排除通过 PIX 和 ASA 的连接故障

目录

简介

本文档提供有关使用 Cisco ASA 5500 系列自适应安全设备 (ASA) 和 Cisco PIX 500 系列安全设备时的故障排除方法和建议。当应用程序或网络源中断或不可用时，防火墙（PIX 或 ASA）通常成为主要目标并可能引起中断。管理员在 ASA 或 PIX 上进行一些测试便能确定是否为 ASA/PIX 引发的问题。

请参阅 PIX/ASA：通过 Cisco 安全设备建立连接并排除连接故障获取有关在 Cisco 安全设备上进行接口相关故障排除的详细信息。

注意： 本文档重点介绍 ASA 和 PIX。在 ASA 或 PIX 上完成故障排除后，有可能需要在其他设备

（路由器、交换机、服务器等等）上进行额外的故障排除。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据与OS 7.2.1和8.3的思科ASA 5510。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

本文档也可用于以下硬件和软件版本：

- ASA和PIX OS 7.0， 7.1， 8.3和以后
- 防火墙服务模块 (FWSM) 2.2、2.3 和 3.1

注意： 特定命令和语法因软件版本而异。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

示例假设 ASA 或 PIX 处于生产状态。ASA/PIX 配置可以相对简单（仅有 50 个配置行），以可以相对复杂（有成百上千的配置行）。用户（客户端）或服务器可以在安全网络（内部）上，也可以在不安全网络（DMZ 或外部）上。

ASA 从此配置开始。此配置旨在为实验室提供一个参考点。

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
```

问题

用户与 IT 部门联系并报告应用程序 X 不再运行。事件将上报至 ASA/PIX 管理员。管理员不大了解此特定应用程序。使用 ASA/PIX，管理员可发现应用程序 X 使用哪些端口和协议，也可发现问题的可能根源。

解决方案

ASA/PIX 管理员需要从用户收集尽可能多的信息。有用的信息包括：

- 源 IP 地址 - 通常指工作组或用户计算机。
- 目标 IP 地址 - 用户或应用程序尝试连接的服务器 IP 地址。
- 应用程序使用的端口和协议

如果能获得这些问题的其中一个答案，通常管理员比较幸运。对于此示例，管理员无法收集任何信息。理想方案是回顾 ASA/PIX syslog 消息，但如果管理员不知道该寻找什么，就很难找到问题。

步骤 1 - 发现用户的 IP 地址

可通过许多方式发现用户的 IP 地址。本文当与 ASA 和 PIX 有关，因此本示例使用 ASA 和 PIX 发现 IP 地址。

用户尝试与 ASA/PIX 通信。此通信可以是 ICMP、Telnet、SSH，也可以是 HTTP。选择的协议在 ASA/PIX 上应具有有限的活动。在此特定示例中，用户对 ASA 的内部接口进行 ping 操作。

管理员需要设置其中一个或多个选项，然后让用户对 ASA 的内部接口进行 ping 操作。

- **Syslog**确保日志记录已启用。日志记录级别需设置为 **debug**。可以将日志记录发送到不同位置。此示例使用 ASA 日志缓冲区。在生产环境中，您可能需要一台外部日志记录服务器。
  `ciscoasa(config)#logging enable ciscoasa(config)#logging buffered debugging` 用户对 ASA 的内部接口进行 ping 操作 (ping 192.168.1.1)。将显示此输出。`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 捕获功能**管理员需创建一个定义 ASA 需捕获哪些流量的访问列表。定义访问列表后，**capture** 命令将合并访问列表并将其应用到接口上。`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` 用户对 ASA 的内部接口进行 ping 操作 (ping 192.168.1.1)。将显示此输出。`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：** 要将捕获文件下载到某个系统（如 ethereal），您可以按照此输出显示的内容进行操作。
  `!--- Open an Internet Explorer and browse with this https link format:`
  `https://[<pix_ip>/<asa_ip>]/capture/<capture name>/pcap` 请参阅 ASA/PIX：使用 CLI 和 ASDM 配置示例的数据包捕获获取有关 ASA 中数据包捕获的详细信息。
- 调试**debug icmp trace** 命令用于捕获用户的 ICMP 流量。`ciscoasa#debug icmp trace` 用户对 ASA 的内部接口进行 ping 操作 (ping 192.168.1.1)。此输出显示在控制台上。`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.` 要禁用 **debug icmp trace**，请使用以下命令之一：**no debug icmp traceundebug icmp traceundebug all**、**Undebug all** 或 **un all**

这三个选项中的每一个都能帮助管理员确定源 IP 地址。在此示例中，用户的源 IP 地址为 192.168.1.50。管理员准备好详细了解应用程序 X 并确定问题的根源。

步骤 2 - 找出问题的根源

通过参考本文档步骤 1 部分中列出的信息，管理员现在知道了应用程序 X 会话的源。管理员准备好详细了解应用程序 X 并开始寻找问题的根源。

为执行以下所列的其中一条建议，ASA/PIX 管理员需要准备 ASA。管理员准备好后，用户将启动应用程序 X 并限制其他所有活动，因为用户的其他活动可能会造成干扰或误导 ASA/PIX 管理员。

- **监控 syslog 消息。**搜索您在步骤 1 中找到的用户的源 IP 地址。用户启动应用程序 X。ASA 管理员发出 **show logging** 命令并查看输出。`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)` 日志显示目标 IP 地址为 172.22.1.1，协议为 TCP，目标端口为 HTTP/80，并且流量发送到外部接口。
- **修改捕获过滤器。**先前使用了 **access-list inside_test** 命令，此处也将用到。
  `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.* 用户启动应用程序 X。然后，ASA 管理员发出 **show capture inside_interface** 命令并查看输出。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> 捕获的流量将为管理员提供几条重要信息：目标地址 - 172.22.1.1端口号 - 80/http协议 - TCP（请注意“S”或同步标记）另外，管理员还知道应用程序 X 的数据流量确实到达 ASA。如果输出已经是此 **show capture inside_interface** 命令的输出，则应用流量从未到达 ASA 或者捕获过滤器未设置为捕获流量：ciscoasa#**show capture inside_interface** 0 packet captured 0 packet shown 这种情况下，管理员应考虑调查用户计算机以及位于用户计算机与 ASA 之间路径上的任何路由器或其他网络设备。**注意：** 当流量到达接口时，**capture** 命令会在所有 ASA 安全策略分析流量之前记录数据。例如，访问列表拒绝接口上的所有传入流量。**Capture** 命令仍会记录流量。然后，ASA 安全策略分析流量。
- 调试管理员不熟悉应用程序 X，因此不知道为应用程序 X 调查启用哪个调试服务。此时调试可能不是最好的故障排除选项。

在获得步骤 2 中收集的信息后，ASA 管理员即获得以下几点重要信息。管理员知道流量到达 ASA 的内部接口、源 IP 地址、目标 IP 地址并且服务应用程序 X 使用 (TCP/80)。从 syslog，管理员还知道最初允许的通信。

步骤 3 - 确认和监控应用流量

ASA 管理员需要确认应用程序 X 流量已离开 ASA 并监控从应用程序 X 服务器返回的所有流量。

- **监控 syslog 消息。**为源 IP 地址 (192.168.1.50) 或目标 IP 地址 (172.22.1.1) 过滤 syslog 消息。从命令行，过滤 syslog 消息看起来像 **show logging|include 192.168.1.50** 或 **show logging|include 172.22.1.1**。在此示例中，在没有过滤器的情况下使用 **show logging** 命令。为方便读取抑制了输出。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 Syslog 消息指示由于 SYN 超时而关闭连接。这告诉管理员 ASA 并未收到应用程序 X 服务器的任何响应。Syslog 消息终止的原因可能有很多。SYN 超时因三方握手完成 30 秒后发生的强制性连接终止而被记录。此问题通常出现在服务器不能响应连接请求，并且在大多数情况下与 PIX/ASA 上的配置不相关时。为解决此问题，请参阅以下清单：确保正确输入 static 命令，并且该命令不与其他 static 命令重叠，例如，static (inside,outside) x.x.x.x y.y.y.y netmask 255.255.255.255
静态NAT在ASA 8.3及以后可以配置如显示此处：object network obj-y.y.y.y
 host y.y.y.y
 nat (inside,outside) static x.x.x.x确保访问列表存在，以便允许从外部访问全局 IP 地址，以及确保绑定到接口：
access-list OUTSIDE_IN extended permit tcp any host x.x.x.x eq www
access-group OUTSIDE_IN in interface outside
要与服务器成功连接，服务器上的默认网关必须指向 PIX/ASA 的 DMZ 接口。请参阅 ASA 系统消息获取有关 syslog 消息的详细信息。

- **创建新的捕获过滤器。**从早期捕获的流量和 syslog 消息，管理员知道应用程序 X 应通过外部接口离开 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`** 用户需要通过应用程序 X 启动一个新会话。用户启动新的应用程序 X 会话后，ASA 管理员需要在 ASA 上发出 **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
  ```
  捕获显示离开外部接口的流量，但不显示来自 172.22.1.1 服务器的任何回复流量。离开 ASA 时，此捕获会显示数据。
- **使用 packet-tracer 选项。**从前面几节，ASA 管理员已经了解了足够的信息，能够使用 ASA 中的 **Packet Tracer** 选项。**注意：** 从版本 7.2 开始，ASA 支持 **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** 命令最重要的输出是最后一行，即 Action:。

步骤 3 中的三个选项都向管理员显示 ASA 与应用程序 X 问题无关。应用程序 X 流量离开 ASA，并且 ASA 未收到来自应用程序 X 服务器的回复。

接下来做什么？

许多组件都可以使用户的应用程序 X 正确运行。组件包括用户的计算机、应用程序 X 客户端、路由、访问策略和应用程序 X 服务器。在前一个示例中，我们已证明 ASA 收到并转发应用程序 X 流量。服务器和应用程序 X 管理员现在应参与其中。管理员应验证应用程序服务正在运行，查看服务器上的所有日志，并验证服务器和应用程序 X 收到的用户流量。

问题：终止 TCP 代理连接错误消息

您将收到以下错误消息：

```
%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
```

解决方案

说明：如果在装配 TCP 网段期间超过了重组缓冲限制，则将显示此消息。

- *source_address/source_port* - 源 IP 地址和启动连接的数据包的源端口。
- *dest_address/dest_port* - 目标 IP 地址和启动连接的数据包的目标端口。
- *interface_inside* - 启动连接的数据包所到达接口的名称。
- *interface_outside* - 启动连接的数据包所退出接口的名称。
- *limit* - 流量类别的已配置初期连接限制。

此问题的解决方法是禁用安全设备中的 RTSP 检查，如下所示。

```
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
```

参考的Cisco Bug ID CSCsl15229 (仅限注册用户)欲了解更详细的信息。

问题："%ASA-6-110003 ：失败的路由找出协议的下一跳从src接口"错误消息

ASA与`error:%ASA-6-110003`丢包流量`srcsrc IP/srcIP/dest Port`。

解决方案

当ASA设法查找在接口路由表的下一跳此错误出现。一般，此消息接收，当ASA有一个转换(xlate)时被建立对一个接口和指出一个不同的接口的路由。检查在NAT语句的一误配置。误配置的解决方法可能解决错误。

问题：与"%ASA-5-305013的ASA阻塞的连接：为转发和反向流"错误消息匹配的不对称NAT规则

连接由ASA阻塞，并且此错误消息接收：

```
%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.
```

解决方案

当NAT执行时， ASA也设法倒转数据包和检查这是否点击任何转换。如果它不点击其中任一或一个不同的NAT转换，则有不匹配。当有为与同样源和目的时的出站和流入的数据流配置的不同的NAT规则您通常看到此错误消息。检查NAT语句担心的流量。

问题：接收错误- %ASA-5-321001 ：资源'为系统到达的conns'限制10000

解决方案

此错误表示在ASA间查找的服务器的连接达到了他们的最大限制。这能是DOS攻击的征兆到在您的网络的一个服务器。请使用在ASA的MPF并且降低初期连接限制。并且，请启动停止的连接检测(DCD)。参考此配置片断：

```
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
```

问题：接收错误%PIX-1-106021 ：拒绝TCP/UDP反向路径检查从src_addr到dest_addr在接口int_name

解决方案

当反向路径检查启用时，此日志消息接收。发出此命令为了解决问题和禁用反向路径检查：

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

问题：Internet连接的中断由于威胁检测

此错误消息在ASA接收：

```
%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
```

解决方案

当一种异常通信流量检测时，此消息由威胁检测生成由于默认配置。消息着重是TCP/UDP端口的Miralix Licen 3000。找出使用端口3000的设备。检查在ASDM图形统计信息威胁检测并且验证击顶制导发现是否显示端口3000和源IP地址。如果它是一个合法设备，您能增加在ASA的基本威胁检测速率为了解决此错误消息。

相关信息

- Cisco ASA 命令参考
- Cisco PIX 命令参考
- Cisco ASA 错误和系统消息
- Cisco PIX 错误和系统消息
- Cisco ASA 5500 系列自适应安全设备支持
- Cisco PIX 500 系列安全设备支持
- 技术支持和文档 - Cisco Systems