配置Cisco ASA Shun功能以免除虛擬裝置

目錄

簡介

本文檔介紹如何配置Cisco ASA以使虛擬裝置免受威脅檢測元件的威脅。Cisco ASA威脅檢測元件對DNS和其他協定執行資料包檢測。Umbrella支援建議對以下ASA配置進行更改，以防止此功能與我們的虛擬裝置發生衝突：

- 如本文所述，免除Virtual Appliance的威脅檢測「shun」功能。
- 免除對Virtual Appliance進行DNS資料包檢查，以允許我們的DNS加密(DNScrypt)，這將在本文中介紹：Cisco ASA防火牆阻止DNS加密。

威脅檢測「Shun」功能

啟用「Shun」功能後，ASA可以完全阻止觸發威脅檢測規則的源IP地址。更多詳細資訊請參閱思科文章：[ASA威脅檢測功能和配置](#)。

虛擬裝置通常向Umbrella DNS解析器傳送大量的DNS查詢。在連線到解析器時出現本地問題（例如臨時網路中斷/延遲）的情況下，這些查詢可能會失敗。由於傳送的查詢數量龐大，即使只有一小部分發生故障，也會導致ASA迴避虛擬裝置；這會導致在一段時間內完全DNS中斷。

免除虛擬裝置

附註：本文中的命令僅作為指導說明，建議您在更改生產環境之前諮詢思科專家。

通過CLI:

- 要免除避開裝置IP，請運行以下命令： **no shun**

通過ASDM介面：

- 選擇Configuration > Firewall > Threat Detection窗格。
- 要免除避開裝置IP地址，請在「排除的網路」欄位中輸入一個地址。可以輸入多個地址或子網，用逗號分隔。

確定裝置是否已「迴避」

如果沒有執行這些步驟，裝置可能會在某些情況下變得「迴避」，從而導致DNS中斷。

當Virtual Appliance沒有外部連線時，Cisco ASA控制檯按以下方式記錄事件：

4|2014年6月06日14:00:42|401004:被避開的資料包：192.168.1.3 ==> 208.67.222.222 on interface inside
4|2014年6月06日14:00:42|401004:迴避的資料包：192.168.1.3 ==> 208.67.222.222（位於內部介面上）

要檢視當前規避的IP地址清單，請在ASA上運行以下命令： **show shun**

要立即清除當前規避的IP地址，請在ASA上運行以下命令： **clear shun**

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）。