Deployment Guide
May-2015 rev. a

APV Oracle PeopleSoft Enterprise 9 Deployment Guide

1 Introduction

This guide provides guidance on configuring the APV Series application delivery controllers for Oracle PeopleSoft Enterprise 9.

Oracle's PeopleSoft applications are designed to address the most complex business requirements. They provide comprehensive business and industry solutions, enabling organizations to increase productivity, accelerate business performance, and provide a lower cost of ownership.

Array Networks APV Series application delivery controllers provide the availability, scalability, performance, security and control essential to keeping Oracle’s PeopleSoft cloud services and enterprise application services running in their power band via server load balancing and global server load balancing.

2 Prerequisites and Assumptions

2.1 Oracle PeopleSoft Enterprise

This document is written with the assumption that you are familiar with Oracle PeopleSoft Enterprise server products. For more information on planning and deploying the Oracle PeopleSoft Enterprise server farm and Web applications, please reference the appropriate document at www.oracle.com.

- For this Deployment Guide, PeopleSoft must be running version 9 or 9.1. This deployment guide configures the APV solution for the PeopleSoft Web Tier.
- If you are using the APV Series to offload SSL or for SSL bridging, we assume you have already obtained the appropriate SSL certificate and key, and it is installed on the APV Series appliance.
- Follow the steps outlined in the Oracle Support Note '*How to Set up PeopleSoft and WebLogic when using a Load Balancer*':

  https://support.oracle.com/oip/faces/secure/km/DocumentDisplay.jspx?id=653998.1

  Be sure to:

  - Edit your PeopleTools Web Profile Configuration Virtual Address with your Virtual Server information.
  - Edit the CookieName parameter in the weblogic.xml file so it is the same for every Web server.
  - Configure the PIA "Inactivity Logout" so it matches the HTTP timeout setting.

2.2 Array Networks APV Series Application Delivery Controllers

The APV appliance must be running version **ArrayOS TM 8.x** or later. For more information on deploying the APV appliance, please refer to the ArrayOS™ Web UI Guide, which is accessible through the product's Web User Interface. We assume that the APV Series appliance is already installed in the network with Management IP, interface IP, VLANs and default gateway configured.

3 APV Series Application Delivery Controller (ADC) Benefits

The Array Networks APV Series delivers all required functions for optimizing application delivery for PeopleSoft Enterprise 9 enterprise environments, such as Layer 4 server load balancing, high availability, SSL acceleration and offloading, DDoS protection, TCP connection multiplexing, site proximity and failover – all in a single, easy-to-manage appliance.

Availability & Scalability

The APV Series' server load balancing ensures maximum uptimes for PeopleSoft Enterprise. Customers can scale their PeopleSoft Enterprise 9 environment to meet capacity and performance needs with APV Series server load balancers.

SSL Offloading and SSL Security

APV Series provides industry-leading performance and cost per SSL TPS for 2048-bit SSL with advanced client certificate handling for secure application support and easy application integration. SSL acceleration reduces the number of servers required for secure applications, improves server efficiency and dramatically improves application performance. Offloading compute-intensive key exchange and bulk encryption, and delivering industry-leading client-certificate performance, SSL acceleration is ideal for scaling PeopleSoft Enterprise environments.

Network and Server Protection

The APV appliance can protect PeopleSoft Enterprise from malicious network and server attacks like DDoS attacks, SYN floods, TCP port scans, UDP floods and UDP port scans, etc. The advanced rate limiting options can rate-limit connections per user, and advanced HTTP profiles can limit HTTP commands and parameters for Web applications.

Site Resilience

The APV Series' global server load balancing directs traffic away from failed data centers and intelligently distributes services between sites based on proximity, language, capacity, load and response times for maximum performance and availability.

TCP Connection Multiplexing

The APV appliance multiplexes several client TCP connections into fewer connections for the HTTP-based services. The APV appliance also reuses existing server connections to greatly reduce server load for TCP processing.

HTTP Dynamic Cache and Compression

The APV appliance supports dynamic HTTP caching and compression and can serve frequently requested content from the APV Series' cache, or force client-side caching, reducing the quantity of data transmitted for faster client response and reduced server load.

4 Configuration Scenarios

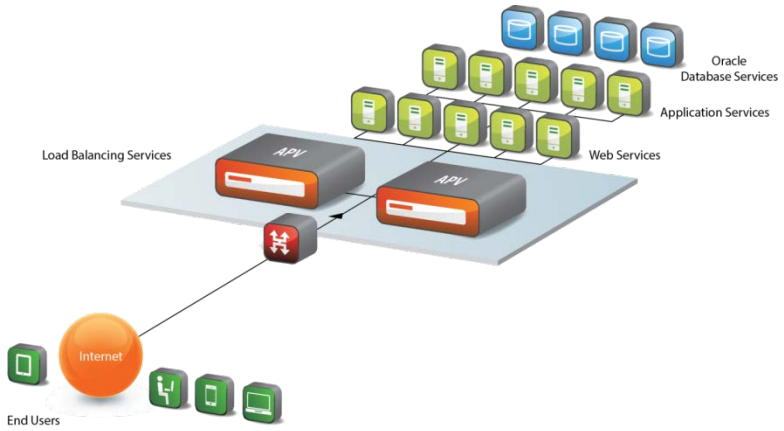


Figure 1: Typical Deployment

4.1 Deployment Considerations

Array Networks® APV Series provides three scenarios for PeopleSoft Enterprise 9 deployment.

1. Scenario 1: Normal Web Access (Internal User)
2. Scenario 2: Secured Web Access/SSL Offloading (External User)
3. Scenario 3: Secured Web Access/SSL Bridge

4.1.1 APV for Normal Access

This scenario is a basic PeopleSoft Enterprise Server deployment, which places the APV in the middle between users and the PeopleSoft Enterprise 9 Web servers for **internal users**. The APV Virtual Service and Real Service are both HTTP. As a reverse proxy, the APV provides additional security, high availability and scalability to the PeopleSoft Enterprise service.

Figure 2: APV Series for Internal Users

Application/ Service	Virtual Service		Real Service		Health Check
	Protocol	Port	Protocol	Port	
PeopleSoft Enterprise Web Tier	HTTP	80	HTTP	80	HTTP

Table 1: Settings for Internal Users

4.1.2 APV for Client Secured Access (SSL Offload)

In this scenario, the APV system is between the client and PeopleSoft Enterprise 9 Web servers, and the APV provides additional encrypted client access to the PeopleSoft Enterprise application services. The APV Virtual Service is HTTPS and Real Service is HTTP. The APV system provides secured access by high-performance SSL/TLS processing, with no extra load to the servers, and transparently to the **external users.**

Figure 3: APV Series for External Users

Application/ Service	Virtual Service		Real Service		Health Check
	Protocol	Port	Protocol	Port	
PeopleSoft Enterprise Web Tier	HTTPS	443	HTTP	80	HTTP

Table 2: Settings for External Users

4.1.3 APV for Client Secured Access and Servers (SSL Bridge)

In this scenario, the APV system is the same as before. External users can have either (or both) normal HTTP or secured HTTPS access. However, the PeopleSoft Enterprise Web tier servers' protocols are changed to secured HTTPS access. The APV system not only provides secured client access, but also secured access to the backend servers as required.

Figure 4: APV Series for SSL Bridge

Application/ Service	Virtual Service		Real Service		Health Check
	Protocol	Port	Protocol	Port	
PeopleSoft Enterprise Web Tier	HTTPS	443	HTTP	443	HTTPS

Table 3: Settings for External Users & Secured Communication to Server

5 Configuring APV for PeopleSoft Enterprise Services

5.1 Configuring APV for Internal Users

This section assumes internal users are using HTTP to access the PeopleSoft Enterprise Tier.

5.1.1 Create a PeopleSoft Enterprise Health Check

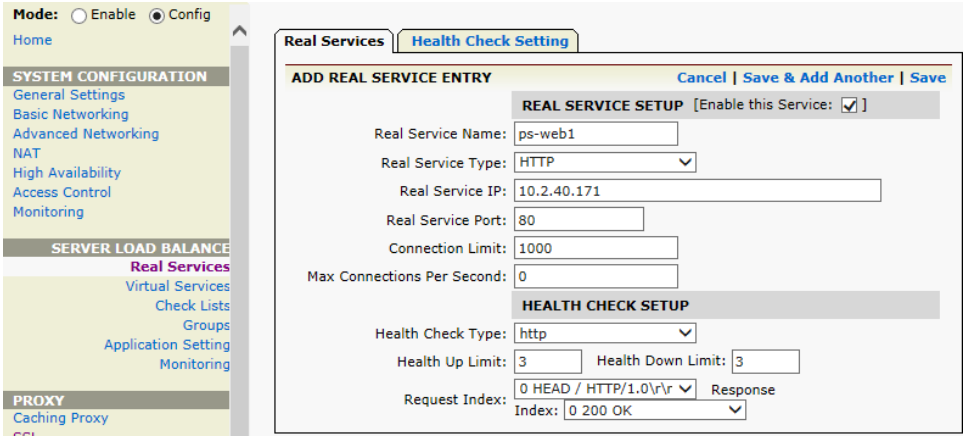
The APV Series' HTTP Health Check is highly customizable. The customer may define a special page for a more comprehensive application health check. For the deployment example, the APV's default HTTP–based, content-based health check can be used without additional setup or changes.

5.1.2 Create PeopleSoft Web Tier Real Service

Add two PeopleSoft Enterprise Web Tier servers in the Real Server Profile with associated health checks. Add each server with its name, IP/port and protocol information as an APV SLB Real Service using the following steps. Please ensure the server health check is up and green (in active status) after this configuration.

1. WebUI **Mode: Config.** From the sidebar, select **Real Services -> Real Services (tab) -> Add** to access the "**ADD REAL SERVICE ENTRY**" configuration page.

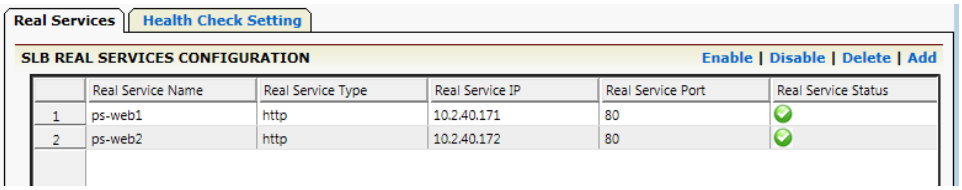
2. The "**ADD REAL SERVICE ENTRY**" screen is for you to configure real servers. In our example, we entered "**ps-web1**" as the Real Service Name. Select "**HTTP**" as the **Real Service Type**, enter IP addresses "**10.2.40.171**" and port "**80**" which is used by the PeopleSoft Enterprise Web Tier Server.



3. Select **http** as the Health Check Type for the default real service health check. Click **Save & Add Another** to add more real services.

4. Follow the same steps as above: add "**ps-web2**" server as a real service. We used IP address 10.2.40.172 for this example.

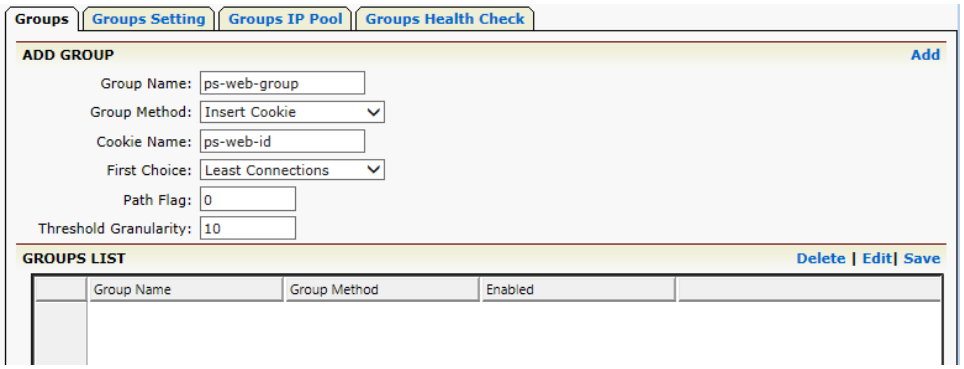
Once the Real Services are added, the newly created Real Services will be displayed in the **SLB REAL SERVICES CONFIGURATION** page**.**



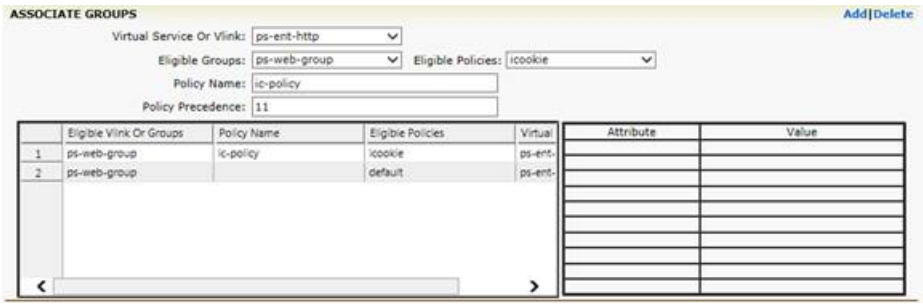
5.1.3 Create a Service Group

From WebUI, **Mode: Config**, to add a new SLB Group,

1. Select **"Groups"** from the sidebar. The **ADD GROUP** configuration window will display.
2. Input a unique name for the Group Name; in the example we used "**ps-web-group"**. Select the **"Insert Cookie"** group method by selecting from the pull down menu. Give a unique cookie name. Select the **"Least Connection"** group method by selecting from the pull-down menu. After making configurations on those parameter fields, click on the action link **"Add"** to create the SLB group.

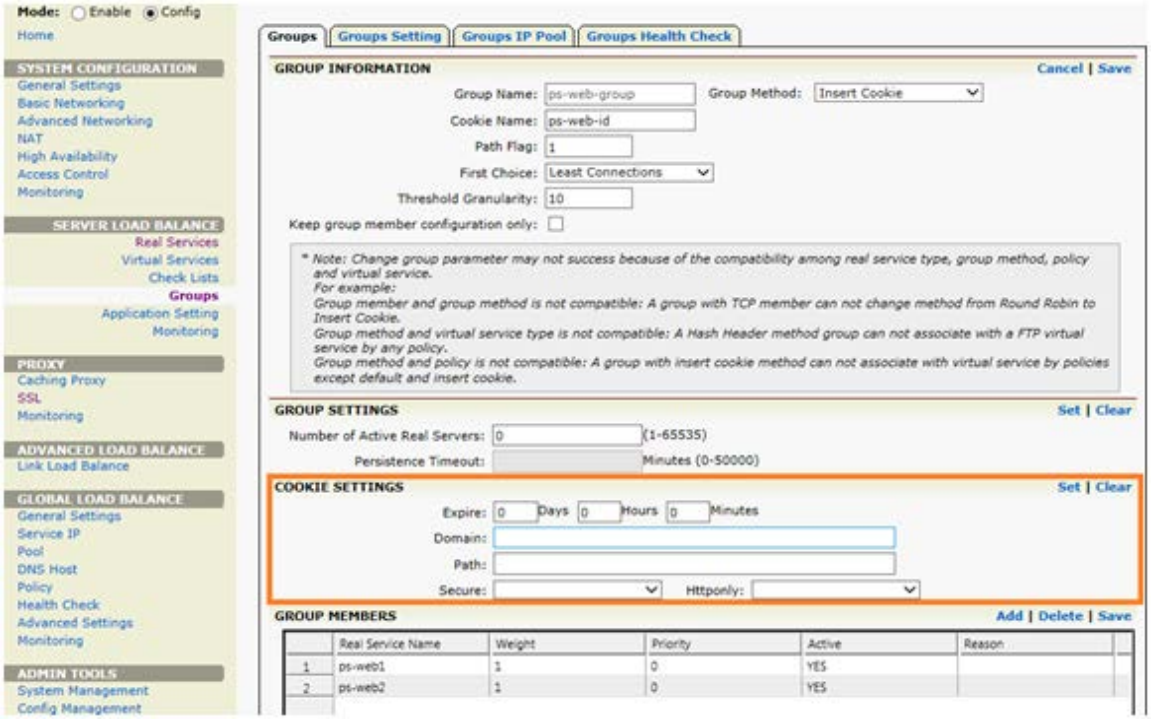


All configured SLB Groups are displayed in the **GROUPS LIST**.



3. To assign PeopleSoft Enterprise Web Tier Servers to the SLB group: Choose "**ps-web-group**" in the **GROUPS LIST** by double clicking on it, or select and click on the action link **"Edit"**. The **GROUP INFORMATION** configuration page will be displayed.
4. Under the "**GROUP MEMBERS**" section, click on "**Add**", and the **ADD GROUP MEMBER** configuration screen will show. Assign real services "**ps-web1**" and "**ps-web2**" to the group and "**Save**"**.** The **GROUPS LIST** will list all Group Members.

Depending on the PeopleSoft Application requirement for cookies, additional cookie parameters can be added. See **COOKIE SETTINGS.**

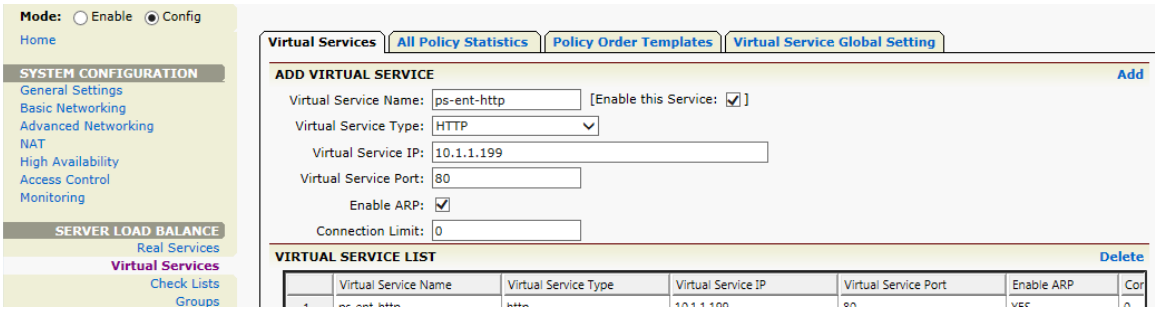


5.1.4 Create a Virtual Service

The next step is to create a PeopleSoft Enterprise Virtual Service for the external client to access. On the APV appliance, the IP/Port and the protocol define a Virtual Service. External client requests will be terminated on it and the APV will proxy the request to the designated SLB Group. Based on the SLB Group method, the APV will load balance the requests to the selected PeopleSoft Enterprise Web Tier Server.

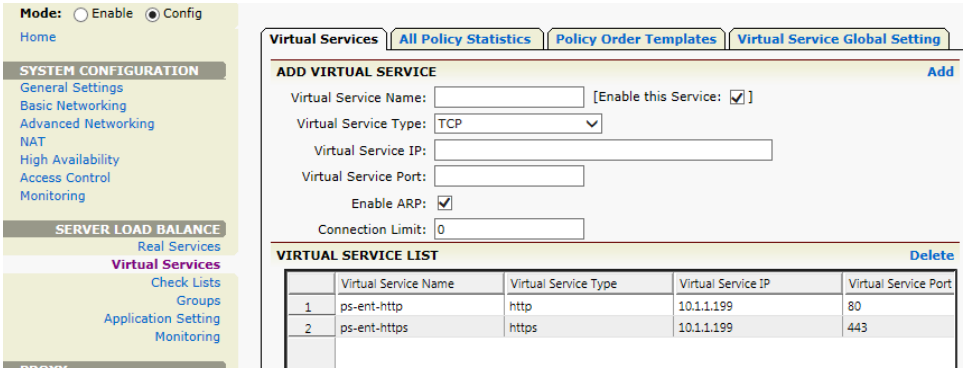
From WebUI, **Mode: Config**, to add a new SLB Virtual Service,

1. Select **“Virtual Services”** from the sidebar. The **ADD VIRTUAL SERVICE** configuration page will display.
2. Enter a unique name (**ps-ent-http**) for the Virtual Service Name. Use the check box to enable the virtual service. Select the virtual service type “**HTTP**” from the selector. Set the virtual service IP and port 80. Use the check box to enable ARP. Set the maximum number of open connections per virtual service. “0” means unlimited. Depending on which type of virtual service is specified, certain parameter fields will appear, change or disappear. Click “**Add**” to create the new SLB Virtual Service.



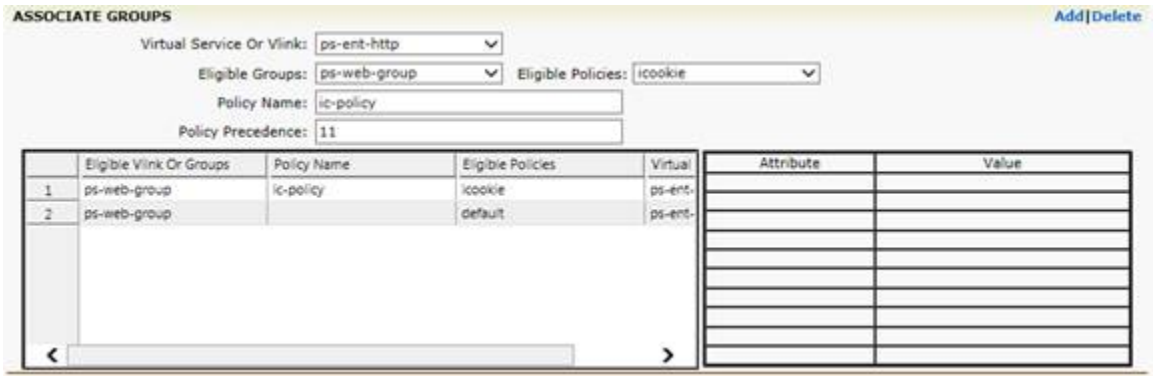
All available virtual services will be displayed under the **VIRTUAL SERVICE LIST**. From the list we can select the Virtual Service for additional setup, such as defining a SLB Group to be associated by the SLB “default” Policy. Following are the configuration steps:

1. From WebUI **Mode: Config**, select **Virtual Services** from sidebar. Double click the SLB Group (ps-ent-http) from the **GROUPS LIST**.



2. Go down to the **ASSOCIATE GROUPS** section, select **ps-web-group** from Eligible Groups, select “**default**” from Eligible Policies. Click **Add**.

3. Under the same **ASSOCIATE GROUPS** section, for the same **ps-web-group**, select “**icookie”** from Eligible Policies. Enter a unique name for the Policy Name and a priority for Policy Precedence. Click **Add**.

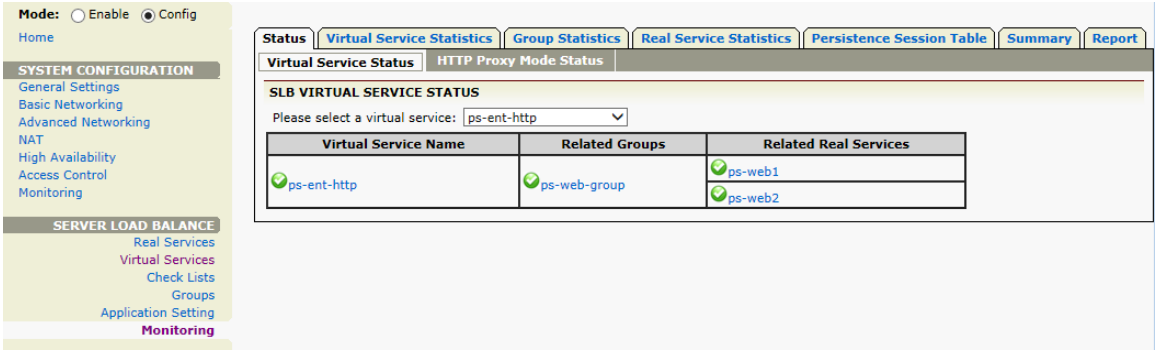


Note: The APV Series' SLB capability supports various virtual service settings. If you would like to use settings beyond those discussed in this deployment guide, consult Array Support services.

5.1.4 Validate the PeopleSoft Enterprise Service Configuration

Validate that the basic configuration is functioning correctly:

1. From WebUI, **SERVER LOAD BALANCE**, **Monitoring** -> **Status** -> **Virtual Service Status**. Select "**ps-ent-http**" as the virtual service.
2. Verify that the SSL offloading configuration is operating as intended. It should be HTTP for the Virtual Service and HTTP for the Real Service.
3. Verify that all "**Service Status**" icons are green.



5.2 Configuring APV Series for External Users

This section guides you in configuring the APV device to load balance PeopleSoft Enterprise in HTTPS (SSL offload) for secured communication with external users.

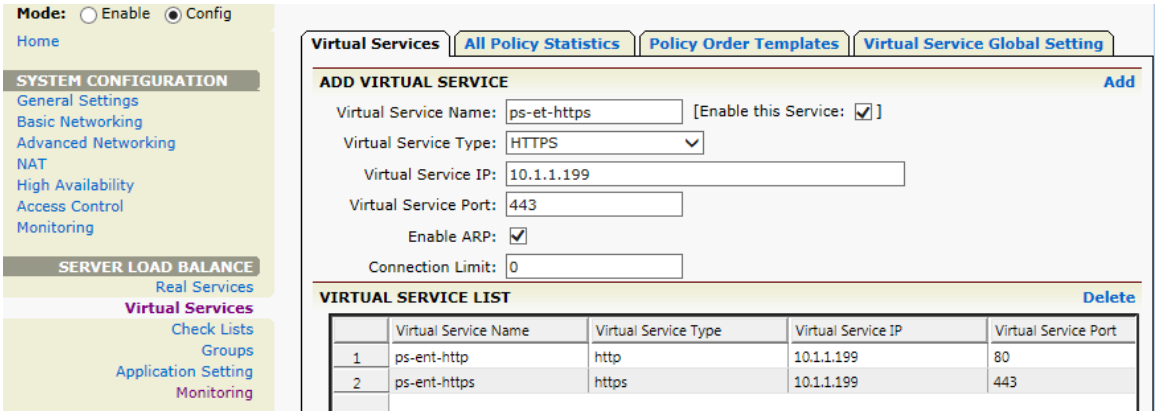
To configure the APV device to load balance PeopleSoft Enterprise HTTPS service, we can use the same Real Service we created in 5.1.2 and service group in 5.1.3. We need only add a new APV Virtual Service with HTTPS, associate an SSL Virtual Host and set the default policy to route the requests to the PeopleSoft Enterprise Web Servers group.

5.2.1 Create PeopleSoft Enterprise HTTPS Virtual Service (SSL Offload)

To create the PeopleSoft Enterprise HTTPS Virtual Service from WebUI **Mode: Config:**

1. Select **Virtual Services** from the WebUI sidebar, input a unique SLB Virtual Service Name (**ps-ent-https** in the example), and select **HTTPS** as the Virtual Service Type. Enter the IP address and port (443) used by the Virtual Service. The IP address can be the PeopleSoft Enterprise service DNS external IP. Click **Add** to create the new PeopleSoft Enterprise HTTPS Virtual Service.

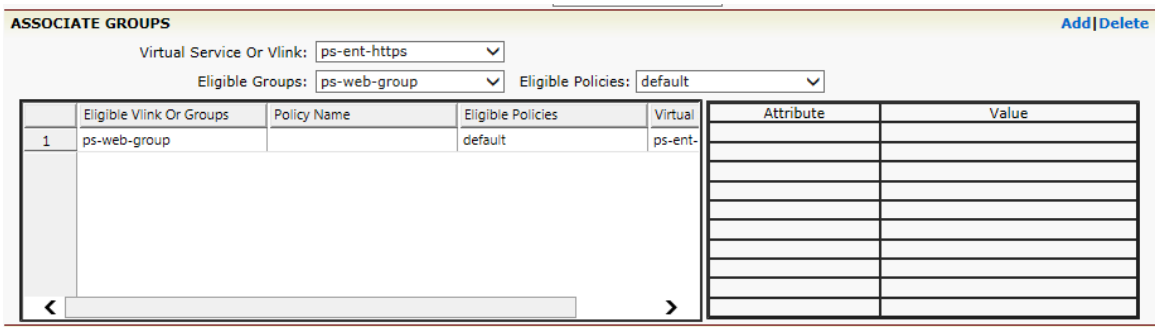
   The **VIRTUAL SERVICE LIST** displays all available Virtual Services.



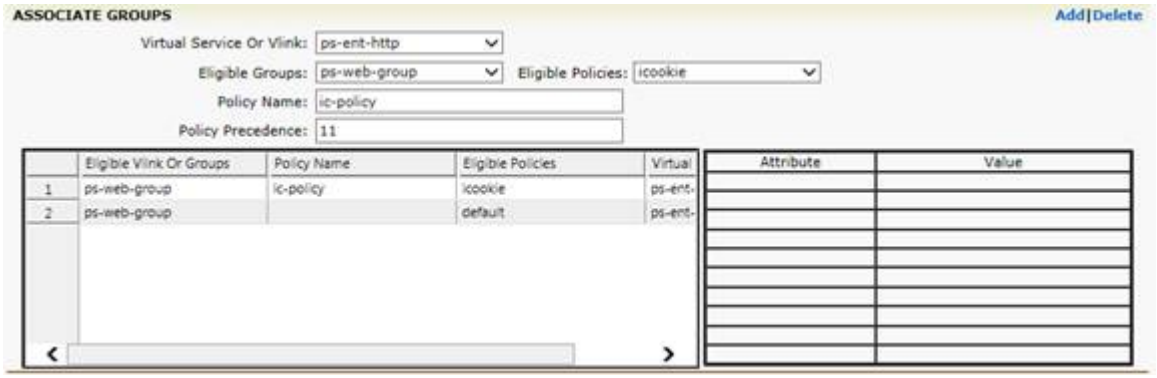
The next step is to associate the SLB Virtual Service with the PeopleSoft Enterprise Web Server Group. Following are the steps:

1. Choose "**ps-ent-https**" in the **VIRTUAL SERVICE LIST** by double clicking on it, or select it and click on the action link "**Edit**". The **VIRTUAL SERVICE INFORMATION** configuration page for the Virtual Service will be displayed.

2. To associate the PeopleSoft Enterprise Web Server Group, go down to the **ASSOCIATE GROUPS;** select the PeopleSoft Enterprise Web Server Group (**ps-web-group**) from Eligible Groups. Also, select "**default**" for Eligible Policies. Click **Add** to complete the association.



3. Under the same **ASSOCIATE GROUPS** section, the same **ps-web-group**, select "**icookie"** from Eligible Policies. Enter a unique name for the Policy Name and a priority for Policy Precedence. Click **Add**.



To enable the SLB HTTPS/TCPS/FTPS Virtual Service on the APV Series, an SSL Certificate/Private Key needs to be associated to the SLB Virtual Service. To do so, the APV Series needs to associate an SSL Virtual Host to the SLB Virtual Service. Each SSL Virtual Host needs to have its own SSL Certificate and Private Key assigned.

Note: One SSL Virtual Host can associate multiple SLB Virtual Services, HTTPS, TCPS and FTPS.

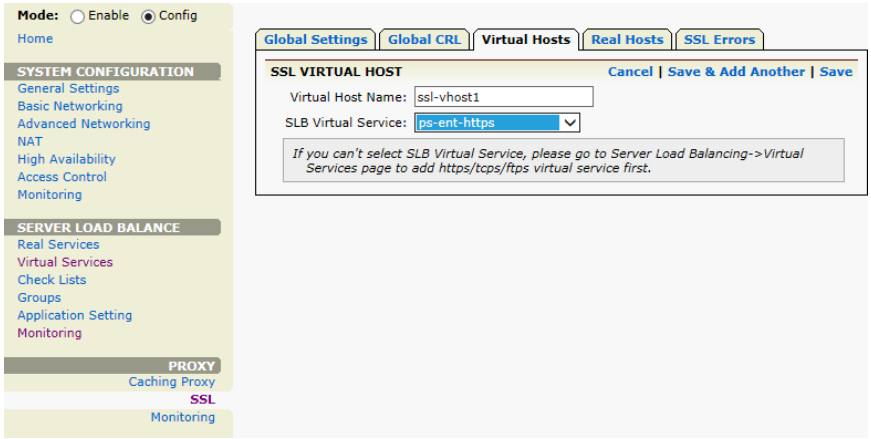
5.2.2 Create SSL Virtual Hosts

Once the HTTPS SLB Virtual Service is configured, we need to set up SSL for the SLB Virtual Service. On the APV Series, SSL setup includes creating an SSL Virtual Host to hold SSL-related information, assigning a Certificate/Private Key, and enabling it. Additional SSL/TLS protocol/cipher options and error handling can be configured through advanced settings.

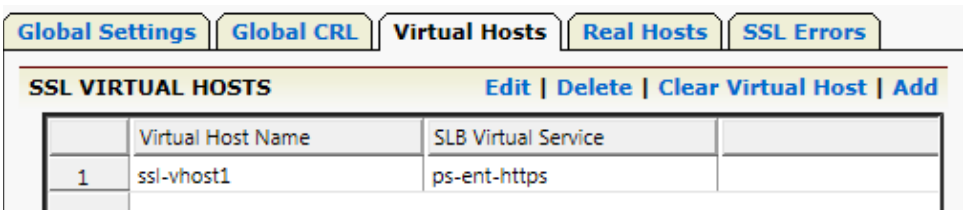
SSL Virtual Host is the SSL engine used to process traffic with the associated certificate and private key. The SSL Virtual Host can associate multiple SLB Virtual Services and different application types which need SSL support, such as HTTPS, FTPS or TCPS.

To create an SSL Virtual Host, from WebUI, Mode**: Config**:

1. Navigate to **SSL** -> **Virtual Hosts**, click "**Add**" to access the **SSL VIRTUAL HOST** menu.
2. Under the **SSL VIRTUAL HOST** menu, enter:
   - **Virtual Host Name**: enter **ssl-vhost1** as in the following example
   - **SLB Virtual Service:** select "**ps-ent-https**".
3. Click "**Save**" to store the information.



The newly created SSL Virtual Host should appear in the SSL Virtual Host name list.



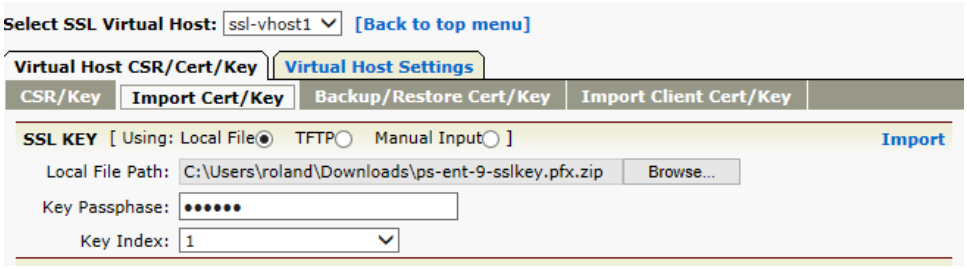
SSL Virtual Host acts as an SSL Server, which requires a Certificate/Private Key to operate. There are two options to assign a Certificate/Private Key:

1. Import the SSL Certificate/Private Key.
2. Optional - Generate a Certificate Signing Request (CSR), along with a self-signed certificate and private key. Send the CSR/Certificate to a public Certificate Authority (CA) to sign off. Then import the signed certificate to the APV Series appliance later.

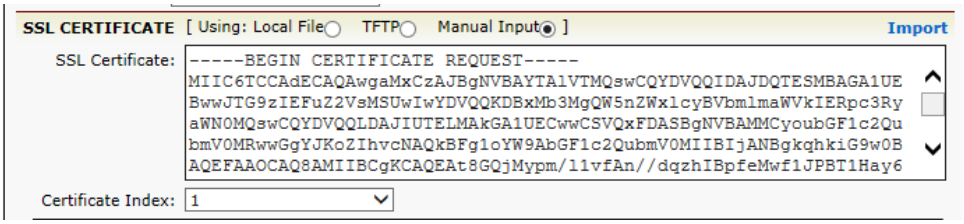
5.2.3 Import a SSL Certificate and (or) Private Key

To import an SSL key and certificate for an SSL Virtual Host, go to the WebUI **Mode: Config**.

1. Navigate to **SSL** -> **Virtual Hosts** and double click the SSL Virtual Host **ssl-vhost1** for which you would like to import a Certificate and/or Key.
2. Click the **"Import Cert/Key"** tab.
3. In **SSL KEY**, the key can be imported through **Local File**, **TFTP**, or **Manual Input**. The following example is using a local disk file "tcps-101.pfx" which is password protected.



4. In **SSL CERTIFICATE**, Local File, TFTP or Manual Input can import a certificate. The following example is using **Manual Input** (cut and paste) of the certificate text in PEM format.

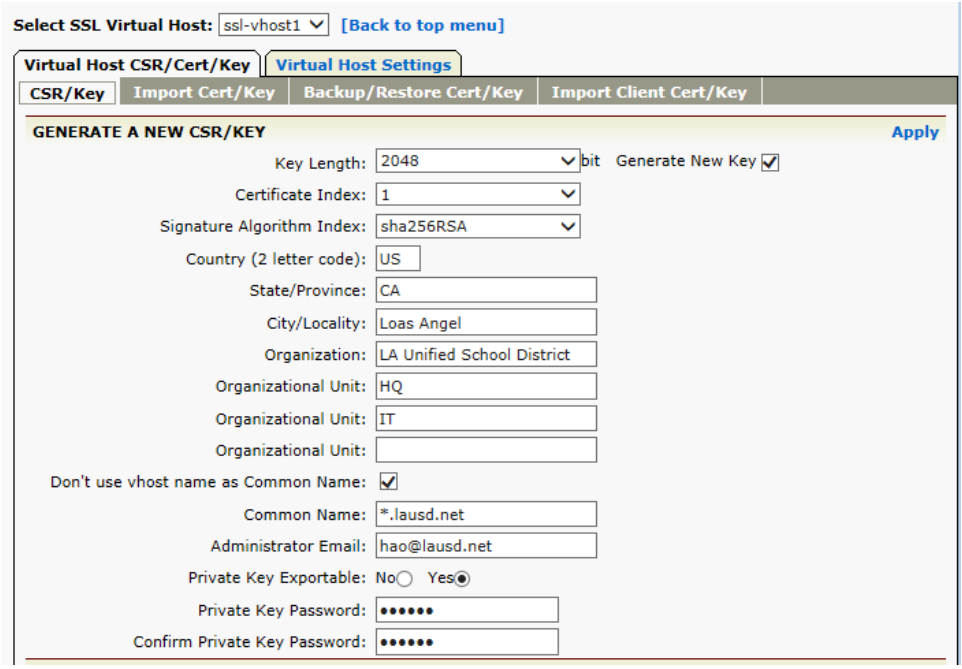


5.2.4 (Optional) Generate a CSR and Self-Signed Certificate

To generate the CSR, go to the WebUI **Mode: Config**.

1. Navigate to **SSL** -> **Virtual Hosts**; double click the SSL Virtual Host **ssl-vhost1** you just created.

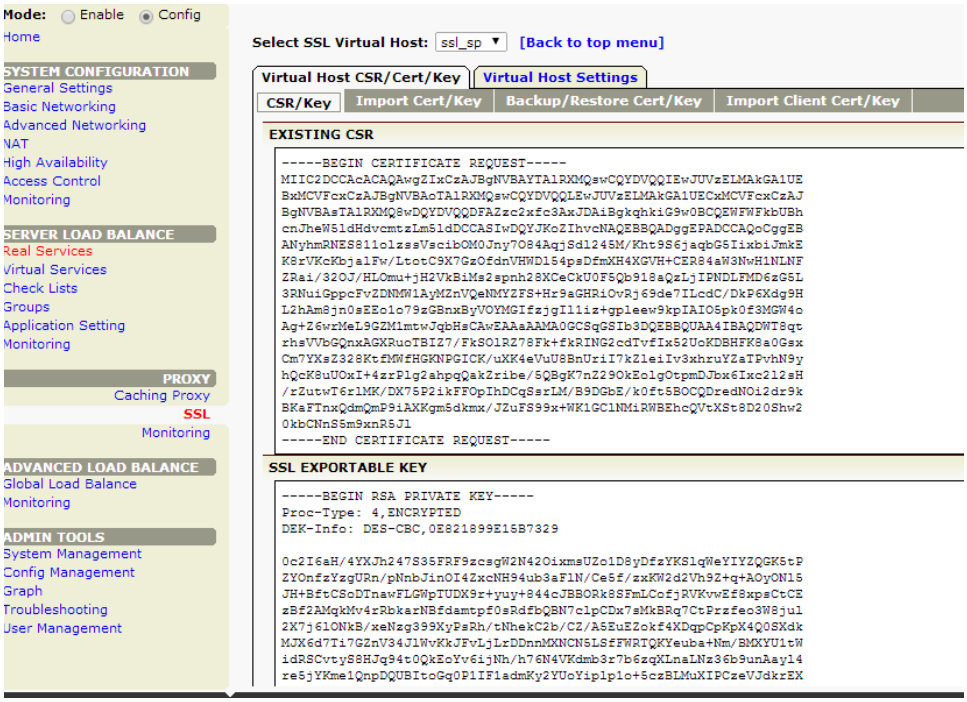
2. Under **Virtual Host CSR/Cert/Key** -> **CSR/Key** menu, fill in the information and click "**Apply**".



Note: The Common Name needs to be the same as the host name (resolved by DNS) to access the SLB Virtual Service.

Note: For an SSL Virtual Host with an existing Certificate/Private Key associated, the APV Series will show the EXISTING CSR and SSL EXPORTABLE KEY. You may remove the existing CSR (and Private Key) and re-generate a new CSR/Self-Signed Certificate.

Once you click **Apply**, a new CSR will be generated, along with the Private Key and Self-Signed Certificate for the SSL Virtual Host. All are available in PEM form, which allows cut and paste to export.

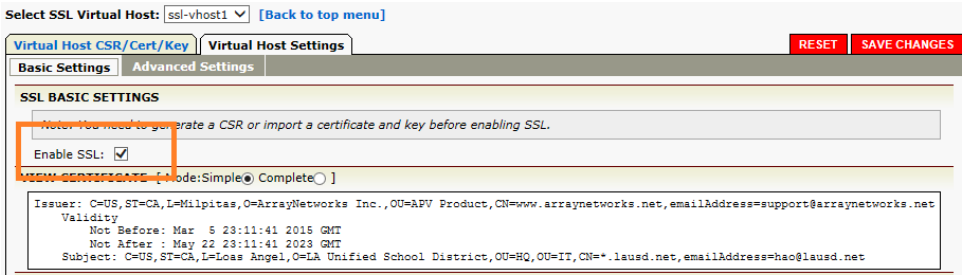


Note: You can cut and paste the CSR text (in PEM format, as shown) and email it to a CA, such as Symantec, Comodo SSL, or GoDaddy, and pay the fee to have it sign off the certificate. Before you have the official SSL certificate, a self-signed SSL certificate is generated with the private key by the APV Series and can be used for testing. But as the issuer (CA) is not known to the client, a security warning will be shown.

5.2.5 Enable SSL Virtual Host

Once the certificate and private key are assigned to the SSL Virtual Host, you can enable it to process SSL traffic. To enable it, go to the WebUI **Mode: Config.**

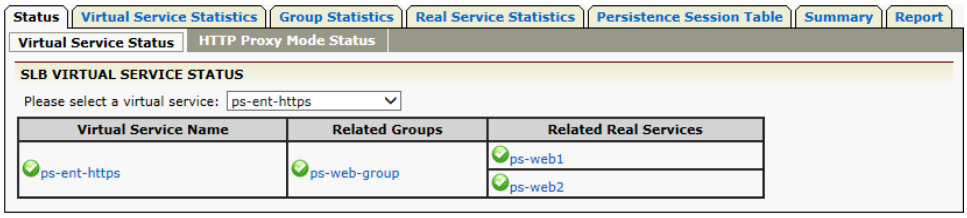
1. Navigate to **SSL** -> **Virtual Hosts** and double click on the SSL Virtual Host **ssl-vhost1**, for which you would like to start run SSL.
2. Select the **Virtual Host Settings** tab and check the **Enable SSL** box.
3. Click **SAVE CHANGES**



5.2.6 Validate the PeopleSoft Enterprise Service Configuration

Validate that the basic configuration is functioning correctly:

1. From WebUI, **SERVER LOAD BALANCE**, **Monitoring** -> **Status** -> **Virtual Service Status**, select "**ps-ent-http**" as the virtual service.
2. Verify that the SSL offloading configuration is operating as intended. HTTPS for the Virtual Service and HTTP for the Real Service.
3. Verify that all "**Service Status**" icons are green.



5.3 Configuring APV PeopleSoft Enterprise Service for SSL Bridge

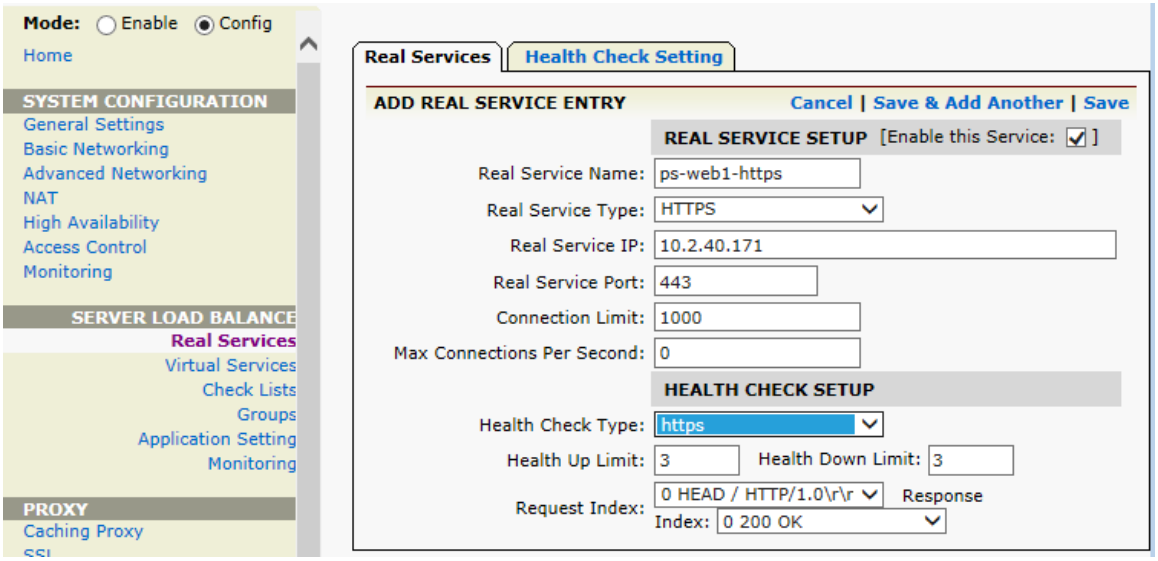
For SSL Bridge mode, the SLB Virtual Service is HTTPS and the PeopleSoft Enterprise Servers (SLB Real Services) are HTTPS as well.

To do so, we need to configure the PeopleSoft Enterprise Servers with HTTPS. Enable SSL Real Host to make the APV act as an SSL client to communicate with PeopleSoft Enterprise Servers.

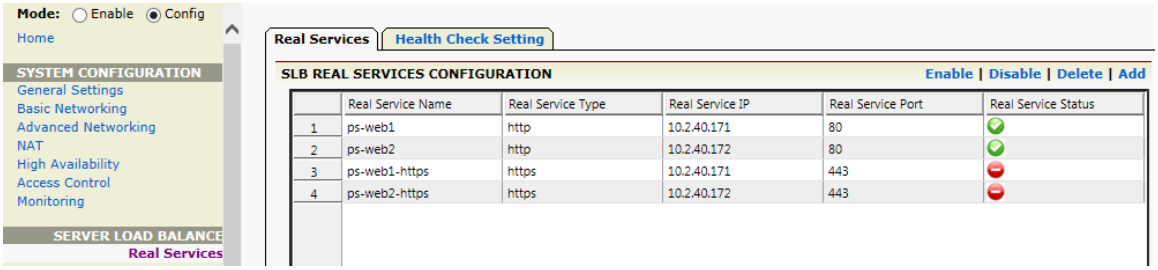
5.3.1 Create PeopleSoft Enterprise Web Tier HTTPS Service

From WebUI, set Mode: Config.

1. Navigate to **Real Services** -> **Add**; the **ADD REAL SERVICE ENTRY** configuration page will appear. Enter a unique name for the Real Service Name (**ps-web1-https**); select HTTPS for the Real Service Type. Enter the IP and Port used by the PeopleSoft Enterprise Server(s). Select HTTPS for the Health Check Type. Click **Save & Add Another** until all are added, then click **Save.**



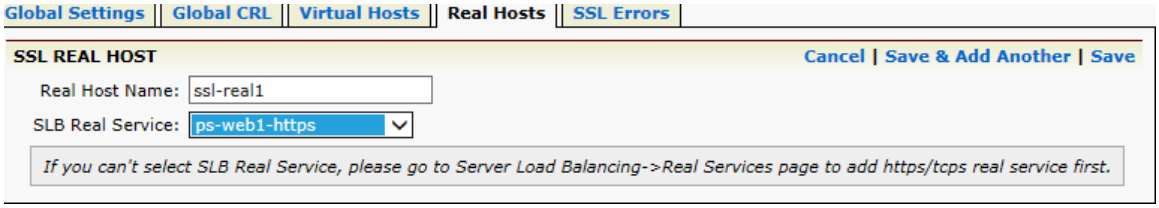
2. Follow the same steps as above and add "**ps-web2-https**" server as a real service. The IP address in the example is 10.2.40.172.
3. Once added, all Real Services should appear in the **SLB REAL SERVICE CONFIGURATION** list.



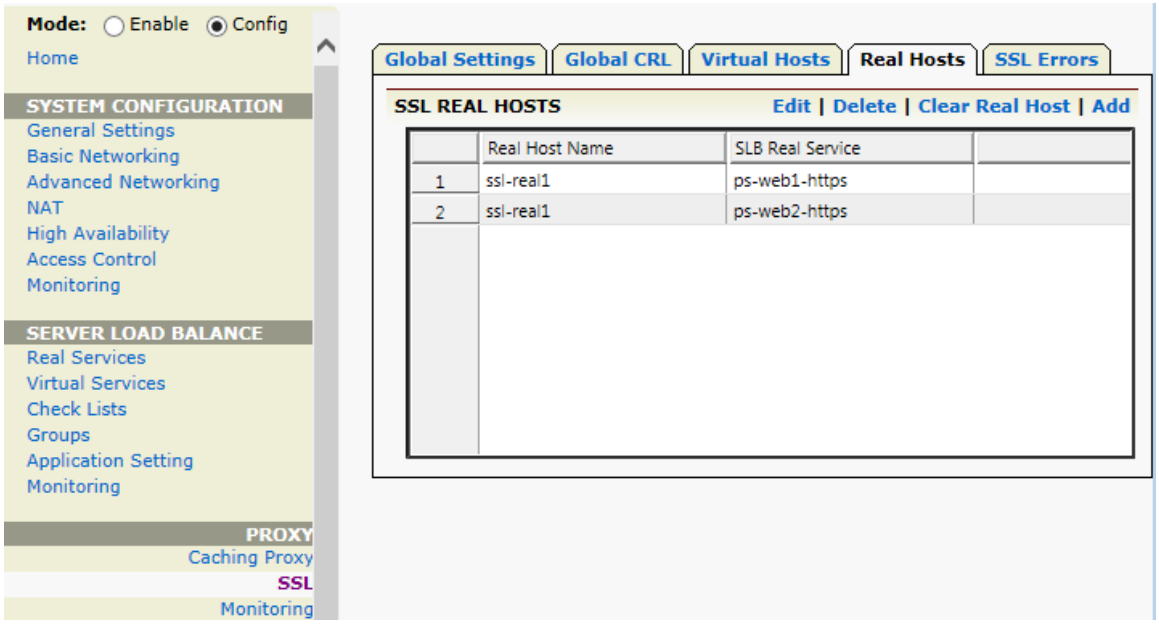
SLB REAL HOSTS displays all available SLB Real Hosts that are configured on the APV and their associated SLB Real Service (the PeopleSoft Enterprise Web Server with HTTPS/443 interface). In the WebUI above, it shows the two servers with HTTPS interface are status=down (RED, did not pass health check). This is because the SSL communication has not been configured yet. We need to configure SSL Real Hosts for them.

5.3.2 Create SSL Real Hosts (SSL Inside)

1. Navigate to **SSL** -> **Real Hosts** -> **Add**. On the **SSL REAL HOST** configuration page, enter a unique name for the Real Host Name (i.e. **ssl-real1**). Select the PeopleSoft Enterprise real service(s) from the pull down of SLB Real Service. Click **Save & Add Another** to enter additional Real Hosts, and click **Save** after last SLB Real Host has been added.

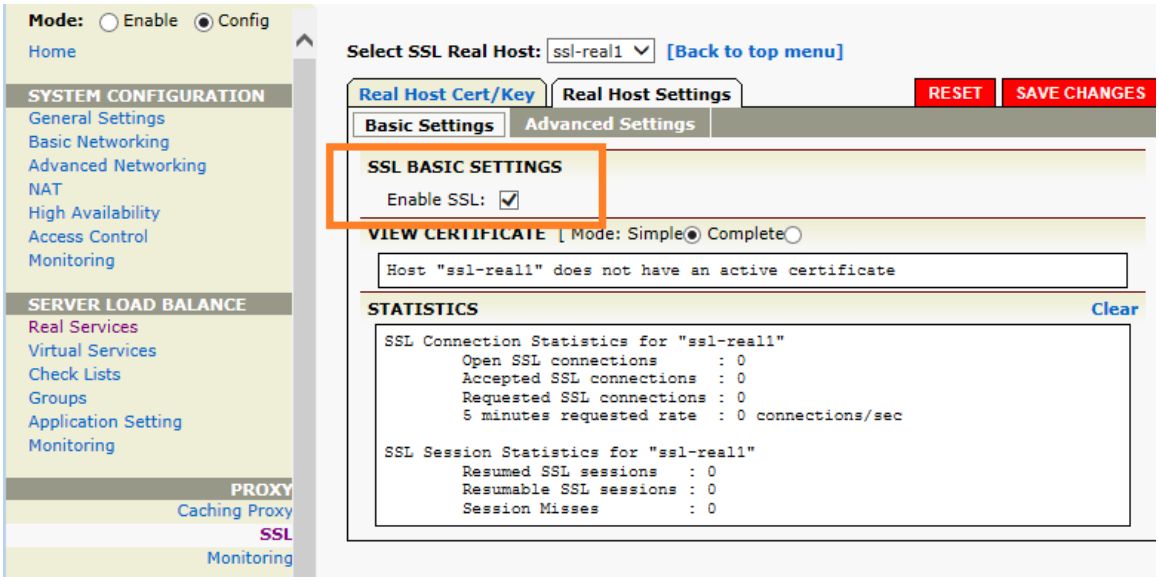


2. **SSL REAL HOSTS** displays all available SSL Real Hosts that are configured on the APV and their associated SLB Real Service (the PeopleSoft Enterprise Web Server with HTTPS/443 interface).



5.3.3 Enable SSL Real Host

1. Under WebUI, enter **Mode: Config**. Navigate to **SSL** -> **Real Hosts**, and under the **SSL REAL HOSTS** double click the SSL Real Host to select it. Then click **Real Host Settings.** Under the **Basic Settings** tab, **SSL BASIC SETTINGS** section, check the **Enable SSL box,** then "**SAVE CHANGES**" to enable the SSL real host to process SSL traffic with backend servers.



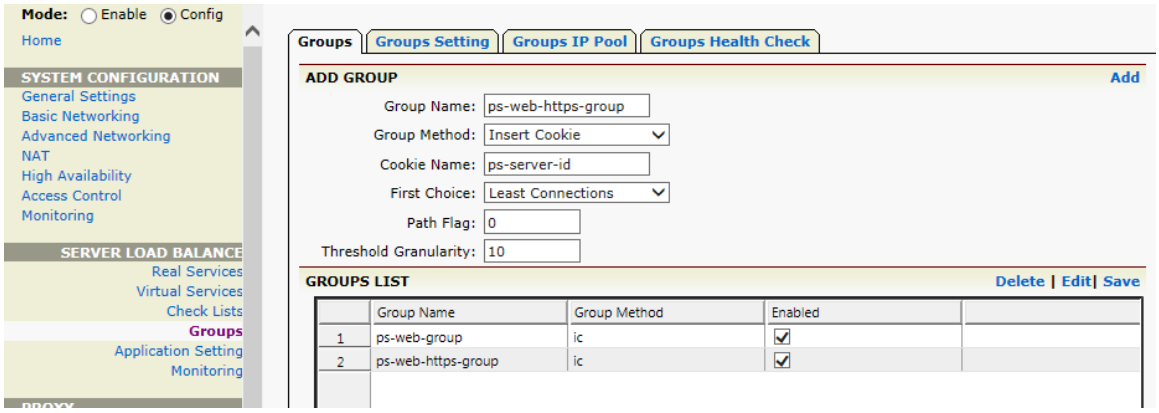
The same SSL Real Host can be associated with multiple backend servers. If backend servers have different SSL requirements, different SSL Real Hosts can be configured for those different needs. Or you can modify the SSL Real Host through advanced setup. For example, if the backend SSL server does not allow SSLv3 access, the APV SSL Real Host used by HTTPS Health Check needs to be configured to be compatible. Or, if the certificate used by the backend SSL server is not valid, then the server certificate check on the APV needs to be turned off. See **SSL** -> **Global Settings**; **Enable Server Certificate Verification.**

- The APV SSL Real Host simulates an SSL/TLS client, thus the SSL Certificate/Private key is not required.

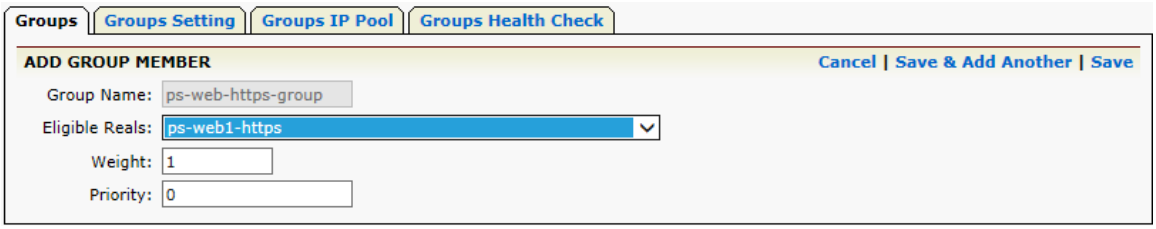
5.3.4 Create HTTPS SLB Group

To add and configure an SLB Group, from WebUI, **Mode: Config:**

1. Select **Groups** from the side bar to access the **ADD GROUP** configuration page. Input a unique name for the Group Name; in the example we've used "**ps-server-https-group"**. Select the **"Insert Cookie"** group method by selecting from the pull down menu. Give a unique cookie name. Select the **"Least Connections"** group method by selecting from the pull down menu. After making configurations on those parameter fields, click on the action link **"Add"** to create the SLB group. The newly created SLB Group will display on the **GROUPS LIST**.



2. To assign PeopleSoft Enterprise Servers (HTTPS) to the SLB Group, choose ”**ps-web-https-group**” from the **GROUPS LIST** by double clicking on it, or select and click on the action link **“Edit”**. The **GROUP INFORMATION** configuration page will display. Go to the **GROUP MEMBERS** section, and click **Add** to access the **ADD GROUP MEMBER** configuration page. Select the PeopleSoft Enterprise Servers HTTPS real services one by one to add to the group.

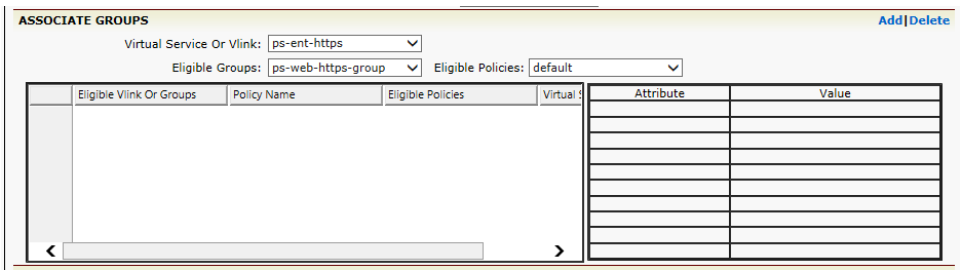


5.3.5 Create an HTTPS Virtual Host

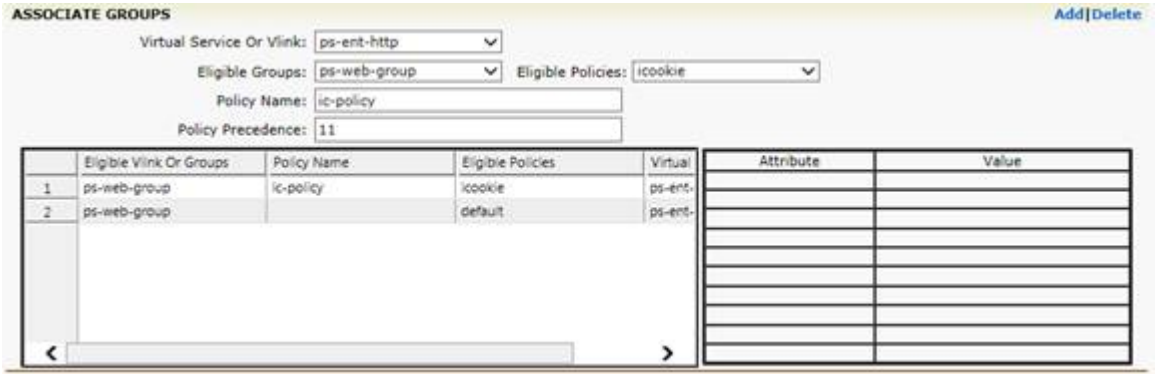
For SSL Bridge mode, the APV system uses an HTTPS interface for both the Virtual Services and Real Services. The same HTTPS SLB Virtual Service “**ps-ent-https**”, created in section 5.2.2, is modified to associate with the “**ps-web-https-group**” SLB Group in the following example.

To reuse “**ps-ent-https**” with a different SLB Group, from WebUI, enter **Mode: Config**.

1. Select **Virtual Services** from sidebar, and double click “**ps-ent-https**” to select it.
2. Go down to the **ASSOCIATE GROUPS** section; click the existing associated group with default policy. Click **Delete** to remove it (with confirmation).
3. Then select “**ps-web-https-group**” as the Eligible Group and “**default**” from the Eligible Policies dropdown. Click **Add** to finish.



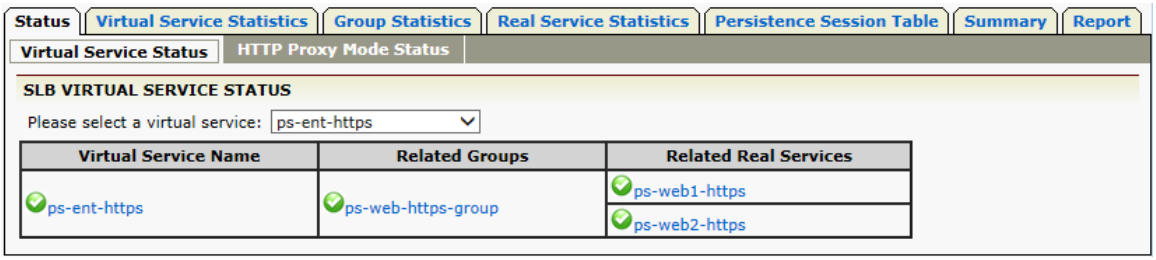
4. Under the same **ASSOCIATE GROUPS** section, and the same **ps-web-https-group**, select "**icookie"** from Eligible Policies. Enter a unique name for the Policy Name and a priority for Policy Precedence. Click **Add**.



5.3.6 Validate the PeopeSoft Enterprise Service Configuration (SSL Bridge)

Validate that the basic configuration is functioning correctly:

1. From WebUI, **SERVER LOAD BALANCE**, **Monitoring** -> **Status** -> **Virtual Service Status**: Select "**ps-ent-https**" as the virtual service.
2. Verify that the SSL Inside configuration is as intended: HTTPS for the Virtual Service and HTTPS for the Real Services.
3. Verify that all "**Service Status**" icons are green



6 Optional Configuration

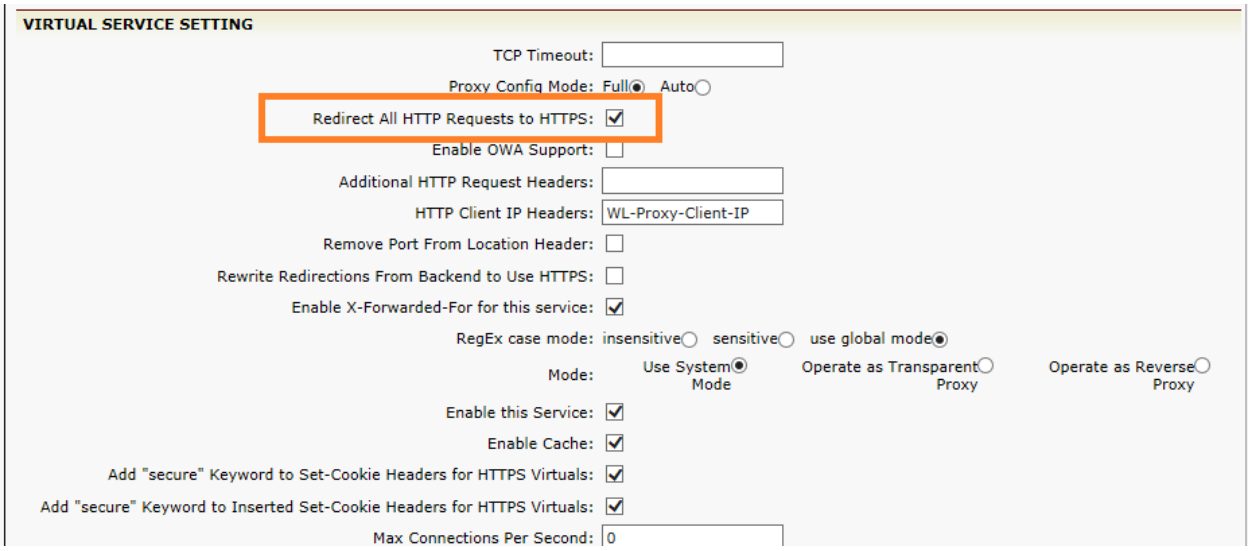
6.1 HTTP to HTTPS Rewrite/Redirect

A user may accidentally type "http://..." (unsecured) instead of https://... (secured), or type just the domain name to access a secured PeopleSoft Enterprise Virtual Service, which would normally cause the PeopleSoft Enterprise client to wait until timeout without serving any content. To make this more user friendly, the APV appliance can be configured to automatically redirect http requests to https.

6.1.1 HTTP Redirect Configuration Steps

To configure the HTTP to HTTPS redirection: From WebUI, **Mode: Config:**

1. Select **Virtual Services** from sidebar; double click the "**ps-ent-http**" Virtual Service to select it.
2. Check the box for "**Redirect All HTTP Requests to HTTPS**"
3. Click **SAVE CHANGE**



6.2 Pass Actual Client IP to PeopleSoft's PIA_access.log

APV can run in Proxy Mode (using the APV's IP to connect to server) or Transparent Mode (using the client's IP to connect to server). In Proxy Mode, the server will not see the actual client IP. Typically, an X-Forwarded-For header is used to carry the client IP to the backend server. However, PeopleSoft would use the customer **WL-Proxy-Client-IP** header to pass the actual client IP from proxy. On the APV Series, to use customized Header (or URL/Cookie/All) to pass the client IP, follow these steps:

From WebUI, **Mode: Config:**

1. Select **Virtual Services** from the sidebar; double click the "**ps-ent-http**" Virtual Service to select it.

Note: the same option is also available for HTTPS virtual services.

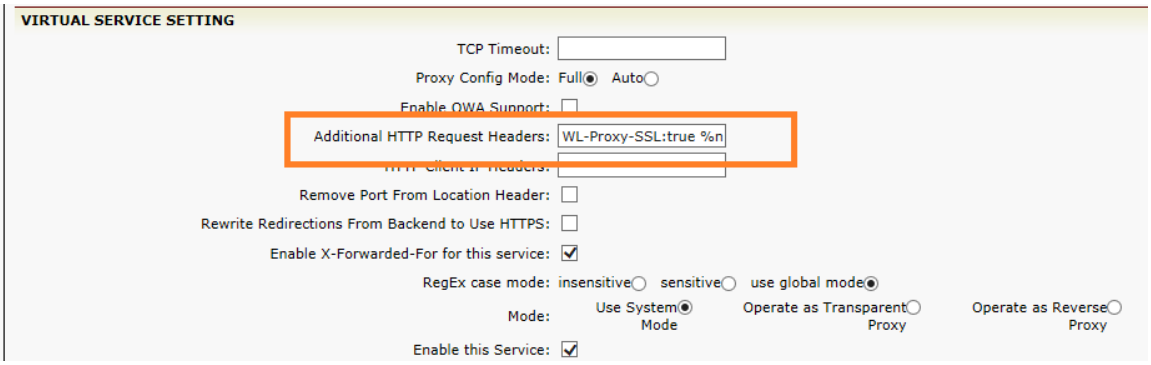
2. Click the **HTTP Forwarding** tab.
3. Enter "**WL-Proxy-Client-IP**" for the "**Customized Name**".
4. Select "**header**" as the "**Mode**".
5. Click **Enable.**

6.3 How to Insert a WL-Proxy-SSL Header

For SSL Offload, if the PeopleSoft Enterprise Web tier is using WebLogic the **WL_Proxy-SS** header is checked by WebLogic and thus it knows the client is over SSL (secured connection). To insert the custom header:

From WebUI, **Mode: Config:**

1. Select **Virtual Services** from sidebar; double click the "**ps-ent-https**" Virtual Service to select it.
2. Enter "**WL-Proxy-SSL: true %n**" for the "**Additional HTTP Request Headers**"
3. Click **SAVE CHANGES.**

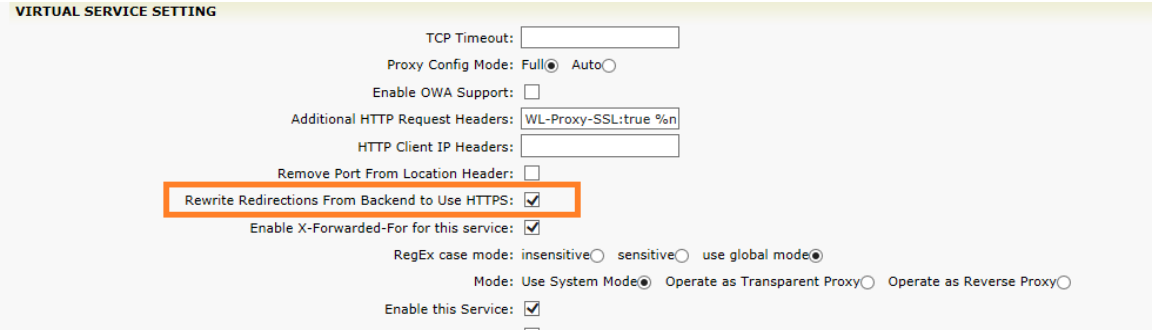


6.4 SSL Offloading – Location Header Rewrite (HTTP to HTTPS)

For SSL Offload, the internal server is via HTTP and external access is via HTTPS. For a Web service with HTTP Redirect response, the location header may be “http” which needs to be rewritten to “https” to facilitate secured access. On the APV, to enable the rewrite:

From WebUI, **Mode: Config**:

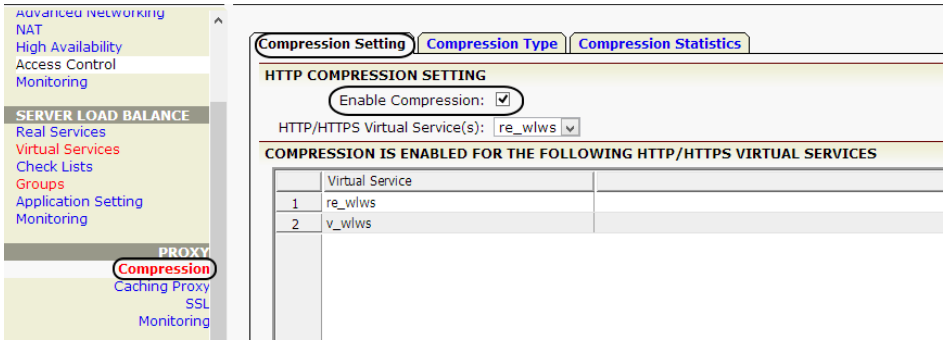
1. Select **Virtual Services** from the sidebar; double click the “**ps-ent-https**” Virtual Service to select it.
2. Check the Box for “**Rewrite Redirections from Backend to Use HTTPS**”.
3. Click **SAVE CHANGES**.



6.5 Enable HTTP Compression

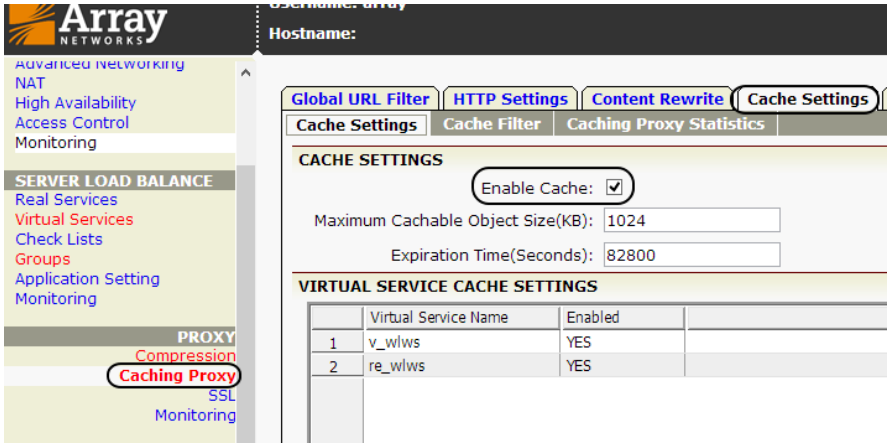
The APV appliance compresses in-line and delivers packet dynamic/static contents over LAN and WAN networks.

Navigate to **Compression** -> **Compression Setting** to enable http compression.



6.6 Enable HTTP Caching

The APV appliance can serve frequently requested contents from the APV Series' own memory cache for increased performance and to allow scaling the capacity of the PeopleSoft Enterprise Server environment. In addition, cache rules can be used to force client browser caching to further accelerate content delivery and lower the server load.

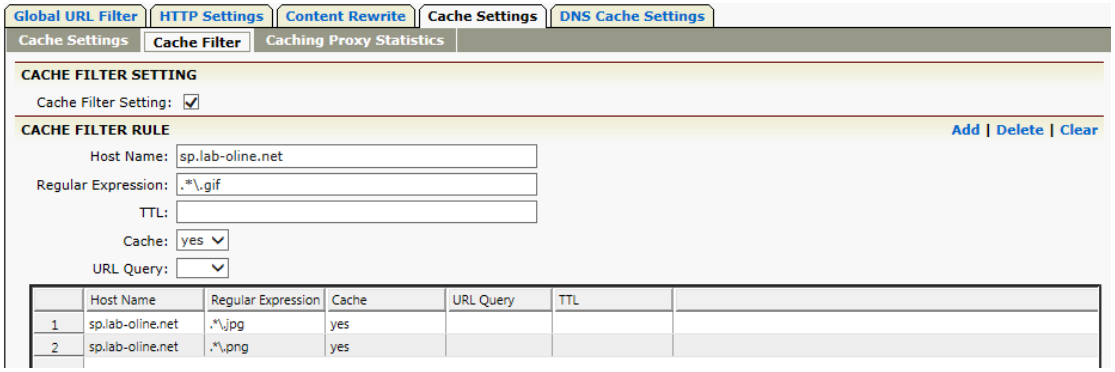


In a typical PeopleSoft Enterprise deployment, access is by an individual login and the main content is usually dynamic, i.e. specific to the individual, and thus not shareable. Therefore, PeopleSoft Enterprise will use HTTP cache control to make the content non-cacheable. However, there are objects, such as small images (gif, jpg, png, etc.) for Web rendering, which are the same among all users. To take advantage of the APV Series' cache, a cache filter can be used to force caching of those shareable objects to reduce server load and accelerate application delivery.

To configure the APV Series cache filter:

1. Under **PROXY**, **Caching Proxy** -> **Cache Setting** -> **Cache Filter**
2. You can enable/disable the Cache Filter.
3. Enter **Cache Filter Rules**:
   - **Host Name:** enter "**sp.lab-online.net**" (this for the lab example).
   - **Regular Expression**: enter a regular expression, for example, for all gifs enter "**.*\.gif**"
   - Cache: select **yes**
4. Click **Add**.

Note: ".*" is the Array Networks regular expression for "any". Please refer to the CLI Handbook for the complete list of regular expressions.



7 References

- To configure PeopleSoft's PIA_access.log with "WL-Proxy-Client-IP", please refer to the following Oracle Support Notes for detailed instructions:

  WebLogic 9.2 and 10.3: How to Enable "HTTP Access Logging" or "HTTP Extended Access Logging" in Order to Collect Detail on HTTP Transactions:

  https://support.oracle.com/oip/faces/secure/km/DocumentDisplay.jspx?id=662319.1

  How to Capture the Client's IP Address using a Front-End Proxy with WebLogic Web Server:

  https://support.oracle.com/oip/faces/secure/km/DocumentDisplay.jspx?id=662708.1

About Array Networks

Array Networks is a global leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore software, Array application delivery, WAN optimization and secure access solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is headquartered in Silicon Valley, is backed by over 400 employees worldwide and is a profitable company with strong investors, management and revenue growth. Poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought leaders including Deloitte, IDC and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity.

Corporate Headquarters
info@arraynetworks.com
408-240-8700
1 866 MY-ARRAY
www.arraynetworks.com

EMEA
rschmit@arraynetworks.com
+32 2 6336382

China
support@arraynetworks.com.cn
+010-84446688

France and North Africa
infosfrance@arraynetworks.com
+33 6 07 511 868

India
isales@arraynetworks.com
+91-080-41329296

Japan
sales-japan@arraynetworks.com
+81-45-664-6116

To purchase Array Networks Solutions, please contact your Array Networks representative at 1-866-MY-ARRAY (692-7729) or authorized reseller

May-2015 rev. a