在DOS攻擊期間使用CAR

目錄

簡介

有時，網路會收到拒絕服務(DoS)攻擊資料包流以及常規網路流量。在這種情況下，可以使用稱為「速率限制」的機制，使網路效能下降，從而使網路保持運行。您可以使用Cisco IOS®軟體透過以下方案實現速率限制：

- 承諾存取速率(CAR)
- 流量調節
- 透過模組化服務品質指令行介面(QoS CLI)進行調節和管制

本文討論用於DoS攻擊的CAR。其它方案只是基本概念的變體。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS軟體版本11.1CC和12.0 mainline，支援CAR。
- Cisco IOS軟體版本11.2和更新版本，支援流量調節。
- Cisco IOS軟體版本12.0XE、12.1E、12.1T，支援模組化QoS CLI。

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

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

速率限制ICMP/Smurf

設定以下存取清單：

```
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

```
interface <interface> <interface #>
  rate-limit input access-group 102 256000 8000 8000 conform-action transmit
  exceed-action drop
```

為了啟用CAR，您必須在機箱上啟用Cisco Express Forwarding(CEF)。此外，您必須為CAR配置CEF交換介面。

示例輸出使用DS3型別頻寬的頻寬值。根據介面頻寬和您想要限制特定流量型別的速率選擇值。對於較小的輸入介面，您可以配置較低的速率。

速率限制TCP SYN封包

11.1(X)CC

如果您知道哪台主機受到攻擊，請配置以下訪問清單：

```
access-list 103 deny tcp any host 10.0.0.1 established
!--- Let sessions in progress run. access-list 103 permit tcp any host 10.0.0.1 !--- Rate limit
the initial TCP SYN packet, because the other packets !--- in the TCP session would have hit the
earlier entry in the ACL. interface <interface> <interface #> rate-limit input access-group 103
8000 8000 8000 conform-action transmit exceed-action drop
```

注意：在本例中，受攻擊的主機是10.0.0.1。

如果您不知道哪台主機受到DoS攻擊，並且想要保護網路，請配置以下訪問清單：

```
access-list 104 deny tcp any any established
!--- Let sessions in progress run. access-list 104 permit tcp any any !--- Rate limit the
initial TCP SYN packet, because the other packets !--- in the TCP session would have hit the
earlier entry in the ACL. interface <interface> <interface #> rate-limit input access-group 104
64000 8000 8000 conform-action transmit exceed-action drop
```

註：所有TCP SYN資料包的速率限製為64000 bps。

12.0(X)[S/T/M]

如果您知道哪台主機受到攻擊，請配置以下訪問清單：

```
access-list 105 permit tcp any host 10.0.0.1 syn
!--- Remember that your interest lies in syn packets only. interface <interface> <interface #>
rate-limit input access-group 105 8000 8000 8000 conform-action transmit exceed-action drop
```

注意：在本例中，10.0.0.1是受攻擊的主機。

如果您不確定哪台主機受到攻擊，並希望保護網路，請配置以下訪問清單：

```
access-list 106 permit tcp any any syn
!--- Remember that your interest lies in syn packets only. interface <interface> <interface #>
rate-limit input access-group 106 64000 8000 8000 conform-action transmit exceed-action drop
```

註：所有TCP SYN資料包的速率限製為64000 bps。

CAR常見問題

如何識別用於限制SYN資料包速率的CAR規則的值？

瞭解您的網路。流量型別決定固定資料量的活動TCP會話數。

- WWW流量的TCP SYN資料包組合比FTP伺服器群流量高得多。
- PC使用者端堆疊傾向於至少確認每個其他TCP封包。其他堆疊可能較少或更頻繁地確認。
- 檢查是否需要在住宅使用者邊緣或客戶網路邊緣應用這些CAR規則。

```
users ---- { ISP } --- web farm
```

對於WWW，以下是流量組合：

對於從Web場下載的每個5k檔案，Web場將接收560位元組，如下所示：

- 80位元組[SYN， ACK]
- 400位元組[320位元組HTTP結構，2 ACK]
- 80位元組[FIN， ACK]

假定Web場的輸出流量和Web場的輸入流量之間的比率為10:1。組成SYN資料包的流量為120:1。

如果您有OC3鏈路，則將TCP SYN資料包速率限製為155 mbps / 120 == 1.3 mbps。

在Web場路由器的輸入介面上設定：

```
rate-limit input access-group 105 1300000 256000 256000 conform-action transmit
exceed-action drop
```

TCP SYN封包速率會隨著TCP作業階段長度的增加而變小。

```
users ---- { ISP } --- MP3/FTP Farm
```

MP3檔案的平均大小一般為4到5 mgbps。下載4 mgbps檔案會生成高達3160位元組的輸入流量：

- 80位元組[SYN， ACK]
- 3000位元組[ACK + FTP get]
- 80位元組[FIN， ACK]

TCP SYN輸出流量的速率是155 mbps / 120000 == 1.3 kbps。

設定:

```
 rate-limit input access-group 105 1300 1200 1200 conform-action transmit
exceed-action drop
```

如何知道是否限制了過多的SYN資料包？

如果您知道伺服器上通常的連線速率，可以比較啟用CAR之前和之後的數字。比較有助於識別連線速率下降的情況。如果發現速率下降，請增加CAR引數以允許更多會話。

檢查使用者是否能夠輕鬆地建立TCP會話。如果您的CAR限制過於嚴格，使用者需要多次嘗試建立TCP會話。

是否可在Gigabit交換器路由器(GSR)上啟用CAR?

會。引擎0和引擎1線卡支援CAR。Cisco IOS軟體版本11.2(14)GS2和更新版本提供CAR支援。CAR的效能影響取決於您應用的CAR規則的數量。

對引擎1線卡效能的影響也大於對引擎0線卡效能的影響。如果您要在引擎0線卡上啟用CAR，您必須知道思科錯誤ID CSCdp80432(僅限註冊客戶)。 如果要啟用CAR以限制多點傳播流量，請確保思科錯誤ID CSCdp32913(僅限註冊客戶)不會影響您。思科錯誤ID CSCdm56071(僅供註冊客戶使用)是啟用CAR前必須瞭解的另一個錯誤。

是否可在Cisco 7500上啟用分散式CAR(dCAR)?

是，RSP/VIP平台支援Cisco IOS軟體版本11.1(20)CC和所有12.0軟體版本中的dCAR。

CAR在一定程度上影響了效能。根據CAR配置，您可以通過OC3上的VIP2-50 [通過dCAR]實現線速[用於Internet混合流量]。請確保思科錯誤ID CSCdm56071(僅限註冊客戶)不會影響您。如果要使用輸出CAR，思科錯誤ID CSCdp52926(僅限註冊客戶)可能會影響您的連線。如果啟用dCAR，思科錯誤ID CSCdp58615(僅供註冊客戶使用)可能會導致VIP崩潰。

是否可在Cisco 7200上啟用CAR?

會。NPE支援Cisco IOS軟體版本11.1(20)CC和所有12.0軟體版本中的CAR。

基於CAR配置，CAR在一定程度上影響效能。取得這些錯誤的修正程式：思科錯誤ID CSCdm85458(僅限註冊客戶)和思科錯誤ID CSCdm56071(僅限註冊客戶)。

注意：介面/子介面中的大量CAR條目降低了效能，因為路由器需要對CAR語句執行線性搜尋，以查詢匹配的「CAR」語句。

其他功能和替代方案

IP接收ACL

Cisco IOS軟體版本12.0(22)S包含Cisco 12000系列網際網路路由器上的IP接收ACL功能。

IP接收ACL功能為目的地為到達路由器的流量提供基本過濾器。此功能可過濾輸入介面上的所有輸入存取控制清單(ACL)，因此路由器可以保護高優先順序路由通訊協定流量免受攻擊。IP接收ACL功能可在路由處理器接收封包之前過濾分散式線卡上的流量。此功能允許使用者過濾對路由器的拒絕服務(DoS)泛洪。因此，此功能可防止路由處理器的效能降低。

有關詳細資訊，請參閱IP接收APL。

IP來源追蹤器

Cisco IOS軟體版本12.0(21)S支援Cisco 12000系列網際網路路由器上的IP來源追蹤器功能。Cisco IOS軟體版本12.0(22)S在Cisco 7500系列路由器上支援此功能。

IP來源追蹤器功能可讓您收集有關流向懷疑受到攻擊的主機的流量的資訊。此功能還允許您輕鬆地跟蹤回網路入口點的攻擊。通過此功能識別網路入口點時，可以使用ACL或CAR有效地阻止攻擊。

如需詳細資訊，請參閱IP來源追蹤器。

相關資訊

- 如何保護您的網路免受Nimda病毒的侵擾
- IP接收APL
- IP來源追蹤器
- 技術支援與文件 - Cisco Systems