Deployment Guide

Oracle Siebel CRM

DG_ OrSCRM_032013.1

TABLE OF CONTENTS

1 INTRODUCTION

Oracle's Siebel Customer Relationship Management (CRM) software is the world's most advanced CRM solution, delivering a combination of transactional, analytical and engagement features to manage all customer-facing transactions. Siebel solutions can be custom tailored into solutions for more than 20 diverse industries, with comprehensive on-premise and on-demand CRM. In order for Siebel to offer a scalable CRM solution, A10 Networks' AX Series provides a scalable and redundant solution in a Siebel multi-server environment. The AX Series Application Deliver Controllers (ADCs) can provide advanced server load balancing services for Siebel CRM as well as application acceleration and optimization.

2 DEPLOYMENT TOPOLOGY

This document shows how the A10 Networks AX Series can be deployed in an Oracle Siebel environment. The tested solution is based on AX Series devices load balancing multiple Oracle Application Servers (OASs) on the front-end layer, followed by Siebel Web Server Extension (SWSE) load balancing on the back-end layer. (Refer to Figure 1.)

This solution is based on multiple AX Series devices but it also can be supported with one (1) physical AX device using Application Delivery Partitions (ADPs). In order to have a robust and scalable Siebel CRM deployment, A10 is recommended for the following reasons:

- Siebel CRM application redundancy is supported with multiple options for load balancing (algorithm not limited to round robin).
- AX Series offers RAM Caching as a standard network optimization for the end-user, network, and web servers where frequently requested objects from the web servers are stored locally in the RAM of the AX Series.
- AX Series provides HTTP Compression features interpreted by standard web browsers by compressing payload traffic to less than normal size.
- aFleX redirect features can be used to process all non-SSL user requests.
- Session persistence features enable all requests to be sent to the same Siebel Application Server (SAS) to minimize inter-server processing and optimize performance.

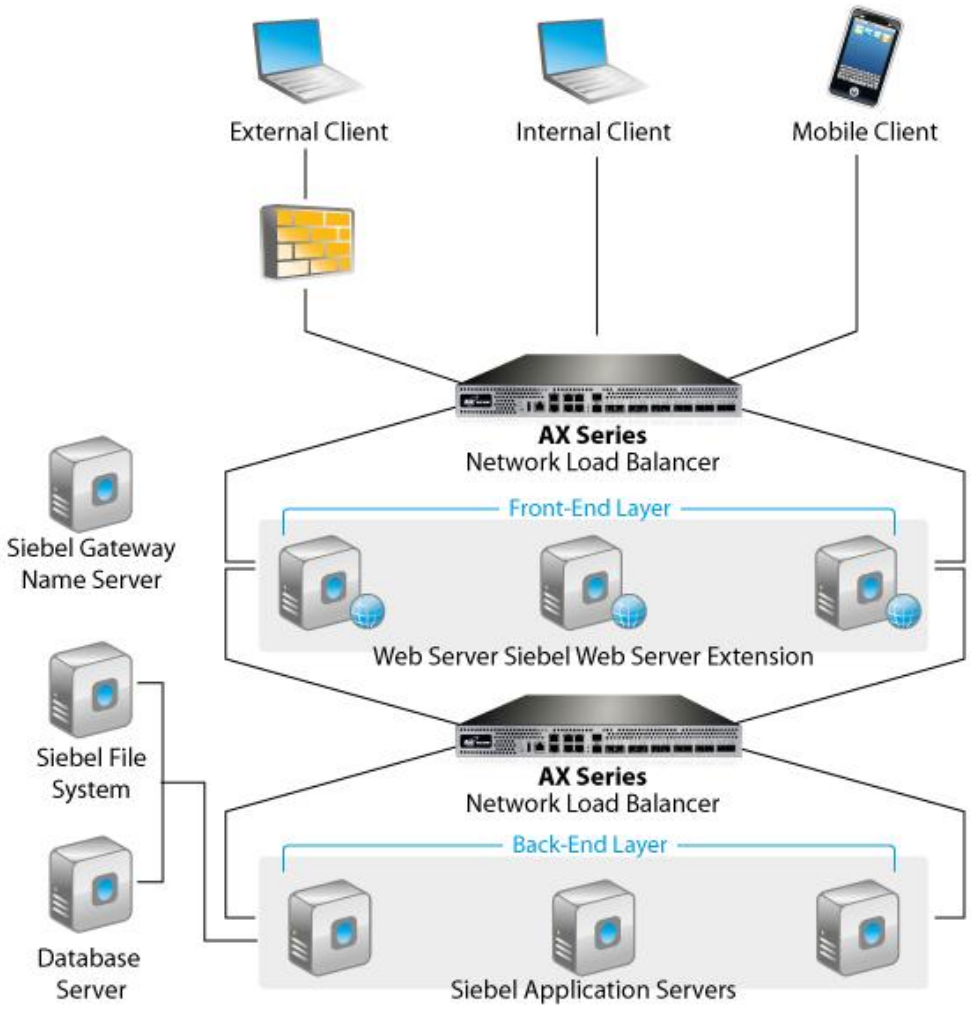

Figure 1: Oracle Siebel CRM 8.0 and AX Series topology overview

The deployment guide is divided into two sections; namely: Basic AX configuration and Advanced AX configuration for Siebel CRM. The Basic AX configuration is a bare minimum configuration that can be used in a Siebel CRM application server load balancing deployment. The Advanced AX configuration section covers optimization and acceleration features offered in the AX Series.

2.1 DEPLOYMENT PREREQUISITES

The deployment guide was tested based on the following prerequisites.

AX Series Requirements:

- The AX Series ADC must be running version 2.7.x.
- One-arm mode deployment configuration must be used.

Oracle Siebel CRM Requirements:

- The Oracle Siebel CRM 8.x.x application was tested and deployed for internal access.
- All Oracle Siebel applications are on Windows 2003 Enterprise Edition server operating system.
- Microsoft SQL Server and ODBC drivers are required based on Siebel system requirements.

Note: *Other Operating Systems (OSs) also are supported with the Siebel CRM application, including: IBM, Solaris, HP-UX, Linux, and Novell Operating Systems. If your deployment is using any of these OSs, refer to your Oracle Siebel installation guide.*

- Client access was tested with:
  - Microsoft Internet Explorer Version 8.0
  - Mozilla Firefox Version 19

Note: *If end-users would like to access the Siebel CRM application from an external site, VPN access or a remote access application should be in place.*

Note: *For additional deployment modes that the AX Series device can support, please visit the following URL:*

http://www.a10networks.com/products/axseries-load-balancing101.php

2.2 SIEBEL CRM SERVER ROLES

Table 1 describes the server roles for the test environment:

Table 1: Server Role Matrix	
Siebel Web Server Extension (SWSE)	Identifies requests for Siebel information coming from Web clients and flags the requests for routing to Siebel servers. The SWSE receives and parses inbound HTTP requests from web- or java-based clients. The SWSE also is responsible for routing requests to the appropriate Siebel server components.
Siebel Enterprise Server (SES)	The SES can be configured, managed and monitored as a single logical group, providing the ability for a system administrator to start and stop services within an SES.
Siebel Name Server	Also known as the Gateway Name Server, the Siebel Name Server is the dynamic registry of Siebel servers and component availability information. It also functions as the central point for definition and assignments of component groups and components, connectivity information and operational parameters.
Siebel File System (SFS)	Consists of a shared directory that is accessible to all Siebel servers in the Siebel Enterprise. It contains the physical files used by the Siebel clients and Siebel servers.

3 ACCESSING THE AX APPLICATION DELIVERY CONTROLLER

This section describes how to access the AX Series device. The AX device can be accessed either from a Command Line Interface (CLI) or Graphical User Interface (GUI):

- CLI – 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 – Web-based interface in which you click to access configuration or management pages and 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 username: "*admin*"
    - Default password: "*a10*".
    - Default IP address: *172.31.31.31*

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

4 AX PRE-CONFIGURATION SETUP FOR ORACLE SIEBEL CRM

This section of the deployment guide explains how to configure the AX device with basic load balancing and needed features for the load balancing to perform. This section covers configuration of some templates (health monitor, source-IP persistence, client-SSL, and IP source NAT) in preparation for configuring the AX device for load balancing.

The purpose of creating all feature templates first, is to make them available to apply to the virtual service using drop-down menus.

4.1 TEMPLATE: HEALTH MONITOR CONFIGURATION

The AX Series can automatically initiate the health status checks of real servers and service ports. This provides clients assurance that all requests go to functional and available servers. If a server or a port does not respond appropriately to a health check, the server will be removed temporarily from the list of available servers. Once the server is restored and starts responding appropriately to the health checks, the server automatically will be added back to the list of available servers.

1. Navigate to **Config Mode > Service > SLB > Health Monitor > Health Monitor**.
2. Click **Add** and name the template "Siebel HC".
3. Select ICMP as the **Type**. If you wish to use any other health check method, you will be able to change the configuration in the Method section.
4. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

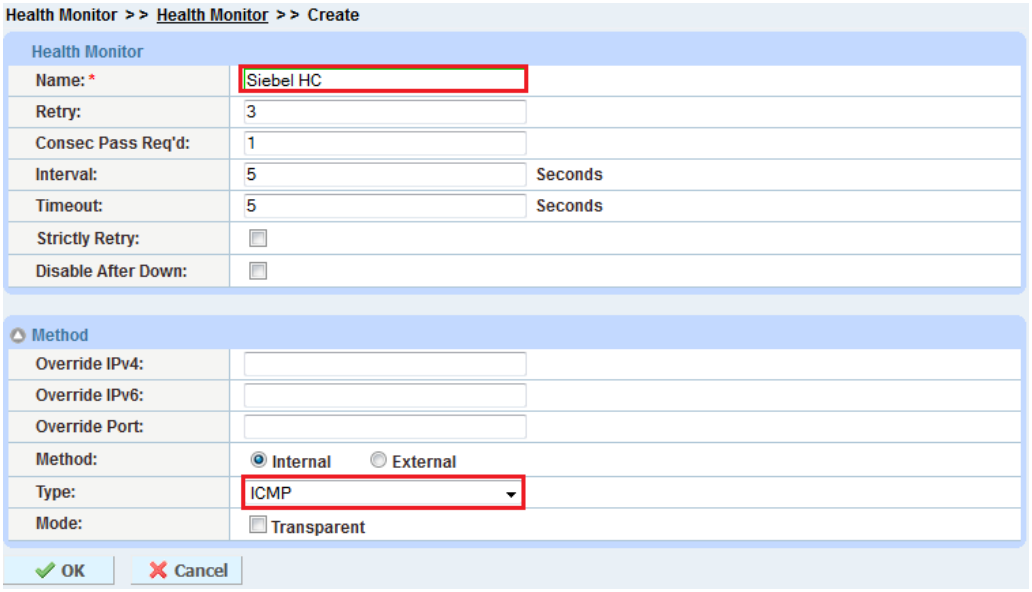

Figure 2: Health Monitor Configuration

Note: *ICMP is one of the basic health check types that the AX Series can provide. If you want HTTP application-layer health checks, refer to the AX Series Application Delivery and Server Load Balancing Guide.*

4.2 TEMPLATE: SOURCE-IP PERSISTENCE CONFIGURATION

The AX Series can support various modes of persistence: cookie persistence, destination-IP persistence, source-IP persistence, and SSL-session-ID persistence. The purpose of persistence is to direct traffic from the same client to the same server.

This Oracle Siebel CRM deployment guide focuses on source-IP persistence configuration.

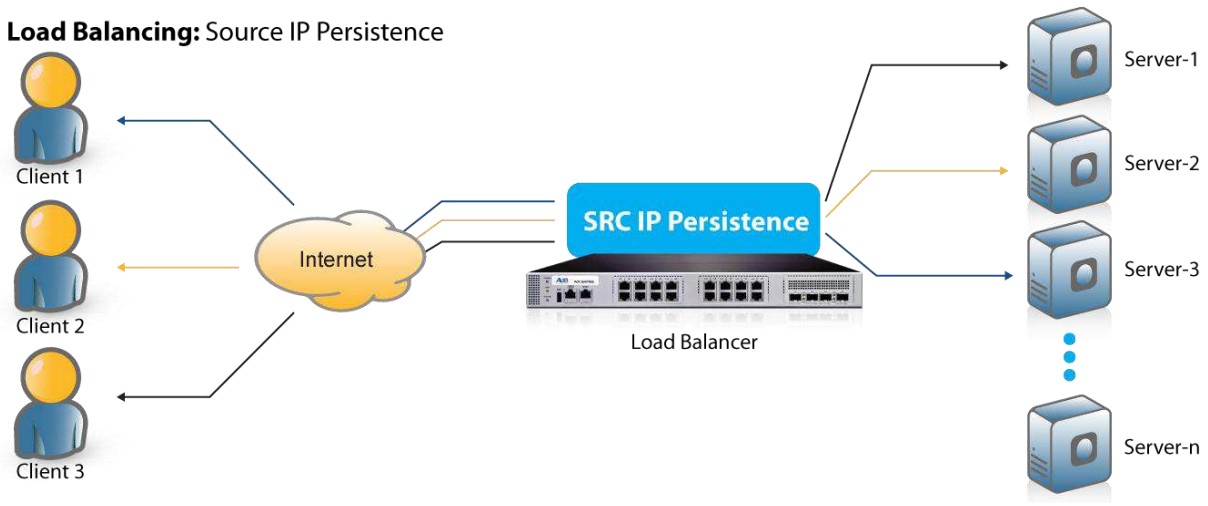

Figure 3: Source-IP persistence

To configure source-IP persistence:

1. Navigate to **Config Mode > Service > Template > Persistent > Source IP Persistence**.
2. Click **Add**.
3. Enter a name for the template; for example: "Source IP Persistence".
4. Select Port from the **Match Type** drop-down list.
5. Leave the **Timeout** set to 5 minutes (the default).
6. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

Figure 4: Source IP persistence template

4.3 IP SOURCE NAT

This section configures the IP Address pool to be used for IP Source Network Address Translation (SNAT). When incoming traffic from a client accesses the VIP address (for example, 172.16.1.200), the client requests are "source NATed", which means that the AX device replaces the client's source IP address based on the configured address pool of the source NAT. SNAT is required when your network topology is based on "one-arm" deployment and if you have internal clients that reside on the same subnet as the VIP. The source NAT template must be applied to the virtual server port for the NAT to take effect.

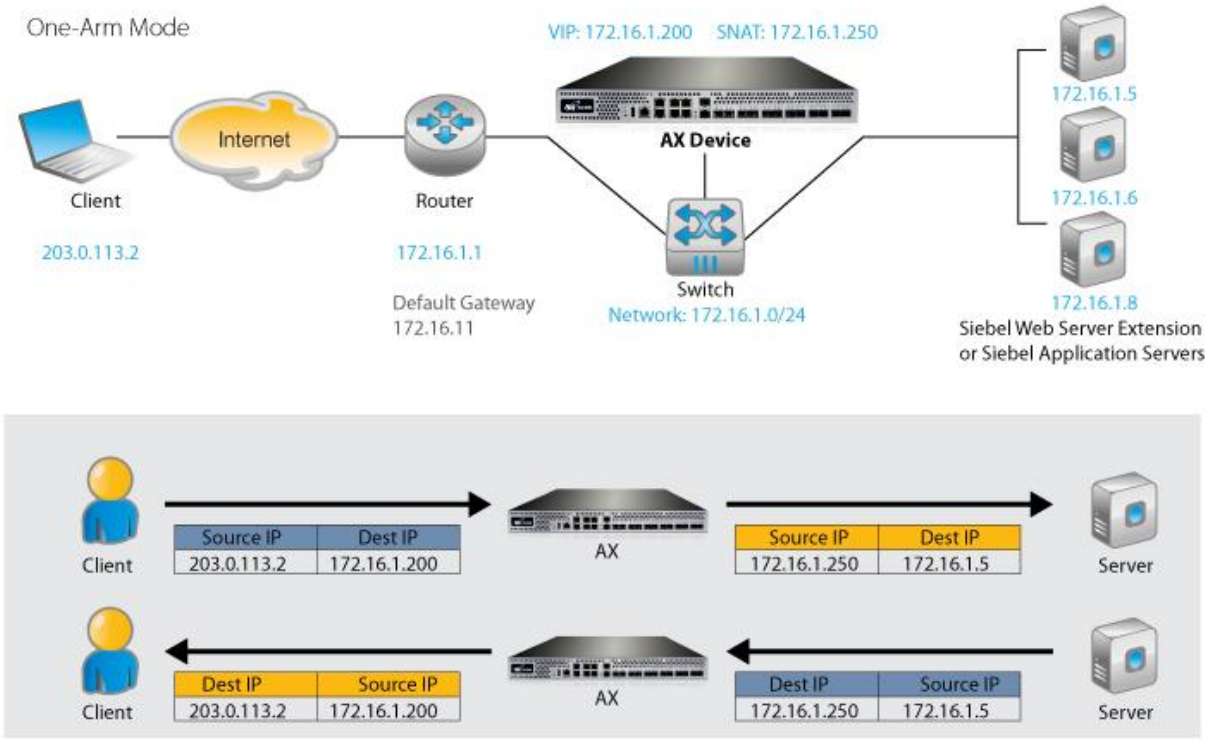

Figure 5: IP source NAT and traffic flow overview

Note: *IP source NAT also must be applied within the back-end layer of the Oracle Siebel CRM deployment where the SCbrokers (listening on port 2321) are load balanced.*

4.4 TEMPLATE: IP SOURCE NAT CONFIGURATION

1. Navigate to **Config Mode > Service > IP Source NAT**.
2. Click **Add**.
3. Enter the following information. (The values shown are examples.)
   - **Name**: "SNAT"
   - **Start IP Address**: 172.16.1.250
   - **End IP Address**: 172.16.1.250
   - **Netmask**: 255.255.255.0
4. Apply the SNAT template to the virtual server port:
   a. Navigate to **Config Mode > Service > SLB > Virtual Service**.
   b. Click on the virtual service name (for example: "_172.16.1.200_HTTPS_443").
   c. Select the pool from the **Source NAT Pool** drop-down list.
5. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

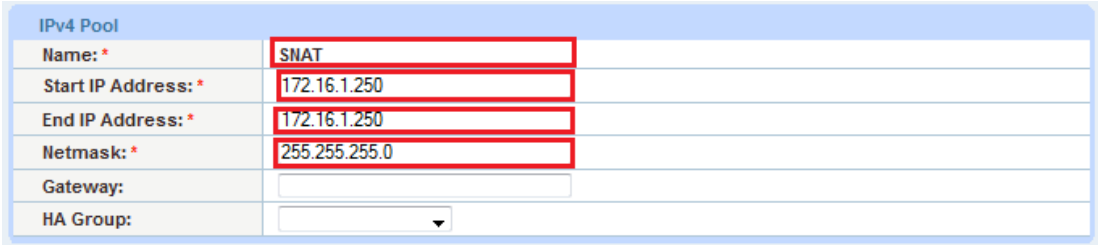

Figure 6: IP source NAT template

Note: *If the Oracle Siebel CRM environment will consist of many concurrent users, it is advisable to configure multiple SNAT IP addresses. One IP address can be used for up to 64,000 flows.*

4.5 CLIENT- SSL CONFIGURATION

SSL Offload acts as an acceleration feature by removing the burden of processing SSL traffic as well as providing secured HTTPS connections to Oracle SWSE. Instead of having the Oracle Siebel servers handle these transactions, the AX Series decrypts all HTTPS traffic and forwards the decrypted traffic to the Siebel Server via (unsecured) HTTP. In addition, instead of having unsecured connections to the SWSE, the AX device will secure the connections.

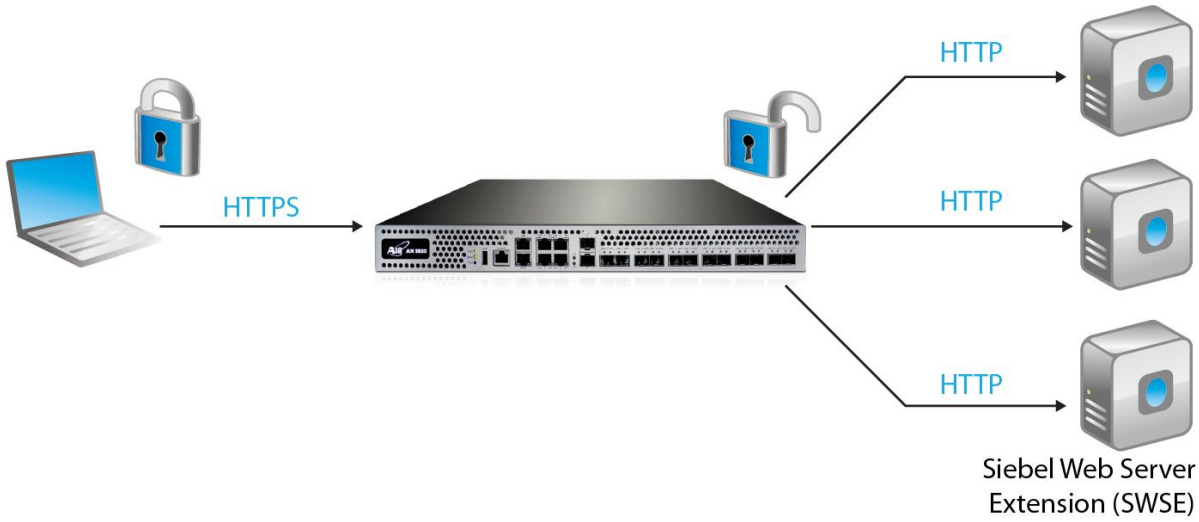

Figure 7: SSL Offload

In this configuration, an SSL certificate is configured for the SWSE HTTPS virtual server. This enables the client to access the SWSE web services in secure mode.

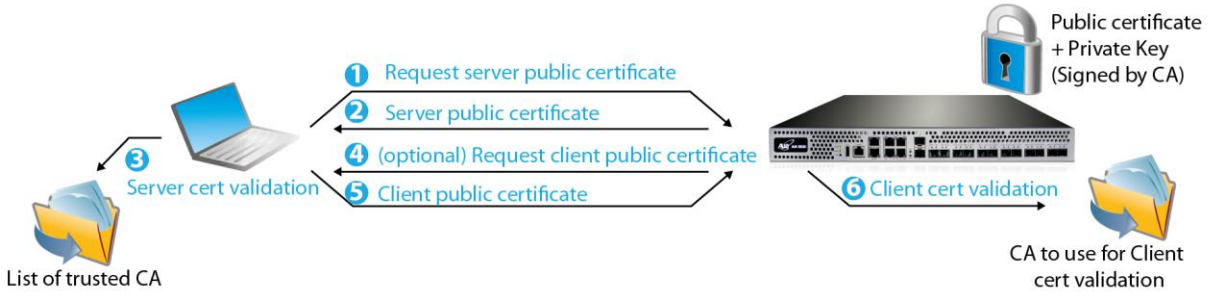

Figure 8: Client SSL

Note: *An SSL certificate can be obtained from various Certificate Authority (CA) companies such as VeriSign, or you can generate a self-signed certificate on the AX device.*

4.6 IMPORT OR GENERATE CERTIFICATE

1. Navigate to **Config Mode > SSL Management > Certificate**.
2. There are two ways to install an SSL certificate and key on the AX device:
   - Option 1: Generate a self-signed certificate on the AX device.
   - Option 2: Import an SSL certificate and key signed by an external Certificate Authority (CA).

4.7 OPTION 1: GENERATE SELF-SIGNED CERTIFICATE ON THE AX DEVICE

1. Navigate to **Config Mode > Service > SSL Management > Certificate**.
2. Click **Create** to add a new SSL certificate.
3. Enter the certificate information. (Values shown are examples.)
   - **File Name:** "SWSE"
   - **Issuer:** "Self"
   - **Common Name:** "SWSE"
   - **Division:** "A10"
   - **Organization:** "A10"

- **Locality:** "San Jose"
- **State or Province:** "CA"
- **Country:** "USA"
- **Email Address:** "siebeladmin@example.com"
- **Valid Days:** "730" (default)
- **Key Size (Bits):** "2048"

Note: *The AX Series device can support 512-, 1028-, 2048-, or 4096-bit keys. The higher the bit size, the more CPU processing that will be required on the AX device.*

4. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

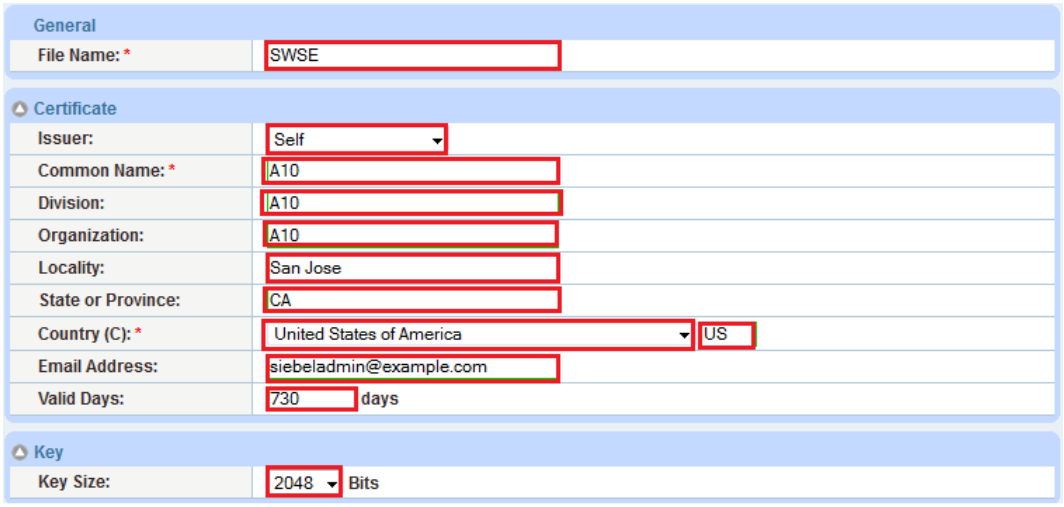

Figure 9: Client-SSL certificate creation

4.8 OPTION 2: IMPORT CA-SIGNED SSL CERTIFICATE AND KEY

1. Navigate to **Config Mode > Service > SSL Management > Certificate**.
2. Click **Import** to add a new SSL certificate.
3. Enter a name for the certificate; for example: "SWSE".

4. Select **Local** and browse to the certificate location, or select **Remote** and enter the file access information.

5. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

Note: *If you are importing a CA-signed certificate for which you used the AX device to generate the CSR, you do not need to import the key. The key is automatically generated on the AX device when you generate the CSR.*

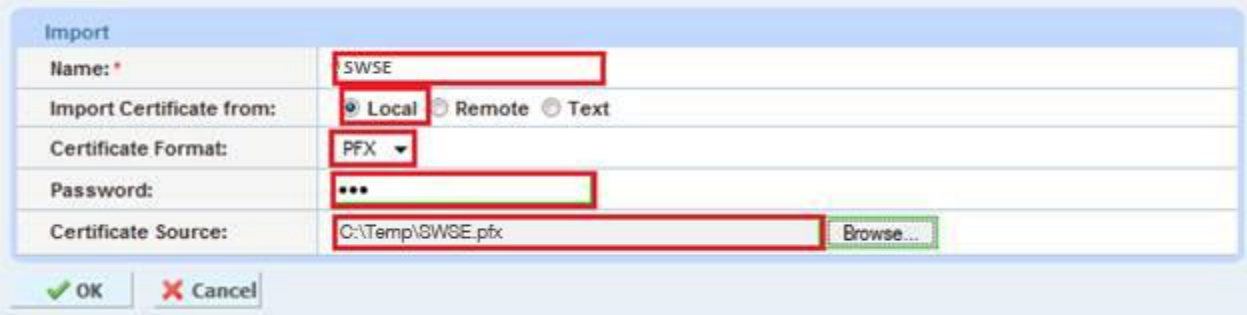

Figure 10: Import SSL certificate

4.9 CONFIGURE AND APPLY CLIENT-SSL TEMPLATE

1. Navigate to **Config Mode > Service > Template > SSL > Client SSL**.

2. Click **Add**.

3. Enter the following information (values shown are examples).

   - **Name:** "SWSE"
   - **Certificate Name:** "SWSE"
   - **Key Name:** "SWSE"
   - **Pass Phrase**, **Confirm Pass Phrase**: "example"

Figure 11: Client SSL configuration

Once the Client SSL template is completed, bind the Client SSL to the HTTPS VIP (Port 443), as follows:

1. Navigate to **Config Mode > Service > SLB > Virtual Server**.
2. Click on the virtual server name.
3. Select the port ("443") and click **Edit**.
4. Select the client-SSL template from the **Client-SSL Template** drop-down list.
5. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

5 RAM CACHING CONFIGURATION

Cacheable data is cached within the AX Series device, thus reducing overhead on each SWSE or SAS server, and increasing the capacity of the Oracle Siebel servers. RAM caching reduces the number of connections and server requests that need to be processed.

Figure 12: RAM Caching Template

5.1 TEMPLATE: RAM CACHING CONFIGURATION

1. Navigate to **Config Mode > Service > Template > Application > RAM Caching**.
2. Click **Add**.
3. Enter the following information:
   - **Name:** "Siebel RAM Caching"
   - **Age:** 3600 seconds
   - **Max Cache Size:** 512 MB
   - **Min Content Size:** 10 Bytes
   - **Max Content Size:** 4194303 Bytes
   - **Replacement Policy:** Least Frequently Used
4. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

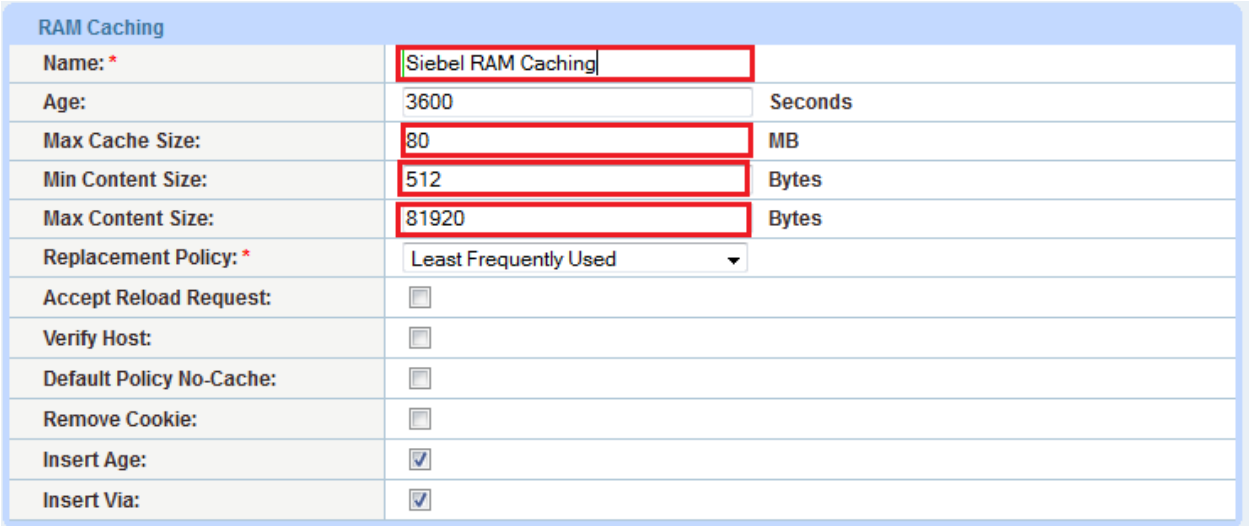

Figure 13: RAM Caching template

If you want your AX deployment to have a policy regarding the URI types that can be cached on the AX Series, enter the file extensions to be cached and the number of seconds to cache matching files.

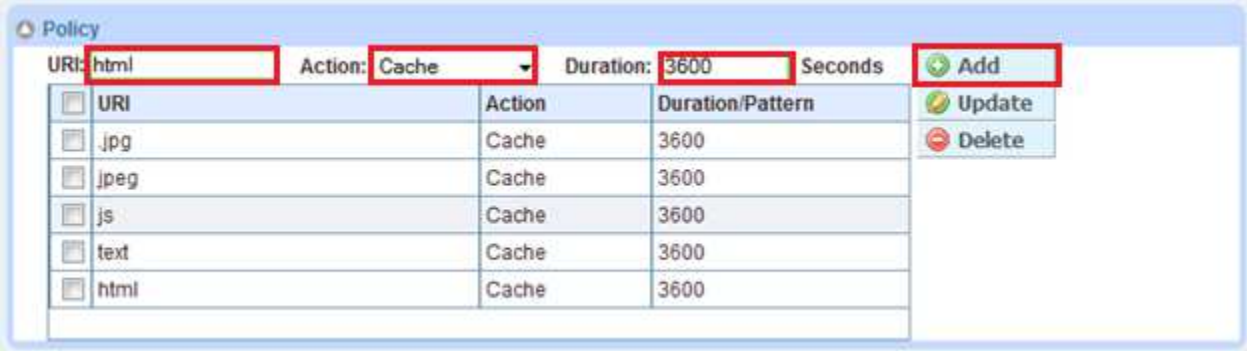

Figure 14: RAM Caching policy

Note: The RAM caching policy option is not required unless you have specific data that requires caching, no-caching or invalidation. These policy options can be configured in the RAM Caching template. For additional information, see the *AX Series Application Delivery and Server Load Balancing Guide*.

6 SECURING ORACLE SIEBEL CRM USING AFLEX

This section of the deployment guide explains how to redirect Oracle Siebel request traffic that comes from HTTP to HTTPS using AX aFleX scripts. aFleX is based on a standard scripting language, TCL, and it enables the load balancer to perform Layer 7 deep-packet inspection (DPI). For examples of aFleX scripts, please refer to the following URL:

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

As an example, one of the most common aFleX scripts that can be used with an Oracle Siebel server is the "*HTTP redirect to HTTPS traffic*" script. You can download additional aFleX script examples with no A10 Support account required from the following URL:

https://www.a10networks.com/vadc/index.php/aflex-examples/

Note: *In addition to the virtual IP (VIP) for HTTPS, you may want to configure the VIP for HTTP (port 80). The HTTP VIP will always redirect users to HTTPS when the VIP receives HTTP traffic. This configuration can be useful for end-users with old browser bookmarks pointing to HTTP. The aFleX script shown in the following section redirects end-users (using HTTPS) to the page they requested. The aFleX script must be bound to virtual server port 80.*

6.1 DEFINE AFLEX SCRIPT

The steps in this section configure the following aFleX script on the AX device:

```
when HTTP_REQUEST {
HTTP::redirect https://[HTTP::host][HTTP::uri]
}
```

(Easy to copy and paste!)

To configure this aFleX script on the AX device:

1. Navigate to **Config Mode > Service > aFleX**.
2. Click **Add**.
3. Within the **Definition** field, enter the TCL code.
4. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

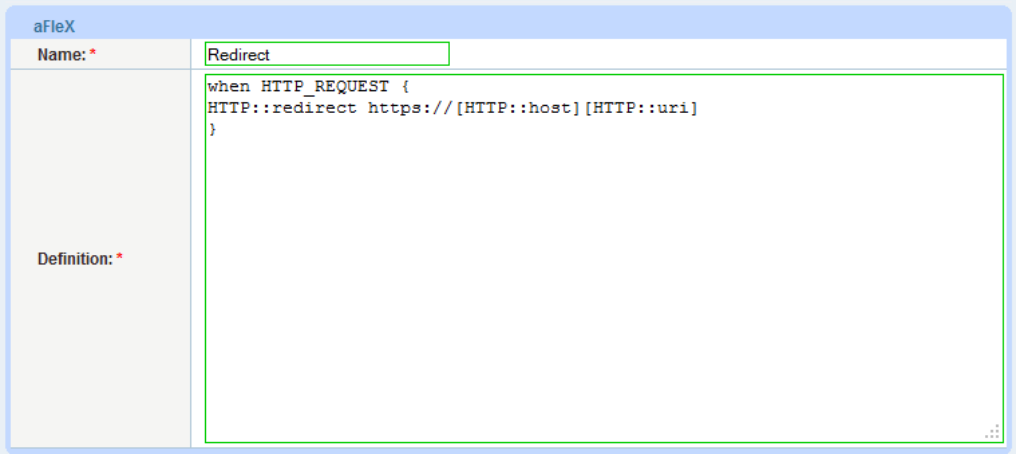

Figure 15: aFleX redirect configuration

Note: *In order for the HTTP-to-HTTPS aFleX redirect script to work, it is required that virtual server port 80 be configured, and for the aFleX redirect script to be applied to the port (virtual server port 80).*

7 FRONT-END LAYER: BUILDING A VIRTUAL IP CONFIGURATION

In the previous chapters of this deployment guide, all the preliminary features required to deploy an Oracle Siebel CRM are configured. This section of the document provides instructions for creating a VIP and applying the features on the virtual service.

7.1 REAL SERVER CONFIGURATION

1. Navigate to **Config Mode > Service > SLB > Server**.
2. Click **Add** to add a new server.
3. Within the **Server** section, enter the following information. (Values shown are examples.)
   - **Name:** "SWSE1"
   - **IP address /Host:** 172.16.1.5

   Note: *Enter additional servers if necessary.*

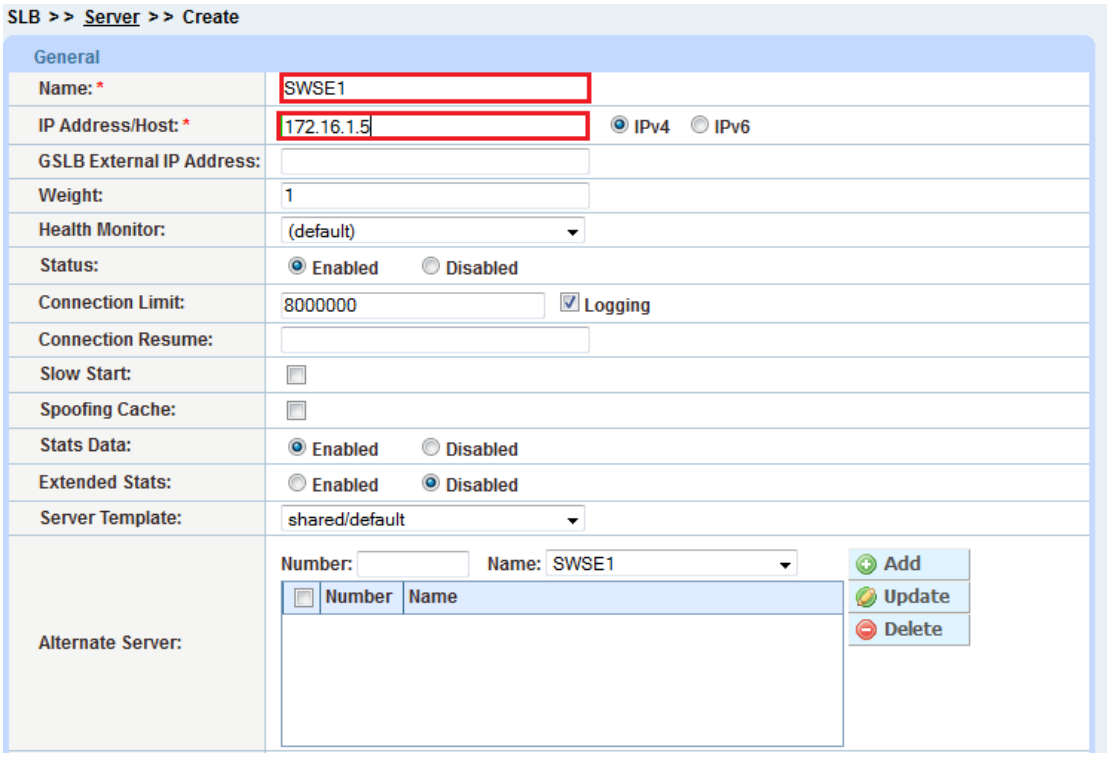

Figure 16: Server configuration

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**.

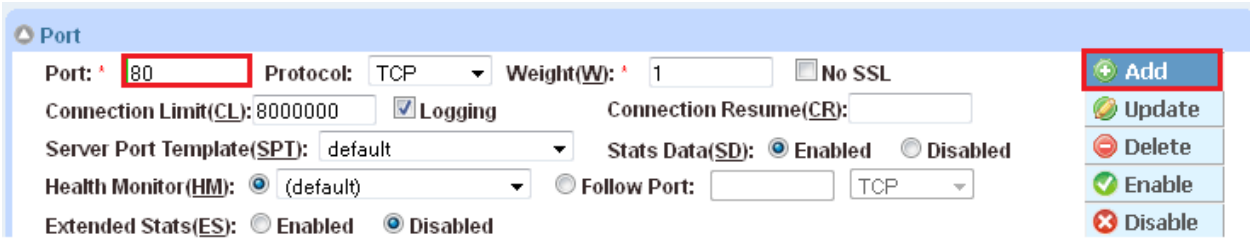

Figure 17: Server port configuration

5. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

7.2 SERVICE GROUP CONFIGURATION

This section demonstrates how to configure the SWSE web servers in a service group. A service group contains a set of real servers from which the AX device can select to service client requests. A service group supports multiple SWSE real servers as one logical server.

1. Navigate to **Config Mode > Service > SLB > Service Group**.
2. Click **Add** to add a new service group.
3. Within the **Server Group** section, enter the following required information:

    - **Name:** "SWSGROUP"
    - **Type:** "TCP"
    - **Algorithm:** "Least Connection"
    - **Health Monitor:** "Siebel HC"

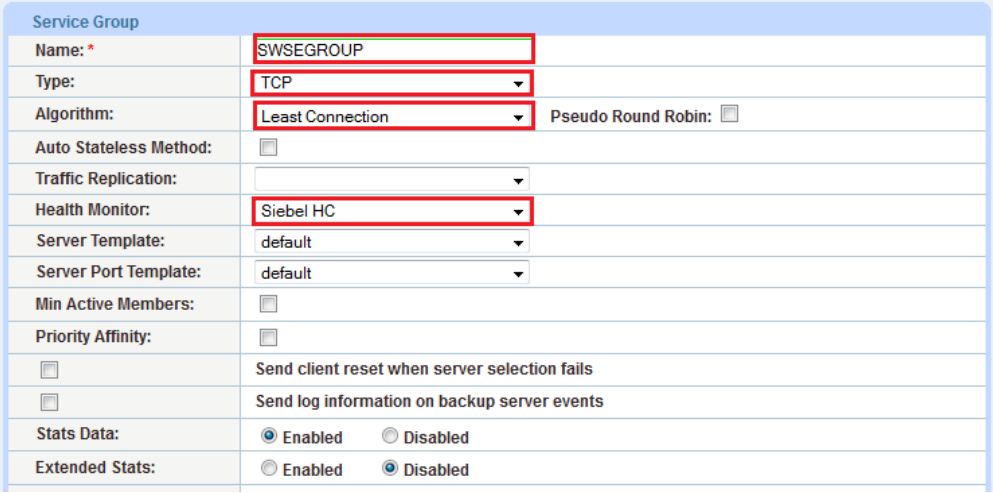

Figure 18: Service group configuration

4. In the **Server** section, add one or more servers from the **Server** drop-down list. For example, select server "SWSE1", enter port 80, and click **Add**.

5. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

In the following example, server names SWSE1 and SWSE2 are entered, each with port 80.

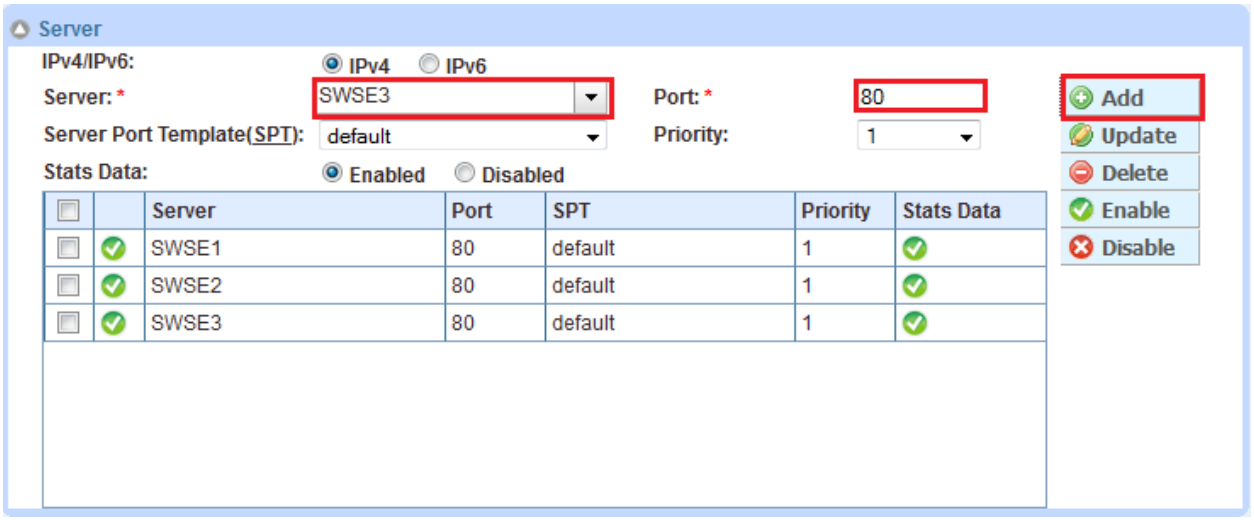

Figure 19: Service-group server configuration

7.3 VIRTUAL SERVER CONFIGURATION

This section demonstrates how to configure the virtual server. Adding the virtual server ports within the AX device will generate a virtual service list based on the protocol type selected.

1. Navigate to **Config Mode > Service > SLB > Virtual Server**.
2. Click **Add**.
3. Enter the following required information. (Values shown are examples.)
   - **Name:** "SWSE-VIP"
   - **IP Address or CIDR Subnet:** 172.16.1.200

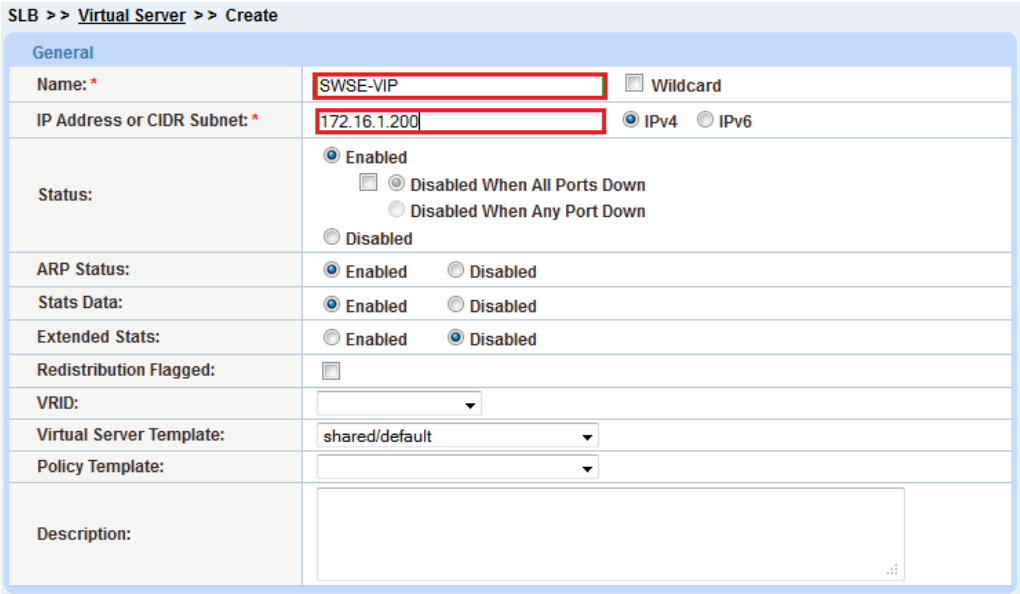

Figure 20: Virtual Server or VIP Configuration

4. Navigate to **Config Mode > Service > SLB > Virtual Server**.
5. In the **Port** section, click **Add**.

6. Enter the virtual server port information:
   - **Type:** HTTPS
   - **Port:** "443"
   - **Service Group:** "SWSEGROUP" to bind the virtual server to the real servers
7. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

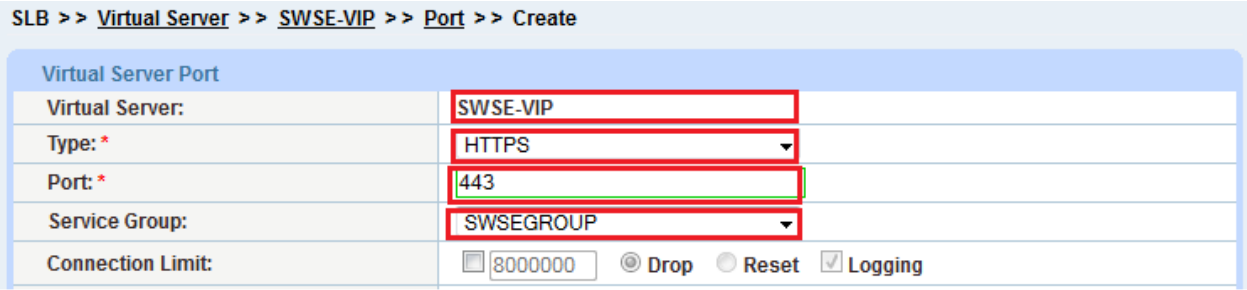

Figure 21: Virtual Server Port Configuration

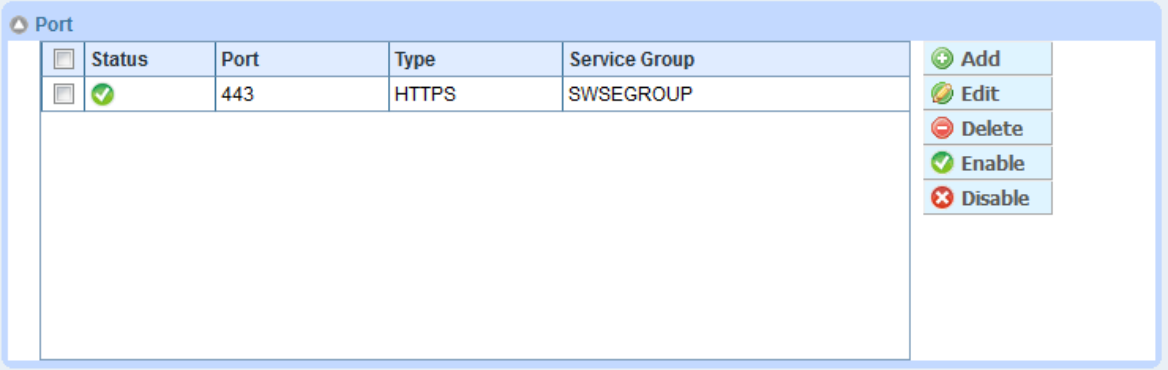

Figure 22: Virtual Port Lists

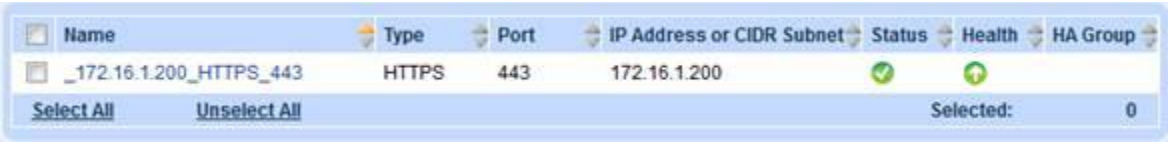

Figure 23: Virtual Services Overview

8 HTTP PORT FOR REDIRECT TO HTTPS

In order for the aFleX redirect to work within the AX device, an HTTP virtual service port (80) must be configured. All port 80 HTTP requests will be redirected to HTTPS (443), if the aFleX script is applied to the HTTP virtual port (80).

1. Navigate to **Config Mode > Service > SLB > Virtual Server**.
2. Click on the virtual server name.
3. In the Port section, click **Add**.
4. Enter the following information:
   - **Type:** HTTP
   - **Port:** "80"
   - **Service Group:** "SWSEGROUP"
   - **Source NAT Pool:** "SNAT"
   - **aFleX:** "Redirect"
5. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

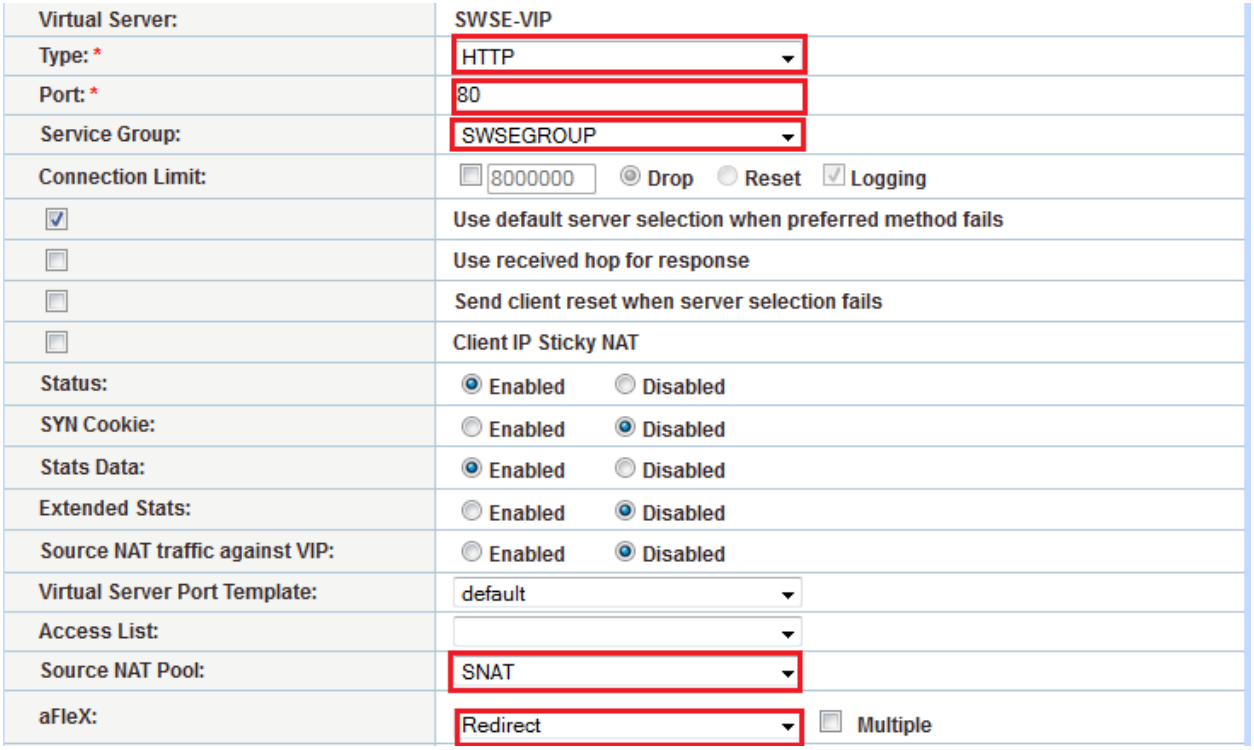

Figure 24: Source NAT and aFleX configuration

9 APPLYING FEATURES TO VIRTUAL SERVICE PORT

This section of the deployment is where all the previous features that were configured will be applied on a VIP. Assuming that the features described in the previous sections are configured, this section applies the features to the virtual service port.

1. Navigate to **Config Mode > Service > SLB > Virtual Service**.
2. Click on the service port name (for example: "_172.16.1.200_HTTPS_443").
3. Select the configured items to apply them to the virtual service port.

Features	Name
Source NAT Pool	SNAT
Client-SSL Template	SWSE
Persistence Template Type	Source IP Persistence
Source-IP Persistence Template	Source IP Persistence
RAM Caching	Siebel RAM Caching

4. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

This concludes the Front-End Layer configuration of the deployment guide, which covers the load balancing of the SWSE servers from the front-end layer of the Oracle Siebel topology.

10 BACK-END LAYER: BUILDING A VIP CONFIGURATION

This section of the deployment guide is where the Oracle Siebel Application Servers are load balanced. This is the second layer of load balancing within the Oracle Siebel, and uses SCBroker TCP port 2321.

To configure the load balancing, log into a separate AX device or ADP to deploy the Back-End Layer load balancing. Follow the same steps above to configure the AX device. You will need the following features: source NAT, source-IP persistence, and health checking.

10.1 BACK-END LAYER: HEALTH CHECK CONFIGURATION

This section of the deployment guide provides detailed instructions for configuring health checking for the SCBroker servers.

1. Navigate to **Config Mode > Service > Health Monitor > Health Monitor**.
2. Enter the following information:
   - **Name:** "SCBroker HC"
   - **Type:** "HTTP"
   - **Port:** "80"
   - **URL:** "/CRMEnt1/scbroker HTTP/1.0"
3. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

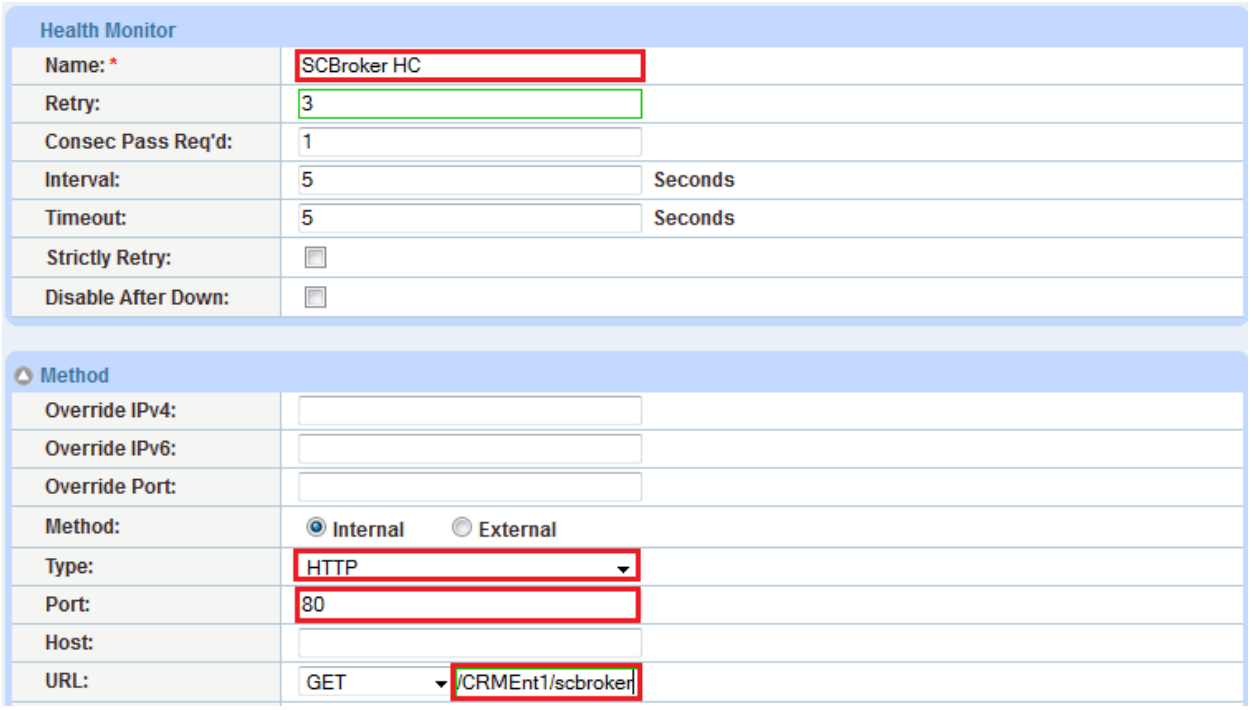

Figure 25: Health Monitor template

10.2 BACK-END LAYER: SOURCE NAT CONFIGURATION

1. Navigate to **Config Mode > Service > SLB > IP Source NAT**.

2. Click **Add**.
3. Enter the following information. (Values shown are examples.)
   - **Name:** "SNAT"
   - **Start IP Address**:192.0.2.250
   - **End IP Address:** 192.0.2.50
   - **Netmask:** 255.255.255.0
4. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

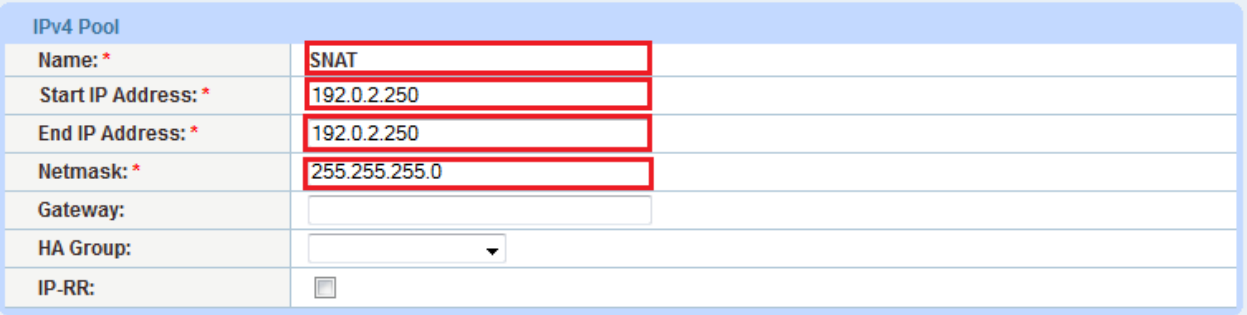

Figure 26: IP Source NAT pool

10.3 BACK-END LAYER: SOURCE-IP PERSISTENCE CONFIGURATION

1. Navigate to **Config Mode > Template > Persistent > Source IP Persistence**.
2. Click **Add**.
3. Enter the following information:
   - **Name:** "Source IP Persistence"
   - **Match Type:** Port
   - **Timeout:** 5 minutes (default)
4. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

Figure 27: Source-IP persistence template

10.4 REAL SERVER CONFIGURATION

This section demonstrates how to configure the Apache HTTP web servers on the AX Series.

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. (Values shown are examples.)
   - **Name:** "SAS1"
   - **IP address /Host:** 192.0.2.5

   Note: *Enter additional servers if necessary.*

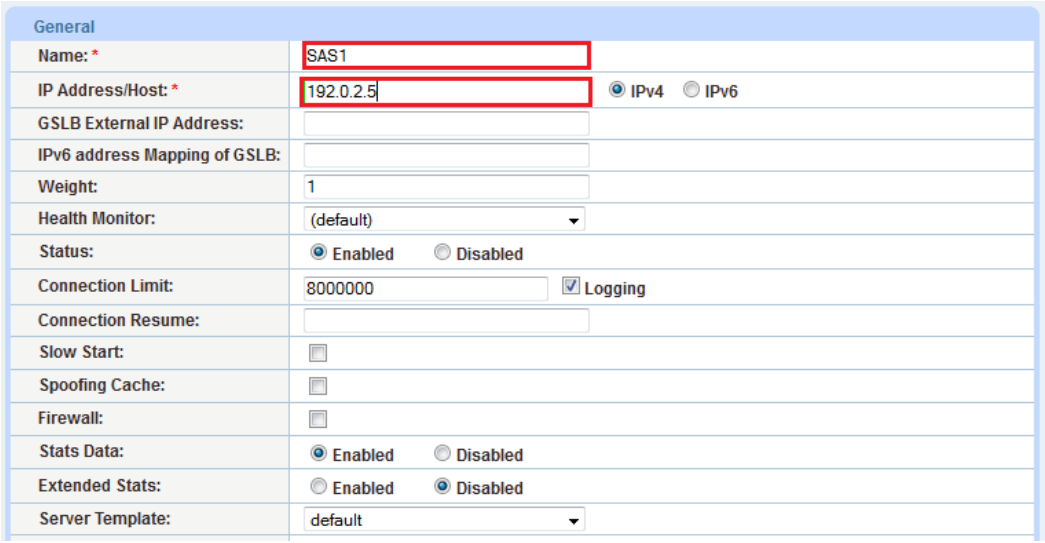

Figure 28: Server Configuration

4. To add a port to the server configuration:

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

   b. Select the **Protocol** (TCP).

   c. Click **Add**.

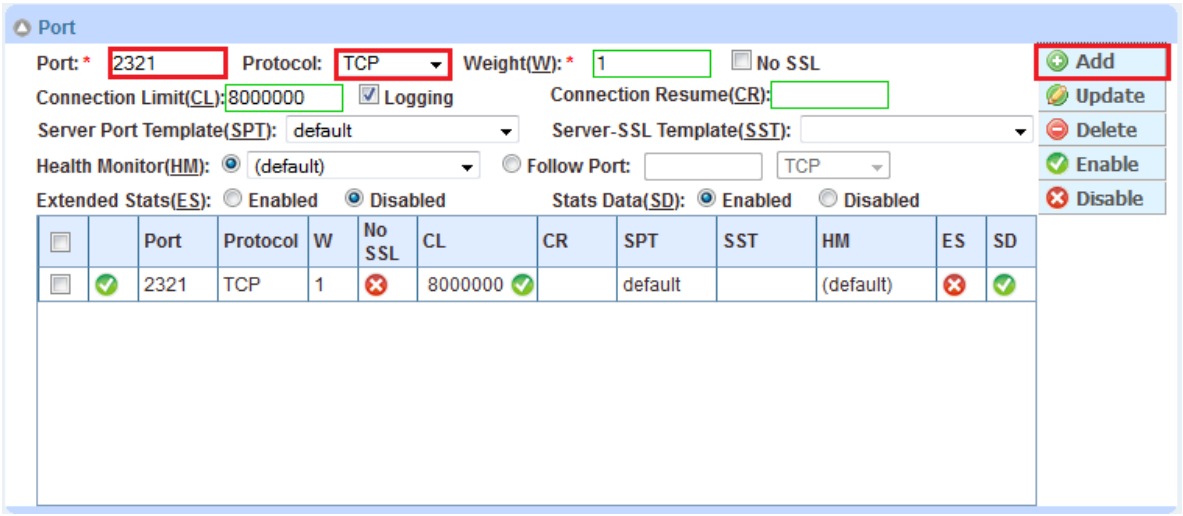

Figure 29: Server port configuration

5. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

10.5 SERVICE GROUP CONFIGURATION

This section demonstrates how to configure the SCBroker web servers in a service group. A service group contains a set of real servers from which the AX device can select to service client requests. A service group supports multiple real servers as one logical server.

1. Navigate to **Config Mode > Service > SLB > Service Group**.
2. Click **Add** to add a new service group.
3. Within the Server Group section, enter the following information:
   - **Name:** "SCBrokerGroup"
   - **Type:** "TCP"
   - **Algorithm:** "Least Connection"
   - **Health Monitor:** "SCBroker HC"

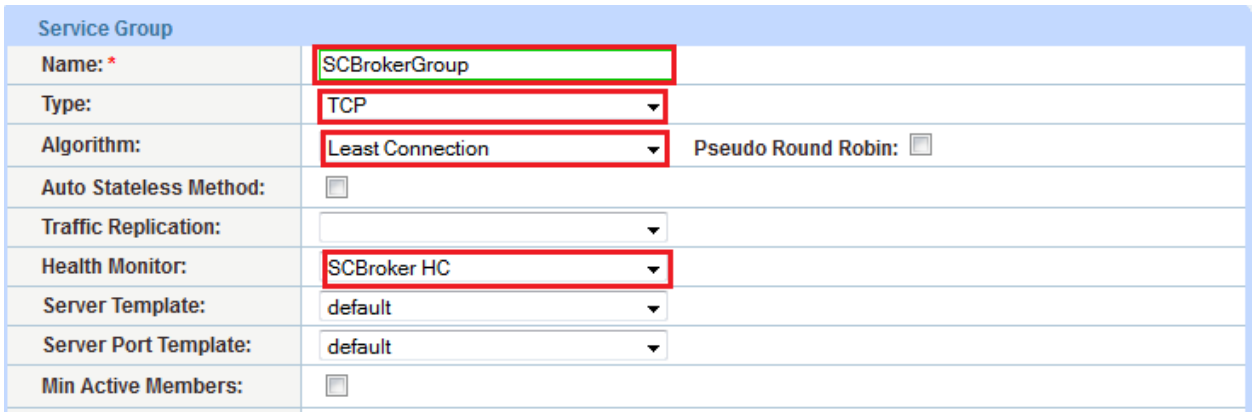

Figure 30: Service group configuration

4. In the **Server** section, add one or more servers from the **Server** drop-down list. For example, select server "SAS1", enter port "2321", and click **Add**.

   In the following example, the server names "SAS1", "SAS2", and "SAS3" are entered, each with port 2321.

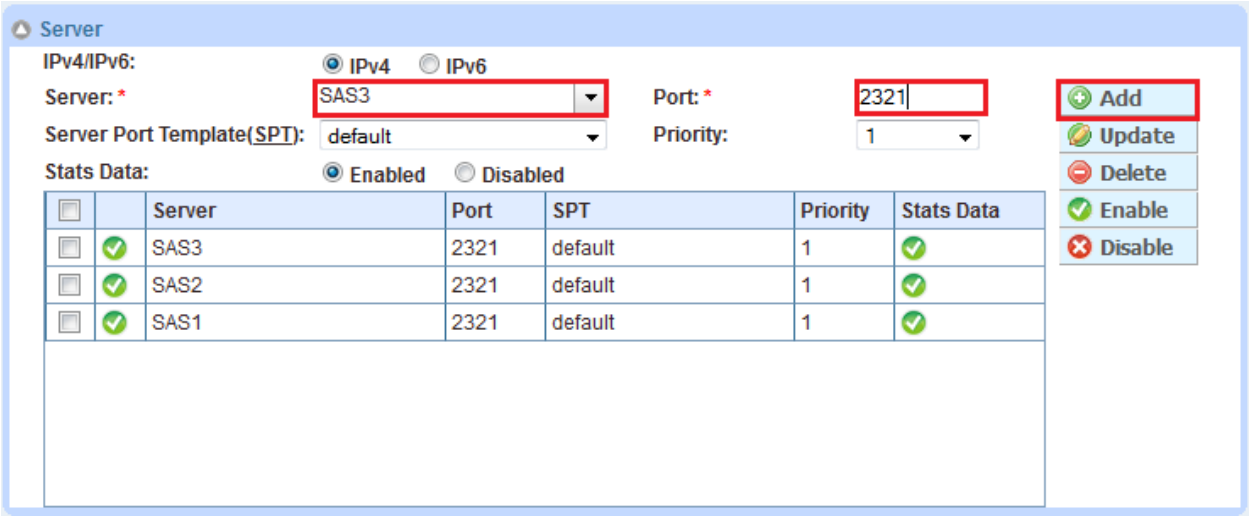

Figure 31: Service-group server configuration

5. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

10.6 VIRTUAL SERVER CONFIGURATION

This section demonstrates how to configure the VIP. Adding the virtual server ports within the AX Series will generate a virtual service list based on the protocol type selected.

1. Navigate to **Config Mode > Service > SLB > Virtual Server**.
2. Click **Add**.
3. Enter the following information:
   - **Name:** "SWSE-VIP"
   - **IP Address or CIDR Subnet:** 192.0.2.200

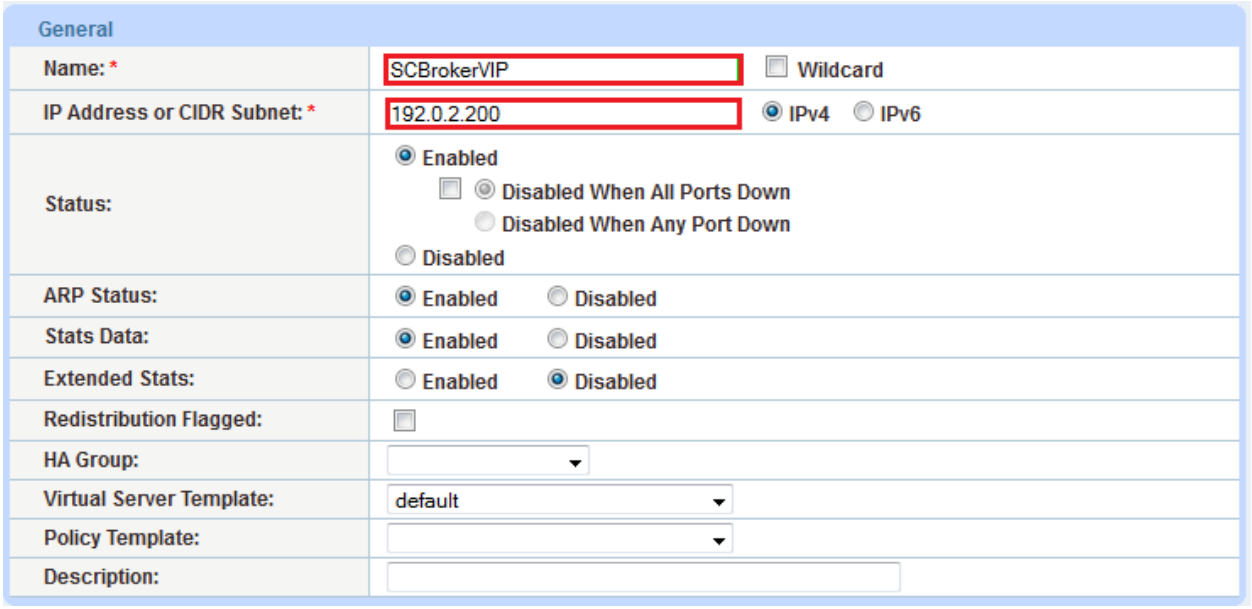

Figure 32: Virtual Server or VIP Configuration

4. In the **Port** section, click **Add**.
5. Enter the virtual server port information:
   - **Type:** "TCP"
   - **Port:** "2321"
   - **Service Group:** "SCBrokerGroup"
   - **Source NAT Pool:** "SNAT"

Figure 33: Virtual-server port configuration

6. In the **Port** section, click **Add**.
7. Enter the virtual server port information:
   - **Type:** "TCP"

- **Port:** "2321"
- **Service Group:** "SCBrokerGroup"
- **Source NAT Pool:** "SNAT"
- **Persistence Template Type:** "Source IP Persistence Template"
- **Source IP Persistence Template:** "Source IP Persistence"

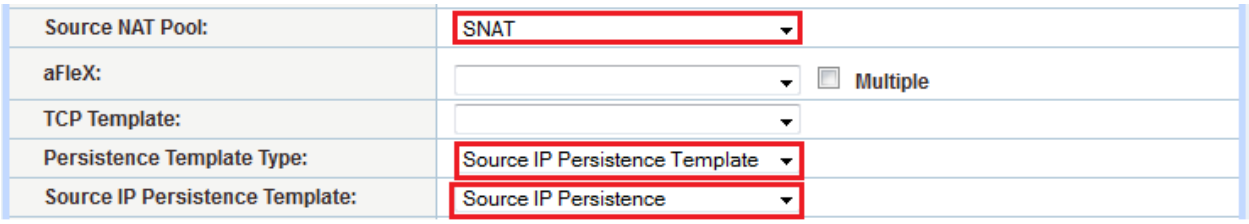

Figure 34: SNAT and source IP persistence templates

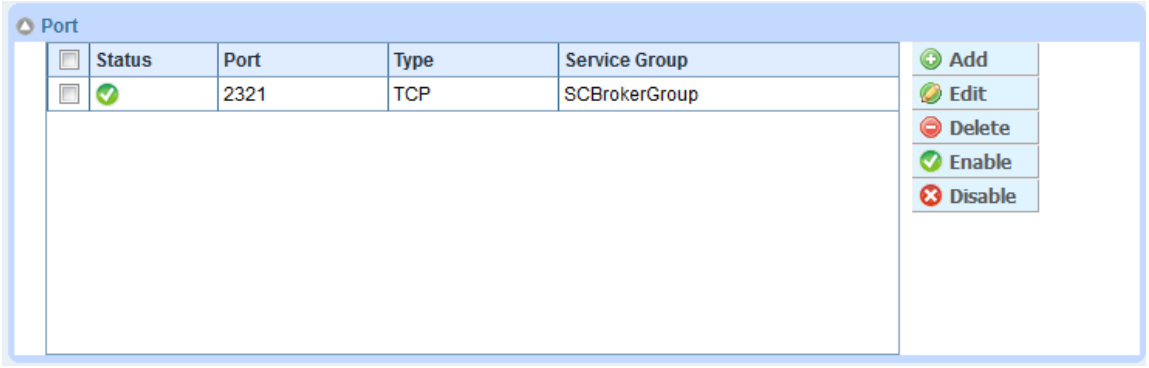

Figure 35: Virtual-port list

8. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

11 SUMMARY AND CONCLUSION

The configuration steps described above show how to set up the AX Series Application Delivery Controller for Oracle Siebel CRM Front-End and Back-End layer traffic. By using the AX Series device to load balance the Oracle Front-End layer Siebel Web Server Extension (SWSE) and the SCBroker Servers, the following key advantages are achieved:

- High availability for Oracle Siebel servers to prevent web and Siebel CRM application access failure, meaning there is no adverse impact on how users can access the applications
- Seamless distribution of client traffic across the SWSE and SCBroker servers for site scalability
- Higher connection throughput, faster end-user responsiveness, and reduced SWSE and SCBroker CPU utilization, by using SSL Offload and RAM Caching
- Improved site performance and reliability to end-users

By using the AX Series Advanced Traffic Manager, significant benefits are achieved for all Oracle Siebel users. For more information about AX Series products, please refer to the following URLs:

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

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

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

APPENDIX A. SAMPLE CLI CONFIGURATIONS

Front-End Layer Oracle Siebel CRM Configuration

```
ip nat pool SNAT 172.16.1.250 172.16.1.250 netmask /24

health monitor "Siebel HC"

slb server SWSE1 172.16.1.5
   port 80  tcp

slb server SWSE2 172.16.1.6
   port 80  tcp

slb server SWSE3 172.16.1.7
   port 80  tcp

slb service-group SWSEGROUP tcp
    method least-connection
    health-check "Siebel HC"
```

```
    member SWSE1:80
    member SWSE2:80
    member SWSE3:80

slb template client-ssl SWSE
   cert SWSE
   key SWSE

slb template persist source-ip "Source IP Persistence"

slb virtual-server SWSE-VIP 172.16.1.200

   port 443  https
      name _172.16.1.200_HTTPS_443
      source-nat pool SNAT
      service-group SWSEGROUP
      template client-ssl SWSE
      template persist source-ip "Source IP Persistence"
      aflex Redirect

   port 80  http
      name _172.16.1.200_HTTP_80
      source-nat pool SNAT
      service-group SWSEGROUP
      aflex Redirect

end
```

Back-End Layer Oracle Siebel CRM Configuration

```
ip nat pool SNAT 192.0.2.250 192.0.2.250 netmask /24

health monitor "SCBroker HC"
 method http url GET "/CRMEnt1/scbroker HTTP/1.0"

slb server SAS1 192.0.2.5
   health-check "SCBroker HC"
   port 2321  tcp
```

```
slb server SAS2 192.0.2.6
   health-check "SCBroker HC"
   port 2321  tcp

slb server SAS3 192.0.2.7
   health-check "SCBroker HC"
   port 2321  tcp

slb service-group SCBrokerGroup tcp
    method least-connection
    health-check "SCBroker HC"
    member SAS1:2321
    member SAS2:2321
    member SAS3:2321

slb template client-ssl SWSE
   cert SWSE
   key SWSE

slb template persist source-ip "Source IP Persistence"

slb virtual-server SCBrokerVIP 192.0.2.200
   port 2321  tcp
      name _192.0.2.200_TCP_2321
      source-nat pool SNAT
      service-group SCBrokerGroup
      template persist source-ip "Source IP Persistence"
end
```