FDM ربع اەرابتخاو AMP فلم ةسايس نيوكت

تايوتحملا

<u>مردق مل ا</u>
<u>قيساس أل ا تابل طتمل ا</u>
<u>تابلطتملا</u>
<u>ةمدختسملاً تانوكملاً</u>
<u>تاميل عت</u>
<u>مىيخرىتا،</u>
<u>ان کې وګټل ا</u>
الت الم
<u>امحال صاو ءاطخاًل ا فاش كتس ا</u>

ةمدقملا

ةراضلا جماربلا نم ةمدقتملا ةيامحلا" فلم ةسايس نيوكت ةيفيك دنتسملا اذه حضوي" (AMP) جمانرب ربع اهرابتخاو (Firepower Device Manager (FDM).

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- زاهج ريدم Firepower (FDM)
- Firepower Threat Defense (FTD)

ةمدختسملا تانوكملا

- FDM لالخ نم رادملا Cisco نم 7.0 رادصإلا يرهاظاا FTD جمانرب •
- ل ثمت .يحيضوتلا ضرعلا ضارغأل مييقتلا صيخرت مدختسي) مييقتلا صيخرت (همادختساو حلاص صيخرت ىلع لوصحلا يف Cisco ةيصوت

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

تاميلعت

صيخرتلا

مدختسملا ةهجاو ىلع زاهجلا ةحفص ىلإ لقتنا ،ةراضلا جماربلا صيخرت نيكمتل .1

.FDM ل (GUI) ةيموسرلا

CISCO, Firepower Device Manager MONITORING POLICIES OBJECTS DEVICE: FTD

```
FDM زاهج ٻيوٻت ةمالع
```

.نيوكتلا ضرع قوف رقناو Smart License ىمسملا عبرملا ناكم ددح .2

Interface 2 Connected 7 Enabled	7 9 >	Routing 1 route View Configuration	>	Updates Geolocation, Rule, VDB, System Upg Security Intelligence Feeds View Configuration	rade,	System Settings Management Access Logging Settings DHCP Server DNS Server Management laterface	
Smart License Evaluation expires in 89 days	89 DAYS	Backup and Restore		Troubleshoot No files created yet		Hostname NTP Cloud Services	
View Configuration	>	View Configuration	>	REQUEST FILE TO BE CREATED		Traffic Settings URL Filtering Preferences	
Site to Site VPN There are no connections yet		Remote Access VPN Requires RA VPN license No connections 1 Group Policy		Advanced Configuration Includes: FlexConfig, Smart CLI		Device Administration Audit Events, Deployment History, Download Configuration	
/iew Configuration	>	View Configuration	>	View Configuration	>	View Configuration	>

FDM زاہج ۃحفص

.ةراضلا جماربلا ىمسملا صيخرتلا نيكمتب مق

and a second s		Lot of Abbe L
Enabled		
This License allows you Firepower and AMP Thr and block malware in fil	to perform Cisco Advanced Malwar eat Grid. You must have this license es transmitted over your network.	e Protection (AMP) with AMP for to apply file policies that detect
Includes: C File Policy		
• • • • •		

نيوكتلا

.FDM يف تاسايسلا ةحفص ىلإ لقتنا .1

ıı ıı ıı cısco∝	Firepower Device Manager	MONITORING	POLICIES	OBJECTS	DEVICE: FTD	

. لوصولا يف مكحتال مسق ىلإ لقتنا ،نامألا تاسايس تحت.



FDM ىلإ لوصولا يف مكحتلا بيوبت ةمالع

Manage	er MON	IITORING	POLICIES	OBJECTS	DEVICE: FTD				⊙ (e 🕒) adr Ad	nin ministrator	@ ~
Ø (Security Pol	icies											
-	$b \rightarrow O SSL$	Decryptior	$n \rightarrow \bigcirc$ Ident	tity $ ightarrow$ 🖌 Se	curity Intelligence	ightarrow Nat	→ 🖌 Access	Control $ ightarrow$	Intrusion				
5 rule	s							Q Search				0	+
			SOURCE			DESTINATION							
	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS		ACTIONS
>	1 Inside_Outside	→ Allow	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	G D	C C

FDM ىلإ لوصولا يف مكحتاا ةدعاق

نم لضفملا فلملا جەن رايخلا ددحو لوصولا ةدعاق يف فلملا جەن مسق قوف رقنا .4 .ةدعاقلا ىلع اەۋارچا مت يتلا تارييغتلا ظفحل قفاوم قوف رقنا .ةلدسنملا ةمئاقلا

Edit Access Rule	0 ×
Order Title Action 1 Inside_Outside_Rule Image: All state of the	n Policy ^① File policy ^① Logging
Evaluation Period This feature needs a license to be purchased. For more details, go to Smart License. SELECT THE FILE POLICY Block Malware All None Block Malware All Cloud Lookup All Block Office Document and PDF Upload, Block Malware Others Block Office Documents Upload, Block Malware Others	CONTROLLING FLES AND MALWARE Use file policies to detect malicious software, or malware, using Advanced Balware Protection for Firepower (AMP for Firepower.) You can also use file policies to perform file control, which allows control over all files of a specific type regardless of whether the files contain malware
Show Diagram	CANCEL

"FDM ل لوصولاب مكحتال ةدعاق فالم ةسايس" بيوبتالا ةمالع

جەن ةنوقيأ نيكمت نم ققحتلا قيرط نع لوصولا ةدعاق ىلع فلملا جەن قيبطت نم دكأت .5 فلملا.

چەن زەر نىڭەت مت	> 1	Inside_Outside	→ Allow	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	Block Malware All
فلم													

فلملا

.رادملا زاهجلا ىلع تارييغتلا رشنو ظفح .

رابتخإ

تالواحم مدختسأ ،لمعي ةراضلا جماربلا ةيامحل ەنيوكت مت يذلا فلملا جەن نأ نم ققحتلل فيضمب صاخلا بيو ضرعتسم نم راض جمانرب رابتخإ فلم ليزنتل ەذە رابتخالا ويرانيس يئاەن.

نم راض جمانرب رابتخإ فلم ليزنت ةلواحم نإف ،هذه ةشاشلا ةطقل يف ضورعم وه امك ةحجان ريغ بيولا ضرعتسم.

6			Problem loading page — Mozilla Firefox				^ _	• ×
	Problem loading	g page 🛛 🗙	+					\sim
÷	\rightarrow C	③ 10.122.	149.2:8080/eicar/eicar_com.zip	\$	0	\pm	Û	
•	The co • The co • If y • If y to a	CONNEC onnection to a site could b ou are unabliour compute access the we	tion was reset while the page was the server was reset while the page was e temporarily unavailable or too busy. Try again to load any pages, check your computer's netw r or network is protected by a firewall or proxy, r b.	loading. In a few moments. work connection. make sure that Firefox is perm Try Ag	ain			

ضرعتسملا ليزنت رابتخإ

ةطساوب هرظح مت فلملاا ليزنت نأ ماظنلا معد عبتت رهظي ،FTD ل (CLI) رماوأ رطس ةهجاو نم ةهجاو ربع ماظنلا معد عبتت ليغشت ةيفيك لوح تاميلعت ىلع لوصحلل .فلملا ةيلمع ماوألاا رطس (CLI) بماوألا رطس

192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File signature verdict Reject and flags 0x00005A00 for 2546d
cffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad of instance 0
192.168.0.10-40016 > 10.122.149.2-8080 6 File Process: drop /eicar/eicar_com.zip
192.168.0.10-40016 > 10.122.149.2-8080 6 IPS Event: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File malware event for 2546dcffc5ad854d4ddc64fbf056871cd5a00
f2471cb7a5bfd4ac23b6e9eedad named eicar_com.zip with disposition Malware and action Block Malware
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 Archive childs been processed No
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort detect_drop: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 deleting firewall session
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST
192.168.0.10-40016 > 10.122.149.2-8080 6 ===> Blocked by File Process
verdict reason is sent to DAD

ماظنلا معد عبتت رابتخإ

ةراضلا جماربلا رظح يف فلملا جەن نيوكت حاجن دكۇي اذە.

اهحالصإو ءاطخألا فاشكتسا

تاحارتقا ىلٍ عجرا ،ةقباسلا تانيوكتلا مادختساٍ دنع حاجنب ةراضلا جماربلا رظح مدع ةلاح يف ةيلاتلا امحالصاٍو ءاطخاًلا فاشكتساً:

. ةراضلا جماربلا صيخرت ةيحالص ءاەتنا مدع نم ققحتلا

.ةحيحص رورم ةكرح فدهتست لوصولاب مكحتلا ةدعاق نأ نم دكأت .2

ة بولطملا ةيامحلاو ةفدهتسملا رورملا ةكرحل حيحص ددحملا تافلملا جهن رايخ نأ نم دكأت .3 ةراضلا جماربلا نم.

معد ىلع لوصحلل Cisco نم TAC ب لصتاف ،لحلل ةلباق ريغ لازت ال ةلكشملا تناك اذإ يفاضإ.

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