排除通過PIX和ASA的連線故障

目錄

簡介

本文檔提供使用Cisco ASA 5500系列自適應安全裝置(ASA)和Cisco PIX 500系列安全裝置的故障排除思路和建議。通常，當應用程式或網路源中斷或不可用時，防火牆（PIX或ASA）往往是主要目標，並被指責是導致停機的原因。通過在ASA或PIX上進行一些測試，管理員可以確定ASA/PIX是否導致問題。

請參閱PIX/ASA:建立通過思科安全裝置的連線並進行故障排除，以瞭解更多有關思科安全裝置上與介面相關的故障排除資訊。

注意：本文檔重點介紹ASA和PIX。在ASA或PIX上完成故障排除後，可能需要對其他裝置（路由器

、交換機、伺服器等）進行其他故障排除。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於採用OS 7.2.1和8.3的Cisco ASA 5510。

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

本文件也適用於以下硬體和軟體版本：

- ASA和PIX OS 7.0、7.1、8.3及更高版本
- 防火牆服務模組(FWSM)2.2、2.3和3.1

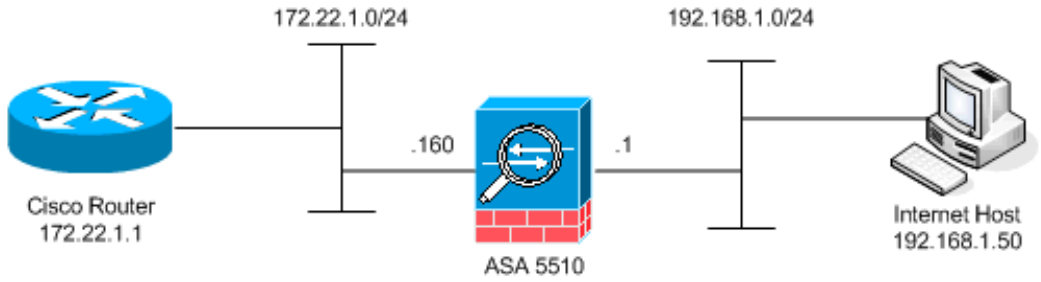
注意：特定命令和語法因軟體版本而異。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

該示例假設ASA或PIX正在生產。ASA/PIX配置可以是相對簡單（只有50行配置）或複雜（數百至數千行配置）。 使用者（客戶端）或伺服器可以位於安全網路（內部）或非安全網路（DMZ或外部）上。



ASA從此配置開始。該配置旨在為實驗室提供一個參考點。

ASA初始配置
ciscoasa#**show running-config** : Saved

```
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.1.1.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list outside_acl extended permit tcp any host
172.22.1.254 eq www
access-list inside_acl extended permit icmp 192.168.1.0
255.255.255.0 any
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq www
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq telnet
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no asdm history enable
arp timeout 14400
global (outside) 1 172.22.1.253
nat (inside) 1 192.168.1.0 255.255.255.0


!--- The above NAT statements are replaced by the
following statements !--- for ASA 8.3 and later. object
network obj-192.168.1.0 subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic 172.22.1.253 static
(inside,outside) 192.168.1.100 172.22.1.254 netmask
255.255.255.255 !--- The above Static NAT statement is
replaced by the following statements !--- for ASA 8.3
and later. object network obj-172.22.1.254 host
172.22.1.254 nat (inside,outside) static 192.168.1.100
access-group outside_acl in interface outside access-
group inside_acl in interface inside timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
```

```
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

問題

使用者聯絡IT部門並報告應用程式X不再工作。事件將上報給ASA/PIX管理員。管理員對此特定應用程式幾乎一無所知。通過使用ASA/PIX，管理員可發現X應用程式使用的埠和協定以及可能導致問題的原因。

解決方案

ASA/PIX管理員需要從使用者處收集儘可能多的資訊。有用資訊包括：

- 源IP地址 — 通常是使用者的工作站或電腦。
- 目標IP地址 — 使用者或應用程式嘗試連線的伺服器IP地址。
- 應用程式使用的埠和協定

如果能夠找到這些問題的答案，通常管理者是幸運的。在本例中，管理員無法收集任何資訊。最好是檢視ASA/PIX系統日誌消息，但如果管理員不知道要查詢什麼，則很難找到問題。

步驟1 — 發現使用者的IP地址

發現使用者的IP地址的方法有多種。本文檔介紹ASA和PIX，因此本示例使用ASA和PIX來發現IP地址。

使用者嘗試與ASA/PIX通訊。此通訊可以是ICMP、Telnet、SSH或HTTP。所選協定在ASA/PIX上的活動應該有限。在此特定示例中，使用者ping ASA的內部介面。

管理員需要設定一個或多個這些選項，然後讓使用者ping ASA的內部介面。

- **系統日誌**確保已啟用日誌記錄。需要將日誌記錄級別設定為**debug**。日誌記錄可以傳送到各個位置。此示例使用ASA日誌緩衝區。在生產環境中可能需要外部日誌伺服器。

  ```
  ciscoasa(config)#logging enable
  ciscoasa(config)#logging buffered debugging
  ```

  使用者ping ASA的內部介面(ping 192.168.1.1)。 將顯示此輸出。

  ```
  ciscoasa#show logging
  !--- Output is suppressed. %ASA-6-302020: Built ICMP connection for faddr 192.168.1.50/512
  gaddr 192.168.1.1/0 laddr 192.168.1.1/0
  %ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.50/512
  gaddr 192.168.1.1/0 laddr 192.168.1.1/0
  !--- The user IP address is 192.168.1.50.
  ```

- **ASA捕獲功能**管理員需要建立一個訪問清單，定義ASA需要捕獲的流量。定義access-list後

，**capture**命令會合併access-list並將其應用於介面。

```
ciscoasa(config)#access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#capture inside_interface access-list inside_test interface inside
```

使用者ping ASA的內部介面(ping 192.168.1.1)。 將顯示此輸出。

```
ciscoasa#show capture inside_interface
   1: 13:04:06.284897 192.168.1.50 > 192.168.1.1: icmp: echo request
 !--- The user IP address is 192.168.1.50.
```

注意：若要將捕獲檔案下載到系統（如ethereal），您可以按照以下輸出所示進行操作。

```
!--- Open an Internet Explorer and browse with this https link format: https://[
```

請參閱ASA/PIX:使用CLI和ASDM捕獲資料包配置示例，以瞭解有關ASA中捕獲資料包的詳細資訊。

- **調試debug icmp trace**命令用於捕獲使用者的ICMP流量。

```
ciscoasa#debug icmp trace
```

使用者ping ASA的內部介面(ping 192.168.1.1)。 此輸出顯示在控制檯上。

```
ciscoasa#
!--- Output is suppressed. ICMP echo request from 192.168.1.50 to 192.168.1.1 ID=512
seq=5120 len=32
ICMP echo reply from 192.168.1.1 to 192.168.1.50 ID=512 seq=5120 len=32
!--- The user IP address is 192.168.1.50.
```

若要停用**debug icmp trace**，請使用以下命令之一：**no debug icmp traceundebug icmp traceundebug all**、**Undebug all**或**un all**

這三個選項均可幫助管理員確定源IP地址。在本例中，使用者的源IP地址是192.168.1.50。管理員準備瞭解有關應用程式X的詳細資訊並確定問題的原因。

步驟2 — 找到問題的原因

根據本文檔的步驟1部分中列出的資訊，管理員現在知道了應用程式X會話的來源。管理員準備瞭解有關應用程式X的更多資訊，並開始查詢可能出現問題的位置。

ASA/PIX管理員需要為ASA做好至少一項列出的建議。管理員準備就緒後，使用者啟動應用程式X並限制所有其他活動，因為其他使用者活動可能會導致ASA/PIX管理員感到混亂或誤導。

- **監控系統日誌消息。**搜尋您在步驟1中找到的使用者的源IP地址。使用者啟動應用程式X。ASA管理員發出**show logging**命令並檢視輸出。

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-6-
305011: Built dynamic TCP translation from inside:192.168.1.50/1107 to
outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP connection 90 for
outside:172.22.1.1/80
(172.22.1.1/80) to inside:192.168.1.50/1107 (172.22.1.254/1025)
```

日誌顯示，目的IP地址為172.22.1.1，協定為TCP，目的埠為HTTP/80，且流量傳送到外部介面。

- **修改捕獲過濾器。access-list inside_test**命令之前曾使用過，現在也在此使用。

```
ciscoasa(config)#access-list inside_test permit ip host 192.168.1.50 any
!--- This ACL line captures all traffic from 192.168.1.50 !--- that goes to or through the
ASA. ciscoasa(config)#access-list inside_test permit ip any host 192.168.1.50 any
```

```
!--- This ACL line captures all traffic that leaves !--- the ASA and goes to 192.168.1.50.
ciscoasa(config)#no access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#clear capture inside_interface
!--- Clears the previously logged data. !--- The no capture inside_interface removes/deletes
the capture.
```

使用者啟動應用程式X。然後，ASA管理員發出**show capture inside_interface**命令並檢視輸出。

```
ciscoasa(config)#show capture inside_interface
1: 15:59:42.749152 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
2: 15:59:45.659145 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
3: 15:59:51.668742 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
```

捕獲的流量為管理員提供了幾條重要資訊：目的地址 — 172.22.1.1埠號 — 80/http協定 — TCP（注意「S」或syn標誌）此外，管理員還知道應用程式X的資料流量確實到達ASA。如果輸出是此**show capture inside_interface**命令輸出，則應用流量從未到達ASA，或者捕獲過濾器未設定為捕獲流量：

```
ciscoasa#show capture inside_interface
0 packet captured
0 packet shown
```

在這種情況下，管理員應考慮調查使用者電腦以及使用者電腦和ASA之間路徑中的任何路由器或其他網路裝置。**注意：當流量到達介面時，capture命令會在任何ASA安全策略分析流量之前記錄資料。**例如，訪問清單會拒絕介面上的所有傳入流量。**capture**命令仍記錄流量。然後，ASA安全策略分析流量。

- **調試**管理員不熟悉應用程式X，因此不知道要為應用程式X調查啟用哪個調試服務。此時，調試可能不是最佳的故障排除選項。

使用步驟2中收集的資訊，ASA管理員可獲得一些有價值的資訊。管理員知道流量到達ASA的內部介面、源IP地址、目標IP地址以及X使用的服務應用程式(TCP/80)。 從系統日誌，管理員也知道最初允許通訊。

步驟3 — 確認和監控應用流量

ASA管理員希望確認應用X流量已離開ASA，並監控來自應用X伺服器的所有返回流量。

- **監控系統日誌消息。**過濾源IP地址(192.168.1.50)或目標IP地址(172.22.1.1)的系統日誌消息。從命令列中，過濾系統日誌消息類似**show logging |包括192.168.1.50或show logging | include 172.22.1.1。在**本例中，使用**show logging命令時**沒有過濾器。為了便於閱讀，抑制了輸出。

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-7-
609001: Built local-host outside:172.22.1.1 %ASA-6-305011: Built dynamic TCP translation
from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP
connection 90 for outside:172.22.1.1/80 (172.22.1.1/80) to inside:192.168.1.50/1107
(172.22.1.254/1025) %ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80
to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout
%ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30
%ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107
to outside:172.22.1.254/1025 duration 0:01:00
%ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00
```

系統日誌消息指示連線因SYN超時而關閉。這告訴管理員ASA未收到任何應用程式X伺服器響應。系統日誌消息終止原因可能有所不同。由於三次握手完成後30秒後強制連線終止，SYN超時被記錄。如果伺服器無法響應連線請求，並且大多數情況下與PIX/ASA上的配置無關，則通常會發生此問題。要解決此問題，請參閱以下核對清單：確保正確輸入靜態命令，並確保該命

令不會與其他靜態命令重疊，例如，

```
static (inside,outside) x.x.x.x  y.y.y.y netmask 255.255.255.255
```

ASA 8.3及更高版本中的靜態NAT可如下圖所示：

```
object network obj-y.y.y.y
 host y.y.y.y
 nat (inside,outside) static x.x.x.x
```

確儲存在訪問清單，以允許從外部訪問全域性IP地址，並確保該地址已繫結到介面：

```
access-list OUTSIDE_IN extended permit tcp any host x.x.x.x eq www
access-group OUTSIDE_IN in interface outside
```

要成功連線到伺服器，伺服器上的預設網關必須指向PIX/ASA的DMZ介面。有關系統日誌消息的詳細資訊，請參閱ASA系統消息。

- **建立新的捕獲篩選器。**從較早捕獲的流量和系統日誌消息中，管理員知道應用程式X應通過外部介面離開ASA。

```
ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80
!--- When you leave the source as 'any', it allows !--- the administrator to monitor any
network address translation (NAT). ciscoasa(config)#access-list outside_test permit tcp host
172.22.1.1 eq 80 any
!--- When you reverse the source and destination information, !--- it allows return traffic
to be captured. ciscoasa(config)#capture outside_interface access-list outside_test
interface outside
```

使用者需要啟動與應用程式X的新會話。使用者啟動新的應用程式X會話後，ASA管理員需要在ASA上發出**show capture outside_interface**命令。

```
ciscoasa(config)#show capture outside_interface
3 packets captured
   1: 16:15:34.278870 172.22.1.254.1026 > 172.22.1.1.80:
S 1676965539:1676965539(0) win 65535 <mss 1380,nop,nop,sackOK>
   2: 16:15:44.969630 172.22.1.254.1027 > 172.22.1.1.80:
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
   3: 16:15:47.898619 172.22.1.254.1027 > 172.22.1.1.80:
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
3 packets shown
```

捕獲顯示離開外部介面的流量，但不顯示來自172.22.1.1伺服器的任何回覆流量。此捕獲在資料離開ASA時顯示資料。

- **使用packet Tracer選項。**從前面幾節中，ASA管理員學到了足夠的資訊，可以使用ASA中的packet-tracer選項。**註：**ASA支援**從7.2**版開始的**packet**-tracer命令。

```
ciscoasa#packet-tracer input inside tcp 192.168.1.50 1025 172.22.1.1 http
!--- This line indicates a source port of 1025. If the source !--- port is not known, any
number can be used. !--- More common source ports typically range !--- between 1025 and
65535. Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC
Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule
Additional Information: MAC Access list Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW
Config: Additional Information: Found no matching flow, creating a new flow Phase: 4 Type:
ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.22.1.0
255.255.255.0 outside Phase: 5 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-
group inside_acl in interface inside
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 7
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
  match ip inside 192.168.1.0 255.255.255.0 outside any
    dynamic translation to pool 1 (172.22.1.254)
    translate_hits = 6, untranslate_hits = 0
Additional Information:
Dynamic translate 192.168.1.50/1025 to 172.22.1.254/1028
using netmask 255.255.255.255

Phase: 9
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
  match ip inside 192.168.1.0 255.255.255.0 outside any
    dynamic translation to pool 1 (172.22.1.254)
    translate_hits = 6, untranslate_hits = 0
Additional Information:

Phase: 10
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
```

```
    Config:
    Additional Information:
    New flow created with id 94, packet dispatched to next module

    Phase: 15
    Type: ROUTE-LOOKUP
    Subtype: output and adjacency
    Result: ALLOW
    Config:
    Additional Information:
    found next-hop 172.22.1.1 using egress ifc outside
    adjacency Active
    next-hop mac address 0030.a377.f854 hits 11
    !--- The MAC address is at Layer 2 of the OSI model. !--- This tells the administrator the
    next host !--- that should receive the data packet. Result: input-interface: inside input-
    status: up input-line-status: up output-interface: outside output-status: up output-line-
    status: up Action: allow
```

packet-tracer命令的最重**要輸出**是最後一行，即`Action:.`

步驟3中的三個選項均向管理員顯示ASA不負責應用程式X問題。應用X流量離開ASA，且ASA未收到來自應用X伺服器的回覆。

下一步是什麼？

有許多元件可讓應用程式X為使用者正常工作。元件包括使用者的電腦、應用程式X客戶端、路由、訪問策略和應用程式X伺服器。在上一個示例中，我們證明ASA接收並轉發應用X流量。伺服器和應用程式X管理員現在應該參與進來。管理員應驗證應用程式服務是否正在運行，檢視伺服器上的任何日誌，以及驗證伺服器和應用程式X是否接收使用者的流量。

問題：終止TCP代理連線錯誤消息

您收到以下錯誤消息：

```
%PIX|ASA-5-507001: Terminating TCP-Proxy connection from
interface_inside:source_address/source_port to interface_outside:dest_address/dest_port -
reassembly limit of limit bytes exceeded
```

解決方案

說明:此訊息會在裝配TCP區段期間超過重組緩衝區限制時顯示。

- *source_address/source_port* — 發起連線的資料包的源IP地址和源埠。
- *dest_address/dest_port* — 發起連線的資料包的目的IP地址和目的地埠。
- *interface_inside* — 發起連線的資料包到達的介面名稱。
- *interface_outside* — 發起連線的資料包退出所在介面的名稱。
- *limit* — 為流量類配置的初始連線限制。

此問題的解決方法是禁用安全裝置中的RTSP檢查，如圖所示。

```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
```

```
 inspect rsh
 no inspect rtsp
```

如需更多詳細資訊，請參閱Cisco錯誤ID CSCsl1529(僅限註冊客戶)。

問題：%ASA-6-110003:路由無法從src interface找到協定的下一跳「 」錯誤消息

ASA丟棄流量，`%ASA-6-110003:src interface:src IP/src portdest interface:dest IP/dest port`錯誤消息。

解決方案

當ASA嘗試在介面路由表上查詢下一跳時，會發生此錯誤。通常，當ASA具有內建到一個介面的轉換(xlate)和指向不同介面的路由時，會收到此消息。檢查NAT語句是否存在配置錯誤。解決配置錯誤可能會解決該錯誤。

問題：連線被ASA阻止，且「 %ASA-5-305013:為正向和反向流匹配的非對稱NAT規則」錯誤消息

連線被ASA阻止，收到以下錯誤消息：

```
%ASA-5-305013: Asymmetric NAT rules matched for forward
 and reverse flows; Connection protocol src
 interface_name:source_address/source_port dest
 interface_name:dest_address/dest_port denied due to NAT reverse path
 failure.
```

解決方案

當執行NAT時，ASA還會嘗試反轉資料包並檢查這是否影響任何轉換。如果它未命中任何或不同的NAT轉換，則存在不匹配。當為具有相同源和目標的出站和傳入流量配置不同的NAT規則時，最常見的是看到此錯誤消息。檢查NAT語句中相關的流量。

問題：接收錯誤 — %ASA-5-321001:已達到系統的資源「10000」限制

解決方案

此錯誤表示位於ASA上的伺服器的連線已達到最大限制。這可能表示對您網路中的伺服器發起了DoS攻擊。在ASA上使用MPF並降低初始連線限制。此外，啟用失效連線檢測(DCD)。 請參閱以下組態片段：

```
class-map limit
 match access-list limit
!
policy-map global_policy
 class limit
```

```
  set connection embryonic-conn-max 50
  set connection timeout embryonic 0:00:10 dcd
!
access-list limit line 1 extended permit tcp any host x.x.x.x
```

問題：接收錯誤%PIX-1-106021:拒絕在介面int_name上從src_addr到dest_addr的TCP/UDP反向路徑檢查

解決方案

啟用反向路徑檢查時，會收到此日誌消息。發出以下命令可解決問題並停用反向路徑檢查：

```
no ip verify reverse-path interface
```

問題：由於威脅檢測導致的Internet連線中斷

ASA上收到此錯誤消息：

```
%ASA-4-733100: [Miralix Licen 3000] drop rate-1 exceeded. Current burst
rate is 100 per second, max configured rate is 10; Current average rate is 4
per second, max configured rate is 5; Cumulative total count is 2526
```

解決方案

由於檢測到異常流量行為時的預設配置，威脅檢測會生成此消息。該消息重點介紹作為TCP/UDP埠的Miralix Licen 3000。找到使用埠3000的裝置。檢查ASDM圖形統計資訊以進行威脅檢測，並驗證排名靠前的攻擊，檢視它是否顯示埠3000和源IP地址。如果裝置是合法裝置，則可以增加ASA上的基本威脅檢測率，以便解決此錯誤消息。

相關資訊

- Cisco ASA命令參考
- Cisco PIX命令參考
- Cisco ASA錯誤和系統消息
- Cisco PIX錯誤和系統消息
- Cisco ASA 5500系列自適應安全裝置支援
- Cisco PIX 500系列安全裝置支援
- 技術支援與文件 - Cisco Systems