ةيطمنلا ةدحولا نيوكتب مق FirePOWER تافلملا يف مكحتلا وأ AMP ةكبشلل مادختساب

تايوتحملا

مدق ملا مدق ملا مدت من المال المال المال المال متابل ط ملا مدن ملا مدن ملا مدن ملا مدن ملا مرابل المول م مرابل المال المال المال المال المال المال مرابل المال المال المال المال المال المال المال مرابل المال المال المال المال المال المال المال مرابل المال المال المال المال المال المال المال المال المال مرابل المال مرابل المال مالمال المال المال المال المال المال المال المال المال

ةمدقملا

جماربلا نم ةمدقتملا ةيامحلا/تافلملا ىلإ لوصولا يف مكحتلا ةفيظو دنتسملا اذه فصي ريدم مادختساب اهنيوكت ةقيرطو FirePOWER ةيطمنلا ةدحولل (AMP) ةكبشلل قراضلا ميكترل لباقلا نامألا ةزهجأ (ASDM).

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- من الما المال المال المال المال الما من مع ما المع ما المال المال المال المال ASDM.
- FirePOWER ناماً زاهج ةفرعم

ةمدختسملا تانوكملا

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

- اةدحول ASA FirePOWER (ASA 5515-X، ASA 5525-X، ASA 5545-X، ASA 5555-X) مي ط من ل ا

ثدحألا تارادصإلاو جمانربلا نم 6.0.0 رادصإلا لغشت يتلا.

• ASDM 7. 5. 1 ثدحألا تارادصإلاو.

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألا 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 ،ةرشابم كتكبش.

ةيساسأ تامولعم

ةددعتم قرط لالخ نم ةسسؤم ةكبش يف ةراضلا ةراضلا جماربلا/جماربلا لخدت نأ نكمي. تازيم مادختسإ نكمي ،اهفيفختو راضلا جمانربلاو جمانربلا اذه تاريثأت ديدحتل ايرايتخإ هرظحو ةكبشلا يف ةراضلا جماربلاو جماربلا لقن فاشتكال FirePOWER ب ةصاخلا.

تافلملا ليمحت (فشكلا) ةبقارم رايتخإ كنكمي ،تافلملا يف مكحتلا ةفيظو مادختساب جەن ذيفنت نكمي ،لاثملا ليبس ىلع .تافلملا ەذە لقنب حامسلا وأ اەرظح وأ اەليزنتو مدختسملا ةطساوب ذيفنتلل ةلباقلا تافلملا ليزنت عنمي يذلا فلملا

اەتبقارم يف بغرت يتلا تافلملا عاونأ ديدحت كنكمي ،ةكبشلل AMP ةفيظو مادختساب نم فيرعتلا تانايب وأ SHA 256 ةئزجت لاسراو عئاش لكشب ةمدختسملا تالوكوتوربلا ربع ليلحتل Cisco Security Intelligence ةعومجم ىلإ اەسفن تافلملا نم خسن ىتح وأ تافلملا راض وأ فيظن ەنأ ىلع تافلملا ةئزجتل يئاەنلا ريصملا ةباحسلا عجرت .قراضلا جماربلا

نم ءزجك امەمادختساو فلم جەنك FirePOWER ل AMP و تافلملا يف مكحتلا نيوكت نكمي مكحتلا دعاوقب ةطبترملا تافلملا تاسايس موقت .لوصولا يف مكحتلل ماعلا نيوكتلا .دعاوقلا طورشب يفت يتلا ةكبشلا رورم ةكرح صحفب لوصولا يف

مدحو نأ نم دكأت :**قظحالم** FirePOWER وانرب/مكحت/ةيامح صيخرت ىلع يوتحت ASA **نيوكت < نيوكتلا** رتخأ ،صيخارتلا نم ققحتلل .قفيظولا هذه نيوكتل FirePOWER > الصيخرت .

File Control/Network AMP ل فلملا جەن نيوكت

فلملا ىلإ لوصولا يف مكحتلا نيوكت

ح **تاسايسلا < ASDM دنيوكتلا د ASA Firepower Configuration > نيوكتلا رتخاو ASDM يل الوخدل الجس ديدج فلم جەن** راوحلا عبرم رەظي **.تافلمل**ا.

ال ايرايتخإ افصوو امسا لخدأ ASA تارييغت نيزخت رايخ قوف رقنا مث ،ديدجلا جەنلل ايرايتخإ افصوو امسا لخدأ FirePOWER. فلملا جەن ةدعاق ةحفص رەظت.

ASA FirePOWER Configur	Configuration > ASA	FirePOWER Conf	iquration > Policies > Files			
Poinces Poinces Access Control Policy On Intrusion Policy					Compare Policies	New File Policy
SSL	File Policy	New File Po	licy	? ×	ed	
Identity Policy		Name	File_Access_Control		Add a new policy	
Device Management Object Management		Description	Network file Access Control			
Configuration		Store AS	5A FirePOWER Changes	Cancel		

مكحتلا فلملا ةدعاق كحنمت .فلملا جەن ىلا ةدعاق ةفاضإل **فلم ةدعاق ةفاضاٍ** قوف رقنا اثحب ايئوض اەحسم وأ اەرظح وأ اەليجست ديرت يتلا تافلملا عاوناً يف تايوتسملا ددعتم ةراض جمارب نع.

لوكوتوربلا وأ (يضارتفا) **يأ** امإ هنأ ىلع قيبطتلا لوكوتورب ددح **:قيبطتلا لوكوتورب** و MAP و MAT و FTP و HTTP ددملا

ىلإ ادانتسا ليزنت/ليمحت وأ يأ نوكي نأ نكمي .فلملا لقن هاجتإ ددح **:لقنلا هاجتا** SMB و FTP و POP3 و IMAP و HTTP لوكوتوربلا صحف كنكمي .قيبطتلا لوكوتورب **يأ** رايخلا مدختسأ .فلملا ليمحتل (SMB و FTP و SMTP و HTTP) لوكوتوربلاو فلملا ليزنتل نومدختسملا ناك اذإ امع رظنلا ضغب ،ةددعتم قيبطت تالوكوتورب ربع تافلملا فاشتكال .هنوقلتي وأ فلملا نولسري

فشك امإ ءارجإلا نوكيس .فلملا ىلإ لوصولا يف مكحتلا ةفيظول ءارجإلا ديدحت :**ءارجإلا** عنميو ثدحلا دلوي **تافلم** ءارج**إ رظحو** ثدحلا دلوي **فلم** ةيلمع **فشك .تافلملا رظح** وأ **تافلملا لاصتالا طبض ةداعإ** ديدحت ايرايتخإ كنكمي ، **تافلملا رظح** ءارجإلا مادختساب .فلملا لاسرإ لااصتالا ءاهنإل.

هيبنتلا ءاشنإ وأ اهل فلملا رظح ديرت يتلا فلملا عون تائف ددح **:فلملا عون تائف**.

عون رايتخال ةقد رثكأ رايخ تافلملا عاوناً رايخ يطعي .تافلملا عاوناً ددح **:تافلملا عاوناً** ددحملا فلملا.

نيوكتلا ظفحل ASA FirePOWER تارييغت نيزخت رتخأ.

and and an Destand				
Application Protocol	Any	Action X Block Files Y		
Direction of Transfer	Any	▼		
File Type Categories		File Types	Selected File Categories and Types	
Office Documents	20	Search name and description	Category: Multimedia	6
Archive	18	All types in selected Categories	Category: Archive	6
Multimedia	30	Transformer and the second se	Category: Office Documents	6
Executables	11			
PDF files	2	ACCDB (Microsoft Access 2007 file)	1	
Encoded	2	AMF (Advanced Module Format for digita		
	6	AMR (Adaptive Multi-Rate Codec File)		
Graphics	12	ARJ (Compressed archive file)		
Graphics		ASF (Microsoft Windows Media Audio/Vid		
Graphics				
Graphics		BZ (bzip2 compressed archive)		

(AMP) ةكبشلاب ةراضلا جماربلا ةيامح نيوكت

ىل لوخدل لجس ASA Firepower Configuration > الق تن او ASDM حال الحس رەظت يتل ادىدجل فلمل جەن ةشاش ىلع رقنا نآلا. "فلمل جەن" ةحفص رەظت.

رايخلا قوف رقنا مث ،ديدجلا جەنلل ايرايتخإ **افصو**و **امسا** لخدأ Store ASA FirePOWER Changes. فلمل جەن دعاوق ةحفص رەظت.

ASA FirePOWER Configur 🗗 🕴	Configuration > ASA Fire	POWER Configura	ation > Policies > Files			
Policies Access Control Policy Ontrol Policy Ontrol Policy Files SSL	Default SSL SSL Policy	Policy				
Actions Alerts		New File Policy ? ×			<u>10</u>	
DNS Policy					Compare Policies	O New File Policy
Device Management	Eile Deliev	Name	Network_Malware_Protection	- 1		
Object Management		Description	Network AMP			
	File_Access_Contro			39:	53	2 🗅 A
Information Time	Network file Access C	Store AS	A FirePOWER Changes Can	cel		

تافلملا ةدعاق كحنمت .فلملا جەنل ةدعاق ةفاضإل **فلم ةدعاق ةفاضإ** رايخ قوف رقنا امحسم وأ اەرظح وأ اەليجست ديرت يتلا تافلملا عاوناً يف تايوتسملا ددعتم مكحتلا ةراض جمارب نع اثحب ايئوض.

و IMAP و SMTP و HTTP) ددحم لوكوتورب وأ (يضارتفا) لوكوتورب يأ ددح **:قيبطتلا لوكوتورب** و FTP و FOP3 و SMB

ىلإ ادانتسا ليزنت /ليمحت وأ يأ نوكي نأ نكمي .فلملا لقن هاجتإ ددح **:لقنلا هاجتا** SMB و FTP و POP3 و HTTP لولاوتوربلا صحف كنكمي .قيبطتلا لوكوتورب **يأ** مدختسأ .تافلملا ليمحتل (SMB و FTP و SMTP و HTTP) لوكوتوربلاو تافلملا ليزنتل نيمدختسملا نع رظنلا ضغب ،ةددعتم قيبطت تالوكوتورب ربع تافلملا فاشتكال رايخ .هلابقتسإ وأ فلملا لاسراب نوموقي نيذلا

نع ثحبلا امإ ءارجإلا نوكي ،ةكبشلاب ةراضلا جماربلا ةيامح ةفيظول ةبسنلاب :**ءارجإلا** ةراضلا جماربلا ةباحس نع ثحبلا جتني .ةراضلا جماربلا رظح وأ ةراضلا جماربلا قعومجم ةفاضإلاب ثدحلا ءاشنإب موقت ءارجإلاا **ةلتكل ةراضلا جماربلا** نأ نيح يف طقف اثدح ءارجإلل ةراضلا جماربلا فلم لاسرا رظح يلإ.

ل ةراضلا جماربلل رظحلا دعاوقو ةراضلا جماربلا ةعومجم نع ثحبلا حمسي :ةظحالم Firepower ديدحتل ءارظنلا ةعومجم يف ثحبلا ةيلمعل اهلاسراو SHA-256 ةئزجت باسحب قراض جمارب ىلع يوتحت ةكبشلا زاتجت يتلا تافلملا تناك اذإ ام.

ةددحملا فلملا تائف ددح **:فلملا عون تائف**.

.تايوتسملا ةددعتم تافلملا عاوناً نم ديزمل ةددحملا **تافلملا عاوناً** ددح **:تافلملا عاوناً**

نيوكتلا ظفحل ASA FirePOWER تارييغت نيزخت رايخ رتخأ.

pplication Protocol	Any	Action 🍀 Block Malware 💌		
irection of Transfer	Any	▼		
le Type Categories	16	File Types	Selected File Categories and Type	es
Archive	17		Category: Executables	8
Multimedia	2	All types in selected Categories	Category: Archive	8
Executables	7	TZ (7-Zip compressed file)	() =====	
PDF files	1	ARJ (Compressed archive file)		
Encoded	0	BINARY_DATA (Universal Binary/Java By		
	0	BINHEX (Macintosh BinHex 4 Compresse		
Graphics	2	BZ (bzip2 compressed archive)		
Graphics System files		CPIO_CRC (Archive created with the cpio		
Graphics		COTO NEWS (Anching second with the sec		
Graphics System files		CPIO_NEWC (Archive created with the cr		

يطعي :يلاتلا ءارجإلاا-ةدعاقلا بيترتب تافلملا تافلملا تافلملا جەن جلاعت :**قظحالم** فشكلا درجم ىلع ةيقبسألا يطعي امم ،ةراضلا جماربلا صحف ىلع ةيولوألا رظحلا ليجستلاو.

، (AMP) ةكبشلا ىلا قدنتسملا قراضلا جماربلا نم قمدقتملا قيامحلا نيوكتب تمق اذا قفاضإ كنكميف ،حيحص ريغ لكشب فلملل يئاهنلا ريصملا فاشتكاب Cisco Cloud مايقو ريصملا فاشتكا نيسحتل SHA-256 قئزجت قميق مادختساب تافلملا قمئاق ىلإ فلملا :يلي امب مايقلا كنكمي ،تافلملا قمئاق عون بسح .لبقتسملا يف تافلملل يئاهنلا

- ىلٍ فلملا ةفاضإب مق ،فيظن يئاەن ريصم ددحت ةباحسلا تناك ول امك فلم ةلماعمل .ةفيظنلا ةمئاقلا
- ىلٍ فلملا ةفاضإب مق ،راض جمانرب ةيصاخ ددحت ةباحسلا تناك ول امك فلم ةلماعمل ةصصخملا ةمئاقلاً.

ن**يوكتل > ASA FirePOWER Configuration > Object Management >** File List ةفاضإل ةمئاقلار ريرحتو SHA-256.



فلملا جەنل لوصولاب مكحتلا جەن نيوكت

ي**ف مكحتلا ةسايس < تاسايسلا > ASA Firepower Configuration > نيوكتلا** ىلإ لقتنا حضوم وه امك ،ةدوجوملا **لوصولا ةدعاق** ريرجت وأ ةديدج **لوصو ةدعاق** امإ ءاشنإب مقو **،لوصولا** ةروصلا هذه يف.

جەن ددحو ،**صحف** بيوبتلا ةمالع ىلإ لقتنا .**حمسي** ءارجإلا نوكي نأ بجي ،فلملا جەن نيوكتل ةلدسنملا ةمئاقلا نم **فلملا**.

لجسلا تافلمو ليجست رايخلا ددجو ،**ليجستلا** رايخ ىلا لقتنا ،ليجستلا نيكمتل نيوكتلا ظفحل **قفاض|/ظفح** رز قوف رقنا .بسانملا.

.ددرتملا رايتلا ةسايس تارييغت ظفحل ASA FirePOWER تارييغت نيزخت رايخ رتخاً

nfiguration > ASA FirePOWER Configuration > Policies > Access Control Policy	б
ASA FirePOWER	
Default Allow All Traffic	Ê
Add Rule	
Name Network-AMP Imsert Below rule Imsert Action Allow IPS: no policies Variables: n/a Files: Network_Malware_Pro Logging: files: Event Viewer	
Zones Networks 🔺 Users Applications Ports URLs 🔺 ISE Attributes Inspection Logging C	Comn
Intrusion Policy Variable Set	
None Default Set	
File Policy	_

رشنلا ىلإ لوصولاب مكحتلا ةسايس

ا .ةلدسنملا ةمئاقلا نم **FirePOWER رييغت رايخ رشن** رتخاو ،ASDM ل **رشنلا** رايخ ىلإ لقتنا. تاريغتار رشنل **رشنلا** رايخ قوف رقنا.

Copley Policies Version 2016 01 07 11/57 AM	
Depiloy Policies Version:2010-01-07 11:57 AM	
Access Control Policy: Default Allow All Traffic	
🖸 Intrusion Policy: Balanced Security and Connectivity	
ວ Intrusion Policy: No Rules Active	
Intrusion Policy: IPS_Policy	
DNS Policy: Default DNS Policy	
ວ System Policy: Default	
D Sensor Policy: firepower	

ةمەملا لامكا نم دكأت **.ةمەملا ةلاح < ASA FirePOWER ةبقارم < ةبقارملا</mark> ىلإ لقتنا نيوكتلا رييغت قيبطتل.**

رادصإلا يف :**قظحالم** 5.4.x، رعشتسملا ىلع لوصولا ةسايس قيبطتل مايي 5.4.x رادصإلا يف تارييغت قيبطت قوف ASA FirePOWER.

فلملا جەن ثادحأل لاصتالا ةبقارم

،فلملا جەنب ةطبترملا ةيطمنلا FirePOWER ةدحو ةطساوب اەۋاشنا مت يتلا ثادحألا ضرعل **يلعفلا تقولا يف قيقدتلا < ASA FirePOWER مبقارم < <mark>ةبقارملا</mark> ىلا لقتنا.**

Eventing							
All ASA FirePOWER Even	nts Connection Intru	usion File Malware File	Security Intelligence				
er							
Reason=File Monitor 🗱							
Refresh R	Rate 5 seconds	* 1/7/16 12:06:30) PM (IST)	•			1
Dessitive Timese							
Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP	
1/6/16 1:29:48 PM	Action	First Packet 1/6/16 11:38:29 AM	Last Packet 1/6/16 1:26:46 PM	Reason File Monitor	Initiator IP 192.168.20.3	Responder IP 10.76.76.160	
1/6/16 1:29:48 PM 1/6/16 2:21:23 AM	Action Allow Allow	First Packet 1/6/16 11:38:29 AM 1/6/16 2:16:47 AM	Last Packet 1/6/16 1:26:46 PM 1/6/16 2:18:21 AM	Reason File Monitor File Monitor	Initiator IP 192.168.20.3 192.168.20.3	Responder IP 10.76.76.160 13.107.4.50	
1/6/16 1:29:48 PM 1/6/16 2:21:23 AM 1/5/16 9:22:57 PM	Action Allow Allow Allow	First Packet 1/6/16 11:38:29 AM 1/6/16 2:16:47 AM 1/5/16 9:16:21 PM	Last Packet 1/6/16 1:26:46 PM 1/6/16 2:18:21 AM 1/5/16 9:22:56 PM	Reason File Monitor File Monitor File Monitor	Initiator IP 192.168.20.3 192.168.20.3 192.168.20.3	Responder IP 10.76.76.160 13.107.4.50 46.43.34.31	
1/6/16 1:29:48 PM 1/6/16 2:21:23 AM 1/5/16 9:22:57 PM 1/5/16 9:21:27 PM	Action Allow Allow Allow Allow	First Packet 1/6/16 11:38:29 AM 1/6/16 2:16:47 AM 1/5/16 9:16:21 PM 1/5/16 9:15:15 PM	Last Packet 1/6/16 1:26:46 PM 1/6/16 2:18:21 AM 1/5/16 9:22:56 PM 1/5/16 9:21:26 PM	Reason File Monitor File Monitor File Monitor File Monitor	Initiator IP 192.168.20.3 192.168.20.3 192.168.20.3 192.168.20.3 192.168.20.3	Responder IP 10.76.76.160 13.107.4.50 46.43.34.31 46.43.34.31	

ةحصلا نم ققحتلا

نيوكتلا اذه ةحص نم ققحتلل ءارجإ اًيلاح دجوي ال.

اهحالصإو ءاطخألا فاشكتسا

ا /ءارجإلا /هاجتإلاا /لوكوتوربلا عاوناً عم حيحص لكشب هنيوكت مت فلملا جهن نأ نم دكأت. لوصولا دعاوق يف حيحصلا فلملا جهن نيمضت نم دكأت .تافلملا.

حاجنب لوصولاب مكحتلا جەن رشن لامتكا نم دكأت.

يف حيحصتلا > ASA FirePOWER مبقارم < مبقارملا) تافلملا ثادحأو لاصتالا ثادحأ قبقارم (مل من من من من من من من من م ال ما قحيحصلا ةدعاقلا علام لي لومي رورملا ةكرح قفدت ناك اذإ امم ققحتلل (**يلعفلا تقولا**.

ةلص تاذ تامولعم

• <u>Cisco Systems - تادنتسملاو ينقتلا معدلا</u>

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