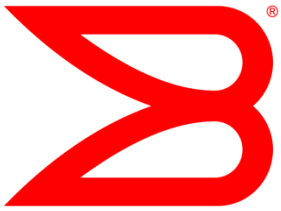


CAMPUS NETWORK

Enhancing the Performance of Microsoft Office SharePoint Server Using Brocade ServerIron and Blue Coat ProxySG

This document provides best-practice guidance using the Microsoft Office SharePoint Server (MOSS) and Brocade ServerIron Application Delivery Controllers with the Blue Coat ProxySG to address the challenges associated with today's mission critical enterprise application deployments,

BROCADE

CONTENTS

INTRODUCTION

Teaming Microsoft Office SharePoint Server (MOSS) and Brocade® ServerIron® with Blue Coat ProxySG allows you to meet the challenges of designing a SharePoint environment by managing various proxy requirements across a distributed enterprise, protecting internal users and networks from spyware and other attacks, and providing application performance acceleration.

The solution described in this paper is targeted at customers with environments that include branch offices and who need Wide Area Network (WAN) optimization. It provides best-practice guidance for Brocade ServerIron ADX deployments using Server Load Balancing (SLB) with Blue Coat ProxySG providing application acceleration.

NOTE: You may also want to read a document entitled, "Deploying the Brocade ServerIron with Microsoft Office SharePoint Server 2007," which provides a reference architecture and procedures for deploying the Brocade ServerIron and the MOSS, available on www.brocade.com.

This solution was installed and tested at the Microsoft Technology Center (MTC), located in Mountain View, California. Brocade and Microsoft cooperated in all phases of the solution development, including lab setup, solution functionality, performance testing, and this document. Brocade and Microsoft jointly validated that the lab setup and solution testing represented best efforts in creating a realistic customer deployment environment. For information on the MTC, visit:
http://www.microsoft.com/mtc/locations/SiliconValley.mspx

For more information on the Brocade ServerIron, specifically detailed data sheets, visit:
http://brocade.com/

For more information on the MOSS, visit: http://www.microsoft.com/sharepoint/default.mspx

Note the following:

- All of the configuration procedures in this document are performed on the Brocade ServerIron.
- You should be familiar with Brocade ServerIron, Blue Coat ProxySG, and Microsoft SharePoint 2007. Refer to the product documentation for all products.
- It is assumed that you have installed both the Brocade ServerIron and the Blue Coat ProxySG in your network and have a general understanding of how they function.
- You have installed the Brocade ServerIron in your network and have a general understanding of how it functions.

OVERVIEW

The solution offers optimized MOSS 2007 application availability, performance, and security by providing application optimization services from the Brocade ServerIron and Blue Coat ProxySG as described in the following sections.

Application Availability

- **Server and application health checks.** Continuously monitors the health of the application availability.
- **Server load balancing.** Efficiently routes the end user and Web services request to the best available server dependent on the load balancing scheme being utilized.
- **Network platform health monitoring.** Ensures continuity of business operations through mirroring end user transactions across a redundant ServerIron network.

Application Performance

- **Server offloading.** To provide better efficiency of the application server resources (CPU and memory), can terminate Secure Socket Layer (SSL); termination of SSL on the Brocade ServerIron frees up 34% of the application server CPU processing.
- **SSL termination.** The Brocade ServerIron 4G-SSL can terminate 35,000 connections per second.
- **Server load balancing.** The ServerIron balances the traffic load between the real servers dependent on the predictor used in order to get optimal resource utilization, maximize throughput, and minimize response time
- **Server health monitoring.** The ServerIron performs health checks to the real servers. This ensures that traffic is not forwarded to a real server that has failed or is not responsive.
- **WAN optimization.** Provides intelligent caching, compression, and protocol optimization that yields up to 32.4444% more transactions and decreases the average transaction time by 640.336% for 32 users.
- **Traffic compression.** Scalable LZ compression functionality.
- **Object caching.** Reduces requests to the server.

Application Security

- **SSL termination.** Efficiently encrypts and decrypts SSL-enabled traffic, which facilitates the use of intrusion detection and prevention solutions before the traffic reaches the back-end servers.
- **End user access control.** Provides Access Control Lists (ACLs) to protect the client-to-server traffic from worms and intruders, which attack vulnerable open server ports not used by the application.
- **SYN-attack protection.** Provides protection to the back-end servers from SYN attacks. The SYN attacks can exhaust the back-end server resources by opening a vast number of partial TCP connections. The Brocade ServerIron 4G-SSL can support 1 million SYN per second.

Microsoft Office SharePoint Server (MOSS)

MOSS 2007 is a portal-based collaboration and document management platform. It hosts Web sites, called "SharePoint Portals," which can be used to access shared workspaces and documents as well as specialized applications, such as Wikis and blogs, from a browser.

MOSS 2007 functionality is based on Web parts, components that implement special functionality, such as a document library, task list, or discussion pane. These Web parts are then structured into Web pages, which are hosted in the SharePoint Portal. SharePoint sites are actually ASP.NET applications, served using Microsoft Internet Information Server (IIS) and a Microsoft SQL Server database as a data storage back-end.

The SharePoint family comprises these different applications:

1. **Windows SharePoint Services** (**WSS**) is a free add-on to Windows Server. WSS offers basic portal infrastructure and collaborative editing of documents, as well as document organization and version control capabilities. It also includes user functionality such as workflows, to-do lists, alerts, and discussion boards, which are exposed as Web parts and embedded into SharePoint Portal pages. (WSS was previously known as SharePoint Team Services.)

2. **MOSS** is an optional paid component of the Microsoft Office application suite. MOSS integrates with WSS and adds greater functionality, including better document management, indexed search functionality, navigation features, RSS support, Wikis, and blogs, as well as features from Microsoft Content Management Server. It also includes business data analysis and integration with Microsoft Office applications, such as project management capabilities or display of Microsoft Office InfoPath forms via a browser. It can host specific libraries, such as the PowerPoint Template Libraries, when the server components of the specific application are installed. (MOSS was previously known as SharePoint Server and SharePoint Portal Server.)

Solution Architecture

MOSS 2007 comprises a three-tier architecture as described below:

3. The **first tier** is a Web browser for a client.

4. The **middle tier** consists of Web and application servers running the WSS application with MOSS plugging-in functionality where required, generally a search service, which crawls the data store creating an index, and a number of other services.

5. The **third tier** is the database server.

(The middle tier can be scaled by load balancing more Web and application servers, and the third tier can be scaled by building larger clusters of SQL Server instances.)

The solution architecture used for the Brocade ServerIron with MOSS was the WSS 3.0 High Availability configuration, shown in Figure 1. The ports used by Microsoft Office SharePoint 2007 Server are HTTP (Port 80) and HTTPS (Port 443).

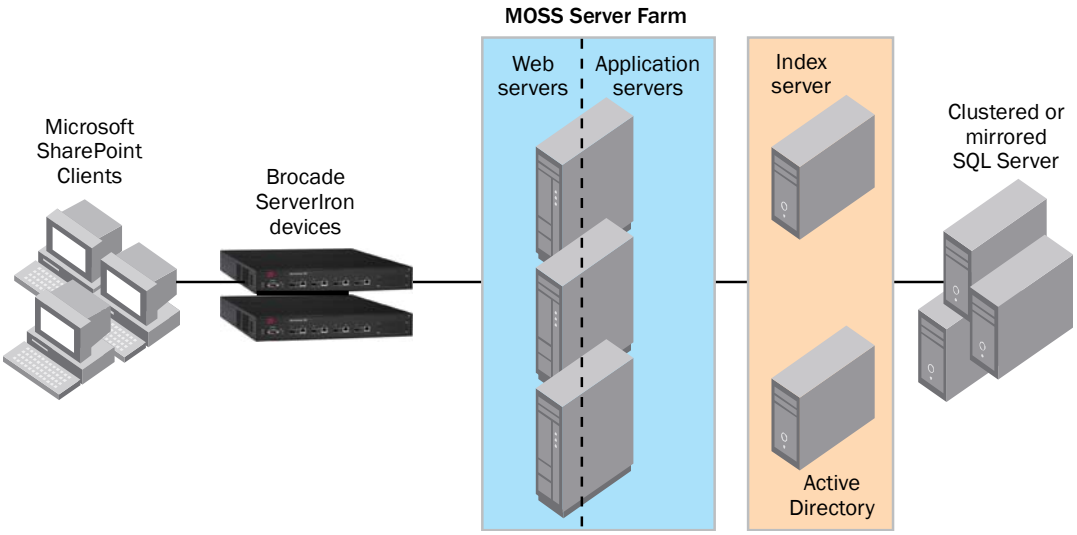


Figure 1. Brocade load balancer with the WSS 3.0 High Availability topology

APPLICATION NETWORKING ARCHITECTURE

In the example shown in Figure 2 and used in this solution testing, an active-hot standby pair of ServerIron ADCs is used to load balance user traffic to the MOSS server farm.

The Blue Coat ProxySGs provide WAN edge compression for the remote user. This WAN optimization decreases the amount of the overall transaction time for user requests and responses by either compressing or caching the transaction information. Client traffic is forwarded to the Blue Coat ProxySG set in transparent (bridged) mode. The Blue Coat ProxySG caches redundant data and compresses the traffic to be sent to the MOSS server farm. At the far end, the Blue Coat ProxySG uncompresses the traffic and adds back the redundant data that has been cached on this Blue Coat ProxySG. Note that if the Blue Coat ProxySG fails, the link from the Local Area Network (LAN) to the WAN goes into passthrough and allows user traffic to flow to the MOSS server without compression or caching.

The Brocade ServerIron reduces the load on resources in the server farm via load balancing. Additionally, if the application uses SSL, then the ServerIron can provide SSL offload services. The ServerIron terminates the SSL connection and forwards clear text “http” traffic to the server farm. By utilizing SSL offload, the Brocade ServerIron removes the burden of SSL termination performed by the server farm, thereby increasing efficiency by removing the load on the server resources and allowing the servers to process more transactions.

NOTE: Increased server efficiency also results if the Brocade ServerIron is used to provide TCP reuse. Using TCP reuse allows the server to utilize current TCP connections instead of building a new session for each TCP connection, which removes the burden on the server resources that maintain TCP sessions.

Figure 2 shows the configuration to test the Brocade ServerIron with Microsoft SharePoint and an Active/Hot Standby implementation.

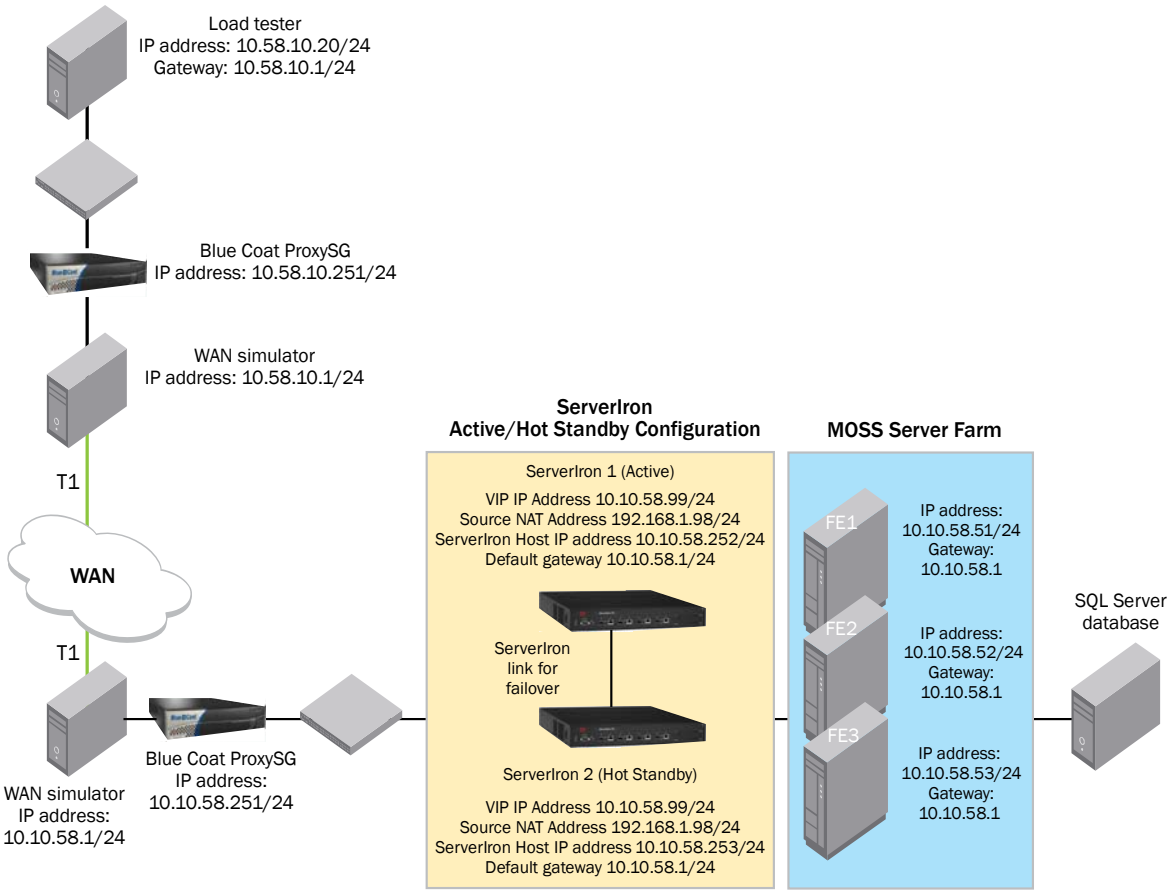


Figure 2. Using an pair of ServerIrons for high availability and Blue Coat ProxySG

For details on the server farm architecture, see Appendix A.

CONFIGURING THE BROCADE SERVERIRON

For a discussion of the connectivity implemented in the test configuration and the resulting traffic flows, see Appendix B.

In the joint solution the Brocade ServerIron was configured to provide the following functionality:

- **Load balancing using Least Connections.** Selects the server with the fewest number of server connections.
- **Active\Hot-Standby redundancy.** Uses a dedicated link between the ServerIrons, which transmits flow-state information, configuration synchronization information, and the redundancy "heartbeat."

Implementation Overview

The Brocade ServerIron used in this solution is deployed in a one-armed mode that is connected to the L2/L3 switch. Key features implemented on the Brocade ServerIron to support this application are:

- Layer 4 load balancing
- Layer 7 load balancing for SSL termination and TCP reuse
- Server health monitoring
- Connection replication for statefull (or state-aware) failover

Configuration Network Topology

Figure 3 shows the network topology used to test the Brocade ServerIron with Microsoft SharePoint solution. The design used the Active/Hot Standby implementation. The "Brocade ServerIron Configuration Tasks" section references this design.

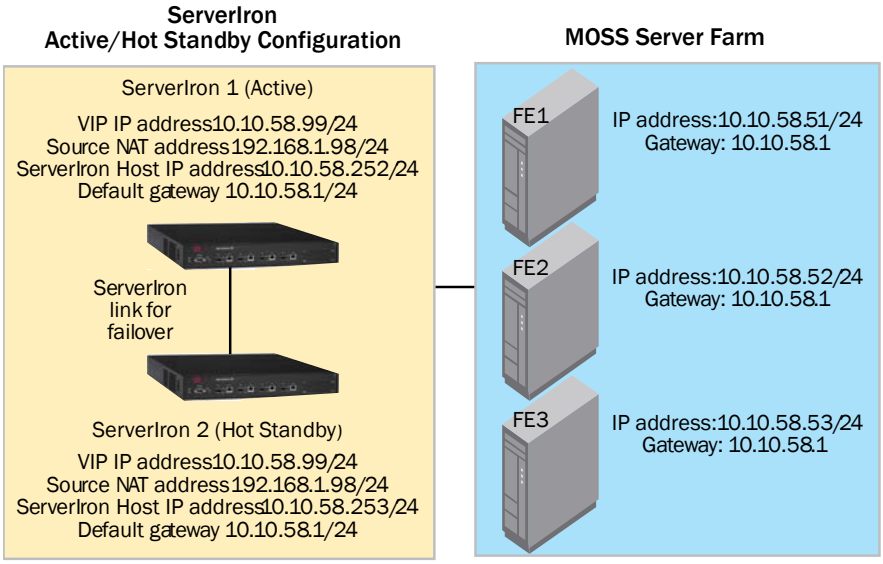


Figure 3. Configuration network topology

Configuration Prerequisites

The following prerequisites are required to deploy the solution:

- Working knowledge of installing and deploying of the MOSS application
- Experience with basic networking and troubleshooting
- Experience installing and deploying Brocade ServerIron products
- Working knowledge of the Brocade ServerIron CLI
- Brocade ServerIron running firmware version 10.2.01gTI2 or later
- Brocade ServerIron TrafficWorks Graphic User Interface (GUI) supported in the Brocade ServerIron version 10 or later

NOTE: Not all steps can be completed using the GUI; for those tasks you will need to use the CLI.

Brocade ServerIron Configuration Tasks

The following are the high-level steps required to deploy the Brocade ServerIron with MOSS 2007 Servers:

1. Configure the Brocade ServerIron management interface
2. Configure L2 active/hot standby redundancy
3. Configure the server farm (real servers)
4. Configure the server source NAT for the real servers to session back to the clients
5. Configure the VIP and bind the real servers to the VIP

For basic configuration using Least Connections load balancing:

6. Configure SSL and perform SSL offload

Managing the Brocade ServerIron

1. At the opening CLI prompt, enter:
```
ServerIron> enable
```
2. Access the configuration level of the CLI, enter:
```
ServerIron# configure terminal
ServerIron (config)#
```
3. To assign an IP address to the ServerIron, enter:
```
ServerIron (config)# ip add 10.10.58.252 255.255.255.0
```
4. To assign a default gateway , enter:
```
ServerIron (config)# ip default-gateway 10.10.58.1
```
5. Additional commands:
```
ServerIron (config)# hostname SP1
ServerIron (config)# enable super-user-password foundry
ServerIron (config)# no enable aaa console
ServerIron (config)# telnet server
ServerIron (config)# username SP1 nopassword
```

NOTE: It is recommended that you use a secure password.

6. To exit from the configuration level of the CLI, enter:
   `SP1 (config)# end`

7. To save the configuration to NVRAM, enter:
   `SP1# write memory`

Managing the Brocade ServerIron (GUI)

To access the ServerIron using the GUI interface, first perform the steps listed above and then complete the following procedure.

Connecting the ServerIron to the Network

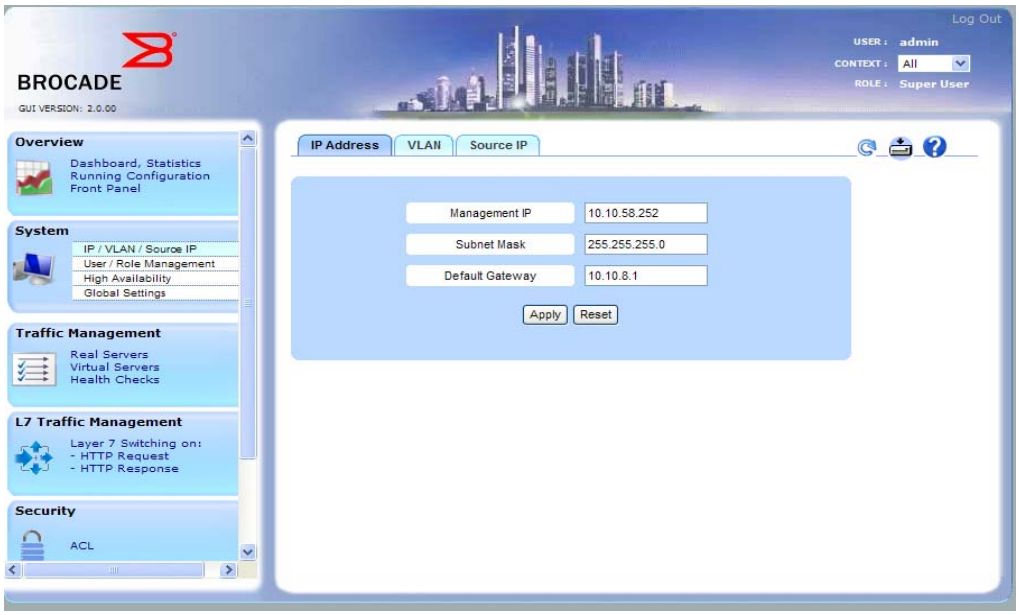
1. Connect the ServerIron to your network infrastructure.
2. Check to see if ping access to the ServerIron IP address is working.
3. Open a browser (MS Internet Explorer or FireFox) window.
4. Type the ServerIron IP address into the browser window and press Enter. The Login window is displayed.

5. Click the HTTP button to display the user name and password dialog box.

NOTE: The default user name and password are “admin” and “foundry” respectively. It is best practice to change the password.

6. Enter user name and password and click **OK**. The home page for the ServerIron Web interface is displayed.

7. In the Network section on the left (not shown below), select **Static Route**. If required, add the static route for traffic returning from the real servers. Note that for this configuration, a flat network is used.



Configuring L2 Active/Hot Standby Redundancy

The configuration used for the ServerIron in this deployment with the Microsoft Office SharePoint Server 2007 was Active-Hot-Standby. In an Active-Hot Standby configuration both ServerIrons share the same Virtual IP (VIP) address and configuration (with the exception of the management IP address). Active-Active is an alternate method for ServerIron redundancy. See the product documentation for the Brocade ServerIron.

In a typical Hot Standby configuration:

- One ServerIron is the *active device* and performs all the Layer 2 switching as well as the Layer 4 SLB switching
- The other ServerIron monitors the switching activities and remains in a hot standby role. If the active ServerIron becomes unavailable, the standby ServerIron immediately assumes the unavailable ServerIron's responsibilities. The failover from the unavailable ServerIron to the standby ServerIron is transparent to users. Both ServerIron switches share a common MAC address known to the clients. Therefore, if a failover occurs, the clients still know the ServerIron by the same MAC address. The active sessions running on the clients continue and the clients and routers do not need to "re-ARP" (Address Resolution Protocol) for the ServerIron MAC address.

NOTE: The following tasks must be performed using the CLI.

At the config prompt:

1. Configure the backup ServerIron (Active) to ServerIron (Hot Standby) VLAN:
   vlan 999 by port –> creates the backup VLAN
   untagged ethe 3 –> associates VLAN to Ethernet port 3 (dedicated link for ServerIron communications
   no spanning-tree
2. Ensure that VLAN 1 has the spanning tree disabled:
   vlan 1 name DEFAULT-VLAN by port
   no spanning-tree
3. Configure the redundant link:
   `server backup ethe 3 0012.f27c.8540 vlan-id 999 –> sets the active server`
   `server backup-preference 5 –>` determines the switch back time

   Where the 0012.f27c.8540 is the Active SI system MAC. (Use **the show chassis** command to obtain the MAC.)
4. Add the interface to monitor for redundancy:
   `server router-ports ethernet 1`

Configuring the Server Farm (Real Servers)

Note that the port http URL command is used for the Layer 7 health check:

```
server real r1 10.10.58.51
     port http
     port http keepalive
     port http url "GET http://intranet/Pages/Default.aspx"

server real r2 10.10.58.52
     port http
     port http keepalive
      port http url "GET http://intranet/Pages/Default.aspx"
```

```
server real r3 10.10.58.53
     port http
     port http keepalive
     port http url "GET http://intranet/Pages/Default.aspx"
```

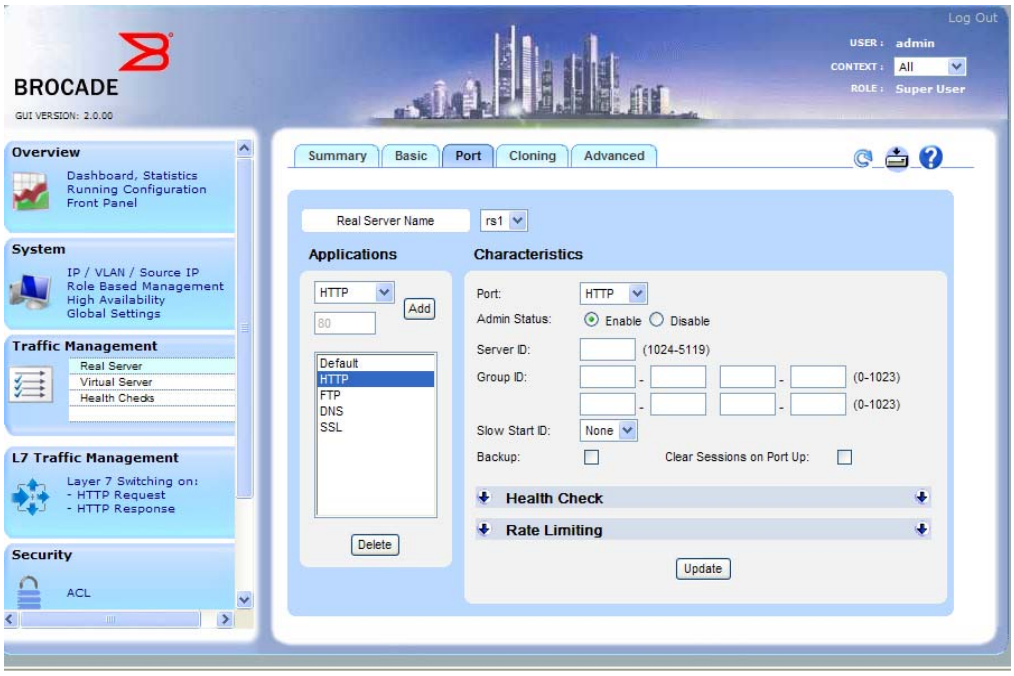
To avoid Layer 4 and Layer 7 health check flapping, use the following command:

```
server no-fast-bringup
```

Configuring the Server Farm (Real Servers) (GUI)

1. In the Traffic Management section on the left, select **Real Server** and click the **Basic** tab. Enter the names of the real servers.

2. Click the **Port** tab to display the port configuration screen, and enter the port type and health check information for every real server.



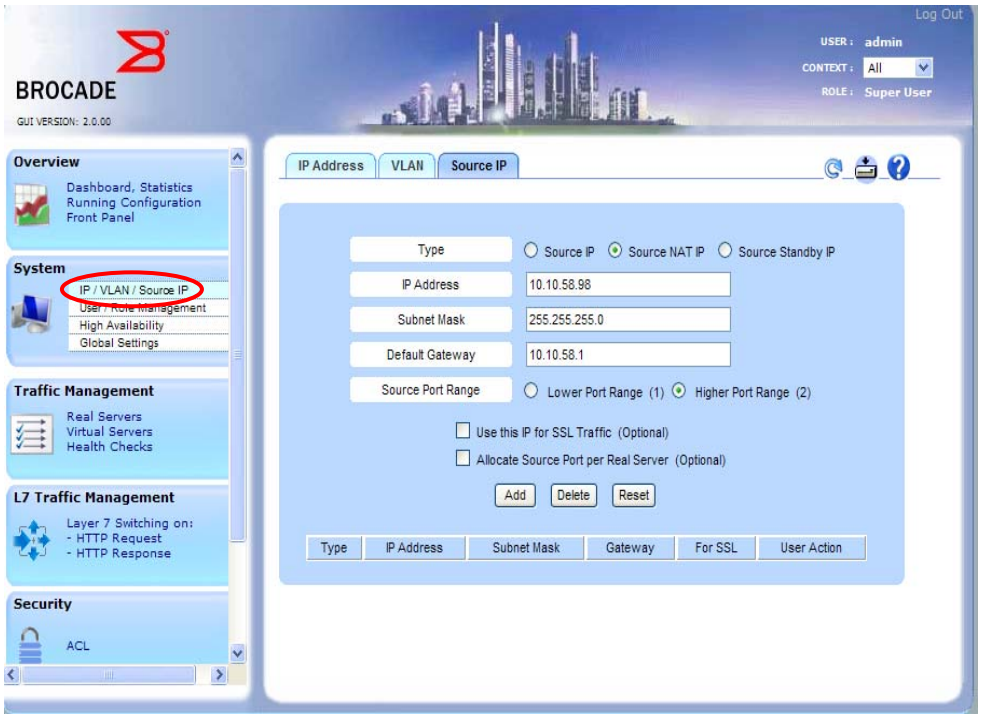
Configuring the Server Source NAT for Real Servers to Session Back to Clients

NOTE: The real servers gateway may be point to the IP address provided in the NAT command:

```
server source-nat
server source-nat-ip 10.10.58.98 255.255.255.0 0.0.0.0 port-range 1
```

Configuring the Server Source NAT for Real Servers to Session Back to Clients (GUI)

1. In the System section on the left, select **Source IP/Source NAT IP**. Enter the source NAT IP statements, **NOTE:** If SSL is used, ensure that "Use this IP for SSL traffic" is checked (shown unchecked below).



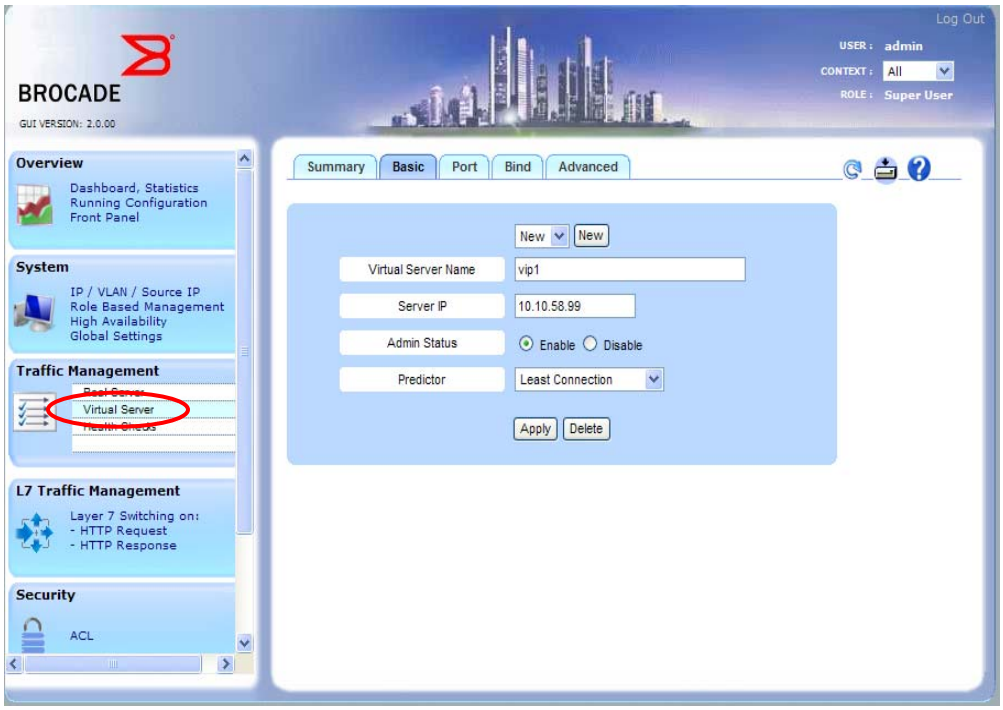
2. Ensure that the source NAT is turned on globally. In the System section on the left, select **Global Settings**.

Configuring the VIP and Binding the Real Servers to the VIP

```
server virtual vip1 10.10.58.99
     port http
     bind http r1 http r2 http r3 http
```

Configuring the VIP and Binding the Real Servers to the VIP (GUI)

1. In the Traffic Management section, select **Virtual Server** and click the **Basic** tab. Create the Virtual IP (VIP) interface.



2. In this screen also include the predictor type. Note that for this configuration Least Connections and Dynamic Weighted Reverse is used.

3. Click **Apply** and then click the **Port** tab to apply the port type used for this VIP interface.

4. Now you must bind the VIP to the real servers. Click the **Bind** tab and bind the associated real servers to their VIP.

Basic Configuration using Least Connections Load Balancing

Least Connections is used in this example, however you could use other predictors. The Least Connections predictor sends a request to the real server that currently has the fewest active connections with clients. For sites where a number of servers have similar performance, the Least Connections option smoothes distribution when a server is overloaded. For sites in which the capacity of servers varies greatly, the Least Connections option maintains an equal number of connections among all servers. Over time, those servers capable of processing and terminating connections faster will receive more connections than slower servers.

1. Follow the directions in the "Configuring the VIP and Binding the Real Servers to the VIP" section and complete the following additional step. In the VIP, place the predictor that will be used for Least Connections:

```
server virtual vip1 10.10.58.99
     predictor least-conn
```

NOTE: You can also use the GUI interface as shown in the VIP configuration screens.

Configuring SSL and Performing SSL Offload

SSL offloading relieves a Web server of the processing burden (CPU and memory) of encrypting and/or decrypting traffic sent via SSL. Configuration of SSL offload can be done with a Certificate Authority (*CA*) or a self-signed certificate generated by a ServerIron. In this deployment, a self-signed certificate is used.

1. At the ServerIron prompt, to generate a key-pair and certificate:

```
SP1# ssl genrsa m-key 1024 f1234
SP1# ssl gencert certkey m-key signkey m-key f1234 bcert
```

2. Configure the VIP to perform SSL:

```
ssl profile zprofile
     keypair-file m-key
```

```
certificate-file bcert
cipher-suite all-cipher-suites
allow-self-signed-cert
session-cache off
```

3. Add an additional Server NAT Command for SSL to point the real servers gateway to the SSL NAT IP address:
   `server source-nat-ip 10.10.58.98 255.255.255.0 0.0.0.0 port-range 1 for-ssl`

5. Configure the VIP to perform SSL:

```
server virtual vip1 10.10.58.99
     port ssl sticky   -> needed with multiple clients IPs
     port ssl ssl-terminate zprofile
     bind ssl r1 http r2 http r3 http
```

Configuring SSL and Performing SSL Offload (GUI)

SSL Keys

1. In the Security section on the left, select **SSL Switching** and click the **SSL Keys** tab. Here you can load a pre-generated key or have the ServerIron generate a key. In this configuration, ServerIron generates the key.

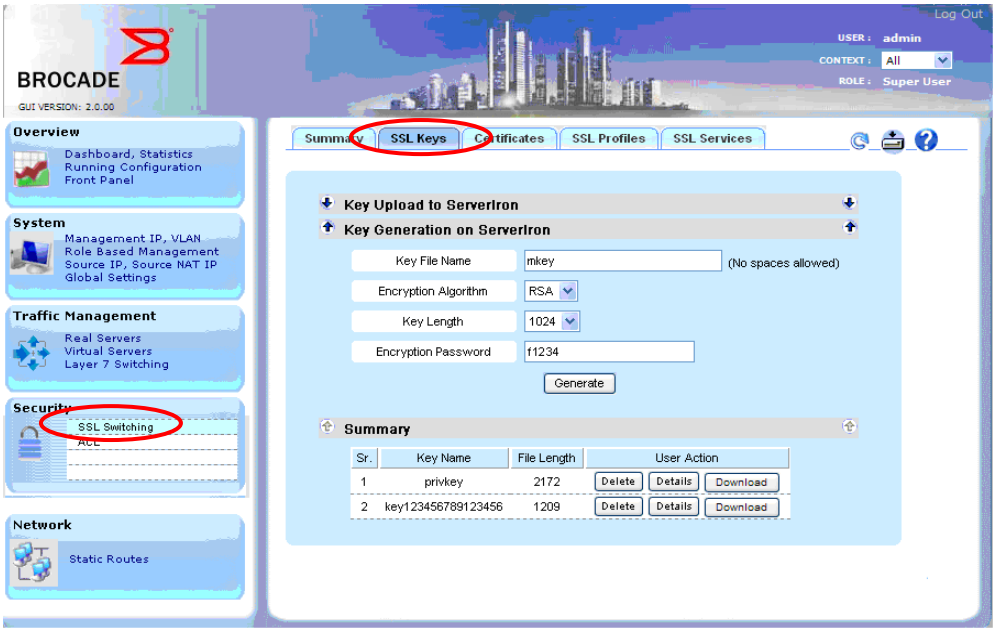
2. (Optional) To generate the key, in the ServerIron section on the right select **Key Generation** and complete the following:

   a. Create a key file name.

   b. Select the encryption algorithm.

   c. Select the key length.

   d. Create an encryption password.



   e. Once the data has been entered, click **Generate**.

SSL Certificate

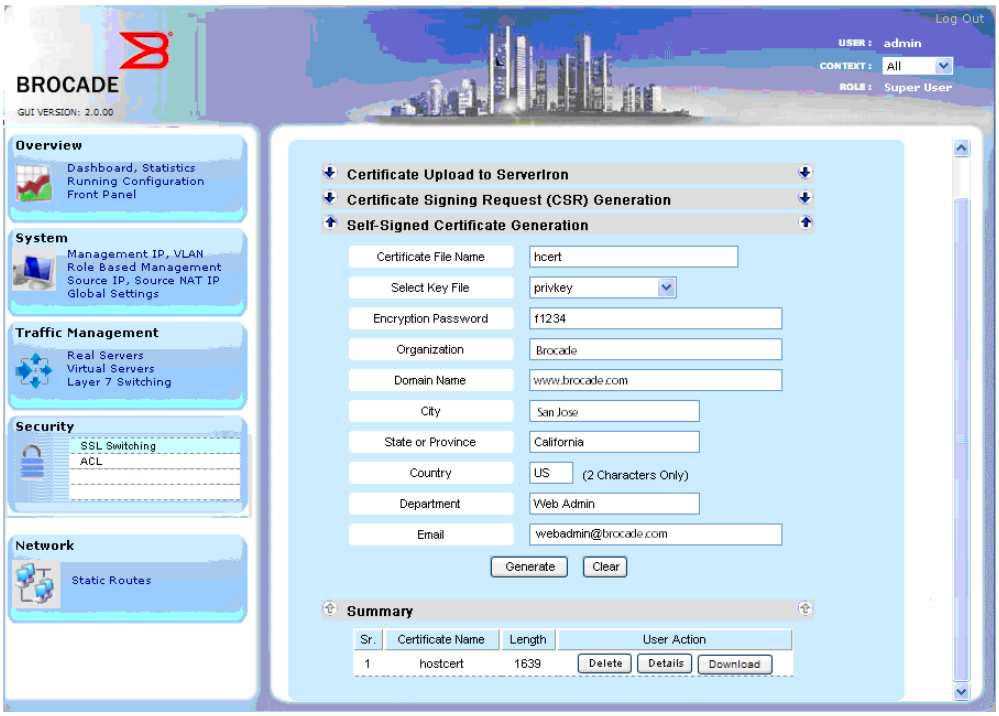
1. In the Security section on the left, select **SSL Switching** and click the **Certificates** tab, in which you can load a pre-generated key or have the ServerIron generate a key. In this configuration, ServerIron generates the key.

2. You can load a pre-generated certificate, generate a Certificate Signing Request (CSR) or have the ServerIron generate a self-signed certificate. In this configuration, the ServerIron generates a self-signed certificate. To generate a self-signed certificate, display the Self-Signed Certificate Generation section and complete the following:

   a. Create a certificate file name.

   b. Select the key file.

   c. Enter the key file encryption password, organization, domain name, city, state or province, country, department, and e-mail address.



   d. Once the data has been entered, click **Generate**.

SSL Profile

1. In the Security area on the left, select **SSL Switching** and click the **SSL Profiles** tab. Here you will create the SSL profile from the key file and certificate that you have either generated or uploaded into the ServerIron. To create the SSL profile, complete the following:

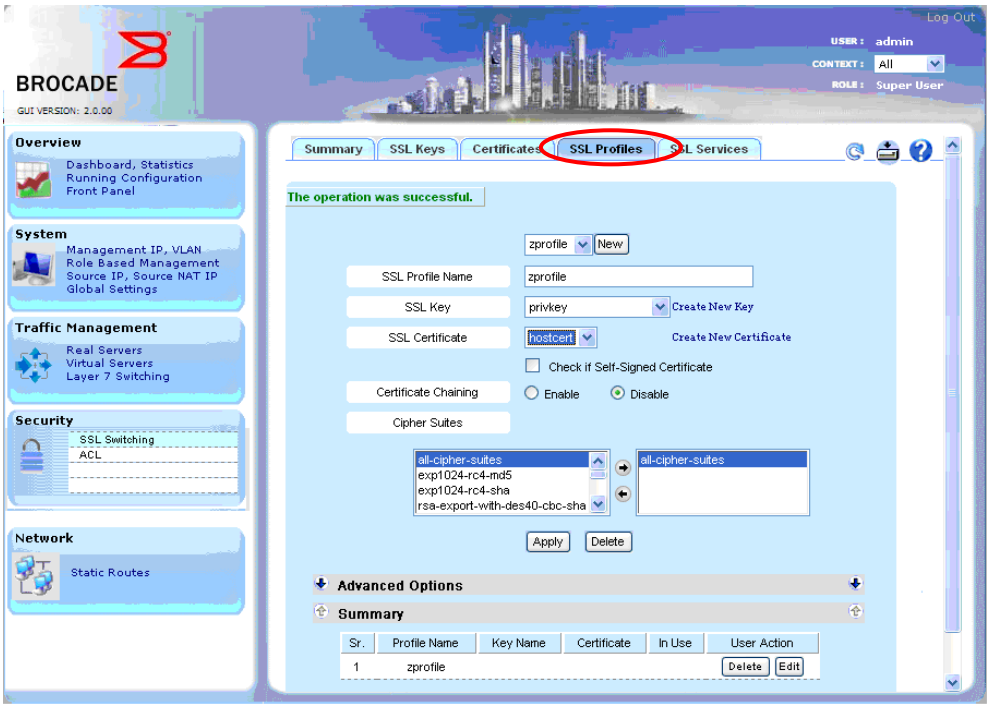
   a. Create an SSL profile name.

   b. Select the SSL key; either choose from the drop-down list or create a new one.

   c. Select the SSL certificate; either choose from the drop-down list or create a new one.

   d. Unless you need it, disable Certificate Chaining.

e. In the Cipher Suites list, select **all-cipher-suites**.



f. Once the data has been entered, click **Apply**.

SSL Services

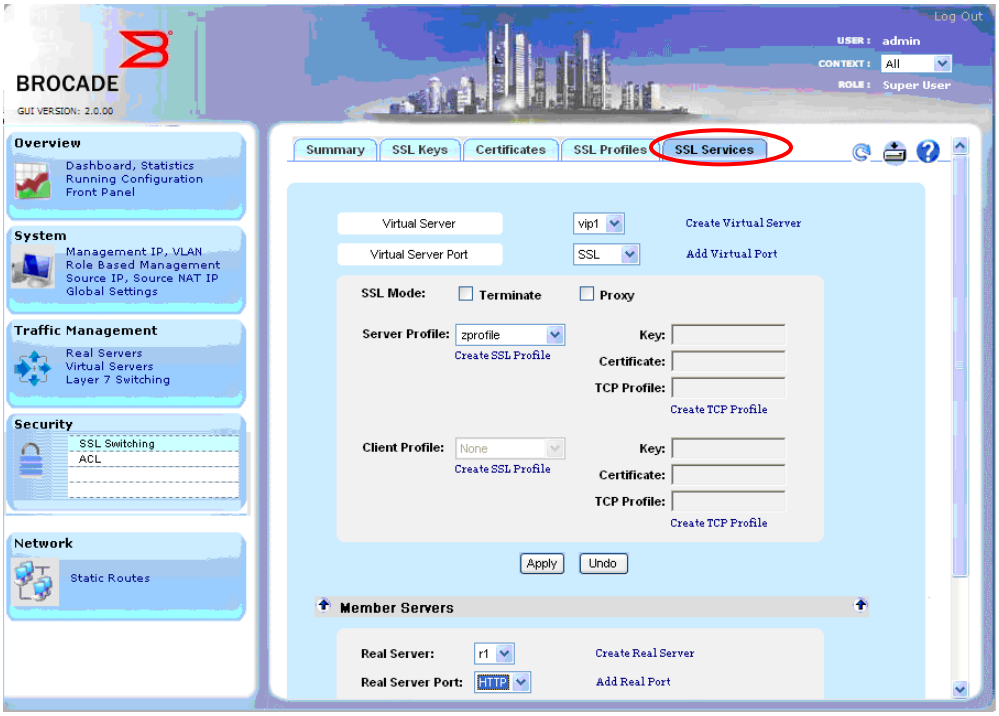
1. In the Security area on the left, select **SSL Switching** and click the **SSL Services** tab, in which you attach the SSL profile to the associated VIP. This may require adding SSL ports to the real servers (if you have not done so already). Complete the following:

   a. Make a choice from the Virtual Server drop-down menu (in this example, vip1).

   b. Make a choice from the Virtual Server Port drop-down menu (in this example, SSL).

   c. Select the SSL mode (Terminate or Proxy). For this configuration, Terminate is used as the SSL connection will be terminated on the ServerIron.

d. From the Server Profile drop-down menu, choose the SSL profile that has just been created.



e. Once the data has been entered, click **Apply**.

2. The last step is to ensure that Microsoft SharePoint responds back to the client with https and not http. Log in to the SharePoint Central Administration, select **Operations**, and select **Alternate Access Mapping (AAM).** Map the http URL to https URL.

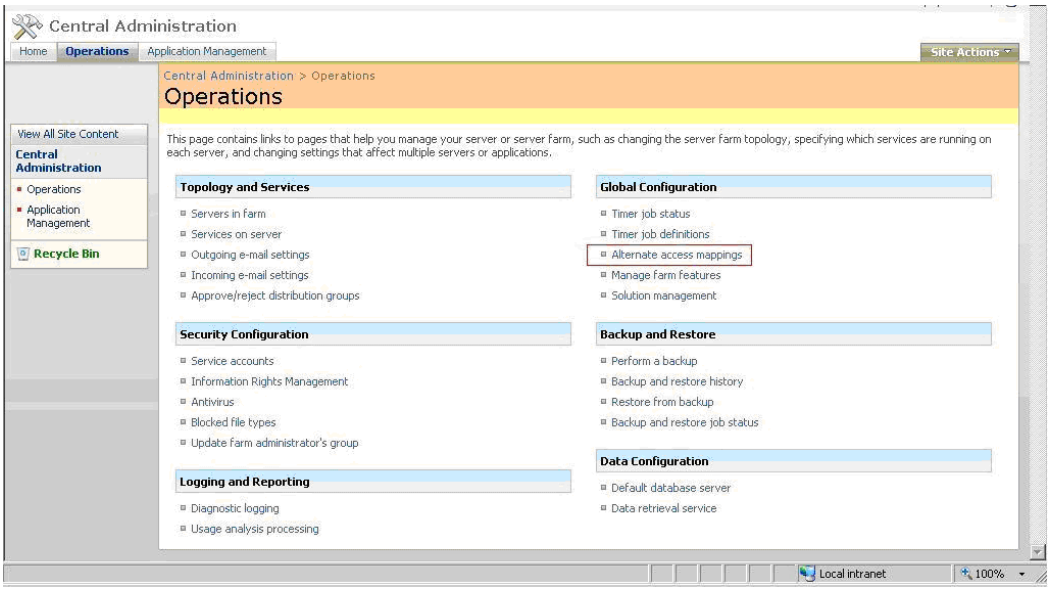
   NOTE: For more information on Alternate Access Mapping refer to the following URL: http//technet.microsoft.com/en-us/library/cc263208.aspx

3. To configure the AAM follow the steps listed below:

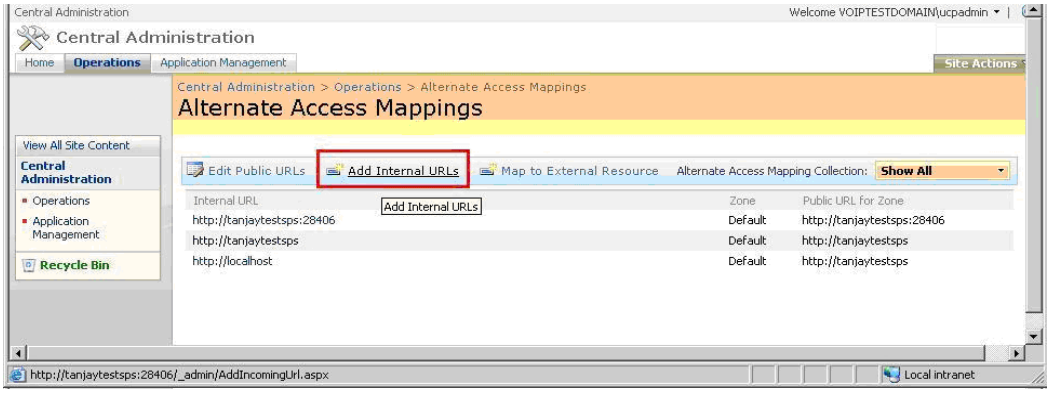
   a. Open SharePoint Server 3.0 Central Administration, click **Start**, point to **Administrative Tools**, and click **SharePoint Server 3.0 Central Administration**.

   b. Click the **Operations** tab.

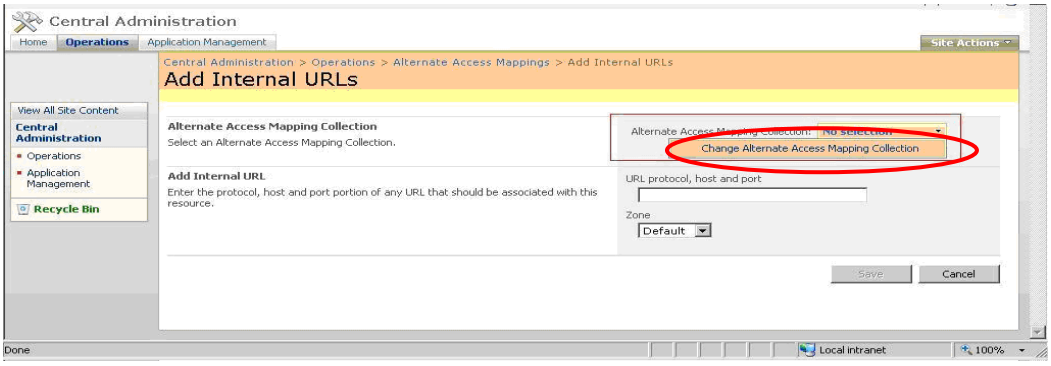
c. In the Global Configuration section, click **Alternate access mappings**.



d. On the Alternate Access Mappings page, click **Add Internal URLs**.

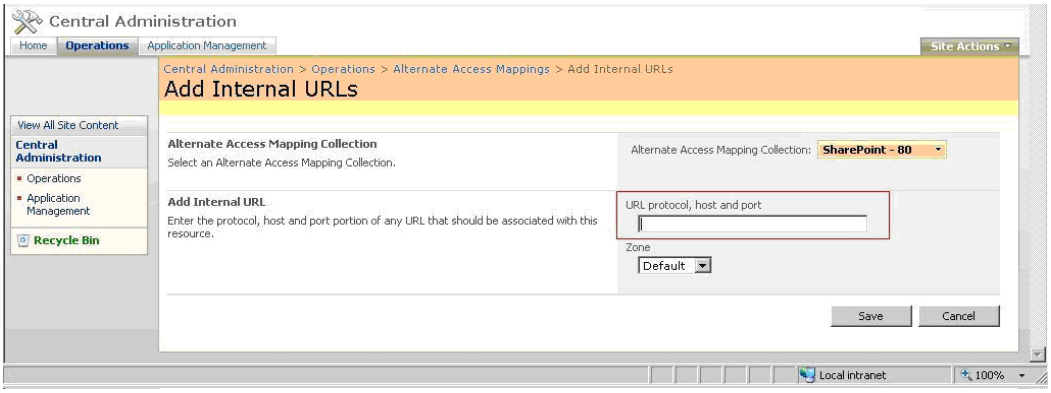


e. On the Add Internal URLs page, click **No Selection**, and then click **Change Alternate Access Mapping Collection.**



f. Click **SharePoint – 80**.

g. On the Add Internal URLs page, in the URL protocol host and port text field, enter: `https://` and the SharePoint Service computer name, and then click **OK**: `https://<SharePointServiceServer Name>`



h. Repeat steps d. through g. and add each of the following URLs:

`http://<SharePointServiceServer fully qualified domain name>`

(http URL with fully qualified domain name (FQDN) of the server)

`https://<SharePointServiceServer fully qualified domain name>`

(https URL with FQDN of the server)

`http://<SharePointServiceServer fully qualified domain name>`

`https://<SharePointServiceServer fully qualified domain name>`

i. On the Alternate Access Mapping page, verify that the following URLs are displayed:

`https://<SharePointServiceServer Name>` (https URL with computer name)

`http://<SharePointServiceServer fully qualified Name>`

(http URL with fully qualified domain name (FQDN) of the server)

j. `https://<SharePointServiceServer fully qualified Name>`

(https URL with FQDN of the server)

For example: `https://SharePointServiceServer1`

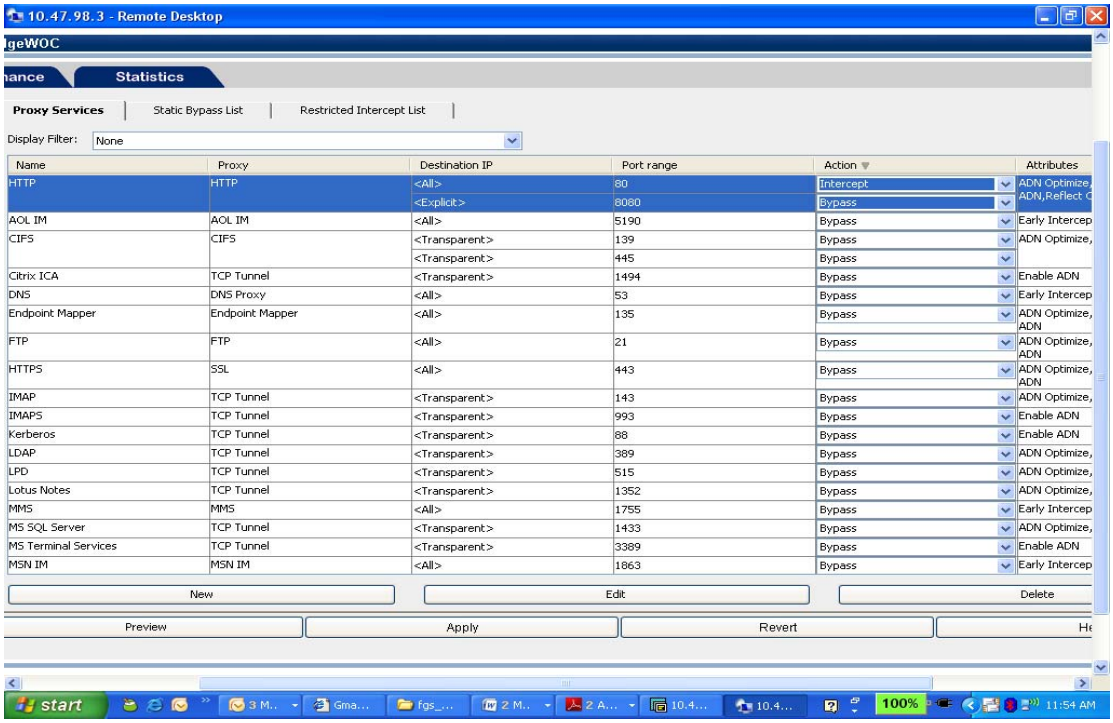
Blue Coat Configuration

When installing the Blue Coat ProxySG devices for the first time, follow the instructions displayed in the Blue Coat ProxySG configuration wizard. For more information about using the Blue Coat ProxySG configuration wizard, visit the Blue Coat Web site and navigate to the Support section:
http://www.bluecoat.com/support/overview

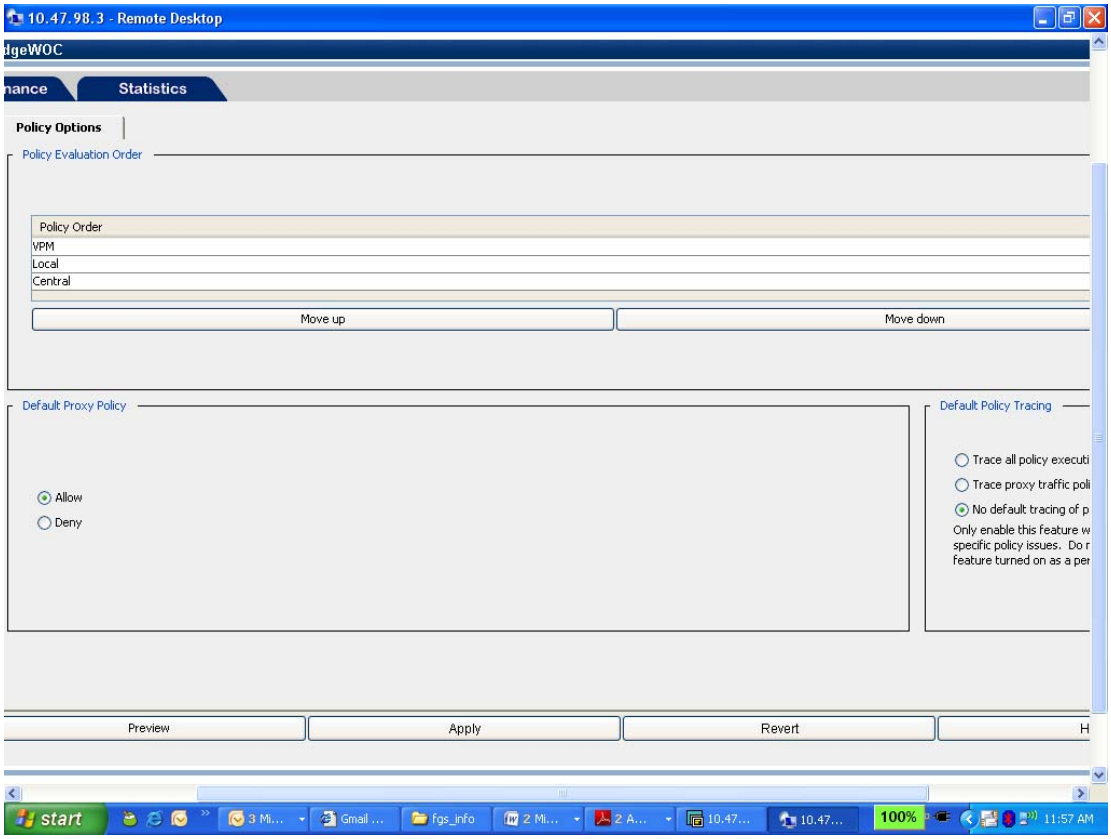
NOTE: To access specific ProxySG information from the Blue Coat Web site, you must have a valid support contract for the ProxySG device.

The next set of screens show the configuration for the Blue Coat ProxySG to intercept the http traffic**.**

1. Go to **Services** > **Proxy Services** (note that this was configured only to intercept http traffic).



2. Then go to **Policy** and **Policy Options** to allow the traffic to be intercepted. Perform this on each Blue Coat ProxySG.



RESULTS

SSL Offload

In this CPU utilization testing scenario, the server running the load tester was attached to the router that connects to the Brocade ServerIron. The load tester simulated 200 users, which generated 100,000 concurrent SSL-encrypted connections to a SharePoint page on the application server, through the Brocade ServerIron, to determine benefits of SSL offload. Note this test was performed using the LAN scenario shown in Figure 4.

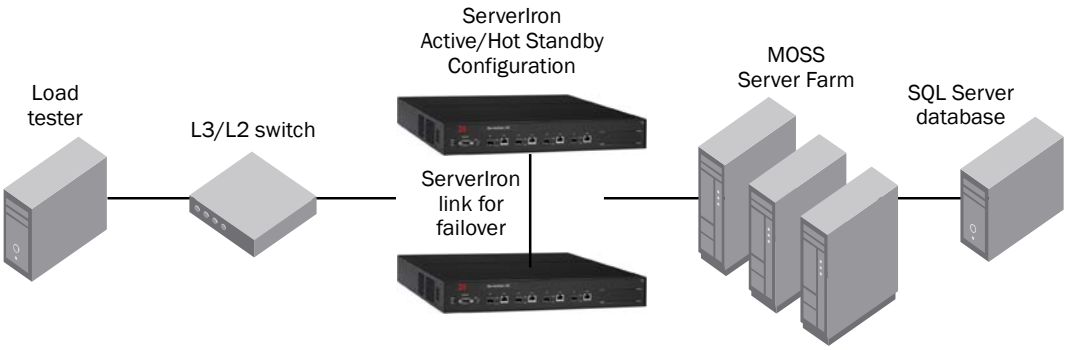
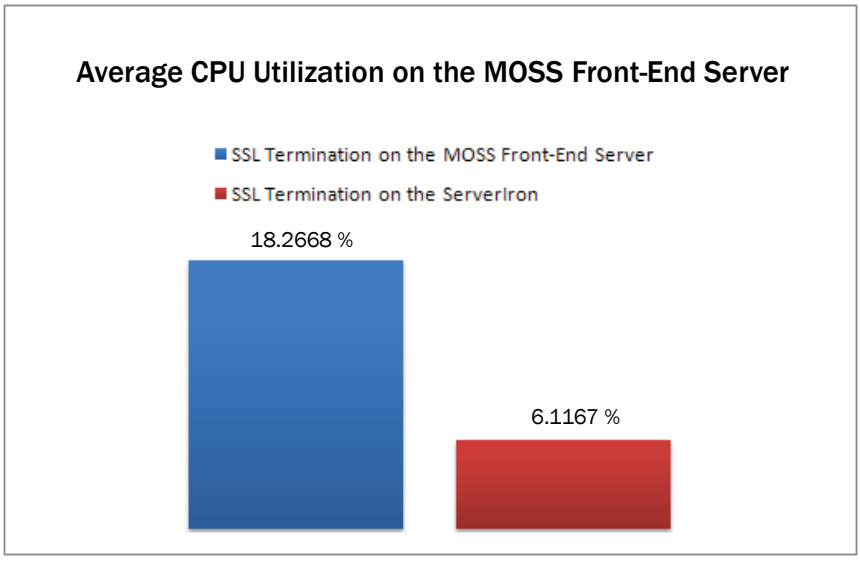


Figure 4. Configuration for SSL offload

Due to the constraints of a T1 link, SSL offload performance would not be prevalent. Testing with LAN connectivity allows for more simulated users to connect, stressing the resources of the servers. Below are the results when testing the Brocade ServerIron performing Layer 4 load balancing to the MOSS servers with SSL termination provided by the servers. Then the Brocade ServerIron was reconfigured for Layer 7 load balancing to terminate SSL on the Brocade ServerIron itself. As shown in the test results below, CPU utilization decreased 34% with the termination of SSL encrypted traffic on the Brocade ServerIron.



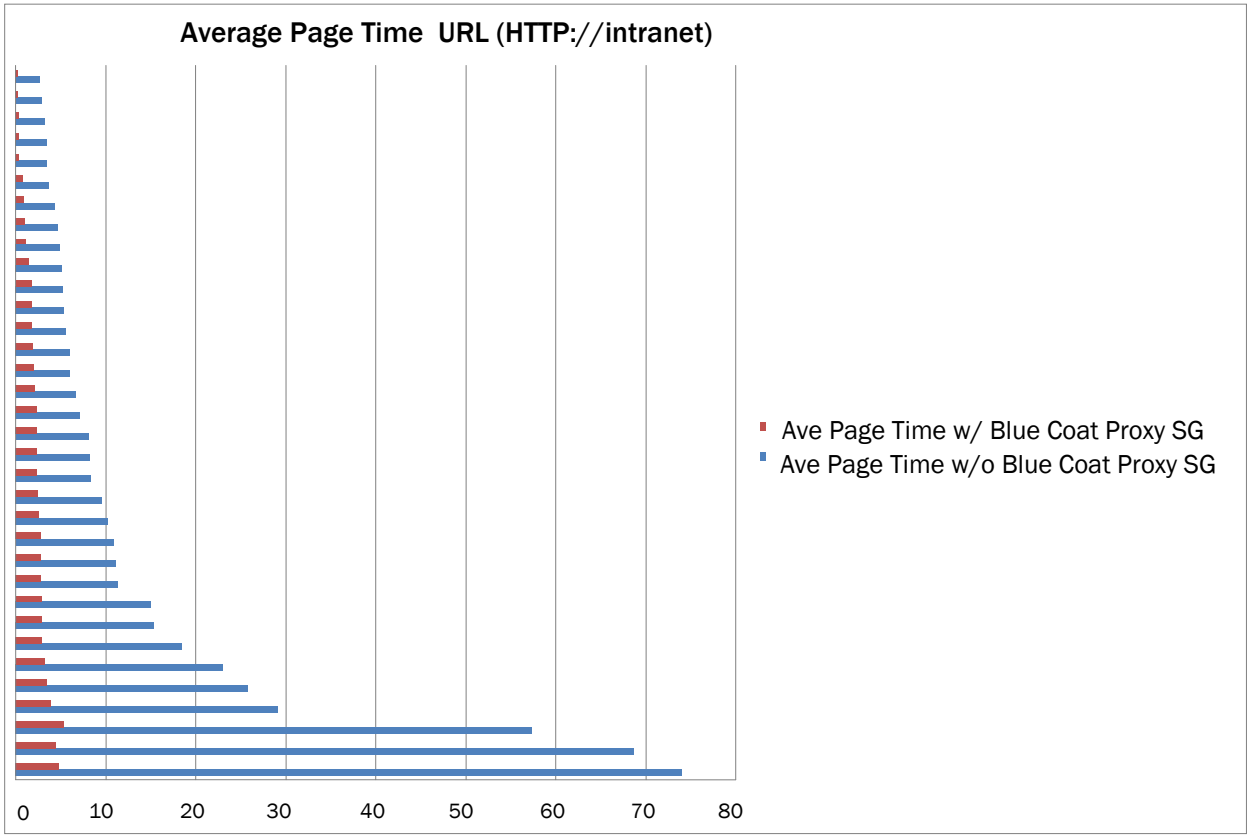
Test: SSL Termination, Run Time 30 min	Average CPU Utilization	Average Available Memory
SSL encryption is performed on the servers	18 %	13,487 KB
SSL encryption is offloaded to the ServerIron	6 %	13,568 KB

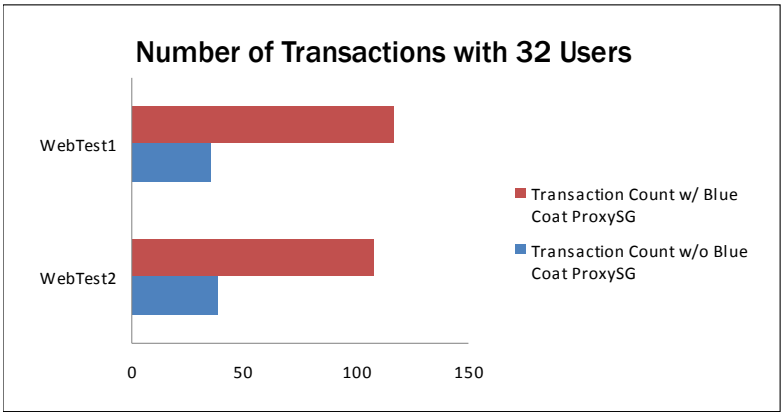
WAN Optimization

In this WAN optimization (WAN Scenario) testing scenario, the server running Virtual Studio Test Suite (VSTS) was attached to the generic Layer 2 switch that is connected to the Blue Coat ProxySG, which is connected to the WAN simulator (providing the layer capabilities and WAN simulation).

VSTS simulated 32 users that generated concurrent connections to SharePoint pages on the application server, where the Brocade ServerIron provided server load balancing using Least Connections as its predictor.

The Blue Coat ProxySG performed compression and caching on the traffic. As shown in the test results below, the average transaction time for 32 users decreased by 84.5% (from 14.29 to 2.22 sec) and the number of transactions for the 32 users increased by about 320% (from 73 to 225 transactions) with the Blue Coat ProxySG.





Test Results	Without Blue Coat ProxySG	With Blue Coat ProxySG
Average URL page time	14.2923 sec	2.2232 sec
Number of transactions	73	225

CONCLUSION

Microsoft Office SharePoint Server 2007 can be effectively deployed behind a Brocade ServerIron load balancer with very few additional considerations. Standard Layer 4 load balancing is sufficient for most deployments, but Layer 7 load balancing can be used to support SSL termination if necessary. For SSL encrypted deployments, the Brocade ServerIron can offload server CPU utilization significantly. SSL termination performed by the application server requires the application server to utilize CPU resources to decrypt the SSL connection and forward the data to the application via clear text (HTTP). This can cause a strain on system resources as demand grows to use of the application. By allowing the Brocade ServerIron to terminate the SSL connection (up to 34,000 SSL transactions per second)removes the strain on the application server. The SSL connection is terminated at the Brocade ServerIron and the data is forwarded to the application server via clear text (HTTP).

The WAN link with and without the Blue Coat ProxySG was observed during in a 20-minute cycle with 32 users performing site navigation on the MOSS application. The Blue Coat ProxySG reduced the amount of unnecessary data traversing the WAN by locally caching data and using compression algorithms on the data that must traverse the WAN.

Because of the size of this WAN link, without Blue Coat ProxySG it would have become congested with 32 users performing site navigation and hence a limited number of transactions were allowed with some of the transactions failing, due to timeout issues. This was seen in both the average transaction times chart and in the transaction count chart, and the end-user would have delayed responses to and from the server.

With the Blue Coat ProxySG, the network becomes more efficient as less data must traverse the WAN. With this efficiency, user transaction times are faster and more transactions can occur (as indicated by the transaction count and average transaction time charts shown earllier) providing the user with faster responses from the application.

For more information on the Blue Coat Proxy SG visit: www.bluecoat.com > Products > Blue Coat ProxySG

APPENDIX A: SOLUTION SERVER FARM ARCHITECTURE

The server farm consists of 8 physical servers: 4 application servers (load balanced by the Brocade ServerIron pair), a database server, the lab active directory server (VM), a MOSS Management server, and an ISA server. Application servers have the following software and hardware configuration.

NOTE: This section presents data from the actual testing, but if you are deploying the solution described in this document, your environment may not look exactly like this one.

The MOSS Server Group

OS: Windows 2008 Enterprise X64 w/Dell SUU Driver Set v5.5.2 / Microsoft MOSS 2007

Hardware	Speed	Sockets	Core	Memory
Dell M600 Server Blade x4	3.00 Ghz	2	4	32 GB

The Database Server

OS: Windows 2008 Enterprise X64 w/Dell SUU Driver Set v5.5.2 / Microsoft SQL Server 2008 X64

Hardware	Speed	Sockets	Core	Memory
Dell M605 Server Blade	2.00 Ghz	2	4	32 GB

The MOSS Management Server

OS: Windows 2008 Enterprise X64 w/Dell SUU Driver Set v5.5.2 / Microsoft MOSS 2007

Hardware	Speed	Sockets	Core	Memory
Dell M605 Server Blade	2.00 Ghz	2	4	32 GB

The ISA Server

The ISA server provides access to the internet and VPN access into the lab.
OS: Windows Server 2003 Enterprise X86 / Microsoft ISA Server 2006 Standard.

Hardware	Speed	Sockets	Core	Memory
HP DL145 G1 RM Server	2.20 Ghz	2	1	2 GB

The Active Directory Server

OS: Windows Server 2008 Enterprise X64 (Windows 2008 Enterprise X86 Guest running under Hyper-V Role, RTM, 2 Virtual Processors, 2GB RAM)

Software	Speed	Sockets	Core	Memory
HP DL580 G4 Server	3.6 GHz (P4 XEON)	4	2	16 GB

APPPENDIX B: TRAFFIC FLOW DISCUSSION

The diagram in Figure 5 shows the connectivity implemented in the test bed and the resulting traffic flows.

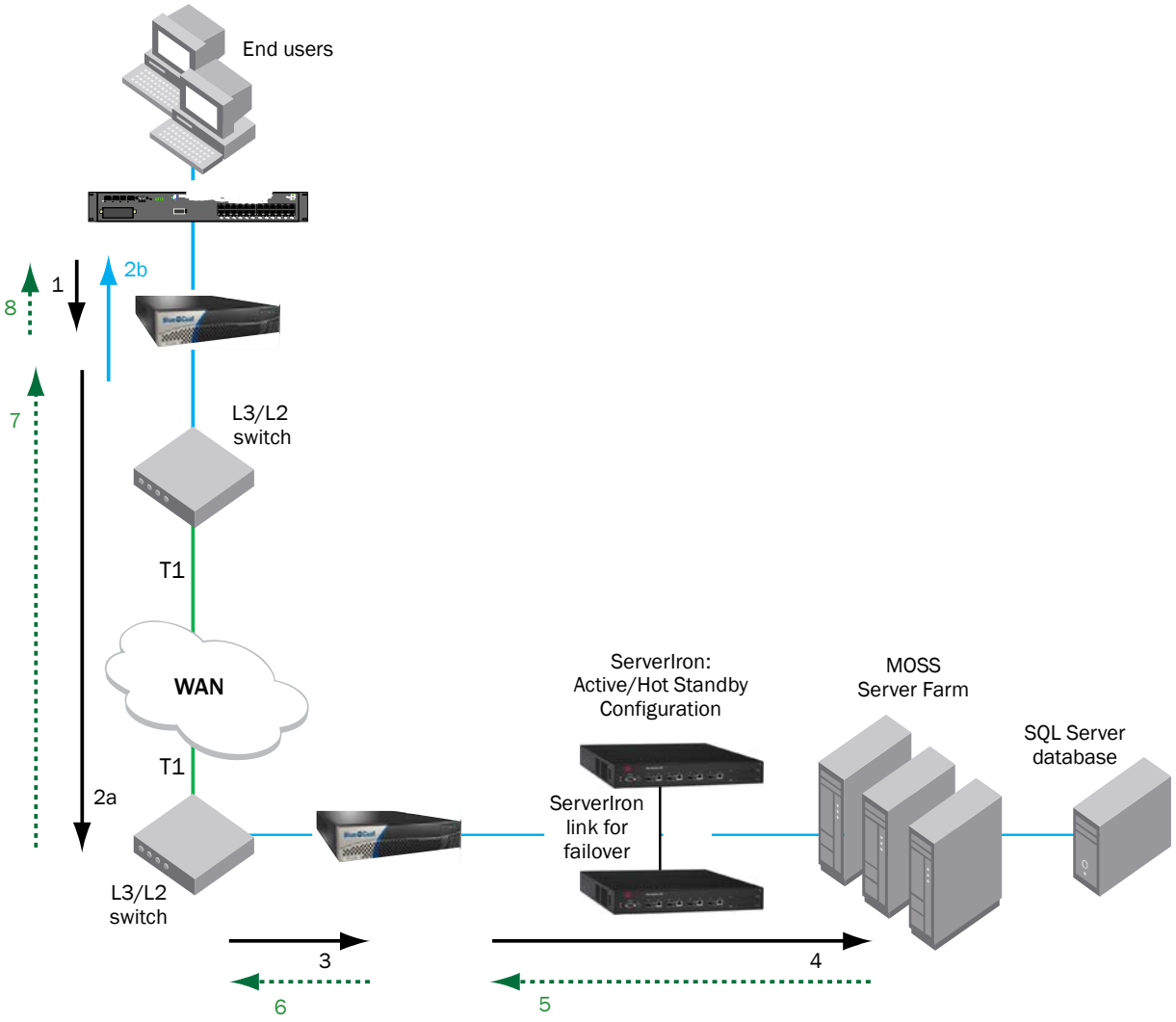


Figure 5. The handshake between a client and the server farm

The following describes the handshake between a client and the server farm and the data transfer phase:

1. The client sends a TCP SYN (synchronize) packet to the server farm VIP address. The packet is forwarded to the branch router. The Blue Coat Proxy SG intercepts the packet.
2. The branch Blue Coat ProxySG applies a new TCP option (0x21) to the packet if the application is identified for optimization by an application classifier. The branch Blue Coat ProxySG adds its device ID and application policy support to the new TCP option field. This option is examined and understood by other Blue Coat ProxySG in the path as the ID and policy fields of the initial Blue Coat ProxySG device. The initial ID and policy fields are not altered by another Blue Coat ProxySG. The packet is forwarded to the branch router and then to the WAN.
3. During the data transfer phase, if the requested data are in its cache, the branch Blue Coat ProxySG returns its cached data to the client. Traffic does not travel through the WAN to the server farm. Hence both response time and WAN link utilization are improved.

4. The packet arrives on the WAN edge router. The WAN edge router intercepts the packet and forwards to the VIP address of the server farm.

5. The data center Blue Coat ProxySG intercepts and inspects the packet. Finding that the first device ID and policy is populated, it updates the last device ID field (first device ID and policy parameters are unchanged). The data center Blue Coat ProxySG forwards the packet to the Brocade ServerIron. The Brocade ServerIron forwards the packet to the server farm VIP with TCP option 21 removed. TCP options are usually ignored by the server, even if it is still in place. The Brocade ServerIron performs load balancing to the data traffic. Other functions the Brocade ServerIron performs include SSL offload, TCP reuse, cookie and IP sticky pertinence.

6. The following steps are for reverse traffic flow. The server farm sends the SYN/ACK packet back to the client with no TCP option. The packet from the server farm is matched in the session table of the Brocade ServerIron and forwarded to the WAN edge router. The Blue Coat ProxySG intercepts the packet and marks the packet with TCP option 0x21. During the data transfer phase, the data center Blue Coat ProxySG caches the data if the data are not in its cache.

7. The data center Blue Coat ProxySG forwards the packet to the WAN edge router.

8. The packet travels through the WAN and arrives at the branch router. The branch router intercepts the packet and forwards it to the user. The branch Blue Coat ProxySG is aware of the Blue Coat ProxySG in the data center because the SYN/ACK TCP option 0x21 contains an ID and application policy. The auto-negotiation of the policy occurs as the branch Blue Coat ProxySG compares its application-specific policy to that of its remote peer defined in the TCP option. At this point, the data center Blue Coat ProxySG and branch Blue Coat ProxySG have determined the application optimizations to apply on this specific TCP flow. During the data transfer phase, the branch Blue Coat ProxySG caches the data if the data are not in its cache.

9. The packet is forwarded to the client.

APPENDIX C: SERVERIRON CONFIGURATION

Basic Configuration - L2 Active /Hot Standby and Least Connection Predictor

```
SLB-telnet@SP1#sh run
!Building configuration...
!Current configuration : 1548 bytes
!
ver 10.2.01gTI2
!
server backup ethe 3 0012.f27c.8540 vlan-id 999
server backup-preference 5
!
!
server no-fast-bringup
no server use-simple-ssl-health-check
server source-nat
server source-nat-ip 10.10.58.98 255.255.255.0 0.0.0.0 port-range 1
server router-ports ethernet 1
!
context default
!
server real R1 10.10.58.51
port http
port http keepalive
port http url "GET http://intranet/Pages/Default.aspx"
!
server real R2 10.10.58.52
port http
port http keepalive
port http url "GET http://intranet/Pages/Default.aspx"
!
server real R3 10.10.58.53
port http
port http keepalive
port http url "GET http://intranet/Pages/Default.aspx"
!
!
server virtual vip1 10.10.58.99
predictor least-conn
port http
bind http R1 http R2 http R3 http
!
vlan 1 name DEFAULT-VLAN by port
no spanning-tree
!
vlan 999 by port
untagged ethe 3
no spanning-tree
!
aaa authentication web-server default local
boot sys fl pri
```

```
no enable aaa console
hostname SP1
ip address 10.10.58.252 255.255.255.0
ip default-gateway 10.10.58.1
telnet server
username admin password .....
snmp-server
clock timezone us Pacific
!
end
```

Basic Configuration - L2 Active/Hot Standby, SSL Offload, and Least Connection Predictor

```
SLB-telnet@SP1#sh run
!Building configuration...
!Current configuration : 1718 bytes
!
ver 10.2.01gTI2
!
ssl profile zprofile
 keypair-file m-key
 certificate-file bcert
 cipher-suite all-cipher-suites
 allow-self-signed-cert
 session-cache off
!
server backup ethe 3 0012.f27c.8540 vlan-id 999
server backup-preference 5
server backup-timer 50
!
!
server no-fast-bringup
no server use-simple-ssl-health-check
server port 80
 session-sync
 tcp
server source-nat
server source-nat-ip 10.10.58.98 255.255.255.0 0.0.0.0 port-range 1 for-ssl
server source-nat-ip 10.10.58.97 255.255.255.0 0.0.0.0 port-range 1
server router-ports ethernet 1
!
context default
!
server real R1 10.10.58.51
 port http
 port http keepalive
 port http url "GET http://intranet/Pages/Default.aspx"
!
server real R2 10.10.58.52
 port default disable
 disable
 port http disable
 port http keepalive
```

```
 port http url "GET http://intranet/Pages/Default.aspx"
!
server real R3 10.10.58.53
 port default disable
 disable
 port http disable
 port http keepalive
 port http url "GET http://intranet/Pages/Default.aspx"
!
!
server virtual vip1 10.10.58.99
 predictor least-conn
 port ssl
 no port ssl sticky
 port ssl ssl-terminate zprofile
 port http
 bind ssl R1 http R2 http R3 http
!
vlan 1 name DEFAULT-VLAN by port
 no spanning-tree
!
vlan 999 by port
 untagged ethe 3
 no spanning-tree
!
aaa authentication web-server default local
boot sys fl pri
no enable aaa console
hostname SP1
ip address 10.10.58.252 255.255.255.0
ip default-gateway 10.10.58.1
telnet server
username admin password .....
snmp-server
clock timezone us Pacific
!
End
```