ASA 8.3 及更高版本：监控并且排除性能问题故障

目录

简介

本文提供了有关可用于监视思科自适应安全设备 (ASA) 性能并排除故障的 ASA 命令的信息。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于运行 8.3 及以上版本的 Cisco 自适应安全设备 (ASA).

本文档中的信息都是基于特定实验室环境中的设备创建的。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，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

故障排除

为了排除性能故障问题，请检查本部分所述的基本区域。

> **注意**：如果有输出**show命令**从您的Cisco设备，您能使用Cisco CLI分析器(仅限注册用户)为了显示潜在问题和修正。确定Cisco CLI分析程序支持**显示**命令。如果使用Cisco CLI分析器，您必须是注册用户，您必须登陆到您的思科帐户，并且您必须有在您的浏览器内启用的Javascript。

速度和双工设置

安全设备被预先配置为自动检测接口上的速度及双工设置。然而，存在几种情况，这些情况可能会造成自动协商过程失败，从而导致速度或双工不匹配（以及性能问题）。对于任务关键型网络基础架构，Cisco 对于每个接口的速度和双工采用手动硬编码，这样就避免了发生错误的机会。这些设备通常不会四处移动，因此，如果您适当地配置了它们，您就不需要进行更改了。

在所有网络设备上，可以检测链路速度，但是必须协商双工。如果两个网络设备被配置为自动协商速度和双工，则它们会交换帧（称为快速链路脉冲 (FLP)），这些帧会通告它们的速度和双工能力。对于未知的链路伙伴，这些脉冲类似于普通的 10 Mbps 帧。对于能对脉冲进行解码的链路伙伴，FLP 包含链路伙伴能提供的所有速度和双工设置。接收 FLP 的站点对帧进行确认，设备双方就彼此都能达到的最高速度和双工设置达成一致。如果一个设备不支持自动协商，则另一个设备接收 FLP 并转换到并行检测模式。为了检测伙伴的速度，设备对脉冲长度进行监听，然后相应地设定速度。问题通常发生在双工设置上。由于必须协商双工，设置为自动协商的设备无法确定其他设备的设置，因此其默认为半双工，如 IEEE 802.3u 标准中所述。

例如，如果将 ASA 接口配置为自动协商并将其连接至针对速度 100 Mbps 和全双工模式进行硬编码的交换机，则 ASA 会发出 FLP。然而，交换机不会响应，因为它的速度和双工是硬编码的，它不会参与自动协商。由于未收到交换机的响应，ASA 会过渡到并行检测模式并感应交换机发出的帧中的脉长。即，ASA 会感应到此交换机设置为 100 Mbps，因此它会相应地设置接口速度。但是，由于交换机不会交换 FLP，ASA 无法检测交换机是否能运行全双工，因此 ASA 会将接口双工设置为半双工，如 IEEE 803.2u 标准中所述。由于交换机会针对速度 100 Mbps 和全双工模式进行硬编码，并且 ASA 刚刚自动协商为 100 Mbps 和半双工（按预期），这样的结果是双工不匹配，从而可能会引起严重性能问题。

速度或双工不匹配主要表现在相关端口上的错误计数器的计数增加。最常见的错误是帧、循环冗余校验 (CRCs) 和残帧。如果接口上的这些值增加，则表明发生了速度/双工不匹配或电缆连接问题。在您继续前，您必须解决此问题。

示例

```
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
 Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
       Input flow control is unsupported, output flow control is unsupported
       MAC address 0013.c480.b2b8, MTU 1500
       IP address 192.168.17.4, subnet mask 255.255.255.0
       311981 packets input, 20497296 bytes, 0 no buffer
       Received 311981 broadcasts, 157 runts, 0 giants 379 input errors, 107 CRC, 273 frame, 0
overrun, 0 ignored, 0 abort 0 pause input, 0 resume input 0 L2 decode drops 121 packets output,
```

```
7744 bytes, 0 underruns 0 pause output, 0 resume output 0 output errors, 0 collisions, 1
interface resets 0 late collisions, 0 deferred 0 input reset drops, 0 output reset drops, 0 tx
hangs input queue (blocks free curr/low): hardware (255/249) output queue (blocks free
curr/low): hardware (255/254)
```

CPU 利用率

如果您注意到 CPU 使用率很高，请完成以下步骤以进行故障排除：

1. 确认 **show xlate count** 中的连接计数较低。
2. 确认内存块正常。
3. 确认 ACL 数量较高。
4. 发出 **show memory detail 命令**，并确认 ASA 使用的内存为正常使用率。
5. 确认 **show processes cpu-hog** 和 **show processes memory** 中的计数正常。
6. 所有存在于安全设备内部或外部的主机都可能会生成恶意或大量的流量，这些流量可能是广播/组播流量，它们会导致高 CPU 利用率。为了解决此问题，请配置一个访问列表以拒绝主机（端对端）之间的流量并检查使用情况。
7. 检查 ASA 接口中的双工和速度设置。与远程接口的设置不匹配会增加 CPU 利用率。

   本示例显示了因为速度不匹配而造成 *input error* 和 *overruns* 的值较大。请使用 **show interface** 命令验证错误：

   ```
   Ciscoasa#sh int GigabitEthernet0/1 Interface GigabitEthernet0/1 "inside", is up, line
   protocol is up Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-
   duplex), Auto-Speed(100 Mbps) Input flow control is unsupported, output flow control is
   unsupported MAC address 0013.c480.b2b8, MTU 1500 IP address 192.168.17.4, subnet mask
   255.255.255.0 311981 packets input, 20497296 bytes, 0 no buffer Received 311981 broadcasts,
   157 runts, 0 giants 7186 input errors, 0 CRC, 0 frame, 7186 overrun, 0 ignored, 0 abort 0
   pause input, 0 resume input 0 L2 decode drops 121 packets output, 7744 bytes, 0 underruns 0
   pause output, 0 resume output 0 output errors, 0 collisions, 1 interface resets 0 late
   collisions, 0 deferred 0 input reset drops, 0 output reset drops, 0 tx hangs input queue
   (blocks free curr/low): hardware (255/249) output queue (blocks free curr/low): hardware
   (255/254)
   ```

   为了解决此问题，请将相应接口的速度设置为 *auto*。

   注意：Cisco 建议您在所有接口上启用 ip verify reverse-path interface 命令，因为此设置会将没有有效源地址的数据包丢弃，从而减少 CPU 使用率。这适用于面临高 CPU 问题的 FWSM。
8. 高 CPU 使用率的另一个原因可以归结于太多的组播路由。发出 show mroute 命令来检查 ASA 是否收到过多组播路由。
9. 使用 show local-host 命令查看网络是否受到了拒绝服务攻击，该攻击表明网络可能受到病毒

攻击。

10. 由于思科漏洞 ID CSCsq48636，可能会发生高 CPU 使用率的情况。有关更多信息，请参阅思科漏洞 ID CSCsq48636（仅限注册用户）。

注意：如果上述提供的解决方案不能解决此问题，请根据要求升级 ASA 平台。有关自适应安全设备平台功能和能力的更多信息，请参阅 Cisco ASA 5500 系列自适应安全设备产品手册。有关更多信息，请联系 TAC（仅限注册用户）。

高内存利用率

以下是造成高内存利用率的可能原因以及相应解决方法：

- **事件日志记录**：事件日志记录会占用大量内存。为了解决此问题，请将所有事件安装并记录到一个外部服务器上，例如 Syslog 服务器。
- **内存泄漏**：安全设备软件中的已知问题可能会导致高内存消耗。为了解决此问题，请升级安全设备软件。
- **启用调试**：调试会占用大量内存。为了解决此问题，请使用 undebug all 命令禁用调试。
- **阻塞端口**：安全设备外部接口上的阻塞端口会导致安全设备占用大量内存来通过指定的端口阻止相关数据包。为了解决此问题，请在 ISP 端阻止恶意流量。
- **威胁检测**：威胁检测功能包括针对各种威胁进行的不同级别的统计信息收集，也包括用以确定主机何时执行扫描的扫描威胁检测功能。**关闭**这一功能以减少内存消耗。

PortFast、信道和中继

默认情况下，许多交换机（例如运行 Catalyst 操作系统 (OS) 的 Cisco 交换机）都被设计为即插即用设备。正因如此，当 ASA 插入交换机时，许多默认端口参数并不适用。例如，在运行 Catalyst OS 的交换机上，默认情况下，信道和中继设置为自动，而 PortFast 设置为禁用。如果将 ASA 连接至运行 Catalyst 操作系统的交换机，请禁用通道、禁用中继并启用 PortFast。

信道也称为 Fast EtherChannel 或 Giga EtherChannel，用于将两个或更多物理端口捆绑到一个逻辑组中，以增加链路上的总吞吐量。如果端口配置为自动建立信道，它会在链路接通时发出端口聚合协议 (PAgP) 帧，以确定它是否是信道的一部分。如果另一设备设法自动协商链路速度和双工

，这些帧可能会造成问题。如果端口上的信道设置为自动，则在链路接通、端口开始转发数据流之前，它将导致大约 3 秒的额外延迟。

> **注意**：在 Catalyst XL 系列交换机上，默认情况下信道没有设置为自动。为此，您应该在连接至 ASA 的所有交换机端口上禁用通道。

中继也称为交换机间链路 (ISL) 或 Dot1q（通用的中继协议），它将多个虚拟 LAN (VLAN) 结合到单个端口（或链路）上。当两台交换机上定义的 VLAN 都超过一个时，这二台交换机之间通常使用中继。如果端口配置为自动中继，它会在链路接通时发出动态中继协议 (DTP) 帧，以确定它所连接的端口是否想要中继。这些 DTP 帧可能会导致链路自动协商产生问题。如果交换机端口上的中继设置为自动，则在链路接通、端口开始转发数据流之前，它将导致大约 15 秒的额外延迟。

PortFast（也称为快速启动）选项可以告诉交换机，有一个第 3 层设备通过交换机端口与外部连接。端口并不会等待默认的 30 秒（15 秒监听，15 秒学习）；相反，这一操作会使交换机在链路接通后立即将端口置于转发状态。重要的是要了解，当您启用 PortFast 时，生成树并没有被禁用。生成树在该端口上仍然处于活动状态。当您启用 PortFast 时，交换机仅仅被通知没有另一台交换机或集线器（只在第 2 层工作的设备）连接到链路的另一端。交换机会绕过正常的 30 秒延迟，同时设法确定是否会让那个端口产生第二层环路。在链路启动后，它仍然参与生成树。该端口会发出网桥数据包数据单元 (BPDU)，并且交换机仍然会在该端口监听 BPDU。由于这些原因，建议您在连接至 ASA 的所有交换机端口上启用 Portfast。

> **注意**：Catalyst OS 版本 5.4 及更高版本包含 **set port host <mod>/<port>** 命令，该命令使您可以使用单个命令来禁用信道和中继以及启用 PortFast。

网络地址转换 (NAT)

每个 NAT 或 NAT 过载 (PAT) 会话会被分配一个称为 *xlate* 的转换插槽。即使您对影响这些 xlate 的 NAT 规则进行了更改，这些 xlate 仍然会存在。在此情况下，进行转换所使用的流量会导致转换插槽耗尽或意外行为的发生，或者两者皆有。本部分说明如何查看和清除安全设备上的 xlate。

> **警告：**当您在安全设备上全局清除转换项时，流经此设备的所有流量可能会短暂中断。

使用外部接口 IP 地址的 PAT 的 ASA 配置示例：

```
object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0

nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface
```

流经安全设备的数据流很可能经过 NAT。要查看安全设备上所使用的转换，请发出 **show xlate** 命令：

```
Ciscoasa#show xlate 5 in use, 5 most used Flags: D - DNS, i - dynamic, r - portmap, s - static,
I - identity, T - twice NAT from any:192.168.1.10 to any:172.16.1.1/24 flags s idle 277:05:26
timeout 0:00:00
```

即使进行了关键的更改，转换插槽仍然可存在。要清除安全设备上的当前转换插槽，请发出 **clear xlate** 命令：

```
Ciscoasa#clear xlate
```

```
Ciscoasa#show xlate 0 in use, 1 most used
```

clear xlate 命令会从 xlate 表中清除所有当前的动态转换。要清除某个特定的 IP 转换，您可以以 **global [ip address]** 为关键字使用 **clear xlate** 命令。

以下是 NAT 的一个 ASA 配置示例：

```
object network inside-net
subnet 0.0.0.0 0.0.0.0
object network outside-pat-pool
range 10.10.10.10 10.10.10.100
nat (inside,outside) source dynamic inside-net  outside-pat-pool
```

观察 **show xlate** 的输出，注意从内部 10.2.2.2 到外部全局 10.10.10.10 的转换：

```
Ciscoasa#show xlate 2 in use, 2 most used Flags: D - DNS, i - dynamic, r - portmap, s - static,
I - identity, T - twice TCP PAT from inside:10.2.2.2/1429 to any:10.10.10.10/64768 flags ri idle
62:33:57 timeout 0:00:30 TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri
idle 62:33:57 timeout 0:00:30
```

清除 10.10.10.10 全局 IP 地址的转换：

```
Ciscoasa# clear xlate global 10.10.10.10
```

在本示例中，从内部 10.2.2.2 到外部全局 10.10.10.10 的转换已经被清除：

```
Ciscoasa#show xlate 1 in use, 2 most used Flags: D - DNS, i - dynamic, r - portmap, s - static,
I - identity, T - twice TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri idle
62:33:57 timeout 0:00:30
```

系统日志

系统日志允许您排除 ASA 上的故障。思科为 Windows NT 提供了一个名为 ASA 防火墙系统日志服务器 (PFSS) 的免费系统日志服务器。您可以从软件下载（仅限注册用户）页面下载 PFSS。

其他一些供应商（例如 Kiwi Enterprises ）提供了适用于各种 Windows 平台（例如 Windows 2000 和 Windows XP）的 Syslog 服务器。 默认情况下，多数 UNIX 和 Linux 计算机都安装了 Syslog 服务器。

当设置系统日志服务器时，请配置 ASA 以便向其发送日志。

例如：

```
logging on logging host <ip_address_of_syslog_server> logging trap debugging
```

> **注意**：此示例将 ASA 配置为将调试（级别 7）及更多关键系统日志发送到系统日志服务器。由于这些 ASA 日志是最详细的，因此只在排除故障时使用它们。为确保正常运行，请将日志记录级别配置为警告（第 4 级）或错误（第 3 级）。

如果您遇到性能下降的问题，请在文本文件中打开 Syslog，搜索与性能问题有关的源 IP 地址。（如果您使用的是 UNIX，您也可以在 Syslog 中以查找字符串的形式查找源 IP 地址。）检查指示外部服务器曾经尝试访问 TCP 端口 113 上的内部 IP 地址（适用于识别协议或 Ident），但 ASA 拒绝了数据包的消息。此类消息应与此示例类似：

```
%ASA-2-106001: Inbound TCP connection denied from
10.64.10.2/35969 to 172.17.110.179/113 flags SYN
```

如果您收到此消息，请向 ASA 发出 service resetinbound 命令。ASA 不会静默地丢弃数据包；反而，此命令会让 ASA 立即重置被安全策略拒绝的所有入站连接。服务器无需等到 Ident 数据包的 TCP 连接超时；相反，它会立即收到一个重置数据包。

SNMP

使用 SNMP 监视 Cisco ASA 性能使是企业部署的推荐方法。Cisco ASA 支持使用 SNMP 1、2c 和 3 版本进行网络监视。

您可将安全设备配置为向网络管理服务器 (NMS) 发送陷阱，或者可使用 NMS 在安全设备上浏览 MIB。MIB 是一个定义集合，安全设备为每个定义维护一个值数据库。有关此项的更多信息，请参阅在 Cisco ASA 上配置 SNMP。

有关 Cisco ASA 支持的所有 MIB，请参阅 ASA MIB 支持列表。在此列表中，这些 MIB 对于性能监视十分有用：

- CISCO-FIREWALL-MIB----包含对故障转移有用的对象
- CISCO-PROCESS-MIB----包含对 CPU 使用率有用的对象
- CISCO-MEMORY-POOL-MIB----包含对内存对象有用的对象。

逆向 DNS 查找

如果您发现 ASA 性能下降，请验证在 ASA 使用的外部地址的授权 DNS 服务器中是否有域名系统指针 (DNS PTR) 记录（也称为反向 DNS 查找记录）。这包括全局网络地址转换 (NAT) 池（或如果接口过载，则为 ASA 外部接口）中的任何地址、任何静态地址和内部地址（如果未对其使用 NAT）。某些应用程序（例如文件传输协议 (FTP) 和 Telnet 服务器）可能会使用逆向 DNS 查找，以确定用户来自何处以及它是否是有效的主机。如果逆向 DNS 查找没有得到解析，那么性能就会在请求超时时下降。

要确保这些主机的 PTR 记录存在，请从您的 PC 或 UNIX 计算机上发出 **nslookup** 命令；加上您连接到互联网时使用的全局 IP 地址。

示例

```
% nslookup 198.133.219.25 25.219.133.198.in-addr.arpa name = www.cisco.com.
```

您应该收到响应，该响应包含分配到该 IP 地址的设备的 DNS 名称。如果没有收到响应，请联系控制 DNS 的人员，请求为每个全局 IP 地址添加 PTR 记录。

在接口上溢出

如果流量突发，在突发流量超出 NIC 上的 FIFO 缓冲区和接收环形缓冲区的缓冲量时，可能会出现丢弃数据包的情况。启用暂停帧进行流量控制，可缓解此问题。暂停 (XOFF) 和 XON 帧由基于 FIFO 缓冲区使用情况的 NIC 硬件自动生成。当缓冲用量超出高水位线标记时，会发送暂停帧。为了启用暂停 (XOFF) 帧进行流量控制，请使用以下命令：

```
hostname(config)#interface tengigabitethernet 1/0 hostname(config-if)# flowcontrol send on
```

有关更多信息，请参阅启用物理接口和配置以太网参数。

显示命令

show cpu usage

show cpu usage 命令用于确定在 ASA CPU 上放置的流量负载。在流量峰值期间、网络高峰期间或者遭受攻击期间，CPU 的使用率会达到峰值。

ASA 有一个用于处理各种任务的 CPU；例如，它可以处理数据包，并可以将调试消息打印到控制台。每个进程都有各自的目的，其中一些进程比其他进程需要占用更多的 CPU 时间。加密很可能是 CPU 最密集的进程，因此如果您的 ASA 让大量流量通过加密隧道，您应考虑一个速度更快的

ASA、一个专用 VPN 集中器，例如 VPN 3000。VAC 从 ASA CPU 卸载加密和解密，并在卡上的硬件中执行此操作。这样 ASA 即可使用 3DES（168 位加密）加密和解密 100 Mbps 的流量。

日志记录是另一个会消耗大量系统资源的进程。因此，建议您在 ASA 上禁用控制台、监视器和缓冲区日志记录。在进行故障排除时，您可以启用这些进程，但是在日常操作中，特别是当您的 CPU 资源耗尽时，您应禁用它们。建议将 Syslog 日志记录或简单网络管理协议 (SNMP) 日志记录（日志历史记录）设置为第 5 级（通知）或更低。此外，您可以通过 **no logging message <syslog_id>** 命令禁用特定 Syslog 消息 ID。

思科自适应安全设备管理器 (ASDM) 还在 Monitoring 选项卡上提供了一个图表，允许您查看 ASA 随时间变化的 CPU 使用情况。您可使用此图表来确定 ASA 上的负载。

您可使用 **show cpu usage** 命令来显示 CPU 利用率统计信息。

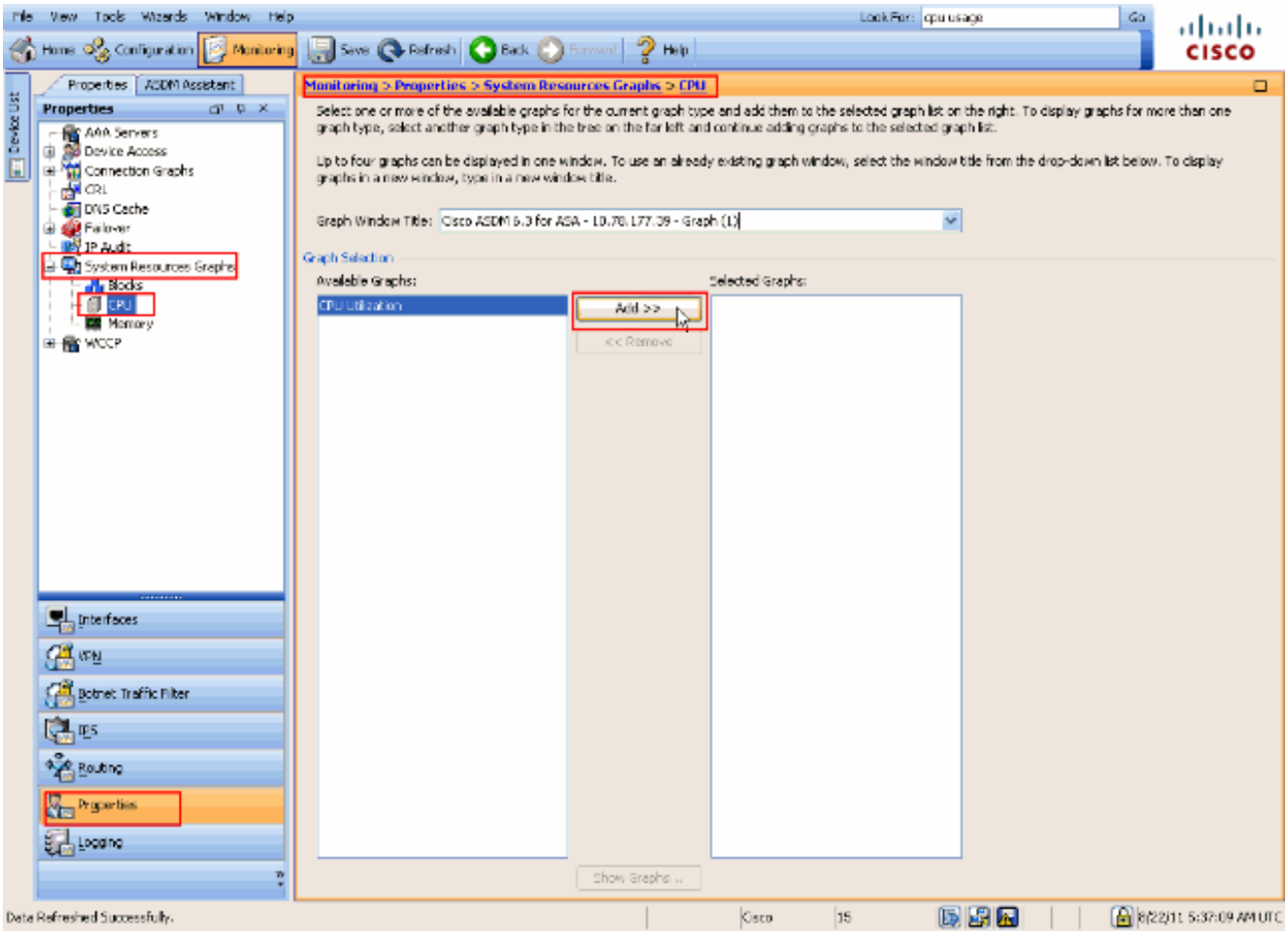
示例

```
Ciscoasa#show cpu usage CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

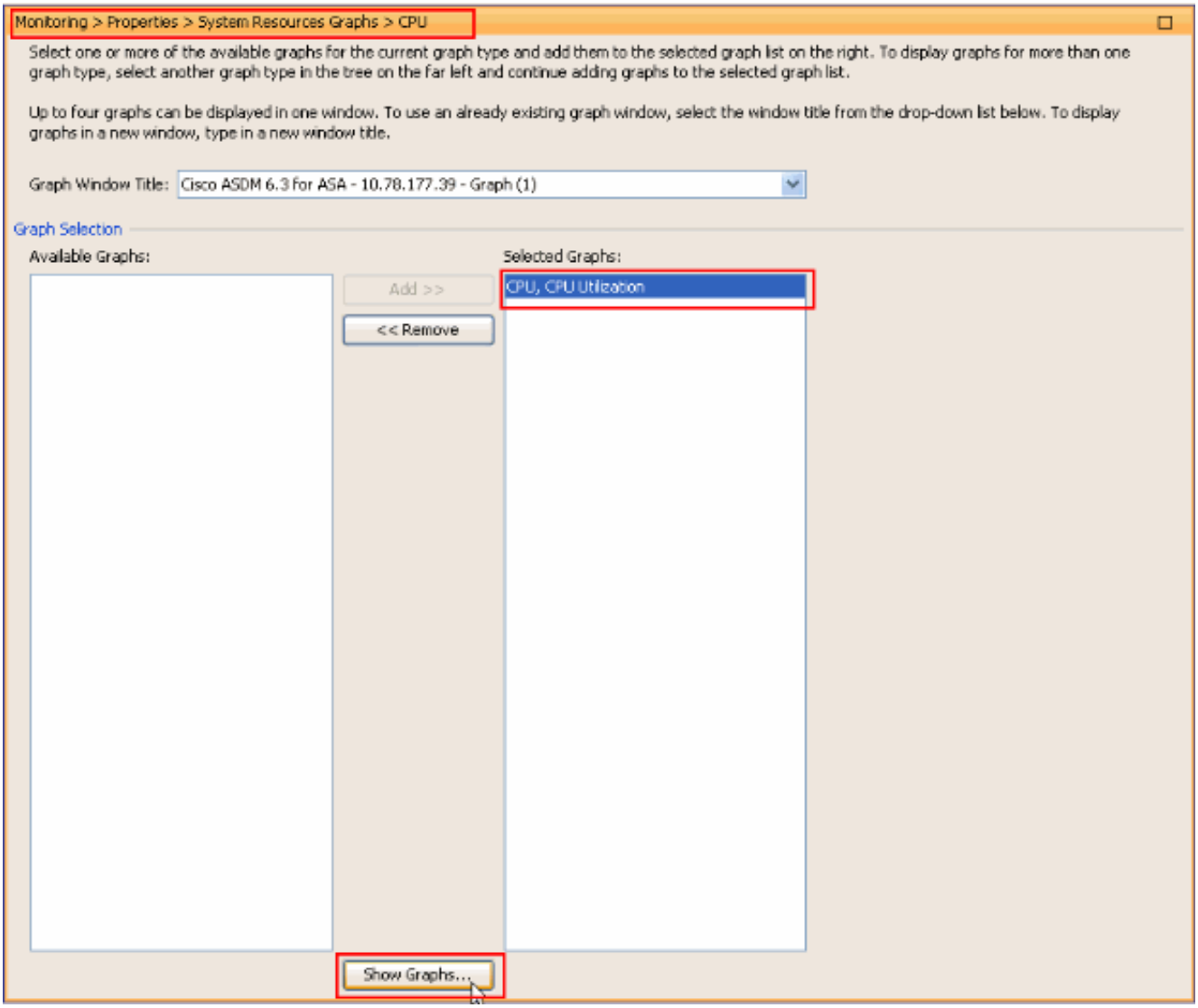
查看 ASDM 上的 CPU 使用情况

完成以下步骤以查看 ASDM 上的 CPU 使用情况：

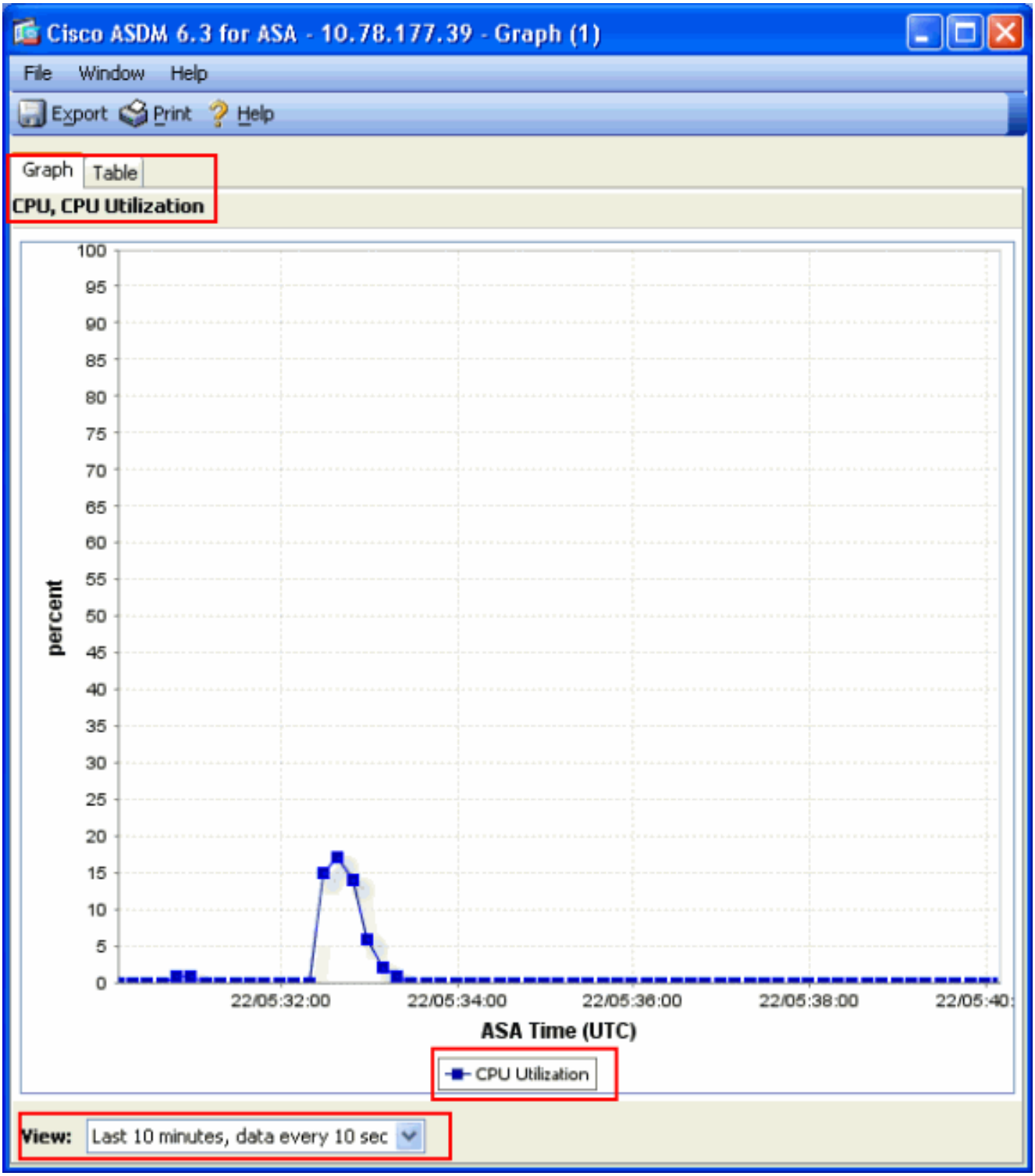
1. 转至 ASDM 中的**监控 > 属性 > 系统资源图形 > CPU** 并选择**图形窗口标题**。然后，从**可用的图形**列表中选择所需的图表并点击**添加**，如图所示。



2. 在**选定图形**部分下添加所需的图表名称后，点击**显示图形**。



下一张图显示了 ASDM 上的 **CPU 使用情况**图表。此图表有不同的可用视图，可从 View 下拉列表中选择视图进行更改。此输出可以根据需要打印或保存到计算机。



输出说明

下表说明了 **show cpu usage** 输出中的字段。

字段	说明
CPU 5 秒内的利用率	过去五秒钟内的 CPU 利用率
1 分钟	过去一分钟内，以 5 秒钟为样本的平均 CPU 利用率
5 分钟	过去五分钟内，以 5 秒钟为样本的平均 CPU 利用率

show traffic

show traffic 命令显示了在给定时间段中有多少流量通过 ASA。结果根据自上次发出命令至现在的时间间隔而得出。要想得到准确的结果，请先发出 **clear traffic** 命令，然后等待 1-10 分钟，再发出 **show traffic** 命令。您也可以发出 **show traffic** 命令，等待 1-10 分钟，然后再次发出该命令，但是仅第二次命令的输出有效。

您可使用 **show traffic 命令**来确定有多少流量通过 ASA。如果有多个接口，该命令可帮助您确定哪些接口发送及接收的数据最多。对于有两个接口的 ASA 设备，外部接口上的入站和出站通流量的总和应等于内部接口上的入站和出站通流量的总和。

示例

```
Ciscoasa#show traffic outside: received (in 124.650 secs): 295468 packets 167218253 bytes 2370
pkts/sec 1341502 bytes/sec transmitted (in 124.650 secs): 260901 packets 120467981 bytes 2093
pkts/sec 966449 bytes/sec inside: received (in 124.650 secs): 261478 packets 120145678 bytes
2097 pkts/sec 963864 bytes/sec transmitted (in 124.650 secs): 294649 packets 167380042 bytes
2363 pkts/sec 1342800 bytes/sec
```

如果您的一个接口上的吞吐量接近或达到了额定吞吐量，则您需要将其升级为一个更快的接口，或者限制进出该接口的流量。不这样做的话，会导致数据包被丢弃。如 show interface 部分所说明的，您可以检查接口计数器以查找有关吞吐量的信息。

show perfmon

show perfmon 命令用于监视 ASA 检查的流量数量和类型。此命令是确定每秒的转换 (xlate) 和连接 (conn) 数量的唯一方式。连接可进一步划分为 TCP 连接和用户数据报协议 (UDP) 连接。有关此命令生成的输出的说明，请参阅输出说明。

示例

```
PERFMON STATS     Current      Average
Xlates              18/s         19/s
Connections         75/s         79/s
```

```
TCP Conns            44/s          49/s
UDP Conns            31/s          30/s
URL Access           27/s          30/s
URL Server Req        0/s           0/s
TCP Fixup          1323/s        1413/s
TCPIntercept          0/s           0/s
HTTP Fixup          923/s         935/s
FTP Fixup             4/s           2/s
AAA Authen            0/s           0/s
AAA Author            0/s           0/s
AAA Account           0/s           0/s
```

输出说明

下表说明了 **show perfmon** 输出中的字段。

字段	说明
转换	每秒建立的转换数
连接	每秒建立的连接数
TCP Conns	每秒的 TCP 连接数
UDP Conns	每秒的 UDP 连接数
URL Access	每秒访问的 URL（网站）数
URL Server Req	每秒发送到 Websense 和 N2H2 的请求数（需要 **filter** 命令）
TCP Fixup	ASA 每秒转发的 TCP 数据包数量
TCP 拦截	每秒超出静态转换的初期限额的 SYN 数据包数
HTTP Fixup	每秒发往端口 80 的数据包数（需要 **fixup protocol http** 命令）
FTP Fixup	每秒检查的 FTP 命令数
AAA Authen	每秒的认证请求数
AAA Author	每秒的授权请求数
AAA Account	每秒的记帐请求数

show blocks

您可以将 show cpu usage 命令与 show blocks 命令结合使用来确定 ASA 是否过载。

数据包处理块（1550 和 16384 字节）

当数据包进入 ASA 接口时，它会放置在输入接口队列上，向上传递到操作系统并放在一个块中。对于以太网数据包，将使用 1550 字节块；如果数据包传入 66 MHz 千兆以太网卡，则使用 16384 字节块。ASA 会根据自适应安全算法 (ASA) 确定是允许还是拒绝数据包，并将数据包处理到出站接口

上的输出队列。如果 ASA 无法支持流量负载，则可用的 1550 字节块（或 66 MHz 千兆以太网的 16384 字节块）数量将接近于 0（如命令输出的 CNT 列中所示）。当 CNT 列达到零时，ASA 会尝试分配更多块，最多 8192 块。如果没有其他可用块，ASA 会丢弃数据包。

故障切换和 Syslog 块（256 字节）

256 字节块主要用于有状态故障切换消息。活动 ASA 会生成数据包并将其发送到待机 ASA，以便更新转换和连接表。在突发数据流期间（这一期间有大量的连接建立或断开），可用的 256 字节块的数量可能会下降到 0。此丢弃表明一个或多个连接未更新到待机 ASA。这通常是可接受的，因为有状态故障切换协议会在下次捕获丢失的 xlate 或连接。但是，如果 256 字节块的 CNT 列长时间保持为或接近 0，则 ASA 会由于其处理的每秒连接数而无法让转换和连接表保持同步。如果不断出现此情况，请将 ASA 升级到速度更快的型号。

从 ASA 发出的系统日志消息也使用 256 字节块，但它们的发布量通常不会导致耗尽 256 字节块池。如果 CNT 列显示 256 字节块的数量接近于 0，请确保在配置要发送到 Syslog 服务器的 Syslog 时，未将 Syslog 级别设置为调试（第 7 级）。此功能通过 ASA 配置中的日志记录陷阱线指示。建议您将日志记录级别设置为通知（第 5 级）或更低，除非您需要更多信息来进行调试。

示例

```
Ciscoasa#show blocks SIZE MAX LOW CNT 4 1600 1597 1600 80 400 399 400 256 500 495 499 1550 1444
1170 1188 16384 2048 1532 1538
```

输出说明

下表说明了 **show blocks** 输出中的列。

列	说明
大小	块池的 E 大小（字节）。每个大小代表一个特定类型
最大	指定字节块池的最大可用块数。启动时从内存切出的最大块数。一般来说，最大可用块数不会改变。 和 1550 字节块，其中自适应安全设备可在需要时动态地创建更多块，最多 8192 块。
低	低水位线标记。此数字指示自启动自适应安全设备或自上次清除块（使用清除块命令）以来此大小的 列中的零指示内存已满的上一个事件。
CNT	该特定大小的块池的当前可用块数。CNT 列中的零表示内存现在已满。

下表说明了 **show blocks** 输出中 SIZE 行的值。

SIZE 值	说明
0	被 dupb 块使用。
4	在应用中复制现有块，例如 DNS、ISAKMP、URL 过滤、uauth、TFTP 和 TCP 模块。此外，此大
80	在 TCP 拦截中用于生成确认数据包和用于故障转移 hello 消息。
256	用于有状态故障转移更新、系统日志记录和其他 TCP 功能。这些块主要用于有状态故障转移消息。故障转移协议会在下次抓取缺失转换或连接。如果 256 字节块的 CNT 列长时间保持为或接近 0，则于0，请确保您不是在调试级(第7级)登录到系统日志服务器的。此功能通过自适应安全设备配置中的
1550	用于存储以太网数据包以通过自适应安全设备处理。当数据包进入自适应安全设备接口时，它会放置0（如命令输出的 CNT 列中所示）。当 CNT 列为零时，自适应安全设备会尝试分配更多块，最多 8
16384	只用于 64 位 66 MHz 千兆以太网卡 (i82543)。有关以太网数据包的更多信息，请参阅 1550 的说明
2048	用于控制更新的控制帧或指导帧。

show memory

show memory 命令显示了 ASA 的物理内存总量（或 RAM），以及当前可用字节数。为了使用此信息，您必须先了解 ASA 如何使用内存。当 ASA 启动时，它会将操作系统从闪存复制到 RAM 并从 RAM 运行操作系统（就像路由器一样）。接下来，ASA 会从闪存复制启动配置并将其放置到 RAM 中。最后，ASA 会分配 RAM 以创建在显示块部分中讨论的块池。此分配完成后，ASA 只在配置大小增加时需要额外 RAM。此外，ASA 会在 RAM 中存储转换和连接条目。

在正常操作过程中，ASA 上的可用内存变化应该很少（如有变化）。通常，内存不足的唯一情况是您遭受攻击且有数十万个连接通过 ASA。为了检查连接，请发出 **show conn count 命令**，会显示通过 ASA 的当前和最大连接数。如果 ASA 耗尽内存，最终会崩溃。在崩溃之前，您可能注意到系统日志中的内存分配失败消息 (%ASA-3-211001)。如果您由于受到攻击而导致内存耗尽，请与 Cisco 技术支持中心 (TAC) 联系。

示例

```
Ciscoasa#show memory Free memory: 845044716 bytes (79%) Used memory: 228697108 bytes (21%) -----
-------- ---------------- Total memory: 1073741824 bytes (100%)
```

show xlate

show xlate count 命令显示了通过 ASA 的当前和最大转换数。转换就是将内部地址映射到外部地址

，它可以是一对一的映射，例如网络地址转换 (NAT)，或者是多对一的映射，例如端口地址转换 (PAT)。此命令是 **show xlate 命令**的一个子集，会输出通过 ASA 的每个转换。命令输出会显示“使用中”的转换，这是指发出命令时 ASA 中的活动转换数；“最常用”是指 ASA 自其启动以来曾有的最大转换数。

> **注意**：单个主机可以与不同的目标之间有多个连接，但是只能有一个转换。如果 xlate 计数远大于内部网络上的主机数量，则可能您的某台内部主机被侵入。如果您的内部主机被入侵，它会伪造源地址并从 ASA 发送数据包。

> **注意**：当启用 vpnclient 配置，且内部主机发出 DNS 请求时，**show xlate** 命令可能会列出一个静态转换的多个 xlate。

示例

```
Ciscoasa#show xlate count 84 in use, 218 most used
```

```
Ciscoasa(config)#show xlate 3 in use, 3 most used Flags: D - DNS, d - dump, I - identity, i - inside, n - no random, o - outside, r - portmap, s - static TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30 UDP PAT from 10.1.1.15/1028 to outside:192.150.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30 ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0 flags ri idle 62:33:57 timeout 0:00:30
```

第一个条目是从内部网络上的主机端口（10.1.1.15，1026）到外部网络上的主机端口（192.150.49.1，1024）的 TDP 端口地址转换。标志“r”表示该转换是一个端口地址转换。标志“i”表示该转换适用于内部地址端口。

第二个条目是从内部网络上的主机端口（10.1.1.15，1028）到外部网络上的主机端口（192.150.49.1，1024）的 UDP 端口地址转换。标志“r”表示该转换是一个端口地址转换。标志“i”表示该转换适用于内部地址端口。

第三个条目是从内部网络上的主机 ICMP id（10.1.1.15，21505）到外部网络上的主机 ICMP id（192.150.49.1，0）的 ICMP 端口地址转换。标志“r”表示该转换是一个端口地址转换。标志“i”表示该转换适用于内部地址 ICMP id。

在从较安全的接口传输至不太安全的接口的数据包中，内部地址字段显示为源地址。反之，在从不太安全的接口传输至较安全的接口的数据包中，内部地址字段显示为目标地址。

show conn count

show conn count 命令显示了通过 ASA 的当前和最大连接数。连接就是将第 4 层信息从内部地址映射到外部地址。当 ASA 收到 TCP 会话的一个 SYN 数据包或者当 UDP 会话中的第一个数据包到达时，会建立连接。当 ASA 收到最后一个 ACK 数据包（此情况在 TCP 会话握手关闭或 UDP 会话超时过期时发生）时，连接会被切断。

极高的连接计数（通常是 50-100 次）可能表示您受到攻击。发出 **show memory 命令**以确保较高的连接计数不会导致 ASA 内存耗尽。如果受到攻击，您可以限制每个静态条目的最大连接数，也可以限制初期连接的最大数量。这一操作可保护您的内部服务器，使它们不会发生过载。有关更多信息，请参阅 Cisco ASA 5500 系列自适应安全设备命令参考。

示例

```
Ciscoasa#show conn count 2289 in use, 44729 most used
```

show interface

show interface 命令可帮助确定双工不匹配问题和电缆问题。它也可以进一步提供有关接口是否超负荷运行的信息。如果 ASA 耗尽 CPU 容量，1550 字节块的数量将接近于 0。（请查看 66 MHz 千兆卡上的 16384 字节块。)另一个指示是接口上的“no buffers”计数的增加。没有缓冲区消息表明接口无法将数据包发送到 ASA 操作系统，因为此数据包没有可用块，且数据包会被丢弃。如果缓冲区级别的增加没有规律，请发出 **show proc cpu 命令**来检查 ASA 上的 CPU 使用情况。如果 CPU 使用率高是因为流量负载大，请升级到可处理该负载的更为强大的 ASA。

数据包进入接口时，它将被放置在输入硬件队列中。如果输入硬件队列已满，则数据包将被放置在输入软件队列中。数据包从其输入队列传递并被放置在 1550 字节块（或在 66 MHz 千兆以太网接口上的 16384 字节块）中。ASA 之后会确定数据包的输出接口并将数据包放入适当的硬件队列。如果硬件队列已满，则数据包将被放置在输出软件队列中。如果两个软件队列中任何一个队列中的最大块数过大，则接口将处于超负荷运行状态。例如，如果 200 Mbps 的流量进入 ASA 并且全部从单个 100 Mbps 接口输出，则输出软件队列会在出站接口上指示较高数字，这表明此接口不能处理该流量。如果遇到这种情况，请将您的接口升级到一个更快的接口。

示例

```
Ciscoasa#show interface Interface GigabitEthernet0/1 "inside", is up, line protocol is up
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), Auto-Speed(100
Mbps) Input flow control is unsupported, output flow control is unsupported MAC address
0013.c480.b2b8, MTU 1500 IP address 192.168.17.4, subnet mask 255.255.255.0 311981 packets
input, 20497296 bytes, 0 no buffer Received 311981 broadcasts, 157 runts, 0 giants 379 input
errors, 107 CRC, 273 frame, 0 overrun, 0 ignored, 0 abort 0 pause input, 0 resume input 0 L2
decode drops 121 packets output, 7744 bytes, 0 underruns 0 pause output, 0 resume output 0
output errors, 0 collisions, 1 interface resets 0 late collisions, 0 deferred 0 input reset
drops, 0 output reset drops, 0 tx hangs input queue (blocks free curr/low): hardware (255/249)
output queue (blocks free curr/low): hardware (255/254)
```

您也应该检查接口是否有错误。如果接收到残帧、输入错误、CRC 或者帧错误，则很可能是因为双工不匹配电缆也可能出现故障。有关双工问题的详细信息，请参阅速度和双工设置。请记住，每个错误计数器代表因为该特定错误所丢弃的数据包的数量。如果看到一个有规律增加的特定计数器，则表示您的 ASA 的性能很可能不佳，您必须找到问题的根本原因。

在检查接口计数器时，请注意，如果该接口设置为全双工，则您不应该遇到任何冲突、延迟冲突或数据包延迟。相比之下，如果接口设置为半双工，则您应该会遇到冲突和一些延迟冲突，而且还可能会遇到一些数据包延迟的情况。冲突、延迟冲突和延迟数据包的总数不应该超过输入和输出数据包数量总和的 10%。如果冲突数量超过了总流量的 10%，则表明链路使用过度，您必须升级到全双工或更快的速度（10 Mbps 到 100 Mbps）。请记住，冲突 10% 意味着 ASA 会丢弃通过该接口的 10% 的数据包；这些被丢弃的数据包必须重新传输。

有关接口计数器的详细信息，请参阅 Cisco ASA 5500 系列自适应安全设备命令参考中的**接口命令**。

show processes

ASA 上的 show processes 命令显示了执行此命令时在 ASA 上运行的所有活动进程。此信息在确定哪些进程占用了过多的 CPU 时间以及哪些进程没有占用任何 CPU 时间时非常有用。为了获得此信息，请发出 **show processes** 命令两次；两次发出命令之间等待大约 1 分钟。对于相关进程，请将第一次输出的 Runtime 值减去第二次输出的 Runtime 值。此结果为您显示了此进程在此时间间隔中收到了多少 CPU 时间（毫秒）。请注意，一些进程被安排为以特定间隔运行，而有些进程则在有信息处理时才会运行。577poll 进程很可能是所有进程中拥有最大 Runtime 值的进程。这是正常的，因为 577poll 进程会对以太网接口进行轮询，以查明它们是否有任何需要处理的数据。

> **注意**：每个 ASA 进程的检查超出了本文范围，但为了完整性在此简要提及。有关 ASA 进程的更多信息，请参阅 ASA 的 show processes 命令。

命令汇总

总之，请使用 **show cpu usage 命令**来识别 ASA 承受的负载。请记住，输出的值是运行平均值；ASA 可以具有被运行平均值屏蔽的更高 CPU 使用率峰值。ASA 到达 80% 的 CPU 使用率后，通过 ASA 的延迟会缓慢增加到大约 90% 的 CPU 使用率。当 CPU 使用率超过 90% 时，ASA 会开始丢弃数据包。

如果 CPU 使用率较高，请使用 **show processes** 命令确定占用最多 CPU 时间的进程。请使用此信息来减少部分由密集进程（例如日志记录）消耗的时间。

如果 CPU 运行不热，但您认为仍要丢弃数据包，请使用 **show interface 命令**来检查 ASA 接口是否有缓冲区和冲突（可能由双工不匹配导致）。如果 no buffer 计数增加，但是 CPU 使用率并不低，则表明接口无法支持流经它的流量。

如果缓冲区情况良好，则请检查块。如果 **show blocks** 输出中的当前 CNT 列接近于 1550 字节块（66 MHz 千兆卡的 16384 字节块）上的 0，则 ASA 很可能由于太忙而丢弃以太网数据包。在这种情况下，CPU 使用率会达到较高的峰值。

如果在建立通过 ASA 的新连接时遇到问题，请使用 **show conn count 命令**来检查通过 ASA 的当前连接计数。

如果当前计数很高，请检查 **show memory** 输出来确保 ASA 不会耗尽内存。如果内存较低，请使用 **show conn** 或 **show local-host** 命令来检查连接源以验证您的网络是否遭到拒绝服务攻击。

您可使用其他命令来测量通过 ASA 的流量数量。**show traffic 命令**显示了汇聚数据包和每接口字节，并且 **show perfmon** 会将流量分成不同类型的 ASA 检查。

相关信息

- Cisco ASA 5500 系列自适应安全设备
- 技术支持 - Cisco Systems