Collecte et dépannage des captures de paquets sur Cisco ESA

Table des matières

Introduction

Composants utilisés

Risques importants et conditions préalables

Informations générales

Configuration des captures de paquets sur AsyncOS

- Démarrer ou arrêter une capture de paquets
- Gestion des captures de paquets
- Contraintes de capture de paquets
- Prise en charge supplémentaire des captures de paquets

Utiliser des filtres de capture de paquets personnalisés

Effectuer une enquête réseau supplémentaire

- TCPSERVICES
- NETSTAT
- RÉSEAU
- ETHERCONFIG
- TRACEROUTE
- PING

Introduction

Ce document décrit comment configurer et collecter des captures de paquets sur le dispositif de sécurité de la messagerie électronique Cisco (ESA) pour le dépannage du réseau.

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Risques importants et conditions préalables

- Les commandes de capture de paquets peuvent entraîner le remplissage de l’espace disque ESA et une dégradation des performances.
- Cisco recommande d'utiliser ces commandes uniquement avec l'aide d'un ingénieur du centre d'assistance technique Cisco.
- Vérifiez que vous disposez d'un accès administratif à l'interface de ligne de commande ou à

la GUI du ESA.

Informations générales

L'assistance technique Cisco peut vous demander de 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. Exécutez une capture de paquets pour déboguer la configuration du réseau ou pour vérifier le trafic réseau qui atteint ou quitte l'appliance.

Configuration des captures de paquets sur AsyncOS

Cette section décrit le processus de capture de paquets.

Démarrer ou arrêter une capture de paquets

1. Pour 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.
    1. Vous pouvez également cliquer sur Edit Settings pour spécifier les adresses IP et les ports que vous souhaitez capturer, puis cliquer sur Submit.
    2. Les numéros de port et les adresses IP peuvent être saisis au format CSV (par exemple : 80, 443). Pour capturer ANY port ou IP, laissez le ou les champs vides.
2. Pour arrêter le processus de capture de paquets, cliquez sur Stop Capture.
    1. Une capture qui commence dans l'interface utilisateur graphique est conservée entre les sessions.

1. Pour démarrer une capture de paquets à partir de l’interface de ligne de commande, entrez la commande packet capture **>** start.
    1. Vous pouvez également utiliser la commande setup pour spécifier les adresses IP et les ports que vous souhaitez capturer.
2. Pour arrêter le processus de capture de paquets, entrez la commande packet capture **>** stop.
    1. L’ESA arrête la capture de paquets à la fin de la session.

Gestion des captures de paquets

Pour gérer vos fichiers, accédez à Aide et support **>** Capture de paquets dans l'interface graphique utilisateur. À partir de cette page, vous pouvez :

- Surveiller la progression : affichez des statistiques en temps réel pour les captures actives, notamment la taille actuelle du fichier et le temps écoulé.
- Télécharger les fichiers : sélectionnez une capture terminée et cliquez sur Télécharger le fichier pour l'enregistrer sur votre ordinateur local.
- Supprimer les fichiers : pour libérer de l'espace, sélectionnez un ou plusieurs fichiers et cliquez sur Supprimer les fichiers sélectionnés.

Contraintes de capture de paquets

- Instance unique : une seule capture de paquets peut être exécutée à la fois.
- Indépendance d'interface : l'interface graphique et l'interface de ligne de commande fonctionnent indépendamment des captures de paquets. L'interface utilisateur graphique affiche et gère uniquement les captures lancées via l'interface Web, tandis que l'interface de ligne de commande affiche uniquement l'état des captures lancées via la ligne de commande.

Prise en charge supplémentaire des captures de paquets

Pour obtenir des instructions plus détaillées, consultez l'aide en ligne d'AsyncOS :

1. Accédez à Aide et support > Aide en ligne.
2. Recherchez Packet Capture.
3. SélectionnezExécution d'une capture de paquets.

Utiliser des filtres de capture de paquets personnalisés

Cette section fournit des informations sur les filtres de capture personnalisés et fournit des exemples.

Voici les filtres standard utilisés :

- ip - Filtre tout le trafic du protocole IP
- tcp - Filtre tout le trafic du protocole TCP
- ip host : filtre une adresse IP source ou de destination spécifique

Voici des exemples de filtres utilisés :

- ip host 10.1.1.1 - Ce filtre capture tout trafic incluant 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.

Effectuer une enquête réseau supplémentaire

Les méthodes décrites ci-dessous peuvent uniquement être utilisées à partir de l'interface de ligne de commande.

TCPSERVICES

La commande tcpservices affiche les informations TCP/IP pour les processus système et de fonctionnalité actuels.

<#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

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

<#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_W
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  C
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
```

RÉSEAU

La sous-commande network sous diagnostic permet d'accéder à des options supplémentaires.

Utilisez cette commande pour vider tous les caches associés au réseau, afficher le contenu du cache ARP, afficher le contenu du cache NDP (le cas échéant) et tester la connectivité SMTP à distance à l'aide de la fonction SMTP.

<#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

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

<#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

Cette commande affiche la route réseau vers un hôte distant.

Utilisez la commande traceroute6 si vous avez une adresse IPv6 configurée sur au moins une interface.

<#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

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 aux pertes de communication possibles.

<#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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.