ىلإ لوصولا يف مكحتلا تاسايس نيوكت رادج ديدەت نع نمآلا عافدلل مكحتلا ىوتسم ASA و ةيامحلا

تايوتحملا

<u>ةمدو،مل</u>
<u>قيس اس أل ا تابل طتمل ا</u>
<u>تابل.طتمل.ا</u>
<u>قمدختسمل تانوكمل ا</u>
<u>قيساسأ تامولعم</u>
<u>نيوكتل</u>
<u>تانىيەكەتلىا</u>
<u>FMC ةطساوب ةرادما ا FTD ل مكحتانا يوتسم ينارا ليوصولنا يف مكحتانا قميناق نيوكت</u>
<u>FDM ةطساوب ةرادما.ا FTD ل مكحتا.ا ىوتسم يال لوصول ا يف مكحتا.ا قميناق نيوكت</u>
<u>CLI مادختساب ASA ا، مِكْجَتَانا يوتَسِم يانا الوَصِولا إِنِفَ مِكْجَتَانا قَمِعْنَاق بَيْوَقْتَ</u>
'shun' رمأليا مادختساب نمآليا قيامحلا رادجل تامجوليا رظحل ل <u>يدب نيوكت</u>
<u>قحصلا نم ققحتا ا</u>

<u>ةلصلا تاذ ءاطخألا</u>

ةمدقملا

نع نمآلا عافدلل مكحتلا ىوتسم ىلإ لوصولا دعاوق نيوكت ةيلمع دنتسملا اذه فصي مالا عافدلل مكحتال العنوبي (ASA) قالدعملا نامألا قزهجأو قيامحلا رادج ديدهت

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- FTD) قيامحلا رادج ديدهت نع نمآلا عافدلا
- (FDM) نمآلاا ةيامحلا رادج ةزهجأ ريدم (FDM)
- FMC) نمآلا ةي امحل رادج قراد إزكرم
- Secure Firewall ASA
- (ACL) لوصولا يف مكحتلا ةمئاق •
- FlexConfig

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- 7.2.5 رادصإلا ،نمآلا ةيامحلا رادج ديدهت دض عافدلا
- Secure Firewall Manager Center، رادصإلاا 7.2.5
- Secure Firewall Device Manager، رادصإلاا 7.2.5
- Secure Firewall ASA، رادصإلا 9.18.3

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا عاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ةيساسأ تامولعم

نم ،فورظلا ضعب يف ؛تانايبلا تاهجاو نيب اههيجوت متيو ةيامح رادج ةداع رورملا ةكرح ربعت ةيامحلا رادج مدختسي نأ نكمي ."نمآلا ةيامحلا رادج" ىلإ ةهجوملا رورملا قكرح ضفر ديفملا رورملا ةكرح دييقتل (ACL) مكحتلا ىوتسم ىلإ لوصولا يف مكحتلا ةمئاق Cisco نم نمآلا يف مكحتلا ةمئاق هيف نوكت نأ نكمي يذلا تقولا ىلع ةلثمألا دحأ نوكي دق ."عبرملا ىلإ" نم) VPN قفن ءاشنإ مهنكمي ءارظنلا يأ يف مكحتلا وه اديفم مكحتلا ىوتسم ىلإ لوصولا نمو رايم في يقوم ال العقوم

"عبرملا لالخ نم" ةيامحلا رادج رورم ةكرح نيمأت

فرعي اذهو ،(ةرداص) ىرخأ ةهجاو ىلإ (ةدراو) ةدحاو ةهجاو نم ةيامحلا ناردج ةداع رورملا ةكرح ربعت لوصولا يف مكحتلا جهن نم لك ةطساوب اهترادإ متتو "عبرملا لالخ نم" رورم ةكرح مساب (ACP) .



عبرملا لالخ نم تانايبلا رورم ةكرح لاثم .1 ةروصلا

"عبرملا ىلإ" ةيامحلا رادج رورم ةكرح نيمأت

وأ عقوم ىلا عقوم نم) FTD ةەجاو ىلإ ةرشابم رورملا ةكرح ەيجوت اەيف متي ىرخأ تالاح كانە ةطساوب اەترادا متتو "عبرملا ىلإ" رورم ةكرح مساب فرعي اذەو ،(دعب نع لوصولل VPN ةكبش ةددحملا ةەجاولا كلتل مكحتلا ىوتسم.



تانايبلا رورم ةكرح ىلع لاثم .2 ةروصلا

مكحتالا يوتسم يال (ACL) لوصولا يف مكحتالا مئاوقب قالعتي اميف ةمهم تارابتعا

- ىلإ (ACL) لوصولاا يف مكحتلا ةمئاق نيوكت بجي ،FMC/FTD نم 7.0 رادصإلاا نم ارابتعا ىلع ةمدختسملا رمألا ةغايص سفن مادختساب ،FlexConfig مادختساب مكحتلا ىوتسم ASA.
- يذلاو ،لوصولا ةعومجم نيوكتب ةيساسألا ةملكلاب مكحتلا ىوتسم قاحلإ متي ىوتسم ةملك نودب .ةنمآلا ةيامحلا رادج ةهجاو "ىلإ" تانايبلا رورم ةكرح ضرفب موقيس ةكرح دييقت ىلع (ACL) لوصولا يف مكحتلا ةمئاق لمعتس ،رمألاب ةقحلملا مكحتلا نمآلا ةيامحلا رادج "لالخ نم" رورملا.
- Telnet وأ ICMP وأ SSH مكحتال ىوتسمال (ACL) لوصوال يف مكحتال ةمئاق ديقت نال
 تاسايسال اقبط (ضفرلا/حامسال) هذه ةجالعم متت .ةنمآ ةيامح رادج ةهجاو ىلإ ةدراول
 ىلعأ قيقبسأ اهالو يساسألا ماظنال تادادعإ
- رورملا ةكرح دييقت ىلع مكحتلا ىوتسمل (ACL) لوصولا يف مكحتلا ةمئاق لمعت وأ FTD ل لوصولا يف مكحتلا ةسايس مكحتت نيح يف ،هسفن نمآلا ةيامحلا رادج "ىلإ" .نمآلا ةيامحلا رادج "لالخ نم" رورملا ةكرح يف ،ASA ل ةيداعلا لوصولا يف مكحتلا مئاوق
- ةياەن يف ينمض "ضفر" دجوي ال ،ةيداعلا (ACL) لوصولا يف مكحتلا ةمئاق فالخب (ACL) لوصولا يف مكحتلا ةمئاق
- تا جل اعقوملا ديدجت" ةزيم مادختسإ نكمي ال ،دنتسملا اذه ءاشنإ تقو يف تكار لوصولا دييقتل "FTD".

نيوكتلا

ةفينعلا VPN ةوق مادختسإ ةنيعم ةلود نم IP نيوانع نم ةعومجم لواحت ،يلاتلا لاثملا يف دض FTD ةيامحل رايخ لضفأ .FTD ةهجاو ىلإ لوخدلا ليجست ةلواحم لالخ نم ةكبشلا يف (ACL) لوصولا يف مكحتلا ةمئاق نيوكت وه هذه VPN ةكبشل ةيشحولا ةوقلا تامجه قوجاوب تالاصتالا هذه رظحل مكحتلا يوتسمل.

تانيوكتلا

FMC ةطساوب ةرادملا FTD ل مكحتلا ىوتسم ىلإ لوصولا يف مكحتلا ةمئاق نيوكت

نيوكتل (FMC) دعب نع لوصولا يف مكحتلا ةدحو يف هتعباتم ىلإ جاتحت يذلا ءارجإلا وه اذه ةكبشل ةمشاغلا ةوقلا تامجه رظحل مكحتلا ىوتسمل (ACL) لوصولا يف مكحتلا ةمئاق VPN تقيجراخلا FTD قوجاو ىلإ قدراولا

لات المدخت من المات المرابع FMC مكحتالا ألام المربع GUI) أي موسرل المدخت من المربع FMC مكحتال المربع HTTPS وطخل كب ةصاخل ادامت عال اتان ايب مادخت ساب لوخدل الجسو.



FMC ىلإ لوخدلا ليجست ةحفص .3 ةروصلا

ىلإ لقتنا ،اذەل .ةعسوم (ACL) لوصولا يف مكحت ةمئاق ءاشنإ ىلإ جاتحت تنأ .2 ةوطخلا تانئاكلا ةرادإ < تانئاكلا.

Firewall Management Center Overview / Dashboards / Dashboard	Overview Ar	nalysis Policies	Devices Objects	Integration	Deploy Q 🤩 🛱	⑦ admin ▼ ^{cloth} SECURE
Summary Dashboard (setter dastboard) Provides a summary of activity on the appliance			Object N Intrusion	Asnagement 1 Rules		Reporting
Network × Threats Intrusion Events	Status Geolo	cation QoS			Show the Last 1 hou	r • II
 Unique Applications over Time 		Top Web App	plications Seen		Top Client Applications Seen	
No Data			No Data		No Da	ta
		Last updated 2 min	utes ago		Last updated 2 minutes ago	
 Traffic by Application Risk 	- ×	► Top Server A	pplications Seen	- ×	Top Operating Systems Seen	- ×

تانئاكلا ةرادإ .4 ةروصلا

يف مكحت ةمئاق ءاشنإل عسوم < لوصولا ةمئاق ىلإ لقتنا ،ىرسيلا ةحوللا نم 2.1 ةوطخلا

.ةعسوم (ACL) لوصولا

Firewall Manageme	ent Center Overvie	w Analysis	Policies	Devices	Objects	Integration		Deploy Q <mark>6</mark> 🌣	admin
> AAA Server	Network						Add Network	▼ Q Filte	er w Unused Objects
Extended Standard	A network object repres network discovery rules	ents one or more l , event searches, r	P addresses. I eports, and so	Network objec on.	ts are used in	various places, in	ncluding access control poli	cies, network variables, intrus	sion rules, identity rules,
> Address Pools	Name						Value	Туре	Override
Application Filters AS Path	any						0.0.0.0/0 ::/0	Group	ର ≣ ୫
Cipher Suite List	any-ipv4						0.0.0/0	Network	Q ≣ ₿
Community List	any-ipv6						::/0	Host	Q ≣ 88
Distinguished Name DNS Server Group	IPv4-Benchmark-Tests						198.18.0.0/15	Network	Q 🗎 👪
> External Attributes	IPv4-Link-Local						169.254.0.0/16	Network	Q ≣ ₩
File List	IPv4-Multicast						224.0.0.0/4	Network	Q 🗎 👪
Geolocation	IPv4-Private-10.0.0.0-8						10.0.0/8	Network	a 🗎 👪
Interface	IPv4-Private-172.16.0.0	-12					172.16.0.0/12	Network	Q ≣ ₩
Key Chain	IPv4-Private-192.168.0	0-16					192.168.0.0/16	Network	a 🗎 👪
> ркі	IPv4-Private-All-RFC19	18					10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	۹ 🗑 🚯
Policy List Port								Displaying 1 - 14 of 14 rows	< < Page 1 of 1 > > C

ةعسوملا (ACL) لوصولا يف مكحتلا ةمئاق ةمئاق .5 ةروصلا

ةعسوملا لوصولا ةمئاق ةفاضإ ددح مث .2.2 ةوطخلا.

	Firewall Managemen	t Center _{overv}	ew Analysis	Policies	Devices	Objects	Integration	Deploy	Q 🧬 🌣	🕜 admin 🕶 🏻 🗧	SECURE
> aa	A Server	Extended						Add Extended Access	List Q Filte	ər	
~ Acc	cess List Extended	An access list object, a traffic based on source	lso known as an a and destination ac	ccess control lis	st (ACL), select s. Supports IP	ts the traffic to v4 and IPv6 a	which a service will ddresses. You use the	apply. Standard-Identifies traffic bas ese objects when configuring particu	sed on destination	on address only. k h as route maps.	dentifies
	Standard										
> Ade	dress Pools	Name						Value		Override	
Ap	olication Filters										
AS	Path						lo records to display				
Cip	her Suite List										
> Co	nmunity List										
> Dis	tinguished Name										
DN	S Server Group										
> Ext	ernal Attributes										
File	List										
> Fle	Config										
Ge	plocation										
Inte	rface										
Key	Chain										
Net	work										
> ркі											
Pol	icy List										
Por	t							No	data to display	< < Page 1	of 1 > > C

ةعسوملا (ACL) لوصولا يف مكحتلا ةمئاق ةفاضا .6 ةروصلا

ةفاضإ رزلا قوف رقنا مث ،ةعسوملا (ACL) لوصولاب مكحتلا ةمئاقل مسا بتكا .2.3 ةوطخلا (ACE) لوصولا يف مكحتلا لاخدإ ءاشنإل

Firewall Mana Objects / Object M	agement Ce anagement	nter	Overview	Analysis Policies	Devices Objects	Integration	Deploy	९ 🧬 🌣 (admin ▼
> AAA Server	New Exte	nded Acc	cess List Obje	ct					
Extended	Name ACL-UNW	ANTED-CO	UNTRY						dress only. Identifies route maps.
> Address Pools Application Filters	Entries (0)							Add	Override
AS Path Cipher Suite List	Sequence	Action	Source	Source Port	Destination	Destination Port	Application		
Community List Distinguished Name									
DNS Server Group External Attributes									
FlexConfig Geologistion									
Interface Key Chain	Allow Ov	errides							
Network								ncel Save	
Policy List Port							No	data to display	< Page 1 of 1 > > C
> Production									

ةعسوملا (ACL) لوصولا يف مكحتلا مئاوق تالاخدا .7 ةروصلا

ةقباطمل ردصملا ةكبشلا ةفاضإب مق مث ،"رظح" ىلا ACE ءارجا رييغتب مق .2.4 ةوطخلا رزلا قوف رقناو ،يأك ةهجولا ةكبشلا ىقبأو ،FTD ىلا اهضفر مزلي يتلا رورملا ةكرح "(ماك لاخدا لامك الحال المعافي) ACE:

- ةكبشل ةمشاغلا ةوقلا تامجه رظحب ەنيوكت مت يذلا ACE لاخدا موقيس ،لاثملا اذه يف VPN لاغران ا تامجه رظحب ان ما ما الالا الالا الالا الالالا الالالا الالالال الالالال الالالال الالالالال الالال

Firewa Objects /	Action: Block		dialis SECURE
> AAA Server	Logging: Default •		
Extended	Log Level:	id I.	dentifies
Standard Address Pools Application Filte	Log Interval: 300 Sec.		/ = M
AS Path	Network Port I Application		× • ••
Community List	Available Networks C + Source	Networks (1) Destination Networks (0)	
> Distinguished N	Q Search by name or value 192.1	68.1.0/24 🕤 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	
> ркі			
Policy List			1
Port		Cancel	orissic
> Prefix List		Cancel	

ةضوفرماا تاكبشاا .8 ةروصاا

ىرخأ ةرم ةفاضإ رزلا قوف رقنا ،ACE تالاخدا نم ديزملا ةفاضا ىلا ةجاحلا ةلاح يف .2.5 ةوطخلا يف مكحتلا ةمئاق نيوكت لامكتسال ظفح رزلا قوف رقنا ،كلذ دعب .2.4 ةوطخلا ررك مث لوصولا

Firewall Managemen Objects / Object Management	Edit Exten	Edit Extended Access List Object Ø								
> AAA Server ~ Access List	Name ACL-UNW	ANTED-CC	DUNTRY							
Extended	Entries (1)								Identifies	
Standard								Add		
> Address Pools										
Application Filters	Sequence	Action	Source	Source Port	Destination	Destination Port	Application		/ = A	
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 Ov	verrides								
> FlexConfig										
Geolocation								Save		
Interface										
Key Chain										
Network										
> ркі										
Policy List										
Port							Displaying 1 - 1 of 1 rows	I< < Page 1	of 1 > > C	
> Drafiv Liet										

ةلمتكملا ةعسوملا (ACL) لوصولا يف مكحتلا مئاوق تالاخدا .9 ةروصلا

ى ال وصول ايف مكحتال قمئاق قيبطتال Flex-Config نئاك نيوكت كمزلي ،مث .3 قوطخل Flex-Config كال وصول يف مكحتال ال رايخل ددجو ،ىرسيل اقحولل الى ل لقتنا ،اذهل .قيجراخل FTD قهجاو ىل ع مكحتال يوتسم FlexConfig > FlexConfig Object.

Ciperts / Object Managemen	nt Center	Overview A	nalysis	Policies	Devices	Objects	Integration		Deploy	۹ 🕯	° ¢	admin 🕶	cisco SECURE
> AAA Server	Extended							Add Ex	tended Acces	s List	Q Filter		
✓ Access List													
Extended	An access list of traffic based on s	oject, also known source and destir	as an acces nation addre	s control list s and ports	(ACL), select Supports IPv	s the traffic to 4 and IPv6 ad	which a service will ap dresses. You use these	pply. Standard-Ider e objects when con	ntifies traffic ba ifiguring partic	ased on d ular featu	estination a res, such a	address only. s route maps	Identifies
Standard													
> Address Pools	Name							Value				Override	
Application Filters	ACL-UNWANTED	D-COUNTRY											/ 🖬 🕅
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									Displaying	1 - 1 of 1	rows I< <	Page 1	of 1 > > C
Delieu Liet													



.FlexConfig نئاك ةفاضإ قوف رقنا .3.1 ةوطخلا

Firewall Manageme	nt Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧳 🌣 🕜 admin 🕶 🖓 SECURE
 > AAA Server > Access List Extended Standard 	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 • 🗄 🔍
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

Flexconfig نﺉاك ةفاضإ .11 ةروصلا

يف مكحتلا ةمئاق جەن نئاك جارداب مق مث FlexConfig نئاكل مسا ةفاضاب مق 3.2 ةوطخلا .ةعسوملا لوصولا يف مكحتلا ةمئاق نئاك < جەن نئاك جاردا < جاردا ددح ،اذەل .(ACL) لوصولا

Firewall Manageme	Name: OBJ-FC-CONTROL-PLANE		@ admin ▼	
> AAA Server ~ Access List	Description:	F	lter	
Standard > Address Pools	Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployn Insert Beployment: Once Type: Append Insert Policy Object Typ Object	•		
Application Filters AS Path Cipher Suite List	Insert System Variable ► Network Insert Secret Key Security Zones	ť	te help of TextObj	∎ α = ∎ α =
Community List Distinguished Name	Standard ACL Object Extended ACL Object		iont) and one incid	En o ⊒
DNS Server Group External Attributes	Route Map	3	outside (PD client	Π α]
File List V FlexConfig ElexConfig	▼ Variables	o	of TextObjects dn	¶∎ α ¶∎ α
Text Object	Name Dimension Default Value Property (Type:Name) Override	Description	es next hop. 2. co	¶a ()
Geolocation Interface	no rectos to aspas	et all a second a se	ers for eigrp. 1. C	¶a Q <u>_</u>
Key Chain Network		21	an AS	唱 Q 唱 Q
> ркі		Cancel	I< < Page 1	of3>>IC

FlexConfig نئاك ريغتم .12 ةروصلا

ةمئاق ددح مث (ACL) لوصولاب مكحتلا ةمئاق نئاك ريغتمل مسا ةفاضإب مق 3.3 ةوطخلا رزلا قوف رقنا ،كلذ دعب ،2.3 ةوطخلا يف اهؤاشنإ مت يتلا ةعسوملا (ACL) لوصولاب مكحتلا ظفح.

Firewall Managemen	Name: OBJ-FC-CONTROL-PLANE	:			⊁ 🕑 admin ▾ 🔤	sco SECURE
AAA Server Access List Extended	Description:	Insert Extended Access List Object Va	iable 🛛 🖓		Filter	
Standard > Address Pools Application Filters AS Path	Copy-pasting any rich	Variable Name: VAR-ACL-UNWANTED-COUNTRY Description:			the help of TextObj	Γ α =
Cipher Suite List Cipher Suite List Distinguished Name DNS Server Group External Attributes File List		Available Objects C Q Search D CL UNMARTED COUNTRY Add	Selected Object		Hent) and one insid a outside (PD client	Ra q = = Ra q = =
✓ FlexConfig FlexConfig Object	▼ Variables Name			ription	ions.	
Text Object Geolocation Interface Key Chain Network			Cancel		Hers for eigrp. 1. C	
> PKI Policy List				Cancel	s I< < Page 1	of 3 > > C*

FlexConfig نئاكل (ACL) لوصولا يف مكحتاا ةمئاق ةلااحإ .13 ةروصلا

ةەجاولل ةدراوك مكحتلا ىوتسم ىلإ لوصولا يف مكحتلا ةمئاق نيوكتب مق ،مث .3.4 ةوطخلا يلي امك ةيجراخلا.

:رماوألا رطس ةغايص

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

الحصولا يف مكحتلا ةمئاق ريغتم مدختسي يذلا ،يلاتال رمألا لاثم ىلإ اذه مجرتي (ACL) لوصولا يف مكحتلا قمئاق ريغتم مدختسي يذلا ،يلاتك (ACL) المائة مي المائي (ACL) المائة عنه معني المائي المائي المائي المائي (ACL) المائة (ACL) المائي المائي المائي المائي المائي المائي المائي المائي (ACL) المائ

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

نئاك ةذفان يف اهب اهنيوكت بجي يتلا ةقيرطلا يه هذه "ظفح" رزلا ددح ،كلذ دعب ،FlexConfig نئاك لذفان يف اهب اهنيوكت بجي يتلا قلياك لامكإل

Firewall Manageme Name: Objects / Object Manageme OBJ-FC-CONTROL-PLANE	admin ▼ admin state cisc	SECURE
> AAA Server Description:	er	
Access List		
Extended A Copy-pasting any rich text might introduce line breaks while generating CLJ. Please verify the CLI before deployment.		
Standard		
> Address Pools		
Application Filters access-group \$VAR-ACL-UNWANTED-COUNTRY in interface outside control-plane the	a help of TextObj	₽ 0, ``
AS Path Cipher Suite List		a ⊂
> Community List		₽ 0,
> Distinguished Name	nt) and one insid	⊑ Q =
DNS Server Group		
> External Attributes b out	utside (PD client	1 C
File List of	TextObjects dn	¶a Q =
YexConfig Variables		
FlexConfig Object Dimension Default Value Property (Type:Name) Override Description	e novt hon 2 co	Bo =
Text Object VAR-ACL-UNWANTED-COUNTRY SINGLE ACL-UNWANTED EXD_ACL-A false	next nop. 2. co	
deolocation ters	rs for eigrp. 1. C	¶a < [™]
Interface 17 as	an AS	¶∎ q =
Key Chain		
Network	K (Prov. I	
> PKI	C Page 1 of	

Flexconfig نﺉاګل لماګلا رماوألا رطس .14 ةروصلا

ا تن النا الن القاني الذي المار الذي المار ال FlexConfig.

Ciperts / Object Management	Center Overview Analysis Policies	Devices Objects	Integration	Deploy Q 🧬	✿ 🕜 admin • │ :१	SECURE
 > AAA Server > Access List Extended Standard 	FlexConfig Object	Device Management Device Upgrade 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	
 Address Pools Application Filters AS Path 	Name	FlexConfig I Certificates	Site to Site Monitoring		he help of TextObj	₽ 0 =
Cipher Suite List > Community List	Default_Insp Default_Insp Default_Insp	pection_Protocol_Disable		Disable Default Inspection. Enable Default Inspection.		唱 Q 唱 Q
 Distinguished Name DNS Server Group 	DHCPv6_Pro	fix_Delegation_Configure		Configure one outside (PD e	client) and one insid	₽ q =
> External Attributes File List	DHCPv6_Pref	IX_Delegation_UnConfigure		Remove configuration of on Configure DNS with the help	e outside (PD client	a a ∎ a
FlexConfig FlexConfig Object	DM	IS_UnConfigure		Remove the DNS configurat	ions.	₽ 0,
Text Object Geolocation	Eigrp_	Interface_Configure		Configures eigrp. 1. Configu	aters for eigrp. 1. C	на с — Па с —
interface Key Chain	Eig	rp_UnConfigure		Clears eigrp configuration fo	or an AS	¶∎ Q 18∎ 0
> PKI	Eign	_onconiguro_Aii		Displaying 1 - 20 of 49 row	s K < Page 1	of 3 > > C



،كب صاخلا FTD ل ەؤاشنإ مت FlexConfig كانە نكي مل اذإ "ديدج جەن" قوف رقنا مث 4.1 ةوطخلا، دوجوملا FlexConfig جەن ريرحتب مق وأ.

þ	Firewall Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	ې 🎝	🕜 admin -	cisco SECURE
													New Policy
F	TexConfig Policy			Status				Last Modified					
						created. Add	a new policy						

FlexConfig ةسايس ءاشنإ .16 ةروصلا

ةمئاق قيبطت ديرت يذلا FTD ددحو ديدجلا FlexConfig جەنل مسا ةفاضإب مق 4.2 ةوطخلا مكحتلا ىوتسمل اەۋاشنإ مت يتلا (ACL) لوصولا يف مكحتلا.

Firewall Management Center	Overview Analysis Policies Devices Objects Integration	Deploy Q 🥩 🌣 🍘 admin 🕶 🖓
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	
	Cancel	Save

FlexConfig ةسايس زامج نييعت .17 ةروصلا

نئاك نع ثحبا ،ىرسىلا ةحوللا نم 4.3 ةوطخلا SlexConfig نئاك نع ثحبا ،ىرسىلا ةحوللا نم 4.3 ةوطخلا فصتنم يف دوجوملا نميألا مەسلا قوف رقنلاب FlexConfig جەن ىلا ەتفاضاب مق مث ،ەالعأ ظفح رزلا قوف رقنا ،كلذ دعب ،ةذفانلا

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 🥩 🌣 🥑 admin 🕶 🔤
FLEXCONFIG-POLICY							You have unsaved changes Preview Config Save Cancel
							Policy Assignments (1)
	Selecte	d Drenend E	levConfige				
Available FlexConfig C FlexConfig Object	# Nam		lexconings		Description		
^							
V User Defined							
BOBJ-FC-CONTROL-PLANE							
✓ System Defined							
Configure							
Default_Inspection_Protocol_Disable							
Protocol_Enable		d Append Fl	exConfias				
Thttp://www.configure							
DHCPv6_Prefix_Delegation_UnConfigure	# Nam	10			Description		
TDNS_Configure	1 ОВЈ	-FC-CONTROL	-PLANE				٩ 🖬
DNS_UnConfigure	Ч						
"i Eigrp_Configure							
"i Eigrp_Interface_Configure							

FlexConfig ةسايس نئاك نييعت .18 ةروصلا

رشن" < "رشن" ىلإ لقتنا ،كلذل ،FTD يف نيوكتلا رييغت رشنل ةعباتملاب مق .5 ةوطخلا مدقتم.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	९ 🧬 🔅	🕜 admin 🕇	cisco SE	CURE
FLEXCONFIG-POLICY								Advanc	ed Deploy	eploy All	ncel
Enter Description						FTD-CONTROL-PLANE		Ready fo	r Deployment	é	
	"à Selecte	ed Prepend f	lexConfigs								
Available FlexConfig Object	# Nar	me			Description						
✓ User Defined											
OBJ-FC-CONTROL-PLANE											
✓ System Defined											
The fault_DNS_Configure						1 device is susiable for deployment					
P Default_Inspection_Protocol_Disable						T device is available for deployment				D2 •9	
Tefault_Inspection_Protocol_Enable	Selecte	ed Append F	lexConfigs								
DHCPv6_Prefix_Delegation_Configure	t No				Description						
DHCPv6_Prefix_Delegation_UnConfigure	" Nat	me			Description						
DNS_Configure	1 OB.	J-FC-CONTROL	-PLANE								۹.
DNS_UnConfigure											
"il Eigrp_Configure											
°i Eigrp_Interface_Configure											
Eigrp_Unconfigure_Ali											

FTD جمانرب يف مدقتملا رشنلا. 19 ةروصلا

، احيحص ءيش لك ناك اذإ .هيلع FlexConfig جەن قيبطت ديرت يذلا FTD ددح مث .5.1 ةوطخلا رشن" قوف رقناف.

P	Fi De	rewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration	I	Deploy Q 🧃	P 🗘	Ø admin ▼	cisco SECURE
1 devi	ice sel	ected Search using device name, user name, type,	group or statu	15								Deploy time: Estin	nate Deploy
		Device	Modified by		Inspect Inte	rruption	Туре	Group	Last Deploy Time	Preview	Stat	us	
~		FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12:05 F	M B.	R	eady for Deployr	nent
•	I	Flex Configuration Template Policy: FLEXCONFIG-POLICY											
https://10	0.88.24	3 5843013/ddd/#ContextExplorer											

FTD رشن ةحص نم ققحتاا .20 ةروصاا

ةعباتمو رشنلا بقعتل اقيلعت فضأ مث ،"رشنلا ديكأت" راطإ رەظيس ،كلذ دعب .5.2 ةوطخلا رشنلا.

Firewall Management Center	Overview	Analysis Policies	Devices Object	s Integration		Deplo	ny Q 🧬	🔅 🕝 admin 🔻 👘	SECURE
1 device selected 1 Q Search using device name, user name, type									
Device	Modified by								
V STD-CONTROL-PLANE	admin				Sep 5	5, 2023 12:05 PM		Ready for Deployment	
Flex Configuration Template Policy: FLEXCONFIG-POLICY		Deployment Confirm	mation		×				
•		You have selected 1 dev	vice to deploy						
		Deployment Notes:							
		You can optionally add	notes about the confi	guration changes					
				Cancel	Deploy				

(FTD) ةعرسلا قىاف لاسرالا جمانرب رشن تاقىلعت .21 ةروصلا

اذإ طقف "رشن" قوف رقنا. FlexConfig تارييغت رشن دنع ريذحت ةلاسر رەظت دق .5.3 ةوطخلا جەنلا نيوكت ةحص نم امامت ادكأتم تنك.



FTD رشنب صاخلا FlexConfig ريذحت .22 ةروصلا

.FTD ل جەنلا رشن حاجن نم دكأت .5.4 ةوطخلا

Ð	Fi De	rewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	, q 🤞	🗘 🕜 adm	in ▼
T	۹	Search using device name, user name, type,	, group or statu	15									Deploy
		Device	Modified by		Inspect Inte	rruption	Туре	Group	Last Deploy Time		Preview	Status	
~		FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12:	05 PM		Completed	
*= •		 Flex Configuration Template Policy: FLEXCONFIG-POLICY 											

FTD جمانرب رشن حجن .23 ةروصلا

تمق اذا وأ كب صاخلاا FTD ل ةديدج (ACL) لوصولاا يف مكحت ةمئاق ءاشنإب تمق اذا .6 ةوطخلا تارييغت نأ زاربا مهملا نمف ،طشن لكشب مادختسالا ديق ةدوجوم مكحت ةمئاق ريرحتب FTD، ب لعفلاب اهؤاشنا مت يتلا تالاصتالا ىلع قبطنت ال اهؤارجا مت يتلا نيوكتلا مق ،كلذ ىلع لوصحلل .ايودي FTD ل ةطشنلا لاصتالا تالواحم حسم ىلا جاتحت ،يلاتلابو .يلي امك ةطشنلا تالاصتالا حسمو FTD ب قصاخلا (CLI) رماوألا رطس ةهجاوب لاصتالاب

نيعم فيضمل IP ناونعل طشنلا لاصتالا حسمل:

> clear conn address 192.168.1.10 all

الله المال المالي المالي المالي المالي المال المال المال المال المال المال المال المال المالي المالي المالي ال

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

IP: نيوانع نم قاطنل ةطشنلا تالاصتالا حسمل

> clear conn address 192.168.1.1-192.168.1.10 all

يوتحملا ناونع رمأ ةياهن يف "all ةيساسألا ةملكلا مادختسإ ةدشب ىصوي :ةظحالم رادج ىلإ ةطشنلا VPN ةكبشل ةمشاغلا ةوقلا لاصتا تالواحم ةلازا ضرفل حضاولا قالطإب ةمشاغلا VPN ةوق موجه ةعيبط موقت امدنع يسيئر لكشب ،نمآلا ةيامحلا .قتباثلا لاصتالا تالواحمل راجفنا

FDM ةطساوب ةرادملا FTD ل مكحتلا ىوتسم ىلإ لوصولا يف مكحتلا ةمئاق نيوكت

ةمئاق نيوكتل (FDM) لوحملا تانايب ةدعاق ةرادا يف متعباتم ىلا جاتحت يذلا ءارجالا وه اذه VPN ةكبشل ةفينعلا ةوقلا تامجه رظحل مكحتلا ىوتسم ىلع (ACL) لوصولا يف مكحتلا تةيجراخلا FTD ةمجاو ىل قدراولا

لوخدلا لجسو HTTPS ربع FDM ب ةصاخلا (GUI) ةيموسرلا مدختسملا ةهجاو حتفا .1 ةوطخلا كب ةصاخلا دامتعالا تانايب مادختساب.



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 ABSOLITELY NO WARRANTY under the terms of "GNU Lesser General Public License, version 2 (C, version 2,1 (C) and version 3 (C)).

FDM ىلإ لوخدلا ليجست ةحفص .24 ةروصلا

:تانئاكلا ىلإ لقتنا ،اذەل .نئاك ةكبش ءاشنإ ىلإ جاتحت .2 ةوطخلا

Firewall Device Manager Monitoring	Policies Objects Device: firepower	> 🖨 Ø ?	admin Administrator
Model Cisco Firepower Threat Defens	Software VDB Intrusion F ie for VMwa 7.2.5-208 353.0 20220511	tule Update Cloud Services High Ava -1540 Not Registered Register Not Con	allability CONFIGURE
roside Net	Vork Cisco Firepower Threat Defense for VMware	MGMT ISP/WAN/Gateway CONSOLE	Internet DNS Server NTP Server Smart License
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

FDM ل ةيسيئرلا تامولعملا ةحول .25 ةروصلا

ديدج ةكبش نئاك ءاشنإل '+' رز ىلع رقنا مث تاكبش ددح ،ىرسيلا ةحوللا نم 2.1. ةوطخلا

Firewall Device Manager	Monitoring Policies Objects Device: firepo	ower		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-10.0.0.0-8	NETWORK 10.0.0/8	3	
	2 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0	0/12	
C UNLS	3 IPv4-Private-192.168.0.0-16	NETWORK 192.168.0.	0.0/16	
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-Privat	tte-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-	
👍 IPSec Proposals		152.100.0.		
Secure Client Profiles				
Sea Identity Sources				
👤 Users				
🞗 Certificates				
🔒 Secret Keys				

نﺉاكلا ءاشﻥإ .26 ةروصلا

ةفاضإب مقو ،نئاكلل ةكبشلا عون ددحو ،ةكبشلا نئاكل مسا ةفاضإب مق .2.2 ةوطخلا ىل اهضفر مزلي يتلا رورملا ةكرح ةقباطمل IP نيوانع قاطن وأ ةكبشلا ناونع وأ IP ناونع FTD. نئاكلا ةكبش لامكإل قفاوم رزلا قوف رقنا مث

ة مشاغلا ةوقلا تامجه رظح ىلإ اەنيوكت مت يتلا نئاكلا ةكبش فدەت ،لاثملا اذه يف قكبشل SPN قكبشل انم قدراولا VPN قكبشل

Firewall Device Manag	er Monitoring Polici	Add Network Object
Object Types ←	Network Obje	Name
C Networks	6 objects	OBJ-NET-UNWANTED-COUNTRY
S Ports	# NAME	defined. User defined Description Actions
 Security Zones Application Filters 	1 IPv4-Private-Al	1e-172.16.0.0-12, IPv4-Private-
C ² URLs	2 IPv4-Private-10	Type
Geolocations	3 IPv4-Private-12	Network Host HQUN Kange
Syslog Servers	4 IPv4-Private-19	192.168.1.0/24
🔏 IKE Policies	5 any-ipv4	e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60
🐴 IPSec Proposals	o any-ipvo	
Secure Client Profiles		CANCEL
Sa Identity Sources		
L Users		
🙊 Certificates		
Secret Keys		

ةكبش نئاك ةفاضإ .27 ةروصلا

،ضرغلا اذهل ،ةعسوم (ACL) لوصولا يف مكحت ةمئاق ءاشنإ ىلإ جاتحت ،كلذ دعب .3 ةوطخلا ايلعلا ةمئاقلا يف "ةادأ" بيوبتلا ةمالع ىلإ لقتنا.

Firewall Device Manager	Monitoring Policies Objects Device: firepow	er	() () () () () () () () () () () () () (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
F 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	10.0.0.0/8	
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	
	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				
Sources				
👤 Users				
🙊 Certificates				
Secret Keys				

زاەجلا تادادعإ ةحفص .28 ةروصلا

.يلي امك مدقتملا نيوكتلا عبرم نم نيوكتلا ضرع ددحو لفسأل ريرمتلاب مق 3.1 ةوطخلا

Firewall Device Manager	Monitoring	Policies Objects Device: fir	epower		admin Administrator Cisco SECURE
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 - Variable) View Configuration	89 DAVS Virtual	Backup and Restore	>	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

FDM مدقتملا نيوكتلا. 29 ةروصلا

اLL نﺉاك ءاشﻥإ رقﻥاو ﺕﺍﻥﺉﺍﻙ < ﻱﻙﺫ اLL ﯼﻝﺇ ﺡﻑﺹﺕ ،ﯼﺭﺱﻱﻝﺍ ﺓﺡﻭﻝﻝﺍ ﻥﻡ ،ﻡﺚ .3.2 ﺓﻭﻃﺦﻝﺍ ﻱﻙﺫ

Firewall Device Manager	Monitoring	Policies	註 Objects	Device: firepower	۵. 🗳		• admin • Administrator	 cisco SECURE
Advanced ← Configuration	Device Summ Objects	iary						
Smart CLI								+
Objects		NAME		туре	DESCRIPTION		ACTIONS	
FlexConfig					There are no Smart CLI objects yet			
FlexConfig Objects					Start by creating the first Smart CLI ob	ject.		
FlexConfig Policy					CREATE SMART CLI OBJECT			
						_		

ةيكذلا (CLI) رماوألا رطس ةمجاو تانئاك .30 ةروصلا

ةمئاق ءاشنإل ةعسوملا (ACL) لوصولا يف مكحتلا ةمئاقل مسا ةفاضإب مق 3.3 ةوطخلا نيوكتب مق مث ،(CLI) رماوألا رطس ةهجاو بلاقل ةلدسنملا ةمئاقلا نم ةعسوملا لوصولا يف هؤاشنإ مت يذلا ةكبشلا نئاك مادختساب ةبولطملا (ACEs) لوصولا يف مكحتلا مئاوق (ACL) لوصولا يف مكحتلا ةمئاق لامكإل قفاوم رزلا قوف رقنا مث ،هالعأ 2.2 ةوطخلا

Firewall Devic	Edit Smart CLI Object	admin	sco SECURE		
Advanced Configuration		Description			
Smart CLI	ACL-UNWANTED-COUNTRY		+		
Objects	Extended Access List		ACTIONS		
FlexConfig	Template	Show disabled	C Reset		
FlexConfig Objects	1 access-list ACL-UNMANTED-COUNTRY extended configure access-list-entry deny ✓				
FlexConfig Policy	3 deny network source [(00)-MET-UNMANTED-COUNTRY ×] destination [may-signed × ~] ○ 4 configure deny port any ~				
	o s deny port source ANY destination ANY o configure logging default				
	○ 7 default log set log-level INFORMATIONAL log-interval	300	_		
		CANCEL	ок		

ةعسوملا (ACL) لوصولا يف مكحتلا ةمئاق ءاشناٍ .31 ةروصلا

لوصولاب مكحتلا ةمئاقل ACE تادحو نم ديزملا ةفاضإ ىلإ ةجاحب تنك اذإ :ةظحالم مث ،يلاحلا ACE راسي قوف سواملا كيرحت لالخ نم كلذب مايقلا كنكميف ،(ACL) نم ديزملا ةفاضإل ةفعاضم ددح مث مهيلع رقنا .رقنلل ةلباق طاقن ثالث رهظتس .(ACE) لوصولا يف مكحتلا تالاخدإ ددجو ىرسېلا ةجوللا ىل لقتنا ،اذەل ،FlexConfig نئاك ءاشنإ ىل جاتحت ،كلذ دعب .4 ةوطخلا FlexConfig تئاك عاشنا قوف رقناو ،FlexConfig تانئاك < FlexConfig

Firewall Device Manager	Monitoring Policies Objects	Device: firepower	S₂ (admin Administrator)	cisco SECURE
Advanced ← Configuration	Device Summary FlexConfig Objects			
Smart CLI			Y Filter	+
Objects	H NAME	DESCRIPTION	ACTIONS	
FlexConfig		There are no FI	lexConfig objects yet.	
FlexConfig Objects		Start by creating th	ie first FlexConfig object.	
FlexConfig Policy		CREATE FL	EXCONFIG OBJECT	

FlexConfig تانئاك .32 ةروصلا

ىلا (ACL) لوصولا يف مكحتلا ةمئاق ءاشنإل FlexConfig نئاكل مسا ةفاضإب مق 4.1 ةوطخلا يلي امك ةيجراخلا ةهجاولل ةدراوك اهنيوكتو مكحتلا يوتسم.

```
:رماوألا رطس ةغايص
```

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

ةعسوملا (ACL) لوصولا يف مكحتلا ةمئاق مدختسي يذلا ،يلاتلا رمألا لاثم ىلإ اذه مجرتي يلي امك 'ACL-UNWANTED-COUNTRY' هالعاً 3.3 ةوطخلا يف اهؤاشنإ مت يتلا

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

رزلا ددح ،كلذ دعب ،FlexConfig نئاك ةذفان يف اهب اهنيوكت بجي يتلا ةقيرطلا يه هذه "مناك لامكإل "قفاوم" FlexConfig.

Firewall Device Ma	nager Monitoring				admin Administrator cisco SECURE
Advanced ←	Device Sur FlexCo	Create FlexConfig Object		Ø X	
Smart CLI		OBJ-FC-CONTROL-PLANE			+
Objects		Description		li.	ICTIONS
FlexConfig		Variables There are no variables yet.			
FlexConfig Objects FlexConfig Policy		Start with adding a new variable.			
		Template	<pre>Control-plane</pre>	C Reset	
		Negate Template A	C Expand	e	
			CANCEL	ок	

FlexConfig نﺉاك ءاشﻥٳ .33 ةروصلا

جەن ىلإ لقتنا .5 ةوطخلا FlexConfig > FlexConfig، جەن ىلإ لقتنا .5 ةوطخلا مالعأ 4.1 ةوطخلا يف مۇاشنإ مت يذلا FlexConfig نئاك ددجو ،'+' رزلا قوف رقناو.

Firewall Device Manager	m () () () () () () () () () () () () ()	O₂ (♣) (∅) (?) : admin Administrator ∨	cisco SECURE
Advanced ← Configuration	Device Summary FlexConfig Policy		
Smart CLI	Group List	Preview	<> Expand
Objects	★ Eller	There is nothing to preview yet.	
FlexConfig	OBJ-FC-CONTROL-PLANE		
FlexConfig Objects	Create new FlexConfig Object CANCEL OK		
FlexConfig Policy			
	SAVE		

FlexConfig ةسايس .34 ةروصلا

يف مكحتلا ةمئاقل حيحصلا نيوكتلا ضرعت FlexConfig ةنياعم نأ نم ققحت .5.1 ةوطخلا ظفحلا رز ىلع رقناو اهؤاشنإ مت يتلا (ACL) لوصولا

Firewall Device Manager	Monitoring Policies Objects Device: firepower	() admin Administrator
Advanced ← Configuration	Device Summary FlexConfig Policy	
Smart CLI	Group List	Preview (> Expand
Objects	* OBJ-FC-CONTROL-PLANE	1 access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
FlexConfig		
FlexConfig Objects		
FlexConfig Policy		
	SAVE	

FlexConfig ةسايس ةنياعم .35 ةروصلا

ةوطخلاا تامجه دض هتيامح ديرت يذلا FTD ىلإ نيوكتلا تارييغت رشنب مق .6 ةوطخلا نم ققحتو ،ايلعلا ةمئاقلا يف رشنلا رز قوف رقنا ،ببسلا اذهلو ،VPN ةكبشل ةيشحولا "نآلا رشن" قوف رقنا مث ،اهرشن متيس يتلا نيوكتلا تارييغت ةحص.

Firewall Device Manager		Nistrator v dividi
Advanced ←	Pending Changes	• ×
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 C LEGEND
Objects	Network Object Added: OBJ-NET-UNWANTED-COUNTRY	
	-	subType: Network C> Expand value: 2.2.2.0/24
FlexConfig	-	isSystemDefined: false in interface outside
FlexConfig Objects		description: name: 08J-NET-URNANTED-COUNTRY
FlexConfig Policy		
	FlexConfig Policy Edited: default-group	
	flexConfigObjects:	ORD TO CONTROL DUANE
	-	UDJ-FC-CURINUC-FLARE
	Extended Access List Added: ACL-UNWANTED-COUNTRY	
	-	entries[0].logging: DEFAULT
	-	entries[0].action: DENY
	entries[0].sourceNetworks:	
		ORT NET IBMANTED FOUNTEV
	MORE ACTIONS Y	CANCEL DEPLOY NOW Y

قلعملا رشنلا. 36 ةروصلا

جەنلا رشن حاجن نم ققحت .6.1 ةوطخلا.



حاجنب رشنلا مت .37 ةروصلا

تمق اذا وأ كب صاخلاا FTD ل ةديدج (ACL) لوصولاا يف مكحت ةمئاق ءاشنإب تمق اذا .7 ةوطخلا تارييغت نأ زاربا مهملا نمف ،طشن لكشب مادختسالا ديق ةدوجوم مكحت ةمئاق ريرحتب FTD، ب لعفلاب اهؤاشنا مت يتلا تالاصتالا ىلع قبطنت ال اهؤارجا مت يتلا نيوكتلا مق ،كلذ ىلع لوصحلل .ايودي FTD ل ةطشنلا لاصتالا تالواحم حسم ىلإ جاتحت ،يلاتلابو .يلي امك ةطشنلا تالاصتالا حسمو FTD ب قصاخلا (CLI) رماوألا رطس ةهجاوب لاصتالاب

نيعم فيضمل IP ناونعل طشنلا لاصتالا حسمل:

> clear conn address 192.168.1.10 all

اەلمكأب ةيعرف ةكبشل ةطشنلا تالاصتالا حسمل:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

IP: نيوانع نم قاطنل ةطشنلا تالاصتالا حسمل

> clear conn address 192.168.1.1-192.168.1.10 all

ىوتحملا ناونع رمأ ةياهن يف "all ةيساسألا ةملكلا مادختسإ ةدشب ىصوي :ةظحالم 📎 رادج ىلإ ةطشنلا VPN ةكبشل ةمشاغلا ةوقلا لاصتا تالواحم ةلازإ ضرفل حضاولا قالطإب ةمشاغلا VPN ةوق موجه ةعيبط موقت امدنع يسيئر لكشب ،نمآلا ةيامحلا CLI مادختساب ASA ل مكحتلا ىوتسم ىلإ لوصولا يف مكحتلا ةمئاق نيوكت

مكحتلا ةمئاق نيوكتل ASA (CLI) رماوأ رطس ةمجاو يف متعباتم ىلإ جاتحت يذلا ءارجإلاا وه اذه ىلإ ةدراولا VPN ةكبشل ةيشحولا ةوقلا تامجه رظحل مكحتلا ىوتسمل (ACL) لوصولا يف :ةيجراخلا ةمجاولا

asa# configure terminal

ناونع رظحل ةعسوم (ACL) لوصولاا يف مكحت ةمئاق نيوكتل يلاتلا رمألا مدختسأ .2 ةوطخلا IP ىلإ اهرظح مزلي يتلا رورملا ةكرحل ةكبشلا ناونع وأ فيضملل IP

- لائم الائم ي الثمرا الذه يف - ACL" ىمست ةديدج (ACL) لوصولاا يف مكحت ةمئاق ءاشنإ كنكمي ،لائملا اذه يف UNWANTED-Country لائدإ يدؤيسو "ACE قمشاغلا الم المائية المرابية المرابية المرابية المرابية المرابية المرابية ال قكبشل

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

ريغ" (ACL) لوصولا يف مكحتلا ةمئاق نيوكتل access-group يلاتلا رمألا مدختسأ .3 ةوطخلا ASA ةهجاول مكحتلا ىوتسم ىلإ (ACL) لوصولا يف مكحتلا ةمئاقك "country-اهيف بوغرملا ةيجراخلا.

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

ةمئاق ريرحتب تمق اذإ وأ ةديدج (ACL) لوصولاا يف مكحت ةمئاق ءاشنإب تمق اذإ .4 ةوطخلا مت يتلا نيوكتلا تارييغت نأ زاربإ مهملا نمف ،طشن لكشب مادختسالا ديق ةمئاق ةمئاق ةجاحب تنأف ،يلاتلابو ،ASA ىلإ لعفلاب اهؤاشنإ مت يتلا تالاصتالا ىلع قبطنت ال اهؤارجإ قطشنلا تالاصتالا حسما ،ببسلا اذهل .ASA ىلإ ايودي طشنلا لاصتالا تالواحم حسم ىلإ مك

نيعم فيضمل IP ناونعل طشنلا لاصتالا حسمل:

asa# clear conn address 192.168.1.10 all

اهلمكأب ةيعرف ةكبشل ةطشنلا تالاصتالا حسمل

asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all

IP: نيوانع نم قاطنل ةطشنلا تالاصتالا حسمل

asa# clear conn address 192.168.1.1-192.168.1.10 all

♦ يوتحملا ناونع رمأ ةياهن يف "all ةيساسألا ةملكلا مادختسإ ةدشب يصوي :ةظحالم رادج ىلإ ةطشنلا VPN ةكبشل ةمشاغلا ةوقلا لاصتا تالواحم ةلازا ضرفل حضاولا قالطإب ةمشاغلا VPN ةوق موجه ةعيبط موقت امدنع يسيئر لكشب ،نمآلا ةيامحلا . ةتباثلا لاصتالا تالواحمل راجفنا

'shun' رمألا مادختساب نمآلا ةيامحلا رادجل تامجهلا رظحل ليدب نيوكت

بنجت" رمألا مادختسإ كنكمي ،نمآلا ةيامحلا رادجل تامجهلا رظحل يروف رايخ دوجو ةلاح يف". مجاهم فيضم نم تالاصتالا رظح رمألا اذه كل حيتي.

- اناونع نم ةيلبقتسملا تالاصتالا عيمج طاقسإ كلذ دعب متي ،IP ناونع بنجت درجمب IP ناونع بنجت درجمب IP ناونع بنجت درجمب ايودي رظحلا ةفيظو ةلازا متت ىتح اهليجستو ردصملا.

ددحملا فيضملا ناونعب لاصتا ناك ءاوس رمألا اذهب ةصاخلا رظحلا ةفيظو قيبطت متي -ال مأ ايلاح اطشن.

طاقسإب موقت تنأف ،لوكوتوربلاو ةەجولاو ردصملا ذفانمو ةەجولا ناونع ديدحتب تمق اذإ -IP نم ةيلبقتسملا تالاصتالا عيمج ىلع ةراشإ عضو ىلإ ةفاضإلاب ةقباطملا لاصتا ردصملا

قباطت يتلا كلت طقف سيلو ،ةيلبقتسملا تالاصتالا عيمج بنجت متي ،ناونعلا ەذە ةددحملا لاصتالا تاملعم.

.ردصملل IP ناونع لڬل طقف OneConnectCommand ىلع لوصحلا ڬنڬمي -

- نيوكت يف مضرع متي ال منإف ،يكيمانيد لكشب تامجەلا رظحل ەمادختسإ متي رمألا نأل عافدلا زامجل ديدەتلا.

. ةەجاولا كلتب ةلصتملا تارايخلا عيمج ةلازا اضيأ متت ،ةەجاو نيوكت ةلازا دنع -

:بنجت رمأ ةغايص -

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

: رمألاا اذه نم no ةغيصلا مدختساً ،ام ةلاسر ليطعتل -

no shun source_ip [vlan vlan_id]

ىلات مل اذه يف .نمآلا ةيامحلا رادجل يلاتل وحنلا ولا عل مت ما مث ،فيضم IP ناونع بنجتل، رمألا مادختسإ متي IP ناونع نم ةدراولا VPN ةكبشل ةمشاغلا ةوقلا تامجه رظحل 'shun' رمألا مادختسا متي ان مان 192.168.1.10.

. FTD ل نيوكتلا لاثم

رمأ قيبطتب مقو (CLI) رماوألا رطس ةهجاو ربع FTD ىلإ لوخدلا ليجستب مق .1 ةوطخلا يلي امك لهاجتلا.

<#root>

>

shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

يف ةمدختسملا ريغ IP نيوانع ديكأتل ةيلاتلا ضرعلا رماوأ مادختسإ كنكمي .2 ةوطخلا FTD يف ةمدختسمل اي المي التي FTD ي ناونع لكل ةمدختسملا ريغ لوصولا تارم ددع ةبقارمو

<#root>
>
show shun
shun (outside) 192.168.1.10 0.0.0.0 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 ل نيوكتلا لاثم

.يلي امك ةنعللا رمأ قبطو CLI ربع ASA ىلإ لوخدلا لجس .1 ةوطخلا

<#root>

asa# shun 192.168.1.10 Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

ا نيوانع ديكأتل ةيلات ال مرعل ارماوأ مادختسإ كنكمي .2 ةوطخلا ASA يف ةمدختسملا ريغ IP نيوانع ديكأتل ASA يف ةمدختسمل اريغ لوصول تارم ددع ةبقارمو ناونع لكل ةمدختسملا ريغ لوصولا تارم ددع ةبقارمو

<#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)

ا عجرم عجار ،"نمآلا ةيامحلا رادج بنجت" رمألا لوح تامولعملا نم ديزم ىلع لوصحلل :ةظحالم <u>عجرم</u> عجار ،"نمآلا ةيامحلا رادج بنجت" رمألا لوح تامولعمل مقال الم ديزم ي العام الم الم عاف الم الم

ةحصلا نم ققحتلا

بسانملا عضولا يف مكحتلا ىوتسم ىلإ (ACL) لوصولا يف مكحتلا ةمئاق نيوكت ديكأتل يلاتك وحنلا ىلع ةعباتملاب مق مث ،نمآلا ةيامحلا رادجل:

ليغشتب مقو (CLI) رماوألا رطس ةهجاو ربع نمآلا ةيامحلا رادج ىلإ لوخدلا لجس .1 ةوطخلا ىوتسم ىلإ (ACL) لوصولا يف مكحتلا ةمئاق نيوكت قيبطت ديكأتل ةيلاتلا رماوألا مكحتلا

:FMC ةطساوب هترادإ متت FTD ل جارخإ لااثم

<#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 ةطساوب هترادإ متت يذلا FTD ل جارخإ لااثم

<#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: ل جارخإلا لااثم
```

<#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

رظحب موقت يتلا مكحتلا ىوتسم ىلع (ACL) لوصولا يف مكحتلا ةمئاق ديكأتل .2 ةوطخلا ةمجاولا ىلإ دراولا TCP 443 لاصتا ةاكاحمل packet-tracer رمألا مدختسأ ،ةبولطملا رورملا ةكرح ددع ةدايز بجي ، <show access-list <acl-name رمألا مادختسإ مث ،نمآلا ةيامحلا رادجل ةيجراخلا VPN ةوق لاصتا رظح اهيف متي ةرم لك يف (ACL) لوصولا يف مكحتلا ةمئاق لوصو تارم (ACL) لوصولا ي ف مكحتلا قمئاق قطساوب نمآلا ةيامحلا رادجب ةيئاوشعلا

نم هيلع لوصحلا مت مداق TCP 443 لاصتا ةاكاحمب packet-tracer رمألا موقي ،لاثملاا اذه يف -انب صاخلا نمآلا ةيامحلا رادجل يجراخلا IP ناونع ىل ٍ ههيجوت متيو 192.168.1.10 فيضملا. تادايز 'show access-list' جارخاٍ ضرعيو اهطاقساٍ متي يتلا رورملا ةكرح 'packet-trace' جارخاٍ دكؤي :ةدوجوملا مكحتلا يوتسمل (ACL) لوصولا يف مكحتلا ةمئاقل لوصولا تارم ددع

FTD ل جارخإ لاثم

<#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 ل جارخإ لاثم

<#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

```
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



يف Cisco نم نمآلا ليمعلاب ةصاخلا VPN ةكبش لثم RAPN لح ذيفنت مت اذإ :ةظحالم 🛇 نمآلا ةيامحلا رادج ةيقيقح لاصتا ةلواحم ءارجإ ذئنيح نكميف ،نمآلا ةيامحلا رادج ةكرح رظحل عقوتم وه امك مكحتلا ىوتسمل لوصولا يف مكحتلا ةمئاق لمع ديكأتل ةبولطملا رورملا.

ةلصلا تاذ ءاطخألا

حيحصت فرعم :يفارغجلا عقوملا ىلإ ةدنتسملا AnyConnect ليمع تالاصتإ | هنإ • Cisco <u>CSCvs65322</u> نم ءاطخألا

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما