ASA/PIX 7.x及更高版本：減少網路攻擊

目錄

簡介

本檔案介紹如何使用思科安全裝置(ASA/PIX)緩解各種網路攻擊，例如拒絕服務(DoS)。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據執行軟體版本7.0和更新版本的Cisco 5500系列調適型安全裝置(ASA)。

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。

相關產品

本文檔還可用於運行軟體版本7.0及更高版本的Cisco 500系列PIX。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

防止SYN攻擊

如何減輕對ASA/PIX的傳輸控制協定(TCP)同步/啟動(SYN)攻擊？

TCP SYN攻擊

TCP SYN攻擊是一種DoS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。

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

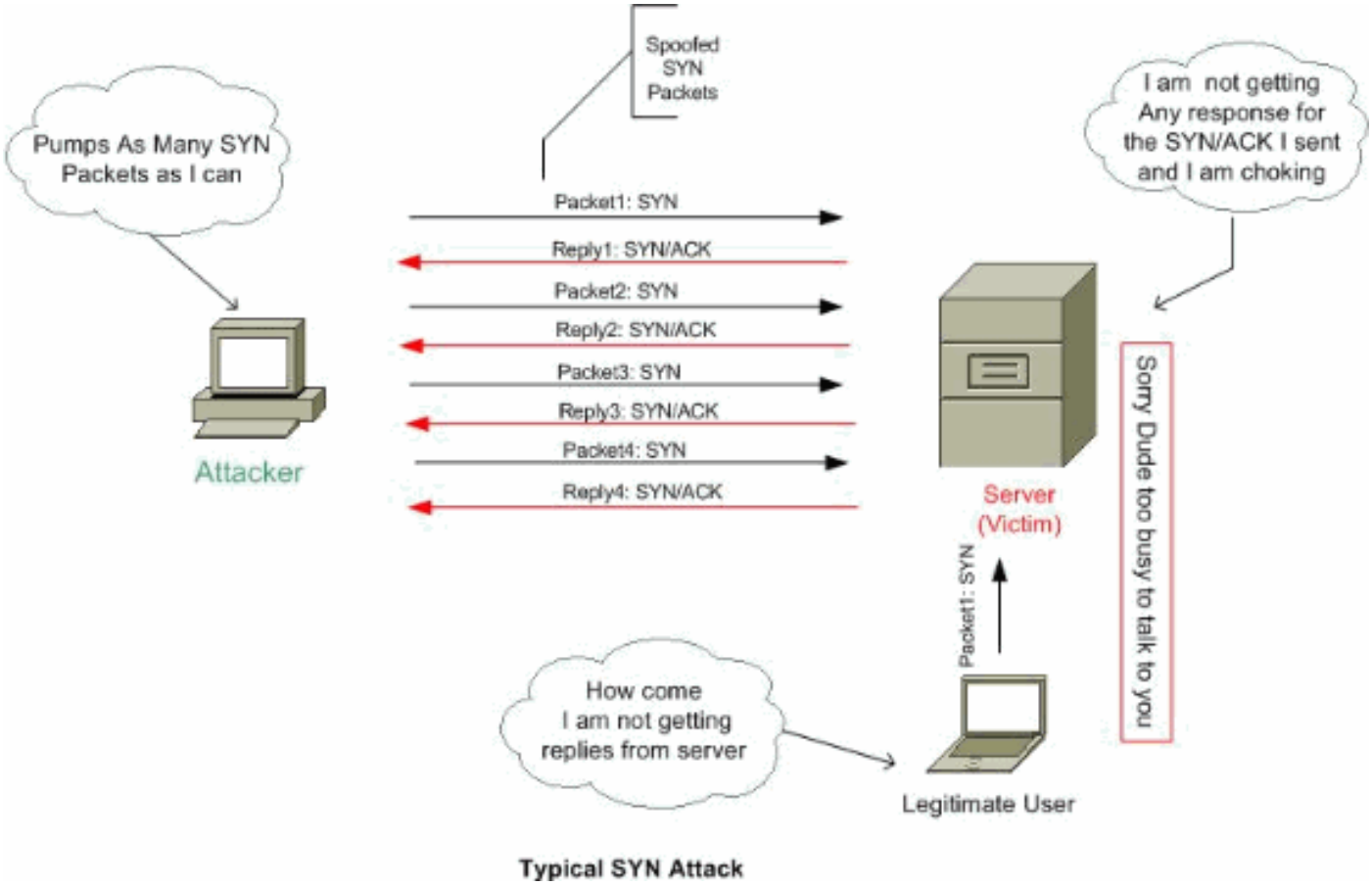
在等待SYN ACK的ACK時，目標主機上的有限大小的連線隊列會跟蹤等待完成的連線。此隊列通常會快速清空，因為ACK預計在SYN ACK後幾毫秒內到達。

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。

如需TCP SYN攻擊的詳細資訊，請參閱防禦TCP SYN泛洪攻擊。



Typical SYN Attack

緩解

本節介紹如何通過設定最大TCP和使用者資料包協定(UDP)連線數、最大初始連線數、連線超時數來緩解SYN攻擊，以及如何禁用TCP序列隨機化。

如果達到初始連線限制，則安全裝置將使用SYN+ACK響應傳送到伺服器的每個SYN資料包，並且不會將SYN資料包傳遞到內部伺服器。如果外部裝置使用ACK資料包做出響應，則安全裝置知道該請求有效（而不是潛在SYN攻擊的一部分）。 然後，安全裝置與伺服器建立連線並將連線連線連線在一起。如果安全裝置沒有從伺服器返回ACK，則它會主動超時該初始連線。

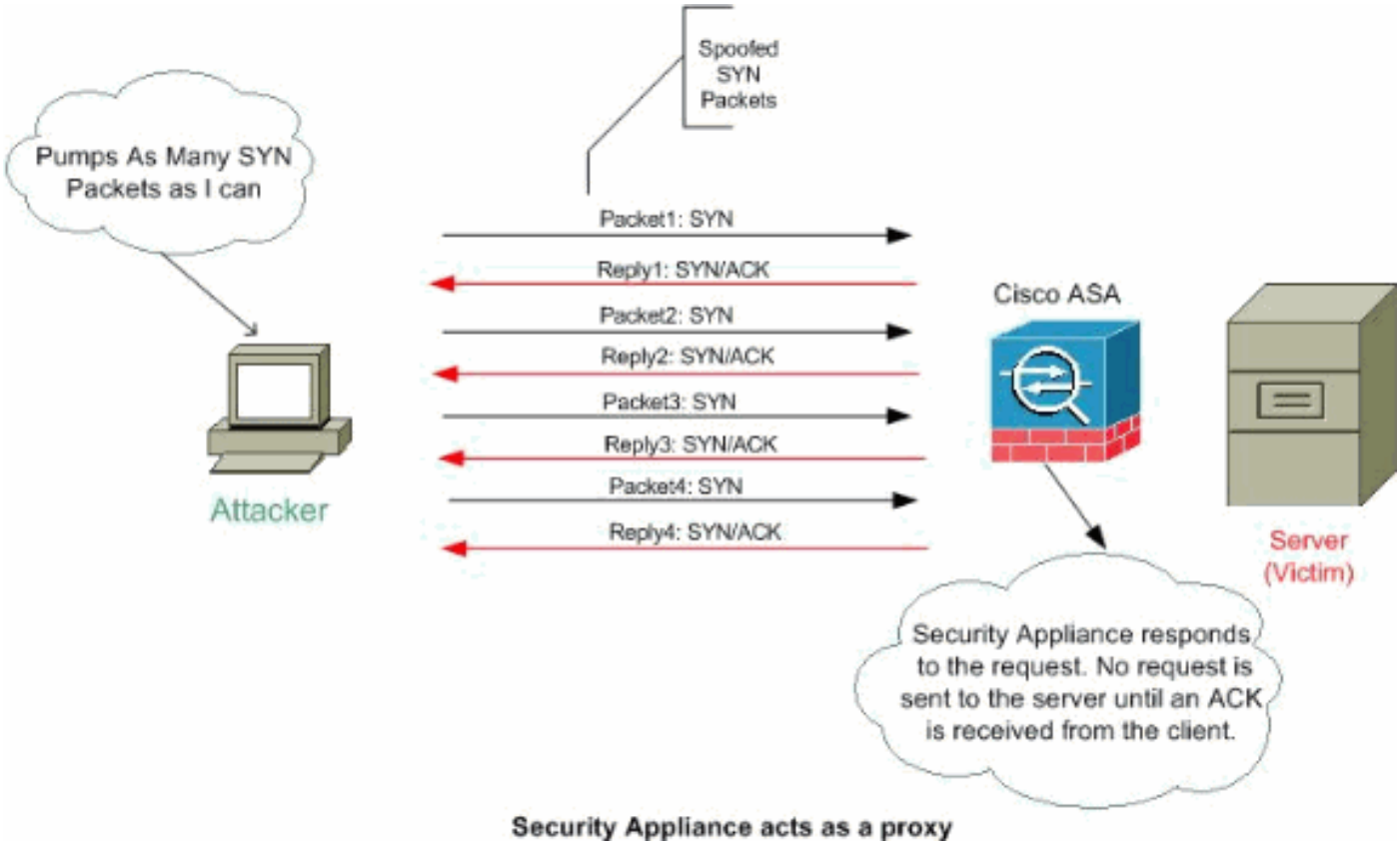
每個TCP連線有兩個初始序號(ISN):一個由客戶端生成，另一個由伺服器生成。安全裝置隨機化傳入和傳出方向的TCP SYN的ISN。

對受保護主機的ISN進行隨機化可防止攻擊者預測新連線的下一個ISN並可能劫持新會話。

如果需要，可以禁用TCP初始序列號隨機化。例如：

- 如果另一個內嵌防火牆也隨機化初始序列號，則無需兩個防火牆都執行此操作，即使此操作不會影響流量。
- 如果透過安全裝置使用外部BGP(eBGP)多重躍點，且eBGP對等體使用MD5，則隨機化會中斷MD5校驗和。
- 您使用的廣域應用服務(WAAS)裝置要求安全裝置不要隨機化連線的序列號。

注意：還可以在NAT配置中配置最大連線數、最大初始連線數和TCP序列隨機化。如果同時使用兩種方法為相同流量配置這些設定，則安全裝置將使用下限。對於TCP序列隨機化，如果使用任一方法禁用該隨機化，則安全裝置將禁用TCP序列隨機化。



完成以下步驟以設定連線限制：

1. 為了識別流量，請根據Using Modular Policy Framework使用**class-map**命令新增類對映。
2. 要新增或編輯策略對映,請輸入以下命令：
   ```
   hostname(config)#policy-map name
   ```
3. 要標識要向其分配操作的類對映（從步驟1），請輸入以下命令：
   ```
   hostname(config-pmap)#class class_map_name
   ```
4. 要設定最大連線數（TCP和UDP）、最大初始連線數、每客戶端 — embryonic-max、每客戶端 — max還是禁用TCP序列隨機化，請輸入以下命令：
   ```
   hostname(config-pmap-c)#set connection {[conn-max number]
   [embryonic-conn-max number] [per-client-embryonic-max number]
   [per-client-max number][random-sequence-number {enable |
   disable}}
   ```
   其中number是介於0和65535之間的整數。預設值為0，表示對連線沒有限制。您可以在一行（任意順序）輸入此命令，也可以將每個屬性作為一個單獨的命令輸入。該命令組合在運行配置的一行中。
5. 要設定連線、半開連線和半閉連線的超時，請輸入以下命令：
   ```
   hostname(config-pmap-c)#set connection {[embryonic hh[:mm[:ss]]]
   [half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]]]}
   ```
   其中**embryonic** hh[:mm[:ss]是介於0:0:5和1192:59:59之間的時間。預設值為0:0:30。您還可以將此值設定為0，這意味著連線永遠不會超時。**half-closed** hh[:mm[:ss]和**tcp** hh[:mm[:ss]值是介於0:5:0和1192:59:59之間的時間。**half-closed**的預設值為0:10:0,**tcp**的預設值為1:0:0。您還可以將這些值設定為0，這意味著連線從不超時。您可以在一行（任意順序）輸入此命令，也可以將每個屬性作為一個單獨的命令輸入。該命令組合在運行配置的一行中。**初始（半開啟）連線** — 初始連線是尚未完成源和目標之間必要握手的TCP連線請求。**Half-closed connection** — 半封閉連線是指通過傳送FIN僅在一個方向上關閉連線。但是，TCP作業階段仍由對等點維護。**Per-client-embryonic-max** — 每個客戶端允許的最大同時初始連線數，介於

0和65535之間。預設值為0，允許無限連線。**Per-client-max** — 每個客戶端允許的最大併發連線數，介於0和65535之間。預設值為0，允許無限制連線。

6. 要在一個或多個介面上啟用策略對映，請輸入以下命令：

```
hostname(config)#service-policy policymap_name {global | interface interface_name}
```

其中**global**將策略對映應用於所有介面，**interface**將策略應用於一個介面。只允許一個全域性策略。可以通過將服務策略應用到介面來覆蓋該介面上的全域性策略。您只能對每個介面應用一個策略對映。

範例：

```
ciscoasa(config)#class-map tcp_syn
ciscoasa(config-cmap)#match port tcp eq 80
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map tcpmap
ciscoasa(config-pmap)#class tcp_syn
ciscoasa(config-pmap-c)#set connection conn-max 100
ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200
ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10
ciscoasa(config-pmap-c)#set connection per-client-max 5
ciscoasa(config-pmap-c)#set connection random-sequence-number enable
ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45
ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0
ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
ciscoasa(config)#service-policy tcpmap global
```

注意：若要驗證任何特定主機的半開放會話總數，請使用以下命令：

```
ASA-5510-8x# show local-host all

Interface dmz: 0 active, 0 maximum active, 0 denied
Interface management: 0 active, 0 maximum active, 0 denied
Interface xx: 0 active, 0 maximum active, 0 denied
Interface inside: 7 active, 18 maximum active, 0 denied

local host: <10.78.167.69>,

    TCP flow count/limit = 2/unlimited

    TCP embryonic count to host = 0

    TCP intercept watermark = unlimited

    UDP flow count/limit = 0/unlimited
```

注意：TCP啟動計顯示半開啟會話的數量。

防止IP欺騙攻擊

PIX/ASA能否阻止IP欺騙攻擊？

IP欺騙

為了獲得訪問權，入侵者使用偽造的源IP地址建立資料包。這利用了使用基於IP地址的身份驗證的

應用程式，並導致未授權使用者（可能還有目標系統上的root訪問許可權）。例如rsh和rlogin服務。

如果資料包未配置為過濾源地址在本地域中的傳入資料包，則可以通過過濾路由器防火牆進行路由。必須注意的是，即使沒有應答資料包可以到達攻擊者，上述攻擊也是可能的。

可能易受攻擊的配置的示例包括：

- 代理防火牆，其中代理應用程式使用源IP地址進行身份驗證
- 到支援多個內部介面的外部網路的路由器
- 具有支援內部網路子網劃分的兩個介面的路由器

緩解

根據路由表，單播反向路徑轉發(uRPF)通過確保所有資料包的源IP地址與正確的源介面相匹配，來防止IP欺騙（資料包使用錯誤的源IP地址來遮蓋其真實源）。

通常，安全裝置在確定資料包轉發位置時只檢視目標地址。單播RPF指示安全裝置也檢視源地址。這就是它稱為**反向路徑轉發**的原因。對於要允許通過安全裝置的任何流量，安全裝置路由表必須包含返回源地址的路由。如需詳細資訊，請參閱RFC 2267 。

注意： `:- %PIX-1-106021:deny protocol reverse path check from src_addr to dest_addr on interface int_name` log消息。使用**no ip verify reverse-path interface(interface name)**命令停用反向路徑檢查，以解決此問題：

`no ip verify reverse-path interface (interface name)`

例如，對於外部流量，安全裝置可以使用預設路由滿足單播RPF保護。如果流量從外部介面進入，並且路由表不知道源地址，則安全裝置將使用預設路由正確將外部介面標識為源介面。

如果流量從路由表已知的地址進入外部介面，但與內部介面相關聯，則安全裝置丟棄該資料包。同樣，如果流量從未知源地址進入內部介面，安全裝置將丟棄該資料包，因為匹配的路由（預設路由）指示外部介面。

單播RPF的實施方式如下：

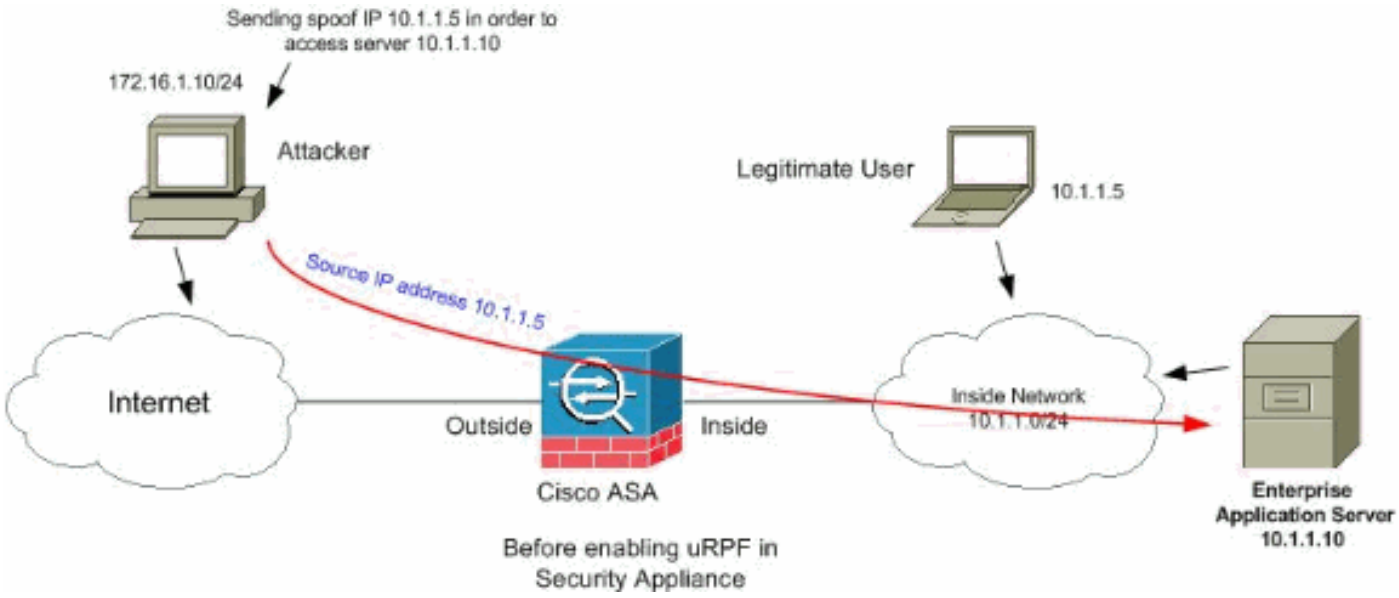
- ICMP資料包沒有會話，因此會檢查每個資料包。
- UDP和TCP具有會話，因此初始資料包需要反向路由查詢。在會話期間到達的後續分組使用作為會話的一部分而維護的現有狀態來檢查。檢查非初始資料包，以確保它們到達初始資料包使用的同一介面。

若要啟用單點傳播RPF，請輸入以下命令：

```
hostname(config)#ip verify reverse-path interface interface_name
```

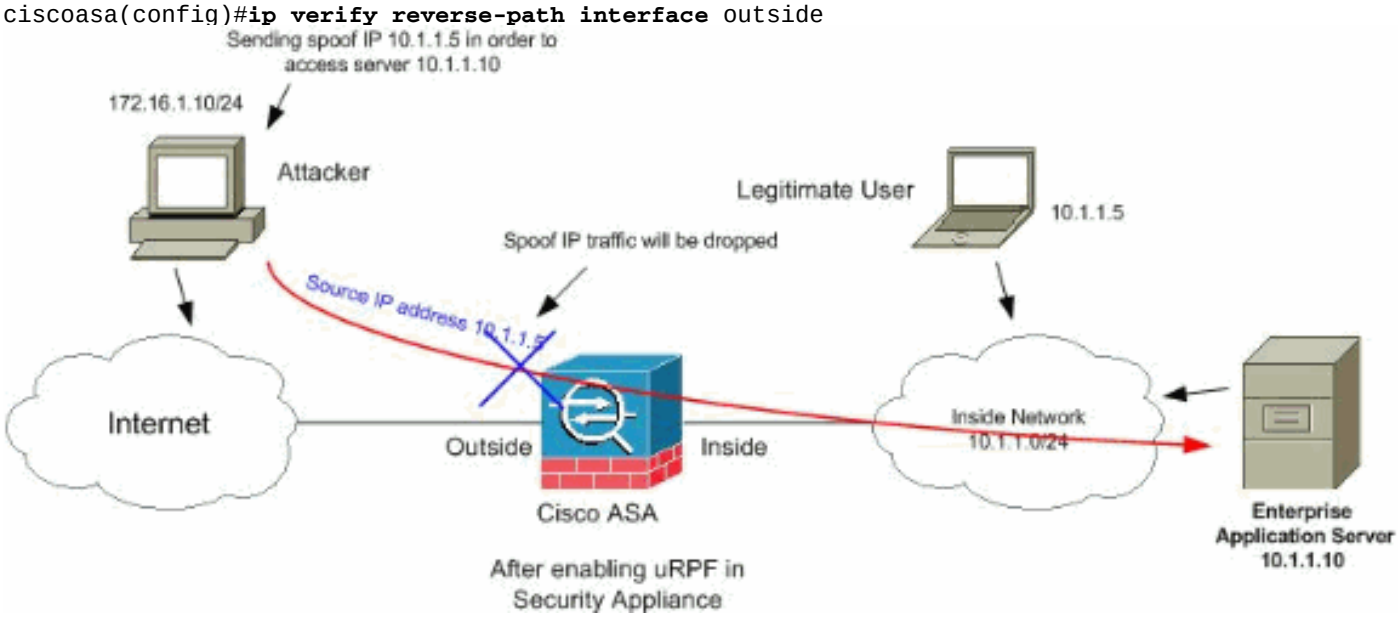
範例：

如圖所示，攻擊者PC通過傳送偽造源IP地址10.1.1.5/24的資料包向應用伺服器10.1.1.10發出請求，然後伺服器向真實IP地址10.1.1.5/24傳送資料包以響應請求。此類非法資料包將攻擊內部網路中的應用伺服器和合法使用者。



單播RPF可以防止基於源地址欺騙的攻擊。您需要在ASA的外部介面中配置uRPF，如下所示：

```
ciscoasa(config)#ip verify reverse-path interface outside
```



使用系統日誌消息進行欺騙識別

安全裝置繼續接收系統日誌錯誤消息，如圖所示。這表示使用欺騙資料包或可能由於非對稱路由而觸發的潛在攻擊。

1.

```
%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port
to IP_address/port flags tcp_flags on interface interface_name
```

說明這是一條與連線相關的消息。當為指定流量型別定義的安全策略拒絕連線到內部地址的嘗試時，會出現此消息。可能的*tcp_flags*值與TCP報頭中連線遭到拒絕時出現的標誌相對應。例如，到達的TCP資料包在安全裝置中沒有連線狀態，因此被丟棄。此封包中的*tcp_flags*是FIN和ACK。*tcp_flags*如下所示：ACK — 已收到確認號。FIN — 資料已傳送。PSH — 接收器向應用程式傳遞資料。RST — 連線已重置。SYN — 同步序列號以啟動連線。URG — 緊急指

標被宣告為有效。PIX/ASA上的靜態轉換失敗的原因很多。但是，一個常見原因是非軍事區(DMZ)介面配置的安全級別(0)與外部介面相同。為了解決此問題，請為所有介面分配不同的安全級別如需詳細資訊，請參閱設定介面引數。如果外部裝置向內部客戶端傳送IDENT資料包（被PIX防火牆丟棄），也會出現此錯誤消息。有關詳細資訊，請參閱由IDENT協定導致的PIX效能問題

2.

```
%PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port
to inside_address/inside_port due to DNS {Response|Query}
```

說明這是一條與連線相關的消息。如果指定的連線因出站deny命令而失敗，則會顯**示此**消息。協定變數可以是ICMP、TCP或UDP。**建議的操作：**使用**show outbound**命令檢查出站清單。

3.

```
%PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst
interface_name: IP_address (type dec, code dec)
```

說明安全裝置拒絕任何入站ICMP資料包訪問。預設情況下，除非特別允許，否則拒絕所有ICMP資料包訪問。

4.

```
%PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on
interface interface_name.
```

說明當資料包到達安全裝置介面時（目的IP地址為0.0.0.0，而安全裝置介面的目的MAC地址為0.0.0），將生成此消息。此外，當安全裝置丟棄源地址無效的資料包時，也會生成此消息，源地址無效的資料包可能包括以下地址之一或其他某個無效地址：環回網路(127.0.0.0)廣播（有限、網路定向、子網定向和所有子網定向）目的主機(land.c)為了進一步增強欺騙資料包檢測，請使用**icmp**命令配置安全裝置以丟棄源地址屬於內部網路的資料包。這是因為**access-list**命令已被棄用，不再保證能正確執行。**建議的操作：**確定外部使用者是否試圖破壞受保護的網路。檢查客戶端是否配置錯誤。

5.

```
%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to
IP_address
```

說明安全裝置收到一個資料包，其IP源地址等於IP目標，目標埠等於源埠。此訊息表示偽裝的封包旨在攻擊系統。這種攻擊稱為陸地攻擊。**建議的操作：**如果此消息持續出現，則表明可能正在進行攻擊。資料包未提供足夠的資訊來確定攻擊的來源。

6.

```
%PIX|ASA-1-106021: Deny protocol reverse path check from
source_address to dest_address on interface interface_name
```

說明攻擊正在進行中。有人試圖欺騙入站連線上的IP地址。單播RPF（也稱為反向路由查詢）檢測到沒有路由所代表的源地址的資料包，並假定它是安全裝置上的攻擊的一部分。當您使用**ip verify reverse-path**命令啟用單播RPF時，系統會顯示此消息。此功能適用於輸入介面的封包。如果已在外部進行配置，則安全裝置會檢查從外部到達的資料包。安全裝置根據源地址查詢路由。如果未找到條目且未定義路由，則會出現此系統日誌消息並丟棄連線。如果有路由，安全裝置會檢查它對應的介面。如果封包到達另一個介面，則可能是偽裝，或者存在非對稱路由環境，該環境有多條路徑通往目的地。安全裝置不支援非對稱路由。如果在內部介面上配置了安全裝置，則會檢查static **route**命令語句或RIP。如果未找到源地址，則內部使用者正在欺騙其地址。**建議的操作：**即使攻擊正在進行中，如果啟用此功能，則無需使用者執行任何操作。安全裝置可抵禦攻擊。**注意：show asp drop命令會顯示加速安全路徑(asp)丟棄的資料包或連線，這可能會幫助您解決問題。**它還指示上次清除asp刪除計數器的時間。使用**show asp drop rpf-violated**命令，當在介面上配置**ip verify reverse-path**時，計數器會遞增，而安全裝置收到的資料包的源IP路由查詢不會產生與接收資料包的介面相同的介面。

```
ciscoasa#show asp drop frame rpf-violated
  Reverse-path verify failed                    2
```

附註： 建議：根據下一條系統消息中顯示的源IP跟蹤流量來源，並調查其傳送欺騙流量的原因。**附註： 系統日誌消息：**106021

7.
```
%PIX|ASA-1-106022: Deny protocol connection spoof from source_address
to dest_address on interface interface_name
```
說明與連線匹配的資料包到達與連線開始處的介面不同的介面。例如，如果使用者在內部介面上啟動連線，但安全裝置檢測到同一連線到達邊界介面，則安全裝置有多個到達目的地的路徑。這就是非對稱路由，在安全裝置上不受支援。攻擊者還可能嘗試將資料包從一個連線追加到另一個連線，作為侵入安全裝置的方法。無論哪種情況，安全裝置都會顯示此消息並丟棄連線。**建議操作：**未配置**ip verify reverse-path**命令時，將顯示此消息。檢查路由是否不對稱。

8.
```
%PIX|ASA-4-106023: Deny protocol src
[interface_name:source_address/source_port] dst
interface_name:dest_address/dest_port [type {string}, code {code}] by
access_group acl_ID
```
說明IP資料包被ACL拒絕。即使未為ACL啟用**log**選項，也會顯示此訊息。**建議操作：**如果消息持續來自同一源地址，則消息可能表示嘗試執行足印或埠掃描。聯絡遠端主機管理員。

9.
```
%PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet
from sip/sport to dip/dport on interface if_name.
```

10.
```
%ASA-4-419002: Received duplicate TCP SYN from
in_interface:src_address/src_port to out_interface:dest_address/dest_port with
different initial sequence number.
```
說明此系統日誌消息表示通過防火牆裝置建立新的連線將導致至少超過配置的最大連線限制之一。系統日誌消息既適用於使用靜態命令配置的連線限制，也適用於使用思科模組化策略框架配置的連線限制。現有連線之一斷開之前，不允許新連線通過防火牆裝置，從而使當前連線計數低於配置的最大值。*cnt* — 當前連線計數*limit* — 配置的連線限制*dir* — 流量的方向，入站或出站*sip* — 源IP地址*sport* — 源埠*dip* — 目標IP地址*dport* — 目標埠*if_name* — 接收通訊單元的介面的名稱，可以是主介面或輔助介面。**建議操作：**由於連線限制的配置理由充分，因此此系統日誌消息可能指示可能的DoS攻擊，在這種情況下，流量的源可能是偽裝IP地址。如果源IP地址不是完全隨機的，識別源地址並使用訪問清單將其阻止可能會有所幫助。在其他情況下，獲得監聽器追蹤並分析流量來源有助於將不需要的流量與合法流量隔離。

ASA 8.x中的基本威脅檢測功能

Cisco安全裝置ASA/PIX支援軟體版本8.0及更高版本中的威脅檢測功能。使用基本威脅檢測，安全裝置監控由於以下原因丟棄的資料包和安全事件的速率：

- 按訪問清單拒絕
- 錯誤的資料包格式（例如invalid-ip-header或invalid-tcp-hdr-length）
- 超出連線限制（系統範圍的資源限制和配置中設定的限制）
- 檢測到DoS攻擊（例如SPI無效、狀態防火牆檢查失敗）
- 基本防火牆檢查失敗(此選項是包含此專案符號清單中的所有防火牆相關資料包丟棄的組合速率。不包括與防火牆無關的丟包，例如介面過載、應用檢查失敗的資料包和檢測到的掃描攻擊。)
- 檢測到可疑的ICMP資料包
- 資料包應用檢測失敗
- 介面過載
- 檢測到掃描攻擊(此選項監控掃描攻擊；例如，第一個TCP資料包不是SYN資料包，或者TCP連

線三次握手失敗。完全掃描威脅檢測(有關詳細資訊，請參閱配置掃描威脅檢測)獲取此掃描攻擊速率資訊，通過將主機分類為攻擊者並自動避開它們（例如），從而對其執行操作。
- 檢測到不完整的會話檢測（例如檢測到TCP SYN攻擊）或未檢測到資料UDP會話攻擊。

當安全裝置檢測到威脅時，會立即傳送系統日誌消息(730100)。

基本威脅檢測僅在存在丟棄或潛在威脅時影響效能。即使在這種情況下，對效能的影響也微乎其微。

當您登入到安全裝置時，會使用**show threat-detection rate**命令來識別潛在的攻擊。

```
ciscoasa#show threat-detection rate
                        Average(eps)    Current(eps) Trigger      Total events
  10-min ACL  drop:                0              0       0                16
  1-hour ACL  drop:                0              0       0               112
  1-hour SYN attck:                5              0       2             21438
  10-min  Scanning:                0              0      29               193
  1-hour  Scanning:              106              0      10            384776
  1-hour Bad  pkts:               76              0       2            274690
  10-min  Firewall:                0              0       3                22
  1-hour  Firewall:               76              0       2            274844
  10-min DoS attck:                0              0       0                 6
  1-hour DoS attck:                0              0       0                42
  10-min Interface:                0              0       0               204
  1-hour Interface:               88              0       0            318225
```

有關配置部分的詳細資訊，請參閱ASA 8.0配置指南的配置基本威脅檢測部分。

系統日誌消息733100

錯誤消息:

```
%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max
configured rate is rate_val; Current average rate is rate_val per second, max configured rate is
rate_val; Cumulative total count is total_cnt
```

系統日誌消息中的指定對象已超過指定的突發閾值速率或平均閾值速率。該對象可以是主機、TCP/UDP埠、IP協定的丟棄活動，或者由於潛在攻擊而執行的各種丟棄。這表示系統可能受到攻擊。

注意：這些具有解決方法的錯誤消息僅適用於ASA 8.0及更高版本。

1. 對象 — 丟棄率計數的一般或特定來源，可能包括以下內容：防火牆錯誤資料包速率限制DoS攻擊ACL drop連線限制ICMP攻擊掃描SYN攻擊檢查介面
2. rate_ID — 超過的已配置速率。對於不同的時間間隔，大多數對象最多可配置三種不同的速率。
3. rate_val — 特定的速率值。
4. total_cnt — 自建立或清除對象以來的總計數。

以下三個範例顯示這些變數是如何發生的：

- 對於由於CPU或匯流排限制而丟棄的介面：

```
%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per
    second,
max configured rate is 8000; Current average rate is 2030 per second,
max configured rate is 2000; Cumulative total count is 3930654
```

- 對於由於潛在攻擊而丟棄的掃描：

```
ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per
    second_
max configured rate is 10; Current average rate is 245 per second_
max configured rate is 5; Cumulative total count is 147409 (35 instances received)
```

- 對於由潛在攻擊造成的壞資料包：

```
%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per
    second,
max configured rate is 400; Current average rate is 760 per second,
max configured rate is 100; Cumulative total count is 1938933
```

建議的操作：

根據消息中顯示的指定對象型別執行以下步驟：

1. 如果syslog消息中的對象是以下值之一：防火牆錯誤資料包速率限制DoS攻擊ACL drop連線限制ICMP攻擊掃描SYN攻擊檢查介面檢查丟棄率對於運行環境是否可接受。
2. 通過運行**threat-detection rate *xxx*** 命令，將特定丟棄的閾值率調整為適當的值，其中*xxx*是以下值之一：acl-dropbad-packet-dropconn-limit-dropdos-dropfw-dropicmp-dropinspect-dropinterface-dropscanning-threatsyn攻擊
3. 如果系統日誌消息中的對象是TCP或UDP埠、IP協定或主機丟棄，請檢查丟棄速率對於運行環境是否可接受。
4. 通過運行**threat-detection rate bad-packet-drop**命令，將特定丟棄的閾值速率調整為適當的值。有關詳細資訊，請參閱《ASA 8.0配置指南》的配置基本威脅檢測部分。

注意：如果您不希望顯示丟棄率超過警告，可以通過運行**no threat-detection basic-threat命令禁用此警**告。

相關資訊

- Cisco 5500系列調適型安全裝置支援頁面
- Cisco 500系列PIX支援頁面
- 防禦TCP SYN泛洪攻擊
- 思科應用緩解公告：識別並緩解內容交換模組中拒絕服務漏洞的利用
- 思科應用緩解公告：識別並緩解對Cisco PIX和ASA裝置和防火牆服務模組中的多個漏洞的利用
- IP欺騙
- 技術支援與文件 - Cisco Systems