

如何為Webex應用配置網路安全裝置其他直通設定

簡介

本文檔介紹如何配置安全網路裝置(SWA/WSA)旁路策略，以確保在特殊部署條件下具有正確的Cisco Webex應用功能。

必要條件

需求

思科建議您瞭解以下主題：

- Async OS for Secure Web Appliance 14.x或更高版本。
- 管理使用者對Secure Web Appliance圖形使用者介面(GUI)的訪問。
- 管理使用者對Secure Web Appliance命令列介面(CLI)的訪問。

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。

問題

根據[Webex服務的網路要求](#)的Webex公共文檔，必須將代理伺服器配置為允許Webex信令流量訪問文檔中列出的域/URL。通過在旁路設定中啟用Webex Application Bypass覈取方塊，安全Web裝置可以滿足大多數環境的需求，但是，為了避免Webex應用中的服務中斷，可能需要在安全Web裝置上執行一些其他配置。建議針對此類案例情景採取以下步驟：

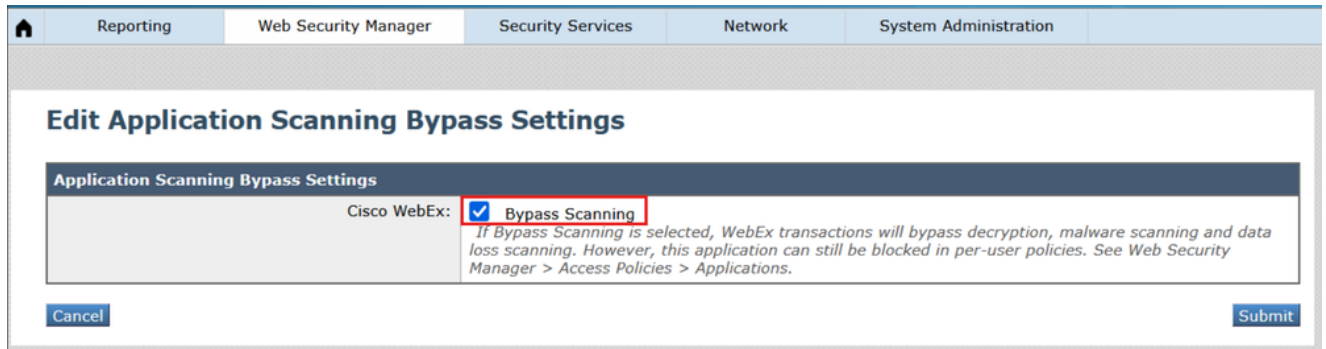
Webex應用程式掃描略過

思科Webex：旁路掃描功能是使Webex應用流量能夠通過安全網路裝置不受過濾的第一步。在所有使用者通過Secure Web Appliance代理Web流量的Webex案頭或移動應用程式環境和部署方案中，都應啟用此功能。

啟用Webex應用掃描旁路的步驟：

1. 在WSA GUI中，瀏覽到Web Security Manager > Bypass Settings > Edit Application Bypass Settings。

2. 選中「Cisco WebEx」覈取方塊。



1_wsa_bypass_scanning_settings

3. 提交和提交更改

啟用此設定後，不會像FQDN新增到安全網路裝置旁路清單後預期的那樣繞過透明流量。相反，Webex應用流量仍然通過安全網路裝置代理，但會通過帶有決策標籤「PASSTHRU_AVC」的解密過程傳遞。以下範例顯示可能會如何在存取記錄中顯示：

```
1761695285.658 55398 192.168.100.100 TCP_MISS/200 4046848 TCP_CONNECT 3.161.225.70:443 - DIRECT/binarie
```

獨特環境的注意事項

在少數情況下，當流量通過安全網路裝置代理時，Webex應用需要額外的配置才能正常工作。

案例 1: Webex網域需要免除身份驗證

這在識別配置檔案中未啟用IP代理，並且使用透明重定向的環境中尤為明顯。根據現有文檔，Webex應用能夠在顯式定義代理的加入域的工作站上進行NTLMSSP身份驗證。否則，最佳做法是為Webex網域設定自訂類別並免除對其進行驗證。

免除Webex網域身份驗證的步驟：

1. 在WSA GUI中，導航到Web Security Manager > Custom and External URL Categories > Add Category。
2. 為新類別指定一個名稱，並將以下域放在站點部分：

.webex.com, .ciscopark.com, .wbx2.com, .webexcontent.com

Custom and External URL Categories: Add Category

Edit Custom and External URL Category	
Category Name:	Webex Domains
Comments: ?	
List Order:	15
Category Type:	Local Custom Category
Sites: ?	.webex.com, .ciscospark.com, .wbx2.com, .webexcontent.com Sort URLs Click the Sort URLs button to sort all site URLs in Alpha-numerical order. (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)
Advanced	Regular Expressions: ? Enter one regular expression per line. Maximum allowed characters 2048.

2_wsa_custom_url_category

- 按一下「Submit」。然後導覽至Web Security Manager > Identification Profiles > Add Identification Profile
- 為新配置檔案指定一個名稱，然後在URL類別的高級部分，選擇在步驟10中建立的新類#2

Identification Profiles: Add Profile

Client / User Identification Profile Settings	
☒ Enable Identification Profile	
Name: ?	Auth Exempt Sites (e.g. my IP Range)
Description:	 (Maximum allowed characters 256)
Insert Above:	2 (Office365.IP) ▼

User Identification Method	
Identification and Authentication: ?	Exempt from authentication / identification ▼ This option may not be valid if any preceding Identification Profile requires authentication on all subnets.

Membership Definition	
Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.	
Define Members by Subnet:	 (examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)
Define Members by Protocol:	☒ HTTP/HTTPS
▼ Advanced	Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents. The following advanced membership criteria have been defined: Proxy Ports: None Selected URL Categories: Webex Domains User Agents: None Selected The Advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories are not applicable for SOCKS transactions or transparent HTTPS (unless decrypted). When Advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.

Cancel

Submit

3_wsa_id_profile

5. 確保將新配置檔案中的Identification and Authentication設定為Exempt from authentication / identification
6. 提交和提交更改。

案例 2: Webex內容網域不能完全允許解密繞行。

啟用了Webex應用程式掃描繞行時，與webexcontent.com相關的少數子域不會自動傳遞解密。只要安全Web裝置的解密證書已新增到裝置的受信任根證書儲存中，或者由運行Webex應用的裝置已信任的內部證書頒發機構簽名，Webex應用就會在解密時信任這些域提供的內容。但是，如果裝置不受管理並且安全Web裝置的解密證書不受信任，則這些域應配置為在解密時傳遞。

當進行透明重定向部署且重定向組使用客戶端IP欺騙存在多個SWA時，可以配置流量根據目標IP重定向到安全Web裝置，同樣，將來自Web伺服器的返回流量配置為根據源地址通過安全Web裝置重新導向。當安全網路裝置配置為使用它使用DNS查詢解析的IP連線到Web伺服器時，返回流量可能會被無意重定向到其他安全網路裝置，隨後被丟棄。由於在Web伺服器上使用旋轉IP地址，此問題不僅影響到Webex，還會影響其他影片流應用程式。

為所有Webex網域配置解密直通的步驟：

1. 確保按照上述說明啟用Webex Application Scanning Bypass。
2. 在WSA GUI中，導航到Web Security Manager > Custom and External URL Categories > Add Category。
3. 為新類別指定一個名稱，並將下一個域放在站點部分：

.webexcontent.com

Custom and External URL Categories: Add Category

Edit Custom and External URL Category

Category Name:

Comments:

List Order:

Category Type:

Sites:

[Sort URLs](#)
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

[Advanced](#) Regular Expressions:

Enter one regular expression per line. Maximum allowed characters 2048.

[Cancel](#) [Submit](#)

4_wsa_url_category

4. 按一下「Submit」。現在，導航到網路安全管理器 > 解密策略 > 新增策略
5. 將新策略命名為，將Identification Profiles and Users設定為「All Users」，並在URL Categories的「高級」部分中選擇在步驟10中建立的新類#3

Decryption Policy: Add Group

Policy Settings

☒ **Enable Policy**

Policy Name:

(e.g., my IP policy)

Description:

(Maximum allowed characters 256)

Insert Above Policy:

Policy Expires:

☐ Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: :

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

☐ All Authenticated Users

☐ Selected Groups and Users ?

Groups: No groups entered

Users: No users entered

☐ Guests (users failing authentication)

☒ All Users (authenticated and unauthenticated users)

If the "All Users" option is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

☒ **Advanced**
Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)

URL Categories:

User Agents: None Selected

5_wsa_decryption_policy

- 按一下「Submit」。#3然後，按一下URL Filtering部分，將在步驟10中建立的自定義類別設定為「Pass Through」。

Decryption Policies: URL Filtering: Webex Passthrough

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	
Webex Passthrough	Custom (Local)	—	☒				—	

CancelSubmit

Predefined URL Category Filtering

No Predefined URL Categories are selected for this policy group.

Overall Web Activities Quota

No quota has been defined. Define quota in Web Security Manager > Define Time Ranges and Quotas.

Uncategorized URLs

This category is unavailable.

CancelSubmit

6_wsa_url_filtering

7. 提交並提交更改。

如果部署了多個安全Web裝置以實現透明重定向並啟用了客戶端IP欺騙，則有兩種解決方案：

1. 將傳出和返回WCCP服務設定為基於客戶端地址而不是伺服器地址進行負載均衡。
2. 在WSA CLI中，設定advancedproxyconfig > DNS > "Find web server by"，以便在連線到Web伺服器的連線中一律使用使用者端提供的IP位址（選項2和3）。有關此設定的更多資訊，請參閱[使用安全Web裝置最佳實踐](#)指南的DNS部分。

驗證

通過設定完成後，Webex流量將在訪問日誌中根據策略處理為通過：

```
1763752739.797 457 192.168.100.100 TCP_MISS/200 6939 TCP_CONNECT 135.84.171.165:443 - DIRECT/da3-wxt08-
1763752853.942 109739 192.168.100.100 TCP_MISS/200 7709 TCP_CONNECT 170.72.245.220:443 - DIRECT/avatar-
1763752862.299 109943 192.168.100.100 TCP_MISS/200 8757 TCP_CONNECT 18.225.2.59:443 - DIRECT/highlights
1763752870.293 109949 192.168.100.100 TCP_MISS/200 8392 TCP_CONNECT 170.72.245.190:443 - DIRECT/retenti
```

檢視和監控webex應用，如果報告任何速度慢或服務中斷，再次檢視訪問日誌並驗證所有webex端流量是否正確處理。

相關資訊

- [Webex服務的網路要求](#)

- [使用安全Web裝置最佳做法](#)

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）。