Configuring Source Groups for Services

A source group is a collection of local servers that initiate flows from within the local web farm. The CSS enables you to treat a source group as a virtual server with its own source IP address to which all IP addresses of services configured in the group will be translated. For example, if you configure several streaming audio transmitters as a group, the CSS will process flows from the group members and give them all the same source IP address.

This chapter describes how to configure source groups for services.

Information in this chapter applies to all CSS 11500 models except where noted.

Overview of Source Groups and Port Mapping

When you configure a source group, a CSS provides network address translation (NAT) of source IP addresses and port address translation (PAT) of source ports. NAT and PAT add a measure of security to your network by not exposing private network addresses and ports to the public side of a CSS. To NAT source IP addresses and source ports for flows originating from a server (server-side) on the private side of the CSS, add existing services to a source group. To NAT source IP addresses and source ports for flows originating from a client (client-side) on the public side of the CSS, add existing services to a source group as destination services. You can also configure access control lists (ACLs) to perform source NATing. For information about ACLs, refer to the *Cisco Content Services Switch Security Configuration Guide*.

Each CSS module (except the SSL module) has one session processor (SP) that is responsible for mastering flows.

- CSS 11501 supports one SP
- CSS 11503 supports a maximum of three SPs
- CSS 11506 supports a maximum of six SPs

The default number of source ports available for a single source group is 63488 (65533 minus the named ports). With one source group configured, the CSS allocates the total number of ports proportionally among all the SPs in the CSS chassis according to the SP relative weight value. To display the relative weight value of an SP, enter the **show chassis session-processors** command as described in the *Cisco Content Services Switch Administration Guide*. The SP relative weight value is not configurable.

For client-side flows, the CSS sends packets to different SPs for flow processing and the flows have access to the source ports in that SP. The CSS performs a simple XOR hash of the TCP or UDP source and destination port numbers to determine the SP that becomes master for that flow. If the port numbers are the same (for example, DNS UDP port 53), then the CSS uses the low order bits of the source and destination IP addresses to calculate the hash value. The CSS uses the hash value to index into a weighted table of SPs and selects the appropriate SP.

When the CSS performs PAT, the master SP for the flow uses a source port from either a source group or the global port mapper, depending on your configuration. (For information about global port mapping, see the "Configuring Global Port Mapping" section in Chapter 2, Configuring Flow and Port Mapping Parameters.)

The CSS chooses a source port so that the hash of the source port and the destination port will cause the CSS to select the same SP for the server-side flow as the SP that mastered the client-side flow.

For the server-side flow from a given destination port, only certain source port numbers hash to the same SP that was used for the client-side flow. For this reason, all ports *available* to a particular SP are not necessarily *eligible* for use when establishing the back-end connection. Therefore, the hash algorithm selects only a percentage of the available ports on any one SP.

To make more available source ports eligible for flows or to provide additional source ports for each SP, use one of the following methods:

- Configure a VIP address range for port mapping using the **portmap vip-address-range** command. For each additional VIP address that you configure for port mapping, you add one more port mapper to your configuration with another 63488 available ports. This method requires that you configure a destination service on a source group. For details, see "Configuring a VIP Address Range for Port Mapping" section.
- Configure services on different destination ports (vary the destination port) to broaden the hash across the SPs and allow a larger percentage of available ports to be eligible for port mapping. This strategy works by making the hashing algorithm less restrictive in the sense that now more source ports can be used to satisfy the hashing equations. Use this method when you cannot use the **vip-address-range** command because of limited server-side address space. For each additional destination port that you configure, the CSS receives an additional set of eligible source ports to use for port mapping as shown in the second column of Table 5-1. This method has the following requirements:
  - Configure your web server to listen on multiple ports (for example ports 80, 81, 82, and so on)
  - For each destination port, configure a new service on the CSS
  - Add the services to a content rule
  - Add the services as destination services to a source group
- Configure multiple source groups to provide an additional 63488 ports for each source group, which the CSS also distributes among the SPs in the same manner as described earlier in this section. This method requires that you:
  - Configure multiple IP addresses on your web server (IP aliases)
  - Create a new service on the CSS for each server IP address

- Add each service to a unique source group as a destination service
- Add the services to a content rule

Table 5-1 illustrates how the number of eligible ports in a CSS 11506 decreases as you increase the number of installed modules (SPs) and how you can dramatically increase the number of eligible ports by configuring a VIP address range for port mapping. In all cases, the CSS is configured with one service in one source group with a single destination port for all flows (for example, port 80). The numbers of eligible ports in Table 5-1 are approximate and are used for illustration only. Your results may vary depending on your configuration.

Table 5-1 Adding Modules (SPs) to a CSS 11506 Decreases the Number of Eligible Source Ports While Adding VIP Addresses for Port Mapping Increases the Number of Eligible Source Ports

Number of Modules (SPs)	Number of Eligible Source Ports for the Chassis	
	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

Table 5-2 shows that, by increasing the number of destination ports, even in a fully-loaded CSS 11506 (six SPs), you can dramatically increase the number of source ports that are eligible for port mapping. You can even more dramatically increase the number of eligible source ports by configuring a higher VIP address range for port mapping. In this example, the destination ports were chosen consecutively.

Table 5-2 Adding Destination Ports or Configuring a VIP Address Range for Port Mapping Increases the Number of Eligible Source Ports

Number of Dest Ports	Number of Eligible Source Ports for the Chassis	
	port-map vip-address-range = 1	port-map vip-address-range = 10
10	28788	287880
20	31757	317570
32	40000	400000

By comparing row six in Table 5-1 with row 1 in Table 5-2, you can see that increasing the number of destination ports to 10 more than doubles the number of source ports eligible for port mapping.

Note that it is algorithmically significant which destination ports you select to increase the number of eligible source ports and it is not a linear relationship. You may need to select several ranges of destination ports to produce the maximum number of eligible source ports.

Adaptive Session Redundancy (ASR) requires that both CSSs have the same number of SPs installed in the same relative order (skipping slots is acceptable) in each chassis. This requirement allows the port mapper to use the same port-selection algorithm used in a non-ASR configuration. There is no further restriction on the number of eligible source ports in an ASR configuration. For more information about ASR, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Source Group Configuration Quick Start

Use the procedure in Table 5-3 to configure a source group for TCP/UDP traffic. To configure a source group for FTP traffic, see the next section. Note that each source group requires a content rule that contains the same services and virtual IP address (VIP) as the source group.

Table 5-3 Source Group Configuration Quick Start

Task and Command Example

1. Create the source group. Source group names can be a maximum of 31 characters. The following example creates a source group ftpgroup.
`(config)# group ftpgroup`
The CLI transitions into config-group mode where you can configure attributes for the source group and activate it.
`(config-group[ftpgroup])#`

2. Configure the source group VIP address to which all service IP addresses will be translated. For example, enter: `(config-group[ftpgroup])# vip address 172.16.36.58` You can assign the same VIP address to multiple source groups, but only one of the source groups can be active at a time.

3. Add previously defined services to the source group. For example, enter:
`(config-group[ftpgroup])# add service server1`
`(config-group[ftpgroup])# add service server2`

4. Activate the source group. `(config-group[ftpgroup])# active` Because a VIP address can belong to only one active source group at a time, the CSS will not allow you to activate a second source group that contains the same VIP address as the one in the active source group.

Table 5-3 Source Group Configuration Quick Start (continued)

Task and Command Example

5. Create a content rule, add the same services and VIP that are configured in the source group, and activate the content rule. The content rule enables the CSS to match requests for the content rule VIP. When either server1 or server2 replies to the request, the CSS NATs the server IP addresses to the source group VIP.
 	
For example, enter:
 	
`(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`

The following running-configuration example shows the results of entering the commands in Table 5-3.

```
!************************** 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
```

Creating a Source Group

Group configuration mode allows you to configure a maximum of 255 source groups on a CSS. To access group configuration mode, use the **group** command from any mode except ACL and boot configuration modes. The syntax for this command is:

group *groupname*

Enter an existing or a new source group name from 1 to 31 characters.

For example, enter:

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

To view a list of existing source groups, enter:

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

Note You can also use the **group** command from within group mode to access or create another source group.

To remove a source group, enter:

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

Configuring the Source Group

This section describes how to configure a source group.

- Configuring a VIP Address for a Source Group
- Configuring a Service on a Source Group
- Adding a Destination Service to the Source Group

For information on configuring source group port mapping, see the "Configuring Source Group Port Mapping" section. After you configure a source group, you can activate it, as described in the "Activating and Suspending a Source Group" section.

Note To make certain modifications to an active source group, you must first suspend the source group using the **suspend** command. Such modifications include: changing the IP address to 0 or using the **no ip address command**, adding or removing a service or destination service, or using the **portmap** command.

Configuring a VIP Address for a Source Group

When a CSS performs NAT, it substitutes a VIP for the source IP address in flows originating from one of the group's sources or destined to one of the group's destinations if you configured the service with the **add destination service** command. NATing provides a measure of security by preventing the source IP address from being exposed on the Internet. You can assign the same VIP address to multiple source groups, but only one of the source groups can be active at a time.

Use the **vip address** command to specify the base VIP address for the group. The syntax for this group configuration mode command is:

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

The options and variables for this command are:

- *ip_or_host* - IP address or name for the group. Enter the address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

  The CSS restricts VIP and IP addresses on source groups to class A, B, or C addresses. The CSS does not allow multicast (class D and E) and IP addresses with ranges beyond the end of the address range.

- **range** *number* - (Optional) Defines the range of IP addresses for the group. Enter a *number* from 1 to 65535. The default is 1. The *ip_or_host* variable is the first address in the range.

  When configuring a source group with the same VIP address as a content rule, the VIP address range for the source group must be the same as the range for the content rule.

Note When you configure the base VIP address of a source group, be sure to leave enough address space for expansion in case the CSS uses all configured port-map entries and you need to increase the VIP address range used for port mapping. See the "Configuring a VIP Address Range for Port Mapping" section.

For example enter:

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

Configuring a Service on a Source Group

To NAT source IP addresses and source ports for flows originating from a server (server-side) on the private side of the CSS, add existing services to a source group. You can configure a maximum of 64 services per source group.

Note The CSS allows a maximum of 1024 services to be associated with source groups.

A service may belong to only one group at a time. When the source group is active and the same service is selected through a content rule, ACL preferred service or sorry service, the source group is used to NAT (Network Address Translation) the source address. The service must be active in order for it to perform source address NATing for the source group.

Be aware that you cannot use a service with:

- The same name in other source groups or use the destination service list within the same source group
- The same address as a source service on another source group

To add previously defined services to the source group, use the add service command. For example, enter:

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

To remove a previously configured service from a source group, use the **remove service** command. For example, to remove service server1 from the source group, enter:

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

Adding a Destination Service to the Source Group

To NAT source IP addresses and source ports for flows originating from a client (client-side) on the public side of the CSS, add existing services to a source group as destination services. You can configure a maximum of 64 services per source group. Be aware that:

- You cannot use a service with the same name in other source groups or use the source service list within the same source group.
- You can use services with duplicate addresses among destination services because the actual service is chosen through content rule selection.
- The destination service must be active and must be added to a content rule for it to perform destination source address NATing for the source group (see Chapter 10, Configuring Content Rules).

Note When the service initiates the flows, adding a destination service to a source group does not allow the destination service flows to be NATed by the source group. This is because the destination service applies group membership based on rule and service match criteria. To ensure that service-initiated connections are NATed, you must also configure ACL match criteria or additional service names with duplicate addresses, and then add those services to a source group. The source group used could be the current source group with the destination service or any other configured source group.

Use the **add destination service** command to add a destination service to a source group. For example, enter:

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

To remove a previously configured destination service from a source group, use the **remove** command.

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

Activating and Suspending a Source Group

When you activate a source group, the CSS uses it to NAT (Network Address Translation) the source IP address. After you configure a source group, you can activate it. Because a VIP address can belong to only one active source group at a time, the CSS does not allow you to activate a second source group that contains the same VIP address as the one in the active source group.

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

Suspend the source group when you need to change its configuration. The group and its attributes remain the same but no longer have an effect on flow creation. Use the **suspend** command to suspend a source group. For example, enter:

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

Configuring Source Group Port Mapping

By default, PAT or port mapping is enabled for source groups on source ports greater than 1023. The CSS translates such source ports to a range starting at 2016. The following sections provide information about how to change the default PAT behavior of the CSS:

- Configuring the Starting Port Number
- Configuring the Total Number of Ports in a Port-Map Range
- Configuring a VIP Address Range for Port Mapping
- Disabling Port Mapping

Before configuring an active source group, make sure that you suspend it.

Configuring the Starting Port Number

By default, the base port (starting port number) for the CSS is 2016. The **portmap base-port** command defines the base port for the CSS. You can enter a base port value from 2016 to 63456. For example, to configure a base port of 3354, enter:

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

To reset the base port to its default value of 2016, use the **no portmap base-port** command. For example, enter:

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

Configuring the Total Number of Ports in a Port-Map Range

The CSS allocates the total number of configured ports proportionally among all the SPs in the CSS chassis according to the session processor relative weight value. To display the relative weight value of a session processor, enter the **show chassis session-processors** command as described in the *Cisco Content Services Switch Administration Guide*.

The more modules you add to the CSS chassis, the less session processing each module performs and the fewer ports the CSS makes available to each module. To display the number of ports that the CSS allocates to each module, enter the **show group portmap** command as described in the "Showing Source Groups" section. For more information about the port mapping behavior of the CSS, see the "Configuring Source Group Port Mapping" section.

By default, the total number of ports in the port-map range for the entire CSS is 63488. This default value should be fine for most applications. To define the total number of ports in the port-map range, use the **portmap number-of-ports** command. Enter a number from 2048 to 63488. If you enter a value that is not a multiple of 32, the CSS rounds up the value to the next possible multiple of 32. For example, to configure the total number of ports to 2048, enter:

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

To reset the number of ports to the default value, use the **no portmap number-of-ports** command. For example, enter:

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

Configuring a VIP Address Range for Port Mapping

For each source group that you configure, a maximum of 63488 (the default) source ports are available for port mapping. However, not all available ports are eligible for flows. For details about source groups and port mapping, see the "Overview of Source Groups and Port Mapping" section.

To increase the number of available ports for port mapping, you can configure the port mapper with additional VIP addresses by specifying a range of VIPs. For each additional VIP address that you configure, the CSS creates a new port mapper to manage the available ports for that VIP. When the CSS performs PAT, the source group roundrobins among all the configured port mappers and the selected port mapper chooses the next eligible port for a given VIP.

Note that configuring a VIP address range for port mapping is different from a Virtual Web Hosting (VWH) configuration where you configure a VIP address range on a source group, not the port mapper. In a VWH configuration, there is only one port mapper available. For information about VWH, see the "Configuring Virtual Web Hosting" section in Chapter 10, Configuring Content Rules.

The CLI enforces the following configuration restrictions:

- You cannot configure virtual Web hosting and a port mapper VIP address range in the same source group. For information about virtual Web hosting, see the "Configuring Virtual Web Hosting" section in Chapter 10, Configuring Content Rules.
- You cannot configure a service (using the **add service** command) and a port mapper VIP address range in the same source group. For information about the **add service** command, see the "Configuring a Service on a Source Group" section.
- You cannot configure a port mapper VIP address range in a source group that is used by an ACL. The reverse is also true. For information about ACLs, refer to the *Cisco Content Services Switch Security Configuration Guide*.
- You can configure a maximum of 255 port mappers on one CSS. You can reach this limit by configuring any of the following:
  - A port-map VIP address range of 255 on one source group
  - A port-map VIP address range of 1 on 255 source groups
  - A combination of port-map VIP address ranges configured on a number of source groups that total 255 port mappers
- Configure the same VIP address ranges on a port mapper and content rule with the same VIP addresses. The maximum VIP address range for a content rule is 65535, greater than the range of 255 allowed on the port mapper. If you need to create a rule with a VIP address range greater than 255, create multiple rules with smaller ranges instead.

To configure additional VIP addresses for the port mapper of a source group, use the **portmap vip-address-range** command in group configuration mode. The syntax of this command is:

portmap vip-address-range *number*

The *number* variable indicates a range of VIP addresses starting with the address specified by the **vip address** command in group configuration mode. Enter an integer from 1 to 255. The default is 1. For information about configuring a VIP address for a source group using the **vip address** command, see the "Configuring a VIP Address for a Source Group" section.

Note When you configure the base VIP address of a source group, be sure to leave enough address space for expansion in case the CSS uses all configured port-map entries and you need to increase the VIP address range used for port mapping. See the "Configuring a VIP Address for a Source Group" section.

Note If you observe no-portmap errors, configure the **portmap vip-address-range** command and set the range to a value greater than that required to support the maximum number of active connections that you anticipate for your application

With a VIP range of 255, the maximum number of eligible ports on an SCM in a fully populated CSS 11506 chassis is 63240. For other SPs or chassis configurations, the number of ports is greater.

For example, to configure the port mapper of a source group with three VIP addresses, enter:

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

If the configured VIP for the source group is 192.168.44.3, then, after entering the above **portmap vip-address-range** command, the three available VIPs for the port mapper would be:

- 192.168.44.3
- 192.168.44.4
- 192.168.44.5

To reset the VIP address range to the default value of 1, enter:

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

Disabling Port Mapping

By default, the CSS NATs source IP addresses *and* PATs source ports for a configured source group. If you configure the **portmap disable** command in a source group, the CSS performs NAT on the source IP addresses but does not perform PAT on the source ports of UDP traffic that matches on that source group.

For UDP applications with high-numbered assigned ports (for example, SIP and WAP), we recommend that you preserve those port numbers by configuring destination services in source groups instead of using the **portmap disable** command. Destination services cause the CSS to NAT the client source ports, but not the destination ports. For information about configuring destination services, see Chapter 3, Configuring Source Groups for Services.

Note If you disable flows for a UDP port using the flow-state table and configure the **portmap disable** command in a source group, traffic for that port that matches on the source group may be returned to the client on an unrecognizable port number. For information about the flow-state table, see Chapter 2, Configuring Flow and Port Mapping Parameters.

The CSS maintains but ignores any **base-port** or **number-of ports** (see the previous options) values configured in the source group. If you later reenable PAT for that source group, any configured **base-port** or **number-of ports** values will take effect. The default behavior for a configured source group is to NAT the source IP address and to PAT the source port for port numbers greater than 1023.

Note The **portmap disable** command does not affect TCP flows.

To disable port mapping, enter:

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

To restore the default CSS behavior of NATing source IP addresses *and* PATing source ports for a configured source group, use the **portmap enable** command. For example, enter:

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

Configuring Source Groups and ACLs

For the CSS to perform NAT for traffic destined to the Internet and not to perform NAT for local traffic, you can use ACLs with source groups to make the decision based on the destination IP address in the ACL.

In the following example, clients on 10.0.1.0 and 10.0.2.0 private subnets want to communicate with each other without the source group NATing their traffic. Three VLANs exist, one for each subnet (VLAN1 and VLAN2) and a VLAN to the Internet through the source group (VLAN3).

1. Create a source group and activate it. In this example, the source group is named outbound and has a VIP address of 192.168.1.10.

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

   Note that the VIP address in the source group must be a public address allowing the routing of response traffic to the CSS. The address can be an IP address in the same subnet as the IP address configured for the VLAN3 circuit (but not the same IP address), or a different public IP address that the routers in the network have static routes pointing to the CSS.

2. Create an ACL that allows the clients on the private subnet to communicate to each other. The following ACL and clause allows clients on 10.0.1.0 subnet to communicate with clients on 10.0.2.0 subnet without the source group using NATing because the CSS uses the bypass option to route the traffic and bypass all rules configured on the CSS.

   ```
   (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. Add a clause to direct all other traffic from the clients on the 10.0.1.0 subnet to the source group, allowing the source IP address to use NAT to connect to 192.168.1.10.

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

4. Add a clause 1 to permit the keepalives for the services on the CSS.

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

5. Apply the ACL to VLAN1.

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

6. If you want to allow traffic from the servers on VLAN2 to the source group but also allow the servers to communicate with VLAN1 without using a NAT IP address, configure the following ACL for VLAN2.

```
(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. For inbound traffic from the Internet, configure an ACL for VLAN3.

```
(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. Globally enable all ACLs on the CSS.

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

Configuring a Source Group for FTP Connections

To use source groups to support FTP sessions to a VIP that is load balanced across multiple services, configure a content rule for the VIP and then a source group.

Note When you use an FTP content rule with a configured VIP address range, be sure to configure the corresponding source group with the same VIP address range (see Chapter 10, Configuring Content Rules).

To configure FTP sessions to a VIP:

1. Configure a content rule as required using the VIP that will be load balanced across multiple servers. The following example shows the portion of a running-config for content rule ftp_rule. Ensure that you use the **application ftp-control** command to define the application type.

```
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. Configure a source group defining the same VIP and services as configured in the content rule.

Note If you are load-balancing passive FTP servers, you must configure services directly in the associated source groups as shown in the following example.

The following running-config example shows source group ftp_group.

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

By default, the CSS waits 5 seconds to initiate the FTP data channel on an active or passive FTP connection for CSS FTP content rules and source groups. You can globally configure the time to wait to initiate the FTP data channel on an active or passive FTP connection. For more information, see the "Configuring the Wait Time to Initiate the FTP Data Channel"section in Chapter 10, "Configuring Content Rules".

Configuring Source Groups to Allow Servers to Resolve Domain Names Using the Internet

The CSS provides support to enable servers to resolve domain names using the Internet. If you are using private IP addresses for your servers and wish to have the servers resolve domain names using domain name servers that are located on the Internet, you must configure a content rule and source group. The content rule and source group are required to specify a public Internet-routable IP address (VIP address) for the servers to allow them to resolve domain names.

To configure a server to resolve domain names:

1. If you have not already done so, configure the server.

   The following example creates Server1 and configures it with a private IP address 10.0.3.251 and activates it.

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

2. Create a content rule to process DNS replies. The content rule to process DNS replies is in addition to the content rules you created to process Web traffic. The content rule example below enables the CSS to NAT inbound DNS replies from the public VIP address (192.168.200.200) to the server's private IP address (10.0.3.251).

   The following example creates content rule dns1 with a public VIP 192.168.200.200 and adds server Server1.

   ```
   (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. Create a source group to process DNS requests. The source group enables the CSS to NAT outbound traffic source IP addresses from the server's private IP address (10.0.3.251) to the public VIP address (192.168.200.200).

   To prevent server source port collisions, the CSS NATs the server's source IP address and port by translating the:

   - Source IP address to the IP address defined in the source group.
   - Port to the port selected by the source group. The source group assigns each server a unique port for a DNS query so that the CSS can match the DNS reply with the assigned port. This port mapping enables the CSS to direct the DNS reply to the correct server.

   The following example creates source group dns1 with public VIP address 192.168.200.200 and adds the service Server1.

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

Showing Source Groups

To display source group configuration information, use the **show group** commands in SuperUser, User, Global Configuration, and Group modes. The options are:

- **show group** - Displays all source group configurations.
- **show group** *group_name* - Displays the source group configuration specified by *group_name*. You cannot specify a group name in Group mode.
- **show group** *group_name* **portmap** - Displays detailed port mapping information for each SP in a CSS.
- **show group** *group_name* **portmap all** - Displays detailed port mapping information about each SP in a CSS for all VIP addresses of the source group port mapper.
- **show group** *group_name* **portmap** *ip_address* - Displays detailed port mapping information about each SP in a CSS for the specified VIP address of the source group port mapper.

For example, enter:

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

Table 5-4 describes the fields in the **show group** command output.

Table 5-4 Field Descriptions for the show group Command Output

Field	Description
Group	Name of the group, whether the group is activated (Active) or suspended (Suspend), and the source IP address for the group.
Portmap VIP Range	Number of configured VIP addresses that the port mapper can use for NAT and the address range.
Session Redundancy	Indicates whether ASR is enabled or disabled for the source group. For details on ASR, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.
Redundancy Global Index	The unique global index value for Adaptive Session Redundancy assigned to the source group using the **redundant-index** command in group configuration mode.
Associated ACLs	Any ACLs associated with the group.
Source/Destination Services	The source or destination services of the source group.
Name	The name of the service.
Hits	The number of content accessed (hit) on the service. This field is incremented for traffic from a group server going out from the source group. Traffic coming into the group does not increment the counter.
State	The state of the service. The possible states are Alive, Dying, or Dead.
DNS Load	The DNS load for the service. A load of 255 indicates that the service is down. An eligible load range is from 2 to 254.

Table 5-4 Field Descriptions for the show group Command Output (continued)

Field	Description
Trans	The number of times that the state of the service has transitioned.
Keepalive	The keepalive type of the service. The possible types are FTP, HTTP, ICMP, NAMED, SCRIPT, or TCP.
Conn	The number of connections currently on the service.
Flow Timeout Multiplier	Number of 16-second multiples that a flow remains idle before the CSS reclaims the flow resources, as configured with the **flow-timeout-multiplier** command. For details on the **flow-timeout-multiplier** command, refer to the Chapter 2, Configuring Flow and Port Mapping Parameters.
Group Service Total Counters	The counters for the group.
Hits/Frames/Bytes	The number of group hits, frames, and bytes. This field is incremented for traffic from a group server going out from the source group. Traffic coming into the group does not increment the counter.
Connection Total/Current	The total number of connections and the current number of connections for the group.
FTP Control Total/Current	The total number of FTP control channels that were mapped and monitored by the CSS, and the current number of those connections that are mapped.
SP Port Map Info	The port map information for each SP in the CSS. Includes the status of the **portmap** command (Enabled or Disabled).
Configured Base Port	The configured starting port number.
Configured Ports per VIP	The total number of ports on each VIP address in the CSS. If the number is not a multiple of 32, the CSS rounds the number up to the next multiple of 32.
Slot	The slot in the CSS chassis where the module resides.

Table 5-4 Field Descriptions for the show group Command Output (continued)

Field	Description
Subslot	The subslot in the module where the SP resides.
Ports Avail to this SP	The total number of source ports available to the SP.
VIP Address	The configured VIP address of the port mapper. For the **show group portmap** command, the CSS displays "all" if there are multiple configured VIPs. For the **all** command option or for a specified VIP address, the fields in the **show group portmap** screen contain information specific to individual port mappers.
Current Mapped Ports	The total number of ports currently in use for flows.
Last Mapped Port	The port number that the CSS used for the most recent NATed flow. Use this field with the Last Mapped VIP field to obtain the latest NAT information.
High Water Mark	The highest number of ports that this source group has had concurrently mapped since the last group was activated. This counter may not be equal to the sum of all individual port mapper high water marks because the high water marks for each port mapper may occur at different times.
Current Ctrl Channels	The total number of FTP control channels that the CSS is currently NATing.
No Portmap Errors	The number of times no port could be allocated by the port mapper.
Last Mapped VIP	The VIP address that the CSS used in the most recently NATed flow. This is the same as the VIP Address field for the **all** command option or a specified VIP address option. Use this field with the Last Mapped Port field to obtain the latest NAT information.

Clearing Source Group Counters

To clear the service and portmap statistics for all source groups displayed through the **show group** command, use the **zero group statistics** command. This command is available in all modes.

For example, enter:

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

To clear the statistics for the group in the current mode, use the **zero all** command in group configuration mode.

For example, enter:

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