

# ىلع ٥٥ يجوت ةداعا و URL ھي جوت ءاغلا عارجا مهف ةنمآلما ينورتكلا ديربللا ئبأوب تاي وتحملما

## ةمدقملا

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملما](#)

[ةيساسأتامولعم](#)

[قلاسرلا جذون](#)

[غنا فيد - لوالا عزجلما](#)

[تانيوكتلما](#)

[عافدلما ئيلمع](#)

[أويرانيسلا](#)

[بويرانيسلا](#)

[ھي جوتلا ةداعا - يناثلا عزجلما](#)

[تانيوكتلما](#)

[ھي جوتلا ةداعا لعف](#)

[ميج ويرانيسلا](#)

[لاد ويرانيسلا](#)

[ھي جوتلا ةداعا - 3 عزجلما](#)

[نويوكتلما](#)

[E ويرانيسلا](#)

[واو ويرانيسلا](#)

[ياز ويرانيسلا](#)

[اھھالص او عاطخألا فاشكتسا](#)

[صخلم](#)

## ةمدقملا

حشرم يف ةمدختسملا ھي جوتلا ةداعا تاي لماع طبرلا ءاغلا نيب قرفلا ئقىيثوا ذه فصي  
صنل او href "ةمسلل حاتملا ئباتكلا ةداعا راي خ مادختسا ئيفيكو ، طبرلا ناونع

## ةيساسألا تابلطتملا

[تابلطتملا](#)

مادختسا ب ئلوبقم مادختسا تاسايس ضرفل وأ ، URL ناونع ئعممس ئلإ ادانتسا عارجا ذاختال  
لکش ب "يشفتلا ئيفصت لم الواقع" ۋېزم نيكىمت بجي ، ئوتحمل او لئاسرلا ئيفصت لم الواقع.

## ةمدختسملا تانوكملما

ةيـلـاتـلـا ةـيـدـامـلـا تـانـوـكـمـلـا وجـمـارـبـلـا تـارـادـصـا إـلـا دـنـتـسـمـلـا اـذـه يـف ةـدـراـوـلـا تـامـوـلـعـمـلـا دـنـتـسـتـ

- Cisco نـم ةـنـمـآـلـا يـنـورـتـكـلـإـلـا دـيـرـبـلـا ةـبـاوـبـ
- يـشـفـتـلـا ةـيـفـصـتـ لـمـاوـعـ
- لـئـاسـرـلـاـوـىـوـتـحـمـلـا ةـيـفـصـتـ لـمـاوـعـ

ةـصـاخـ ةـيـلـمـعـمـ ةـيـيـبـ يـف ةـدـوـجـوـمـلـا ةـزـهـجـأـلـا نـم دـنـتـسـمـلـا اـذـه يـف ةـدـرـاـوـلـا تـامـوـلـعـمـلـا ءـاـشـنـا مـتـ  
تنـاـكـ اذاـ (ـيـضـاـرـتـفـاـ) حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـا اـذـه يـف ةـمـدـخـتـسـمـلـا ةـزـهـجـأـلـا عـيـمـجـ تـأـدـبـ  
رمـأـ يـأـلـ لـمـتـحـمـلـا رـيـثـأـتـلـلـ كـمـهـفـ نـم دـكـأـتـفـ ،ـلـيـغـشـتـلـا دـيـقـ كـتـكـبـشـ.

## ةـيـسـاسـأـ تـامـوـلـعـمـ

لمـاوـعـ مـاـدـخـتـسـابـ URL ةـيـفـ وـأـ ةـعـمـسـىـلـعـ ءـاـنـبـ عـاـرـجـاـ ذـاـخـتـاـ يـهـ URL ةـيـفـصـتـ ةـزـيـمـ تـارـدـقـ ئـدـحـاـ  
طبـتـرـمـلـا طـرـشـلـاـ) URL نـاـونـعـ صـحـفـ ةـجـيـتـنـ ئـلـاـ اـدـاـنـتـسـاـ .ـيـوـتـحـمـلـا وـأـ لـئـاسـرـلـا ةـيـفـصـتـ  
URL نـاـونـعـ ئـلـعـ ةـحـاـتـمـلـا ةـثـالـثـلـا تـاءـاـرـجـاـلـا دـحـأـ قـيـبـطـتـ نـكـمـيـ ،ـURL نـاـونـعـ

- Defang URL
- Cisco نـاـمـأـ لـيـكـوـىـلـاـ هـيـجـوـتـلـاـ ةـدـاعـاـ
- ةـيـصـنـ ةـلـاسـرـبـ URL لـادـبـتـسـاـ

وـهـيـجـوـتـلـاـ ةـدـاعـاـ Defangـ URL نـاـونـعـ تـارـاـيـخـ نـيـبـ كـوـلـسـلـاـ حـرـشـ وـهـ دـنـتـسـمـلـاـ اـذـهـ يـفـ زـيـكـرـتـلـاـ  
ريـغـ دـيـدـهـتـلـاـ فـاـشـتـكـاـلـ URL نـاـونـعـ ةـبـاتـكـ ةـدـاعـاـ تـارـدـقـلـ اـحـيـضـوـتـ وـاـزـجـوـمـ اـفـصـوـمـدقـيـ اـمـكـ  
يـشـفـتـلـاـ ةـيـفـصـتـ لـمـاعـلـ يـسـوـرـيـفـلـاـ.

## ةـلـاسـرـلـاـ جـذـوـمـنـ

ددـعـتـمـ ةـلـاسـرـلـاـ عـوـنـ يـهـ تـارـاـبـتـخـاـلـاـ عـيـمـجـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـيـجـذـوـمـنـلـاـ ةـلـاسـرـلـاـ  
هـذـهـ ئـاـشـنـاـ مـتـيـ اـمـ دـاعـ .ـصـنـلـاـوـ لـهـسـلـاـ/ـصـنـلـاـ عـاـزـجـأـ نـمـ الـكـ نـمـضـتـتـ وـلـيـدـبـلـاـ/ـعـاـزـجـأـلـاـ  
ـيـوـتـحـمـلـاـ عـوـنـ سـفـنـ ئـلـعـ يـوـتـحـتـوـ يـنـورـتـكـلـإـلـاـ دـيـرـبـلـاـ جـمـانـرـبـ ةـطـسـاـوبـ اـيـئـاـقـلـتـ عـاـزـجـأـلـاـ  
ـلـهـسـلـاـ/ـصـنـلـاـ عـوـنـ رـيـحـتـ مـتـ ،ـضـرـغـلـاـ اـذـهـلـوـ .ـرـيـغـوـ HTMLـ تـالـبـقـقـتـسـمـلـ قـسـنـمـلـاـ  
ـاـيـوـدـيـ htmlـ/ـصـنـلـاـوـ

```
Content-Type: multipart/alternative; boundary="====7781793576330041025=="
MIME-Version: 1.0
From: admin@example.com
Date: Mon, 04 Jul 2022 14:38:52 +0200
To: admin@cisco.com
Subject: Test URLs
====7781793576330041025==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
This is text part of the message
Link1: http://malware.testing.google.test/testing/malware/
and some text
Link2: http://cisco.com
and some text
====7781793576330041025==
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
```

This is an HTML part of the message

Link1: <http://malware.testing.google.test/testing/malware/> and some text

Link2: [CLICK ME](#) some text

Link3: <http://malware.testing.google.test/testing/malware/> and some text

Link4: <http://cisco.com> and some text

=====7781793576330041025=====

## غنـافـيـدـ - لـوـأـلـاـ عـزـجـلـاـ

تاني وكتل

نیوکتلا مختسی، لاؤالا عزلایف

- ڦھفاكم /AS) ڦيڻاچارٽ فالا ڀئاوش علا ديربلا ڦھفاكم جمارب دادع ا لٽي طمعت عم ديربلا جهن ڀش فتلما ڦي ڦفصنت لم امو و (AMP) ڦراصلما جماربلا نم ڦم دق تملما ڦي ا ماحلا /AV) تاسوري فلما (OF)

Policies									
<a href="#">Add Policy...</a>									
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	URLTest	(use default)	(use default)	(use default)	(use default)	URL_SCORE	Disabled	(use default)	

- URL\_SCORE يوتحم ئىفصت لمعانى كەمت مەت: دراولار ئىوطحملانى ئىفصت لمعانى

Filters				
Order	Filter Name	Description   Rules   Policies	Duplicate	Delete
1	URL_SCORE	URL_SCORE: if (url-reputation(-10.00, -6.00 , "", 0, 1)) { log-entry("\$filterName"); uri-reputation-defang(-10.00, -6.00,"",0); }		

يـتـلا ،ـةـراـضـلـا نـيـوـانـع ـقـقـبـاطـمـل URL نـاـونـع ـعـمـس ـةـلـاح ـىـوـتـحـمـلـا ـةـيـفـصـتـ لـمـاعـ مـدـخـتـسـيـ عـاغـلـا عـارـجـاـوـ ـىـوـتـحـمـلـا ـةـيـفـصـتـ لـمـاعـ مـسـاـ لـيـجـسـتـ مـتـيـ ،ـعـارـجـاـكـ ـ10.00ـ وـ 6.00ـ نـيـبـ اـمـ قـقـحـتـ ـةـذـوـخـأـمـ url-reputation-defang طـابـتـرـالـاـ.

عاف دل ا ئيلم

كفي ؛اري سفت مدخلت سملاليل مدقعي .يع افدل الامعلوا وه ام حضون نأناكمب ةيمهألا نمو  
ةيُور لئاسرلا يمليتسن ناكما ب لازى ال .هيلع رقنلا نكمي ال ثيحب URL ناونع طابترا  
خسن و URL ناونع.

ویرانی سلا

ال حشرمب يسوري فلا ريع ديدهتلا نع فشكلا  
يشه فتللا

## غنا فيد | وتحمل حشرم عاجإ

ال AdvancedConfig href ڈاعیو نیکم م بیول ناماً قباتك بنلا

يُوصى بـ HTML تامالع درج متى امدنع URL ناوونع ةباتك ڈاعاً مدت ،يُوصى بـ HTML دادع الـ ایف قلأ. طقف HTML تامالع درج متى امدنع URL ناوونع ةباتك ڈاعاً مدت ،يُوصى بـ HTML دادع الـ ایف قلأ. طقف HTML تامالع درج متى امدنع URL ناوونع ةباتك ڈاعاً مدت ،يُوصى بـ HTML دادع الـ ایف قلأ. طقف HTML تامالع درج متى امدنع URL ناوونع ةباتك ڈاعاً مدت ،يُوصى بـ HTML دادع الـ ایف قلأ.

[Link1: http://malware-testing.google/test/testing/malware/](http://malware-testing.google/test/testing/malware/), and some text

Link2: [CLICK ME](#) some text

[Link3: http://malware-testing.google/test/testing/malware/](http://malware-testing.google/test/testing/malware/), and some text

فی اینجا می‌بینیم که URL ناونع لیست موتور جستجو را در HTML از طریق `<a href="URL">عنوان URL</a>` ایجاد کردیم. این URL ممکن است محتوایی داشته باشد که ممکن است برای کاربر مفید باشد. مثلاً اگر URL معرفی کننده یک فایل PDF باشد، کاربر می‌تواند آن را کلیک کرده و فایل را دانلود کند.

ةرقفلـا href لـخـاد طـقـف بـسـانـمـلـا URL نـاـونـع يـنـاـثـلـا طـابـتـرـالـا نـمـضـتـيـ. ةـفـلـتـخـمـ رـصـانـعـ يـأـ نـمـضـتـتـ الـةـرـيـخـأـلـا A.

دـنـعـ وـأـ طـابـتـرـالـا قـوـفـ رـشـفـمـلـا كـيـرـحـتـ دـنـعـ حـيـحـصـلـا نـاـونـعـلـا ةـظـحـاـلـمـ اـمـئـادـ نـكـمـيـ ةـظـحـاـلـمـ ةـيـجـمـرـبـلـا تـامـيـلـعـتـلـا ىـلـعـ رـوـثـعـلـا نـكـمـيـ الـ، ظـحـلـا عـوـسـلـ. ةـلـاسـرـلـلـ رـدـصـمـلـا زـمـرـلـا ضـرـعـ نـيـرـوـهـشـمـلـا يـنـورـتـكـلـلـا دـيـرـبـلـا ءـالـمـعـ ضـعـبـ عـمـ ٰلـوـهـسـبـ رـدـصـمـلـا.

ةـراـضـلـا URL نـيـوـانـعـ دـيـدـحـتـ ءـاغـلـا مـتـيـ، ةـيـفـصـتـ لـمـاعـبـ ٰلـاـسـرـلـا ةـقـبـاـطـمـ درـجـمـبـ تـنـكـ عـيـطـتـسـيـ URLs وـطـاقـنـلـا رـمـأـ OUTBREAKCONFIG عـمـ URL نـاـونـعـ لـيـجـسـتـ نـيـكـمـتـ دـنـعـ يـفـ تـسـسـاـ mail\_log.

```
Mon Jul 4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Condition: URL Reputation Rule Mon Jul 4 14:46:43 2022 Info: MID 139502 Custom Log Entry: URL_SCORE Mon Jul 4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Mon Jul 4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Mon Jul 4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Mon Jul 4 14:46:43 2022 Info: MID 139502 rewritten to MID 139503 by url-reputation-defang-action filter 'URL_SCORE'
```

اهـتـبـاتـكـ ةـدـاعـاـ تـمـتـ ٰلـاـسـرـكـلـذـ نـعـ جـتـنـيـوـ

```
=====7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: 7bit
```

This is an HTML part of the message

Link1: http://malware.testing.google.test/testing/malware/ and some text

Link2: CLICK ME some text

Link3: http://malware.testing.google.test/testing/malware/ and some text

Link4: http://cisco.com and some text

```
=====7781793576330041025====
```

ةـدـرـجـ زـيـيـمـتـ ةـمـاـلـعـ يـهـ MIME ٰلـاـسـرـنـمـ html/صـنـلـاـ عـزـجـ ىـلـعـ مـتـ يـذـلـاـ طـبـرـلـاـ ءـاغـلـاـ ةـجـيـتـنـ الـكـ طـبـرـ ءـاغـلـاـ مـتـ، نـيـلـوـلـاـ نـيـتـرـقـفـلـاـ يـفـ سـمـلـ نـوـدـبـ كـرـتـ زـيـيـمـتـلـاـ ةـمـاـلـعـ ىـوـتـحـمـ وـ ةـرـقـفـلـاـ يـفـ URL نـاـونـعـ رـصـنـعـلـاـ نـمـ صـنـلـاـ عـزـجـ كـرـتـ وـ HTML ٰرـفـشـ درـجـ مـتـ ثـيـحـ نـيـطـبـرـلـاـ ةـرـقـفـلـاـ نـمـ URL نـاـونـعـ نـأـ ةـظـحـاـلـمـ بـجـيـ HTML رـصـنـعـبـ صـاـخـلـاـ صـنـلـاـ عـزـجـ نـمـ نـاـونـعـ وـهـ ىـلـوـلـاـ نـوـكـيـ الـأـبـجـيـ HTML Aـ، زـيـيـمـتـ تـامـاـلـعـ نـوـدـبـ نـكـلـوـ طـابـتـرـالـاـ ءـاغـلـاـ ةـرـقـفـلـاـ ةـيـزـجـتـ ءـاغـلـاـ مـتـيـ الـ، رـقـنـلـلـ الـبـاـقـ رـصـنـعـلـاـ هـيـ اـبـوـغـرـمـ اـكـوـلـسـ نـوـكـيـ الـ دـقـ . طـابـتـرـاـ هـرـابـتـعـاـ مـتـيـ الـ، Aـ، زـيـيـمـتـ تـامـاـلـعـ يـأـ نـيـبـ هـعـضـ وـ يـفـ هـذـيـفـنـتـ وـهـخـسـنـ وـ طـابـتـرـالـاـ ةـيـفـرـ ٰلـوـهـسـبـ مـدـخـتـسـمـلـلـ نـكـمـيـ ، الـوـأـ. نـيـبـبـسـلـ فـاشـتـكـاـ ىـلـاـ لـيـمـتـ يـنـورـتـكـلـلـاـ دـيـرـبـلـاـ جـمـارـبـ ضـعـبـ نـأـ وـهـ يـنـاـثـلـاـ بـبـسـلـاـوـ. ضـرـعـتـسـمـلـ رـقـنـلـلـ الـبـاـقـ اـطـبـارـ هـلـعـجـ وـصـنـلـاـ لـخـادـ URL نـيـوـانـعـ نـمـ حـيـحـصـ لـكـشـ

يـدـاعـلـاـ عـزـجـلـاـ/صـنـلـاـ نـمـضـتـيـ MIME ٰلـاـسـرـنـمـ طـيـسـبـلـاـ عـزـجـلـاـ/صـنـلـاـ ىـلـعـ ٰرـطـنـ قـلـنـلـفـ مـهـفـيـ الـ يـذـلـاـ MUA ٰطـسـاـبـ لـهـسـلـاـ/صـنـلـاـ ضـرـعـ مـتـيـ. صـنـلـاـ جـذـوـمـنـ يـفـ URL يـنـاـونـعـ ىـرـتـ الـ، نـيـثـيـدـحـلـاـ يـنـورـتـكـلـلـاـ دـيـرـبـلـاـ ءـالـمـعـ مـظـعـمـ يـفـ. ةـيـجـمـرـبـلـاـ HTML تـامـيـلـعـ اـدـمـعـ كـبـ صـاـخـلـاـ يـنـورـتـكـلـلـاـ دـيـرـبـلـاـ لـيـمـعـ نـيـوـكـتـبـ مـقـتـ مـلـاـمـ ٰلـاـسـرـلـلـ ةـيـدـاعـلـاـ ءـاـزـجـأـلـاـ/صـنـلـاـ يـلـوـأـ EML قـيـسـنـتـ وـهـ، ٰلـاـسـرـلـلـ رـدـصـمـلـاـ زـمـرـلـاـ نـمـ قـقـحـتـلـاـ ىـلـاـ جـاتـحـتـ، ةـدـاعـ. كـلـذـبـ مـاـيـقـلـلـ اـهـنـمـ قـقـحـتـلـاـوـ ةـيـفـرـلـ ٰلـاـسـرـلـلـ ةـاـزـجـأـ ةـيـفـرـلـ ٰلـاـسـرـلـلـ.

ردصملا ئلارسلا نم يداع عزج/صنلا نم URLs انه جارداا رهظي.

Link1: http://malware.testing.google.test/testing/malware/ and some text Link2: http://cisco.com and some text

نوكى ،يضاارت فالكشب اهلىت ف عزن مت و ئىتىخ ئجيتن ئىلع تلصح طباورلا هذه دح او نع ئىفلىت خم ئجيتن MIME عون نم يداعلا عزجلا/صنلا ئىلع ھذاختا مت يذلا طبرلا ئاغلإ عارجلإ ساوقاً نىب طاقنلا لکو ئروظحملاتا ملکلا نىب عقى .HTML/صنلا عزج يف يتلا كلت عبزم.

=====7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: 7bit This is text part of the message Link1: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some text Link2: http://cisco.com and some text =====7781793576330041025==

:صىخلتلما

- ئروظحم لتك ئىلإ URL ئباتك ديعى "يداعلا عزجلا"/"صنلا" ئىلع ليغشتلا ئاغلإ
- HTML A زىيىمت ئامالع نم URL ناونع ئباتك ديعى TEXT/HTML عزج ئىلع ليغشتلا ئاغلإ
- يذلار، سمالتم زىيىمت تامالع نىب دوجوملا صنلا نودب A زىيىمت ئامالع نوكى ام دنعن اضىأ URL ناونع نوكى نأ نكمى

## ب ويرانيسلا

حشرمب يسوريفلارىغ ديدهتلانع فشكىلا	ال
يىشفتلما	
ىوتحملاب حشرم ئارجا	غانافيد
هاداع او AdvancedConfig href نيكىمت مت بىولا ناما	معن
صنلما ئباتك	

دحأ مادختسى دعب ئىزجتلما ئاغلإ عارجإ كولس رىيغت ئيفيك لوح تامولعم ويرانيسلا اذه رفو وي ىوتسمب صاخلا CLI رمأ وە webSecurityAdvancedConfig. webSecurityAdvancedConfig تارايىخ رىيغتب انه تادادعإلا دحأ كل حمسى. حسمب ئاصاخلا تادادعإلا طبضب حمسى يذلا زاهجلالا لىطعتلما ئارجإل يضاارتفالا كولسلا.

```
> websecurityadvancedconfig Enter URL lookup timeout in seconds: [15]> Enter the maximum number of URLs that can be scanned in a message body: [100]> Enter the maximum number of URLs that can be scanned in the attachments in a message: [25]> Do you want to rewrite both the URL text and the href in the message? Y indicates that the full rewritten URL will appear in the email body. N indicates that the rewritten URL will only be visible in the href for HTML messages. [N]> Y
```

رېشى ي ز باوجلا ،عبارلا لاؤسلا يف يىتلما URL ناونع لسالس ئفاك ئلارسلا نم HTML ئىلإ دنتسملا MIME عزج ئلاح يف هنأ ئىلإ رصانع يأ جراخ وا صن عزج هنإف، رصانع عزج A-tag، رصانع href ئامىت وە ئاتنپ نكلو، ئاتسەم اهتاذ ئلارسلا نوكى ويرانيسلا اذه يفو. اهتباتك هادع ام تت اليلق ئىفلىت خم.

زمرىب هنراق وىرخأ ئرم HTML نىوانع مادختسا ب HTML عزج دوك ئىلع ئرظن قىلما ينورتكللإا ديربلا ئاباوب ئاطس اوب هتجلام تمت يذلا

Link1: <http://malware.testing.google.test/testing/malware/> and some text

Link2: [CLICK ME](#) some text

Link3: http://malware.testing.google.test/testing/malware/ and some text

Link4: http://cisco.com and some text

URL نیوانع وہ ھقباطی ام لک نإف ، صنل ا ئباتک ڈاعا و href رایخ نیکمت متي امدن ع رصونع صن عزج اؤم م اعج href URL ناونع ناک عاووس اوئاگل ا متي ۃي فصتلل HTML ۃقیثونم رخآ عزج یف ھيلع روشعل ا مت اؤ ، زییمت ۃمالع HTML.

=====7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: 7bit

This is an HTML part of the message

Link1: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some text

Link2: CLICK ME some text

Link3: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some text

Link4: http://cisco.com and some text

=====7781793576330041025====

ۃمالع رصونع ديرجت متي امدن ع اهکي كفت مت یتل ا URL نیوانع ۃباتک ڈاعا ا عزج ل/ا صنل ا عزج ۃباتک ڈاعا عم A زییمت للا URL ناونع قیسنت قباطی امدن ع طابترالاب صاخل ا صنل ا عزج ۃباتک ڈاعا عم A زییمت للا نم یداعل ا عزج ل/ا صنل ا یف ۃدوچوملا ۃقیرطلا سفنب ہتباتک داعملما صنل ا عزج لمع متي نیب اهع ض و متي طاقنل ا لکو ۃروظحملا تاملکل ا نیب رصونعل ا عض و متي جمارب عالم ضعب لمعجیو، ھقصلو URL ناونع خسن نم مدخلتسمل ا کلذ عنمی .ۃعربم ساوقا رقنلل الباقي صنل ا ینورتکل إللا ديربل ا.

صیخلتل ا:

- ۃروظحم لتك یل ا ۃباتک دیعی "یداعل ا عزج ل/ا" یل ع لیغشتل ا عاگل ا
- زییمت ۃمالع نم URL ناونع ۃباتک دیعی TEXT/HTML A زییمت ۃمالع ديرجت متي امدن ع A
- URL لسالس ۃفاک ۃباتک ڈاعا یل ا TEXT/HTML عزج یل ع تیبٹتل ا عاگل ا لیغشت ی دوی
- ۃروظحم لتك ع م قباطتت یتل ا

## ھیجوتل ا ۃداعا - یناثل ا عزج ل/ا

### تانیوکتل ا

نیوکتل ا مدخلتسی یناثل ا عزج ل/ا یف

- لطعم نموی ضارف الـ AS/AV/AMP نیوکت ع م ديربل ا جھن

Policies									
Add Policy...									
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	URLTest	(use default)	(use default)	(use default)	(use default)	URL_SCORE	Disabled	(use default)	

- یوتحم ۃي فصت لماع نیکمت مت : دراول ا یوتحملا ۃي فصت لماع URL\_SCORE

Filters				
<a href="#">Add Filter...</a>				
Order	Filter Name	Description   Rules   Policies	Duplicate	Delete
1	URL_SCORE	URL_SCORE: if (url-reputation[-10.00, -6.00 , "", 0, 1]) { log-entry("\$filterName"); url-reputation-proxy-redirect[-10.00, -6.00,"",0]; }		

يـتـلـا،ـرـاضـلـا URL نـاـوـنـعـةـقـبـاطـمـلـا URLـاـوـتـحـمـلـاـةـيـفـصـتـلـمـاعـمـدـخـتـسـيـ وـىـوـتـحـمـلـاـةـيـفـصـتـلـمـاعـمـسـاـلـيـجـسـتـمـتـيـ،ـعـارـجـاـكـ.ـ00ـ10ـ وـ00ـ6ـ نـيـبـلـجـسـتـهـذـوـخـأـمـ.

جولان داعل

رقنلا ئلاس رلا ملتسمل رقنلا تقو مييقتل Cisco ناما ليكو ئمدخ ئلا هيچوتلا ئداعا حييت  
عنمي يذلاو، ئباحسلا يف Cisco نم بيو لا ناما ليكو ئلا هيچوت ئداعا او طابترا لا قوف  
راض هنأ ئيلع عقولما فيرعت مت اذإ لوص ولما

میج ویرانی سلسلہ

ال حشرمب يسوري فلاريغ دي دهتلا نع فشكلا  
ييش فلتلا

هیجوت ڈاعی یوتحمل احشرم عارجا

ال ۋە دادلىق AdvancedConfig href نىكىمەت مەت بى يولۇنامىڭ

م ت ي ذ ل ا ق ر ف ل ا ع م ل و ا ل ا ع ز ج ل ا ن م (أ) وي ران ي س ل ل ك و ل س ل ل ي ف ا د ج ه با ش م وي ران ي س ل ل ا ذ ه م ت ي .ه ت ي ب ث ت ء ا غ ل ي ن م ال د ب URL ن او ن ع ه ي ج و ت ء د ا ع ئ ء و ت ح م ل ا ة ي ف ص س ت ء ا ع ج ا ي ف ه و ا ر ج ا ي ن ع ي ا م م ، ة ي ض ا ر ت ف ال ا ت ا د ا د ع ال ا ل ل WebSecurityAdvancedConfig ت ا د ا د ع ئ ء د ا د ع ت س ا ئ ل ع ه ن ي ي ع ت م ت ... N.

ةراضللا طاقنلا موقت .ميميقتو URLs ناونع لك فاشتكاب ينورتكللا ديربلا ةرابع موقت URL\_SCORE url-reputation-proxy-redirect-action ءارجلا ذخأتو

```
Tue Jul 5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/  
has reputation -9.4 matched Condition: URL Reputation Rule Tue Jul 5 12:42:19 2022 Info: MID  
139508 Custom Log Entry: URL_SCORE Tue Jul 5 12:42:19 2022 Info: MID 139508 URL  
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL  
redirected to Cisco Security proxy Tue Jul 5 12:42:19 2022 Info: MID 139508 URL  
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL  
redirected to Cisco Security proxy Tue Jul 5 12:42:19 2022 Info: MID 139508 URL  
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL  
redirected to Cisco Security proxy Tue Jul 5 12:42:19 2022 Info: MID 139508 rewritten to MID  
139509 by url-reputation-proxy-redirect-action filter 'URL SCORE'
```

دوچوبلما سفن. ۋەلسىرلا نم HTML عزج يف URL نىوانع ئېباتك ۋەداعا! ئېفييک ىلۇغۇن قىلۇزىيەت ۋەمالۇ رىصنەل href مەسى يف ۋەدوچوبلما URL نىوانع ئېباتك ۋەداعا! مەتى، ئۆرەنەيسلى يەطبىرلا ئاغلىغا ئارچا! عەم رىصنەن نىم صىنلار عزج يف ۋەدوچوبلما URL نىوانع يەطخەت مەتى و طققى ناونع ئېباتك ۋەداعا! مەتى، ھېچجوت ۋەداعا! ئارچا! عەم نىڭ ھەلمكىپ A زىيەت ۋەمالۇ رىصنەن دىيرجەت مەتى URL href مەسى يف.

-----7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: 7bit

This is an HTML part of the message

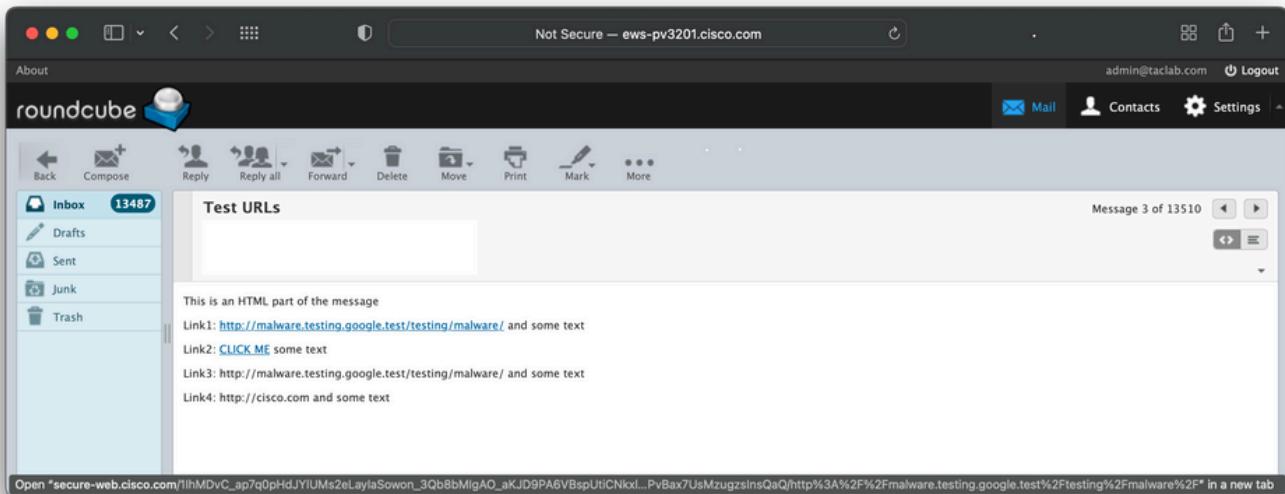
[Link1: http://malware.testing.google.test/testing/malware/](http://malware.testing.google.test/testing/malware/) and some text

Link2: [CLICK ME](#) some text

Link3: <http://malware.testing.google.test/testing/malware/> and some text

Link4: <http://cisco.com> and some text

-----7781793576330041025-----



ةلسلس لك نأله مهفلل لهسأ هيجهوتلا ةداعاً ودبـتـ، MIME عـزـجـ نـمـ يـدـاعـلـاـ عـزـجـلـاـ/ـصـنـلـاـ يـفـ اـهـتـبـاتـكـ ةـدـاعـاـ مـتـيـ ـقـجـيـتـنـلـاـ قـبـاطـتـ يـتـلـاـ URLـ نـاـونـعـ.

--7781793576330041025= Content-Type: text/plain; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: 7bit This is text part of the message Link1:  
http://secure-  
web.cisco.com/lduptzzum1fIIuAgDNq\_\_M\_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn  
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-  
b740jVOznKsikLcnmdC4pIBtIolsZ707Mml0C4HECgyxBRF\_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi\_-  
EyXHQb3pTzMpyFbQ861V1fDq96VcNM9qiDzG1TgFwej4J\_-QM-  
72i3qCp9eYFDXR1COY4T9bkDVO\_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa  
re%2F and some text Link2: http://cisco.com and some text --7781793576330041025==  
اصلخیل:

- يتلـا URL نـاونـع ظـلـسـلـسـ ظـبـاتـكـ دـيـعـيـ يـدـاعـلـاـ عـزـجـلـاـ/ـصـنـلـاـ ئـلـعـ لـيـغـشـتـلـاـ هـيـجـوـتـ ظـدـاعـاـ Cisco Web Secure
  - يـتلـا ئـخـأـلـاـ URL لـسـالـسـ عـيـمـجـ كـرـتـيـ هـنـكـلـوـ Cisco Web Secure لـيـكـوـ وـقـمـدـخـ مـادـخـتـسـابـ ظـلـدـعـمـ رـيـغـ قـبـاطـتـ

لاد ویرانی سلا

حشرمب يسوري فلاريغ دي دهتلا نع فشكلا  
يشفتلا

ج

یوتحمل احش رم عارجا

٥ داعٰ جوی

## نام او AdvancedConfig href مت بیولا ناماً صنلا ۃباتک

لسالس ۃفاک ۃباتک ۃداعاً ل. واؤلا عزجاً لایف دراولالا (ب) ويرانیس لل هباشم ويرانیس للا اذه کلذب مايقلما متی. اهنیکمت مت ۃلاس رلا نم HTML عزج یف قباطتت یتلالا URL ناونع "Do you want to rewrite both the URL text and the href in the message? .. لاؤس ..

=====7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: 7bit

This is an HTML part of the message

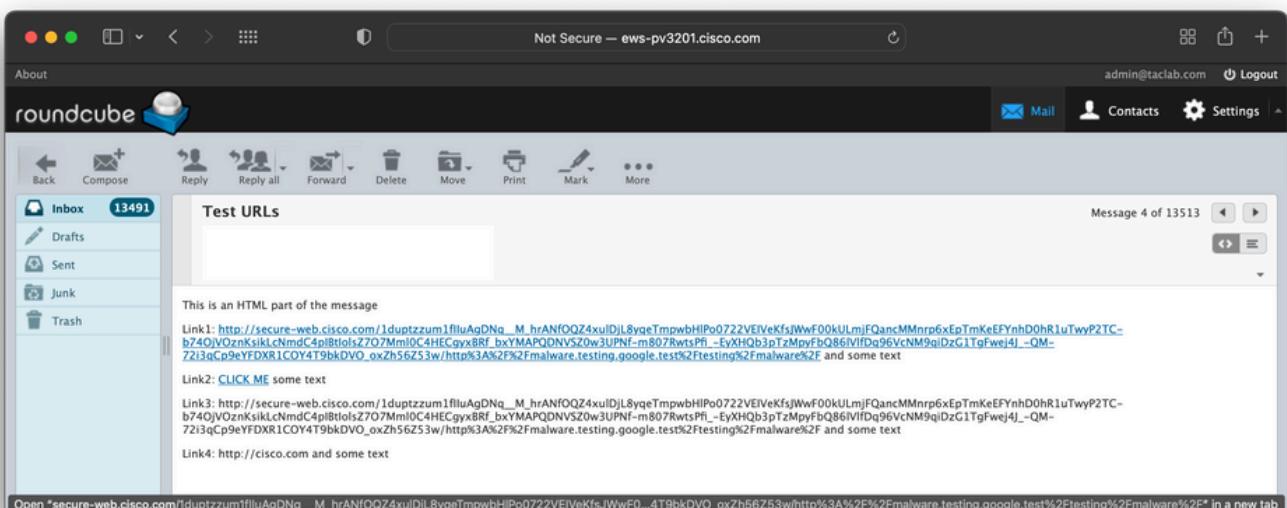
Link1: [Link2: \[CLICK ME\]\(#\) some text](http://secure-web.cisco.com/1duptzzum1fIIuAgDNq_M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn_rp6xEpTmKeEFYnhD0hR1uTwyp2TC-b740jVOznKsikLcNmcdC4pIBtIolsZ707Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_EyXHQb3pTzMpyFbQ861V1fDq96VcNM9qiDzG1TgFwej4J_QM-72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text</a></p></div><div data-bbox=)

Link3: [some text](http://secure-web.cisco.com/1duptzzum1fIIuAgDNq_M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn_rp6xEpTmKeEFYnhD0hR1uTwyp2TC-b740jVOznKsikLcNmcdC4pIBtIolsZ707Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_EyXHQb3pTzMpyFbQ861V1fDq96VcNM9qiDzG1TgFwej4J_QM-72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text)

Link4: <http://cisco.com> and some text

=====7781793576330041025====

یتلالا URL ناونع لسالس عيمج ھي جوت ۃداعاً مت، صنلا ۃباتک ۃداعاً مت، ناميکمت درجمب ع م نآلأ ينورتكللإا ديربلالا لمي مع یف ۃدوچوملأا ۃلاس رلا مدق ت. یوتحملأا حشم طورش قباطت عز ضرعى یذلا بیولالا ديربلالا لمي مع جاخأ عجار، لضفأ لکشب اذه مهفل. ھي جوتلما ۃداعاً لکلأا لاس رلا نم /html/صنلا.



رييغت نأ ثيچ C ويرانيسلا يف امك هسفن وه MIME ۆلاسرنم يداعلا عزل/ا/صنلا ۆلاسرلا نم ۆيداعلا عازجألا/ا/صنلا ىلع رثؤي ال WebSecurityAdvancedConfig.

--7781793576330041025= Content-Type: text/plain; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: 7bit This is text part of the message Link1:  
http://secure-  
web.cisco.com/lduptzzumlfIIuAgDNq\_\_M\_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn  
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-  
b740jVOznKsikLcnmdC4pIBtIolsZ7O7Mml0C4HECgyxBRF\_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi\_-  
EyXHQb3pTzMpyFbQ861V1fdQ96VcNM9qiDzG1TgFwej4J\_-QM-  
72i3qCp9eYFDXR1COY4T9bkDVO\_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa  
re%2F and some text Link2: http://cisco.com and some text --7781793576330041025=

ا ل ت خ ي ص:



٥- عِجَلٌ ٣ - ٤٦

ریغ تادی دهتلاری ثابت نع فشكلا تادادع! مایق ۋېفیک لوح تامولۇم عزجلا اذه رفووی URL حس مب ۋېسۈرەلە.

نيوكوتل

نيلوألا نيازجلا يف مدخلتس ملا ىوتجملا ٰي فرصت لماع ليطاعت متى ،ضرغلا اذهل

- نیکمٹ عمومی ضارف ایسا AS/AV/AMP نیوکت عم دیرپلا جھن

Policies										
<a href="#">Add Policy...</a>										
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete	
1	URLtest	(use default)	(use default)	(use default)	(use default)	Enabled (no filters)	Retention Time: Virus: 1 day Other: 4 hours	(use default)	(use default)	

- ئىس ورىفلا رىغ تادىدەتلا نع فشكىللى "يشفتلا ۋېفصىت لىمابۇع صحىفە" نىيوكت مەت دىرپلا لىئاسىرىن ئەدوجۇملا URLs ۋەفاك ۋېباتك ۋەداعىل URL ۋېباتك ۋەداعىا ۋەعومجەم مادختىساب ۋەراضىلما يىنورت كىلىلا

## Mail Policies: Outbreak Filters

Outbreak Filtering for Policy: URLTest

Enable Outbreak Filtering (Customize settings)

**Outbreak Filter Settings**

Quarantine Threat Level: <input type="button" value="3"/>	<input type="button" value="1"/> Days <input type="button" value="8"/>
Maximum Quarantine Retention:	Viral Attachments: <input type="button" value="1"/> Days <input type="button" value="8"/>
	Other Threats: <input type="button" value="4"/> Hours <input type="button" value="8"/>
	<input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning: <input type="button" value="None configured"/>	
<b>Message Modification</b>	
<input checked="" type="checkbox"/> Enable message modification. Required for non-viral threat detection (excluding attachments)	
Message Modification Threat Level: <input type="button" value="3"/>	<input type="button" value="1"/> <input type="button" value="3"/> <input type="button" value="5"/> <input type="button" value="7"/>
Message Subject:	Prepend <input type="button" value="[[SUSPICIOUS MESSAGE]]"/> Insert Variables   Preview Text <input type="button" value="Edit"/>
Include the X-IronPort-Outbreak-Status headers:	<input type="radio"/> Enable for all messages <input type="radio"/> Enable only for threat-based outbreak <input checked="" type="radio"/> Disable
Include the X-IronPort-Outbreak-Description header:	<input type="radio"/> Enable <input type="radio"/> Disable
Alternate Destination Mail Host (Other Threats only):	(examples: example.com, 10.0.0.1, 2001:420:80:1::5)
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input checked="" type="radio"/> Enable only for unsigned messages (recommended) <input type="radio"/> Enable for all messages <input type="radio"/> Disable
Bypass Domain Scanning <input type="button" value="?"/>	(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)
Threat Disclaimer:	<input type="radio"/> None <input type="radio"/> <small>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies &gt; Text Resources &gt; Disclaimers</small>

نیوانع عیمج ۃباتک ۃداعا مرت، ۃراض ۃلس اوب ۃلس رلا فین صت مرتی ام دن ع URL Cisco Web Secure.

## ویرانیسلا E

حشرمب یسوري فلاریغ دیده تلار نع فشكلا	معن
یش فتلار	
یوتحملار حشرم عارجا	ال
ۃداع او AdvancedConfig href="نیکم مرت بیولاناما"	ال
صنلا ۃباتک	

OF و صنلا ۃباتک ۃداعا لی طمعت عم ۃلس رلا ۃباتک ۃداعا لمع ۃی فیک ویرانیسلا ادھ حضوی Enabled و WebSecurityAdvancedConfig href="طقف".

```
Wed Jul 6 14:09:19 2022 Info: MID 139514 Outbreak Filters: verdict positive Wed Jul 6 14:09:19 2022 Info: MID 139514 Threat Level=5 Category=Phish Type=Phish Wed Jul 6 14:09:19 2022 Info: MID 139514 rewritten URL u'http://malware.testing.google.test/testing/malware/' Wed Jul 6 14:09:19 2022 Info: MID 139514 rewritten URL u'http://cisco.com' Wed Jul 6 14:09:19 2022 Info: MID 139514 rewritten URL u'http://malware.testing.google.test/testing/malware/' Wed Jul 6 14:09:19 2022 Info: MID 139514 rewritten URL u'http://malware.testing.google.test/testing/malware/' Wed Jul 6 14:09:19 2022 Info: MID 139514 rewritten to MID 139515 by url-threat-protection filter 'Threat Protection' Wed Jul 6 14:09:19 2022 Info: Message finished MID 139514 done Wed Jul 6 14:09:19 2022 Info: MID 139515 Virus Threat Level=5 Wed Jul 6 14:09:19 2022 Info: MID 139515 quarantined to "Outbreak" (Outbreak rule:Phish: Phish)
```

عیمج ۃباتک ۃداعا ظحالم نکمی، عیرسلا ققحتلا دعب. یداعلارا عزجباً أدبن لف کلذ ثدھی Cisco Web Secure. ۃراض لیکو تامد خیلای یداعلارا عزجلارا/صنلا URL نیوانع ۃدامد خیلای URL نیوانع ۃفاتک ۃنکمم URL ناوونع ۃباتک ۃداعا نآل عابولارا یش فتل.

=====7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: quoted-printable This is text part of the message Link1: http://secure-web.cisco.com/11ZWFnZYM5Rp\_tvvnco4I3GtnExIEFqpirK= f5WBmD\_7X-8wSvnmoQxYNYhb4ap1EtOXP\_-0CMTnyw6WX63xZIFnj5S\_n0vY18F9GOJWCSoVJpK= 30Eq81B-jcbjx9BWlZaNbl-t-utOLj107Z3j8XCAdowHe1t7GGF8Lft1GNFRCVLEM\_wQZyo-uxh= UfkHZVETXPZAddg6-uCeoeimiRZUOAzqvew2axm903AUpieDdfeMHYXpmzeMwu574FRGbbr7uV=tB65hfY29t2r\_VyWA24b6nyaKyJ\_hmRf2A4PBWOTe37cRLveONF9cI3P51GxU/http%3A%2F%2F=malware.testing.google.test%2Ftesting%2Fmalware%2F and some text Link2: http://secure-web.cisco.com/1o7068d-d0bG3Sqwcifil89X-tY7S4csHT6=LsLToTUYJqWzfLfODch91yXWFJ8a0xPq1PQBSACgJ1Dt4hCZipXXmC1XI3-XdNLGBMd0bLfj1cB= hY\_OwlBfLD-zC86M02dm\_fOXCqKT0tDET3RD\_KAeUWTWhWZvN9i81LPcwBBBi9TLjMAMnRKPmeg= En\_YQvDnCzTB4qYkG8aUQlFsecXB-V\_HU1vL8IRFRP-uGINjhHp9kWCnntJBJEm0MheA1T6mBJJ= ZhBZmfymfOddxs-xIGiYXn3juN1TvuOlCceo3YeaIVrbOXc01zs3FO8xvNjOnwVKN181yGKPQ9Y= cn5aSWvg/http%3A%2F%2Fcisco.com and some text =====7781793576330041025==

**اذهن اسرا نم متجل اعم تم ميذلا اصبنلا عزج وه اذه**

=====7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: quoted-printable

This is an HTML part of the message

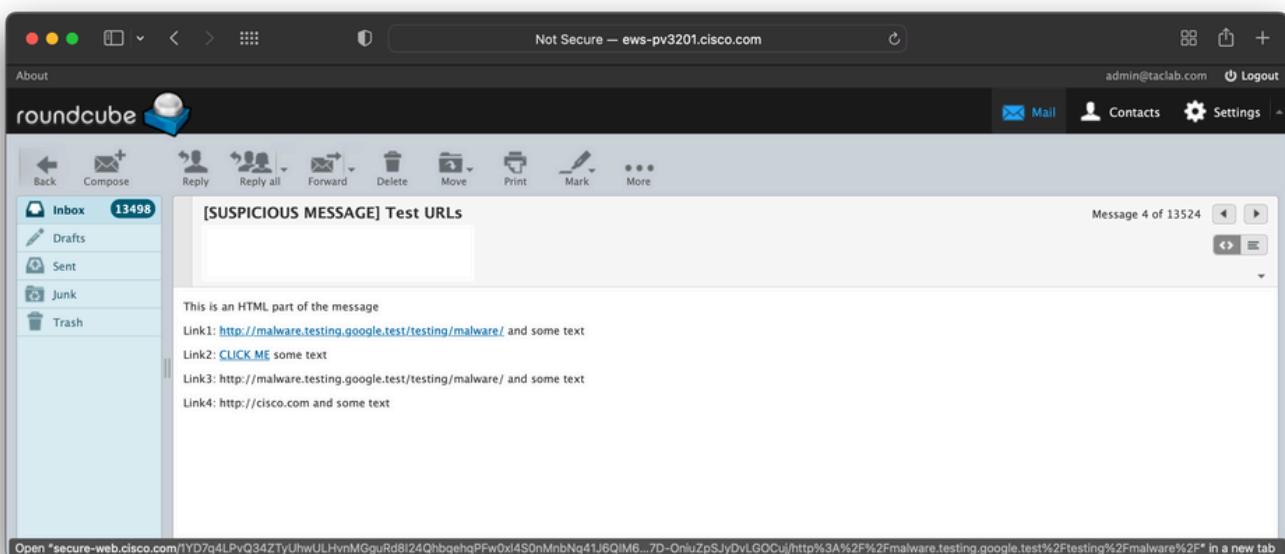
=20

Link1: <http://malware.testing.google.test/testing/malware/> and some text

Link2: [CLICK ME< /a>](#) some text

Link3: <http://malware.testing.google.test/testing/malware/> and some= textLink4: <http://cisco.com> and some text=20 =====7781793576330041025==

-



**اذا 4. طابرالا ئباتك ۋە داعا مىت مل اذامىل يە انە اھت ظحالم نكىمى يىتلە ئىلولى ئەطقنلى لىعلو يىضارت فارلا لىكشىپ HTML نم اصبنلا عزج موقىي . باوجلا فرعت تىنأف ئىيانع ب ئلاق مىلما تارق عەم لىاحلا وە امك لىثامم كولس كانە ناك اذا . طقق a-tag رىصانع لىلە href تامىس ۋە جل اعم و مىيقتىب ئباتك ۋە داعا او WebSecurityAdvancedConfig href نىكىمت بىجىف ، بوغرم يىداعلە عزجلا اصبنلا صىخلىتلىا . طبضلىاب كلذب موقىي يىلاتلىا وىرانىسىلىا اصبنلا:**

- ناونع ئىلسلىس عىمچ ئباتك دىعىي يىداعلە عزجلا اصبنلا لىغشتلىا ھىجوت ۋە داعا URL Cisco Web Secure
- ۋە مىس نم طقق URL ناونع ئباتك ۋە داعا مىت TEXT/HTML عزجلا لىغشتلىا ۋە داعا html A-Tag href نم بى يول نم آلا لىكىلە قىمەت سىاب Cisco

واو ویرانی سلا

معن	حشرمب يسوريفلارىغ دىدەتلا نۇفعشىكلىا يىشفتلا
ال	ىوتجملا حشرم عارجا
معن	ةداع او AdvancedConfig href نىكىمەت مەت بىولانام صىنلا ئېباتك

راه ئەل صنلا ۋېبەتک ۋە دەعى او webSecurityAdvancedConfig href نىكەمەت وىرانىسلا اذە حىتى  
رېغ تادىدەتلا فاشتکا تارىيەت ھرفوت يىذلا URL ناونۇ ۋېبەتک ۋە دەعى يىف كولسلا ئېفييڭ  
عاچا جىلۇغ رەۋىي ال WebSecurityAdvancedConfig نامەف بجى، ۋە طۆحلەللا ھەذە يىف. ئېس ورىفلا  
كولسلا رېغت فېيک ئىرنو html/صنلا عزىز طققى مېقۇن انعد. ئې داعىلا MIME/صنلا

-----7781793576330041025-- Content-Type: text/html; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: quoted-printable

This is an HTML part of the message

=20

Link1: <a href="http://secure-web.cisco.com/1dqafaGfZ6Gmc\_TKmEH8FIG\_-10TxJMFka=1-vbjf0-oZc9G-byKGdhMW\_qCESYCPDl0tJfFkI9k069nitsXnL49WLXoXErSWx-YfvWvnBjP18=D3Vjoi501Aghm9yJJaK\_1q6f38p4NiMa18jdSIMp\_1caEdG0LdzeZHh9\_B7\_XinulBHeVsVFAw=\_IkqA7jeUsyfzIDtmJ45YqbI3Dq-WFWhsMqSHpcgkRP6aA\_jw-aKMeoC09uLDowOhAKRy5w-nVfc=EJ-tmvEV941DIAiRlPYosumpsj5e\_4Jvq4B\_PDOFcVrynghkMBGBHLetVirz-SOjRFRHZKSpzNh=bn1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text</a>

[Link2: CLICK ME](#) some text

Link3: [and some text](http://secure-web.cisco.com/1dgafaGfZ6Gmc_TKmEH8FIG_-10TxJMF_=kg1-vbjf0-oZc9G-byKGdhMW_gCESYCPD1QtJffKI9k069nitsXnL49WLXoXErSWx-YfvWvnBjP=18D3Vjoi501Aqhm9yJJAK_1g6f38p4NiMa18jdSIMp_1caEdG0LdzeZHg_B7_XinulBHeVsVF=Aw-IkgA7jEusyfzIDtmJ45YgbI3Dg-WFWhSMgSHpcqkRP6aAjw-aKMEOC09uLDowOhAKrY5w-nv=fceBJ-tmvEV941DIAiRlPYosumpsj5e_4Jvg4B_PDOFcVrYnqhkBGBHLEtVirz-SQjRFRHZKSpz=NhbN1LU8WGA/http%3A%2F%2Fmalware.testing.qooqle.test%2Ftesting%2Fmalware%2F=)

Link4: <a href="http://secure-web.cisco.com/lI8PMIMwyH1YpcRmMiJuqY9F2WGS37D= ksLIADF8z6Mw8ke-Qgd4LygPhRy9rI0WRcHVJ2Vtg1wHXhviN9ntrQN8UzWinsycfwfbHeY6rde=sp0lWhj2DWsowiId45mwDsRxopfhRDWv3mKLHr4ZX70z8eW\_QI8Vxu\_\_-YtpYXgtl1\_mT73FjCs= 5mMHkfIqsS52FXyro-MoX9vu9v14wXSHwH4tpXHVR-Jq2yq\_FWp3eiOTpkkJ6X1wTaofCKssBQcb=RhbFFVuua3GZWWFYoQnDmAgvLbj\_8KZNz8a1FF8Iy\_zUWM07S4pZ2KsT-0qPtllAnUEJEjdvmcgO= GDmeolL6m-q/http%3A%2F%2Fcisco.com and some text</a>

=20 -----7781793576330041025=====

لک نأ دیحولا قرفلا عم D ويرانیسلا يف تناك يتللا ادج ٥٥باسم تاجرخملانأ ظحالم نكمي لسالس عيمج ليدعـت متـي .ـثـيـبـخـلـاـ كـلـتـ طـقـفـ سـيـلـوـ،ـاهـتـبـاتـكـ ـدـاعـاـ تـمـتـ URLـ نـيـوانـعـ .ـانـهـ ـةـراـضـلـاـ رـيـغـ لـسـالـسـلـاـ عـمـ HTMLـ عـزـجـ يـفـ قـبـاطـتـتـ يـتـلـاـ URLـ نـاـونـعـ

This is an HTML part of the message

Link1: [CLICK ME](http://secure-web.cisco.com/1dgafafGfZ6Gmc_TkmEH8FIG_!0TxjIMFkg1~vbjf0~oZc9G~byKgdhMW_gCESYCPDIQjlfk19k069nitsXnL49WLXoXErSwx-YfvWvnBjP18D3Vjo50lAqhm9yJlk_Ag6f38p4N1MaI8jdSIMP_1caEdG0ldezZHMg_B7_XinulBHeKvFsFAw~lkqA7!EusyzfzIDtm45Ygb13Dg-WFWhSMgSHpcakRP6aAjw-aKMEoC09uLDowOhAkRySw-nVfcEj-tmvE94LDAIRjPyosumps5e_4Jvg4B_PDOFCvRynghkMBCBHLeVrz-SQjRFRHZKSpzNhb11U8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text</a></p><p>Link2: <a href=) some text

Link3:

ا خل تلا: صي

- URL ناونع لسالس عي مج ئباتك ديعي يداعلا عزجل/اصنلا ىلع ليغشتلا هيجوت ئداعا Cisco Web Secure
  - ع م ئمس نم URL ئباتك ديعي TEXT/HTML عزجل ىلع ليغشتلا ئداعا إل ل نمآل ليكولا ئمدخ عم قباطتت يتلا ئرخألا URL لسالس عي مج و رصنعملا نم اصنلا عزج Cisco Web

## یا ز ویرانی سلا

حشرمب يسوريفلارىغ دىدەتلا نۇفعشىكىلا يىشفتىلا	معن
يۇتحىملارىچىرىم عارجى	غۇنافىيد
ەداعا! AdvancedConfig href نىكىمت مەت بىولانام صىنلارىقاباتكى	معن

نیوکللا نم ریخآللا ویرانیسلا اذه ققحتی

- نیکمٽ عموٽ ضارٹف الی AS/AV/AMP نیوکٽ عم دیربلا ج٥٥

Policies										
Add Policy...										
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete	
1	URLTest	(use default)	(use default)	(use default)	(use default)	URL_SCORE	Retention Time: Virus: 1 day Other: 4 hours	(use default)		

- ةداعاً ومجم مادختساب ئيسوري فلارىغ تادي دهتلا نع فشكى كلل صحفلا نىوكت متى ديربلا لئاسرىف ةدوجوملا URL نىوانع عيمج ئباتك ةداعاً URL ناونع ئباتك (ةقباسلا تاهوي رانىسلا لثم) ئراضلا ينورتكللإا
  - URL SCORE يوتحجم ئيفصت لماع نىكمت مت : دراوللا يوتحجملأا ئيفصت لماع

Order	Filter Name	Description   Rules   Policies	Duplicate	Delete
1	URL_SCORE	URL_SCORE: if (url-reputation(-10.00, -6.00 , "", 0, 1)) { log-entry("\$FilterName"); url-reputation-defang(-10.00, -6.00,"",0); }		

دوخاً url-reputation-defang طابرالا.

عم ينورتكللإا ديربلا ةباوب ةطساوب اهمييقت و ةلاسرلا ةخسن سفن لاسرا متى جئاتنلا:

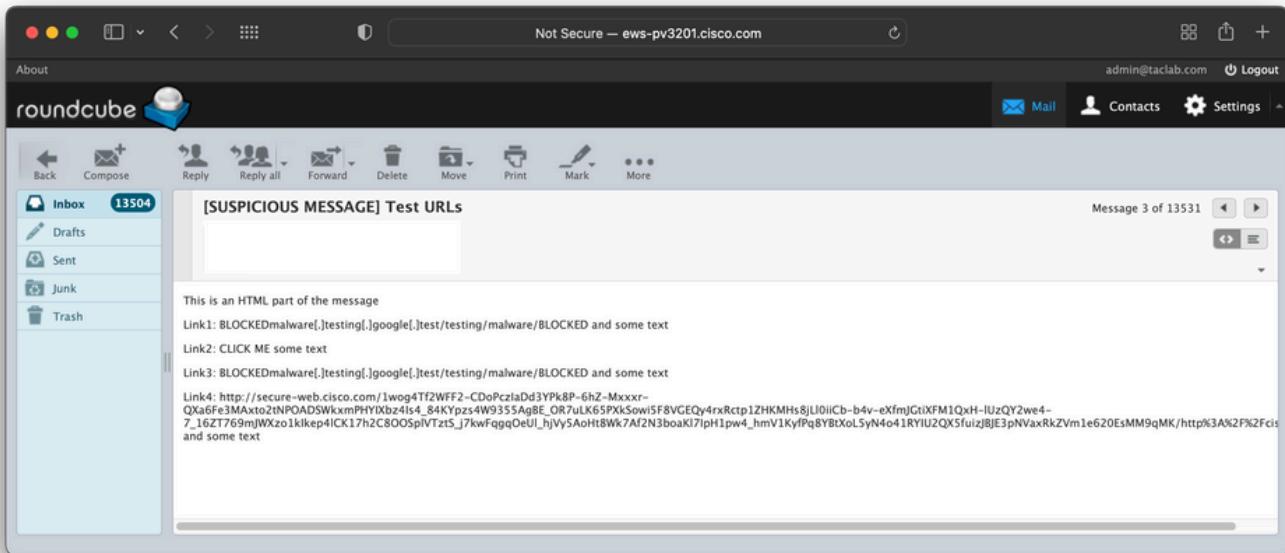
```
Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Condition: URL Reputation Rule Wed Jul 6 15:13:10 2022 Info: MID 139518 Custom Log Entry: URL_SCORE Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 rewritten to MID 139519 by url-reputation-defang-action filter 'URL_SCORE' Wed Jul 6 15:13:10 2022 Info: Message finished MID 139518 done Wed Jul 6 15:13:10 2022 Info: MID 139519 Outbreak Filters: verdict positive Wed Jul 6 15:13:10 2022 Info: MID 139519 rewritten URL u'http://cisco.com' Wed Jul 6 15:13:10 2022 Info: MID 139519 rewritten URL u'http://cisco.com' Wed Jul 6 15:13:10 2022 Info: MID 139519 rewritten to MID 139520 by url-threat-protection filter 'Threat Protection' Wed Jul 6 15:13:10 2022 Info: Message finished MID 139519 done Wed Jul 6 15:13:10 2022 Info: MID 139520 Virus Threat Level=5
```

ثيـحـ،ـيـوـتـحـمـلـاـ ةـيـفـصـتـ لـمـاوـعـ ةـطـسـاـوبـ الـوـأـ ةـلـاـسـرـلـاـ دـيـرـبـلـاـ تـاقـفـدـتـ حـرـشـيـ  
ـقـيـبـطـتـ مـتـيـوـ URL-REPUTATION-DEFANG-  
ـعـازـجـأـ نـمـ لـكـ يـفـ ةـرـاضـلـاـ URLـ نـيـوـانـعـ عـيـمـجـ لـيـطـعـتـ ئـلـاـ عـارـجـ إـلـاـ اـذـهـ يـدـوـيـ ACTION.  
ـصـنـلـاـ ةـبـاتـكـ ةـدـاعـاـوـ html MIMEـ WebSecurityAdvancedConfig hrefـ نـأـلـاـ/ـصـنـلـاـ  
ـلـكـ حـسـمـ مـتـيـ اـمـدـنـعـ HTMLـ صـنـلـخـادـ قـبـاطـتـ يـتـلـاـ URLـ نـاـوـنـعـ لـسـالـسـ لـكـ نـيـكـمـتـ مـتـيـ  
ـلـكـ عـضـوـوـ ةـرـوـظـحـمـلـاـ تـاـمـلـكـلـاـ نـيـبـ URLـ نـاـوـنـعـ صـنـلـعـ اـعـازـجـأـ ةـبـاتـكـ ةـدـاعـاـوـ زـيـيـمـتـ ةـمـالـعـ رـصـانـعـ  
ـزـيـيـمـتـ ةـمـالـعـ يـفـ عـضـوـيـ اـلـ رـاضـخـآـ URLsـ عـمـ ثـدـحـيـ عـيـشـلـاـ سـفـنـ.ـعـبـرـمـ سـاـوـقـأـ نـيـبـ طـاقـنـلـاـ  
ـفـاشـتـكـابـ OFـ مـوـقـيـ.ـةـلـاـسـرـلـاـ يـلـاتـلـاـ "ـيـشـفـتـلـاـ"ـ ةـيـفـصـتـ لـمـاعـ جـلـاعـيـ HTMLـ رـصـانـعـ  
ـهـنـإـفـ،ـكـلـذـلـ ـةـجـيـتـنـوـ(ـ5ـ=ـدـيـدـهـلـاـ ـيـوـتـسـمـ)ـ ةـرـاضـاـنـبـ ةـلـاـسـرـلـاـ فـرـعـيـوـ ةـرـاضـلـاـ URLـ نـيـوـانـعـ  
ـةـلـاـسـرـلـاـ لـخـادـاهـيـلـعـ رـوـثـعـلـاـ مـتـ يـتـلـاـ ةـرـاضـلـاـ رـيـغـوـ ةـرـاضـلـاـ URLـ نـيـوـانـعـ عـيـمـجـ ةـبـاتـكـ دـيـعـيـ  
ـهـنـإـفـ،ـهـذـهـ URLsـ نـيـوـانـعـ لـيـدـعـتـبـ لـعـفـلـابـ مـاـقـ دـقـ يـوـتـحـمـلـاـ ةـيـفـصـتـ لـمـاعـ عـارـجـ إـنـأـلـ اـرـطـنـ  
ـدـمـعـتـمـ لـكـشـبـ اـهـنـيـوـكـتـ مـتـ ثـيـحـ طـقـفـ ةـرـاضـلـاـ رـيـغـ URLـ نـيـوـانـعـ يـقـابـ ةـبـاتـكـ ةـدـاعـاـبـ مـوـقـيـ  
ـنـمـ عـزـجـكـ يـنـورـتـكـلـلـإـلـاـ دـيـرـبـلـاـ لـيـمـعـ يـفـ ةـضـرـعـمـلـاـ ةـلـاـسـرـلـاـ هـيـجـوـتـ عـاـغـلـاـ مـتـ.ـكـلـذـبـ مـاـيـقـلـلـ  
ـعـزـجـكـ يـنـورـتـكـلـلـإـلـاـ دـيـرـبـلـاـ لـيـمـعـ يـفـ ةـضـرـعـمـلـاـ ةـلـاـسـرـلـاـ رـيـغـ URLـ نـاـوـنـعـ نـمـ عـزـجـوـ ةـرـاضـلـاـ Rـيـغـ ـيـجـوـتـ ةـدـاعـاـ تـمـتـ يـذـلـاـ رـاضـلـاـ رـيـغـ ـيـجـوـتـ ةـدـاعـاـ ـيـ5ـ5ـ.

```
=====7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: quoted-printable
```

This is an HTML part of the message

```
=20  
Link1: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLO= CKED and some text  
  
Link2: CLICK ME some text  
  
Link3: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLO= CKED and some text  
  
Link4: http://secure-web.cisco.com/1wog4Tf2WFF2-CD0PczIaDd3YPk8P-6h= Z-Mxxxr-QXa6Fe3MAXto2tNPOADSWkxmPHYIXbz4Is4_84KYpz84W9355AgBE_OR7uLK65PXkSo=  
wi5F8VGEQy4rxRctp1ZHKMHS8jLl0iiCb-b4v-eXfmJGtiXFm1QxH-lUzQY2we4-7_16ZT769mJ=  
WXzo1kIkep4lCK17h2C80OSp1VTztS_j7kwFqggOeUl_hjVy5AoHt8Wk7Af2N3boaK17IpHlpw4=  
_hmV1KyfPq8YBtXoL5yN4o41RYIU2QX5fuizJBJE3pNVaxRkZVmle620EsMM9qMK/http%3A%2F=%2Fcisco.com and  
some text
```



عيمج هيجوت ةداعا مدت. ئلاس نم يداعلا عزجل/اصنلا ىلع ئارجلا سفن قيبطت متي. ئراضللا URL نيوانع هيجوت ئاغلا متي و Cisco Web Secure ليكوللا ريغ URL نيوانع.

=====7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: quoted-printable This is text part of the message Link1: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some text Link2: http://secure-web.cisco.com/lwog4Tf2WFF2-CDoPczIaDd3YPk8P-6hZ-M= xxxr- QXa6Fe3MAXto2tNPOADSWkxmPHYIXbz4Is4\_84Kypzs4W9355AgBE\_OR7uLk65PxkSowi5= F8VGEQy4rxRctp1ZHKMhs8jL10iiCb-b4v-eXfmJGtiXFM1QxH-1UzQY2we4-7\_16ZT769mJWXz= o1kIkep41CK17h2C8OOSplVTztS\_j7kwFqggQeUl\_hjV5AoHt8Wk7Af2N3boaK17IpH1pw4\_hm= V1KyfPq8YBtXoL5yN4o41RYIU2QX5fuizJBJE3pNVaxRkZVmle620EsMM9qMK/http%3A%2F%2F= cisco.com and some text =====7781793576330041025==

صيخلتللا:

- ئروظحمل تك يللا ئاباتك ديعي "يداعلا عزجل/اصنلا" ىلع CF ليرغشت ةداعا
- امدنع A زييمت ئاما ع نم URL ئاباتك ديعي TEXT/HTML ليرغشت ةداعا
- زييمت ئاما ع ديرجت متي A
- لتك عم قباطتت يتللا URL لسالس ئفاك ئاباتك TEXT/HTML عزج ىلع ليرغشت ةداعا
- لتك عزج لسالس عيمج ئاباتك ديعي يداعلا عزجل/اصنلا ىلع ليرغشتلا هيجوت ةداعا
- URL ناوونع لسالس عيمج ئاباتك ديعي يداعلا عزجل/اصنلا ىلع ليرغشتلا Cisco Web Secure (راض ريغ)
- عزج عم html A-Tag href URL ئاباتك ديعي، TEXT/HTML نم OUTBREAKCONFIG عزج ىلع ليرغشتلا ئادعإ
- نمآللا ليكولا ئامدح عم قباطتت يتللا ئرخألا URL لسالس عيمج و رصنعلاب صاخلا اصنلا (راض ريغ) Cisco نم بيلول

## اهحالص او ئاطخألا فاشكتسا

طبربلا ناوونع ئاباتك ئادعاب ئلاس ملا يف قيقحتلل ئجاج كانه نوكت امدنع طاقنلا كلت عبتا.

- ئللا ئاباجلا او رمألا URL يرج mail\_log. ئيجست نيك متب مق OUTBREAKCONFIG  
Do you wish to enable logging of URL's? [N]>"
- ئاعومجم ملا ماظن ئاضعأ نم وضع لك تاداع WEBSECURITYADVANCECONFIG ئاحصلنا نم ققحتلا
- اقفو ناطوبضم href و اصنلا ئاباتك ئادع رايغ نأ نم دكأت و ينورتكللا ديربلا ئابا بول

رثوت ال و زاهجلا ىوتسم ىلع صاخ رمألا اذه نأ ركذت . زاهج لك ىلع ٰقيرطلسا سفنبو كذل  
ةعومجملما ماظن وأ ٰقيرطملا تادادعإ ىلع انه اهؤارجا مت يتلا تارييغتلما

- ٰفيصت لماع نيكمت نم دكأت، ٰيوكتملا ٰفيصت لماع ٰقطشنأو طورش نم ققحت  
ٰفيصت لماع دوجو مدعا نم ققحت . حيحصللا دراولا ديربلا جهن ىلع هقيبطتو ٰيوكتملا  
ٰجلاعمل يطختلا هنكمي يذلا يئاهنلا عارجيلا مادختساب لباق نم هتجلاعيم تمت رخآ ىوتجم  
يرخألا ٰفيصتلا لماع.

- ٰناسرلا عاجرسا ركذت . ٰيئاهنلا ٰناسرلا او ردمسلل ٰيلوألا ٰخسنلا نم ققحت  
امدنع اهيلىع دامتعالا نكمي ال MSG لثم ٰصاخلا تاقيسنلل نأ، قيسنتب  
ينورتكللا ديربلا عالمع ضعب كل حمسى . ٰناسرلا يف قيقحتلاب رمألا قلعتي  
ينورتكللا ديرب ليمع عم ٰناسرلا ٰخسن دادرتسا ٰلواحمو، ردمسللا ٰناسرلا ضرع  
امنيب ٰناسرلا ردمص ضرع MS Outlook for Mac كل حمسى، لاثملالا ليبس ىلع . فلتخم  
طقف سوّرلا ضرع Windows رادصا حمسى.

## صلخ

امدنع لصفا لكشب ٰرفوتتملا نـيوكـتـلـا تـارـايـخـ مـهـفـ يـفـ ٰدعـاسـمـلـاـ وـهـ ٰلاقـمـلـاـ هـذـهـ نـمـ ضـرغـلـاـ  
اهـفـانـبـ مـتـيـ ٰثـيـدـحـلـاـ لـىـاـسـرـلـاـ نـأـ رـكـذـتـنـ نـأـ مـهـمـلـاـ نـمـ وـ URLـ نـاـونـعـ ٰبـاتـكـ ٰداعـابـ رـمـأـلاـ قـلـعـتـيـ  
ضرـعـ نـكـمـيـ هـنـأـ يـنـعـيـ اـذـهـوـ MIMEـ رـايـعـمـ مـادـخـتـسـابـ يـنـورـتـكـلـلـاـ دـيـرـبـلـاـ جـمـارـبـ بـلـغـأـ ٰطـسـاوـبـ  
وـأـ يـنـورـتـكـلـلـاـ دـيـرـبـلـاـ لـيـمـعـ تـايـنـاـكـمـاـ ىـلـعـ اـدـامـتـعـاـ فـلـتـخـمـ لـكـشـبـ ٰناسـرـلـاـ ٰخـسـنـ سـفـنـ  
عالـمـعـ مـظـعـمـ مـدـخـتـسـيـ،ـ يـضـارـتـفـاـ لـكـشـبـ (ـH~T~M~L~)ـ عـضـوـلـبـاـقـمـ صـنـلـاـ)ـ ٰنـكـمـمـلـاـ عـاصـوـأـلـاـ  
وـ HTMLـ ٰبـاتـكـ ٰداعـابـ رـمـأـلاـ قـلـعـتـيـ اـمـدـنـعـ لـىـاـسـرـلـاـ ضـرـعـلـ H~T~M~L~ ٰثـيـدـحـلـاـ يـنـورـتـكـلـلـاـ دـيـرـبـلـاـ  
URLـ نـيـوانـعـ ٰبـاتـكـ ٰداعـابـ مـوقـتـ ٰيـصـارـتـفـاـلـاـ دـيـرـبـلـاـ ٰبـاـوـبـ نـأـ ٰاعـارـمـ عـاجـرـلـاـ،ـ URLـ  
بـجـيـوـ ٰيـفـاكـ نـوـكـتـ الـ يـتـلـاـ تـالـاحـلـاـ نـمـ رـيـثـكـ يـفـ a~tagـ رـصـنـعـلـ hrefـ ٰقـمـسـ لـخـادـ طـقـفـ ٰدوـجـوـمـلـاـ  
رمـأـلاـ مـادـخـتـسـابـ صـنـلـاـ ٰبـاتـكـ ٰداعـابـوـ hrefـ نـمـ لـكـ نـيـكـمـتـلـ اـهـرابـتـعـاـ  
مـاظـنـ رـبـعـ قـسـانـتـلـلـوـ،ـ زـاهـجـلـاـ ىـوتـسـمـ ىـلـعـ رـمـأـ اـذـهـ نـأـ رـكـذـتـ .ـ webSecurityAdvancedConfigـ

## 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).