使用Cisco路由器識別和跟蹤資料包泛洪

目錄

簡介

拒絕服務(DoS)攻擊在Internet上很常見。對此類攻擊作出響應的第一步是確定攻擊型別。許多常用的DoS攻擊都基於高頻寬資料包泛洪或其他重複的資料包流。

將許多DoS攻擊流中的資料包與Cisco IOS®軟體訪問清單條目匹配時，可以將其隔離。這對於過濾攻擊很有價值。在描述未知攻擊時，以及在追蹤「偽裝」資料包流返回到其實際源時，它也是很有用的。

Cisco路由器功能（例如調試日誌記錄和IP記帳）有時也可用於類似目的，尤其是用於新的或不尋常的攻擊。但是，在最新版本的Cisco IOS軟體中，訪問清單和訪問清單日誌記錄是識別和跟蹤常見攻擊時的首要功能。

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。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

最常見的DoS攻擊

可能會發生多種DoS攻擊。即使您忽略使用軟體錯誤來關閉具有相對較少流量的系統的攻擊，但事實仍然是，可以通過網路傳送的任何IP資料包都可用於執行泛洪DoS攻擊。當你受到攻擊時，你總是必須考慮你所看到的東西不屬於通常類別的可能性。

但是，受此警告的約束，記住許多攻擊是相似的，也是一件好事。攻擊者之所以選擇常見漏洞，是因為它們特別有效，尤其難以跟蹤，或者是因為工具可用。許多DoS攻擊者缺乏技能或動機來創造自己的工具，並使用網際網路上的程式。這些工具往往越來越流行。

撰寫本文時（1999年7月），大多數客戶要求思科協助的請求都涉及「smurf」攻擊。此次攻擊有兩個受害者：一個「終極目標」和一個「反射器」 攻擊者向反射器子網的廣播地址傳送ICMP回應請求刺激流(「ping」)。這些資料包的源地址被偽造為最終目標的地址。對於攻擊者傳送的每個資料包，反射器子網上的許多主機都會做出響應。這淹沒了最終目標，浪費了兩名受害者的頻寬。

稱為「fraggle」的類似攻擊以相同方式使用定向廣播，但使用UDP回應請求，而不是網際網路控制消息協定(ICMP)回應請求。Fraggle通常獲得比藍精靈更小的放大係數，並且受歡迎程度較低。

Smurf攻擊通常是由於網路鏈路過載而引起的。有關這些攻擊和防禦措施的完整說明，請參閱拒絕服務攻擊資訊 。

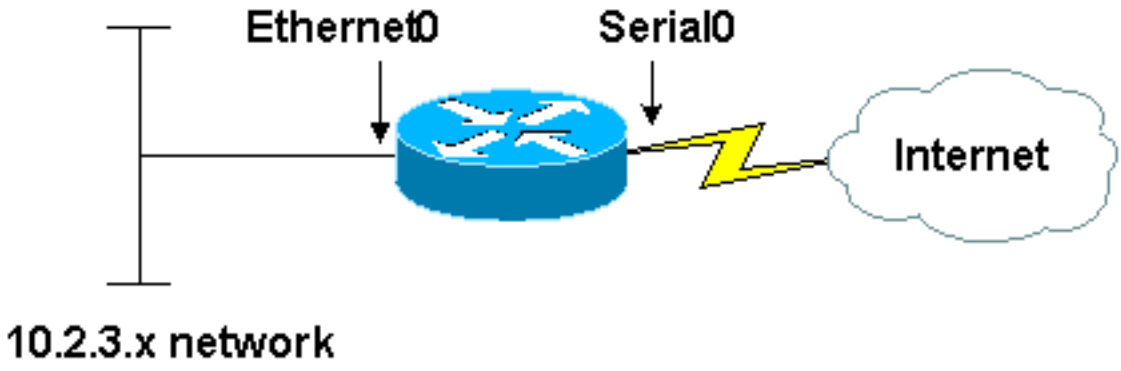
另一種常見攻擊是SYN泛洪，其中目標電腦被TCP連線請求泛洪。連線請求資料包的源地址和源TCP埠是隨機的。其目的是強制目標主機維護許多從未完成的連線的狀態資訊。

SYN泛洪攻擊通常是因為目標主機（通常是HTTP或SMTP伺服器）變得非常緩慢、崩潰或掛起。從目標主機返回的流量也可能在路由器上引起故障。這是因為此返回流量流向原始資料包的隨機源地址，缺少「真實」IP流量的位置屬性，並且可能會使路由快取溢位。在Cisco路由器上，此問題通常表現為路由器記憶體不足。

smurf和SYN泛洪攻擊共同構成了向Cisco報告的泛洪DoS攻擊的絕大部分，快速識別它們非常重要。使用思科存取清單時，這兩種攻擊（以及一些「第二層」攻擊，例如ping泛洪）可輕易識別。

DoS特徵訪問清單

想象一台帶有兩個介面的路由器。乙太網0連線到企業或小型ISP的內部LAN。Serial 0通過上游ISP提供Internet連線。Serial 0上的輸入資料包速率以全鏈路頻寬「掛鉤」，而LAN上的主機運行緩慢、崩潰、掛起或顯示DoS攻擊的其他跡象。路由器連線的小站點沒有網路分析器，即使有蹤跡，其人員也很少或完全沒有閱讀分析器跟蹤的經驗。



現在，假設您套用存取清單，如以下輸出所示：

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

此清單完全不會過濾任何流量；所有條目都是許可的。但是，由於它以有用的方式將資料包分類，因此可以使用清單來暫時診斷所有三種型別的攻擊：smurf、SYN泛洪和fraggle。

Smurf終極目標

如果您發出**show access-list**命令，就會看到類似以下的輸出：

```
Extended IP access list 169
    permit icmp any any echo (2 matches)
    permit icmp any any echo-reply (21374 matches)
    permit udp any any eq echo
    permit udp any eq echo any
    permit tcp any any established (150 matches)
    permit tcp any any (15 matches)
    permit ip any any (45 matches)
```

到達串列介面的大部分流量包括ICMP回應應答資料包。這很可能是smurf攻擊的特徵，我們的站點是最終目標，而不是反射器。修改訪問清單時，可以收集有關攻擊的詳細資訊，如以下輸出所示：

```
interface serial 0
no ip access-group 169 in

no access-list 169
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply log-input
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any
```

```
interface serial 0
ip access-group 169 in
```

此處的更改是將關鍵字**log-input**新增到與可疑流量匹配的訪問清單條目中。(低於11.2的Cisco IOS軟體版本缺少此關鍵字。請改用「**log**」關鍵字。) 這會導致路由器記錄與清單專案相符的封包資訊。如果假設已配置**logging buffered**，則可以檢視使用**show log**命令生成的消息（由於速率限制，可能需要一段時間才能累積消息）。 這些消息類似於以下輸出：

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.72
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.154
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.59
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.82
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.56
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.84
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.33
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

回應回覆封包的來源位址以位址字首192.168.212.0/24、192.168.45.0/24和172.16.132.0/24進行聚集。(192.168.x.x和172.16.x.x網路中的私人位址不會在Internet上；這是實驗插圖。) 這是smurf攻擊的特徵，源地址是smurf反射器的地址。如果在相應的Internet「whois」資料庫中查詢這些地址塊的所有者，您可以找到這些網路的管理員，並請求他們幫助處理攻擊。

在藍精靈事件的此時此刻，記住這些反射者是同伴受害者，而不是攻擊者，這一點非常重要。對於攻擊者而言，在任何DoS泛洪中對IP資料包使用自己的源地址的情況極為罕見，而在正常工作的欺騙性攻擊中，他們不可能這樣做。泛洪資料包中的任何地址都應假定為完全偽造的，或某種型別的

受害者地址。smurf攻擊的最終目標的最有效方法是聯絡反射器，或者要求反射器重新配置網路以關閉攻擊，或者要求反射器協助追蹤刺激流。

由於smurf攻擊的最終目標通常是由來自Internet的傳入鏈路過載造成的，因此通常沒有響應，只能與反射器聯絡。當資料包到達目標控制下的任何機器時，大多數損壞已經發生。

一種權衡措施是要求上游網路提供商過濾掉所有ICMP回應應答，或來自特定反射器的所有ICMP回應應答。建議不要永久保留此型別的篩選器。即使對於臨時過濾器，也應只過濾回應應答，而不是過濾所有ICMP資料包。另一種可能性是讓上游提供商使用服務品質和速率限制功能來限制回應要求可用的頻寬。合理的頻寬限制可以無限期地保留。這兩種方法都依賴於上游提供者具有必要容量的裝置，有時該容量不可用。

Smurf反射器

如果傳入流量由回應請求而不是回應回覆組成（換句話說，如果第一個訪問清單條目而不是第二個條目計算出的匹配數比合理預期的要多得多），您會懷疑存在將網路用作反射器的smurf攻擊，或者可能是簡單的ping泛洪。無論哪種情況，如果攻擊成功，您都會認為串列線路的出線端和進線端都將被淹沒。事實上，由於放大係數的原因，您預期輸出側比輸入側更過載。

有幾種方法可以區分smurf攻擊和簡單的ping泛洪：

- Smurf刺激資料包傳送到定向廣播地址，而不是單播地址，而普通ping泛洪幾乎總是使用單播。您可以在適當的存取清單專案上看到使用**log-input**關鍵字的地址。
- 如果您用作smurf反射器，則系統的乙太網端的**show interface**顯示會出現不相稱的輸出廣播，**show ip traffic**顯示中傳送的廣播數量通常不相稱。標準ping泛洪不會增加後台廣播流量。
- 如果您被用作smurf反射器，則傳往Internet的流量將多於從Internet傳入的流量。一般情況下，串列介面上的輸出資料包比輸入資料包多。即使刺激流完全填充輸入介面，響應流也大於刺激流，並且分組丟棄被計數。

smurf反射器比smurf攻擊的最終目標有更多選項。如果反射器選擇關閉攻擊，則適當使用**no ip directed-broadcast**（或等效的非IOS命令）通常就足夠了。即使沒有活動攻擊，這些命令也屬於每個配置。有關防止Cisco裝置被用於smurf攻擊的詳細資訊，請參閱改進Cisco路由器的安全性。有關一般的smurf攻擊的更多常規資訊和有關保護非Cisco裝置的資訊，請參閱拒絕服務攻擊資訊頁面 。

smurf反射器比最終目標更接近攻擊者，因此更適合跟蹤攻擊。如果您選擇跟蹤攻擊，您需要與相關的ISP合作。如果您希望在完成跟蹤後執行任何操作，您需要與適當的執法機構合作。如果您尋求跟蹤攻擊，建議您儘快讓執法人員參與進來。有關跟蹤泛洪攻擊的技術資訊，請參見跟蹤部分。

弗萊格爾

fraggle攻擊與smurf攻擊類似，不同之處在於UDP echo請求用於刺激流，而不是ICMP echo請求。訪問清單的第三和第四行標識欺詐攻擊。受害者的適當響應是相同的，不同之處在於，在大多數網路中，UDP回應與ICMP回應相比是一項不太重要的服務。因此，您可以完全禁用它們，負面影響較少。

SYN泛洪

訪問清單的第五和第六行為：

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
```

第一行匹配設定了確認位的任何TCP資料包。就我們的目的而言，這實際表示會與任何非TCP SYN的封包相符。第二行僅匹配TCP SYN資料包。SYN泛洪很容易從這些清單條目上的計數器中識別。在正常流量中，非SYN TCP資料包的數量比SYN多出至少兩倍，通常更像四或五倍。在SYN泛洪中，SYN的資料包數量通常會比非SYN TCP資料包多出很多倍。

建立此簽名的唯一非攻擊條件是大量真正的連線請求過載。一般來說，這種過載不會意外發生，也不會像真正的SYN泛洪那樣涉及那麼多的SYN資料包。此外，SYN泛洪通常包含具有完全無效源地址的資料包；使用**log-input**關鍵字可以檢查連線請求是否來自此類地址。

有一種稱為「進程表攻擊」的攻擊與SYN泛洪有一些相似之處。在進程表攻擊中，TCP連線完成，然後允許超時而無需更多的協定流量，而在SYN泛洪中，僅傳送初始連線請求。由於進程表攻擊需要完成TCP初始握手，因此通常必須使用攻擊者具有訪問許可權的真實電腦的IP地址來發起此攻擊（通常為竊取訪問許可權）。 因此，使用資料包日誌記錄很容易將進程表攻擊與SYN泛洪區分開來。進程表攻擊中的所有SYN都來自一個或多個地址，或者最多來自一個或多個子網。

SYN泛洪受害者的響應選項非常有限。受到攻擊的系統通常是一項重要的服務，阻止對系統訪問通常可以實現攻擊者的目的。許多路由器和防火牆產品（包括Cisco的產品）具有可用於減少SYN泛洪影響的功能。但是，這些特徵的有效性取決於環境。有關詳細資訊，請參閱Cisco IOS防火牆功能集的文檔、Cisco IOS TCP攔截功能的文檔以及改進Cisco路由器的安全性。

可以跟蹤SYN泛洪，但跟蹤過程需要從攻擊者到受害者的路徑上的每個ISP的幫助。如果您決定嘗試跟蹤SYN泛洪，請儘早與執法部門聯絡，並與您自己的上游服務提供商合作。請參閱本文檔的跟蹤部分，瞭解有關使用思科裝置進行跟蹤的詳細資訊。

其他攻擊

如果您認為自己受到攻擊，而且可以使用IP源地址和目的地址、協定號和埠號來描述攻擊的特徵，則可以使用訪問清單來測試您的假設。建立與可疑流量匹配的訪問清單條目，將其應用於適當的介面，然後觀察匹配計數器或記錄流量。

日誌記錄和計數器警告

訪問清單條目上的計數器會計算該條目的所有匹配項。如果將訪問清單應用於兩個介面，則顯示的計數是聚合計數。

訪問清單日誌不會顯示與條目匹配的每個資料包。日誌記錄受速率限制，可避免CPU過載。日誌記錄顯示您是一個具有合理代表性的示例，但並非完整資料包跟蹤。請記住，有些資料包是看不到的。

在某些軟體版本中，存取清單記錄功能只在某些交換模式下運作。如果訪問清單條目計算大量匹配項，但記錄不完整，請嘗試清除路由快取，以強制資料包進行進程交換。如果要在具有多個介面的負載較重的路由器上執行此操作，請務必小心。重建快取時，可能會丟棄大量流量。儘可能使用思科快速轉發。

存取清單和記錄會對效能產生影響，但影響不大。在運行超過80%的CPU負載的路由器上，或在將訪問清單應用於高速介面時，請務必小心。

追蹤

DoS資料包的源地址幾乎總是設定為與攻擊者本身無關的值。因此，在識別攻擊者時它們沒有用處。識別攻擊源的唯一可靠方法是逐跳通過網路對其進行跟蹤。此過程包括重新配置路由器和檢查日

誌資訊。從攻擊者到受害者的路徑需要所有網路運營商合作。確保這種合作通常需要執法機構的參與，如果要對攻擊者採取任何行動，執法機構也必須參與。

DoS泛洪的跟蹤過程相對簡單。從已知承載泛洪流量的路由器（名稱為「A」）開始，識別出A接收流量的路由器（名稱為「B」）。接著一個人登入B，並找到B接收流量的路由器（名稱為「C」）。此過程會一直持續，直到找到最終源。

此方法存在多種複雜情況，如以下所述：

- 「最終源」可以是被攻擊者攻陷的電腦，但實際上它屬於另一個受害者並由其操作。在這種情況下，跟蹤DoS泛洪只是第一步。
- 攻擊者知道他們可能會被跟蹤，因此通常只在有限時間內持續發動攻擊。可能沒有足夠的時間來實際跟蹤洪水。
- 攻擊可能來自多個來源，尤其是攻擊者相對複雜的情況下。必須努力確定儘可能多的來源。
- 通訊問題使跟蹤過程變慢。通常一個或多個網路運營商沒有合適的技術人員可用。
- 即使找到了攻擊者，法律和政治方面的顧慮也可能使其難以對攻擊者採取行動。

大多數跟蹤DoS攻擊的努力都失敗了。因此，許多網路運營商甚至不會嘗試追蹤攻擊，除非他們受到壓力。其他許多人只追蹤「嚴重」攻擊，對「嚴重」的定義不同。 有些人在執法介入的情況下才協助追查線索。

使用「log-input」進行追蹤

如果選擇跟蹤通過Cisco路由器的攻擊，最有效的方式是構建與攻擊流量相匹配的訪問清單條目，向其附加**log-input**關鍵字，並將訪問清單應用於介面出站，通過該介面將攻擊流傳送到其最終目標。訪問清單生成的日誌條目標識流量到達的路由器介面，如果介面是多點連線，則給出接收流量的裝置的第2層地址。然後可使用第2層地址來標識鏈路中的下一台路由器，例如，使用**show ip arp** ***mac-address*** 命令。

SYN泛洪

為了跟蹤SYN泛洪，您可以建立類似於以下內容的訪問清單：

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

這會記錄所有目的地為目標主機的SYN資料包，包括合法SYN。為了確定最有可能實際通向攻擊者的路徑，請詳細檢查日誌條目。通常，泛洪的源是最大數量的匹配資料包到達的源。源IP地址本身沒有意義。您正在查詢源介面和源MAC地址。有時，可以將泛洪資料包與合法資料包區分開來，因為泛洪資料包可能具有無效的源地址。源地址無效的任何資料包都可能是泛洪的一部分。

泛洪可能來自多個來源，儘管這對於SYN泛洪而言比較罕見。

Smurf刺激

若要追蹤smurf刺激流，請使用類似以下的存取清單：

```
access-list 169 permit icmp any any echo log-input
access-list 169 permit ip any any
```

請注意，第一個專案不會將其自身限製為目的地為反射器位址的封包。原因是大多數smurf攻擊使用

多個反射器網路。如果您未與最終目標聯絡，則可能不知道所有反射器地址。隨著您的跟蹤距離攻擊源越來越近，您可能會開始看到回應要求前往越來越多的目的地；這是個好兆頭。

但是，如果您處理大量ICMP流量，可能會生成過多日誌記錄資訊，使您難以閱讀。如果發生這種情況，您可以將目的地址限製為已知使用的反射器之一。另一個有用的戰術是使用利用以下事實的條目：255.255.255.0的網路掩碼在Internet中非常常見。而且，由於攻擊者發現smurf反射器的方式，實際用於smurf攻擊的反射器地址更可能匹配該掩碼。以。0或。255結尾的主機地址在Internet中非常少見。因此，您可以為smurf刺激流構建相對特定的識別器，如以下輸出所示：

```
access-list 169 permit icmp any host known-reflector echo log-input access-list 169 permit icmp
any 0.0.0.255 255.255.255.0 echo log-input access-list 169 permit icmp any 0.0.0.0 255.255.255.0
echo log-input access-list 169 permit ip any any
```

使用此清單，您可以從日誌中消除許多「雜訊」資料包，同時您仍然可以在更接近攻擊者時發現其他刺激流。

不使用「log-input」進行跟蹤

log-input關鍵字存在於Cisco IOS軟體版本11.2和更高版本中，以及在特別為服務提供者建立的特定11.1型軟體中。舊版軟體不支援此關鍵字。如果使用搭載較舊軟體的路由器，有三個可行的選項：

- 建立訪問清單，但不記錄日誌，但包含與可疑流量匹配的條目。依次應用每個介面的*input*端上的清單，然後檢視計數器。尋找匹配率高的介面。該方法效能開銷很小，有利於源介面的識別。它最大的缺點是不提供鏈路層源地址，因此主要適用於點對點線路。
- 使用**log**關鍵字(而不是**log-input**)建立存取清單專案。 再次將清單依次應用於每個介面的傳入端。此方法仍不提供源MAC地址，但可用於檢視IP資料。例如，驗證資料包流是否真正是攻擊的一部分。效能影響可以從中等到高不等，而且較新的軟體比較舊的軟體效能更好。
- 使用**debug ip packet detail**命令收集有關資料包的資訊。此方法提供MAC地址，但可能會嚴重影響效能。使用此方法很容易出錯，使路由器無法使用。如果使用此方法，請確保路由器以快速、自主或最佳模式交換攻擊流量。使用訪問清單將調試限於您真正需要的資訊。將調試資訊記錄到本地日誌緩衝區，但關閉將調試資訊記錄到Telnet會話和控制檯的功能。如果可能，應安排人員親臨路由器，以便根據需要重新通電。請記住，**debug ip packet**指令不會顯示有關快速交換封包的資訊。您需要發出**clear ip cache**命令才能捕獲資訊。每個**clear**命令都會為您提供一或兩個偵錯輸出資料包。

相關資訊

- Kerberos
- 技術支援與文件 - Cisco Systems