Cisco IOS經典防火牆/IPS:設定內容型存取控制(CBAC)以進行拒絕服務保護

目錄

簡介

本檔案介紹使用CBAC的Cisco IOS® Classic Firewall中拒絕服務(DoS)引數的最佳化程式。

CBAC提供進階流量過濾功能，並可用作網路防火牆的組成部分。

DoS通常是指有意或無意地使網路資源（例如WAN鏈路頻寬、防火牆連線表、終端主機記憶體、CPU或服務功能）不堪重負的網路活動。在最壞的情況下，DoS活動會淹沒易受攻擊（或目標的）資源，導致資源不可用，並且會禁止對合法使用者進行WAN連線或服務訪問。

如果思科IOS防火牆在傳統防火牆(ip inspect)和基於區域的策略防火牆中維護「半開放」TCP連線數計數器，以及通過防火牆和入侵防禦軟體的總連線速率，則有助於緩解DoS活動。

必要條件

需求

本文件沒有特定需求。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

半開放連線是指尚未完成三向SYN-SYN/ACK-ACK握手的TCP連線，TCP對等體始終使用三次握手來協商其相互連線的引數。大量半開放連線可能表示惡意活動，例如DoS或分散式拒絕服務(DDoS)攻擊。某種DoS攻擊的示例是由惡意軟體（例如蠕蟲或病毒）故意開發的，這些軟體會感染Internet上的多個主機，並試圖使用SYN攻擊將特定的Internet伺服器壓垮，其中Internet或組織專用網路中的多個主機向伺服器傳送大量SYN連線。SYN攻擊會對Internet伺服器造成危害，因為伺服器的連線表可能會載入「偽造」的SYN連線嘗試，這些嘗試的到達速度比伺服器處理新連線的速度更快。這是一種DoS攻擊，因為受害者伺服器的TCP連線清單中的大量連線阻止了合法使用者訪問受害者Internet伺服器。

Cisco IOS防火牆還將只具有一個方向流量的使用者資料包通訊協定(UDP)作業階段視為「半開放」，因為許多使用UDP進行傳輸的應用程式會確認資料已接收。沒有返回流量的UDP作業階段可能表示DoS活動或兩台主機之間的連線（其中一個主機已無回應）。許多型別的UDP流量（如日誌消息、SNMP網路管理流量、流語音和影片媒體以及信令流量）都只使用單向流量來傳輸其流量。其中許多型別的流量應用特定於應用的智慧，以防止單向流量模式對防火牆和IPS DoS行為產生負面影響。

在Cisco IOS軟體版本12.4(11)T和12.4(10)之前，Cisco IOS狀態資料包檢測在應用檢測規則時，預設提供對DoS攻擊的防護。Cisco IOS軟體版本12.4(11)T和12.4(10)修改了預設DoS設定，因此不會自動應用DoS保護，但連線活動計數器仍然處於使用中。當DoS保護處於活動狀態時（即，在較舊軟體版本上使用預設值，或者將值調整為影響流量的範圍），將在應用檢查的介面上（在應用防火牆的方向上）啟用DoS保護，以便防火牆策略配置協定進行檢查。只有當流量進入或離開某個介面，並且在TCP連線或UDP會話的初始流量（SYN資料包或第一個UDP資料包）的相同方向上應用檢查時，才會對網路流量啟用DoS保護。

Cisco IOS防火牆檢查提供多個可調整的值，以防止DoS攻擊。12.4(11)T和12.4(10)之前的Cisco IOS軟體版本具有預設的DoS值，如果沒有在連線速率超過預設值的網路中針對適當的網路活動層級進行設定，這些值可能會干擾適當的網路運作。通過這些引數，可以配置防火牆路由器的DoS保護開始生效的點。當路由器的DoS計數器超過預設或配置的值時，路由器將為超出配置的max-incomplete或1分鐘高值的每個新連線重置一個舊的半開放連線，直到半開放會話數下降至max-incomplete低值以下。如果啟用了日誌記錄，並且路由器上配置了入侵防禦系統(IPS)，則路由器會傳送系統日誌消息，防火牆路由器會通過安全裝置事件交換(SDEE)傳送DoS簽名消息。 如果不根據網路的正常行為調整DoS引數，正常的網路活動可能會觸發DoS保護機制，從而導致應用故障、網路效能變差以及Cisco IOS防火牆路由器上的CPU使用率高。

設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

適用於Cisco IOS軟體傳統(IP Inspect)防火牆和入侵防禦系統的拒絕服務調整

傳統Cisco IOS防火牆為路由器維護一組全域性DoS計數器，並且所有介面上所有防火牆策略的所有防火牆會話都應用於該組防火牆計數器。

在應用傳統防火牆時，Cisco IOS傳統防火牆檢測預設提供對DoS攻擊的防護。對於防火牆策略配置為檢查的每個服務或協定，在應用防火牆的方向的所有應用檢查的介面上啟用DoS保護。Classic Firewall提供多個可調整的值，以防止DoS攻擊。表1中顯示的傳統預設設定(來自版本12.4(11)T之前的軟體映像)如果未針對連線速率超過預設值的網路中的適當網路活動級別進行配置，則可能會干擾正確的網路操作。可以使用exec命令**show ip inspect config**檢視DoS設定，這些設定包含在**sh ip inspect all**的輸出中。

CBAC使用超時和閾值來確定管理會話狀態資訊的時間，以及確定何時丟棄未完全建立的會話。這些超時和閾值全域性應用於所有會話。

表1傳統防火牆預設DoS保護限制		
DoS保護價值	**12.4(11)T/12.4(10)之前**	**12.4(11)T/12.4(10)及更高版本**
max-incomplete high *value*	500	無限制
max-incomplete low *value*	400	無限制
一分鐘高*值*	500	無限制
一分鐘低*值*	400	無限制
tcp max-incomplete host *value*	50	無限制

配置為應用Cisco IOS VRF感知防火牆的路由器為每個VRF維護一組計數器。

「ip inspect one-minute high」和「ip inspect one-minute low」的計數器在路由器操作的前一分鐘內維護所有TCP、UDP和網際網路控制消息協定(ICMP)連線嘗試的總和，無論連線是否成功。連線速率上升可能表示專用網路上的蠕蟲感染或試圖對伺服器進行DoS攻擊。

雖然不能「停用」防火牆的DoS保護，但您可以調整DoS保護，使其不會生效，除非防火牆路由器的會話表中存在大量半開放連線。

DoS防火牆保護

請按照以下步驟將防火牆的DoS保護調整為網路活動：

1. 請確保您的網路未感染病毒或蠕蟲，這些病毒或蠕蟲可能導致錯誤的半開放連線值或嘗試的連線速率。如果您的網路不是「乾淨」的，則無法正確調整防火牆的DoS保護。您必須觀察網路在正常活動週期內的活動。如果在網路活動不足或空閒的一段時間內調整網路的DoS保護設定，正常活動級別可能會超過DoS保護設定。
2. 將max-incomplete high值設定為非常高的值：

```
ip inspect max-incomplete high 20000000
ip inspect one-minute high 100000000
ip inspect tcp max-incomplete host 100000 block-time 0
```

這可以防止路由器在您觀察網路的連線模式時提供DoS保護。如果您希望禁用DoS保護，請立

即停止此過程。**注意：**如果路由器運行Cisco IOS軟體版本12.4(11)T或更高版本，或者12.4(10)或更高版本，則無需提高預設DoS保護值；預設情況下，它們已設定為最大限制。**注意：如果要啟用更具攻擊性的TCP主機特定的拒絕服務防**御（包括阻止對主機的連線啟動），則必須設定**ip inspect tcp max-incomplete host命令中指定的阻止時**間

3. 使用以下命令清除Cisco IOS防火牆統計資訊：

```
show ip inspect statistics reset
```

4. 將路由器保持此狀態一段時間，可能長達24至48小時，這樣您便可以在正常網路活動週期內至少一天觀察網路模式。**注意：**雖然將值調整到非常高的水準，但您的網路無法受益於Cisco IOS防火牆或IPS DoS保護。
5. 觀察期後，使用以下命令檢查DoS計數器：

```
show ip inspect statistics
```

要調整DoS保護，必須觀察的引數以粗體突出顯示:

```
Packet inspection statistics
   [process switch:fast switch]
  tcp packets: [218314:7878692]
  udp packets: [501498:65322]
   packets: [376676:80455]
   packets: [5738:4042411]
  smtp packets: [11:11077]
  ftp packets: [2291:0]
Interfaces configured for inspection 2
Session creations since subsystem
   startup or last reset 688030
Current session counts
   (estab/half-open/terminating) [0:0:0]
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
Last session created 00:00:05
Last statistic reset never
Last session creation rate 1
Maxever session creation rate 330
Last half-open session total 0
TCP reassembly statistics
  received 46591 packets out-of-order; dropped 16454
  peak memory usage 48 KB; current usage: 0 KB
  peak queue length 16
```

6. 將**ip inspect max-incomplete high**配置為比路由器指定的maxever session count half-open值高25%。1.25乘數比觀察到的行為增加25%的空間，例如：

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
56 * 1.25 = 70
```

設定:

```
router(config)
   #ip inspect max-incomplete high 70
```

注意：本文檔介紹使用倍數1.25倍的網路典型活動來設定實施DoS保護的限制。如果您在典型網路活動高峰期觀察網路，則必須提供足夠的預留空間，以避免在除了非典型情況以外的所有情況下啟用路由器的DoS保護。如果您的網路定期發現超過此值的合法網路活動大量爆發，路由器會使用DoS保護功能，這會對一些網路流量產生負面影響。您必須監控路由器日誌以檢測DoS活動，並在確定限制是合法網路活動導致的後，調整**ip inspect max-incomplete high**和/或**ip inspect one-minute high**限制以避免觸發DoS。可以通過以下日誌消息的存在來識別DoS保

護應用程式：

7. 將**ip inspect max-incomplete low**設定為路由器顯示的最大作業階段計數半開放值的值，例如：

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
```

設定:

```
router(config)
   #ip inspect max-incomplete low 56
```

8. **ip inspect one-minute high**和**one-minute low**計數器會維護路由器操作之前一分鐘內所有TCP、UDP和網際網路控制訊息通訊協定(ICMP)連線嘗試的總和，無論連線是否成功。連線速率上升可能表示專用網路上的蠕蟲感染或試圖對伺服器進行DoS攻擊。在12.4(11)T和12.4(10)的**show ip inspect statistics**輸出中新增了附加檢查統計資訊，以揭示會話建立率的高水位線。如果運行的Cisco IOS軟體版本低於12.4(11)T或12.4(10)，則檢查統計資訊不包含以下行：

```
Maxever session creation rate [value]
```

12.4(11)T和12.4(10)之前的Cisco IOS軟體版本不維護檢查maxever一分鐘連線速率的值，因此您必須根據觀察的「maxever會話計數」值計算應用的值。對幾個在生產中使用對Cisco IOS防火牆版本12.4(11)T的狀態檢測網路的觀察表明，Maxever會話建立速率往往會超過「maxever會話計數」中三個值（已建立、半開放和終止）的總和大約10%。為了計算ip inspect one-minute low value，請將指示的「established」值乘以1.1，例如：

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
(207 + 56 + 35) * 1.1 = 328
```

設定:

```
ip inspect one-minute low 328
```

如果路由器執行Cisco IOS軟體版本12.4(11)T或更新版本，或12.4(10)或更新版本，只需套用「Maxever session creation rate」檢查統計資訊中顯示的值：

```
Maxever session creation rate 330
```

設定:

```
ip inspect one-minute low 330
```

9. 計算和配置**ip inspect一分鐘高**。ip inspect one-minute high值必須比計算得出的1-minute low值大25%，例如：

```
ip inspect one-minute low (330) * 1.25 = 413
```

設定:

```
ip inspect one-minute high 413
```

注意：本文檔介紹使用倍數1.25倍的網路典型活動來設定實施DoS保護的限制。如果您在典型網路活動高峰期觀察網路，則必須提供足夠的預留空間，以避免在除了非典型情況以外的所有情況下啟用路由器的DoS保護。如果您的網路定期發現超過此值的合法網路活動大量爆發，路由器會使用DoS保護功能，這會對一些網路流量產生負面影響。您必須監控路由器日誌以檢測DoS活動，並在確定限制是合法網路活動導致的後，調整**ip inspect max-incomplete high**和/或**ip inspect one-minute high**限制以避免觸發DoS。可以通過以下日誌消息的存在來識別DoS保護應用程式：

10. 您需要根據您對伺服器功能的瞭解，定義**ip inspect tcp max-incomplete host**的值。本文檔無法提供每主機DoS保護配置的指導原則，因為此值因終端主機硬體和軟體效能而有很大差異。如果您不確定要為DoS保護配置的適當限制，則實際上有兩個用於定義DoS限制的選項：較好的選項是將基於路由器的每主機DoS保護配置為高值（小於或等於最大值4,294,967,295），並應用每台主機的作業系統或基於主機的外部入侵保護系統(如思科安全代理(CSA))提供的主機特定保護。檢查網路主機上的活動和效能日誌，並確定其最高持續連線速率。由於傳統防火牆僅提供一個全域性計數器，因此您必須應用所有網路主機檢查其最大連線速率後確定的最大值。仍建議您使用特定於作業系統的活動限制和基於主機的IPS（如

CSA）。**注意**：Cisco IOS防火牆針對針對特定作業系統和應用程式漏洞的定向攻擊提供有限保護。Cisco IOS防火牆的DoS保護不能保證對暴露於潛在惡意環境的終端主機服務進行保護。

11. 監控網路的DoS保護活動。理想情況下，您必須使用系統日誌伺服器，或者最好使用思科監控和報告站(MARS)來記錄DoS攻擊檢測事件。如果檢測非常頻繁，則需要監視和調整DoS保護引數。有關TCP SYN DoS攻擊的詳細資訊，請參閱定義防禦TCP SYN拒絕服務攻擊的策略。

驗證

目前沒有適用於此組態的驗證程序。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- **Cisco PIX防火牆軟體**
- **Cisco Secure PIX防火牆命令參考**
- **安全產品現場通知（包括PIX）**
- **要求建議 (RFC)**
- **技術支援與文件 - Cisco Systems**