Solucionar problemas de tratamento de dados por UTD e filtragem de URL

Contents

Introduction

Este documento descreve como solucionar problemas do Unified Threat Defense (UTD), também conhecido como filtragem de Snort e Uniform Resource Locator (URL) em roteadores IOS® XE WAN Edges.

Informações de Apoio

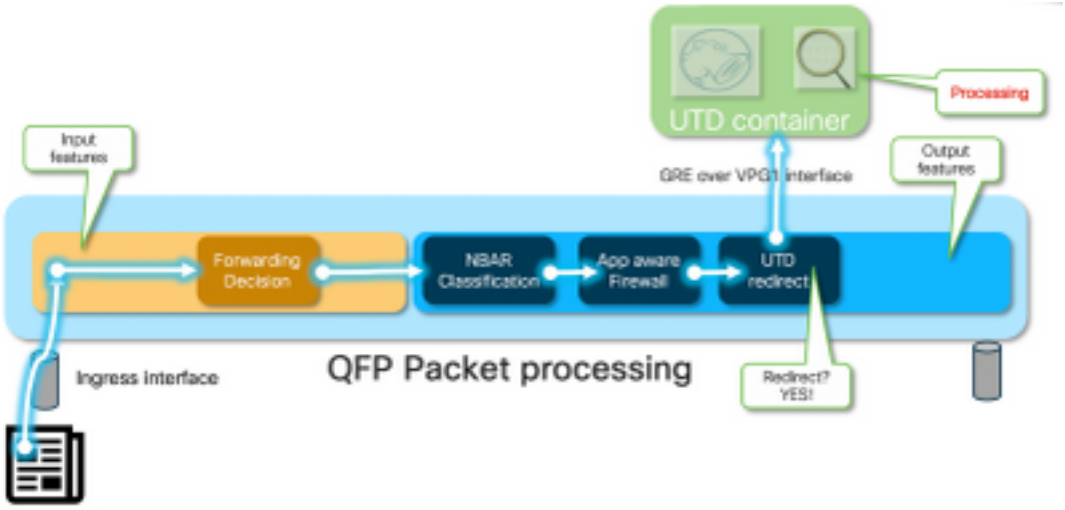
O Snort é o Sistema de Prevenção de Invasão (IPS) mais amplamente implantado no mundo. Desde 2013, a empresa que criou uma versão comercial do software Snort, a Sourcefire é adquirida pela Cisco. A partir do software IOS® XE SD-WAN 16.10.1, contêineres de filtragem de UTD/URF foram adicionados à solução Cisco SD-WAN.

O contêiner se registra no roteador IOS®XE usando a estrutura app-nav. A explicação desse processo está além do escopo deste documento.

Exibição de alto nível do Datapath

Em um nível alto, os dados ficam assim:

Da LAN/WAN ao contêiner



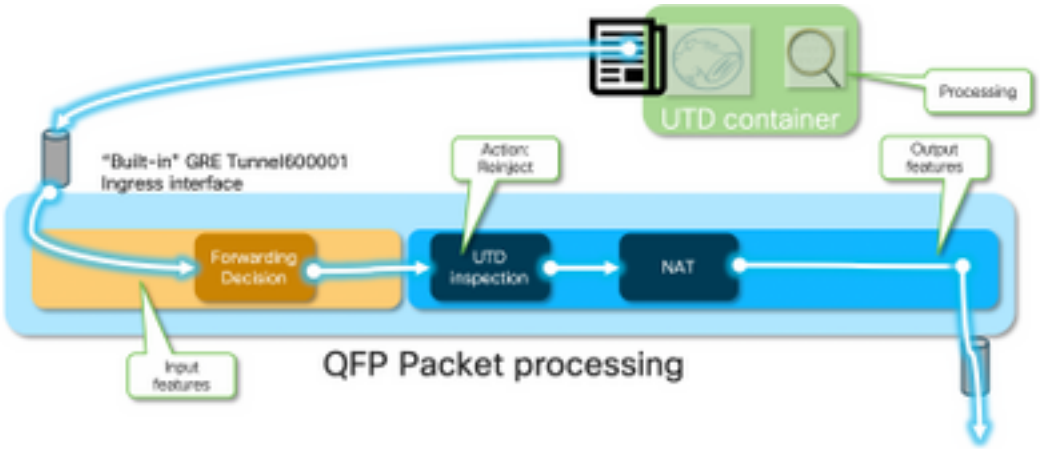
O tráfego vem do lado da LAN. Como o IOS® XE sabe que o contêiner está em um estado saudável, ele encaminha o tráfego para o contêiner UTD. O desvio usa a interface VirtualPortGroup1 como a interface de saída, que encapsula o pacote dentro de um túnel GRE (Generic Routing Encapsulation).

O roteador executa a ação "PUNT" usando a causa :64 (pacote do Service Engine)" e envia o tráfego para o RP (Route Processor). Um cabeçalho punt é adicionado e o pacote é enviado ao contêiner usando uma interface de saída interna em direção ao contêiner "[internal0/0/svc_eng:0]"

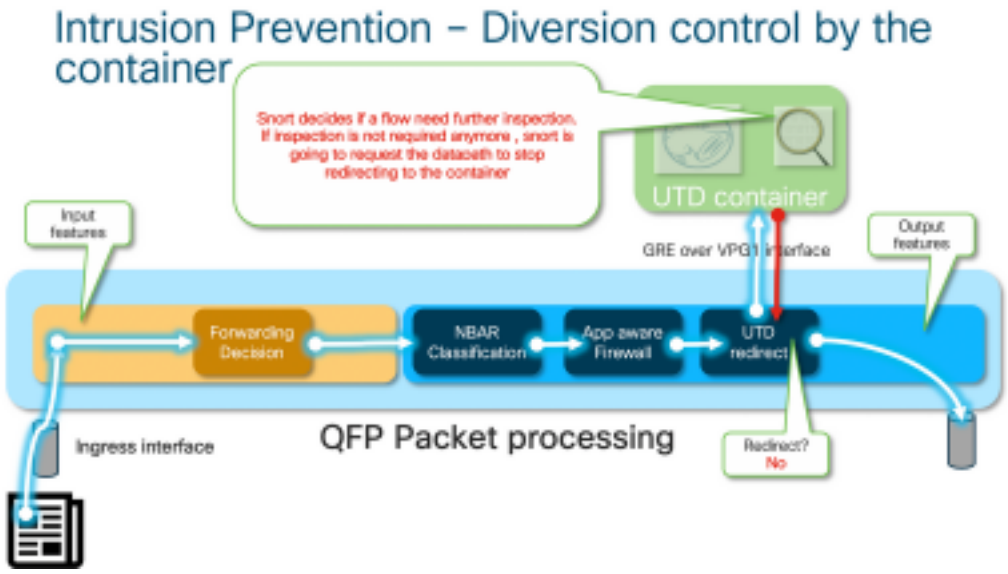
Neste estágio, o Snort aproveita seus pré-processadores e conjuntos de regras. O pacote pode ser descartado ou encaminhado com base nos resultados do processamento.

Do contêiner para LAN/WAN

Supondo que o tráfego não deva ser descartado, o pacote é encaminhado de volta ao roteador após o processamento UTD. Ele aparece no QFP (Quantum Flow Processor Processador de fluxo quântico) como vindo do Tunnel6000001. Em seguida, é processado pelo roteador e deve ser (esperamos) roteado para a interface WAN.



O contêiner controla o resultado de desvio na inspeção UTD no datapath IOS® XE.



Por exemplo, com o fluxo HTTPS, os pré-processadores estão interessados em ver os pacotes Hello do servidor / Cliente Hello com negociação TLS. Depois, o fluxo não é redirecionado, pois há pouco valor na inspeção do tráfego criptografado TLS.

Mergulho profundo no Datapath

Do ponto de vista do packet-tracer, esse conjunto de ações será visto (192.168.16.254 é um 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
```

Pacote de entrada da LAN ou da WAN na direção do contêiner

Neste cenário específico, o pacote rastreado vem da LAN. Do ponto de vista do redirecionamento, há diferenças relevantes se o fluxo vem da LAN ou da WAN.

O cliente tenta acessar www.cisco.com em 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>
```

O tráfego correspondente à condição é rastreado na entrada na interface 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>
```

No Feature Invocation Array (FIA) de saída da interface de saída, o UTD FIA decidiu desviar esse pacote para o contêiner.

```
  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>
```

O pacote é colocado no túnel padrão Tunnel600001 e é roteado através da interface VPG1. Neste estágio, o pacote original é 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
```

O pacote é transmitido internamente ao contêiner.

> **Note**: Nesta seção, são fornecidas mais informações sobre as internas dos contentores apenas para fins de informação. O contêiner UTD não pode ser acessado através da interface CLI normal.

Indo mais fundo no próprio roteador, o tráfego chega em um VRF interno na interface eth2 do processador de rota:

```
[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 é uma interface TIPC (Transport Inter Process Communication) conectada ao processo IOSd. O canal OneP é executado sobre ele para passar configurações e notificações entre o contêiner IOSd e UTD.

Do que você está preocupado, "eth2 [interface do contêiner]" é ligado a "VPG1 [192.0.2.1/192.168.2.2]" são os endereços enviados pelo vManage para o IOS-XE e o contêiner.

Se você executar **tcpdump**, poderá ver o tráfego encapsulado GRE indo para o contêiner. O encapsulamento GRE inclui um cabeçalho 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.....
```

Pacote de entrada do contêiner para o lado LAN ou WAN

Após o processamento do Snort (supondo que o tráfego não seja descartado), ele é injetado novamente no caminho de encaminhamento do QFP.

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

Tunnel600001 é a interface de saída do contêiner.

```
  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
```

Como o tráfego já foi inspecionado, o roteador sabe que é uma reinjeção.

```
  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
```

O tráfego recebe NATed e sai em direção à Internet.

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

Integração de registro de fluxo UTD com rastreamento de pacote

O IOS-XE 17.5.1 adicionou a integração de registro de fluxo UTD com rastreamento de pacote, em que a saída de rastreamento de caminho incluirá um veredito UTD. O veredito pode ser um dos seguintes, por exemplo:

- o pacote que o UTD decide bloquear/alertar para o Snort
- allow/drop para URLF
- bloquear/permitir AMP

Para pacotes que não têm as informações de veredito UTD, nenhuma informação de registro de fluxo é registrada. Além disso, observe que não há registro de aprovação/autorização de IPS/IDS devido a um possível impacto negativo no desempenho.

Para habilitar a integração de log de fluxo, use o modelo de complemento CLI com:

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

Exemplo de saída para diferentes veredictos:

Tempo limite de pesquisa 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)
```

Reputação e veredito de URLF 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
```

Reputação do URLF e bloco de veredito:

```
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
```

Pré-requisito:

Verificando se a versão UTD é compatível com o 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)
```

Se "NÃO SUPORTADO" for exibido, a atualização do contêiner será necessária como primeira etapa antes de iniciar a solução de problemas.

Verifique a configuração válida do servidor de nome no contêiner

Alguns dos serviços de segurança, como AMP e URLF, exigirão que o contêiner UTD possa resolver nomes para os provedores de serviços de nuvem, portanto, o contêiner UTD deve ter configurações de servidor de nome válidas. Isso pode ser verificado verificando-se o arquivo resolv.conf do contêiner no shell do 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 design, o Unified Thread Defense deve ser configurado completamente com o caso de uso do Direct Internet Access (DIA). O contêiner tentará resolver **api.bcti.brightcloud.com** para consultar reputações e categorias de URLs. Neste exemplo, nenhum dos URLs inspecionados é bloqueado mesmo que a configuração apropriada seja aplicada

Troubleshoot

Sempre olhe para o arquivo de log do contêiner.

```
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 o arquivo de log no próprio flash.

A exibição do log pode ser realizada com o comando:

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

A exibição do log revela:

```
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
```

Por padrão, o vManage provisiona um contêiner que usa o servidor OpenDNS [208.67.222.222 e 208.67.220.220]

Causa raiz

O tráfego do Sistema de Nomes de Domínio (DNS) para resolver **api.bcti.brightcloud.com** é descartado em algum lugar no caminho entre o contêiner e os servidores DNS de guarda-chuva. Certifique-se sempre de que ambos os DNS estejam acessíveis.

Problema 2

Em um cenário em que os sites da categoria Computador e Informações da Internet devem ser bloqueados, a solicitação http para www.cisco.com é descartada corretamente enquanto as solicitações HTTPS não são.

Troubleshoot

Como explicado antes, o tráfego é direcionado para o contêiner. Quando esse fluxo é encapsulado no cabeçalho GRE, o software é anexado e também um cabeçalho VPATH.

Aproveitando esse cabeçalho, o sistema permite passar uma condição de depuração para o próprio contêiner. Isso significa que os contêineres UTD podem ser bem servidos.

Neste cenário, o endereço IP do cliente é 192.168,16.254. Vamos resolver problemas com o tratamento de ronco pelo próprio contêiner para o tráfego que vem do meu 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
```

Esse conjunto de comandos instrui o IOS-XE a marcar o tráfego de ou para 192.168.16.254. Isso permite que o flag debug-me seja passado para o contêiner através do cabeçalho 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

O Snort depura apenas esse fluxo específico enquanto outros são processados normalmente.

Neste estágio, você pode pedir ao usuário para acionar o tráfego do cliente em direção a www.cisco.com.

A próxima etapa seria recuperar os registros:

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

No caso de tráfego HTTP, o pré-processador HTTP de snort descobre a URL na solicitação 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
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

No caso de tráfego https, o DNS de destino foi extraído do hello do servidor pelo pré-processador 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
```

Aqui você não vê a página de bloqueio sendo acionada, pois o software não relata os resultados da consulta de inicialização.

Causa raiz

CSCvo77664 "A filtragem de URL do UTD para pesquisa de categoria está falhando com falha

de pesquisa do webroot" é sobre o tráfego que está vazando quando o software ainda não tem resposta à nossa solicitação de veredito de URL.

Problema 3

Neste cenário, intermitentemente, as sessões de navegação na Web que devem ser permitidas pela filtragem de URL [devido à sua classificação] são descartadas. Por exemplo, o acesso a www.google.com não é possível aleatoriamente, mesmo que a categoria "mecanismo de pesquisa na Web" seja permitida.

Troubleshoot

Etapa1: Coletando estatísticas gerais

Observação Esta saída do comando é redefinida a 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 ================================================================================
```

- "requisição atrasada" - representa o HTTP GET ou o certificado cliente/servidor HTTPS [onde SNI / DN pode ser extraído para pesquisa. A solicitação atrasada é encaminhada.
- "solicitações muito atrasadas" - significa que algum tipo de contador de descarte de sessão onde mais pacotes no fluxo são descartados até que o roteador receba um veredito de URL do Brightcloud. Em outras palavras, qualquer coisa após o HTTP GET inicial ou o restante do fluxo SSL será descartado até que um veredito seja recebido.
- "solicitações extremamente atrasadas" - quando a consulta de sessão para Brightcloud foi redefinida sem fornecer um veredito. O tempo limite da sessão é de 60 segundos para a versão < 17.2.1. A partir de 17.2.1, a sessão de consulta para Brightcloud expirará após 2 segundos. [via CSCvr98723 UTD: Tempo limite de solicitações de URL após dois segundos]

Nesse cenário, vemos contadores globais que destacam uma situação não saudável.

Etapa 2: Olhando o arquivo de log do aplicativo

O software Unified Thread Detection gravará eventos no arquivo de log do aplicativo.

```
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 extrai o arquivo de log do aplicativo de contêiner e o salva na própria flash.

A exibição do log pode ser realizada com o comando:

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

> **Observação:** na versão 20.6.1 e posterior do software IOS-XE, não é mais necessário mover manualmente o log do aplicativo UTD. Esses registros agora podem ser exibidos usando o comando padrão **show logging process vman module utd**

A exibição do log revela:

```
.....
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
....
```

- “ERRO: Não é possível enviar ao host api.bcti.brightcloud.com" - significa que a sessão de consulta para Brightcloud expirou [60 segundos < 17.2.1 / 2 segundos >= 17.2.1]. Esse é o sinal de uma conectividade ruim com o Brightcloud.
  Para demonstrar o problema, o uso do EPC [Embedded Packet Capture] permitiria visualizar o problema de conectividade.
- "SPP-URL-FILTERING txn_id miss match verdict" - Esta condição de erro requer uma explicação um pouco mais detalhada. A consulta Brightcloud é executada por meio de um POST, em que uma ID de consulta é gerada pelo roteador

Problema 4

Neste cenário, o IPS é o único recurso de segurança habilitado no UTD, e o cliente está tendo problemas com a comunicação da impressora, que é um aplicativo TCP.

Troubleshoot

Para solucionar esse problema de datapath, primeiro pegue a captura de pacote do host TCP que está tendo o problema. A captura mostra um handshake triplo TCP bem-sucedido, mas os pacotes de dados subsequentes com dados TCP parecem ter sido descartados pelo roteador cEdge. Em seguida, ative o rastreamento de pacotes, mostrando o seguinte:

```
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)
```

A saída acima indicou que os pacotes 8 e 9 foram desviados para o mecanismo UTD, mas não foram injetados novamente no caminho de encaminhamento. A verificação dos eventos de registro do mecanismo UTD também não revela nenhum descarte de assinatura Snort. Em seguida, verifique as estatísticas internas do UTD, que revelam algumas quedas de pacotes devido ao normalizador 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 raiz

A causa raiz do problema é o mau comportamento da pilha TCP nas impressoras. Quando a opção Timestamp é negociada durante o handshake triplo do TCP, o RFC7323 afirma que o TCP DEVE enviar a opção TSopt em cada pacote que não é o <RST>. Um exame mais detalhado da captura de pacotes mostrará que os pacotes de dados TCP sendo descartados não têm essas opções habilitadas. Com a implementação do UTD do IOS-XE, o normalizador do Snort TCP com a opção de bloqueio é ativado independentemente do IPS ou IDS.

Referências

- Guia de configuração de segurança: Defesa unificada contra ameaças