在FTD訪問控制策略中使用基本域不匹配子域對FQDN對象進行故障排除(&n)

目錄

問題

在思科防火牆威脅防禦(FTD)訪問控制策略中配置完全限定域名(FQDN)對象時，基本域條目不會自動與子域匹配。例如，在建立允許配置為「example.com」的目標對象的策略時，將阻止子域「maps.example.com」，而不是允許通過同一策略規則。此行為引發了以下問題：基本域是否可用作所有子域的萬用字元，以及在FTD策略中實施萬用字元FQDN匹配的正確配置方法是什麼？

環境

- FTD版本7.2。其他版本也可能會受到影響。
- FMC 7.2版。其他版本也可能會受到影響。
- 在訪問控制策略中配置的FQDN對象。

解析

- 觀察到的行為是FQDN對象的預期操作。
- 在Cisco FMC中，FQDN對象設計為匹配準確的域名，並且不會自動用作子域的萬用字元。
- 要正確配置子域匹配，必須使用URL過濾和URL條件而不是FQDN對象。

配置子域匹配的URL過濾

要匹配FMC中的域及其所有子域，請使用以下配置步驟：

步驟1.導航到訪問控制策略規則配置

在FMC中，導航到Policies > Access Control > Access Control Policy > [Your Policy Name] > Rules。

步驟2.建立或編輯訪問控制規則

建立新規則或編輯要實施子域匹配的現有訪問控制規則。

步驟3.配置URL條件

在規則配置中，新增URL條件而不是使用FQDN對象。配置URL條件以包含具有匹配子域的相應萬用字元語法的基域。

步驟4.應用URL過濾策略

確保在訪問控制策略中啟用並正確配置URL過濾以有效處理URL條件。

步驟5.部署配置

將配置更改部署到目標FTD裝置，以實施子域匹配功能。

備用配置方法

如果URL過濾不適用於特定使用情形，請考慮為每個需要顯式匹配的子域建立多個FQDN對象，或者使用具有IP地址範圍的網路對象（如果域解析為可預測的IP地址空間）。

原因

Cisco FMC中的FQDN對象設計為執行精確的域名匹配，而不是萬用字元匹配。這是系統的預期行為。FQDN對象功能不包括隱式子域匹配功能，此功能需要使用URL過濾條件來實現所需的子域匹配行為。

相關內容

- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214698-understand-fqdn-feature-on-firepower-thr.html
- https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/214505-configure-fqdn-based-object-for-access-c.html
- 思科錯誤ID CSCwf000588
- 思科技術支援與下載

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）。