أستكشاف أخطاء معالجة DataPath وإصلاحها وتصفية URL وUTD بوابة

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء الدفاع الموحد عن التهديد (UTD) وإصلاحها (URL) على موجهات حواف شبكة WAN بنظام التشغيل IOS® XE.

معلومات أساسية

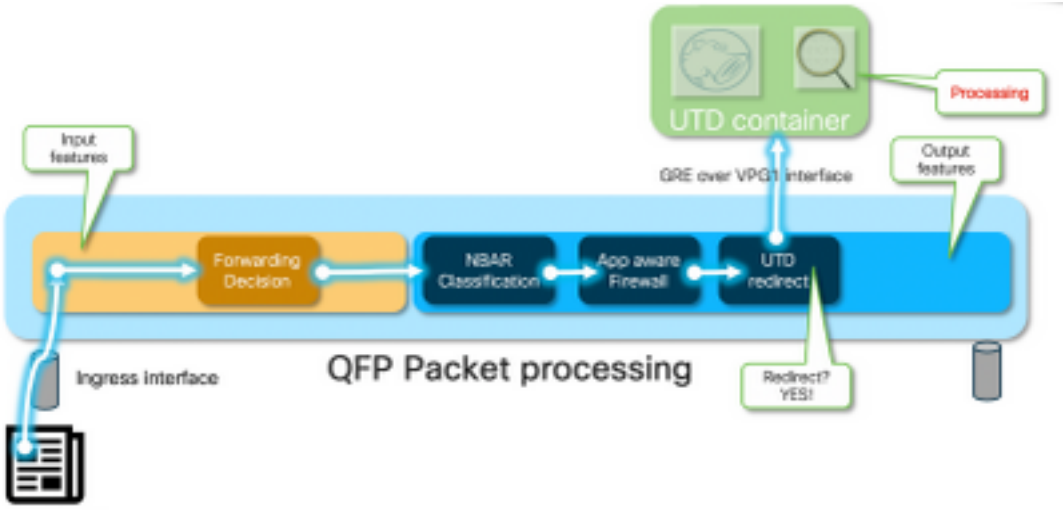
يعد برنامج Snort نظام منع التسلل (IPS) الأكثر انتشارا في العالم. منذ عام 2013، الشركة التي أنشأت تقنية برنامج Snort، يتم شراء Sourcefire من قبل Cisco. بدءا من برنامج 16.10.1 IOS® XE SD-WAN، تمت إضافة حاويات تصفية UTD/URF إلى حل Cisco SD-WAN.

تقوم الحاوية بالتسجيل إلى موجه IOS® XE باستخدام إطار عمل app-nav. وتفسير هذه العملية خارج نطاق هذا المستند.

طريقة عرض DataPath عالية المستوى

على مستوى عال، يبدو الشكل التالي:

من شبكة LAN/WAN إلى الحاوية



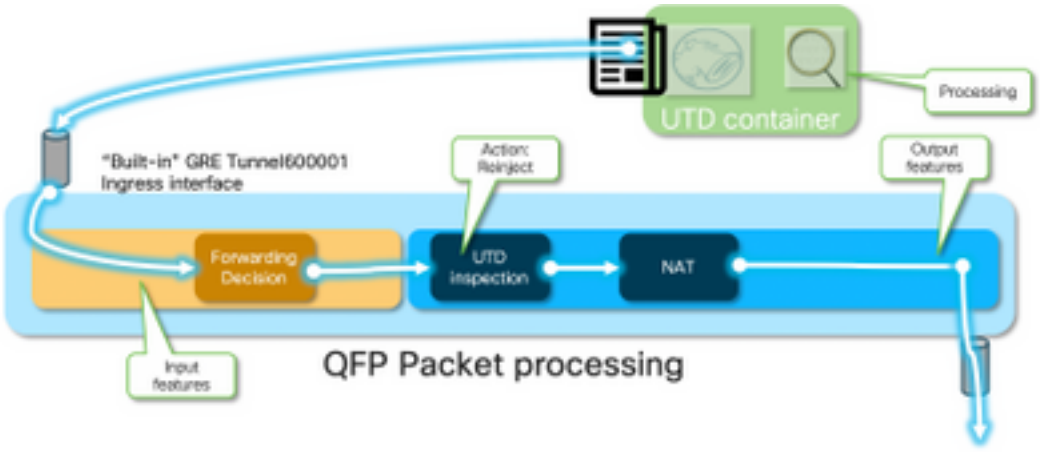
تأتي حركة المرور من جانب شبكة LAN. بما أن IOS® XE يعرف أن الحاوية في حالة سليمة، فإنه يحول حركة المرور إلى حاوية UTD. يستخدم التحويل واجهة VirtualPortGroup1 كواجهة مخرج، والتي تتضمن الحزمة داخل نفق تضمين التوجيه العام (GRE).

يجري الموجه الإجراء "PUNT" باستخدام السبب: 64 (حزمة محرك الخدمة)" ويرسل حركة مرور البيانات نحو معالج التوجيه (RP). تتم إضافة رأس نقطة ويتم إرسال الحزمة إلى الحاوية باستخدام واجهة مخرج داخلية باتجاه الحاوية "[internal0/0/svc_eng:0]"

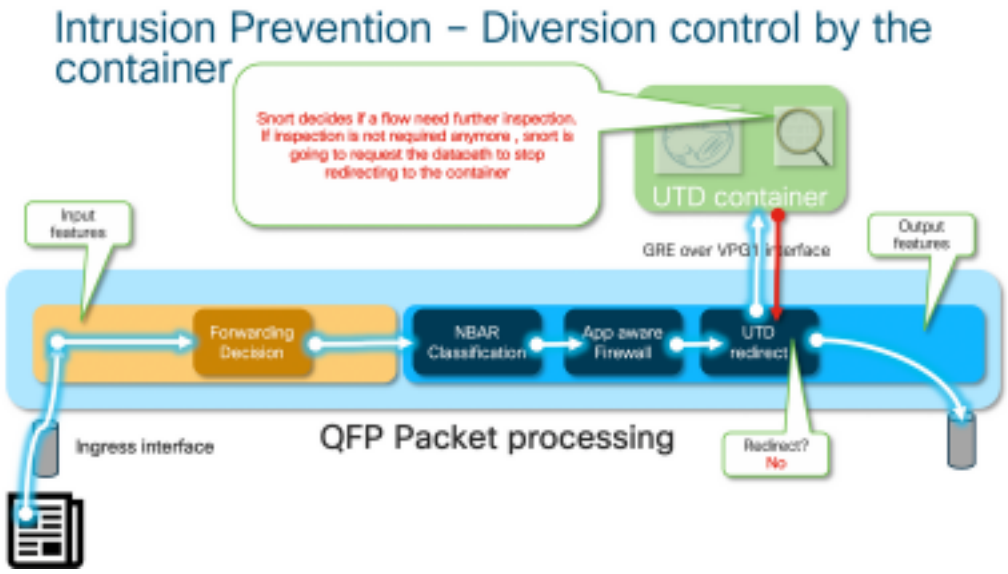
وفي هذه المرحلة، تستفيد شركة Snort من المعالجات الأولية ومجموعات القواعد الخاصة بها. يمكن إسقاط الحزمة أو إعادة توجيهها استنادا إلى نتائج المعالجة.

من الحاوية إلى شبكة LAN/WAN

بافتراض أنه لا يفترض إسقاط حركة المرور، تتم إعادة توجيه الحزمة مرة أخرى إلى الموجه بعد معالجة UTD. يظهر على معالج تدفق الكم (QFP) كقادم من نفق 600001. ثم تتم معالجتها بواسطة الموجه ويجب توجيهها (أمل) نحو واجهة شبكة WAN.



تتحكم الحاوية في نتيجة التحويل في فحص UTD في بيانات IOS® XE.



على سبيل المثال، مع تدفق HTTPS، يكون المعالجون المبادئات مهتمين برؤية حزم مرحبا / مرحبا بالخادم مع تفاوض TLS. بعد ذلك، لا تتم إعادة توجيه التدفق نظرا لقلة القيمة في فحص حركة مرور TLS المشفرة.

داتاباث ديب ديب ديفي

من وجهة نظر متعقب الحزم، سيتم عرض مجموعة الإجراءات هذه (192.168.16.254 هو عميل ويب):

```
debug platform condition ipv4 192.168.16.254/32 both
debug platform condition start
debug platform packet-trace packet 256 fia-trace data-size 3000
```

مدخل ربط من LAN أو WAN جانب باتجاه الحاوية

في هذا السيناريو الخاص، تأتي الحزمة التي تم تتبعها من الشبكة المحلية (LAN). من وجهة نظر إعادة التوجيه، هناك إختلافات ذات صلة إذا كان التدفق يأتي من الشبكة المحلية (LAN) أو شبكة WAN.

يحاول العميل الوصول إلى www.cisco.com على HTTPS

```
cedge6#show platform packet-trace packet 14
Packet: 14          CBUG ID: 3849209
Summary
  Input     : GigabitEthernet2
  Output    : internal0/0/svc_eng:0
  State     : PUNT 64  (Service Engine packet)
  Timestamp
    Start   : 1196238208743284 ns (05/08/2019 10:50:36.836575 UTC)
    Stop    : 1196238208842625 ns (05/08/2019 10:50:36.836675 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet2
    Output      : <unknown>
    Source      : 192.168.16.254
    Destination : 203.0.113.67
    Protocol    : 6 (TCP)
      SrcPort   : 35568
      DstPort   : 443
  Feature: DEBUG_COND_INPUT_PKT
    Entry       : Input - 0x8177c67c
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 2933 ns
<snip>
```

تتبعت حركة مرور تطابق الشرط مدخل على قارن GigabitEthernet2.

```
  Feature: UTD Policy (First FIA)
    Action         : Divert
    Input interface : GigabitEthernet2
    Egress interface: GigabitEthernet3
  Feature: OUTPUT_UTD_FIRST_INSPECT
    Entry       : Output - 0x817cc5b8
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 136260 ns
  Feature: UTD Inspection
    Action         : Divert             <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Input interface : GigabitEthernet2
    Egress interface: GigabitEthernet3
  Feature: OUTPUT_UTD_FINAL_INSPECT
    Entry       : Output - 0x817cc5e8
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 43546 ns
<snip>
```

على مصفوفة إستدعاء ميزة الخروج (FIA) من واجهة الخروج، قرر UTD FIA تحويل هذه الحزمة إلى الحاوية.

```
  Feature: IPV4_OUTPUT_LOOKUP_PROCESS_EXT
    Entry       : Output - 0x81781bb4
    Input       : GigabitEthernet2
    Output      : Tunnel6000001
<removed>
  Feature: IPV4_OUTPUT_LOOKUP_PROCESS_EXT
    Entry       : Output - 0x81781bb4
    Input       : GigabitEthernet2
    Output      : Tunnel6000001
<removed>
  Feature: IPV4_INPUT_LOOKUP_PROCESS_EXT
    Entry       : Output - 0x8177c698
```

```
    Input       : Tunnel6000001
    Output      : VirtualPortGroup1
    Lapsed time : 880 ns
<snip>
```

توضع الحزمة على النفق الافتراضي 600001 ويتم توجيهها عبر واجهة VPG1. في هذه المرحلة، يتم تضمين الحزمة الأصلية في GRE.

```
  Feature: OUTPUT_SERVICE_ENGINE
    Entry       : Output - 0x817c6b10
    Input       : Tunnel6000001
    Output      : internal0/0/svc_eng:0
    Lapsed time : 15086 ns
<removed>
  Feature: INTERNAL_TRANSMIT_PKT_EXT
    Entry       : Output - 0x8177c718
    Input       : Tunnel6000001
    Output      : internal0/0/svc_eng:0
    Lapsed time : 43986 ns
```

يتم إرسال الحزمة داخليا إلى الحاوية.

> **ملاحظة**: تقدم معلومات إضافية في هذا القسم عن المعلومات الداخلية المتعلقة بالحاويات ألغراض الإعلام فقط. لا يمكن الوصول إلى حاوية UTD عبر واجهة واجهة سطر الأوامر العادية.

الذهاب أعمق في الموجه نفسه، يصل حركة المرور إلى VRF داخلي على واجهة معالج التوجيه ETH2:

```
[cedge6:/]$ chvrf utd  ifconfig
eth0      Link encap:Ethernet  HWaddr 54:0e:00:0b:0c:02
          inet6 addr: fe80::560e:ff:fe0b:c02/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1375101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1366614 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:96520127 (92.0 MiB)  TX bytes:96510792 (92.0 MiB)

eth1      Link encap:Ethernet  HWaddr 00:1e:e6:61:6d:ba
          inet addr:192.168.1.2  Bcast:192.168.1.3  Mask:255.255.255.252
          inet6 addr: fe80::21e:e6ff:fe61:6dba/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:2000  Metric:1
          RX packets:1069 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2001 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:235093 (229.5 KiB)  TX bytes:193413 (188.8 KiB)

eth2      Link encap:Ethernet  HWaddr 00:1e:e6:61:6d:b9
          inet addr:192.0.2.2  Bcast:192.0.2.3  Mask:255.255.255.252
          inet6 addr: fe80::21e:e6ff:fe61:6db9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:2000  Metric:1
          RX packets:2564233 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2564203 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:210051658 (200.3 MiB)  TX bytes:301467970 (287.5 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
```

```
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

ETH0 هو واجهة إتصاالت النقل بين العمليات (TIPC) متصلة بعملية IOSd. تعمل قناة OneP فوقها لترحيل التكوينات والإخطارات ذهابا وإيابا بين حاوية IOS و UTD.

مما يهمك، يتم ربط "eth2 [واجهة الحاوية]" إلى "VPG1 [192.0.2.1/192.168.2.2]" وهي العناوين التي يتم دفعها بواسطة vManage إلى IOS-XE والحاوية.

إذا قمت بتشغيل **tcpdump**، فيمكنك رؤية حركة مرور GRE المضمنة التي تنتقل إلى الحاوية. يتضمن تضمين GRE رأس VPATH.

```
[cedge6:/]$  chvrf utd  tcpdump -nNvvvXi eth2    not udp
tcpdump: listening on eth2, link-type EN10MB (Ethernet), capture size 262144 bytes
06:46:56.350725 IP (tos 0x0, ttl 255, id 35903, offset 0, flags [none], proto GRE (47), length
121)
    192.0.2.1 > 192.0.2.2: GREv0, Flags [none], length 101
gre-proto-0x8921
0x0000:  4500 0079 8c3f 0000 ff2f ab12 c000 0201  E..y.?.../......
0x0010:  c000 0202 0000 8921 4089 2102 0000 0000  .......!@.!.....
0x0020:  0000 0000 0300 0001 0000 0000 0000 0000  ................
0x0030:  0004 0800 e103 0004 0008 0000 0001 0000  ................
0x0040:  4500 0039 2542 4000 4011 ce40 c0a8 10fe  E..9%B@.@..@....
0x0050:  ad26 c864 8781 0035 0025 fe81 cfa8 0100  .&.d...5.%......
0x0060:  0001 0000 0000 0000 0377 7777 0363 6e6e  .........www.cnn
0x0070:  0363 6f6d 0000 0100 01                   .com.....
```

بناج WAN أو LAN إلى حاوية من طبر لخدم

بعد معالجة SNORT (بافتراض عدم إسقاط حركة المرور)، يتم إعادة دمجه في مسار إعادة توجيه QFP.

```
cedge6#show platform packet-trace packet 15
Packet: 15          CBUG ID: 3849210
Summary
  Input     : Tunnel6000001
  Output    : GigabitEthernet3
  State     : FWD
```

النفق 600001 هو واجهة مخرج من الحاوية.

```
  Feature: OUTPUT_UTD_FIRST_INSPECT_EXT
    Entry       : Output - 0x817cc5b8
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 2680 ns
  Feature: UTD Inspection
    Action         : Reinject
    Input interface : GigabitEthernet2
    Egress interface: GigabitEthernet3
  Feature: OUTPUT_UTD_FINAL_INSPECT_EXT
    Entry       : Output - 0x817cc5e8
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
```

```
    Lapsed time : 12933 ns
```

بما أن حركة المرور قد تم فحصها بالفعل، فإن الموجه يعرف أن هذا هو إعادة حقن.

```
  Feature: NAT
    Direction   : IN to OUT
    Action      : Translate Source
    Steps       :
    Match id    : 1
    Old Address : 192.168.16.254 35568
    New Address : 172.16.16.254  05062
```

المرور يدخل و"NATed" وبيطلع عالنت.

```
  Feature: MARMOT_SPA_D_TRANSMIT_PKT
    Entry       : Output - 0x8177c838
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 91733 ns
```

تكامل تسجيل تدفق UTD مع تتبع الحزمة

أضاف IOS-XE 17.5.1 دمج تسجيل تدفق UTD مع تتبع الحزمة، حيث سيتضمن إخراج تتبع المسار حكم في UTD. يمكن أن يكون الحكم أحد الأمور التالية، على سبيل المثال:

- الحزمة التي يقرر UTD حظرها/تنبيهها للشيخ
- السماح/الإسقاط ل URLF
- حظر/السماح ل AMP

بالنسبة للحزم التي ال تحتوي على معلومات قرار UTD، ال يتم تسجيل أي معلومات تسجيل تدفق. الحظ أيضا عدم تسجيل إصدار قرار IPS/IDS/السماح بسبب تأثير الأداء السلبي المحتمل.

لتمكين تكامل تسجيل التدفق، أستخدم قالب وظيفة CLI الإضافية مع:

```
utd engine standard multi-tenancy
utd global
  flow-logging all
```

إخراج المثال للأحكام المختلفة:

مهلة بحث URL:

```
show platform packet-trace  pack all | sec Packet: | Feature: UTD Inspection
Packet: 31          CBUG ID: 12640
Feature: UTD Inspection
   Action                  : Reinject
   Input interface         : GigabitEthernet2
   Egress interface        : GigabitEthernet3
   Flow-Logging Information :
    URLF Policy ID         : 1
    URLF Action            : Allow(1)
    URLF Reason            : URL Lookup Timeout(8)
```

يسمح سمعة URLF والحكم:

```
Packet: 21          CBUG ID: 13859
  Feature: UTD Inspection
    Action                   : Reinject
    Input interface          : GigabitEthernet3
    Egress interface         : GigabitEthernet2
    Flow-Logging Information :
     URLF Policy ID          : 1
     URLF Action             : Allow(1)
     URLF Reason             : No Policy Match(4)
     URLF Category           : News and Media(63)
     URLF Reputation         : 81
```

السمعة والحكم في قضية URLF:

```
Packet: 26          CBUG ID: 15107
  Feature: UTD Inspection
    Action                   : Reinject
    Input interface          : GigabitEthernet3
    Egress interface         : GigabitEthernet2
    Flow-Logging Information :
     URLF Policy ID          : 1
     URLF Action             : Block(2)
     URLF Reason             : Category/Reputation(3)
     URLF Category           : Social Network(14)
     URLF Reputation         : 81
```

طلب الشرارة:

التحقق من توافق إصدار UTD مع IOS XE

```
cedge7#sh utd eng sta ver
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.10.33_SV2.9.16.1_XEmain
IOS-XE Supported UTD Regex: ^1\.10\.([0-9]+)_SV(.*)_XEmain$
UTD Installed Version: 1.0.2_SV2.9.16.1_XE17.5 (UNSUPPORTED)
```

إذا تم عرض "غير مدعوم"، يلزم ترقية الحاوية خطوة أولى قبل بدء أستكشاف الأخطاء وإصلاحها.

التحقق من تكوين خادم أسماء صالح في الحاوية

تتطلب بعض خدمات الأمان مثل AMP و URLF أن تكون حاوية UTD قادرة على حل أسماء مزود خدمة السحابة، لذلك يجب أن تحتوي حاوية UTD على تكوينات صحيحة لخادم الأسماء. يمكن التحقق من هذه الإعدادات من خلال التحقق من ملف resolv.conf للحاوية الموجودة تحت shell النظام:

```
cedge:/harddisk/virtual-instance/utd/rootfs/etc]$ more resolv.conf
nameserver 208.67.222.222
nameserver 208.67.220.220
nameserver 8.8.8.8
```

المشكلة 1

وفقا للتصميم، يجب تهيئة ميزة الدفاع الموحد عبر مؤشر الترابط بشكل كامل مع حالة إستخدام الوصول المباشر إلى الإنترنت (DIA). ستحاول الحاوية حل api.bcti.brightcloud.com من أجل الاستعلام عن فئات وسمات عنوان URL. في هذا المثال، الـ يتم حظر أي من عناوين

URL التي تم فحصها حتى إذا تم تطبيق التكوين المناسب

استكشاف الأخطاء وإصلاحها

دائما ما تنظر إلى ملف سجل الحاوية.

```
cedge6#app-hosting move appid utd log to bootflash:
Successfully moved tracelog to bootflash:
iox_utd_R0-0_R0-0.18629_0.20190501005829.bin.gz
```

التي تنسخ ملف السجل على ذاكرة Flash (الذاكرة المؤقتة) نفسها.

يمكن عرض السجل باستخدام الأمر:

```
cedge6#  more /compressed iox_utd_R0-0_R0-0.18629_0.20190501005829.bin.gz
```

يكشف عرض السجل:

```
2019-04-29 16:12:12 ERROR: Cannot resolve host api.bcti.brightcloud.com: Temporary failure in
name resolution
2019-04-29 16:17:52 ERROR: Cannot resolve host api.bcti.brightcloud.com: Temporary failure in
name resolution
2019-04-29 16:23:32 ERROR: Cannot resolve host api.bcti.brightcloud.com: Temporary failure in
name resolution
2019-04-29 16:29:12 ERROR: Cannot resolve host api.bcti.brightcloud.com: Temporary failure in
name resolution
2019-04-29 16:34:52 ERROR: Cannot resolve host api.bcti.brightcloud.com: Temporary failure in
name resolution
2019-04-29 16:40:27 ERROR: Cannot resolve host api.bcti.brightcloud.com: Temporary failure in
name resolution
```

بشكل افتراضي، يوفر vManage حاوية تستخدم خادم OpenDNS [208.67.222.222 و 208.67.220.220]

سبب جذري

تم إسقاط حركة مرور نظام اسم المجال (DNS) لحل **api.bcti.Ghtcloud.com** في مكان ما في المسار بين الحاوية وخوادم DNS المظلة. تأكد دائما من إمكانية الوصول إلى كل نظامي DNS.

المشكلة 2

في سيناريو يفترض فيه حظر جميع فئة الكمبيوتر ومعلومات الإنترنت، يتم إسقاط طلب http إلى www.cisco.com بشكل صحيح بينما تم إسقاط طلبات HTTPS.

استكشاف الأخطاء وإصلاحها

كما هو موضح مسبقا، يتم ضرب حركة المرور على الحاوية. عندما يتم تضمين هذا التدفق في رأس GRE، يتم تضمين معلومات البرنامج وكذلك رأس VPATH. باستخدام هذا الرأس، يسمح النظام بتمرير حالة تصحيح أخطاء إلى الحاوية نفسها. هذا يعني أن حاويات UTD صالحة للتشغيل بشكل جيد.

في هذا السيناريو، يكون عنوان IP للعميل 192.168.16.254. دعنا نستكشف أخطاء معالجة الشيء عن طريق الحاوية نفسها لحركة المرور التي تأتي من العميل الخاص بي.

```
debug platform condition ipv4 192.168.16.254/32 both
debug platform condition feature utd controlplane submode serviceplane-web-filtering level
verbose
debug platform condition start
```

ترشد هذه المجموعة من الأوامر IOS-XE لتعليم حركة المرور من وأ إلى 192.168.16.254. يمكن من تمرير عالمة debug-me إلى الحاوية عبر رأس VPATH

LSMPI punt header	Outer IP header (e.g. 192.0.2.x)	GRE header	vPath header (conditional debug flag is here)	Inner (original) IP packet

يقوم الشخير بتصحيح هذا التدفق المحدد فقط بينما تتم معالجة الآخرين بشكل طبيعي.

في هذه المرحلة، يمكنك مطالبة المستخدم بتشغيل حركة مرور البيانات من العميل إلى www.cisco.com.

تتمثل الخطوة التالية في إستدراد السجالت:

```
app-hosting move appid utd log to bootflash:
```

في حالة حركة مرور HTTP، يكتشف معالج HTTP المسبق عنوان URL في طلب الحصول.

```
2019-04-26 13:04:27.773:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 39540, p->dst_port
= 80
2019-04-26 13:04:27.793:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 80, p->dst_port =
39540
2019-04-26 13:04:27.794:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 39540, p->dst_port
= 80
2019-04-26 13:04:27.794:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 39540, p->dst_port
= 80
2019-04-26 13:04:27.794:(#1):SPP-URL-FILTERING got utmdata_p
2019-04-26 13:04:27.794:(#1):SPP-URL-FILTERING HTTP Callback, direction = 00000080

2019-04-26 13:04:27.795:(#1):SPP-URL-FILTERING White list regex match not enabled
2019-04-26 13:04:27.795:(#1):SPP-URL-FILTERING Black list regex match not enabled
2019-04-26 13:04:27.795:(#1):SPP-URL-FILTERING URL database Request: url_len = 12, msg overhead
12 url: www.cisco.com/ <<<<<<<
2019-04-26 13:04:27.795:(#1):SPP-URL-FILTERING Send to URL database: req_id=0x10480047
2019-04-26 13:04:27.795:(#1):SPP-URL-FILTERING Sent to URL database 24 bytes
2019-04-26 13:04:27.795:(#1):SPP-URL-FILTERING Send to URL database done, idx: 71, URL:
www.cisco.com/
2019-04-26 13:04:27.795:(#1):SPP-URL-FILTERING Received from URL database 24 bytes
2019-04-26 13:04:27.816:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 80, p->dst_port =
39540
2019-04-26 13:04:27.816:(#1):SPP-URL-FILTERING Found UTMData at 0x007f8d9ee80878, action =
0000000a
2019-04-26 13:04:27.816:(#1):SPP-URL-FILTERING Utm_verdictProcess: vrf_id 1, category 0x63,
score 81 <<<<<<<<<<<<<<<<<<<<<<<<
2019-04-26 13:04:27.816:(#1):SPP-URL-FILTERING Category 0x3f
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
2019-04-26 13:04:27.816:(#1):SPP-URL-FILTERING index = 63, action = 1
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
2019-04-26 13:04:27.816:(#1):SPP-URL-FILTERING Blocking category = 0x3f
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

في حالة حركة مرور https، تم إستخراج DNS الوجهة من الخادم مرحبا بواسطة المعالج المسبق HTTPS

```
2019-05-01 00:56:18.870:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 35322, p->dst_port
= 443
2019-05-01 00:56:18.886:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 443, p->dst_port =
35322
2019-05-01 00:56:18.887:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 35322, p->dst_port
= 443
2019-05-01 00:56:18.887:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 35322, p->dst_port
= 443
2019-05-01 00:56:18.903:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 443, p->dst_port =
35322
2019-05-01 00:56:18.906:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 443, p->dst_port =
35322
2019-05-01 00:56:18.906:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 35322, p->dst_port
= 443
2019-05-01 00:56:18.907:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 443, p->dst_port =
35322
2019-05-01 00:56:18.907:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 443, p->dst_port =
35322
2019-05-01 00:56:18.907:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 443, p->dst_port =
35322

2019-05-01 00:56:18.908:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 443, p->dst_port =
35322
2019-05-01 00:56:18.908:(#1):SPP-URL-FILTERING utm_sslLookupCallback
2019-05-01 00:56:18.908:(#1):SPP-URL-FILTERING got utmdata_p
2019-05-01 00:56:18.909:(#1):SPP-URL-FILTERING White list regex match not enabled
2019-05-01 00:56:18.909:(#1):SPP-URL-FILTERING Black list regex match not enabled
2019-05-01 00:56:18.909:(#1):SPP-URL-FILTERING URL database Request: url_len = 11, msg overhead
12 url: www.cisco.com  <<<<<<<<
2019-05-01 00:56:18.909:(#1):SPP-URL-FILTERING Send to URL database: req_id=0x10130012
2019-05-01 00:56:18.909:(#1):SPP-URL-FILTERING Sent to URL database 23 bytes
2019-05-01 00:56:18.909:(#1):SPP-URL-FILTERING Send to URL database done, idx: 18, URL:
www.cisco.com
2019-05-01 00:56:18.909:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 443, p->dst_port =
35322
2019-05-01 00:56:18.910:(#1):SPP-URL-FILTERING Found UTMData at 0x007f1d9c479640, action =
00000008
2019-05-01 00:56:18.910:(#1):SPP-URL-FILTERING Verdict very late, in queryig state 2, idx=18
2019-05-01 00:56:18.910:(#1):SPP-URL-FILTERING UTM preprocessor p->src_port = 443, p->dst_port =
35322

2019-05-01 00:56:18.910:(#1):SPP-URL-FILTERING Found UTMData at 0x007f1d9c479640, action =
00000009
2019-05-01 00:56:18.910:(#1):SPP-URL-FILTERING Verdict very late, in queryig state 2, idx=18
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
2019-05-01 00:56:18.909:(#1):SPP-URL-FILTERING Received from URL database 24 bytes
```

ال ترى هنا صفحة الحظر قيد التشغيل لأن البرنامج ال يقوم بالإبلاغ عن نتائج استعلام webroot.

سبب جذري

CSCvo77664 "فشل تصفية UTD URL للبحث عن الفئة مع فشل البحث عن WebBroot" حول حركة المرور التي يتم تسريبها عندما ال يكون لدى البرنامج إستجابة لطلب الحكم الخاص ب URL الخاص بنا بعد.

المشكلة 3

في اذه السيناريو، بشكل متقطع، يتم إسقاط جلسات لمع إستعراض الويب التي يجب السماح اهب ةطساوب ةيفصت URL [ببسب تاصنيفها]. على سبيل المثال، ال نكمي ثحب كرحم "ةئفب حامسلا ةلاح في ىتح يئاوشع لكشب www.google.com إلى لوصولا الويب".

استكشاف الأخطاء وإصلاحها

الخطوة 1: جمع الإحصاءات العامة

ظحال إعادة تعيين إخراج الأمر هذا لك 5 دقائق

```
cedge7#show utd engine standard statistics internal
*************Engine #1*************
<removed> =============================================================================== HTTP
Inspect - encodings (Note: stream-reassembled packets included): <<<<<<<<<< generic layer7 HTTP
statistics POST methods: 0 GET methods: 7 HTTP Request Headers extracted: 7 HTTP Request Cookies
extracted: 0 Post parameters extracted: 0 HTTP response Headers extracted: 6 HTTP Response
Cookies extracted: 0 Unicode: 0 Double unicode: 0 Non-ASCII representable: 0 Directory
traversals: 0 Extra slashes ("//"): 0 Self-referencing paths ("./"): 0 HTTP Response Gzip
packets extracted: 0 Gzip Compressed Data Processed: n/a Gzip Decompressed Data Processed: n/a
Http/2 Rebuilt Packets: 0 Total packets processed: 13 <removed>
=============================================================================== SSL
Preprocessor: <<<<<<<<<< generic layer7 SSL statistics SSL packets decoded: 38 Client Hello: 8
Server Hello: 8 Certificate: 2 Server Done: 6 Client Key Exchange: 2 Server Key Exchange: 2
Change Cipher: 10 Finished: 0 Client Application: 2 Server Application: 11 Alert: 0 Unrecognized
records: 11 Completed handshakes: 0 Bad handshakes: 0 Sessions ignored: 4 Detection disabled: 1

<removed> UTM Preprocessor Statistics < URL filtering statistics including ---------------------
------ URL Filter Requests Sent: 11 URL Filter Response Received: 5 Blacklist Hit Count: 0
Whitelist Hit Count: 0 Reputation Lookup Count: 5 Reputation Action Block: 0 Reputation Action
Pass: 5 Reputation Action Default Pass: 0 Reputation Action Default Block: 0 Reputation Score
None: 0 Reputation Score Out of Range: 0 Category Lookup Count: 5 Category Action Block: 0
Category Action Pass: 5 Category Action Default Pass: 0 Category None: 0 UTM Preprocessor
Internal Statistics ------------------------------------ Total Packets Received: 193 SSL Packet
Count: 4 Action Drop Flow: 0 Action Reset Session: 0 Action Block: 0 Action Pass: 85 Action
Offload Session: 0 Invalid Action: 0 No UTM Tenant Persona: 0 No UTM Tenant Config: 0 URL Lookup
Response Late: 4 <<<<< Explanation below URL Lookup Response Very Late: 64 <<<<< Explanation
below URL Lookup Response Extremely Late: 2 <<<<< Explanation below Response Does Not Match
Session: 2 <<<<< Explanation below No Response When Freeing Session: 1 First Packet Not From
Initiator: 0 Fail Open Count: 0 Fail Close Count : 0 UTM Preprocessor Internal Global Statistics
------------------------------------------- Domain Filter Whitelist Count: 0 utmdata Used Count:
11 utmdata Free Count: 11 utmdata Unavailable: 0 URL Filter Response Error: 0 No UTM Tenant Map:
0 No URL Filter Configuration : 0 Packet NULL Error : 0 URL Database Internal Statistics -------
------------------------ URL Database Not Ready: 0 Query Successful: 11 Query Successful from
Cloud: 6 <<< 11 queries were succesful but 6 only are queried via brightcloud. 5 (11-6) queries
are cached Query Returned No Data: 0 <<<<<< errors Query Bad Argument: 0 <<<<<< errors Query
Network Error: 0 <<<<<< errors URL Database UTM disconnected: 0 URL Database request failed: 0
URL Database reconnect failed: 0 URL Database request blocked: 0 URL Database control msg
response: 0 URL Database Error Response: 0
=============================================================================== Files processed:
none ===============================================================================
```

- "طلب متأخر" - يمثل HTTP GET أو عادة عميل/خادم HTTPS [حيث يكون إستخراج SNI / DN للبحث. تم إعادة توجيه الطلب المتأخر.
- "طلبات متأخرة جدا" - يعني ذلك أن نوعا من إسقاط جلسة العمل يتم فيه إسقاط إستعلام URL من Ghtcloud. حكم هجوم ملتمس يتم إسقاط الحزم الأخرى في التدفق حتى يتم تدفق SSL وباقي الأولي HTTP على الحصول بعد أي شيء يتم إسقاط. متيس، ىرخآ نعمبو

الحكم.

- "طلبات متأخرة للغاية" - عند إعادة تعيين استعلام جلسة العمل ل Brightcloud دون إصدار حكم. ستنتهي مهلة جلسة العمل بعد 60 ثانية للإصدار < 17.2.1. من 17.2.1 فصاعدًا، سوف تنتهي مهلة جلسة الاستعلام إلى Brightcloud بعد ثانيتين. [عبر CSCvr98723 UTD: انتهاء مهلة طلبات URL بعد ثانيتين]

في هذا السيناريو، نرى العدادات العالمية التي تسلط الضوء على حالة غير صحية.

الخطوة 2: النظر إلى ملف سجل التطبيق

سيقوم برنامج "اكتشاف مؤشرات الترابط الموحدة" بتسجيل الأحداث في ملف سجل التطبيقات.

```
cedge6#app-hosting move appid utd log to bootflash:
Successfully moved tracelog to bootflash:
iox_utd_R0-0_R0-0.18629_0.20190501005829.bin.gz
```

الذي يستخرج ملف سجل تطبيق الحاوية ويحفظه على الذاكرة المؤقتة نفسها.

يمكن عرض السجل باستخدام الأمر:

```
cedge6#  more /compressed iox_utd_R0-0_R0-0.18629_0.20190501005829.bin.gz
```

> **ملاحظة:** في الإصدار 20.6.1 من برنامج IOS-XE والإصدارات الأحدث، لم يعد مطلوبا نقل سجل تطبيق UTD يدويا. يمكن عرض هذه السجلات الآن باستخدام الأمر القياسي **show logging process vman module utd**

يكشف عرض السجل:

```
.....
2020-04-14 17:47:57.504:(#1):SPP-URL-FILTERING txn_id miss match verdict txn_id 245 , utmdata
txn_id 0 2020-04-14 17:47:57.504:(#1):SPP-URL-FILTERING txn_id miss match verdict txn_id 248 ,
utmdata txn_id 0 2020-04-14 17:47:57.504:(#1):SPP-URL-FILTERING txn_id miss match verdict txn_id
249 , utmdata txn_id 0 2020-04-14 17:47:57.504:(#1):SPP-URL-FILTERING txn_id miss match verdict
txn_id 250 , utmdata txn_id 0 2020-04-14 17:47:57.660:(#1):SPP-URL-FILTERING txn_id miss match
verdict txn_id 251 , utmdata txn_id 0 2020-04-14 17:47:57.660:(#1):SPP-URL-FILTERING txn_id miss
match verdict txn_id 254 , utmdata txn_id 0 2020-04-14 17:47:57.660:(#1):SPP-URL-FILTERING
txn_id miss match verdict txn_id 255 , utmdata txn_id 0 2020-04-14 17:48:05.725:(#1):SPP-URL-
FILTERING txn_id miss match verdict txn_id 192 , utmdata txn_id 0 2020-04-14
17:48:37.629:(#1):SPP-URL-FILTERING txn_id miss match verdict txn_id 208 , utmdata txn_id 0
2020-04-14 17:49:55.421:(#1):SPP-URL-FILTERING txn_id miss match verdict txn_id 211 , utmdata
txn_id 0 2020-04-14 17:51:40 ERROR: Cannot send to host api.bcti.brightcloud.com: Connection
timed out 2020-04-14 17:52:21 ERROR: Cannot send to host api.bcti.brightcloud.com: Connection
timed out 2020-04-14 17:52:21 ERROR: Cannot send to host api.bcti.brightcloud.com: Connection
timed out 2020-04-14 17:53:56 ERROR: Cannot send to host api.bcti.brightcloud.com: Connection
timed out 2020-04-14 17:54:28 ERROR: Cannot send to host api.bcti.brightcloud.com: Connection
timed out 2020-04-14 17:54:29 ERROR: Cannot send to host api.bcti.brightcloud.com: Connection
timed out 2020-04-14 17:54:37 ERROR: Cannot send to host api.bcti.brightcloud.com: Connection
timed out
....
```

- "خطأ: لا يمكن الإرسال إلى المضيف api.bcti.Ghtcloud.com" - يعني أن جلسة الاستعلام إلى Ghtcloud قد تم توقيتها [60 ثانية < 17.2.1 / 2 ثانية >= 17.2.1]. هذه علامة على الاتصال غير الصحيح ب Brightcloud.
  لتوضيح المشكلة، من شأن إستخدام EPC [Embedded Packet Capture] أن يسمح

بتصور مشكلة الاتصال.

- "قباطت مدع مكح قباطت SPP-URL-Filtering TXN_ID" - بلطتت ةلاح الخطأ هذه مزيدا نم التوضيح. يتم تنفيذ استعلام LiveCloud ربع POST حيث يتم إنشاء مرعف استعلام بواسطة الموجه

المشكلة 4

في هذا السيناريو، تعد بروتوكول IPS ميزة الأمان الوحيدة الممكنة في التوقيت العالمي المنسق (UTD)، ويواجه العميل مشاكل في اتصال الطباعة الذي يعد تطبيق TCP.

استكشاف الأخطاء وإصلاحها

لاستكشاف أخطاء هذه المشكلة وإصلاحها، قم أولا بأخذ التقاط الحزمة من ضيف TCP الذي لديه المشكلة. يظهر الالتقاط مصافحة TCP الثلاثية الاتجاهات ناجحة، ولكن يبدو أن حزم البيانات التالية مع بيانات TCP تم دق إسقاطها بواسطة موجه cEdge. تمكين تتبع الحزم التالي، والذي يظهر ما يلي:

```
edge#show platform packet-trace summ
Pkt   Input                    Output                    State  Reason
0     Gi0/0/1                  internal0/0/svc_eng:0     PUNT   64  (Service Engine packet)
1     Tu2000000001             Gi0/0/2                   FWD
2     Gi0/0/2                  internal0/0/svc_eng:0     PUNT   64  (Service Engine packet)
3     Tu2000000001             Gi0/0/1                   FWD
4     Gi0/0/1                  internal0/0/svc_eng:0     PUNT   64  (Service Engine packet)
5     Tu2000000001             Gi0/0/2                   FWD
6     Gi0/0/1                  internal0/0/svc_eng:0     PUNT   64  (Service Engine packet)
7     Tu2000000001             Gi0/0/2                   FWD
8     Gi0/0/2                  internal0/0/svc_eng:0     PUNT   64  (Service Engine packet)
9     Gi0/0/2                  internal0/0/svc_eng:0     PUNT   64  (Service Engine packet)
```

ولكن لم الحزمة رقم 8 و 9 في الحزمة أعلاه إلى المسار الخارجي الإلى محرك UTD لم يتم تحويلها إلى المحول تتم إعادة حقنهم مرة أخرى في مسار إعادة التوجيه. التحقق من أحداث تسجيل محرك UTD ال Snort. تحقق بعد ذلك من الإحصائيات الداخلية لكشف أيضا عن أي حالات إسقاط توقيع Snort. يعكس البروتوكول UTD، والتي تكشف عن بعض حالات إسقاط الحزم بسبب تطبيع بروتوكول TCP:

```
edge#show utd engine standard statistics internal
<snip>
Normalizer drops:
           OUTSIDE_PAWS: 0
             AHEAD_PAWS: 0
           NO_TIMESTAMP: 4
                BAD_RST: 0
             REPEAT_SYN: 0
            WIN_TOO_BIG: 0
               WIN_SHUT: 0
                BAD_ACK: 0
             DATA_CLOSE: 0
          DATA_NO_FLAGS: 0
             FIN_BEYOND: 0
```

سبب جذري

يرجع السبب الجذري للمشكلة إلى سلوك مكدس TCP بشكل خاطئ على الطابعات. عندما يتم التفاوض على خيار الطابع الزمني أثناء مصافحة TCP 3-way، يشير RFC7323 إلى أنه

يجب على TCP إرسال الخيار TSopt في كل حزمة غير <RST>. سيؤدي الفحص الأقرب للالتقاط الحزمة إلى إظهار عدم تمكين حزم بيانات TCP التي تم إسقاطها. باستخدام تنفيذ IOS-XE UTD، يتم تمكين تصحيح TCP باستخدام خيار الكتلة بغض النظر عن IPS أو المعرفات.

المراجع

- دليل تكوين الأمان: الدفاع الموحد ضد التهديدات

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).