

ديربلا ۋارابۇ ئىمأتل URL ئىفصبىت نىوكت نەمآلا ينورتكىلىڭ Secure Email Gateway ۋە باحسلا ۋارابۇ Cloud Gateway

تايىوت حملا

[قىدقمىلا](#)

[ئىساساتامولۇم](#)

[ئىساسالاتابلىطتىملا](#)

[URL ئىوانع ئىفصبىت نىكىمىت](#)

[URL ئىوانع ئىفصبىت تاءارجاعاشىدا](#)

[قوقۇتمىلارىغى URL \(ئىوانع\) ناونع](#)

[قۇرۇغۇملارىغى URL \(ئىوانع\) ناونع](#)

[اھىف كۈشكىملا URL \(ئىوانع\) ناونع](#)

[قىياچىملا URL \(ئىوانع\) ناونع](#)

[لىئاسىرلا بىقىعت](#)

[ئىطاخ وحن ىللىق قىنصىملا وأۇ ئىفصبىت URL \(ئىوانع\) ناونع نىع غالبا](#)

[لماوع ئەتساپ قىيىسىتلى لىئاسىر و قراپلىلا URL ئىوانع فاشتاكا مەتىلى راشتنالا وأىئاوشىللا دىربلا ۋەفاكەم ئىفصبىت](#)

[قىچلىملىا](#)

[قرصىتىخىملا URL ئىوانع ئىفصبىت معىدىكىمىت](#)

[ئىفاضاتامولۇم](#)

[Cisco Secure Email Gateway](#)

[Secure Email Cloud Gateway](#)

[بىولارىدمۇ قىئاتو Cisco Secure Email](#)

[تاجىتنەم قىئاتو Cisco Secure](#)

قىدقمىلا

Cisco Secure Email Gateway ئىلەن ئىوانع ئىفصبىت نىوكت ئىفييڭ دەنسىملا اذە حضوى ئىوانع ئىفصبىت مادختسالا تاسرامىلار لىضىفأو ئىباحسلا ۋارابۇلار URL.

ئىساساتامولۇم

حمس. [ينورتكىلىلا دىربلا نامأىل AsyncOS 11.1](#) ئىوانع ئىفصبىت مىدقىت مەت لىئاسىرلا تاقفرم يىف URL ئىوانع نىع آثىحب حسمللى Cisco Secure Email نىوكتىپ رادصىلا اذە لىئاسىرلا ئىفصبىت لماوع مادختسەت. لىئاسىرلا كىلتىف اهنىوكت مەت يىتلە تاءارجىلا ذىفنت و لىئاسىرلا يىف URL ئىوانع دوجو نىم قىقىتلىل URL ناونع ئىفو URL ناونع ئەعمىسىوت حملەو ضرفىل لىئاسىرلا ئىفصبىت لماوع مادختسە لوصىف عجار،لىصافتىلا نىم دىزەل. تاقفرملا و رىغ URL ئىوانع نىم ئىامحلا" و "ئىوت حملە ئىفصبىت لماوع" و "ينورتكىلىلا دىربلا تاساسايس تەنرتىنالا ربع تامىلىع تىلا وأۇ [مەدختىسىملا لىيلد](#) يىف "اھىف بوغرملا رىغ وأۇ قوقۇتمىلا

ةمئاق يف اهيف بوغرملا ريغ وأ ققوثوملا ريغ تاطابترالا نم ئيامحلاو مكحتلا جمد متى، يوتحمل ئيفصتو، راشتنالاو، يئاوشعل ديربلا ئحفاكم تاييلمعب ئصالخا لمعلا راظتنا، يليل ام ىلع هذه مكحتلا لماع لمعت و لئاسرلا و:

- تاقفرمل او لئاسرلا يف ققوثوملا ريغ URL نيوانع نم ئيامحلا ئيلاعف ةدایز.
- راشتنالا ئيفصت لماع يف URL نيوانع ئيفصت جمد متى، كلذ ىلا ئفاضالاب لعفلاب كلتمت كتسس فم تناك اذا يتح قيبطتلل ئلباق ئزرعملا ئيامحلا هذه نوكت ىلا ئدنتسملاتاديدهتل نم ئلثامم ئيامح وأ Cisco Web Security Appliance نامألا زاهج لوحديلا ئطقون دناع تاديدهتل رظحت اهنألا بيولا
- ئجرد ىلع عانب عارج ذاختال لئاسرلا وأ يوتحمل ئيفصت لماع مادختس اًاضيأ كنكمي، لاثملال يبس ىلع لئاسرلا يف URL نيوانعل (WBRS) بيولا ىلا آدانتسا ئعمسلالا ئداعا ئفورعم ريغ وأ ئدياحم ئعمسب عتمت يتلا URL نيوانع ئباتك ئداعا كنكمي رقنلا تقو اهناما مييقتل Cisco Web Security Proxy ىلا اههيجوت.
- يئاوشعل ديربلا ىلع لضفالكشب فرعنلا
- تاييمزراخ نم اهريغ ولئاسرلا يف ئدوچوملا تاطابترالا ئيف و ئعمس زاهجل مدختسي، لاثملال يبس ىلع يئاوشعل ديربلا ديدحت يف ئدعاسم لليئاوشعل ديربلا فيعرعت نوكت نأ حجرألا نمف، يقيوسن بيو عقوم ىلا يمتنني ئلاسري ف طابترا كانه ناك اذا ئقيوسن ئلاسركل اسركل
- ئكرشلل لوبقملا مادختسالا تاسايس ضرف مععد
- ىلع، ئينوناقلا ريغ ئطشنألا وأ نيغلابل ىوتحم) URL نيوانع ئيف مادختس انكمي مادختسالا تاسايس ضرفل لئاسرلاو يوتحمل ئيفصت لماع عم (لاثملال يبس ئكرشلا ىدل لوبقملا
- آراركت رثكألا وحنلا ىلع اورقن نيذلا كتسس فم يف نيمدختسملا ديدحت كل حيتت رقنلا مت يتلا تاطابترالاو ئيامحلا اهتباتك ئداعا تمت ئلاسري ف URL ناونع قوف اعويش رثكألا وحنلا ىلع اهقوف.

 URL ناونع ئيفصت تمدق [ينورتكللإا ديربلا نامألا AsyncOS 11.1](#) رادصا يف: ظحالم ٥٥ جاو ىلع "websecurityadvancedconfig" رمألا مادختساب. ئرصتخملالا URL نيوانعل امعد رايخ ثيبحت مت. اهنويكت و ئرصتخملالا تامدخل ىلع فرعنلا نكمأ، (CLI) رماؤألا رطس، رادصا إلا اذه ىلا ئيقربلا داعب [ينورتكللإا ديربلا نامألا AsyncOS 13.5](#) يف اذه نيوكتللا URL نيوانع عيسوت ليطعتل رايح دجوي ال. ئرصتخملالا URL نيوانع عيمج عيسوت متى ينورتكللإا ديربلا نامألا AsyncOS 13.5 ماظنب Cisco يصوت، ببسلا اذهل و. ئرصتخملالا ىلع عالطالا ئجري. URL نيوانع نع عافدلل ئيامحلا لئاسو ثدحأ ريفوتل ثدحأ رادصا وأ مادختسملا ليلد يف "اهيف بوغرملا ريغ وأ ئراضلا URL نيوانع نم ئيامحلا" لصف ماظنل (CLI) رماؤألا رطس ئهجاول يعجملا ليلدلاو تنرتنا إلا رباع تاميلعنتلا Cisco Email Security Appliance.

 ديربلا نامألا [AsyncOS 14.2](#) مادختسإ متى، دنتسملالا اذهل ئبسنلاب: ظحالم مدقملالا ئشاشلا تاطقلو ئلثملل [ينورتكللإا](#).

 قمعتم URL ناونع عافدليلد اضيأ Cisco نم نمألا ينورتكللإا ديربلا رفوي: ظحالم ايف docs.ces.cisco.com.

ئيساسألا تابلطتملا

،ةباحسلا ةرآب ع وأ Cisco Secure Email Gateway URL نيوانع ئيفوصت لكتنيوك دن ع ضعب يلى امي ف .ةبولطملا فئاًظولا ىلع دمتعت ئرخأ تازيم نيوكت أضيأ كيلع بجي نيوانع ئيفوصت عم بنج ىلإ آبنج اهنـيـكـمـتـ مـتـيـ يـتـلـاـ ئـيـجـذـوـمـنـلـاـ تـازـيـمـلـاـ:

- ديربلا ةحفاكم صحفلا ةزيم ناف ،يـئـاوـشـعـلـاـ دـيـرـبـلـاـ دـضـ ةـنـسـحـمـ ئـيـامـحـ ىـلـعـ لـوـصـحـلـلـ ربـتـعـتـ .اهـبـ لـوـمـعـمـلـاـ دـيـرـبـلـاـ دـسـاـيـسـلـ ًأـقـفـوـيـمـوـمـعـ لـكـشـبـ اـهـنـيـكـمـتـ بـجـيـ يـئـاوـشـعـلـاـ دـيـرـبـلـاـ ةـحـفـاـكـمـ Cisco IronPort ئـيـفـ نـمـ اـمـاـ ةـزـيمـ يـئـاوـشـعـلـاـ دـيـرـبـلـاـ ةـحـفـاـكـمـ ةـزـيمـ دـيـرـبـلـاـ Cisco (IMS) .
- لمـاـعـ وـأـ رـاـشـتـنـالـاـ ئـيـفـوصـتـ لـمـاـعـ نـافـ ،ةـرـاضـلـاـ جـمـارـبـلـاـ دـضـ ةـنـسـحـمـ ئـيـامـحـ ىـلـعـ لـوـصـحـلـلـ ئـسـاـيـسـلـ ًأـقـفـوـيـمـوـمـعـ لـكـشـبـ اـهـنـيـكـمـتـ بـجـيـ (VOF) تـاسـورـيـفـلـاـ رـاـشـتـنـاـ ئـيـفـوصـتـ اـهـبـ لـوـمـعـمـلـاـ دـيـرـبـلـاـ
- مـاـدـخـتـسـالـاـ تـاسـاـيـسـ ضـرـفـلـ وـأـ URL نـاـونـعـ ًعـمـسـ ىـلـاـ ةـدـنـتـسـمـلـاـ تـاءـعـاـرـجـ إـلـلـ ئـبـسـنـلـابـ اـهـنـيـكـمـتـ بـجـيـ VOF نـافـ ،يـوـتـحـمـلـاـوـلـيـاـسـرـلـاـ ئـيـفـوصـتـ لـمـاـعـ مـاـدـخـتـسـابـ لـوـبـقـمـلـاـ يـمـوـمـعـ لـكـشـبـ

نيوانع ئيفوصت نيكـمـتـ URL

URL نـيـوانـعـ ئـيـفـوصـتـ ذـيـفـنـتـلـ ةـزـيمـلـاـ نـيـكـمـتـ الـوـأـ كـيـلـعـ بـجـيـ Cisco Secure Email Gateway اوـنـمـ URL نـيـوانـعـ ئـيـفـوصـتـ نـيـكـمـتـ لـوـفـسـمـلـلـ نـكـمـيـ .ةـبـاحـسـلـاـ ةـرـآـبـ عـ وأـ (CLI) رـمـاـوـلـاـ رـطـسـ ةـهـجـاوـ وـأـ (GUI) ئـيـمـوـسـرـلـاـ مـدـخـتـسـمـلـاـ

تـامـدـخـ ىـلـاـ لـقـتـنـاـ ،ئـيـمـوـسـرـلـاـ مـدـخـتـسـمـلـاـ ةـهـجـاوـنـمـ URL نـيـوانـعـ ئـيـفـوصـتـ نـيـكـمـتـلـ نـيـكـمـتـ قـوـفـ رـقـنـاـوـ URL نـيـوانـعـ ئـيـفـوصـتـ > نـامـأـلـاـ

ادـهـ نـمـضـتـيـ URLـ نـيـوانـعـلـ ًعـمـسـلـاـوـ تـائـفـلـاـ ئـيـفـوصـتـ لـمـاـعـ نـيـكـمـتـ قـوـفـ رـقـنـاـ ،كـلـذـ دـعـبـ نـيـوانـعـ دـدـعـلـ ىـصـقـأـلـاـ دـحـلـاـوـ URLـ نـيـوانـعـ نـعـ ثـحـبـلـاـ ًلـهـمـلـ تـاسـرـاـمـمـلـاـ لـضـفـأـ مـيـقـ لـاثـمـلـاـ URLـ (نيـوانـعـ) نـاـونـعـ لـيـجـسـتـ رـايـخـ نـكـمـيـوـ ،اـهـصـفـ مـتـ يـتـلـاـ URLـ

The screenshot shows the 'URL Filtering Overview' page. At the top, there's a checked checkbox for 'Enable URL Category and Reputation Filters'. Below it, there's a dropdown menu labeled 'Use a URL allowed list' with 'None' selected. To the right of this, there's a section for 'Web Interaction Tracking' with a checked checkbox for 'Enable Web Interaction Tracking'. Under 'Advanced Settings', there are three rows of configuration: 'URL Lookup Timeout' set to 5, 'Maximum Number of URLs scanned in Message Body' set to 400, and 'Maximum Number of URLs scanned in Message Attachments' also set to 400. Below these is a section for 'Rewrite URL text and HREF in Message' with two radio button options: 'Yes' (selected) and 'No'. Finally, there's a 'URL Logging' section with a checked checkbox for 'Enable'.

يلاحللا تقولا يف نيوكتلا ىلع اهتيرجأ يتلا تارييغتلاب مازتللا نم دكأت: ظحالم.

نیوانع ۋېفصت تاءارجإ ئاشنإ URL

دوجوملا URL نیوانع دض عارجإ ذختت ال اهناف، اهدرفم بـ URL نیوانع ۋېفصت نیكمت دنعتاقفرم ىلع يوتحت يتلا لئاسرلا وأ لئاسرلا لخاد.

ىلإ ئېسنىلاب تاقفرمل او لئاسرلا يف ئەنمضملا URL (نیوانع) ناونع مىيقت متي نيمضتل URL ناونعل ۋە حلاص ۋە سلس يأ مىيقت متي. رداصل او دراولدا دىربلا تاسايىس: ئيلاتلا تانوكملا بـ لسالس

- HTTP وـ HTTPS وـ WWW
- IP نیوانع وـ لاجملما
- (:) نيتطقنب ۋە قوبسم ذفانملا ماقرا
- ۋەریغص وـ ۋەریبک فرحأ

متى مل اذى URL نیوانع مظعمل Mail_Log URL ناونع لجس لاخدا نوكى: ظحالم. ۋە لئاسرلا فرعم لئاسرلا بقعت ۋە جارم ىجىرىف، يف mail_logs ناونع لىجىست (MID). URL ناونع لىيصادفت "صخت بـ يوبت ۋە مالع لئاسرلا بقعت نممضتىي اـ URL".

اذا ، هناف ، ال مأ اهي ف بوغرم ريغ ئلاسرلا تناك اذا ام ديدحتل URL نيوانع ماظنلا مّيقى امدنع
ةرداصلا لئاسرلا ىلع ئلاسرلا ئيلولوألا يطعي ، لمحلا ئرادال رمالا مزل.

يف URL ناونع ئيف وأ URL ناونع ئعمس ىلا آدانتسا لئاسرلا ىلع تاءارجإ ذيفنت كنكمي
تاقفرملما تاذ لئاسرلا وأ ئلاسرلا صن.

عيمج ىلع (يئاهنلا ئارجإ) طاقس إلأ ئارجإ قيبيطت يف بغرت تناك اذا ، لاثملما ليبس ىلع
ناونع ئيف عونلا نم اطرش فضأف ، رابكلا ئيف يف URL نيوانع نمضتت يتلا لئاسرلا
رابكلا ئيف ديدحت عم URL.

لئاسرلا عيمج ىلع هراتخت يذلا ئارجإ قيبيطت متيسف ، ئيف ددحت مل اذا.

ريغو ، اهي ف كوكشملماو ، ئدياحملماو ، ئلّصفملماو ، ئقوثوملا URL نيوانع ئعمس تاجرد قاطن نا
مدختسا . صсх قاطن ديدحت كنكمي . ريرحتلل لباق ريغ واقبس مادحه نوكى ئقوثوملا
اهتعمس ئجرد دعب متي مل يتلا URL نيوانعل "فوريغ ريغ".

ناك اذا ثيحب ىوتحملل ئيفصت لمعاع ئاشنـا كنكمي ، ئارجإ ذاخت اواعيرس URL نيوانع صحفل
مدختسملـا ئهجـونـم . ئارجإ قيبيطـتـ مـتـيـسـ يـلـاتـلـابـفـ ،ـ حـلـاصـ URL نـاـونـعـ ئـلـاسـرـلـلـ
لماع ئفاضـاـ > درـاـولـاـ ىـوـتـحـمـلـاـ ئـيـفـصـتـ لـمـاـعـ < دـيـرـبـلـاـ تـاـسـاـيـسـ ىـلـاـ لـقـتـنـاـ ،ـ (ـGـUـIـ)ـ ئـمـوسـرـلـاـ
ـ ئـيـفـصـتـ.

يـلـاتـلـاـ وـحـنـلـاـ ىـلـعـ URL نـيـوـانـعـ بـ ئـطـبـتـرـمـلـاـ تـاءـارـجـإـاـ نـوـكـتـ

- ناونع نم رطخلا ئلازا URL

- ناكـمـابـ لـازـيـ الـ نـكـلـوـ ،ـ هـقـوـفـ رـقـنـلـلـ لـبـاـقـ رـيـغـ هـلـعـ جـلـ URL نـاـونـعـ لـيـدـعـتـ مـتـيـ
ـ نـاـونـعـ يـفـ ئـيـفـاضـاـ فـورـحـ لـاخـداـ مـتـ)ـ .ـ دـوـصـقـمـلـاـ URL نـاـونـعـ ئـعـارـقـ ئـلـاسـرـلـاـ مـلـتـسـمـ
ـ (ـيـلـصـأـلـاـ URLـ)

- ئيـصـنـ ئـلـاسـرـبـ URL نـاـونـعـ ئـدـاعـاـ

- رـبـعـ رـوـرـمـلـلـ هـقـوـفـ رـقـنـلـاـ دـنـعـ URL نـاـونـعـ ئـبـاتـكـ ئـدـاعـاـ مـتـتـ Cisco Security Proxy
ـ ئـلـعـ رـذـعـتـيـ دقـ ،ـ Cisco Security Proxyـ مـكـحـ ئـلـاـ آـدانـتـسـاـ يـفـاضـاـ قـقـحـتـ ئـارـجـإـ
ـ عـقـوـمـلـاـ ئـلـاـ لـوـصـوـلـاـ مـدـخـتـسـمـلـاـ

- ئيـصـنـ ئـلـاسـرـبـ URL نـاـونـعـ ئـدـاعـاـ

- ئـلـاسـرـلـاـ لـخـادـ URL نـاـونـعـ ئـبـاتـكـ ئـدـاعـاـ لـوـفـسـمـلـلـ نـكـمـيـ ،ـ رـايـخـلـاـ اـذـهـ مـادـخـتـسـابـ
ـ دـيـعـبـلـاـ ضـرـعـتـسـمـلـاـ لـزـعـلـ آـيـجـرـاخـ هـلـاسـرـاـوـ

ئقوثوملا ريغ URL (نيوانع) ناونع

رطح ئمئاق ئبتع وه اذه .ـ هـيـفـ بـوغـرمـ رـيـغـ وأـ رـاضـ وأـ ئـيـاغـلـلـ ئـيـسـ URLـ كـولـسـ :ـ هـبـ قـوـثـومـ رـيـغـ
ـ URLـ نـيـوـانـعـ نـأـلـ اـهـرـظـحـ مـتـيـ الـ لـئـاسـرـ كـانـهـ نـوـكـتـ نـأـ نـكـمـيـ ،ـ كـلـذـعـمـ وـ ،ـ اـهـبـ ئـصـوـمـلـاـ نـامـأـلـاـ
ـ نـامـأـلـاـ ىـلـعـ مـيـلـسـتـلـلـ ئـيـولـوـأـلـاـ يـطـعـيـ .ـ لـقـأـ دـيـدـهـتـ ىـوـتـسـمـ ىـلـعـ يـوـتـحـتـ اـهـيـفـ ئـدـوـجـوـمـلـاـ

(ـلـمـاـكـلـابـ اـهـفـذـحـ وأـ ئـلـاسـرـلـاـ لـزـعـ لـوـفـسـمـلـلـ نـكـمـيـ)ـ .ـ رـظـحـلـاـ :ـ هـبـ ئـصـوـمـلـاـ ئـارـجـإـ)

ـ نـعـ فـشـكـلـلـ URLـ نـيـوـانـعـ ئـيـفـصـتـلـ ىـوـتـحـمـلـاـ ئـيـفـصـتـ لـمـاـعـلـ آـقـاـيـسـ لـاثـمـلـاـ اـذـهـ رـفـوـيـ
ـ ئـقـوـثـومـلـاـ رـيـغـ URLـ نـيـوـانـعـ :

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 ناونع صحفب Cisco Secure Email موقى، اذه ىوتحمل اهيف صت لماع قيبطت عم لزع ةدحوي ف ئلاس رلا عضيوا (-6.00 - 10.00) ةجردب ةقوثوملا ريع ةعمسلـا URL_UNTRUSTED. رمـأـلـاـ نـمـ لـاثـمـ يـلـيـ اـمـيـفـ mail_logs:

<#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 inbox
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
```

هـلـيـجـسـتـ مـتـوـهـ بـ قـوـثـومـلـاـ عـقـوـمـ رـيـغـ URLـ ihaveabadreputation.comـ دـدـحـمـ رـبـتـعـيـ ئـلـاـ هـعـقـوـمـ تـلـزـعـوـهـ بـ قـوـثـومـ رـيـغـ URLـ نـاـونـعـ URLـ ةـيـفـصـتـ تـفـشـكـ 9.5ـ مـقـرـلـاـ ئـلـعـ URL_UNTRUSTED.

ةيفرضت لمامع نيكمت لاح يف طقف كلذ ىلع آلاثم mail_logs نم قباسلا لاثمل رفوي جهـنـلـ ةـيـفـاضـاـ تـامـدـخـ نـيـكـمـتـ مـتـ اـذـاـ درـاـوـلـاـ دـيـرـبـلـاـ ةـسـاـيـسـلـ URLـ نـيـوانـعـ ةـيـفـصـتـلـ ىـوـتـحـمـلـ دقـ نـاـكـ اـذـاـ اـمـ ىـلـاـ ئـرـخـأـلـاـ تـامـدـخـلـاـ رـيـشـتـسـفـ ،ـيـئـاوـشـعـلـاـ دـيـرـبـلـاـ ةـحـفـاـكـمـ لـثـمـ ،ـهـسـفـنـ دـيـرـبـلـاـ URLـ نـاـوـنـعـ لـاـثـمـ يـفـ .ـاهـبـ ةـصـاخـلـاـ دـعـاـوـقـلـاـوـ تـامـدـخـلـاـ كـلـتـ نـمـ URLـ نـاـوـنـعـ فـاشـتـكـاـ مـتـ مـتـيـوـ ،ـدـرـاـوـلـاـ دـيـرـبـلـاـ ةـسـاـيـسـلـ Cisco Anti-Spam Engine (CASE)ـ كـرـحـمـ نـيـكـمـتـ مـتـ ،ـهـسـفـنـ يـفـ ًـالـوـأـكـلـذـ ىـلـاـ ئـرـاشـإـلـاـ مـتـ .ـيـئـاوـشـعـ دـيـرـبـكـ ًـيـبـاجـيـاـ نـوـكـيـلـ ٥ـدـيـدـحـتـوـ ةـلـاـسـرـلـاـ صـنـ صـحـفـ ًـجـلـاعـمـ تـايـلـمـعـ رـاسـمـ يـفـ ىـلـوـأـلـاـ ةـمـدـخـلـاـ يـهـ يـئـاوـشـعـلـاـ دـيـرـبـلـاـ ةـحـفـاـكـمـ نـأـلـ ًـأـرـظـنـ mail_logsـ دـيـرـبـلـاـ ةـجـلـاعـمـ تـايـلـمـعـ رـاسـمـ يـفـ ًـأـقـحـالـ ىـوـتـحـمـلـاـ ةـيـفـصـتـ لـمـاـعـ يـتـأـتـ .ـدـيـرـبـلـاـ

<#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
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 inbox
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 matched
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
```

تـايـوـتـحـمـ عـمـ قـبـاطـتـ تـاجـرـدـ وـأـ دـعـمـسـ وـأـ دـعـاـوـقـ ىـلـعـ CASEـ وـأـ دـعـمـسـ وـأـ دـعـاـوـقـ ىـلـعـ IPASـ دـصـرـ مـتـ ،ـلـاـثـمـلـاـ اـذـهـ يـفـ .ـاهـدـحـوـ URLـ نـيـوانـعـ تـادـيـدـهـتـ نـعـ فـشـكـلـلـ ًـدـدـحـمـ ًـلـاـسـرـ وـأـ لـاجـمـ وـأـ لـسـرـ ihaveabadreputation.comـ (ISQـ)ـ يـئـاوـشـعـلـاـ دـيـرـبـلـاـ لـزـعـلـ ًـيـلـعـ ًـمـالـعـ عـضـوـمـتـوـ ،ـلـزـعـوـ ،ـلـزـعـوـ URL_UNTRUSTEDـ URL_QUARANTINE_UNTRUSTEDـ .ـكـلـذـ نـمـ ًـلـاـسـرـلـاـ رـيـرـحـتـ مـتـيـ اـمـدـنـعـ ًـالـوـأـ URL_UNTRUSTEDـ لـزـعـلـاـ ًـدـدـحـوـ ىـلـاـ ًـلـاـسـرـلـاـ لـقـتـنـتـ لـزـعـلـاـ رـايـعـمـبـ ةـصـاخـلـاـ نـيـوـكـتـلـاـ رـيـيـاعـمـ /ـيـنـمـزـلـاـ دـحـلـاـ ءـافـيـتـسـاـ دـنـعـ وـأـ لـوـفـسـمـ ةـطـسـاـوبـ لـزـعـلـاـ URL_UNTRUSTEDـ ىـلـاـ كـلـذـ دـعـبـ ًـلـاـسـرـلـاـ لـقـنـ مـتـيـ ،ـISQـ .ـ

ةـيـفـصـتـلـ ةـيـفـاضـاـ تـاءـارـجـ اوـ طـورـشـ نـيـوـكـتـ نـكـمـيـ ،ـلـوـفـسـمـلـاـ تـالـيـضـفـتـ ىـلـاـ ًـادـانـتـسـاـ ىـوـتـحـمـلـاـ

ةفorumلا ريغ URL (نيوانع) ناونع

ديدهتل اىوتسم ىلع مكح ديكلأتل تازيم ضرعي ال وأاقباس ٥مميقت متى مل: ةفorum ريغ ريغ مكحلا اذه . ةعمس ٤جرد ديتحت ةيفاك تانايip URL ناونع ةعمس ٤مدخ ىدل رفوتت ال URL ناونع ةعمس ب ةصالخ ئاسايis يف ةرشابم ةدراولـا تاءارجـالـل بـسـانـمـاـ.

اراض نوكـي دق رخـآ ئـوـتـحـمـ دـوـجـوـنـمـ قـقـحـتـلـلـ ئـيـلـاتـ تـاـكـرـحـمـبـ يـئـوـضـلـاـ حـسـمـلـاـ :هـبـ ئـصـوـمـ ئـارـجـاـ.

ىـلـعـ يـوـتـحـتـ URLـ نـيـوانـعـ "ـةـعـمـسـ نـوـدـ نـمـ"ـ وـأـ ئـفـورـمـلـاـ رـيـغـ URLـ (ـنـيـوانـعـ)ـ نـاـونـعـ نـوـكـيـ نـأـ نـكـمـيـ نـوـكـتـ نـأـ نـكـمـيـ الـوـ ئـمـوـدـعـمـ وـأـ ئـلـيـلـقـ تـارـايـزـ ئـكـرـحـ تـدـهـشـ URLـ (ـنـيـوانـعـ)ـ نـاـونـعـ وـأـ ئـدـيـدـجـ تـالـاجـمـ ئـقـوـثـومـ رـيـغـ ىـلـاـ نـيـوانـعـلـاـ هـذـهـ لـوـحـتـتـ نـأـ نـكـمـيـ . دـيـدـهـتـلـاـ ئـوـتـسـمـ ىـلـعـ مـكـحـ وـقـمـيـقـمـ ئـعـمـسـ اـلـ اـذـهـ URLـ نـاـونـعـلـ ٤ـبـسـنـلـابـ . اـهـيـشـنـمـ وـاـهـلـاجـمـ نـعـ تـاـمـوـلـعـمـلـاـ نـمـ دـيـزـمـ ىـلـعـ لـوـصـحـلـاـ مـتـيـ اـمـدـنـعـ نـمـضـتـيـ دـحـاوـ وـأـ لـيـجـسـتـلـلـ ئـوـتـحـمـ ئـيـفـصـتـ لـمـاعـ مـادـخـتـسـابـ Ciscoـ يـصـوتـ ،ـ(ـهـذـهـ URLـ نـيـوانـعـ)ـ نـاـونـعـ لـاسـرـاـ مـتـيـ AsyncoSـ ،ـ 14.2ـ رـادـصـاـلـاـ نـمـ ٤ـرـابـعـاـ . ئـفـورـمـلـاـ رـيـغـ URLـ نـاـونـعـ فـاشـتـكـاـ لـلـيـلـحـتـلـلـ Talos Intelligence Cloud Serviceـ ئـيـبـاحـسـلـاـ ئـمـدـخـلـاـ ىـلـاـ ئـفـورـمـلـاـ رـيـغـ URLـ (ـنـيـوانـعـ)ـ ،ـكـلـذـ ىـلـاـ ئـفـاضـاـ . ئـفـلـتـخـمـلـاـ دـيـدـهـتـلـاـ تـارـشـفـمـ ىـلـعـ هـلـيـغـشـتـ مـتـيـ يـذـلـاـ قـيـمـعـلـاـ URLـ نـاـونـعـ ،ـنـاـونـعـ ىـلـاـ ٤ـرـاشـاـلـوـؤـسـمـلـلـ ئـفـورـمـلـاـ رـيـغـ URLـ (ـنـيـوانـعـ)ـ نـاـونـعـلـ دـيـرـبـلـاـ لـجـسـ لـاخـداـ رـفـوـيـ نـيـوانـعـ ئـيـامـحـ مـادـخـتـسـابـ نـكـمـمـلـاـ حـالـصـاـلـاوـ (ـMIDـ)ـ ٤ـلـاسـرـ فـرـعـمـ يـفـ ئـنـمـضـمـلـاـ URLـ (ـنـيـوانـعـ)ـ URLـ (ـنـيـوانـعـ)ـ تـاـقـيـبـطـتـلـاـ قـجـمـبـ ئـجـاـولـ Cisco Secure Emailـ بـاسـحـ تـاـدـادـعـ نـيـوـكـتـ ئـيـفـيـكـ عـجـاـرـ (ـAPIـ)ـ .ـتـاـمـوـلـعـمـلـاـ نـمـ دـيـزـمـ ىـلـعـ لـوـصـحـلـلـ (ـMicrosoft Azureـ (ـMicrosoft 365ـ)ـ - Ciscoـ)ـ يـفـ

نـيـوانـعـ نـعـ فـشـكـلـلـ URLـ نـيـوانـعـ ئـيـفـصـتـلـ ئـوـتـحـمـ ئـيـفـصـتـ لـمـاعـلـ آـقـاـيـسـ لـاـثـمـلـاـ اـذـهـ رـفـوـيـ ئـفـورـمـلـاـ رـيـغـ URLـ :

Content Filter Settings			
Name:	URL_UNKOWN		
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 =====>>")	

نـاـونـعـ نـعـ آـثـبـ صـحـفـلـاـبـ Cisco Secure Emailـ مـوـقـيـ ،ـاـذـهـ ئـوـتـحـمـلـاـ ئـيـفـصـتـ لـمـاعـ مـادـخـتـسـابـ رـمـأـلـاـ نـمـ لـاـثـمـ يـلـيـ اـمـيـفـ mail_logsـ .ـيـفـ لـجـسـ رـطـسـ ئـبـاتـكـوـ ئـفـورـمـ رـيـغـ ئـعـمـسـ بـ mail_logsـ:

<#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
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
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 inbox
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.inter
Tue Jul 5 16:51:56 2022 Info: Message finished MID 16 done
Tue Jul 5 16:52:01 2022 Info: DCID 13 close
```

هـتـدـهـاـشـمـ مـتـتـوـعـمـسـ هـلـسـيـلـ URLـ mytest.example.com/test_url_2022070503ـ نـاـونـعـ
دـنـعـ لـجـسـلـاـ رـطـسـ ةـبـاتـكـبـ URLـ UNKNOWNـ ىـوـتـحـمـلـاـ ئـيـفـصـتـ لـمـاعـ مـاقـ.ـ مـاـدـخـتـسـابـ
ئـلـاـ هـنـيـوـكـتـ mail_logsـ.

```

Tue Jul  5 16:54:42 2022 Debug: ECS: Finish polling
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation service notified.
Tue Jul  5 16:55:42 2022 Debug: ECS: Initiating remediation
Tue Jul  5 16:55:42 2022 Info: ECS: Initiating message remediation:
{'from': ['test@test.com'], 'URL': 'http://mytest.example.com/test_url_2022070503', 'message ID':
'<20220705165003.1870404@ip-172-31-43-120.us-east-2.compute.internal>', 'MID': 16, 'verdict':
'MALICIOUS', 'message UUID': 'e90dec74-f50b-4a63-9ab2-6adda4fcf422'}
Tue Jul  5 16:55:42 2022 Debug: ECS: Unprocessed Remediation Data : [{"url_hash":
'8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyxxyy', 'message_details': '{"mid": 16,
"birth_time": "165039913", "from_addrs": ["test@test.com"], "recipients": ["■ ■ ■ ■ ■ ■"], "delivery_status": 1, "remediation_req_status": 3}', 'created_at': '2022-07-05 16:52:42.04515', 'verdict': '{"url": "http://mytest.example.com/test_url_2022070503", "verdict": "MALICIOUS"}', 'message_uuid': 'e90dec74-f50b-4a63-9ab2-6adda4fcf422', 'message_id': '<20220705165003.1870404@ip-127-0-0-1.internal>'}
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation records: [
  [
    {
      "id": 16,
      "url": "<20220705165003.1870404@ip-127-0-0-1.internal>",
      "birth_time": "165039913",
      "status": "delete",
      "req_status": 3,
      "details": "[{"url": "http://mytest.example.com/test_url_2022070503", "conviction_timestamp": "2022-07-05 16:52:42.04515", "url_hash": "8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyxxyy"}]",
      "recipients": [
        "test@test.com"
      ]
    }
  ]
]
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation initiated.
Tue Jul  5 16:55:42 2022 Debug: ECS: Successfully recorded remediation initiation status into datastore.

```

هـل اـمـتـكـ او هـسـفـنـ حـالـصـ إـلـاـ عـاـعـدـتـسـ اـمـدـنـعـ،ـيـلـاتـلـابـ كـلـذـ دـعـبـوـ:

```

Tue Jul  5 16:55:42 2022 Info: Message 16 containing URL 'http://mytest.example.com/test_url_2022070503'
Tue Jul  5 16:55:55 2022 Info: Message 16 was processed due to URL retrospection by Mailbox Remediation

```

فـورـعـمـلـاـ رـيـغـ (URLـ نـيـوانـعـ)ـ نـاـونـعـ صـوـصـخـ بـعـارـجـ |ـ ذـاـخـتـاـ رـاـبـتـعـالـاـ يـفـ نـوـلـوـفـسـمـلـاـ ذـخـأـيـ نـأـ بـجـيـ
ـتـاـقـفـرـمـلـاـ وـيـنـوـرـتـكـلـإـلـاـ دـيـرـبـلـاـ لـئـاسـرـيـفـ ةـظـوـحـلـمـ دـدـايـزـ كـانـهـ تـنـاـكـ اـذـاـ .ـمـهـرـيـدقـتـ بـسـ
ـفـاضـإـلـابـ .ـيـوـتـحـمـلـاـ ةـيـفـصـتـ لـمـاـعـ رـيـرـقـتـ وـ ةـعـجـارـمـ يـجـرـيـفـ ،ـلـاـيـتـحـالـاـبـ ةـقـلـعـتـمـلـاـ
ـفـورـعـمـلـاـ رـيـغـ (URLـ نـيـوانـعـ)ـ نـاـونـعـ هـيـجـوـتـ ةـدـاعـإـلـ نـيـوـكـتـلـاـ عـارـجـ |ـ نـيـلـوـفـسـمـلـلـ نـكـمـيـ ،ـكـلـذـىـلـاـ
ـ>ـ عـارـجـ |ـ ةـفـاضـإـلـاـ لـقـتـنـاـ ،ـلـاـثـمـلـاـ اـذـهـ يـفـ .ـرـقـنـلـاـ تـقـوـمـيـقـتـلـ Ciscoـ نـاـمـأـ لـيـكـوـ ةـمـدـخـىـلـاـ
ـانـبـ صـاخـلـاـ ةـيـفـصـتـ لـمـاـعـ لـخـادـ URLـ UNKNOWNـ ةـيـفـصـتـ لـمـاـعـ URLـ UNKNOWNـ

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

1

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:

None



Check URLs within

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

Action on URL within the message body and subject:

 ریکفتل او عاجلا ۃعجارت یجڑی . نیلوؤسملا ضعب یدل تاقفرملہ ۃلزا رایخ لضفی ال . عوضومل او ۃلاسرلا صن نیوکت رایخ یف طقف

ىلإ هيچوتلا ۋە داعا ئارج ۋە فاضا عەم، لاثملا اذەك ثەدمىلا ىوتحملا ۋە يىفصىت لىماع نآلا ودبى Cisco Secure Proxy:

Content Filter Settings			
Name: <input type="text" value="URL_UNKNOWN"/> Currently Used by Policies: Default Policy Description: Log messages with Unknown URLs. (Includes messages with attachments.) Order: <input type="text" value="2"/> (of 3)			
Conditions			
Add Condition...			Delete
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)	

اھي ف کوکش مل ا URL (نیوانع) ناونع

بوجرم ریغ نوکی دق وأ رطاخم دوجو لى! ریشی نأ نكمي يذلا URL ناونع كولس :هیف كوكشم لدعمب زيمتى مكحلا اذه نأ ال، تاسسۇملا عيمجىل گۈنمە سىيل رمألا اذه نأ نم مغىرلا ئىلعلو. هېف ئىولولار روظىملا ریغ مكحلا يطعى (FP). ئىباچىي إلارا شاراشىلل آيىبسن نمآ وصفخىنم ئىللىك URL نىوانع ئىلع يوتحتلى ئاسىر روهەتلى يىدۇي دق يذلا رمألا، نامالا ئىلع مىلسەتلل ئەعجارملا دعب روظىلار وققحال تاكىرىم بىئىوضىلا حسىملا :بىصۇملا ئارجىلا.

روثعلـا نـيلـوـفـسـمـلـلـنـكـمـيـ،ـفـوـرـعـمـلـرـيـغـ URLـ(ـنـيـوـانـعـ)ـنـاـوـنـعـنـيـوـكـتـبـاـنـمـقـاـنـنـأـلـأـرـظـانـ وـأـ Cisco Security Proxyـ كـوـكـشـمـ URLـ(ـنـيـوـانـعـ)ـنـاـوـنـعـلـاسـرـاـدـيـفـمـلـنـمـهـنـأـىـلـعـ لـمـاـكـلـابـ URLـ(ـنـيـوـانـعـ)ـنـاـوـنـعـرـطـخـقـلـاـزـالـعـاـجـإـلـاـمـادـخـتـسـاـ

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)	

ةدياحملـا URL (نيوانع) ناوـنـع

نـاوـنـع نـأـ،ـيـنـعـمـبـ.ـمـيـيـقـتـ مـتـ دـقـفـ،ـكـلـذـعـمـوـ.ـيـبـلـسـ وـأـيـبـاجـيـاـ كـولـسـ نـوـدـبـ URLـ:ـدـيـاحـمـ.ـعـمـسـلـاـ مـاـكـحـأـ نـمـ رـبـكـأـلـاـ عـزـجـلـاـ وـهـ اـذـهـفـ،ـيـلـاتـلـابـوـ.ـأـيـلـاحـ ةـفـورـعـمـ رـطـاخـمـ ـهـ لـسـيـلـ.ـاـرـاضـ نـوـكـيـ دـقـ رـخـآـيـوـتـحـمـ دـوـجـوـنـمـ قـقـحـتـلـلـ ةـيـلـاتـ تـاـكـرـحـمـبـ يـئـوـضـلـاـ حـسـمـلـاـ:ـهـ بـىـصـوـمـ عـارـجـاـ.

لـيـاسـرـلـاـ دـدـعـ مـيـيـقـتـبـ مـقـ.ـدـيـدـهـتـكـ ةـيـبـلـسـ ةـجـرـدـبـ دـيـاحـمـ URLـ نـاوـنـعـ ةـيـفـرـنـيـلـوـؤـسـمـلـلـ نـكـمـيـ.ـاهـ اـنـمـقـ يـتـلـاـ ةـقـقـيـرـطـلـاـ رـاـغـىـلـعـ.ـكـرـيـدـقـتـلـ أـقـفـوـ ةـدـيـاحـمـلـاـ URLـ (ـنـيـوـانـعـ)ـ نـاوـنـعـ رـاـرـكـتـوـ.ـاهـيـفـ كـوـكـشـمـلـاـ URLـ (ـنـيـوـانـعـ)ـ نـاوـنـعـوـ ةـفـورـعـمـلـاـ رـيـغـ URLـ (ـنـيـوـانـعـ)ـ نـاوـنـعـ ثـيـدـحـتـبـ.ـرـيـكـفـتـلـاـ نـكـمـيـ Cisco Security Proxyـ،ـ ةـيـعـرـفـ ةـعـوـمـجـ نـمـضـتـيـ صـصـخـمـ قـاطـنـ وـأـ دـيـاحـمـلـاـ URLـ نـاوـنـعـ يـفـ.ـنـمـ يـبـلـسـلـاـ بـنـاجـلـاـ نـمـ ةـيـعـرـفـ ةـعـوـمـجـ نـمـضـتـيـ صـصـخـمـ قـاطـنـ وـأـ دـيـاحـمـلـاـ URLـ نـاوـنـعـ يـفـ.ـةـيـفـصـتـ لـمـاعـ ذـيـفـنـتـعـمـ ةـدـيـاحـمـلـاـ URLـ نـيـوـانـعـلـ أـصـحـفـ لـاثـمـلـاـ اـذـهـ حـضـوـيـ.ـةـدـيـاحـمـلـاـ نـيـوـانـعـلـاـ:ـاـذـهـ درـاـوـلـاـ يـوـتـحـمـلـاـ

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)	

لئاسرلا بقعت

يـف لـئـاسـرـلـا تـافـرـعـمـب ةـنـرـتـقـمـلـا URL (ـنـيـوـانـعـ) نـاوـنـعـلـ لـئـاسـرـلـا بـقـعـتـ تـارـايـخـ عـجـارـ دـيـدـحـتـ كـنـكـمـيـوـ ئـلـا لـوـخـدـلـا لـيـجـسـتـبـ URL نـيـوـانـعـ مـوقـتـ الـ ،ـنـايـحـأـلـا ضـعـبـ لـاـثـمـلـا لـيـبـسـ ئـلـعـ .ـلـئـاسـرـلـا بـقـعـتـ لـيـصـاـفـتـ يـفـ اـهـعـقـوـمـ

The screenshot shows the 'Email and Web Manager' interface with the 'Tracking' tab selected. The main content area displays 'Message Tracking' details for a message with ID `<202207060249228218@kncefd.top>`. The 'Processing Details' section includes tabs for 'Summary' and 'URL Details', with 'URL Details' highlighted by a red box. Below this, it shows 'Messages 34' and the date '05 Jul 2022'. Two log entries are listed:

- 18:49:58 Message 342164 URL: <https://www.mobilesuica.jp-ui.buzz/>, URL reputation: -7.1, Condition: URL Reputation Rule.
- 18:49:58 Message 342164 URL: <https://www.mobilesuica.jp-ui.buzz/>, URL reputation: -7.1, Action: URL redirected to Cisco Security proxy.

URL نـيـوـانـعـ ةـيـامـحـ مـادـخـتـسـابـ لـئـاسـرـلـلـ مـدـقـتـمـلـا ثـحـبـلـا تـارـايـخـ أـضـيـأـ لـئـاسـرـلـا بـقـعـتـ رـفـوـيـ اـهـعـمـ لـعـافـتـلـاوـ:

The screenshot shows the 'Email and Web Manager' interface with the 'Tracking' tab selected. On the left, a sidebar lists categories like DLP Violations, DMARC, External Threat Feeds, Forged Email Detection, and Geo Location. The main panel contains several filter sections, each highlighted by a red box:

- Outbreak Filters:** Includes checkboxes for 'Messages with Malicious URLs' and 'Messages with Neutral URLs'.
- URL Categories:** A dropdown menu with 'All' and 'Select' buttons, listing categories such as Adult, Advertisements, Alcohol, Animals and Pets, Arts, Astrology, Auctions, and Business and Industry.
- Web Interaction Tracking:** Includes fields for 'URL Clicked' and 'Mailflow Direction' (Inbound and Outbound).

ةـفـنـصـمـلـا وـأـةـفـنـصـمـلـا رـيـغـ URL (ـنـيـوـانـعـ) نـاوـنـعـ نـعـ غـالـبـإـلـا ئـطـاخـ وـحـنـ ئـلـعـ

نیوانع) ناونع ًاضيأ کانه .فینصت وًاعمس نود نم هنأ ًانايحأ غالبإلا URL ناونعل نكمي تابلط ٽرايزب لصفت ،هذه URL نیوانع دهاشم نع غالبإلل .ئطاخ لكشب اهفينصت مت URL Cisco Talos نم بیولا فینصت [يـفـ ظـعـمـسـلـاـزـكـرمـمعـدـ](#) [Talos](#).

ٽحفـصـ يـترـكـذـتـ ىـلـعـ ئـلـاحـلـاـ ضـرـعـ كـنـكـمـيـ ،URLـ نـاـونـعـ نـعـ غالـبـإـلـاـ دـعـبـ.

قـيـوـسـتـلـاـ لـئـاسـرـوـ ةـرـاضـلـاـ URLـ نـیـوـانـعـ فـاشـتـكـاـ مـتـيـ الـ
وـأـ يـئـاوـشـعـلـاـ دـيـرـبـلـاـ ٽـحـفـاـكـمـ ٽـيـفـصـتـ لـمـاـوـعـ ٽـطـسـاـوـبـ
رـاشـتـنـالـاـ

نم ديدعلا نيب نم طقف نارايم عم الـ اـمـهـ اـمـهـ ٥ـتـيـفـوـعـوـمـلـاـ ٽـعـمـسـ نـأـلـ اـذـهـ ٽـدـحـيـ نـأـنـكـمـيـ
ديـدـحـتـلـ رـاشـتـنـالـاـوـ يـئـاوـشـعـلـاـ دـيـرـبـلـاـ ٽـحـفـاـكـمـ ٽـيـفـصـتـ لـمـاـوـعـ اـهـمـدـخـتـسـتـ يـتـلـاـ رـيـيـاعـمـلـاـ
لـثـمـ ،ـعـارـجـاـ ـذـاخـتـاـلـ ـقـبـولـطـمـلـاـ دـوـدـحـلـاـ ـضـفـخـبـ ـمـقـ ،ـذـهـ ـقـيـفـصـتـلـاـ لـمـاـوـعـ ـقـيـسـاسـحـ ـةـدـاـيـزـلـ .ـاـهـمـاـكـحـأـ
ـاهـطـاـقـسـاـ وـأـ لـئـاسـرـلـاـ لـزـعـ وـأـ صـوـصـنـ اـهـلـادـبـتـسـاـ وـأـ URLـ نـیـوـانـعـ ـقـبـاتـكـ ـدـاعـاـ

نـاـونـعـ ٽـعـمـسـ ٽـجـرـدـ ىـلـعـ ـعـانـبـ لـئـاسـرـلـاـ وـأـ ٽـوـتـحـمـلـاـ ٽـيـفـصـتـ لـمـاـوـعـ ـعـاـشـنـاـ کـنـكـمـيـ ،ـکـلـذـ نـمـ ـآـلـدـبـ
URLـ.

قـحـلـمـلـاـ

ٽـرـصـتـخـمـلـاـ URLـ نـیـوـانـعـ ٽـيـفـصـتـ مـعـدـ نـیـكـمـتـ

 دـيـرـبـلـاـ نـامـأـلـ 13.0ـ ىـتـحـ 11.1ـ AsyncOSـ ىـلـعـ طـقـفـ مـسـقـلـاـ اـذـهـ قـبـطـنـيـ :ـظـحـاـلـمـ
ـيـنـورـتـكـلـإـلـاـ

رمـاـوـأـلـاـ رـطـسـ ـهـجـاـوـ ـةـطـسـاـوـبـ ٽـرـصـتـخـمـلـاـ URLـ نـیـوـانـعـ ٽـيـفـصـتـ مـعـدـ عـارـجـاـ نـکـمـيـ
(CLI)ـ websecurityadvbabledconfigـ رـمـاـلـاـ مـاـدـخـتـسـاـبـ ،ـطـقـفـ

```
<#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, tl.gd, plurk.com, url4.eu, j.mp, goo.gl, yfrog.com

URL نیوانع ۆیفیصت نیوکت تاسرامم لصفا قیقحتل رمألا اذه نیکمتب Cisco یصوت رصتخم URL ناوونع مادختسا هیف متی تقویا یف دیربلا تالجس سکعنن، هنیکمتب درجمب ۆلاسرلا لخاد:

Mon Aug 27 14:56:49 2018 Info: MID 1810 having URL: <http://bit.ly/2tztQUi> has been expanded to <https://tinyurl.com/yd2qjw2n>

لاثم نم، ۆلاقملا هذه یف حضوم وە امك URL نیوانع ۆیفیصت نیکمتب درجمب متی یدلا یلصألا طابترا لیجست ًاضيأ متی امك، bit.ly طابترا لیجست ۆظاحالم اننكمي یلإ ٥٤ یسوت.

• ۆیفاضا تامولعم

Cisco Secure Email Gateway

- [رادصألا تاظحالم](#)
- [مدختسملا لیلد](#)
- [رمأولا رطس ًةھجأول یعجمملاللیلدلا \(CLI\)](#)
- [ناقیب طتلارچمرب ًةھجأو چمرب ۆلدا \(API\) Cisco Secure Email Gateway](#)
- [یف مدختسملا حوت فملارادصملأا Cisco Secure Email Gateway](#)
- [نمضتی Cisco نم یوتحملانامألي ضارت فالازاھجلاتیبشت لیلد vESA](#)

Secure Email Cloud Gateway

- [رادصألا تاظحالم](#)
- [مدختسملا لیلد](#)

بیولا ریدمو Cisco Secure Email

- [قف اوتلا ًةفوفصم و رادصألا تاظحالم](#)
- [مدختسملا لیلد](#)
- [ناقیب طتلارچمرب ًةھجأو چمرب ۆلدا \(API\) Cisco Secure Email Gateway](#)
- [ریدمو بیولا Cisco نم یوتحملانامألي ضارت فالازاھجلاتیبشت لیلد vSMA](#)

Tاجتنم Cisco Secure

- [تاجتنم ۆظفحم ًةيمستل ًةینقتللا ًةینبللا Cisco Secure](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).