收集思科ESA上的数据包捕获并对其进行故障排除

目录

简介

使用的组件

重要风险和前提条件

背景信息

在AsyncOS上配置数据包捕获

- 启动或停止数据包捕获
- 管理数据包捕获
- 数据包捕获限制
- 对数据包捕获的其他支持

使用自定义数据包捕获过滤器

执行其他网络调查

- TCPSERVICES
- NETSTAT
- 网络
- ETHERCONFIG
- TRACEROUTE
- PING

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进行网络故障排除。

使用的组件

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

重要风险和前提条件

- 数据包捕获命令可能导致ESA磁盘空间耗尽，并可能导致性能下降。
- Cisco建议您只在Cisco TAC工程师的帮助下使用这些命令。
- 确保您对ESA的CLI或GUI具有管理访问权限。

背景信息

思科技术支持可以要求您深入了解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。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。

在AsyncOS上配置数据包捕获

本节介绍数据包捕获过程。

启动或停止数据包捕获

1. 要从GUI开始数据包捕获，请导航到右上角的Help and Support菜单，选择Packet Capture，然后单击Start Capture。
    1. 或者，单击Edit Settings以指定要捕获的IP地址和端口，然后单击Submit。
    2. 可以使用CSV格式输入端口号和IP地址(例如：80, 443)。 要捕获ANY端口或IP，请将此字段留空。
2. 要停止数据包捕获过程，请单击Stop Capture。
    1. 在GUI中开始的捕获会在会话之间保留。

1. 要从CLI开始数据包捕获，请输入packetcapture > start命令。
    1. 或者，使用setup命令指定要捕获的IP地址和端口。
2. 要停止数据包捕获过程，请输入packetcapture > stop命令。
    1. 会话结束时，ESA会停止数据包捕获。

管理数据包捕获

要管理文件，请在GUI中导航到帮助和支持>数据包捕获。从此页面，您可以：

- 监控进度：查看活动捕获的实时统计信息，包括当前文件大小和运行时间。
- Download Files：选择已完成的捕获，然后单击Download File将其保存到本地计算机。
- 删除文件：要释放空间，请选择一个或多个文件，然后单击“删除选定文件”。

数据包捕获限制

- 单实例：一次只能运行一个数据包捕获。
- 接口独立性:GUI和CLI独立运行数据包捕获。GUI仅显示和管理通过Web界面启动的捕获，而CLI仅显示通过命令行启动的捕获的状态。

对数据包捕获的其他支持

有关更多详细说明，请访问AsyncOS联机帮助:

1. 导航到帮助和支持>联机帮助。
2. 搜索Packet Capture。
3. 选择Running a Packet Capture。

使用自定义数据包捕获过滤器

本节提供有关自定义捕获过滤器的信息并提供示例。

以下是使用的标准过滤器：

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

以下是正在使用的过滤器的示例：

- ip host 10.1.1.1 — 此过滤器捕获包括10.1.1.1作为源或目标的所有流量。
- 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。

执行其他网络调查

以下描述的方法只能从CLI中使用。

TCPSERVICES

tcpservices命令显示当前功能和系统进程的TCP/IP信息。

<#root>

example.com>

tcpservices

```
System Processes (Note: All processes can 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TCP（传入和传出）的网络连接、路由表以及大量网络接口和网络协议统计信息。

<#root>

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_
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  
Data 1    - 10.0.202.0    10.0.202.7        110624529     -     - 117062552515 122028093     - 30126949
```

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。

使用此命令可刷新所有与网络相关的缓存、显示ARP缓存的内容、显示NDP缓存的内容（如果适用），并使用SMTPING测试远程SMTP连接。

<#root>

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

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带有组播地址的ARP应答相关的双工和MAC信息设置。

<#root>

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

此命令显示到远程主机的网络路由。

如果在至少一个接口上配置了IPv6地址，请使用traceroute6命令。

<#root>

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连通性，并提供与通信中可能的延迟和丢包相关的统计信息。

```
<#root>

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
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。