明白和运用UDP、CSS 11000的内容规则和源组

目录

简介

用户数据报协议(UDP)流量是单向的。只有当UDP数据包处理时， CSS设置在一个方向的一Flow Control Block (FCB)。如果响应数据包到达，返回路径的FCB只设置。由于UDP的单向本质，源组是常用的在CSS提供UDP流的双方的之间映射。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CSS 11000/11500
- WebNS软件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

主题

UDP内容规则

UDP内容规则配置提供在服务器的一组的中负载均衡。这样，它跟需要没有不同配置TCP内容规则。内容规则是提供负载均衡。

配置

```
!************************** 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
```

客户端点击与DNS请求的Virtual IP (VIP)地址。CSS负载平衡在活动服务之间的DNS请求在规则。FCB为VIP连接的客户端设置。

UDP内容规则必须有处理对应的源组返回UDP流量。一旦DNS，这是对初始DNS请求的DNS答复。如果没有源组，从DNS服务器的答复上一步不会NAT对VIP地址，并且DNS客户端将拒绝请求。这能通过发出**show flows 0.0.0.0**命令看到。

```
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是客户端， 10.86.213.124是VIP，并且192.168.2.3是服务器。注意从服务器的回复流没有一个NAT Dst。

注意： 应该也注意第3层(L3)内容规则为相似描述的UDP工作以上。L3内容规则没有配置的协议或

端口。

```
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
```

使用此内容规则， UDP或TCP数据流能点击此VIP和装载平衡到后端服务器。

与内容规则一道的UDP源组

UDP源组用于处理UDP回程数据流。在示例中，这是对DNS请求的一DNS答复，点击内容规则dns。客户能配置组用三个不同的方式为了达到NAT UDP回程数据流。

1. 从内容规则的后端服务器可以在组内被复制。您会需要添加每组对上述配置。

   ```
   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
   ```

   使用此配置， DNS答复从dns_s1或dns_s2到达，并且源组匹配被做。这造成数据包NAT到在规则配置的VIP地址。知道是重要的源端口为什么不NAT。源组不NAT源端口，如果它是一个著名的IP端口，是端口少于1024。要概括， DNS请求点击DNS内容规则是被均衡的负载。在CSS前面是161.44.67.245:2586 - > VIP (10.86.213.124):53。在CSS和服务器之间是161.44.67.245:2586 - > dns_s1 (192.168.2.3):53。从服务器的回复上一步是Dns_s1(192.168.2.3):53 - > 161.44.67.245:2586。DNS答复匹配源组，当点击VIP的时(10.86.213.124):53 CSS - > 161.44.67.245:2586。**show flows命令**输出：

   ```
   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
   ```

   因为源端口少于1024是，并且是公认端口，源端口没有NAT，即使点击源组。仅源IP地址将NAT回到VIP地址。为了使适当地工作的这类配置：在内容规则和源组的VIP地址必须是相同的。响应数据流的源端口一定著名的。例如Radius，是端口1645。如果上述示例是一个RADIUS验证和答复对， Radius答复将有从1645 NAT的其源端口到源组端口(例如， 8192)。是可能的这将导致RADIUS请求发生故障。这是**portmap disable命令**被添加到源组的原因。
2. 从内容规则的后端服务器可以在组内被复制作为目标服务。当DNS请求自客户端时，进来目标服务允许将NAT的源IP地址以及源端口。用户配置如下所示。**注意：** 为了清晰，一个不同的VIP地址在源组上把放比内容规则的。VIP地址是10.86.213.125。这是，以便获得NAT在CSS和服务器之间不是相同的象VIP地址的源地址。在这种情况下，当DNS请求从客户端到达，时内容规则和源组匹配被做。目的IP地址将NAT到负载被平衡的服务器。由于源组通过添加目标匹配，源IP地址和源端口将NAT。在CSS前面是161.44.67.245:2644 - > VIP (10.86.213.124):53。在CSS和服务器之间是10.86.213.125:8192-> dns_s1 (192.168.2.3):53。因为源组匹配在DNS的请求时被做了， portmap条目在源组内由从服务器的DNS答复上一步创建和匹配。从服务器的回复上一步是Dns_s1(192.168.2.3):53 - > 10.86.213.125:8192。源组端口映射条目处理NAT源IP地址和客户端的初始源端口。从CSS通过的DNS答复到客户端是VIP (10.86.213.124):53 - > 161.44.67.245:2644。**show flows命令**输

出：

```
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
```

使用此配置，在内容规则的VIP能匹配源组VIP地址，但是不必须。公认端口(少于1024)限制仍然存在。目标服务配置，如果服务器需要发现客户端的实际IP地址，不应该使用。

3. 不可以有在组定义的服务，并且组为IP地址范围更喜欢通过ACL条款。

```
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
```

ACL原因语句将看起来类似于：

```
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
```

注意： 这，当客户不想要对NAT所有流量到/从某一地址时，通常使用。照此，他们能控制什么流量获得NAT。

仅NAT的UDP源组

另一使用源组与UDP流量是对从专用IP地址空间的NAT流量在CSS后对公共IP地址。在这种情况下，因为负载均衡没有要求，内容规则没有要求。UDP源组将用于NAT流量。后端服务可以添加用专用IP地址，如下面示例所显示。

```
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
```

或者，服务不可以被添加到组，并且源组可以通过ACL条款更喜欢。

```
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
```

DNS请求自后端服务器进来并且匹配源组。FCB创建，并且NAT转换完成。当DNS答复接收时，源组端口映射条目内部地创建。在回归流源组查找完成，获取的内部portmap条目，创建的FCB，并且DNS答复正确地获得NAT的上一步。

因为负载均衡没有要求，内容规则没有要求。因为使用在请求，创建的端口映射信息源组处理在答复上一步的NAT转换。

公认端口限制(少于1024)仍然被坚持。众所周知的来源端口不会NAT，但是端口大于或等于1024将NAT。

UDP配置选项

使用版本5.0， 7.10和7.20命令参数， **dnsflow [enable (event)|禁用]**是可用的。**enable (event)**是默认，并且意味着FCB为DNS流创建。**禁用**原因没有FCB创建，虽然匹配功能的内容规则和源组将是相同的。使用版本6.10， **noflow**命令功能通过配置参数被扩展了。

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

端口号对应于SIP(5060)、SNMP(161)、SNMP(162)和DNS(53)。

在**noflow后的**想法纯粹地是性能。一份UDP答复/请求协议例如DNS (SNMP和RADIUS是其他两普通一个)不得到好处从映射一FCB的CSS功能在快速路径，和实际上，开销能减速处理此种流量性能。另外，因为UDP流量是单向的并且没有终结器数据包(例如TCP RST或FIN)， UDP流通过碎片收集只删除，添加更多开销。**noflow**实施细节，然而，影响了配置要求。

版本5.0和2G CSS11500版本只有**dnsflow disable命令**参数此时。版本6.10有流**状态**配置表，能执行SNMP、SNMP陷阱和DNS UDP流的**禁用流程**。

如果**dnsflow禁用**或**禁用流程**命令发出，源组没有为示例在UDP源组中要求与一个内容规则或UDP源组一道NAT的此的仅部分文档。当**noflow**命令发出时，内部源组没有用于记录流数据包，并且此内部端口映射条目，没有关联与任何已配置的源组，因而处理回程数据流。

提供此信息是尽量详细的。BU，然而，建议源组在没有流事例配置。这是一致在流和**noflow**配置之间，并且源组允许用户发现命中计数器，内部一个不。

警告

描述是难UDP内容规则和源组如何应该工作，因为有引起了多和意外行为的Bug，例如DDTS CSCec02038。这是仅特定对版本6.10，没有内容规则和配置。

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

返回UDP请求将发生故障，并且CSS将返回ICMP不可达的。如果UDP请求使用同一源及目的地端口，有与负载均衡UDP流量的一一般问题使用在UDP源组中配置的内容规则与本文的内容规则部分一道。这经常发生与Radius (源及目的地端口将是1645)。CSS识别流。

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

这是FCB和fastpath映射如何识别。使用同一源及目的地端口时，当客户端派出UDP数据包，他们是在快速路径一次被均衡，第一次，然后映射的仅负载。除非FCB获得垃圾收集，是UDP的至少15秒，所有将来请求去同一个服务器。

相关信息

- CSS 11000系列内容服务交换机产品支持
- CSS11500硬件产品支持页面
- WebNS软件产品支持页
- CSS 11000软件下载
- CSS11500软件下载
- 技术支持 - Cisco Systems