Compreendendo e aplicando o UDP, as regras de conteúdo, e os grupos da fonte no CSS11000

Índice

Introdução

O tráfego do User Datagram Protocol (UDP) é unidirecional. O CSS ajusta-se - acima de um bloco de controle de fluxo (FCB) em um sentido, simplesmente quando um pacote de UDP é processado. O FCB para o caminho de retorno estabelece-se somente se o pacote de resposta chega. Devido à natureza unidirecional do UDP, os grupos da fonte são usados frequentemente no CSS fornecer o mapeamento entre os dois lados do fluxo UDP.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CSS 11000/11500
- Software webns

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.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Assuntos

Regras de conteúdo UDP

Uma regra de conteúdo UDP é configurada fornecer o Balanceamento de carga entre um grupo de server. Desta maneira, é não diferente do que precisando de configurar uma regra de conteúdo TCP. A regra de conteúdo é fornecer o Balanceamento de carga.

Configuração

```
************************** GLOBAL
************************
  ip route 0.0.0.0 0.0.0.0 10.86.213.1 1
!************************ INTERFACE
************************
interface  2/1
  bridge vlan 10
!************************** CIRCUIT
************************
circuit VLAN1
  ip address 192.168.2.2 255.255.255.0
circuit VLAN10
 ip address 10.86.213.117 255.255.255.0
!************************** SERVICE
************************
service dns_s1
  ip address 192.168.2.3
  active
service dns_s2
  ip address 192.168.2.4
  active
!************************** OWNER
************************
owner UDP
  content dns
    port 53
    protocol udp
    add service dns_s1
    add service dns_s2
    vip address 10.86.213.124
```

O cliente bate o endereço do IP virtual (VIP) com um pedido DNS. A carga CSS equilibra o pedido DNS entre os serviços ativo na regra. Um FCB estabelece-se para o cliente à conexão de VIP.

Uma regra de conteúdo UDP deve ter um grupo da fonte correspondente para segurar o tráfego do retorno UDP. No caso do DNS, esta é a resposta de DNS ao pedido inicial DNS. Se você não tem um grupo da fonte, a resposta para trás do servidor DNS não será NATed ao endereço VIP, e o cliente de DNS rejeitará o pedido. Isto pode ser visto emitindo o comando de **0.0.0.0 do show flows**.

```
CSS# show flows 0.0.0.0
-------------- ----- -------------- ----- -------------- --- ------- ------
Src Address SPort Dst Address DPort NAT Dst Address Prt In Port OutPort
-------------- ----- -------------- ----- -------------- --- ------- ------
161.44.67.245 2543 10.86.213.124 53 192.168.2.3 UDP 2/1 2/8
192.168.2.3 53 161.44.67.245 2543 0.0.0.0 UDP 2/8 2/1
```

161.44.67.245 é o cliente, 10.86.213.124 é o VIP, e 192.168.2.3 é o server. Observe que o fluxo da resposta do server não tem um `endereço NAT Dst`.

Nota: Deve-se igualmente notar que uma regra de conteúdo da camada 3 (L3) trabalha para o UDP da mesma forma descrito acima. Uma regra de conteúdo L3 não tem o protocolo ou a porta configurado.

```
CSS# show flows 0.0.0.0
-------------- ----- -------------- ----- -------------- --- ------- ------
Src Address SPort Dst Address DPort NAT Dst Address Prt In Port OutPort
-------------- ----- -------------- ----- -------------- --- ------- ------
161.44.67.245 2543 10.86.213.124 53 192.168.2.3 UDP 2/1 2/8
192.168.2.3 53 161.44.67.245 2543 0.0.0.0 UDP 2/8 2/1
```

Com esta regra de conteúdo, o UDP ou o tráfego TCP podem bater estes VIP e equilíbrio da carga a um servidor backend.

Grupos da fonte UDP conjuntamente com uma regra de conteúdo

Um grupo da fonte UDP é usado para segurar o tráfego de retorno UDP. No exemplo, esta é uma resposta de DNS ao pedido DNS, que bateu a regra de conteúdo `dns`. Um cliente pode configurar o grupo em três maneiras diferentes a fim conseguir o tráfego de retorno do NATing UDP.

1. Os servidores backend da regra de conteúdo podem ser duplicados dentro do grupo. Você precisaria de adicionar um grupo à configuração acima.
   ```
   CSS# show flows 0.0.0.0
   -------------- ----- -------------- ----- -------------- --- ------- ------
   Src Address SPort Dst Address DPort NAT Dst Address Prt In Port OutPort
   -------------- ----- -------------- ----- -------------- --- ------- ------
   161.44.67.245 2543 10.86.213.124 53 192.168.2.3 UDP 2/1 2/8
   192.168.2.3 53 161.44.67.245 2543 0.0.0.0 UDP 2/8 2/1
   ```
   Com esta configuração, a resposta de DNS chega do `dns_s1` ou do `dns_s2`, e o fósforo do grupo da fonte é feito. Isto causa o pacote ser NATed ao endereço VIP configurado na regra. É importante compreender porque a porta de origem não está indo ser NATed. Os grupos da fonte não NAT a porta de origem se é uma porta conhecida IP, que são portas menos de 1024.Para recaplitular, o pedido DNS bate a regra de conteúdo DNS para ser carga equilibrada. Na frente do CSS são 161.44.67.245:2586 - > VIP (10.86.213.124):53. Entre o CSS e o server são 161.44.67.245:2586 - > o dns_s1 (192.168.2.3):53. A resposta para trás do server é Dns_s1(192.168.2.3):53 - > 161.44.67.245:2586. A resposta de DNS combina o grupo da fonte quando bate o CSS para VIP (10.86.213.124):53 - > 161.44.67.245:2586.**O comando show flows** output:
   ```
   CSS(config)# show flows 0.0.0.0
   -------------- ----- -------------- ----- -------------- --- ------- ------
   Src Address SPort Dst Address DPort NAT Dst Address Prt InPort OutPort
   -------------- ----- -------------- ----- -------------- --- ------- ------
   192.168.2.3 53 161.44.67.245 2586 161.44.67.245 UDP 2/8 2/1
   161.44.67.245 2586 10.86.213.124 53 192.168.2.3 UDP 2/1 2/8
   ```
   Desde que a porta de origem é menos de 1024, e é uma porta bem conhecida, a porta de origem não é NATed, mesmo que bata um grupo da fonte. Somente o endereço IP de origem será NATed de volta ao

endereço VIP.Para que o este tipo de configuração trabalhe corretamente:O endereço VIP na regra de conteúdo e no grupo da fonte deve ser o mesmo.A porta de origem no tráfego de resposta deve ser conhecida. Por exemplo raio, que é a porta 1645. Se o exemplo acima era um par da autenticação RADIUS e da resposta, a resposta do raio teria seu NATed da porta de origem desde 1645 a uma porta do grupo da fonte (por exemplo, 8192). É provável isto causaria a requisição RADIUS falhar. Esta é a razão que o **comando disable do portmap** esteve adicionado ao grupo da fonte.

2. Os servidores backend da regra de conteúdo podem ser duplicados dentro do grupo como serviços de destino. O serviço de destino permite o endereço IP de origem assim como a porta de origem ser NATed quando o pedido DNS vem dentro do cliente. A configuração de cliente é mostrada abaixo.**Nota:** Para maior clareza, um endereço diferente VIP é posto sobre o grupo da fonte do que na regra de conteúdo. O endereço VIP é 10.86.213.125. Isto é de modo que o endereço de origem que obtém o NATed entre o CSS e o server não seja o mesmo que o endereço VIP.Neste caso, quando o pedido DNS chega do cliente, a regra de conteúdo e o fósforo do grupo da fonte são feitos. O endereço IP de destino será NATed ao server equilibrado carga. Porque o grupo da fonte foi combinado através do destino adicionar, o endereço IP de origem e a porta de origem serão NATed. Na frente do CSS são 161.44.67.245:2644 - > VIP (10.86.213.124):53. Entre o CSS e o server é o dns_s1 10.86.213.125:8192-> (192.168.2.3):53.Desde que o fósforo do grupo da fonte foi feito na altura do pedido DNS, a entrada de mapa de porta dentro do grupo da fonte foi criada, e é combinada pela resposta de DNS para trás do server. A resposta para trás do server é Dns_s1(192.168.2.3):53 - > 10.86.213.125:8192.A entrada do mapa de portas do grupo da fonte segura o NATing o endereço IP de origem e a porta de origem original do cliente. A resposta de DNS passada do CSS ao cliente é VIP (10.86.213.124):53 - > 161.44.67.245:2644.**O comando show flows** output:

```
CSS(config)# show flows 0.0.0.0
-------------- ----- -------------- ----- -------------- --- ------- ------
Src Address SPort Dst Address DPort NAT Dst Address Prt InPort OutPort
-------------- ----- -------------- ----- -------------- --- ------- ------
192.168.2.3 53 10.86.213.125 8192 161.44.67.245 UDP 2/8 2/1
161.44.67.245 2644 10.86.213.124 53 192.168.2.3 UDP 2/1 2/8
```

Com esta configuração, o VIP na regra de conteúdo pode combinar o endereço do grupo da fonte VIP mas não faz tem que. A limitação da porta bem conhecida (menos de 1024) ainda existe. A configuração do serviço de destino não deve ser usada se o server precisa de ver o endereço IP real do cliente.

3. Não pode haver nenhum serviço definido no grupo, e o grupo é preferido para uma escala dos endereços IP de Um ou Mais Servidores Cisco ICM NT através de uma cláusula ACL.

```
CSS(config)# show flows 0.0.0.0
-------------- ----- -------------- ----- -------------- --- ------- ------
Src Address SPort Dst Address DPort NAT Dst Address Prt InPort OutPort
-------------- ----- -------------- ----- -------------- --- ------- ------
192.168.2.3 53 10.86.213.125 8192 161.44.67.245 UDP 2/8 2/1
161.44.67.245 2644 10.86.213.124 53 192.168.2.3 UDP 2/1 2/8
```

A indicação da causa ACL olharia similar a:

```
CSS(config)# show flows 0.0.0.0
-------------- ----- -------------- ----- -------------- --- ------- ------
Src Address SPort Dst Address DPort NAT Dst Address Prt InPort OutPort
-------------- ----- -------------- ----- -------------- --- ------- ------
192.168.2.3 53 10.86.213.125 8192 161.44.67.245 UDP 2/8 2/1
161.44.67.245 2644 10.86.213.124 53 192.168.2.3 UDP 2/1 2/8
```

Nota: Isto é usado geralmente quando o cliente não quer ao NAT todo o tráfego a ou de um determinado endereço. Desse

modo, podem controlar o que o tráfego obtém a NATed.

Grupos da fonte UDP para o NAT somente

Um outro uso dos grupos da fonte com tráfego UDP é ao tráfego NAT do espaço de endereço IP privado atrás do CSS aos endereços IP públicos. Neste caso, nenhuma regra de conteúdo é exigida porque nenhum Balanceamento de carga é exigido. O grupo da fonte UDP será usado simplesmente ao NAT o tráfego. Os serviços backend podem ser adicionados com os endereços IP privados, segundo as indicações do exemplo abaixo.

```
CSS(config)# show flows 0.0.0.0
-------------- ----- -------------- ----- -------------- --- ------- ------
Src Address SPort Dst Address DPort NAT Dst Address Prt InPort OutPort
-------------- ----- -------------- ----- -------------- --- ------- ------
192.168.2.3 53 10.86.213.125 8192 161.44.67.245 UDP 2/8 2/1
161.44.67.245 2644 10.86.213.124 53 192.168.2.3 UDP 2/1 2/8
```

Ou, nenhum serviços pode ser adicionado ao grupo, e o grupo da fonte pode ser preferido através de uma cláusula ACL.

```
CSS(config)# show flows 0.0.0.0
-------------- ----- -------------- ----- -------------- --- ------- ------
Src Address SPort Dst Address DPort NAT Dst Address Prt InPort OutPort
-------------- ----- -------------- ----- -------------- --- ------- ------
192.168.2.3 53 10.86.213.125 8192 161.44.67.245 UDP 2/8 2/1
161.44.67.245 2644 10.86.213.124 53 192.168.2.3 UDP 2/1 2/8
```

O pedido DNS vem dentro do servidor backend e combina o grupo da fonte. O FCB é criado e a transformação NAT é feita. A entrada de mapeador de porta do grupo da fonte foi criada internamente quando a resposta de DNS é recebida. No fluxo do retorno a consulta do grupo da fonte é feita, a entrada de mapa de porta interna recuperada, o FCB criado, e a resposta de DNS obtém a parte traseira do NATed corretamente.

Nenhuma regra de conteúdo é exigida porque nenhum Balanceamento de carga é exigido. O grupo da fonte segura a transformação NAT na resposta para trás porque usa a informação de mapeador de porta criada no pedido.

A limitação da porta bem conhecida (menos de 1024) é aderida ainda a. Uma porta do origem bem conhecida não será NATed, mas move superior ou igual a 1024 será NATed.

Opções de configuração UDP

Com liberações 5.0, 7.10, e 7.20 o comando parameter, **dnsflow [permita|o desabilitação]** está disponível. **permita** é o padrão, e significa que o FCB está criado para fluxos DNS. **o desabilitação** faz com que nenhum FCB seja criado embora a regra de conteúdo, e as funções de harmonização do grupo da fonte serão a mesma. Com liberação 6.10, a **funcionalidade do comando noflow** era prolongada através do parâmetro de configuração.

```
flow-state [5060|161|162|53] udp [flow-disable|flow-enable][nat-disable|nat-enable]
```

Os números de porta correspondem a SIP(5060), a SNMP(161), a SNMP(162), e a DNS(53).

A ideia atrás do **noflow** era puramente desempenho. Uma resposta UDP/protocolo do pedido tal como o DNS (o SNMP e o RAIO são outros dois uns comuns) não ganha nenhum benefício da

função CSS de traçar um FCB no caminho rápido, e de fato, as despesas gerais pode retardar o desempenho de processar este tipo de tráfego. Além, desde que o tráfego UDP é unidirecional e não tem nenhum pacote de terminador (tal como o TCP RST ou FIN), o fluxo UDP é suprimido somente através da coleção de lixo, que adiciona mais despesas gerais. Os detalhes de implementação de **noflow**, contudo, efetuaram os requisitos de configuração.

As liberações 5.0 e as liberações 2G CSS11500 têm somente o parâmetro de **comando disable do dnsflow** neste tempo. A liberação 6.10 tem a tabela de configurações do fluxo-**estado**, que pode fazer o fluxo-**desabilitação** para o SNMP, SNMP traps, e o DNS UDP flui.

O grupo da fonte não está exigido para os exemplos nos grupos da fonte UDP conjuntamente com uma regra de conteúdo ou grupos da fonte UDP para seções do NATing somente deste documento se o **desabilitação do dnsflow** ou os comandos do fluxo-**desabilitação** foram emitidos. Quando o comando do **noflow** é emitido, um grupo do origem interna está usado para não se manter a par de nenhum pacote do fluxo, e assim esta entrada de mapeador de porta interna, que não é associada com o qualquer grupo da fonte configurado, segura o tráfego de retorno.

Esta informação é fornecida para ser o mais detachado possível. O BU, contudo, recomenda que o grupo da fonte esteja configurado em nenhuns exemplos do fluxo. Este é ser consistente entre o fluxo e as **configurações de fluxo de rede**, e igualmente o grupo da fonte permite que o usuário considere os contadores de acertos, que interno não faz.

Caveats

Éduro documentar como as regras de conteúdo e os grupos da fonte UDP são supostos para trabalhar porque há os erros que causaram impar e o comportamento inesperado, tal como DDTS CSCec02038. Isto é específico liberar 6.10, somente sem uma regra de conteúdo e a configuração.

```
flow-state [161|162|53] udp flow-disable nat-enable
```

O pedido do retorno UDP falharia, e o CSS retornaria um ICMP não alcançável. Há um problema geral com tráfego do Balanceamento de carga UDP usando a regra de conteúdo configurada nos grupos da fonte UDP conjuntamente com uma seção da regra de conteúdo deste documento, se o pedido UDP usa a mesma porta de origem e de destino. Isto acontece o mais frequentemente com raio (a porta de origem e de destino será 1645). O CSS identifica o fluxo.

```
[ip source address|ip source port|ip dest address|ip dest port]
```

Isto é como o FCB e os mapeamentos rápidos de caminho são identificados. Quando um cliente manda pacotes de UDP usando a mesma porta de origem e de destino, são somente carga equilibrada uma vez, a primeira vez que, e traçada então no caminho rápido. A menos que o FCB obtiver o lixo recolhido, que é pelo menos 15 segundos para o UDP, todos os pedidos futuros vão ao mesmo server.

Informações Relacionadas

- Sustentação do produto dos CSS 11000 Series Content Services Switch
- Páginas de suporte dos produtos de hardware CSS11500
- Páginas de suporte do produto do software webns
- Download do software CSS11000

- Download do software CSS11500
- Suporte Técnico - Cisco Systems