

瞭解CSC的DNS和SWG回退設定

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[哪些DNS回退設定會導致SWG回退？](#)

[哪些DNS回退設定不會導致SWG回退？](#)

[獨立SWG回退設定](#)

簡介

本檔案介紹思科安全使用者端(CSC)的DNS和安全Web閘道(SWG)回退設定。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據思科安全使用者端。

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。

概觀

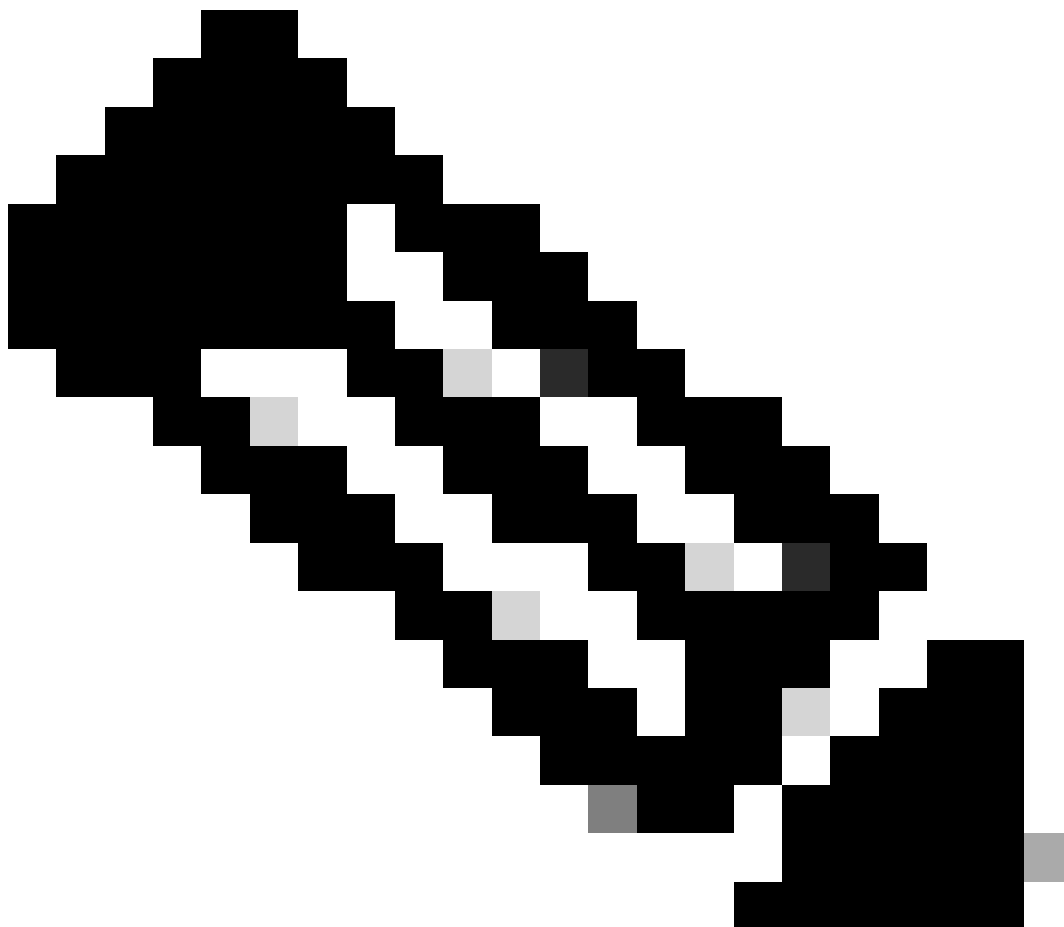
直到2024年4月25日左右，思科安全客戶端的SWG模組回退行為無法控制，無論DNS模組的狀態如何，並且取決於DNS回退設定以啟用/禁用SWG保護。為了解決此問題，Umbrella已將DNS模組和SWG模組的行為分離，從而能夠根據需要進行獨立管理。5.1.3.62版和更新版本中的思科安全客戶端可以使用此功能，其中Umbrella將DNS和SWG回退設定分離，以便實現增強的粒度控制。舊版本上的客戶端未執行單獨的SWG模組回退。

啟用DNS回退後安全Web閘道回退功能時，CSC的SWG模組會遵循DNS模組的行為。但是，並非所有DNS回退設定都會發生這種情況。下一節將詳細介紹SWG模組執行或未執行的DNS回退設定。

哪些DNS回退設定會導致SWG回退？

以下DNS回退設定會導致SWG回退：

- 客戶信任網路：在DNS回退設定中設定客戶信任網路域是最簡單的方法之一。通過託管解析為RFC1918地址的內部域，DNS和SWG可以同時回退。Umbrella的客戶端被編碼為查詢該域。如果成功將域解析為私有IP地址，則會將裝置識別為位於私有受保護網路上，從而導致DNS模組關閉。Web模組也遵循這種回退機制，當DNS模組成功解析域時，同樣可以執行回退。
 - AnyConnect受信任網路檢測
 - AnyConnect VPN檢測
-



附註：運行早於5.1.3.62版本的Cisco Secure Clients上，DNS回退設定仍然有效，因為它是在分離DNS和SWG回退設定之前實施的。

DNS Backoff Settings

Backoff Behind Virtual Appliance

Enables the routing of DNS traffic through the local network if a virtual appliance is detected. When disabled and a virtual appliance is detected, DNS traffic is routed through Umbrella and web traffic is not.

☐ Disabled

Customer Trusted Network

Enables the addition of a subdomain, which when detected results in all traffic to and from it bypassing Umbrella. Subdomain must return an IP address in the RFC-1918 local range.

☒ Enabled

Subdomain

sub.domain.com

ADD

Protected Network Detection

Enables the detection by endpoints of Umbrella registered networks. When detected, Umbrella is bypassed and endpoints rely on network protection.

☐ Disabled

AnyConnect Trusted Network Detection

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Excludes dynamic split tunneling.

☒ Enabled

AnyConnect VPN Detection

Enables the detection by endpoints that a full-tunnel VPN session is active. When detected, DNS traffic forwarding to Umbrella is disabled. Cisco VPNs only.

☒ Enabled

Secure Web Gateway Backoff Settings

Secure Web Gateway backoff follows DNS backoff

When enabled, the endpoint Secure Web Gateway module will follow DNS backoff behavior

When disabled, the endpoint Secure Web Gateway module can be configured with the following backoff settings independent of DNS backoff settings

☒ Enabled

27885424859028

哪些DNS回退設定不會導致SWG回退？

配置這兩個DNS回退功能不會導致SWG回退。因此，您必須有選擇性地配置SWG回退設定，與DNS配置狀態無關。下一節將對此進行更詳細的討論。

- 虛擬裝置後退：從AnyConnect 4.10.07061(MR7)和Secure Client 5.0.02075(MR2)開始，SWG模組可以在存在Umbrella虛擬裝置的網路上保持啟用。如果您先前依賴虛擬裝置的存在來禁用給定網路上的SWG模組和Web重定向，則可以改為使用受信任網路域或AnyConnect受信任網路檢測。
- 受保護網路檢測

DNS Backoff Settings

Backoff Behind Virtual Appliance

Enables the routing of DNS traffic through the local network if a virtual appliance is detected. When disabled and a virtual appliance is detected, DNS traffic is routed through Umbrella and web traffic is not.

☒ Enabled

Customer Trusted Network

Enables the addition of a subdomain, which when detected results in all traffic to and from it bypassing Umbrella. Subdomain must return an IP address in the RFC-1918 local range.

☐ Disabled

Subdomain

sub.domain.com

ADD

Protected Network Detection

Enables the detection by endpoints of Umbrella registered networks. When detected, Umbrella is bypassed and endpoints rely on network protection.

☒ Enabled

AnyConnect Trusted Network Detection

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Excludes dynamic split tunneling.

☐ Disabled

AnyConnect VPN Detection

Enables the detection by endpoints that a full-tunnel VPN session is active. When detected, DNS traffic forwarding to Umbrella is disabled. Cisco VPNs only.

☐ Disabled

Secure Web Gateway Backoff Settings

Secure Web Gateway backoff follows DNS backoff

When enabled, the endpoint Secure Web Gateway module will follow DNS backoff behavior.

When disabled, the endpoint Secure Web Gateway module can be configured with the following backoff settings independent of DNS backoff settings.

☐ Disabled

Customer Trusted Network

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Specific to Cisco Secure Client only and excludes dynamic split tunneling.

☒ Enabled

Trusted Server (https://<server>:<port>)

eg. https://www.xyzoom.com:443

ADD

Certificate Hash

Hash is the SHA256 fingerprint of the server certificate.

SHA256 fingerprint of the server certificate

AnyConnect Trusted Network Detection

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Excludes dynamic split tunneling.

☒ Enabled

AnyConnect VPN Detection

Enables the detection by endpoints that a full-tunnel VPN session is active. When detected, Web traffic forwarding to Umbrella is disabled. Cisco VPNs only.

☒ Enabled

27885587178772

獨立SWG回退設定

如果在您的環境中未啟用這些DNS回退功能，您可以專門使用此處概述的SWG回退設定之一，以確保SWG保持禁用狀態：

- 客戶信任網路
- AnyConnect受信任網路檢測
- AnyConnect VPN檢測

此新功能允許SWG模組獨立於DNS模組運行。使用5.1.3.62及更新版本的思科安全客戶端可以使用此功能。在控制面板中配置一個顯式SWG回退切換：

- 客戶信任網路：其中一個選項是使用SWG回退設定下的Customer Trusted Network選項，在該選項中，您可以配置客戶端可以聯絡的內部伺服器，以確認該伺服器位於受保護的網路上。您需要確保Web伺服器可由客戶端訪問，獲取該伺服器上的證書，並將證書雜湊複製到Umbrella儀表板。

其他兩個選項僅適用於VPN連線：

- AnyConnect受信任網路檢測
- AnyConnect VPN檢測

Secure Web Gateway Backoff Settings

Secure Web Gateway backoff follows DNS backoff

When enabled, the endpoint Secure Web Gateway module will follow DNS backoff behavior.

When disabled, the endpoint Secure Web Gateway module can be configured with the following backoff settings independent of DNS backoff settings.

☐ Disabled

Customer Trusted Network

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Specific to Cisco Secure Client only and excludes dynamic split tunneling.

☒ Enabled

Trusted Server (https://<server>:<port>)

eg. https://www.xyzcom:443.

[ADD](#)

Certificate Hash

Hash is the SHA256 fingerprint of the server certificate.

SHA256 fingerprint of the server certificate

AnyConnect Trusted Network Detection

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Excludes dynamic split tunneling.

☒ Enabled

AnyConnect VPN Detection

Enables the detection by endpoints that a full-tunnel VPN session is active. When detected, Web traffic forwarding to Umbrella is disabled. Cisco VPNs only.

☒ Enabled

27886005743764

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）。