

Entendiendo y aplicando el UDP, las reglas de contenido, y a los grupos fuente en el CSS11000

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Temas](#)

[Reglas de contenido UDP](#)

[Grupos fuente UDP conjuntamente con una regla de contenido](#)

[Grupos fuente UDP para el NAT solamente](#)

[Opciones de configuración UDP](#)

[Advertencias](#)

[Información Relacionada](#)

[Introducción](#)

El tráfico del User Datagram Protocol (UDP) es unidireccional. El CSS configura un bloque del control de flujo (FCB) en una dirección, sólo cuando se procesa un paquete UDP. El FCB para el trayecto de retorno se configura solamente si llega el paquete de respuesta. Debido a la naturaleza unidireccional del UDP, los grupos fuente son de uso frecuente en el CSS proporcionar la asignación entre los dos lados del flujo UDP.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CSS 11000/11500
- Software de WebNS

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando,

asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

Temas

Reglas de contenido UDP

Se configura una regla de contenido UDP para proporcionar el Equilibrio de carga entre un grupo de servidores. De esta manera, es no diferente que necesitando configurar una regla de contenido TCP. La regla de contenido es proporcionar el Equilibrio de carga.

Configuración

```
***** 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
```

El cliente golpea IP virtual el direccionamiento (VIP) con una petición DNS. La carga CSS equilibra la petición DNS entre los servicios activos en la regla. Un FCB se configura para el cliente a la conexión VIP.

Una regla de contenido UDP debe tener un grupo fuente correspondiente para manejar el tráfico de la vuelta UDP. En el caso del DNS, ésta es la respuesta de DNS a la petición inicial DNS. Si usted no tiene un grupo fuente, la respuesta detrás del servidor DNS no será NATed al direccionamiento VIP, y el cliente DNS rechazará la petición. Esto puede ser vista publicando el

comando de 0.0.0.0 del 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 es el cliente, 10.86.213.124 es el VIP, y 192.168.2.3 es el servidor. Note que el flujo de la contestación del servidor no tiene un direccionamiento del dst NAT.

Nota: Debe también ser observado que una regla de contenido de la capa 3 (L3) trabaja para el UDP descrito de manera semejante arriba. Una regla de contenido L3 no tiene el protocolo ni viró hacia el lado de babor 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
```

Con esta regla de contenido, o el UDP o tráfico TCP puede golpear este VIP y equilibrio de la carga a un servidor de extremo posterior.

[Grupos fuente UDP conjuntamente con una regla de contenido](#)

Utilizan a un grupo fuente UDP para manejar el tráfico de retorno UDP. En el ejemplo, esto es una respuesta de DNS a la petición DNS, que golpeó la regla de contenido `dns`. Un cliente puede configurar al grupo en tres maneras diferentes para alcanzar el tráfico de retorno del NATing UDP.

1. Los servidores de extremo posterior de la regla de contenido pueden ser duplicados dentro del grupo. Usted necesitaría agregar a un grupo a la configuración antedicha.

```
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
```

Con esta configuración, la respuesta de DNS llega del `dns_s1` o de `dns_s2`, y se hace la coincidencia del grupo fuente. Esto hace el paquete ser NATed al direccionamiento VIP configurado en la regla. Es importante entender porqué el puerto de origen no va a ser NATed. Los grupos fuente no NAT el puerto de origen si es un puerto bien conocido IP, que son puertos menos de 1024. Para recapitular, la petición DNS golpea la regla de contenido DNS para ser carga equilibrada. Delante del CSS es 161.44.67.245:2586 - > VIP (10.86.213.124):53. Entre el CSS y el servidor es 161.44.67.245:2586 - > el `dns_s1` (192.168.2.3):53. La contestación detrás del servidor es `Dns_s1`(192.168.2.3):53 - > 161.44.67.245:2586. La respuesta de DNS hace juego al grupo fuente cuando golpea el CSS para VIP (10.86.213.124):53 - > 161.44.67.245:2586. El comando `show flows` hecho salir:

```
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 Puesto que el puerto de origen es menos de 1024, y es un puerto conocido, el puerto de origen no es NATed, aunque golpeó a un grupo fuente. Solamente la dirección IP de origen será NATed de nuevo al direccionamiento VIP. Para que este tipos de configuración trabajen correctamente: El direccionamiento VIP en la regla de contenido y el grupo fuente debe ser lo mismo. El puerto de origen en el tráfico de respuesta debe ser bien sabido. Por ejemplo radio, que es el puerto 1645. Si el ejemplo antedicho fuera un par de la autenticación de RADIUS y de la respuesta, la respuesta del radio tendría su NATed del puerto de origen a partir de 1645 a un puerto del grupo fuente (por ejemplo, 8192). Es probable esto causaría el pedido de RADIUS de fallar. Ésta es la razón que agregaron al **comando disable del portmap al grupo fuente**.

2. Los servidores de extremo posterior de la regla de contenido pueden ser duplicados dentro del grupo como servicios de destino. El servicio de destino tiene en cuenta para que la dirección IP de origen así como el puerto de origen sean NATed cuando la petición DNS viene adentro del cliente. La configuración del cliente se muestra abajo. **Nota:** Para mayor claridad, un diverso direccionamiento VIP se pone en el grupo fuente que en la regla de contenido. El direccionamiento VIP es 10.86.213.125. Esto es de modo que la dirección de origen que consigue el NATed entre el CSS y el servidor no sea lo mismo que el direccionamiento VIP. En este caso, cuando la petición DNS llega del cliente, se hacen la regla de contenido y la coincidencia del grupo fuente. El IP Address de destino será NATed al servidor equilibrado carga. Porque correspondieron con al grupo fuente vía el destino del agregar, la dirección IP de origen y el puerto de origen serán NATed. Delante del CSS es 161.44.67.245:2644 -> VIP (10.86.213.124):53. Entre el CSS y el servidor es el dns_s1 10.86.213.125:8192-> (192.168.2.3):53. Puesto que la coincidencia del grupo fuente fue hecha a la hora de la petición DNS, la entrada de portmap dentro del grupo fuente fue creada, y es correspondida con por la respuesta de DNS detrás del servidor. La contestación detrás del servidor es Dns_s1(192.168.2.3):53 -> 10.86.213.125:8192. La entrada del mapa del puerto del grupo fuente dirige el NATing la dirección IP de origen y el puerto de fuente original del cliente. La respuesta de DNS pasajera del CSS al cliente es VIP (10.86.213.124):53 -> 161.44.67.245:2644. **El comando show flows** hecho salir:

```
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 Con esta configuración, el VIP en la regla de contenido puede hacer juego el direccionamiento del grupo fuente VIP pero no hace tuvo que. La restricción del puerto conocido (menos de 1024) todavía existe. La configuración del servicio de destino no debe ser utilizada si el servidor necesita ver el IP Address real del cliente.

3. No puede haber servicio definido en el grupo, y prefieren al grupo para un rango de los IP Addresses vía una 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 La declaración de la causa ACL parecería 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: Esto se utiliza generalmente cuando el cliente no quiere al NAT todo el tráfico a o desde cierto direccionamiento. De este modo, pueden controlar lo que consigue el tráfico a NATed.

Grupos fuente UDP para el NAT solamente

Otro uso de los grupos fuente con el tráfico UDP está al tráfico NAT del espacio de IP Address privado detrás del CSS a los IP Address públicos. En este caso, no se requiere ninguna regla de contenido porque no se requiere ningún Equilibrio de carga. Utilizarán al grupo fuente UDP simplemente al NAT el tráfico. Los servicios de extremo posterior pueden ser agregados con los IP Address privados, tal y como se muestra en del ejemplo abajo.

```
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, ningunos servicios pueden ser agregados al grupo, y el grupo fuente puede ser preferido vía una 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
```

La petición DNS viene adentro del servidor de extremo posterior y hace juego al grupo fuente. Se crea El FCB y se hace la transformación de NAT. La entrada del mapeo de puerto del grupo fuente internamente fue creada cuando se recibe la respuesta de DNS. En el flujo de vuelta se hacen las operaciones de búsqueda del grupo fuente, la entrada de portmap interna extraída, el FCB creado, y la respuesta de DNS consigue la parte posterior del NATed correctamente.

No se requiere ninguna regla de contenido porque no se requiere ningún Equilibrio de carga. El grupo fuente maneja la transformación de NAT en la respuesta detrás porque utiliza la información de portmapper creada en la petición.

La restricción del puerto conocido (menos de 1024) todavía se adhiere. Un puerto de la fuente conocida no será NATed, sino vira mayor o igual 1024 hacia el lado de babor será NATed.

Opciones de configuración UDP

Con las versiones 5.0, 7.10, y 7.20 el comando parameter, **dnsflow [permiso|la neutralización]** está disponible. **el permiso** es el valor por defecto, y significa que el FCB está creado para los flujos DNS. **la neutralización** no hace ningún FCB ser creada aunque la regla de contenido, y las funciones que corresponden con del grupo fuente serán lo mismo. Con la versión 6.10, **la operatividad del comando noflow** era extendido vía el parámetro de la configuración.

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

Los números del puerto corresponden a SIP(5060), a SNMP(161), a SNMP(162), y a DNS(53).

La idea detrás del **noflow** era puramente funcionamiento. Una respuesta UDP/un protocolo de la petición tal como DNS (el SNMP y el RADIUS son dos otros unos comunes) no gana ninguna ventaja de la función CSS de asociar un FCB en el fastpath, y de hecho, los gastos indirectos puede retrasar el funcionamiento de procesar este tipo de tráfico. Además, puesto que el tráfico UDP es unidireccional y no tiene ningún paquete exterminador (tal como el TCP RST o FIN), el flujo UDP se borra solamente vía la acumulación de basura, que agrega más gastos indirectos. Los detalles de instrumentación del **noflow**, sin embargo, han efectuado los requisitos para la configuración.

Las versiones 5.0 y las versiones 2G CSS11500 tienen solamente el parámetro de **comando disable del dnsflow** ahora. La versión 6.10 tiene la Tabla de configuración del flujo-estado, que puede hacer la flujo-**neutralización** para el SNMP, SNMP traps, y fluye el DNS UDP.

No requieren al grupo fuente para los ejemplos en los grupos fuente UDP conjuntamente con una regla de contenido o los grupos fuente UDP para las secciones del NATing solamente de esto documento si se han publicado los comandos de la **neutralización** o de la flujo-**neutralización del dnsflow**. Cuando se publica el comando del **noflow**, utilizan a un grupo de la fuente interna para no no perder de vista el ningún paquete del flujo, y esta entrada interna del mapeo de puerto, que no se asocia a cualquier grupo fuente configurado, maneja así el tráfico de retorno.

Esta información se proporciona para ser lo más detallada. El BU, sin embargo, recomienda que configuren al grupo fuente en los ningunos casos del flujo. Éste es ser constante entre el flujo y las **configuraciones noflow**, y también el grupo fuente permite que el usuario considere a los contadores de aciertos, que no lo hace el interno.

[Advertencias](#)

Es duro documentar cómo suponen las reglas de contenido y a los grupos fuente UDP para trabajar porque hay los bug que han causado impar y la conducta inesperada, tal como DDTS [CSCec02038](#). Esto es específico liberar 6.10, solamente sin una regla de contenido y la configuración.

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

La petición de la vuelta UDP fallaría, y el CSS volvería un ICMP fuera de alcance. Hay un problema general con el tráfico del Equilibrio de carga UDP usando la regla de contenido configurada en los grupos fuente UDP conjuntamente con una sección de la regla de contenido de este documento, si la petición UDP utiliza el mismo puerto de origen y de destino. Esto sucede lo más a menudo posible con el radio (el puerto de origen y de destino será 1645). El CSS identifica el flujo.

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

Éste es cómo se identifican el FCB y los mapeos de trayectos rápidos. Cuando un cliente envía los paquetes UDP usando el mismo puerto de origen y de destino, son solamente carga equilibrada una vez, la primera vez que, y después asociada en el fastpath. A menos que el FCB consiga la basura recogida, que es por lo menos 15 segundos para el UDP, todas las peticiones futuras van al mismo servidor.

Información Relacionada

- [Soporte de productos de los CSS 11000 Series Content Services Switch](#)
- [Páginas de soporte del producto de hardware CSS11500](#)
- [Páginas de soporte del producto de software de WebNS](#)
- [Descarga del software CSS11000](#)
- [Descarga del software CSS11500](#)
- [Soporte Técnico - Cisco Systems](#)