

Deploying Array Networks APV Series Application Delivery Controllers with Oracle WebLogic 12c

Table of Contents

1 Introduction	3
1.1 Array Networks APV Appliance	3
1.2 Basic APV Configuration for WebLogic	3
1.3 APV Application Delivery Controller Benefits	3
1.4 APV SSL Offloading/Acceleration	4
SSL Offloading	4
SSL Inside	5
SSL Bridging (SSL Offloading + SSL Inside)	5
1.5 APV Configuration Summary	5
2 Configuring the APV Series for WebLogic Load Balancing	6
2.1 Configuration Steps	6
2.1.1 Create the WebLogic HTTP Health Check	6
2.1.2 Create the WebLogic Real Services	7
2.1.3 Create the WebLogic Group	8
2.1.4 Create the WebLogic (HTTP) Virtual Service	9
2.2 Validate the Configuration and Service	10
3 Configure the APV Series for WebLogic SSL Offload	12
3.1 Configuration Steps	12
3.1.1 Create the WebLogic Real Services	12
3.1.2 Create the WebLogic SLB Group	12
3.1.3 Create the Secured "HTTPS" WebLogic Virtual Service	12
3.1.4 Create the SSL Virtual Hosts	14
3.1.5 Import the Cert/Key or Create a CSR with Self-Signed Cert/Key	14
3.1.6 Enable the SSL Virtual Host	16
3.2 Validate Configuration and Service	16
4 Configure the APV Series for WebLogic SSL Inside	18
4.1 Configuration Steps	18
4.1.1 Create the WebLogic (HTTPS) Real Services	18
4.1.2 Create the SSL Real Host	19
4.1.3 Create the WebLogic (HTTPS) Group	21

4.1.4 Create a WebLogic HTTP SLB Virtual Service.....	22
4.2 Validate Configuration and Service	22
5 Configure the APV Series for WebLogic SSL Bridging	24
5.1 Configuration Steps.....	24
5.1.1 Create the WebLogic (HTTPS) Real Services.....	24
5.1.2 Create the WebLogic (HTTPS) Group,	24
5.1.3 Create the WebLogic (HTTPS) Virtual Services	24
5.2 Validate the Configuration and Service	25
6 Configure Other APV Series Features for WebLogic	26
6.1 HTTP Rewrite/Redirect	26
6.2 How to Insert a WL-Proxy-SSL Header.....	27
6.3 Advanced SSL Virtual Host Settings – Disable SSLv3	27
6.4 How to Disable Server Certificate Verification.....	28
6.5 HTTP Compression	29
7. Conclusion.....	31
Appendix: CLI Configuration Lab Example	32

1 Introduction

This document is written with the assumption that you are familiar with Oracle WebLogic products. For more information on planning and deploying the WebLogic 12c, Please reference the appropriate documentation at docs.oracle.com:

http://docs.oracle.com/cd/E24329_01/Web.1211/e24443/deploy.htm

1.1 Array Networks APV Appliance

The APV appliance must be running version ArrayOS™ 8.x or later. For more information on deploying the APV appliance please refer to the ArrayOS Web UI Guide, which is included in the product CD or may be accessed through the product 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.

Learn about your WebLogic deployment in your network and note down VLAN information and IP address. You will need them for configuring virtual sites and load balancing policies on the APV appliance.

1.2 Basic APV Configuration for WebLogic

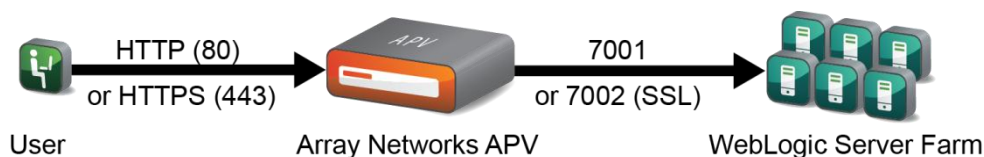


Figure 1: Basic APV Configuration for WebLogic

For the APV series, the ArrayOS APV 8.5.0.x software version is used in this deployment guide.

1.3 APV Application Delivery Controller Benefits

The Array Networks APV Series application delivery controllers provide all required application delivery functions for optimizing application delivery for WebLogic environments, such as Layer 4 server load balancing, high availability, SSL acceleration and offloading, DDoS protection, and TCP connection multiplexing, caching and compression – all in a single, easy-to-manage appliance.

Availability & Scalability

The APV's server load balancing ensures 99.999% uptime for WebLogic Server deployments. Customers can scale their WebLogic environment to meet capacity and performance needs with APV server load balancers.

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.

ISP Link Availability

The APV's link load balancing with advanced link failover and bandwidth management optimizes the availability, security, cost and performance of WebLogic deployments across multiple WAN connections.

TCP Connection Multiplexing

The APV appliance multiplexes several client TCP connections into fewer WebLogic TCP connections for increased throughput and performance. The APV appliance also reuses existing server connections.

Content Cache

The APV appliance serves frequently requested content from cache for increased performance and helps scale the capacity of the WebLogic Server environment.

HTTP Compression

The APV appliance compresses and delivers WebLogic traffic over LAN and WAN networks.

Network and Server Protection

The APV appliance protects the WebLogic Server from malicious network and server attacks such as DDoS attacks, SYN floods, TCP port scans, UDP floods and UDP port scans, etc.

1.4 APV SSL Offloading/Acceleration

Each APV Series appliance (including the vAPV virtual appliance with software SSL) comes with SSL enabled to support SSL offloading for backend servers. SSL offloading (also called SSL acceleration) reduces server load, provides SSL acceleration with high performance hardware, and provides simple key management and advanced 2-way (client) certificate support.

Following are a few ways to use the APV Series with WebLogic SSL traffic:

SSL Offloading

When performing SSL offloading, the APV Series accepts client-encrypted traffic, decrypts (or terminates) it, and then sends the traffic to the servers unencrypted. By saving the servers from having to perform the decryption duties, the APV Series improves server efficiency and frees server resources for other tasks. SSL certificates and keys are stored on the APV system.

SSL Inside

In this scenario, the APV Series accepts unencrypted client traffic and then encrypts it before sending it to the servers. While less common than SSL offloading or bridging, this can be useful for organizations that require all traffic behind the system to be encrypted.

SSL Bridging (SSL Offloading + SSL Inside)

With SSL Bridging, also known as SSL re-encryption/inside, the APV Series accepts client-encrypted traffic, decrypts it for processing, and then re-encrypts the traffic before sending it to the servers. This is useful for organizations that have requirements for the entire transaction to be SSL encrypted. In this case, SSL certificates and keys are stored on both the APV Series appliance and the WebLogic Servers.

1.5 APV Configuration Summary

WebLogic Service	Virtual Service		Real Service		Health Check
	Protocol	Port	Protocol	Port	
Basic	HTTP	80	HTTP	7001	HTTP
SSL Offloading	HTTPS	443	HTTP	7001	HTTP
SSL Inside	HTTP	80	HTTPS	7002	HTTPS
SSL Bridging	HTTPS	443	HTTPS	7002	HTTPS

2 Configuring the APV Series for WebLogic Load Balancing

2.1 Configuration Steps

Ensure that the APV/vAPV appliance is accessible from the network, and that WebUI is enabled. To access the APV appliance's WebUI, enter <https://<apv ip>:8888> from the browser (we recommend using Internet Explorer). Log-in; the default user account/password is "array/admin". For the Array Networks pilot login, the default is no enable password. Simply click Login to enter the WebUI.

2.1.1 Create the WebLogic HTTP 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. Basic protocol-based Health Checks, such as ICMP and TCP/TCPs, are built-in and can be used as default.

For the deployment example, the APV Series' Health Check can simulate access to the WebLogic Administration Console: <http://<wls host>:<wls port>/console> and check for the HTTP return code.

On the APV Series, the HTTP Health Check Request/Response Table is used to configure the content-based Request/Response health check. The APV Series' health check will send the string and match the response to determine the availability of the real service.

To configure the content-based health check request/response, enter WebUI, Mode: **Config**,

1. From the sidebar **SERVER LOAD BALANCE**, select "**Real Services**" => "**Health Check Setting**". The **HEALTH CHECK SETTING** screen opens.
2. Enter a number for the **Request Index** (0 for the example) and enter "**HEAD /console HTTP/1.0 \r\n\r\n**" string for the **Request String**.
3. Enter a number for the **Response Index** (1 for the example) and enter "**302**" string for the **Response String**. Click **SAVE CHANGES**.

The screenshot displays the 'Health Check Setting' configuration page. At the top, there are tabs for 'Real Services' and 'Health Check Setting', and buttons for 'RESET' and 'SAVE CHANGES'. The main section is titled 'HEALTH CHECK SETTING' and contains the following fields:

- Enable Health Check: ☒
- Health Check Interval(seconds): 5
- Server Timeout(seconds): 5
- Enable Failover: ☐
- Retries Before Failover: 3
- Request Index: 0
- Request String: HEAD / HTTP/1.0\r\n\r\n
- Existing Requests: 0 HEAD / HTTP/1.0\r\n\r\n (with Delete and Clear buttons)
- Response Index: 1
- Response String: 302 (highlighted with a red box)
- Existing Responses: 1 302 (with Delete and Clear buttons)
- Health Earlywarning: 0 (0-60000 milliseconds) (with Clear button)
- Enable L2SLB Route: ☐

2.1.2 Create the WebLogic Real Services

Real Services are two WebLogic Web servers. Add each server with its unique name, IP/port and protocol information as a Real Service using the following steps:

1. From 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 “**WLWS01**” as the Real Service Name. Select “**HTTP**” as the Real Service Type, enter IP addresses “**10.2.40.171**” and port “**7001**” which is used by the WebLogic Web Server.

Real Services | Health Check Setting

ADD REAL SERVICE ENTRY Cancel | Save & Add Another | Save

REAL SERVICE SETUP [Enable this Service: ☒]

Real Service Name: WLWS01

Real Service Type: HTTP

Real Service IP: 10.2.40.171

Real Service Port: 7001

Connection Limit: 1000

Max Connections Per Second: 0

HEALTH CHECK SETUP

Health Check Type: http

Health Up Limit: 3 Health Down Limit: 3

Request Index: 0 HEAD /console HTTP Response Index: 0 200 OK

3. Select **HTTP** as the Health Check Type for the real service health check. The default Request Index 0 and Response Index 0 are used. Click **Save & Add Another** to add more real services.
4. Follow the same steps as above: add “**WLWS02**” server as a real service with the IP address **10.2.40.172**.

Note: You may also add WebLogic Web Services with the Real Service type. The default port used by the WebLogic Web Service for HTTPS is 7002. You may use HTTPS as the Health Check Type.

Mode: ☐ Enable ☒ Config

Home

SYSTEM CONFIGURATION

- General Settings
- Basic Networking
- Advanced Networking
- NAT
- High Availability
- Access Control
- Monitoring

SERVER LOAD BALANCE

Real Services

SLB REAL SERVICES CONFIGURATION Enable | Disable | Delete | Add

	Real Service Name	Real Service Type	Real Service IP	Real Service Port	Real Service Status
1	WLWS01	http	10.2.40.171	7001	✓
2	WLWS02	http	10.2.40.172	7001	✓
3	WLWS01-HTTPS	https	10.2.40.171	7002	✓
4	WLWS02-HTTPS	https	10.2.40.172	7002	✓

Technical Notes:

Enable this Service: Check the box to enable or disable the Real Service. If disabled, the APV Series will not dispatch new traffic to the Real Service.

Connection Limit: 1000

Set the maximum connections 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.

Health Check Setup:

The HTTP Health Check Request and Response is editable to simulate HTTP requests and responses to determine the real service's availability. Each real service can have its own health check.

2.1.3 Create the WebLogic Group

The APV Series' SLB Group is a set of servers grouped together to receive traffic according to the chosen load balancing method. To create an SLB Group, from WebUI, Mode: **Config**;

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 **"g-weblogic"**. Select the **"Insert Cookie"** group method by selecting from the pull down menu. Enter a unique cookie name. Select the **"Least Connections"** group method by selecting from the pull down menu. Enter **"1"** for the Path Flag. After making configurations on those parameter fields, click on the action link **"Add"** to create the SLB group. All configured SLB Groups will be displayed in the **GROUPS LIST**.

The screenshot shows the 'Groups' configuration page with tabs for 'Groups Setting', 'Groups IP Pool', and 'Groups Health Check'. The 'ADD GROUP' form is active, showing fields for Group Name (g-weblogic), Group Method (Insert Cookie), Cookie Name (WebLogic-ServerID), First Choice (Least Connections), Path Flag (1), and Threshold Granularity (10). An 'Add' button is in the top right. Below the form is the 'GROUPS LIST' table with columns for Group Name, Group Method, and Enabled. The table contains two entries: 'g-weblogic' and 'ps-web-group', both with 'ic' as the Group Method and 'Enabled' checked.

	Group Name	Group Method	Enabled
1	g-weblogic	ic	<input checked="" type="checkbox"/>
2	ps-web-group	ic	<input checked="" type="checkbox"/>

3. To assign the WebLogic Servers to the SLB group, choose **"g-weblogic"** in the GROUPS LIST by double clicking on it or selecting it and clicking on the action link **"Edit"**. The **GROUP INFORMATION** configuration screen opens.
4. Under the **"GROUP MEMBERS"** section, click **"Add"**; the **ADD GROUP MEMBER** configuration screen opens. Assign real services **"WLWS01"** and **"WLWS02"** to the group and click **"Save"**.

ADD GROUP MEMBER Cancel | Save & Add Another | Save

Group Name:

Eligible Reals:

Weight:

Priority:

2.1.4 Create the WebLogic (HTTP) Virtual Service

The next step is to create a WebLogic Virtual Service for the external WebLogic client to access. On the APV appliance, a Virtual Service is defined by a Virtual IP/Port and the protocol. External WebLogic client requests will be terminated on it and the APV appliance forward them to the designated SLB Group, based on the SLB Group method. The APV Series will load balance or assign the requests to the selected WebLogic server.

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

1. Select the feature link **Virtual Services** from the sidebar. The **"ADD VIRTUAL SERVICE"** configuration screen opens.
2. Enter **"weblogic"** for the Virtual Service Name. Use the check box to enable the virtual service. Select the virtual service type **"HTTP"** from the pull down menu. 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. Once a virtual service has been added, it will be on the **VIRTUAL SERVICES LIST**.

Mode: ☐ Enable ☒ Config

Virtual Services All Policy Statistics | Policy Order Templates | Virtual Service Global Setting

ADD VIRTUAL SERVICE Add

Virtual Service Name: [Enable this Service: ☒

Virtual Service Type:

Virtual Service IP:

Virtual Service Port:

Enable ARP: ☒

Connection Limit:

VIRTUAL SERVICE LIST Delete

	Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	Enable ARP
1	web1	http	10.2.40.112	80	YES
2	weblogic-http	http	10.1.1.199	80	YES

Once the SLB Virtual Service is created, the APV Series needs know how (via SLB Policy or Rule) and which SLB Group to pass the traffic to. For the Virtual Service to associate an SLB Group and "default" policy, please follow these steps:

3. Select the **"weblogic"** Virtual Service on the **VIRTUAL SERVICES LIST** by double clicking on it or clicking on it and selecting the action link **"Edit"**. The **VIRTUAL SERVICE INFORMATION** configuration page will open and present a new series of tabs for completing the virtual services configuration.

- Go down to In the **ASSOCIATE GROUPS** section, select SLB Group **g-weblogic** from Eligible Groups, and select “**default**” from Eligible Policies. Click **Add**.
- Under the same **ASSOCIATE GROUPS** section, for the same SLB Group **g-weblogic**, select “**icookie**” from Eligible Policies. Enter a unique name for the Policy Name and a priority for Policy Precedence. Click **Add** to complete the Virtual Service configuration.

ASSOCIATE GROUPS Add | Delete

Virtual Service Or Vlink:

Eligible Groups: Eligible Policies:

Policy Name:

Policy Precedence:

	Eligible Vlink Or Groups	Policy Name	Eligible Policies	Virtual
1	g-weblogic	weblogic-icookie	icookie	weblog
2	g-weblogic		default	weblog

Attribute	Value
Groups	g-weblogic
Policy Name	weblogic-icookie
Policy	icookie
Associated Group	q-weblogic

2.2 Validate the Configuration and Service

Validate that the basic configuration is functioning correctly:

- From WebUI, **SERVER LOAD BALANCE, Monitoring -> Status -> Virtual Service Status**, select “**weblogic**” as the virtual service.
- Verify that all “**Service Status**” icons are green.

Mode: ☒ Enable ☐ Config

Home

SYSTEM CONFIGURATION

- General Settings
- Basic Networking
- Advanced Networking
- NAT
- High Availability
- Access Control
- Monitoring

SERVER LOAD BALANCE

- Real Services
- Virtual Services
- Check Lists
- Groups
- Application Setting
- Monitoring**

Status **Virtual Service Statistics** **Group Statistics** **Real Service Statistics** **Persistence Session Table** **Summary** **Report**

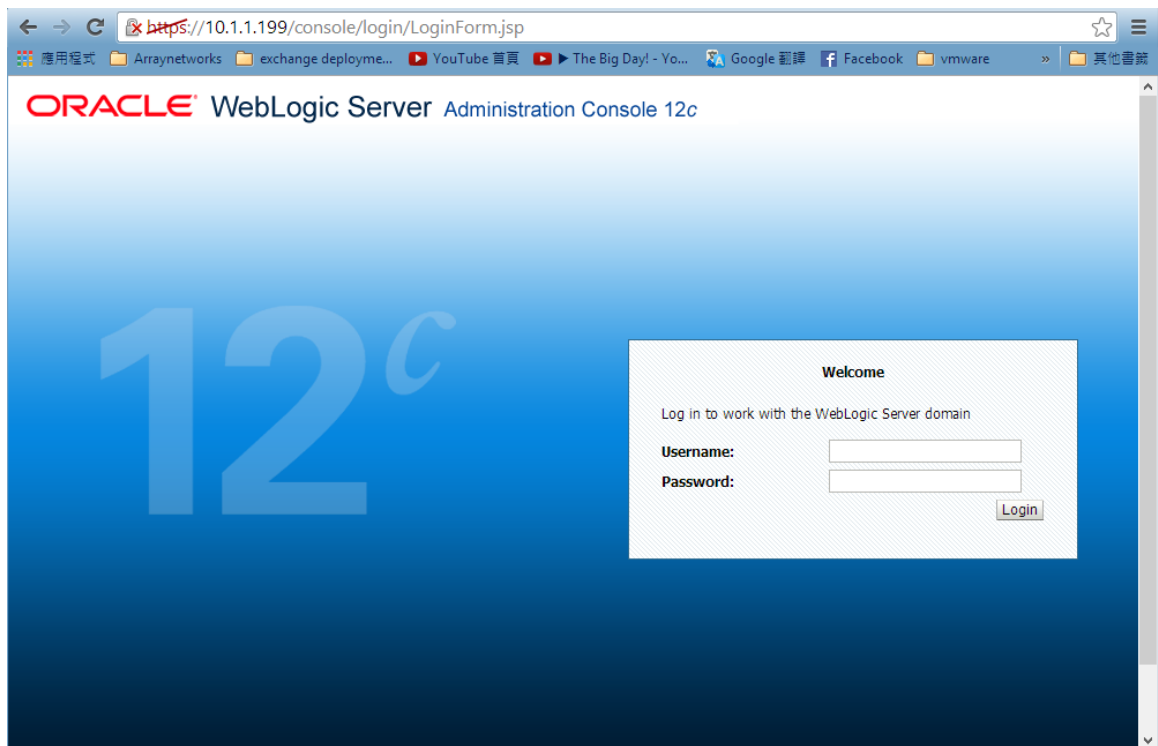
Virtual Service Status **HTTP Proxy Mode Status**

SLB VIRTUAL SERVICE STATUS

Please select a virtual service:

Virtual Service Name	Related Groups	Related Real Services
✓ weblogic	✓ g-weblogic	✓ WLWS01
		✓ WLWS02

- Launch the Web browser and navigate to the VIP address



4. Input the required Username and Password to login.

3 Configure the APV Series for WebLogic SSL Offload

For SSL offloading, the APV Series' SLB Service needs to be HTTPS, and WebLogic Servers will run with HTTP. The SLB Group and SLB Real Service are configured the same as for normal WebLogic load balancing. However, new HTTPS Virtual Services need to be added and SSL Virtual Hosts need to be configured to take care of SSL processing.

In summary, based on the SLB Real Services and Groups configured in the previous example, we add the following to support SSL Offload:

- Create an SLB Virtual Service of type “**HTTPS**” and associate it to the WebLogic SLB Group (see section 2.1.2)
- Create SSL Virtual Hosts:
 - Import SSL certificates signed by a certificate authority or create a self-signed certificate on the APV Series.
 - Enable the SSL Virtual Hosts.

3.1 Configuration Steps

3.1.1 Create the WebLogic Real Services

Follow the same steps as section 2.1.2 Create the WebLogic Real Services

3.1.2 Create the WebLogic SLB Group

Follow the same steps as section 2.1.3 Create the WebLogic Group

3.1.3 Create the Secured "HTTPS" WebLogic Virtual Service

The next step is to create the HTTPS-based WebLogic Virtual Service for secured access. Similar to section 2.1.4, following are the steps to create the WebLogic HTTPS Virtual Service from WebUI (**Config**),

1. Select “**Virtual Services**” from the sidebar. The **ADD VIRTUAL SERVICE** configuration screen opens.
2. Enter a unique Virtual Service Name (**weblogic-https** in the example), select **HTTPS** as the Virtual Service Type. Enter the IP address and port (443) used by the Virtual Service. Use the check box to enable ARP. Set the maximum number of open connections per virtual service. “0” means unlimited. Click **Add** to create the new WebLogic HTTPS Virtual Service.

Virtual Services | All Policy Statistics | Policy Order Templates | Virtual Service Global Setting

ADD VIRTUAL SERVICE Add

Virtual Service Name: [Enable this Service: ☒]

Virtual Service Type:

Virtual Service IP:

Virtual Service Port:

Enable ARP: ☒

Connection Limit:

VIRTUAL SERVICE LIST Delete

	Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	Enable ARP
1	web1	http	10.2.40.112	80	YES

Once added, the newly created **weblogic-https** virtual service will be available on the **VIRTUAL SERVICE LIST**. The next step is to associate the SLB Virtual Service with the WebLogic HTTPS SLB Group. Following are the steps:

- Choose "**weblogic-https**" in the **VIRTUAL SERVICE LIST** by double clicking on it or selecting it and clicking on the action link "**Edit**". The **VIRTUAL SERVICE INFORMATION** configuration page for the Virtual Service will be displayed.
- To associate the WebLogic SLB Group, go down to the **ASSOCIATE GROUPS** section and select the WebLogic SLB Group (**g-weblogic**) from Eligible Groups. Also, select "**default**" for Eligible Policies. Click **Add**.
- Under the same **ASSOCIATE GROUPS** section, for the same **g-weblogic** group, select "**icookie**" from Eligible Policies. Enter a unique name for the Policy Name and a priority for Policy Precedence. Click **Add** to complete the association.

ASSOCIATE GROUPS Add | Delete

Virtual Service Or Vlink:

Eligible Groups: Eligible Policies:

	Eligible Vlink Or Groups	Policy Name	Eligible Policies	Virtual S	Attribute	Value
1	gp-weblogic	ic-policy2	icookie	vs-weblogic		
2	gp-weblogic		default	vs-weblogic		

Note: for SSL offloading, because the APV Series will terminate the client SSL connections, a WL-Proxy-SSL header can be inserted with the client request so that the WebLogic server will continue to build its URIs to use HTTPS. To insert the WL-Proxy-SSL header for each WebLogic client request on the APV Series, please refer to section 6.2 How to Insert a WL-Proxy-SSL Header.

To enable SSL termination for SLB HTTPS/TCP/FTP Virtual Services 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.

3.1.4 Create the 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 as well.

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

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

1. Navigate to **SSL -> Virtual Hosts -> Add**. The **SSL VIRTUAL HOST** screen opens.
2. Enter a unique SSL Virtual Host Name (**ssl-vhost1**) and select the HTTPS SLB Virtual Service, then click **Save**.

Mode: ☐ Enable ☒ Config

Home

SYSTEM CONFIGURATION

- General Settings
- Basic Networking
- Advanced Networking
- NAT
- High Availability
- Access Control
- Monitoring

SERVER LOAD BALANCE

- Real Services
- Virtual Services
- Check Lists
- Groups
- Application Setting
- Monitoring

PROXY

- Caching Proxy
- SSL

Global Settings | Global CRL | **Virtual Hosts** | Real Hosts | SSL Errors

SSL VIRTUAL HOST Cancel | Save & Add Another | Save

Virtual Host Name:

SLB Virtual Service:

If you can't select SLB Virtual Service, please go to Server Load Balancing->Virtual Services page to add https/tcps/ftps virtual service first.

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

Global Settings | Global CRL | **Virtual Hosts** | Real Hosts | SSL Errors

SSL VIRTUAL HOSTS Edit | Delete | Clear Virtual Host | Add

	Virtual Host Name	SLB Virtual Service
1	ssl-vhost1	weblogic-https

3.1.5 Import the Cert/Key or Create a CSR with Self-Signed Cert/Key

The SSL server requires a proper Certificate (and Private Key) for the SSL/TLS handshake so that the client knows it is connected to the intended server with security.

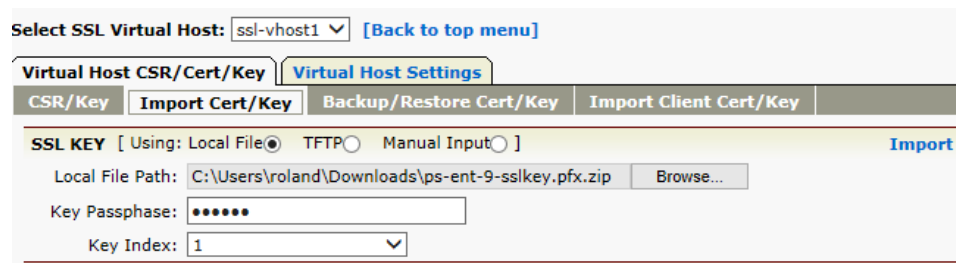
There are two options to add a certificate/key to be used by the SSL Virtual Host on the APV:

- A. Import an SSL Certificate and Key
- B. Generate a Self-Signed CSR/Certificate and Key

Option A: Import an SSL Certificate and 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 the **SSL KEY** window, the key can be imported through **Local File**, **TFTP**, or **Manual Input**. The following example is using a local disk file “ps-ent-9-sslkey.pfx.zip” 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.



Option B: Generate a Self-Signed Certificate from the APV.

Go WebUI, Mode: **Config**.

1. Navigate to **SSL -> Virtual Hosts ->** and double click the newly created SSL Virtual Host. Click on **Virtual Host CSR/Cert/Key -> CSR/Key**, enter the information and click **Apply** to generate a CSR/Private Key (option) and a Self-Signed Certificate (which can be used for testing).

Mode: ☐ Enable ☒ Config

Home

SYSTEM CONFIGURATION

- General Settings
- Basic Networking
- Advanced Networking
- NAT
- High Availability
- Access Control
- Monitoring

SERVER LOAD BALANCE

- Real Services
- Virtual Services
- Check Lists
- Groups
- Application Setting
- Monitoring

PROXY

- Caching Proxy
- SSL**
- Monitoring

ADVANCED LOAD BALANCE

- Link Load Balance

GLOBAL LOAD BALANCE

- General Settings
- Service IP

Select SSL Virtual Host: ssl-vhost1 [Back to top menu]

Virtual Host CSR/Cert/Key **Virtual Host Settings**

CSR/Key Import Cert/Key Backup/Restore Cert/Key Import Client Cert/Key

GENERATE A NEW CSR/KEY

Key Length: 2048 bit Generate New Key ☒

Certificate Index: 1

Signature Algorithm Index: sha256RSA

Country (2 letter code): US

State/Province: Californis

City/Locality: Milpitas

Organization: ABC Corporation

Organizational Unit: HQ

Organizational Unit: IT

Organizational Unit:

Don't use vhost name as Common Name: ☒

Common Name: *.abc.com

Administrator Email: hao.abc.com

Private Key Exportable: No ☐ Yes ☒

Private Key Password: *****

Confirm Private Key Password: *****

Once the Private Key/Certificate is available for the SSL Virtual Host, we can enable the SSL Virtual Host to process encrypted traffic by the following steps.

3.1.6 Enable the SSL Virtual Host

Login to WebUI, Mode: **Config** -

1. Navigate to **SSL -> Virtual Hosts** and double click the SSL Virtual Hosts. Click on the **Virtual Host Settings** tab and select **Enable SSL** under the **SSL BASIC SETTINGS**. Click **SAVE CHANGE** to enable the SSL Virtual Host.

Mode: ☐ Enable ☒ Config

Home

SYSTEM CONFIGURATION

- General Settings
- Basic Networking
- Advanced Networking
- NAT
- High Availability
- Access Control
- Monitoring

SERVER LOAD BALANCE

- Real Services
- Virtual Services
- Check Lists
- Groups
- Application Setting
- Monitoring

PROXY

- Caching Proxy
- SSL**
- Monitoring

Select SSL Virtual Host: ssl-vhost1 [Back to top menu]

Virtual Host CSR/Cert/Key **Virtual Host Settings** **RESET** **SAVE CH**

Basic Settings **Advanced Settings**

SSL BASIC SETTINGS

Note: You need to generate a CSR or import a certificate and key before enabling SSL.

Enable SSL: ☒

VIEW CERTIFICATE [Mode: Simple ☒ Complete ☐]

Issuer: C=US, ST=CA, L=Milpitas, O=ArrayNetworks Inc., OU=APV Product, CN=www.arraynetworks.net, emailAddress=support@arraynetworks.net

Validity

Not Before: Mar 3 23:34:46 2015 GMT

Not After: May 20 23:34:46 2023 GMT

Subject: C=US, ST=Californis, L=Milpitas, O=ABC Corporation, OU=HQ, OU=IT, CN=*.abc.com, emailAddress=it@abc.com

VIEW INTERMEDIATE CA CERTIFICATE [Mode: Simple ☒ Complete ☐]

Interca is not present for vhost "ssl-vhost1"

VIEW TRUSTED CA CERTIFICATES [Mode: Simple ☒ Complete ☐]

Rootca is not present for vhost "ssl-vhost1"

3.2 Validate Configuration and Service

Validate that the basic configuration is functioning correctly:

1. From WebUI, **SERVER LOAD BALANCE, Monitoring -> Status -> Virtual Service Status**. Select "weblogic" as the virtual service.

2. Verify that the SSL offloading configuration is as intended: HTTPS for the Virtual Service and HTTP for the Real Service.
3. Verify that that all “**Service Status**” icons are green.

Status	Virtual Service Statistics	Group Statistics	Real Service Statistics	Persistence Session Table	Summary	Report
Virtual Service Status	HTTP Proxy Mode Status					
SLB VIRTUAL SERVICE STATUS						
Please select a virtual service: <input type="text" value="weblogic-https"/>						
Virtual Service Name		Related Groups		Related Real Services		
✔ weblogic-https		✔ g-weblogic		✔ WLWS01		
				✔ WLWS02		

4 Configure the APV Series for WebLogic SSL Inside

For SSL Inside configuration, the SLB Virtual Service is HTTP (port 80) and the WebLogic Servers (SLB Real Services) are HTTPS (port 7002, which is the default HTTPS port for WebLogic Web Server).

The APV appliance utilizes SSL session multiplexing to reuse existing SSL sessions with the real services, thus avoiding CPU-intensive key exchange (full handshake) operations. This reduces the overall number of SSL sessions on the WebLogic server, and therefore accelerates SSL transactions while maintaining secured access to the WebLogic server. This also serves as the basis for SSL Bridging (see next section).

4.1 Configuration Steps

4.1.1 Create the WebLogic (HTTPS) Real Services

Login to WebUI and set Mode: **Config**.

1. Navigate to **Real Services** -> **Add**; the **ADD REAL SERVICE ENTRY** screen opens.
2. Enter a unique name for the Real Service name (**WLWS01-HTTPS**); select HTTPS for the Real Service Type. Enter the IP and Port (7002) used by the WebLogic Server(s). Select HTTPS for the Health Check Type. Click **Save & Add Another** until the last Real Service is entered, then click **Save**.

The screenshot shows the WebLogic configuration interface. On the left is a sidebar with a navigation menu. The 'Mode' is set to 'Config'. The sidebar menu includes 'Home', 'SYSTEM CONFIGURATION' (General Settings, Basic Networking, Advanced Networking, NAT, High Availability, Access Control, Monitoring), 'SERVER LOAD BALANCE' (Real Services, Virtual Services, Check Lists, Groups, Application Setting, Monitoring), and 'PROXY' (Caching Proxy, SSL). The main content area has two tabs: 'Real Services' and 'Health Check Setting'. The 'ADD REAL SERVICE ENTRY' form is displayed under the 'Real Services' tab. It includes a 'REAL SERVICE SETUP' section with fields for Real Service Name (WLWS01-HTTPS), Real Service Type (HTTPS), Real Service IP (10.2.40.171), Real Service Port (7002), Connection Limit (1000), and Max Connections Per Second (0). There is also a 'HEALTH CHECK SETUP' section with fields for Health Check Type (https), Health Up Limit (3), Health Down Limit (3), Request Index (0 HEAD / HTTP/1.0\r\r), and Response Index (0 200 OK). At the top right of the form are buttons for 'Cancel', 'Save & Add Another', and 'Save'. A checkbox 'Enable this Service' is checked.

3. Follow the same steps as above to add “**WLWS02-HTTPS**” server as a Real Service. The IP address in this example is 10.2.40.72.

Note: the HTTPS Health Check provides an SSL health check for the real service. If the SSL handshake succeeds, the Array appliance will send the pre-defined HTTP request to the real service. If the response from the real service is the same as the expected response, the real service is marked as “up”; otherwise, it is marked as “down”. When

using HTTPS Health Check, users should pre-define HTTP requests and matched responses.

4.1.2 Create the SSL Real Host

Login to WebUI, set Mode: **Config**.

1. Navigate to **SSL -> Real Hosts -> Add**. The **SSL REAL HOST** screen opens.
2. Enter a unique name for the Real Host Name (i.e. **ssl-real1**). Select the WebLogic real service(s) from the pull down of SLB Real Service. Click **Save & Add Another** until all are entered, and click **Save** after the last SLB Real Service has been entered.

Global Settings | Global CRL | Virtual Hosts | Real Hosts | SSL Errors

SSL REAL HOST Cancel | Save & Add Another | Save

Real Host Name:

SLB Real Service: WLWS01-HTTPS
WLWS02-HTTPS

If you can't select, go to Server Load Balancing->Real Services page to add https/tcps real service first.

The **SSL REAL HOSTS** lists all available SSL Real Hosts that are configured on the APV Series, as well as its associated SLB Real Service (the WebLogic Web Server with HTTPS/7002 interface).

Global Settings | Global CRL | Virtual Hosts | Real Hosts | SSL Errors

SSL REAL HOSTS Edit | Delete | Clear Real Host | Add

	Real Host Name	SLB Real Service
1	ssl-real1	rs-weblogic01-https
2	ssl-real1	rs-weblogic02-https

3. Enable the SSL Real Host – go to **SSL -> Real Hosts**. On the **SSL REAL HOSTS** window, double click the SSL Real Host. Then click **Real Host Settings**. The **SSL BASIC SETTINGS** screen open.
4. Under the **Basic Settings** tab, in the **SSL BASIC SETTINGS** section, check the **Enable SSL** box then click “**SAVE CHANGES**” to enable the APV Series to use HTTPS to communicate with WebLogic servers.

Mode: ☐ Enable ☒ Config

Home

SYSTEM CONFIGURATION

- General Settings
- Basic Networking
- Advanced Networking
- NAT
- High Availability
- Access Control
- Monitoring

SERVER LOAD BALANCE

- Real Services
- Virtual Services
- Check Lists
- Groups
- Application Setting
- Monitoring

PROXY

- Caching Proxy
- SSL**
- Monitoring

Select SSL Real Host: ssl-real1 [Back to top menu]

Real Host Cert/Key **Real Host Settings**

Basic Settings **Advanced Settings**

SSL BASIC SETTINGS

Enable SSL: ☒

VIEW CERTIFICATE [Mode: Simple ☒ Complete ☐]

Host "ssl-real1" does not have an active certificate

STATISTICS [Clear](#)

SSL Connection Statistics for "ssl-real1"

```

Open SSL connections      : 0
Accepted SSL connections  : 0
Requested SSL connections : 0
5 minutes requested rate  : 0 connections/sec

```

SSL Session Statistics for "ssl-real1"

```

Resumed SSL sessions      : 0
Resumable SSL sessions    : 0
Session Misses            : 0

```

- The same SSL Real Host can be associated with multiple backend services. If backend servers have different SSL requirements, different SSL Real Host can be configured to accommodate the different needs.
- If the APV SSL Real Host simulates an SSL/TLS client, the SSL Certificate/Private key is an option. If the real service requires a client certificate (two ways, which is quite normal for machine-to-machine), the APV SSL Real Host can import/associate a Client Certificate and Private Key. The imported client certificate must be encoded by DER rules during client authentication.
- The APV Series' SSL Real Host will validate the Real Service server certificate. If the server certificate is invalid per the APV, the SSL/TLS handshake will fail. For example, if the issuer of the certificate is unknown. In order to be a Trusted Certificate Authority, import the issuer certificate (root/intermediate CAs) to the APV appliance. Alternatively, you can disable the server certificate check. See section 6.4 How to Disable Server Certificate Verification.

Once the WebLogic real services are added, all SLB Real Services should be on the real service list with their status. To check this, just click **Real Services** from sidebar from WebUI. For Real Service Status, green means the Real Service is available (this is updated by the APV health check); red means it is unavailable. The APV Series SLB will not select unavailable server(s) to send client traffic to for application service.

Mode: ☐ Enable ☒ Config

Home

SYSTEM CONFIGURATION

- General Settings
- Basic Networking
- Advanced Networking
- NAT
- High Availability
- Access Control
- Monitoring

SERVER LOAD BALANCE

- Real Services**

Real Services **Health Check Setting**

SLB REAL SERVICES CONFIGURATION [Enable](#) | [Disable](#) | [Delete](#) | [Add](#)

	Real Service Name	Real Service Type	Real Service IP	Real Service Port	Real Service Status
1	WLWS01	http	10.2.40.171	7001	✓
2	WLWS02	http	10.2.40.172	7001	✓
3	WLWS01-HTTPS	https	10.2.40.171	7002	✓
4	WLWS02-HTTPS	https	10.2.40.172	7002	✓

After the SLB Real Services are configured, we can proceed to add the SLB Group, configure the SLB Group Method, assign member(s) and set various parameters as needed.

4.1.3 Create the WebLogic (HTTPS) Group

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

1. Select **Groups** from side bar to access the **ADD GROUP** configuration page.
2. Input a unique name for the Group Name; in the example, we used “**g-weblogic-https**”. 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. Enter “**1**” for the Path Flag. After making configurations on those parameter fields, click on the action link “**Add**” to create the SLB group. The newly created SLB Group will be displayed on the **GROUPS LIST**.

ADD GROUP		
Group Name:	g-weblogic-https	
Group Method:	Insert Cookie	
Cookie Name:	WebLogic-ServerID	
First Choice:	Least Connections	
Path Flag:	1	
Threshold Granularity:	10	
Add		
GROUPS LIST		
Group Name	Group Method	Enabled
1 g-weblogic	ic	<input checked="" type="checkbox"/>
2 g-weblogic-https	ic	<input checked="" type="checkbox"/>
Delete Edit Save		

3. To assign WebLogic Servers (HTTPS) to the SLB Group, choose “**g-weblogic-https**” under the **GROUPS LIST** by double clicking on it or selecting it and clicking on the action link “**Edit**”. The **GROUP INFORMATION** configuration page will be displayed. Go to the **GROUP MEMBERS** section, and click **Add**. Then select the WebLogic HTTPS real services to add to the group.

ADD GROUP MEMBER	
Group Name:	g-weblogic-https
Eligible Reals:	WLWS01-HTTPS
Weight:	1
Priority:	0
Cancel Save & Add Another Save	

Once you are finished adding real services to the SLB Group, check the **GROUP MEMBERS** to make sure the members are properly displayed.

GROUP MEMBERS						Add Delete Save	
	Real Service Name	Weight	Priority	Active	Reason		
1	WLWS01-HTTPS	1	0	YES			
2	WLWS02-HTTPS	1	0	YES			

4.1.4 Create a WebLogic HTTP SLB Virtual Service

The Virtual Service configured in section 2.1.4 Create the WebLogic Virtual Service (“weblogic”) can be modified to associate with the WebLogic HTTPS SLB group (**g-weblogic-https**) to complete the SSL Inside setup.

To change the Virtual Service to a different SLB Group with “insert cookie” and “default” policies login to WebUI, Mode: **Config**:

1. Navigate to **Virtual Services**; double click the Virtual Service (**weblogic**). The **VIRTUAL SERVICE INFORMATION** screen opens.
2. Under **ASSOCIATE GROUPS**, click the existing group with **Eligible Vlink** or **Eligible Groups** to select it, then click “Delete”. Do this for both the “icookie” and “default” Eligible Policies.
3. Then select the HTTPS Group (**g-weblogic-https**) from the Eligible Groups pull down menu, and “default” form Eligible Policies. Click **Add**.
4. Under the same **ASSOCIATE GROUPS** section, for the same SLB Group **g-weblogic-https**, select “icookie” from Eligible Policies. Enter a unique name for the Policy Name and a priority for Policy Precedence. Click **Add** to complete the SSL Inside Virtual Service configuration.

ASSOCIATE GROUPS						Add Delete	
Virtual Service Or Vlink: weblogic							
Eligible Groups: g-weblogic-https		Eligible Policies: default					
	Eligible Vlink Or Groups	Policy Name	Eligible Policies	Virtual	Attribute	Value	
1	g-weblogic-https	weblogic-icookie	icookie	weblog			
2	g-weblogic-https		default	weblog			

4.2 Validate Configuration and Service

Validate that the basic configuration is functioning correctly:

1. From the WebUI, **SERVER LOAD BALANCE, Monitoring -> Status -> Virtual Service Status**, select “weblogic” as the virtual service.
2. Verify that the SSL Inside configuration is as intended: HTTP for the Virtual Service and HTTPS for the Real Service.
3. Verify that all “**Service Status**” icons are green.

Status	Virtual Service Statistics	Group Statistics	Real Service Statistics	Persistence Session Table	Summary	Report
Virtual Service Status		HTTP Proxy Mode Status				
SLB VIRTUAL SERVICE STATUS						
Please select a virtual service: <input type="text" value="weblogic"/>						
Virtual Service Name		Related Groups		Related Real Services		
✓ weblogic		✓ g-weblogic-https		✓ WLWS01-HTTPS		
				✓ WLWS02-HTTPS		

Note: If your certificates of **SSL REAL HOSTS** are self-signed, you should disable **Enable Server Certificate Verification**, see 6.4 How To Disable Server Certificate Verification.

5 Configure the APV Series for WebLogic SSL Bridging

For SSL Bridging, the SLB Virtual Service is HTTPS (port 443) and the WebLogic Servers (SLB Real Services, port 7002) is configured with HTTPS.

To do so, we need to configure the WebLogic Web Server with HTTPS and default port 7002.

5.1 Configuration Steps

5.1.1 Create the WebLogic (HTTPS) Real Services

For the WebLogic servers, **WLWS01-HTTPS** and **WLWS02-HTTPS** can be used to support SSL Bridging. Please refer to section 4.1.1 for the configuration steps. Also, make sure SSL Real Host is configured as well.

After the SLB Real Service is configured and SSL Real Host is enabled, we can proceed to create the SLB Group, configure the SLB method, assign member(s) and set up various parameters as needed.

5.1.2 Create the WebLogic (HTTPS) Group,

The WebLogic HTTPS Group, **g-weblogic-https**, can be used to support SSL Bridging. Please see section 4.1.2 for detailed setup steps.

5.1.3 Create the WebLogic (HTTPS) Virtual Services

The WebLogic Virtual Service **weblogic-https** configured earlier for SSL Offloading can be used to support SSL Bridging as the Virtual Service. Please refer to section 3.1.3 for detailed HTTPS Virtual Service and SSL Virtual Host configuration steps.

To change the Group, login to WebUI, Mode: **Config**:

1. Select “**Virtual Services**” from the sidebar. Double click the Virtual Service (**weblogic-https**) to select it. The **VIRTUAL SERVICE INFORMATION** screen opens.
2. Under **ASSOCIATE GROUPS**, click the existing group (**g-weblogic**) with **Eligible Vlink** or **Eligible Groups** to select it and click “**Delete**”. Do this for both “**icookie**” and “**default**” Eligible Policies.
3. Then select the HTTPS Group (**g-weblogic-https**) from the Eligible Groups pull down menu, and “**default**” form Eligible Policies. Click **Add**.
4. Under the same **ASSOCIATE GROUPS** section, for the same SLB Group **g-weblogic-https**, select “**icookie**” from Eligible Policies. Enter a unique name for the Policy Name and a priority for Policy Precedence. Click **Add** to complete the SSL Bridge Virtual Service configuration.

ASSOCIATE GROUPS Add | Delete

Virtual Service Or VLink: weblogic-https

Eligible Groups: g-weblogic-https Eligible Policies: default

	Eligible VLink Or Groups	Policy Name	Eligible Policies	Virtual
1	g-weblogic-https	weblogic-ic	icookie	weblog
2	g-weblogic-https		default	weblog

Attribute	Value
Groups	g-weblogic-https
Policy Name	weblogic-ic
Policy	icookie
Associated Group	g-weblogic-https

5.2 Validate the Configuration and Service

Validate that the basic configuration is functioning correctly:

1. From WebUI, **SERVER LOAD BALANCE, Monitoring -> Status -> Virtual Service Status**, select “**weblogic-https**” as the virtual service.
2. Verify that the SSL Bridge configuration is as intended: HTTPS for the Virtual Service and HTTPS for the Real Service.
3. Verify that all “**Service Status**” icons are green.

Status Virtual Service Statistics Group Statistics Real Service Statistics Persistence Session Table Summary Report

Virtual Service Status HTTP Proxy Mode Status

SLB VIRTUAL SERVICE STATUS

Please select a virtual service: weblogic-https

Virtual Service Name	Related Groups	Related Real Services
✔ weblogic-https	✔ g-weblogic-https	✔ WLWS01-HTTPS
		✔ WLWS02-HTTPS

6 Configure Other APV Series Features for WebLogic

6.1 HTTP Rewrite/Redirect

For SSL Offloading, we provide only secure HTTPS access to the WebLogic servers. However, the client may inadvertently type `http://...`(unsecured) rather than `https://...` to access the secured WebLogic service. Rather than waiting for timeout, to make this more user friendly, the APV appliance can be configured to auto redirect http requests to https.

To configure the HTTP to HTTPS redirection:

1. Add a new Virtual Service "**weblogic**" for HTTP and virtual service port "**80**" with the same IP address for the HTTPS Virtual Service (port 443).
2. Select the "**weblogic**" Virtual Service on the **VIRTUAL SERVICES LIST** by double clicking on it or clicking on it and selecting the action link "**Edit**". The **VIRTUAL SERVICE INFORMATION** configuration page will open and present a new series of tabs for completing the virtual services configuration.
3. Select the virtual service "**weblogic**" to edit.
4. Check the box for "Redirect ALL HTTP Requests to HTTPS"

The screenshot shows the 'VIRTUAL SERVICE INFORMATION' configuration page for a virtual service named 'weblogic'. The page has a top navigation bar with tabs: 'Virtual Service Settings' (selected), 'Virtual Service Statistics', 'URL Rewrite', 'URL Filter', 'HTTP Forwarding', 'TCP Option', 'ePolicy', and 'HTTP Error Redirect'. The 'VIRTUAL SERVICE INFORMATION' section contains fields for 'Virtual Service Name' (weblogic), 'Virtual Service Type' (HTTP), 'Virtual Service IP' (10.1.1.199), 'Virtual Service Port' (80), 'Enable ARP' (checked), and 'Connection Limit' (0). Below this is a note: '* Note: Change virtual service parameter will delete all original configuration of this virtual service: policy, URL rewrite, URL filter etc.' The 'VIRTUAL SERVICE SETTING' section contains various options: 'TCP Timeout' (empty), 'Proxy Config Mode' (Full selected, Auto unselected), 'Redirect All HTTP Requests to HTTPS' (checkbox, highlighted with an orange box), 'Enable OWA Support' (checkbox), 'Additional HTTP Request Headers' (empty), 'HTTP Client IP Headers' (empty), 'Remove Port From Location Header' (checkbox), 'Rewrite Redirections From Backend to Use HTTPS' (checkbox), 'Enable X-Forwarded-For for this service' (checked), 'Regex case mode' (insensitive unselected, sensitive unselected, use global mode selected), 'Mode' (Use System Mode selected, Operate as Transparent Proxy unselected, Operate as Reverse Proxy unselected), 'Enable this Service' (checked), 'Enable Cache' (checked), 'Add "secure" Keyword to Set-Cookie Headers for HTTPS Virtuals' (checked), 'Add "secure" Keyword to Inserted Set-Cookie Headers for HTTPS Virtuals' (checked), and 'Max Connections Per Second' (0).

6.2 How to Insert a WL-Proxy-SSL Header

For SSL Offloading, the **WL-Proxy-SSL** header can be checked by WebLogic Web applications and thus confirm the client is connected over SSL (secured connection). To insert the custom header:

Login to WebUI, Mode: **Config**.

1. Select **Virtual Services** from the sidebar; double click “**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**.

The screenshot shows the 'VIRTUAL SERVICE SETTING' configuration page. The 'Additional HTTP Request Headers' field is highlighted with an orange box and contains the text 'WL-Proxy-SSL:true %n'. Other visible settings include: TCP Timeout, Proxy Config Mode (Full/Auto), Enable OWA Support, Remove Port From Location Header, Rewrite Redirections From Backend to Use HTTPS, Enable X-Forwarded-For for this service, RegEx case mode (insensitive/sensitive/use global mode), Mode (Use System/Operate as Transparent/Operate as Reverse Proxy), and Enable this Service (checked).

6.3 Advanced SSL Virtual Host Settings – Disable SSLv3

The APV Series' SSL Virtual Host has many options. In particular, SSLv3 has many known vulnerabilities, so if backward compatibility is not required, we suggest disabling it.

To disable SSLv3, login to WebUI, Mode: **Config**:

1. Navigate to **SSL -> Virtual Hosts** and double click SSL Virtual Hosts to select it.
2. Go to **Virtual Host Settings -> Advanced Settings**. The **SSL ADVANCED SETTINGS** screen opens.
3. For **CIPHER SUITES**, disable **EXP-DES-CBC-SHA** and **EXP-RC4-MD5**, both of which are only supported by SSL3.0.
4. Uncheck SSLv3.0, and click **SAVE CHANGES** to store the change.

Select SSL Virtual Host: ssl-vhost1 [\[Back to top menu\]](#)

Virtual Host CSR/Cert/Key **Virtual Host Settings** RESET SAVE CHANGES

Basic Settings **Advanced Settings**

SSL ADVANCED SETTINGS

SSL Versions: SSLv3.0: ☐ TLsv1.0: ☒ TLsv1.2: ☐

Enable Session Reuse: ☒

Enable SSL Renegotiation: ☐

CLIENT AUTHENTICATION

Enable Client Authentication: ☐

Note:
You need to import the trusted CA certificate to enable client authentication.

CIPHER STRENGTH REDIRECTION Apply

Minimum Acceptable Cipher Strength: 40 bits

Redirect URL:

CIPHER SUITES

Disabled Cipher Suites:

- AES128-SHA256
- AES256-SHA256
- EXP-RC4-MD5
- EXP-DES-CBC-SHA

Enabled Cipher Suites:

- RC4-MD5
- RC4-SHA
- DES-CBC3-SHA
- DES-CBC-SHA
- AES128-SHA
- AES256-SHA

>> <<

Move Up Move Down

6.4 How to Disable Server Certificate Verification.

For the SSL Inside configuration, the APV appliance works similar to a client browser. The APV Series has a list of known, trusted CA certificates/public keys that are used to verify real service (application server) certificates' authenticity. If the APV Series cannot identify the issuing CA for the server certificate from the APV's trusted CAs, communication with the real service will fail. If the server certificate is self-signed for quick testing, we can disable the SSL server certificate check on the APV system so that communication with the real service will not fail.

To disable the server certificate verification, from WebUI, Mode: **Config**:

1. Navigate to **SSL**; the **SSL GLOBAL SETTINGS** screen opens.
2. Uncheck the box for **Enable Server Certificate Verification**.
3. Click **SAVE CHANGES**.

Global Settings **Global CRL** **Virtual Hosts** **Real Hosts** **SSL Errors** RESET SAVE CHANGES

SSL GLOBAL SETTINGS

Ignore close_notify Alert Messages: ☒

Enable Sending close_notify Alert Messages: ☒

Enable Server Certificate Verification: ☐

Enable SSL Renegotiation: ☐

Enable Memory CRL Support: ☐

Session Cache Idle Timeout: 43200 (60-86400 Seconds)

6.5 HTTP Compression

The APV appliance supports in-line/dynamic compression of HTTP objects, which reduces bandwidth use and speeds up application delivery. Following are the steps for the basic setup.

From WebUI, Mode: **Config**:

1. Click Compression to open the HTTP COMPRESSION SETTING screen.
2. Check the box Enable Compression to enable global compression. By default, all HTTP/HTTPS Virtual Services are enabled with HTTP compression. Individual Virtual Services can be selected and disabled.

Mode: ☐ Enable ☒ Config

Home

SYSTEM CONFIGURATION

- General Settings
- Basic Networking
- Advanced Networking
- NAT
- High Availability
- Access Control
- Monitoring

SERVER LOAD BALANCE

- Real Services
- Virtual Services
- Check Lists
- Groups
- Application Setting
- Monitoring

PROXY

- Compression
- Caching Proxy

Compression Setting | **Compression Type** | Compression Statistics

HTTP COMPRESSION SETTING [Enable VS Compression](#) [Disable VS Compression](#)

Enable Compression: ☒

HTTP/HTTPS Virtual Service(s): ps-ent-http

COMPRESSION IS ENABLED FOR THE FOLLOWING HTTP/HTTPS VIRTUAL SERVICES

	Virtual Service
1	weblogic-https
2	weblogic
3	ps-ent-https
4	ps-ent-http

Note: By default, the following MIME types are compressed by the APV Series for all browsers (User-Agent):

- Text (text/plain)
- HTML (text/HTML)
- XML (text/XML)

Due to compatibility issues, not all MIME types are supported on all browsers. Therefore, the APV appliance allows configuration of additional User Agent/MIME types to be compressed for more effective compression use.

3. Click the Compression Type tab. The COMPRESSION MIME TYPES screen opens.
4. Click **Apply Tested User Agents**; more compression types added.
5. For each **Add MIME Type**, enter **Mozilla** for the User Agent and add “JS”, “CSS”, and “PDF” to complete.

Compression Setting

Compression Type

Compression Statistics

COMPRESSION MIME TYPES

Add MIME Type|Delete MIME Type|Apply Tested User Agents

User Agent:

MIME Types:

JS (JavaScript)

CSS (Cascading Style Sheet)

PDF (Portable Document Format)

DOC (Microsoft Word Document)

PPT (Microsoft Powerpoint Slide)

XLS (Microsoft Excel Table)

SUPPORTED C

	User A		
1	Mozilla		
2	Mozilla	js	
3	Mozilla	pdf	
4	Mozilla/5.0	css	
5	Mozilla/5.0	js	
6	MSIE 6	css	
7	MSIE 6	js	
8	MSIE 7.0	css	
9	MSIE 7.0	js	
10	MSIE 9.0	css	

Note: For compression statistics, from WebUI go to **Compression => Compression Statistics**.

Note: In some cases, certain HTTP objects have an issue with compression. To exclude particular HTTP object(s) from compression, go to **Compression => Compression Setting**, and add the URL to the **URL EXCLUDE LIST**.

7. Conclusion

This concludes the Array Networks APV deployment guide for Oracle WebLogic Web Server. Array Networks APV Series application delivery controllers provide Layer 7 server load balancing, high availability, SSL acceleration and offloading, DDoS protection, and TCP connection multiplexing, caching and compression to improve the performance, scalability, availability and security for WebLogic server deployments.

Appendix: CLI Configuration Lab Example

[Real Services]

```
slb real http "WLWS01" 10.2.40.171 7001 1000 http 3 3
slb real http "WLWS02" 10.2.40.172 7001 1000 http 3 3
slb real https "WLWS01-HTTPS" 10.2.40.171 7002 1000 https 3 3
slb real https "WLWS02-HTTPS" 10.2.40.172 7002 1000 https 3 3
```

[Group information]

```
slb group method "gp-weblogic" ic "WebLogic-ServerID" 1 lc 10
slb group member "gp-weblogic" "WLWS01"
slb group member "gp-weblogic" "WLWS02"

slb group method "gp-weblogic-https" ic "WebLogic-ServerID" 1 lc 10
slb group member "gp-weblogic-https" "WLWS01-HTTPS"
slb group member "gp-weblogic-https" "WLWS02-HTTPS"
```

[Virtual Services]

```
slb virtual http "vs-weblogic" 10.1.1.11 80 arp 0
slb virtual https "vs-weblogic-https" 10.1.1.11 443 arp 0
```

[Regular SLB]

```
slb policy icookie "ic-policy1" "vs-weblogic" "gp-weblogic" 11
slb policy default "vs-weblogic" "gp-weblogic"
```

[SSL Offload]

```
slb policy icookie "ic-policy2" "vs-weblogic-https" "gp-weblogic" 12
slb policy default "vs-weblogic-https" "gp-weblogic"
```

[SSL Inside]

```
slb policy icookie "ic-policy2" "vs-weblogic-https" "gp-weblogic" 13
slb policy default "vs-weblogic-https" "gp-weblogic"
```

[SSL Bridge]

```
slb policy icookie "ic-policy3" "vs-weblogic-https" "gp-weblogic-https" 14
slb policy default "vs-weblogic-https" "gp-weblogic-https"
```

[SSL Configuration Information]

```
ssl host real "ssl-real1"
ssl host virtual "ssl-vhost1"
```

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
+81-44-589-8315

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