透過UTD和URL過濾排除資料路徑處理故障

目錄

簡介

本檔案介紹如何在IOS® XE WAN邊緣路由器上排查統一威脅防禦(UTD)(也稱為Snort和統一資源定位器(URL)過濾)故障。

背景資訊

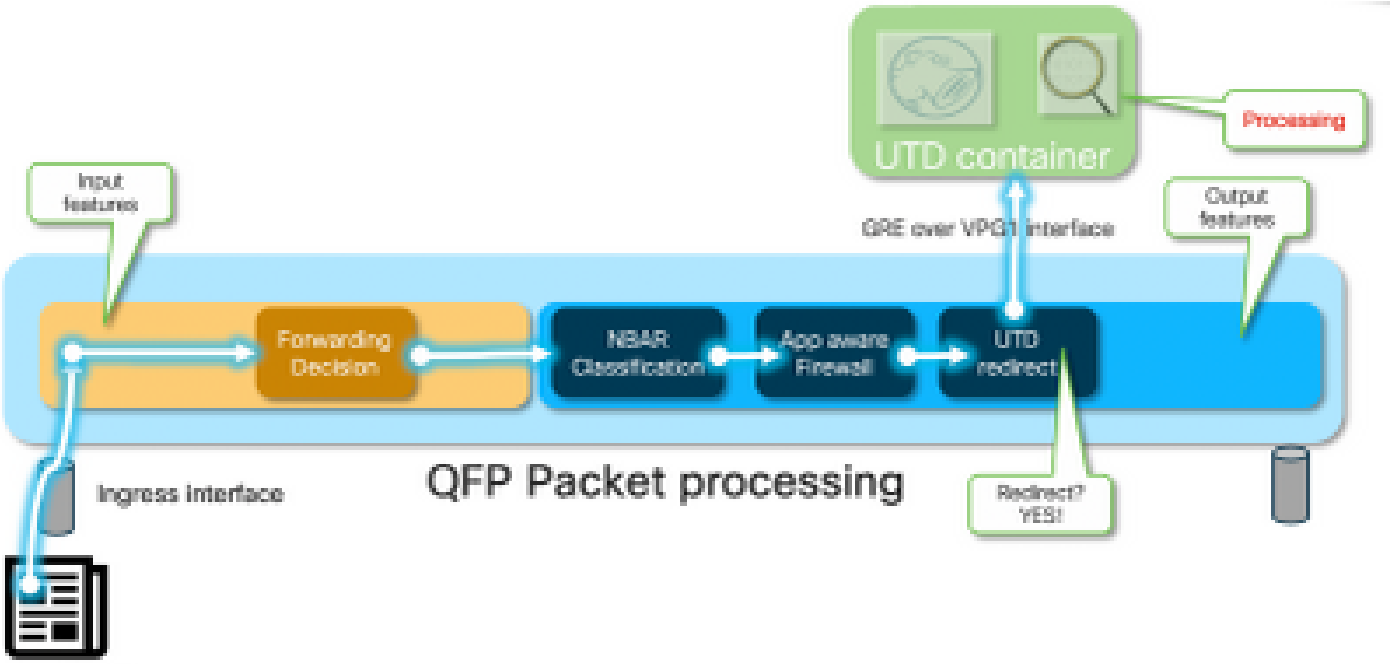
Snort是世界上部署最廣泛的入侵防禦系統(IPS)。自2013年以來，建立商業版Snort軟體的公司Sourcefire被思科收購。從16.10.1 IOS® XE SD-WAN軟體開始，UTD/URF過濾容器已增加到Cisco SD-WAN解決方案。

容器使用app-nav架構註冊到IOS®XE路由器。該過程的說明不在本檔案的範圍之內。

資料路徑高級檢視

在較高層級，資料路徑如下所示：

從LAN/WAN到容器



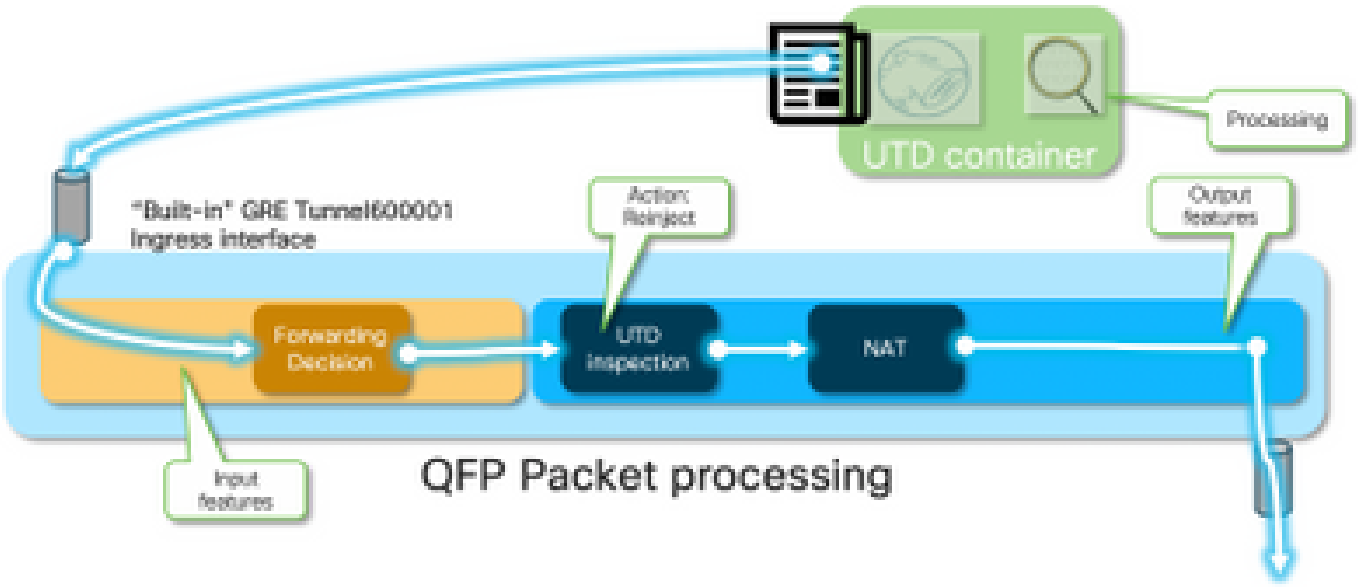
流量來自LAN端。由於IOS® XE知道容器處於正常狀態，因此它會將流量轉移到UTD容器。此轉移使用VirtualPortGroup1介面作為輸出介面，將封包封裝在通用路由封裝(GRE)通道中。

路由器使用原因：64（服務引擎封包）執行「PUNT」動作，並將流量傳送到路由處理器(RP)。增加一個傳送報頭，並使用朝向容器「[internal0/0/svc_eng：0]」的內部輸出介面將資料包傳送到容器

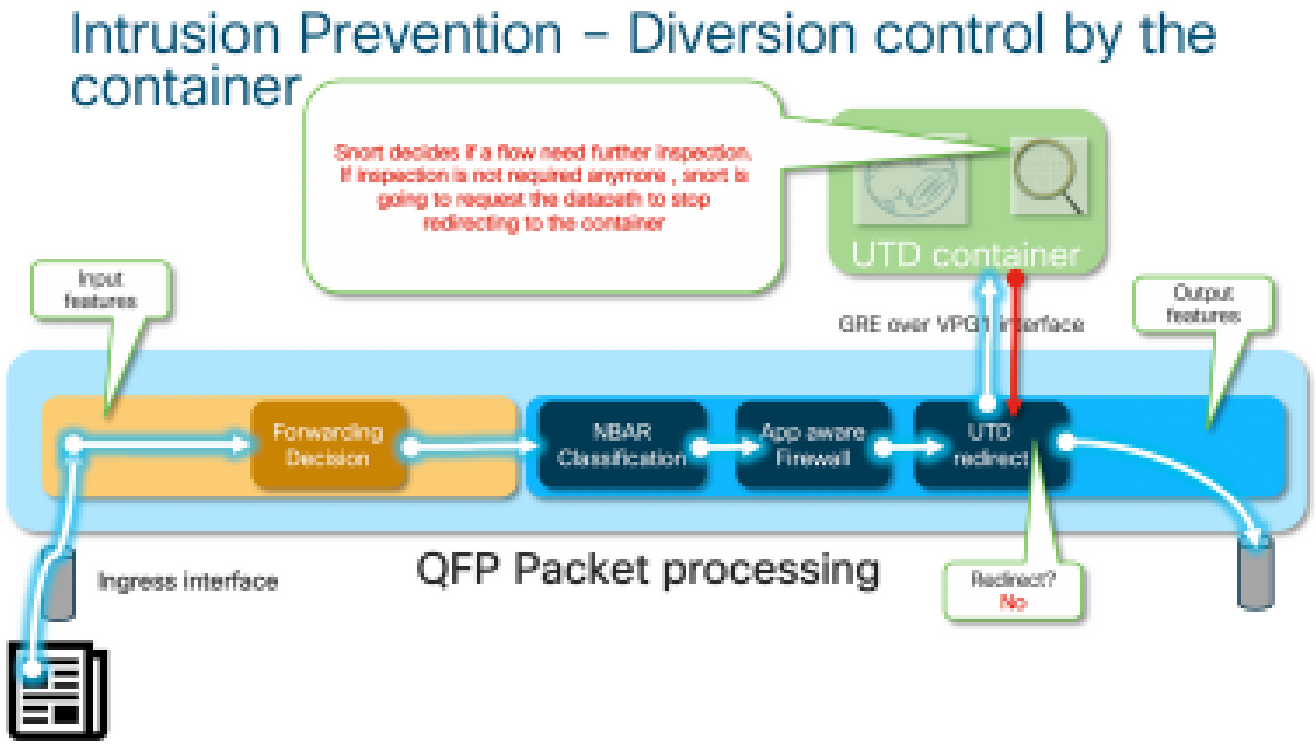
在此階段，Snort會利用其前處理器和規則集。可以根據處理結果丟棄或轉發資料包。

從容器到LAN/WAN

假設流量不應被丟棄，則資料包會在UTD處理之後轉發迴路由器。它在Quantum Flow Processor (QFP)上顯示為來自Tunnel6000001。然後由路由器進行處理，並且必須（希望）路由到WAN介面。



容器控制IOS® XE資料路徑中UTD檢查的轉移結果。



例如，對於HTTPS流，前處理器有興趣檢視具有TLS協商的伺服器Hello/客戶端Hello資料包。然後，由於檢查TLS加密流量幾乎沒有價值，因此流量不會被重定向。

資料路徑深入分析

從Packet Tracer的角度來看，將看到這些操作集（192.168.16.254是Web客戶端）：

```
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
```

從LAN或WAN端到容器的入口資料包

在此特定案例中，追蹤的封包來自LAN。從重定向的角度來看，如果流量來自LAN或WAN，則存在相關差異。

客戶端嘗試透過HTTPS訪問www.cisco.com

```
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>
```

與條件匹配的流量在介面GigabitEthernet2上以入口進行跟蹤。

```
  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>
```

在輸出介面的輸出功能呼叫陣列(FIA)上，UTD FIA決定將此封包轉向容器。

```
  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>
```

封包會被置於預設的通道通道上600001並透過VPG1介面進行路由。在此階段，原始資料包採用GRE封裝。

```
  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
```

資料包在內部傳輸到容器。

注意：本節中有關容器內部結構的進一步資訊僅供參考。無法通過常規CLI介面訪問UTD容器。

在路由器自身中越深入，流量到達路由處理器介面eth2上的內部VRF：

```
[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是連線到IOSd進程的傳輸進程間通訊(TIPC)介面。OneP通道透過它來在IOSd和UTD容器之間來回傳遞配置和通知。

根據您關心的問題，「eth2 [容器介面]」橋接到「VPG1 [192.0.2.1/192.168.2.2]」是vManage推送到IOS-XE和容器的地址。

如果運行tcpdump，則會看到傳輸到容器的GRE封裝流量。GRE封裝包括VPATH報頭。

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

從容器到LAN或WAN端的入口資料包

在Snort處理之後（假設流量不會被丟棄），它會重新注入回QFP轉發路徑。

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

通道600001來自容器的出口介面。

```
  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
```

由於流量已經過檢查，因此路由器知道這是重新注入。

```
  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
```

流量經過NAT處理並傳向Internet。

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

UTD流日誌記錄與Packet-trace整合

IOS-XE 17.5.1增加了UTD流日誌記錄與packet-trace的整合，其中path-trace輸出將包括UTD判定。判定可為下列其中一項，例如：

- UTD決定阻止/告知Snort的資料包
- 允許/丟棄URLF
- 封鎖/允許AMP

對於沒有UTD判定資訊的資料包，不會記錄流日誌記錄資訊。另請注意，由於潛在的負面效能影響，沒有記錄IPS/IDS透過/允許判定。

要啟用流日誌記錄整合，請將CLI外掛模板與以下內容配合使用：

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

不同裁決的輸出示例：

URL查詢超時：

```
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信譽和判定允許：

```
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信譽和判定區塊：

```
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
```

先決條件：

檢查UTD版本是否與IOS XE相容

```
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)
```

如果顯示「UNSUPPORTED」，則需要首先升級容器，然後再開始故障排除。

檢查容器中是否有有效的名稱伺服器配置

某些安全服務（如AMP和URLF）要求UTD容器能夠解析雲服務提供商的名稱，因此UTD容器必須具有有效

```
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
```

問題1

根據設計，統一執行緒防禦必須使用直接網際網路訪問使用案例(DIA)進行完全配置。容器將嘗試解析**api.b**

疑難排解

請始終檢視容器日誌檔案。

```
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
```

這會將記錄檔複製到快閃記憶體本身。

可以使用以下命令顯示日誌：

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

顯示日誌會顯示：

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

預設情況下，vManage調配使用OpenDNS伺服器的容器[208.67.222.222和208.67.220.220]

根本原因

用於解析**api.bcti.brightcloud.com**的域名系統(DNS)流量被丟棄在容器和umbrella DNS伺服器之間的某個路徑

問題2

在電腦和Internet資訊類別網站應被阻止的場景中，對www.cisco.com的http請求會被正確丟棄，而對HTTPS請

疑難排解

如前所述，流量被傳送至容器。當此流封裝在GRE報頭中時，軟體將附加VPATH報頭。利用此報頭，系統

在本場景中，客戶端IP地址是192.168,16.254。對於來自我的客戶端的流量，讓我們排除容器自身的Snort處

```
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
```

這組命令指示IOS-XE標籤來自或發往192.168.16.254的流量。這將允許透過VPATH報頭將調試與我標誌傳

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僅調試特定流，而其它流則正常處理。

在此階段，您可以要求使用者觸發從客戶端到www.cisco.com的流量。

下一步是擷取記錄：

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

對於HTTP流量，snort HTTP前處理器在get請求中發現URL。

```
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:
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  <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

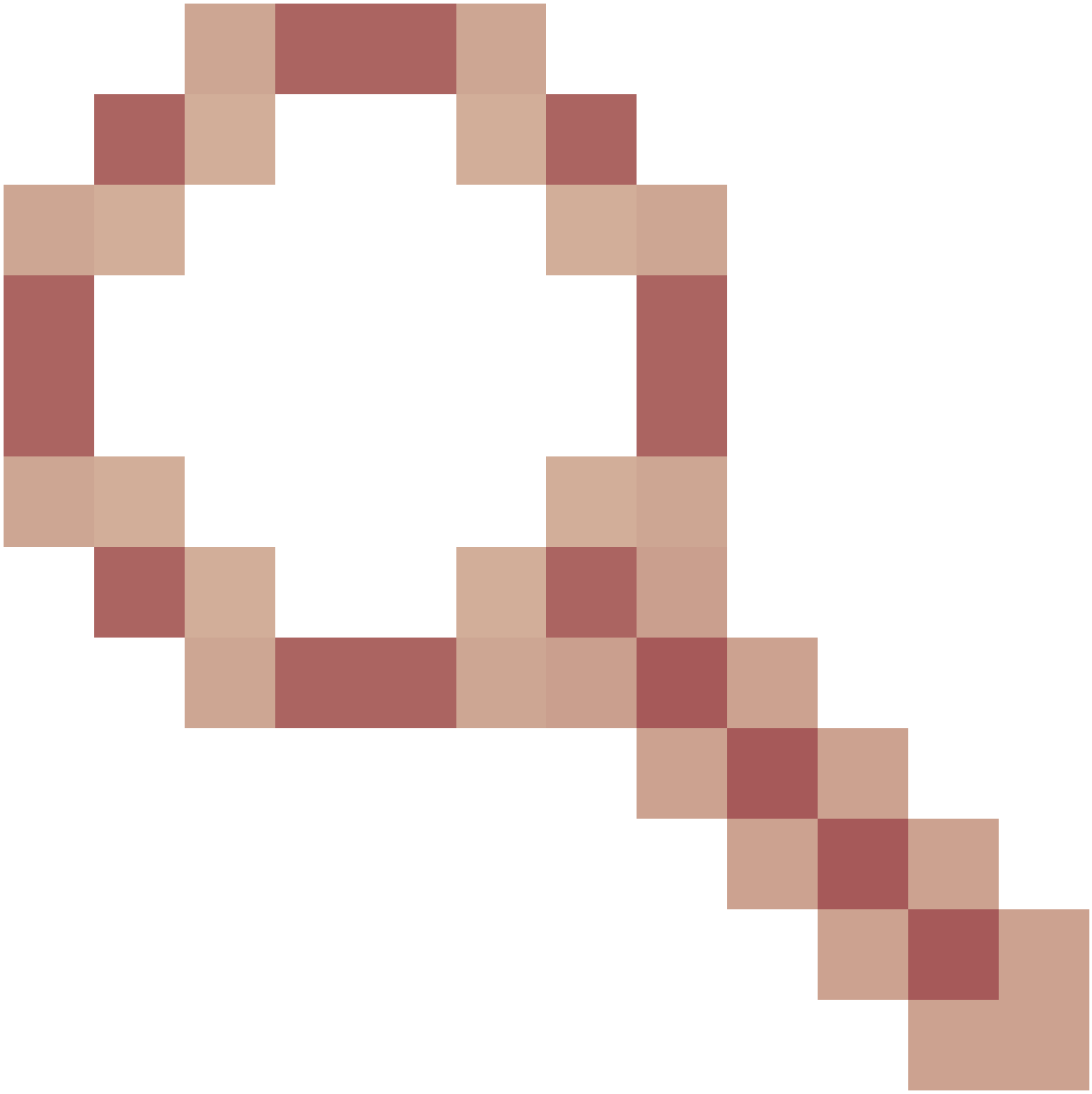
對於https流量，已使用HTTPS前處理器從伺服器hello中提取目標DNS

```
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:
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
```

此處您看不到正在觸發的阻止頁，因為軟體未報告Webroot查詢的結果。

根本原因



[CSCvo77664](#) 「UTD

問題3

在此案例中，會間歇性捨棄URL-Filtering應允許的Web瀏覽工作階段（因其分類）。例如，即使允許類別「

疑難排解

步驟1：收集一般統計資料

> **注意**此命令輸出每5分鐘重置一次

<#root>

```
cedge7#
```

```
show utd engine standard statistics internal
```

```
*************Engine #1*************
<removed>
==============================================================================
HTTP Inspect - encodings (Note: stream-reassembled packets included): <<<<<<<<<< generic layer7 HTTP st
    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 brigh
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」-表示HTTP GET或HTTPS客戶端/伺服器證書[可從中提取SNI/DN以進行查詢。轉發延
- 「非常晚請求」-表示某種型別的會話丟棄計數器，在該計數器中，流中的其他資料包將被丟棄，直到
- 「極晚請求」-重設Brightcloud會話查詢時未提供判定結果。版本< 17.2.1的會話將在60秒後超時。從

在此場景中，我們看到突出顯示不良情況的全局計數器。

步驟2：檢視應用程式日誌檔案

統一執行緒檢測軟體將在應用程式日誌檔案中記錄事件。

```
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
```

該命令將提取容器應用程式日誌檔案並將其儲存到快閃記憶體中。

可以使用以下命令顯示日誌：

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

注意：在IOS-XE軟體版本20.6.1及更高版本中，不再需要手動移動UTD應用程式日誌。現在可

顯示日誌會顯示：

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

- 「錯誤：無法傳送到主機api.bcti.brightcloud.com」-表示到Brightcloud的查詢會話已超時[60秒< 17.2.1
  為了演示問題，使用EPC（嵌入式資料包捕獲）可以直觀地顯示連線問題。

- 「SPP-URL-FILTERING txn_id miss match verdict」-此錯誤情況需要多一些解釋。Brightcloud查詢透

問題4

在此場景中，IPS是UTD中唯一啟用的安全功能，並且客戶遇到了TCP應用的印表機通訊問題。

疑難排解

若要疑難排解此資料路徑問題，請先從發生問題的TCP主機擷取封包。捕獲顯示TCP三次握手成功，但帶有

```
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)
```

上述輸出表明第8個和第9個資料包已轉移至UTD引擎，但它們未重新注入轉發路徑。檢查UTD引擎日誌記錄

```
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
```

根本原因

問題的根本原因是印表機上的TCP堆疊行為不當。在TCP三次握手期間協商Timestamp選項時，RFC7323表明

參考資料

- 安全配置指南：統一威脅防禦