CSS 11000 での UDP、コンテンツ ルール、およびソース グループに関する説明と適用

目次

概要

ユーザ データグラム プロトコル（UDP）のトラフィックは単方向です。 CSS は UDP パケットが処理される場合にのみ、1 方向の Flow Control Block（FCB）を設定します。 リターン パスの FCB は、応答パケットが着信した場合にだけ設定されます。 UDP の単方向性質のため、UDP フローの両側間をマッピングするために CSS ではしばしば送信元グループが使用されます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- CSS 11000/11500
- WebNS ソフトウェア

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

トピック

UDP コンテンツルール

UDP コンテンツルールはサーバのグループの中のロード バランシングを提供するために設定されます。 このように、それは TCP コンテンツルールを設定する必要がありますと異なって。 コンテンツルールはロード バランシングを提供することです。

設定

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

クライアントは DNS 要求の Virtual IP （ VIP ）アドレスを見つけます。 CSS ロードはルールのアクティブなサービス間の DNS 要求のバランスをとります。 FCB は VIP 接続へのクライアントのために設定されます。

UDP コンテンツルールは戻り UDP トラフィックを処理する対応するソースグループがなければなりません。 DNS の場合には、これは最初の DNS 要求への DNS 応答です。 ソースグループを持たない場合、応答は VIP アドレスに DNSサーバからネットワークアドレス交換されないし、DNS クライアントは要求を拒否します。 これは **show flows 0.0.0.0** コマンドの発行によって見られる場合があります。

```
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 はクライアントです、10.86.213.124 は VIP であり、192.168.2.3 はサーバです。 サーバからの応答フローに NAT Dst ないことに注意して下さい。

注: レイヤ3（L3）コンテンツルールが上述されている UDP のために同じようにはたらくことにまた注意する必要があります。 L3 コンテンツルールに設定されるプロトコルかポートがありません。

```
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
```

このコンテンツルールを使うと、UDP か TCPトラフィックはバックエンドサーバにこの VIP およびロード バランスを見つけることができます。

コンテンツルールと共の UDP ソースグループ

UDP ソースグループが UDP リターントラフィックを処理するのに使用されています。 例では、これはコンテンツルール dns 見つける DNS 要求への DNS 応答です。 顧客は UDP リターントラフィックをネットワークアドレス交換することを実現させるために 3 つのさまざまな方法のグループを設定できます。

1. コンテンツルールからのバックエンドサーバはグループの内で複写することができます。 上の設定にグループを追加する必要があります。

   ```
   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
   ```

   この設定によって、DNS 応答は dns_s1 か dns_s2 から着き、ソースグループ一致はなされます。 これはパケットをルールで設定される VIP アドレスにネットワークアドレス交換します。 送信元ポートがなぜネットワークアドレス交換されない筈であるか理解することは重要です。 ポートより少しより 1024 であるソースグループはそれがよく知られている な IP ポートである場合 NAT 送信元ポート。再生するために、DNS 要求はバランスをとられる口ードであるために DNS コンテンツルールを見つけます。 CSS の前に 161.44.67.245:2586 は- > VIP（10.86.213.124):53 あります。 CSS とサーバ間で 161.44.67.245:2586 は- > dns_s1（192.168.2.3):53 あります。 サーバからの応答を返は Dns_s1(192.168.2.3):53 - > 161.44.67.245:2586 です。 DNS 応答は VIP（10.86.213.124):53 - > 161.44.67.245:2586 のための CSS を見つけるときソースグループと一致します。**show flows** コマンド 出力:

   ```
   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
   ```

   送信元ポートが 1024 より小さく、よく知られたポートであるので、送信元ポートはソースグループを見つけたのに、ネ

ットワークアドレス交換されません。 ソース IP アドレスだけ VIP アドレスに戻ってネットワークアドレス交換されます。きちんとはたらくこの種 の 設定に関しては:コンテンツルールおよびソースグループの VIP アドレスは同じである必要があります。応答トラフィックの送信元ポートはよく知られているである必要があります。 ポート 1645 であるたとえば Radius。 上の例が RADIUS認証および応答ペアだった場合、Radius 応答に 1645 からソースグループ ポートにネットワークアドレス交換された送信元ポートがあります (たとえば、8192)。 それは本当らしいですこれ引き起こします失敗する RADIUS要求を。 これは **portmap disable コマンドが**ソースグループに追加されたという理由です。

2. コンテンツルールからのバックエンドサーバは宛先サービスとしてグループの内で複写することができます。 DNS 要求がクライアントから入る時ネットワークアドレス交換されるべきソース IP アドレス、また送信元ポートを宛先サービス可能に。 カスタマー コンフィギュレーションは下記に示されています。**注:** 明確にするために、別の VIP アドレスはコンテンツルールのよりソースグループに置かれます。 VIP アドレスは 10.86.213.125 です。 これはように CSS とサーバの間でネットワークアドレス交換される gets が VIP アドレスと同じではない送信元アドレスあります。この場合 DNS 要求がクライアントから、到着するとき、コンテンツルールおよびソースグループ一致は両方なされます。 宛先 IP アドレスはロードによってバランスをとられたサーバにネットワークアドレス交換されます。 ソースグループが追加宛先によって、一致したのでソース IP アドレスおよび送信元ポートは両方ネットワークアドレス交換されます。 CSS の前に 161.44.67.245:2644 は- > VIP (10.86.213.124):53 あります。 CSS とサーバ間で 10.86.213.125:8192-> dns_s1 (192.168.2.3):53 はあります。ソースグループ一致が DNS 要求の時になされたのでソースグループ内の portmap エントリはサーバからの DNS 応答背部によって作成され、一致します。 サーバからの応答を返はです Dns_s1(192.168.2.3):53 - > 10.86.213.125:8192。ソースグループ ポートマップ エントリはソース IP アドレスおよびクライアントのオリジナルソースポートをネットワークアドレス交換することを処理します。 CSS 渡される DNS 応答はからクライアントへの VIP (10.86.213.124):53 - > 161.44.67.245:2644 です。**show flows** コマンド 出力:

```
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
```

この設定を使うと、コンテンツルールの VIP はソースグループ VIP アドレスを一致することができますが、ことができません。 よく知られたポート (より少しにより 1024) まだ存在 する 制約事項。 宛先サービス 設定はクライアントの実際のIPアドレスを見るサーバ必要使用するべきではありません。

3. グループで定義されるサービスがある場合もないしグループは ACL 句によって IP アドレスの範囲のために好まれます。

```
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 原因文は類似したにに検知 します:

```
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: これは通常顧客はある特定のアドレスに/から NAT にすべてのトラフィックがほしいと思わないとき使用されます。 こうすれば、それらはトラフィックがネットワークアドレス交換されて得るものを制御できます。

NAT だけのための UDP ソースグループ

UDP トラフィックのソースグループのもう一つの使用は CSS の後ろのプライベート IP アドレス領域からの公共 IP アドレスに NAT トラフィックにあります。 この場合ロード バランシングが必要とならないので、コンテンツルールが必要となりません。 UDP ソースグループは NAT にトラフィック単に使用されます。 バックエンドサービスは下記の例に示すように私用 IP アドレスと、追加することができます。

```
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
```
または、サービスはグループに追加しソースグループは ACL 句によって好むことができます。

```
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 要求はバックエンドサーバから入り、ソースグループを一致します。 FCB は作成され、NAT 変換は行われます。 ソースグループ ポートマッパ エントリは内部で DNS 応答が受け取られるとき作成されました。 帰りフローでソースグループ ルックアップは行われます、内部 portmap エントリ、作成される FCB および正しくネットワークアドレス交換される DNS 応答 gets は取得されます。

ロード バランシングが必要とならないのでコンテンツルールが必要となりません。 ソースグループは要求で作成されるポートマッパ 情報を使用するので応答の NAT 変換を処理します。

より 1024) まだに付着させるよく知られたポート 制約事項 (より少しに。 既知 の 送信元 ポートはネットワークアドレス交換されませんが、1024 に等しい、 またはそれ以上のポートはネットワークアドレス交換されます。

UDP 設定 オプション

リリース 5.0、7.10、および 7.20 を使ってコマンドパラメータ、**dnsflow [イネーブル|ディセーブルは]**利用できます。 **イネーブルは**デフォルトで、FCB が DNS フローのために作成されることを意味します。 **ディセーブルは**コンテンツルールおよびソースグループ一致する機能が同じであるけれども FCB を作成します。 リリース 6.10 によって、**noflow** コマンド 機能性はコンフィギュレーションパラメータによって拡張でした。

```
flow-state [5060|161|162|53] udp [flow-disable|flow-enable][nat-disable|nat-enable]
```
ポート番号は SIP(5060)、SNMP(161)、SNMP(162)、および DNS(53) に対応します。

noflow の後ろの概念は全くパフォーマンスでした。 DNS のような UDP 応答は/要求 プロトコルは（SNMP および RADIUS は 2 他のよくある物です）ファストパスの FCB を、および実際マッピング することの CSS 機能からの利点が、オーバーヘッドこのトラフィック の 種類の処理のパフォーマンスを減速できますありません。 さらに、UDP トラフィックは単方向で、ターミネータ パケットが（TCP RST か FIN のような）ないので、UDP フローはオーバーヘッドを追加する Garbage Collection によってだけ削除されます。 しかし **noflow** のインプリメンテーションの詳細はコンフィギュレーション必要条件に影響しました。

リリースに 5.0 および 2G CSS 11500 リリースに現時点で **dnsflow disable コマンド** パラメータがありますただ。 リリース 6.10 に SNMP、SNMPトラップおよび DNS UDP フローのためのフロー **ディセーブルを**することができるフロー**州の**コンフィギュレーションテーブルがあります。

dnsflow ディセーブルかフロー **ディセーブル** コマンドが発行される場合これのセクションだけネットワークアドレス交換するためのコンテンツルールか UDP ソースグループと共に UDP ソースグループの例にソースグループが資料必要となりません。 **noflow** コマンドが発行されるとき、内部 ソースグループがフロー パケットを把握しないのに使用されこうしてあらゆる設定されたソースグループと関連付けられないこの内部 ポートマッパ エントリはリターントラフィックを処理します。

この情報はできるだけ詳しいために提供されます。 しかし BU はソースグループがフロー場合で設定されないことを推奨します。 これはフローと **noflow** コンフィギュレーション間で一貫しているでありまたソースグループはユーザが内部 1 つがヒット カウンタを見ることを許可します。

警告

異様および予期せぬ動作を引き起こした DDTS CSCec02038 のようなバグがあるので UDP コンテンツルールおよびソースグループがはたらくはずどのようにであるか文書化することは困難です。 これはコンテンツルールおよび設定なしでだけリリース 6.10 に特定、です。

flow-state [161|162|53] udp flow-disable nat-enable
戻り UDP 要求は失敗し、CSS は到達不能 ICMP を戻します。 UDP 要求が同じ送信元ポート および 宛先ポートを使用する場合この資料のコンテンツルール セクションと共に UDP ソースグループで設定されるコンテンツルールを使用してロード バランシング UDP トラフィックに一般的な問題があります。 これは最も頻繁に Radius と起こります（送信元ポート および 宛先ポートは 1645）あります。 CSS はフローを識別します。

[ip source address|ip source port|ip dest address|ip dest port]
これは FCB および fastpathマッピングがどのように識別されるかです。 クライアントが同じ送信元ポート および 宛先ポートを使用して UDP パケットを送信するとき、最初に一度バランスをとられ、次にファストパスでマッピング される ロードだけです時。 FCB が UDP のための少なくとも 15 秒であるガーベージを集められて得なければ、すべての今後の要求は同じサーバに行きます。

関連情報

- CSS 11000 シリーズ コンテンツ サービス スイッチの製品サポート
- CSS 11500 ハードウェア製品 サポートページ
- WebNSソフトウェア 製品サポートページ
- CSS 11000 ソフトウェアダウンロード

- CSS 11500 ソフトウェアダウンロード
- テクニカルサポート - Cisco Systems