Deployment Guide
May-2019 rev. a

Array Networks APV/vAPV Series ADCs and SAP NetWeaver Enterprise Portal Deployment Guide

Table of Contents

1 Introduction

This guide provides information on configuring the APV/vAPV Series application delivery controller for SAP NetWeaver Enterprise Portal.

The **SAP NetWeaver Enterprise Portal** is one of the building blocks in the SAP NetWeaver architecture. With only a Web browser, users can begin work once they have been authenticated in the portal, which offers a single point of access to information, enterprise applications, and services both inside and outside an organization. The NetWeaver Portal also provides the tools to manage this knowledge, to analyze and interrelate it, and to share and collaborate. With its coherent interface, role-based content, and personalization features, the portal enables you to focus exclusively on data relevant to your daily decision-making processes.

Array Networks APV Series application delivery controllers provide the availability, scalability, performance, security and control essential to keeping cloud services and enterprise applications running in their power band.

1.1 Prerequisites and Assumptions

SAP Enterprise Portal

This document is written with the assumption that you are familiar with SAP Enterprise Portal server products. For more information on planning and deploying the SAP Enterprise Portal server please reference the appropriate document on the SAP site.

Array Networks APV Series

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

1.2 APV Series Application Delivery Controllers (ADCs) Benefits

The Array Networks APV Series delivers all required application delivery functions for optimizing application delivery for SAP Enterprise Portal 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 (SLB) ensures maximum uptime for SAP services. Customers can scale their SAP Enterprise Portal environment to meet capacity and performance needs with APV server load balancers.

SSL Offloading and SSL Security

APV Series provides industry-leading performance and $/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, APV Series SSL acceleration is ideal for scaling secure Software-as-a-Service (SaaS) services, e-commerce environments and business-critical applications requiring high-volume secure connectivity

Network and Server Protection

The APV appliance can protect SAP services 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's 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 HTTP- based services. The APV appliance also reuses existing server connections.

Cache Offload

The APV appliance serves frequently requested content from cache for increase performance and thus scales the capacity of Web based services.

2 Configuration Scenarios

2.1 Deployment Considerations

Array Networks APV/vAPV Series provides two deployment options for SAP Enterprise Portal:

1. Configure the APV/vAPV device with **HTTP** for the SAP Enterprise Portal.

   This scenario is a basic SAP Enterprise Portal Server deployment that places the APV/vAPV in the middle between the users and the SAP Enterprise Portal.

Application /Service	Virtual Service		Real Service		Health Check
	Protocol	Port	Protocol	Port	
SAP Enterprise Portal	HTTP	80	HTTP	50000	HTTP

2. Configure the APV/vAPV device with **HTTPS** for the SAP Enterprise Portal.

   In this scenario, the APV/vAPV system is a reverse proxy. The system is placed in the network between the external clients and the servers. It provides security, scalability, availability, server offload, and much more, all completely transparent to the external users.

Application /Service	Virtual Service		Real Service		Health Check
	Protocol	Port	Protocol	Port	
SAP Enterprise Portal	HTTPS	443	HTTP	50000	HTTP

2.2 Configuring APV/vAPV for SAP Enterprise Portal Services

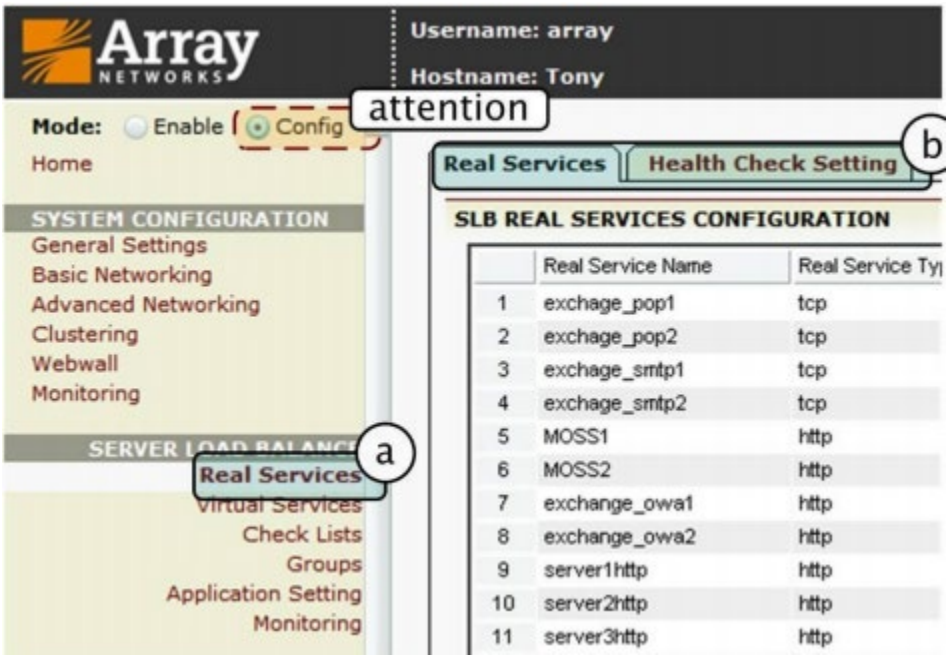
2.2.1 Configuring APV/vAPV for Internal Users

This section assumes the internal users are using HTTP to access the SAP Enterprise Portal.

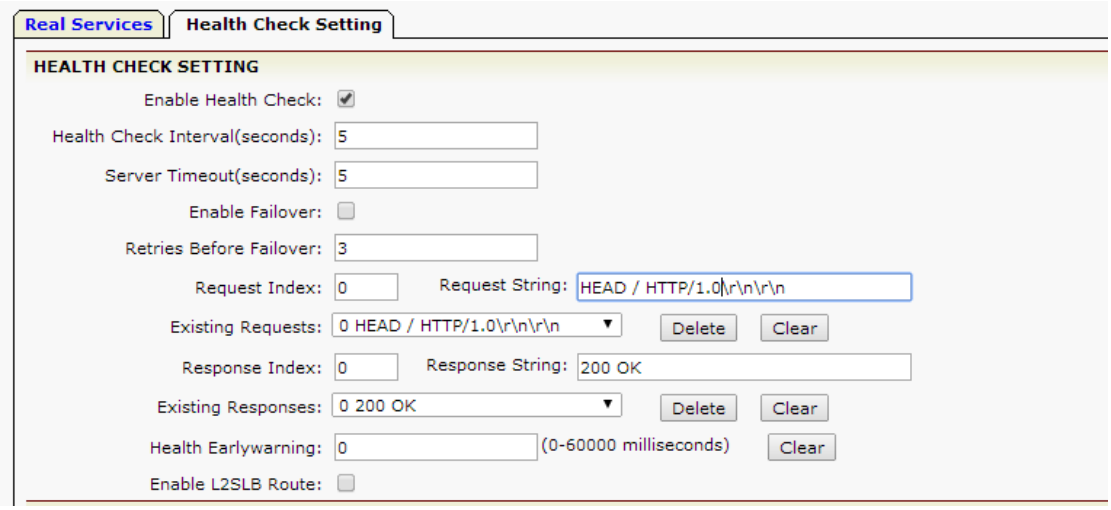
2.2.2 Create the SAP Enterprise Portal health check

Make certain you are in Config mode and have selected the feature **Real Services** from the sidebar. The configuration window will display two tabs, Real Services and Health Check Setting.

A simple HTTP content health check can be better than the TCP/ICMP health check for SAP service availability:



1. Click on the **"Health Check Setting"** tab **[b]**, a new window will display.
2. Select "**0 GET / HTTP/1.0\r\n\r\n**" (see figure below).
3. Input the fields relating to the Response String.
4. In our example we need to input **"GET / HTTP/1.0\r\n\r\n"**
5. In Existing Responses select **"0 200 OK"**.
6. Finish the Health Check Setting by clicking **"SAVE CHANGES"**

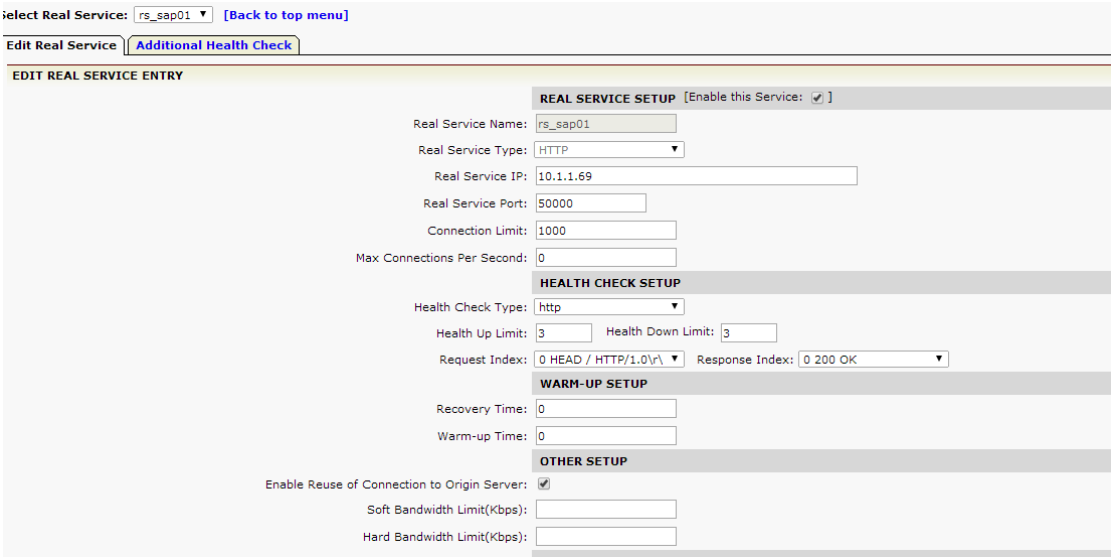


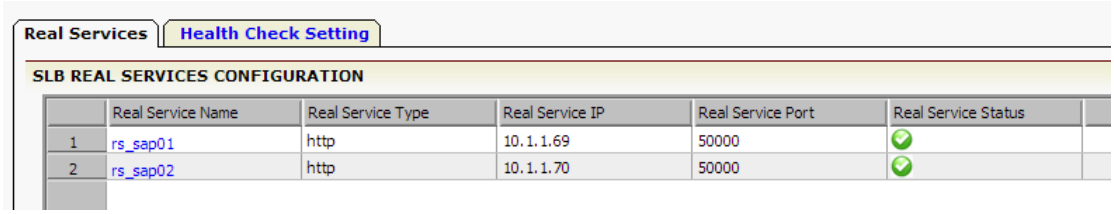
2.2.2 Create a Real Service

Add two SAP Enterprise Portal Web servers in the Real Service profile with the associated health check. 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 for active status after this configuration.

1. Select the action link **"Add Real Service Entry"**. The configuration window will present a new screen for SLB Real Services Configuration.
2. Enable this Service: **Check box** to enable or disable the Real Service. If disabled, APV will not dispatch new traffic to the Real Service.
3. Input the Real Service Name, in our example we input "**rs_sap01**" as our Real Service name.
4. Select **HTTP** as the Real Service Type.
5. Input the SAP Enterprise Portal Web Server IP "**10.1.1.69"** and "**50000"** as the Real Service Port.
6. Connection Limit: **1000**
7. Set max connection to the real service. This setting helps with application stability without overloading the server or application. Increase the number if the server is capable of handling greater loads.
8. Max Connection Per Second – leave default "**0**." If the Real Server application has a performance issue, the APV Series' SLB will allow a connection rate limit to the backend service.
9. Select **HTTP** as the Health Check Type.
10. Select **"0 GET / HTTP/1.0\r\n\r\n"** as the Request Index.
11. Select **"0-200"** as the Response Index.
12. If there are additional SAP Enterprise Portal Servers in your environment, click "**Save and add another**" real service (SAP Enterprise Portal Web Server) and

follow the same procedure as above. You can see the real service status when you complete the creation.





2.2.3 Create a Service Group

Make certain you are in Config mode and select "**Groups**". The configuration window will display three tabs, **Groups**, **Groups Setting** and **Group IP Pool**.

To add a new SLB Group, in the **ADD GROUP** menu, enter the following information:

- **Group Name:** enter "**g_sp01**"
- **Group Method:** select "**Persistence**"
- **Session Type:** select "**ip**"
- **First Choice:** select "**Round Robin**"

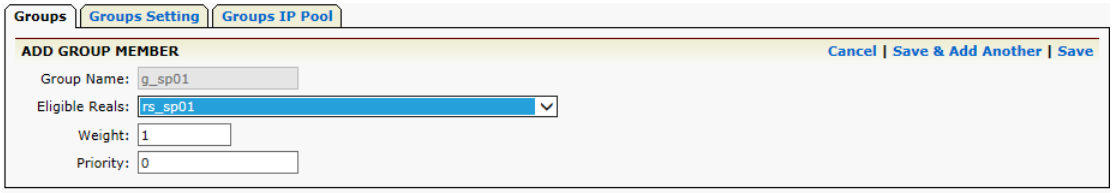
- Click "**Add**" to add the new g_sp01 SLB Group. The g_sp01 should appear in the **GROUP LIST**.

The SLB **Group Method** uses individual source IP persistency and the **First Choice** is Round Robin. This means for a new client (new IP address), the APV Series will select a server using the Round Robin method. For subsequent access for the same client (IP),

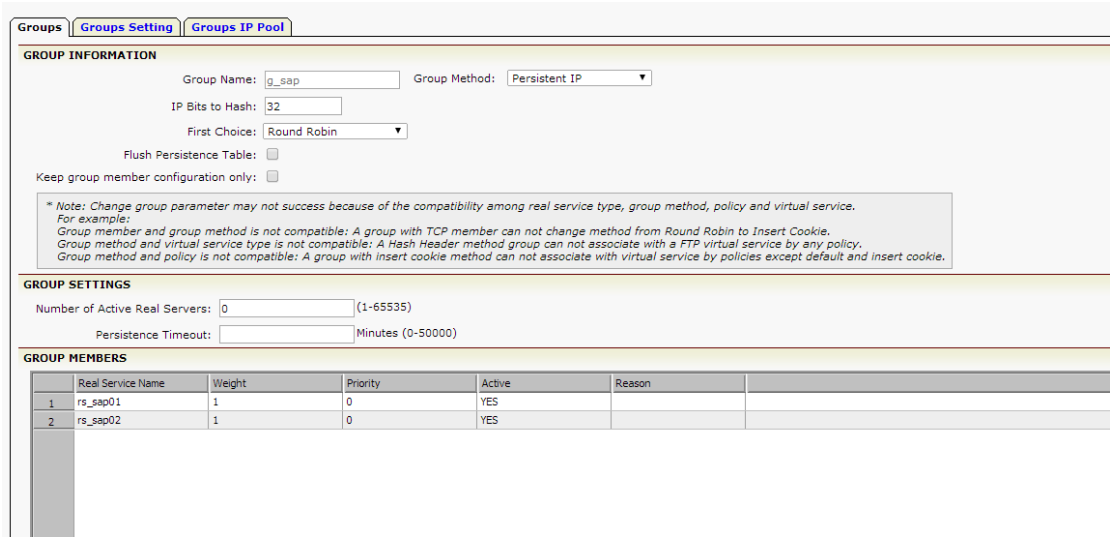
the APV Series will route the request to the same server. This helps distribute load better among all SAP NetWeaver servers.

For SharePoint 2013 with Distributed Cache Service, the user login token is in the Distributed Cache Service on all SharePoint 2013 servers in the cluster. Server affinity is not required and the least connections can be used for the group method. However, this depends on a fully functional Distributed Cache Service.

- To add real service(s) into the SLB Group, click "s_sp01" from the **GROUPS LIST**. Menu **GROUP INFORMATION** and **GROUP MEMBERS** for g_sp01 should appear.
- Under the **GROUP MEMBERS** menu click "**Add**" to access the **ADD GROUP MEMBER** menu
- **Eligible Reals** field: select each SharePoint 2013 server you wish to add to the group.



Now Group g_sp01 is complete.



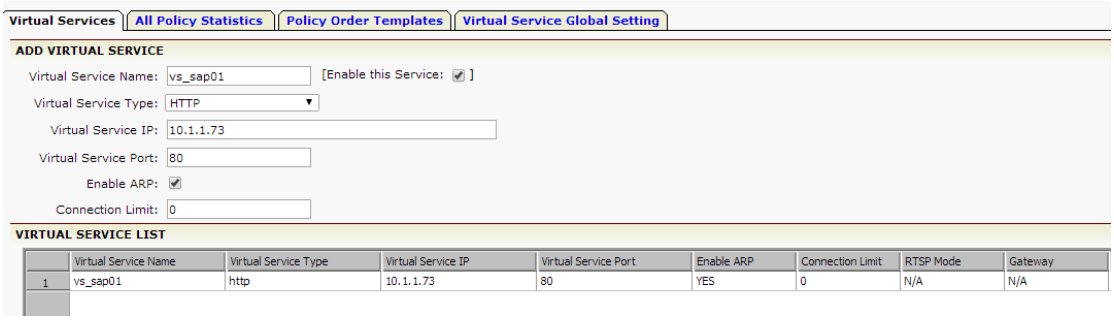
2.2.4 Create a Virtual Service

The next step is to create an SLB Virtual Service for the APV Series to allow the client to access these services. On the APV appliance, a Virtual Service is defined by a Virtual IP/Port and the protocol. External client requests will be terminated on it and the APV appliance will load balance the requests to different Real Services. Below is the configuration for the SAP Enterprise Portal server VIP.

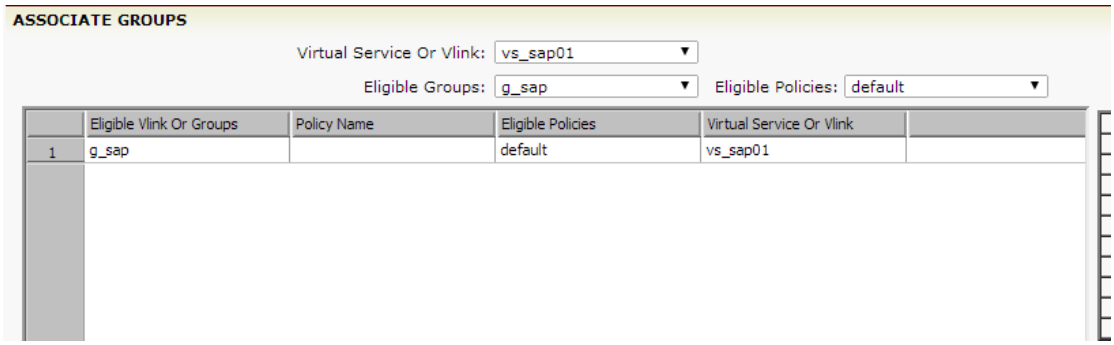
1. Enter "**vs_sap01**" for the Virtual Service Name. Use the check box to enable the virtual service. Select the virtual service type **http** from the selector. Set the

virtual service IP “**10.1.1.73**” and port **80**. Use the check box to enable **ARP**. Set the maximum number of open connections per virtual service. “**0**” means no limitation. Then click “**Add**” to add the APV Series SLB Virtual Service.

Depending on which type of virtual service is specified, certain parameter fields will appear, change or disappear. Click on the desired action link to add a virtual service. Once a virtual service has been added, it will be displayed within the table. Select a virtual service in the table and double click on it or click on the action link “**Edit.**” A new configuration window will present a new series of tabs for completing the virtual services configuration.



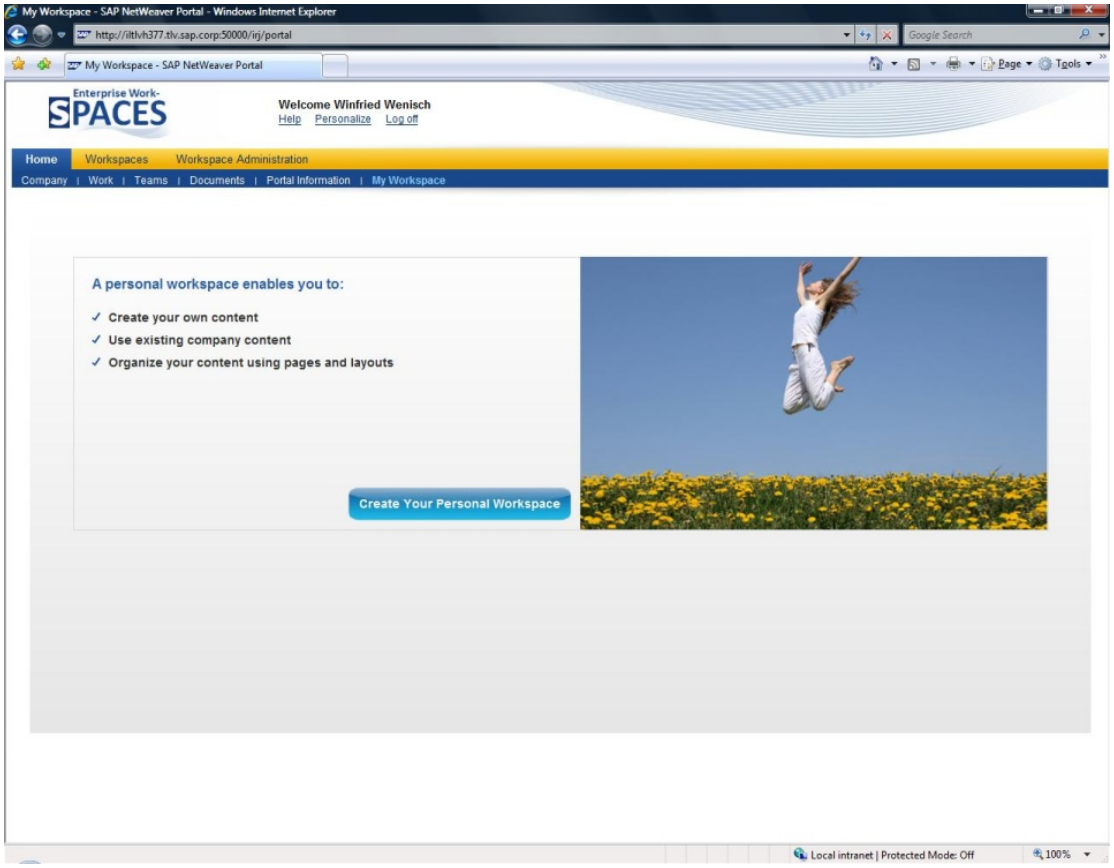
2. Select the pre-created “**g_sap**” and set the Eligible Policies as “**default**”. Click the “**Add**” button to save this Virtual Service-SLB Group association. The g_sap01 will be shown in the ASSOCIATE GROUPS list.



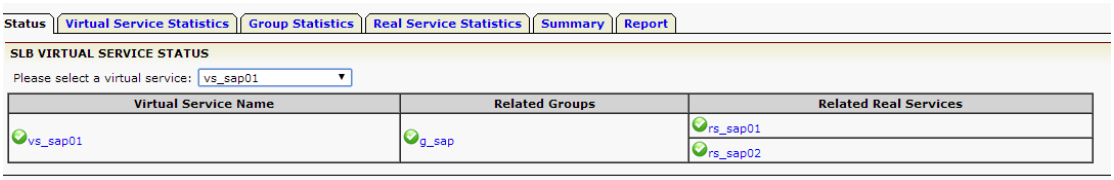
Note: APV Series SLB supports various virtual service settings. Check with Array Support if you would like use them.

2.2.5 Validate SAP Enterprise Portal Service

Input the appropriate URL to access your SAP Enterprise Portal and make sure you can access every resource from the SAP Enterprise Portal



You also can monitor the real service statistics from the APV Web interface.

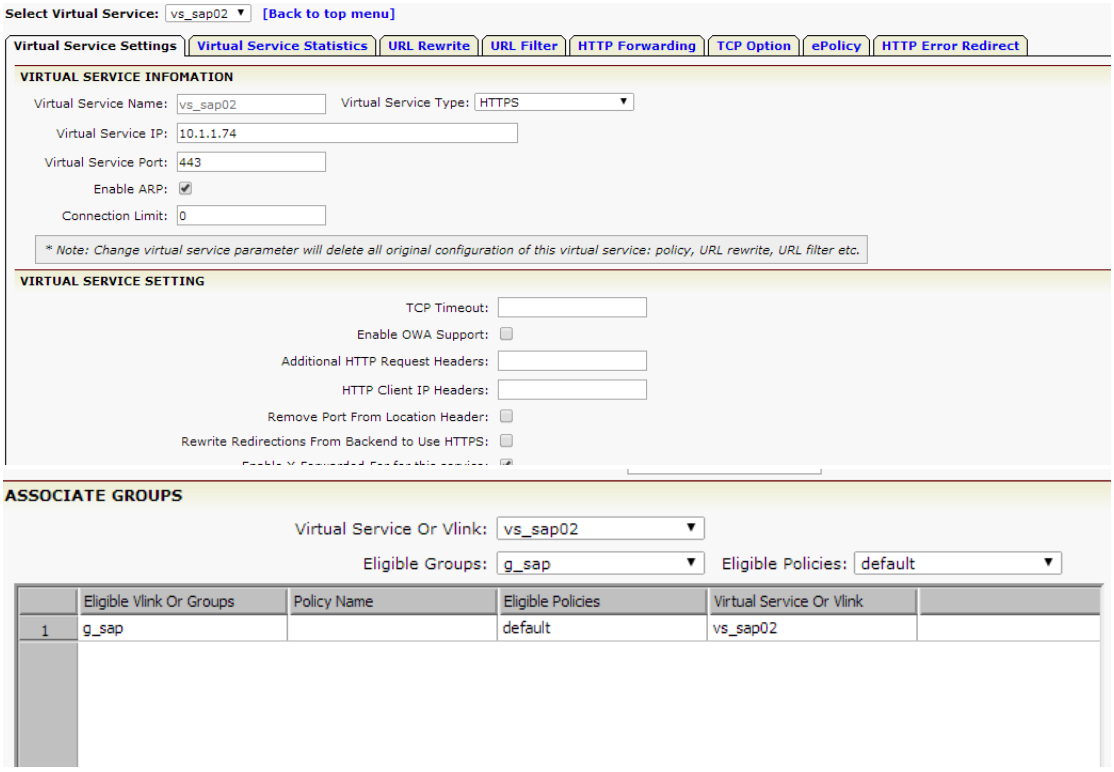


2.3 Configuring APV/vAPV for External Users

This section guides you in configuring the APV/vAPV device to load balance SAP Enterprise Portal via HTTPS to securely encrypt communication from external users. To configure the APV/vAPV device to load balance the SAP Enterprise Portal server you can use the real service we created in **2.2.2 Create Real Service** and **2.2.3 Create Service Group**.

2.3.1 Create an HTTPS Virtual Service and Associate to the Real Service Group

Follow the 2.2.4 section to create a Virtual Service, however, select the type "**HTTPS**" and associate it to the real service groups you created earlier.



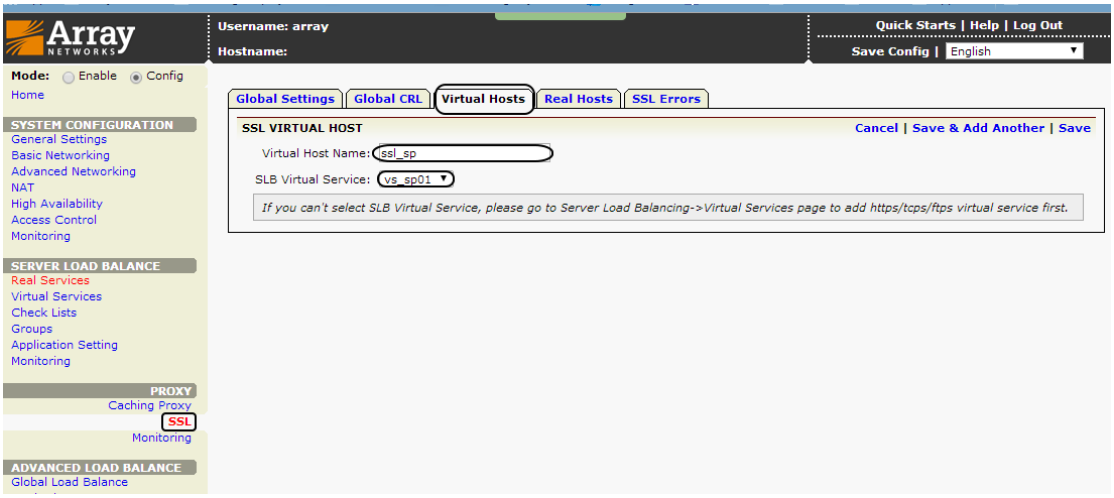
To enable an SLB HTTPS/TCPS Virtual Service on the APV Series, an SSL Certificate/Private Key needs be assigned to it. To do so, the APV Series needs to associate an SSL Virtual Host to the SLB HTTPS/TCPS Virtual Service. Each SSL Virtual Host must have its own SSL Certificate and Private Key assigned.

Note: One SSL Virtual Host can associate multiple SLB Virtual Services in a mix of HTTPS and TCPS.

2.3.2 Create SSL Virtual Hosts

To create the SSL Virtual Hosts, Navigate to **SSL** -> **Virtual Hosts**, and click "**Add**".

Input the Virtual Host Name ("**ssl_sp**" in the following example) and select the SLB Virtual Service "**vs_sp01**". Then click "**Save**" to store the information.



Note: There are two options to assign a SSL Certificate/Private Key:

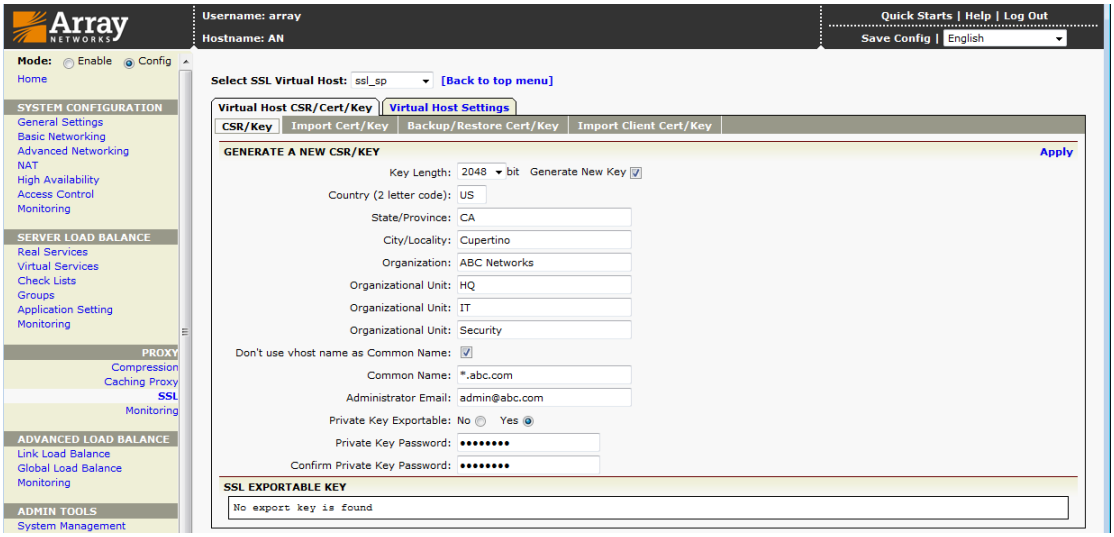
1. Import a SSL Certificate/Private Key from a backend server (external).
2. Generate a self-signed Certificate (CSR) and Private Key and send the CSR/Certificate to a public Certificate Authority (CA) to sign off. It can then be imported to the APV Series appliance.

2.3.3 Generate a Certificate Signing Request (CSR) and Self-Signed Certificate from the APV/vAPV

Navigate to **SSL** -> **Virtual Hosts** -> and double click the SSL Virtual Hosts you just created.

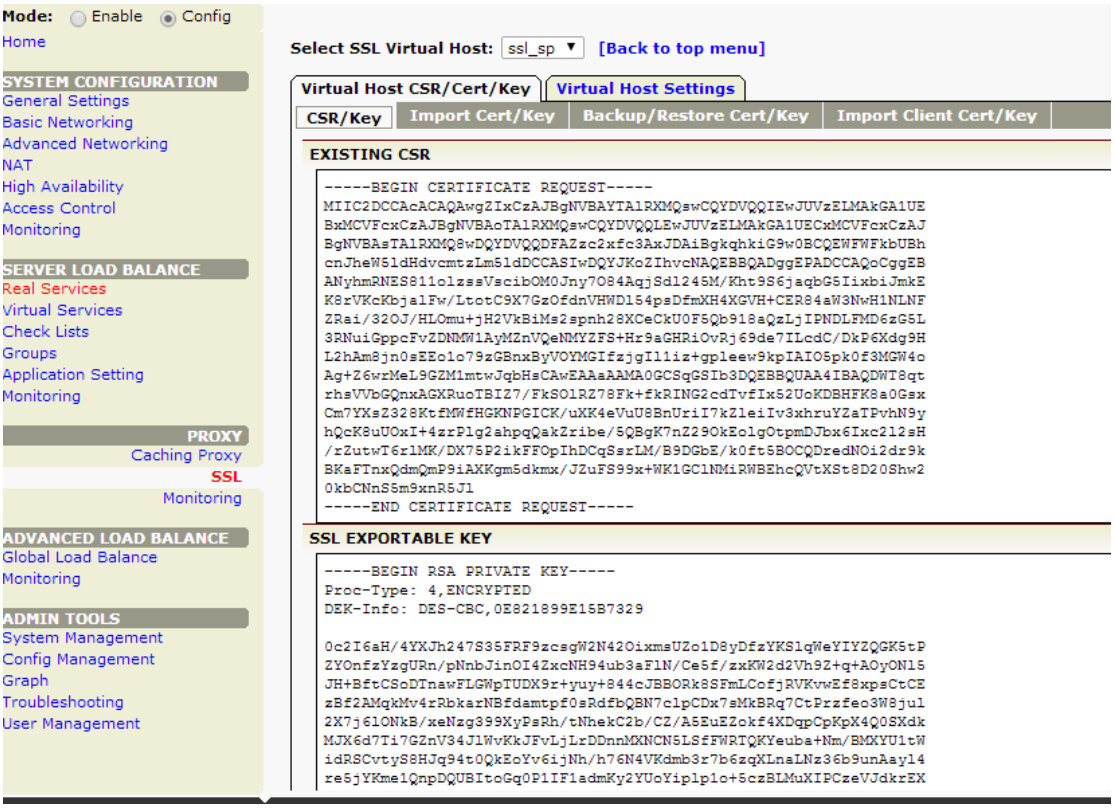
Virtual Host CSR/Cert/Key -> **CSR/Key** to generate a CSR and private key.

Fill in the proper information and click "**Apply**".

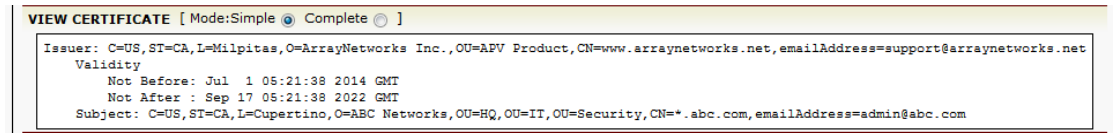


The CSR information will be generated by the APV Series. You can cut and paste the CRS information and email it to a CA to have it sign off the certificate.

Before you have the official SSL certificate, a self-signed SSL certificate can be installed and used for testing.

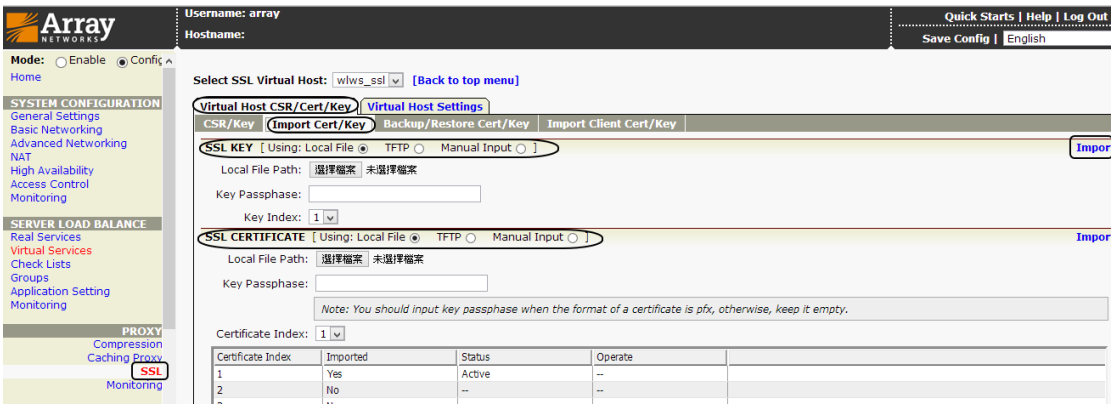


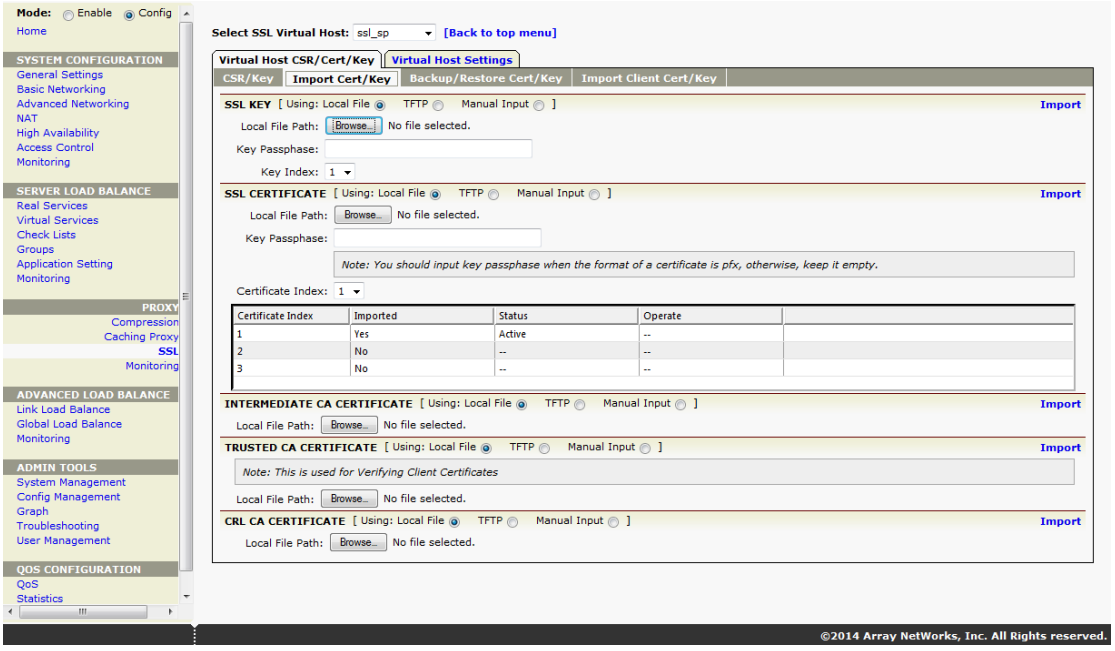
Example Self-Signed SSL Certificate.



2.3.4 Import SSL Certificate and Key

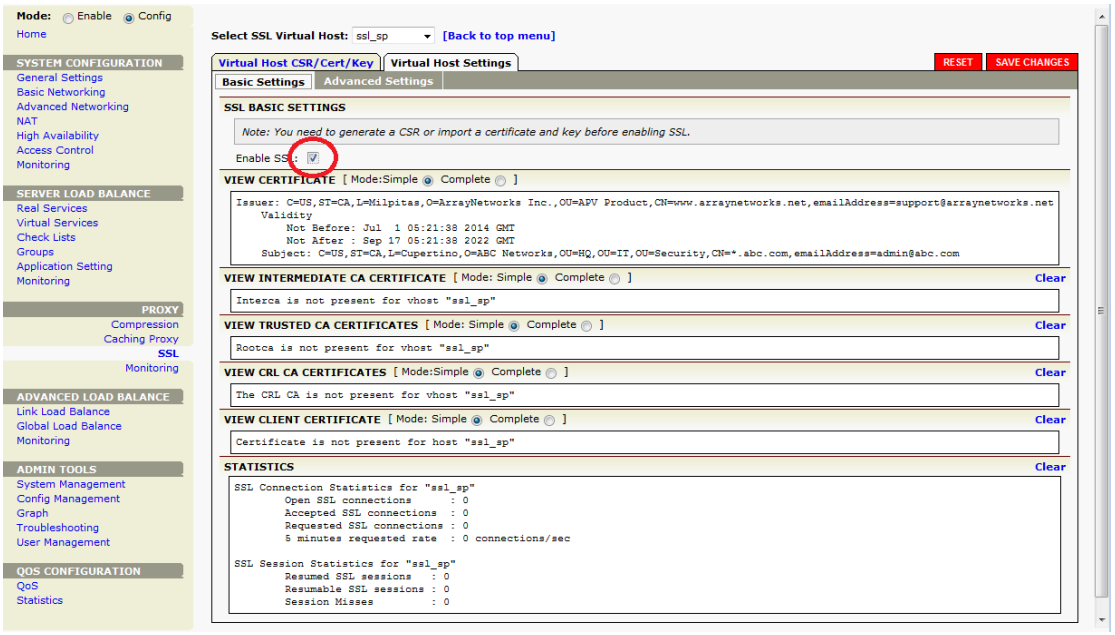
Navigate to **SSL** -> **Virtual Hosts** -> and double click the SSL Virtual Hosts you just created. Next navigate to **Virtual Host CSR/Cert/Key ->Import Cert/Key**, and import the Cert/Key either from a file or manual import.





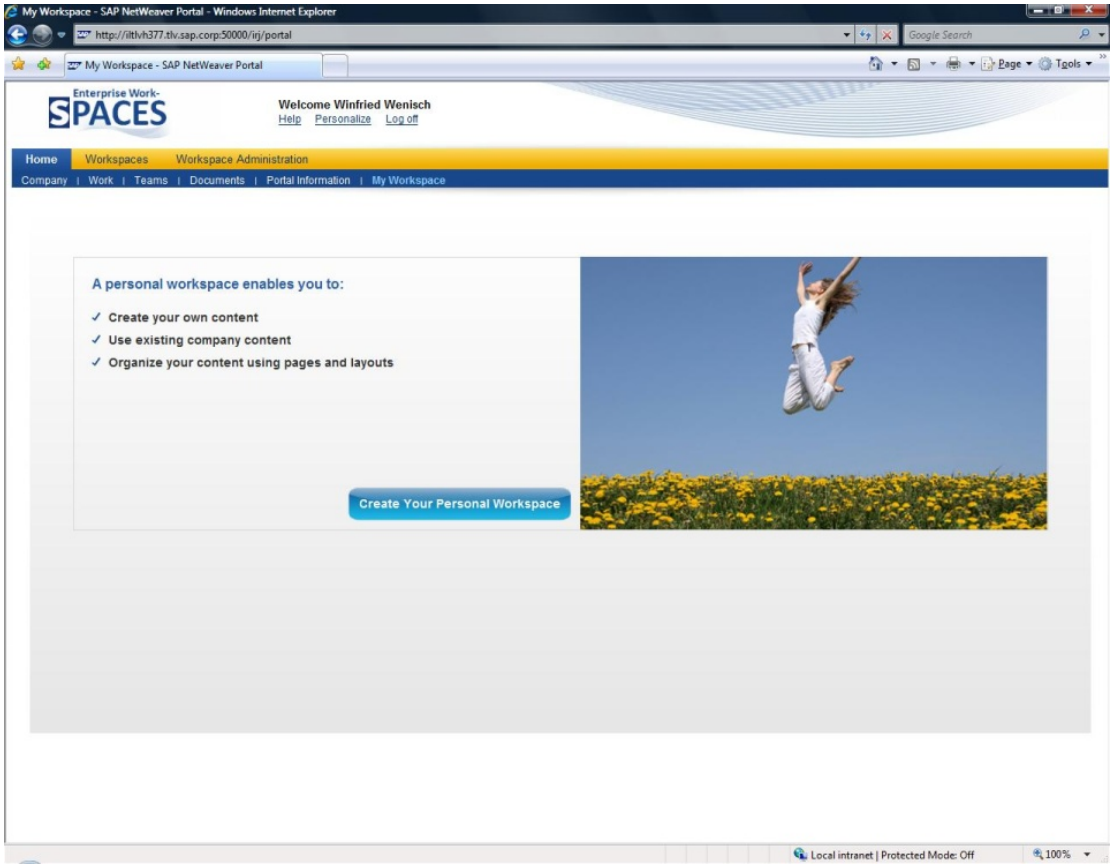
2.3.5 Start SSL

To test (with the self-signed certificate) or run with the production certificate, you will need to Enable SSL. Go **SSL->Virtual Hosts** and double click the virtual host "**ssl_sp**". Select the tab "**Virtual Host Settings**" and select the **Enable SSL** check box.



2.3.6 Validate SAP Enterprise Portal Service

Input the appropriate "HTTPS" URL to access your SAP Enterprise Portal and make sure you can access every resource from the Portal.


My Workspace - SAP NetWeaver Portal - Windows Internet Explorer
http://iltlvh377.tlv.sap.corp:50000/irj/portal
My Workspace - SAP NetWeaver Portal
Enterprise Work-
SPACES
Welcome Winfried Wenisch
Help Personalize Log off
Home
Workspaces
Workspace Administration
Company | Work | Teams | Documents | Portal Information | My Workspace
A personal workspace enables you to:
✓ Create your own content
✓ Use existing company content
✓ Organize your content using pages and layouts
Create Your Personal Workspace
Local intranet | Protected Mode: Off
100%

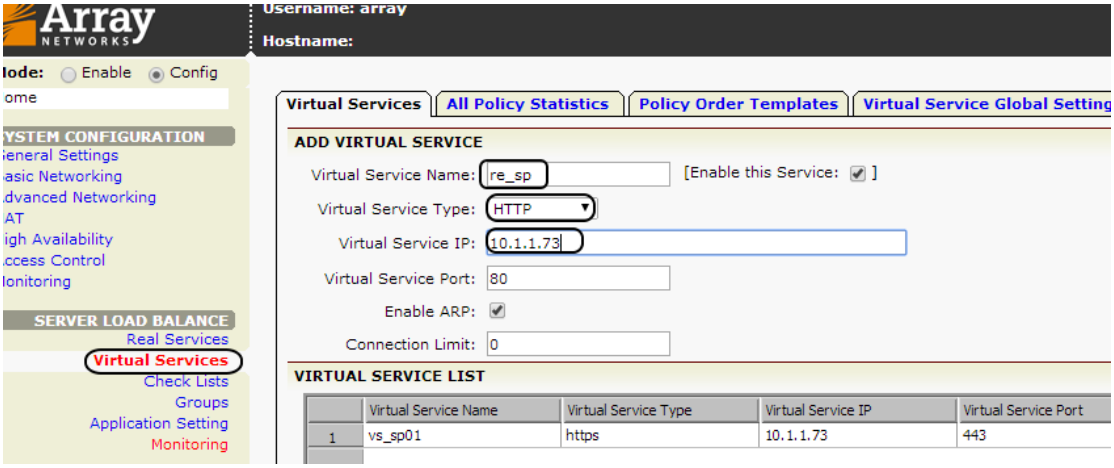
3 Optional Configuration

3.1 HTTP Rewrite/Redirect

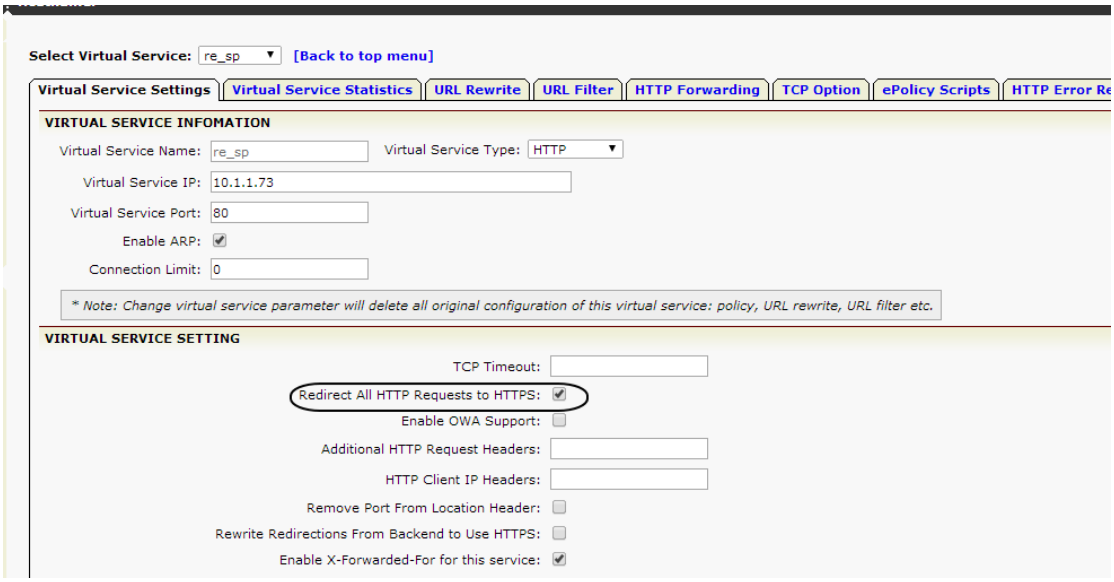
Oftentimes, users will type “HTTP://...” (unsecured) rather than “HTTPS://...” when they attempt to access the secured SAP Enterprise Portal Server, which will normally result in an error. To make this more user friendly, the APV appliance can be configured to auto redirect HTTP requests to HTTPS.

3.1.1 Create Another HTTP Virtual Service

Create another HTTP virtual service and point it to the same IP address as your HTTPS IP address.



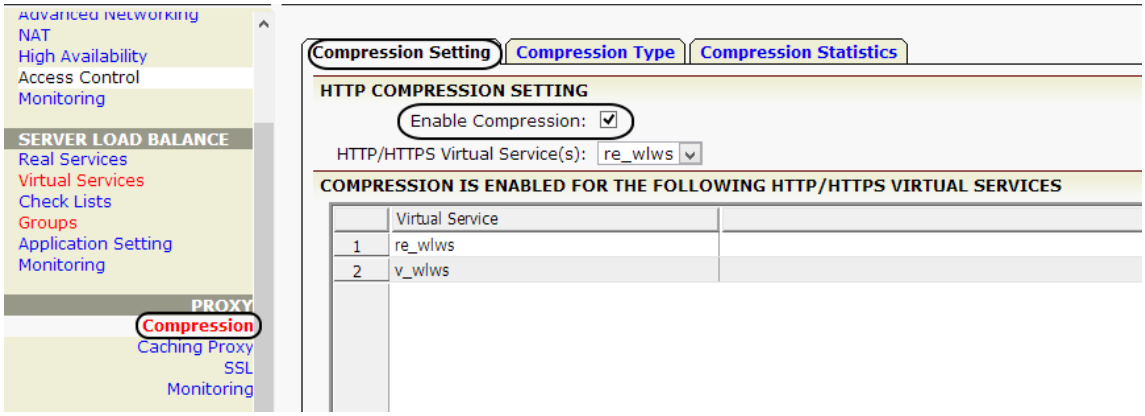
Double click the HTTP Virtual Service IP and enable “**Redirect All HTTP Requests to HTTPS**”



3.2 Enable HTTP Compression

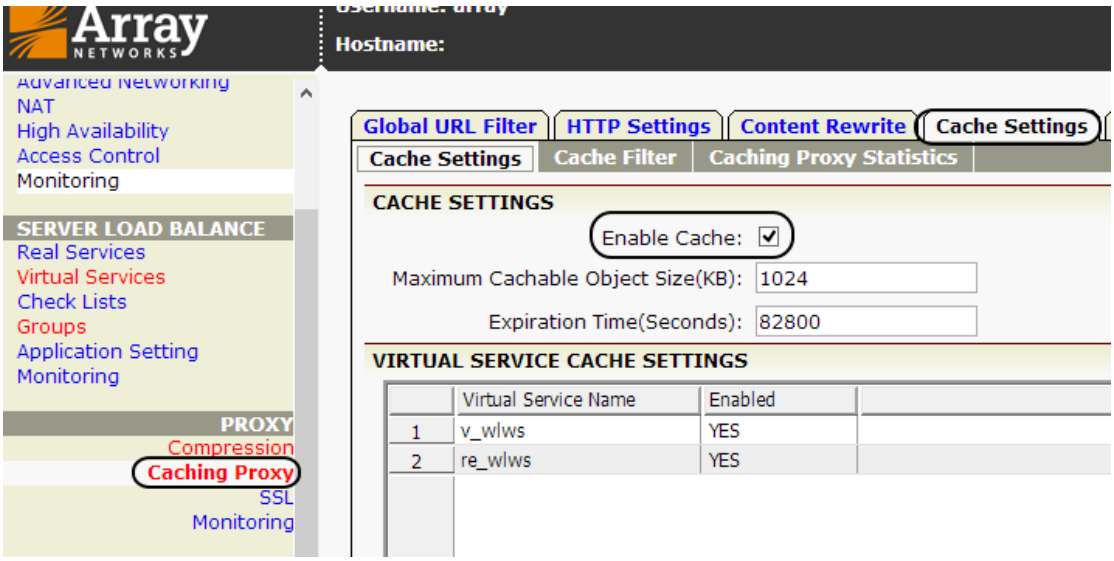
The APV appliance compresses in-line and delivers dynamic/static packet contents over LAN and WAN networks.

Navigate to **Compression** -> **Compression Setting** to enable the HTTP compression.



3.3 Enable RAM Caching

The APV appliance serves frequently requested contents from APV memory cache for increased performance and thus scales the capacity of the SAP Enterprise Portal Server environment. In addition, a cache rule can be put in place to utilize client browser cache, which further accelerates content delivery and lowers server load.



About Array Networks

Array Networks solves performance and complexity challenges for businesses moving toward virtualized networking, security and application delivery. Headquartered in Silicon Valley, Array addresses the growing market demand for network functions virtualization (NFV), cloud computing, and software-centric networking. Proven at more than 5,000 worldwide customer deployments, Array is recognized by leading analysts, enterprises, service providers and partners for pioneering next-generation technology that delivers agility at scale.

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
nsedrati@arraynetworks.com
+33 6 07 511 868

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

Japan
sales-japan@
arraynetworks.com
+81-44-589-8315

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

May 2019 rev. a