

配置DNS隧道VPN安全類別

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[開啟DNS隧道VPN](#)

簡介

本文檔介紹如何在Umbrella中配置DNS隧道VPN安全類別。

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Umbrella DNS。

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

DNS隧道VPN將與與DNS隧道VPN服務關聯的伺服器分類到可以阻止或允許並報告的安全類別下。這些服務允許終端使用者將傳出流量偽裝為DNS查詢，從而可能違反可接受的使用、資料丟失預防或安全策略。因此，這些服務會帶來潛在的安全威脅，並降低您環境中的整體可視性。

通過此安全類別提供即時可視性，您可以減少DNS隧道風險以及潛在的資料丟失。您可以完全阻止此類別，或僅監控報告中的結果；這可以讓您靈活地確定什麼才是解決問題的正確方法，具體取決於您的風險承受能力、可接受的使用或人力資源政策。

開啟DNS隧道VPN

可以像在Policies > Security Settings下啟用任何其他安全類別，然後編輯現有安全設定。或者，可以在策略配置嚮導本身中完成：

Setting Name

Default Settings

- Malware**
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more
- Newly Seen Domains**
Domains that have become active very recently. These are often used in new attacks.
- Command and Control Callbacks**
Prevent compromised devices from communicating with attackers' infrastructure
- Phishing Attacks**
Fraudulent websites that aim to trick users into handing over personal or financial information
- Dynamic DNS**
Block sites that are hosting dynamic DNS content
- Potentially Harmful Domains**
Domains that exhibit suspicious behavior and may be part of an attack.
- DNS Tunneling VPN**
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.

CANCEL

SAVE

115014823666

可以通過Activity Search報告來過濾DNS隧道：

Security Categories

Select All

- Command and Control
- Malware
- Phishing
- Unauthorized IP Tunnel Access
- Newly Seen Domains
- Potentially Harmful
- DNS Tunneling VPN**

APPLY

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）。