UTD 및 URL 필터링에 의한 데이터 경로 처리 문제 해결

목차

소개

이 문서에서는 IOS® XE WAN Edge 라우터에서 Snort 및 URL(Unified Resource Locator) 필터링이라고도 하는 UTD(Unified Threat Defense)를 트러블슈팅하는 방법에 대해 설명합니다.

배경 정보

Snort는 세계에서 가장 널리 구축된 IPS(Intrusion Prevention System)입니다. 2013년부터 Snort 소프트웨어의 상용 버전을 만든 Sourcefire는 Cisco에 인수되었습니다. 16.10.1 IOS® XE SD-WAN 소프트웨어부터 UTD/URF 필터링 컨테이너가 Cisco SD-WAN 솔루션에 추가되었습니다.

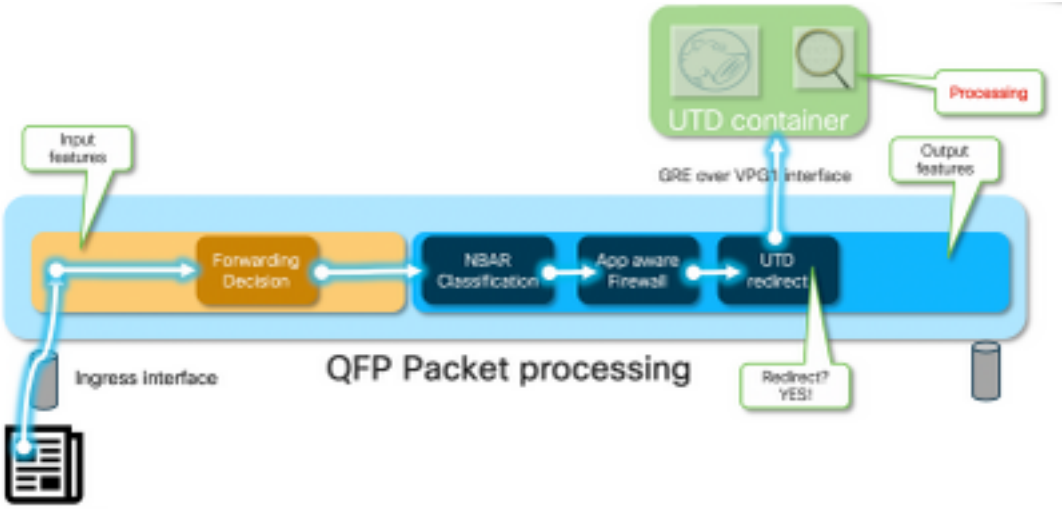
컨테이너는 app-nav 프레임워크를 사용하여 IOS® XE 라우터에 등록합니다. 이 프로세스에 대한

설명은 이 문서의 범위를 벗어납니다.

데이터 경로 상위 수준 보기

상위 레벨에서 데이터 경로는 다음과 같습니다.

LAN/WAN에서 컨테이너까지



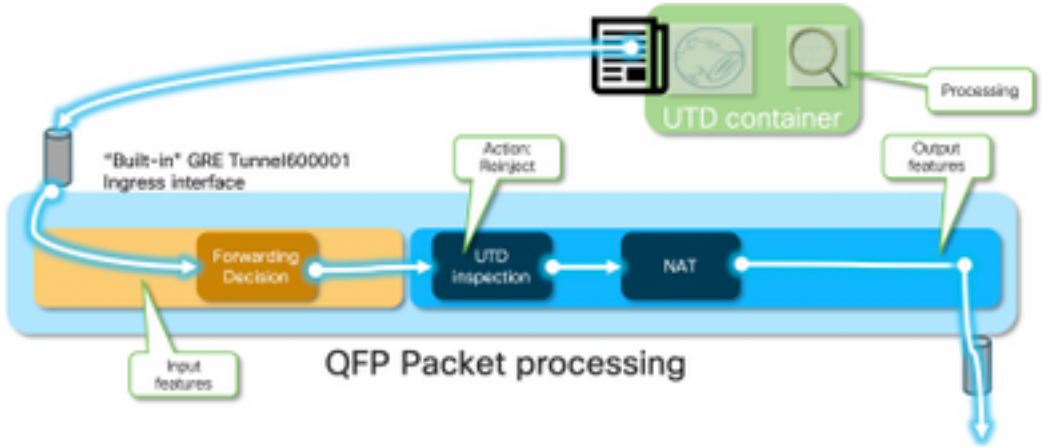
트래픽은 LAN에서 옵니다. IOS® XE는 컨테이너가 정상 상태임을 인식하므로 트래픽을 UTD 컨테이너로 전환합니다. 우회는 VirtualPortGroup1 인터페이스를 이그레스 인터페이스로 사용하며, 이 인터페이스는 GRE(Generic Routing Encapsulation) 터널 내부에 패킷을 캡슐화합니다.

라우터는 원인: 64 (Service Engine packet)"를 사용하여 "PUNT" 작업을 수행하고 트래픽을 RP(Route Processor)로 전송합니다. 펀트 헤더가 추가되고 패킷이 컨테이너 "[internal0/0/svc_eng:0]"에 대한 내부 이그레스 인터페이스를 사용하여 컨테이너에 전송됩니다.

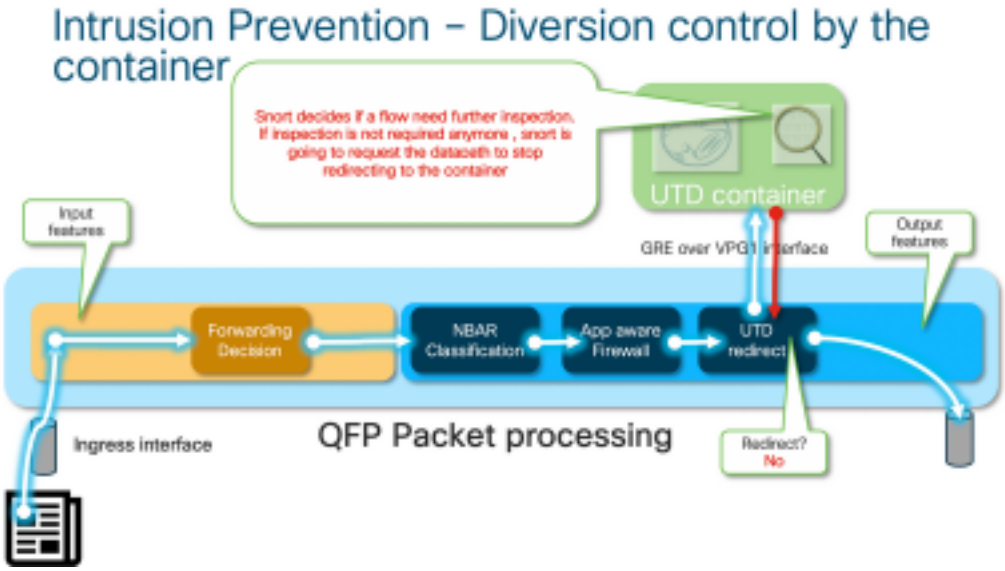
이 단계에서 Snort는 프리프로세서 및 규칙 세트를 활용합니다. 처리 결과에 따라 패킷을 삭제하거나 전달할 수 있습니다.

컨테이너에서 LAN/WAN으로

트래픽이 삭제되어야 한다고 가정할 경우 UTD 처리 후 패킷이 라우터로 다시 전달됩니다. Tunnel600001에서 가져온 QFP(Quantum Flow Processor)에 나타납니다. 그런 다음 라우터에서 처리되고 WAN 인터페이스로 라우팅되어야 합니다(바라건대).



컨테이너는 IOS® XE 데이터 경로에서 UTD 검사의 전환 결과를 제어합니다.



예를 들어, HTTPS 플로우의 경우 프리프로세서는 TLS 협상이 포함된 서버 Hello/Client Hello 패킷을 확인하고자 합니다. TLS 암호화 트래픽을 검사하는 데 값이 거의 없으므로 나중에 플로우가 리디렉션되지 않습니다.

데이터 경로 심층 분석

패킷 추적기의 관점에서 이러한 작업 집합이 표시됩니다(192.168.16.254은 웹 클라이언트).

```
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
```

LAN 또는 WAN 측에서 컨테이너를 향하는 인그레스 패킷

이 특정 시나리오에서는 추적된 패킷이 LAN에서 옵니다. 리디렉션의 관점에서 플로우가 LAN 또는 WAN에서 오는지 여부는 관련 차이점이 있습니다.

클라이언트가 HTTPS에서 www.cisco.com에 액세스하려고 시도합니다.

```
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>
```

조건과 일치하는 트래픽은 인터페이스 GigabitEthernet2에서 인그레스(ingress)를 추적합니다.

```
  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>
```

이그레스 인터페이스의 이그레스 기능 호출 어레이(FIA)에서 UTD FIA는 이 패킷을 컨테이너로 전환하기로 결정했습니다.

```
  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>
```

패킷은 기본 터널 Tunnel60001에 배치되며 VPG1 인터페이스를 통해 라우팅됩니다. 이 단계에서는 원래 패킷이 GRE로 캡슐화됩니다.

```
  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
```

패킷이 내부적으로 컨테이너에 전송됩니다.

> **참고:** 이 섹션에서는 컨테이너 내역에 대한 추가 정보를 참조용으로만 제공합니다. UTD 컨테이너는 일반 CLI 인터페이스를 통해 액세스할 수 없습니다.

라우터 자체에서 더 깊이 들어가면 트래픽이 경로 프로세서 인터페이스 eth2의 내부 VRF에 도착합니다.

```
[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)
```

Eth0은 IOSd 프로세스에 연결된 TIPC(Transport Inter Process Communication) 인터페이스입니다. OneP 채널은 IOSd와 UTD 컨테이너 간에 컨피그레이션 및 알림을 전달하기 위해 이를 통해 실행됩니다.

염려하는 사항에서 "eth2 [container interface]"는 vManage가 IOS-XE 및 컨테이너에 푸시한 주소로서 "VPG1 [192.0.2.1/192.168.2.2]"에 브리징됩니다.

tcpdump를 실행하는 경우 **GRE 캡슐화된** 트래픽이 컨테이너로 이동하는 것을 볼 수 있습니다. GRE 캡슐화에는 VPATH 헤더가 포함됩니다.

```
[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.....
```

컨테이너에서 LAN 또는 WAN 쪽으로 인그레스 패킷

Snort 처리(트래픽을 삭제하지 않을 것으로 가정)한 후 다시 QFP 포워딩 경로로 다시 주입됩니다.

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

Tunnel60001은 컨테이너의 이그레스 인터페이스입니다.

```
  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
```

트래픽이 이미 검사되었으므로 라우터는 이를 재주입한다는 것을 알고 있습니다.

```
  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
```

트래픽은 NAT를 받고 인터넷을 향해 이동합니다.

```
  Feature: MARMOT_SPA_D_TRANSMIT_PKT
```

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

패킷 추적과 UTD 플로우 로깅 통합

IOS-XE 17.5.1은 packet-trace와의 UTD 플로우 로깅 통합을 추가했습니다. 여기서 path-trace 출력에는 UTD 판정이 포함됩니다. 예를 들어, 판정은 다음 중 하나일 수 있습니다.

- UTD에서 Snort에 대해 차단/경고하기로 결정한 패킷
- URLF 허용/삭제
- AMP 차단/허용

UTD 판정 정보가 없는 패킷의 경우 플로우 로깅 정보가 로깅되지 않습니다. 또한 부정적인 성능에 영향을 미칠 수 있으므로 IPS/IDS 통과/허용 판정을 로깅하지 않습니다.

플로우 로깅 통합을 활성화하려면 CLI Add-On 템플릿을 다음 기능과 함께 사용합니다.

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

다른 판정에 대한 출력 예:

URL 조회 시간 초과:

```
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)
```

URLF 평판 및 판정 허용:

```
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
```

URLF 평판 및 판정 블록:

```
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
```

사전 요청:

UTD 버전이 IOS XE와 호환되는지 확인

```
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)
```

"UNSUPPORTED(지원되지 않음)"가 표시되면 문제 해결을 시작하기 전의 첫 번째 단계로 컨테이너 업그레이드가 필요합니다.

컨테이너에서 유효한 네임서버 컨피그레이션 확인

AMP 및 URLF와 같은 일부 보안 서비스에서는 UTD 컨테이너가 클라우드 서비스 공급자의 이름을 확인할 수 있어야 하므로 UTD 컨테이너에는 유효한 네임서버 구성이 있어야 합니다. 시스템 셸 아래의 컨테이너에 대한 resolv.conf 파일을 확인하여 확인할 수 있습니다.

```
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
```

문제 1

설계에 따라 DIA(Direct Internet Access Use Case)를 사용하여 통합 스레드 방어를 모두 구성해야 합니다. 컨테이너는 URL 평판 및 카테고리를 쿼리하기 위해 api.bcti.brightcloud.com을 확인하려고 시도합니다. 이 예에서는 올바른 컨피그레이션이 적용되더라도 검사된 URL이 차단되지 않습니다

문제 해결

항상 컨테이너 로그 파일을 확인합니다.

```
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
```

는 로그 파일을 플래시 자체에 복사합니다.

다음 명령을 사용하여 로그를 표시할 수 있습니다.

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

로그 표시:

```
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
```

기본적으로 vManage는 OpenDNS 서버를 사용하는 컨테이너를 프로비저닝합니다[208.67.222.222 및 208.67.220.220]

근본 원인

api.bcti.brightcloud.com을 확인하기 위한 DNS(Domain Name System) 트래픽은 컨테이너와 우산 DNS 서버 사이의 경로 어딘가에 있습니다. 항상 두 DNS에 모두 연결할 수 있는지 확인합니다.

문제 2

컴퓨터 및 인터넷 정보 범주 웹 사이트를 차단해야 하는 시나리오에서 HTTPS 요청이 없는 동안 www.cisco.com에 대한 http 요청이 올바르게 삭제됩니다.

문제 해결

앞에서 설명한 것처럼, 트래픽은 컨테이너에 펀딩됩니다. 이 흐름이 GRE 헤더에 캡슐화되면 소프트웨어는 VPATH 헤더와 함께 추가됩니다. 이 헤더를 사용하면 시스템에서 디버그 조건을 컨테이너 자체에 전달할 수 있습니다. 즉, UTD 컨테이너는 서비스 가능한 상태가 됩니다.

이 시나리오에서는 클라이언트 IP 주소가 192.168,16.254입니다. 클라이언트에서 오는 트래픽에 대해 컨테이너 자체의 snort 처리 문제를 해결하겠습니다.

```
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
```

이 명령 집합은 IOS-XE가 192.168.16.254에서 오는 트래픽을 표시하도록 지시합니다. 그러면 debug-me 플래그가 VPATH 헤더를 통해 컨테이너에 전달되도록 할 수 있습니다

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

Snort는 다른 플로우가 정상적으로 처리되는 동안에만 해당 플로우를 디버깅합니다.

이 단계에서는 사용자에게 클라이언트에서 www.cisco.com으로 향하는 트래픽을 트리거하도록 요청할 수 있습니다.

다음 단계는 로그를 검색하는 것입니다.

app-hosting move appid utd log to bootflash:

HTTP 트래픽의 경우 snort HTTP 프리프로세서는 get 요청에서 URL을 검색합니다.

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

https 트래픽의 경우 HTTPS 프리프로세서에 의해 서버 hello에서 대상 DNS가 추출되었습니다.

```
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
```

소프트웨어에서 webroot 쿼리의 결과를 보고하지 않으므로 차단 페이지가 트리거되는 것을 볼 수 없습니다.

근본 원인

CSCvo77664 "Webroot 조회 실패로 범주 조회에 대한 UTD URL 필터링이 실패했습니다."는 소프트웨어가 아직 URL 판정 요청에 응답하지 않을 때 트래픽이 유출되는 것을 의미합니다.

문제 3

이 시나리오에서는 URL-Filtering [분류 때문]에서 허용해야 하는 웹 검색 세션이 간헐적으로 삭제됩니다. 예를 들어, www.google.com에 액세스하는 것은 "웹 검색 엔진" 카테고리가 허용되더라도 임의로 불가능합니다.

문제 해결

1단계: 일반 통계를 수집하는 중

> **참고** 이 명령 출력은 5분마다 재설정됩니다.

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

- "late request" - HTTP GET 또는 HTTPS 클라이언트/서버 인증서를 나타냅니다. [여기서 SNI/DN을 추출하여 조회할 수 있습니다. 늦은 요청이 전달됩니다.
- "very late requests" - 라우터가 Brightcloud에서 URL 판정을 받을 때까지 흐름의 추가 패킷이 삭제되는 일종의 세션 삭제 카운터를 의미합니다. 다시 말해, 최초 HTTP GET 이후 또는 SSL 흐름의 나머지 모든 내용은 판정을 받을 때까지 삭제됩니다.
- "극도로 늦은 요청" - 판정을 제공하지 않고 Brightcloud에 대한 세션 쿼리가 재설정된 경우 버전 < 17.2.1에 대해 세션이 60초 후 시간 초과됩니다. 17.2.1부터 Brightcloud에 대한 쿼리 세션이 2초 후 시간 초과됩니다. [CSCvr98723을 통해 UTD: 2초 후 URL 요청 시간 초과]

이 시나리오에서는 비정상 상황을 강조하는 글로벌 카운터가 표시됩니다.

2단계: 애플리케이션 로그 파일 보기

Unified Thread Detection 소프트웨어가 애플리케이션 로그 파일에 이벤트를 기록합니다.

```
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
```

컨테이너 애플리케이션 로그 파일을 추출하여 플래시 자체에 저장합니다.

다음 명령을 사용하여 로그를 표시할 수 있습니다.

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

참고: IOS-XE 소프트웨어 버전 20.6.1 이상에서는 UTD 애플리케이션 로그를 수동으로 이동

할 필요가 없습니다. 이제 표준 명령 show logging process vman module **utd**를 사용하여 이러한 로그를 볼 수 있습니다.

로그 표시:

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

- "오류: 호스트 api.bcti.brightcloud.com에 보낼 수 없음" - Brightcloud에 대한 쿼리 세션이 시간 초과되었음을 의미합니다[60초 < 17.2.1 / 2초 >= 17.2.1]. 이는 Brightcloud와의 연결이 잘못되었음을 나타냅니다.
  이 문제를 시연하기 위해 EPC [Embedded Packet Capture](EPC [Embedded Packet Capture])를 사용하면 연결 문제를 시각화할 수 있습니다.
- "SPP-URL-FILTERING txn_id miss match verdict" - 이 오류 조건에 대한 자세한 설명이 필요합니다. Brightcloud 쿼리는 라우터에서 쿼리 ID를 생성하는 POST를 통해 수행됩니다

문제 4

이 시나리오에서는 IPS가 UTD에서 활성화된 유일한 보안 기능이며 고객은 TCP 애플리케이션인 프린터 통신에 문제가 발생합니다.

문제 해결

이 데이터 경로 문제를 해결하려면 먼저 문제가 있는 TCP 호스트에서 패킷 캡처를 수행합니다. 캡처는 성공적인 TCP 3-way 핸드셰이크를 표시하지만, TCP 데이터가 포함된 후속 데이터 패킷은 cEdge 라우터에서 삭제된 것 같습니다. 다음 enable packet-trace(다음 표시):

```
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)
```

위의 출력에서 패킷 번호 8 및 9가 UTD 엔진으로 전환되었지만 전달 경로에 다시 삽입되지 않았습니다. UTD 엔진 로깅 이벤트를 확인해도 Snort 시그니처 삭제는 표시되지 않습니다. 다음으로 TCP 노멀라이저로 인해 일부 패킷 삭제를 나타내는 UTD 내부 통계를 확인합니다.

```
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
```

근본 원인

문제의 근본 원인은 프린터에서 TCP 스택이 잘못 작동하기 때문입니다. TCP 3-way 핸드셰이크 중에 Timestamp 옵션이 협상된 경우 RFC7323은 TCP가 모든 비<RST> 패킷에서 TSopt 옵션을 전송해야 한다고 나타냅니다. 패킷 캡처를 자세히 검사하면 삭제된 TCP 데이터 패킷에 이러한 옵션이 활성화되지 않은 것으로 표시됩니다. IOS-XE UTD 구현에서는 IPS 또는 IDS에 관계없이 블록 옵션을 사용하는 Snort TCP 노멀라이저가 활성화됩니다.

참조

- 보안 구성 가이드: 통합 위협 방어