Exemplo de configuração da vigilância de microfluxo do Catalyst 6500 Series Switch

Índice

Introdução

Este documento descreve a vigilância de microfluxo em Catalyst 6500 Series Switch.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em um Cisco Catalyst 6500 Series Switch que seja executado em um Supervisor Engine 720.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Está aqui um exemplo do uso para sua consideração. Há uma exigência da universidade limitar cada estudante a uma largura de banda de 10Mbps quando usarem o Internet. Se o policiamento do agregado é configurado, a seguir há uma distribuição desigual da largura de banda entre os estudantes. A vigilância de microfluxo pode melhor ajudar-nos a conseguir esta tarefa.

A vigilância de microfluxo ajuda usuários a policiar o tráfego baseado em fluxos. Um fluxo é definido geralmente por IP da fonte (SRC IP), por IP de destino (DST IP), por porta IP SRC-DST, SRC-DST, ou por SRC-relação. Aqui está um exemplo:

```
Source 10.0.0.1 sending a tcp stream to 15.0.0.1 with a source tcp port of 50
and destination 2000
Source 10.0.0.1 sending a tcp stream to 15.0.0.2 with a source tcp port of 60
and destination 2000.
```

Se a classificação é feita com base no SRC IP, a seguir o número de fluxos iguala um. Se a classificação é feita com base no DST IP, a seguir o número de fluxos iguala dois. Se a classificação é feita com base na porta DST, a seguir o número de fluxos iguala um.

> **Note**: As vigilâncias de microfluxo podem somente ser aplicadas na direção de ingresso, ao contrário do policer agregado.

Quando nós aplicarmos uma política de serviços sob uma relação, a interface física ou a interface virtual do interruptor (SVI), a política de serviços está programada no hardware. O Ternary Content Addressable Memory do Qualidade de Serviço (QoS) (TCAM) é usado a fim armazenar a entrada. Adicionalmente, desde que o interruptor deve recordar os fluxos, armazena a informação de fluxo individual no hardware. O Netflow TCAM é usado por esse motivo. Daqui, há dois lugares onde você pode verificar a programação no hardware: o Access Control List (ACL) TCAM e o Netflow TCAM.

Desde que o mesmo Netflow TCAM é usado por outros recursos, como o Network Address Translation (NAT), a exportação de dados de Netflow (NDE), e o Protocolo de Comunicação de Cache da Web (WCCP), é possível que há um conflito na vigilância de microfluxo que programa no hardware. Algumas encenações do conflito TCAM são fornecidas na extremidade deste documento.

Exemplos de configuração

Exemplo 1

Há um Cisco Catalyst 6500 Series Switch contratado no roteamento de interVLAN. As fontes de tráfego são ficadas situadas no **VLAN20**, e têm estes endereços IP de Um ou Mais Servidores Cisco ICM NT: 20.20.20.2 e 20.20.20.3. Ambos a tentativa das fontes para enviar o tráfego para o endereço IP 30.30.30.2, que é ficado situado no **VLAN 30**. O objetivo é atribuir 100Kbps da largura de banda a cada fonte.

1. Crie e trace um ACL em um mapa de classe a fim combinar o tráfego que vem destas duas

fontes.

```
ip access-list ext vlan20_30
permit ip 20.20.20.0 0.0.0.255 30.30.30.0 0.0.0.255


class-map POLICE_DIFF_SRC
match access-group name vlan20_30
```

2. Aplique o mapa de classe em um **mapa de política**. Configurar a taxa de informação comprometida (CIR) e os valores de intermitência como necessário.

```
policy-map POLICE_DIFF_SRC
class POLICE_DIFF_SRC
police flow mask src-only 100000 3000 conform transmit exceed drop
```

Estão aqui as opções que estão disponíveis depois que a **polícia flui máscara**:

```
police flow mask ?
dest-only
full-flow
src-only
```

3. Aplique a política de serviços sob o ingresso SVI ou sob a interface física do ingresso. Caso que você a aplica sob a relação VLAN, configurar os **qos dos mls VLAN-baseados** sob a interface física. Isto instrui o ® do Cisco IOS para procurar uma política sob a relação VLAN assim que um pacote alcançar uma interface de camada 2 em um VLAN específico.

```
interface vlan 20
service-policy input POLICE_DIFF_SRC
```

Exemplo 2

Há um Catalyst 6500 Series Switch contratado no switching de Camada 2 do tráfego no mesmo VLAN. Deomonstrates deste exemplo como restringir o tráfego que vem de 10.10.10.2 e vai para 10.10.10.3 no VLAN a 100Kbps da largura de banda. A fim ter o tráfego da camada 2-switched da influência do vigilante, você deve incorporar o comando **construído uma ponte sobre qos dos mls** sob a relação VLAN10.

```
ip access-list ext VLAN10
permit ip 10.10.10.0 0.0.0.255 10.10.10.0 0.0.0.255
class-map POLICE_SAME


match access-group name VLAN10
policy-map POLICE_SAME
class POLICE_SAME
police flow mask src-only 100000 3000 conform transmit exceed drop
```

```
int vlan 10
service-policy in POLICE_SAME
mls qos bridged
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

1. Incorpore o **comando ip dos qos dos mls da mostra**, e a verificação para **FL ID** ao lado do nome do vigilante. Se FL ID é 1, a seguir a política está no uso para a vigilância de microfluxo.

```
6500#show mls qos ip
 QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

 Int Mod Dir  Class-map DSCP  Ag  Trust   FL   AgForward-By   AgPoliced-By
                                                    Id            Id
------------------------------------------------------------------------------

Fa3/3  1 In   POLICE_SAM   0   0*   dscp    1   11266001160            0
```

   Estão aqui alguns pontos notáveis baseados nesta saída:

   A política é traçada no hardware.A relação em que é aplicada é **Fa3/3**.Se há um Distributed Forwarding Card (DFC) - line card (LC) permitido atual no chassi, a seguir o QoS policia é programado separadamente para cada DFC e Policy Feature Card (PFC). O número de módulo dá a entrada para o PFC/DFC no slot1.O Supervisor Engine 720 cria um agregado ID (AgID) para cada policer agregado que é criado. 1020 AgIDs são os ID úteis máximos, que são uma limitação do hardware. Isto não é relevante para a vigilância de microfluxo, mas é um comando útil para o policer agregado.O campo da confiança não guarda nenhuma importância neste caso.FL ID=1, como discutido previamente.O AgForward? Por e AgPoliced-por não são usados a fim calcular os pacotes que são transmitidos ou deixados cair pela vigilância de microfluxo (há um comando separado para aquele). Contudo, os mesmos contadores são usados a fim calcular os pacotes transmitidos/deixados cair por um policer agregado.

2. Incorpore o **tcam da mostra comando ip físico do type1 dos qos do interface> int < vlan/or** a fim determinar se o ACL é programado no QoS TCAM.

```
6500#show tcam interface fa3/3 qos type1 ip
   QOS Results:   A - Aggregate Policing       F - Microflow Policing
   M - Mark          T - Trust
   U - Untrust
   ------------------------------------------------------
    FT     ip 10.10.10.0 0.0.0.255 10.10.10.0 0.0.0.255  ==> entry is
```

```
programmed correctly
MU     ip any any
```

3. Verifique a saída do comando do **nowrap do IP QoS do Netflow dos mls da mostra** a fim descobrir se os fluxos são instalados no Netlflow TCAM.

```
6500#show mls NetFlow ip qos nowrap
Displaying NetFlow entries in Active Supervisor EARL in module 1
DstIP           SrcIP           Prot         : SrcPort :   DstPort   Src i/f
:AdjPtr    Pkts
Bytes         LastSeen      QoS       PoliceCount  Threshold   Leak          Drop
Bucket
-------------------------------------------------------------------------------------
-----------
0.0.0.0          0.0.0.0            0                     :0                   :0
--
0x0       140394
67383880   15:16:29        0x0                  0                    0           0
NO             0

0.0.0.0         10.10.10.2      0                     :0                   :0           --

0x0           227
108506        15:16:22        0x0                  35996208    0           0
NO         3386
```

Nesta saída, você pode ver que o fluxo (fonte-somente) está instalado no Netflow TCAM, e há **35,996,208** pacotes que foram policiados.

Possíveis problemas

Épossível que a política de serviços não está programada no hardware nestas encenações. Estão aqui algumas razões possíveis:

1. Há uma limitação do hardware no número de agregado/vigilâncias de microfluxo que pode ser configurado. A fim reservar recursos do hardware, a política de serviços não é programada no hardware.

   Incorpore o comando **qoscan da capacidade do hardware da plataforma da mostra** a fim verificar a Disponibilidade dos vigilantes.

```
6500#show platform hardware capacity qos
QoS Policer Resources
 Aggregate policers: Module                    Total         Used     %Used
                     1                          1024           102     10%
                     6                          1024           102     10%
 Microflow policer configurations: Module      Total         Used     %Used
                                   1              64           32        50%
                                   6              64           32        50%
```

2. Devido a um conflito da máscara do fluxo com os outros recursos configurados sob a mesma relação, a vigilância de microfluxo não pôde poder aos fluxos de cache no Netflow TCAM.

   É importante compreender o conceito da máscara do fluxo. A fim apoiar a aceleração de hardware de determinadas características, há as partes dedicadas do hardware (TCAM) que são usadas a fim instalar determinadas características. Há as características múltiplas que usam o mesmo TCAM, tal como o Netflow NAT WCCP. Usam um TCAM que seja chamado geralmente o Netflow TCAM, visto que para características como seguranças ACL, o Policy-Based Routing (PBR) usa o ACL TCAM.

   Para o Netflow TCAM, uma máscara do fluxo é precisada a fim instalar entradas no hardware. As máscaras do fluxo do Netflow determinam a granularidade dos fluxos a ser medidos. As máscaras muito específicas do fluxo gerenciem um grande número entradas de tabela do Netflow, e um de grande volume das estatísticas para exportar. O fluxo menos específico mascara o agregado as estatísticas de tráfego em menos entradas de tabela do Netflow, e gerencie um volume mais baixo de estatísticas.

   O artigo da configuração da tabela do Netflow descreve as características da exigência da máscara do fluxo (apoiada).

   Inscreva o **comando show fm summary**, e determine se a relação está em um estado **inativo**. Um estado inativo indica que há alguma característica configurada sob a relação que não pode ser programada no hardware. Pacotes recebidos nessa relação que exigem que a característica está programada no software.

```
6500#show fm summary
Interface: Vlan13 is up
TCAM screening for features: INACTIVE inbound
TCAM screening for features: INACTIVE outbound
Interface: Vlan72 is up
TCAM screening for features: ACTIVE inbound
TCAM screening for features: ACTIVE outbound
Interface: Vlan84 is up
TCAM screening for features: ACTIVE inbound
TCAM screening for features: INACTIVE outbound
```

   Incorpore o comando do **<> da relação do fie do fm da mostra**, e determine se a vigilância de microfluxo é configurada no hardware.

```
6500#show fm fie int vlan 10
Interface Vl10:
Feature interaction state created: Yes
 Flowmask conflict status for protocol IP :
FIE_FLOWMASK_STATUS_SUCCESS
Flowmask conflict status for protocol OTHER :
FIE_FLOWMASK_STATUS_SUCCESS Interface Vl10 [Ingress]:
 Slot(s) using the protocol IP : 1
 FIE Result for protocol IP : FIE_SUCCESS_NO_CONFLICT
Features Configured : [empty] - Protocol : IP
```

```
FM Label when FIE was invoked : 66  Current FM Label : 66
Last Merge is for slot: 0  num# of strategies tried : 1
 num# of merged VMRs in bank 1 = 0
 num# of free TCAM entries in Bank1 = Unknown
 num# of merged VMRs in bank 2 = 1
 num# of free TCAM entries in Bank2 = Unknown
 Slot(s) using the protocol OTHER : 1
 FIE Result for protocol OTHER : FIE_SUCCESS_NO_CONFLICT
 Features Configured : OTH_DEF   - Protocol : OTHER
 FM Label when FIE was invoked : 66
 Current FM Label : 66
 Last Merge is for slot: 0
 Features in Bank1 = OTH_DEF
+-------------------------------------+
       Action Merge Table
+-------------------------------------+
  OTH_DEF      RSLT    R_RSLT  COL
+-------------------------------------+
  SB           HB      P       0
   X            P       P       0
+-------------------------------------+
 num# of strategies tried : 1
 Description of merging strategy used:
 Serialized Banks: FALSE
 Bank1 Only Features: [empty]
 Bank2 Only Features: [empty]
 Banks Swappable: TRUE
 Merge Algorithm: ODM
 num# of merged VMRs in bank 1 = 1
 num# of free TCAM entries in Bank1 = 32745
 num# of merged VMRs in bank 2 = 0
 num# of free TCAM entries in Bank2 = 32744 Interface Vl10 [Egress]:
No Features Configured
No IP Guardian Feature Configured
No IPv6 Guardian Feature Configured
IP QoS Conflict resolution configured, QoS policy name: POLICE_SAME
```

As máscaras compatíveis do fluxo devem ser usadas para as características configuradas sob a mesma relação que compartilham do Netflow TCAM. As máscaras compatíveis do fluxo estão disponíveis para quase todos os tipos de combinações.

Outros comandos úteis

- Aplique a política
- A verificação FL-ID=1 - **mostre os qos IP dos mls**
- Verifique QoS TCAM - **mostre o tipo-1 IP dos qos do <> int do tcam**
- Verifique o Netflow TCAM - **mostre o nowrap do módulo do IP QoS do Netflow dos mls**
- Verifique para ver se há a Disponibilidade dos vigilantes - **mostre a tela da capacidade do hardware da plataforma**
- Verifique para ver se há o **log de mostra do** conflito da máscara do fluxo (FM), **mostre o sumário do fm**
- Verifique para ver se há as características configuradas sob a relação - **mostre a relação do fie do fm**