サービスのソース グループの設定

ソース グループとは、ローカルの Web ファーム内からフローを発信するローカル サーバの集合体です。CSS では、ソース グループを、専用の送信元 IP アドレスを持つ仮想サーバとして扱うことができます。グループ内の設定されたサービスの IP アドレスはすべて、この専用の送信元 IP アドレスに変換されます。たとえば、複数のストリーミング オーディオ送信装置を 1 つのグループとして設定すると、CSS はそのグループのメンバーから発信されたフローを処理し、そのフローすべてに同じ送信元 IP アドレスを与えます。

この章では、サービスのソース グループの設定方法について説明します。

この章の内容は、特に指定のない限り、すべての CSS 11500 モデルに共通です。

ソース グループとポート マッピングの概要

ソース グループを設定すると、CSS によって送信元 IP アドレスの network address translation（NAT; ネットワーク アドレス変換）とソース ポートの port address translation（PAT; ポート アドレス変換）が実行されます。NAT と PAT によって、プライベート ネットワークのアドレスとポートが CSS のパブリック ネットワーク側に公開されなくなるので、ネットワークのセキュリティが一段と高まります。CSS のプライベート ネットワーク側のサーバから発信されるフロー（サーバ側フロー）を対象に、送信元 IP アドレスとソース ポートの NAT 変換を行うには、既存のサービスをソース グループに追加します。CSS のパブリック ネットワーク側のクライアントから発信されるフロー（クライアント側フロー）を対象に、送信元 IP アドレスとソース ポートの NAT 変換を行うには、既存のサービスを宛先サービスとしてソース グループに追加します。送信元の NAT 変換は、access control list（ACL; アクセス コントロール リスト）を設定して実行することも可能です。ACL の詳細については、『*Cisco Content Services Switch Security Configuration Guide*』を参照してください。

CSS の各モジュール（SSL モジュールを除く）は、いずれもフロー管理用の session processor（SP; セッション プロセッサ）を 1 基内蔵しています。

- CSS 11501 は 1 基の SP をサポートしています。
- CSS 11503 は最大 3 基の SP をサポートしています。
- CSS 11506 は最大 6 基の SP をサポートしています。

1 つのソース グループで利用できるソース ポートの数は、デフォルトでは 63488（65533 から名前付きポートを除いた数）です。ソース グループを 1 つ設定した環境において、CSS はシャーシ内の各 SP 間の相対的な重みに比例するように、これらの SP にポートの合計数を分配します。SP の相対的な重みは、**show chassis session-processors** コマンドで確認できます（『*Cisco Content Services Switch Administration Guide*』を参照）。SP の相対的な重み値は設定できません。

クライアント側のフローについては、CSS はフロー処理のために複数の SP にパケットを送信し、その SP のソース ポートにフローが着信します。CSS は TCP または UDP のソース ポート番号と宛先ポート番号に単純な XOR ハッシュを実行

して、このフローを管理するマスター SP を特定します。ソース ポート番号と宛先ポート番号が同じ場合（DNS UDP ポート 53 など）、CSS は、ソースと宛先の IP アドレスの下位ビットを使用してハッシュ値を計算します。このハッシュ値を使用して SP の加重テーブル内にインデックスを付け、適切な SP を選択します。

CSS が PAT を実行する場合に、処理対象のフローのマスター SP は、設定に応じて、グローバル ポート マッパーまたはソース グループから得られたソース ポートを使用します（グローバル ポート マッピングの詳細については、第 2 章「フロー パラメータとポート マッピング パラメータの設定」の「グローバル ポート マッピングの設定」を参照してください）。CSS は、ソース ポートのハッシュ値と宛先ポートによって、クライアント側フローのマスターと同じ SP がサーバ側フローでも選択されるように、ソース ポートを選択します。

指定の宛先ポートからのサーバ側フローでは、クライアント側フローで使用されたのと同じ SP にハッシュされるのは、一部のソース ポート番号だけです。そのため、バックエンド接続の確立時に、特定の SP で利用可能なポートが適切でないことがあります。したがって、ハッシュ アルゴリズムで選択されるのは、SP で利用可能なポートの一部です。

フローに使用できるソース ポート数を増やしたり、各 SP にソース ポートを追加するには、次のいずれかの方法で行います。

- **portmap vip-address-range** コマンドを使用してポート マッピングの VIP アドレス範囲を設定する。ポート マッピングに設定する追加の VIP アドレスごとに、利用可能な他の 63488 個のポートとともに、もう 1 つのポート マッパーを追加します。この方法では、ソース グループに宛先サービスを設定する必要があります。詳細については、「ポート マッピングの VIP アドレス範囲の設定」を参照してください。
- 複数の宛先ポートにサービスを設定して、いくつかの異なる宛先ポートを確保する。この結果、SP を通過するハッシュ値の幅が広がり、ポート マッピングに使用できるポートが増えます。この方法では、ハッシュ方程式を満たすソース ポートの数が増え、ハッシュ アルゴリズムの制約が緩和されます。サーバ側のアドレス空間が制限されているため **vip-address-range** コマンドが使用できない場合には、この方法を使います。設定する追加の宛先ポートごとに、利用可能なソース ポートの追加セットを受け取り、表 5-1 の 2 番目のカラムに示すポート マッピングで使用します。この方法における要件は次のとおりです。

  - 複数のポート（たとえば、ポート 80、81、82 など）を監視するように Web サーバを設定する。
  - 各宛先ポートに対して、CSS に新しいサービスを設定する。
  - コンテンツ ルールにサービスを追加する。
  - ソース グループにサービスを宛先サービスとして追加する。
- 複数のソース グループを設定し、各ソース グループに 63488 個のポートを新しく追加する。この項で前述したように、追加されたポートは SP 間で分配されます。この方法における要件は次のとおりです。
  - Web サーバに複数の IP アドレスを設定する（IP エイリアス）。
  - サーバの IP アドレスごとに新しいサービスを CSS に作成する。
  - 一意のソース グループに各サービスを宛先サービスとして追加する。
  - コンテンツ ルールにサービスを追加する。

表 5-1 は、モジュール（SP）の装着数を増やすと CSS 11506 で利用可能なポート数が減ること、およびポート マッピングの VIP アドレス範囲を設定することで利用可能なポート数を大幅に増やす方法を示しています。どの場合も CSS のすべてのフローに対して、1 つのソース グループにサービスと宛先ポート（ポート 80 など）が 1 つずつ設定されます。表 5-1 に示している利用可能なポートの数は、一例です。設定によって、数が異なることがあります。

表 5-1　CSS 11506 の装着モジュール（SP）数の追加による利用可能ソース ポート数の減少、ポート マッピングの VIP アドレスの追加による利用可能ソース ポート数の増加

	シャーシで利用可能なソース ポートの数	
装着モジュール（SP）の数	**port-map vip-address-range = 1**	**port-map vip-address-range = 10**
1	63488	634880
2	33728	337280
3	21824	218240
4	16616	166160
5	13144	131440
6	11408	114080

表 5-2 は、宛先ポートを増やすことによって、SP を最大数（6 基）まで装着した CSS 11506 でも、ポート マッピングに使用できるソース ポート数が大幅に増加することを示しています。ポート マッピングにより大きな VIP アドレス範囲を設定すると、利用可能なソース ポートの数をさらに大幅に増やすことができます。この例では、宛先ポートは連続して選択されています。

表 5-2　宛先ポートの追加またはポート マッピングの VIP アドレス範囲の設定による利用可能なソース ポート数の増加

	シャーシで利用可能なソース ポートの数	
宛先ポート数	port-map vip-address-range = 1	port-map vip-address-range = 10
10	28788	287880
20	31757	317570
32	40000	400000

表 5-1 の 6 行目と表 5-2 の 1 行目を比べると、宛先ポート数を 10 ポートに増やした場合、ポート マッピングに使用できるソース ポートの数が倍以上になることがわかります。

アルゴリズム上の理由により、利用可能なソース ポート数を効果的に増やすためには、どの宛先ポートを選択するかが重要になります。宛先ポートの増加数と利用可能なソース ポートの増加数は、比例関係にあるわけではありません。利用可能なソース ポート数を最大限に増やすには、いくつかの範囲の宛先ポート群を選択する必要がある場合があります。

Adaptive Session Redundancy（ASR; 適応型セッションの冗長性）の場合、それぞれの CSS で、各シャーシの同じ相対位置（スロットをスキップすることはできる）に同じ数の SP が装着されている必要があります。この装着により、ポート マッパーは非 ASR 構成で使用されているものと同じポート選択アルゴリズムを使用できます。ASR 構成で利用できるソース ポートには、他に制限はありません。ASR の詳細については、『*Cisco Content Services Switch Redundancy Configuration Guide*』を参照してください。

ソース グループ設定のクイック スタート

表 5-3 の手順を使用して、TCP/UDP トラフィック用のソース グループを設定します。FTP トラフィック用のソース グループの設定については、次の項を参照してください。各ソース グループには、そのソース グループと同じサービスおよび VIP を含むコンテンツ ルールが 1 つ必要です。

表 5-3　ソース グループ設定のクイック スタート

作業とコマンドの例

1. ソース グループを作成します。ソース グループ名の長さは最大 31 文字です。次の例では、ソース グループ ftpgroup を作成します。
`(config)# group ftpgroup`
 	
CLI はグループ設定モードに移行するので、そこでソース グループのアトリビュートを設定し、そのアトリビュートを有効化できます。
`(config-group[ftpgroup])#`

2. すべてのサービスの IP アドレスの変換先となるソース グループの VIP アドレスを設定します。次に設定例を示します。 `(config-group[ftpgroup])# vip address 172.16.36.58` これと同じ VIP アドレスを複数のソース グループに割り当てることができますが、同時にアクティブにできるのは 1 つのソース グループだけです。

3. 定義済みのサービスをソース グループに追加します。次に例を示します。
`(config-group[ftpgroup])# add service server1`
`(config-group[ftpgroup])# add service server2`

4. ソース グループをアクティブにします。 `(config-group[ftpgroup])# active` VIP アドレスは一度に 1 つのアクティブなソース グループでしか使用できないため、アクティブなソース グループで使用されている VIP アドレスを持つ 2 つ目のソース グループをアクティブにすることはできません。

表 5-3　ソース グループ設定のクイック スタート（続き）

作業とコマンドの例

5. コンテンツ ルールを作成して、ソース グループで設定したものと同じサービスおよび VIP を追加し、コンテンツ ルールをアクティブにします。このコンテンツ ルールにより、CSS はコンテンツ ルール VIP に対する要求を照合できるようになります。server1 または server2 が要求に応答すると、そのサーバの IP アドレスがソース グループ VIP に NAT 変換されます。
 	
次に例を示します。
 	
`(config-owner[arrowpoint.com])# content ftpsource1`
 	
`(config-owner-content[arrowpoint.com-ftpsource1])# add service server1`
 	
`(config-owner-content[arrowpoint.com-ftpsource1])# add service server2`
 	
`(config-owner-content[arrowpoint.com-ftpsource1])# vip address 172.16.36.58`
 	
`(config-owner-content[arrowpoint.com-ftpsource1])# active`

表 5-3 に示した各コマンドを実行すると、次のような実行設定が得られます。

```
!************************** GROUP ***************************
group ftpgroup
  vip address 172.16.36.58
  add service server1
  add service server2
  active

!************************** OWNER ***************************
owner arrowpoint
  content ftpsource1
    add service server2
    vip address 172.16.36.58
    active
```

ソース グループの作成

グループ設定モードでは、最大 255 個のソース グループを CSS に設定できます。グループ設定モードにアクセスするには、ACL モードおよびブート設定モード以外の任意のモードで **group** コマンドを使用します。このコマンドのシンタックスは次のとおりです。

group *groupname*

1 ～ 31 文字で既存または新規のソース グループ名を入力します。

次に入力例を示します。

```
(config)# group ftpgroup
(config-group[ftpgroup])#
```

ソース グループのリストを表示するには、次のように入力します。

```
(config)# group ?
```

（注）　グループ モードで **group** コマンドを使用して、他のグループにアクセスしたり、グループを新規作成することもできます。

ソース グループを削除するには、次のように入力します。

```
(config)# no group ftpgroup
```

ソース グループの設定

ここでは、ソース グループの設定方法について説明します。

- 「ソース グループの VIP アドレスの設定」
- 「ソース グループへのサービスの設定」
- 「ソース グループへの宛先サービスの追加」

ソース グループ ポート マッピングの設定については、「ソース グループ ポート マッピングの設定」を参照してください。ソース グループを設定した後、そのグループを有効化できます（「ソース グループの有効化と一時停止」を参照）。

（注）　アクティブなソース グループに変更を加える場合、変更の種類によっては、まず **suspend** コマンドを実行してソース グループを一時停止する必要があります。このような変更には、IP アドレスの 0 への変更または **no ip address** コマンドの実行、サービスまたは宛先サービスの追加や削除、または **portmap** コマンドの実行などがあります。

ソース グループの VIP アドレスの設定

add destination service コマンドでサービスを設定した場合、CSS は NAT 変換で、ソース グループのソースから発信されたフロー、またはソース グループの宛先の 1 つに送信されたフローの送信元 IP アドレスを VIP に置換します。NAT 変換はセキュリティ確保の一手段で、ソースの IP アドレスがインターネット上に公開されることを防止します。これと同じ VIP アドレスを複数のソース グループに割り当てることができますが、同時にアクティブにできるのは 1 つのソース グループだけです。

vip address コマンドを使用してソース グループの基本 VIP アドレスを指定します。このグループ設定モードのコマンドのシンタックスは次のとおりです。

vip address *ip_or_host* {**range** *number*}

このコマンドのオプションと変数は次のとおりです。

- *ip_or_host* ：ソース グループの IP アドレスまたは名前。ドット付き 10 進表記の IP アドレス（たとえば、192.168.11.1）またはニーモニック ホスト名（たとえば、myhost.mydomain.com）で入力します。

  CSS では、ソース グループの VIP アドレスと IP アドレスは、A、B、C のいずれかのクラスに限定されます。マルチキャスト アドレス（クラス D および E）や、アドレス上限を超える範囲の IP アドレスは許可されません。

- **range** *number* ：（オプション）ソース グループの IP アドレス範囲を定義する。*number* には 1 ～ 65535 の範囲内の数値を入力します。デフォルトは 1 です。*ip_or_host* 変数は、範囲の最初のアドレスです。

（注）　ソース グループの基本 VIP アドレスを設定するときは、設定したすべてのポート マッピングのエントリが CSS で使用される場合に備え、十分なアドレス空間を残してください。また、ポート マッピングで使用する VIP アドレス範囲を広げる必要があります。「ポート マッピングの VIP アドレス範囲の設定」を参照してください。

次に例を示します。

```
(config-group[ftpgroup])# vip address 172.16.36.58 range 3
```

ソース グループへのサービスの設定

CSS のプライベート ネットワーク側のサーバから発信されるフロー（サーバ側フロー）を対象に、送信元 IP アドレスとソース ポートの NAT 変換を行うには、既存のサービスをソース グループに追加します。ソース グループごとに最大 64 の宛先サービスを設定できます。

サービスは、一度に 1 つのグループだけに所属できます。そのソース グループがアクティブで、コンテンツ ルール、ACL の優先サービス、またはソーリー サービスにより同じサービスがヒットした場合、そのソース グループが送信元アドレスのネットワーク アドレス変換（NAT）に使用されます。ソース グループに対して送信元アドレスの NAT 変換を実行するには、サービスがアクティブである必要があります。

次のような場合にはサービスを使用できないので注意してください。

- 他のソース グループに同じ名前がある場合、または同じソース グループ内の宛先サービス リストを使用する場合
- 他のソース グループの送信元サービスと同じアドレスを持つ場合

定義済みのサービスをソース グループに追加するには、add service コマンドを使用します。次に例を示します。

```
(config-group[ftpgroup])# add service server1
```

ソース グループから設定済みのサービスを削除するには、**remove service** コマンドを使用します。たとえば、ソース グループからサービス server1 を削除するには、次のように入力します。

```
(config-group[ftpgroup])# remove service server1
```

ソース グループへの宛先サービスの追加

CSS のパブリック ネットワーク側のクライアントから発信されるフロー（クライアント側フロー）を対象に、送信元 IP アドレスとソース ポートの NAT 変換を行うには、既存のサービスを宛先サービスとしてソース グループに追加します。ソース グループごとに最大 64 の宛先サービスを設定できます。次のことに注意してください。

- 他のソース グループにある同じ名前のサービスを使用することも、同じソース グループ内のソース サービス リストを使用することもできません。
- 実際のサービスはコンテンツ　ルールで選択されるため、他の宛先サービスと重複するアドレスを持つサービスは使用できます。
- ソース グループに対する宛先 / 送信元アドレスの NAT 変換が実行できるためには、宛先サービスがアクティブでコンテンツ ルールに追加されている必要があります（第 10 章「コンテンツ ルールの設定」を参照）。

（注）　宛先サービスがフローを開始した場合、ソース グループにそのサービスを追加しても、そのソース グループによってそのフローは NAT 変換されません。これは、ルールと宛先サービスの照合条件によって、サービスがグループ メンバーであることが決まるためです。接続を開始したサービスを NAT 変換するには、ACL 一致基準も設定するか、または重複したアドレスを持つサービス名を追加設定してから、ソース グループにそれらのサービスを追加する必要があります。使用するソース グループは、その宛先サービスを設定した現在のソース グループか、またはその他の設定済みソース グループのいずれかになります。

ソース グループに宛先サービスを追加するには、**add destination service** コマンドを使用します。次に例を示します。

```
(config-group[ftpgroup])# add destination service server2
```

ソース グループから設定済みの宛先サービスを削除するには、**remove** コマンドを使用します。

```
(config-group[ftpgroup])# remove destination service server2
```

ソース グループの有効化と一時停止

ソース グループを有効にすると、送信元 IP アドレスがそのソース グループで NAT 変換されます。ソース グループを設定した後、そのグループを有効化できます。VIP アドレスは一度に 1 つのアクティブなソース グループでしか使用できないため、アクティブなソース グループで使用されている VIP アドレスを持つ 2 つ目のソース グループをアクティブにすることはできません。

```
(config-group[ftpgroup])# active
```

設定を変更する場合にはソース グループを一時停止します。グループとそのアトリビュートは変わりませんが、これらはフローの作成に影響しなくなります。ソース グループを一時停止するには、**suspend** コマンドを使用します。次に入力例を示します。

```
(config-group[ftpgroup])# suspend
```

ソース グループ ポート マッピングの設定

デフォルトでは、ソース ポートの番号が 1023 より大きいソース グループで PAT（またはポート マッピング）が有効になっています。CSS は、該当するソース ポートを 2016 から始まる範囲に変換します。以降の項では、CSS のデフォルトの PAT 動作を変更する方法を説明します。

- 「開始ポート番号の設定」
- 「ポート マッピング範囲の合計ポート数の設定」
- 「ポート マッピングの VIP アドレス範囲の設定」
- 「ポート マッピングの無効化」

アクティブなソース グループを設定する前に、ソース グループを一時停止する必要があります。

開始ポート番号の設定

デフォルトでは、CSS の基本ポート（開始ポート番号）は 2016 です。**portmap base-port** コマンドでは、CSS の基本ポートを定義します。2016 ～ 63456 の基本ポート値を入力できます。たとえば、基本ポートを 3354 に設定するには、次のように入力します。

```
(config-group[ftpgroup])# portmap base-port 3354
```

基本ポートをデフォルト値の 2016 にリセットするには、**no portmap base-port** コマンドを使用します。次に例を示します。

```
(config-group[ftpgroup])# no portmap base-port
```

ポート マッピング範囲の合計ポート数の設定

CSS は設定済みポートの合計数を、シャーシ内のセッション プロセッサ（SP）間で、SP の相対的な重みに比例するように割り振ります。セッション プロセッサの相対的な重みは、**show chassis session-processors** コマンドで確認できます（『*Cisco Content Services Switch Administration Guide*』を参照）。

CSS のシャーシに装着するモジュールの数が増えれば、モジュール単位でのセッション処理量が減り、CSS が 1 つのモジュールに割り当てるポート数も少なくなります。各モジュールに割り当てられているポート数は、**show group portmap** コマンドで確認できます（「ソース グループの表示」を参照）。CSS のポート マッピング動作の詳細については、「ソース グループ ポート マッピングの設定」の項を参照してください。

デフォルトでは、CSS 全体でのポート マッピング範囲のポート合計数は 63488 です。ほとんどの用途では、デフォルト値を変更する必要はありません。ポート マッピング範囲の合計ポート数を定義するには、**portmap number-of-ports** コマンドを使用します。2048 ～ 63488 の値を入力します。32 の倍数でない値を入力すると、次の 32 の倍数に切り上げられます。たとえば、合計ポート数を 2048 に設定するには、次のように入力します。

```
(config-group[ftpgroup])# portmap number-of-ports 2048
```

ポート数をデフォルト値にリセットするには、**no portmap number-of-ports** コマンドを使用します。次に入力例を示します。

```
(config-group[ftpgroup])# no portmap number-of-ports
```

ポート マッピングの VIP アドレス範囲の設定

設定する各ソース グループでは、ポート マッピングには最大で 63488（デフォルト）のソース グループが利用可能です。ただし、利用可能なすべてのポートがフローに使用できるわけではありません。ソース グループとポート マッピングの詳細については、「ソース グループとポート マッピングの概要」を参照してください。

ポート マッピングに利用できるポート数を増やすには、VIP の範囲を指定して追加の VIP アドレスでポート マッパーを設定します。設定する追加 VIP アドレスごとに、VIP で利用可能なポートを管理するために新しいポート マッパーが作成されます。CSS が PAT を実行するとき、ソース グループは設定されているすべてのポート マッパー間でラウンドロビンを使用し、選択されたポート マッパーが指定の VIP に対して次に使用可能なポートを選択します。

ポート マッピングの VIP アドレス範囲の設定は、Virtual Web Hosting（VWH; 仮想 Web ホスティング）の設定とは異なります。VWH の設定では、ソース グループにポート マッパーではなく VIP アドレス範囲を設定します。VWH の設定で利用可能なポート マッパーは 1 つだけです。VWH については、第 10 章「コンテンツ ルールの設定」の「仮想 Web ホスティングの設定」を参照してください。

CLI では次の設定制限があります。

- 同じソース グループに VWH とポート マッパー VIP アドレス範囲は設定できません。VWH については、第 10 章「コンテンツ ルールの設定」の「仮想 Web ホスティングの設定」を参照してください。
- 同じソース グループにサービス（**add service** コマンドを使用）とポート マッパー VIP アドレス範囲は設定できません。**add service** コマンドについては、「ソース グループへのサービスの設定」を参照してください。
- ACL で使用するソース グループにポート マッパー VIP アドレス範囲は設定できません。また、この逆も設定できません。ACL の詳細については、『*Cisco Content Services Switch Security Configuration Guide*』を参照してください。
- 各 CSS には最大 255 のポートを設定できます。ポート数を最大にするには、次のように設定します。
  - ソース グループでポート マッピング VIP アドレスを 255 に設定する。
  - 255 のそれぞれのソース グループでポート マッピング アドレス範囲を 1 に設定する。
  - ソース グループの数（ポート マッパーの合計は 255）が設定されているポート マッピング VIP アドレス範囲を組み合わせる。
- VIP アドレスが同じポート マッパーとコンテンツ ルールには、同じ VIP アドレス範囲を設定します。コンテンツ ルールの VIP アドレス範囲の上限は 65535 で、ポート マッパーの上限である 255 より大きい数値になっています。255 より大きい VIP アドレス範囲でルールを作成する必要が生じた場合は、255 以下の範囲を指定して複数のルールを作成してください。

ソース グループのポート マッパーの追加 VIP アドレスを設定するには、**portmap vip-address-range** コマンドをグループ設定モードで使用します。このコマンドのシンタックスは次のとおりです。

portmap vip-address-range *number*

number 変数は、グループ設定モードの **vip address** コマンドで指定したアドレスで始まる VIP アドレス範囲を示します。1 ～ 255 の整数を指定します。デフォルトは 1 です。**vip address** コマンドによるソース グループの VIP アドレスの設定

については、「ソース グループの VIP アドレスの設定」を参照してください。

（注）　ソース グループの基本 VIP アドレスを設定するときは、設定したすべてのポート マッピングのエントリが CSS で使用される場合に備え、十分なアドレス空間を残してください。また、ポート マッピングで使用する VIP アドレス範囲を広げる必要があります。「ソース グループの VIP アドレスの設定」を参照してください。

（注）　no-portmap エラーを監視する場合は、**portmap vip-address-range** コマンドを使用して範囲の値を、アプリケーションに必要なアクティブな接続数より大きな値に設定してください。

VIP の範囲が 255 の場合、フル実装の CSS 11506 シャーシの SCM で使用できるポートの最大数は 63240 です。他の SP またはシャーシ構成では、ポート数はより大きな値になります。

たとえば、3 つの VIP アドレスを持つソース グループのポート マッパーを設定するには、次のように入力します。

```
(config-group[ftpgroup])# portmap vip-address-range 3
```

ソース グループの VIP が 192.168.44.3, の場合、上記の **portmap vip-address-range** コマンドを入力すると、ポート マッパーの使用可能な 3 つの VIP は次のようになります。

- 192.168.44.3
- 192.168.44.4
- 192.168.44.5

VIP アドレス範囲をデフォルト値の 1 に戻すには、次のように入力します。

```
(config-group[ftpgroup])# no portmap vip-address-range
```

ポート マッピングの無効化

デフォルトでは、送信元 IP アドレスを NAT 変換し、設定されたソース グループのソース ポートを PAT 変換します。ソース グループの **portmap disable** コマンドを設定すると、送信元 IP アドレスでは NAT 変換が行われますが、ソース グループに一致する UDP トラフィックのソース ポートでは PAT 変換は実行されません。

大きなポート番号が割り当てられている UDP アプリケーション（SIP や WAP）の場合、**portmap disable** コマンドを使用するかわりに、ソース グループの宛先サービスを設定することにより、このポート番号を維持することをお勧めします。宛先サービスにより、宛先ポートではなく、クライアント側のソース ポートが NAT 変換されます。宛先サービスの詳細については、第 3 章「サービスのソース グループの設定」を参照してください。

（注）　フロー状態テーブルを使用して UDP ポートのフローを無効にし、ソース グループの **portmap disable** コマンドを設定すれば、ソース グループに一致するポートのトラフィックを、認識不可なポート番号のクライアントに返すことができます。フロー状態テーブルについては、第 2 章「フロー パラメータとポート マッピング パラメータの設定」を参照してください。

CSS は、ソース グループ内に設定された **base-port** または **number-of-ports**（前述のオプションを参照）の値を維持はしますが無視します。後でこのソース グループの PAT を再度有効にすると、設定済みのすべての **base-port** または **number-of-ports** の値が有効になります。設定済みソース グループに対するデフォルトの動作では、送信元 IP アドレスが NAT 変換され、1023 より大きいポート番号のソース ポートが PAT 変換されます。

（注）　**portmap disable** コマンドは TCP フローには影響しません。

ポート マッピングを無効にするには、次のように入力します。

```
(config-group[ftpgroup])# portmap disable
```

CSS のデフォルト動作（送信元 IP アドレスの NAT 変換と設定済みソース グループのソース ポートの PAT 変換）に戻すには、**portmap enable** コマンドを使用します。たとえば、次のように入力します。

```
(config-group[ftpgroup])# portmap enable
```

ソース グループと ACL の設定

インターネットに送信されたトラフィックを NAT 変換し、ローカル トラフィックを NAT 変換しないようにする場合、ソース グループで ACL を使用して、ACL の宛先 IP アドレスを基準に決定することができます。

次の例では、10.0.1.0 と 10.0.2.0 プライベート サブネットのクライアントは、ソース グループがトラフィックを NAT 変換することなく、互いに通信させています。合計 3 つの VLAN（各サブネットに 1 つの VLAN（VLAN1 と VLAN2）、およびソース グループ（VLAN3）によってインターネットに接続される VLAN）を使用しています。

1. ソース グループを作成し、そのグループを有効にします。この例では、ソース グループの名前が outbound で、その VIP アドレスは 192.168.1.10 です。

```
(config) # group outbound
Create group <outbound>, [y/n]:y
(config-group[outbound]) # vip address 192.168.1.10
(config-group[outbound]) # active
```

   ソース グループの VIP アドレスは、応答トラフィックを CSS にルーティングできる公開アドレスであることが必要です。アドレスは、VLAN3 回線（同じ IP アドレスではない）に設定された IP アドレスとして同じサブネットの IP アドレス、またはネットワーク内のルーターに CSS へのスタティック ルートが設定されている別の公開 IP アドレスとすることができます。

2. プライベート サブネット上のクライアントが互いに通信できる ACL を作成します。次の ACL と句では、10.0.1.0 サブネット上のクライアントは、ソース グループで NAT 変換を実行することなく、10.0.2.0 サブネット上のクライアントと通信できます。これは、CSS が bypass オプションを使用してトラフィックをルーティングし、CSS に設定されたすべてのルールを無視するためです。

```
(config) # acl 1
Create ACL <1>, [y/n]:y
(config-acl[1]) # clause 2 bypass any 10.0.1.0 255.255.255.0
destination 10.0.2.0 255.255.255.0
```

3. 句を追加して、10.0.1.0 サブネット上のクライアントからの他のトラフィックをすべてソース グループにルーティングし、送信元 IP アドレスで NAT 変換を行って 192.168.1.10 に接続できるようにします。

```
(config-acl[1]) # clause 10 permit any 10.0.1.0 255.255.255.0
destination any sourcegroup outbound
```

4. 句 1 を追加して、CSS 上のサービスのキープアライブを可能にします。

```
(config-acl[1]) # clause 1 permit icmp any destination any
```

5. VLAN1 に ACL を適用します。

```
(config-acl[1]) # apply circuit-(VLAN1)
(config-acl[1]) # exit
```

6. VLAN2 上のサービスからのトラフィックをソース グループにルーティングし、同時に NAT IP アドレスを使用せずにサーバが VLAN1 と通信できるようにするには、VLAN2 に次の ACL を設定します。

```
(config) # acl 2
Create ACL <2>, [y/n]:y
(config-acl[2]) # clause 2 bypass any 10.0.2.0 255.255.255.0
destination 10.0.1.0 255.255.255.0
(config-acl[2]) # clause 10 permit any 10.0.2.0 255.255.255.0
destination any sourcegroup outbound
(config-acl[2]) # apply circuit-(VLAN2)
(config-acl[2]) # exit
```

7. インターネットからの着信トラフィックの場合、VLAN3 に ACL を設定します。

```
(config) # acl 3
Create ACL <3>, [y/n]:y
(config-acl[23) # clause 1 permit any any destination any
(config-acl[3]) # apply circuit-(VLAN3)
(config-acl[3]) # exit
```

8. CSS のすべての ACL をグローバルに有効にします。

```
(config) # acl enable
```

FTP 接続のためのソース グループの設定

ソース グループを使用して、複数のサービス間で負荷分散される VIP への FTP セッションをサポートするには、VIP のコンテンツ ルールを設定してから、ソース グループを設定します。

（注）　FTP コンテンツ ルールに VIP アドレスの範囲を設定して使用する場合は、対応するソース グループも同じ VIP アドレスの範囲で設定する必要があります（第 10 章「コンテンツ ルールの設定」参照）。

VIP への FTP セッションを設定するには、次の手順に従います。

1. 複数のサーバ間でロード バランシングが行われる VIP を使用して、必要に応じてコンテンツ ルールを設定します。次の例は、コンテンツ ルール ftp_rule の実行設定の一部です。アプリケーション タイプの定義には、**application ftp-control** コマンドを使用します。

```
content ftp_rule
vip address 192.168.3.6
protocol tcp
port 21
application ftp-control
add service serv1
add service serv2
add service serv3
active
```

2. コンテンツ ルールで設定したものと同じ VIP アドレスおよびサービスを定義するソース グループを設定します。

（注）　パッシブ FTP サーバのロード バランシングを行っている場合は、次の例に示すように、対応するソース グループにサービスを直接設定する必要があります。

次の例の実行設定は、ソース グループ ftp_group を示しています。

```
group ftp_group
vip address 192.168.3.6
add service serv1
add service serv2
add service serv3
active
```

サーバでのインターネットによるドメイン名解決のためのソース グループの設定

CSS は、インターネット上でのサーバのドメイン名解決に対応しています。使用しているサーバにプライベート IP アドレスが割り当てられており、インターネット上のドメイン ネーム サーバを使用してサーバにドメイン名の解決を行わせる場合は、そのようにコンテンツ ルールとソース グループを設定する必要があります。コンテンツ ルールおよびソース グループでは、インターネットでルーティング可能なパブリック IP アドレス（VIP アドレス）をドメイン名の解決を行うサーバとして指定する必要があります。

サーバがドメイン名を解決するように設定するには、次の手順に従います。

1. サーバを設定していない場合は、サーバを設定します。

   次の例では、Server1 を作成し、このサーバにプライベート IP アドレス 10.0.3.251 を割り当ててアクティブにします。

   ```
   (config)# service Server1
   (config-service[Server1])# ip address 10.0.3.251
   (config-service[Server1])# active
   ```

2. DNS 応答を処理するコンテンツ ルールを作成します。DNS 応答を処理するコンテンツ ルールは、Web トラフィックを処理するために作成した一連のコンテンツ ルールとは別のものです。次のコンテンツ ルールの例では、CSS で着信 DNS 応答をパブリック VIP アドレス（192,168,200,200）からサーバのプライベート IP アドレス（10.0.3.251）に NAT 変換します。

   この例では、コンテンツ ルール dns1 を作成して、パブリック VIP アドレス 192,168,200,200 を設定し、サーバ Server1 を追加します。

```
(config-owner[arrowpoint.com])# content dns1
(config-owner-content[arrowpoint.com-dns1])# vip address
192.168.200.200
(config-owner-content[arrowpoint.com-dns1])# add service Server1
(config-owner-content[arrowpoint.com-dns1])# active
```

3. DNS 要求を処理するソース グループを作成します。ソース グループにより、CSS は発信トラフィックの送信元 IP アドレスをサーバのプライベート IP アドレス（10.0.3.251）からパブリック VIP アドレス（192,168,200,200）へ NAT 変換できるようになります。

   サーバのソース ポートの衝突を回避するため、CSS では、次のように、サーバの送信元 IP アドレスおよびポートを NAT 変換します。

   - 送信元 IP アドレスをソース グループに定義された IP アドレスに変換する。
   - ポートをソース　グループで選択されたポートに変換する。ソース　グループにより、各サーバに DNS 問い合せのための一意のポートが割り当てられるため、CSS は、割り当てられたポートと DNS 応答を照合することができます。このポートのマッピングにより、DNS 応答を適切なサーバに返すことができるようになります。

   次の例では、ソース グループ dns1 を作成し、パブリック VIP アドレス 192,168,200,200 を設定して、Server1 を追加します。

```
(config)# group dns1
(config-group[dns1])# vip address 192.168.200.200
(config-group[dns1])# add service Server1
(config-group[dns1])# active
```

ソース グループの表示

ソース グループの設定情報を表示するには、スーパーユーザ、ユーザ、グローバル設定、およびグループの各モードで **show group** コマンドを使用します。このコマンドには、次のオプションがあります。

- **show group** ：すべてのソース グループ設定を表示する。
- **show group** *group_name* ：*group_name* で指定されたソース グループ設定を表示する。グループ モードでグループ名は指定できません。
- **show group** *group_name* **portmap** ：CSS 内の各 SP の詳細なポート マッピング情報を表示する。
- **show group** *group_name* **portmap all** ：ソース グループのポート マッパーのすべての VIP アドレスに対して、CSS 内の各 SP の詳細なポート マッピング情報を表示する。
- **show group** *group_name* **portmap** *ip_address* ：ソース グループのポート マッパーの指定された VIP アドレスに対して、CSS 内の各 SP の詳細なポート マッピングを表示する。

次に使用例を示します。

```
(config)# show group
```

表 5-4 に、**show group** コマンドで表示されるフィールドについて説明します。

表 5-4　show group コマンド出力のフィールド

フィールド	説明
Group	グループの名前、グループがアクティブ（Active）か一時停止（Suspend）のどちらの状態であるか、およびグループの送信元 IP アドレス
Portmap VIP Range	ポート マッパーが NAT およびアドレス範囲に使用できる設定された VIP アドレスの数
Session Redundancy	ソース グループについて ASR が有効または無効のどちらに設定されているかを示す。ASR の詳細については、『*Cisco Content Services Switch* Redundancy *Configuration Guide*』を参照してください。

表 5-4　show group コマンド出力のフィールド（続き）

フィールド	説明
Redundancy Global Index	グループ設定モードで **redundant-index** コマンドを使用してソース グループに割り当てられた、一意の ASR グローバル インデックス値
Associated ACLs	グループに関連付けられた ACL
Source/Destination Address	ソース グループの送信元または宛先サービス
Name	サービスの名前
Hits	サービスのコンテンツ アクセス（ヒット）数。このフィールドは、グループ サーバからのトラフィックがソース グループから送信されているときに増加します。このグループが受信するトラフィックでは、カウンタは増加しません。
State	サービスの状態。Alive、Dying、または Dead の状態があります。
DNS Load	サービスの DNS の負荷。値 255 は、サービスがダウンしていることを表します。適切な負荷範囲は 2 ～ 254 です。
Trans	サービスの状態が移行した回数
Keepalive	サービスのキープアライブ タイプ。値は、FTP、HTTP、ICMP、NAMED、SCRIPT、または TCP です。
Conn	サービスでの現在の接続数
Flow Timeout Multiplier	フローのアイドル状態が継続しうる最大時間（16 の倍数の秒単位）。この時間が経過すると、CSS は **flow-timeout-multiplier** コマンドによる設定に従って、そのフローのリソースを再要求します。**flow-timeout-multiplier** コマンドの詳細については、第 2 章「フロー パラメータとポート マッピング パラメータの設定」を参照してください。
Group Service Total Counters	グループのカウンタ

表 5-4　show group コマンド出力のフィールド（続き）

フィールド	説明
Hits/Frames/Bytes	グループのヒット数、フレーム数、およびバイト数。このフィールドは、グループ サーバからのトラフィックがソース グループから送信されているときに増加します。このグループが受信するトラフィックでは、カウンタは増加しません。
Connection Total/Current	グループの接続合計数と現在の接続数
FTP Control Total/Current	CSS でマッピングおよび監視されていた FTP 制御チャネルの合計数、および現在マップされている接続の数
SP Port Map Info	CSS 内の各 SP のポート マップ情報。**portmap** コマンドの状態（有効または無効）を含みます。
Configured Base Port	設定された最初のポート番号
Configured Ports per VIP	CSS 内の各 VIP アドレスの合計ポート数。合計数が 32 の倍数でない場合は、次の 32 の倍数に切り上げられます。
Slot	モジュールを装着している CSS シャーシのスロット
Subslot	SP を装着しているモジュールのサブスロット
Ports Avail to this SP	SP で使用可能なソース ポートの合計数
VIP Address	ポート マッパーの設定された VIP アドレス。**show group portmap** コマンドでは、複数の VIP が設定されている場合には「all」が表示されます。**all** コマンド オプションまたは指定された VIP アドレスの場合、**show group portmap** 画面のフィールドには、個別のポート マッパーの情報が表示されます。
Current Mapped Ports	フローで現在使用中のポートの総数
Last Mapped Port	最も新しく NAT 変換されたフローに使用されたポート番号。このフィールドを Last Mapped VIP フィールドとともに使用して、最新の NAT 情報を取得します。

表 5-4　show group コマンド出力のフィールド（続き）

フィールド	説明
High Water Mark	最後のグループが起動されてからソース グループが同時にマップしたポートの最大数。このカウンタは、個々のポート マッパーの high water mark の合計と異なる場合があります。各ポート マッパーの high water mark は異なる時間に発生する場合があるからです。
Current Ctrl Channels	CSS が現在 NAT 変換している FTP 制御チャネルの合計数
No Portmap Errors	ポート マッパーによりポートが割り当てられなかった回数
Last Mapped VIP	CSS が最新の NAT 変換フローで使用する VIP アドレス。この VIP アドレスは、**all** コマンド オプションまたは指定した VIP アドレス オプションの VIP Address フィールドと同じです。このフィールドを Last Mapped Port フィールドとともに使用して、最新の NAT 情報を取得します。

ソース グループのカウンタのクリア

show group コマンドによって表示された統計情報をゼロにリセットするには、**zero all** コマンドを使用します。

次に使用例を示します。

```
(config-group[ftpgroup])# zero all
```