

# ينورتك لإل دي ربل لئاسر نع فشكلا تاءانثتسا عاشنإو ESA ىلع ةلحتنملا

## تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[ينورتك لإل دي ربل لئاسر لئاحتنا وه ام](#)

[ةلحتنملا ينورتك لإل دي ربل لئاسر فاشتك اة فيك](#)

[نيددحم نيلس رمل لئاحتنا لئاسر لئاحتنا اة فيك](#)

[ننوكتلا](#)

[سوملاق عاشنا](#)

[ةلئاسر ةيفصت لماع عاشنا](#)

[TRUSTED\\_SPOOF\\_HOSTS ىتصنم لئاسر تاءانثتسا اة فاضا](#)

[ةحصلا نم ققحتلا](#)

[ةلحتنملا لئاسر لئاسر نم ققحتلا](#)

[مدختسملا مساعانثتسا لئاسر رمل لئاسر نم ققحتلا](#)

[ةلصت اذ تامولعم](#)

## ةمدقملا

Cisco ESA ىلع ينورتك لإل دي ربل لئاسر نع فشكلا ةلحتنملا اة فيك دننتملا اذ حوضي دي ربل لئاسر لئاسر راب مهل حومسملا نيمدختسملا تاءانثتسا عاشنإ اة فيك و ةلحتنملا ينورتك لإل.

## ةيساسألا تابلطتملا

### تابلطتملا

ةدراولا دي ربل لئاسر نم لك ةجلاعمب (ESA) ينورتك لإل دي ربل لئاسر نامأ زاغ موقى نأ بجي اهراپت عاب لئاسرلا ىلع ةمالع عضول Relaylist نم ىسايق نيوكت مادختساو، ةرداصلاو ةرداص.


### ةمدختسملا تانوكملا

نمضتت ةمدختسملا ةددحملا تانوكملا:

- ةيلخادلا كئالاجم ةفاك نيزختل مدختسي: سوملاقلا
- ينورتك لإل دي ربل لئاسر فاشتكال قطنملا عم لماعتلل مدختسي: لئاسرلا ةيفصت لماع

هليلع لمعللا يوتحمللا ةيفصت لم اولعل نكل مي سأللا لادوا ةلحتنملا

- عض .اتقوم ةلحتنملا ينورتكللالا ديربلا لئاسر تاراركت نيزختل مدختسي :جهنلا لزع ىلا اهرادصا مت يتلا لئاسرلل IP ناووع ةفاضل رابتعالا يف لادوا نم لسرمللا اذو نم ةيلبقتسملا لئاسرلا عنمل MY\_TRUSTED\_SPOOF\_HOSTS جهنلا لزع .
- MY\_TRUSTED\_SPOOF\_HOSTS: اهب قوثلوملا لاسرلل IP نينوانع ىلا ةراشلال ةمئاق . لسرملل حامسلاو لزعلا يطخت ىلا ةمئاقلا هذه ىلا لسرملل IP ناووع ةفاضل يدوت نيلسرمللا ةومجم يف مهب قوثلوملا نيلسرمللا عضو كنكمي . ةفللا ملباب ءالوه نم ةلحتنملا لئاسرلا لزع متي ال ىتح MY\_TRUSTED\_SPOOF\_HOSTS نيلسرمللا .
- Relaylist: لىنورتكللالا ديربلا لئاسرلا وءا ، لىحرلل اهب حومسملا IP نينوانع ةقداصل ةمئاق . رداص نأ ضررت في ، هذه نيلسرمللا ةومجم ربع ينورتكللالا ديربلا ميلست ةلاح يف . رداص . ةلحتنم ةلاسر تسيل ةلاسرلا .

 نعلتخم ءيشب نيلسرمللا يتومجم نم يا ءاعدتسا مت اذا : ةطالم ةيفصتلا لماع لىدعت كىللع بجىف ، RELAYLIST و MY\_TRUSTED\_SPOOF\_HOSTS كىدل نوكتس ف ، نىعمتسم ةدع كىدل ناك اذا ، اضيا . فدارملا نيلسرمللا ةومجم مساب MY\_TRUSTED\_SPOOF\_HOSTS نم دحاو عمتسم نم رثكا

AsyncOS نم رادصا يا عم ESA ىلا دننتسملا اذو يف ةدراولا تامولعملل دننتست

ةصاخ ةيلمعم ةئيبي يف ةدووجلل ءزهجالا نم دننتسملا اذو يف ةدراولا تامولعملل ءاشن مت تناك اذا . (يضا رتفا) حوسم نىوكتب دننتسملا اذو يف ةمدختسما ءزهجالا عىمجتا ءب رما يا لىل مئامل رىثا لىل كمهف نم دكا تىف ، لىغشتلا دىق كىكشبش

## ةيساسا تامولعمل

ةلاصللا بابسا انا نم دىدعلا كانه . Cisco ESA ىللىضا رتفا لكشب لاحتنالا نىكمت متي ESA لوؤسم دىرى ، كلذىللى عئاشلا لثمكو . كنن ةباين لاسرلاب رىخالا تالاجملل حامسلا يف ةلحتنملا لئاسرلا عضو لالخنم ةلحتنملا ينورتكللالا ديربلا لئاسر يف مئحتلا . اهمايلست لبق لىحصلا رجلا

نع فشكلا الوأ بجى ، ةلحتنملا ينورتكللالا ديربلا ىللى لزع ءارجل لثم نىعم ءارجل اذختال . ةلحتنملا ينورتكللالا ديربلا

## ينورتكللالا ديربلا لاحتنا وه ام

ةلاسرلا نأ وديبى شىحب ينورتكللالا ديربلا سأل فىفىزت وه ينورتكللالا ديربلا لاحتنا وه ينورتكللالا ديربلا لئاسر لاحتنا . قىقىقحلا ردىملا رىغ ام ناكم وءا ام صخش نم تاشن سانلا نأل اهىف بوغرملا رىغ لئاسرلا وىلا لىتالا دىصتلا تالمح يف مدختسى كىتكت ردىم نم ةلسرما هأن نودقتعى ام دنن ينورتكللالا ديربلا ةلاسرلحتفل لىم رثكا نونوكى فىعش .

## ةلحتنملا ينورتكللالا ديربلا فاشتكا ةيفىك

يوتحى سأل (نم) نم لهسو (نم ديرب) فورظم لسرمل ىللى يوتحت لئاسر ةيا ةيفصت دىرت

ينورت كلالا ديربلا ناووع ي ف ك ب ة صاخلا ة دراوالا تالاجملا دح اىلع

نيددحم نيلسرمل لاحتنا اب حامسلا ةيفي ك

ىلع ةمالع عضو متي ، ةلاقملا هذه نمض رفوتملا لئاسرلا ةيفصت لماع ذي فننت دنع  
سأرلا ىلع ءارج اذخاتال ىوتحملا ةيفصت لماع مدختسي و ، سأر مادختساب ةلحتنملا لئاسرلا  
ىلا لسرملاب صاخلا IP ناووع ةفاضل ىوس كي لع ام ، ءانثتسا ةفاضلا .  
MY\_TRUSTED\_SPOOF\_HOSTS.

## نيوكتلا

اشن SendGroup

1. ةماع ةرظن > ديربلا تاسايس ىلا لقتنا ، ESA ةيموسرلا مدختسملا ةهجاو نم .
2. ةفاضل رقنا .
3. MY\_TRUSTED\_SPOOF\_HOSTS دح ، "مسالا" ل قح ي ف .
4. 1. دح ، رمألا ل قح ي ف .
5. لوبقم دح ، جهنلا ل قح ل .
6. تاريغيغتل لظفحل لاسرا قوف رقنا .
7. نيوكتلا لظفحل تاريغيغتل ذي فننت قوف رقنا ، اريخأ .

### Add Sender Group to LocalHostTest

Sender Group Settings	
Name:	MY_TRUSTED_SPOOF_HOSTS
Order:	1
Comment:	
Policy:	ACCEPTED
SBRS (Optional):	<input type="checkbox"/> to <input type="checkbox"/> <input type="checkbox"/> Include SBRS Scores of "None" <i>Recommended for suspected senders only.</i>
DNS Lists (Optional): (?)	<input type="text"/> <i>(e.g. 'query.blacklist.example, query.blacklist2.example')</i>
Connecting Host DNS Verification:	<input type="checkbox"/> Connecting host PTR record does not exist in DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).

Cancel Submit Submit and Add Senders >>

لاثم:

سوماق عاشن ا

ESA: ىلع اهل لاحتنالا ليطعت ديرت يتلا تالاجملا لك لسوماق عاشن اب مق

1. سيماولا > ديربلا تاسايس ىلا لقتنا ، ESA ل (GUI) ةيموسرلا مدختسملا ةهجاو نم .
2. سوماق ةفاضل رقنا .
3. لماعل قصل لاوخسنلا ءارج ا ، "VALID\_INTERNAL\_DOMAINS" دح ، "مسالا" ل قح ي ف .  
ءاطخأ نم اي لاخ لئاسرلا ةيفصت
4. لاجملا لخدأ . لاحتنالا فاشتك ديرت يتلا تالاجملا لك ةفاضل مق ، طورش ةفاضل تحت  
ةفاضل قوف رقناو لاجملا راطتنا لبق @ ةمالع عم

5. اهل مك أب تام لك لة ق با ط م را ي تخ إ ن ا خ دي د ح ت ا غ ل إ م د ك أ ت .
6. س و م ا ق ل ا ت ا ر ي غ ت ظ ف ح ل ل ا س ر ا ق و ف ر ق ن ا .
7. ن ي و ك ت ل ا ظ ف ح ل ت ا ر ي غ ت ل ا ذ ي ف ن ت ق و ف ر ق ن ا ، ا ر ي خ أ .

لا ث م :

## Add Dictionary

**Dictionary Properties**

<b>Name:</b>	<input type="text" value="VALID_INTERNAL_DOMAINS"/>
<b>Advanced Matching:</b>	<input type="checkbox"/> Match whole words <input type="checkbox"/> Case Sensitive
<b>Smart Identifiers: ?</b>	Match specific patterns such as social security numbers and credit card numbers.

**Dictionary** Number of terms: 1

<b>Add Terms:</b> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">@example.com</div> <p style="font-size: small;">Separate multiple entries with line breaks.</p> <p>Weight: ? <input type="text" value="1"/></p> <p style="text-align: right;"><input type="button" value="Add"/></p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 70%;">Term</th> <th style="width: 10%;">Weight</th> <th style="width: 20%;">Delete</th> </tr> </thead> <tbody> <tr> <td>@mydomain.com</td> <td style="text-align: center;">1</td> <td style="text-align: center;"><input type="button" value="🗑"/></td> </tr> </tbody> </table>	Term	Weight	Delete	@mydomain.com	1	<input type="button" value="🗑"/>
Term	Weight	Delete					
@mydomain.com	1	<input type="button" value="🗑"/>					

## ة ل ا س ر ة ي ف ص ت ل م ا ع ا ا ش ن إ

هؤ ا ش ن إ م ت ي ذ ل ا س و م ا ق ل ا ن م ة د ا ف ت س ا ل ل ل ا س ر ة ي ف ص ت ل م ا ع ا ا ش ن إ ل ا ج ا ت ح ت ، ك ل ذ د ع ب "VALID\_INTERNAL\_DOMAINS":

1. ن ر ا ق ط خ ر م أ ل ا ل ا ت ط ب ر . (CLI) ن م ا ل ا S A E .
2. ر م ا و أ ل ا ة ي ف ص ت ل م ا و ع ل ي غ ش ت ب م ق .
3. د ي د ج ة ل ا س ر ة ي ف ص ت ل م ا ع ا ا ش ن إ ل د ي د ج ر م أ ل ل ي غ ش ت ب م ق .
4. ن ي ل س ر م ل ا ة و م ج م ا م س أ ل ت ا ر ي ر ح ت ا ر ج ا م ، ه ق ص ل و ا ذ ه ة ي ف ص ت ل ا ل م ا ع ل ا ث م خ س ن .  
ر م أ ل ا م ز ل ا ذ ا ة ي ل ع ل ل ا :

```

mark_spoofed_messages:
if(
    (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
    OR (header-dictionary-match("VALID_INTERNAL_DOMAINS", "From", 1)))
AND ((sendergroup != "RELAYLIST")
AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS"))
)
{
insert-header("X-Spoof", "");
}

```

5. نيوكتل ظفحل مازتللالا لغشو ةيسيئرلا (CLI) رماوالا رطس ةهجاو رماوا هجوم ىل عجرا.
6. ةيفصت لماع > ديربلا تاسايس > (GUI) ةيموسرلا مدختسملا ةهجاو ىل لقتنا ةدراوالا ىوتحمل
7. X-Spoof ناوع ىل عارجا ذختي دراو ىوتحم ةيفصت لماع عاشن:

1. رخآ سارة فاضا.
2. X-Spoof: سارلا مسا.
3. دوجوم ناوع عاقتنا رز.
4. (جهن) يطايتحا خسن: عارجا فاضا.

✎ ةلاسرلا نم ةخسنب انه ةحضملا ةلاسرلا راركت ةزيم ظفتحت: ةظالم ملتسملا ىل ةلصالا ةلاسرلا لاسرلا يف رمتستو.

### Add Action

Quarantine

Encrypt on Delivery

Strip Attachment by Content

Strip Attachment by File Info

Strip Attachment With Macro

URL Category

URL Reputation

Add Disclaimer Text

Bypass Outbreak Filter Scanning

Bypass DKIM Signing

Send Copy (Bcc:)

Notify

#### Quarantine Help

Flags the message to be held in one of the system quarantine areas.

Send message to quarantine: Policy

Duplicate message

*Send a copy of the message to the specified quarantine, and continue processing the original message. Any additional actions will apply to the original message.*

### Add Incoming Content Filter

**Content Filter Settings**

Name:

Currently Used by Policies: *No policies currently use this rule.*

Editable by (Rcles): *No custom user roles available*

Description:

Order: 26 (of 26)

### Conditions

[Add Condition...](#)

Order	Condition	Rule	Delete
1	Other Header	header("X-Spoof")	🗑️

### Actions

[Add Action...](#)

Order	Action	Rule	Delete
1	Quarantine	duplicate-quarantine("Policy")	🗑️

Cancel
Submit

8. ةيموسررلا مدختسمللا ةهجاو يف دراوولا ديربللا تاسايسب يوتحمللا ةيفصت لماع طبر .  
دراوولا ديربللا تاسايس >ديربللا تاسايس (GUI) >
9. اهذيفنتو تارييفنتلا لاسرا .

## إضافة MY\_TRUSTED\_SPOOF\_HOSTS لتأمين تاءانثتس إضافة

ةومجم يلا (فيضملا ءامسأ أو IP نيوانع ) تاءانثتسالا ةيفصا إضافة يلا جاتحت ، اريخأ MY\_TRUSTED\_SPOOF\_HOST فرعم

1. ةماع ةرظن > ديربللا تاسايس :ببول ربع (GUI) ةيموسررلا مدختسمللا ةهجاو ربع لقننتلا .  
HAT يلع
2. اهجتفب مقو MY\_TRUSTED\_SPOOF\_HOSTS نيلسررملا ةومجم قوف رقنا .
3. مسا وأ فيضملا مسا وأ قاطنلا وأ IP ناونع ةفاضلا ...لسررم ةفاضلا قوف رقنا .  
يئزجال فيضملا .
4. لسررملا تارييفنت ظفحل لاسرا قوف رقنا .
5. نيوكنتلا ظفحل تارييفنتلا ذيفنت قوف رقنا ، اريخأ .

لثام:

## ةحصللا نم ققحتلا

ةلحتنملا لئاسررلا لزع نم ققحتلا

ةيفصتلا لماع لمع ةحص نم ققحت .فورظملا لسررمك كئالاجم دحأ ددحت رابتخا ةلاسرا لاسرا لزع يه ةعقوتملا ةجيتنلا .ةلاسرا كئلت يلع ةلاسرا بقعت ذيفنت لالخنم عقوتم وه امك مهل حومسمللا نيلسررملا ءالؤهل دعب تاءانثتسإ ي ءاشناب مقت مل كئال ةلاسرا لالحتنالاب .

<#root>

Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <xxxx\_xxxx@domain.com>

Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'

Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user\_1@example.com>

Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT in the i

Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative  
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative  
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN  
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative  
Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message filter:quarantine\_spoofed\_messag  
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done

## مدخستس مالا مس اناثتس لئاسر ميسلست نم ققحتلال

يف اهيلي راشم لاسر مالا (تاعومجم) ةعومجم في IP نيوانع لاحتتال اناثتس الال ولسررم دعي هالع اةيفصتلال لماع

نوكت ام ةداع. رداص ديرب لاسر لال ESA لبق نم همادختس لمتي هنال Relaylist لى لراش لال ممت عاشن لى لال اذه ني مضت يدوي الو، رداص ديرب Relaylist ةطساوب اه لاسر لال ممتي لئال لئاسر لال ةيفصتلال لماع ةطساوب يحصل لال رجح لال في اهعضو ممتي ةرداص لئاسر و اةيطاخ تايباجي لال هالع.

لى هتفاض لال ممت يذال اناثتس الال ةيفصاخ ب صاخ لال IP ناو نعل لئاسر لال بقت لال م اذهل حمسي). لزع اارج س لى لى و ع قوت مالا اارج لال ميسلست ممتي MY\_TRUSTED\_SPOOF\_HOSTS. (لاحتتال لال IP

<#root>

Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11  
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user\_1@example.com>  
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <user\_xxxx@domain.com>  
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'  
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user\_1@example.com>  
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT in the i  
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN  
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative  
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery  
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]  
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]  
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598

Message accepted for delivery'

Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done

## ةلص تاذا تامولعم

- [ةلحتتس مالا ESA ديرب ةيفصت](#)
- [لسر مالا نم ققحتلال مادختس اب ةقعل مالا ةيامح](#)

Cisco نم ةيلخادلال تامولعم لال

هذه طيسبتل ىوتحملا ةيفصت لم اوع/لئاسرلا تاحشرم ل RAT ضيرعت لوح ةزيم ب لظ كانه  
ةيلمعلا:

(RAT) ملتسملا لوصو لودج ضرع - ENH: Cisco [CSCus49018](#) نم ااطخألا حيصت فرعم  
طورشللا ةيفصت ل



ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيد نوك تنل ةللأل ةمچرت لصف انءمچم اءمچرئى. ةصاأل مءتبلب  
Cisco يلخت. فرتحم مچرت مءم دقئى تىل ةى فارتحال ةمچرتل عم لءال وه  
ىل اءمءاد ءوچرلاب ي صوءو تامچرتل هذه ةقदनء اهتئل وئسم Cisco  
Systems (رفوتم طبارلا) ي لصلأل يزلچنءل دن تسمل