ESA — 数据包捕获和网络调查

目录

简介

本文档介绍如何在思科邮件安全设备(ESA)上配置和收集数据包捕获，以及执行其他网络调查和故障排除。

背景信息

当您与思科技术支持联系时，可能会要求您深入了解ESA的出站和入站网络活动。设备能够拦截和显示通过设备所连接的网络传输或接收的TCP、IP和其他数据包。您可能希望运行数据包捕获以调试网络设置或验证到达或离开设备的网络流量。

> **注意**：本文档引用的软件不是思科维护或支持的软件。提供该信息只是为了方便您使用。如需进一步帮助，请联系软件供应商。

请注意，之前使用的 tcpdump CLI命令将替换为新命令 packetcapture 命令。此命令提供类似于 tcpdump 命令，也可在GUI上使用。

如果运行AsyncOS版本6.x或更低版本，请参阅有关如何使用 tcpdump 命令。此外，Packet Capture Filters部分中介绍的过*滤器选*项也对新的packetcapture命令有效。

AsyncOS 7.x及更高版本上的数据包捕获

本节介绍AsyncOS 7.x及更高版本上的数据包捕获过程。

开始或停止数据包捕获

要从GUI开始数据包捕获，请导航至右上角的**Help and Support**菜单，选择**Packet Capture**，然后单击**Start Capture**。要停止数据包捕获进程，请单击“停**止捕获”**。

注意：在GUI中开始的捕获会在会话之间保留。

要从CLI开始数据包捕获，请输入 **packetcapture > start** 命令。要停止数据包捕获过程，请输入 **packetcapture > stop** 命令，ESA在会话结束时停止数据包捕获。

数据包捕获功能

以下是可用于控制数据包捕获的有用信息列表：

- ESA将捕获的数据包活动保存到文件并在本地存储。您可以配置最大数据包捕获文件大小、数据包捕获运行的时间长度以及捕获运行在哪个网络接口上。您还可以使用过滤器将数据包捕获限制为通过特定端口的流量或来自特定客户端或服务器IP地址的流量。
- 从GUI导**航至Help and Support > Packet Capture**，以查看存储的数据包捕获文件的完整列表。当数据包捕获运行时，“数据包捕获”(Packet Capture)页面显示当前统计信息（如文件大小和已用时间）的捕获状态。
- 选择捕获，然后单击**Download File**以下载存储的数据包捕获。
- 要删除数据包捕获文件，请选择一个或多个文件，然后单击“删除选定**的文件”**。
- 要使用GUI编辑数据包捕获设置，请从“帮助和支持”(Help and Support)菜单**中选择“**数据包捕获”(Packet Capture)，然后单击“编辑**设置”(Edit Settings**)。
- 要使用CLI编辑数据包捕获设置，请输入 **packetcapture > setup** 命令。

注意：GUI仅显示从GUI开始的数据包捕获，而不显示从CLI开始的数据包捕获。同样，CLI仅显示从CLI开始的当前数据包捕获的状态。一次只能运行一个捕获。

提示：有关数据包捕获选项和过滤器设置的其他信息，请参阅本文**档的数据包**捕获过滤器部分。要从GUI访问AsyncOS联机帮助，请导航到**帮助和支持>联机帮助>搜索**数据包**捕获>选**择**运行数据包捕获。**

AsyncOS版本6.x及更低版本上的数据包捕获

本节介绍AsyncOS 6.x及更早版本上的数据包捕获过程。

开始或停止数据包捕获

您可以使用 tcpdump 命令，以捕获TCP/IP和通过ESA所连接的网络传输或接收的其他数据包。

要开始或停止数据包捕获，请完成以下步骤：

1. 输入 **diagnostic > network > tcpdump** 命令。下面是示例输出：

```
example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
[]> network

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> tcpdump

- START - Start packet capture
- STOP - Stop packet capture
- STATUS - Status capture
- FILTER - Set packet capture filter
- INTERFACE - Set packet capture interface
- CLEAR - Remove previous packet captures
[]>
```

2. 设置接口（Data 1、Data 2或Management）和过滤器。

   注意：过滤器使用与Unix相同的格式 tcpdump 命令。
3. 选择**START** 以开始捕获，**STOP**以结束捕获。

   注意：捕获正在进行时，请勿退出tcpdump菜单。您必须使用第二个CLI窗口才能运行任何其他命令。捕获过程完成后，必须从本地桌面使用安全复制(SCP)或文件传输协议(FTP)，以便从名为Diagnostic的目录下载文件(有关详细信息，请参阅*Packet Capture Filters*部分)。 文件使用数据包捕获(PCAP)格式，可以通过Ethereal或Wireshark等程序进行查看。

数据包捕获过滤器

的 **Diagnostic > NET** CLI命令使用标准tcpdump过滤器语法。本节提供有关tcpdump捕获过滤器的信息，并提供一些示例。

以下是使用的标准过滤器：

- **ip** — 过滤所有IP协议流量
- **tcp** — 过滤所有TCP协议流量
- **ip host** — 特定IP地址源或目标的过滤器

以下是一些正在使用的过滤器的示例：

- **ip host 10.1.1.1** — 此过滤器捕获任何包含10.1.1.1作为源或目标的流量。
- **ip host 10.1.1.1或ip host 10.1.1.2** — 此过滤器捕获包含10.1.1.1或10.1.1.2作为源或目标的流量

。

要检索捕获的文件，请导航至**var > log > diagnostic**或**data > pub > diagnostic**，以访问Diagnostic目录。

注意：使用此命令时，可能会导致ESA磁盘空间耗尽，并导致性能下降。思科建议您仅在思科TAC工程师的帮助下使用此命令。

其他网络发现和调查

注意：以下方法只能从CLI中使用。

TCPSERVICES

的 tcpservices 命令将显示当前功能和系统进程的TCP/IP信息。

```
example.com> tcpservices

System Processes (Note: All processes may not always be present)
  ftpd.main    - The FTP daemon
  ginetd       - The INET daemon
  interface    - The interface controller for inter-process communication
  ipfw         - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon

Feature Processes
  euq_webui    - GUI for ISQ
  gui          - GUI process
  hermes       - MGA mail server
  postgres     - Process for storing and querying quarantine data
  splunkd      - Processes for storing and querying Email Tracking data

COMMAND      USER         TYPE NODE   NAME
postgres     pgsql        IPv4 TCP    127.0.0.1:5432
interface    root         IPv4 TCP    127.0.0.1:53
ftpd.main    root         IPv4 TCP    10.0.202.7:21
gui          root         IPv4 TCP    10.0.202.7:80
gui          root         IPv4 TCP    10.0.202.7:443
ginetd       root         IPv4 TCP    10.0.202.7:22
java         root         IPv6 TCP    [::127.0.0.1]:18081
hermes       root         IPv4 TCP    10.0.202.7:25
hermes       root         IPv4 TCP    10.0.202.7:7025
api_serve    root         IPv4 TCP    10.0.202.7:6080
api_serve    root         IPv4 TCP    127.0.0.1:60001
api_serve    root         IPv4 TCP    10.0.202.7:6443
nginx        root         IPv4 TCP    *:4431
nginx        nobody       IPv4 TCP    *:4431
nginx        nobody       IPv4 TCP    *:4431
java         root         IPv4 TCP    127.0.0.1:9999
```

NETSTAT

此实用程序显示传输控制协议（传入和传出）、路由表以及许多网络接口和网络协议统计信息的网络连接。

```
example.com> netstat

Choose the information you want to display:
1. List of active sockets.
2. State of network interfaces.
3. Contents of routing tables.
4. Size of the listen queues.
5. Packet traffic information.
```

Example of Option 1 (List of active sockets)

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 10.0.202.7.10275      10.0.201.4.6025        ESTABLISHED
tcp4       0      0 10.0.202.7.22         10.0.201.4.57759       ESTABLISHED
tcp4       0      0 10.0.202.7.10273      a96-17-177-18.deploy.static.akamaitechnologies.com.80
TIME_WAIT
tcp4       0      0 10.0.202.7.10260      10.0.201.5.443     ESTABLISHED
tcp4       0      0 10.0.202.7.10256      10.0.201.5.443     ESTABLISHED
```

Example of Option 2 (State of network interfaces)

```
Show the number of dropped packets? [N]> y

Name    Mtu Network       Address              Ipkts Ierrs Idrop     Ibytes    Opkts Oerrs
Obytes  Coll  Drop
Data 1    - 10.0.202.0    10.0.202.7        110624529     -     - 117062552515 122028093     -
30126949890     -     -
```

Example of Option 3 (Contents of routing tables)

```
Routing tables

Internet:
Destination        Gateway            Flags      Netif Expire
default            10.0.202.1         UGS         Data 1
10.0.202.0         link#2             U           Data 1
10.0.202.7         link#2             UHS         lo0
localhost.example. link#4             UH          lo0
```

Example of Option 4 (Size of the listen queues)

```
Current listen queue sizes (qlen/incqlen/maxqlen)
Proto Listen         Local Address
tcp4  0/0/50         localhost.exampl.9999
tcp4  0/0/50         10.0.202.7.7025
tcp4  0/0/50         10.0.202.7.25
tcp4  0/0/15         10.0.202.7.6443
tcp4  0/0/15         localhost.exampl.60001
tcp4  0/0/15         10.0.202.7.6080
tcp4  0/0/20         localhost.exampl.18081
tcp4  0/0/20         10.0.202.7.443
tcp4  0/0/20         10.0.202.7.80
tcp4  0/0/10         10.0.202.7.21
```

```
tcp4  0/0/10         10.0.202.7.22
tcp4  0/0/10         localhost.exampl.53
tcp4  0/0/208        localhost.exampl.5432
```

Example of Option 5 (Packet traffic information)

```
            input           nic1           output
   packets  errs idrops      bytes    packets  errs      bytes colls drops
        49     0     0       8116         55     0       7496     0     0
```

网络

diagnostic下的network子命令提供对其他选项的访问。您可以使用此命令刷新所有网络相关缓存、显示ARP缓存的内容、显示NDP缓存的内容（如果适用），并允许您使用SMTPING测试远程SMTP连接。

```
example.com> diagnostic


Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> network


Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]>
```

ETHERCONFIG

的 etherconfig 命令允许您查看和配置与接口、VLAN、环回接口、MTU大小以及接受或拒绝组播地址的ARP应答的双工和MAC信息相关的某些设置。

```
example.com> etherconfig


Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]>
```

TRACEROUTE

显示到远程主机的网络路由。或者，您可以使用 traceroute6 命令。

```
example.com> traceroute google.com

Press Ctrl-C to stop.
traceroute to google.com (216.58.194.206), 64 hops max, 40 byte packets
1 68.232.129.2 (68.232.129.2) 0.902 ms
68.232.129.3 (68.232.129.3) 0.786 ms 0.605 ms
2 139.138.24.10 (139.138.24.10) 0.888 ms 0.926 ms 1.092 ms
3 68.232.128.2 (68.232.128.2) 1.116 ms 0.780 ms 0.737 ms
4 139.138.24.42 (139.138.24.42) 0.703 ms
208.90.63.209 (208.90.63.209) 1.413 ms
139.138.24.42 (139.138.24.42) 1.219 ms
5 svl-edge-25.inet.qwest.net (63.150.59.25) 1.436 ms 1.223 ms 1.177 ms
6 snj-edge-04.inet.qwest.net (67.14.34.82) 1.838 ms 2.086 ms 1.740 ms
7 108.170.242.225 (108.170.242.225) 1.986 ms 1.992 ms
108.170.243.1 (108.170.243.1) 2.852 ms
8 108.170.242.225 (108.170.242.225) 2.097 ms
108.170.243.1 (108.170.243.1) 2.967 ms 2.812 ms
9 108.170.237.105 (108.170.237.105) 1.974 ms
sfo03s01-in-f14.1e100.net (216.58.194.206) 2.042 ms 1.882 ms
```

PING

Ping允许您使用IP地址或主机名测试主机的可达性，并提供与通信中可能的延迟和/或丢包相关的统计信息。

```
example.com> ping google.com

Press Ctrl-C to stop.
PING google.com (216.58.194.206): 56 data bytes
64 bytes from 216.58.194.206: icmp_seq=0 ttl=56 time=2.095 ms
64 bytes from 216.58.194.206: icmp_seq=1 ttl=56 time=1.824 ms
64 bytes from 216.58.194.206: icmp_seq=2 ttl=56 time=2.005 ms
64 bytes from 216.58.194.206: icmp_seq=3 ttl=56 time=1.939 ms
64 bytes from 216.58.194.206: icmp_seq=4 ttl=56 time=1.868 ms
64 bytes from 216.58.194.206: icmp_seq=5 ttl=56 time=1.963 ms

--- google.com ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.824/1.949/2.095/0.088 ms
```