■  ■
Distinguished Name     DNS Server Group     External Attributes	DHCPv6_1 DHCPv6_9	Prefix_Delegation_Configure		Configure one outside (PD o	client) and one insid e outside (PD client	⊑α      □
File List ✓ FlexConfig		DNS_Configure		Configure DNS with the help	p of TextObjects dn	<b>₽</b> _0 ⊂
FlexConfig Object Text Object		DNS_UnConfigure		Remove the DNS configurations. 📲 Q. Configures eigrp. 1. Configures next hop. 2. co., 🖷 Q.		
Geolocation Interface Key Chain	Eigr	p_Interface_Configure		Configures interface parame	aters for eigrp. 1. C or an AS	∎α () ■α
Network	Ei	grp_Unconfigure_All		Clears eigrp configuration. Displaying 1 - 20 of 49 row	s K < Page 1	¶∎ α, ີ of3 > >  C

図 15.FlexConfig Policyメニュー

ステップ 4.1:次に、FTD用に作成されたFlexConfigがない場合はNew Policyをクリックするか、 既存のFlexConfigポリシーを編集します。

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

図 16.FlexConfigポリシーの作成

ステップ 4.2:新しいFlexConfigポリシーの名前を追加し、作成したコントロールプレーンACLを 適用するFTDを選択します。

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	WE T
		cel Save

図 17.FlexConfigポリシーデバイスの割り当て

ステップ 4.3:左側のパネルで、上記のステップ3.2で作成したFlexConfigオブジェクトを検索し、ウィンドウの中央にある右矢印をクリックしてFlexConfigポリシーに追加します。その後、「Save」ボタンをクリックします。

Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Dej	oloy Q	\$ 🕜 admin 🕶	cisco SECURE
									w Config	e Cancel
									Policy A	Assignments (1)
	" Solooto	d Dropond F	lovConfigs							
Available FlexConfig	Selecte	a Prepena r	lexconligs							
X	# Nam	ne		ſ	Description					
	_									
V User Defined										
CONTROL-PLANE										
V System Defined										
Default_DNS_Configure										
Default_Inspection_Protocol_Disable										
Protocol_Enable	_ Selecte	d Append F	lexConfias							
The DHCPv6_Prefix_Delegation_Configure										
DHCPv6_Prefix_Delegation_UnConfigure	# Nam	ne		ſ	Description					
DNS_Configure	1 ОВЈ	-FC-CONTROL	-PLANE							۹ 🖥
DNS_UnConfigure	Ц —									
B Eigrp_Configure										
Bigrp_Interface_Configure										
" <sup>9</sup> Eigrp_Unconfigure_All										

- 図 18.FlexConfigポリシーオブジェクトの割り当て
- ステップ5:設定変更をFTDに展開するため、Deploy > Advanced Deployの順に移動します。

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q	🤗 🌣 (	🗿 admin 🕶	cisco SE	CURE
FLEXCONFIG-POLICY								Advanced [	Deploy De	eploy All	ncel
Enter Description						FTD-CONTROL-PLANE		Ready for De	ployment	é	
Available ElexConfig + ElexConfig Object	" Selecte	d Prepend F	lexConfigs								
	# Nan	ne			Description						
V User Defined											
BOBJ-FC-CONTROL-PLANE											
✓ System Defined											
" Default_DNS_Configure						1 de las la subistica for destament					
Default_Inspection_Protocol_Disable						I device is available for deployment				₽ +9	
Default_Inspection_Protocol_Enable	Selecte	d Append F	lexConfigs								
DHCPv6_Prefix_Delegation_Configure DHCPv6_Prefix_Delegation_LinConfigure	# Nan	ne			Description						
DNS_Configure	1 ОВЈ	-FC-CONTROL	-PLANE								۹.
DNS_UnConfigure											

図 19.FTDの高度な導入

ステップ 5.1:次に、FlexConfigポリシーを適用するFTDを選択します。すべてが正しい場合は、 「配置」をクリックします。

þ,	Firewall Management Center Deploy / Deployment	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🧳	🗘 🕜 adm	in ▼ <sup>shalla</sup> SECURE
1 device :	selected Search using device name, user name, ty	pe, group or statu	15								Deploy time:	Estimate Deploy
	Z Device	Modified by		Inspect Inte	erruption	Туре	Group	Last Deploy Time		Preview	Status	
~ .	FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12:0	05 PM	B	Ready for De	ployment
÷ •	<ul> <li>Flex Configuration</li> <li>Template Policy: FLEXCONFIG-POLICY</li> </ul>											
https://10.88.	.243.58:43013/ddd/#ContextExplorer											

図 20.FTD導入の検証

ステップ 5.2:その後、「配備の確認」ウィンドウが表示され、配備を追跡するためのコメント を追加して「配備」に進みます。

Firewall Management Center Deploy / Deployment					२. 🥙 🌣 🕜 admir	
1 device selected						
	Modified by					
V STD-CONTROL-PLANE	admin		Sep 5	5, 2023 12:05 PM	Ready for Depl	oyment
✓ Flex Configuration ✓ Flex Configuration ✓ Template Policy: FLEXCONFIG-POLICY		Deployment Confirmation	×			
		You have selected 1 device to deploy Deployment Notes:				
		You can optionally add notes about the configuration c	hanges			
			Cancel Deploy			

図 21.FTD導入に関するコメント

ステップ 5.3: FlexConfigの変更を導入するときに警告メッセージが表示される場合があります。 ポリシー設定が正しいことが完全に確認できている場合にのみ、Deployをクリックします。



図 22.FTD展開Flexconfigの警告

### ステップ 5.4: FTDのポリシー展開が正常に行われたことを確認します。

Firewall Management Center Deploy / Deployment	Overview Analysis	Policies Devices Objects Integ	ration Deploy Q	🤩 🌣 🕜 admin 🗸 🔤 🖏 SECURE
Q Search using device name, user name, typ	e, group or status			Deploy
Device	Modified by	Inspect Interruption Type Group	Last Deploy Time Preview	Status
V FTD-CONTROL-PLANE	admin	FTD	Sep 5, 2023 12:05 PM	Completed
V Flex Configuration     Template Policy: FLEXCONFIG-POLICY				

図 23.FTDの導入に成功

手順 6: FTD用に新しいコントロールプレーンACLを作成する場合、またはアクティブに使用されている既存のコントロールプレーンACLを編集する場合は、加えられた設定変更がFTDへの確 立済みの接続に適用されないことを強調することが重要です。したがって、FTDへのアクティブ な接続試行を手動でクリアする必要があります。そのためには、次のようにFTDのCLIに接続し、 アクティブな接続をクリアします。

特定のホストIPアドレスのアクティブな接続をクリアするには、次の手順を実行します。

サブネットネットワーク全体のアクティブな接続をクリアするには、次の手順を実行します。

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

特定の範囲のIPアドレスに対するアクティブな接続をクリアするには、次の手順を実行します。

> clear conn address 192.168.1.1-192.168.1.10 all

◆ 注: clear conn addressコマンドの最後にキーワード「all」を使用して、アクティブな VPN総当たり攻撃によるセキュアなファイアウォールへの接続試行を強制的にクリアすることを強く推奨します。これは主に、VPN総当たり攻撃の性質によって絶え間ない接続試行の 爆発が発生している場合に行われます。

FDMによって管理されるFTDのコントロールプレーンACLの設定

外部FTDインターフェイスへの着信VPNブルートフォース攻撃をブロックするようにコントロー ルプレーンACLを設定するためにFDMで実行する必要がある手順を次に示します。

ステップ1:HTTPS経由でFDM GUIを開き、クレデンシャルでログインします。



cisco SECURE

Cisco Secure Firewall Device Manager

Username	
Password	
	0
	LOG IN

© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. This product contains some software licensed under the "GNU Lesser General Public License, versions 2, 2, 1 and 3" provided with ABSOLITE!V No WARRANT! under the terms of "GNU Lesser General Public License, versions 2, 2, and version 3, 2, 1

### ステップ2:オブジェクトネットワークを作成する必要があります。この場合は、次のオブジェ クトに移動します。

Firewall Device Mana	iger Monitoring	Policies Objects D	Device: firepower	> 🖄 Ø ?	admin Administrator					
Mod Cisc	el o Firepower Threat Defen:	Software Vise for VMwa 7.2.5-208 3	DB Intrusion Rule Up 53.0 20220511-1540	date Cloud Services High /	Availability  CONFIGURE CONFIGURE					
0/1 Cisco Firepower Threat Defense for VMware   Cisco Firepower Threat Defense for VMware  Cisco Firepower Threat Defense for VMware  ()/0 0/1  ()/1 ()/1 ()/1 ()/1 ()/1 ()/1 ()/1 (										
			0/0							
Interfaces Connected Enabled 3 of 3 View All Interfaces	>	Routing There are no static routes y View Configuration	et >	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service					

## ステップ 2.1:左側のパネルからNetworksを選択し、「+」ボタンをクリックして新しいネットワ ークオブジェクトを作成します。

Firewall Device Manager	Monitoring Policies Objects Device: firepow	er 🖒 🖄 🗐 ? : admin dministrator	SECURE
Object Types ←	Network Objects and Groups		
C Networks	6 objects	<b>Y</b> Filter	+
S Ports		Preset filters: System defined, User defined	
8 Security Zones	H NAME	TYPE VALUE	ACTIONS
🐬 Application Filters	1 IPv4-Private-10.0.0-8	NETWORK 10.0.0/8	
A URLs	2 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0/12	
9 Coolections	3 IPv4-Private-192.168.0.0-16	NETWORK 192.168.0.0/16	
V Geolocations	4 any-ipv4	NETWORK 0.0.0.0/0	
Syslog Servers	5 any-ipv6	NETWORK ::/0	
IKE Policies	6 IPv4-Private-All-RFC1918	Group IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private- 192.168.0.0-16	
🛖 IPSec Proposals			
Secure Client Profiles			
Sa Identity Sources			
👤 Users			
🙊 Certificates			
Secret Kevs			

図 26.オブジェクトの作成

ステップ 2.2:ネットワークオブジェクトの名前を追加し、オブジェクトのネットワークタイプ を選択し、FTDに対して拒否する必要があるトラフィックに一致するIPアドレス、ネットワーク アドレス、またはIPの範囲を追加します。次に、[OK]ボタンをクリックしてオブジェクトネット ワークを完了します。

– この例で設定するオブジェクトネットワークは、192.168.1.0/24サブネットからのVPNブルート フォース攻撃をブロックすることを目的としています。

Firewall Device Manager	Monitoring Polici	work Object		admin Administrator
Object Types ←	Network Obje			
C Networks	6 objects OBJ-NET-	UNWANTED-COUNTRY		+
S Ports	Description		defined. Us	er defined
8 Security Zones	NAME DOUGHINION		170.10	ACTIONS
P Application Filters	1 IPv4-Private-Al		.e=172.16.	0.0-12, IPv4-Private-
🖉 URLs	2 IPv4-Private-1( Type	0		
Geolocations	3 IPv4-Private-1: ONetwork	Host FQDN Range		
Syslog Servers	4 IPv4-Private-11 Network	0/24		
🔏 IKE Policies	5 any-ipv4 e.g. 192.168.2.	0/24 or 2001:DB8:0:CD30::/60	_	
🖷 IPSec Proposals	6 any-ipv6		_	
Secure Client Profiles		CANC	ELOK	
Sa Identity Sources				
1 Users				
🙊 Certificates				
🔒 Secret Keys				

図 27.ネットワークオブジェクトの追加

ステップ3:次に、拡張ACLを作成する必要があります。それには、トップメニューのDeviceタブに移動します。

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	
8 Security Zones	# NAME	TYPE VALUE	ACTIONS
🐬 Application Filters	1 IPv4-Private-All-RFC1918	Group IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private- 192.168.0.0-16	
C <sup>2</sup> URLs	2 IPv4-Private-10.0.0.0-8	NETWORK 10.0.0/8	
Geolocations	3 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0/12	
Syslog Servers	4 IPv4-Private-192.168.0.0-16	NETWORK 192.168.0.0/16	
🔏 IKE Policies	5 any-ipv4	NETWORK 0.0.0.0/0	
🛖 IPSec Proposals	6 any-lpv6	NETWORK ::/0	
Secure Client Profiles	7 OBJ-NET-UNWANTED-COUNTRY	NETWORK 192.168.1.0/24	
Secure Client Profiles			
Identity Sources			
1 Users			
🙊 Certificates			
Secret Kevs			

図 28.デバイス設定ページ

ステップ 3.1:下にスクロールして、次のようにAdvanced Configurationの画面でView Configurationを選択します。

Firewall Device Manager	Policies Objects Device: firepower	> 🚔 @ ?	admin Administrator
	0/0 		
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 Service
Smart License Evaluation expires in 89 days Tier: Not selected (Threat Defense Virtual - Variable) View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Management Interface Hostname Time Services See more
Site-to-Site VPN There are no connections yet View Configuration	Remote Access VPN Requires RA VPN license No connections   1 Group Policy Configure	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	Device Administration Audit Events, Deployment History, Download Configuration View Configuration

図 29.FDMの詳細設定

ステップ 3.2:次に、左側のパネルからSmart CLI > Objectsに移動し、CREATE SMART CLI OBJECTをクリックします。

Firewall Device Manage	er Monitoring	Ø Policies	Objects	Device: firepower	_	۵.	2	e admin • Administra	tor
Advanced ← Configuration	Device Summ Objects	lary							
Smart CLI									+
Objects		NAME		TYPE	DESCRIPTION			ACTIONS	
FlexConfig				S	There are no Smart Start by creating the fir	CLI objects yet. st Smart CLI obj	ect.		
FlexConfig Objects					CREATE SMART	CLI OBJECT	]		

図 30.スマートCLIオブジェクト

ステップ 3.3:作成する拡張ACLの名前を追加し、CLIテンプレートのドロップダウンメニューか らExtended Access Listを選択し、上記のステップ2.2で作成したネットワークオブジェクトを使 用して必要なACEを設定し、OKボタンをクリックしてACLを完成させます。

Firewall Devic	Edit Smort OLL Object	admin titulit SECURE
Advanced Configuration	Eait Smart CLI Object	Description
Smart CLI	ACL-UNWANTED-COUNTRY	
Objects	Extended Access List ~	ACTIONS
FlexConfig	Template	Show disabled
FlexConfig Objects	1       access-list ACL-UNAWATED-COUNTRY extended         2       configure access-list-entry deny ∨         3       deny network source [00].HET/UNAMITED-COUNTRY ∨ ] desti         4       configure deny port any ∨         5       deny port source NY destination NYY         6       configure logging default ∨         7       default log set log-level INFORMATIONAL log-interval	nation [ any-1004 × ~ ] L 300 CANCEL OK

図 31.拡張ACLの作成

◆ 注:ACLにさらにACEを追加する必要がある場合は、現在のACEの左側にマウスを置くと、 クリック可能な3つのドットが表示されます。それらをクリックし、Duplicateを選択して ACEを追加します。

ステップ 4:次に、FlexConfigオブジェクトを作成する必要があります。これには、左側のパネ ルに移動し、FlexConfig > FlexConfig Objectsを選択し、CREATE FLEXCONFIG OBJECTをクリ ックします。

Firewall Device Manager	Monitoring Policies Objects	Device: firepower	C C C C C C C C C C C C C C C C C C C	cisco SECURE
Advanced ← Configuration	Device Summary FlexConfig Objects			
Smart CLI			<b>T</b> Filter	+
Objects	# NAME	DESCRIPTION	ACTIONS	
FlexConfig		There are no FlexCor Start by creating the first	nfig objects yet. st FlexConfig object.	
FlexConfig Objects FlexConfig Policy		CREATE FLEXCON	NFIG OBJECT	

図 32.FlexConfigオブジェクト

ステップ 4.1 : コントロールプレーンACLを作成し、外部インターフェイスのインバウンドとして設定するには、FlexConfigオブジェクトの名前を次のように追加します。

### コマンドライン構文:

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

これは、次のコマンド例に変換されます。この例では、上記のステップ3.3で作成した拡張ACL「ACL-UNWANTED-COUNTRY」を次のように使用しています。

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

FlexConfigオブジェクトウィンドウでこのように設定する必要があります。その後、OKボタンを 選択してFlexConfigオブジェクトを完了します。

Firewall Device Ma	nager Monitoring	Create ElexConfig Object			admin Administrator Cisco SECURE
Advanced ← Configuration	Device Su FlexCo	Name			
Smart CLI		OBJ-FC-CONTROL-PLANE			+
Objects	i i i			li.	
FlexConfig		Variables There are no variables yet. Start with adding a new variable.			
FlexConfig Policy		+ ADD VARIABLE			
		Template	<pre>C Expand Y in interface outside control-plane</pre>	🗘 Reset	
		Negate Template 🛕 no access-group ACL-UMANITED-COUR	C Expand NTRY in interface outside control-plane	🗘 Reset	
			CANCEL	ок	

図 33.FlexConfigオブジェクトの作成

ステップ 5: FlexConfigポリシーの作成に進み、Flexconfig > FlexConfig Policyに移動し、「+」 ボタンをクリックして、上記のステップ4.1で作成したFlexConfigオブジェクトを選択します。

Firewall Device Manaç	Jer Monitoring Policies Objects Device: firepower	▷ (admin admin admin administration)	→ viluili SECURE
Advanced ← Configuration	Device Summary FlexConfig Policy		
Smart CLI Objects	Group List	Preview There is nothing to preview yet.	<ul> <li>Expand</li> </ul>
FlexConfig FlexConfig Objects FlexConfig Policy	Create.new.ElexConfig.Object CANCEL OK		
	SAVE		

図 34.FlexConfigポリシー

ステップ 5.1 : FlexConfigプレビューに、作成されたコントロールプレーンACLの正しい設定が表示されていることを確認し、Saveボタンをクリックします。

Firewall Device Manager	Monitoring Policies Objects Device: firepower	Similar Secure
Advanced ← Configuration	Device Summary FlexConfig Policy	
Smart CLI	Group List	Preview  +> Expand
FlexConfig	0BJ-FC-CONTROL-PLANE	control-plane
FlexConfig Objects		
FlexConfig Policy		
	SAVE	

図 35.FlexConfigポリシープレビュー

手順 6: VPN総当たり攻撃から保護したいFTDに設定変更を展開します。それには、トップメニ ューのDeploymentボタンをクリックし、展開する設定変更が正しいことを確認して、DEPLOY NOWをクリックします。



図 36.保留中の展開

### ステップ 6.1:ポリシーの展開が正常に行われたことを検証します。

Firewall Device Mar	ager 🗰 🐨 🏪 🧰 🔿 🔿	admin istrator
Advanced Configuration Smart CLI Objects	Pending Changes	
FlexConfig FlexConfig Objects FlexConfig Policy	Last successful deployment was on 05 Sep 2023 11:09 AM. You can see what was deployed in previous jobs in the Deployment Histor	in interface outside X
	SAVE	

図 37.展開が成功しました

手順 7: FTD用に新しいコントロールプレーンACLを作成する場合、またはアクティブに使用されている既存のコントロールプレーンACLを編集する場合は、加えられた設定変更がFTDへの確 立済みの接続に適用されないことを強調することが重要です。したがって、FTDへのアクティブ な接続試行を手動でクリアする必要があります。そのためには、次のようにFTDのCLIに接続し、 アクティブな接続をクリアします。

特定のホストIPアドレスのアクティブな接続をクリアするには、次の手順を実行します。

サブネットネットワーク全体のアクティブな接続をクリアするには、次の手順を実行します。

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

特定の範囲のIPアドレスに対するアクティブな接続をクリアするには、次の手順を実行します。

> clear conn address 192.168.1.1-192.168.1.10 all

◆ 注: clear conn addressコマンドの最後にキーワード「all」を使用して、アクティブな VPN総当たり攻撃によるセキュアなファイアウォールへの接続試行を強制的にクリアすることを強く推奨します。これは主に、VPN総当たり攻撃の性質によって絶え間ない接続試行の 爆発が発生している場合に行われます。

CLIを使用したASAのコントロールプレーンACLの設定

外部インターフェイスへの着信VPNブルートフォース攻撃をブロックするようにコントロールプ レーンACLを設定するには、ASA CLIで次の手順を実行する必要があります。

ステップ 1:CLIを介してセキュアファイアウォールASAにログインし、次のように「configure terminal」にアクセスします。

asa# configure terminal

ステップ2:次のコマンドを使用して、ASAに対してブロックする必要があるトラフィックのホ ストIPアドレスまたはネットワークアドレスをブロックするように拡張ACLを設定します。

– この例では、「ACL-UNWANTED-COUNTRY」という名前の新しいACLを作成し、設定した ACEエントリによって、192.168.1.0/24サブネットからのVPNブルートフォース攻撃をブロック します。

asa(config)# access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

ステップ 3:次のaccess-groupコマンドを使用して、「ACL-UNWANTED-COUNTRY」ACLを外 部ASAインターフェイスのコントロールプレーンACLとして設定します。

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

ステップ 4:新しいコントロールプレーンACLを作成する場合、またはアクティブに使用されて いる既存のコントロールプレーンACLを編集する場合は、加えられた設定変更がASAへの既存の 接続に適用されないことを強調することが重要です。そのため、ASAへのアクティブな接続試行 を手動でクリアする必要があります。このため、次のようにアクティブな接続をクリアします。

特定のホストIPアドレスのアクティブな接続をクリアするには、次の手順を実行します。

asa# clear conn address 192.168.1.10 all

サブネットネットワーク全体のアクティブな接続をクリアするには、次の手順を実行します。

asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all

特定の範囲のIPアドレスに対するアクティブな接続をクリアするには、次の手順を実行します。

asa# clear conn address 192.168.1.1-192.168.1.10 all

◆ 注: clear conn addressコマンドの最後にキーワード「all」を使用して、アクティブな VPN総当たり攻撃によるセキュアなファイアウォールへの接続試行を強制的にクリアするこ とを強く推奨します。これは主に、VPN総当たり攻撃の性質によって絶え間ない接続試行の 爆発が発生している場合に行われます。

「shun」コマンドを使用してセキュアファイアウォールの攻撃をブロックする代替設定

セキュアなファイアウォールに対する攻撃を即時にブロックするオプションがある場合は、「 shun」コマンドを使用できます。huncommandコマンドを使用すると、攻撃ホストからの接続を ブロックできます。

- IPアドレスを回避すると、送信元IPアドレスからの以降のすべての接続はドロップされ、ブロッ

キング機能が手動で削除されるまでログに記録されます。

- huncommandのblocking関数は、指定されたホストアドレスとの接続が現在アクティブであるか どうかにかかわらず適用されます。

- 宛先アドレス、送信元ポートと宛先ポート、およびプロトコルを指定した場合、一致する接続 をドロップし、送信元IPからの以降のすべての接続を回避します

アドレス。これらの特定の接続パラメータに一致するものだけでなく、将来のすべての接続が 排除されます。

-送信元IPアドレスごとにonescuncommandのみを指定できます。

- hushuncommandは攻撃を動的にブロックするために使用されるため、脅威防御デバイスの設定 には表示されません。

– インターフェイス設定が削除されると、そのインターフェイスに接続されているすべての shunも削除されます。

- Shunコマンド構文:

shun source\_ip [ dest\_ip source\_port dest\_port [ protocol]] [ vlan vlan\_id]

– 回避を無効にするには、このコマンドのno形式を使用します。

no shun source\_ip [ vlan vlan\_id]

ホストIPアドレスを回避するには、セキュアファイアウォールで次の手順を実行します。 この例 では、「shun」コマンドを使用して、送信元IPアドレス192.168.1.10からのVPNブルートフォー スアタックをブロックしています。

FTDの設定例

ステップ1:CLIを使用してFTDにログインし、次のようにshunコマンドを適用します。

<#root>

>

shun 192.168.1.10

Shun 192.168.1.10 added in context: single\_vf

ステップ2:次のshowコマンドを使用して、FTD内の排除IPアドレスを確認し、IPアドレスごとの排除ヒットカウントをモニタできます。

#### <#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)

#### ASAの設定例

ステップ1:CLIを使用してASAにログインし、次のようにshunコマンドを適用します。

#### <#root>

#### asa#

shun 192.168.1.10

Shun 192.168.1.10 added in context: single\_vf

Shun 192.168.1.10 successful

ステップ2:次のshowコマンドを使用して、ASAの排除IPアドレスを確認し、IPアドレスごとの 排除ヒットカウントをモニタできます。

<#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
mgmt=OFF, cnt=0

Shun 192.168.1.10 cnt=0, time=(0:01:39)

◆ 注: secure firewall shunコマンドの詳細については、『<u>Cisco Secure Firewall Threat</u> <u>Defense Command Reference</u>』を参照してください

# 確認

コントロールプレーンACL設定がセキュアファイアウォールに対して設定されていることを確認 するには、次の手順を実行します。

ステップ1:CLIを介してセキュアファイアウォールにログインし、次のコマンドを実行して、コントロールプレーンACL設定が適用されていることを確認します。

FMCによって管理されるFTDの出力例を次に示します。

#### <#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

### FDMによって管理されるFTDの出力例を次に示します:

#### <#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

#### ASAの出力例:

<#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

ステップ2: コントロールプレーンACLが必要なトラフィックをブロックしていることを確認す るには、packet-tracerコマンドを使用して、セキュアファイアウォールの外部インターフェイス への着信TCP 443接続をシミュレートします。次に、show access-list <acl-name>コマンドを使 用します。VPNのブルートフォース接続がコントロールプレーンACLによってブロックされるた びに、ACLのヒットカウントが増加します。

- この例では、packet-tracerコマンドにより、ホスト192.168.1.10から送信され、セキュアファイ アウォールの外部IPアドレスに宛てられた着信TCP 443接続がシミュレートされます。「packettracer」の出力はトラフィックがドロップされていることを示し、「show access-list」の出力は コントロールプレーンACLのヒットカウントの増分を示します。

FTDの出力例

<#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

#### ASAの出力例

#### <#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



# 関連バグ

・ ENH | 位置情報ベースのAnyConnectクライアント接続: Cisco Bug ID CSCvs65322

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。