ESA - Captures de paquets et analyse du réseau

Contenu

Introduction

Ce document décrit comment configurer et collecter des captures de paquets sur l'appliance de sécurité de la messagerie Cisco (ESA) et effectuer des recherches et des dépannages réseau supplémentaires.

Informations générales

Lorsque vous contactez l'assistance technique de Cisco pour un problème, vous devrez peut-être fournir des informations sur l'activité réseau sortante et entrante de l'ESA. L'appliance permet d'intercepter et d'afficher les paquets TCP, IP et autres qui sont transmis ou reçus sur le réseau auquel l'appliance est connectée. Vous pouvez exécuter une capture de paquets afin de déboguer la configuration du réseau ou de vérifier le trafic réseau qui atteint ou quitte l'appliance.

> **Note**: Ce document fait référence à des logiciels qui ne sont pas gérés ou pris en charge par Cisco. Les informations sont fournies comme courtoisie pour votre commodité. Pour obtenir de l'aide, contactez le fournisseur du logiciel.

Il est important de noter que le tcpdump La commande CLI est remplacée par la nouvelle commande packetcapture dans AsyncOS versions 7.0 et ultérieures. Cette commande offre des fonctionnalités similaires à tcpdump , et il est également disponible sur l'interface utilisateur graphique.

Si vous exécutez AsyncOS version 6.x ou antérieure, reportez-vous aux instructions relatives à l'utilisation de tcpdump dans la section *Packet Captures on AsyncOS Versions 6.x et antérieures* de ce document. En outre, les options de filtre décrites dans la section *Packet Capture Filters* sont

également valides pour la nouvelle commande packetcapture.

Captures de paquets sur AsyncOS versions 7.x et ultérieures

Cette section décrit le processus de capture de paquets sur AsyncOS versions 7.x et ultérieures.

Démarrer ou arrêter une capture de paquets

Afin de démarrer une capture de paquets à partir de l'interface utilisateur graphique, accédez au menu **Aide et support** en haut à droite, choisissez **Capture de paquets**, puis cliquez sur **Démarrer la capture**. Afin d'arrêter le processus de capture de paquets, cliquez sur **Arrêter la capture**.

> **Note**: Une capture qui commence dans l'interface utilisateur graphique est conservée entre les sessions.

Afin de démarrer une capture de paquets à partir de l'interface de ligne de commande, saisissez **packetcapture > start** erasecat4000_flash:. Afin d'arrêter le processus de capture de paquets, entrez la commande **packetcapture > stop** , et l'ESA arrête la capture de paquets à la fin de la session.

Fonctionnalité de capture de paquets

Voici une liste d'informations utiles que vous pouvez utiliser pour manipuler les captures de paquets :

- L'ESA enregistre l'activité de paquet capturée dans un fichier et la stocke localement. Vous pouvez configurer la taille maximale du fichier de capture de paquets, la durée d'exécution de la capture de paquets et l'interface réseau sur laquelle la capture s'exécute. Vous pouvez également utiliser un filtre afin de limiter la capture de paquets au trafic via un port ou un trafic spécifique à partir d'une adresse IP client ou serveur spécifique.

- Accédez à **Help and Support > Packet Capture** à partir de l'interface utilisateur graphique afin d'afficher une liste complète des fichiers de capture de paquets qui sont stockés. Lorsqu'une capture de paquets s'exécute, la page Capture de paquets affiche l'état de la capture en cours avec les statistiques actuelles, telles que la taille du fichier et le temps écoulé.

- Choisissez une capture et cliquez sur **Télécharger le fichier** afin de télécharger une capture de paquets stockée.

- Afin de supprimer un fichier de capture de paquets, choisissez un ou plusieurs fichiers et cliquez sur **Supprimer les fichiers sélectionnés**.

- Afin de modifier les paramètres de capture de paquets avec l'interface utilisateur graphique, choisissez **Capture de paquets** dans le menu Aide et support et cliquez sur **Modifier les paramètres**.

- Afin de modifier les paramètres de capture de paquets avec l'interface de ligne de commande, saisissez **packetcapture > setup** erasecat4000_flash:.

Note: L'interface utilisateur graphique affiche uniquement les captures de paquets qui commencent dans l'interface utilisateur graphique, et non celles qui commencent par l'interface de ligne de commande. De même, l'interface de ligne de commande affiche uniquement l'état d'une capture de paquets en cours qui a commencé dans l'interface de ligne de commande. Une seule capture peut être exécutée à la fois.

Astuce : Pour plus d'informations sur les options de capture de paquets et les paramètres de filtre, reportez-vous à la section **Packet Capture Filters** de ce document. Afin d'accéder à l'aide en ligne d'AsyncOS à partir de l'interface utilisateur graphique, accédez à **Aide et support > Aide en ligne >** rechercher la **capture de paquets >** choisissez **Exécution d'une capture de paquets.**

Captures de paquets sur AsyncOS versions 6.x et antérieures

Cette section décrit le processus de capture de paquets sur AsyncOS versions 6.x et antérieures.

Démarrer ou arrêter une capture de paquets

Vous pouvez utiliser le tcpdump afin de capturer TCP/IP et d'autres paquets qui sont transmis ou reçus sur un réseau auquel l'ESA est connecté.

Exécutez ces étapes afin de démarrer ou d'arrêter une capture de paquets :

1. Saisissez le **diagnostic > network > tcpdump** dans l'interface de ligne de commande de l'ESA. Voici un exemple de résultat :

```
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. Définissez l'interface (Données 1, Données 2 ou Gestion) et le filtre.

Note: Le filtre utilise le même format que l'Unix tcpdump erasecat4000_flash:.

3. Choisissez **START** afin de commencer la capture et **STOP** afin de l'arrêter.

Note: Ne quittez pas le menu tcpdump lorsque la capture est en cours. Vous devez utiliser une deuxième fenêtre CLI pour exécuter d'autres commandes. Une fois le processus de capture terminé, vous devez utiliser la copie sécurisée (SCP) ou le protocole FTP (File Transfer Protocol) à partir de votre bureau local afin de télécharger les fichiers à partir du répertoire nommé Diagnostic (reportez-vous à la section *Packet Capture Filters* pour plus de détails). Les fichiers utilisent le format PCAP (Packet Capture) et peuvent être examinés à l'aide d'un programme tel qu'Ethereal ou Wireshark.

Filtres de capture de paquets

Les **Diagnostic > NET** La commande CLI utilise la syntaxe de filtre tcpdump standard. Cette section fournit des informations sur les filtres de capture tcpdump et fournit quelques exemples.

Voici les filtres standard utilisés :

- **ip** - Filtres pour tout le trafic de protocole IP
- **tcp** - Filtres pour tout le trafic de protocole TCP
- **ip host** - Filtres d'une adresse IP source ou de destination spécifique

Voici quelques exemples des filtres utilisés :

- **ip host 10.1.1.1** - Ce filtre capture tout trafic qui inclut 10.1.1.1 comme source ou destination.
- **ip host 10.1.1.1 ou ip host 10.1.1.2** - Ce filtre capture le trafic qui contient 10.1.1.1 ou 10.1.1.2 comme source ou destination.

Pour récupérer le fichier capturé, accédez à **var > log > diagnostic** ou **data > pub > diagnostic** afin d'accéder au répertoire Diagnostic.

Note: Lorsque cette commande est utilisée, elle peut entraîner le remplissage de l'espace disque de votre ESA et également une dégradation des performances. Cisco vous recommande d'utiliser cette commande uniquement avec l'aide d'un ingénieur TAC Cisco.

Détection et investigation de réseau supplémentaires

Note: Les méthodes ci-dessous ne peuvent être utilisées qu'à partir de l'interface de ligne de commande.

TCPSERVICES

Les tcpservices affiche les informations TCP/IP pour les processus système et les fonctionnalités en cours.

```
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

Cet utilitaire affiche les connexions réseau pour le protocole de contrôle de transmission (entrant et sortant), les tables de routage et un certain nombre de statistiques d'interface réseau et de protocole réseau.

```
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
```

RÉSEAU

La sous-commande network sous diagnostic permet d'accéder à d'autres options. Vous pouvez l'utiliser pour vider tous les caches liés au réseau, afficher le contenu du cache ARP, afficher le contenu du cache NPD (le cas échéant) et vous permettre de tester la connectivité SMTP distante à l'aide de la fonctionnalité SMTPPING.

```
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

Les etherconfig vous permet d'afficher et de configurer certains des paramètres liés aux informations duplex et MAC pour les interfaces, les VLAN, les interfaces de bouclage, les tailles MTU et l'acceptation ou le rejet des réponses ARP avec une adresse de multidiffusion.

```
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

Affiche la route réseau vers un hôte distant. Vous pouvez également utiliser le traceroute6 si une adresse IPv6 est configurée sur au moins une interface.

```
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

La commande ping vous permet de tester l'accessibilité d'un hôte à l'aide de l'adresse IP ou du nom d'hôte et fournit des statistiques relatives à la latence et/ou aux pertes de communication possibles.

```
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
```