Verifique as violações de políticas do plano de controle nas plataformas Nexus

Contents

Introdução

Este documento descreve detalhes sobre Políticas de plano de controle (CoPP) em switches Cisco Nexus e seu impacto relevante em violações de classe não padrão.

Pré-requisitos

A Cisco recomenda que você compreenda as informações básicas com relação à Política de Plano de Controle (CoPP), suas diretrizes e limitações, e a configuração geral, bem como a funcionalidade de política de Qualidade de Serviço (QoS) (CIR). Para obter mais informações sobre esse recurso, consulte os documentos aplicáveis:

- Guia de configuração de segurança do Cisco Nexus 9000 Series NX-OS, versão 10.2(x)
- CoPP nos switches Nexus 7000 Series
- Guia de configuração da qualidade de serviço do NX-OS para Cisco Nexus 9000 Series, versão 10.2(x)

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a requisitos específicos de software e hardware.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O tráfego do plano de controle é redirecionado para o módulo supervisor pelas listas de controle de acesso (ACLs) de redirecionamento programadas para direcionar o tráfego correspondente que passa por duas camadas de proteção, os limitadores de taxa de hardware e o CoPP. Quaisquer interrupções ou ataques ao módulo supervisor, se deixados desmarcados, podem resultar em sérias interrupções da rede; portanto, o CoPP está lá para servir como um mecanismo de proteção. Se houver instabilidade no nível do plano de controle, é importante verificar o CoPP, pois padrões de tráfego anormais criados a partir de loops ou inundações, ou dispositivos invasores podem taxar e impedir que o supervisor processe o tráfego legítimo. Esses ataques, que podem ser perpetrados inadvertidamente por dispositivos invasores ou maliciosamente por invasores, geralmente envolvem altas taxas de tráfego destinadas ao módulo supervisor ou à CPU.

O CoPP (Control Plan Policing, Política de plano de controle) é um recurso que classifica e policia todos os pacotes recebidos nas portas in-band (painel frontal) destinadas ao endereço do roteador ou que exigem qualquer envolvimento do supervisor. Esse recurso permite que um mapa de política seja aplicado ao plano de controle. Esse mapa de política se parece com uma política de Qualidade de Serviço (QoS - Quality of Service) normal e é aplicado a todo o tráfego que entra no switch a partir de uma porta que não seja de gerenciamento. A proteção do módulo supervisor por policiamento permite que o switch minimize inundações de tráfego que vão além da taxa de entrada comprometida (CIR) para cada classe pelo descarte de pacotes para evitar que o switch seja sobrecarregado e, portanto, um impacto no desempenho.

É importante monitorar continuamente os contadores CoPP e justificá-los, que é a finalidade deste documento. As violações de CoPP, se deixadas desmarcadas, podem impedir que o plano de controle do processo de tráfego genuíno na classe afetada associada. A configuração de CoPP é um processo fluido e contínuo que deve responder aos requisitos de rede e infraestrutura. Há três políticas de sistema padrão para CoPP. Por padrão, a Cisco recomenda o uso da política padrão strict como ponto inicial e é usada como base para este documento.

O CoPP aplica-se somente ao tráfego em banda recebido através das portas do painel frontal. A porta de gerenciamento out-of-band (mgmt0) não está sujeita a CoPP. O hardware do dispositivo Cisco NX-OS executa o CoPP por mecanismo de encaminhamento. Portanto, escolha taxas para que o tráfego agregado não sobrecarregue o módulo supervisor. Isso é especialmente importante para switches modulares/de fim de linha,

pois a CIR se aplica ao tráfego agregado de todos os módulos de tráfego vinculado à CPU.

Hardware aplicável

O componente abordado neste documento é aplicável a todos os switches de data center Cisco Nexus.

Interpretação do policiamento do plano de controle

O foco deste documento é abordar as violações de classe não padrão mais comuns e críticas vistas nos switches Nexus.

Perfil Padrão CoPP Padrão

Para entender como interpretar CoPP, a primeira verificação deve ser para garantir que um perfil seja aplicado e para entender se um perfil padrão ou personalizado é aplicado no switch.

Observação: como prática recomendada, todos os switches Nexus devem ter o CoPP habilitado. Se esse recurso não estiver habilitado, ele poderá causar instabilidade para todo o tráfego do plano de controle, pois plataformas diferentes podem restringir o tráfego vinculado ao Supervisor (SUP). Por exemplo, se o CoPP não estiver habilitado em um Nexus 9000, o tráfego destinado ao SUP será limitado a uma taxa de 50 pps, portanto, o switch se tornará quase inoperante. O CoPP é considerado um requisito nas plataformas Nexus 3000 e Nexus 9000.

Se o CoPP não estiver habilitado, ele poderá ser reabilitado ou configurado no switch pelo uso do **setup** comando ou pela aplicação de uma das políticas padrão sob a opção de configuração: copp profile [dense|lenient|moderate|strict].

Um dispositivo não protegido não classifica e separa adequadamente o tráfego em classes e, portanto, qualquer comportamento de negação de serviço para um recurso ou protocolo específico não está confinado a esse escopo e pode afetar todo o plano de controle.

Observação: as políticas de CoPP são implementadas por redirecionamentos de classificação TCAM (Ternary Content-Addressable Memory) e podem ser vistas diretamente sob **show system internal access-list input statistics module X | b CoPP** ou **show hardware access-list input entries detail**.

N9K1# show copp status Last Config Operation: None Last Config Operation Timestamp: None Last Config Operation Status: None Policy-map attached t

Classes de Vigilância do Plano de Controle

O CoPP classifica o tráfego com base nas correspondências que correspondem às ACLs IP ou MAC. Assim, é importante entender qual tráfego é classificado em qual classe.

As classes, que dependem da plataforma, podem variar. Portanto, é importante entender como verificar as aulas.

Por exemplo, no topo de rack (TOR) do Nexus 9000:

```
N9K1# show policy-map interface control-plane
Control Plane

Service-policy input: copp-system-p-policy-strict
...
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
...
```

Neste exemplo, o mapa de classes copp-system-p-class-critical abrange o tráfego relacionado aos protocolos de roteamento, como Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Router Protocol (EIGRP) e inclui outros protocolos, como o vPC.

A convenção de nomes das ACLs IP ou MAC é basicamente autoexplicativa para o protocolo ou recurso envolvido, com o prefixo copp-system-p-acl-[protocol|feature].

Para visualizar uma classe específica, ela pode ser especificada diretamente enquanto o comando **show** é executado. Por exemplo:

```
N9K-4# show policy-map interface control-plane class copp-system-p-class-management
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
```

match access-group name copp-system-p-acl-ssh
match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
set cos 2
police cir 36000 kbps , bc 512000 bytes
module 1 :
transmitted 0 bytes;
5-minute offered rate 0 bytes/sec
conformed 0 peak-rate bytes/sec

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec

Embora os perfis padrão de CoPP estejam normalmente ocultos como parte da configuração padrão, você pode ver a configuração com **show running-conf copp all**:

<#root>

N9K1# show running-config copp all

!Command: show running-config copp all
!Running configuration last done at: Tue Apr 26 16:34:10 2022
!Time: Sun May 1 16:41:55 2022

version 10.2(1) Bios:version 05.45
control-plane
scale-factor 1.00 module 1
class-map type control-plane match-any copp-system-p-class-critical
match access-group name

copp-system-p-acl-bgp

match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6

```
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
(snip)
...
```

O mapa de classes copp-system-p-class-critical, visto anteriormente, faz referência a várias instruções de correspondência que chamam as ACLs do sistema, que por padrão estão ocultas, e faz referência à classificação sobre a qual é feita a correspondência. Por exemplo, para BGP:

<#root>

N9K1# show running-config aclmgr all | b

copp-system-p-acl-bgp

```
ip access-list
```

copp-system-p-acl-bgp

```
10 permit tcp any gt 1023 any eq bgp
20 permit tcp any eq bgp any gt 1023
(snip)
```

Isso significa que qualquer tráfego BGP corresponde a essa classe e é classificado como copp-system-p-class-critical, juntamente com todos os outros protocolos nessa mesma classe.

O Nexus 7000 usa uma estrutura de recursos de CoPP muito semelhante à do Nexus 9000:

N77-A-Admin# show policy-map interface control-plane
Control Plane
service-policy input copp-system-p-policy-strict

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt

```
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert
set cos 7
police cir 36000 kbps bc 250 ms
conform action: transmit
violate action: drop
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
conformed 4516900216 bytes,
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
```

É importante observar que em um Nexus 7000, como esses são switches modulares, você vê a classe dividida por módulo; no entanto, a CIR se aplica ao agregado de todos os módulos e o CoPP se aplica a todo o chassi. A verificação e as saídas de CoPP podem ser vistas apenas do Contexto de Dispositivo Virtual (VDC) padrão ou do administrador.

É especialmente importante verificar CoPP em um Nexus 7000 se problemas de plano de controle forem vistos, pois a instabilidade em um VDC com excesso de tráfego vinculado à CPU que causa violações de CoPP pode afetar a estabilidade de outros VDCs.

Em um Nexus 5600, as classes variam. Assim, para o BGP é sua própria classe separada:

```
N5K# show policy-map interface control-plane
Control Plane
(snip)
class-map copp-system-class-bgp (match-any)
match protocol bgp
police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;
(snip)
```

Em um Nexus 3100, há 3 classes de protocolo de roteamento, portanto, para verificar a qual classe o BGP pertence, faça referência cruzada da 4 ACL CoPP referenciada:

O EIGRP é manipulado por sua própria classe no Nexus 3100.

<#root>

N3K-C3172# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy

class-map copp-s-routingProto2 (match-any)
match access-group name copp-system-acl-routingproto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-v6routingProto2 (match-any)
match access-group name copp-system-acl-v6routingProto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-eigrp (match-any)
match access-group name copp-system-acl-eigrp
match access-group name copp-system-acl-eigrp6
police pps 200
OutPackets 0
DropPackets 0
class-map copp-s-routingProto1 (match-any)
match access-group name

copp-system-acl-routingproto1

match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 0
DropPackets 0

N3K-C3172# show running-config aclmgr

!Command: show running-config aclmgr
!No configuration change since last restart
!Time: Sun May 1 18:14:16 2022

version 9.3(9) Bios:version 5.3.1
ip access-list copp-system-acl-eigrp
10 permit eigrp any 224.0.0.10/32
ipv6 access-list copp-system-acl-eigrp6
10 permit eigrp any ff02::a/128
ip access-list

copp-system-acl-routingproto1

10 permit tcp any gt 1024 any eq bgp

```
20 permit tcp any eq bgp any gt 1024


30 permit udp any 224.0.0.0/24 eq rip
40 permit tcp any gt 1024 any eq 639
50 permit tcp any eq 639 any gt 1024
70 permit ospf any any
80 permit ospf any 224.0.0.5/32
90 permit ospf any 224.0.0.6/32
ip access-list copp-system-acl-routingproto2
10 permit udp any 224.0.0.0/24 eq 1985
20 permit 112 any 224.0.0.0/24
ipv6 access-list copp-system-acl-v6routingProto2
10 permit udp any ff02::66/128 eq 2029
20 permit udp any ff02::fb/128 eq 5353
30 permit 112 any ff02::12/128
ipv6 access-list copp-system-acl-v6routingproto1
10 permit 89 any ff02::5/128
20 permit 89 any ff02::6/128
30 permit udp any ff02::9/128 eq 521
```

Nesse caso, o BGP é correspondido pela ACL copp-system-acl-routingproto1, e assim a classe de CoPP em que o BGP se encaixa é copp-s-routingProto1.

Estatísticas e Contadores de Política de Plano de Controle

O CoPP suporta estatísticas de QoS para rastrear os contadores agregados de tráfego que confirmam ou violam a taxa de entrada comprometida (CIR) para uma classe específica, para cada módulo.

Cada mapa de classe classifica o tráfego vinculado à CPU, com base na classe à qual ele corresponde e anexa uma CIR para todos os pacotes que se enquadram nessa classificação. Como exemplo, a classe relacionada ao tráfego BGP é usada como referência:

Em um topo de rack (TOR) Nexus 9000 para copp-system-p-class-critical:

<#root>

class-map copp-system-p-class-critical (match-any)
match access-group name

copp-system-p-acl-bgp

```
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
```

```
police cir 36000 kbps , bc 1280000 bytes
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
```

Na seção do mapa de classes, após as instruções de correspondência, você vê as ações que se relacionam a todo o tráfego dentro da classe. Todo o tráfego classificado no copp-system-p-class-critical é definido com uma Classe de Serviço (CoS) de 7, que é o tráfego de prioridade mais alta, e essa classe é vigiada com uma CIR de 36000 kbps e uma taxa de burst comprometido de 1280000 bytes.

O tráfego em conformidade com essa política é encaminhado ao SUP para ser processado e todas as violações são descartadas.

<#root>

set cos 7

police cir 36000 kbps , bc 1280000 bytes

A próxima seção contém as estatísticas relacionadas ao módulo, para switches de topo de rack (TOR), com um único módulo, o módulo 1 refere-se ao switch.

module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec

As estatísticas vistas na saída são históricas, portanto isso fornece um instantâneo das estatísticas atuais no momento em que o comando é executado.

Há duas seções para interpretar aqui: as seções transmitidas e soltas:
O ponto de dados transmitido rastreia todos os pacotes transmitidos que estão em conformidade com a política. Esta seção é importante, pois fornece informações sobre o tipo de tráfego que o supervisor processa.

O valor da taxa oferecida de 5 minutos fornece informações sobre a taxa atual.
A taxa e a data de pico em conformidade fornecem um instantâneo da taxa de pico mais alta por segundos que ainda está em conformidade com a política e a hora em que ela ocorreu.
Se um novo pico for visto, ele substituirá esse valor e data.

A parte mais importante das estatísticas é o ponto de dados descartado. Assim como as estatísticas transmitidas, a seção eliminada rastreia os bytes cumulativos eliminados devido a violações à taxa de polícia. Ele também fornece a taxa de violação para os últimos 5 minutos, o pico violado e, se houver um pico, o carimbo de data/hora dessa violação de pico. E novamente, se um novo pico é visto, então ele substitui esse valor e data. Em outras plataformas, os resultados variam, mas a lógica é muito semelhante.

O Nexus 7000 usa uma estrutura idêntica e a verificação é a mesma, embora algumas classes variem um pouco nas ACLs referenciadas:

<#root>

class-map

copp-system-p-class-critical

 (match-any)
match access-group name

copp-system-p-acl-bgp

match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert

set cos 7

police cir 36000 kbps bc 250 ms

conform action: transmit

violate action: drop
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
conformed 4516900216 bytes,

```
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
```

Em um Nexus 5600:

<#root>

class-map copp-system-class-bgp

(match-any)

match protocol bgp

police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;

Embora não forneça informações sobre taxa ou picos, ele ainda fornece os bytes agregados em conformidade e violados.

Em um Nexus 3100, a saída do plano de controle mostra OutPackets e DropPackets.

class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1
match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 8732060
DropPackets 0

OutPackets se referem a pacotes em conformidade, enquanto DropPackets se referem a violações à CIR. Neste cenário, você não vê descartes na classe associada.

Em um Nexus 3500, a saída mostra pacotes correspondentes de HW e SW:

class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1

police pps 900
HW Matched Packets 471425
SW Matched Packets 471425

Os Pacotes HW correspondentes referem-se aos pacotes que são correspondidos em HW pela ACL. Os pacotes correspondentes de SW são os que estão em conformidade com a política. Quaisquer diferenças entre os pacotes correspondentes de HW e SW implicam uma violação.

Nesse caso, não há descartes vistos nos pacotes de classe do protocolo de roteamento 1 (que inclui o BGP), pois os valores correspondem.

Verificar se há violações ativas de queda

Como as estatísticas de vigilância do plano de controle são históricas, é importante determinar se as violações ativas estão aumentando. A forma padrão de executar essa tarefa é comparar duas saídas completas e verificar quaisquer diferenças.

Essa tarefa pode ser executada manualmente ou os switches Nexus fornecem a ferramenta de comparação que pode ajudar a comparar as saídas.

Embora a saída inteira possa ser comparada, ela não é necessária porque o foco está apenas nas estatísticas descartadas. Assim, a saída de CoPP pode ser filtrada para se concentrar apenas nas violações.

O comando é: show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y

---

 **Observação**: o comando deve ser executado duas vezes para que o diff possa comparar a saída atual com a anterior.

```
N9K-3# show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y
    class-map copp-system-p-class-l3uc-data (match-any)            class-map copp-system-p-class-l3uc-data (match-any)
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
        violated 0 peak-rate byte/sec                                  violated 0 peak-rate byte/sec
    class-map copp-system-p-class-critical (match-any)             class-map copp-system-p-class-critical (match-any)
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
        violated 0 peak-rate byte/sec                                  violated 0 peak-rate byte/sec
    class-map copp-system-p-class-important (match-any)            class-map copp-system-p-class-important (match-any)
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
        violated 0 peak-rate byte/sec                                  violated 0 peak-rate byte/sec
    class-map copp-system-p-class-openflow (match-any)             class-map copp-system-p-class-openflow (match-any)
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
        violated 0 peak-rate byte/sec                                  violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-router (match-any      class-map copp-system-p-class-multicast-router (match-any
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
        violated 0 peak-rate byte/sec                                  violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-host (match-any)       class-map copp-system-p-class-multicast-host (match-any)
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
        violated 0 peak-rate byte/sec                                  violated 0 peak-rate byte/sec
    class-map copp-system-p-class-l3mc-data (match-any)            class-map copp-system-p-class-l3mc-data (match-any)
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
        violated 0 peak-rate byte/sec                                  violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal (match-any)               class-map copp-system-p-class-normal (match-any)
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
        violated 0 peak-rate byte/sec                                  violated 0 peak-rate byte/sec
    class-map copp-system-p-class-ndp (match-any)                  class-map copp-system-p-class-ndp (match-any)
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
        violated 0 peak-rate byte/sec                                  violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp (match-any)          class-map copp-system-p-class-normal-dhcp (match-any)
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
        violated 0 peak-rate byte/sec                                  violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp-relay-response       class-map copp-system-p-class-normal-dhcp-relay-response
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
        violated 0 peak-rate byte/sec                                  violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-igmp (match-any)          class-map copp-system-p-class-normal-igmp (match-any)
      module 1 :                                                     module 1 :
        dropped 0 bytes;                                               dropped 0 bytes;
```

O comando anterior permite que você veja o delta entre duas classes e encontre aumentos de violação.

Observação: como as estatísticas de CoPP são históricas, outra recomendação é limpar as estatísticas após a execução do comando, para verificar se há aumentos ativos. Para limpar as estatísticas de CoPP, execute o comando: **clear copp statistics**.

Tipos de quedas CoPP

CoPP é uma estrutura de vigilância simples, pois qualquer tráfego vinculado à CPU que viole a CIR é descartado. As implicações, no entanto, variam significativamente dependendo do tipo de quedas.

Embora a lógica seja a mesma, não é o mesmo descartar o tráfego destinado a copp-system-p-class-critical.

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes

Comparado ao tráfego descartado destinado ao mapa de classe copp-system-p-class-monitoring.

```
class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
```

O primeiro trata principalmente de protocolos de roteamento, o segundo trata do Internet Control Message Protocol (ICMP), que tem uma das prioridades mais baixas e a CIR. A diferença na CIR é cem vezes maior. Portanto, é importante entender as classes, os impactos, as verificações comuns e as recomendações.

Classes CoPP

Monitoramento de classe - copp-system-p-class-monitoring

Essa classe engloba o ICMP para IPv4 e IPv6 e o traceroute do tráfego direcionado ao switch em questão.

```
class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
```

Impacto

Uma concepção equivocada comum quando a perda de pacotes ou a latência são solucionadas por problemas é fazer ping no switch através de suas portas in-band, que são limitadas por taxa pelo CoPP. Como o CoPP policia fortemente o ICMP, mesmo com baixo tráfego ou congestionamento, a perda de pacotes pode ser vista por um ping para interfaces in-band diretamente se elas violarem a CIR.

Por exemplo, através de um ping para interfaces diretamente conectadas em portas roteadas, com um payload de pacote de 500, as quedas podem ser vistas periodicamente.

<#root>

```
N9K-3# ping 192.168.1.1 count 1000 packet-size 500
...
--- 192.168.1.1 ping statistics ---
1000 packets transmitted, 995 packets received,
```

`0.50% packet loss`

```
round-trip min/avg/max = 0.597/0.693/2.056 ms
```

No Nexus, para onde os pacotes ICMP foram destinados, você verá que o CoPP os descartou quando a violação foi detectada e a CPU foi protegida:

<#root>

N9K-4# show policy-map interface control-plane class copp-system-p-class-monitoring
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
module 1 :
transmitted 750902 bytes;
5-minute offered rate 13606 bytes/sec
conformed 13606 peak-rate bytes/sec
at Sun May 01 22:49:24 2022

dropped 2950 bytes;

5-min violate rate 53 byte/sec

violated 53 peak-rate byte/sec at Sun May 01 22:49:24 2022

Para solucionar problemas de latência ou perda de pacotes, é recomendável usar hosts alcançáveis através do switch pelo plano de dados, não destinados ao switch em si, que seria o tráfego do plano de controle. O tráfego do plano de dados é encaminhado/roteado no nível do hardware sem intervenção do SUP e, portanto, não é policiado pelo CoPP, e geralmente não sofre quedas.

Recomendações

- Envie um ping através do switch através do plano de dados, não para o switch, para verificar resultados falsos positivos para perda de pacotes.
- Limitar o Network Monitoring System (NMS) ou ferramentas que usam o switch de forma agressiva para evitar um burst na taxa de entrada comprometida para a classe. Lembre-se de que o CoPP se aplica a todo o tráfego agregado que se enquadra na classe.

Gerenciamento de Classe - copp-system-p-class-management

Como visto aqui, essa classe abrange diferentes protocolos de gerenciamento que podem ser usados para comunicação (SSH, Telnet),

transferências (SCP, FTP, HTTP, SFTP, TFTP), relógio (NTP), AAA (Radius/TACACS) e monitoramento (SNMP), para comunicações IPv4 e IPv6.

class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
match access-group name copp-system-p-acl-ssh
match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
set cos 2
police cir 36000 kbps , bc 512000 bytes

Impacto

Os comportamentos ou descartes mais comuns associados a esta classe incluem:

- Lentidão do CLI percebida quando conectado por SSH/Telnet. Se houver quedas ativas na classe, as sessões de comunicação poderão ser lentas e sofrer quedas.
- Transfira arquivos com protocolos FTP, SCP, SFTP, TFTP no switch. O comportamento mais comum observado é uma tentativa de transferir imagens de inicialização do sistema/kickstart por portas de gerenciamento em banda. Isso pode levar a tempos de transferência mais altos e sessões de transmissão fechadas/terminadas, determinados pela largura de banda agregada para a classe.
- Problemas de sincronização de NTP, essa classe também é importante porque atenua agentes ou ataques de NTP invasores.
- Os serviços AAA Radius e TACACS também se enquadram nessa classe. Se o impacto for percebido nessa classe, ele pode afetar os serviços de autorização e autenticação no switch para contas de usuário, o que também pode contribuir para o atraso nos comandos CLI.
- O SNMP também é policiado nessa classe. O comportamento mais comum observado devido a quedas devido à classe SNMP está nos servidores NMS, que realizam caminhadas, coletas em massa ou verificações de rede. Quando ocorre instabilidade periódica, geralmente ela é correlacionada ao cronograma de coleta do NMS.

Recomendações

- Se a lentidão do CLI for percebida, junto com quedas nessa classe, use o acesso de console ou o acesso fora de banda de

gerenciamento (mgmt0).

- Se as imagens do sistema precisarem ser carregadas no switch, use a porta de gerenciamento fora de banda (mgmt0) ou as portas USB para a transferência mais rápida.

- Se os pacotes NTP forem perdidos, verifique o show ntp peer-status e verifique a coluna de acessibilidade, nenhum descarte será convertido em 377.

- Se forem observados problemas com os serviços AAA, use usuários somente locais para fazer a identificação e solução de problemas, até que o comportamento seja mitigado.

- A mitigação de problemas de SNMP inclui comportamento menos agressivo, coleta direcionada ou minimização de verificadores de rede. Examine os tempos periódicos dos scanners aos eventos vistos no nível da CPU.

Dados unicast de classe L3 - copp-system-p-class-l3uc-data

Essa classe lida especificamente com pacotes de glean. Esse tipo de pacote também é tratado pelo HWRL (Hardware Rate Limiter, Limitador de taxa de hardware).

Se a solicitação ARP (Address Resolution Protocol Protocolo de Resolução de Endereços) para o próximo salto não for resolvida quando os pacotes IP de entrada forem encaminhados em uma placa de linha, a placa de linha encaminhará os pacotes para o módulo supervisor.

O supervisor resolve o endereço MAC para o próximo salto e programa o hardware.

```
class-map copp-system-p-class-l3uc-data (match-any)
match exception glean
set cos 1
```

Isso normalmente ocorre quando são usadas rotas estáticas e o próximo salto é inalcançável ou não resolvido.

Quando uma solicitação ARP é enviada, o software adiciona uma adjacência de queda /32 no hardware para evitar que os pacotes para o mesmo endereço IP do próximo salto sejam encaminhados ao supervisor. Quando o ARP é resolvido, a entrada de hardware é atualizada com o endereço MAC correto. Se a entrada ARP não for resolvida antes de um período de timeout, a entrada será removida do hardware.

Observação: o CoPP e o HWRL trabalham em conjunto para garantir que a CPU esteja protegida. Embora pareça executar funções semelhantes, o HWRL ocorre primeiro. A implementação é baseada no local em que o recurso específico é implementado nos mecanismos de encaminhamento no ASIC. Essa abordagem serial permite proteções de granularidade e multicamada que classificam todos os pacotes vinculados à CPU.

O HWRL é executado por instância/mecanismo de encaminhamento no módulo e pode ser visualizado com o comando **show hardware rate-limiter**. O HWRL está fora do escopo deste documento técnico.

<#root>

show hardware rate-limiter

Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated bytes since last clear counters

Module: 1
R-L Class Config Allowed Dropped Total
+---------------+----------+--------------------+--------------------+--------------------+

L3 glean 100 0 0 0

L3 mcast loc-grp 3000 0 0 0
access-list-log 100 0 0 0
bfd 10000 0 0 0
fex 12000 0 0 0
span 50 0 0 0
sflow 40000 0 0 0
vxlan-oam 1000 0 0 0
100M-ethports 10000 0 0 0
span-egress disabled 0 0 0
dot1x 3000 0 0 0
mpls-oam 300 0 0 0
netflow 120000 0 0 0
ucs-mgmt 12000 0 0 0

Impacto

- O tráfego do plano de dados é apontado para o supervisor como uma violação, pois não pode ser processado no hardware e, portanto, cria pressão na CPU.

Recomendações

- A resolução comum para essa questão, para minimizar as quedas de glean, é garantir que o próximo salto seja alcançável e habilitar a aceleração de glean pelo comando de configuração: **hardware ip glean throttle**.

No Nexus 7000 8.4(2), ele também introduziu suporte de filtro de bloom para adjacências glean para módulos M3 e F4. Consulte: Guia de configuração de roteamento unicast do NX-OS do Cisco Nexus 7000 Series

Reveja todas as configurações de rotas estáticas que usam endereços de próximo salto inalcançáveis ou use protocolos de roteamento dinâmico que removeriam dinamicamente essas rotas da RIB.

Classe crítica - class-map copp-system-p-class-critical

Essa classe faz referência aos protocolos de plano de controle mais críticos de uma perspectiva de L3, que incluem protocolos de roteamento para IPv4 e IPv6, (RIP, OSPF, EIGRP, BGP), autorrP, canal de porta virtual (vPC) e l2pt e IS-IS.

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes

Impacto

Quedas na instabilidade de copp-system-p-class-critical transferência para protocolos de roteamento, que podem incluir adjacências perdidas ou falhas de convergência, ou propagação de atualização/NLRI.
Os descartes de política mais comuns nessa classe podem estar relacionados a dispositivos invasores na rede que atuam de forma anormal (devido a erro de configuração ou falha) ou escalabilidade.

Recomendações

- Se não forem detectadas anomalias, como um dispositivo invasor ou instabilidade de L2 que provoque uma reconvergência contínua dos protocolos de camada superior, uma configuração personalizada de CoPP ou uma classe mais tolerante poderá ser necessária para acomodar a escala.

- Consulte o guia de configuração de CoPP para saber como configurar um perfil de CoPP personalizado a partir de um perfil padrão que existe atualmente.
Copiando a política de práticas recomendadas de CoPP

Classe importante - copp-system-p-class-important

Essa classe está relacionada aos protocolos de redundância do primeiro salto (FHRP), que incluem HSRP, VRRP e também LLDP

class-map copp-system-p-class-important (match-any)
match access-group name copp-system-p-acl-hsrp
match access-group name copp-system-p-acl-vrrp
match access-group name copp-system-p-acl-hsrp6
match access-group name copp-system-p-acl-vrrp6
match access-group name copp-system-p-acl-mac-lldp
set cos 6
police cir 2500 kbps , bc 1280000 bytes

Impacto

O comportamento mais comum visto aqui que leva a quedas são os problemas de instabilidade da camada 2, que levam a dispositivos que passam para cenários de estado ativo (cérebro dividido), temporizadores agressivos, configurações incorretas ou escalabilidade.

Recomendações:

- Certifique-se de que, para o FHRP, os grupos estejam configurados corretamente e que as funções estejam ativa/em espera ou primária/secundária, sejam negociadas adequadamente e não haja oscilações no estado.
- Verifique se há problemas de convergência em L2 ou problemas com propagação multicast para o domínio L2.

Class L2 Unpoliced - copp-system-p-class-l2-unpoliced

A classe não policiada L2 se refere a todos os protocolos críticos da camada 2 que são a base para todos os protocolos da camada superior e, portanto, são considerados quase não policiados com a maior CIR e prioridade.

Efetivamente, essa classe lida com STP (Spanning-Tree Protocol), LACP (Link Aggregation Control Protocol), Cisco Fabric Service over Ethernet (CFSoE)

```
class-map copp-system-p-class-l2-unpoliced (match-any)
match access-group name copp-system-p-acl-mac-stp
match access-group name copp-system-p-acl-mac-lacp
match access-group name copp-system-p-acl-mac-cfsoe
match access-group name copp-system-p-acl-mac-sdp-srp
match access-group name copp-system-p-acl-mac-l2-tunnel
match access-group name copp-system-p-acl-mac-cdp-udld-vtp
set cos 7
police cir 50 mbps , bc 8192000 bytes
```

Essa classe tem uma CIR de polícia de 50 Mbps, a mais alta entre todas as classes, juntamente com a absorção de taxa de intermitência mais alta.

Impacto

Quedas nessa classe podem levar à instabilidade global, já que todos os protocolos e comunicações de camada superior em planos de dados, controle e gerenciamento dependem de uma estabilidade subjacente de Camada 2.

Problemas com violações de STP podem causar TCNs e problemas de convergência de STP, que incluem contestações de STP, liberações de MAC, movimentações e comportamentos de aprendizagem desabilitados, que causam problemas de acessibilidade e podem causar loops de tráfego que desestabilizam a rede.

Essa classe também faz referência ao LACP e, portanto, manipula todos os pacotes EtherType associados a 0x8809, que incluem todos os LACPDUs usados para manter o estado das ligações de canal de porta. A instabilidade nessa classe pode fazer com que os canais de porta atinjam o tempo limite se os LACPDUs forem descartados.

O Cisco Fabric Service over Ethernet (CSFoE) faz parte dessa classe e é usado para comunicar os estados de controle de aplicativos críticos entre os switches Nexus e, portanto, é essencial para a estabilidade.

O mesmo se aplica a outros protocolos dentro dessa classe, que inclui CDP, UDLD e VTP.

Recomendações

- O comportamento mais comum está relacionado à instabilidade da Ethernet L2. Verifique se o STP foi projetado corretamente de forma determinística com as melhorias de recursos relevantes em jogo para minimizar o impacto de dispositivos de reconvergência ou invasores na rede. Verifique se o tipo de porta STP apropriado está configurado para todos os dispositivos de host final que não participam da extensão L2 estão configurados como portas de tronco de borda/borda para minimizar TCNs.

- Use aprimoramentos de STP, como BPDUguard, Loopguard, BPDUfilter e RootGuard, onde apropriado, para limitar o escopo de uma falha ou problemas com erros de configuração ou dispositivos invasores na rede.

- Consulte: Guia de configuração de switching de camada 2 do Nexus 9000 NX-OS, versão 10.2(x)

- Verifique os comportamentos de movimentação de MAC que podem levar à desativação da aprendizagem e liberações de MAC. Consulte:Solução de problemas e métodos preventivos de movimentação do Nexus 9000 Mac

Roteador Multicast de Classe - class-map copp-system-p-class-multicast-router

Essa classe se refere aos pacotes PIM (Protocol Independent Multicast) do plano de controle usados para o estabelecimento e o controle de árvores roteadas compartilhadas por multicast através de todos os dispositivos habilitados para PIM no caminho do plano de dados e inclui o FHR (First-Hop Router), o LHR (Last-Hop Router), o IHR (Intermediate-Hop Routers) e os RPs (Rendezvous Points). Os pacotes classificados nessa classe incluem registro PIM para origens, junções PIM para receptores para IPv4 e IPv6, em geral qualquer tráfego destinado a PIM (224.0.0.13) e Multicast Source Discovery Protocol (MSDP). Esteja ciente de que há várias classes adicionais, que lidam com partes muito específicas da funcionalidade de multicast ou RP que são tratadas por classes diferentes.

```
class-map copp-system-p-class-multicast-router (match-any)
match access-group name copp-system-p-acl-pim
match access-group name copp-system-p-acl-msdp
match access-group name copp-system-p-acl-pim6
match access-group name copp-system-p-acl-pim-reg
match access-group name copp-system-p-acl-pim6-reg
match access-group name copp-system-p-acl-pim-mdt-join
match exception mvpn
set cos 6
police cir 2600 kbps , bc 128000 bytes
```

Impacto

O principal impacto nos descartes relacionados a essa classe está associado a problemas que se comunicam com fontes multicast pelo registro PIM em direção aos RPs ou joins PIM não processados corretamente, o que desestabilizaria as árvores de caminho mais curto ou compartilhado em direção às fontes do fluxo multicast ou aos RPs. O comportamento pode incluir lista de interface de saída (OIL) não preenchida corretamente devido a junções ausentes, ou (S, G), ou (*, G) não vistos consistentemente no ambiente. Também podem surgir problemas entre domínios de roteamento multicast que dependem do MSDP para interconexão.

Recomendações

- O comportamento mais comum para problemas relacionados ao controle PIM refere-se a problemas de escala ou comportamentos falsos. Um dos comportamentos mais comuns é visto devido à implementação no UPnP, que também pode causar problemas de esgotamento de memória. Isso pode ser solucionado por filtros e escopo reduzido dos dispositivos invasores. Para obter detalhes sobre como reduzir e filtrar pacotes de controle multicast que dependem da função de rede do dispositivo, consulte: Configurar a filtragem multicast no Nexus 7K/N9K - Cisco

Class Multicast Host - copp-system-p-class-multicast-host

Essa classe se refere ao Multicast Listener Discovery (MLD), especificamente aos tipos de pacotes de consulta, relatório, redução e MLDv2 do MLD. O MLD é um protocolo IPv6 que um host usa para solicitar dados multicast para um grupo específico. Com as informações obtidas através do MLD, o software mantém uma lista de grupos multicast ou associações de canal em uma base por interface. Os dispositivos que recebem pacotes MLD enviam os dados multicast que recebem para os grupos solicitados ou canais fora do segmento de rede dos receptores conhecidos. MLDv1 é derivado de IGMPv2 e MLDv2 é derivado de IGMPv3. O IGMP usa os tipos de mensagem do Protocolo IP 2, enquanto o MLD usa os tipos de mensagem do Protocolo IP 58, que é um subconjunto das mensagens do ICMPv6.

```
class-map copp-system-p-class-multicast-host (match-any)
match access-group name copp-system-p-acl-mld
set cos 1
police cir 1000 kbps , bc 128000 bytes
```

Impacto

As quedas nessa classe se traduzem em problemas nas comunicações multicast IPv6 de link local, o que pode fazer com que os relatórios de ouvinte dos receptores ou as respostas às consultas gerais sejam descartados, o que impede a descoberta de grupos multicast que os hosts desejam receber. Isso pode afetar o mecanismo de rastreamento e não encaminhar adequadamente o tráfego através das interfaces esperadas que solicitaram o tráfego.

Recomendações

- Como o tráfego MLD é significativo em um nível de link local para IPv6, se quedas forem vistas nessa classe, as causas de comportamento mais comuns estão relacionadas a escala, instabilidade de L2 ou dispositivos invasores.

Dados multicast de camada 3 de classe - copp-system-p-class-l3mc-data e dados multicast de camada 3 de classe IPv6 - copp-system-p-class-l3mcv6-data

Essas classes se referem ao tráfego que corresponde a um redirecionamento de exceção de multicast para o SUP. Nesse caso, há duas condições que são tratadas por essas classes. A primeira é a falha de Encaminhamento de Caminho Reverso (RPF) e a segunda é a falha de destino. A falta de destino refere-se a pacotes multicast em que a consulta no hardware para a tabela de encaminhamento multicast da Camada 3 falha e, portanto, o pacote de dados é enviado para a CPU. Às vezes, esses pacotes são usados para disparar/instalar o plano de controle multicast e adicionar as entradas das tabelas de encaminhamento de hardware, com base no tráfego do plano de dados. Os pacotes multicast de plano de dados que violam o RPF também corresponderiam a essa exceção e seriam classificados como uma violação.

class-map copp-system-p-class-l3mc-data (match-any)
match exception multicast rpf-failure
match exception multicast dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes

class-map copp-system-p-class-l3mcv6-data (match-any)
match exception multicast ipv6-rpf-failure
match exception multicast ipv6-dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes

Impacto

Falhas de RPF e erros de destino implicam em um problema de design ou configuração relacionado ao fluxo de tráfego através do roteador multicast. Erros de destino são comuns na criação de estado, quedas podem levar à programação e criação de falhas de (*, G), (S, G).

Recomendações

- Realize alterações no projeto básico de RIB unicast ou adicione mroute estático para orientar o tráfego através de uma interface específica, no caso de falhas de RPF.
- Consulte O Roteador Não Encaminha Pacotes Multicast para o Host Devido à Falha de RPF

Classe IGMP - copp-system-p-class-igmp

Essa classe se refere a todas as mensagens IGMP, para todas as versões que são usadas para solicitar dados multicast para um grupo específico, e usadas pela funcionalidade de snooping IGMP para manter os grupos e a OIL (Outgoing Interface List, lista de interface de saída) relevante que encaminha o tráfego para os receptores interessados na Camada 2. As mensagens de IGMP são localmente significativas porque não atravessam um limite de Camada 3, pois seu tempo de vida (TTL) deve ser 1, conforme documentado em RFC2236 (Internet Group Management Protocol, Versão 2). Os pacotes IGMP tratados por essa classe incluem todas as consultas de associação (gerais ou específicas de origem/grupo), juntamente com a associação e relatórios de saída dos receptores.

class-map copp-system-p-class-normal-igmp (match-any)
match access-group name copp-system-p-acl-igmp
set cos 3
police cir 3000 kbps , bc 64000 bytes

Impacto

As quedas nessa classe seriam convertidas em problemas em todos os níveis de uma comunicação multicast entre origem e receptor, dependendo do tipo de mensagem IGMP descartada devido à violação. Se os relatórios de associação dos receptores forem perdidos, o roteador não estará ciente dos dispositivos interessados no tráfego e, portanto, não incluirá a interface/VLAN em sua lista de interfaces de saída relevante. Se esse dispositivo também for o consultante ou o roteador designado, ele não disparará as mensagens de junção PIM relevantes para o RP se a origem estiver além do domínio local da camada 2, portanto, ele nunca estabelecerá o plano de dados através da árvore multicast até o receptor ou o RP. Se o relatório de licença for perdido, o receptor poderá continuar a receber tráfego indesejado. Isso também pode afetar todas as consultas IGMP

relevantes disparadas pelo consultante e a comunicação entre os roteadores multicast em um domínio.

Recomendações

- Os comportamentos mais comuns associados a quedas de IGMP estão relacionados à instabilidade de L2, problemas com temporizadores ou escala.

Classe Normal - copp-system-p-class-normalcopp-system-p-class-normal

Essa classe se refere ao tráfego que corresponde ao tráfego ARP padrão e também inclui o tráfego associado ao 802.1X, usado para o controle de acesso à rede baseado em porta. Essa é uma das classes mais comuns que encontra violações, pois as solicitações ARP, o ARP Gratuito e os pacotes ARP Reverso são transmitidos e propagados por todo o domínio da Camada 2. É importante lembrar que os pacotes ARP não são pacotes IP, esses pacotes não contêm um cabeçalho L3 e, portanto, a decisão é tomada exclusivamente no escopo dos cabeçalhos L2. Se um roteador for configurado com uma interface IP associada a essa sub-rede, como uma interface virtual do switch (SVI), o roteador enviará os pacotes ARP para o SUP para serem processados, pois eles são destinados ao endereço de broadcast do hardware. Qualquer tempestade de broadcast, loop de Camada 2 (devido a STP ou flaps) ou um dispositivo de roteamento na rede pode levar a uma tempestade ARP, que faz com que as violações aumentem significativamente.

```
class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
```

Impacto

O impacto das violações nessa classe depende muito da duração dos eventos e da função do switch no ambiente. As quedas nessa classe implicam que os pacotes ARP são descartados atualmente e, portanto, não processados pelo mecanismo SUP, o que pode levar a dois comportamentos principais causados por resoluções ARP incompletas.

Da perspectiva do host final, os dispositivos na rede não são capazes de resolver ou completar a resolução de endereço com o switch. Se esse dispositivo atuar como o gateway padrão para o segmento, ele poderá fazer com que os dispositivos não consigam resolver seu gateway e, portanto, não consigam rotear para fora de seu segmento Ethernet L2 (VLAN). Os dispositivos ainda podem se comunicar no segmento local se puderem concluir a resolução ARP para outros hosts finais no segmento local.

Da perspectiva do switch, se a tempestade e as violações forem predominantes, isso também pode fazer com que o switch não seja capaz de concluir o processo para a solicitação ARP gerada. Essas solicitações são normalmente geradas para resoluções de sub-rede do próximo salto ou diretamente conectadas. Embora as respostas ARP sejam de natureza unicast, pois são endereçadas ao MAC de propriedade do switch, elas são classificadas nessa mesma classe, pois ainda são pacotes ARP. Isso se traduz em problemas de acessibilidade porque o switch não pode processar adequadamente o tráfego se o próximo salto não for resolvido e pode levar a problemas com a regravação do cabeçalho da Camada 2, se o gerenciador de adjacências não tiver uma entrada para o host.

O impacto também depende do escopo do problema básico que disparou a violação do ARP. Por exemplo, em uma tempestade de broadcasts, os hosts e o switch continuam a usar o ARP para tentar resolver a adjacência, o que pode levar a tráfego de broadcast adicional na rede, e como os pacotes ARP são da camada 2, não há tempo de vida (TTL) da camada 3 para interromper um loop de L2 e, portanto, eles continuam a executar

um loop, e crescer exponencialmente através da rede até que o loop seja interrompido.

Recomendações

- Resolva qualquer instabilidade básica de L2 que possa causar tempestades ARP no ambiente, como STP, flaps ou dispositivos invasores. Interrompa esses loops conforme necessário, usando qualquer método desejado para abrir o caminho do link.

- O controle de tempestades também pode ser usado para mitigar uma tempestade ARP. Se o storm control não estiver habilitado, verifique as estatísticas do contador nas interfaces para verificar a porcentagem de tráfego de broadcast visto nas interfaces em relação ao tráfego total que passa pela interface.

- Se não houver tempestade, mas quedas constantes ainda forem vistas no ambiente, verifique o tráfego SUP para identificar quaisquer dispositivos invasores, que enviam constantemente pacotes ARP na rede, que possam afetar o tráfego legítimo.

- Os aumentos que podem ser vistos dependem do número de hosts na rede e da função do switch no ambiente, o ARP é projetado para tentar novamente, resolver e atualizar entradas e, portanto, espera-se que veja o tráfego ARP o tempo todo. Se forem observadas apenas quedas esporádicas, elas podem ser transitórias devido à carga da rede e nenhum impacto é percebido. Mas é importante monitorar e conhecer a rede para identificar e diferenciar corretamente uma situação esperada de uma situação anormal.

Class NDP - copp-system-p-acl-ndp

Essa classe se refere ao tráfego associado à descoberta/anúncio de vizinhos IPv6 e à solicitação de roteador e aos pacotes de anúncio que usam mensagens ICMP para determinar endereços locais da camada de enlace de vizinhos, e é usada para alcance e controle de dispositivos vizinhos.

class-map copp-system-p-class-ndp (match-any)
match access-group name copp-system-p-acl-ndp
set cos 6
police cir 1400 kbps , bc 32000 bytes

Impacto

As violações nessa classe podem impedir a comunicação IPv6 entre dispositivos vizinhos, já que esses pacotes são usados para facilitar a descoberta dinâmica ou informações de camada de enlace/local entre hosts e roteadores no enlace local. Uma interrupção dessa comunicação também pode causar problemas com acessibilidade além ou através do link local associado. Se houver problemas de comunicação entre vizinhos IPv6, verifique se não há descartes nessa classe.

Recomendações

- Examine todos os comportamentos ICMP anormais dos dispositivos vizinhos, particularmente aqueles relacionados à descoberta de vizinhos e/ou descoberta de roteador.

- Certifique-se de que todos os valores esperados de temporizador e intervalo para as mensagens periódicas sejam consistentes em todo o ambiente e honrados. Por exemplo, para mensagens de anúncio de roteador (mensagens RA).

DHCP de classe normal - copp-system-p-class-normal-dhcp

Essa classe se refere ao tráfego associado ao Protocolo Bootstrap (cliente/servidor BOOTP), comumente conhecido como pacotes DHCP (Dynamic Host Control Protocol) no mesmo segmento Ethernet local para IPv4 e IPv6. Isso se relaciona especificamente somente à comunicação de tráfego que se origina de qualquer cliente bootp ou destinada a qualquer servidor BOOTP, através de toda a troca de pacotes de descoberta, oferta, solicitação e confirmação (DORA), e também inclui a transação cliente/servidor DHCPv6 através das portas UDP 546/547.

```
class-map copp-system-p-class-normal-dhcp (match-any)
match access-group name copp-system-p-acl-dhcp
match access-group name copp-system-p-acl-dhcp6
set cos 1
police cir 1300 kbps , bc 32000 bytes
```

Impacto

As violações nessa classe podem fazer com que os hosts finais não consigam adquirir corretamente um IP do servidor DHCP e, assim, retornem ao intervalo de endereço IP privado automático (APIPA), 169.254.0.0/16. Tais violações podem ocorrer em ambientes onde os dispositivos tentam inicializar simultaneamente e, assim, ir além da CIR associada à classe.

Recomendações

- Verifique com as capturas, nos hosts e no servidor DHCP, se a transação DORA inteira foi vista. Se o switch fizer parte dessa comunicação, também será importante verificar os pacotes processados ou direcionados para a CPU e verificar as estatísticas no switch: **show ip dhcp global statistics** e nos redirecionamentos: **show system internal access-list sup-redirect-stats module 1 | grep -i dhcp**.

Resposta de Retransmissão DHCP Normal de Classe - copp-system-p-class-normal-dhcp-relay-response

Essa classe se refere ao tráfego associado à funcionalidade de retransmissão de DHCP para IPv4 e IPv6, direcionado aos servidores DHCP configurados configurados sob a retransmissão. Isso se refere especificamente somente à comunicação de tráfego que se origina de qualquer servidor BOOTP ou que se destina a qualquer cliente BOOTP através de toda a troca de pacotes DORA, e também inclui transação cliente/servidor DHCPv6 através das portas UDP 546/547.

```
class-map copp-system-p-class-normal-dhcp-relay-response (match-any)
match access-group name copp-system-p-acl-dhcp-relay-response
match access-group name copp-system-p-acl-dhcp6-relay-response
set cos 1
police cir 1500 kbps , bc 64000 bytes
```

Impacto

As violações para essa classe têm o mesmo impacto que as violações para a classe copp-system-p-class-normal-dhcp, porque ambas são partes da mesma transação. Essa classe se concentra principalmente nas comunicações de resposta dos servidores do agente de retransmissão. O Nexus não atua como o servidor DHCP; ele foi projetado apenas para atuar como um agente de retransmissão.

Recomendações

- As mesmas recomendações do DHCP de classe normal aplicam-se aqui. Como a função do Nexus é apenas atuar como um agente de retransmissão, no SUP você espera ver toda a transação entre o host e o switch atuando como retransmissão, e o switch e os servidores configuram.

- Certifique-se de que não haja dispositivos invasores, como servidores DHCP inesperados na rede que respondam ao escopo, ou dispositivos presos em um loop que inunde a rede com pacotes DHCP Discover. Verificações adicionais podem ser executadas pelos comandos: show ip dhcp relay e **show ip dhcp relay statistics**.

Fluxo NAT de classe - copp-system-p-class-nat-flow

Essa classe se refere ao tráfego de fluxo NAT do switch de software. Quando uma nova conversão dinâmica é criada, o fluxo é encaminhado por software até que a conversão seja programada no hardware e, em seguida, é policiado pelo CoPP para limitar o tráfego apontado para o supervisor enquanto a entrada é instalada no hardware.

```
class-map copp-system-p-class-nat-flow (match-any)
match exception nat-flow
set cos 7
police cir 800 kbps , bc 64000 bytes
```

Impacto

Quedas nessa classe normalmente ocorrem quando uma alta taxa de conversões e fluxos dinâmicos novos é instalada no hardware. O impacto está relacionado aos pacotes comutados por software que são descartados e não entregues ao host final, o que pode levar a perda e retransmissões. Quando a entrada é instalada no hardware, nenhum tráfego adicional é apontado para o supervisor.

Recomendações

- Verifique as diretrizes e limitações do NAT dinâmico na plataforma relevante. Existem limitações conhecidas que são documentadas em plataformas, como o 3548, no qual a conversão pode levar alguns segundos. Consulte: Restrições para NAT dinâmico

Exceção de Classe - copp-system-p-class-exception

Essa classe se refere aos pacotes de exceção associados aos pacotes de opção IP e de IP ICMP inalcançável. Se um endereço de destino não estiver presente no banco de informações de encaminhamento (FIB) e resultar em uma perda, o SUP enviará um pacote ICMP inalcançável de volta ao remetente. Os pacotes com opções IP ativadas também se enquadram nessa classe. Consulte o documento IANA para obter detalhes sobre as opções IP: IP Option Numbers

```
 class-map copp-system-p-class-exception (match-any)
match exception ip option
match exception ip icmp unreachable
match exception ipv6 option
match exception ipv6 icmp unreachable
set cos 1
police cir 150 kbps , bc 32000 bytes
```

Impacto

Essa classe é fortemente policiada e os descartes nessa classe não são indicativos de uma falha, mas sim de um mecanismo de proteção para limitar o escopo de pacotes de opções IP e de ICMP inalcançáveis.

Recomendações

- Verifique se há algum fluxo de tráfego visto ou direcionado para a CPU para destinos fora da FIB.

Redirecionamento de Classe - copp-system-p-class-redirect

Essa classe se refere ao tráfego associado ao Precision Time Protocol (PTP), usado para sincronização de tempo. Isso inclui o tráfego multicast para o intervalo reservado 224.0.1.129/32, o tráfego unicast na porta UDP 319/320 e o Ethetype 0X88F7.

```
class-map copp-system-p-class-redirect (match-any)
match access-group name copp-system-p-acl-ptp
match access-group name copp-system-p-acl-ptp-l2
match access-group name copp-system-p-acl-ptp-uc
set cos 1
police cir 280 kbps , bc 32000 bytes
```

Impacto

Quedas nessa classe podem causar problemas em dispositivos que não foram sincronizados corretamente ou não estabeleceram a hierarquia apropriada.

Recomendações

- Garanta a estabilidade dos relógios e que eles estejam configurados corretamente. Verifique se o dispositivo PTP está configurado para o modo multicast ou unicast PTP, mas não ambos ao mesmo tempo. Isso também é documentado sob as diretrizes e limitações e pode levar o tráfego além da taxa de entrada comprometida.

- Reveja o projeto e a configuração do relógio de limite e de todos os dispositivos PTP no ambiente. Verifique se todas as diretrizes e limitações foram seguidas por plataforma, pois elas variam.

OpenFlow de Classe - copp-system-p-class-openflow

Essa classe se refere ao tráfego associado às operações do agente OpenFlow e à conexão TCP correspondente entre o controlador e o agente.

```
class-map copp-system-p-class-openflow (match-any)
match access-group name copp-system-p-acl-openflow
set cos 5
police cir 1000 kbps , bc 32000 bytes
```

Impacto

Quedas nessa classe podem causar problemas em agentes que não recebem e processam corretamente as instruções do controlador para gerenciar o plano de encaminhamento da rede

Recomendações

- Certifique-se de que nenhum tráfego duplicado seja visto na rede ou qualquer dispositivo que impeça a comunicação entre o controlador e os agentes.
- Verifique se a rede L2 não tem instabilidade (STP ou loops).

Solucionar problemas de quedas de CoPP

Os primeiros passos para solucionar problemas de violações de CoPP são determinar:

- Impacto e escopo da questão.
- Entender o fluxo de tráfego através do ambiente e a função do switch na comunicação afetada.
- Determine se há violações na classe associada suspeita e repita conforme necessário.

Por exemplo, o comportamento listado foi detectado:

- Os dispositivos não podem se comunicar com outros dispositivos fora de sua rede, mas podem se comunicar localmente.
- O impacto foi isolado para a comunicação roteada fora da VLAN, e o switch atua como o gateway padrão.
- Uma verificação dos hosts indica que eles não podem fazer ping no gateway. Após uma verificação de sua tabela ARP, a entrada para o gateway permanece como Incompleta.
- Todos os outros hosts que têm o gateway resolvido não têm problemas de comunicação. Uma verificação de CoPP no switch que atua como gateway indica que há violações no copp-system-p-class-normal.

<#root>

class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
module 1 :
transmitted 3292445628 bytes;

dropped 522023852 bytes;

- Além disso, várias verificações de comando mostram que os descartes estão ativamente aumentando.

- Essas violações podem fazer com que o tráfego ARP legítimo seja descartado, o que leva a um comportamento de negação de serviços.

É importante destacar que o CoPP isola o impacto no tráfego associado à classe específica, que neste exemplo são ARP e copp-system-p-class-normal. O tráfego relacionado a outras classes, como OSPF, BGP não deve ser descartado por CoPP, pois eles se enquadram inteiramente em uma classe diferente. Se não for marcada, as questões ARP podem propagar-se para outros problemas, que podem afetar os protocolos que dependem dele para começar. Por exemplo, se um cache ARP atingir o tempo limite e não for atualizado devido a violações excessivas, uma sessão TCP, como o BGP, pode ser encerrada.

- Recomenda-se a realização de verificações do plano de controle, como Ethanalyzer, estatísticas in-band de CPU-mac e processo de CPU para isolar ainda mais o assunto.

Ethanalyzer

Como o tráfego vigiado pelo CoPP é associado somente ao tráfego vinculado à CPU, uma das ferramentas mais importantes é o Ethanalyzer. Essa ferramenta é uma implementação Nexus do TShark e permite que o tráfego enviado e recebido pelo supervisor seja capturado e decodificado. Ele também pode usar filtros baseados em diferentes critérios, como protocolos ou informações de cabeçalho, tornando-se assim uma ferramenta inestimável para determinar o tráfego enviado e recebido pela CPU.

A recomendação é primeiro examinar o tráfego ARP visto pelo supervisor quando a ferramenta Ethanalyzer é executada diretamente na sessão do terminal ou enviada a um arquivo para análise. É possível definir filtros e limites para focalizar a captura em um padrão ou comportamento específico. Para fazer isso, adicione filtros de exibição flexíveis.

Uma concepção equivocada comum é que o Ethanalyzer captura todo o tráfego que passa pelo switch. O tráfego do plano de dados, entre hosts, é comutado ou roteado pelos ASICs de hardware entre as portas de dados não exige envolvimento da CPU e, portanto, não é normalmente visto pela captura do Ethanalyzer. Para capturar o tráfego do plano de dados, outras ferramentas, como ELAM ou SPAN, são aconselhadas a serem usadas. Por exemplo, para filtrar o ARP, use o comando:

ethanalyzer local interface inband display-filter arp limit-captured-frames 0 autostop duration 60 > arpcpu

Campos configuráveis importantes:

- interface inband - refere-se ao tráfego direcionado ao SUP

- display-filter arp - se refere ao filtro de tubarão aplicado, a maioria dos filtros Wireshark é aceita

- limit-captured-frames 0 - refere-se ao limite, 0 equivale a ilimitado, até ser interrompido por outro parâmetro ou interrompido manualmente por Ctrl+C

- autostop duration 60 - refere-se à parada do Ethanalyzer após 60 segundos, criando assim um instantâneo de 60 segundos do tráfego ARP visto na CPU

A saída do Ethanalyzer é redirecionada para um arquivo no flash de inicialização com > arpcpu, para ser processada manualmente. Após 60 segundos, a captura é concluída e o Ethanalyzer termina dinamicamente, e o arquivo arpcpu está no flash de inicialização do switch, que pode ser processado para extrair os principais talkers. Por exemplo:

show file bootflash:arpcpu | sort -k 3,5 | uniq -f 2 -c | sort -r -n | head lines 50

669 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:47 -> ff:ff:ff:ff:ff:ff ARP Who has 10.1.1.1? Tell 10.1.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:43 -> ff:ff:ff:ff:ff:ff ARP Who has 10.2.1.1? Tell 10.2.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:41 -> ff:ff:ff:ff:ff:ff ARP Who has 10.3.1.1? Tell 10.3.1.2

Esse filtro é classificado com base em: as colunas de origem e de destino, as correspondências exclusivas encontradas (mas ignora a coluna de data), conta as instâncias e adiciona o número visto e, finalmente, classifica de cima para baixo, com base na contagem, e exibe os primeiros 50 resultados.

Neste exemplo de laboratório, em 60 segundos, mais de 600 pacotes ARP foram recebidos de três dispositivos, que foram identificados como os dispositivos suspeitos de serem infratores. A primeira coluna no filtro detalha o número de instâncias para esse evento que foram vistas no arquivo de captura na duração especificada.

É importante entender que a ferramenta Ethanalyzer atua no driver em banda, que é essencialmente a comunicação no ASIC. Teoricamente, o pacote precisa passar pelo kernel e o gerenciador de pacotes para ser entregue ao próprio processo associado. O CoPP e o HWRL atuam antes que o tráfego seja visto no Ethanalyzer. Mesmo que as violações aumentem ativamente, parte do tráfego ainda passa e está em conformidade com a taxa de polícia, o que ajuda a fornecer informações sobre os fluxos de tráfego apontados para a CPU. É uma distinção importante, pois o tráfego visto no Ethanalyzer NÃO é o tráfego que violou a CIR e foi descartado.

O Ethanalyzer também pode ser usado de forma aberta, sem nenhum filtro de exibição ou filtro de captura especificado para capturar todo o tráfego SUP relevante. Isso pode ser usado como uma medida de isolamento como parte da abordagem para solucionar problemas.

Para obter detalhes adicionais e o uso do Ethanalyzer, consulte a Nota Técnica:

Guia de solução de problemas do Ethanalyzer no Nexus 7000

Uso do Ethanalyzer na plataforma Nexus para análise de tráfego de plano de controle e plano de dados

---

Observação: o Nexus 7000, antes do lançamento do código 8.X, só pode executar capturas do Ethanalyzer por meio do VDC do administrador, que abrange o tráfego vinculado ao SUP de todos os VDCs. O Ethanalyzer específico do VDC está presente nos códigos 8.X.

Estatísticas In-band de CPU-MAC

As estatísticas in-band associadas ao tráfego de CPU mantêm estatísticas relevantes do tráfego de CPU TX/RX in-band. Essas estatísticas podem ser verificadas com o comando: show hardware internal cpu-mac inband stats, que fornece informações sobre a taxa atual e as estatísticas de taxa de pico.

show hardware internal cpu-mac inband stats`

================ Packet Statistics =====================
Packets received: 363598837
Bytes received: 74156192058
Packets sent: 389466025
Bytes sent: 42501379591
Rx packet rate (current/peak): 35095 / 47577 pps
Peak rx rate time: 2022-05-10 12:56:18
Tx packet rate (current/peak): 949 / 2106 pps
Peak tx rate time: 2022-05-10 12:57:00

Como prática recomendada, recomenda-se que uma linha de base seja criada e rastreada, pois, devido à função do switch e da infraestrutura, a saída do switch **show hardware internal cpu-mac inband stats** varia significativamente. Neste ambiente de laboratório, os valores normais e os picos históricos geralmente não são maiores que algumas centenas de pontos percentuais, portanto, isso é anormal. O comando também **show hardware internal cpu-mac inband events** é útil como referência histórica, pois contém dados relacionados ao uso máximo e ao horário em que foi detectado.

Processar CPU

Os switches Nexus são sistemas baseados em Linux, e o Nexus Operating System (NXOS) aproveita o programador preemptivo da CPU, multitarefas e multithreading de sua respectiva arquitetura de núcleos, para fornecer acesso justo a todos os processos e, portanto, picos nem sempre são indicativos de um problema. No entanto, se forem observadas violações de tráfego sustentadas, é provável que o processo associado também seja muito usado e apareça como um recurso principal sob as saídas da CPU. Tire vários instantâneos dos processos da CPU para verificar o alto uso de um processo específico usando: **show processes cpu sort | exclude 0.0 or show processes cpu sort | grep <process>**.

As verificações da CPU do processo, estatísticas em banda e do Ethanalyzer fornecem informações sobre os processos e o tráfego processados atualmente pelo supervisor e ajudam a isolar a instabilidade contínua no tráfego do plano de controle que pode ser propagado em problemas do plano de dados. É importante entender que a CoPP é um mecanismo de proteção. É reacionário porque atua apenas no tráfego apontado para o SUP. Ele foi projetado para proteger a integridade do supervisor ao descartar as taxas de tráfego, que excedem os intervalos esperados. Nem todos os descartes indicam um problema ou exigem intervenção, pois sua importância está relacionada à classe CoPP específica e ao impacto verificado, com base no projeto de infraestrutura e rede. Quedas devido a eventos de burst esporádicos não se traduzem em impacto, pois os protocolos têm mecanismos incorporados, como keepalive e repetições que podem lidar com eventos transitórios. Manter o foco em eventos sustentados ou anormais além das linhas de base estabelecidas. Lembre-se de que o CoPP deve aderir aos protocolos e recursos específicos do ambiente e deve ser monitorado e iterado continuamente para ajustá-lo, com base nas necessidades de escalabilidade à medida que evoluem. Se ocorrerem quedas, determine se o CoPP deixou cair o tráfego involuntariamente ou em resposta a um mau funcionamento ou ataque. Em ambos os casos, analisar a situação e avaliar a necessidade de intervir através da análise do impacto e das medidas corretivas no ambiente, que podem estar fora do âmbito do próprio switch.

Informações adicionais

Plataformas/códigos recentes podem ter a capacidade de executar um SPAN-para-CPU, pelo espelho de uma porta e punt do tráfego do plano de dados para a CPU. Isso normalmente é fortemente limitado pela taxa limite de hardware e CoPP. Recomenda-se o uso cuidadoso de SPAN para CPU, e isso está fora do escopo deste documento.

Consulte a Nota Técnica listada para obter mais informações sobre esse recurso:

Procedimento de SPAN para CPU do Nexus 9000 Cloud Scale ASIC NX-OS

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.