

Troubleshoot Connections through the PIX and ASA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Related Products](#)

[Conventions](#)

[Background Information](#)

[Problem](#)

[Solution](#)

[Step 1 - Discover the IP Address of the User](#)

[Step 2 - Locate the Cause of the Problem](#)

[Step 3 - Confirm and Monitor Application Traffic](#)

[What is Next?](#)

[Problem: Terminating TCP-Proxy Connection Error Message](#)

[Solution](#)

[Problem: "%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface" Error Message](#)

[Solution](#)

[Problem: Connection Blocked by ASA with the " %ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows" Error Message](#)

[Solution](#)

[Problem: Receive error - %ASA-5-321001: Resource 'conns' limit of 10000 reached for system](#)

[Solution](#)

[Problem: Receive error %PIX-1-106021: Deny TCP/UDP reverse path check from src_addr to dest_addr on interface int_name](#)

[Solution](#)

[Problem: Interruption of Internet Connectivity due to Threat Detection](#)

[Solution](#)

[Related Information](#)

[Introduction](#)

This document provides troubleshooting ideas and suggestions for when you use the Cisco ASA 5500 Series Adaptive Security Appliance (ASA) and the Cisco PIX 500 Series Security Appliance. More often than not, when applications or network sources break or are not available, firewalls (PIX or ASA) tend to be a primary target and blamed as the cause of outages. With some testing on the ASA or PIX, an administrator can determine whether or not the ASA/PIX causes the

problem.

Refer to [PIX/ASA: Establish and Troubleshoot Connectivity through the Cisco Security Appliance](#) in order to learn more about the interface related troubleshooting on the Cisco security appliances.

Note: This document focuses on the ASA and PIX. Once troubleshooting is complete on the ASA or PIX, it is likely that additional troubleshooting might be necessary with other devices (routers, switches, servers, and so forth).

[Prerequisites](#)

[Requirements](#)

There are no specific requirements for this document.

[Components Used](#)

The information in this document is based on Cisco ASA 5510 with OS 7.2.1 and 8.3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[Related Products](#)

This document can also be used with these hardware and software versions:

- ASA and PIX OS 7.0, 7.1, 8.3, and later
- Firewall Services Module (FWSM) 2.2, 2.3, and 3.1

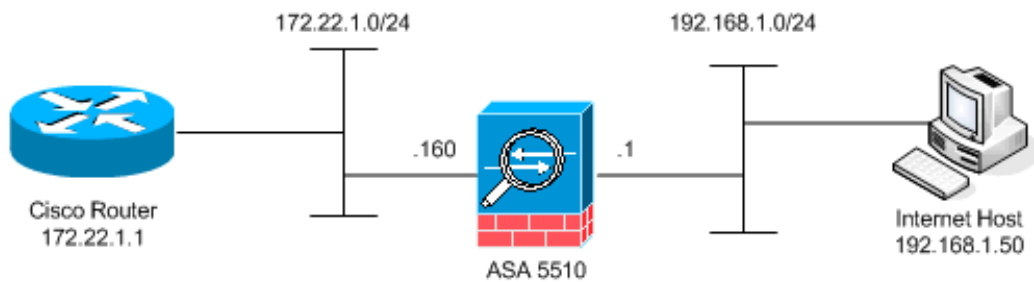
Note: Specific commands and syntax can vary between software versions.

[Conventions](#)

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

[Background Information](#)

The example assumes the ASA or PIX is in production. The ASA/PIX configuration can be relatively simple (only 50 lines of configuration) or complex (hundreds to thousands of configuration lines). Users (clients) or servers can either be on a secure network (inside) or an unsecure network (DMZ or outside).



The ASA starts with this configuration. The configuration is intended to give the lab a reference point.

ASA Initial Configuration

```
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
```

Problem

A user contacts the IT department and reports that application X no longer works. The incident escalates to the ASA/PIX administrator. The administrator has little knowledge of this particular application. With the use of the ASA/PIX, the administrator discovers what ports and protocols application X uses as well as what might be the cause of the problem.

Solution

The ASA/PIX administrator needs to gather as much information from the user as possible. Helpful information includes:

- Source IP address—This is typically the work station or computer of the user.
- Destination IP address—The server IP address that the user or application tries to connect.
- Ports and protocols the application uses

Often the administrator is fortunate if able to get an answer to one of these questions. For this example, the administrator is not able to gather any information. A review of ASA/PIX syslog messages is ideal but it is difficult to locate the problem if the administrator does not know what to look for.

Step 1 - Discover the IP Address of the User

There are many ways to discover the IP address of the user. This document is about the ASA and PIX, so this example uses the ASA and PIX to discover the IP address.

The user attempts to communicate to the ASA/PIX. This communication can be ICMP, Telnet, SSH, or HTTP. The protocol chosen should have limited activity on the ASA/PIX. In this specific example, the user pings the inside interface of the ASA.

The administrator needs to set up one or more of these options and then have the user ping the inside interface of the ASA.

- **Syslog** Make sure logging is enabled. The logging level needs to be set to **debug**. Logging can be sent to various locations. This example uses the ASA log buffer. You might need an external logging server in production environments.

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

 The user pings the inside interface of the ASA (ping 192.168.1.1). This output is displayed.

```
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 Capture Feature** The administrator needs to create an access-list that defines what traffic the ASA needs to capture. After the access-list is defined, the **capture** command incorporates the access-list and applies it to an interface.

```
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
```

 The user pings the inside interface of the ASA (ping 192.168.1.1). This output is displayed.

```
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.
```

Note: In order to download the capture file to a system such as ethereal, you

can do it as this output shows.

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

`https://[<pix_ip>/<asa_ip>]/capture/<capture name>/pcap` Refer to [ASA/PIX: Packet Capturing using CLI and ASDM Configuration Example](#) in order to know more about Packet Capturing in ASA.

- **Debug**The **debug icmp trace** command is used to capture the ICMP traffic of the user.`ciscoasa#debug icmp trace` The user pings the inside interface of the ASA (ping 192.168.1.1). This output is displayed on the console.`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. In order to disable **debug icmp trace**, use one of these commands:**no debug icmp trace****undebug icmp trace****undebug all**, **Undebug all**, or **un all**

Each of these three options helps the administrator to determine the source IP address. In this example, the source IP address of the user is 192.168.1.50. The administrator is ready to learn more about application X and determine the cause of the problem.

Step 2 - Locate the Cause of the Problem

With reference to the information listed in the [Step 1](#) section of this document, the administrator now knows the source of an application X session. The administrator is ready to learn more about application X and to begin to locate where the issues might be.

The ASA/PIX administrator needs to prepare the ASA for at least one of these listed suggestions. Once the administrator is ready, the user initiates application X and limits all other activity since additional user activity might cause confusion or mislead the ASA/PIX administrator.

- **Monitor syslog messages.** Search for the source IP address of the user that you located in [Step 1](#). The user initiates application X. The ASA administrator issues the **show logging** command and views the output.`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) The logs reveal that the destination IP address is 172.22.1.1, the protocol is TCP, the destination port is HTTP/80, and that traffic is sent to the outside interface.
- **Modify the capture filters.** The **access-list inside_test** command was previously used and is used here.`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. The user initiates application X. The ASA administrator then issues the **show capture inside_interface** command and views the output.`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> The captured traffic provides the administrator with several pieces of valuable information: Destination address—172.22.1.1 Port number—80/http Protocol—TCP (notice the "S" or syn flag) In addition, the administrator also knows that the data traffic for application X does arrive at the ASA. If the output had been this **show capture**

inside_interface command output, then the application traffic either never reached the ASA or the capture filter was not set to capture the traffic:

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

In this case, the administrator should consider investigating the user's computer and any router or other network devices in the path between the user computer and the ASA. **Note:** When traffic arrives at an interface, the **capture** command records the data before any ASA security policies analyze the traffic. For example, an access-list denies all incoming traffic on an interface. The **capture** command still records the traffic. The ASA security policy then analyzes the traffic.

- **Debug** The administrator is not familiar with application X and therefore does not know which of the debug services to enable for application X investigation. Debug might not be the best troubleshooting option at this point.

With the information collected in Step 2, the ASA administrator gains several bits of valuable information. The administrator knows the traffic arrives at the inside interface of the ASA, source IP address, destination IP address and the service application X uses (TCP/80). From the syslogs, the administrator also knows that the communication was initially permitted.

[Step 3 - Confirm and Monitor Application Traffic](#)

The ASA administrator wants to confirm that application X traffic has left the ASA as well as monitor any return traffic from the application X server.

- **Monitor syslog messages.** Filter syslog messages for the source IP address (192.168.1.50) or the destination IP address (172.22.1.1). From the command line, filtering syslog messages look like **show logging | include 192.168.1.50** or **show logging | include 172.22.1.1**. In this example, the **show logging** command is used without filters. The output is suppressed in order to make reading easy.

```
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 The syslog message indicates the connection closed because of SYN timeout. This tells the administrator that no application X server responses were received by the ASA. Syslog message termination reasons can vary. The SYN timeout gets logged because of a forced connection termination after 30 seconds that occurs after the three-way handshake completion. This issue usually occurs if the server fails to respond to a connection request, and, in most cases, is not related to the configuration on PIX/ASA. In order to resolve this issue, refer to this checklist: Make sure the static command is entered correctly and that it does not overlap with other static commands, for example,

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

The static NAT in ASA 8.3 and later can be configured as shown here:

```
object network obj-
Y.Y.Y.Y
 host y.y.y.y
```

nat (inside,outside) static x.x.x.x Make sure that an access list exists in order to permit access to the global IP address from the outside and that it is bound to the interface:

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

For a successful connection with the server, the default gateway on the server must point

towards the DMZ interface of PIX/ASA. Refer to [ASA System Messages](#) for more information on the syslog messages.

- **Create a new capture filter.** From earlier captured traffic and syslog messages, the administrator knows that application X should leave the ASA through the outside

```
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
```

The user needs to initiate a new session with application X. After the user has initiated a new application X session, the ASA administrator needs to issue the **show capture outside_interface** command on the ASA.

```
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
```

- **Use the packet-tracer option.** From previous sections, the ASA administrator has learned enough information to use the **packet-tracer** option in the ASA. **Note:** The ASA supports the

```
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
```

The most important output of the **packet-tracer** command is the last line, which is Action: allow.

The three options in Step 3 each show the administrator that the ASA is not responsible for the application X issues. The application X traffic leaves the ASA and the ASA does not receive a reply from the application X server.

What is Next?

There are many components that allow application X to work correctly for users. The components include the user's computer, the application X client, routing, access policies, and the application X server. In the previous example, we proved that the ASA receives and forwards the application X traffic. The server and application X administrators should now get involved. Administrators should verify that the application services are running, review any logs on the server, and verify that the user's traffic is received by the server and application X.

Problem: Terminating TCP-Proxy Connection Error Message

You receive this error message:

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

Solution

Explanation: This message displays when the reassembly buffer limit is exceeded during assembling TCP segments.

- *source_address/source_port* - The source IP address and the source port of the packet initiating the connection.
- *dest_address/dest_port* - The destination IP address and the destination port of the packet initiating the connection.
- *interface_inside* - The name of the interface on which the packet which initiated the connection arrives.
- *interface_outside* - The name of the interface on which the packet which initiated the connection exits.
- *limit* - The configured embryonic connection limit for the traffic class.

The resolution for this issue is to disable the RTSP inspection in the security appliance as shown.

```
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
```

Refer to Cisco bug ID [CSCsl15229](#) ([registered](#) customers only) for more details.

Problem: "%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface" Error Message

ASA drops traffic with the error:%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port error message.

Solution

This error occurs when the ASA tries to find the next hop on an interface routing table. Typically, this message is received when ASA has a translation (xlate) built to one interface and a route pointing out a different interface. Check for a misconfiguration on the NAT statements. Resolution of the misconfiguration may resolve the error.

Problem: Connection Blocked by ASA with the "%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows" Error Message

The connection is blocked by ASA, and this error message is received:

```
%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.
```

Solution

When the NAT is performed, ASA also tries to reverse the packet and checks if this hits any translation. If it does not hit any or a different NAT translation, then there is a mismatch. You most commonly see this error message when there are different NAT rules configured for outbound and incoming traffic with same source and destination. Check the NAT statement for the concerned traffic.

Problem: Receive error - %ASA-5-321001: Resource 'conns' limit of 10000 reached for system

Solution

This error signifies that the connections for a server located across an ASA have reached their maximum limit. This could be an indication of a DoS attack to a server in your network. Use MPF on the ASA and reduce the embryonic connections limit. Also, enable Dead Connection Detection (DCD). Refer to this configuration snippet:

```
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
```

Problem: Receive error %PIX-1-106021: Deny TCP/UDP reverse path check from src_addr to dest_addr on interface

[int_name](#)

[Solution](#)

This log message is received when the reverse path check is enabled. Issue this command in order to resolve the problem and disable the reverse path check:

```
no ip verify reverse-path interface <interface name>
```

[Problem: Interruption of Internet Connectivity due to Threat Detection](#)

This error message is received on the ASA:

```
%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
```

[Solution](#)

This message is generated by threat detection due to the default configuration when an anomalous traffic behavior is detected. The message focuses on Miralix Licen 3000 which is a TCP/UDP port. Locate the device which is using port 3000. Check on the ASDM graphical statistics for threat detection and verify the top attacks to see if it shows port 3000 and the source IP address. If it is a legitimate device, you can increment the basic threat detection rate on ASA in order to resolve this error message.

[Related Information](#)

- [Cisco ASA Command Reference](#)
- [Cisco PIX Command Reference](#)
- [Cisco ASA Error and System Messages](#)
- [Cisco PIX Error and System Messages](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances Support](#)
- [Cisco PIX 500 Series Security Appliances Support](#)
- [Technical Support & Documentation - Cisco Systems](#)