Solución de problemas de manejo de datapath por UTD y filtrado de URL

Contenido

Introducción

Este documento describe cómo resolver problemas de Unified Threat Defense (UTD), también conocido como filtrado de localizador uniforme de recursos (URL) en routers IOS® XE WAN Edges.

Antecedentes

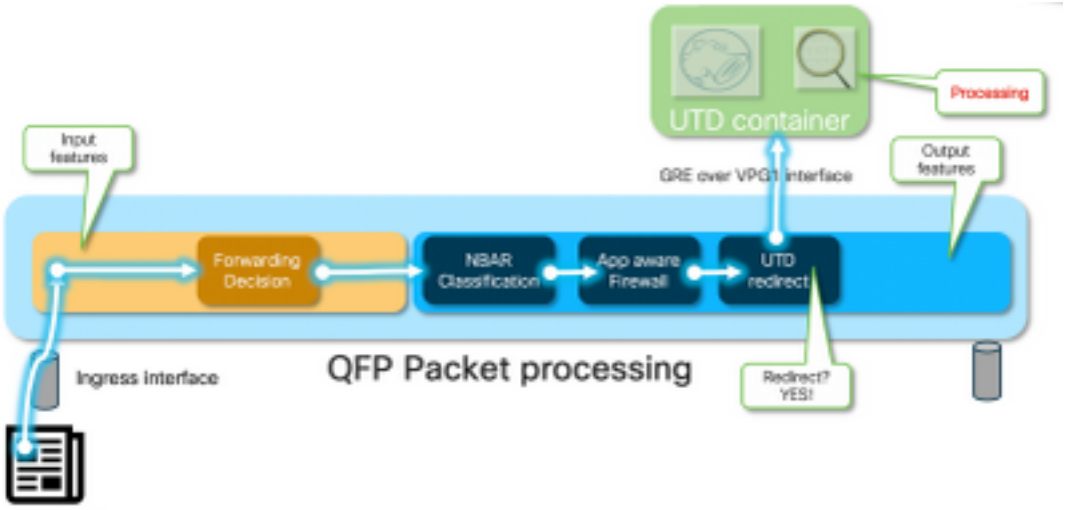
Snort es el sistema de prevención de intrusiones (IPS) más implementado en el mundo. Desde 2013, la empresa que creó una versión comercial del software Snort, Sourcefire es adquirida por Cisco. A partir del software 16.10.1 IOS® XE SD-WAN, se han agregado contenedores UTD/URF-Filtering a la solución Cisco SD-WAN.

El contenedor se registra en el router IOS ® XE mediante el marco de navegación de la aplicación. La explicación de ese proceso está fuera del alcance de este documento.

Vista de alto nivel de Datapath

En un nivel superior, el datapath se ve así:

De la LAN/WAN al contenedor



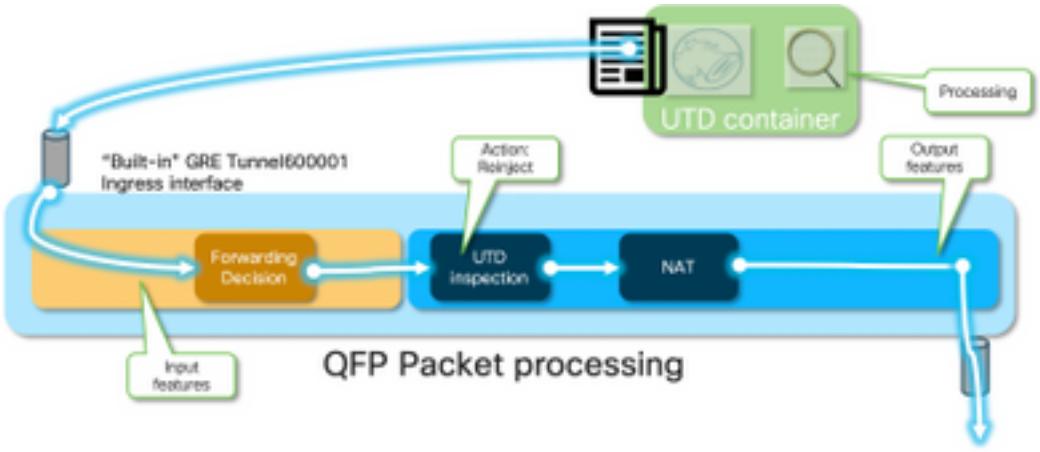
El tráfico proviene del lado LAN. Dado que IOS® XE sabe que el contenedor se encuentra en estado saludable, desvía el tráfico al contenedor UTD. La desviación utiliza la interfaz VirtualPortGroup1 como interfaz de salida, que encapsula el paquete dentro de un túnel de encapsulación de routing genérico (GRE).

El router realiza la acción "PUNT" usando la causa :64 (paquete del motor de servicio)" y envía el tráfico hacia el procesador de ruta (RP). Se agrega un encabezado punt y el paquete se envía al contenedor usando una interfaz de salida interna hacia el contenedor "[internal0/0/svc_eng:0]"

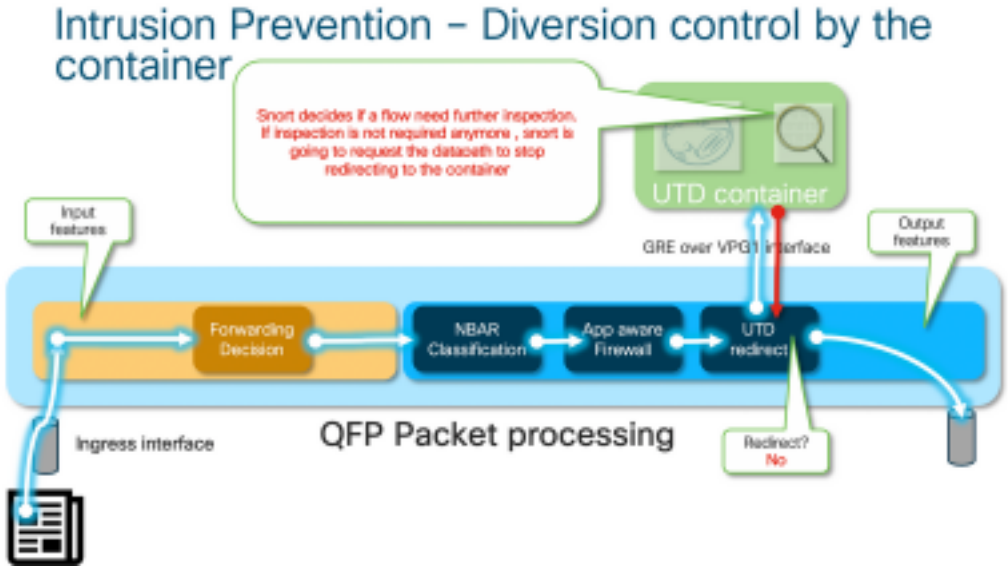
En esta etapa, Snort aprovecha sus preprocesadores y conjuntos de reglas. El paquete se puede descartar o reenviar en función de los resultados del procesamiento.

Del contenedor a LAN/WAN

Suponiendo que no se supone que se interrumpa el tráfico, el paquete se reenvía al router después del procesamiento de UTD. Aparece en el procesador de flujo cuántico (QFP) como procedente del túnel6000001. A continuación, el router lo procesa y debe enrutarse (con suerte) hacia la interfaz WAN.



El contenedor controla el resultado de la desviación en la inspección de UTD en la ruta de datos IOS ® XE.



Por ejemplo, con el flujo HTTPS, los preprocesadores están interesados en ver los paquetes Hello del servidor/Cliente con negociación TLS. Después, el flujo no se redirige porque hay poco valor en inspeccionar el tráfico cifrado TLS.

División profunda de Datapath

Desde el punto de vista del rastreador de paquetes, se verán esos conjuntos de acciones (192.168.16.254 es un cliente web):

```
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
```

Paquete de entrada desde el lado LAN o WAN hacia el contenedor

En este escenario en particular, el paquete de seguimiento proviene de la LAN. Desde el punto de vista de la redirección, existen diferencias relevantes si el flujo proviene de LAN o WAN.

El cliente intenta acceder a www.cisco.com en 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>
```

El tráfico que coincide con la condición se rastrea en la interfaz 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>
```

En la matriz de invocación de funciones de salida (FIA) de la interfaz de salida, la FIA de UTD decidió desviar este paquete al contenedor.

```
  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>
```

El paquete se coloca en el túnel predeterminado Tunnel600001 y se enruta a través de la interfaz VPG1. En esta etapa, el paquete original está encapsulado 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
```

El paquete se transmite internamente al contenedor.

> **Nota:** En esta sección se proporciona más información sobre los contenedores internos únicamente con fines informativos. No se puede acceder al contenedor UTD a través de la interfaz CLI normal.

Al profundizarse en el propio router, el tráfico llega a un VRF interno en la interfaz eth2 del procesador de ruta:

```
[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 es una interfaz de comunicación entre procesos de transporte (TIPC) conectada al proceso IOSd. El canal OneP se ejecuta sobre él para pasar configuraciones y notificaciones de ida y vuelta entre el IOSd y el contenedor UTD.

De lo que le preocupa, "eth2 [interfaz contenedor]" se enlaza a "VPG1 [192.0.2.1/192.168.2.2]" son las direcciones que vManage envía al IOS-XE y al contenedor.

Si ejecuta **tcpdump**, puede ver el tráfico encapsulado GRE que va al contenedor. La encapsulación GRE incluye un encabezado 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.....
```

Paquete de entrada desde el contenedor hacia el lado LAN o WAN

Después del procesamiento de Snort (suponiendo que el tráfico no se descarte), se vuelve a insertar en la ruta de reenvío de QFP.

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

Tunnel600001 es la interfaz de salida del contenedor.

```
  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
```

Dado que el tráfico ya se ha inspeccionado, el router sabe que se trata de una reinyección.

```
  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
```

El tráfico se convierte en NATed y se dirige a Internet.

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

Integración de registro de flujo UTD con Packet-trace

IOS-XE 17.5.1 agregó integración de registro de flujo UTD con packet-trace, donde la salida path-trace incluirá un veredicto UTD. El veredicto puede ser uno de los siguientes, por ejemplo:

- el paquete que UTD decide bloquear/alertar para Snort
- permitir/soltar para URLF
- bloquear/permitir AMP

Para los paquetes que no tienen la información de veredicto de UTD, no se registra ninguna información de registro de flujo. Tenga en cuenta también que no hay registro del veredicto IPS/IDS pass/allow debido al posible impacto negativo en el rendimiento.

Para habilitar la integración de registro de flujo, utilice la plantilla de complemento de CLI con:

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

Ejemplo de resultado para diferentes veredictos:

Límite de tiempo de búsqueda de 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)
```

Reputación de URLF y veredicto Permitir:

```
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
```

Bloque de veredicto y reputación de 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
```

Prerequesita:

Comprobación de si la versión UTD es compatible con 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)
```

Si se muestra "NO ADMITIDO", la actualización del contenedor es necesaria como primer paso antes de comenzar la resolución de problemas.

Verifique la configuración válida del servidor de nombres en el contenedor

Algunos de los servicios de seguridad, como AMP y URLF, requerirán que el contenedor UTD pueda resolver los nombres de los proveedores de servicios en la nube, por lo que el contenedor UTD debe tener configuraciones de servidor de nombres válidas. Esto puede verificarse comprobando el archivo resolv.conf para el contenedor bajo el shell del sistema:

```
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
```

Problema 1

Por diseño, Unified Thread Defense debe configurarse junto con el caso práctico de acceso directo a Internet (DIA). El contenedor intentará resolver **api.bcti.brightcloud.com** para consultar las categorías y reputación de URL. En este ejemplo, ninguna de las URL inspeccionadas se bloquea incluso si se aplica la configuración adecuada

Troubleshoot

Siempre mire el archivo de registro del contenedor.

```
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
```

Que copia el archivo de registro en la memoria flash.

La visualización del registro se puede lograr con el comando:

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

Al mostrar el registro, se muestra:

```
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
```

De forma predeterminada, vManage aprovisiona un contenedor que utiliza el servidor OpenDNS [208.67.222.222 y 208.67.220.220]

Causa raíz

El tráfico del sistema de nombres de dominio (DNS) para resolver **api.bcti.brightcloud.com** se descarta en alguna parte de la ruta entre el contenedor y los servidores DNS generales. Asegúrese siempre de que ambos DNS sean accesibles.

Problema 2

En un escenario en el que se supone que los sitios web de la categoría Informática e Información de Internet están bloqueados, la solicitud http a www.cisco.com se descarta correctamente mientras que las solicitudes HTTPS no lo están.

Troubleshoot

Como se explicó anteriormente, el tráfico se impulsa al contenedor. Cuando este flujo se encapsula en el encabezado GRE, el software agrega también un encabezado VPATH. Al

aprovechar este encabezado, el sistema permite pasar una condición de depuración al propio contenedor. Esto significa que los contenedores de UTD están bien en funcionamiento.

En este escenario, la dirección IP del cliente es 192.168,16.254. Solucionemos los problemas de manejo de la sonda por el propio contenedor para el tráfico que viene de mi cliente.

```
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
```

Este conjunto de comandos indica al IOS-XE que marque el tráfico desde o hacia 192.168.16.254. Que permite que el indicador debug-me se transmita al contenedor a través del encabezado 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

Snort depura sólo ese flujo específico mientras que otros se procesan normalmente.

En esta etapa, puede pedir al usuario que active el tráfico del cliente hacia www.cisco.com.

El siguiente paso sería recuperar los registros:

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

En el caso del tráfico HTTP, el preprocesador snort HTTP detecta la URL En la solicitud get.

```
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
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

En el caso del tráfico https, el DNS de destino ha sido extraído del servidor hello por el preprocesador 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
```

Aquí no ve la página de bloqueo que se está activando ya que el software no informa los resultados de la consulta de webroot.

Causa raíz

CSCvo77664 "El filtrado de URL de UTD para la búsqueda de categorías falla con la búsqueda

de webroot" se trata de que el tráfico se está filtrando cuando el software aún no ha respondido a nuestra solicitud de veredicto de URL.

Problema 3

En esta situación, de forma intermitente, se eliminan las sesiones de exploración web que debería permitir el filtrado de URL [debido a su clasificación]. Por ejemplo, el acceso a www.google.com no es posible al azar aunque se permita la categoría "motor de búsqueda web".

Troubleshoot

Paso 1: Recopilación de estadísticas generales

> **Nota** Esta salida de comando se restablece cada 5 minutos

```
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 ============================================================================
```

- "solicitud tardía": representa HTTP GET o el certificado de cliente/servidor HTTPS [donde se

puede extraer SNI/DN para la búsqueda. La solicitud tardía se reenvía.

- "solicitudes muy tardías": significa que algún tipo de contador de caída de sesión donde se descartan más paquetes en el flujo hasta que el router recibe un veredicto de URL de Brightcloud. En otras palabras, cualquier cosa después del HTTP GET inicial o del resto del flujo SSL se descartará hasta que se reciba un veredicto.
- "solicitudes extremadamente tardías": cuando se ha restablecido la consulta de sesión a Brightcloud sin emitir un veredicto. La sesión se agotará después de 60 segundos para la versión < 17.2.1. A partir de 17.2.1, la sesión de consulta a Brightcloud se agotará después de 2 segundos. [a través de CSCvr98723 UTD: Tiempo de espera de solicitudes URL tras dos segundos]

En este escenario, vemos contadores globales que destacan una situación poco saludable.

Paso 2: Consultar el archivo de registro de la aplicación

El software Unified Thread Detection grabará los eventos en el archivo de registro de la aplicación.

```
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
```

que extrae el archivo de registro de la aplicación del contenedor y lo guarda en la memoria flash.

La visualización del registro se puede lograr con el comando:

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

> **Nota:** En la versión 20.6.1 y posteriores del software IOS-XE, ya no es necesario mover manualmente el registro de aplicaciones UTD. Estos registros ahora se pueden ver usando el comando estándar **show logging process vman module utd**

Al mostrar el registro, se muestra:

```
.....
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
```

....

- "ERROR: No se puede enviar al host api.bcti.brightcloud.com" - significa que la sesión de consulta a Brightcloud ha estado agotando el tiempo de espera [60 segundos < 17.2.1 / 2 segundos >= 17.2.1]. Este es el signo de una mala conectividad con Brightcloud.
  Para demostrar el problema, el uso de EPC [Embedded Packet Capture] permitiría visualizar el problema de conectividad.
- "SPP-URL-FILTERING txn_id miss match verdict" - Esta condición de error requiere un poco más de explicación. La consulta Brightcloud se realiza a través de un POST donde el router genera un ID de consulta

Problema 4

En esta situación, IPS es la única función de seguridad habilitada en UTD y el cliente está experimentando problemas con la comunicación de la impresora, que es una aplicación TCP.

Troubleshoot

Para resolver este problema de ruta de datos, primero tome la captura de paquetes del host TCP que tiene el problema. La captura muestra un intercambio de señales TCP de 3 vías exitoso, pero los paquetes de datos subsiguientes con datos TCP parecen haber sido descartados por el router cEdge. Luego habilite packet-trace, que mostró lo siguiente:

```
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)
```

El resultado anterior indicó que el paquete número 8 y 9 se han desviado al motor UTD pero no se han reinyectado en el trayecto de reenvío. La verificación de los eventos de registro del motor UTD tampoco revela ninguna pérdida de firma Snort. Luego verifique las estadísticas internas de UTD, que sí muestran algunas caídas de paquetes debido al normalizador de 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
```

Causa raíz

La causa raíz del problema se debe a un mal comportamiento de la pila TCP en las impresoras. Cuando se negocia la opción Timestamp durante el intercambio de señales de TCP de 3 vías, RFC7323 establece que el TCP DEBE enviar la opción TSopt en cada paquete que no sea de<RST>. Un examen más detallado de la captura de paquetes mostrará que los paquetes de datos TCP que se descartan no tienen estas opciones habilitadas. Con la implementación UTD de IOS-XE, el normalizador TCP Snort con la opción de bloque se habilita independientemente de IPS o IDS.

Referencias

- Guía de configuración de seguridad: Defensa unificada frente a amenazas