ESA - 패킷 캡처 및 네트워크 조사

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 패킷 캡처를 구성 및 수집하고 추가 네트워크 조사 및 트러블슈팅을 수행하는 방법에 대해 설명합니다.

배경 정보

Cisco 기술 지원 부서에 문제를 문의하면 ESA의 아웃바운드 및 인바운드 네트워크 활동에 대한 통찰력을 제공하라는 메시지가 표시될 수 있습니다.어플라이언스는 어플라이언스가 연결된 네트워크를 통해 전송되거나 수신된 TCP, IP 및 기타 패킷을 가로채고 표시하는 기능을 제공합니다.네트워크 설정을 디버깅하거나 어플라이언스에 도달하거나 나가는 네트워크 트래픽을 확인하기 위해 패킷 캡처를 실행할 수 있습니다.

> **참고:**이 문서는 Cisco에서 유지 관리하거나 지원하지 않는 소프트웨어를 참조합니다.이 정보는 귀하의 편의를 위해 제공됩니다.자세한 내용은 소프트웨어 공급업체에 문의하십시오.

이전에 사용한 tcpdump CLI 명령이 새로운 packetcapture 명령을 실행합니다.이 명령은 tcpdump 명령을 사용하여 GUI에서 사용할 수도 있습니다.

AsyncOS 버전 6.x 이하를 실행하는 경우, 사용 방법에 대한 지침을 참조하십시오. tcpdump 이 문서의 AsyncOS *버전 6.x 및 이전* 섹션의 *Packet Captures*에 있는 명령또한 Packet *Capture Filters* 섹션에 설명된 필터 옵션은 새 packetcapture 명령에도 유효합니다.

AsyncOS 버전 7.x 이상에서 패킷 캡처

이 섹션에서는 AsyncOS 버전 7.x 이상에서 패킷 캡처 프로세스에 대해 설명합니다.

패킷 캡처 시작 또는 중지

GUI에서 패킷 캡처를 시작하려면 오른쪽 위의 **Help and Support(도움말 및 지원)** 메뉴로 이동하여 Packet Capture(**패킷 캡처)를** 선택한 다음 **Start Capture(캡처 시작)를 클릭합니다**.패킷 캡처 프로세스를 중지하려면 **Stop Capture**를 클릭합니다.

> **참고:**GUI에서 시작되는 캡처는 세션 간에 유지됩니다.

CLI에서 패킷 캡처를 시작하려면 **packetcapture > start** 명령을 사용합니다.패킷 캡처 프로세스를 중지하려면 **packetcapture > stop** 명령이 실행되고 ESA는 세션이 종료될 때 패킷 캡처를 중지합니다.

패킷 캡처 기능

패킷 캡처를 조작하기 위해 사용할 수 있는 유용한 정보 목록은 다음과 같습니다.

- ESA는 캡처된 패킷 활동을 파일에 저장하고 로컬에 저장합니다.최대 패킷 캡처 파일 크기, 패킷 캡처가 실행되는 시간, 캡처가 실행되는 네트워크 인터페이스를 구성할 수 있습니다.특정 포트 또는 특정 클라이언트 또는 서버 IP 주소에서 오는 트래픽으로 패킷 캡처를 제한하려면 필터를 사용할 수도 있습니다.
- GUI에서 **Help and Support(도움말 및 지원) > Packet Capture(패킷 캡처)로 이동하여** 저장된 패킷 캡처 파일의 전체 목록을 확인합니다.패킷 캡처가 실행되면 Packet Capture(패킷 캡처) 페이지에는 파일 크기 및 경과 시간 등 현재 통계와 함께 진행 중인 캡처의 상태가 표시됩니다.
- 저장된 패킷 캡처를 다운로드하려면 캡처를 선택하고 **Download File**을 클릭합니다.
- 패킷 캡처 파일을 삭제하려면 하나 이상의 파일을 선택하고 **Delete Selected Files**(선택한 파일 삭제)를 클릭합니다.
- GUI를 사용하여 패킷 캡처 설정을 편집하려면 Help and Support(도움말 및 지원) 메뉴**에서 Packet Capture(패킷 캡처**)를 선택하고 Edit Settings(설정 **편집)**를 클릭합니다.
- CLI로 패킷 캡처 설정을 수정하려면 **packetcapture > setup** 명령을 사용합니다.

> **참고:**GUI는 CLI로 시작하는 패킷 캡처를 표시하지 않고 GUI에서 시작하는 패킷 캡처를 표시합니다.마찬가지로 CLI는 CLI에서 시작된 현재 패킷 캡처의 상태만 표시합니다.한 번에 하나의 캡처만 실행할 수 있습니다.

> **팁**:패킷 캡처 옵션 및 필터 설정에 대한 자세한 내용은 이 문서의 **Packet Capture Filters** 섹션을 참조하십시오.GUI에서 AsyncOS Online Help(AsyncOS 온라인 도움말)에 액세스하려면 **Help and Support(도움말 및 지원) > Online Help(온라인 도움말) > Search** for **Packet Capture(패킷 캡처 검색) > Running a Packet Capture(패킷 캡처 실행)를 선택합니다.**

AsyncOS 버전 6.x 및 이전 버전의 패킷 캡처

이 섹션에서는 AsyncOS 버전 6.x 및 이전 버전의 패킷 캡처 프로세스에 대해 설명합니다.

패킷 캡처 시작 또는 중지

사용 가능한 tcpdump 명령을 사용하여 ESA가 연결된 네트워크를 통해 전송되거나 수신된 TCP/IP 및 기타 패킷을 캡처합니다.

패킷 캡처를 시작하거나 중지하려면 다음 단계를 완료합니다.

1. 다음을 입력합니다. **diagnostic > network > tcpdump** 명령을 사용하여 ESA의 CLI에 연결합니다.다음은 출력의 예입니다.

```
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. 인터페이스(Data 1, Data 2 또는 Management)와 필터를 설정합니다.

   참고:필터는 Unix와 동일한 형식을 사용합니다. tcpdump 명령을 사용합니다.
3. 캡처를 시작하려면 **START**를 선택하고 종료하려면 STOP을 선택합니다.

   참고:캡처가 진행 중인 동안에는 tcpdump 메뉴를 종료하지 마십시오. 다른 명령을 실행하려면 두 번째 CLI 창을 사용해야 합니다.캡처 프로세스가 완료되면 로컬 데스크톱에서 SCP(Secure Copy) 또는 FTP(File Transfer Protocol)를 사용하여 Diagnostic이라는 디렉토리에서 파일을 다운로드해야 합니다(자세한 내용은 *Packet Capture Filters* 섹션 참조). 파일은 PCAP(Packet Capture) 형식을 사용하며 Ethereal 또는 Wireshark와 같은 프로그램으로 검토할 수 있습니다.

패킷 캡처 필터

더 **Diagnostic > NET** CLI 명령은 표준 tcpdump 필터 구문을 사용합니다.이 섹션에서는 tcpdump 캡처 필터에 대한 정보를 제공하고 몇 가지 예를 제공합니다.

다음은 사용되는 표준 필터입니다.

- **ip** - 모든 IP 프로토콜 트래픽에 대한 필터
- **tcp** - 모든 TCP 프로토콜 트래픽에 대한 필터
- **ip host** - 특정 IP 주소 소스 또는 대상에 대한 필터

다음은 사용 중인 필터의 몇 가지 예입니다.

- **ip host 10.1.1.1** - 이 필터는 소스 또는 대상으로 10.1.1.1을 포함하는 모든 트래픽을 캡처합니다.
- **ip host 10.1.1.1 또는 ip host 10.1.1.2** - 이 필터는 10.1.1.1 또는 10.1.1.2을 소스 또는 대상으로 포함하는 트래픽을 캡처합니다.

캡처된 파일을 검색하려면 **var > log > diagnostic** 또는 **data > pub > diagnostic**으로 이동하여 진단 디렉토리에 연결합니다.

> **참고:**이 명령을 사용하면 ESA 디스크 공간이 가득 차고 성능이 저하될 수 있습니다.Cisco에서는 Cisco TAC 엔지니어의 도움을 받는 경우에만 이 명령을 사용하는 것이 좋습니다.

추가 네트워크 검색 및 조사

> **참고:**아래 방법은 CLI에서만 사용할 수 있습니다.

TCPSERVICES

더 tcpservices 명령은 현재 기능 및 시스템 프로세스에 대한 TCP/IP 정보를 표시합니다.

```
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

이 유틸리티는 전송 제어 프로토콜(수신 및 발신 모두), 라우팅 테이블, 다수의 네트워크 인터페이스 및 네트워크 프로토콜 통계에 대한 네트워크 연결을 표시합니다.

```
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
```

네트워크

diagnostic 아래의 network 하위 명령은 추가 옵션에 대한 액세스를 제공합니다.이 옵션을 사용하여 모든 네트워크 관련 캐시를 플러시하고, ARP 캐시의 내용을 표시하고, NDP 캐시의 내용을 표시하고(해당되는 경우), SMTPPING을 사용하여 원격 SMTP 연결을 테스트할 수 있습니다.

```
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

더 etherconfig 명령을 사용하면 인터페이스, VLAN, 루프백 인터페이스, MTU 크기, 멀티캐스트 주소로 ARP 회신의 수락 또는 거부에 대한 이중 및 MAC 정보와 관련된 일부 설정을 보고 구성할 수 있습니다.

```
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.
[]>
```

트레이스라우트

원격 호스트에 대한 네트워크 경로를 표시합니다.또는 traceroute6 하나 이상의 인터페이스에 IPv6 주소가 구성된 경우 명령을 사용합니다.

```
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

Ping을 사용하면 IP 주소 또는 호스트 이름을 사용하여 호스트의 연결성을 테스트할 수 있으며, 통신 중 레이턴시 및/또는 삭제와 관련된 통계를 제공합니다.

```
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
```