Понимание и иримененение UDP, Content Rules и Source Groups на CSS 11000

Содержание

Введение

Трафик Протокола UDP однонаправлен. CSS устанавливает Блок управления потоками (FCB) в одном направлении, только когда обработан пакет UDP. Если ответный пакет поступает, FCB для адреса возврата только установлен. Из-за однонаправленности UDP исходные группы часто используются на CSS для обеспечения сопоставления между двумя сторонами потока UDP.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- CSS 11000/11500
- Программное обеспечение webns

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить

потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Темы

Правила содержимого UDP

Правило содержимого UDP настроено для обеспечения распределения нагрузки среди группы серверов. Таким образом это является не другим, чем необходимость настроить правило содержимого TCP. Правило содержимого должно предоставить распределение нагрузки.

!--- конфигурацию

```
************************** 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
```

Клиент поражает Виртуальное IP (VIP) адрес с запросом DNS. CSS балансирует нагрузку запроса DNS между активными сервисами на правиле. FCB установлен для клиента к подключению VIP.

Правило содержимого UDP должно иметь соответствующую исходную группу для обработки трафика UDP return. В случае DNS это - DNS - ответ к начальному запросу DNS. Если у вас не будет исходной группы, то ответ назад от сервера DNS не будет преобразован

посредством NAT к адресу VIP, и DNS - клиент отклонит запрос. Это может быть замечено путем запуска **команды show flows 0.0.0.0**.

```
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 клиент, 10.86.213.124 VIP, и 192.168.2.3 сервер. Заметьте, что ответ вытекает из сервера, не имеет `NAT Dst Address`.

Примечание: Нужно также обратить внимание, что Уровень 3 (L3) правило содержимого работает для UDP, таким же образом описанного выше. Правило содержимого L3 не имеет протокола или порта настроенными.

```
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
```

С этим правилом содержимого или UDP или Трафик TCP могут поразить этот VIP и балансировку нагрузки к конечному серверу.

Исходные группы UDP в сочетании с правилом содержимого

Исходная группа UDP используется для обработки ответного трафика UDP. В примере это - DNS - ответ к запросу DNS, которые поражают правило содержимого `dns`. Клиент может настроить группу тремя другими способами для достижения ответного трафика UDP преобразования посредством NAT.

1. Конечные серверы от правила содержимого могут быть дублированы в группе. Необходимо было бы добавить группу к вышеупомянутой конфигурации.

   ```
   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
   ```

   С этой конфигурацией DNS - ответ поступает от `dns_s1` или `dns_s2` , и соответствие исходной группы сделано. Это заставляет пакет быть преобразованным посредством NAT к адресу VIP, настроенному на правиле. Важно понять, почему исходный порт не будет преобразованным посредством NAT. Исходные группы не будут NAT исходный порт, если это будет известный порт IP, которые являются портами меньше чем 1024.Для резюме запрос DNS поражает правило содержимого DNS, чтобы быть с балансировкой нагрузки. Перед CSS 161.44.67.245:2586-> VIP (10.86.213.124):53. Между CSS и сервером 161.44.67.245:2586-> dns_s1 (192.168.2.3):53. Ответом назад от сервера является Dns_s1 (192.168.2.3):53-> 161.44.67.245:2586. DNS - ответ совпадает с исходной группой, когда это поражает CSS для VIP (10.86.213.124):53-> 161.44.67.245:2586.Команда **show flows** вывела:

   ```
   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
```
Так как исходный порт - меньше чем 1024 и является известным портом, исходный порт не преобразован посредством NAT, даже при том, что это поразило исходную группу. Только IP - адрес источника будет преобразованной посредством NAT спиной к адресу VIP.Для данного типа конфигурации для работы должным образом:Адрес VIP на правиле содержимого и исходной группе должен быть тем же.Исходный порт на ответном трафике должен быть известным. Например, Радиус, который является портом 1645. Если бы вышеупомянутым примером была пара Проверки подлинности RADIUS и ответа, то ответ Радиуса имел бы свой исходный порт преобразованным посредством NAT с 1645 к порту исходной группы (например, 8192). Вероятно, что это заставило бы Запрос RADIUS отказывать. Это - причина, что **команда portmap disable** была добавлена к исходной группе.

2. Конечные серверы от правила содержимого могут быть дублированы в группе как целевые сервисы. Когда запрос DNS входит от клиента, целевой сервис обеспечивает IP - адрес источника, а также исходный порт, чтобы быть преобразованным посредством NAT. Конфигурацию заказчика показывают ниже.**Примечание:** Для ясности другой адрес VIP помещен на исходную группу, чем на правиле содержимого. Адрес VIP 10.86.213.125. Это - то, так, чтобы адрес источника, который становится преобразованным посредством NAT между CSS и сервером, не был тем же как адресом VIP.В этом случае, когда запрос DNS поступает от клиента, и правило содержимого и соответствие исходной группы сделаны. IP - адрес назначения будет преобразован посредством NAT к серверу с балансировкой нагрузки. Поскольку с исходной группой совпали через добавить назначение, и IP - адрес источника и исходный порт будут преобразованы посредством NAT. Перед CSS 161.44.67.245:2644-> VIP (10.86.213.124):53. Между CSS и сервером 10.86.213.125:8192-> dns_s1 (192.168.2.3):53.Так как соответствие исходной группы было сделано во время запроса DNS, запись Portmap в исходной группе была создана и совпадается DNS - ответом назад от сервера. Ответом назад от желания сервера является Dns_s1 (192.168.2.3):53-> 10.86.213.125:8192.Запись схемы порта исходной группы обрабатывает преобразование посредством NAT IP - адрес источника и первый исходный порт клиента. DNS - ответ, который передают от CSS до клиента, является VIP (10.86.213.124):53-> 161.44.67.245:2644.Команда **show flows** вывела:
```
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
```
С этой конфигурацией VIP на правиле содержимого может совпасть с адресом VIP исходной группы, но это не имеет к. Известный порт (меньше чем 1024) ограничение все еще существует. Если сервер должен видеть реальный IP - адрес клиента, конфигурация целевого сервиса не должна использоваться.

3. Может быть no service, определенный на группе, и группа предпочтена для диапазона IP-адресов с помощью выражения 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
```
Оператор причины ACL выглядел бы подобным:
```
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
```
Примечание: Когда клиент не хочет к NAT весь трафик к или от определенного адреса, это обычно используется. Этим способом они могут управлять тем, какой трафик становится преобразованным посредством NAT.

Исходные группы UDP для NAT только

Другое использование исходных групп с трафиком UDP к трафику NAT от пространства закрытого IP - адреса позади CSS к открытым IP - адресам. В этом случае никакое правило содержимого не требуется, потому что не требуется никакое распределение нагрузки. Исходная группа UDP будет использоваться только к NAT трафик. Вспомогательные сервисы могут быть добавлены с закрытыми IP - адресами, как показано в примере ниже.

```
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
```
Или, no service могут быть добавлены к группе, и исходная группа может быть предпочтена с помощью выражения 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
```
Запрос DNS входит от конечного сервера и совпадает с исходной группой. FCB создан, и преобразование NAT сделано. Когда DNS - ответ получен, запись сопоставителя портов исходной группы была внутренне создана. На потоке return поиск исходной группы сделан, полученная запись внутреннего зеркала портов, FCB, созданный, и DNS - ответ получает преобразованную посредством NAT спину правильно.

Никакое правило содержимого не требуется, потому что не требуется никакое распределение нагрузки. Исходная группа обрабатывает преобразование NAT на ответе назад, потому что это использует сведение о зеркале портов, созданное на запросе.

Ограничение известного порта (меньше чем 1024) все еще придерживаются к. Порт хороша известного источник не будет преобразован посредством NAT, но порты, больше, чем, или равняться 1024, будет преобразовано посредством NAT.

Параметры конфигурации UDP

С версиями 5.0, 7.10, и 7.20 параметр командной строки, **dnsflow [enable|disable]** доступен. **включите** по умолчанию и означает, что FCB создан для потоков DNS. **отключите** не заставляет FCB быть созданным, хотя правило содержимого и функции соответствия исходной группы будут тем же. С выпуском 6.10 **возможности команды noflow** были расширены через параметр конфигурации.

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

Номера портов соответствуют SIP (5060), SNMP (161), SNMP (162), и DNS (53).

Идея позади **noflow** была просто производительностью. Ответ UDP / протокол запроса, такой как DNS (SNMP и RADIUS являются двумя другими общими) не получает выгоды от функции CSS сопоставления FCB в fastpath, и фактически, издержки могут замедлить производительность обработки этого типа трафика. Кроме того, так как трафик UDP однонаправлен и не имеет никакого пакета разделителя (такого как RST TCP или FIN), поток UDP только удален через сбор мусора, который добавляет больше издержек. Сведения о внедрении **noflow**, однако, произвели конфигурационные требования.

CSS 11500 версий 5.0 и 2G освобождает, только имеют **dnsflow, отключают** параметр командной строки в это время. Выпуск 6.10 имеет таблицу конфигурации **состояния потоком**, которая может сделать **поток - отключает** для SNMP, trap-сообщений SNMP и потоков UDP DNS.

Если **команды dnsflow отключают или flow-disable** были выполнены, исходная группа не требуется для примеров в Исходных группах UDP в сочетании с Правилом содержимого или Исходных группах UDP для преобразования посредством NAT Только разделы этого документа. Когда **команда noflow** выполнена, группа внутреннего ресурса используется, чтобы не отслеживать пакеты потока, и таким образом эта внутренняя запись сопоставления портов, которая не привязана ни к какой настроенной исходной группе, обрабатывает ответный трафик.

Эта информация предоставлена, чтобы быть максимально подробной. BU, однако, рекомендует, чтобы исходная группа не была настроена ни в каких случаях потока. Это должно быть последовательно между потоком и **беспотоковыми конфигурациями**, и также исходная группа позволяет пользователю видеть счетчики попаданий, которые не делает внутренний.

Предупреждения

Трудно к документу, как правила содержимого UDP и исходные группы, как предполагается, работают, потому что существуют дефекты, которые вызвали нечетный и неожиданное поведение, такое как DDTS CSCec02038. Это является определенным для Выпуска 6.10, только без правила содержимого и конфигурации.

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

Запрос UDP return отказал бы, и CSS возвратит сообщение о недоступности ICMP. Если запрос UDP использует тот же порт источника и порт назначения, существует общая проблема с распределением нагрузки трафика UDP с помощью правила содержимого, настроенного в Исходных группах UDP в сочетании с разделом Правила содержимого этого документа. Это происходит чаще всего с Радиусом (порт источника и порт назначения будет 1645). CSS определяет поток.

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

Это - то, как определены FCB и отображения прямого выбора. Когда клиент отсылает пакеты UDP с помощью того же порта источника и порт назначения, они только с балансировкой нагрузки однажды, первоначально, и затем сопоставленный в fastpath. Пока FCB не собран "мусор", который составляет по крайней мере 15 секунд для UDP, все будущие запросы переходят к тому же серверу.

Дополнительные сведения

- Поддержка продуктов коммутаторов контент-сервисов CSS 11000
- Страницы технической поддержки аппаратного продукта CSS 11500
- Страницы технической поддержки продукта программного обеспечения webns
- Загрузка программного обеспечения CSS 11000
- Загрузка программного обеспечения CSS 11500
- Техническая поддержка - Cisco Systems