# ىلإ ادانتسا دراولا ةيفصتلا لماع نيوكت ESA يف DKIM نم ققحتلا

## ەمدقملا

ىلع ءارجإ يأ ذاختال (ESA) ينورتكلإلا ديربلا نامأ زاهج نيوكت ةيفيك دنتسملا اذه حضوي لماع نيوكت لالخ نم (DKIM) لاجملا حيتافمل فرعملا ينورتكلإلا ديربلا ةحص نم ققحتلا لئاسر ةيفصت لماع وأ دراو ىوتحم ةيفصت

## ةيساسألا تابلطتملا

#### تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- اسإ •
- ىوتحملا ةيفصت لماع نيوكتب ةيساسأ ةفرعم •
- لئاسرلا ةيفصت لماوع نيوكتب ةيساسأ ةفرعم •
- ةصاخلا تالاحلاو تاسوريفلاو تاسايسلل يحصلا رجحلا نيوكت لوح تامولعم ايزكرم ةيشافلاب

#### ةمدختسملا تانوكملا

ةنيعم ةيدام تانوكمو جمارب تارادصإ ىلع دنتسملا اذه رصتقي ال.

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.

## نيوكتلا

#### DKIM نم ققحتلا نيوكت .1 ةوطخلا

.ديربلا قفدت جەن < ديربلا جەن ىلإ لقتنا .DKIM نم ققحتلا نيڭمت نم دكأت

جەنلا تاملعم يف .SPF نم قىقحتلا ەبشى ESA ىلع DKIM نم قىقحتلا نيوكتل .**ىلِ DKIM** نم قىقحتلا ليغشتب مق ةطاسبب ،دىربلا قىفدت جەنل **قيضارتڧالا** 

#### يئاەنلا ءارجإلا نم ققحتلا .2 ةوطخلا

ىلع .ميك ةرادا اەب موقت يتلا ققحتلا ةيلمعل اقفو ەذاختا نيعتي يذلا ءارجإلا ديدحت ،الوأ لزع ءارجا وە يئاەنلا ءارجإلا ناك اذإ .لزع ءارجا وأ ةمالع ةفاضإ وأ طاقسإ :لاثملا ليبس اەنيوكت مت يتلا يحصلا رجحلا تاءارجا عجار ،ديربلل.

• المناقر المرابة المنف المنف المنافع المنافع الما المنافع الما المنافع المالي المنافع المالي المنافع المالي ا

.يشفتلاو تاسوريفلل يحصلا رجحلاو ةسايسلا <ESA >Monitor دا

:(SMA) ةيزكرملا ةرادإلا نيوكتب تمق اذإ •

ىلإ لق⊤نا SMA تاسوريفلل يحصلا رجحلاو ةسايسلا< لئاسرلا لزع< ينورتكلإلا ديربلا< SMA ىل لق⊤نا ةروصلا يف حضوم وه امك ،يشفتلاو:

### **Policy, Virus and Outbreak Quarantines**

Quarantines					
Add Policy Quarantine Search Across Quarantines					
Quarantine Name	Туре	Messages	Default Action	Las	
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release		
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release		
Policy	Centralized Policy	0	Retain 10 days then Delete		
Unclassified	Unclassified	0	Retain 30 days then Release		
Virus	Antivirus	0	Retain 30 days then Delete		
			Available space	for	

دادعإو لاجملا/**DKIM** ىلا قدنتسملا لئاسرلا ةقداصم تامدخل صاخ يحص رجح دوجو مدع ةلاح يف قرياق المار (SPF) قريام الماري المع راطا/(DMARK) قريا المار و

:**جەنلا لزع ةفاضإ** ددح ،يشفتلاو سوريفلاب صاخلا يحصلا رجحلاو جەنلا يف لمعلا ءانثاً

دادعإ كنكمي ،انه:

- ال :يحصل ارجحل مسا ex، DkimQuarantine
- ءارجإلاو كتسسؤم تاجايتحإ ىلع دمتعيو كيلٍ رمألا عجري :ءاقبتسالا ةرتف اهرادصإ وأ اهفذح متيس ينورتكلإلا ديربلا ىلإ ءاقبتسالا ةرتف دعب .يضارتفالا :ةروصلا يف حضوم وه امك ،كب صاخلا ديدحتلا لللخ نم اهديدحت متيو ،اهميلستو

#### **Add Quarantine**

Settings	
Quarantine Name:	
Retention Period:	40 Hours ᅌ
Default Action:	<ul> <li>Delete         <ul> <li>Release</li> </ul> </li> <li>Free up space by applying default action on messages upor Additional options to apply on Release action (when used Modify Subject         <ul> <li>Modify Subject</li> <li>Add X-Header</li> <li>Strip Attachments</li> </ul> </li> </ul>
Local Users:	No users defined.
Externally Authenticated Users:	External authentication is disabled. Go to System Administrat

Cancel

#### ESA ل دراولا ةيفصتلا لماع .3 ةوطخلا

:ESA ل دراو ىوتحم ةيفصت لماع ءاشنإ .أ

لماع <mark>ةفاضا < ةدراولا ىوتحملا ةيفصت لماوع < ديربلا تاسايس < ESA ىل لقتنا ةيفصت.</mark>

:حشرملل **بيترتلاو فصول**او **مسالا** نيوكت كنكمي :لوألا مسقلا •

## **Add Incoming Content Filter**

Content Filter Settings			
Name:			
Currently Used by Policies:	No policies currently use this rule.		
Description:			
Order:	6 ᅌ (of 6)		

عيطتسي تنأو طرش دحاو نم رثكأ ،تفضأ عيطتسي تنأ .طرش ةفاضإ :يناثلا مسقلا • قيقدت DKIM ىلع ءارجإ تذختا in order to حشرم ىوتحم ريثك تلكش ينعملاو ةعقوتملا جئاتنلا - ةقداصملا

ا تارابتحإ يف هلاسرلا تحجن • فقداصملا ءارجإ متي مل :دياحم • لل لباق أطخ ثدح :قرارحلا قجرد • إ نكمي ال أطخ ثدح :رورريمريب • تارابتخإ تلشف :تباث لشف • لاسرلا عيقوت متي مل None. Add Condition	ەقداصمل. دادرتسا. محالص] تقىداصملا ت	
Message Body or Attachment Message Body URL Category URL Reputation	DKIM A Is DKIM Au	uthentication hentication Passed?
Message Size Message Language Macro Detection Attachment Content Attachment File Info Attachment Protection Subject Header Other Header	DKIM Autho	<ul> <li>Pass</li> <li>Neutral (message not signed)</li> <li>Temperror (recoverable error occurred)</li> <li>Permerror (unrecoverable error occurred)</li> <li>Hardfail (authentication tests failed)</li> <li>None (authentication not performed)</li> </ul>
Envelope Sender Envelope Recipient Receiving Listener Remote IP/Hostname Reputation Score DKIM Authentication		

ققحتلا لبق ةلاسرلا عيقوت لسرملا ىلع بجي :DKIM نم ققحتلا تابلطتم : ققحتلل DNS يف حاتم ماع حاتفم ىلع لاسرالا لاجم يوتحي نأ بجي .اهنم.

• الجس لاخدا ةفاضا لثم دحاو ءارجا نم رثكاً ةفاضإ كنكمي .ءارجا ددح :ثلاثلا مسقلا. ،ةلاحلا هذه يف .كلذ ىلا امو ،هيبنتلاو ،ينورتكلالا ديربلا طاقساو ،لزعلا ىلإ لاسراو. :قروصلا يف حضوم وه امك ،اقبسم نوكملا لزعلا ددح

Quarantine	Quarantina
Encrypt on Delivery	Quarantine
Strip Attachment by Content	Flags the message to be held in one of the system quarantine
Strip Attachment by File Info	areas.
Strip Attachment With Macro	Send message to guarantine: 🗸 Armandos Quarantine
URL Category	Policy
URL Reputation	
Add Disclaimer Text	<ul> <li>Duplicate message</li> </ul>
Bypass Outbreak Filter Scanning	Send a copy of the message to the specified quarantine, and
Bypass DKIM Signing	will apply to the original message.
Send Copy (Bcc:)	
Notify	
Change Recipient to	
Send to Alternate Destination Host	
Deliver from IP Interface	
Strip Header	
Add/Edit Header	
Forged Email Detection	
Add Message Tag	
Add Log Entry	
S/MIME Sign/Encrypt on Delivery	
Encrypt and Deliver Now (Final Action)	
S/MIME Sign/Encrypt (Final Action)	
Bounce (Final Action)	
Skip Remaining Content Filters	

ديربلا قفدت جەن ىلإ دىدج ةيڧصت لماع ةڧاضإ:

ثيح ديرب قفدت جەن لك ىلع ةيفصتلا لماع فضأ ESA نم .ةيفصت لماع ءاشنإ درجمب ديربلا جەن< ESA ىلإ لقتنا .يئاەنلا ءارچإلا مادختساب DKIM نم ققحتلا ديرت قروصلا يف حضوم وہ امك ،**دراولا**:

#### **Incoming Mail Policies**

Find Policies								
Email Address:		Recipient     Sender		pient ler	Find Policies			
Policie	Policies							
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	Allow_only_user	(use default)	(use default)	(use default)	(use default)	(use default)	(use default)	Û
2	Tizoncito	(use default)	(use default)	(use default)	(use default)	(use default)	(use default)	ŵ
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Quarantine Virus Positive: Quarantine	Disabled	Not Available	File_Test	Retention Time: Virus: 1 day Other: 4 hours	

**.ديربلا قفدت جەن** فص و **ىوتحملا ةيفصت لماوع** دومع قوف رقنا

 $\boxtimes$ 

جەن تادادعإك ەنيوكت مت ەنأ (يضارتڧالا مادختسإ) ءارجإلا ينعي ال :**قظحالم** ةبولطملا ةيفصتلا لماوع عم ديرب قڧدت جەن لك نيوكتب مق .ةيضارتڧا.

:ESA ل لئاسر ةيفصت لماع ءاشنإ .ب

:تاميلعتلا عبتاو رماوألا **ةيفصت لماوع** لخدأ ESA CLI نم حشرم ةلاسر لك تلكش

```
ESA. com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> NEW
Enter filter script. Enter '.' on its own line to end.
DKIM_Filter:
If (dkim-authentication == "hardfail" )
{
    quarantine("DkimQuarantine");
}
.
1 filters added.
```

.**ةدحاو ةيفصت لماوع ةفاضإ تمت** :حاضيإلا ةليسو عجار ،ةيفصتلا لماع ءاشنإ درجمب

لماع لبق نم ةمدختسملا كلت اهسفن يه اهنيوكت بولطملا تاءارجإلاو طورشلا نوكت. دراولا يوتحملا ةيفصت.

## ةحصلا نم ققحتلا

حيحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا.

دراولا ىوتحملا ةيفصت لماع:

ESA (WebUI) بيو مدختسم ةەجاو نم •

:ةيفصتلا لماع نيوكت نم ققحتلا .أ

لماع نيوكت بجي **.ةدراولا يوتحملا ةيفصت لماوع< ديربلا تاسايس< ESA** يلإ لقتنا .ةضورعملا قمئاقلا يف اقبسم ددحملا بيترتلل اقفو ةيفصتلا

:ةيفصتلا لماع قيبطت نم ققحتلا .ب

.د**راولا ديرٻلا تاسايس< ديرٻلا تاسايس<ESA** يلإ لقتنا

ديربلاا قفدت جەن فصو ىوتحملا ةيفصت لماوع دومع يف ةيفصتلا لماع مسا راەظإ بجي. لماوع ديدحتل تاحشرملا ةمئاق قوف رقنا ،مسالا ةيؤر كنكمي الو ةريبك ةمئاقلا تناك اذإ جەنلا ىلع ةقبطملا ةيفصتلا.

لئاسرلا ةيفصت لماع:

From ESA CLI: ESA. com> filters Choose the operation you want to perform: - NEW - Create a new filter.

```
DELETE - Remove a filter.
IMPORT - Import a filter script from a file.
EXPORT - Export filters to a file
MOVE - Move a filter to a different position.
SET - Set a filter attribute.
LIST - List the filters.
DETAIL - Get detailed information on the filters.
LOGCONFIG - Configure log subscriptions used by filters.
ROLLOVERNOW - Roll over a filter log file.
[]> list
```

Num Active Valid Name

1 y y DKIM\_Filter هطاشنو ةيفصتلا لماع نيوكت مت اذإ ام ةمئاقلا رەظت.

## اهحالصإو ءاطخألا فاشكتسا

اهحالصإو نيوكتلا ءاطخأ فاشكتسال اهمادختسا كنكمي تامولعم مسقلا اذه رفوي.

نيوكتلا نم ققحتلا:

:نم دكأتلا بجي

- ققحتالا دنع :ديربال قفدت جهن ديدجت مت •
- الئاسرلا ةيفصت لماع وأ ىوتحملا ةيفصت لماع يف هنيوكت مت ءارجإ كانه •

ديربلا قفدتب طبترم ةيفصتلا لماع ناً نم ققحت ،ىوتحملا ةيفصت لماع ةلاح يف • لئاسرلا بقعت نم ققحتلاً:

:ةظحالملاب لئاسرلا بقعت انل حمسي

• الأملال ليبس ىلع: DKIM، الأم ققحتال المحيات.

(دحاو نيوكت مت اذإ) ەنيوكت مت يذلا لجسلا لاخدا •

• (ذختملا ءارجإلاو مسالا) قبطملا ةيفصتلا لماع نم عبتت ESA:

```
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 From: <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 RID 0 To: <userb@domainb.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 Message-ID '<3903af$2r@mgt.esa.domain.com>Fri Apr 26
11:33:44 2019 Info: MID 86 DKIM: permfail body hash did not verify [final]
Fri Apr 26 11:33:44 2019 Info: MID 86 Subject "Let's go to camp!"
Fri Apr 26 11:33:44 2019 Info: MID 86 ready 491 bytes from <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 matched all recipients for per-recipient policy
Allow_only_user in the inbound table
Fri Apr 26 11:33:46 2019 Info: MID 86 interim verdict using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 interim AV verdict using Sophos CLEAN
Fri Apr 26 11:33:46 2019 Info: MID 86 antivirus negative
Fri Apr 26 11:33:46 2019 Info: MID 86 AMP file reputation verdict : UNSCANNABLE
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: GRAYMAIL negative
Fri Apr 26 11:33:46 2019 Info: MID 86 Custom Log Entry: The content that was found was:
DkimFilter
Fri Apr 26 11:33:46 2019 Info: MID 86 Outbreak Filters: verdict negative
Fri Apr 26 11:33:46 2019 Info: MID 86 quarantined to "DkimQuarantine" by add-footer filter
'DkimFilter '
```

## ةلص تاذ تامولعم

- <u>ESA-SPF-DKIM-DMARK تاسرامملا لضفأ</u>
- <u>ينورتكل|لا ديربلا نامأ زامجل يئاەنلا مدخَّتُسُملا ليُلد</u> •
- **DKIM RFC4871**
- DKIM RFC8301
- **DKIM RFC8463**
- <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