在SG200/300系列代管交換器上防止ICMP巨型訊框

目標

本文的目的是解釋為什麼SG200和SG300系列交換器會防止某些ICMP巨型訊框並允許其他巨型訊框在交換器上通過。本文說明一些問題是由於ICMP巨型幀。本文還說明了什麼是拒絕服務(DoS)攻擊，以及它與ICMP巨型幀的關係。

適用裝置

· SG200
· SG300

交換器上的ICMP巨型訊框

以下說明什麼是巨型幀，以及為什麼在SG200和SG300系列交換機上不允許ICMP巨型幀。

巨量訊框

千兆乙太網交換機（SG200和SG300系列）和快速乙太網交換機（SF200系列交換機）支援巨型幀。巨型幀是擴展乙太網幀，其大小從標準1,518位元組到9,000位元組不等。因此，巨型幀通過每幀傳送更多資料來提高資料傳輸速度，從而減少了報頭的開銷。

網際網路控制訊息通訊協定 (ICMP)

ICMP是一個網路層協定，屬於Internet協定套件的一部分，用於生成ICMP消息以響應IP資料包中的錯誤或用於診斷或路由目的。ICMP錯誤始終報告給源資料包的原始源IP地址。儘管該協定對於確保正確的資料分發非常重要，但惡意使用者可能會利用它進行不同的拒絕服務(DoS)攻擊。

DoS攻擊使網路和伺服器資源不可用或無法響應合法使用者，因為網路中存在大量虛假流量。使用暴力進行的DoS攻擊會向伺服器傳送大量流量，從而消耗伺服器和網路頻寬。以下是使用ICMP的常見DoS攻擊型別。

· ICMP Ping泛洪攻擊 — 在ICMP Ping泛洪攻擊中，該攻擊通常使用來自主機的ping命令向目標系統傳送大量ping資料包。這樣，被攻擊的系統就無法對合法流量做出響應。

· ICMP Smurf攻擊 — ICMP Smurf攻擊使用偽裝ping資料包泛洪受害者電腦。這些是經過修改的資料包，其中包含目標受攻擊者的偽裝IP地址。這會導致將錯誤資訊廣播給本地網路中的所有主機。這些主機都向目標系統傳送應答，而目標系統則被應答淹沒。如果使用的網路中有很多主機，則被攻擊主機將被大量通訊量有效地欺騙。

注意：IP欺騙是指使用偽造源IP地址的IP資料包，其目的是隱藏傳送方的資訊。

·死亡的Ping — 在死亡的Ping攻擊中，攻擊者向受害者傳送一個大於最大IP資料包大小65.536位元組的ICMP回應請求資料包。由於收到的ICMP回應請求資料包大於正常IP資料包大小，因此必須將其分段。因此，受害者無法重組資料包，因此作業系統崩潰或重新啟動。

· ICMP核攻擊 — 在此類攻擊中，核通過包含型別3的目標無法到達消息的ICMP資料包傳送到受害者。此攻擊的結果是目標系統中斷與現有連線的通訊。

在SG200和SG300系列交換機中，拒絕服務防禦使網路管理員能夠配置阻止某些ICMP資料包。預設情況下，由於許多網路攻擊（例如DoS）使用ICMP，因此會阻止某些ICMP巨型幀，因此，出於安全原因，這些交換機的防火牆會阻止ICMP巨型幀。這會導致必要的ICMP分段和DF設定訊息無法到達傳送者。因此，傳送方沒有資訊以較小的規模傳送其資料包，也沒有獲得TCP確認其資料包是否成功。隨後，傳送方繼續以同樣大的大小重新傳送幀，但幀始終無法到達目的地，從而導致被稱為「黑洞」的情況。

使用Web配置實用程式配置巨型幀，然後選擇Port management > Port Settings，然後選擇Security > Denial of Service Prevention > Security Suite Settings以配置DoS防護。

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）。