ESA - التقاط الحزم وتحقيق الشبكة

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين وتجميع التقاط الحزم على جهاز أمان البريد الإلكتروني من Cisco (ESA)، وإجراء مزيد من تحقيقات الشبكة واستكشاف الأخطاء وإصلاحها.

معلومات أساسية

عند الاتصال بدعم Cisco التقني لمعالجة مشكلة، قد يطلب منك توفير رؤية حول نشاط الشبكة الصادر والوارد ل ESA. يوفر الجهاز القدرة على اعتراض وعرض TCP و IP والحزم الأخرى التي يتم إرسالها أو استقبالها عبر الشبكة المتصلة بها الجهاز. قد تحتاج إلى تشغيل التقاط حزمة لتصحيح أخطاء إعداد الشبكة أو التحقق من حركة مرور الشبكة التي تصل إلى الجهاز أو تتركه.

> **ملاحظة**: يشير هذا المستند إلى البرامج التي لا يتم صيانتها أو دعمها بواسطة Cisco. يتم توفير المعلومات كنوع من المجاملة لراحتك. للحصول على مزيد من المساعدة، اتصل بمورد البرامج.

من المهم أن نذكر أن tcpdump يتم إستبدال رمز واجهة سطر الأوامر (CLI) بالجديد packetcapture في إصدارات AsyncOS 7.0 والإصدارات الأحدث. يوفر هذا الأمر وظيفة مماثلة لوظيفة tcpdump وتكون أيضا متاحة للاستخدام على واجهة المستخدم الرسومية.

إذا قمت بتشغيل الإصدار 6.x من AsyncOS أو إصدار أقدم، فراجع الإرشادات حول كيفية إستخدام tcpdump أمر في *التقاط الحزمة على AsyncOS 6.x* قسم من هذا المستند. أيضا، فإن خيارات المرشح التي يتم وصفها في قسم *مرشحات التقاط الحزم* تكون صالحة لأمر التقاط الحزم الجديد أيضا.

التقاط الحزمة على AsyncOS الإصدار 7.x والإصدارات الأحدث

يصف هذا القسم عملية التقاط الحزمة على AsyncOS الإصدار 7.x والإصدارات الأحدث.

بدء التقاط حزمة أو إيقافه

in order to بدأت ربط التقاط من ال gui، انتقل إلى **المساعدة ودعم** قائمة في الأعلى يمين، **ربط التقاط**، وبعد ذلك طقطقت **بدء التقاط**. لإيقاف عملية التقاط الحزمة، انقر على **إيقاف التقاط**.

> **ملاحظة**: يتم الاحتفاظ بالتقاط الذي يبدأ في واجهة المستخدم الرسومية (GUI) بين الجلسات.

in order to بدأت ربط التقاط من ال CLI، ال **packetcapture > start** erasecat4000_flash:. لإيقاف عملية التقاط الحزمة، أدخل **packetcapture > stop** أمر، و ال ESA يوقف الربط التقاط عندما الجلسة ينتهي.

وظيفة التقاط الحزمة

فيما يلي قائمة بالمعلومات المفيدة التي يمكنك إستخدامها لمعالجة التقاط الحزمة:

- يقوم ESA بحفظ نشاط الحزمة الملتقطة في ملف وتخزينه محليا. أنت يستطيع شكلت الحد الأقصى للحزمة capture مبرد حجم، طول الوقت ل أي الربط ركض التقاط، وعلى أي شبكة قارن أن ركض التقاط. أنت يستطيع أيضا استعملت مرشح in order to حددت الربط التقاط إلى حركة مرور من خالل ميناء خاص أو حركة مرور من زبون خاص أو اندل عنوان.
- انتقل إلى **المساعدة ودعم > التقاط الحزمة** من واجهة المستخدم الرسومية (GUI) لعرض قائمة كاملة من ملفات التقاط الحزمة التي يتم تخزينها. عندما يتم تشغيل التقاط حزمة، تعرض صفحة التقاط الحزمة حالة التقاط قيد التقدم باستخدام الإحصائيات الحالية، مثل حجم الملف والوقت المنقضي.
- أختر التقاط وانقر فوق **تنزيل ملف** لتنزيل التقاط حزمة مخزنة.
- لحذف ملف التقاط حزمة، أختر ملف أو أكثر وانقر **حذف الملفات المحددة**.
- أخترت in order to حررت الربط التقاط عملية إعداد مع ال gui، **ربط التقاط** من المساعدة والدعم قائمة وطقطقة **يحرر عملية إعداد**.
- دخلت in order to حررت الربط التقاط عملية إعداد مع ال CLI، ال **packetcapture > setup** erasecat4000_flash:.

> **ملاحظة**: ال يعرض واجهة المستخدم الرسومية (GUI) الصور الحزم التي تبدأ في واجهة المستخدم الرسومية، ولكن تلك التي تبدأ ب CLI. بالمثل، يعرض ال CLI فقط الحزم التي تبدأ في ال CLI. يمكن تشغيل التقاط واحد فقط في كل مرة.

تلميح: للحصول على معلومات إضافية حول خيارات التقاط الحزمة وإعدادات المرشح، راجع قسم **عوامل تصفية التقاط الحزمة** في هذا المستند. للوصول إلى تعليمات AsyncOS عبر الإنترنت من واجهة المستخدم الرسومية، انتقل إلى **التعليمات والدعم** > **المساعدة عبر الإنترنت** > البحث عن **التقاط الحزمة** > أختر **تشغيل التقاط الحزمة.**

التقاط الحزمة على AsyncOS الإصدار 6.x والإصدارات الأقدم

يصف هذا القسم عملية التقاط الحزمة على AsyncOS الإصدار 6.x والإصدارات الأقدم.

بدء التقاط حزمة أو إيقافه

يمكنك إستخدام tcpdump من أجل التقاط TCP/IP والحزم الأخرى التي يتم إرسالها أو استقبالها عبر شبكة يتم إرفاق ESA بها.

أتمت هذا steps in order to بدأت أو أوقفت ربط التقاط:

1. أدخل **diagnostic** > **network** > **tcpdump** في واجهة سطر الأوامر (CLI) الخاصة بالإيسا. فيما يلي مثال للمخرجات:

```
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. قم بتعيين الواجهة (البيانات 1 أو البيانات 2 أو الإدارة) وعامل التصفية.

ملاحظة: يستخدم عامل التصفية نفس تنسيق [نظام Unix](#) tcpdump erasecat4000_flash:.

3. أخترت **أبدأ** in order to بدأت قبض **وإيقاف** in order to أنهيت وه.

ملاحظة: ال تخرج من قائمة tcpdump عندما يكون االلتقاط قيد التقدم. أنت ينبغي استعملت ثاني CLI نافذة in order to ركضت أي أمر آخر. بمجرد اكتمال عملية االلتقاط، يجب عليك إستخدام بروتوكول النسخ الآمن (SCP) أو نقل الملفات (FTP) من سطح المكتب المحلي لتنزيل الملفات من الدليل المسمى "التشخيص" (ارجع إلى قسم

عوامل تصفية التقاط الحزم للحصول على تفاصيل). تستخدم الملفات تنسيق التقاط الحزم (PCAP) ويمكن مراجعتها باستخدام برنامج مثل Wireshark أو EtherCurrent.

عوامل تصفية التقاط الحزم

يعرض الأمر **Diagnostic > NET** يستخدم أمر CLI صياغة مرشح tcpdump القياسية. يوفر هذا بعض الأمثلة.

هذه هي عوامل التصفية القياسية التي يتم إستخدامها:

- **IP** - عوامل التصفية لجميع حركة مرور بروتوكول IP
- **TCP** - عوامل التصفية لجميع حركة مرور بروتوكول TCP
- **مضيف IP** - عوامل التصفية لمصدر أو وجهة عنوان IP محدد

فيما يلي بعض الأمثلة على عوامل التصفية المستخدمة:

- **ip host 10.1.1.1** - يتضمن هذا المرشح أي حركة مرور تتضمن 10.1.1.1 كمصدر أو وجهة.
- **مضيف IP 10.1.1.2 أو مضيف IP 10.1.1.1** - يطابق عامل التصفية هذا حركة مرور البيانات التي تحتوي على إما 10.1.1.1 أو 10.1.1.2 كمصدر أو وجهة.

لاسترداد الملف الملتقط، انتقل إلى **var > log > التشخيص** أو **pub > البيانات**. للوصول إلى دليل التشخيص **التشخيص**.

ملاحظة: عند إستخدام هذا الأمر، يمكن أن يتسبب في مساحة قرص ESA كبيرة، كما يمكن أن يتسبب في انخفاض الأداء. Cisco يوصي أنك تستعمل هذا الأمر فقط مع المساعدة من Cisco TAC.

اكتشاف الشبكة الإضافية واستكشافها

ملاحظة: لا يمكن إستخدام الأساليب التالية إلا من واجهة سطر الأوامر.

خدمات TCPSERVICES

يعرض الأمر tcpservices سيعرض الأمر معلومات TCP/IP للميزة الحالية وعمليات النظام.

```
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
```

نتستات

تعرض هذه الأداة المساعدة إتصالات الشبكة لبروتوكول التحكم في الإرسال (الوارد والصادر على حد سواء) وجداول التوجيه وعدد من إحصائيات واجهة الشبكة وبروتوكول الشبكة.

```
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
```

الشبكة

يوفر الأمر الفرعي للشبكة تحت التشخيص الوصول إلى خيارات إضافية. يمكن إستخدام هذه الخيارات لتفريغ ذاكرة التخزين المؤقت المتعلقة بالشبكة بالكامل، وإظهار محتويات ذاكرة التخزين المؤقت لـ ARP، وإظهار محتويات ذاكرة التخزين المؤقت لـ NDP (إذا كان ذلك ممكنا)، والسماح باختبار اتصال SMTP عن بعد باستخدام SMTP.

```
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

يسمح أمر etherconfig بعرض أو تعديل العديد من مكونات الشبكة، بما في ذلك إعدادات الوسائط وVLANs وLoopback وMTU ومعالجة عناوين multicast.

ضرعي رمألا etherconfig يسمح رمأ تنأ نأ يشاهدو لكشيو ضعب نم ضعب العمليا ةعداد إ متعلق ب duplex و MAC ةمولعم تاهجاولل، VLANs، الاسترجاع نراق، MTU مجح، وقبول أو ضفر دودر ARP عم multicast ناونع.

```
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

عرض مسار الشبكة إلى مضيف بعيد. بدلا من ذلك، يمكنك إستخدام traceroute6 إذا كان لديك عناوين IPv6 مكونة على واجهة واحدة على الأقل.

```
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
```

بينغ

يسمح لك إختبار الاتصال باختبار قابلية الوصول للمضيف باستخدام عنوان IP أو اسم المضيف وتوفير إحصائيات تتعلق بزمن الوصول المحتمل و/أو حالات السقوط في الاتصال.

```
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
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).