定義防止TCP SYN拒絕服務攻擊的策略

目錄

摘要

以網路裝置為目標的網際網路服務提供商(ISP)可能會受到拒絕服務攻擊。

- **TCP SYN攻擊**:傳送方傳送無法完成的連線數量。這會導致連線隊列填滿，從而拒絕為合法TCP使用者提供服務。

本文包含有關潛在TCP SYN攻擊發生方式的技術說明，以及使用Cisco IOS軟體防禦該攻擊的建議方法。

注意：Cisco IOS 11.3軟體具有主動防止TCP拒絕服務攻擊的功能。設定TCP攔截（防止拒絕服務攻擊）檔案中介紹了此功能。

必要條件

需求

本文件沒有特定先決條件。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

問題描述

TCP SYN攻擊

正常TCP連線啟動時，目的主機收到來自源主機的SYN（同步/啟動）資料包，並傳送回SYN ACK（同步確認）。 在建立連線之前，目的主機必須收到SYN ACK的ACK（確認）。這稱為「TCP三次握手」。

在等待SYN ACK的ACK時，目標主機上的有限大小的連線隊列會跟蹤等待完成的連線。此隊列通常會快速清空，因為ACK預計在SYN ACK後幾毫秒內到達。

TCP SYN攻擊利用這種設計讓攻擊源主機生成帶有隨機源地址的TCP SYN資料包來攻擊受攻擊主機。受害目的主機將SYN ACK傳送回隨機源地址，並向連線隊列新增一個條目。由於SYN ACK的目的地是不正確或不存在的主機，因此「三次握手」的最後一部分永遠不會完成，該條目將保留在連線隊列中，直到計時器超時（通常大約一分鐘）。通過快速從隨機IP地址生成虛假的TCP SYN資料包，可以填滿連線隊列並拒絕TCP服務（如電子郵件、檔案傳輸或WWW）給合法使用者。

由於來源的IP地址是偽造的，因此沒有簡單的方法來跟蹤攻擊的發起者。

此問題的外部表現包括無法獲取電子郵件、無法接受與WWW或FTP服務的連線，或者主機上的大量TCP連線處於SYN_RCVD狀態。

防禦對網路裝置的攻擊

防火牆背後的裝置

TCP SYN攻擊的特點是從隨機源IP地址湧入SYN資料包。阻止入站SYN資料包的防火牆後面的所有裝置都已受到保護，不會受到此攻擊模式的攻擊，無需執行進一步的操作。防火牆的示例包括思科專用網際網路交換(PIX)防火牆或配置了訪問清單的思科路由器。有關如何在Cisco路由器上設定存取清單的範例，請參閱增加IP網路上的安全性的檔案。

提供公共服務的裝置（郵件伺服器、公共Web伺服器）

防止來自隨機IP地址對防火牆後裝置進行SYN攻擊相對簡單，因為您可以使用訪問清單明確地將入站訪問限制到選定的幾個IP地址。但是，在面向網際網路的公共Web伺服器或郵件伺服器的情況下，無法確定哪些傳入IP源地址是友好地址還是不友好地址。因此，對於來自隨機IP地址的攻擊，沒有明確的防禦措施。主機可使用以下幾種選項：

- 增加連線隊列的大小（SYN ACK隊列）。
- 減少等待三次握手的超時時間。
- 使用供應商軟體修補程式來檢測和規避問題（如果可用）。

您應該聯絡主機供應商，看他們是否建立了特定修補程式來解決TCP SYN ACK攻擊。

注意：在伺服器上過濾IP地址無效，因為攻擊者可以更改其IP地址，並且地址可能與合法主機的地址相同，也可能不同。

防止網路在不知不覺中發動攻擊

由於此拒絕服務攻擊的主要機制是產生源自隨機IP地址的流量，因此我們建議過濾目的地為Internet的流量。基本概念是在資料包進入Internet時丟棄其源IP地址無效的資料包。這不會阻止對您的網路的拒絕服務攻擊，但可以幫助受攻擊方排除您的位置作為攻擊者的來源。此外，它還會使您的網路作為此類攻擊基礎的吸引力下降。

阻止傳輸無效IP地址

通過在將您的網路連線到Internet的路由器上過濾資料包，您可以僅允許具有有效源IP地址的資料包離開您的網路並進入Internet。

例如，如果您的網路由網路172.16.0.0組成，並且您的路由器使用串列0/1介面連線到ISP，則可以應用訪問清單，如下所示：

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 0/1
ip access-group 111 out
```

注意：訪問清單的最後一行確定是否有任何帶有無效源地址的流量進入Internet。使用這條線路並不重要，但有助於確定可能攻擊的來源。

阻止接收無效IP地址

對於向終端網路提供服務的ISP，我們強烈建議驗證來自您客戶端的傳入資料包。這可以通過在邊界路由器上使用入站資料包過濾器來實現。

例如，如果客戶端通過名為「serial 1/0」的串列介面將以下網路號連線到路由器，則可以建立以下訪問清單：

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0.

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 1/0
ip access-group 111 in
```

注意：訪問清單的最後一行確定是否有任何源地址無效的流量進入Internet。這條線並不重要，但有助於確定可能攻擊的來源。

本主題已經在NANOG（北美網路運營商1s組）郵件清單中進行了一些詳細討論。存檔清單位於：http://www.merit.edu/mail.archives/nanog/index.html

有關TCP SYN拒絕服務攻擊和IP欺騙的詳細說明，請參閱：http://www.cert.org/advisories/CA-

1996-21.html

http://www.cert.org/advisories/CA-1995-01.html

相關資訊

- 技術支援 - Cisco Systems