為Secure Connect使用者配置遠端訪問的SIG策略

目錄

簡介

本文檔介紹如何為Secure Connect使用者建立遠端訪問的SIG策略。

概觀

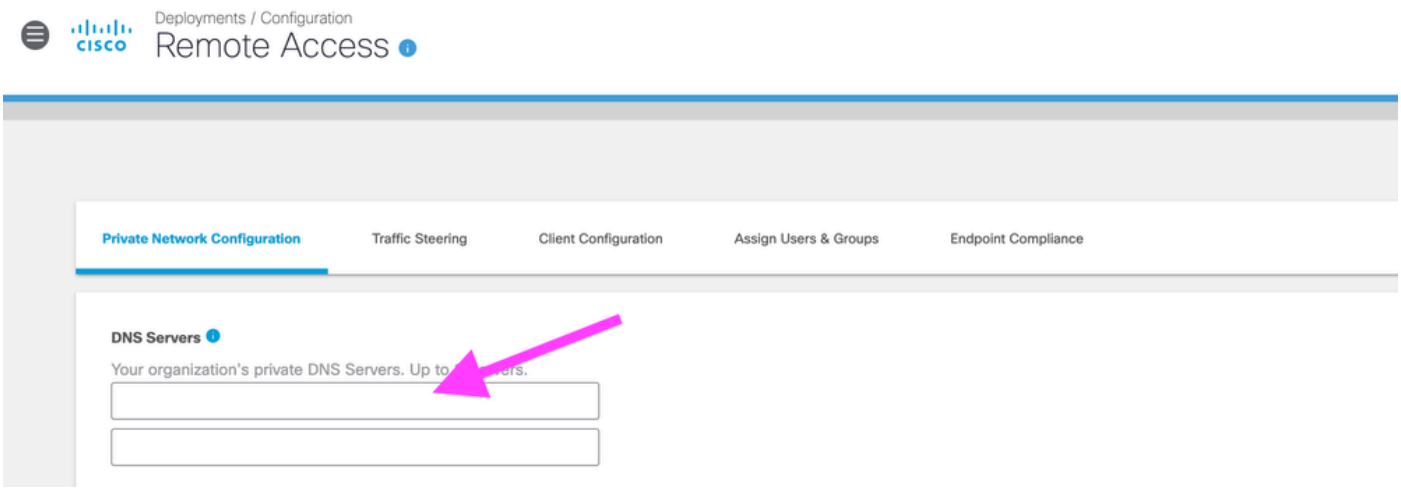
本知識庫文章適用於使用Secure Connect軟體包的客戶，該軟體包包括Umbrella中的遠端訪問(VPNaaS)功能。

管理員可以配置Umbrella防火牆、Web和資料丟失策略以應用於通過AnyConnect連線到遠端訪問的漫遊使用者。

DNS策略

可以將DNS查詢傳送到Umbrella解析程式(例如208.67.222.222)。但是，這不會在Umbrella控制面板上啟用DNS流量的識別、策略或報告。

- 這僅提供DNS解析，因此通常不建議使用。
- 在VPN DNS配置中使用外部DNS解析程式可防止解析內部DNS區域。

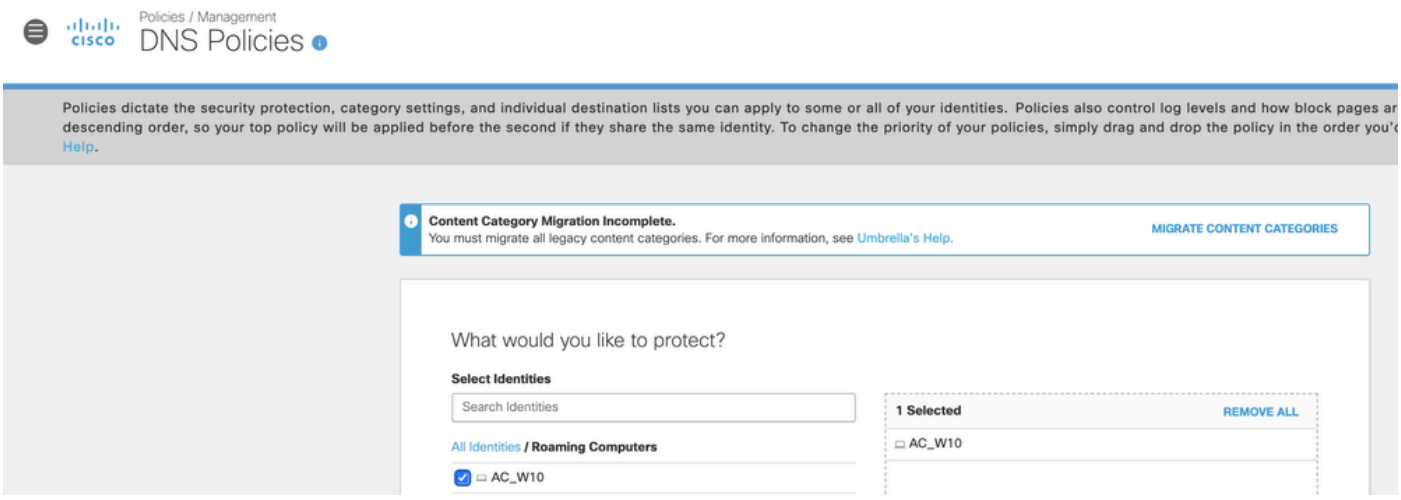


4410210378004

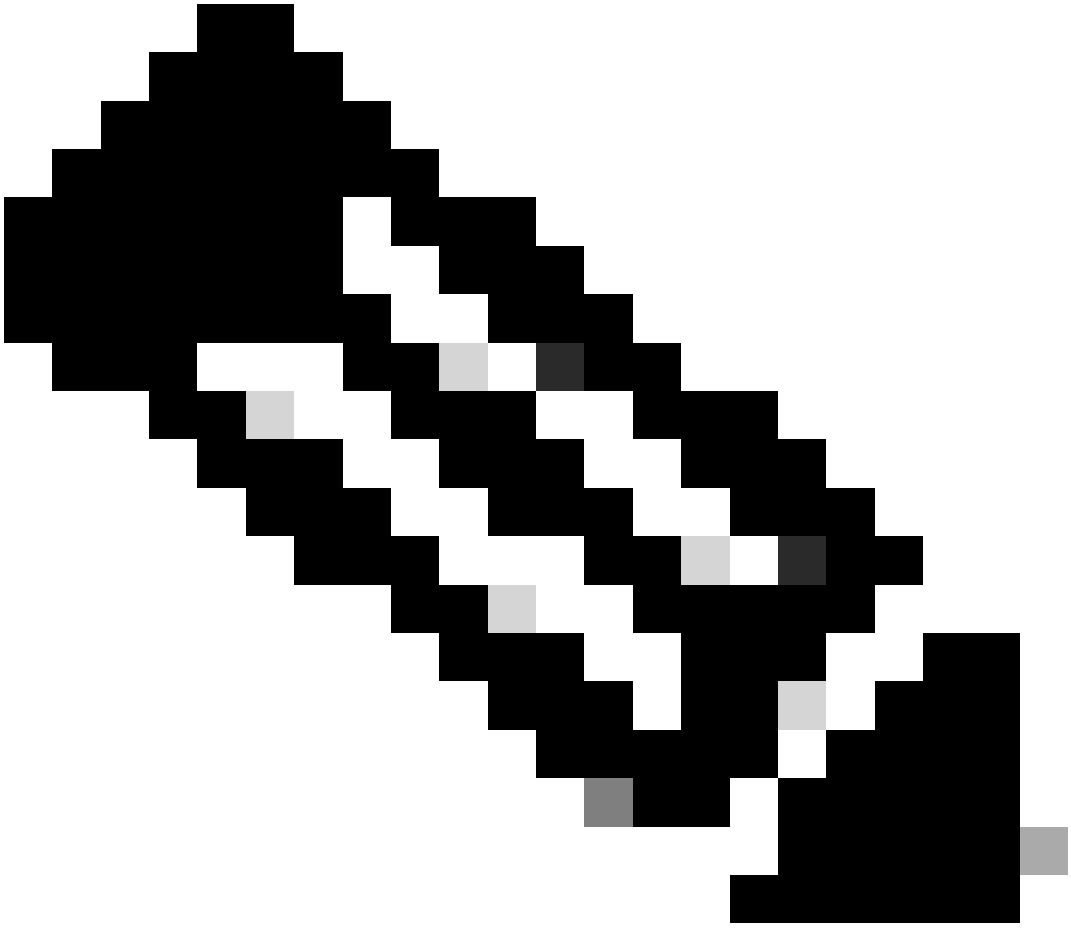
要為DNS查詢新增身份、策略和報告，必須考慮以下三種方法之一：

- （推薦）— 部署Umbrella AnyConnect漫遊模組(通過「部署」>「漫遊電腦」)。 外部DNS流量直接傳送到Umbrella，並應用「漫遊電腦」身份。此模組還支援可選的AD使用者標識。
- 將流量從您的內部DNS伺服器轉發到Umbrella，並使用網路身份標識流量。所有使用者都收到相同的策略/身份，並且沒有精細的使用者報告。
- 在您的本地網路上使用Umbrella Virtual Appliance將流量轉發到Umbrella。DNS查詢可以通過其內部（VPN池IP地址）標識。可以新增AD集成 — 需要安裝其他內部元件。

此示例顯示如何為單個AnyConnect客戶端配置DNS策略(Policies > DNS Policies) — 僅當部署了Umbrella AnyConnect漫遊模組時，才可能配置DNS策略：



4410210455444



附註：使用Umbrella模組進行AnyConnect時，根據分割隧道配置，可以選擇在隧道內部或外部傳送DNS流量。

防火牆策略

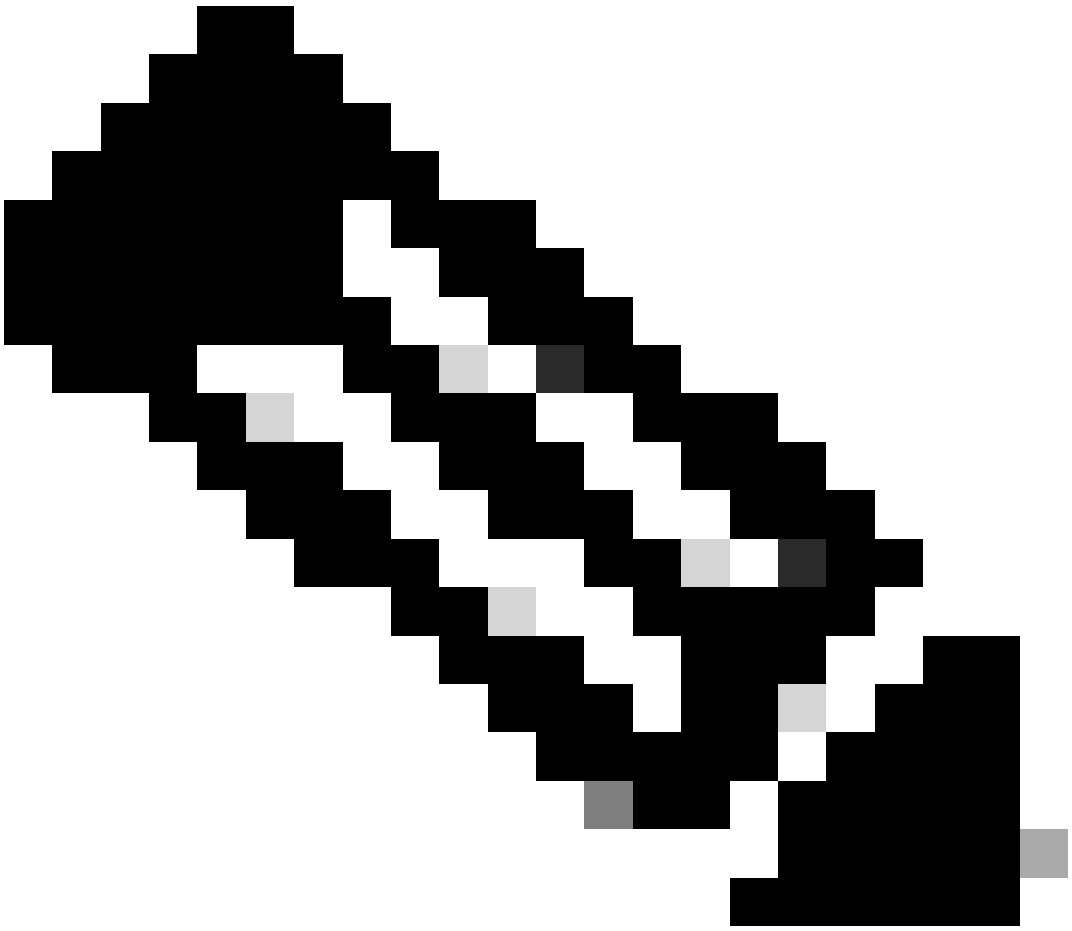
防火牆策略應用於遠端訪問(AnyConnect)客戶端和網際網路之間的流量。 根據以下文檔，在「部署>防火牆策略」中配置規則： 管理防火牆。

預設防火牆規則適用於遠端訪問客戶端。 如果要為遠端訪問使用者建立特定策略，可以選擇建立新的防火牆策略，然後選擇「Remote Access orgid:<ID>」作為源隧道標識。
相同的防火牆策略適用於所有遠端訪問使用者。

- 防火牆策略不用於控制RA客戶端和專用/分支網路之間的訪問。這必須由內部部署防火牆控制。
- 與所有Umbrella防火牆規則一樣，這些規則控制遠端訪問客戶端的出站連線。不允許入站連線。
- 遠端訪問客戶端的源IP地址始終從VPN池動態分配。

- 建議不要使用「源IP」為特定電腦建立規則，因為IP是動態重新分配的
- 通過使用「源CIDR」範圍，可以建立影響特定遠端訪問資料中心的使用者的規則。 每個資料中心都在「Deployments > Remote Access」頁面上配置了不同的VPN池範圍。

4409322341524



附註：每個使用者標識對於防火牆策略不可用。

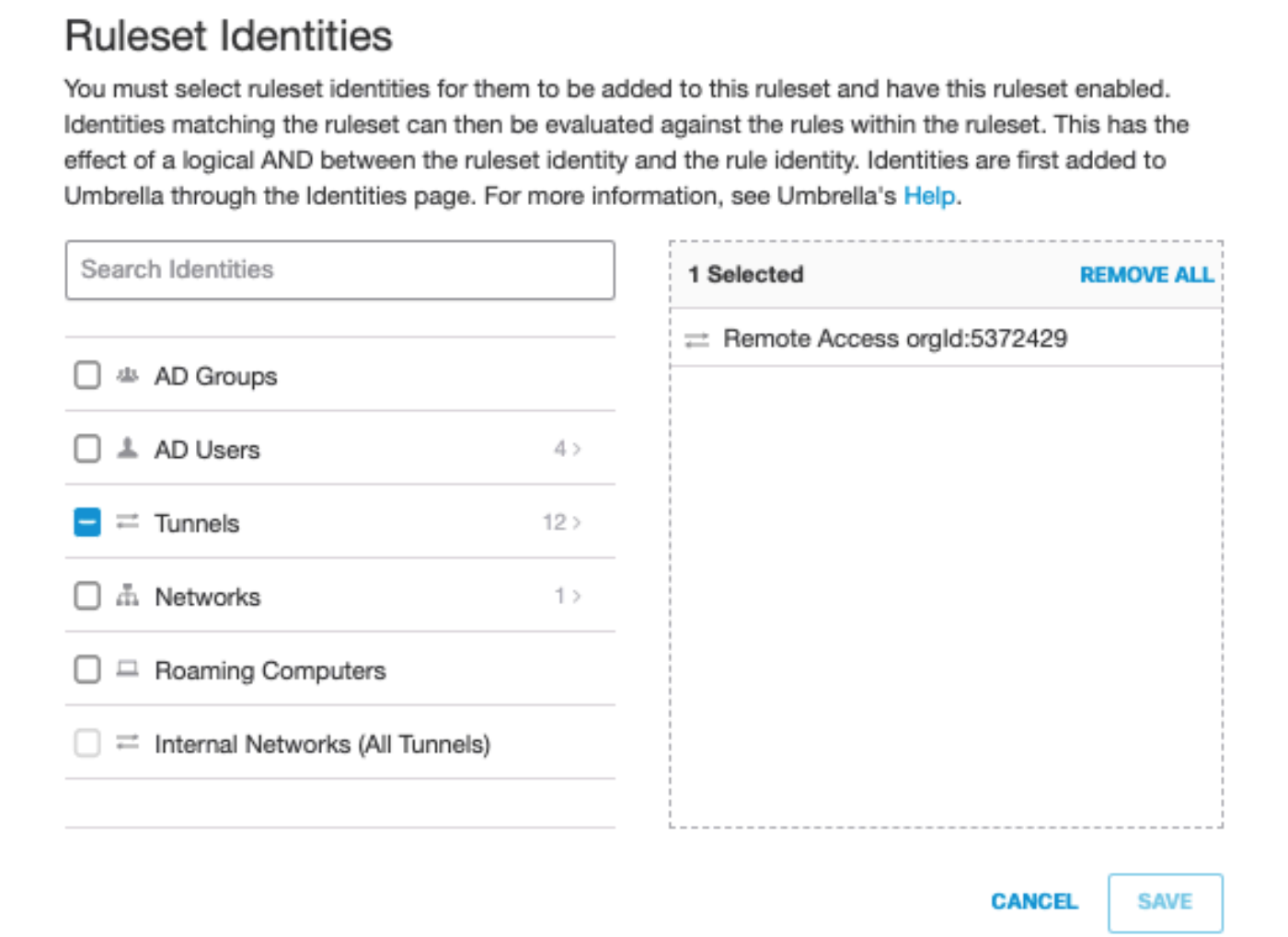
Web策略

Web策略應用於遠端訪問(AnyConnect)客戶端和網際網路之間的流量。 根據以下文檔，在「部署> Web策略」中配置規則：管理Web策略。

- Web策略不用於控制RA客戶端和專用/分支Web伺服器之間的訪問。 Web策略僅適用於外部網站。

預設Web策略適用於遠端訪問客戶端。 但是，我們建議創建新規則集，以專門為遠端訪問客戶端定義安全設定。 定義規則集標識時，從隧道清單中選擇Remote Access orgid:<ID> 。相同的Web策略適用於所有遠端訪問使用者。

建立規則集後，可以新增一個Web規則,用於定義內容類別過濾和應用程式設定。



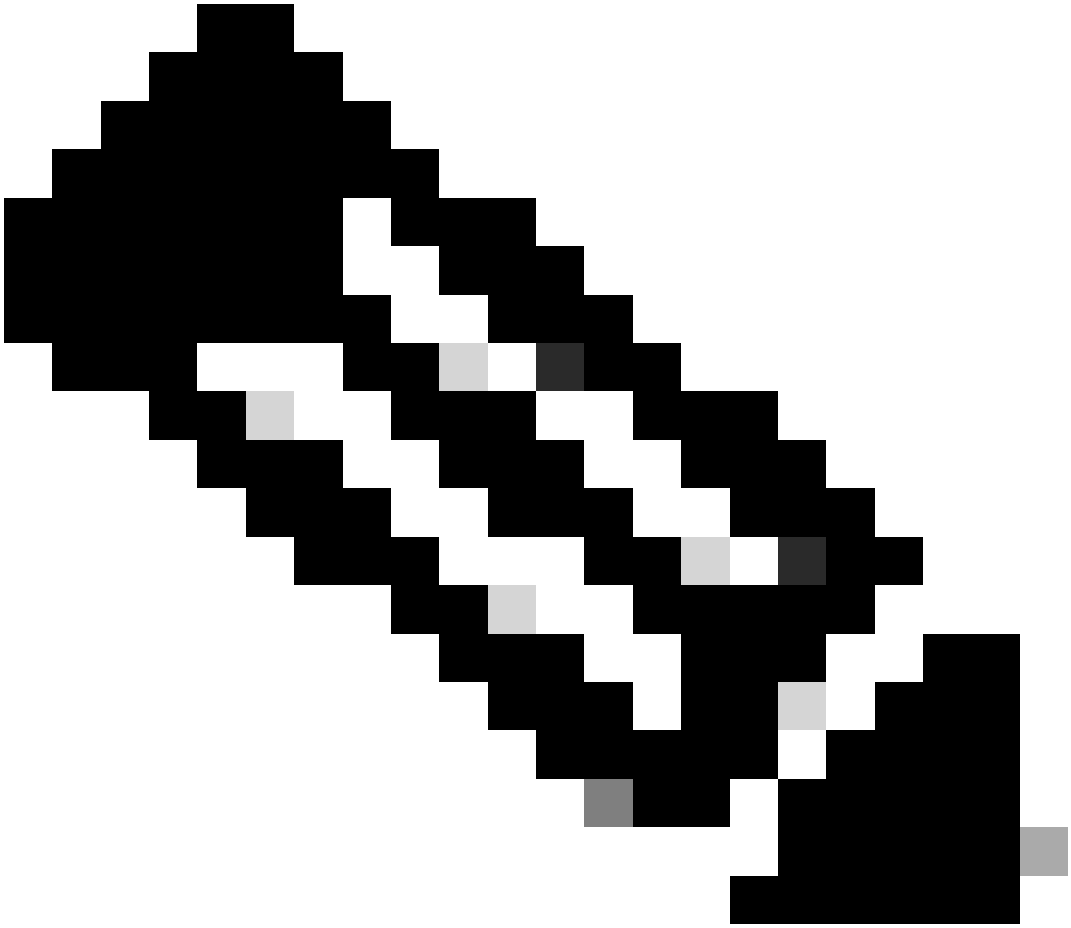
4409322363924

Web使用者識別

預設情況下，不能針對每個使用者或組控制遠端訪問流量。 相同的策略適用於基於「遠端訪問規則

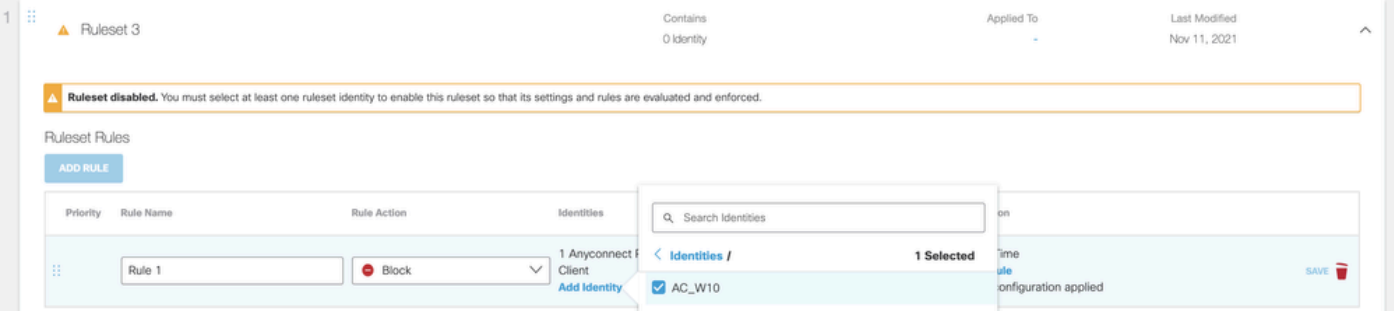
」標識的所有RA流量。要新增使用者/組標識，您有兩個選項：

- 安裝AnyConnect Umbrella漫遊安全模組並啟用SWG代理功能。代理將Web流量直接傳送到Umbrella SWG，並應用「漫遊電腦」身份。此模組還支援可選的AD使用者標識。
- 在影響「遠端訪問規則」標識的Web規則集中啟用SAML。連線到遠端訪問後，在生成Web瀏覽器流量時，將再次提示RA使用者通過SAML進行身份驗證。



附註：使用Umbrella模組進行AnyConnect時，根據分割隧道配置，可以選擇在隧道內部或外部傳送SWG流量。

此示例顯示如何為單個AnyConnect客戶端配置DNS策略(Policies > DNS Policies) — 僅當部署了Umbrella AnyConnect漫遊模組時才能進行配置：

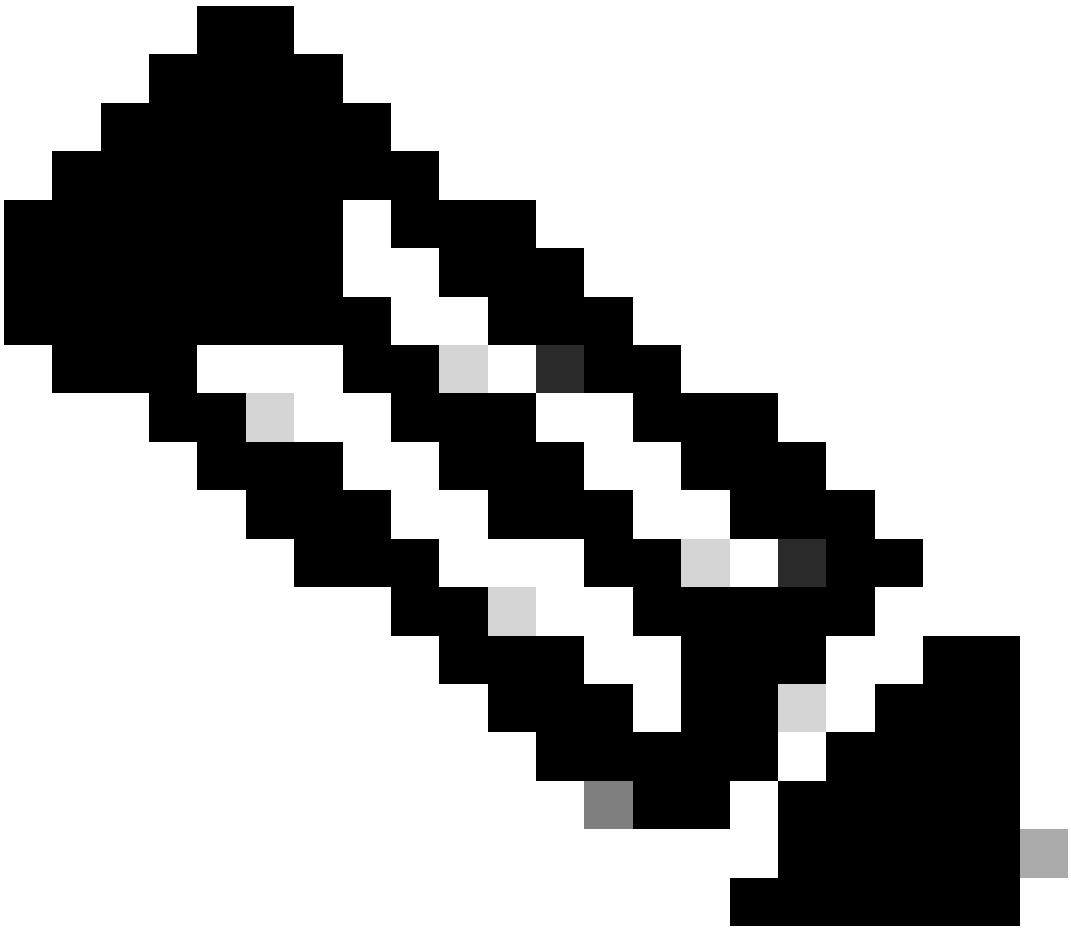


4410210499476

DLP策略

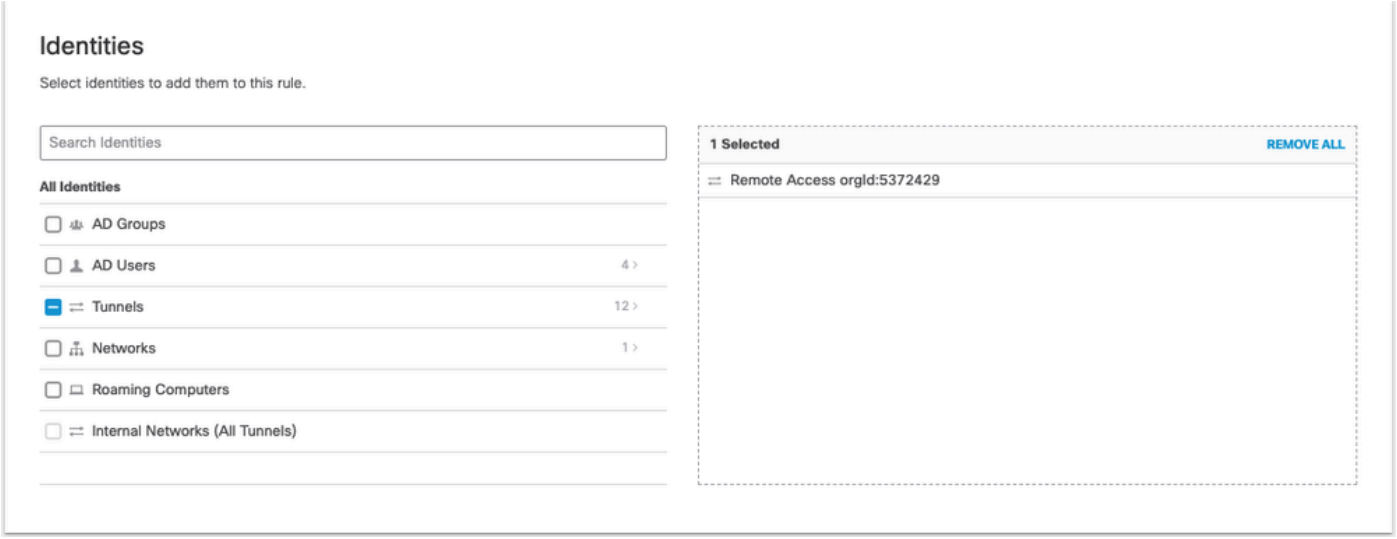
資料丟失策略適用於遠端訪問(AnyConnect)客戶端和網際網路之間的流量。根據以下文檔配置「部署>資料丟失防護策略」中的規則：管理資料保護策略。

- DLP策略不用於控制RA客戶端和專用/分支Web伺服器之間的訪問。 DLP策略僅適用於流量外部網站。



附註：要應用DLP策略，您必須首先為遠端訪問使用者建立了一個Web規則集。Web規則集必須啟用HTTPS解密。

為資料保護規則選擇標識時，請選擇Remote Access orgid:<ID>。相同的資料保護策略適用於所有使用者。要完成DLP規則，您還需要選擇或定義DLP分類器。



4409322428820

DLP使用者標識

DLP從安全Web網關（Web策略）獲取使用者身份。 有關如何新增使用者標識的說明，請參閱Web策略部分。

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）。