

ديربللا ةرأبع ني مأتل URL ةي فصت ني وكت Secure Email Gateway نم آلل ي نورت كل إل Cloud Gateway ةباحسلا ةرأبعو

تايوت حمللا

[ةمدقملا](#)

[ةي ساسأ تامولعم](#)

[ةي ساسألا تابلطتملا](#)

[URL نيوانع ةي فصت ني وكت](#)

[URL نيوانع ةي فصت تاعارجا عاشنلا](#)

[ةقو وشملا ريغ URL \(نيوانع\) ناوانع](#)

[ةفورعمللا ريغ URL \(نيوانع\) ناوانع](#)

[اهي ف كوكشملا URL \(نيوانع\) ناوانع](#)

[ةدياحملا URL \(نيوانع\) ناوانع](#)

[لئاسرلا بقعت](#)

[ئطاخ وحن لعل ةفنصملا وأ ةفنصملا ريغ URL \(نيوانع\) ناوانع نغالبلا](#)

[لماوع ةطساوب قيوس تلبلا لئاسرو ةراضلا URL نيوانع فاشتكلا متي ال
راشتنالا وأ يئوشعللا ديربلا ةحفاكم ةي فصت](#)

[قحلملا](#)

[ةرصتخملا URL نيوانعلا URL نيوانع ةي فصت معد ني وكت](#)

[ةي فاضا تامولعم](#)

[Cisco Secure Email Gateway قئاثو](#)

[Secure Email Cloud Gateway قئاثو](#)

[بيولا ري دم و Cisco Secure Email قئاثو](#)

[Cisco Secure تاجت نم قئاثو](#)

ةمدقملا


Cisco Secure Email Gateway لعل URL نيوانع ةي فصت ني وكت ةي فكيك دنتسمللا اذه حضوي URL نيوانع ةي فصت مادختسال تاسرامملا لصف أو ةي باحسلا ةرأبعلاو


ةي ساسأ تامولعم


حمس [ي نورت كل إللا ديربلا نامأل AsyncOS 11.1](#) عم ةرم لوأل URL نيوانع ةي فصت مي دقت مت لئاسرلا تاقفرم ي URL نيوانع نغ أثحب حسملل Cisco Secure Email ني وكتب رادصللا اذه لئاسرلا ةي فصت لماوع مدختست. لئاسرلا كلت ي فاهني وكت مت يتلا تاعارجالا ذيفنتو لئاسرلا ي URL نيوانع دوجو نم ققحتلل URL ناوانع ةئفو URL ناوانع ةعمس يوتحمللاو ضرفل لئاسرلا ةي فصت لماوع مادختسا" لوصف عجار، لي صافاتلا نم دي زملا. تاقفرملاو ريغ URL نيوانع نم ةي امحللا"و "يوتحمللا ةي فصت لماوع"و "ي نورت كل إللا ديربلا تاسايس تترت نإل ربع تاميلعلتلا وأ [مدختسمللا ليلا](#) ي ف "اهي ف بوغرملا ريغ وأ ةقو وشملا

عمائق يف اهيف بوغرملا ريغ وأ عقووملا ريغ تااطابترا لا نم ةيماحللاو مكحتلا جمدم تي، يوتحمللا ةيفصتو، راشتنال او، يئواوشعلال ديربللا ةحفاكم تاي لمعب ةصاخلا لمعلال راظتنا، يلي ام يلع هذه مكحتلا لمواع لمعتو. لئاسرلاو:

- تاقفرملاو لئاسرلا يف عقووملا ريغ URL نيوانع نم ةيماحللا ةيلعاف ةدايز.
- راشتناللا ةيفصت لمواع يف URL نيوانع ةيفصت جمدم تي، كلذ يلى ةفاضلاب لعفلاب كلتمت كتسسؤم تناك اذى تح قي بطتلل ةلباق ةززعمللا ةيماحللا هذه نوكت يلى ةدنتسمل تاديدهتلا نم ةلثامم ةيماحل وأ Cisco Web Security Appliance نامأل زاخ لوخدلا ةطقن دنع تاديدهتلا رطحت اهأل بيولا.
- ةجرد يلع ءانب ءارجا ذاخاتال لئاسرلا وأ يوتحمللا ةيفصت لمواع مادختسا أضيأ كنكمي، لاثملا لئاسرلا يلع. لئاسرلا يف URL نيوانعل (WBR) بيولا يلى اذانتسا ةعمسللا ةداعال ةفورعم ريغ وأ ةدياحم ةعمسب عتتمتت يلى URL نيوانع ةباتك ةداعا كنكمي رقرنلا تقو اهناما ميقيقتل Cisco Web Security Proxy يلى اههيجوت.
- يئواوشعلال ديربللا يلع لضفأ لكشب فرعتلا.
- تاي مزرراوخ نم اهريغو لئاسرلا يف ةدووملا تااطابترا لا ةئفو ةعمس زاخال مدختسي، لاثملا لئاسرلا يلع. يئواوشعلال ديربللا ديحت يف ةدعاسملا يئواوشعلال ديربللا فيرعت نوكت نا حجالا نم ف، يقيوست بيوع قوم يلى يمتني ةلاسري ف طابترال كانه ناك اذى ةيقيوست ةلاسر ةلاسرلا.
- ةكرشلال لوبقملا مادختساللا تاسايس ضرعم.
- يلع، ةينوناقلا ريغ ةطشنأل وأ نيغلابللا يوتحمل (URL نيوانع ةئف مادختسا كنكمي مادختساللا تاسايس ضرفل لئاسرلاو يوتحمللا ةيفصت لمواع عم (لاثملا لئاسرلا ةكرشلال يلى لوبقملا).
- أراكت رثكال وحنلا يلع اورقن نيذلا كتسسؤم يف ني مدختسمللا ديحت كل حيتت رقرنلا مت يلى تااطابترا لاو ةيماحللا ةباتك ةداعا تمت ةلاسري ف URL ناو نع قوف أعويش رثكال وحنلا يلع اهقوف.

 URL ناو نع ةيفصت تم دق [ينورتكلاللا ديربللا نامأل AsyncOS 11.1](#) رادصا يف: ةظالم ةهجاو يلى "websecurityadvancedconfig" رمأل مادختساب. ةرصتخملا URL نيوانعل امعد راخي شيحت مت. اهنيوكتو ةرصتخملا تامدخال يلى فرعتلا كنمأ، (CLI) رماوأل رطس رادصاللا اذى يلى ةيقرتلا دعب. [ينورتكلاللا ديربللا نامأل AsyncOS 13.5](#) يف اذى نيوتلا URL نيوانع عيسوت لئاسرلا راخي دجوي ال. ةرصتخملا URL نيوانع عيسوت متي نيورتكلاللا ديربللا نامأل AsyncOS 13.5 ماظن ب Cisco ي صوت، ببسلا اذلو. ةرصتخملا يلى عالطاللا يجرى. URL نيوانع نع عافدللا ةيماحللا لئاسو شحأ ري فوئل شحأ رادصا وأ مادختسمللا ليلى يف "اهيف بوغرملا ريغ وأ ةراضلا URL نيوانع نم ةيماحللا" لصف AsyncOS ماظن (CLI) رماوأل رطس ةهجاو لي عجرملا ليلى دللاو تنرتنالا ربع تاميلىل Cisco Email Security Appliance زاخال.

 [ديربللا نامأل AsyncOS 14.2](#) مادختسا متي، دننتسمللا اذهل ةبسنلاب: ةظالم ةمدقملا ةشاشلا تاقلو ةلثمأل [ينورتكلاللا](#).

 قمعتم [URL ناو نع عافد ليلى](#) اضىأ Cisco نم نمأللا نيورتكلاللا ديربللا رفوي: ةظالم docs.ces.cisco.com يف.

ةيساساللا تابلطتلا

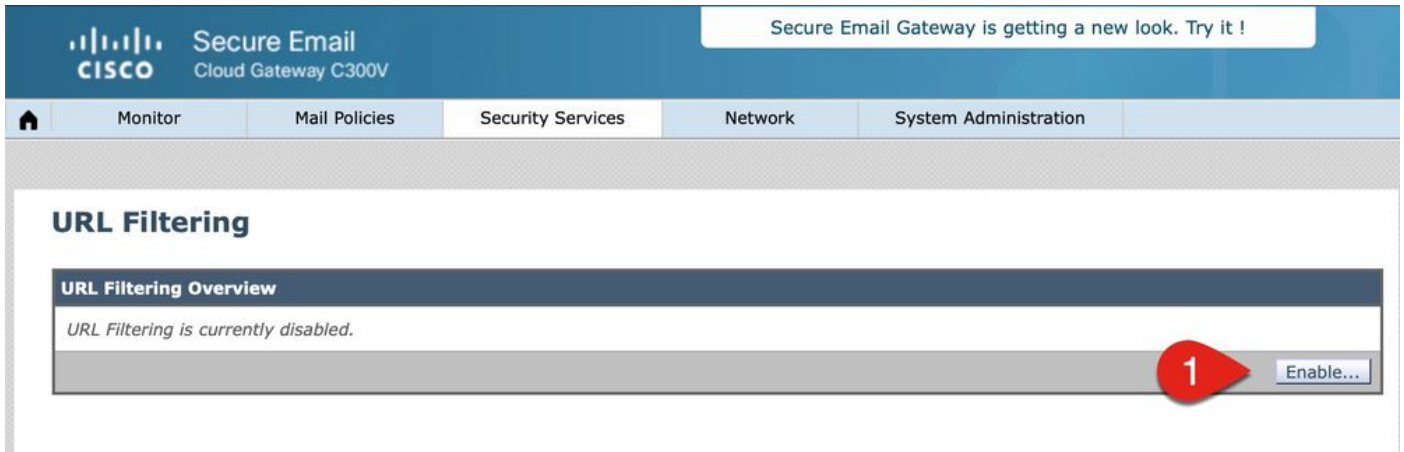
، ةباحسلا ةرّابع وأ Cisco Secure Email Gateway ىل ع URL نيوانع ةيفصتلا كنڤوكت دنع
ضعب يلى امي ف . ةبولطملا فئاظولا ىل ع دمتعت ىرخأ تازيم نيوكت أضيأ كىل ع بجي
URL نيوانع ةيفصت عم بنج ىل ا أبنج اهنڤكمت متي يتلا ةيجذومنلا تازيملا

- ديربلا ةحفاكمل صحفلا ةزيم نإف ، يئاوشعلا ديربلا دض ةنّسحم ةيامح ىل ع لوصحلل
ربتعت . اه ب لومعمل ديربلا ةسايسل أقف و يمومع لكشب اهنڤكمت بجي يئاوشعلا
ديربلا ةحفاكمل Cisco IronPort ةئف نم اما ةزيم يئاوشعلا ديربلا ةحفاكمل ةزيم
Cisco (IMS) نم ددعتل يكدل صحفلا ةئف نم وأ (IPAS) يئاوشعلا
- لم اوع وأ راشتنالا ةيفصت لم اوع نإف ، ةراضلا جماربلا دض ةنّسحم ةيامح ىل ع لوصحلل
ةسايسل أقف و يمومع لكشب اهنڤكمت بجي (VOF) تاسوريفلا راشتنا ةيفصت
اه ب لومعمل ديربلا
- مادختسالا تاسايس ضرفل وأ URL ناوئع ةعمس ىل ا ةدنتسمل اءارجلل ةبسنلاب
اهنڤكمت بجي VOF نإف ، ىوتحمل او لئاسرلا ةيفصت لم اوع مادختساب لوبقملا
يمومع لكشب

URL نيوانع ةيفصت نيكمت

Cisco Secure Email Gateway ىل ع URL نيوانع ةيفصت ذيفنتل ةزيملا نيكمت آلوا كىل ع بجي
ةهجاو نم URL نيوانع ةيفصت نيكمت لوؤسملل نكمي . ةباحسلا ةرّابع وأ
Gateway (CLI) رماوأل رطس ةهجاو وأ (GUI) ةيموسرلا مدختسمل

تامدخ ىل ا لقتنا ، (GUI) ةيموسرلا مدختسمل ةهجاو نم ، URL نيوانع ةيفصت نيكمتل
نكمت قوف رقناو URL نيوانع ةيفصت > نامأل



اذه نمضتي . URL نيوانع ل ةعمسلاو تائفلا ةيفصت لم اوع نيكمت قوف رقنا ، كلذ دعب
نيوانع ددعل ىصقأل دحلاو ، URL نيوانع نع ثحبلا ةلهمل تاسرامملا لصفأ ميقل لاثملا
URL (نيوانع) ناوئع ليجست رايخ نكمي و ، اهصحف مت يتلا URL

Secure Email Gateway is getting a new look. Try it!

Secure Email
Cloud Gateway C300V

Monitor Mail Policies Security Services Network System Administration

URL Filtering

URL Filtering Overview

Enable URL Category and Reputation Filters

Use a URL allowed list:

Web Interaction Tracking: Enable Web Interaction Tracking

Advanced Settings:

URL Lookup Timeout:

Maximum Number of URLs scanned in Message Body:

Maximum Number of URLs scanned in Message Attachments:

Rewrite URL text and HREF in Message: Yes
Select the 'Yes' option to display the rewritten URL in the message body.
 No
Select the 'No' option to display the rewritten URL in the HREF part of the HTML message.

URL Logging: Enable Disable

Cancel Submit

يُلاحَظ تقوِلا يف نيوكتل اللى ع اهتيرجأ يتل التاريخيغتللاب مازتللالا نم دكأت: ةظحالم

URL نيوانع ةيفصت تاءارجإ عاشنإ

ةدوجوملا URL نيوانع دصَّءارجإ ذختت ال اهنإف، اهدرفمب URL نيوانع ةيفصت نيكمت دنع تاقفرم لىل ع يوتحت يتل لئاسرلا وأ لئاسرلا لخد.

لىل ةبس نلاب تاقفرملاو لئاسرلا يف ةنمضملا URL (نيوانع) ناوع مبيقت متي نيضمتل URL ناوع ل ءحلص ةلسلس يأمبيقت متي. رداصل او دراو لا ديربلا تاسايس ةيلالاتل تانوكمللاب لسالس:

- HTTP وأ HTTPS وأ WWW
- IP نيوانع وأ لاجملا
- (:) ني تطقنب ةقوبسم ذفانملا ماقراً
- ةريغص وأ ةريكب فرحاً

م تي مل اذا URL نيوانع مظعم ل Mail_Log نم ايئرم URL ناوع ل جس لاخدإ نوكي: ةظحالم (MID). ةلسرلا فرعم لئاسرلا بقعت ةعجارم يجرُف، mail_logs يف URL ناوع ليچست URL ناوع ليصافت "صخت بيوبت ةمالع لئاسرلا بقعت نمضت ال".

إذا، فإن، ما أهيف بوغرم ريغ ةلاسرلا تناك إذا ام ديحتل URL نيوانع ماظنلا مقيي ام دنع ةرداصل لئاسرلا لىل ةدراولا لئاسرلل ةيولوأل يطعي، لمحلل ةرادال رمأل مزل

في URL ناووع ةئف وأ URL ناووع ةعمس لىل أدانتسا لئاسرلا لىل ةءارجل ذيفنت كنكمي ةاقفرملا تاذ لئاسرلا وأ ةلاسرلا صن

عيمي لىل (يئاهنلا ةارجل) طاقسإل ةارجل قيبطت في بغرت تنك إذا، لاثملا لىبس لىل ناووع ةئف عونلا نم أطرش فضا، رابكلا ةئف في URL نيوانع نمضتت يتلا لئاسرلا رابكلا ةئف ديحت عم URL

لئاسرلا عيمي لىل ةراتخت يذلا ةارجل قيبطت متيسف، ةئف ددحت مل إذا

ريغو، أهيف كوكشملاو، ةدياحملاو، ةلضملاو، ةقووملا URL نيوانع ةعمس تاجرد قاطن لىل مدختسا. صصخم قاطن ديحت كنكمي. ريحتلل لباق ريغو أقبسم أدجم نوكي ةقووملا اهتعمس ةجرد ديحت دعب متي مل يتلا URL نيوانع "ةفورعم ريغ"

ناك إذا ثيحب يوتحملل ةيفصت لماع عاشن كنكمي، ةارجل ذاختاو أعيرس URL نيوانع صحفل مدختسملا ةهجاو نم. ةارجل قيبطت متيسف يلاتلابف، حلصل URL ناووع ةلاسرلل لماع ةفاضل > دراولا يوتحملل ةيفصت لماع > ديربلا تاسايس لىل لقتنا، (GUI) ةيموسرلا ةيفصت

ي: لياتل وحنلا لىل URL نيوانع ةطبترملا ةءارجلل نوكت

- URL ناووع نم رطخلا ةلازا
 - ناكمإ لازي ال نكلو، هقوف رقنلل لباق ريغ هلعلل URL ناووع لىدعت متي ناووع في ةفاضل فورح لاخدإ مت. دوصقملا URL ناووع ةءارق ةلاسرلا ملتسم (ي.لصلال URL)
- Cisco Security Proxy لىل هيجوتلا ةءارجل
 - Cisco Security Proxy ربع رورملا هقوف رقنلا دنع URL ناووع ةباتك ةءارجل مت لىل رذعتي دق، Cisco Security Proxy مكح لىل أدانتسا. يفاضل ققحت ةارجل عقوملا لىل لوصول مدختسملا
- ةيصرن ةلاسرب URL ناووع لادبتسا
 - ةلاسرلا لخداد URL ناووع ةباتك ةءارجل لوؤسملل نكمي، رايخلل اذم مادختساب ديعلل ضرعتسملا لزلل أيچارخا هلاسراو

ةقووملا ريغ URL (نيوانع) ناووع

رطح ةمئاق ةبتع وه اذم. هيف بوغرم ريغ وأ راض وأ ةياغلل ئيس URL كولس: هب قووم ريغ URL نيوانع نأل اهرطح متي ال لئاسرلانه نوكت نأ نكمي، كلذ عمو، اهب يصولملا نامأل نامأل لىل ميسرلل ةيولوأل يطعي. لقا ديدهت يوتسم لىل يوتحت اهيف ةدوجوملا

(لمالكلاب اهفدح وأ ةلاسرلا لزلل لوؤسملل نكمي). رطحلا: هب يصولملا ةارجل

نع فشكلل URL نيوانع ةيفصت يوتحملل ةيفصت لماعل أقايس لاثملا اذم رفوي ةقووملا ريغ URL نيوانع:

Content Filter Settings	
Name:	URL_QUARANTINE_UNTRUSTED
Currently Used by Policies:	Default Policy
Description:	Quarantine messages with known Untrusted URLs. (Includes messages with attachments.)

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Quarantine	quarantine("URL_UNTRUSTED")	

يذ URL ناونعل صحفب Cisco Secure Email موقوي ، اذه يوتحمل اةيفصت لماع قيبت عم
 لزع ةدحوي فة لاسرل اعضوي و (-6.00 لى | -10.00) ةجرذب ةقوئومل ريغ ةعمسلا
 mail_logs رمال نم لاثم يلى امي ف URL_UNTRUSTED.

<#root>

```
Tue Jul 5 15:01:25 2022 Info: ICID 5 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country United
Tue Jul 5 15:01:25 2022 Info: ICID 5 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 15:01:25 2022 Info: Start MID 3 ICID 5
Tue Jul 5 15:01:25 2022 Info: MID 3 ICID 5 From: <test@test.com>
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Domains for which SDR is requested: reverse DNS host: example.
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:01:25 2022 Info: MID 3 ICID 5 RID 0 To: <end_user>
Tue Jul 5 15:01:25 2022 Info: MID 3 Message-ID '<20220705145935.1835303@ip-127-0-0-1.internal>'
Tue Jul 5 15:01:25 2022 Info: MID 3 Subject "test is sent you a URL => 15504c0618"
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Tracker Header : 62c45245_jTikQ21V2NYfmrGzMwQMBd68fxqFFueNmElw
Tue Jul 5 15:01:25 2022 Info: MID 3 ready 3123 bytes from <test@test.com>
Tue Jul 5 15:01:25 2022 Info: MID 3 matched all recipients for per-recipient policy DEFAULT in the inbo
Tue Jul 5 15:01:25 2022 Info: ICID 5 close

Tue Jul 5 15:01:25 2022 Info: MID 3 URL https://www.ihaveabadreputation.com/ has reputation -9.5 matched

Tue Jul 5 15:01:25 2022 Info: MID 3 quarantined to "Policy" (content filter:URL_QUARANTINE_UNTRUSTED)

Tue Jul 5 15:01:25 2022 Info: Message finished MID 3 done
```

هوليجست متوهب قوئوم ريغ (URL) ihaveabadreputation.com تامولعمل اعقوم ددحم ربت عي
 لى اعقوم تلزعو هب قوئوم ريغ URL ناونعل URL ةيفصت تفشك 9.5 مقرلا لى
 URL_UNTRUSTED.

ةيفصت لماع نيكمت لاجي ف طقف كلذىل ع الاثم mail_logs نم قباسل لاثم لرفوي جهنل ةيفاضا تامدخ نيكمت مت اذا . دراوال ديربل ةسايسل URL نيوانع ةيفصت لوتحم لادق ناك اذا ام لىل اىرخال تامدخ لريشتس ف ، ةيئاوشع ل ديربل ةحفاكم لثم ، هسفن ديربل URL ناوع لاثم في . اهب ةصاخل دعاقول او تامدخ ل كلت نم URL ناوع فاشتكام مت م تي و ، دراوال ديربل ةسايسل Cisco Anti-Spam Engine (CASE) كرحم نيكمت مت ، هسفن في الؤا كلذىل ةراشال مت . ةيئاوشع ديربك اىباجي نوكل هدحت و ةلاسرل صرل صحتف ةجال عم تاي لمع راسم في لىل و الؤا ةمدخ ل ه ةيئاوشع ل ديربل ةحفاكم نال ارظن mail_logs ةجال عم تاي لمع راسم في اقحال لوتحم ل ةيفصت لماع يتات . ديربل

<#root>

```
Tue Jul 5 15:19:48 2022 Info: ICID 6 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country United States
Tue Jul 5 15:19:48 2022 Info: ICID 6 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 15:19:48 2022 Info: Start MID 4 ICID 6
Tue Jul 5 15:19:48 2022 Info: MID 4 ICID 6 From: <test@test.com>
Tue Jul 5 15:19:48 2022 Info: MID 4 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-0-1
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A
Tue Jul 5 15:19:49 2022 Info: MID 4 ICID 6 RID 0 To: <end_user>
Tue Jul 5 15:19:49 2022 Info: MID 4 Message-ID '<20220705151759.1841272@ip-127-0-0-1.internal>'
Tue Jul 5 15:19:49 2022 Info: MID 4 Subject "test is sent you a URL => 646aca13b8"
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-0-1
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Tracker Header : 62c45695_mqwp1hpxGDqtgUp/XTLGFKD60hwNKKsghUKA
Tue Jul 5 15:19:49 2022 Info: MID 4 ready 3157 bytes from <test@test.com>
Tue Jul 5 15:19:49 2022 Info: MID 4 matched all recipients for per-recipient policy DEFAULT in the inbound
Tue Jul 5 15:19:49 2022 Info: ICID 6 close

Tue Jul 5 15:19:49 2022 Info: MID 4 interim verdict using engine: CASE spam positive

Tue Jul 5 15:19:49 2022 Info: MID 4 using engine: CASE spam positive

Tue Jul 5 15:19:49 2022 Info: ISQ: Tagging MID 4 for quarantine
Tue Jul 5 15:19:49 2022 Info: MID 4 URL https://www.ihaveabadreputation.com/ has reputation -9.5 matches
Tue Jul 5 15:19:49 2022 Info: MID 4 quarantined to "URL_UNTRUSTED" (content filter:URL_QUARANTINE_UNTRUSTED)
Tue Jul 5 15:19:49 2022 Info: Message finished MID 4 done
```

تايوتحم عم قباطت تاجرد و ةعمس و دعاقو لىل IPAS و CASE دعاقو اهي ف يوتحت تاقو و كانه صرمت ، لاثم ل اذ في . اهدحو URL نيوانع تاديدهت نع فشكلل ةدحم ةلاسر و لاجم و لاسرر ihaveabadreputation.com ، لزعو ، (ISQ) ةيئاوشع ل ديربل لزل هيلع ةمالع عضو مت و ، URL_UNTRUSTED لوتحم ل ةيفصت لماع ةطساوب URL_UNTRUSTED . كلذ نم ةلاسرل ريرحت م تي ام دنع . الؤا URL_UNTRUSTED لزل ةدحو لىل ةلاسرل لقتنت لزل راي عمب ةصاخل نيوكتل راي اع م / ني نمزل دل اءا فيتسا دنع و لوؤسم ةطساوب لزل لىل ISQ . كلذ دعب ةلاسرل لقتنت م تي ، URL_UNTRUSTED .

ةيفصت ل ةيفاضا تاءارج او طورش نيوكت نكمي ، لوؤسم ل تاليفت لىل اءانتسا لوتحم ل .


ةفورعمل رىغ URL (نىوانع) ناووع


ددهتلا ىوتسم ىلع مكح ديكأتل تازيم ضرعي ال وأ أقباس هميقت متي مل :ةفورعمل رىغ رىغ مكحل اذه .ةعمس ةجرد ديدحتل ةيفاك تانايب URL ناووع ةعمس ةمدخ ىدل رفوتت ال URL ناووع ةعمسب ةصاخ ةسايس يف ةرشابم ةدراول تاءارجل بسانم .


اراض نوكي دق رخآ ىوتحم دوجو نم ققحتلل ةيلات تاكرحمب ىئوضلا حسملا :هب ىصوم ءارجا

ىلع ىوتحت URL نىوانع "ةعمس نود نم" وأ ةفورعمل رىغ URL (نىوانع) ناووع نوكي نا نكمي نوكت نا نكمي ال وةم ودم وأ ةليلق تارايز ةكرح تدهش URL (نىوانع) ناووع وأ ةديج تالاجم ةقووم رىغ ىل نىوانعلا هذه لوحتت نا نكمي .ددهتلا ىوتسم ىلع مكحو ةممي قم ةعمس اهل اذه URL ناووعل ةبسنلاب .اهئشنمو اهلاجم نع تامولعمل نم ديزم ىلع لوصحلا متي ام دنع نمضت ي دحاو وأ لىجستلل ىوتحم ةيفصت لماع مادختساب Cisco ىصوت ،(هذه URL نىوانع) ناووع لاسرا متي ، AsyncOS نم 14.2 رادصال نم آرابتعا .فورعمل رىغ URL ناووع فاشتكا لىلحتل Talos Intelligence Cloud Service ةباحتلا ىل ةفورعمل رىغ URL (نىوانع) ،كلذ ىل ةفاضل .ةفلتخملا ددهتلا تارشؤم ىلع هلىغشت متي يذلا قيمعمل URL ناووع ناووع ىل ةراش لوؤسمل ةفورعمل رىغ URL (نىوانع) ناووعل ديربلا لىجس لاخدا رفوي نىوانع ةيماح مادختساب نكمملا حالصالاو (MID) ةلاسر فرعم يف ةنمضمل URL (نىوانع) URL (API) تاقىبطل ةجمرب ةهجاول Cisco Secure Email باسح تاداعل نيوكت ةيفيك عجار) .(تامولعمل نم ديزم ىلع لوصحل Cisco - Microsoft Azure (Microsoft 365) يف

نىوانع نع فشكلل URL نىوانع ةيفصتلا ىوتحم ةيفصت لماعل آقايس لاثملا اذه رفوي ةفورعمل رىغ URL :

Content Filter Settings	
Name:	URL_UNKNOWN
Currently Used by Policies:	Default Policy
Description:	Log messages with Unknown URLs. (Includes messages with attachments.)
Order:	2  (of 2)

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-no-reputation("", 1, 1)	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<<<=== LOGGING UNKNOWN URL FOR MAIL_LOGS ===>>>")	

ناووع نع اثحب صحفلااب Cisco Secure Email موقى ،اذه ىوتحمل ةيفصت لماع مادختساب رمال نم لاثم ىلي امي ف mail_logs. يف لىجس رطس ةباتكو ةفورعمل رىغ ةعمسب URL mail_logs:

<#root>

Tue Jul 5 16:51:53 2022 Info: ICID 20 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country Unit
Tue Jul 5 16:51:53 2022 Info: ICID 20 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 16:51:53 2022 Info: Start MID 16 ICID 20
Tue Jul 5 16:51:53 2022 Info: MID 16 ICID 20 From: <test@test.com>
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-0-1
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N
Tue Jul 5 16:51:53 2022 Info: MID 16 ICID 20 RID 0 To: <end_user>
Tue Jul 5 16:51:53 2022 Info: MID 16 Message-ID '<20220705165003.1870404@ip-127-0-0-1.internal>'
Tue Jul 5 16:51:53 2022 Info: MID 16 Subject "test is sent you a URL => e835eadd28"
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-0-1
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Tracker Header : 62c46c29_vrAqZZys2Hqk+BFINVrzdNLLn81kuIf/K6o
Tue Jul 5 16:51:53 2022 Info: MID 16 ready 3208 bytes from <test@test.com>
Tue Jul 5 16:51:53 2022 Info: MID 16 matched all recipients for per-recipient policy DEFAULT in the inbound
Tue Jul 5 16:51:53 2022 Info: ICID 20 close
Tue Jul 5 16:51:54 2022 Info: MID 16 interim verdict using engine: CASE spam negative
Tue Jul 5 16:51:54 2022 Info: MID 16 using engine: CASE spam negative

Tue Jul 5 16:51:54 2022 Info: MID 16 URL http://mytest.example.com/test_url_2022070503 has reputation no

Tue Jul 5 16:51:54 2022 Info: MID 16 Custom Log Entry: <<<=== LOGGING UNKNOWN URL FOR MAIL_LOGS ===>>>

Tue Jul 5 16:51:54 2022 Info: MID 16 queued for delivery
Tue Jul 5 16:51:54 2022 Info: Delivery start DCID 13 MID 16 to RID [0]
Tue Jul 5 16:51:56 2022 Info: Message done DCID 13 MID 16 to RID [0]
Tue Jul 5 16:51:56 2022 Info: MID 16 RID [0] Response '2.6.0 <20220705165003.1870404@ip-127-0-0-1.internal>
Tue Jul 5 16:51:56 2022 Info: Message finished MID 16 done
Tue Jul 5 16:52:01 2022 Info: DCID 13 close

هتدهاشم متتو ةعمس هل سېل URL mytest.example.com/test_url_2022070503 ناونع
دنع لچسلا رطس ةباتكب URL_UNKNOWN يوتحمل ةيفصت لماع ماق "noscore" مادختساب
ت mail_logs لىل هنيوكت

ك لذة طحال م نكمي و. ةقووم ريغ ةعمسب هنا ديدحتو URL ناونع صحف متي، Talos Intelligence
Cisco Secure Email Gateway لىل ةمدخل لىل ةراضقتسا ةرود دعب
"بقتلا" يوتسم دنع ECS تالچس يف

URL Reputation

[Help](#)

What is the reputation of the URL in the message body, subject or the message attachments? This rule evaluates the URL using either the Web Based Reputation Score (WBRs) or using information from the External Threat Feed engine.

Matching Condition

URL Reputation

- Untrusted (-10.0 to -6.0)
- Questionable (-5.9 to -3.1)
- Neutral (-3.0 to 0.0)
- Favorable (0.1 to 5.9)
- Trusted (6.0 to 10.0)
- Custom Range (min to max)

Unknown



External Threat Feeds

This option is currently unavailable because no threat feed sources have been configured. To create one, go to Mail Policies > External Threat Feeds Manager.

Use a URL allowed list:  

Check URLs within

- Message Body and Subject
- Attachments
- All (Message Body, Subject and Attachments)

Action on URL within the message body and subject:

ريكفتلاو ءارجإل ءعجارم يجري . نيلوؤس مل اضعب يدل تاقرملا ءلازا راخي لضفي ال .
عوضوملاو ءلاسرلا صن نيوكت راخي ف طقف

ىلإ هيجوتلا ءءاعإ ءارجإ ءفاضإ عم ، لاثلما اذهك ثءءملا يوتءملا ءيفصت لماع نآلا وءبي
Cisco Secure Proxy:

Content Filter Settings			
Name:	URL_UNKNOWN		
Currently Used by Policies:	Default Policy		
Description:	Log messages with Unknown URLs. (Includes messages with attachments.)		
Order:	2 (of 3)		

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-no-reputation("", 1, 1)	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<<<=== LOGGING UNKNOWN URL FOR MAIL_LOGS ===>>>")	
2	URL Reputation	url-no-reputation-proxy-redirect-strip("",0)	

اهيف كوكشملا URL (نيوانع) ناونع

بوغرم ريغ نوكي دق وا رطاخم ءوجو ىلإ ريشي نأ نكمي يذلا URL ناونع كولس :هيف كوكشم
لءممب زيمتي مكءلا اذه نأ ال ، تاسسؤملا عيمءل أنمآ سيل رمألا اذه نأ نم مءرلا ىلعو .هيف
ءيولوألا روطءملا ريغ مكءلا يطيغي . (FP) ءبءاكلا ءيبءءيإل تاراشإل آيبسن نم أو ضفءم
ءرطء URL نيوانع ىلع يوتءت لئاسر روهظ ىلإ يءؤي دق يذلا رمألا ، نامألا ىلع ميلىستلل
ءعءارملا ءعب رطءلاو ءقءال تاكءمب يئوضلا ءسمل :هب ىصوملا ءارجإل

روءءلا نيلوؤس ملل نكمي ، ءفورءملا ريغ URL (نيوانع) ناونع نيوكتب انمق اننأل آرظن
وأ Cisco Security Proxy ىلإ اهيف كوكشم URL (نيوانع) ناونع لاسرا ءيفملا نم هئأ ىلع
لمءكلااب URL (نيوانع) ناونع رطء ءلازال ءارجإل ماءءتسا

Content Filter Settings	
Name:	URL_REWRITE_QUESTIONABLE
Currently Used by Policies:	Default Policy
Description:	Re-write URLs on the cusp of Untrusted reputation to be scanned again at click time, very small subset of URLs
Order:	3 (of 3)

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-5.90, -3.10 , "bypass_urls", 1, 1)	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	URL Reputation	url-reputation-proxy-redirect-strip(-5.90, -3.10,"",0)	

ةدياحم ل URL (نـوانع) ناونع

URL ناونع نأ، نعمب. هم يقيقت مت دق ف، كلذ عمو. يبلس وأ يباچي كولس نودب URL: دياحم
 ةعمس ل ماكأ نم ربكأ ل عزال وه اذف، لالت لابو. ألال ةفور عم رطاخم هل س ل
 اراض نوكي دق رخأ يوتحم دوجو نم ققحت ل ل ةيلات تاكحمب يئوض ل احس مل: هب ي صوم اراچ

لئاسر ل ادع م يقيقتب مق. ديدهت ك ةيبلس ةجر دب دياحم URL ناونع ةيؤر نيلوؤس مل ل نكمي
 اهب انمق يتل ةقير طال رارغ ل لع. ك ريدقتل أقفو ةدياحم ل URL (نـوانع) ناونع رارك و
 اهي ف كوكش مل URL (نـوانع) ناونعو ةفور عم ل ريغ URL (نـوانع) ناونع شي دحتب
 ريكفتل نكمي، Cisco Security Proxy ل URL (نـوانع) ناونع لاسر اراچ نم ةدافتس ل
 نم يبلس ل بانال نم ةيعرف ةومجم نم مضتي ص صخم قاطن وأ دياحم ل URL ناونع ي
 ةيفصت لماع ذي فنن عم ةدياحم ل URL نـوانع ل أصح ف لاثم ل اذ هضوي. ةدياحم ل نـوانع ل
 اذ دراو ل يوتحم ل

Content Filter Settings	
Name:	URL_NEUTRAL
Currently Used by Policies:	No policies currently use this rule.
Description:	Send questionable Neutral URLs to be scanned again at click time. (Includes messages with attachments.)
Order:	4 (of 4)

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-3.00, -0.50 , "", 1, 1)	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	URL Reputation	url-reputation-proxy-redirect-strip(-3.00, -0.50,"",0)	

(نيوانع) ناوانع أضيأ كانه . فينصت وأ ةعمس نود نم هنا أنايحأ غالبإل URL ناوانع نكمي تابلط ةرايزب لصفت ، هذه URL نيوانع دهاشم نع غالبإل . ئطاخ لكشبه اهفينصت م URL [Talos في ةعمس ل زكرم معد](#) ةحفص ىلع Cisco Talos نم بيولا فينصت

ةحفص [يتركذت](#) ىلع ةلجال ضرع كنكمي ، URL ناوانع نع غالبإل دعب

قيوستل لئاسرو ةراضل URL نيوانع فاشتكا متي ال وأ يئاوشعلا ديربلا ةحفاكم ةيفصت لماع ةطساوب راشتنالا

نم ديدعل ني ب نم طقف ناراي عم ال امه ام هتئف و قوملا ةعمس نأل اذه ثدحي نأ نكمي ديدحتل راشتنالا و يئاوشعلا ديربلا ةحفاكم ةيفصت لماع اهمدختست يتل ريباعملا لثم ، ءارج ذاختال ةبولطملا دودحل ضفخ بمق ، هذه ةيفصت لماع ةيساسح ةدايزل . اهمكحأ اهطاقس وأ لئاسرلا لزع وأ صوصن اهلمح لحتل اهلا دبتسا وأ URL نيوانع ةباتك ةداع

ناوانع ةعمس ةجرد ىلع ءانب لئاسرلا وأ يوتحمل ةيفصت لماع ءاشن كنكمي ، كلذ نم آل دب URL .

قحل مالا

ةرصتخملا URL نيوانعلا URL نيوانع ةيفصت معد ني كمت



ديربلا نامأل 13.0 ىتح AsyncOS 11.1 ىلع طقف مسقلا اذه قبطني : ةظالم
ينورتكلإلا

رماوأل رطس ةهجاو ةطساوب ةرصتخملا URL نيوانعلا URL نيوانع ةيفصت معد ءارج نكمي
(CLI) طقف websecurityadvancedconfig رمال مادختساب ،

```
<#root>
```

```
myesa.local>
```

```
websecurityadvancedconfig
```

```
...
```

```
Do you want to enable URL filtering for shortened URLs? [N]>
```

For shortened URL support to work, please ensure that ESA is able to connect to following domains: bit.ly, tinyurl.com, ow.ly, tumblr.com, ff.im,youtu.be, t1.gd, plurk.com, url4.eu, j.mp, goo.gl, yfrog

URL نېوانع ةي ف ص ت نېو ك ت ت اس رام م ل ض ف ا ق ي ق ح ت ل ر م ا ل ا ا ذ ه ن ي ك م ت ب Cisco ي ص و ت ر ص ت خ م URL ن ا و ن ع م ا د خ ت س ا ه ي ف م ت ي ت ق و ي ا ي ف د ي ر ب ل ا ت ا ل ح س س ك ع ن ت ، ه ن ي ك م ت د ر ج م ب ة ل ا س ر ل ا ل خ ا د :

Mon Aug 27 14:56:49 2018 Info: MID 1810 having URL: http://bit.ly/2tztQUi has been expanded to https://

mail_logs ل ا ث م ن م ، ة ل ا ق م ل ا ه ذ ه ي ف ح ض و م و ه ا م ك URL ن ي و ا ن ع ة ي ف ص ت ن ي ك م ت د ر ج م ب م ت ي ي ذ ل ا ي ل ص ا ل ا ط ا ب ت ر ا ل ا ل ي ح س ت ا ض ي ا م ت ي ا م ك ، bit.ly ط ا ب ت ر ا ل ي ح س ت ة ط ح ا ل م ا ن ن ك م ي ه ي ل ا ه ع ي س و ت .

• ة ي ف ا ض ا ت ا م و ل ع م

ق ن ا ث و Cisco Secure Email Gateway

- [ر ا د ص ا ل ا ت ا ط ح ا ل م](#)
- [م د خ ت س م ل ا ل ي ل د](#)
- [\(CLI\) ر م ا و ا ل ا ر ط س ة ه ج ا و ل ي ع ج ر م ل ا ل ي ل د ل ا](#)
- [Cisco Secure Email Gateway ل \(API\) ت ا ق ي ب ط ت ل ا ة ج م ر ب ة ه ج ا و ة ج م ر ب ة ل د ا](#)
- [Cisco Secure Email Gateway ي ف م د خ ت س م ل ا ح و ت ف م ل ا ر د ص م ل ا](#)
- [Cisco \(ن م ض ت ي\) ن م ي و ت ح م ل ا ن ا م ا ل ي ض ا ر ت ف ا ل ا ز ا ه ج ل ا ت ي ب ت ت ل ي ل د](#)

ق ن ا ث و Secure Email Cloud Gateway

- [ر ا د ص ا ل ا ت ا ط ح ا ل م](#)
- [م د خ ت س م ل ا ل ي ل د](#)

ب ي و ل ا ر ي د م و Cisco Secure Email ق ن ا ث و

- [ق ف ا و ت ل ا ة ف و ف ص م و ر ا د ص ا ل ا ت ا ط ح ا ل م](#)
- [م د خ ت س م ل ا ل ي ل د](#)
- [ر ي د م و Cisco Secure Email Gateway ل \(API\) ت ا ق ي ب ط ت ل ا ة ج م ر ب ة ه ج ا و ة ج م ر ب ة ل د ا ب ي و ل ا](#)
- [Cisco \(ن م ض ت ي\) ن م ي و ت ح م ل ا ن ا م ا ل ي ض ا ر ت ف ا ل ا ز ا ه ج ل ا ت ي ب ت ت ل ي ل د](#)

ق ن ا ث و Cisco Secure ت ا ج ت ن م

- [Cisco Secure ت ا ج ت ن م ة ط ف ح م ة ي م س ت ل ة ي ن ق ت ل ا ة ي ن ب ل ا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك ة ق م ق د ن و ك ت ن ل ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر م . ة ص ا خ ل م ه ت غ ل ب
Cisco مچرت م ا م د ق م م ا ت ل ا ة م ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د ع و چ ر ل ا ب م ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت م ل و ئ س م
Systems (ر ف و ت م ط ب ا ر ل ا) م ل ص ا ل ا م ل م چ ن ا ل ا دن ت س م ل ا