

O servidor DHCP não funciona em um roteador que execute o Cisco IOS XE SD-WAN com diâmetro

Índice

[Introdução](#)

[Problema](#)

[Solução](#)

Introdução

Este original descreve os problemas típicos que puderam ser esperados quando política centralizada dos dados para o acesso à internet direto (diâmetro) e o servidor DHCP é configurado no serviço-lado VPN do mesmo roteador que executa o software IOS®-XE SDWAN. Os problemas similares puderam ser considerados com todo o outro tráfego que ingressos ao dispositivo do lado VPN do serviço e são pretendidos para o processamento local do roteador.

Problema

O servidor DHCP não funciona no roteador com ® do Cisco IOS - software XE SDWAN. O diâmetro é configurado com uma política centralizada dos dados como mostrado aqui:

```
policy
data-policy _LAN_DIA
  vpn-list LAN
    sequence 1
      match
        destination-data-prefix-list EXCLUDE_SUBNET
      !
      action accept
      set
        local-tloc-list
        color biz-internet lte
        encaps ipsec
      !
    !
  !
  sequence 11
    action accept
    nat use-vpn 0
  !
!
default-action accept
!
lists
  data-prefix-list EXCLUDE_SUBNET
  ip-prefix 10.0.0.0/8
!
```

```

site-list DIA_BRANCHES
  site-id 7
  site-id 6
!
vpn-list LAN
  vpn 10
!
!
!
apply-policy
site-list DIA_BRANCHES
  data-policy _LAN_DIA_EXCLUDE from-service
!
!

```

Solução

A fim fazer este trabalho, os pacotes DHCP devem ser excluídos da política dos dados, desde que se vê claramente do rastreamento de pacotes debuga que pacotes aos endereços de broadcast não pode ser distribuído (GOTA 72 Ipv4RoutingErr) e são NATed (ação: REDIRECT_NAT) de acordo com a política SDWAN (característica: Política dos dados SDWAN DENTRO):

```

B2#show platform packet-trace summary
<skipped>
28  V190          V190          DROP    72  (Ipv4RoutingErr)
29  Gi0/1/0       Gi0/0/0       FWD
30  V190          V190          DROP    72  (Ipv4RoutingErr)

```

```

B2#show platform packet-trace packet 28
Packet: 28          CBUG ID: 28
Summary
  Input      : Vlan90
  Output     : Vlan90
  State      : DROP 72  (Ipv4RoutingErr)
Timestamp
  Start     : 14482257476440 ns (12/17/2018 13:56:58.524691 UTC)
  Stop      : 14482257534440 ns (12/17/2018 13:56:58.524749 UTC)

```

```

Path Trace
Feature: IPV4(Input)
  Input      : Vlan90
  Output     : <unknown>
  Source     : 0.0.0.0
  Destination : 255.255.255.255
  Protocol   : 17 (UDP)
  SrcPort    : 68
  DstPort    : 67
Feature: DEBUG_COND_INPUT_PKT
  Entry      : Input - 0x10e44b40
  Input      : Vlan90
  Output     : <unknown>
  Lapsed time : 106 ns
Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
  Entry      : Input - 0x10e5ca94
  Input      : Vlan90
  Output     : <unknown>
  Lapsed time : 253 ns
Feature: IPV4_INPUT_FOR_US_MARTIAN
  Entry      : Input - 0x10e5cb24

```

Input : Vlan90
Output : <unknown>
Lapsed time : 4853 ns
Feature: IPV4_INPUT_FNF_FIRST_EXT
Entry : Input - 0x10e48968
Input : Vlan90
Output : <unknown>
Lapsed time : 600 ns
Feature: SDWAN Data Policy IN
VRF : 1
Seq : 1
DNS Flags : (0x0) NONE
Policy Flags : 0x10
Action : REDIRECT_NAT
Feature: SDWAN_DATA_POLICY_IN_EXT
Entry : Input - 0x10eb9d7c
Input : Vlan90
Output : <unknown>
Lapsed time : 5360 ns
Feature: IPV4_INPUT_DST_LOOKUP_ISSUE
Entry : Input - 0x10e5c9d8
Input : Vlan90
Output : <unknown>
Lapsed time : 200 ns
Feature: IPV4_INPUT_ARL
Entry : Input - 0x10e46158
Input : Vlan90
Output : <unknown>
Lapsed time : 200 ns
Feature: IPV4_INTERNAL_DST_LOOKUP_CONSUME
Entry : Input - 0x10e5cac4
Input : Vlan90
Output : <unknown>
Lapsed time : 253 ns
Feature: STILE_LEGACY_DROP
Entry : Input - 0x10eb294c
Input : Vlan90
Output : <unknown>
Lapsed time : 306 ns
Feature: INGRESS_MMA_LOOKUP_DROP
Entry : Input - 0x10eae2a4
Input : Vlan90
Output : <unknown>
Lapsed time : 213 ns
Feature: INPUT_DROP_FNF_AOR
Entry : Input - 0x10e5b864
Input : Vlan90
Output : <unknown>
Lapsed time : 386 ns
Feature: INPUT_FNF_DROP
Entry : Input - 0x10e48cf8
Input : Vlan90
Output : <unknown>
Lapsed time : 493 ns
Feature: INPUT_DROP_FNF_AOR_RELEASE
Entry : Input - 0x10e5b234
Input : Vlan90
Output : <unknown>
Lapsed time : 213 ns
Feature: INPUT_DROP
Entry : Input - 0x10e439d4
Input : Vlan90
Output : <unknown>
Lapsed time : 106 ns

```
Feature: IPV4_INTERNAL_FOR_US
Entry      : Input - 0x10e5cb54
Input      : Vlan90
Output     : <unknown>
Lapsed time : 4640 ns
```

A política dos dados é alterada para excluir como mostrado pacotes DHCP (portas 67,68 UDP) do NAT aqui:

```
B2# show sdwan policy from-vsmart
from-vsmart data-policy _LAN_DIA
direction from-service
vpn-list LAN
sequence 1
match
  destination-data-prefix-list EXCLUDE_SUBNET
action accept
set
  local-tloc-list
  color biz-internet lte
  encaps ipsec
sequence 11
match
  destination-port 67-68
  protocol 17
action accept
sequence 21
match
  source-port 67-68
  protocol 17
action accept
sequence 31
action accept
  nat use-vpn 0
  no nat fallback
default-action accept
from-vsmart lists vpn-list LAN
vpn 10
from-vsmart lists data-prefix-list EXCLUDE_SUBNET
ip-prefix 10.0.0.0/8
```

O rastreamento de pacotes debuga mostrará que uma imagem diferente para pacotes DHCP e elas punted a RP CPU para um processamento local mais adicional (estado: PONTAPÉ 60) como devem ser:

```
B2#show platform packet-trace summary
Pkt  Input          Output          State  Reason
<skipped>
88   V190            internal0/0/rp:0 PUNT   60  (IP subnet or broadcast pac
89   INJ.7           Gi0/1/0.MOD0    FWD
90   Gi0/1/0         internal0/0/rp:0 PUNT   60  (IP subnet or broadcast pac
91   INJ.7           Gi0/1/0.MOD0    FWD
92   Gi0/0/0         internal0/0/rp:0 PUNT   60  (IP subnet or broadcast pac
93   Gi0/1/1         Ce0/2/0         FWD
94   Gi0/0/0         internal0/0/rp:0 PUNT   60  (IP subnet or broadcast pac
95   V190            internal0/0/rp:0 PUNT   60  (IP subnet or broadcast pac
96   INJ.7           Gi0/1/0.MOD0    FWD
97   Gi0/1/1         internal0/0/rp:0 PUNT   60  (IP subnet or broadcast pac
98   INJ.7           Gi0/1/0.MOD0    FWD
```

B2# show platform packet-trace packet 88

Packet: 88 CBUG ID: 88

Summary

Input : Vlan90
Output : internal0/0/rp:0
State : PUNT 60 (IP subnet or broadcast pac

Timestamp

Start : 16485953871600 ns (12/17/2018 14:30:22.221086 UTC)
Stop : 16485953959680 ns (12/17/2018 14:30:22.221174 UTC)

Path Trace

Feature: IPV4(Input)

Input : Vlan90
Output : <unknown>
Source : 0.0.0.0
Destination : 255.255.255.255
Protocol : 17 (UDP)
SrcPort : 68
DstPort : 67

Feature: DEBUG_COND_INPUT_PKT

Entry : Input - 0x10e44b40
Input : Vlan90
Output : <unknown>
Lapsed time : 93 ns

Feature: IPV4_INPUT_DST_LOOKUP_CONSUME

Entry : Input - 0x10e5ca94
Input : Vlan90
Output : <unknown>
Lapsed time : 320 ns

Feature: IPV4_INPUT_FOR_US_MARTIAN

Entry : Input - 0x10e5cb24
Input : Vlan90
Output : <unknown>
Lapsed time : 8053 ns

Feature: IPV4_INPUT_FNF_FIRST_EXT

Entry : Input - 0x10e48968
Input : Vlan90
Output : <unknown>
Lapsed time : 533 ns

Feature: SDWAN Data Policy IN

VRF : 1
Seq : 1
DNS Flags : (0x0) NONE
Policy Flags : 0x0
Action : NONE

Feature: SDWAN_DATA_POLICY_IN_EXT

Entry : Input - 0x10eb9d7c
Input : Vlan90
Output : <unknown>
Lapsed time : 5626 ns

Feature: IPV4_INPUT_LOOKUP_PROCESS_EXT

Entry : Input - 0x10e5cc70
Input : Vlan90
Output : internal0/0/rp:0
Lapsed time : 1600 ns

Feature: IPV4_INPUT_FNF_FINAL_EXT

Entry : Input - 0x10e489c8
Input : Vlan90
Output : internal0/0/rp:0
Lapsed time : 386 ns

Feature: IPV4_INPUT_IPOPTIONS_PROCESS_EXT

Entry : Input - 0x10e5ce10
Input : Vlan90
Output : internal0/0/rp:0

Lapsed time : 186 ns
Feature: IPV4_INPUT_GOTO_OUTPUT_FEATURE_EXT
Entry : Input - 0x10e46278
Input : Vlan90
Output : internal0/0/rp:0
Lapsed time : 493 ns
Feature: CBUG_OUTPUT_FIA_EXT
Entry : Output - 0x10e44c00
Input : Vlan90
Output : internal0/0/rp:0
Lapsed time : 560 ns
Feature: IPV4_INTERNAL_ARL_SANITY_EXT
Entry : Output - 0x10e46128
Input : Vlan90
Output : internal0/0/rp:0
Lapsed time : 253 ns
Feature: IPV4_OUTPUT_THREAT_DEFENSE_EXT
Entry : Output - 0x10eb5cc4
Input : Vlan90
Output : internal0/0/rp:0
Lapsed time : 266 ns
Feature: IPV4_VFR_REFRAG_EXT
Entry : Output - 0x10e5cf10
Input : Vlan90
Output : internal0/0/rp:0
Lapsed time : 66 ns
Feature: IPV4_OUTPUT_DROP_POLICY_EXT
Entry : Output - 0x10e5e900
Input : Vlan90
Output : internal0/0/rp:0
Lapsed time : 2586 ns
Feature: DEBUG_COND_OUTPUT_PKT_EXT
Entry : Output - 0x10e44ba0
Input : Vlan90
Output : internal0/0/rp:0
Lapsed time : 133 ns
Feature: INTERNAL_TRANSMIT_PKT_EXT
Entry : Output - 0x10e45420
Input : Vlan90
Output : internal0/0/rp:0
Lapsed time : 5066 ns

IOSd Path Flow: Packet: 88 CBUG ID: 88

Feature: INFRA
Pkt Direction: IN
Packet Rcvd From DATAPLANE

Feature: IP
Pkt Direction: IN
Source : 0.0.0.0
Destination : 255.255.255.255

Feature: IP
Pkt Direction: IN
Packet Enqueued in IP layer
Source : 0.0.0.0
Destination : 255.255.255.255
Interface : Vlan90

Feature: UDP
Pkt Direction: IN
src : 0.0.0.0(68)
dst : 255.255.255.255(67)
length : 308

Este é comportamento esperado e os problemas similares puderam ser manchados com todo o outro tráfego que for pretendido para um processamento de CPU do route processor (RP) do dispositivo local (por exemplo sincronização do Network Time Protocol (NTP) se o roteador atua como uma fonte NTP) se a política centralizada dos dados não exclui o tipo do tráfego particular apropriadamente.

Nota: Para obter mais informações sobre do rastreamento de pacotes de Datapath, refira: <https://www.cisco.com/c/en/us/support/docs/content-networking/adaptive-session-redundancy-asr/117858-technote-asr-00.html>