Configure Control Plane Access Control Policies for Secure Firewall Threat Defense and ASA

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
Configurations
Configure a control-plane ACL for FTD managed by FMC
Configure a control-plane ACL for FTD managed by FDM
Configure a control-plane ACL for ASA using CLI
Alternative configuration to block attacks for secure firewall using the 'shun' Command
Verify
Related Bugs

Introduction

This document describes the process to configure control plane access rules for Secure Firewall Threat Defense and Adaptive Security Appliance (ASA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Firewall Threat Defense (FTD)
- Secure Firewall Device Manager (FDM)
- Secure Firewall Management Center (FMC)
- Secure Firewall ASA
- Access Control List (ACL)
- FlexConfig

Components Used

The information in this document is based on these software and hardware versions:

- Secure Firewall Threat Defense version 7.2.5
- Secure Firewall Manager Center version 7.2.5
- Secure Firewall Device Manager version 7.2.5
- Secure Firewall 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The traffic usually traverses a firewall and is routed between data interfaces; in some circumstances, it is beneficial to deny traffic destined 'to' the secure firewall. The Cisco secure firewall can use a control-plane access control list (ACL) to restrict 'to-the-box' traffic. An example of when a control-plane ACL can be useful would be to control which peers can establish a VPN (Site-to-Site or Remote Access VPN) tunnel to the secure firewall.

Secure Firewall 'through-the-box' traffic

Traffic normally traverses firewalls from one interface (inbound) to another interface (outbound), this is known as 'through-the-box' traffic and is managed by both, the Access Control Policies (ACP) and the Pre-filter rules.



Image 1. Through-the-box traffic example

Secure Firewall 'to-the-box' traffic

There are other cases in which traffic is directly destined to an FTD interface (Site-to-Site or Remote Access VPN), this is known as 'to-the-box' traffic and is managed by the control-plane of that specific interface.



Image 2. To-the-box traffic example

Important Considerations Regarding Contol Plane ACLs

- As of FMC/FTD version 7.0, a control plane ACL must be configured using FlexConfig, using the same command syntax used on the ASA.
- The keyword control-plane is appended to the access-group configuration, which enforces traffic 'to' the secure firewall interface. Without the control-plane word appended to the command, the ACL

would restrict traffic 'through' the secure firewall.

- A control-plane ACL does not restrict SSH, ICMP or TELNET inbound to a secure firewall interface. These are processed (permitted/denied) according to the Platform Settings Policies and have a higher precedence.
- A control-plane ACL restricts traffic 'to' the secure firewall itself, whereas the Access Control Policy for the FTD or the normal ACLs for the ASA, controls traffic 'through' the secure firewall.
- Unlike a normal ACL, there is not an implicit 'deny' at the end of the ACL.
- The object-group search (OGS) feature does not work over control-plane ACLs, <u>CSCwi58818</u>.
- At the time of this document being created, the FTD Geolocation feature cannot be used to restrict access 'to' the FTD.

Configure

In the next example, a set of IP addresses from a certain country tries to VPN brute force into the network by attempting to log in to the FTD RAVPN. The best option to protect the FTD against these VPN brute force attacks is to configure a control plane ACL to block these connections to the outside FTD interface.

Configurations

Configure a control-plane ACL for FTD managed by FMC

This is the procedure you need to follow in an FMC to configure a control plane ACL to block incoming VPN brute force attacks to the outside FTD interface:

Step 1. Open the FMC Graphic User Interface (GUI) via HTTPS and Log in with your credentials.



Image 3. FMC Log In page



Firewall Management Center Overview / Dashboards / Dashboard	Overview /	Analysis Policie	s Devices	Objects	Integration		Deploy Q 🌔	🦻 🌣 🕜 admin -	cisco SECURE
Summary Dashboard (switch disabloard) Provides a summary of activity on the appliance				Object M Intrusion	fanagement Rules				Reporting
Network × Threats Intrusion Events	Status Geol	ocation QoS					Show the Last	1 hour	• 11
Unique Applications over Time	- ×	F Top Web	pplications See				Top Client Applications See	n	
No Data Last updated 2 minutes ago				No Data				No Data	
Traffic by Application Risk	- ×	► Top Serve	Applications Se	en		- ×	Top Operating Systems See	n	

Image 4. Object Management

Step 2.1. From the left panel, navigate to **Access List > Extended** to create an extended ACL.

Cipects / Object Management	Center _{Overview}	Analysis Policie	Bevices	Objects	Integration	Dep	loy Q 🤩 🛱 🕄	admin - disco SECURE
> AAA Server	Network					Add Network	▼ Q. Filter	
✓ Access List							Show I	Jnused Objects
Extended	A network object represents network discovery rules, eve	one or more IP addresse ent searches, reports, and	s. Network objec so on.	ts are used in v	arious places, i	including access control policies, n	etwork variables, intrusior	n rules, identity rules,
Standard								
> Address Pools	Name					Value	Туре	Override
Application Filters	any					0.0.0.0/0	Group	Q 🗑 👪
AS Path								0 2 4
Cipher Suite List	any-ipv4					0.0.0.0/0	Network	≪ ≣ 6
> Community List	any-ipv6					::/0	Host	Q 🗑 👪
> Distinguished Name	IPv4-Benchmark-Tests					198.18.0.0/15	Network	۹ 🗑 🚯
DNS Server Group								0.5.4
> External Attributes	IPv4-Link-Local					169.254.0.0/16	Network	Q ≣ 88
File List	IPv4-Multicast					224.0.0.0/4	Network	Q ≣ ₿
> FlexConfig	IPv4-Private-10.0.0.0-R					10.0.0.0/8	Notwork	0 = #
Geolocation	1PV4-P11Vate=10.0.0.0-8					10.0.0.0/8	Network	~ 80
Interface	IPv4-Private-172.16.0.0-12					172.16.0.0/12	Network	९ ≣ ₿
Key Chain	IPv4-Private-192.168.0.0-16	5				192.168.0.0/16	Network	Q 🗑 👪
Network						10.0.0.0/8		
> ркі	IPv4-Private-All-RFC1918					172.16.0.0/12 192.168.0.0/16	Group	Q 🗎 👪
Policy List								
Port						Displayi	ng 1 - 14 of 14 rows 🖂 <	Page 1 of 1 > > C
> Drefiv List								

Image 5. Extended ACL menu

Step 2.2. Then, select Add Extended Access List.

Firewall Manageme Objects / Object Manageme	ent Center	Overview Analysis	Policies	Devices	Objects	Integration	Deploy	¢ 🔮 🗘	🕜 admin 🗸 🏻 🗧	SECURE
> AAA Server	Extended						Add Extended Acces	ss List ् २ Filte	er	
✓ Access List										
Extended	An access list ob traffic based on s	ject, also known as an ource and destination	access control lis address and port	it (ACL), selec: s. Supports IP	ts the traffic to /4 and IPv6 ad	which a service will apply. dresses. You use these obje	Standard-Identifies traffic b ects when configuring partic	ased on destination cular features, suc	on address only. k h as route maps.	lentifies
Standard										
> Address Pools	Name						Value		Override	
Application Filters										
AS Path						o 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							N	data to display	< < Page 1	of 1 > > C
> Prefix List										

Image 6. Add Extended ACL

Step 2.3. Type a name for the extended ACL, and then, click on the **Add** button to create an access control entry (ACE):

Firewall Mana Objects / Object M	agement Center	Overview	Analysis Policies	Devices Objects	Integration	Deploy	९ 🧬 🌣 0	admin •
> AAA Server > Access List	New Extended Ac	ccess List Obje	ct					
Extended	Name ACL-UNWANTED-C	DUNTRY						dress only. Identifies oute maps.
 Address Pools Application Filters AS Path 	Entries (0)						Add	Override
Cipher Suite List Community List	Sequence Action	Source	Source Port	Destination	Destination Port	Application		
 Distinguished Name DNS Server Group External Attributes 								
File List								
Geolocation Interface Key Chain	Allow Overrides							
Network							Save	
Policy List Port						No e	data to display ∣< <	Page 1 of $1 > > C$

Image 7. Extended ACL entries

Step 2.4. Change the ACE action to **Block**, then add the source network to match the traffic that needs to be denied to the FTD, keep the destination network as Any, and click on the Add button to complete the ACE entry:

- In this example, the ACE entry configured blocks VPN brute force attacks coming from the 192.168.1.0/24 subnet.

Citer Constant Consta	Action: Block			cisco SECURE
 > AAA Server > Access List Extended Standard > Address Pools Application Filt 	Logging: Default Log Level: Informational Log Interval: 300 Sec.			Identifies L
AS Path Cipher Suite Lit- > Community Lis > Distinguished N DNS Server Gro > External Attribu File List > FiexConfig	Network Port Application Available Networks C + Q. Search by name or value	Source Networks (1) 192.168.1.0/24	Destination Networks (0) any	
Geolocation Interface Key Chain Network PKI Policy List Port Port	IPv4-Link-Local IPv4-Multicast IPv4-Private-10.0.0.0-8 IPv4-Private-172.16.0.0-12	Enter an IP address Add	Enter an IP address Add	of 1 > > ℃

Image 8. Denied Networks

Step 2.5. In case you need to add more ACE entries, then click on the **Add** button again and repeat step 2.4. After this, click on the Save button to complete the ACL configuration.

Firewall Managemen	Edit Exten	ided Acc	ess List Object					0	cisco SECURE
➢ AAA Server ✓ Access List	Name ACL-UNW	ANTED-CC	UNTRY						
Extended	Entries (1)								Identifies
Standard								Add	
> Address Pools								_	
Application Filters	Sequence	Action	Source	Source Port	Destination	Destination Port	Application		/ E M
AS Path	1	Block	192.168.1.0/24					11	
Cipher Suite List									
> Community List									
> Distinguished Name									
DNS Server Group									
> External Attributes									
File List	Allow Ov	rrides							
> FlexConfig									
Geolocation								Save	
Interface									
Key Chain									
Network									
> ркі									
Policy List									
Port							Displaying 1 - 1 of 1 rows	IC < Page 1	of 1 > > C

Image 9. Completed Extended ACL entries

Step 3. Then, you need to configure a Flex-Config Object to apply the control-plane ACL to the outside FTD interface. For this, navigate to the left panel, and select the option **FlexConfig > FlexConfig Object**.



Image 10. FlexConfig Object menu

Step 3.1. Click Add FlexConfig Object.

Firewall Management	t Center _{Overview}	Analysis Pol	icies Devices	Objects	Integration		Deploy Q	. 🥐 🛠	ŧ 🕜 admin v	eisco SECURE
> AAA Server ~ Access List Extended Standard	FlexConfig Object	t vice configuration co	mmands, variables, a	ind scripting lar	nguage instructions.	It is used in FlexConf	d FlexConfig Obje	t Q F	filter	
> Address Pools	Name						Description			
Application Filters AS Path	Default_DNS_Configure						Configure Defaul	DNS with	the help of TextOt	xj P∎ Q 🗎
Cipher Suite List	Default_Inspection_Protocol_	Disable					Disable Default In	spection.		¶∎ Q
> Community List	Default_Inspection_Protocol_I	Enable					Enable Default In	spection.		¶∎ Q =
> Distinguished Name DNS Server Group	DHCPv6_Prefix_Delegation_C	onfigure					Configure one ou	tside (PD c	lient) and one insi	d P∎ Q 🗎
> External Attributes	DHCPv6_Prefix_Delegation_U	InConfigure					Remove configur	ation of one	outside (PD clien	nt 🐴 Q 🗎
File List	DNS_Configure						Configure DNS w	ith the help	of TextObjects de	n 🖺 Q 🗑
✓ FlexConfig FlexConfig Object	DNS_UnConfigure						Remove the DNS	configurati	ons.	¶∎ Q
Text Object	Eigrp_Configure						Configures eigrp.	1. Configu	res next hop. 2. c	o 🖪 🤉 🗎
Geolocation	Eigrp_Interface_Configure						Configures interfa	ice parame	ters for eigrp. 1. (o 🖻 q 🗎
Key Chain	Eigrp_UnConfigure						Clears eigrp cont	guration fo	r an AS	¶∎ Q
Network	Eigrp_Unconfigure_All						Clears eigrp cont	iguration.		Fa Q 📄
> ркі							Displaying 1 - 20	of 48 rows	IC < Page 1	of 3 > > C
Policy List										

Image 11. Add Flexconfig Object

Step 3.2. Add a name for the FlexConfig object and then, insert an ACL policy object. For this, select **Insert** > **Insert Policy Object** > **Extended ACL Object**.

Firewall Manageme	Name: OBJ-FC-CONTROL-PLANE							⊱ 🕝 admin 🕶 🔤	sco SECURE
> AAA Server	Description:							Filter	
Extended	Copy-pasting any rich t	ext might introd	luce line break	s while generating CLI.	Please verify the	CLI before deployr	nent.		
Standard									
> Address Pools	Insert 🔻 🔛	Deployment:	Once		Type:	Append	•		
Application Filters	Insert Policy Object	Text Object						the hole of ToutOhi	B o E
AS Path	Insert System Variable	Network						the help of TextObj	
Cipher Suite List	Insert Secret Key	Security Zon	es						¶∎ Q 🗑
> Community List		Standard AC	L Object						Γ ₁ α <u>≡</u>
> Distinguished Name		Extended AC	L Object						
DNS Server Group		Route Map						lient) and one insid	Ч а –
> External Attributes								e outside (PD client	R Q 🗑
								of TextObjects dn	Fa Q 📄
✓ FlexConfig	▼ Variables								E o E
	Name	C	imension	Default Value	Property	Override	Description	ions.	
Text Object					(Type:Name)			ires next hop. 2. co	¶∎ < ``
Geolocation				No records to dis	splay			eters for eigrp. 1. C	⊑ α
Interface									
Key Chain								or an AS	唱 Q =
Network									Γ ∎ α =
> ркі								s I< < Page 1	of 3 > > C
Policy List							Cancel Save		

Image 12. FlexConfig Object variable

Step 3.3. Add a name for the ACL object variable and then, select the extended ACL that was created in the Step 2.3, after this, click on the **Save** button.

Firewall Manageme	Name:					
	OBJ-FC-CONTROL-PLANE				ליין @admin און מיי	SECURE
> AAA Server > Access List	Description:	Insert Extended Access List Object	t Variable 🛛 💿		Filter	
Extended Standard > Address Pools Application Filters AS Path Cipher Suite List > Community List > Distinguished Name DNS Server Group > External Attributes File List	Copy-pasting any rich	Variable Name: VAR-ACL-UNWANTED-COUNTRY Description: Available Objects C Q Search C Search	Selected Object		the help of TextObj ilient) and one insid p outside (PD client	
✓ FlexConfig	▼ Variables				y or rexcobjects un	
	Name			riotion	ions.	暗 へ
Text Object					ires next hop. 2. co	¶∎ < `
Geolocation					aters for eigrp. 1. C	唱 Q 📄
Interface Key Chain			Cancel		xr an AS	₽ _ Q =
Network						Ha Q
> PKI					Page 1	0137710

Image 13. FlexConfig Object variable ACL assignment

Step 3.4. Then, configure the control-plane ACL as inbound for the outside interface.

Command line syntax:

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

This translates into the next command example, which uses the ACL variable created in the Step 2.3 'VAR-

ACL-UNWANTED-COUNTRY':

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

This is how it must be configured into the FlexConfig object window, after this, select the **Save** button to complete the FlexConfig Object.

Firewall Manageme	Name:						⊱ 🙆 admin 🔻 🕛	We secure
Objects / Object Managemer	OBJ-FC-CONTROL-PLANE							
> AAA Server	Description:						Filter	
 ✓ Access List 								
Extended	A Conversating any rich text might in	troduce line break	re while generating CLL	Diagen unrify the	CI I before deploy	ment		
Standard			a while generating out.	-		intent.		
> Address Pools	Insert 🕶 🔢 Deploymen	Conce		Type:	Append	*		
Application Filters	access-group \$VAR-ACL-UNWANTED-COUN	TRY in interface outsi	de control-plane				the help of TextObi	FL Q
AS Path								
Cipher Suite List								Б (
> Community List								¶a Q
> Distinguished Name							lient) and one insid	Rac ⊒
DNS Server Group							and one mard	
> External Attributes							a outside (PD client	Γ α 📄
File List							of TextObjects dn	R _a Q
✓ FlexConfig	▼ Variables							B o E
FlexConfig Object	Name	Dimension	Default Value	Property	Override	Description	ions.	
Text Object				(Type:Name)			res next hop. 2. co	η α 📄
Geolocation	VAR-ACL-UNWANTED-COUNTRY	SINGLE	ACL-UNWANTED	EXD_ACL:A	false		eters for eigrp. 1. C	¶a q ≣
Interface								
Key Chain							br an AS	ч а ч –
Network								Γ <u>α</u>
> ркі							s I< < Page 1	of 3 > > C
Policy List						Cancel Save		

Image 14. Flexconfig Object complete command line

Note: It is highly recommended to configure the control-plane ACL just for the interfaces receiving incoming remote access VPN sessions in the secure firewall, like the Outside interface.

Step 4. You need to apply the FlexConfig Object configuration to the FTD, for this, navigate to **Devices** > **FlexConfig**.

Firewall Managemer	t Center _{Overview} Analysis Policies	Devices Objects	Integration	Deploy Q 🧬 🕏	ጅ 🕜 admin 🕶 🏻 🖞	secure
AAA Server Access List Extended Standard Address Pools Application Filters	FlexConfig Object FlexConfig Object include device configuration command	Device Management Device Upgrade NAT QoS Platform Settings FlexConfig	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	
AS Path Cipher Suite List	Default_Insp	I Certificates		Disable Default Inspection.	he help of TextObj	Β α Β Ι α
Community List Distinguished Name	Default_Ins	pection_Protocol_Enable		Enable Default Inspection.		₽ 0, 11
DNS Server Group > External Attributes	DHCPv6_Pre	ftx_Delegation_Configure x_Delegation_UnConfigure		Configure one outside (PD cl Remove configuration of one	ient) and one insid	a ∎α ∎α
File List ∀ FlexConfig	C	NS_Configure		Configure DNS with the help	of TextObjects dn	Γ α - Π
FlexConfig Object Text Object	E	IS_UnConfigure		Remove the DNS configuration	res next hop. 2. co	aα ∎α ∎
Geolocation Interface	Eigrp_	Interface_Configure		Configures interface parame	ters for eigrp. 1. C	₽ 0, 1
Key Chain Network	Eigr	rp_UnConfigure		Clears eigrp configuration fo	r an AS	¶∎α. ¶∎α.≣
> ркі				Displaying 1 - 20 of 49 rows	IK < Page 1	of 3 > > C*

Image 15. FlexConfig Policy menu

Step 4.1. Then, click on New Policy if there is not an already FlexConfig created for your FTD, or edit the existing FlexConfig policy.

New Pr	
	icy
FlexConfig Policy Status Last Modified	
There are no policies created. Add a new policy	

Image 16. FlexConfig Policy creation

Step 4.2. Add a name for the new FlexConfig policy and select the FTD you would like to apply the controlplane ACL created.

Firewall Management Center Devices / FlexConfig	Overview Analysis Policies	Devices Objects	Integration		Deploy Q 🌓 🌣 🕻	admin • shalls SECURE
FlexConfig Policy	New Policy			0		
	Name: FLEXCONFIG-POLICY Description:					
	Targeted Devices Select devices to which you want	to apply this policy.	Salastad Devices	_		
	Q Search by name or value		FTD-CONTROL-PLANE	ו		
	FTD-CONTROL-PLANE	Add to Policy				
			Cancel	re		

Image 17. FlexConfig Policy device assignment

Step 4.3. From the left panel, search for the FlexConfig object created in the step 3.2, then, add it to the FlexConfig policy by clicking on the right arrow located in the middle of the window, after this, click on the **Save** button.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 🥩 🌣 🕢 admin 🕇 🖓 secure
FLEXCONFIG-POLICY							You have unsaved changes Preview Config Save Cancel
Enter Description							Policy Assignments (1)
		ed Prepend F	lexConfias				
Available FlexConfig C FlexConfig Object	# Nar	ne			Description		
OBJ-FC-CONTROL-PLANE							
V System Defined	-						
Default_DNS_Configure							
Default_Inspection_Protocol_Disable							
Default_Inspection_Protocol_Enable	Selecte	ed Append F	lexConfigs				
DHCPv6_Prefix_Delegation_Configure	# Nar	ne			Description		
DHCPv6_Prefix_Delegation_UnConfigure		110			Description		
n DNS_Configure	1 OB.	I-FC-CONTROL	-PLANE				٩ 🖷
J DNS_UnConfigure							
"i Eigrp_Configure							
"B Eigrp_Interface_Configure							
^g Eigrp_UnConfigure							
" ⁹ Eigrp_Unconfigure_All							

Image 18. FlexConfig Policy object assignment

Step 5. Proceed to deploy the configuration change to the FTD, for this, navigate to **Deploy** > **Advanced Deploy**.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q	. 🧳 🌣	😗 admin 🔻	cisco SEC	CURE
FLEXCONFIG-POLICY								Advance	d Deploy	eploy All	ncel
Enter Description						FTD-CONTROL-PLANE		Ready for	Deployment	å	
	" Selecte	ed Prepend F	lexConfigs								
Available FlexConfig Object	# Nar	ne			Description						
V User Defined											
OBJ-FC-CONTROL-PLANE											
✓ System Defined											
Configure											
Default_Inspection_Protocol_Disable						I device is available for deployment				₽ +9	
The section Protocol Enable	Selecte	ed Append F	lexConfigs								
DHCPv6_Prefix_Delegation_Configure											
DHCPv6_Prefix_Delegation_UnConfigure	# Nar	ne			Description						
ী DNS_Configure	1 OB.	J-FC-CONTROL	-PLANE								۹ 🖬
DNS_UnConfigure											

Image 19. FTD Advanced Deploy

Step 5.1. Then, select the FTD to which you want the FlexConfig policy applied. If everything is correct, then click **Deploy**.

Firewall Management Center Deploy / Deployment	Overview Analysis	Policies Device:	s Objects Integration	Deploy	Q 🧬	☆ ⑦ admin ▼ store
1 device selected Y Q Search using device name, user name, type	e, group or status					Deploy time: Estimate Deploy
Device	Modified by	Inspect Interruption	Type Group	Last Deploy Time	Preview	Status
V STD-CONTROL-PLANE	admin		FTD	Sep 5, 2023 12:05 PM	B	Ready for Deployment
Flex Configuration Template Policy: FLEXCONFIG-POLICY						
https://10.88.243.58:43013/ddd/#ContextExplorer						

Image 20. FTD Deployment validation

Step 5.2. After this, a Deployment Confirmation window is displayed, add a comment to track down the deployment and proceed to **Deploy**.

Ę	F	irewall Management Center	Overview	Analysis Policies Devic	es Objects	Integration		Deplo	y Q 🧬	☆ @ admin ▼ attude SEC	URE
1 der	vice se										
			Modified by								
		FTD-CONTROL-PLANE	admin				Sep 5	5, 2023 12:05 PM		Ready for Deployment	
\$. •		 Flex Configuration Template Policy; FLEXCONFIG-POLICY 		Deployment Confirmatio	n		×				
				You have selected 1 device to	deploy						
				Deployment Notes:							
				You can optionally add notes	about the configu	ration changes					
							Deploy				

Image 21. FTD Deployment comments

Step 5.3. A warning message could appear when deploying FlexConfig changes. Click on **Deploy** only if you are completely certain that the policy configuration is correct.

[Fi	rewall Manag	ement Center			admin =	dulu anas	
- Lini			Validation Mes	sages: FTD-CONTROL-PLANE	×	aumin •		
1 devi	ce sel							
T		Search using dev	1 total 0 e	errors 1 warning 0 info				
			PG.TEMPLATE.T	emplatePolicy: FLEXCONFIG-POLICY				
~	1	FTD-CONTROL	 Warning: 	FlexConfig policies intentionally do not contain extensive input validation. Please ensure that the configurations in this FlexConfig policy are		on Warnings		
		 Flex Configuration 		correct. Incorrect configurations will result in a failed deployment that may cause a network interruption. This is only a generic warning and is an indication of an incorrect configuration.	not			
×-		Template Poli						
				Close	low			

Image 22. FTD Deployment Flexconfig warning

Step 5.4. Confirm that the policy deployment is successful for the FTD.

Ę	Fi De	rewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🧳	🔅 🕜 admi	in ▼ stanta SECURE
Ţ	٩	Search using device name, user name, type,	, group or statu	s									Deploy
		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.	Completed	
*= •	1	 Flex Configuration Template Policy: FLEXCONFIG-POLICY 									l		

Image 23. FTD Deployment successful

Step 6. If you create a new control-plane ACL for your FTD or if you edited an existing one that is actively in use, then, it is important to highlight that the configuration changes made do not apply to already established connections to the FTD, therefore, you need to manually clear the active connection attempts to the FTD. For this, connect to the CLI of the FTD and clear the active connections.

To clear the active connection for a specific host IP address:

> clear conn address 192.168.1.10 all

To clear the active connections for a whole subnet network:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

To clear the active connections for a range of IP addresses:

> clear conn address 192.168.1.1-192.168.1.10 all

Note: It is highly recommended to use the keyword '**all**' at the end of the clear conn address command to force the clearing of the active VPN brute force connection attempts to the secure firewall, mainly when the nature of the VPN brute force attack is launching a blast of constant connection attempts.

[VIDEO] Configure a control-plane ACL for FTD managed by FMC

Configure a control-plane ACL for FTD managed by FDM

This is the procedure you need to follow in an FDM to configure a control plane ACL to block incoming VPN brute force attacks to the outside FTD interface:

Step 1. Open the FDM GUI via HTTPS and Log in with your credentials.



© 2015-2023 Casco 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 ABSOLUTE!V NO WARRANTY under the terms of "GNU Lesser General Public License, version 21, 10 and version 310".

Image 24. FDM Log In page

Monitoring Policies Ubjects admin Firewall Device Manager cisco SECURE Administrator High Availability 🕜 Not Configured Model Cisco Firepower Threat Defense for VMwa... VDB 353.0 Rule Up 7.2.5-208 CONFIGURE 20220511-1540 Not Registered | R A Internet 0/1 Cisco Firepower Threat Defense for VMware 🕚 0/0 System Settings Interfaces Updates Routing nt Acc There are no static routes yet Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds Enabled 3 of 3 ng Settings DHCP Server / Relay View All Interface > View Configuration > View Configuration > DDNS Service DNS Server Management Interfac Smart License Backup and Restore Troubleshoot 89 Hostname Evaluation expires in 89 days No files created yet Time Services

Step 2. You need to create an object network. For this, navigate to Objects:

Image 25. FDM main dashboard

Step 2.1. From the left panel, select Networks and then click on the '+' button to create a new network object.

Firewall Device Manager	Monitoring Policies Objects Device: firepow	er 🔎	admin ×	cisco SECURE
Object Types ←	Network Objects and Groups			
C Networks	6 objects		Y Filter	+
S Ports			Preset filters: System defined, User defined	
8 Security Zones	# NAME	TYPE VALUE		ACTIONS
🐬 Application Filters	1 IPv4-Private-10.0.0-8	NETWORK 10.0.0/8		
ℓ URLs	2 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0/12		
Geolocations	3 IPv4-Private-192.168.0.0-16	NETWORK 192.168.0.0/16		
	4 any-ipv4	NETWORK 0.0.0/0		
Syslog Servers	5 any-ipv6	NETWORK ::/0		
🔑 IKE Policies	6 IPv4-Private-All-RFC1918	Group IPv4-Private-10.0 192.168.0.0-16	0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-	
🐴 IPSec Proposals				
Secure Client Profiles				
Sources				
1 Users				
Q Certificates				
Secret Keys				

Image 26. Object creation

Step 2.2. Add a name for the network object, select the Network type for the object, add the IP address, network address or the range of IPs to match the traffic that needs to be denied to the FTD. Then, click the **Ok** button to complete the object network.

- In this example, the object network configured is intended to block VPN brute force attacks coming from the 192.168.1.0/24 subnet.

Firewall Device Manager	Monitoring Polici			? : admin Administrator ~ "tistle SECURE
Object Types ←	Network Obje	Add Network Object	9 ×	
Le Networks	6 objects	OBJ-NET-UNWANTED-COUNTRY		defined, User defined
Security Zones	# NAME	Description		ACTIONS
P Application Filters	1 IPv4-Private-A		h.	e-172.16.0.0-12, IPv4-Private-
C ² URLs	2 IPv4-Private-10	Type		
Geolocations	3 IPv4-Private-1:	Natwork		
Syslog Servers	4 IPv4-Private-1	192.168.1.0/24		
RE Policies	6 any-ipv6	e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60		
🐴 IPSec Proposals		CANCEL	w	
Secure Client Profiles		UNIDE	~	
Sa Identity Sources				
L Users				
🙊 Certificates				
Secret Keys				

Image 27. Add Network Object

Step 3. Then, you need to create an extended ACL, for this, navigate to the Device tab at the top menu.

Firewall Device Manager	Monitoring Policies Objects Device: firepow	er	cisco SECURE
Object Types 🗧 🔶	Network Objects and Groups		
C Networks	7 objects	T Filter	+ 🔍
S Ports		Preset filters: System defined. User defined	
8 Security Zones	N 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	
🖉 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	
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	
	6 any-ipv6	NETWORK ::/0	
	7 OBJ-NET-UNWANTED-COUNTRY	NETWORK 192.168.1.0/24	
Secure Client Profiles			
Sea Identity Sources			
👤 Users			
🙊 Certificates			
🔒 Secret Keys			

Image 28. Device settings page

Step 3.1. Scroll down and select **View Configuration** from the Advanced Configuration square as shown in the image.

Interfaces Routing There are no static routes yet Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds System Settings View All Interfaces View Configuration View Configuration DHCP Server / Relay Smart License Backup and Restore Troubleshoot Management Interface Evaluation expires in 89 days Backup and Restore No files created yet Management Interface View Configuration View Configuration Request FILE TO BE CREATED See more		0/0		
Smart License Backup and Restore Troubleshoot Management Interface Evaluation expires in 89 days Backup and Restore No files created yet Time Services Time: Not selected (Threat Defense Virtual - Variable) View Configuration No files created yet REQUEST FILE TO BE CREATED See more Site-to-Site VPN Remote Access VPN Advanced Configuration Device Administration	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
Site-to-Site VPN Remote Access VPN Advanced Configuration Device Administration	Smart License Evaluation expires in 89 days Tier: Not selected (Threat Defense Virtual - Variable)	Backup and Restore	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Management Interface Hostname Time Services See more
There are no connections yet Requires RA VPN license Includes: FlexConfig. Smart CLI Audit Events, Deployment History	Site-to-Site VPN There are no connections yet	Remote Access VPN Requires RA VPN license	Advanced Configuration Includes: FlexConfig, Smart CLI	Device Administration Audit Events, Deployment History,

Image 29. FDM Advanced Configuration

Step 3.2. Then, from the left panel, navigate to **Smart CLI > Objects** and click on **CREATE SMART CLI OBJECT**.

Firewall Device Manager	Monitoring	Policies	₩ Objects	Device: firepower	(2		?	:	admin Administrator	vibility SECURE	
Advanced ← Configuration	Device Summ Objects	ary										
Smart CLI											+	
Objects		NAME		туре	DESCRIPTION					ACTIONS		
FlexConfig					There are no Smart CL	I objects yet.	inet					
FlexConfig Objects					Start by creating the first of	Smart OLI ODJ	ect.					
FlexConfig Policy					CREATE SMART CL	OBJECT						

Image 30. Smart CLI Objects

Step 3.3. Add a name for the extended ACL to create, select **Extended Access List** from the CLI template drop-down menu, and configure the ACEs required by using the network object created in the step 2.2, then click the OK button to complete the ACL.

Firewall Devic	Edit Smart CLI Object	admin	en e
Advanced Configuration		Description	
Smart CLI Objects	CLI Template		ACTIONS
FlexConfig	Extended Access List	Show disabled	Reset
FlexConfig Objects	1 access-list ACL-UNAWNIED-COUNTRY extended 2 configure access-list-entry deny ~ 3 deny network source [003-mET-UNAWNIED-COUNTRY x ~] destin 4 configure deny port any ~	ation [any-ipod X v]	
	⊙ 5 deny port source ANY destination ANY ○ 6 configure logging default ∨ ○ 7 default log set log-level INFORMATIONAL log-interval	300	
		CANCEL	ок

Image 31. Extended ACL creation

Note: If you need to add more ACEs for the ACL, you can do it by hovering the mouse over the left of the current ACE; then three clickable dots do not appear. Click on them and select Duplicate to add more ACEs.

Step 4. Then, you need to create a FlexConfig object, for this, navigate to the left panel and select **FlexConfig > FlexConfig Objects**, and click on **CREATE FLEXCONFIG OBJECT**.

Firewall Device Manager	Monitoring Policies Objects	Device: firepower	tor v think SECURE
Advanced ← Configuration	Device Summary FlexConfig Objects		
Smart CLI		Y Filter	+
Objects	# NAME	DESCRIPTION ACTIONS	
FlexConfig FlexConfig Objects FlexConfig Policy		There are no FlexConfig objects yet. Start by creating the first FlexConfig object.	

Image 32. FlexConfig Objects

Step 4.1. Add a name for the FlexConfig object to create and configure the control-plane ACL as inbound for the outside interface as shown in the image.

Command line syntax:

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

This translates into the next command example, which uses the extended ACL created in the Step 3.3 'ACL-UNWANTED-COUNTRY':

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

This is how it can be configured into the FlexConfig object window, after this, select the **OK** button to complete the FlexConfig Object.

Firewall Device Ma	anager Monitoring				<u></u>	admin Administrator	cisco SECURE	
Advanced ← Configuration	Device Sur FlexCo	Name			0 ×			
Smoot OL		OBJ-FC-CONTROL-PLANE					+	
Objects		Description				CTIONS		
00,000					li.			
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-UNNANTED-CO	UNTRY in interface outside	control-plane				
		Negate Template 🛆		Expand	🗘 Reset			
		1 no access-group ACL-UNMANTED	-COUNTRY in interface outsi	ide control-plane				
				CANCEL	ок			

Image 33. FlexConfig Object creation

Note: It is highly recommended to configure the control-plane ACL just for the interfaces receiving incoming remote access VPN sessions in the secure firewall, like the Outside interface.

Step 5. Proceed to create a FlexConfig Policy, for this, navigate to **FlexConfig Policy**, click on the '+' button, and select the FlexConfig object that was created in the step 4.1.

Firewall Device Manager	Monitoring Policies Objects Device: firepower	S admin Administrator ✓	cisco SECURE
Advanced ← Configuration	Device Summary FlexConfig Policy		
Smart CLI	Group List	Preview	<> Expand
Objects	♥ ▼ Filter	There is nothing to preview yet.	
FlexConfig	OBJ-FC-CONTROL-PLANE		
FlexConfig Objects	Creste.new ElexConfig.Object CANCEL OK		
FlexConfig Policy			
	SAVE		

Image 34. FlexConfig Policy

Step 5.1. Validate that the FlexConfig preview shows the correct configuration for the control-plane ACL created and click on the **Save** button.

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

Image 35. FlexConfig Policy preview

Step 6. Deploy the configuration changes to the FTD you would like to protect against the VPN brute force attacks, for this, click on the **Deployment** button at the top menu, validate that the configuration changes to deploy are correct, and then, click on **DEPLOY NOW**.

Firewall Device Manager	Pending Changes	admin Vistrator × dividu SECURE
Advanced ← Configuration	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 G LEGEND
Objects	Network Object Added: OBJ-NET-UNWANTED-COUNTRY	
FlexConfig	-	subType: Network ↔ Expand value: 2.2.2.0/24 in interface outside dnsResolution: IPV4_NU0_IPV6
FlexConfig Objects	1	description: name: 08J-NET-UNKANTED-COUNTRY
FlexConfig Policy		
	<pre>// Procedury Concy Entred: default-group /lexConfigObjects: -</pre>	083-FC-CONTROL-PLANE
	S Extended Access List Added: ACL-UNWANTED-COUNTRY	
	- - entries[0].sourceNetworks:	entries[0].logging: DEFAULT entries[0].action: DENY name: ACL-UNMANTED-COUNTRY
		ORT NET IBMANTER COUNTRY
	MORE ACTIONS V	CANCEL DEPLOY NOW Y

Image 36. Pending Deployment

Step 6.1. Validate that the policy deployment is successful.



Image 37. Deployment successful

Step 7. If you create a new control-plane ACL for your FTD or if you edited an existing one that is actively in use, then, it is important to highlight that the configuration changes made do not apply to already established connections to the FTD, therefore, you need to manually clear the active connection attempts to the FTD. For this, connect to the CLI of the FTD and clear the active connections.

To clear the active connection for a specific host IP address:

```
> clear conn address 192.168.1.10 all
```

To clear the active connections for a whole subnet network:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

To clear the active connections for a range of IP addresses:

> clear conn address 192.168.1.1-192.168.1.10 all

Note: It is highly recommended to use the keyword '**all**' at the end of the clear conn address command to force the clearing of the active VPN brute force connection attempts to the secure firewall, mainly when the nature of the VPN brute force attack is launching a blast of constant connection attempts.

Configure a control-plane ACL for ASA using CLI

This is the procedure you need to follow in an ASA CLI to configure a control plane ACL to block incoming VPN brute force attacks to the outside interface:

Step 1. Log in to the secure firewall ASA via CLI and get access to the 'configure terminal'.

asa# configure terminal

Step 2. Use the next command to configure an extended ACL to block a host IP address or network address for the traffic that needs to be blocked to the ASA.

- In this example, you create a new ACL called 'ACL-UNWANTED-COUNTRY' and the ACE entry configured blocks VPN brute force attacks coming from the 192.168.1.0/24 subnet.

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

Step 3. Use the next access-group command to configure the 'ACL-UNWANTED-COUNTRY' ACL as a control-plane ACL for the outside ASA interface.

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

Note: It is highly recommended to configure the control-plane ACL just for the interfaces receiving incoming remote access VPN sessions in the secure firewall, like the Outside interface.

Step 4. If you create a new control-plane ACL or if you edited an existing one that is actively in use, then, it is important to highlight that the configuration changes made do not apply to already established connections to the ASA, therefore, you need to manually clear the active connection attempts to the ASA. For this, clear the active connections.

To clear the active connection for a specific host IP address:

asa# clear conn address 192.168.1.10 all

To clear the active connections for a whole subnet network:

asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all

To clear the active connections for a range of IP addresses:

asa# clear conn address 192.168.1.1-192.168.1.10 all

Note: It is highly recommended to use the keyword '**all**' at the end of the clear conn address command to force the clearing of the active VPN brute force connection attempts to the secure firewall, mainly when the nature of the VPN brute force attack is launching a blast of constant connection attempts.

Alternative configuration to block attacks for secure firewall using the 'shun' Command

In case of an immediate option to block attacks for the secure firewall, then you can use the 'shun' command. Theshuncommand lets you block connections from an attacking host, here you have further details about this shun command:

- Once you shun an IP address, then, all future connections from the source IP address are dropped and logged until the blocking function is removed manually.
- The blocking function of the shuncommand is applied whether or not a connection with the specified host address is currently active.
- If you specify the destination address, source and destination ports, and the protocol, then you drop the matching connection as well as placing a shun on all future connections from the source IP address; all future connections are shunned, not just those that match these specific connection parameters.
- You can only have oneshuncommand per source IP address.
- Because the shuncommand is used to block attacks dynamically, it is not displayed in the threat defensed evice configuration.
- Whenever an interface configuration is removed, all shuns that are attached to that interface are also removed.
- Shun command syntax:

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

• To disable a shun, use the no form of this command:

no shun source_ip [vlan vlan_id]

To shun a host IP address, then proceed as follows for the secure firewall. In this example, the 'shun' command is used to block VPN brute force attacks coming from the source IP address 192.168.1.10.

Configuration example for FTD.

Step 1. Log in to the FTD via CLI and apply the shun command.

<#root>

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

Shun 192.168.1.10 successful

Step 2. You can use the show commands to confirm the shun IP addresses in the FTD and to monitor the shun hit counts per IP address:

```
<#root>
>
show shun
shun (outside) 192.168.1.10 0.0.0.0 0 0 0
>
show shun statistics
diagnostic=0FF, cnt=0
outside=0N, cnt=0
Shun 192.168.1.10 cnt=0, time=(0:00:28)
```

Configuration example for ASA

Step 1. Log in to the ASA via CLI and apply the shun command.

<#root>

asa#

shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

Step 2. You can use the show commands to confirm the shun IP addresses in the ASA and to monitor the shun hit counts per IP address:

<#root>

asa#

```
show shun
shun (outside) 192.168.1.10 0.0.0.0 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)
```

Note: For more information about the secure firewall shun command, check the <u>Cisco Secure Firewall</u> <u>Threat Defense Command Reference</u>

Verify

To confirm the control-plane ACL configuration is in place for the secure firewall, then proceed:

Step 1. Log in to the secure firewall via CLI and run the next commands to confirm the control-plane ACL configuration is applied.

Output example for the FTD managed by 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
```

Output example for the FTD managed by 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
```

Output example for 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
```

Step 2. To confirm the control-plane ACL is blocking the traffic required, use the **packet-tracer** command to simulate an incoming TCP 443 connection to the outside interface of the secure firewall, then use the **show access-list <acl-name>** command, the ACL hit count can increment every time a VPN brute force connection to the secure firewall is blocked by the control-plane ACL:

- In this example, the packet-tracer command simulates an incoming TCP 443 connection sourced from host 192.168.1.10 and destined to the outside IP address of our secure firewall. The 'packet-tracer' output confirms the traffic is being dropped and the 'show access-list' output displays the hit count increments for our control-plane ACL in place:

Output example for 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

Output example for 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
```

Note: If an RAVPN solution like the Cisco Secure Client VPN is implemented in the secure firewall, then, a real connection attempt to the secure firewall could be performed to confirm the control-plane ACL is working as expected to block the traffic required.

Related Bugs

- ENH | Geo-location based AnyConnect Client connections: Cisco bug ID CSCvs65322
- DOC: ASA/FTD Object Group Search does not support Control Plane ACLs: Cisco bug ID <u>CSCwi58818</u>