

ىلع ٥٥ يجوت ٽداع٩و URL ٦ا عاغل٩ ئارج٩ مهف ٽنمآل٩ ينورتكلل٩ ديربل٩ ٽباوب

تايي وتحمل٩

[قىمدقمل٩](#)

[قىس اس آل٩ تابل طتمل٩](#)

[تابل طتمل٩](#)

[قىمدىختس مل٩ تابل طتمل٩](#)

[قىس اس ا تامولىع](#)

[قلاس بىرلا جذون](#)

[غۇن افييد - لە ول٩ عزجل٩](#)

[تائنى وكتل٩](#)

[عاف دل٩ ا قىلىمع](#)

[أويىرانى سل٩](#)

[ب وىرلانى سل٩](#)

[هېجوتل٩ ٽداعا - يناثل٩ عزجل٩](#)

[تائنى وكتل٩](#)

[هېجوتل٩ ٽداعا لىعف](#)

[مېچ وىرلانى سل٩](#)

[لەد وىرلانى سل٩](#)

[هېجوتل٩ ٽداعا - 3 عزجل٩](#)

[نېي وكتل٩](#)

[E وىرلانى سل٩](#)

[واو وىرلانى سل٩](#)

[ئاز وىرلانى سل٩](#)

[اھھالىص او عاطخا لە فاش كتسا](#)

[صىخلم](#)

ٽمدقمل٩

حشرم يف ٽمدختس مل٩ هېجوتل٩ ٽداعا تايىلمۇ طبرلا عاغل٩ نىب قىرفلا ٽقىيىۋاده فصىي
صىنل او href ٽمىسىل حاتملا ٽباتكلا ٽداعا رايىخ مادختسا ئيفىك، طبرلا ناونع

قىس اس آل٩ تابل طتمل٩

تابل طتمل٩

مادختساب ٽلوبقىم مادختس ا تاسايس ضرفل وا، URL ناونع ٽعمىس ئىل ادانتسا عارج٩ ذاختال

لکشب "یشفتلا ۃیفھصت لمابع" ۃزیم نیکھمت بجی، یوتحمل او لئاسرلا ۃیفھصت لمابع.

ۃمدختسملا تانوکملما

ۃیلاتلا ۃیداملا تانوکملما وجماربلما تارادصلما ایلما دنتسملا اذھیف ۃدرالا تامولعملا دنتسست:

- نام ۃنماںلا ینورتكللما دیربلما ۃباؤب Cisco
- یشفتلا ۃیفھصت لمابع
- لئاسرلا و یوتحملما ۃیفھصت لمابع

ۃصاخ ۃیلمع ۃئیب یف ۃدوچوملا ۃزهچا نام دنتسملا اذھیف ۃدرالا تامولعملا عاشنامت تنالک اذا. (یضارتھا) حوسنم نیوکتب دنتسملا اذھیف ۃمدختسملا ۃزهچا عیمج تأدباً رمأ یأ لمحتملما ریثأتلل کمھف نام دکأٹف، لیغشتلا دیق کتک بش.

ۃیساساً تامولعم

لمابع مادختساب URL ۃیف و ۃعمس یلعا ناب عارج ڈاختا یہ URL ۃیفھصت ۃزیم تاردق یدھا طبترملما طرشلما URL ناونع صحف ۃجیتن یلما ادانتسا. یوتحملما و او لئاسرلا ۃیفھصت URL ناونع یلعا ۃحاتملما ۃثالثلا تاءارج الا دحأ قیبھت نکمی، URL ناونع ب:

- ناونع نام رطخلما ۃلمازا
- یلما ہیجوتلا ۃداع Cisco Security Proxy
- ۃیصن ۃلاسرب URL لادبتسا

و ہیجوتلا ۃداع Defang. URL ناونع تارایخ نیب کولسلا حرش و ہ دنتسملا اذھیف زیکرتلما ریغ دیدھتلما فاشتکا ل URL ناونع ۃباتک ۃداع تاردقل احیض و تو ارجوم افص و مدقی امک یشفتلا ۃیفھصت لمابع یسوريفلما.

ۃلاسرلا جذومن

ددعتم ۃلاسرلا عون یہ تارابتھا عیمج یف ۃمدختسملا ۃیجذومنلا ۃلاسرلا ہ ذھیف ۃداع html / صنلما لھسلما / اصنلما یوتحملما عون سفن یلعا یوتحتھو ینورتكللما دیربلما جمانرب ۃطس اوپ ایئاقلت عازج الا لھسلما / اصنلما یوتحم ریحھت مھ، ضرغلما اذھلھو HTML ریغ و HTML تالبقوتسمل قسنملا ایودی html / صنلما.

```
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----

غنافي د - لوالا عزجا

تانيوكلا

نـيوكـلـا مـدـخـتـسـي ،ـلـوـأـلـا عـزـجـلـا يـفـ

- ةحفاكم / (AS) ةيضارتفالا يئاوشعلـا ديـربـلـا ةـحـفـاكـمـ جـمـارـبـ دـادـعـا لـيـطـعـتـ عـمـ دـيـربـلـا جـهـنـ
- ةيفصـتـ لـمـاوـعـوـ (AMP) ةـرـاضـلـا جـمـارـبـلـا نـمـ ةـمـدـقـتـمـلـا ةـيـامـحـلـا / (AV) تـاسـوريـفـلـا

(OF) یش فتل

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)	

- URL_SCORE يوتحم ۆي فصت لماع نى كەمت مەت : دراولە يوتحملا ۆي فصت لماع

Filters			
	Add Filter...		
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); }	

كلت، ةراضلـا URL نـيـوانـع ةـقـبـاطـمـل URL نـاـوـنـع ةـعـمـس ةـلـاحـىـوـتـحـمـلـا ةـيـفـصـتـ لـمـاعـ مـدـخـتـسـيـ
ـيـوـتـحـمـلـا ةـيـفـصـتـ لـمـاعـ مـسـاـ لـيـجـسـتـ مـتـيـ، ءـارـجـاـكـ ـ10.00ـ وـ6.00ـ نـيـبـ اـمـ ـىـلـاـ رـيـشـتـ يـتـلـاـ
ـطـابـتـرـالـاـ url-reputation-defang ءـاغـلـاـ ءـارـجـاـ ذـاخـتـاـ مـتـيـ وـ.

عاف دل او يلمع

مق ؛ اريسفت مدخلتسملاليلدمدقى . يعافدىالىمعلا وەام حضون نأ ناكمب ةيمهألا نمو لىاسرلا يملىتسىناكماپ لازىال . هقوقى رقنىلا نكمىال ثيحب URL ناونع ديدحت ئاغلاب خسنو URL ناونع ةيۇر.

أ ویرانی سلا

حشرمب يسوري فلاريغ ديدهتلا نع فشكلا يشفتللا	ال
ىوتحملأا حشرم عارجإ	غضنافي د
AdvancedConfig href نيكمت مت بيولـا نامـا صـنـلـا ظـبـاتـكـ ةـداعـاوـ	ال

يضا ارتفالا تاداع إلاب هن يوكت مت يذلا طابت رالا عاغلإ عارجأ ڦجيتن وي رانيسلا اذه حرشی قلأا. طقف HTML تامالع درج متی ام دنبع URL ناونع ڦباتک ڏداعا مت، يضا ارتفالا دادع إلاب یف اهلخ ادب URL نیوانع ضعب یلع یوتحت HTML ڦرقف یلع ڦرظان:

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

بـسـانـمـاـ زـيـيـمـتـ مـتـيـ ،ـنـيـيـلـوـأـلـاـ نـيـتـرـقـفـلـاـ يـفـ .ـطـارـلـاـ ةـهـجـوـىـلـاـ رـيـشـيـوـاهـسـفـنـ ةـمـالـعـلـاـ يـفـ ةـقـفـرـمـلـاـ `href=` رـصـنـعـلـاـ نـمـضـتـيـ اـذـهـ نـمـضـتـيـ نـأـ نـكـمـيـ .ـطـارـلـاـ ةـهـجـوـىـلـاـ زـيـيـمـتـلـاـ ةـمـالـعـ رـصـانـعـ نـمـضـ ئـوـتـحـمـلـاـ رـيـشـيـ نـأـ نـكـمـيـ نـمـ لـكـ يـفـ URLـ نـاـوـنـعـ طـابـتـرـاـ سـفـنـ 1ـ لـوـأـلـاـ طـابـتـرـاـلـاـ نـمـضـتـيـ URLـ نـاـوـنـعـ طـابـتـرـاـلـاـ نـوـكـتـ نـأـ نـكـمـيـ كـلـتـ URLـ نـيـوـانـعـ نـأـ ةـظـاحـاـلـمـ نـكـمـيـ .ـرـصـنـعـلـاـ نـمـ صـنـلـاـ عـزـجـوـ ةـمـسـ ةـرـقـفـلـاـ hrefـ لـخـادـ طـقـفـ بـسـانـمـلـاـ URLـ نـاـوـنـعـ يـنـاـثـلـاـ طـابـتـرـاـلـاـ نـمـضـتـيـ .ـفـلـتـخـمـ رـصـانـعـ يـأـ نـمـضـتـتـ الـ ةـرـيـخـأـلـاـ Aـ .ـ

 قوف رـشـؤـمـلـاـ كـيـرـحـتـبـ مـوقـتـ اـمـدـنـعـ حـيـحـصـلـاـ نـاـوـنـعـلـاـ ةـظـاحـاـلـمـ اـمـئـادـ نـكـمـيـوـ :ـةـظـاحـاـلـمـ عـوـسـلـ .ـةـلـاسـرـلـاـبـ ةـصـاخـلـاـ رـدـصـمـلـلـ ةـيـجـمـرـبـلـاـ تـامـيـلـعـتـلـاـ ضـرـعـبـ مـوقـتـ اـمـدـنـعـ وـأـ طـابـتـرـاـلـاـ عـالـمـعـ ضـعـبـعـ مـ ةـلـوـهـسـبـ رـدـصـمـلـاـ ةـيـجـمـرـبـلـاـ تـامـيـلـعـتـلـاـ يـلـعـ رـوـثـعـلـاـ نـكـمـيـ الـ ،ـظـحـلـاـ نـيـرـوـهـشـمـلـاـ يـنـورـتـكـلـإـلـاـ دـيـرـبـلـاـ

ةـرـاضـلـاـ URLـ نـيـوـانـعـ دـيـدـحـتـ ءـاعـلـاـ مـتـيـ ،ـعـيـفـصـتـ لـمـاعـبـ ةـلـاسـرـلـاـ ةـقـبـاطـمـ درـجـمـبـ تـامـالـعـلـاـ يـلـعـ رـوـثـعـلـاـ نـكـمـيـ OUTBREAKCONFIGـ رـمـأـلـاـ مـاـدـخـتـسـابـ URLـ نـيـجـسـتـ نـيـكـمـتـ دـنـعـ يـفـ URLـ نـيـوـانـعـ mail_logـ .ـ

```
Mon Jul  4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/ has
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
Mon Jul  4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/ has
Mon Jul  4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/ has
Mon Jul  4 14:46:43 2022 Info: MID 139502 rewritten to MID 139503 by url-reputation-defang-action filter
```

اهـتـبـاتـكـ ةـدـاعـاـ تـمـتـ ةـلـاسـرـكـلـذـ 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====

ةدرج م زييمت ۋەمالۇ ئەلەسەرنم HTML/صىنلا عزجىلىع مەت يىذلا طېرلا ئاغلى ئارجا ۋەجىتن
الك طېر ئاغلى مەت، نېيىلۋەلا نېيترقىلى يىف. سەمل نودب كرت زىيەمىتلە ۋەمالۇ ىوتەمەن
ۋەرقىلى يىف URL ناونۇع رەصنىعىلا نم صىنلا عزج كرت و HTML ۋەرفش درج مەت ثىح نېيەپرلا
ۋەرقىلى نم URL ناونۇع نا ئەظەھارلىم بچىي HTML رەصنىعىب صىاخلا صىنلا عزج نم ناونۇع وە ئىلۋەلا
نوكىي الأ بچىي HTML A، تامالىع نودب نكىلو طابىت رالا ئاغلى ئارجا ذاختا دىعىب اىئەرم لازىي ال ئىلۋەلا
مەتىي ال انه URL ناونۇع نا ئەجىت ئەڭلىڭىز ئەزىز ئەن
ھېف اپوغرم اکولس نوكىي ال دق. طابىت را هەرابىتغا مەتىي ال، زىيەمىت تامالىع يى ئىبھەع ضۇرۇم
يىف ھەذىفەن تەخسەن و طابىت رالا ئېۋەر ئەلەسەب مەدختىسىملىك نكەمەي، ال و نېيەپبىسىل
فاشتىكا ئىلە ليەمت يىنورت كىلەلا دىرىپلا جەمەرپەن ئەن ئەن ئەن ئەن ئەن ئەن ئەن ئەن ئەن
رەقنىلى ئەباق اطبار ھەلۈچۈچ و صىنلا لخاد URL نىوانىع نم حېچىص لەكش.

يىداعىلا عزجلا/صىنلا نم ضۇرتىي. ئەلەسەرنم طېسېلى عزجلا/صىنلا ئىلىع ۋەرەظن قىلنلىف
مەھفىي ال يىذلا MUA ۋەتساوب لەسلى/صىنلا ضرۇم مەتىي. صىنلا جەزۈمن يىف URL يىنداونۇع
ىرىت ال، نېيىتىدەلە يىنورت كىلەلا دىرىپلا ئەلەم مەظۇم يىف. ئېجەرمىپلە HTML تامىلىع
ادىم كېب صىاخلا يىنورت كىلەلا دىرىپلا لىمەع نېيەكتەپ مەت مەل ام ئەلەسەرلىل ئەداعىلا ئازجاڭلا/صىنلا
يىلۋاؤ EML قىسەنەت وەو، ئەلەسەرلىل رەصمەلە زەرمەلە نم قىقەتلىلا ئىلە جاتحت، ئەداع. كەلذب مايىقلە
اھنم قىقەتلىل او MIME ئازجاڭ ئېۋەر ئەلەسەرلىل.

رەصمەلە ئەلەسەرلىلا نم يىداعىلا عزج/صىنلا نم URLs انه جاردىلا رەھظى.

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

Link2: <http://cisco.com> and some text

نوكىي، يىضاپتىفال كىشىب. اھلىتىف عزىز مەت و ئەثىب خەجىتن ئىلىع تەلصەخ طېاولىلا ھەذە ئىدەجىلە
نەع ئەفلىت خەجىتن MIME عون نم يىداعىلا عزجلا/صىنلا ئىلىع ھەذاختا مەت يىذلا طېرلا ئاغلى ئارجاڭ
سەۋىقأ نېيەپ طاقىنلا لەك و ۋەرەۋەچەملى تامىل كىلەلا نېيەپ عقىي HTML/صىنلا عزج يىف يىتلا كەلتىلە
ۋەجىتلىق بەرمە.

=====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==

صيخلتل:

- ةروظحم لتك ئل URL ۋېباتك دىعى "يداعلا عزجلا"/"صنلا"لىغشتلا ئاغلا
- زىيىمت ۋەمالۇ نم URL ناونع ۋېباتك دىعى TEXT/HTML A عزج ئىلع لىغشتلا ئاغلا يذلار، سمالتىم زىيىمت تامالۇ نىب دوجوملا صنلا نووب A زىيىمت ۋەمالۇ نوكت امدىن اضىيأ URL ناونع نوکي نأ نكىمى

ب ويرانىسلا

حىشىمىپ يىسوري فلارىغ دىدەتلا نىع فشكىلا يىش فلتلا	ال
ىوتىحملار حىشىمىپ ئارجا	غۇنا فىيد
AdvancedConfig href صنلا ۋېباتك دىعى	مۇن

دەخلىسى دىرىجىتلى ئاغلا ئارجا كۈلسىز رىيغەت ئەفيك لوح تامولۇم ويرانىسلا اذە رفوى
ىوتىسىم بىرلىك CLI رىمأ وە webSecurityAdvancedConfig. WebSecurityAdvancedConfig تارايىخ
رىيغەتب انى تادادعەلە دەخلى ئەم سىزى. حىسىم بىرلىك URL تادادعەلە طبىضىب حىمىسى يىذلار زاھىجلا
لىطعتلار ئارجالى يىضارتىفالا كۈلسىلە.

> 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 rewrite

...

هنا لى ا ئباج إلـا رـيـشـت..، عـبارـلـا لـأـفـسـلـا يـفـ
يـتلـا URL نـاوـنـع لـسـالـسـ لـكـ نـإـفـ، ئـلـاسـرـلـا نـمـ HTML ئـلـا دـنـتسـمـلـا عـزـجـ ئـلـاحـ يـفـ
وـأـصـنـ عـزـجـ نـوـكـتـ، رـصـنـعـلـ Aـtagـ مـتـ يـتـلـا ئـلـاحـلـا تـنـاـكـ اـيـأـقـبـاطـ
نـكـلـوـ، ئـعـاتـسـمـ اـهـتـاـذـ ئـلـاسـرـلـا نـوـكـتـ وـيـرـانـيـسـلـا اـذـهـ يـفـوـ. اـهـتـبـاـتـكـ ئـدـاعـاـتـمـ رـصـانـعـ يـأـ جـرـاخـ
الـيـلـقـ ئـفـلـتـخـ جـئـاـتـنـبـ.

زمـربـ هـنـرـاقـ وـىـرـخـاـ ئـرـمـ HTML نـيـوـانـعـ مـادـخـتـسـابـ MIME/text HTML عـزـجـ دـوـكـ ئـلـعـ ئـرـظـنـ قـلـاـ
يـنـورـتـكـلـإـلـا دـيـرـبـلـا ئـبـاـوبـ ئـطـسـاـوبـ هـتـجـلـاعـمـ تـمـتـ يـذـلـاـ.

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 نـيـوـانـعـ وـهـ قـبـاطـيـ اـمـ لـكـ نـإـفـ، صـنـلـا ئـبـاـتـكـ ئـدـاعـاـ وـ hrefـ رـايـخـ نـيـكـمـتـ مـتـيـ اـمـدـنـعـ
رـصـنـعـ صـنـ عـزـجـ وـأـصـنـ hrefـ نـمـ اـعـزـجـ URL نـاوـنـعـ نـاـكـ عـاـوـسـ اـهـيـأـغـلـاـ مـتـيـ ئـيـفـصـتـلـلـ HTML
ـقـيـثـوـنـمـ رـخـاـ عـزـجـ يـفـ هـيـلـعـ رـوـثـعـلـاـ مـتـ وـأـ زـيـيـمـتـ ئـمـاـلـعـ Aـtagـ.

```
=====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-----

قمالع رصنعم ديرجت متى ام دن ع اهكى كفت مت يتلـا URL نـي وانع ئـباتـك ئـداعـا نـآلـا متـي URL نـاونـع قـيـسـنـت قـبـاطـي اـمـدـنـع طـابـتـرـالـابـ صـاـخـلـاـ صـنـلـاـ عـزـجـ ئـبـاتـك ئـداعـا عـمـ A زـيـيـمـتـلـاـ نـمـ يـدـاعـلـاـ عـزـجـلـاـ /ـصـنـلـاـ يـفـ ئـدـوـجـوـمـلـاـ ئـقـيـرـطـلـاـ سـفـنـبـ هـتـبـاتـكـ دـاعـمـلـاـ صـنـلـاـ عـزـجـ لـمـعـ مـتـيـ نـيـبـ اـهـعـضـ وـمـتـيـ طـاقـنـلـاـ لـكـ وـرـوـظـحـمـلـاـ تـامـلـكـلـاـ نـيـبـ رـصـنـعـلـاـ عـضـ وـمـتـيـ MIME ئـلـاسـرـ جـمارـبـ ئـالـمـ عـضـعـبـ لـعـجـيـوـ،ـهـقـصـلـوـ URL نـاـونـعـ خـسـنـنـمـ مـدـخـتـسـمـلـاـ كـلـذـعـنـمـيـ .ـعـبـرـمـ سـاـوـقـأـ رـقـنـلـلـ الـبـاـقـ صـنـلـاـ يـنـورـتـكـلـلـاـ دـيـرـبـلـاـ

صیخلتلا:

- ڦروظحم لٽک یل URL ڦباتک دیعی "يداعل ا عزجلا"/"صنلا" یل ع لیغشتلا ٽاغلإ
 - HTML A زییمت ڦمالع نم URL ناونع ڦباتک دیعی TEXT/HTML عزج یل ع لیغشتلا ٽاغلإ
 - زییمت ڦمالع دیرحت متی امدع A
 - URL لسالس ڦفاك ڦباتک ڦداعا یل TEXT/HTML عزج یل ع تیبٺتلار ٽاغلإ لیغشت یدؤی ڦروظحم لٽک عم قباطتت یتلار

هـجـوـتـلـا ةـدـاعـا - يـنـاـثـلـا عـزـجـلـا

تائیوکتلا

نیوکتل مدخلت سی ینا ثلا عز جلا یف

- لطعم نم و يضر ارتفالا AS/AV/AMP نيوكت عم ديربل ا جه

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)		

- URL_SCORE یوتحم ۆیفصت لمامع نیکمەت مەت : دراولە یوتحملا ۆیفصت لمامع

Filters			
Order	Filter Name	Description Rules Policies	
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); }	 

،ةراضلـ URL نـيـوانـعـ ةـقـبـ اـطـمـلـ URL نـاـونـعـ عـمـسـلـاـ ةـلـاحـ ئـوـتـحـمـلـاـ ةـيـفـصـتـ لـمـاعـ مـدـخـتـسـيـ،ـ ئـوـتـحـمـلـاـ ةـيـفـصـتـ لـمـاعـ مـسـاـ لـيـجـسـتـ مـتـيـ،ـ عـارـجـإـكـ 10.00- وـ6.00- نـيـبـ اـمـ ئـلـاـ رـيـشـتـ يـتـلـاـ عـارـجـإـلـاـ ذـاخـتـ | redirect action مـتـيـ وـ.

٥٤ لِعْنَادِي وَتِلْجَوٍ

رقنلا ۋەلسىرلا مىلتىسىملىكى رقنىلا تقو مىيىقتل Cisco ناما لىكى و ئەمدەخ ىلى ھېجوتلىا ۋەداعا حىيت
عنمەي يىذلار، ۋە باحسلىا يىف Cisco نەم بىولما ناما لىكى و ىلىا ٥٥٥ ھېجوت ۋەداعا و طابىتىرالا قوف
راپىش ھەنأىلە عقوقمىلما فىرىعەت مەت اذا لۈوصۇلما.

میج ویرانی سل

حشرمب يسوري فلارىغ ديده تلانع فشكلا يشفتلا	ال
ىوتحملالا حشرم عارجا	ييجوت ةداعا
AdvancedConfig href نيك مت متب يولانا صتلاباتك ةداعا	ال

مٽ يذلا قرفلا عم لـوألا عزجلـا نـم (أ) ويـرانـيـسـلـلـ كـولـسـلـلـ يـفـ اـدـجـ هـبـ اـشـمـ ويـرانـيـسـلـاـ اـذـهـ مـتـ يـ.ـ هـتـيـ بـثـتـ عـاـغـلـاـ نـمـ الـدـبـ URLـ نـاـونـعـ هـيـجـوـتـ ةـدـاعـإـلـ ةـوـتـحـمـلـ ةـيـفـصـتـ عـاـرـجـاـ يـفـ هـوـارـجـ "ـيـنـعـيـ اـمـ ،ـيـضـاـرـتـفـالـاـ تـادـادـعـالـاـ إـلـاـ WebSecurityAdvancedConfigـ تـادـادـعـاـ ةـدـادـعـسـاـ"ـ يـلـعـ تـادـادـعـإـلـاـ هـذـهـ نـيـعـتـ ..ـ Nـ.

ةراضللا طاقنلا موقت .ميموقت URLs ناونع لك فاشتكاب ينورتكللا ديربلا ةرابع موقت URL_SCORE url-reputation-proxy-redirect-action عارجلا ذخأتو

```
Tue Jul 5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/ has re  
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 re  
Tue Jul 5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/ has re  
Tue Jul 5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/ has re  
Tue Jul 5 12:42:19 2022 Info: MID 139508 rewritten to MID 139509 by url-reputation-proxy-redirect-action
```

دوچوملا سفن . ئەلسىرلا نم HTML عزج يف URL نىوانع ۋېباتك ۋەداعى ئېفيك ىلۇغ ۋەرظن قىلۇ زىيىمت ۋەمالۇ رىصنىل href ۋەمىس يف ۋەدوچوملا URL نىوانع ۋېباتك ۋەداعى مەتى ، أويغانىسىلار يف طېرىلما ئاغلى ئارجى ئەم رىصنىع نىم صىنلارا عزج يف ۋەدوچوملا URL نىوانع يىطخت مەتى و طقىف ناونع ۋېباتك ۋەداعى مەتت ، ھېجوت ۋەداعى ئارجى ئەم نىكل ھەلمكاب A زىيىمت ۋەمالۇ رىصنىع دىيرجت مەتى URL ۋەمىس يف href.

```
--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

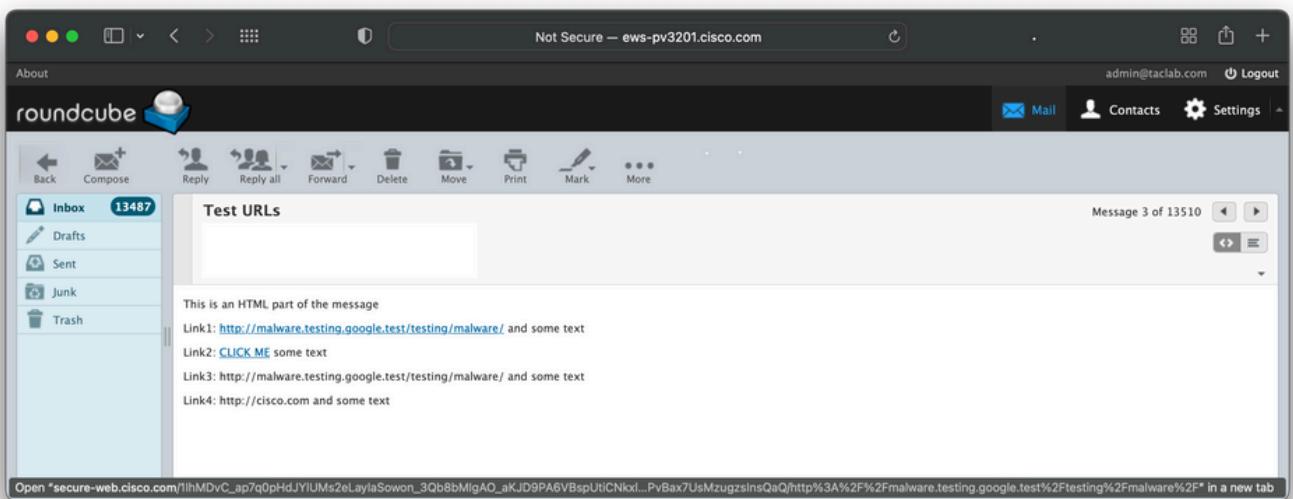
Link2: [CLICK ME](#) some text

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

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

-----7781793576330041025-----

و Link1 نم لك ريشي :ني طشن ني طابترا ينورتكللا ديربلا لي مع ضرعه ، كل ذل قجيتن و
ديربلا لي مع يف ةضرعمل ا ئلاس رلا نكلو Cisco نم بيولا نامأ ليك و مدمخ لىا
لىا . يضارف ا لكشب اهتباتك ةداعا متى ال يتلا او a ةماليع نم صنلا عزج ضرعت ينورتكللا
عزج ضرعه يذلا بيولا ديرب لي مع نم جارخ لىا لىع ةرظن عاقل لاجرلا ، اذه تحت لضفأ يوتسم
ئلاس رلا نم html/صنلا.



ةلسلس لك نأْل مهفلل لهسأْ هيجوتلا ةداع| ودبـت، MIME عـزـجـنـمـ يـدـاعـلـاـ عـزـجـلـاـ/ـصـنـلـاـ يـفـ اـهـتـبـاتـكـ ةـدـاعـ|ـ مـتـيـ ةـجـيـتـنـلـاـ 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/1duptzzum1fIIuAgDNq__M_hrANf0QZ4xu1DjL8yqeTmpwbH1Po0722VEIVeKfs
Link2: <http://cisco.com> and some text

=====7781793576330041025==

صيخلتلا:

- يتلـا URL نـاونـع ظـلـسـلـس ةـبـاتـك دـيـعـي يـدـاعـلـا عـزـجـلـا/صـنـلـا ىـلـع لـيـغـشـتـلـا هـيـجـوـت ةـدـاعـا Cisco Web Secure
- يـتـلـا ئـرـخـأـلـا URL لـسـالـسـعـيـمـجـ كـرـتـيـ هـنـكـلـوـ Cisco Web Secure لـيـكـوـ وـقـمـدـخـ عـمـ قـبـاطـتـتـ اـبـ مـادـخـتـسـ اـبـ ظـلـدـعـ رـيـغـ قـبـاطـتـ

لـادـ ويـرـانـيـسـلـا

حـشـرـمـبـ يـسـوـرـيـفـلـا رـيـغـ دـيـدـهـتـلـا نـعـ فـشـكـلـا يـشـفـتـلـا	إـلـ
ىـوـتـحـمـلـا حـشـرـمـ ءـارـجـا	هـيـجـوـتـ ةـدـاعـا
صـنـلـا ةـبـاتـكـ ةـدـاعـاـوـاـ نـاـمـاـ نـيـكـمـتـ مـتـ بـيـوـلـاـ AdvancedConfig hrefـ	مـعـنـ

لـسـالـسـ ةـفـاـكـ ةـبـاتـكـ ةـدـاعـإـلـ .لـوـأـلـا عـزـجـلـا يـفـ درـاـوـلـا (ـبـ) ويـرـانـيـسـلـاـ اـذـهـوـ كلـذـبـ مـاـيـقـلـا مـتـيـ .اهـنـيـكـمـتـ مـتـ ةـلـاـسـرـلـاـ نـمـ HTMLـ عـزـجـ يـفـ قـبـاطـتـتـ يـتـلـاـ URLـ نـاـوـنـعـ webSecurityAdvancedConfigـ "Do you want to rewrite both the URL text and the href in the message? .. لـأـوـسـلـاـ ىـلـعـ

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

This is an HTML part of the message

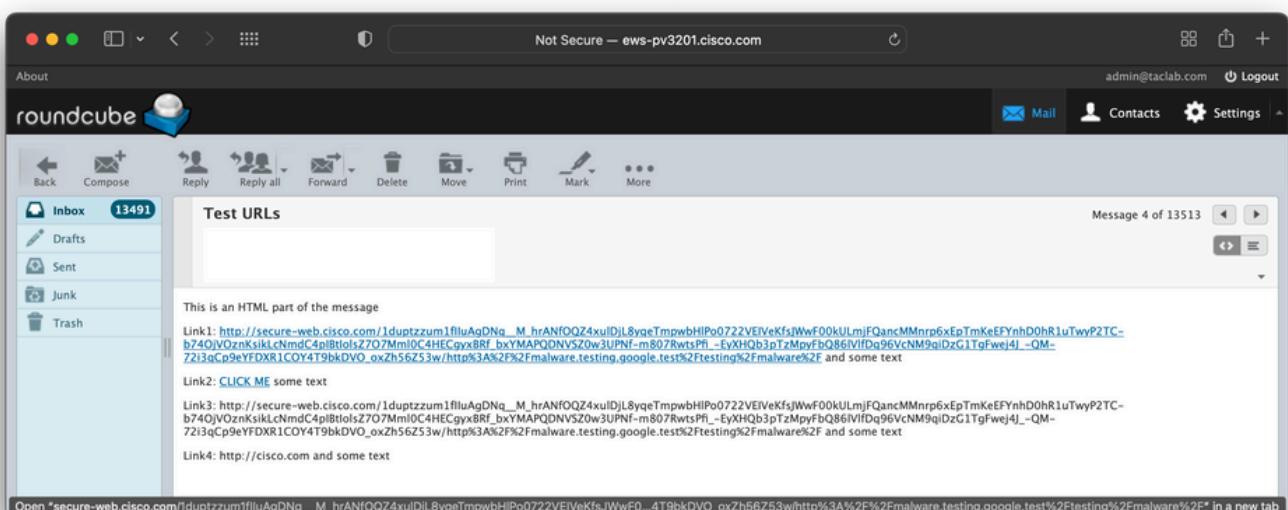
Link1: http://secure-web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANf0QZ4xu1DjL8yqeTmpwbH1Po0722VEIVeKfsJWwF0

Link2: [CLICK ME](#) some text

Link3: http://secure-web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANf0QZ4xu1DjL8yqeTmpwbH1Po0722VEIVeKfsJWwF0

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

يَتْلُى URL نَأْوَنْعَ لَسَالِسْ عَيْمَجْ هِيَجَوْتْ ٰدَاعِإِوْ href نَيِّكَمَتْ درَجَمَبْ عَمْ نَآلَا يَنْورْتَكَلْ إِلَى دِيرْبَلَا لَيِّمَعْ يَفْ ٰدَوْجَوْمَلَا ٰلَاسَرَلَا مَدَقَتْ . يَوْتَحْمَلَا حَشَرَمْ طَوْرَشْ قَبَاطَتْ عَزْ ضَرَعَيْ يَذَلَّا بِيَوَلَا دِيرَبْ لَيِّمَعْ جَارَخَا عَجَارْ، لَضَفَأْ لَكَشَبْ اَذَهْ مَهَفَلْ . هِيَجَوْتَلَا ٰدَاعِإِلَكْ ٰلَاسَرَلَا نَمْ /html/صَنَلَا



رِيَيْغَتْ نَأْ ثَيْحَ C وَيَرَانِي سَلَا يَفْ اَمَكْ هَسْفَنْ وَهَ MIMَE ٰلَاسَرَنْمَ يَدَاعَلَا عَزَجَلَا/صَنَلَا

WebSecurityAdvancedConfig چۈنلە ئەلا ئەلا دىاعىتىسىنىڭ ئىلەر رەتىۋىي ئەل.

```
--=====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/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xu1DjL8yqeTmpwbH1Po0722VEIVeKfs
Link2: <http://cisco.com> and some text

-----7781793576330041025=====

الخلتلا: صي

- يتلـا URL نـاونـع لـسـالـس ةـبـاتـك دـيـعـي يـدـاعـلـا عـزـجـلـا/صـنـلـا ىـلـع لـيـغـشـتـلـا هـيـجـوـت ةـدـاعـإ
ليـكـوـهـمـدـخـعـمـقـبـاطـتـتـ Cisco Web Secure
 - عـمـهـمـسـنـمـURL ةـبـاتـكـ عـزـجـلـا ىـلـع TEXT/HTML Redirect لـيـغـشـتـ دـيـعـي
ليـكـوـهـمـدـخـعـمـصـنـيـفـقـبـاطـتـتـرـخـأـURL ـقـلـسـلـسـيـأـىـلـإـفـاضـإـلـابـصـنـلـا عـزـجـCisco Web Secure

٥- عزجا - ةداعا - جوٰل جي

ریغ تادیده‌تل ریثأت نع فشكلا تادادع! مایق ئیفیک لوح تامولعم عزجل اذه رفووی URL حسمب ئیسوريفلار.

نیوکرک

نيلول والا نيازجلا يف مدخلت سملاء وتحملا ئي فصت لمعا ليطعت متى، ضرغلا اذهل

- نیکمٹ عمومی ضارف الی AS/AV/AMP نیوکٹ عم دیربل 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)	Enabled (no filters)	Retention Time: Virus: 1 day Other: 4 hours	(use default)		

- ئىسوري فلارىغ تادىدەتلا نع فشكىلل "يشفتلا ئيفصىت لىماع صحف" نىيوكت مەت لئاسرىف ئەدوجوملى URLs ئېباتك ئەداعىل URL ئېباتك ئەداعاً ئۇمۇجىم مادختساب قىراضىلما يىنورت كىللا دىرىپلى

Mail Policies: Outbreak Filters

Outbreak Filtering for Policy: URLTest

Enable Outbreak Filtering (Customize settings) 

Outbreak Filter Settings

Quarantine Threat Level:  3 	Maximum Quarantine Retention:
	Viral Attachments: <input type="text" value="1"/> Days 
	Other Threats: <input type="text" value="4"/> Hours 
	<input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning:  None configured	

Message Modification

Enable message modification. Required for non-viral threat detection (excluding attachments)

Message Modification Threat Level:  3 	Prepend  [SUSPICIOUS MESSAGE]  
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 	
Threat Disclaimer:	None  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 > Text Resources > Disclaimers

Cancel **Submit**

نیوانع عیمج ۃباتک ۃداعا مدت، ۃراض ۃلسراوب ۃلسرا فینصت متي امدنع URL Cisco Web Secure.

ویرانیسلا E

حشرمب یسوري فلا ریغ دیده تلا نع فشكلا یشفتلا	معن
یوتحمل ا حشرم ءارج	ال
صنلا ۃباتک ۃداع او AdvancedConfig href نیکممت متبیولا ناما	ال

و صنلا ۃباتک ۃداعا لیطبعت عم ۃلسرا ۃباتک ۃي فيك ويرانيسلا اذه حضوي Enabled و WebSecurityAdvancedConfig href.

```

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/ma
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/ma

```

```
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 'Thre...
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)
```

عيمج ةباتك ةداع| ةظحالم نكمي ،عيرسلا ققحتلا دعب .يداعل|ا عزج بـ أدبنـلـف
كلـذـ ثـدـحـيـ Cisco Web Secure. ليـكـوـ تـامـدـخـ لـىـاـ يـدـاعـلـاـ عـزـجـلـاـ/ـصـنـلـاـ لـخـادـ ةـدوـجـوـمـلـاـ URLـ نـيـوانـعـ
ةـراـضـلـاـ ةـلـاسـرـلـاـ لـخـادـ ةـدوـجـوـمـلـاـ URLـ نـيـوانـعـ ةـفـاكـلـ ةـنـكـمـمـ URLـ نـاـونـعـ ةـبـاتـكـ ةـداعـ اـنـأـلـ
عـابـولـاـ يـشـفـتـلـ.

=====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-8wSvnm0QxYNYhb4ap1Et0Xp_-0CMTnyw6WX63xZIFnj5S_n0vY18F9G0JWCSoVJpK=30Eq81B-jcbjx9BW1ZaNb1-t-uTOLj107Z3j8XCAd0wHe1t7GGF8Lft1GNFRCVLEM_wQZyo-uxh=UfkhZVETXPZAddg6-uCeoeimiRZUOAzqvgw2axm903AUpieDdfeMHYXpmzeMwu574FRGbbr7uV=tB65hfy29t2r_VyWA24b6nyaKyJ_hmRf2A4PBWOTe37cRLveONF9cI3P51GxU/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text

Link2: http://secure-web.cisco.com/1o7068d-d0bG3Sqwcifi189X-tY7S4csHT6=LsLToTUYJqWzfLfODch91yXwfJ8a0xPq1PQBSACgJ1Dt4hCZipXXmC1XI3-XdNLGBMd0bLfj1cB=hY_0W1BfLD-zC86M02dm_fOXCqKT0tDET3RD_KAeUWTWhWZvN9i81LPcwBBBi9TLjMAMnRKPMeg=En_YQvDnCzTB4qYkG8aUQ1FsecXB-V_HU1vL8IRFRP-uGINjhHp9kWCnntJBJEm0MheA1T6mBJJ=ZhBZmfymf0ddXs-xIGiYXn3juN1Tvu01Cceo3Yeaivrb0Xc01Zs3F08xvNj0nwvKN181yGKPQ9Y=cn5aSWvg/http%3A%2F%2Fcisco.com and some text

=====7781793576330041025==

ةـلـاسـرـلـاـ عـزـجـ وـهـ اـذـهـ مـهـ تـجـلـاعـمـ تـمـتـ يـذـلـاـ/ـصـنـلـاـ M~IM~E.

=====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

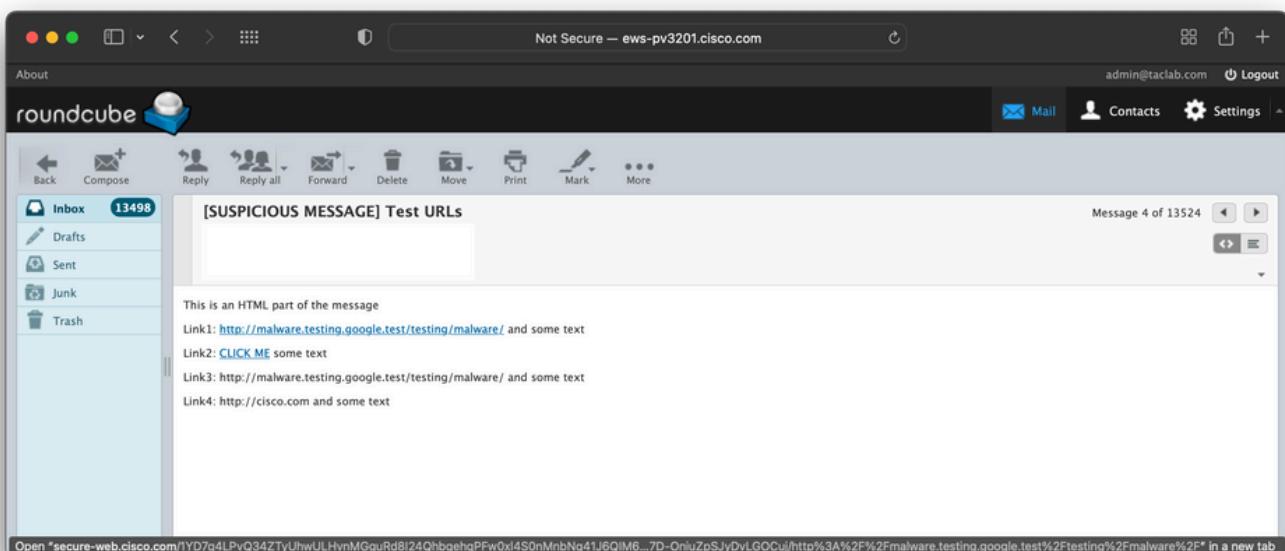
Link2: [CLICK ME<=](#)
[/a> some text](#)

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

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

=20

=====7781793576330041025====



اذا 4. طاب ترا لا قباتك قداعا مرت مل اذامل يه انه اهت ظحالم نكمي يتلا ىل والا ٽطقنلا لعلو
يضرارت فالكشب MIME نم html/charset نم Cisco Web Secure ليكو وقمدح عم قباتك قداعا مرت مل اذامل يه انه اهت ظحالم نكمي يتلا ىل والا ٽطقنلا لعلو
عم لاحلا وه امك لثامم كولس كانه ناك اذا طقف href رصانع عل href نيكمت بجييف ، بوغرم يداعل عزجللا عزجللا اصلنلا
قباتك قداع او WebSecurityAdvancedConfig href . طب ضلاب كل ذب موقعي يلاتلا ويرانيسلا اصلنلا.

:صيخلتلا

- URL ناونع ٽلس لس عيمج قباتك ديعي يداعل عزجللا اصلنلا ليغشتلا هيوجوت قداعا
- Cisco Web Secure ليكو وقمدح عم قباتك قداعا مرت
- قمس نم طقف URL ناونع قباتك قداعا مرت، TEXT/HTML عزجللا اصلنلا ليغشتلا هيوجوت قداعا
- html A-Tag href نم بيول نم آلا ليكولا قمس نم طقف URL ناونع قباتك قداعا مرت

واو ويرانيسلا

حشرمب يسوريفلارىغ ديدهتلانع فشكلا يىشفتلما	معن
ىوتحملا حشرم ئارجا	ال
نويكمت مت بىولاناما AdvancedConfig href صنلما ئېباتك ۋەداعا او	معن

راهظاً صنلما ئېباتك ۋەداعا webSecurityAdvancedConfig href نويكمت ويرانيسلا اذه حىتى
رىغ تادىدەتلارا تارىيغت ھرفوت يىذلا URL ناونع ئېباتك ۋەداعا يىف كولسلا ئېفيك
ئازجا ىلىع رىۋىي ال WebSecurityAdvancedConfig نامەف بجى، ۋەظحلللا ھەذى يىف. ئىسوريفلارا
كولسلا رىغت فيك يىرن و html/صنلما عزج طققى مىقىن انعد. ئىداعلارا MIME/صنلما

=====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://secure-web.cisco.com/1dgafaGfZ6Gmc_TKmEH8FIG_-10TxJMFkg=1-vbjf0-oZc9G-byKGdhMW_gCESYCPD10tJffkI9k069nitsXnL49WLXoXErSwx-YfvWvnBjP18=D3Vjoi501Aqhm9yJJaK_1g6f38p4NiMa18jdSIMp_1caEdG0LdzeZHHg_B7_Xinu1BHeKVsVFAw=-Ikga7jEusyfzIDtmJ45YgbI3Dg-WFWhSMgSHpcqkRP6aAjw-aKMEoC09u1DowOhAKrY5w-nVfc=EJ-tmveV94LDIAiR1PYosumpsj5e_4Jvg4B_PD0fCvRynghkMBGBHLETVirz-SQjRFRHZKSpzNh=bn1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F

[and some text](#)

[Link2: CLICK ME](#) some text

Link3: http://secure-web.cisco.com/1dgafaGfZ6Gmc_TKmEH8FIG_-10TxJMF=kg1-vbjf0-oZc9G-byKGdhMW_gCESYCPD10tJffkI9k069nitsXnL49WLXoXErSwx-YfvWvnBjP=18D3Vjoi501Aqhm9yJJaK_1g6f38p4NiMa18jdSIMp_1caEdG0LdzeZHHg_B7_Xinu1BHeKVsVF=

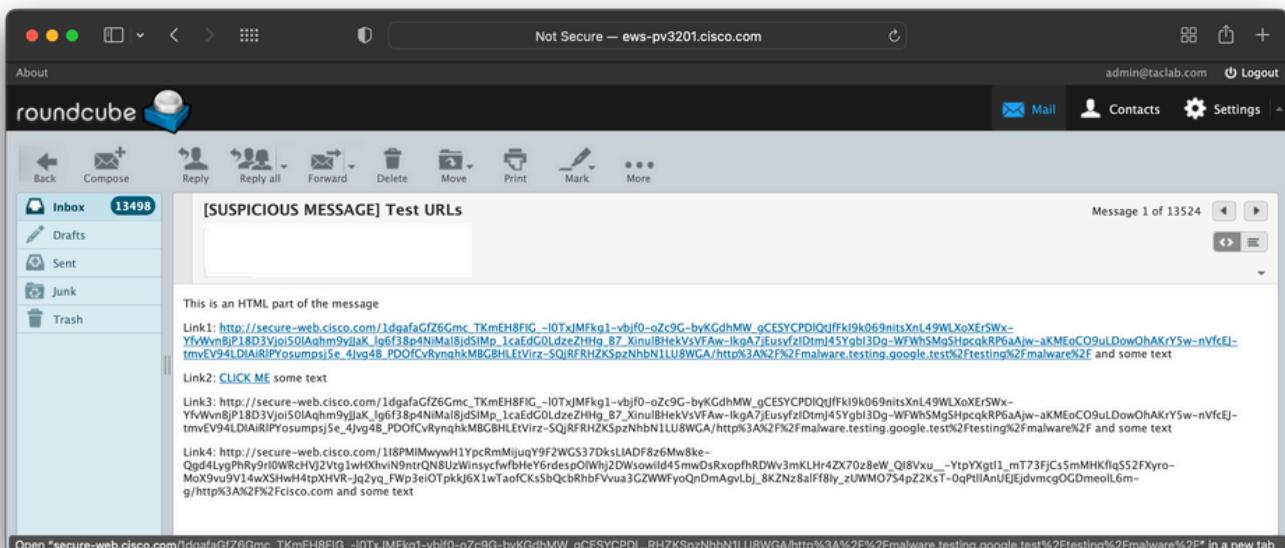
Aw-IkgA7jEusyfzIDtmJ45YgbI3Dg-WFWhSMgSHpcqkRP6aAjw-aKMEoCO9uLDowOhAKrY5w-nV=fcEJ-tmVEV94LDIAiR1PYosumpsj5e_4Jvg4B_PDOfCvRynqhkMBGBHLEtVirz-SQjRFRHZKSpz=NhbN1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text

Link4:

=20

=====7781793576330041025====

لك نأ ديجول قرفلا عم D ويرانيسلا يف تناك يتل ادج ةباثم تاجرخملانأ ظحالمنكمي
 لسالس عيمج ليدعتمتي . ئثيبخلا كلت طقف سيلو، اهتباتك ةداعا تمت URL نيوانع
 انه ئراضلا ريغ لسالسلا عم HTML عزج يف قباطتت يتلا URL ناونع



صيخلتل:

- URL ناونع لسالس عيمج ئباتك ديعي يداعلا عزجلا/صنلا ىلع ليغشتلا هيجوت ةداعا لـ Cisco Web Secure
- عزج م html A-Tag href ئماتك ديعي TEXT/HTML URL نم لـ Cisco Web لـ نمآل لـ Cisco Web

ياز ويرانيسلا

حشرمب يسوري فلارىغ ديده تلانع فشكلا يشفتلا	معن
ىوتحملاب حشرم ئارجا	غانافي د
نيكمت متن امأ AdvancedConfig href صىنلا ئباتك ئداع او	معن

نويوكتلانم ريخالا ويرانيسلا اذه ققحتي.

- نيكمت عمومي ضارتفالا AS/AV/AMP نويوكت عم ديربلا جىن

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)		

- ئداعا ۋەمجم مادختساب ئىسوري فلارىغ تادىدەتلانع فشكلىل صحفلانىيوكت مەتى ديربلا لىاسرىف ۋەدوجوملاب URL نىوانع عىمەج ئباتك ئداعا ئەل URL ناونع ئباتك (قىباصلاتا ھەويرانىسلا لىثم) ئراضلارىنورتىلەلە
- ىوتحم ئيفىصىت لىماع نىكمت مەت: دراولابى ىوتحملاب ئيفىصىت لىماع URL_SCORE

Filters										
Add Filter...										
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,""); };								

كلت، ئراضلاب URL نىوانع ۋەقباطملىك ناونع ۋەممس ۋەللاجى ىوتحملاب ئيفىصىت لىماع مادختسى ىوتحملاب ئيفىصىت لىماع مسالىجىست مەتى، ئارجاك. -10.00 و -6.00 نىب ام ئىلا رىشتىلەلە طابتىرالا url-reputation-defang ئارجا ئاغلىدا خەتكەنلە.

عم ينورتىلەلە ديربلا ئېباوب ئەتساوب اهمىيقتىو ئەلسىرلا ئەخسۇن سفن لاسرا مەتى جئاتىنلە:

```

Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
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 r
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 rewritten to MID 139519 by url-reputation-defang-action filter
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 Threat Level=5 Category=Phish Type=Phish
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 'Thre  
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
```

ثيچ، يوتحملـا ئيفـصـتـلـمـاوـعـ طـسـاوـبـ الـأـقـلـاسـرـلـاـ يـنـورـتـكـلـإـلـاـ دـيـرـبـلـاـ تـاقـفـدـتـ حـرـشـيـ
URL-REPUTATION-DEFANG-
عـازـجـأـ نـمـ لـكـ يـفـ ئـراـضـلـاـ URLـ نـيـوانـعـ عـيمـجـ لـيـطـعـتـ إـلـاـ ئـارـجـ إـلـاـ اـذـهـ يـدـؤـيـ
ACTION.ـ
صـنـلـاـ ئـبـاتـكـ ئـدـاعـاـوـ صـنـلـاـ htmlـ MIMEـ WebSecurityAdvancedConfig hrefـ نـأـلـ
لـكـ حـسـمـ مـتـيـ اـمـدـنـعـ HTMLـ صـنـلـاـ قـبـاطـتـ يـتـلـاـ URLـ نـاـونـعـ لـسـالـسـ لـكـ نـيـكـمـتـ مـتـيـ
لـكـ عـضـوـوـ ئـروـظـحـمـلـاـ تـامـلـكـلـاـ نـيـبـ URLsـ نـاـونـعـ صـنـلـاـ عـازـجـأـ ئـبـاتـكـ ئـدـاعـاـوـ زـيـمـتـ مـتـيـ
زـيـمـتـ ئـمـالـعـ يـفـ عـضـوـيـ الـ رـاضـلـاـ عـمـ ثـدـحـيـ عـيـشـلـاـ سـفـنـ.ـ عـبـرـمـ سـاـوـقـأـ نـيـبـ طـاقـنـلـاـ
فـاشـتـكـابـ OFـ مـوـقـيـ.ـ ئـلـاـسـرـلـاـ يـلـاتـلـاـ "ـيـشـفـتـلـاـ ئـيـفـصـتـلـمـاعـ"ـ جـلـاعـيـ HTMLـ رـصـانـعـ
هـنـإـفـ،ـ كـلـذـلـ ـةـجـيـتنـوـ.ـ (ـدـيـدـهـلـاـ ئـوـتـسـمـ)ـ ئـرـاضـاـهـنـأـبـ ئـلـاـسـرـلـاـ فـرـعـيـوـ ئـرـاضـلـاـ URLـ نـيـوانـعـ
ـلـاـسـرـلـاـ لـخـادـاهـيلـعـ روـثـعـلـاـ مـتـ يـتـلـاـ ئـرـاغـوـ ئـرـاضـلـاـ رـيـغـوـ ئـرـاضـلـاـ URLـ نـيـوانـعـ عـيمـجـ ئـبـاتـكـ دـيـعـيـ
ـنـإـفـ،ـ هـذـهـ URLsـ نـيـوانـعـ لـيـدـعـتـبـ لـعـفـلـابـ مـاـقـ دـقـ ئـوـتـحـمـلـاـ ئـيـفـصـتـلـمـاعـ ئـارـجـاـ نـأـلـ اـرـظـانـ
ـدـمـعـتـمـ لـكـشـبـاهـنـيـوـكـتـمـتـ ئـيـجـحـ طـقـفـ ئـرـاغـ ئـرـاضـلـاـ رـيـغـ URLـ نـيـوانـعـ يـقـابـ ئـبـاتـكـ ئـدـاعـابـ مـوـقـيـ
ـنـمـ عـزـجـكـ يـنـورـتـكـلـإـلـاـ دـيـرـبـلـاـ لـيـمـعـ يـفـ ئـضـوـرـعـمـلـاـ ئـلـاـسـرـلـاـ هـيـجـوـتـ عـاـغـلـاـ مـتـ.ـ كـلـذـبـ مـاـيـقـلـلـ
ـيـجـوـتـ ئـدـاعـاـ تـمـتـ يـذـلـاـ رـاضـلـاـ رـيـغـ URLـ نـاـونـعـ نـمـ عـزـجـوـ ئـرـاضـلـاـ URLـ نـيـوانـعـ ٥٥.

```
=====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

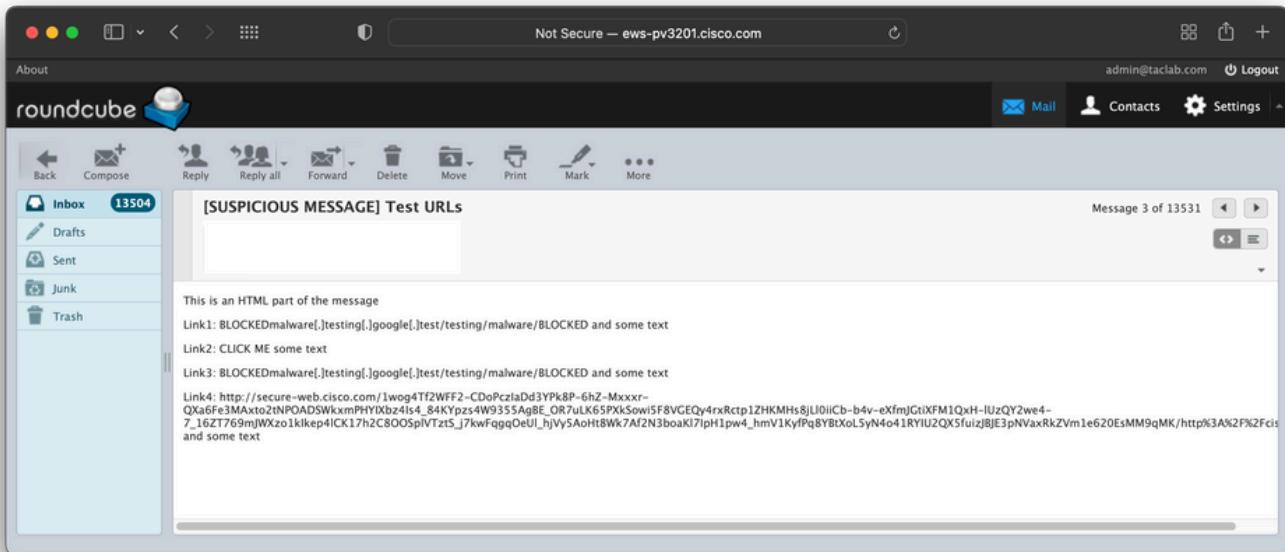
Link3: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLO=CKED and some text

Link4: http://secure-web.cisco.com/1wog4Tf2WFF2-CDoPczIaDd3YPk8P-6h=Z-Mxxxr-QXa6Fe3MAxto2tNPOADSwkxmPHYIXbz4Is4_84KYpzs4W9355AgBE_OR7uLK65PXkSo=wi5F8VGEQy4rxRctp1ZHKMhs8jL10iiCb-b4v-eXfmJGtiXFM1QxH-1UzQY2we4-7_16ZT769mJ=

WXzo1kIkep41CK17h2C800Sp1VTztS_j7kwFqqq0eU1_hjVv5AoHt8Wk7Af2N3boaK17IpH1pw4=
_hmV1KyfPq8YBtXoL5yN4o41RYIU2QX5fuizJBJE3pNVaxRkZVm1e620EsMM9qMK/http%3A%2F=%
%2Fcisco.com and some text

=20

=====7781793576330041025=====



عيمج ييجوت ةداعا مرت ماسنلا عاجلا عزجل/صنلا ىلع متي كوكيل Cisco Web Secure نيوانع URL راضللا ريغ.

=====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/1wog4Tf2WFF2-CD0PczIaDd3YPk8P-6hZ-Mxxr-QXa6Fe3MAxto2tNPOADSWkxmPHYIXbz4Is4_84KYpzs4W9355AgBE_0R7uLK65PXkSowi5=F8VGEQy4rxRctp1ZHKMHs8jL10iCb-b4v-eXfmJGtiXFM1QxH-1UzQY2we4-7_16ZT769mJWXz=o1kIkep41CK17h2C800Sp1VTztS_j7kwFqqq0eU1_hjVv5AoHt8Wk7Af2N3boaK17IpH1pw4=_hmV1KyfPq8YBtXoL5yN4o41RYIU2QX5fuizJBJE3pNVaxRkZVm1e620EsMM9qMK/http%3A%2F=%cisco.com and some text

=====7781793576330041025==

صيخلتل:

- ةروظحم لتك ىلإ URL ةباتك ديعي "يداعلا عزجل/صنلا" ىلع CF ليعشت ةداع

- امدنع HTML A زييمنت ةممالع نم URL ئزج ىلع TEXT/HTML ئزج ىلع ئباثك ديعي CF ئزج ىلع ئباثك ديرجت متي A زييمنت ةممالع
- عم قباتتت يتلارا URL لسالس ئفاك ئباثك TEXT/HTML ئزج ىلع CF ئزج ىلع ئباثك ديرجت متي
- URL ناونع لسالس عيمج ئباثك ديعي يداعلا عزجلارا/صنلا ىلع لىغشتلا هيچوت ئداعا (راض ريخ) Cisco Web Secure
- ئزج عم html A-Tag href ئممس نم URL ئباثك ديعي TEXT/HTML ئزج ىلع لىغشتلا ئداعا ليكولا ئمدخ عم قباتتت يتلارا URL لسالس عيمج ورصنعلاب صاخلا صنلا (راض ريخ) بيولا ىلع Cisco ل ناما

اهحالص او ئاطخألا فاشكتسا

طبربلا ناونع ئباثك ئداعاب ئلأسملارا يف قيقحتلل ئجاج كانه نوكت امدنع طاقنلا كيلت عبتا.

- ئباجإلا او رمألا OUTBREAKCONFIG ئيچشتب مق. mail_log يف URL ئيچشت نيكمنت برق. Do you wish to enable logging of URL's? [N]>
- ماظن ئاضعا نم وضع لك تتح ئدوجوملا تادادعإلا WEBSECURITYADVANCECONFIG نم ققحت href وصنلا ئباثك ئداعا رايخ نيءييغت نم دكأت وينورتكللا ديربلا ئباوبل ئعومجملا زاهجلا ئوتسم ىلع صاخ رمألا اذه نأ ركذت. زاهج لك ىلع رايخلارا سفن هنأ نم وكلذل اقفو ئعومجملا ماظن وأ ئعومجملا تادادعإ ىلع انه اهؤارجا مت يتلارا تارييغتلارا رثؤت الو.
- ئيفصت لماع نيكمنت نم دكأتو، ئوتحملارا ئيفصت لماع ئطشنأو طورش نم ققحت ئيفصت لماع دوجو مدع نم ققحت. حيحصلارا دراولارا ديربلا جهن ىلع هقيبطة وئوتحملارا يطختلا هنكمي يذلا يئاهنلا ئراجإلا مادختساب لباق نم ٥ متجلاعم تمت رخآ ئوتحم ئرجألا ئيفصتلا لماعو ئجلاعمل.
- ئلاسرلا عاجرتسا ركذت ركذت. ئيئاهنلا ئلاسرلاو ردىمىل ئيلوألا ئخسنلا نم ققحت امدنع اهيلع دامتعمالا نكمي اى MSG لثم ئصالا تاقييسنتلا نأ، EML، قيسنتب ينورتكللا ديربلا ئالمع ضعب كل حمسى. لئاسرلا يف قيقحتلاب رمألا قلعتي ينورتكللا ديرب ليمع عم ئلاسرلا ئخسن دادرتسا ئلواحم، ردىمىل ئلاسرلا ضرع ئلاسرلا ردىمىل ضرع كل حمسى، لاثملارا ليبس ىلع. فلتخم طقف سوؤرلا ضرع Windows رادصا حمسى امنىب.

صخلم

امدنع لضفأ لكشب ئرفوتملارا نيكوتلارا تارييغ مەف يف ئدعاسملارا وە ئلاقملارا هذه نم ضرغلا اهؤانب متي ئيىدحلا لئاسرلا نأ ركذتن نأ مەمملا نم و. URL ناونع ئباثك ئداعاب رمألا قلعتي ضرع نكمي هنأ ينعي اذهو MIME. رايعدم مادختساب ينورتكللا ديربلا جمارب بلغا ئطساوب وأ ينورتكللا ديربلا ليمع تايناكما ىلع ادامتغا فلتخم لكشب ئلاسرلا ئخسن سفن ئالمع مظعم مدختسى، يضارتفا لكشب HTML عضولباقم صنلا) ئنكمملارا عاضوألا و HTML ئباثك ئداعاب رمألا قلعتي امدنع. لئاسرلا ضرع HTML ئيىدحلا ينورتكللا ديربلا URL نيوانع ئباثك ئداعاب موقت ئيضارتفالا ينورتكللا ديربلا ئباقب نأ ئاعارم ئاجرلا، بجي و ئيفاك نوكت اى يتلارا تالاحلارا نم رېيثك يف a-tag. رصانعل href ئممس لخاد طقف ئدوجوملا رمألا مادختساب صنلا ئباثك ئداعاب href نم لك نيكمنت اهراپتىع ماظن رباع قسانتلىل، زاهجلا ئوتسم ىلع رمأ اذه نأ ركذت webSecurityAdvancedConfig.

عومجملا ماظن ئاضعا نم وضع لك ىلع لصفنم لكشب رئيغتلارا قيي بطت بجي، ئعومجملا.

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).