Deployment Guide

Blue Coat CacheFlow Transparent Cache Switching

TABLE OF CONTENTS

1 INTRODUCTION

The demand for bandwidth has increased drastically over recent years, as megabyte-hungry Web 2.0 technology and mobile devices insatiably consume new capacity as soon as it becomes available. According to TeleGeography, a global bandwidth research service, the demand for international bandwidth grew 45 percent in 2011, while the compounded rate of growth was 57 percent annually between 2007 and 2011. In addition, rich media content has increased and the migration of traditional television content to the Internet is accelerating the demand for more bandwidth.

Blue Coat CacheFlow appliances provide a high performance caching solution that enables service providers to manage the drastic increase in network traffic and rapid subscriber growth. Utilizing highly effective Web caching technology, CacheFlow appliances save bandwidth on expensive international links and backhaul traffic, while improving the end-user Web experience.

To maximize the efficiency of the CacheFlow devices, the A10 Thunder Series and AX Series Application Delivery Controllers (ADCs) can balance the traffic flows for Blue Coat CacheFlow appliances.

2 DEPLOYMENT GUIDE OVERVIEW

This deployment guide shows how to install and deploy the A10 ADC with Blue Coat CacheFlow caching appliances. The deployment guide focuses on how end-user HTTP (80) requests can be served using Transparent Cache Switching (TCS) with the Thunder Series and AX Series ADCs. The configuration sections show how to deploy load balancing , health monitoring, DDoS protection, and device persistence for each traffic flow for Blue Coat CacheFlow appliances.

3 DEPLOYMENT GUIDE PREREQUISITES

This Blue Coat CacheFlow integration was tested with the following setup:

A10 tested configuration:

- The A10 Networks ADC must be running ACOS version 2.7.x or higher
- Blue Coat CacheFlow integration was tested with AX Series hardware-based appliances, as well as SoftAX virtual appliances.
- Blue Coat CacheFlow appliance requirements:
  - ♦ Blue Coat CacheFlow 5000
  - ♦ CacheFlow Release 3.2.2.3 or higher

Note: *The features described in this guide are supported in Thunder Series and AX Series devices. Testing was performed using an AX device.*

4 ACCESSING THE ACOS DEVICE

This section describes how to access the AX Series device from a Command Line Interface (CLI) or Graphical User Interface (GUI):

- CLI – The CLI is a text-based interface in which you type commands on a command line. You can access the CLI directly through the serial console or over the network using either of the following protocols:
  - ♦ Secure protocol – Secure Shell (SSH) version 2
  - ♦ Unsecure protocol – Telnet (if enabled)
- GUI – This is a web-based interface in which you click buttons, menus and other graphical icons to access the configuration or management pages. From these pages, you can type or select values to configure or manage the device. You can access the GUI using the following protocol:
  - ♦ Secure protocol – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

Note: *HTTP requests are redirected to HTTPS by default on the AX device.*

Default Access Information:

- Default Username: “admin”
- Default password: “a10”
- Default IP Address of the device: “172.31.31.31”

For detailed information on how to access the AX Series device, refer to the *System Configuration and Administration Guide*.

5 ARCHITECTURE OVERVIEW

The figure below shows a simplified topology for the A10-Blue Coat solution. The deployment of the Blue Coat CacheFlow appliance is simple, with no modification required to the subscriber's browser or other applications. Request traffic is redirected from the AX device to the next available Blue Coat CacheFlow appliance based on the load balancing algorithm; or, in the event of cache server outage, traffic will be redirected transparently back to the source server (Internet).

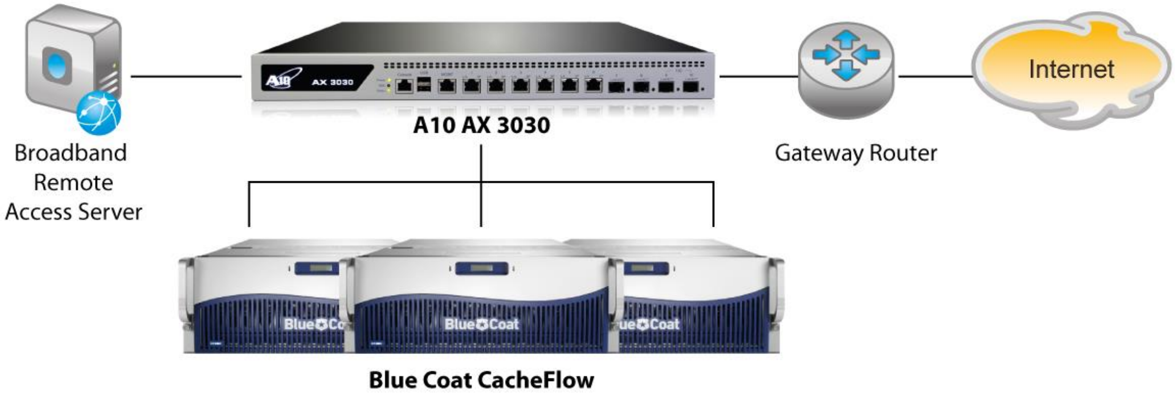
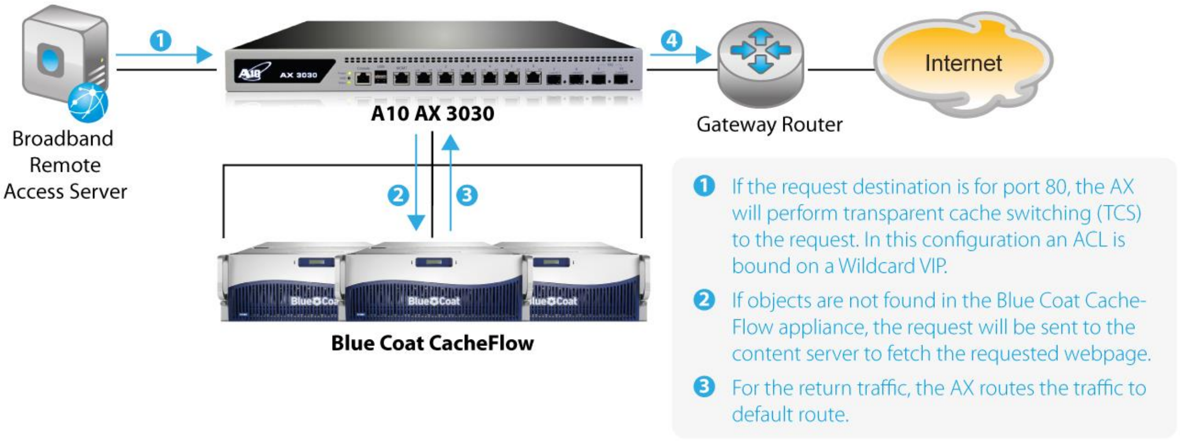


Figure 1: Architecture overview

5.1 TRAFFIC WORKFLOW: HTTP REQUEST

This section explains the basic workflow for a subscriber request based on HTTP (port 80) traffic. The solution shown here can be applied to any protocol port. The most common ports used in Transparent Cache Switching are port 443 (HTTPS) and port 21 (FTP).

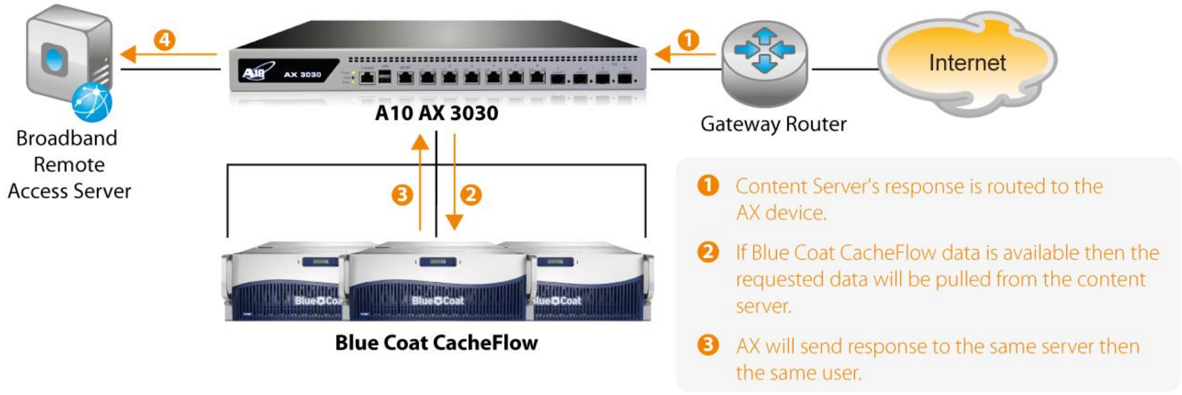


1. If the request destination is for port 80, the AX will perform transparent cache switching (TCS) to the request. In this configuration an ACL is bound on a Wildcard VIP.
2. If objects are not found in the Blue Coat Cache-Flow appliance, the request will be sent to the content server to fetch the requested webpage.
3. For the return traffic, the AX routes the traffic to default route.

Figure 2: HTTP request

5.2 TRAFFIC WORKFLOW: HTTP RESPONSE

This section explains the HTTP response from the content servers, based on a subscriber's request.



1 Content Server's response is routed to the AX device.

2 If Blue Coat CacheFlow data is available then the requested data will be pulled from the content server.

3 AX will send response to the same server then the same user.

Figure 3: HTTP Response

6 CONFIGURATION

This section provides detailed instructions for configuring SLB resources (real servers, service group, virtual services, and virtual services) for load balancing traffic to Blue Coat CacheFlow appliances.

The tested configuration is based on “routed mode” deployment, which offers multiple benefits. It is a simple and non-intrusive installation that requires no configuration changes on the clients or the servers. In addition, the servers retain the ability to see clients' real IP addresses.

When deploying an ACOS device in routed mode, there are a few points to keep in mind:

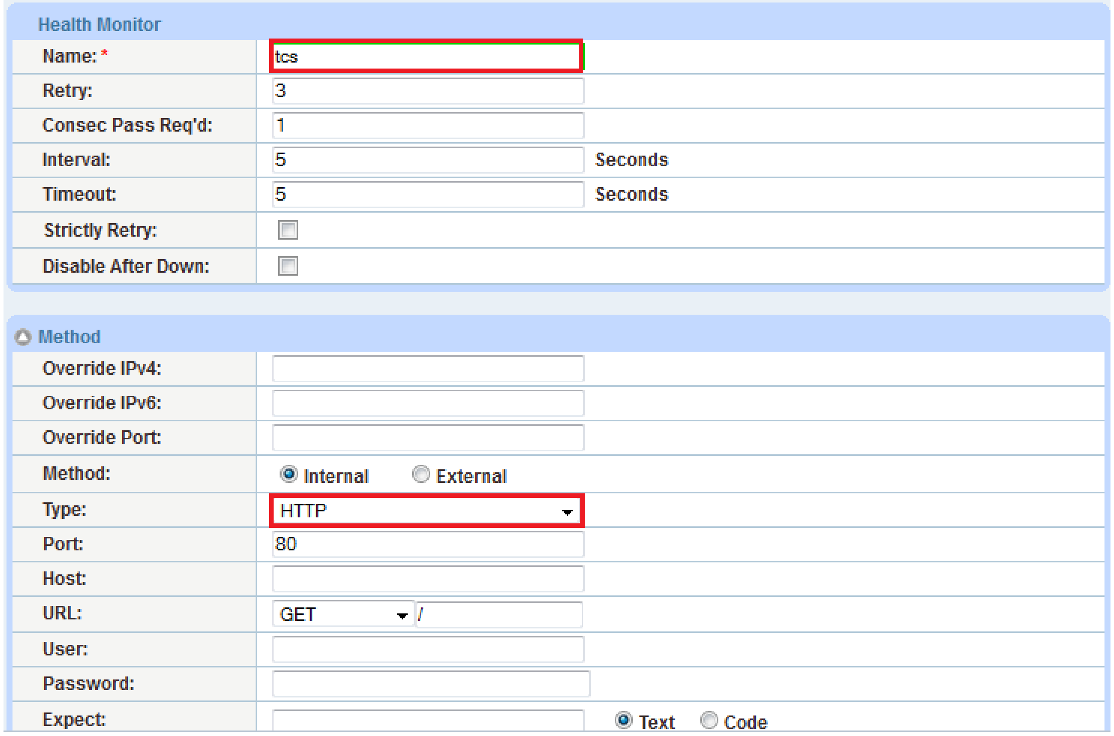
- The servers must use the ACOS device as their default gateway.
- The clients must be on a different subnet than the servers.
- Before you start the configuration, you must create templates, such as health monitoring templates.

7 HEALTH MONITOR CONFIGURATION

A10 Thunder Series and AX Series ADCs can be configured to automatically initiate health status checks for real servers and service ports. Health checks are used to assure that all requests are sent to functional and available servers. If a server (or a service) does not respond appropriately to a health check, the server is temporarily removed from the list of available servers until it starts responding appropriately to the health checks. At this point, the server is automatically added back to the list of available servers.

To configure a health check on the ACOS device:

1. Navigate to **Config Mode > SLB > Service**.
2. Select **Add** from the **Health Monitor** drop-down list. In the **Name** field, enter “tcs”.
3. Select **Method** “HTTP”.
4. Click **OK**, and then proceed to the next section to create a real server configuration for each Blue Coat CacheFlow appliance.



Health Monitor

Name: *	tcs	
Retry:	3	
Consec Pass Req'd:	1	
Interval:	5	Seconds
Timeout:	5	Seconds
Strictly Retry:	□	
Disable After Down:	□	

Method

Override IPv4:		
Override IPv6:		
Override Port:		
Method:	● Internal ○ External	
Type:	HTTP	
Port:	80	
Host:		
URL:	GET /	
User:		
Password:		
Expect:		● Text ○ Code

Figure 4: Health monitor configuration

8 SERVER CONFIGURATION

Follow the procedure below to create server configurations in ACOS for the Blue Coat CacheFlow appliances.

1. Navigate to **Config Mode > Service > SLB > Server**.

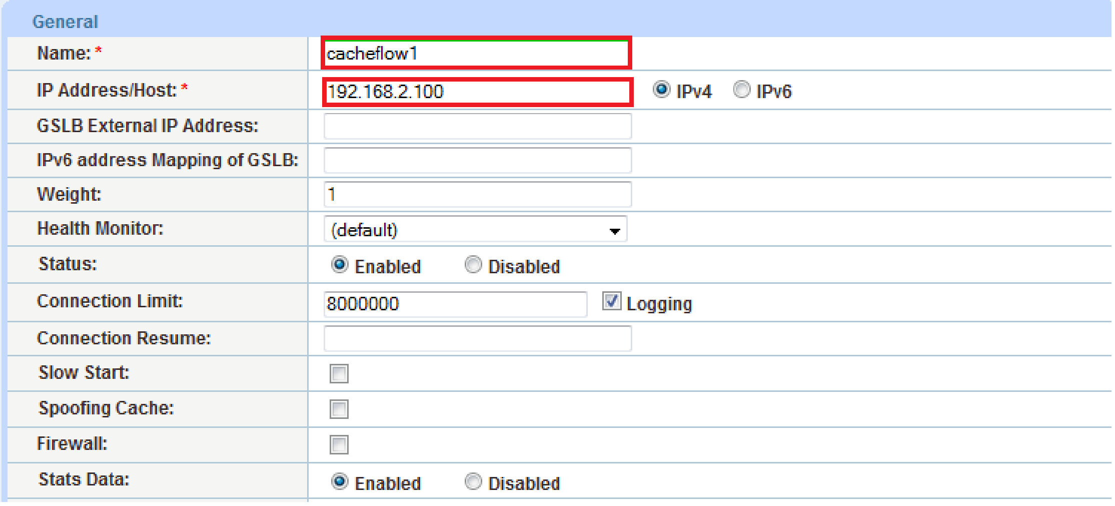
2. Click **Add** to add a new server.

3. Within the Server section, enter the following required information:

   - **Name:** "cacheflow1"

   - **IP address/Host:** "192.0.2.100"

Note: *Enter additional servers if necessary.*



General

Name: *	cacheflow1
IP Address/Host: *	192.168.2.100 ● IPv4 ○ IPv6
GSLB External IP Address:	
IPv6 address Mapping of GSLB:	
Weight:	1
Health Monitor:	(default)
Status:	● Enabled ○ Disabled
Connection Limit:	8000000 ☑ Logging
Connection Resume:	
Slow Start:	□
Spoofing Cache:	□
Firewall:	□
Stats Data:	● Enabled ○ Disabled

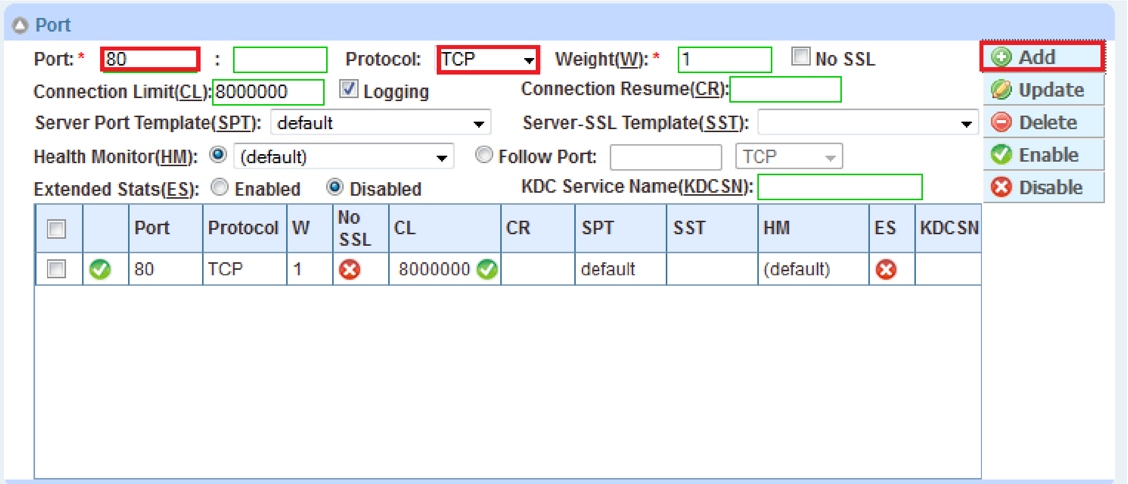
Figure 5: Server configuration

4. To add a port to the server configuration:

   a. Enter the port number in the **Port** field.

   b. Select the **Protocol**.

   c. Click **Add**.



Port: * 80 : Protocol: TCP Weight(W): * 1 □ No SSL

Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):

Server Port Template(SPT): default Server-SSL Template(SST):

Health Monitor(HM): ● (default) ○ Follow Port: TCP

Extended Stats(ES): ○ Enabled ● Disabled KDC Service Name(KDCSN):

□		Port	Protocol	W	No SSL	CL	CR	SPT	SST	HM	ES	KDCSN
□	✓	80	TCP	1	☒	8000000 ✓		default		(default)	☒	

Figure 6: Server port configuration

Note: *If you need to add additional ports, you can add it to the port list by following the same* instructions *above.*

5. Click **OK**, and then click **Save** to save the configuration.

9 SERVICE GROUP CONFIGURATION

Follow the procedure below to configure a service group.

1. Navigate to **Config Mode > Service > SLB > Service Group**.

2. Click **Add**.

3. Enter or select the following values:

   - **Name:** "cacheflowsg"

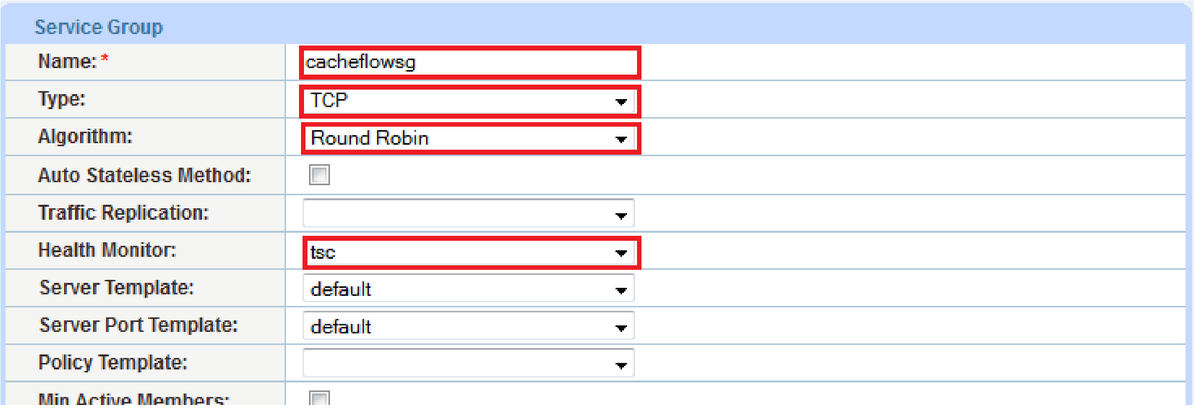
   - **Type:** "TCP"

   - **Algorithm:** "Round Robin"

   - **Health Monitor:** "tsc"

4. In the Server section, select a server from the Server drop-down list and enter "80" in the **Port** field.

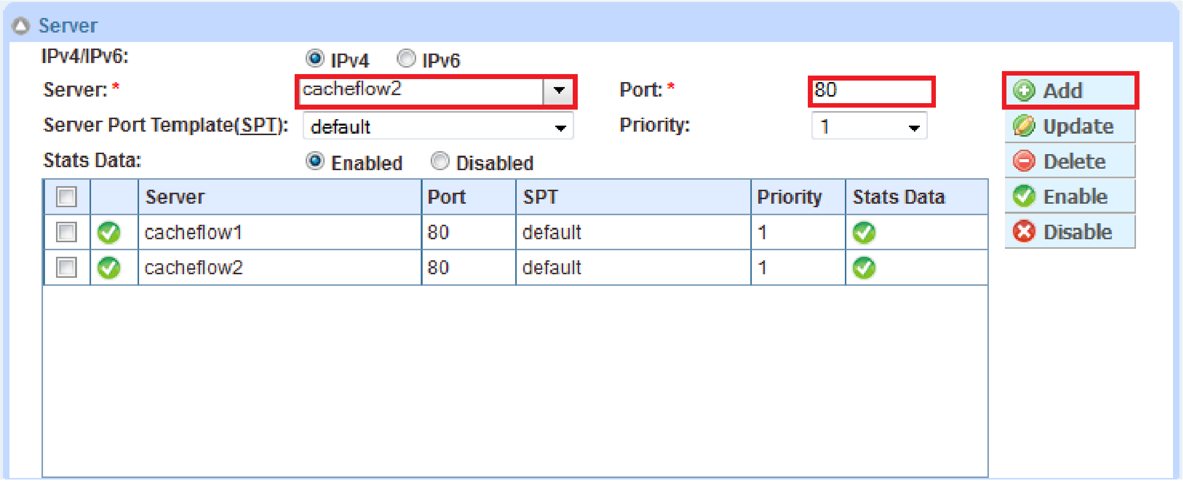
5. Click **Add**. Repeat for each server.



Service Group

Name: *	cacheflowsg
Type:	TCP
Algorithm:	Round Robin
Auto Stateless Method:	□
Traffic Replication:	
Health Monitor:	tsc
Server Template:	default
Server Port Template:	default
Policy Template:	
Min Active Members:	□

Figure 7: Service group configuration



Server

IPv4/IPv6: ● IPv4 ○ IPv6

Server: * cacheflow2

Port: * 80

Server Port Template(SPT): default

Priority: 1

Stats Data: ● Enabled ○ Disabled

□		Server	Port	SPT	Priority	Stats Data
□	✓	cacheflow1	80	default	1	✓
□	✓	cacheflow2	80	default	1	✓

Figure 8: Server configuration

Note: *If you have other ports such as "443", you will be required to create another service group.*

6. Click **OK**, then click **Save** to save the configuration.

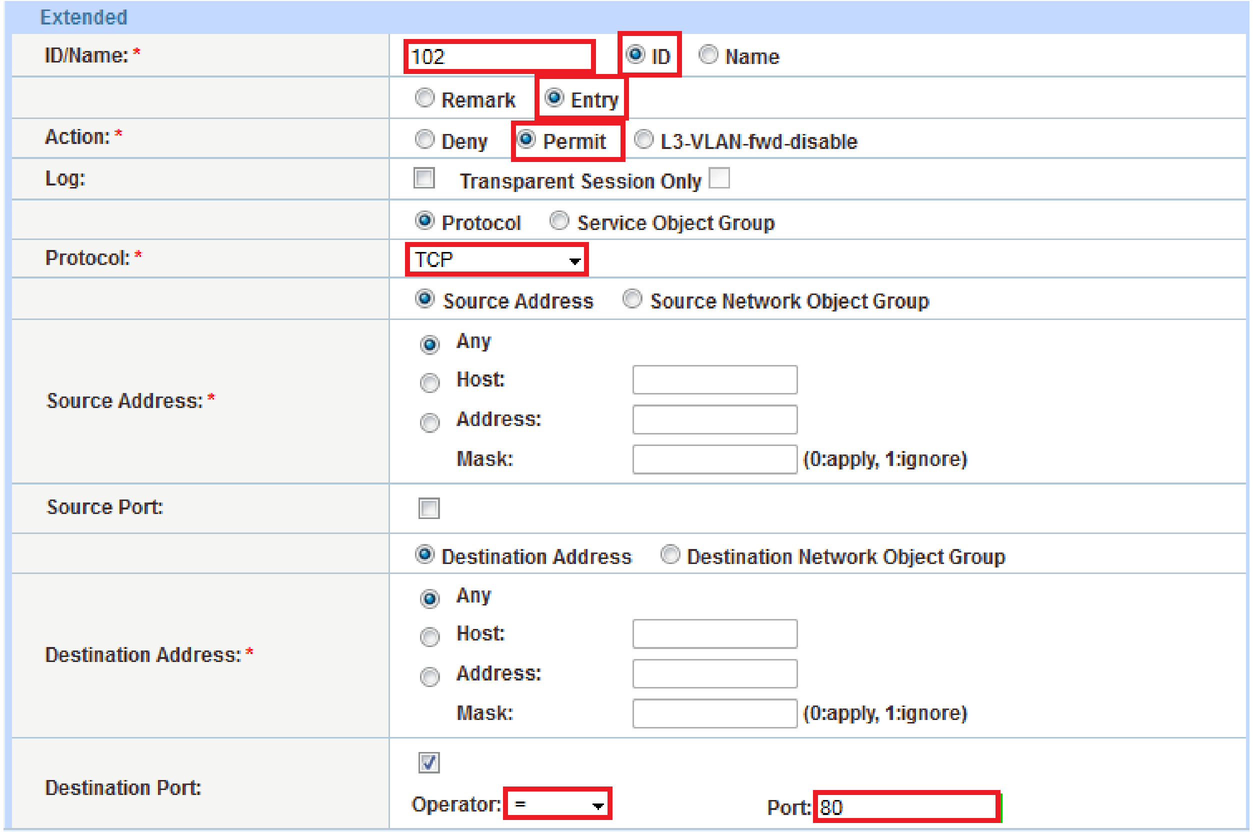
10 ACCESS LIST CONFIGURATION

Before the configuring virtual server, you are required to create an Access Control List (ACL). The ACL must use the permit action, and match on client addresses as the source address, and on the content server address(es) as the destination address. During configuration of the virtual server, you bind the ACL to the virtual server.

1. Navigate to **Config Mode > Security > Network > ACL**.
2. Select **Extended** and click **Add**.

   Enter the following values:

   - Enter **ID/Name**: 102 and select **ID**.
   - Select **Entry**.
   - Select "**Permit**" from the Action area.
   - From the drop-down menu, select "TCP".
   - The source address and destination address will vary based on your IP addresses.
   - **Destination port** must be selected:
     - Operator: **"="**
     - Port: "80"
3. Click **OK**, then click **Save** to save the configuration.



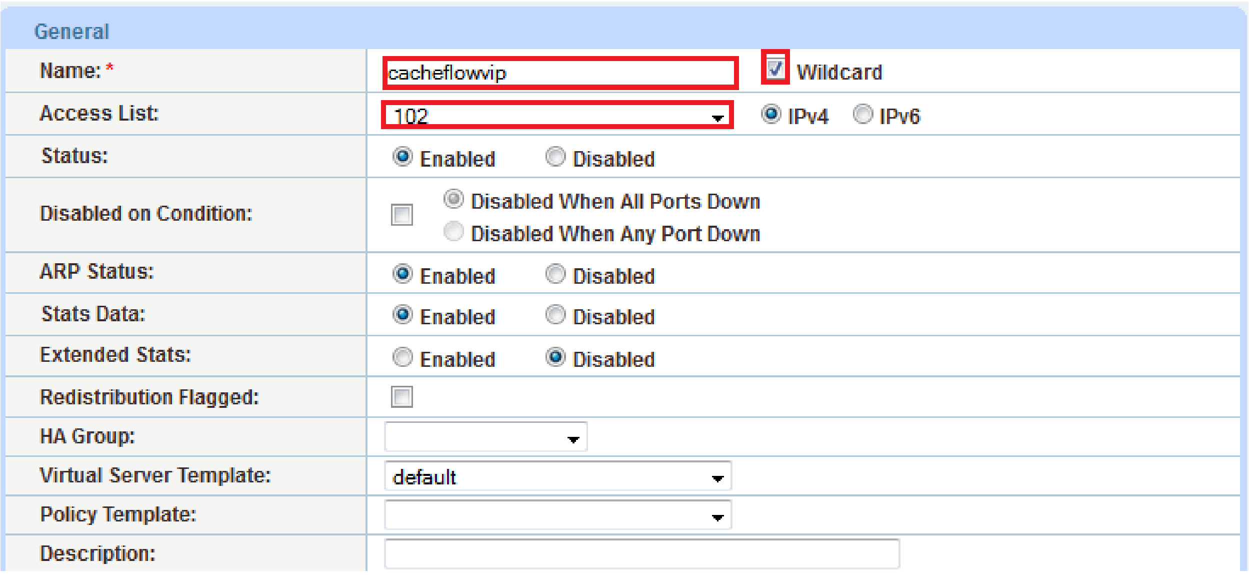
Extended	
ID/Name: *	102 ● ID ○ Name
	○ Remark ● Entry
Action: *	○ Deny ● Permit ○ L3-VLAN-fwd-disable
Log:	□ Transparent Session Only □
	● Protocol ○ Service Object Group
Protocol: *	TCP
	● Source Address ○ Source Network Object Group
Source Address: *	● Any ○ Host: ○ Address: Mask: (0:apply, 1:ignore)
Source Port:	□
	● Destination Address ○ Destination Network Object Group
Destination Address: *	● Any ○ Host: ○ Address: Mask: (0:apply, 1:ignore)
Destination Port:	☑ Operator: = Port: 80

Figure 9: ACL configuration

11 VIRTUAL SERVER CONFIGURATION

This section contains the configuration of a wildcard virtual server. Also known as a "Virtual IP" (VIP), the virtual server has the IP address (VIP) that a client accesses during an initial request.

1. Navigate to **Config Mode > Service > SLB > Virtual Server**.
2. In the **General** section, enter the following:
   - **Name**: “cacheflowvip”
   - **Wildcard**: Select the checkbox.
   - **Access List**: select "102" from the drop-down menu.

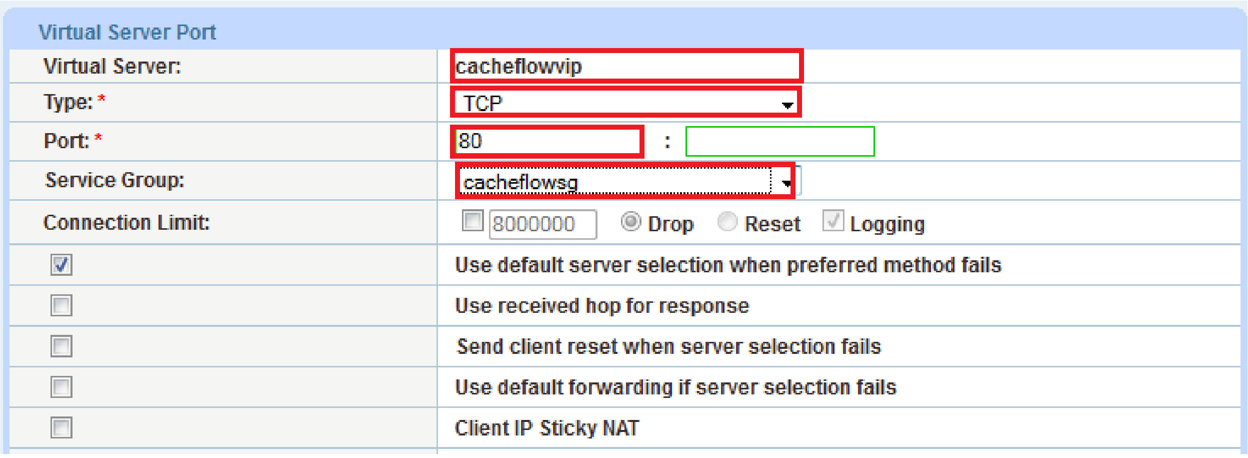


General

Name: *	cacheflowvip ☑ Wildcard
Access List:	102 ● IPv4 ○ IPv6
Status:	● Enabled ○ Disabled
Disabled on Condition:	□ ● Disabled When All Ports Down ○ Disabled When Any Port Down
ARP Status:	● Enabled ○ Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Redistribution Flagged:	□
HA Group:	
Virtual Server Template:	default
Policy Template:	
Description:	

Figure 10: Virtual server configuration

3. In the **Port** section, click **Add**.
4. Enter or select the following values:
   - **Virtual Server:** "cacheflowvip"
   - **Type:** “TCP”
   - **Port:** “80”
   - **Service Group:** “cacheflowsg”



Virtual Server Port

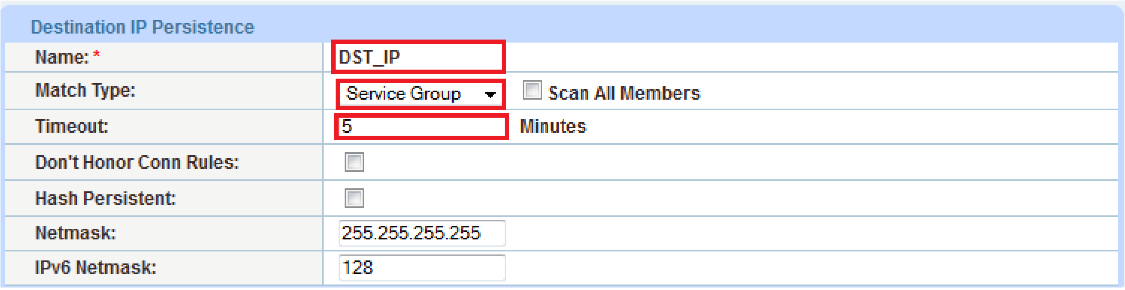
Virtual Server:	cacheflowvip
Type: *	TCP
Port: *	80 :
Service Group:	cacheflowsg
Connection Limit:	□ 8000000 ● Drop ○ Reset ☑ Logging
☑	Use default server selection when preferred method fails
□	Use received hop for response
□	Send client reset when server selection fails
□	Use default forwarding if server selection fails
□	Client IP Sticky NAT

Figure 11: Virtual-server port configuration

5. In the Persistence template section, select "Destination IP Persistence Template" and select "create".

6. Enter or select the following values:

   - **Name:** "DST_IP"
   - **Match Type:** "Service Group"
   - **Timeout:** "5" minutes



Destination IP Persistence

Name: *	DST_IP
Match Type:	Service Group □ Scan All Members
Timeout:	5 Minutes
Don't Honor Conn Rules:	□
Hash Persistent:	□
Netmask:	255.255.255.255
IPv6 Netmask:	128

Figure 12: Persistence configuration

7. Click **OK**, then click **Save** to save the configuration.

12 SUMMARY AND CONCLUSION

The sections above show how to deploy an ACOS device for optimization of Blue Coat CacheFlow deployments. By using an ACOS device to load balance traffic across a farm of Blue Coat CacheFlow devices, the following key advantages are achieved:

- Significant bandwidth reduction and improved HTTP throughput over time. In addition, this solution can save on expensive international links and backhaul traffic, while improving the end-user Web experience.
- Seamless distribution of cache request traffic across multiple Blue Coat CacheFlow appliances for site availability and scalability.
- Improved site performance and reliability to subscribers by deploying DDoS mitigation features from A10 Networks.

By using the A10 Thunder Series and AX Series Application Delivery Controllers (ADCs), significant benefits are achieved for web subscribers. For more information about Thunder Series and AX Series products, please refer to the following URLs:

http://www.a10networks.com/products/axseries.php

http://www.a10networks.com/resources/solutionsheets.php

http:/www.a10networks.com/resources/casestudies.php

A. CLI COMMANDS FOR ACOS CONFIGURATION

This section shows the CLI commands for implementing the sample configuration described above:

```
hostname AX3030-LAB
trunk 4
 ethernet 7 to 8
 name "BRAS"
!sample access-list
access-list 102 permit tcp ipaddr 0.0.3.255 any eq 80
access-list 102 permit tcp ipaddr 0.0.0.255 any eq 80
access-list 102 permit tcp ipaddr 0.0.1.255 any eq 80
health monitor tcs
 method http
 ip anomaly-drop drop-all
slb server cacheflow1 192.168.2.100
   port 80 tcp
slb server cacheflow2 192.168.2.101
   health-check tcs
   port 80 tcp
slb service-group cacheflowsg tcp
    health-check tcs
    member cacheflow1:80
    member cacheflow2:80
slb template persist destination-ip DST_IP
   match-type service-group
slb virtual-server cacheflowvip 0.0.0.0 acl 102
   port 80 tcp
      name _wildcard_v4_102_TCP_80
      no-dest-nat
      template persist destination-ip DST_IP
end
```

Note: *The value shown in this example for the **name** command, under **port 80 tcp** is auto-generated when you configure the virtual port. You can edit this string if desired.*