如何在Secure Web裝置上阻止未知應用程式

目錄

簡介

本文檔介紹在Cisco Secure Web Appliance上阻止未知應用的幾種方法。

阻止未知應用程式的方法

您可以單獨或組合使用這些方法。

> **附註**：本知識庫文章所參考的軟體不是思科維護或支援的。此資訊出於方便而提供。如需更多幫助，請與軟體供應商聯絡。

根據使用者代理字串阻止應用程式

第一種防禦是使用使用者代理字串來阻止未知應用程式。

- 在下方新增使用者代理 **Web Security Manager** > **Access Policies** > **Protocols and User Agents** 列<表示所需的訪問策略>。
- 在下方新增使用者代理字串 **Block Custom User Agents** （每行一個）。

> **附註**：您可以使用參考下提供的連結搜尋使用者代理。

根據應用可視性控制阻止應用

如果啟用了應用可視性控制(AVC)(位於 **GUI** > **Security Services** > **Web Reputation and Anti-Malware**)，然後可以根據應用程式型別（如代理、檔案共用、Internet實用程式等）阻止訪問。你可以在 **Web Security Manager** > **Access Policies** > **Applications** 列<表示所需的訪問策略>。

根據MIME型別阻止應用程式

如果使用者代理不存在，您可以嘗試新增多用途Internet郵件擴展(MIME)型別：

- 新增MIME型別 **Web Security Manager** > **Web Access Policies** > **Objects** 列<表示所需的訪問策略>。
- 在 **Block Custom MIME Types** 部分（每行一個）。 例如，要阻止BitTorrent應用程式，請輸入 application/x-bittorrent.

附註：您可以使用參考下提供的連結搜尋MIME型別。

阻止訪問策略中的URL類別

確保在訪問策略中阻止過濾規避、非法活動、非法下載等類別。如果某些應用程式使用已知的URL或IP地址進行連線，則可以阻止其關聯的預定義URL類別，或使用其IP地址、完全限定域名(FQDN)或與域匹配的正規表示式在受阻的自定義URL類別中配置它們。你可以在 **Web Security Manager > Access Policies > URL Categories** 列。

限制訪問策略中的HTTP CONNECT埠配置

某些應用程式可以使用HTTP CONNECT方法連線到不同的埠。在HTTP CONNECT埠配置域中，僅允許您的環境中所需的已知埠或特定埠：

- 可在 **Web Security Manager** > **Access Policies** > **Protocols and User Agents** 列<表示所需的訪問策略>。
- 新增允許的埠 **HTTP CONNECT Ports**.

阻止特定IP地址的訪問

對於您只知道要訪問的目標IP地址的應用程式，您可以使用L4流量監控功能阻止這些特定IP地址的訪問。可以在下面新增目標IP **Web Security Manager > L4 Traffic Monitor > Additional Suspected Malware Addresses**.

如何查詢應用程式使用的使用者代理或MIME型別

如果您不知道某些應用程式正在使用哪種使用者代理或MIME型別，則可以執行以下任一步驟來查詢此資訊：

- 在客戶端電腦上使用WireShark(Ethereal)運行資料包捕獲並過濾「http」協定。
- 在Secure Web Appliance上運行捕獲(位於 **Support and Help** > **Packet Capture**)，根據客戶端的IP地址進行過濾。

參考

附註：此處所列的外部網站僅供參考。連結和內容不受思科控制，並且可能更改。

使用者代理清單

使用者代理String.Com(位於useragentstring.com)

MIME型別清單

- 常見MIME型別(位於mozilla.org)
- MIME型別：MIME型別的完整清單(位於w3cub.com)
- MIME型別的完整清單(位於sitepoint.com)