測試爆發過濾器URL重寫

目錄

簡介

本文檔介紹如何測試URL重寫的爆發過濾器(OF)消息修改選項。

背景資訊

如果郵件威脅級別超過郵件修改閾值，則爆發過濾器功能會重寫郵件中的所有URL，如果使用者按一下其中任何URL，則將其重定向到思科網路安全代理啟動顯示頁面。 AsyncOS會重寫郵件內的所有URL（指向繞過域的URL除外）。

以下選項可用於URL重寫：

- 僅對未簽名的郵件啟用。此選項允許AsyncOS重寫滿足或超過郵件修改閾值但未簽名的未簽名郵件中的URL。Cisco建議將此設定用於URL重寫。 **附註**：如果您的網路上的伺服器或裝置負責驗證DomainKeys/DKIM簽名，則郵件安全裝置可能會重寫已簽署DomainKeys/DKIM的郵件中的URL，並使郵件簽名無效。如果郵件使用S/MIME加密，或者包含S/MIME簽名，則裝置會考慮已簽名的郵件。
- 如果您的網路上的伺服器或裝置負責驗證DomainKeys/DKIM簽名，則郵件安全裝置可能會重寫已簽署DomainKeys/DKIM的郵件中的URL，並使郵件簽名無效。如果郵件使用S/MIME加密，或者包含S/MIME簽名，則裝置會考慮已簽名的郵件。
- 為所有郵件啟用。此選項允許AsyncOS重寫所有達到或超過郵件修改閾值的郵件中的URL，包括已簽名的郵件。如果AsyncOS修改已簽名的消息，則簽名無效。
- 禁用。此選項禁用爆發過濾器的URL重寫。

您可以修改策略以排除修改中特定域的URL。要繞過域，請在Bypass Domain Scanning欄位中輸入IPv4地址、IPv6地址、CIDR範圍、主機名、部分主機名或域。使用逗號分隔多個條目。

旁路域掃描功能與URL過濾使用的全域性允許清單類似，但相互獨立。有關該白名單的詳細資訊，請參閱《ESA使用手冊》中的「為URL過濾建立白名單」。

測試爆發過濾器URL重寫

在ESA上測試有兩種選擇。

第一部分測試

在電子郵件正文中包含惡意URL。 可以使用的安全測試URL:

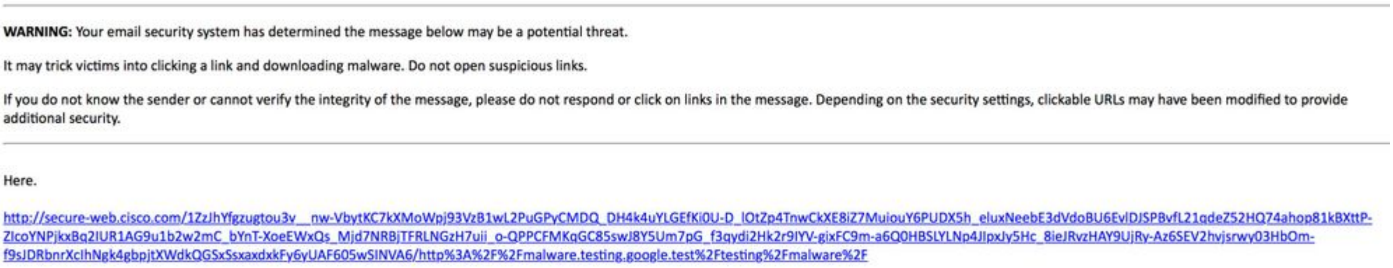
http://malware.testing.google.test/testing/malware/

傳送時，郵件日誌示例應包含類似以下內容：

```
Tue Jul  3 09:31:38 2018 Info: MID 185843 Outbreak Filters: verdict positive
Tue Jul  3 09:31:38 2018 Info: MID 185843 Threat Level=5 Category=Malware Type=Malware
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten URL
u'http://malware.testing.google.test/testing/malware/'
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten URL
u'http://malware.testing.google.test/testing/malware/'
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten URL
u'http://malware.testing.google.test/testing/malware/'
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten to MID 185844 by url-threat-protection
filter 'Threat Protection'
Tue Jul  3 09:31:38 2018 Info: Message finished MID 185843 done
Tue Jul  3 09:31:38 2018 Info: MID 185844 Virus Threat Level=5
Tue Jul  3 09:31:38 2018 Warning: MID 185844 Failed to add disclaimer as header. Disclaimer has
been added as attachment.
Tue Jul  3 09:31:38 2018 Info: MID 185844 rewritten to MID 185845 by add-heading filter 'Heading
Stamping'
Tue Jul  3 09:31:38 2018 Info: Message finished MID 185844 done
Tue Jul  3 09:31:38 2018 Info: Message finished MID 185846 done
Tue Jul  3 09:31:38 2018 Info: MID 185845 enqueued for transfer to centralized quarantine
"Outbreak" (Outbreak rule Malware: Malware)
Tue Jul  3 09:31:38 2018 Info: MID 185845 queued for delivery
```

請注意，郵件日誌向我們顯示「重寫的URL」，指示OF已通過思科網路安全代理重寫此URL。 此外，請注意，郵件可能位於病毒爆發隔離區中，如以下示例所示。

最終結果將顯示以下已送達的電子郵件正文：



WARNING: Your email security system has determined the message below may be a potential threat.

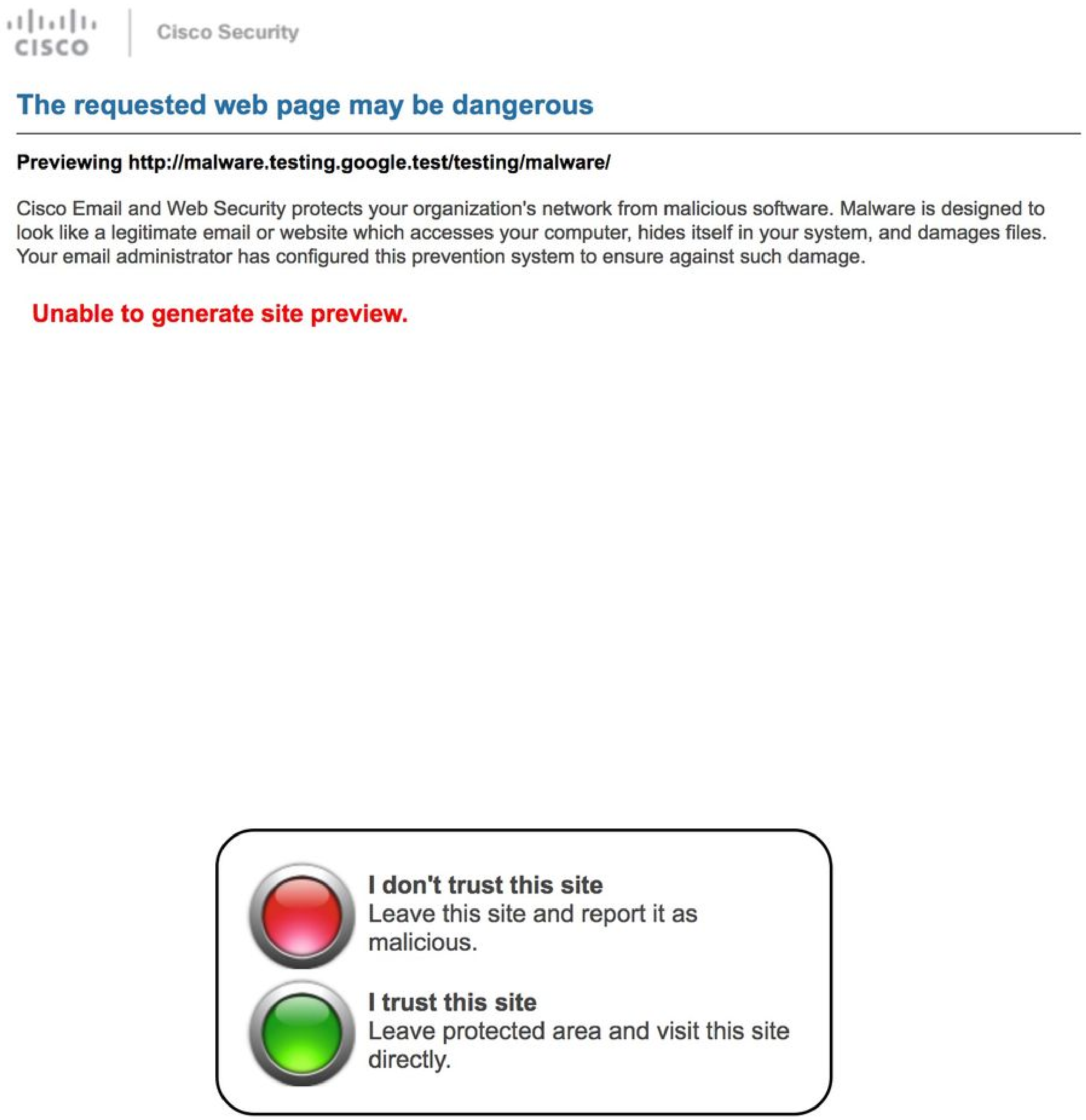
It may trick victims into clicking a link and downloading malware. Do not open suspicious links.

If you do not know the sender or cannot verify the integrity of the message, please do not respond or click on links in the message. Depending on the security settings, clickable URLs may have been modified to provide additional security.

Here.

http://secure-web.cisco.com/1ZzJhYfgzugtou3v__nw-VbytKC7kXMoWpj93VzB1wL2PuGPyCMDQ_DH4k4uYLGEfKi0U-D_lOtZp4TnwCkXE8iZ7MuiouY6PUDX5h_eluxNeebE3dVdoBU6EvIDJSPBvfL21qdeZ52HQ74ahop81kBXttP-ZlcoYNPjkxBq2IUR1AG9u1b2w2mC_bYnT-XoeEWxQs_Mjd7NRBjTFRLNGzH7uii_o-QPPCFMKqGC85swJ8Y5Um7pG_f3qydi2Hk2r9lYV-gixFC9m-a6Q0HBSLYLNp4JlpxJy5Hc_8ieJRvzHAY9UjRy-Az6SEV2hvjsrwy03HbOm-f9sJDRbnrXclhNgk4gbpjtXWdkQGSxSsxaxdxkFy6yUAF605wSINVA6/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F

終端使用者現在收到電子郵件時，按一下重寫的URL，系統會將它們重定向到思科網路安全代理並檢視：



The requested web page may be dangerous

Previewing http://malware.testing.google.test/testing/malware/

Cisco Email and Web Security protects your organization's network from malicious software. Malware is designed to look like a legitimate email or website which accesses your computer, hides itself in your system, and damages files. Your email administrator has configured this prevention system to ensure against such damage.

Unable to generate site preview.

I don't trust this site
Leave this site and report it as malicious.

I trust this site
Leave protected area and visit this site directly.

附註：將根據原始URL或網站的HTML/編碼顯示「無法生成網站預覽」。 具有CSS、HTML窗格或複雜渲染的網站將無法生成網站預覽。

第二部分測試

第二個選項是在郵件正文或附件中包含資料，以便觸發OF觸發器。

若要成功，有兩個選項：

1. 建立一個大小為25000和30000位元組且名為「hello.voftest」的檔案（簡單文本檔案將執行），並將該檔案附加到測試電子郵件。這將觸發病毒附件規則。

2. 將以下GTUBE(「Generic Test for Unsolicited Bulk Email」)72位元組測試字串文本放入電子郵件正文：

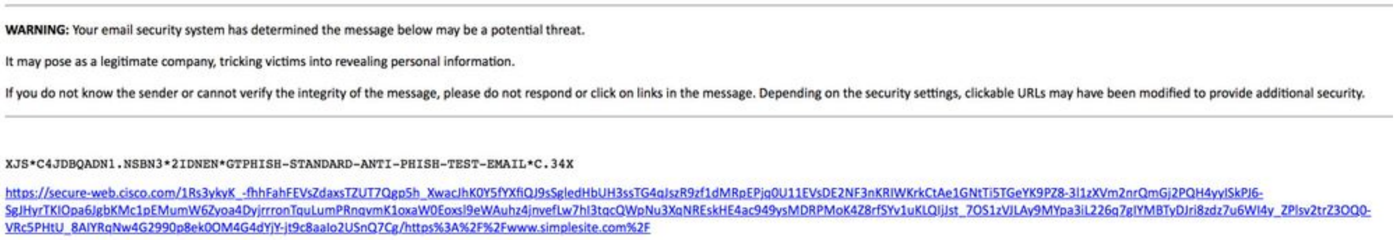
```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTPHISH-STANDARD-ANTI-PHISH-TEST-EMAIL*C.34X
```

這將觸發OF和網路釣魚規則。 郵件日誌示例應包含類似以下內容：

```
Tue Jul  3 09:44:12 2018 Info: MID 185880 Outbreak Filters: verdict positive
Tue Jul  3 09:44:12 2018 Info: MID 185880 Threat Level=5 Category=Phish Type=Phish
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten URL u'https://www.simplesite.com/'
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten URL u'https://www.simplesite.com/'
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten URL u'https://www.simplesite.com/'
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten to MID 185881 by url-threat-protection
filter 'Threat Protection'
Tue Jul  3 09:44:12 2018 Info: Message finished MID 185880 done
Tue Jul  3 09:44:12 2018 Info: MID 185881 Virus Threat Level=5
Tue Jul  3 09:44:12 2018 Warning: MID 185881 Failed to add disclaimer as header. Disclaimer has
been added as attachment.
Tue Jul  3 09:44:12 2018 Info: MID 185881 rewritten to MID 185882 by add-heading filter 'Heading
Stamping'
Tue Jul  3 09:44:12 2018 Info: Message finished MID 185881 done
Tue Jul  3 09:44:13 2018 Info: MID 185882 enqueued for transfer to centralized quarantine
"Outbreak" (Outbreak rule Phish: Phish)
Tue Jul  3 09:44:13 2018 Info: MID 185882 queued for delivery
```

請注意，郵件日誌向我們顯示「重寫的URL」，指示OF已通過思科網路安全代理重寫此URL。 此外，請注意，郵件可能位於病毒爆發隔離區中，如以下示例所示。

最終結果將顯示以下已送達的電子郵件正文：



WARNING: Your email security system has determined the message below may be a potential threat.

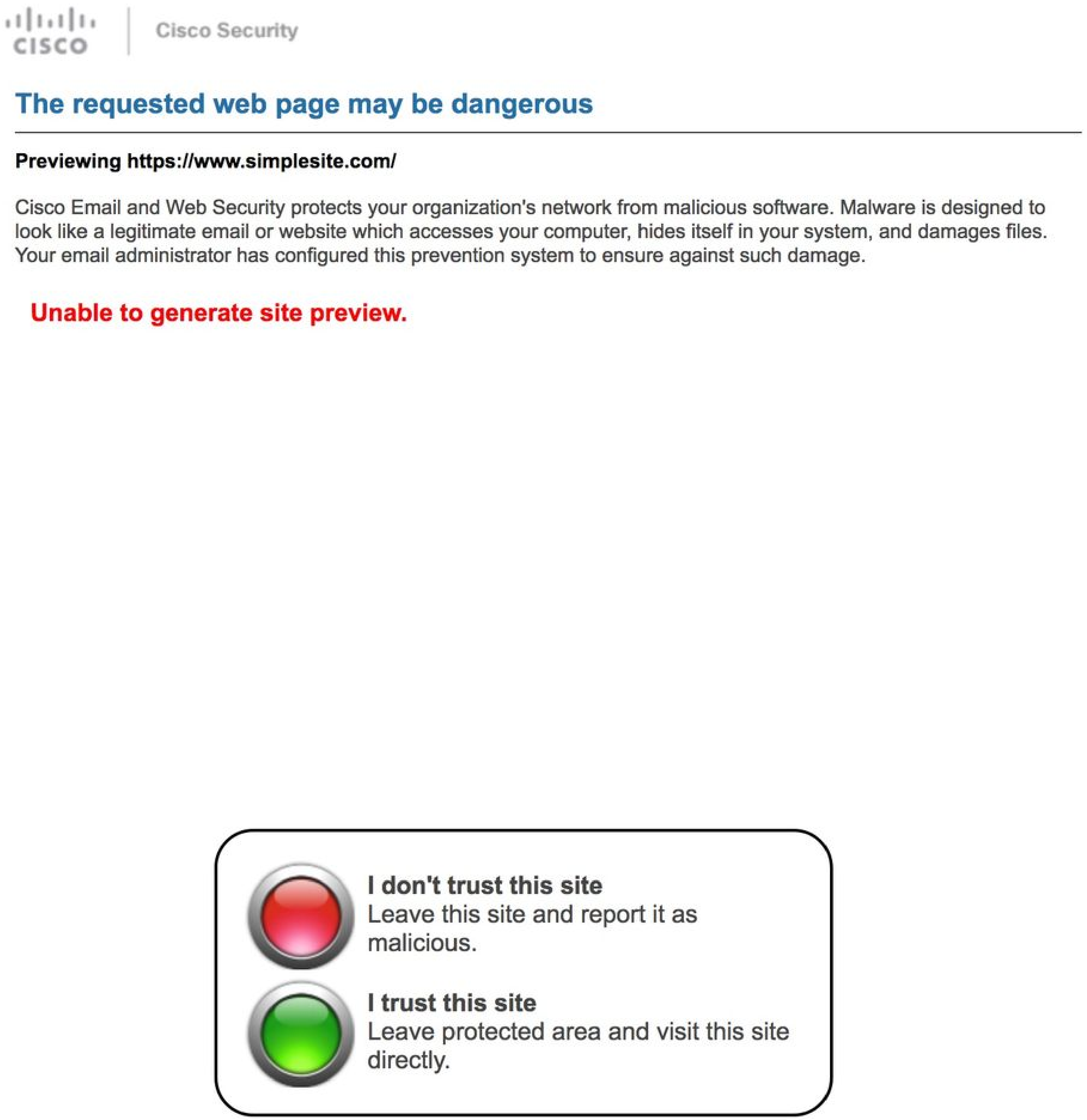
It may pose as a legitimate company, tricking victims into revealing personal information.

If you do not know the sender or cannot verify the integrity of the message, please do not respond or click on links in the message. Depending on the security settings, clickable URLs may have been modified to provide additional security.

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTPHISH-STANDARD-ANTI-PHISH-TEST-EMAIL*C.34X
```

https://secure-web.cisco.com/1Rs3ykyK_-fhhFahFEVsZdaxsTZUT7Qgp5h_XwacJhK0Y5fYXfiQJ9sSgledHbUH3ssTG4qJszR9zf1dMRpEPjq0U11EVsDE2NF3nKRIWKrkCtAe1GNtTi5TGeYK9PZ8-3l1zXVm2nrQmGj2PQH4yylSkPJ6-
SgJHyrTKIOpa6JgbKMc1pEMumW6Zyoa4DyjrrronTquLumPRnqvmK1oxaW0Eoxsl9eWAuhz4jnveflw7hl3tqcQWpNu3XqNREskHE4ac949ysMDRPMoK4Z8rfSYv1uKLQIjJst_7OS1zVJLAy9MYpa3iL226q7gIYMBTyDJri8zdz7u6WI4y_ZPlsv2trZ3OQ0-
VRc5PHtU_8AIYRqNw4G2990p8ek0OM4G4dYjY-jt9c8aalo2USnQ7Cg/https%3A%2F%2Fwww.simplesite.com%2F

終端使用者現在收到電子郵件時，按一下重寫的URL，系統會將它們重定向到思科網路安全代理並檢視：



The requested web page may be dangerous

Previewing https://www.simplesite.com/

Cisco Email and Web Security protects your organization's network from malicious software. Malware is designed to look like a legitimate email or website which accesses your computer, hides itself in your system, and damages files. Your email administrator has configured this prevention system to ensure against such damage.

Unable to generate site preview.

🟥 **I don't trust this site**
Leave this site and report it as malicious.

🟩 **I trust this site**
Leave protected area and visit this site directly.

附註：將根據原始URL或網站的HTML/編碼顯示「無法生成網站預覽」。 具有CSS、HTML窗格或複雜渲染的網站將無法生成網站預覽。

相關資訊

- 思科電子郵件安全裝置最終使用手冊
- 技術支援與文件 - Cisco Systems