

在安全網路裝置中配置自定義URL類別

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[自訂URL類別](#)

[即時源URL類別](#)

[建立自訂URL類別的步驟](#)

[定義使用規則運算式](#)

[限制和設計問題](#)

[在策略中使用自定義URL類別](#)

[為訪問策略配置URL過濾器的步驟](#)

[為解密策略配置URL過濾器的步驟](#)

[為資料安全策略組配置URL過濾器的步驟](#)

[設定使用自訂URL類別控制上傳要求的步驟](#)

[在外部DLP策略中配置控制上傳請求的步驟](#)

[略過和傳遞URL](#)

[設定Web要求的Web代理略過](#)

[報告](#)

[在存取記錄中檢視自訂URL類別](#)

[疑難排解](#)

[類別不匹配](#)

[參考](#)

簡介

本文檔介紹安全Web裝置(SWA)中的自定義統一資源定位器(URL)類別結構。

必要條件

需求

思科建議您瞭解以下主題：

- 代理程式如何運作。
- 安全網路裝置(SWA)管理。

思科建議您：

- 已安裝物理或虛擬安全網路裝置(SWA)。

- 許可證已啟用或已安裝。
- 安裝精靈已完成。
- 對SWA的管理訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。


本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

自訂URL類別

URL過濾引擎允許您過濾訪問、解密和資料安全策略中的事務。為策略組配置URL類別時，可以配置自定義URL類別 (如果有) 和預定義URL類別的操作。

您可以建立描述特定主機名和Internet協定(IP)地址的自定義和外部即時源URL類別。此外，您還可以編輯和刪除URL類別。

當將這些自定義URL類別包括在相同的訪問、解密或思科資料安全策略組中並為每個類別分配不同的操作時，更高包含的自定義URL類別的操作優先。

 **注意：**如果域名系統(DNS)將多個IP解析為網站，並且其中一個IP是自定義阻止清單，則網路安全裝置會阻止所有IP的網站，無論這些IP是否未列在自定義阻止清單中。

即時源URL類別

外部即時源類別用於提取特定站點的URL清單，例如從Microsoft獲取Office 365 URL。

如果在建立和編輯自定義和外部URL類別時為「類別型別」選擇「外部即時源類別」，則必須選擇源格式 (思科源格式或Office 365源格式)，然後提供到相應原始檔伺服器的URL。

以下是每個摘要檔案的預期格式：

- Cisco Feed Format -必須是逗號分隔值(.csv)檔案；即，副檔名為.csv的文本檔案。 .csv檔案中的每個條目都必須位於單獨的行上，格式設定為地址/逗號/地址型別 (例如：www.cisco.com , site或ad2.*\com , regex)。有效地址型別為站點和正規表示式。

以下摘自思科摘要格式.csv檔案：

```
www.cisco.com,site
\.xyz,regex
ad2.*\com,regex
www.cisco.local,site
1:1:1:11:1:1::200,site
```

- Office 365源格式 -這是一個XML檔案，位於Microsoft Office 365伺服器或您儲存檔案的本地伺服器上。它由Office 365服務提供，無法修改。

檔案中的網路位址以XML標籤括住，此結構為：products > product > address list > address。在當前實現中，「地址清單型別」可以是IPv6、IPv4或URL [可以包括域和正規表示式(regex)模式]。

以下是Office 365摘要檔案的片段：

```
<products updated="4/15/2016">
<product name="o365">
<addresslist type="IPv6">
<address>fc00:1040:401::d:80</address>
<address>fc00:1040:401::a</address>
<address>fc00:1040:401::9</address>
</addresslist>
<addresslist type="IPv4">
<address>10.71.145.72</address>
<address>10.71.148.74</address>
<address>10.71.145.114</address>
</addresslist>
<addresslist type="URL">
<address>*.cisco.com</address>
<address>*.example.local</address>
</addresslist>
</product>
<product name="LYO">
<addresslist type="URL">
<address>*.subdomain.cisco.com</address>
<address>*.example.local</address>
</addresslist>
</product>
</products>
```

 注意：請勿將http://或https://包含為檔案中的所有站點條目的一部分，否則會發生錯誤。換句話說，www.cisco.com被正確地分析，而<http://www.cisco.com>產生錯誤

建立自訂URL類別的步驟

步驟 1. 選擇網路安全管理器>自定義和外部URL類別。

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention


Web Traffic Tap Policies

SOCKS Policies

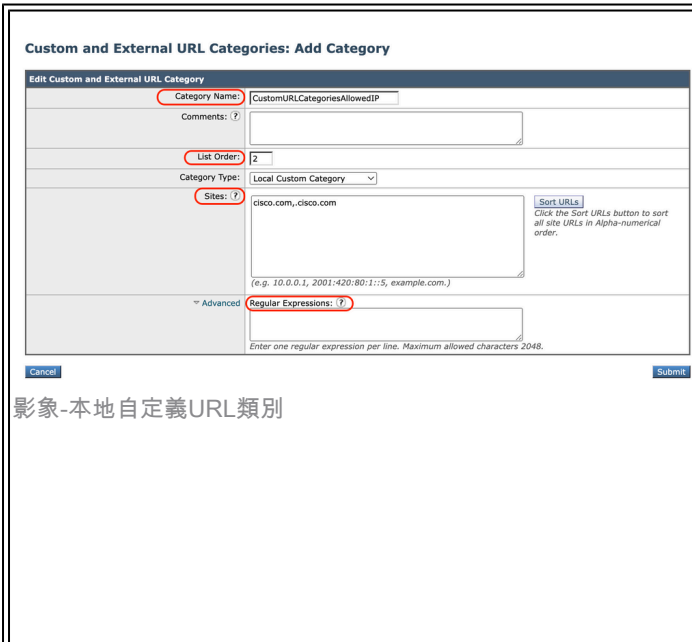
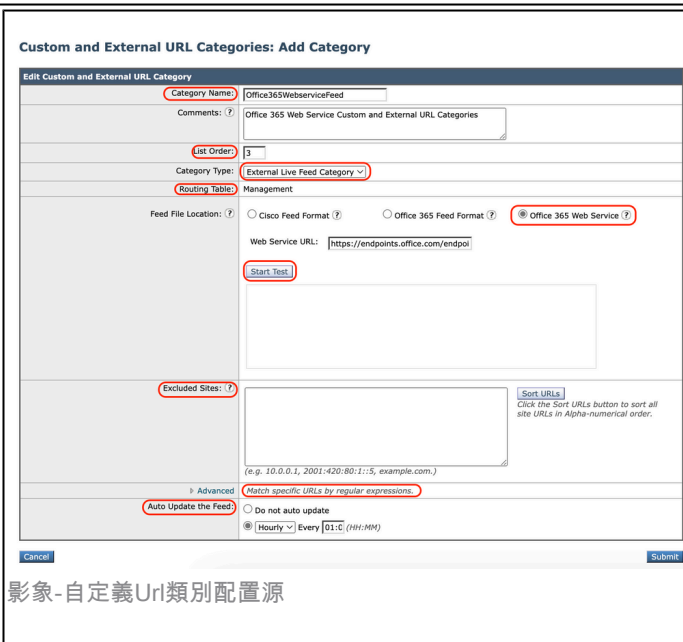
Custom Policy Elements

Custom and External URL Categories

URL過濾器引擎根據自定義URL類別按指定順序評估客戶端請求。

 注意：當URL過濾器引擎將URL類別與客戶端請求中的URL匹配時，它會首先根據策略組中包含的自定義URL類別評估URL。如果請求中的URL與包含的自定義類別不匹配，則URL過濾器引擎會將其與預定義的URL類別進行比較。如果URL不符合任何內含的自訂或預先定義的URL類別，則請求會取消分類。


- Category Type：選擇Local Custom Category或External Live Feed Category。
- 路由表：選擇管理或資料。此選項僅在啟用「拆分路由」時可用；也就是說，它不適用於本地自定義類別。

 <p>影象-本地自定義URL類別</p>	 <p>影象-自定義Url類別配置源</p>
本地自定義類別	外部即時摘要類別


定義使用規則運算式


Secure Web Appliance使用的正規表示式語法與其他Velocity模式匹配引擎實現所使用的正規表示式語法略有不同。

此外，裝置不支援使用反斜線來轉義正斜線。如果您需要在規則運算式中使用正斜線，只要鍵入不帶反斜線的正斜線即可。

 注意：從技術上講，AsyncOS for Web使用Flex正規表示式分析器


要測試正規表示式，您可以使用此連結：[flex lint - Regex Tester/Debugger](#)

 注意：返回超過63個字元的正規表示式將失敗並產生無效條目錯誤。請務必形成不可能傳回63個字元以上的規則運算式

 注意：執行大量字元比對的規則運算式會消耗資源，而且可能影響系統效能。因此，可以謹慎應用正規表示式。


您可以在下列位置使用規則運算式：

- 訪問策略的自定義URL類別。建立用於訪問策略組的自定義URL類別時，可以使用正規表示式指定與輸入模式匹配的多台Web伺服器。
- 要阻止的自定義使用者代理。編輯訪問策略組要阻止的應用程式時，可以使用正規表示式輸入要阻止的特定使用者代理。

 提示：無法為正規表示式設定Web代理旁路。

以下是Flex規則運算式中的字元類別清單

字元類別	
.	除換行以外的任何字元
\w \d \s	單字、數字、空格
\W \D \S	不是單詞、數字、空格
[abc]	任何a、b或c
[^abc]	不是a、b或c
[a-g]	a與g之間的字元
錨點	
^abc\$	字串的開始/結束
\b	字邊界
跳脫字元	
\. * \	轉義的特殊字元
\t \n \r	定位點，換行，回車
\u00A9	unicode轉義©
群組與旁觀	
(abc)	捕獲組
\1	返回對組#1的引用
(? : abc)	非捕獲組
(?=abc)	正面展望
(?!abc)	負面展望
數量詞與替代	
a* a+ a?	0或更多、1或更多、0或1
a{5} a{2, }	剛好五、二或更多
a{1,3}	1到3之間
a+? a{2, }?	匹配儘可能少
ab cd	match ab或cd

 注意：請小心長模式中的未轉義點，特別是在較長模式的中間，並注意此元字元（星號 *），尤其是與點字元結合時。任何模式都包含一個未轉義的點，在點被停用後會返回超過 63 個字元。

永遠逸出*(star)和。（點）帶有\（反斜線），如*和\。

如果在正規表示式中使用.cisco.local，則域Xcisco.local也匹配。

未跳脫字元會影響效能，並在Web瀏覽過程中造成速度變慢。這是因為模式匹配引擎必須經過數千或數百萬種可能性才能找到正確條目的匹配項，並且它可能會對允許的策略的相似URL存在一些安全問題

可以使用命令列介面(CLI)選項advancedproxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex，啟用或停用預設regex conversion to lower case for case-insensitive matches。如果您有區分大小寫的問題，請使用。

限制和設計問題

- 在這些URL類別定義中，您最多可以使用30個外部即時原始檔，每個檔案包含的條目不能超過5000個。
- 如果外部饋送條目數增加，則會導致效能下降。
- 可以在多個自定義URL類別中使用同一地址，但所列類別的順序是相關的。

如果將這些類別包括在同一策略中，並為每個類別定義不同的操作，則會應用為自定義URL類別表中最高列出的類別定義的操作。

- 當原生檔案傳輸通訊協定(FTP)要求以透明方式重新導向到FTP代理時，它不包含FTP伺服器的主機名稱資訊，只包含IP位址。

因此，某些僅具有主機名資訊的預定義URL類別和Web信譽過濾器與本地FTP請求不匹配，即使這些請求發往這些伺服器。

如果要阻止對這些站點的訪問，必須建立自定義URL類別才能使用它們的IP地址。

- 未分類的URL是不匹配任何預定義URL類別或包括的自訂URL類別的URL

在策略中使用自定義URL類別

URL過濾引擎允許您過濾訪問、解密和資料安全策略中的事務。為策略組配置URL類別時，可以配置自定義URL類別（如果有）和預定義URL類別的操作。

為訪問策略配置URL過濾器的步驟

步驟 1. 選擇網路安全管理器>訪問策略。

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

動作	說明
封鎖	Web代理拒絕與此設定匹配的事務。
重新導向	將原始流向此類別URL的流量重定向到您指定的位置。當您選擇此動作時，會出現 [Redirect To]欄位。輸入要將所有流量重定向到的URL。
允許	始終允許客戶端請求此類別中的網站。 允許的要求會略過所有進一步的篩選和惡意程式掃描。 僅對受信任的網站使用此設定。您可以將此設定用於內部網站。
監視	Web代理既不允許也不阻止該請求。相反，它會繼續根據其他策略組控制設定（如Web信譽過濾器）評估客戶端請求。
警告	Web Proxy一開始會封鎖要求並顯示警告頁面，但可讓使用者按一下警告頁面中的超文字連結來繼續。
基於配額	當個別使用者接近您指定的磁碟區或時間配額時，會顯示警告。當達到配額時，會顯示區塊頁面。
基於時間	Web代理在您指定的時間範圍內阻止或監控請求。

步驟 5. 在Predefined URL Category Filter部分，為每個類別選擇以下操作之一：

- 使用全域設定
- 監視
- 警告
- 封鎖
- 基於時間
- 基於配額

Predefined URL Category Filtering						
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.						
Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.						
Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn	Quota-Based	Time-Based
Animals and Pets	Select all	Select all	Select all	Select all		
Arts			✓			
Predefined Quota Profile: 10GBdailyLimit Astrology In time range: MorningShift Action: Warn Otherwise: Block					✓	
						✓

影像-選取預先定義類別的動作

步驟 6. 在未分類的URL部分，選擇要對未歸入預定義或自定義URL類別的網站進行客戶端請求時執行的操作。此設定也會決定URL類別集更新所產生之新類別與合併類別結果的預設動作。

Uncategorized URLs	
Specify an action for urls that do not match any category.	
Uncategorized URLs:	Monitor
Default Action for Update Categories: ?	Most Restrictive

影像-選擇未分類URL的操作

步驟 7. 提交並提交更改。

為解密策略配置URL過濾器的步驟

步驟 1. 選擇網路安全管理器>解密策略。

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

動作	說明
透過	透過客戶端和伺服器之間的連線，而不檢查流量內容。
監視	Web代理既不允許也不阻止該請求。相反，它會繼續根據其他策略組控制設定（如Web信譽過濾器）評估客戶端請求。
解密	允許連線，但檢查流量內容。裝置對流量進行解密，並將訪問策略應用於已解密的流量，就像它是純文字檔案超文本傳輸協定(HTTP)連線一樣。當連線解密並應用訪問策略時，您可以掃描流量以查詢惡意軟體。
drop	刪除連線，而且不將連線要求傳遞至伺服器。裝置不會通知使用者已斷開連線。

步驟 5. 在未分類的URL部分，選擇要對未歸入預定義或自定義URL類別的網站進行客戶端請求時執行的操作。

此設定也會決定URL類別集更新所產生之新類別與合併類別結果的預設動作。

影象-未分類的解密策略

步驟 6. 提交並提交更改。

⚠ 注意：如果要阻止超文本傳輸協定安全(HTTPS)請求的特定URL類別，請選擇解密解密解密解密策略組中的該URL類別，然後選擇阻止訪問策略組中的同一URL類別。

為資料安全策略組配置URL過濾器的步驟

步驟 1. 選擇網路安全管理器> Cisco資料安全。

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

Custom and External URL Categories

動作	說明
允許	始終允許此類別中網站的上傳請求。僅適用於自定義URL類別。 允許的要求會略過所有進一步的資料安全掃描，並且會根據存取原則評估要求。 僅對受信任的網站使用此設定。您可以將此設定用於內部網站。
監視	Web代理既不允許也不阻止該請求。相反，它會繼續根據其他策略組控制設定（如Web信譽過濾器）評估上傳請求。
封鎖	Web代理拒絕與此設定匹配的事務。

步驟 5. 在Predefined URL Category Filtering部分中，為每個類別選擇以下操作之一：

- 使用全域設定
- 監視
- 封鎖

Predefined URL Category Filtering		
<i>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</i>		
<i>Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.</i>		
Category	Use Global Settings	Override Global Settings
		Monitor ☺
	Select all	Select all Select all
☺ Hunting		<input checked="" type="checkbox"/> <input type="checkbox"/>
☹ Illegal Activities		<input type="checkbox"/> <input checked="" type="checkbox"/>

影象-資料安全預定義URL選擇操作


步驟 6. 在未分類的 URL 部分，選擇要對不屬於預定義或自定義URL類別的網站的上傳請求採取的操作。

此設定也會決定URL類別集更新所產生之新類別與合併類別結果的預設動作。

Uncategorized URLs	
<i>Specify an action for urls that do not match any category.</i>	
Uncategorized URLs:	<input type="text" value="Block"/>
Default Action for Update Categories: (?)	<input type="text" value="Least Restrictive"/>

影象-未分類的資料安全性

步驟 7. 提交並提交更改。

 注意：如果未停用最大檔案大小限制，網路安全裝置將在URL過濾中選擇「允許」或「監控」選項時繼續驗證最大檔案大小。

設定使用自訂URL類別控制上傳要求的步驟

每個上傳請求都分配給「出站惡意軟體掃描」策略組，並繼承該策略組的控制設定。

Web代理收到上傳請求報頭後，它擁有決定是否必須掃描請求正文的必要資訊。

DVS引擎掃描請求並將判定結果返回給Web代理。如果適用，終端使用者會看到阻止頁面。

步驟 1	選擇網路安全管理器>出站惡意軟體掃描。								
步驟 2	在目標列中，按一下要配置的策略組的連結。								
步驟 3	在Edit Destination Settings部分中，從下拉選單中選擇Define Destinations Scanning Custom Settings」。								
步驟 4	<p>在要掃描的目標部分中，選擇以下選項之一：</p> <table border="1"><thead><tr><th>選項</th><th>說明</th></tr></thead><tbody><tr><td>不掃描任何上傳</td><td>DVS引擎不會掃描任何上傳請求。系統會根據訪問策略評估所有上傳請求</td></tr><tr><td>掃描所有上傳</td><td>DVS引擎會掃描所有上傳請求。根據DVS引擎掃描判定結果，根據訪問策略阻止或評估上傳請求</td></tr><tr><td>掃描上傳到指定的自定義URL類別</td><td>DVS引擎掃描屬於特定自定義URL類別的上傳請求。上傳請求將根據訪問策略被阻止或評估，具體取決於DVS引擎掃描裁決。 按一下Edit custom categories list選擇要掃描的URL類別</td></tr></tbody></table>	選項	說明	不掃描任何上傳	DVS引擎不會掃描任何上傳請求。系統會根據訪問策略評估所有上傳請求	掃描所有上傳	DVS引擎會掃描所有上傳請求。根據DVS引擎掃描判定結果，根據訪問策略阻止或評估上傳請求	掃描上傳到指定的自定義URL類別	DVS引擎掃描屬於特定自定義URL類別的上傳請求。上傳請求將根據訪問策略被阻止或評估，具體取決於DVS引擎掃描裁決。 按一下Edit custom categories list選擇要掃描的URL類別
選項	說明								
不掃描任何上傳	DVS引擎不會掃描任何上傳請求。系統會根據訪問策略評估所有上傳請求								
掃描所有上傳	DVS引擎會掃描所有上傳請求。根據DVS引擎掃描判定結果，根據訪問策略阻止或評估上傳請求								
掃描上傳到指定的自定義URL類別	DVS引擎掃描屬於特定自定義URL類別的上傳請求。上傳請求將根據訪問策略被阻止或評估，具體取決於DVS引擎掃描裁決。 按一下Edit custom categories list選擇要掃描的URL類別								
步驟 5	提交您的變更。								
步驟 6	在Anti-Malware Filtering列中，按一下策略組的連結。								

步驟 7	在Anti-Malware Settings部分中，選擇Define Anti-Malware Custom Settings。
步驟 8	在Cisco DVS Anti-Malware Settings部分中，選擇要為此策略組啟用的反惡意軟體掃描引擎。
步驟 9	在惡意軟體類別部分，選擇是監控還是阻止各種惡意軟體類別。 本部分列出的類別取決於您啟用的掃描引擎。
步驟 10	提交並提交更改。

在外部DLP策略中配置控制上傳請求的步驟

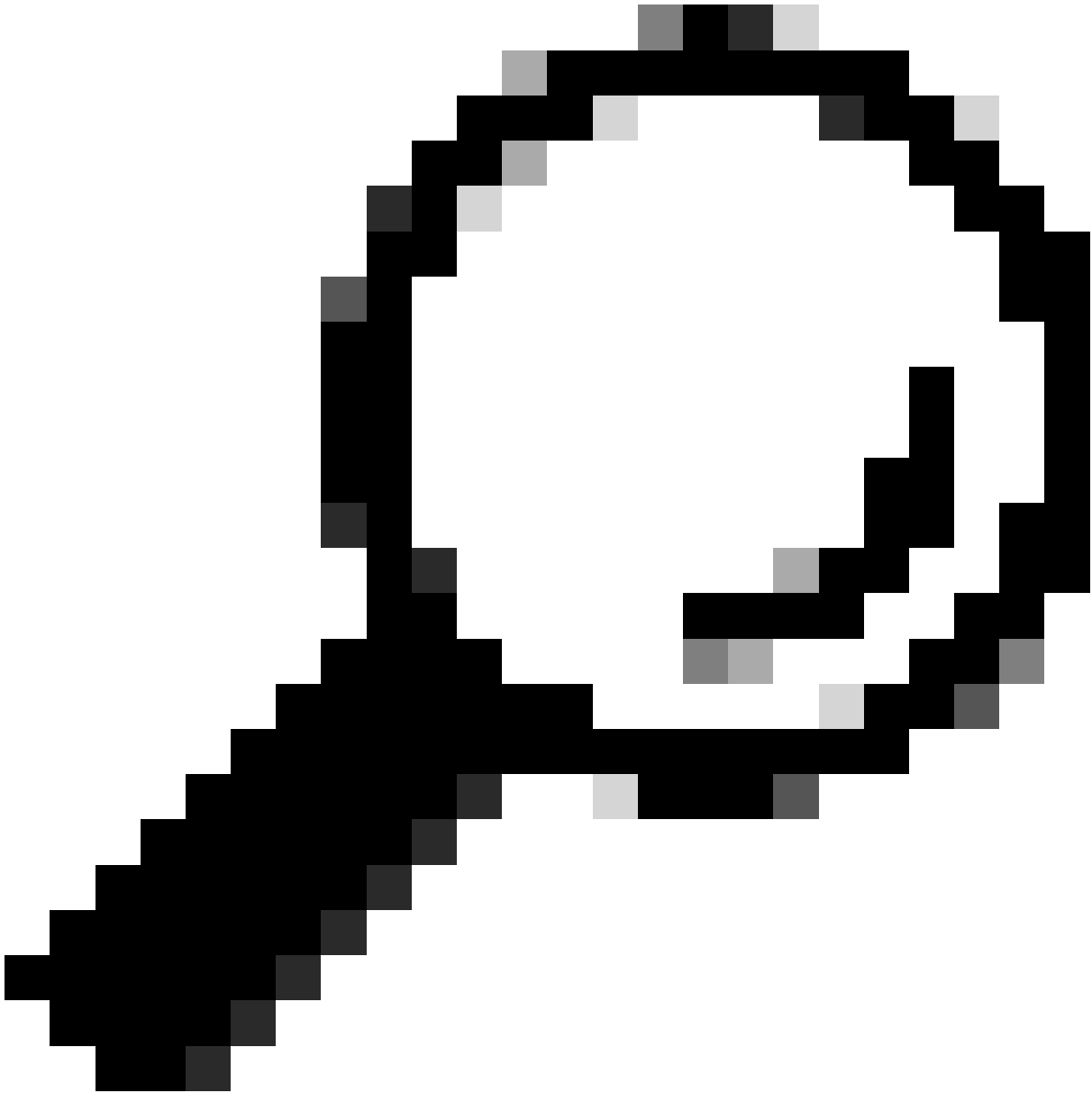
一旦Web代理收到上傳請求報頭，它就會獲得必要資訊，以決定請求是否可以轉到外部DLP系統進行掃描。

DLP系統會掃描請求並將判定結果返回給Web代理，即阻止或監控（根據訪問策略評估請求）。

步驟 1	選擇網路安全管理器 > 外部資料丟失防護。
步驟 2	按一下要設定之原則群組的「目的地」資料欄下的連結。
步驟 3	在Edit Destination Settings部分下，選擇「Define Destinations Scanning Custom Settings」。
步驟 4	<p>在要掃描的目標部分，選擇以下選項之一：</p> <ul style="list-style-type: none"> 請勿掃描任何上傳。不會將任何上傳要求傳送到已設定的防資料遺失(DLP)系統進行掃描。系統會根據訪問策略評估所有上傳請求。 掃描所有上傳。所有上傳請求都將傳送到已配置的DLP系統進行掃描。上傳請求被阻止或根據訪問策略進行評估，具體取決於DLP系統掃描判定。 掃描上傳至指定的自訂和外部URL類別除外。屬於特定自定義URL類別的上傳請求會從DLP掃描策略中排除。按一下Edit custom categories list選擇要掃描的URL類別。
步驟 5	提交並提交更改。

略過和傳遞URL

您可以在透明代理實施中配置安全Web裝置，以繞過來自特定客戶端或發往特定目標的HTTP或HTTPS請求。



提示：對於需要資料流透過裝置的應用程式，您可以使用直通功能，而無需對目標伺服器進行任何修改或進行證書檢查

⚠ 注意：域對映功能在HTTPS透明模式下工作。在顯式模式和HTTP資料流中，此功能不起作用。

- 必須配置本地自定義類別，以允許流量使用此功能。

- 啟用此功能時，它會根據網域對應中設定的伺服器名稱修改或指派伺服器名稱，即使有可用的伺服器名稱指示(SNI)資訊也一樣。
- 如果流量與域對映匹配，並且配置了相應的自定義類別、解密策略和直通操作，則此功能不會基於域名阻止流量。
- 驗證無法搭配此傳遞功能使用。身份驗證需要解密，但在此情況下流量不會被解密。
- 流量不受監控。您必須將UDP資料流配置為不進入網路安全裝置，而是必須直接透過防火牆連線到Internet以訪問WhatsApp、Telegram等應用程式。
- WhatsApp、Telegram和Skype在透明模式下工作。但是，由於對應用的限制，某些WhatsApp等應用無法以「顯式」模式工作。

確保您為需要將流量傳遞到特定伺服器的裝置定義了標識策略。具體來說，您必須：

- 選擇Exempt from authentication/identification。
- 指定此辨識設定檔必須套用的位址。您可以使用IP地址、無類域間路由(CIDR)塊和子網。


步驟 1	啟用HTTPS代理。				
步驟 2	<p>選擇網路安全管理器 > 域對映。</p> <ol style="list-style-type: none"> 選擇Add Domain。 輸入域名或目標伺服器。 如果指定了某些域，請選擇優先順序的順序。 輸入IP地址。 按一下Submit。 				
步驟 3	<p>選擇網路安全管理器 > 自定義和外部URL類別。</p> <ol style="list-style-type: none"> 選擇Add Category。 請提供這些資訊。 <table border="1" data-bbox="336 1771 1485 2051"> <thead> <tr> <th data-bbox="336 1771 464 1888">設定</th> <th data-bbox="464 1771 1485 1888">說明</th> </tr> </thead> <tbody> <tr> <td data-bbox="336 1888 464 2051">類別名稱</td> <td data-bbox="464 1888 1485 2051">輸入此URL類別的辨識碼。當您設定原則群組的URL篩選器時，就會顯示此名稱。</td> </tr> </tbody> </table>	設定	說明	類別名稱	輸入此URL類別的辨識碼。當您設定原則群組的URL篩選器時，就會顯示此名稱。
設定	說明				
類別名稱	輸入此URL類別的辨識碼。當您設定原則群組的URL篩選器時，就會顯示此名稱。				


	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 20%; text-align: center;">設定</th> <th style="text-align: center;">說明</th> </tr> </thead> <tbody> <tr> <td style="text-align: center; vertical-align: middle;">清單順序</td> <td>指定此類別在自訂URL類別清單中的順序。輸入「1」作為清單中的第一個URL類別。 URL過濾器引擎根據自定義URL類別按指定順序評估客戶端請求。</td> </tr> <tr> <td style="text-align: center; vertical-align: middle;">類別型別</td> <td>選擇Local Custom Category。</td> </tr> <tr> <td style="text-align: center; vertical-align: middle;">進階</td> <td>您可以在此段落中輸入規則運算式，以指定其他位址集。 您可以使用規則運算式來指定多個符合您輸入之樣式的地址。</td> </tr> </tbody> </table> <p>c. 提交並提交更改。</p>	設定	說明	清單順序	指定此類別在自訂URL類別清單中的順序。輸入「1」作為清單中的第一個URL類別。 URL過濾器引擎根據自定義URL類別按指定順序評估客戶端請求。	類別型別	選擇Local Custom Category。	進階	您可以在此段落中輸入規則運算式，以指定其他位址集。 您可以使用規則運算式來指定多個符合您輸入之樣式的地址。
設定	說明								
清單順序	指定此類別在自訂URL類別清單中的順序。輸入「1」作為清單中的第一個URL類別。 URL過濾器引擎根據自定義URL類別按指定順序評估客戶端請求。								
類別型別	選擇Local Custom Category。								
進階	您可以在此段落中輸入規則運算式，以指定其他位址集。 您可以使用規則運算式來指定多個符合您輸入之樣式的地址。								
<p>步驟 4</p>	<p>選擇網路安全管理器 > 解密策略。</p> <ol style="list-style-type: none"> a. 建立新的解密策略。 b. 選擇您為繞過特定應用的HTTPS流量而建立的標識配置檔案。 c. 在高級面板中，按一下「URL類別」連結。 d. 在Add列中，按一下以增加在步驟3中建立的自定義URL類別。 e. 選擇Done。 f. 在「解密策略」頁中，按一下URL過濾連結。 g. 選擇Pass Through。 h. 提交並提交更改。 <p>(可選) 您可以使用%(格式說明符)檢視訪問日誌資訊。</p>								

設定Web要求的Web代理略過

將自定義URL類別增加到代理繞行清單後，系統會對源和目標繞行自定義URL類別的所有IP地址和域名。

步驟 1	選擇Web Security Manager > Bypass Settings。
------	-------------------------------------------

步驟 2	按一下Edit Bypass Settings。
步驟 3	輸入要繞過Web Proxy的地址。  注意：將/0配置為旁路清單中的任何IP的子網掩碼時，裝置將繞過所有Web流量。在這種情況下，裝置會將配置解釋為0.0.0.0/0。
步驟 4	選擇要增加到代理旁路清單的自定義URL類別。
步驟 5	提交並提交您的更改。

 注意：無法為正規表示式設定Web代理旁路。

報告

在「報告」>>「URL類別」頁面中提供了URL統計資訊的綜合顯示，其中包括匹配的前幾個URL類別和阻止的前幾個URL類別的相關資訊。

此頁面顯示節省頻寬和Web交易的類別特定資料。

區段	說明
時間範圍（下拉選單）	選擇報表的時間範圍。
按事務總數排名靠前的URL類別	此段落會以圖表格式列出在網站上造訪的常用URL類別。
按阻止和警告的交易排名靠前的URL類別	以圖形格式列出觸發每個事務發生的阻止或警告操作的頂級URL。
匹配的URL類別	顯示指定時間範圍內按URL類別劃分的事務處理方式，以及每個類別中使用的頻寬和花費的時間。 如果未分類的URL百分比高於15-20%，請考慮以下選項： <ul style="list-style-type: none"> 對於特定的在地化URL，您可以建立自定義URL類別並將其應用於特定使用者或組策略。 您可以將未分類、分類錯誤和URL報告給思科進行評估和資料

區段

說明

庫更新。

- 驗證是否已啟用Web信譽過濾器 and 防惡意軟體過濾器。

URL-Categories

Printable PDF

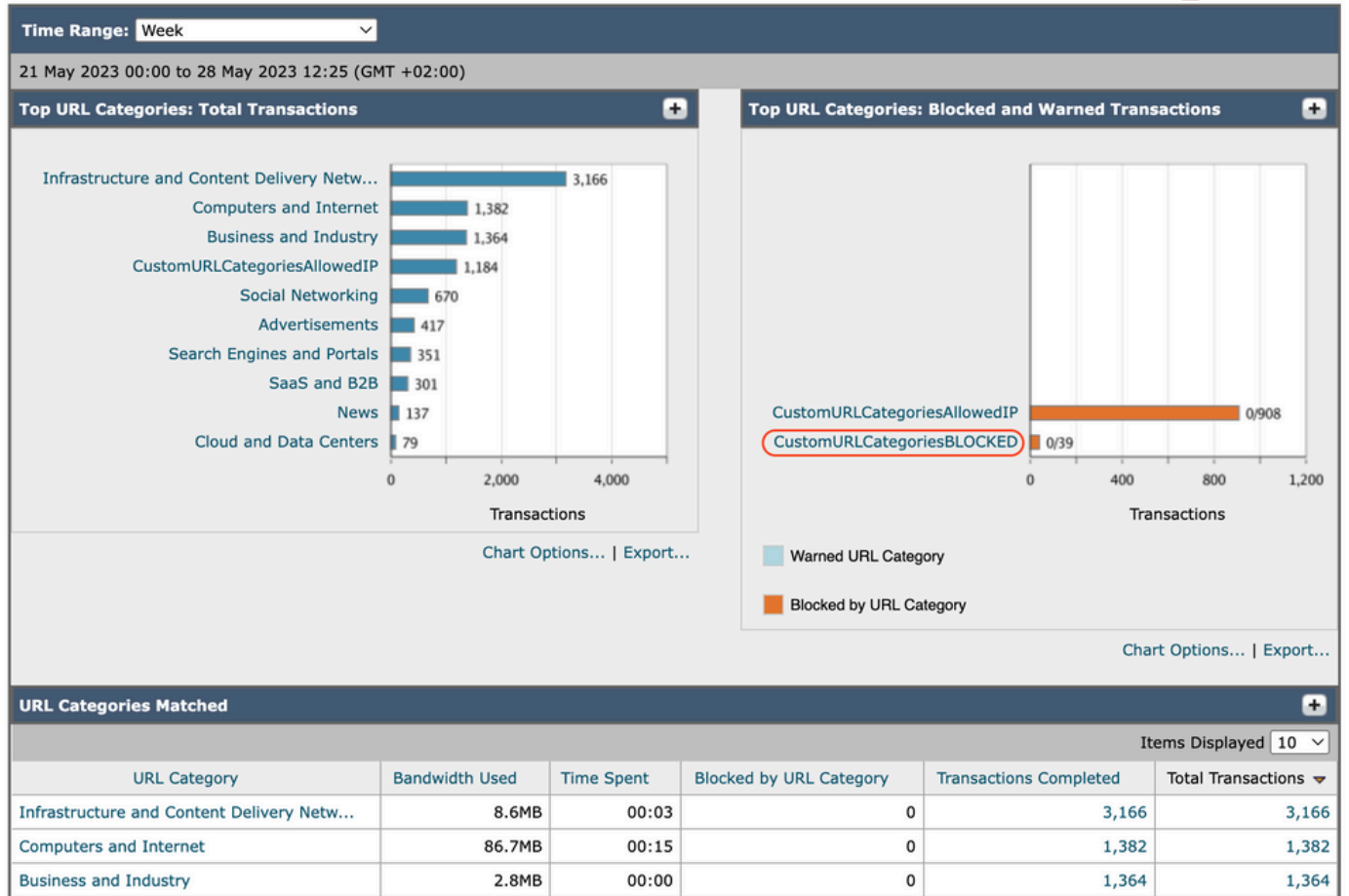
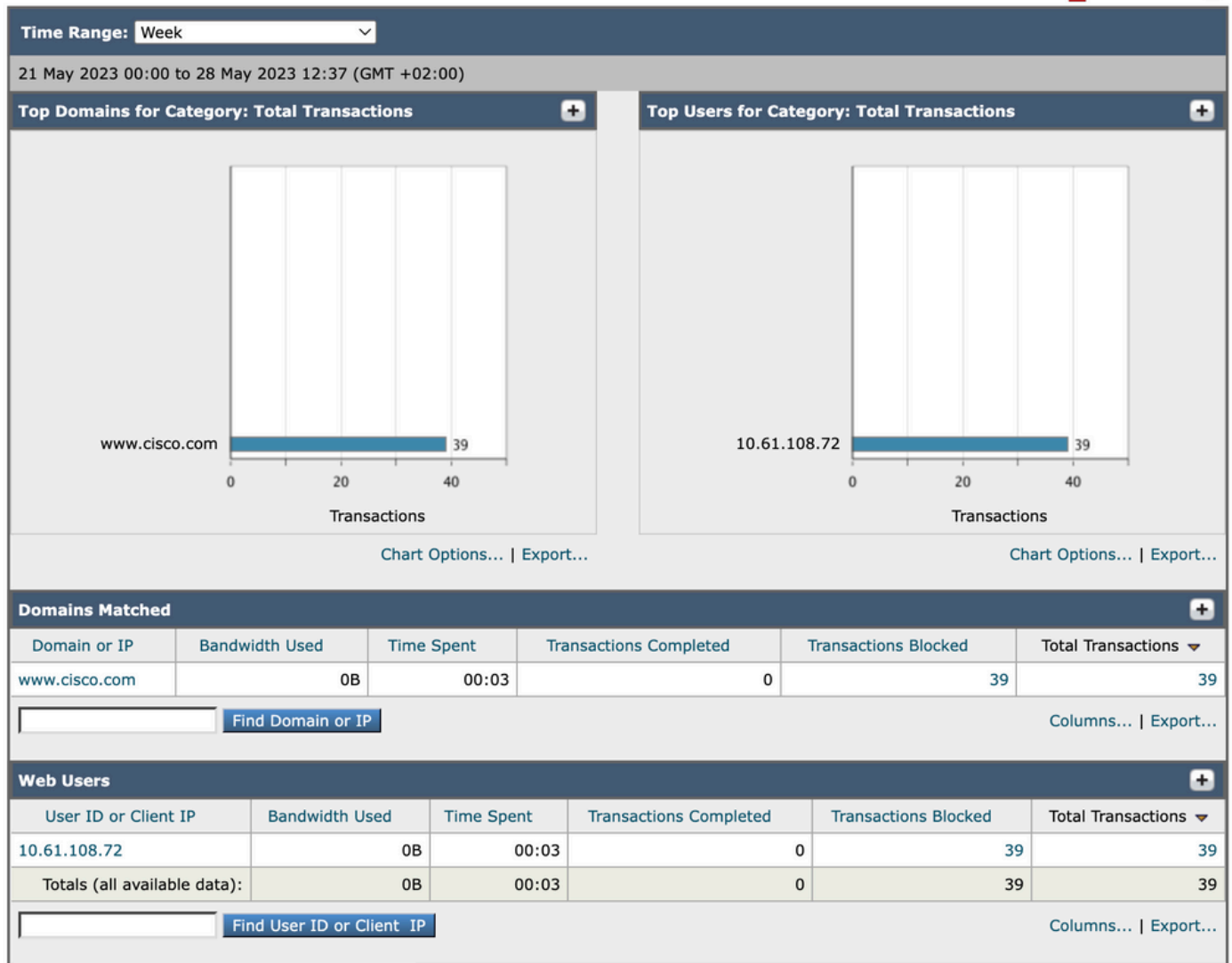


Image-URL類別報告

您可以按一下任何類別名稱，檢視與該類別相關的詳細資訊，例如「相符的網域」或「使用者清單」。



影像-詳細報告頁面

預定義的URL類別集可以在您的網路安全裝置上定期自動更新。

當這些更新發生時，舊的類別名稱會繼續出現在報告中，直到與舊類別相關聯的資料太舊，無法包括在報告中。

URL類別集更新後生成的報告資料使用新類別，因此您可以在同一報告中同時檢視舊類別和新類別。

在來自報表的「URL類別」頁面的URL統計資料中，瞭解如何解譯這些資料非常重要：

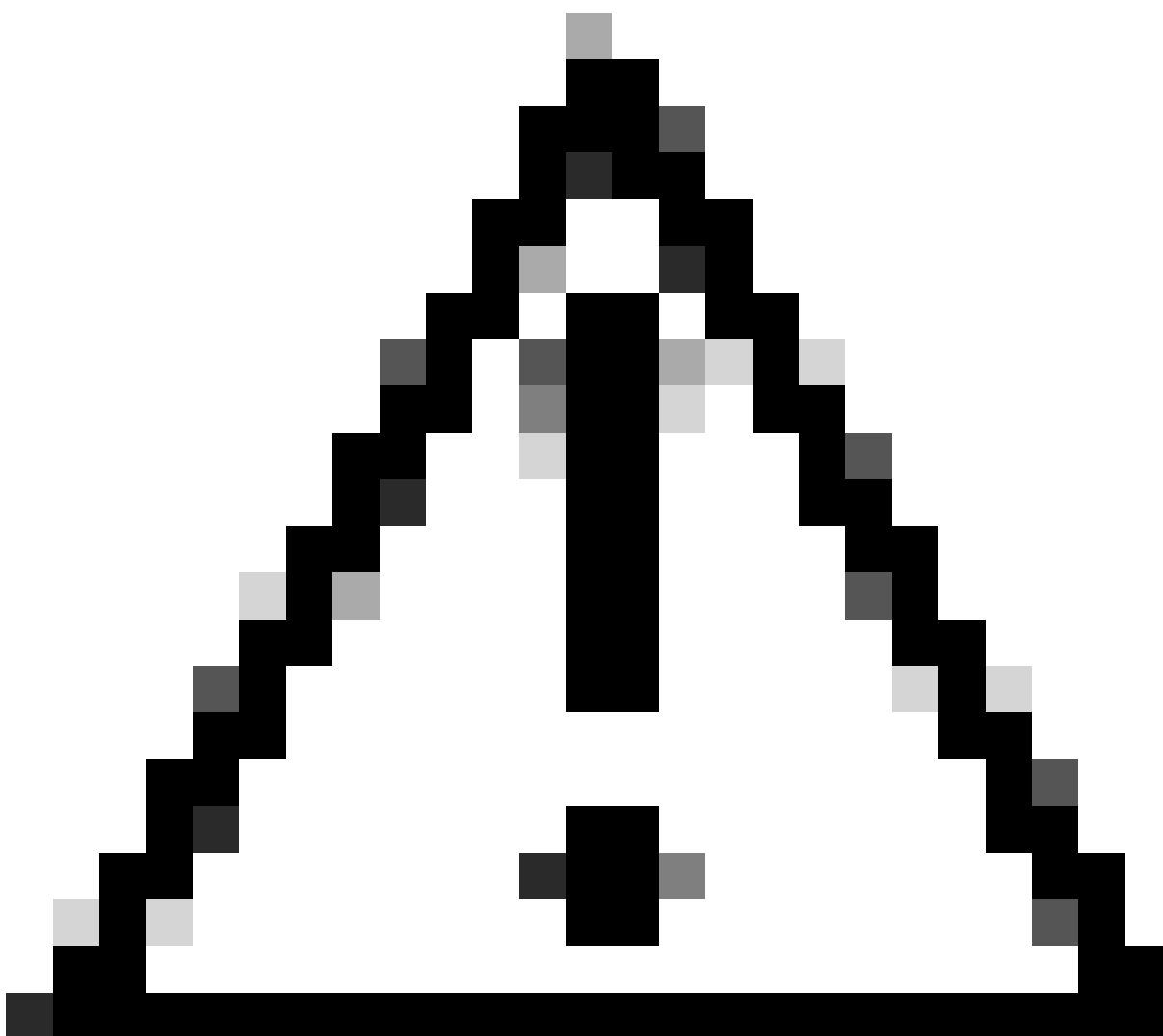
資料型別	說明
略過URL篩選	表示在URL過濾之前阻止的策略、埠和管理使用者代理。
未分類的URL	表示查詢URL過濾引擎但未匹配類別的所有事務。

在存取記錄中檢視自訂URL類別

Secure Web Appliance在訪問日誌中使用前面帶有「c_」的自訂URL類別名稱的前四個字元。

在本示例中，類別名稱為CustomURLCategoriesBLOCKED，並在訪問日誌中看到C_Cust（僅針對註冊使用者）：

```
1685269516.853 86 10.61.108.72 TCP_DENIED_SSL/403 0 GET https://www.cisco.com:443/ - NONE/- - DROP_CUST
```



注意：如果使用Sawmill分析訪問日誌，請考慮自定義URL類別名稱。如果自訂URL類別的前四個字元包含空格，Sawmill無法正確剖析存取日誌專案。而僅在前四個字元中使用支援的字元。

 秘訣：如果您想要在存取日誌中包含自訂URL類別的完整名稱，請將%XF格式說明符加入存取日誌。

當Web訪問策略組將自定義URL類別設定為Monitor，並且某些其他元件(如Web信譽過濾器或不同裁決掃描(DVS)引擎)做出允許或阻止自定義URL類別中URL請求的最終決定，則請求的訪問日誌條目將顯示預定義的URL類別而不是自定義URL類別。

有關如何在訪問日誌中配置自定義欄位的詳細資訊，請訪問：[在訪問日誌中配置效能引數-思科](#)

疑難排解

類別不匹配

從訪問日誌中，您可以看到該請求屬於哪個自定義URL類別（如果選項與預期不符）：

- 如果要求分類為其他自訂URL類別，請檢查是否有重複的URL或其他類別中的相符一般表示式，或將自訂URL類別移至頂端並再次測試。仔細檢查符合的自訂URL類別會更好。
- 如果請求被歸類為預定義類別，請檢查現有自定義URL類別中的條件，如果所有條件都匹配，請嘗試增加IP地址並進行測試，或確保使用的是拼寫和正確的正規表示式（如果有）。

預定義的類別不是最新的

如果預定義的類別不是最新的，或者您在訪問日誌中看到URL category部分的「err」，請確保為Updater啟用TLSv1.2。

要更改更新程式SSL配置，請在GUI中使用以下步驟：

步驟 1.在System Administration中選擇SSL Configuration

System Administration

Policy Trace

Alerts

Log Subscriptions

Return Addresses

SSL Configuration

Users

Network Access

映像- ssl配置

步驟 2.選擇編輯設定。

步驟 3.在更新服務部分中，選擇TLSv1.2

SSL Configuration

SSL Configuration	
<p>Disabling SSLv3 for all services is recommended for best security. Depending on your network requirements, you may also choose to disable some versions of TLS for specific services.</p> <p>Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential. So to avoid communications errors, always select a contiguous set of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1 disabled.</p>	
Appliance Management Web User Interface:	<p>Changing this option will disconnect all active Web User Interface connections on Commit. You will need to log in again.</p> <p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>
Proxy Services:	<p>Proxy services include HTTPS Proxy and credential encryption for secure client.</p> <p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.3 <input checked="" type="checkbox"/> TLS v1.2 <input type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p> <p><input checked="" type="checkbox"/> Disable TLS Compression (Recommended) TLS compression should be disabled for best security.</p> <p>Cipher(s) to Use: EECDH:DSS:RSA:NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA</p>
Secure LDAP Services:	<p>Secure LDAP services include Authentication, External Authentication, SaaS SSO, and Secure Mobility.</p> <p>Enable protocol versions: <input type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>
RADSEC Services:	<p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1</p>
Secure ICAP Services (External DLP):	<p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>
Update Service:	<p>Enable protocol versions: <input type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>

Cancel Submit

影像-更新服務TLSv1.2

步驟 4.提交並提交更改

要更改更新程式SSL配置，請從CLI執行以下步驟：

步驟 1.在CLI中，運行sslconfig

步驟 2.鍵入version並按Enter

步驟 3.選擇Updater

步驟 4.選擇TLSv1.2

步驟 5.按Enter退出嚮導

步驟6.提交更改。

```
SWA_CLI> sslconfig
```

Disabling SSLv3 is recommended for best security.

Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential 1.2, while leaving TLS 1.1 disabled.

Choose the operation you want to perform:

- VERSIONS - Enable or disable SSL/TLS versions
- COMPRESS - Enable or disable TLS compression for Proxy Service
- CIPHERS - Set ciphers for services in Secure Web Appliance
- FALLBACK - Enable or disable SSL/TLS fallback option
- ECDHE - Enable or disable ECDHE Authentication.

[> versions

SSL/TLS versions may be enabled or disabled for the following services:

- LDAPS - Secure LDAP Services (including Authentication, External Authentication, SaaS SSO, Secure Client)
- Updater - Update Service
- WebUI - Appliance Management Web User Interface
- RADSEC - Secure RADSEC Services (including Authentication, External Authentication)
- SICAP - Secure ICAP Service
- Proxy - Proxy Services (including HTTPS Proxy, Credential Encryption for Secure Client)

Currently enabled SSL/TLS versions by service: (Y : Enabled, N : Disabled)

	LDAPS	Updater	WebUI	RADSEC	SICAP	Proxy
TLSv1.0	N	N	N	N/A	N	N
TLSv1.1	Y	Y	N	Y	Y	N
TLSv1.2	N	N	Y	Y	Y	Y
TLSv1.3	N/A	N/A	N/A	N/A	N/A	Y

Select the service for which to enable/disable SSL/TLS versions:

1. LDAPS
2. Updater
3. Proxy
4. RADSEC
5. SICAP
6. WebUI
7. All Services

[> 2

Currently enabled protocol(s) for Updater are TLSv1.1.

To change the setting for a specific protocol, select an option below:

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2

[> 3

TLSv1.2 support for Update Service is currently disabled. Do you want to enable it? [N]> Y

Currently enabled protocol(s) for Updater are TLSv1.1, TLSv1.2.

參考

[思科網路安全裝置最佳實踐指南-思科](#)

[BRKSEC-3303 \(ciscolive\)](#)

[Cisco Secure Web Appliance的AsyncOS 14.5使用手冊- GD \(常規部署 \) -連線、安裝和配置 \[Cisco Secure Web Appliance\] -思科](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。