Présentation et application d'UDP, des règles de contenu et des groupes source sur CSS 11000

Contenu

Introduction

Le trafic de Protocole UDP (User Datagram Protocol) est unidirectionnel. Le CSS a installé un bloc de contrôle de flux (FCB) dans une direction, seulement quand un paquet UDP est traité. Le FCB pour le chemin de retour est seulement installé si le paquet de réponse arrive. En raison de la nature unidirectionnelle de l'UDP, les groupes sources sont employés souvent sur le CSS pour fournir le mappage entre les deux côtés de l'écoulement d'UDP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CSS 11000/11500
- Logiciel de WebNS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Thèmes

Règles de contenu d'UDP

Une règle de contenu d'UDP est configurée de fournir l'Équilibrage de charge parmi un groupe de serveurs. De cette façon, il n'est pas différent que devant configurer une règle de contenu de TCP. La règle de contenu est de fournir l'Équilibrage de charge.

Configuration

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

Le client frappe l'adresse virtuelle IP (VIP) avec une demande de DN. Le CSS équilibrent la charge la demande de DN entre les services actifs sur la règle. Un FCB est installé pour le client à la connexion de VIP.

Une règle de contenu d'UDP doit avoir un groupe source correspondant pour traiter le trafic UDP de retour. Dans le cas des DN, c'est la réponse de DN à la demande initiale de DN. Si vous n'avez pas un groupe source, la réponse de retour du serveur DNS ne sera pas NATed à l'adresse de VIP, et le client DNS rejettera la demande. Ceci peut être vu en émettant la commande de **0.0.0.0**

d'écoulements d'exposition.

```
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 est le client, 10.86.213.124 est le VIP, et 192.168.2.3 est le serveur. Notez que l'écoulement de réponse du serveur n'a pas une `adresse NAT de Dst`.

Remarque: Il devrait également noter qu'une règle de contenu de la couche 3 (L3) fonctionne pour l'UDP de la même manière décrit ci-dessus. Une règle de contenu L3 n'a pas le protocole ou met en communication configuré.

```
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
```

Avec cette règle de contenu, l'UDP ou le trafic TCP peut frapper ce VIP et équilibrer la charge à un serveur principal.

Groupes sources d'UDP en même temps qu'une règle de contenu

Un groupe source d'UDP est utilisé pour traiter le trafic de retour d'UDP. Dans l'exemple, c'est une réponse de DN à la demande de DN, qui a frappé des `dn de` règle de contenu. Un client peut configurer le groupe de trois manières différentes afin de réaliser le trafic de retour d'UDP de NATing.

1. Les serveurs principaux de la règle de contenu peuvent être reproduits dans le groupe. Vous devriez ajouter un groupe à la configuration ci-dessus.

   ```
   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
   ```

   Avec cette configuration, la réponse de DN arrive de `dns_s1` ou de `dns_s2`, et la correspondance de groupe source est faite. Ceci entraîne le paquet être NATed à l'adresse de VIP configurée sur la règle. Il est important de comprendre pourquoi le port de source ne va pas être NATed. Les groupes sources pas NAT le port de source si c'est un port réputé IP, qui sont des ports moins de 1024.Pour récapituler, les DN demandent des hit que la règle de contenu de DN d'être chargement a équilibrés. Devant le CSS est 161.44.67.245:2586 - > le VIP (10.86.213.124):53. Entre le CSS et le serveur est 161.44.67.245:2586 - > dns_s1 (192.168.2.3):53. La réponse de retour du serveur est Dns_s1(192.168.2.3):53 - > 161.44.67.245:2586. La réponse de DN concurrence le groupe source quand elle frappe le CSS pour le VIP (10.86.213.124):53 - > 161.44.67.245:2586.**L'exposition circule la** sortie de commande :

   ```
   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
```
Puisque le port de source est moins de 1024, et est un port connu, le port de source n'est pas NATed, quoiqu'il ait frappé un groupe source. Seulement l'adresse IP source sera NATed de nouveau à l'adresse de VIP.Pour ce type de configuration à fonctionner correctement :L'adresse de VIP sur la règle de contenu et le groupe source doit être identique.Le port de source sur le trafic de réponse doit être réputé. Par exemple rayon, qui est le port 1645. Si l'exemple ci-dessus était une paire d'authentification et de réponse de rayon, la réponse de rayon aurait son port NATed de source à partir de 1645 à un port de groupe source (par exemple, 8192). Il est probable ceci entraînerait la demande RADIUS d'échouer. C'est la raison pour laquelle la commande de **débronchement de portmap** a été ajoutée au groupe source.

2. Les serveurs principaux de la règle de contenu peuvent être reproduits dans le groupe comme services de destination. Le service de destination tient compte pour que l'adresse IP source aussi bien que le port de source soit NATed quand la demande de DN entre du client. La configuration de client est affichée ci-dessous.**Remarque:** Pour la clarté, une adresse différente de VIP est mise sur le groupe source que sur la règle de contenu. L'adresse de VIP est 10.86.213.125. C'est de sorte que l'adresse source qui obtient NATed entre le CSS et le serveur ne soit pas identique que l'adresse de VIP.Dans ce cas, quand la demande de DN arrive du client, la règle de contenu et la correspondance de groupe source sont faites. L'adresse IP de destination sera NATed au serveur équilibré par chargement. Puisque le groupe source a été concurrencé par l'intermédiaire de la destination d'ajouter, l'adresse IP source et le port de source seront NATed. Devant le CSS est 161.44.67.245:2644 - > le VIP (10.86.213.124):53. Entre le CSS et le serveur est 10.86.213.125:8192-> dns_s1 (192.168.2.3):53.Puisque la correspondance de groupe source a été faite au moment de la demande de DN, l'entrée de portmap au sein du groupe source a été créée, et est appariée par le dos de réponse de DN du serveur. La réponse de retour du serveur est Dns_s1(192.168.2.3):53 - > 10.86.213.125:8192.Les traitements NATing d'entrée de mappage de port de groupe source l'adresse IP source et la source d'origine du client mettent en communication. La réponse de DN passée du CSS au client est le VIP (10.86.213.124):53 - > 161.44.67.245:2644.**L'exposition circule la** sortie de commande :
```
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
```
Avec cette configuration, le VIP sur la règle de contenu peut apparier l'adresse de VIP de groupe source mais elle ne fait pas doit. La restriction de port connu (moins de 1024) existe toujours. La configuration de service de destination ne devrait pas être utilisée si le serveur doit voir la vraie adresse IP du client.

3. Il ne peut y avoir aucun service défini sur le groupe, et le groupe est préféré pour une plage des adresses IP par l'intermédiaire d'une clause d'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 déclaration de cause d'ACL semblerait semblable à :
```
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
```

Remarque: Ceci est habituellement utilisé quand le client ne veut pas à NAT tout le trafic à ou d'une certaine adresse. De cette manière, ils peuvent contrôler quel trafic obtient NATed.

Groupes sources d'UDP pour NAT seulement

Une autre utilisation des groupes sources avec le trafic UDP est au trafic NAT de l'espace adresse d'adresse IP privée derrière le CSS aux adresses IP publique. Dans ce cas, aucune règle de contenu n'est exigée parce qu'aucun Équilibrage de charge n'est exigé. Le groupe source d'UDP sera utilisé simplement à NAT le trafic. Les services principaux peuvent être ajoutés avec les adresses IP privées, suivant les indications de l'exemple ci-dessous.

```
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, aucun services ne peut être ajouté au groupe, et le groupe source peut être préféré par l'intermédiaire d'une clause d'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 demande de DN entre du serveur principal et concurrence le groupe source. Le FCB est créé et la transformation NAT est faite. L'entrée de portmapper de groupe source a été intérieurement créée quand la réponse de DN est reçue. Sur l'écoulement de retour la consultation de groupe source est faite, l'entrée interne de portmap récupérée, le FCB créé, et la réponse de DN obtient le dos de NATed correctement.

Aucune règle de contenu n'est exigée parce qu'aucun Équilibrage de charge n'est exigé. Le groupe source manipule la transformation NAT sur la réponse de retour parce qu'il utilise les informations de portmapper créées sur la demande.

La restriction de port connu (moins de 1024) encore. Un port réputé de source ne sera pas NATed, mais met en communication supérieur ou égal à 1024 sera NATed.

Options de configuration d'UDP

Avec des versions 5.0, 7.10, et 7.20 le paramètre de commande, **dnsflow [enable|le débronchement]** est disponible. **l'enable** est le par défaut, et signifie que le FCB est créé pour des écoulements de DN. **le débronchement** ne cause aucun FCB d'être créé bien que la règle de contenu, et les fonctions assorties de groupe source soient identique. Avec la version 6.10, la fonctionnalité de commande de **noflow** a été étendue par l'intermédiaire du paramètre de configuration.

flow-state [5060|161|162|53] udp [flow-disable|flow-enable][nat-disable|nat-enable]
Les numéros de port correspondent à SIP(5060), à SNMP(161), à SNMP(162), et à DNS(53).

L'idée derrière le **noflow** était purement représentation. Une réponse d'UDP/protocole de demande tel que des DN (le SNMP et le RAYON sont deux autres ceux communs) ne gagne aucun avantage de la fonction CSS de tracer un FCB dans le fastpath, et en fait, le temps système peut ralentir la représentation de traiter ce type de trafic. En outre, puisque le trafic UDP est unidirectionnel et n'a aucun paquet de Terminator (tel que le TCP RST ou la FIN), l'écoulement d'UDP est seulement supprimé par l'intermédiaire du nettoyage de la mémoire, qui ajoute plus de temps système. Les détails d'implémentation de **noflow**, cependant, ont effectué les configurations requises.

Les versions 5.0 et les versions 2G CSS 11500 ont seulement le paramètre de commande de **débronchement de dnsflow** à ce moment. La version 6.10 a la table de configuration d'écoulement-**état**, qui peut faire l'écoulement-**débronchement** pour le SNMP, des déroutements SNMP, et UDP de DN circule.

Le groupe source n'est pas prié pour les exemples aux groupes sources d'UDP en même temps qu'une règle de contenu ou des groupes sources d'UDP pour des sections de NATing seulement de ce document si les commandes de **débronchement** ou d'écoulement-**débronchement de dnsflow** ont été émises. Quand la commande de **noflow** est émise, un groupe source interne est utilisé pour ne maintenir l'aucun paquet d'écoulement, et cette entrée interne de portmapper, qui n'est pas associée avec tout groupe source configuré, traite ainsi le trafic de retour.

Ces informations sont fournies pour être le puis détaillé possible. Le BU, cependant, recommande que le groupe source soit configuré dans les aucun cas d'écoulement. C'est d'être cohérent entre l'écoulement et les configurations de **noflow**, et également le groupe source permet à l'utilisateur pour voir les compteurs de hit, que les internes ne font pas.

Mises en garde

Il est difficile de documenter comment des règles de contenu et les groupes sources d'UDP sont censés fonctionner parce qu'il y a des bogues qui ont entraîné impair et le comportement inhabituel, tel que DDTS CSCec02038. C'est spécifique à la version 6.10, seulement sans règle de contenu et configuration.

flow-state [161|162|53] udp flow-disable nat-enable
La demande de retour d'UDP échouerait, et le CSS renverrait un ICMP inaccessible. Il y a un problème d'ordre général avec le trafic UDP d'Équilibrage de charge utilisant la règle de contenu configurée aux groupes sources d'UDP en même temps qu'une section de règle de contenu de ce document, si la demande d'UDP utilise la mêmes source et destination port. Ceci se produit le plus souvent avec le rayon (la source et la destination port seront 1645). Le CSS identifie l'écoulement.

[ip source address|ip source port|ip dest address|ip dest port]
C'est comment les mappages FCB et de fastpath sont identifiés. Quand un client envoie des paquets UDP utilisant la mêmes source et destination port, ils sont seulement chargement équilibré une fois, la première fois que, et alors tracé dans le fastpath. À moins que le FCB obtienne les déchets collectés, qui sont au moins de 15 secondes pour l'UDP, toutes les futures demandes vont au même serveur.

Informations connexes

- Support de produit de Commutateurs de services satisfaits de gamme 11000 CSS
- Pages de support de produit matériel CSS 11500
- Pages de support de logiciel de WebNS
- Téléchargement logiciel CSS 11000
- Téléchargement logiciel CSS 11500
- Support technique - Cisco Systems