Deployment Guide
May-2015 rev. A

Deploying Array Networks APV Series Application Delivery Controllers with Microsoft Exchange 2013

1 Introduction

This document is written with the assumption that you are familiar with Microsoft Exchange products and the Array APV/vAPV appliances' basic WebUI interface.

1.1 Microsoft Exchange 2013

For Microsoft Exchange 2013, changes from Exchange 2010 are far less complex than previous releases; however, there have been major architectural changes to the Exchange server roles. Instead of five server roles, in Exchange 2013 the number of server roles has been reduced to two:

- **Client Access Server (CAS)**
  The CAS provides authentication, limited redirection, and proxy services (for the specific Mailbox server when the client accesses it). The CAS offers all the usual client access protocols: HTTP, POP and IMAP, and SMTP.
- **Mailbox server**
  The Mailbox server includes all of the traditional server components: the Client Access protocols, Transport service, Mailbox databases, and Unified Messaging. The Mailbox server handles all activity for the active mailboxes on that server.

In addition, for Exchange 2013 there are several notable changes to load balancing:

- Only CAS needs to be load balanced
- Client session server affinity is no longer required
- Outlook connectivity now uses RPC over HTTP/HTTPS, meaning that L7 processing is more useful when SSL offloading is used (though L4 load balancing is still used in non-SSL offloading deployments).

To understand the new features of Exchange 2013, refer to the following URL:

http://technet.microsoft.com/en-us/library/jj150540%28v=exchg.150%29.aspx

SSL offloading is supported after Exchange 2013 SP1. To configure SSL offloading in Exchange 2013, please refer to the following link:

http://technet.microsoft.com/en-us/library/dn635115%28v=exchg.150%29.aspx

For SSL offloading, we assume the SSL Certificate and Key are available.

1.2 Deployment Overview and Prerequisites

There are multiple ways to deploy APV Series application delivery controllers with Exchange 2013, such full reverse proxy, transparent, direct return, SSL offloading, etc. We recommend using reverse proxy mode, and SSL offload as an option.

In this example, two servers are used. Each server hosts the CAS and Mailbox roles in a Database Availability Group (DAG) configuration. This provides high availability and uses a minimum number of Exchange Servers.

Clients then connect to the Virtual IPs (VIPs) on the APV Series appliance rather than connecting directly to one of the CAS servers. These connections are then load balanced across the CAS servers to distribute the load according to the load-balancing algorithm selected on the APV Series.

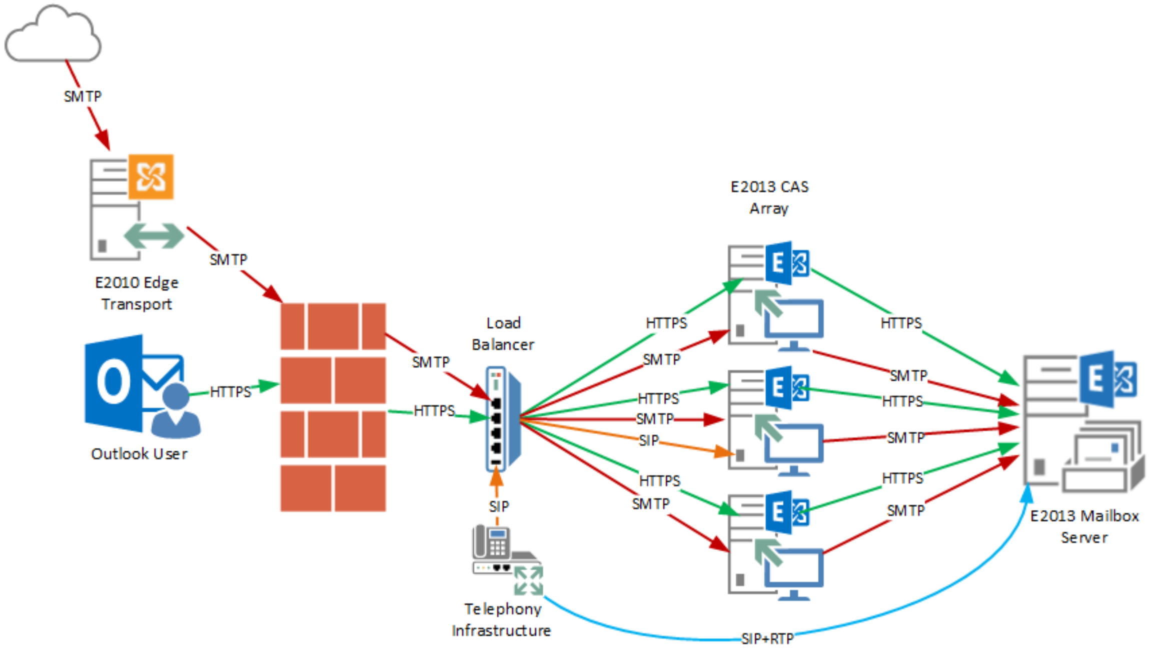


Figure 1: Basic Load Balancer Configuration for Exchange 2013

The APV or vAPV load balancer is running version ArrayOS™ 8.x or later. For more Information on deploying the APV/vAPV appliance, please refer to the ArrayOS APV Application Guide and CLI Guide that are included in the ArrayOS 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.

1.2.1 APV SSL Offloading/Acceleration

Each APV Series appliance (including vAPV with software SSL) comes with SSL enabled to support SSL offloading for the backend servers. This simplifies certificate/key management, reduces server load, and accelerates SSL with high-performance hardware. Following are typical ways to use the APV Series' SSL functions:

1. SSL Offloading

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

2. SSL Inside

In this scenario, the APV Series accepts unencrypted client traffic and then encrypts it before sending it to the servers. While more uncommon than offloading or bridging, this can be useful for organizations that require all traffic behind the system (or through the open network) to be encrypted. In this case, the APV Series is acting as an SSL client, so there is no need for it to store the SSL certificate and keys. (The Exchange Servers will need to store the certificates and keys. However, the APV Series will expect a valid certificate from the Exchange Servers.)

3. SSL Bridging (Offload + 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 system and the Exchange Servers.

1.3 APV Series Application Delivery Controller Benefits

The APV Series application delivery controllers provide all required application delivery functions for optimizing application delivery for Exchange environments, such as Layer 4 server load balancing, high availability, Layer 7 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 Series' server load balancing ensures 99.999% uptime for Exchange Mail Application deployments. Customers can scale their Exchange Mail environment to meet capacity and performance needs with APV server load balancers.

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.

ISP Link Availability

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

TCP Connection Multiplexing

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

Content Cache

The APV Series appliance serves frequently requested content from cache for increased performance, and to help scale the capacity of the Exchange CAS Server environment.

HTTP Compression

The APV Series appliance compresses and delivers Exchange Mail traffic over LAN and WAN networks.

Network and Server Protection

The APV Series appliance’s reverse proxy architecture protects the Exchange CAS Servers from malicious network and server attacks such as DDoS attacks, SYN floods, TCP port scans, UDP floods and UDP port scans, etc.

2 Configure L4 Load Balancing for Exchange

For Exchange 2013 L4 Load Balancing, all Exchange 2013 traffic is directed to Virtual Services that use the same VIP and different TCP ports. The port numbers are mapped to all of the Exchange 2013 mail services.

2.1 Configuration Steps

Be sure that the APV/vAPV system is accessible from the network and WebUI is enabled. To access the APV system 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 Array Networks pilot login, the default is no enable password. Simply click Login to enter the WebUI.

2.1.1 Define the Application Health Check

For basic L4 load balancing, the APV Series’ built-in TCPS/TCP/ICMP protocol-based health checks can be used to detect CAS availability. No additional configuration is required.

2.1.2 Create the Real Services – L4 CAS

Real Services are the two Exchange Client Access servers (CAS01, CAS02). The CAS is configured with SSL and no SSL offloading from the APV. Following is the summary of all Real Services that need to be added to the APV configuration.

IP	Real Service Name	Protocol	Port	HC Type	Req/Rep
CAS01 (10.2.40.180)	rs_cas01_https	TCP	443	TCP	None
	rs_cas01_smtp	TCP	25	TCP	None
	rs_cas01_smtps	TCP	587	TCP	None
	rs_cas01_pop3s	TCP	995	TCP	None
	rs_cas01_imaps	TCP	993	TCP	None
CAS02 (10.2.40.181)	rs_cas01_https	TCP	443	TCP	None
	rs_cas02_smtp	TCP	25	TCP	None
	rs_cas02_smtps	TCP	587	TCP	None
	rs_cas02_pop3s	TCP	995	TCP	None
	rs_cas02_imaps	TCP	993	TCP	None

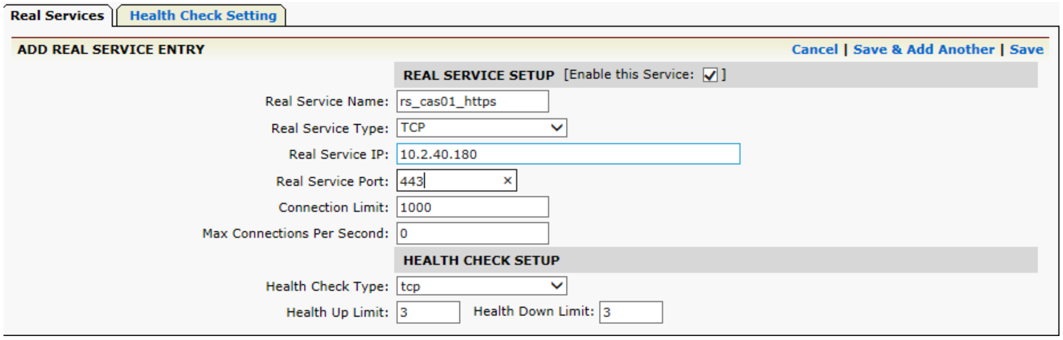
Table 1 - L4 Real Services Configuration

Add each CAS Real Service with the following steps: enter WebUI, **Mode: Config.**

1. Select **Real Services** from the sidebar. **Real Services** *(*tab*)* -> **Add***.* The “**ADD REAL SERVICE ENTRY**” screen opens.

2. The “**ADD REAL SERVICE ENTRY**” screen allows you to configure real services. Enter a unique name for the Real Service Name (**rs_cas01_https**). From the **Real Service Type** pulldown, select “**TCP**”. Enter the Real Service IP/Port (10.2.40.180/443) that are used by the Exchange CAS Server 1.

3. For **HEALTH CHECK SETUP**, from the **Health Check Type** pulldown menu select “**tcp**”. Click **Save & Add Another** to add more Real Services.



ADD REAL SERVICE ENTRY

REAL SERVICE SETUP [Enable this Service: ☑]

Real Service Name: rs_cas01_https
Real Service Type: TCP
Real Service IP: 10.2.40.180
Real Service Port: 443
Connection Limit: 1000
Max Connections Per Second: 0

HEALTH CHECK SETUP

Health Check Type: tcp
Health Up Limit: 3 Health Down Limit: 3

4. Follow the same steps as above: add all Real Services according to Table 1 – L4 CAS Real Services.

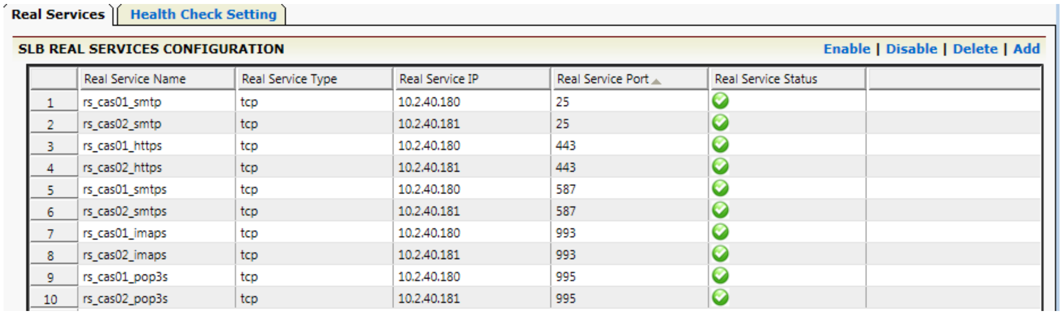
Technical Notes:

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.

Max Connections Per Second: 0
The APV system can rate-limit new TCP connections per second to the backend server. “0” means no limitation.

Once all the Real Services are added, **SLB REAL SERVICES CONFIGURATION** will list all of them.



SLB REAL SERVICES CONFIGURATION

	Real Service Name	Real Service Type	Real Service IP	Real Service Port	Real Service Status
1	rs_cas01_smtp	tcp	10.2.40.180	25	✓
2	rs_cas02_smtp	tcp	10.2.40.181	25	✓
3	rs_cas01_https	tcp	10.2.40.180	443	✓
4	rs_cas02_https	tcp	10.2.40.181	443	✓
5	rs_cas01_smtps	tcp	10.2.40.180	587	✓
6	rs_cas02_smtps	tcp	10.2.40.181	587	✓
7	rs_cas01_imaps	tcp	10.2.40.180	993	✓
8	rs_cas02_imaps	tcp	10.2.40.181	993	✓
9	rs_cas01_pop3s	tcp	10.2.40.180	995	✓
10	rs_cas02_pop3s	tcp	10.2.40.181	995	✓

2.1.3 Create the Group – L4 CAS

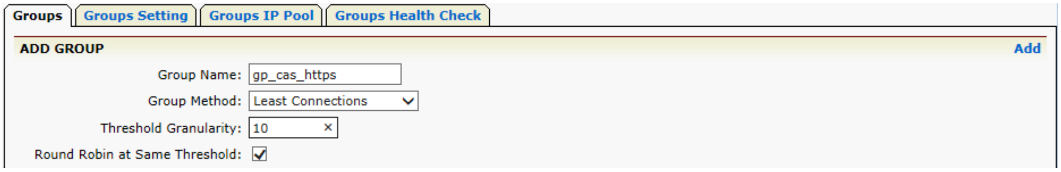
The APV Series’ SLB Group defines the load balancing method and the set of servers in the group. The following Group Table contains all group information that needs to be entered in the APV appliance.

Group Name	Method	Member
gp_cas_https	Least Connection	rs_cas01_https
		rs_cas02_https
gp_cas_smtp	Least Connection	rs_cas01_smtp
		rs_cas02_smtp
gp_cas_smtps	Least Connection	rs_cas01_smtps
		rs_cas02_smtps
gp_cas_pop3s	Least Connection	rs_cas01_pops
		rs_cas02_pops
gp_cas_imaps	Least Connection	rs_cas01_imaps
		rs_cas02_imaps

Table 2 - L4 Groups Configuration

To create an SLB Group, from WebUI, **Mode: Config**:

1. Select **"Groups"** from the sidebar. The **ADD GROUP** screen opens.
2. Enter a unique name for the Group Name; in the example, "**gp_cas_https"**. From the Group Method pulldown menu, select **"Least Connections"**. Click **"Add"** to create the SLB group.



ADD GROUP

Group Name: gp_cas_https

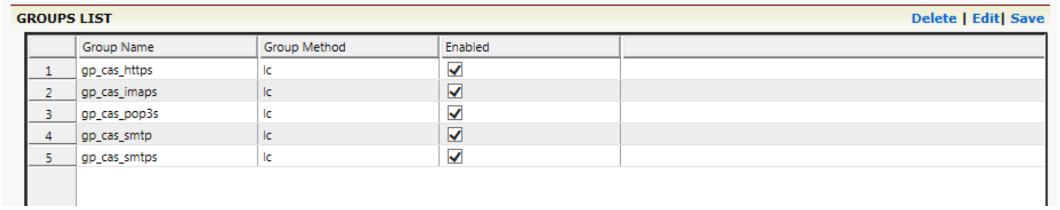
Group Method: Least Connections

Threshold Granularity: 10

Round Robin at Same Threshold: ☑

3. Follow the same steps as above to add all Groups in Table 2 – L4 Groups Configuration.

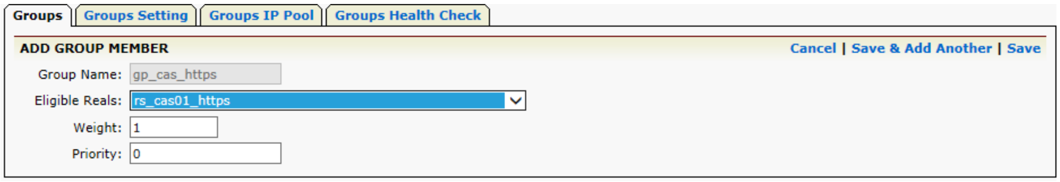
All configured SLB Groups are displayed on the **GROUPS LIST**. The next step is to add group members for each Group.



GROUPS LIST

	Group Name	Group Method	Enabled
1	gp_cas_https	lc	☑
2	gp_cas_imaps	lc	☑
3	gp_cas_pop3s	lc	☑
4	gp_cas_smtp	lc	☑
5	gp_cas_smtps	lc	☑

1. To add Real Services to the SLB group, on the **GROUPS LIST,** double click or select and click on the action link **"Edit"** to select the SLB Group (gp_cas_https). The **GROUP INFORMATION** screen opens.
2. Under the "**GROUP MEMBERS**" section, click "**Add**". The **ADD GROUP MEMBER** configuration screen opens.
3. From the Eligible Reals pulldown menu, select "**rs_cas01_https**". Click **Save & Add Another** and select "**rs_cas02_https**" and "**Save**"**.**



ADD GROUP MEMBER

Group Name: gp_cas_https

Eligible Reals: rs_cas01_https

Weight: 1

Priority: 0

4. Do the same for all of the groups to add members.

2.1.4 Create the SLB Virtual Services – L4 Exchange

The next step is to create the Virtual Services for the Exchange clients to access. On the APV appliance, a Virtual Service is defined by the Virtual IP/Port and the protocol. Because the APV system is operating as a reverse proxy, client connections are terminated at the Virtual Service, and based on the SLB Policy(s) select an SLB Group and per-Group Method to select a Real Service. Then on behalf of the client, the APV Series makes a new connection to the Real Service and splices the traffic between the two connections.

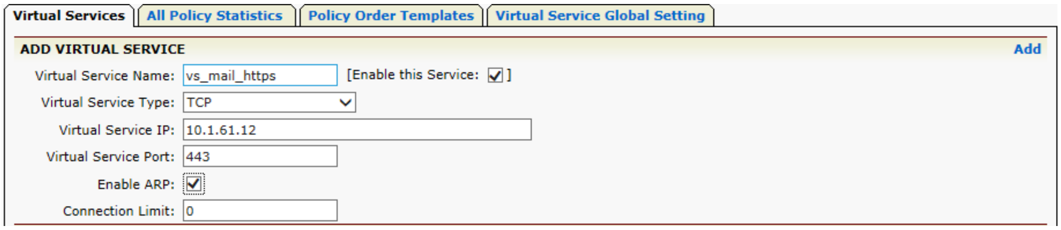
The following table summarizes the L4 SLB Exchange Virtual Services:

Virtual Service	Protocol/ Port	SLB Policy				Group
		Type	Name	String	Rank	
vs_mail_https	tcp/443	default	None	None	None	gp_cas_https
vs_smtp	tcp/25	default	None	None	None	gp_cas_smtp
vs_smtps	tcp/587	default	None	None	None	gp_cas_smtps
vs_pop3s	tcps/995	default	None	None	None	gp_cas_pop3s
vs_imaps	tcps/993	default	None	None	None	gp_cas_imaps

Table 3 - L4 Virtual Services Configuration

To create a new SLB Virtual Service, enter WebUI, **Mode: Config**.

1. From the sidebar, select **Virtual Services**. The "**ADD VIRTUAL SERVICE**" screen opens**.**
2. Enter a unique name for the Virtual Service Name (**vs_mail_https**). Use the check box to enable the virtual service. From the Virtual Service Type pulldown menu, select "**TCP**". Enter the Virtual Service IP and Port (**10.1.61.12/443**). 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.



ADD VIRTUAL SERVICE

Virtual Service Name: vs_mail_https [Enable this Service: ☑]

Virtual Service Type: TCP

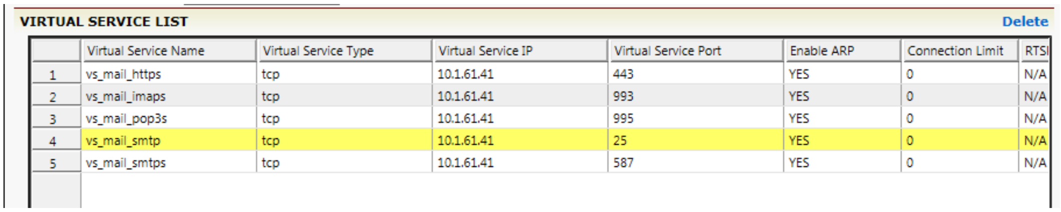
Virtual Service IP: 10.1.61.12

Virtual Service Port: 443

Enable ARP: ☑

Connection Limit: 0

Once a virtual service has been added, it will be on the **VIRTUAL SERVICE LIST**.



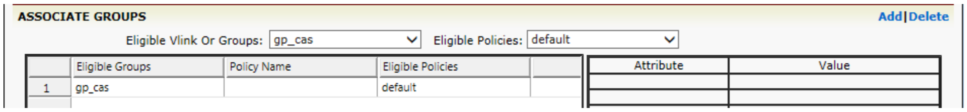
VIRTUAL SERVICE LIST

	Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	Enable ARP	Connection Limit	RTSI
1	vs_mail_https	tcp	10.1.61.41	443	YES	0	N/A
2	vs_mail_imaps	tcp	10.1.61.41	993	YES	0	N/A
3	vs_mail_pop3s	tcp	10.1.61.41	995	YES	0	N/A
4	vs_mail_smtp	tcp	10.1.61.41	25	YES	0	N/A
5	vs_mail_smtps	tcp	10.1.61.41	587	YES	0	N/A

The APV Series appliance uses SLB Policy(s) to link SLB group(s) to a Virtual Service. For the Virtual Service to associate an SLB Group with the “default” policy, please follow these steps:

1. Select the Virtual Service (***va_mail_https***) on the **VIRTUAL SERVICE LIST** by double clicking on it, or clicking it and selecting the action link “**Edit**”. The **VIRTUAL SERVICE INFORMATION** screen opens with a new series of tabs for completing the virtual services configuration.

2. Go down to the **ASSOCIATE GROUPS** section. From the **Eligible vLink or Groups** pulldown menu, select “***gp_cas_https***” and from the **Eligible Policies** pulldown menu, select “***default***”. Click **Add** to complete the Virtual Service configuration.



ASSOCIATE GROUPS

Eligible Vlink Or Groups: gp_cas Eligible Policies: default

	Eligible Groups	Policy Name	Eligible Policies	
1	gp_cas		default	

Attribute	Value

3. Repeat the same steps for all Virtual Services.

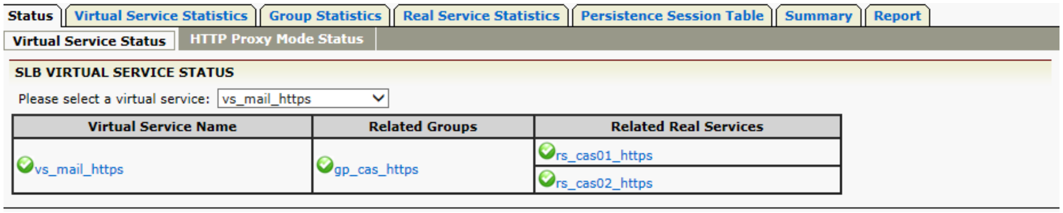
2.2 Validate Configuration and Service

Validate that the basic configuration is functioning correctly:

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

2. Verify that the 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.



SLB VIRTUAL SERVICE STATUS

Please select a virtual service: vs_mail_https

Virtual Service Name	Related Groups	Related Real Services
✓vs_mail_https	✓gp_cas_https	✓rs_cas01_https
		✓rs_cas02_https

4. Launch the Web browser and navigate to the VIP address

5. Input the required Username and Password to login to Exchange 2013.

3 Configure L7 Load Balancing + SSL Offload for Exchange

The Exchange 2013 Client Access Servers are configured with SSL offloading. One of the advantages of SSL offloading is the ability to more easily manage certificates. Rather than having separate SSL certificates for each Client Access Server, a single SSL certificate is imported to the APV appliance.

In addition to SSL certificate management, the Array APV Series appliance can provide SSL acceleration and server load reduction through clear HTTP content, L7-based content routing/rewrite and health checking. In addition, the APV system can offload SSL processing for SMTP, POP3 and IMAP.

3.1 Configuration Steps

To begin, be sure the APV/vAPV Series appliance is accessible from the network and 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 Array Networks pilot login, the default is no enable password. Simply click Login to enter the WebUI.

3.1.1 Define the Application Health Check – per Exchange Protocol

As each CAS HTTP interface supports multiple Exchange protocols, without differential protocols, if any one of the protocols is down it may render the whole CAS down. Per the Microsoft Exchange 2013 Health Probe Checking recommendation (see the following link), Exchange 2013 has a built-in monitoring solution. The APV appliance can take advantage of this to health-check for each protocol.

http://blogs.technet.com/b/exchange/archive/2014/03/05/load-balancing-in-exchange-2013.aspx

Technical Notes:

Exchange 2013 includes a built-in monitoring solution, known as Managed Availability. Managed Availability includes an offline responder. When the offline responder is invoked, the affected protocol (or server) is removed from service. To ensure that load balancers do not route traffic to a Client Access server that Managed Availability has marked as offline, load balancer health probes must be configured to check.

If the load balancer health probe receives a 200 status response, then the protocol is up; if the load balancer receives a different status code, then Managed Availability has marked that protocol instance as 'down' on the Client Access server. As a result, the load balancer should also consider that end point down and remove the Client Access server from the applicable load balancing pool.

The following table shows the Exchange HTTP request URL strings that need to be used for the health check. Also, the APV Series' Health Check Index is used in the example.

Exchange Protocol	Request URL String	Response Code	APV HC Index	
			Req	Rep
OWA	GET /owa/HealthCheck.htm HTTP/1.0 \r\n\r\n	200	10	10
OAB	GET /OAB/HealthCheck.htm HTTP/1.0 \r\n\r\n	200	11	11
RPC	GET /RPC/HealthCheck.htm HTTP/1.0 \r\n\r\n	200	12	12
MAPI	GET /MAPI/HealthCheck.htm HTTP/1.0 \r\n\r\n	200	13	13
EWS	GET /EWS/HealthCheck.htm HTTP/1.0 \r\n\r\n	200	14	14
ECP	GET /ECP/HealthCheck.htm HTTP/1.0 \r\n\r\n	200	15	15
AutoDiscover	GET /Autodiscover/HealthCheck.htm HTTP/1.0 \r\n\r\n	200	16	16
Active Sync	GET /Microsoft-Server-ActiveSync/HealthCheck.htm HTTP/1.0 \r\n\r\n	200	17	17

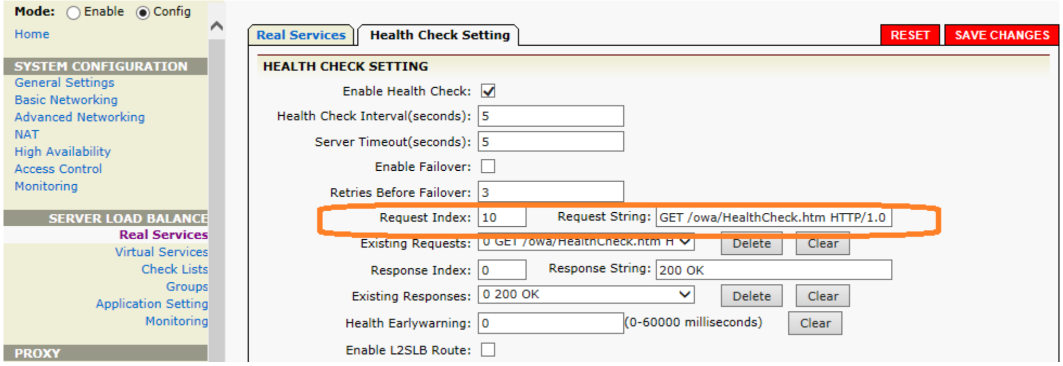
Table 4 - L7 Content Health Check Configuration

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

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

1. From sidebar **SERVER LOAD BALANCE** option, select "**Real Services**" -> "**Health Check Setting**". The **HEALTH CHECK SETTING** screen opens.

2. Enter a number for the **Request Index** (10 for the example) and enter "**GET /owa/HealthCheck.htm HTTP/1.0 \r\n\r\n**" string for the **Request String**. Click **SAVE CHANGES**.



Mode: ○ Enable ● Config

HEALTH CHECK SETTING

Enable Health Check: ☑
Health Check Interval(seconds): 5
Server Timeout(seconds): 5
Enable Failover: □
Retries Before Failover: 3
Request Index: 10 Request String: GET /owa/HealthCheck.htm HTTP/1.0
Existing Requests: 0 GET /owa/HealthCheck.htm H
Response Index: 0 Response String: 200 OK
Existing Responses: 0 200 OK
Health Earlywarning: 0 (0-60000 milliseconds)
Enable L2SLB Route: □

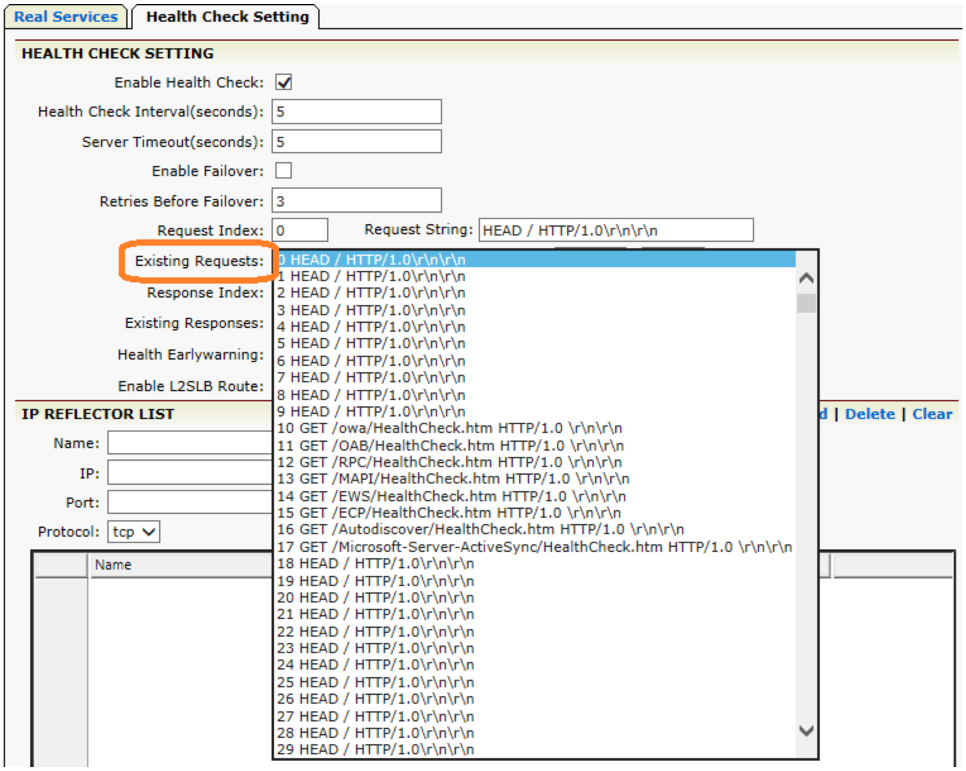
3. Repeat step 2 for all health check settings (for request indexes 11 to 17 on Table 4) to complete this step.

Technical Notes:

- By default, the APV appliance defines an HTTP health table of HTTP requests and HTTP responses to be used by the HTTP health check. The default index inside the health table for HTTP requests and responses is "0, 0". The default request is "HEAD / HTTP/1.0" and the default response is "200 OK".

- You can define your own HTTP requests and the responses to be used by the HTTP health check. For example, you may simply change the request to get a CGI script that returns an HTTP status 200 OK when the database server is “up” and a 404 NOT FOUND when the database server is “down”.
- You may combine any request and response indexes for the health check.

To view the change, from the **HEALTH CHECK SETTING** screen, pull down the **Existing Requests** menu.



HEALTH CHECK SETTING

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:

Response Index:

Existing Responses:

Health Earlywarning:

Enable L2SLB Route:

```
0 HEAD / HTTP/1.0\r\n\r\n
1 HEAD / HTTP/1.0\r\n\r\n
2 HEAD / HTTP/1.0\r\n\r\n
3 HEAD / HTTP/1.0\r\n\r\n
4 HEAD / HTTP/1.0\r\n\r\n
5 HEAD / HTTP/1.0\r\n\r\n
6 HEAD / HTTP/1.0\r\n\r\n
7 HEAD / HTTP/1.0\r\n\r\n
8 HEAD / HTTP/1.0\r\n\r\n
9 HEAD / HTTP/1.0\r\n\r\n
10 GET /owa/HealthCheck.htm HTTP/1.0 \r\n\r\n
11 GET /OAB/HealthCheck.htm HTTP/1.0 \r\n\r\n
12 GET /RPC/HealthCheck.htm HTTP/1.0 \r\n\r\n
13 GET /MAPI/HealthCheck.htm HTTP/1.0 \r\n\r\n
14 GET /EWS/HealthCheck.htm HTTP/1.0 \r\n\r\n
15 GET /ECP/HealthCheck.htm HTTP/1.0 \r\n\r\n
16 GET /Autodiscover/HealthCheck.htm HTTP/1.0 \r\n\r\n
17 GET /Microsoft-Server-ActiveSync/HealthCheck.htm HTTP/1.0 \r\n\r\n
18 HEAD / HTTP/1.0\r\n\r\n
19 HEAD / HTTP/1.0\r\n\r\n
20 HEAD / HTTP/1.0\r\n\r\n
21 HEAD / HTTP/1.0\r\n\r\n
22 HEAD / HTTP/1.0\r\n\r\n
23 HEAD / HTTP/1.0\r\n\r\n
24 HEAD / HTTP/1.0\r\n\r\n
25 HEAD / HTTP/1.0\r\n\r\n
26 HEAD / HTTP/1.0\r\n\r\n
27 HEAD / HTTP/1.0\r\n\r\n
28 HEAD / HTTP/1.0\r\n\r\n
29 HEAD / HTTP/1.0\r\n\r\n
```

IP REFLECTOR LIST

Name:

IP:

Port:

Protocol: tcp

3.1.2 Create the Real Services – L7 CAS with Individual Protocol

For Exchange, multiple ports are used to support different mail protocols, such as SMTP (TCP:25), POP3 (TCP:110), IMAP (TCP:143), and multiple services in addition to HTTP share TCP port 80, such as OWA (Outlook Web Access), Outlook (RPC/MAPI), ActiveSync, etc. Those Exchange services sharing port 80 are independent of each other and may enable/disable, up/down individually. Therefore, to determine the availability of individual services that share port 80, the APV Series needs to define the inner L7 protocols as separate Real Services and use the previously defined application health checks for the respective services.

IP	Real Service Name	Protocol	Port	HC Type	Req/Rep
CAS01 (10.2.40.180)	rs_cas01_owa	HTTP	80	HTTP	10/10
	rs_cas01_oab	HTTP	80	HTTP	11/11
	rs_cas01_rpc	HTTP	80	HTTP	12/12
	rs_cas01_mapi	HTTP	80	HTTP	13/13
	rs_cas01_ews	HTTP	80	HTTP	14/14
	rs_cas01_ecp	HTTP	80	HTTP	15/15
	rs_cas01_autodiscover	HTTP	80	HTTP	16/16
	rs_cas01_ActiveSync	HTTP	80	HTTP	17/17
	rs_cas01_smtp	TCP	25	TCP	None
	rs_cas01_pop3	TCP	110	TCP	None
	rs_cas01_imap	TCP	143	TCP	None
CAS02 (10.2.40.181)	rs_cas02_owa	HTTP	80	HTTP	10/10
	rs_cas02_oab	HTTP	80	HTTP	11/11
	rs_cas02_rpc	HTTP	80	HTTP	12/12
	rs_cas02_mapi	HTTP	80	HTTP	13/13
	rs_cas02_ews	HTTP	80	HTTP	14/14
	rs_cas02_ecp	HTTP	80	HTTP	15/15
	rs_cas02_autodiscover	HTTP	80	HTTP	16/16
	rs_cas02_ActiveSync	HTTP	80	HTTP	17/17
	rs_cas02_smtp	TCP	25	TCP	None
	rs_cas02_pop3	TCP	110	TCP	None
	rs_cas02_imap	TCP	143	TCP	None

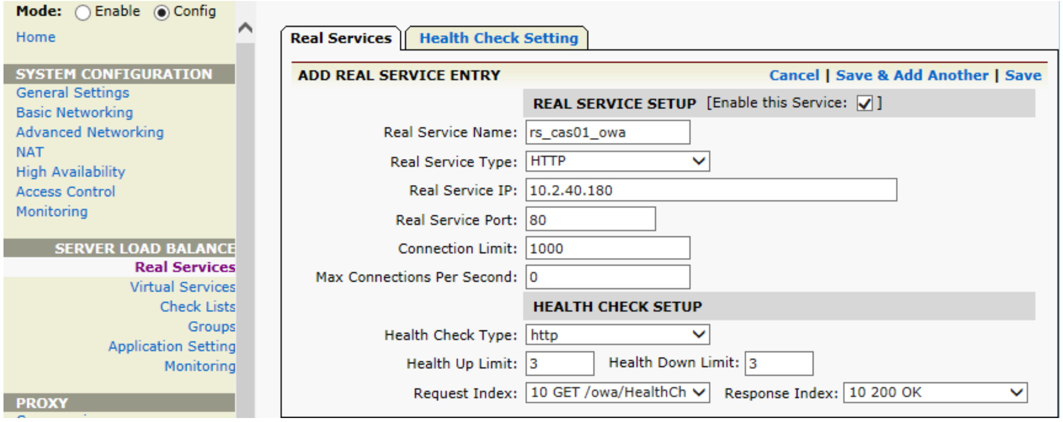
Table 5 - L7 Real Services Configuration

To configure the Real Services, enter WebUI, Mode: **Config**:

1. From the sidebar "**SERVER LOAD BALANCE**" option, select **Real Services** -> **Add**. The **ADD REAL SERVICE ENTRY** screen opens.

2. Enter a unique name for the Real Service name; in our example, we entered "**r_cas01_owa".** Select "**HTTP**" as the Real Service Type, enter IP address "**10.2.40.180**" and port "**80**" which is used by the CAS01 Server.

3. Select **http** as the Health Check Type. For the Request Index and Response Index, pull down the selection and enter corresponding entries from the above table. For OWA health check, we use request Index 10 and Response Index 10, which expects a "200" return code. Click **Save & Add Another** to add more real services.



ADD REAL SERVICE ENTRY

REAL SERVICE SETUP [Enable this Service: ☑]

Real Service Name: rs_cas01_owa
Real Service Type: HTTP
Real Service IP: 10.2.40.180
Real Service Port: 80
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: 10 GET /owa/HealthCh Response Index: 10 200 OK

4. Follow the same steps 2 & 3 to add all Real Services listed on Table 5 to finish the L7 CAS Real Services creation.

3.1.3 Create the Group – L7 CAS

The APV Series' SLB Group defines the load balancing method and the set of servers in the group. Per Microsoft, Exchange 2013 has no persistence requirement, so the "Least Connection" method is used. The following is the L7 Group Table that contains all group information that needs to be entered in the APV appliance.

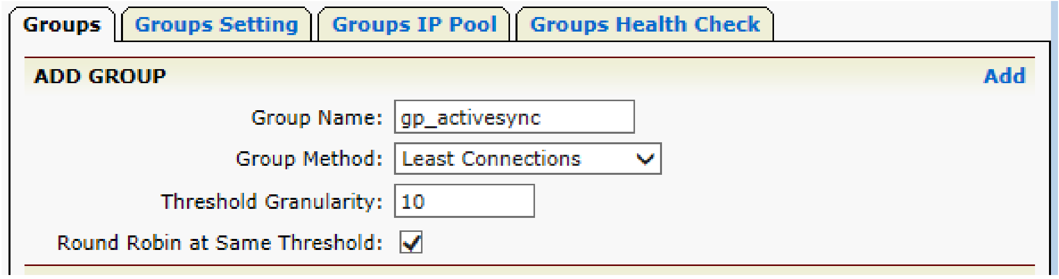
Group Name	Method	Member
gp_activesync	Least Connection	rs_cas01_ActiveSync
		rs_cas02_ActiveSync
gp_autodiscover	Least Connection	rs_cas01_autodiscover
		rs_cas02_autodiscover
gp_ecp	Least Connection	rs_cas01_ecp
		rs_cas02_ecp
gp_ews	Least Connection	rs_cas01_ews
		rs_cas02_ews
gp_imap	Least Connection	rs_cas01_imap
		rs_cas02_imap
gp_mapi	Least Connection	rs_cas01_mapi
		rs_cas02_mapi
gp_oab	Least Connection	rs_cas01_oab
		rs_cas02_oab
gp_owa	Least Connection	rs_cas01_owa
		rs_cas02_owa
gp_pop3	Least Connection	rs_cas01_pop3
		rs_cas02_pop3

gp_rpc	Least Connection	rs_cas01_rpc
		rs_cas02_rpc
gp_smtp	Least Connection	rs_cas01_smtp
		rs_cas02_smtp

Table 6 - L7 Groups Configuration

To add a new SLB Group, enter WebUI, Mode: **Config:**

1. Select **"Groups"** from the sidebar. The **ADD GROUP** screen opens.
2. Input a unique name for Group Name; in the example we used "**gp_activesync**". Select the **"Least Connections"** group method by selecting from the pulldown menu. Click **"Add"** to create the SLB group.



Group Name: gp_activesync

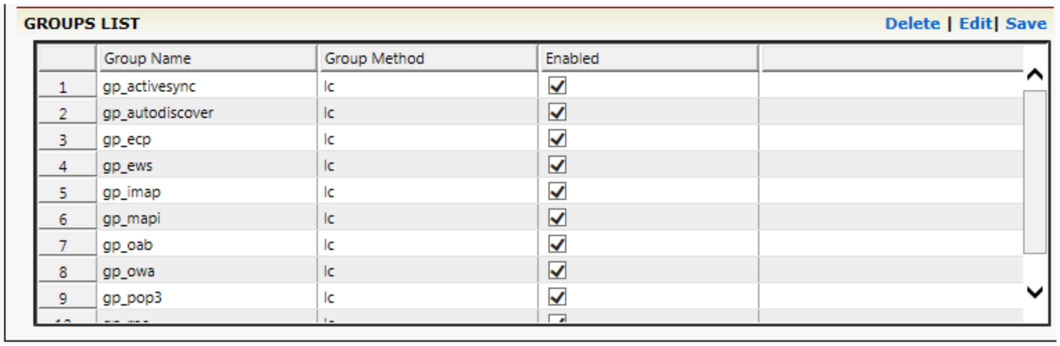
Group Method: Least Connections

Threshold Granularity: 10

Round Robin at Same Threshold: ☑

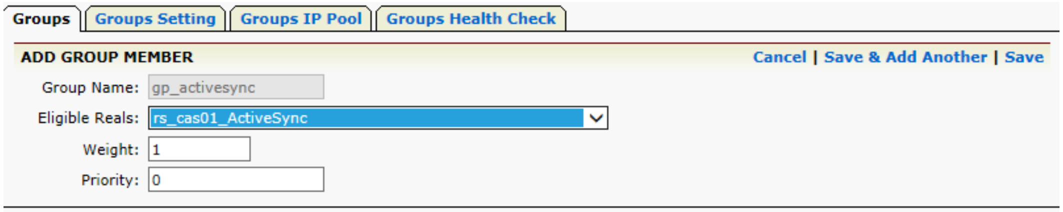
3. Follow the same steps as above to add all Groups listed on Table 6.

All configured SLB Groups are displayed on the **GROUPS LIST**. The next step is to add group members for each Group.



	Group Name	Group Method	Enabled
1	gp_activesync	lc	☑
2	gp_autodiscover	lc	☑
3	gp_ecp	lc	☑
4	gp_ews	lc	☑
5	gp_imap	lc	☑
6	gp_mapi	lc	☑
7	gp_oab	lc	☑
8	gp_owa	lc	☑
9	gp_pop3	lc	☑

4. To add Real Services to the SLB group, access the **GROUPS LIST** by double clicking on it, or selecting it and clicking on the action link **"Edit"** to select the SLB Group (**gp_activesync**). The **GROUP INFORMATION** screen opens.
5. Under the "**GROUP MEMBERS**" section, click on "**Add**". The **ADD GROUP MEMBER** configuration screen opens.
6. From the Eligible Reals pulldown menu; select "**rs_cas01_ActiveSync**", click **Save & Add Another** and select "**rs_cas02_ActiveSync**" and "**Save**".



ADD GROUP MEMBER

Group Name: gp_activesync

Eligible Reals: rs_cas01_ActiveSync

Weight: 1

Priority: 0

7. Follow Table 6; repeat step 4, 5, and 6 to add members to each group.

3.1.4 Create the Virtual Service – L7 Exchange with SSL offload + QoS URL

The next step is to create the HTTPS-based Exchange Virtual Service for SSL offloading. Also to add the “qos url” L7 SLB Policy to route client HTTPS access to different Groups (Exchange services) based on the URL request string (similar to the content-based health check).

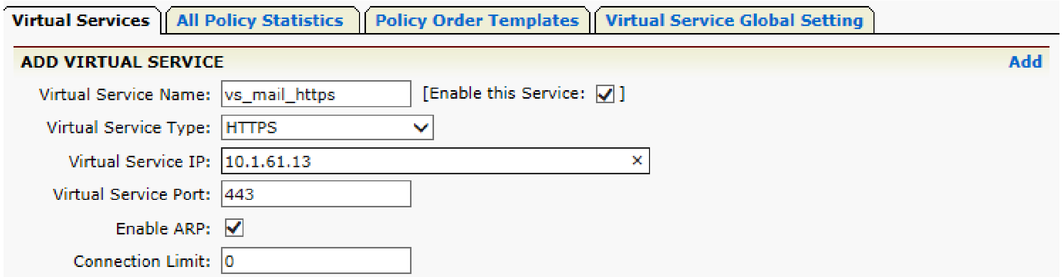
Virtual Service	Protocol/ Port	SLB Policy				Group
		Type	Name	String	Rank	
vs-mail-https	https/443	qos_url	p_owa	/owa	100	gp_owa
			p_oab	/oab	110	gp_oab
			p_rpc	/rpc	120	gp_rpc
			p_mapi	/mapi	130	gp_mapi
			p_ews	/ews	140	gp_ews
			p_ecp	/ecp	150	gp_ecp
			p_autodiscover	/autodiscover	160	gp_autodiscover
			p_activesync	/Microsoft-Server-ActiveSync	170	gp_activesync
vs_smtp	tcp/25	default	None	None	None	gp_cas_smtp
vs_smtps	tcps/587	default	None	None	None	gp_cas_smtp
vs_pop3s	tcps/995	default	None	None	None	gp_cas_pop3
vs_imaps	tcps/993	default	None	None	None	gp_cas_imap

Table 7 - L7 Virtual Service Configuration

Following are the steps to create the Exchange HTTPS Virtual Service. From WebUI Mode: **Config**:

1. Select **“Virtual Services”** from the sidebar. The **ADD VIRTUAL SERVICE** screen opens.

2. Enter a unique Virtual Service Name (**vs_mail_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 Exchange HTTPS Virtual Service.

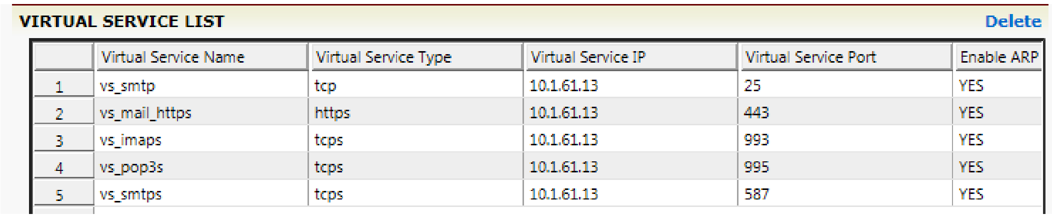


ADD VIRTUAL SERVICE | Add

Virtual Service Name:	vs_mail_https [Enable this Service: ☑]
Virtual Service Type:	HTTPS
Virtual Service IP:	10.1.61.13
Virtual Service Port:	443
Enable ARP:	☑
Connection Limit:	0

3. Do the same as step 2 for vs_smtps, vs_imaps, and vs_pop3s, with TCPS as the Virtual Service Type and with different ports, and with vs_smtp with TCP as the Virtual Service Type.

Once added, all Virtual Services are available on the **VIRTUAL SERVICE LIST**.



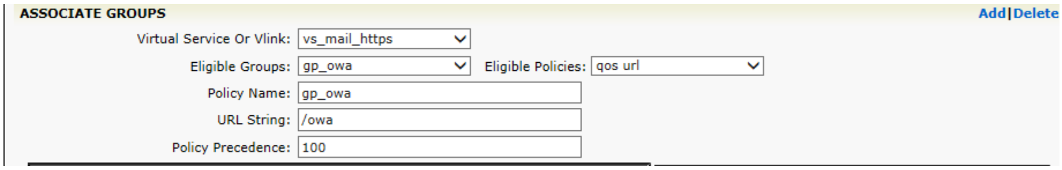
VIRTUAL SERVICE LIST | Delete

	Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	Enable ARP
1	vs_smtp	tcp	10.1.61.13	25	YES
2	vs_mail_https	https	10.1.61.13	443	YES
3	vs_imaps	tcps	10.1.61.13	993	YES
4	vs_pop3s	tcps	10.1.61.13	995	YES
5	vs_smtps	tcps	10.1.61.13	587	YES

The next step is to associate each Virtual Service with the SLB Group(s). The "qos url" configuration steps are shown in the following example:

4. Select the Virtual Service to work on: double click "**vs_mail_https**" on the **VIRTUAL SERVICE LIST**. The **VIRTUAL SERVICE INFORMATION** screen opens.

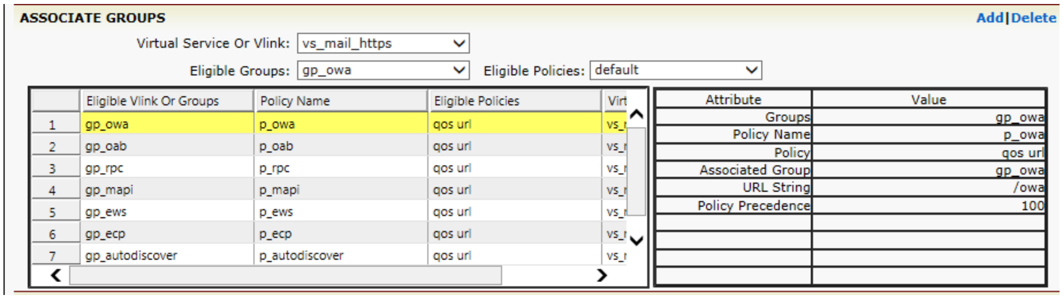
5. Go down to **ASSOCIATE GROUPS;** select the group "**gp_owa**" from Eligible Groups and select "**qos url"** from Eligible Policies. Enter a unique name for the Policy Name. Enter **"/owa"** for the URL String and "100" for Policy Precedence. Click **Add.**



ASSOCIATE GROUPS | Add|Delete

Virtual Service Or Vlink:	vs_mail_https
Eligible Groups:	gp_owa Eligible Policies: qos url
Policy Name:	gp_owa
URL String:	/owa
Policy Precedence:	100

6. Do the same as step 5 for all "qos url" policies with different URL String/Groups and Precedence as defined by Table 7.



ASSOCIATE GROUPS | Add|Delete

Virtual Service Or Vlink: vs_mail_https

Eligible Groups: gp_owa   Eligible Policies: default

	Eligible Vlink Or Groups	Policy Name	Eligible Policies	Virt
1	gp_owa	p_owa	qos url	vs_
2	gp_oab	p_oab	qos url	vs_
3	gp_rpc	p_rpc	qos url	vs_
4	gp_mapi	p_mapi	qos url	vs_
5	gp_ews	p_ews	qos url	vs_
6	gp_ecp	p_ecp	qos url	vs_
7	gp_autodiscover	p_autodiscover	qos url	vs_

Attribute	Value
Groups	gp_owa
Policy Name	p_owa
Policy	qos url
Associated Group	gp_owa
URL String	/owa
Policy Precedence	100

Technical Notes:

- All associated groups will be on the Eligible vLink or Groups list. To see more details, just click to select the group and the Attributes and Values will show on the right.
- If for some reason there is no match with the client URL, we can set a default group for the virtual service. The default group members can be any one of the CAS L7 real services.

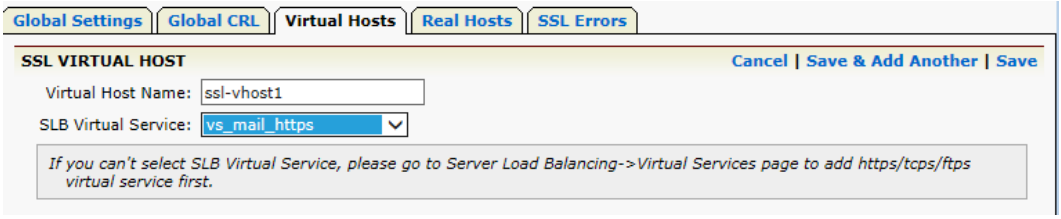
To offload/terminate SSL, the APV Series appliance needs an SSL Virtual Host to associate with the SLB Virtual Service. The SSL Virtual Host has its SSL Certificate/Private Key and SSL/TLS parameters for processing the needed SSL/TLS communication. One SSL Virtual Host can serve multiple SLB Virtual Services which may have different application types, such as HTTPS, FTPS or TCPS.

3.1.5 Create the SSL Virtual Hosts

On the APV appliance, SSL setup requires creating an SSL Virtual Host, assigning a Certificate/Key, and enabling it. Additional SSL/TLS protocol/cipher options and error handling can be configured as well.

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

1. Select **"SSL"** from the sidebar. Click **Virtual Hosts -> Add**. The **SSL VIRTUAL HOST** screen opens.
2. Enter a unique SSL Virtual Host Name (**ssl-vhost1**) and select the SLB Virtual Service (**vs_mail_https**). Then click **Save.**



SSL VIRTUAL HOST

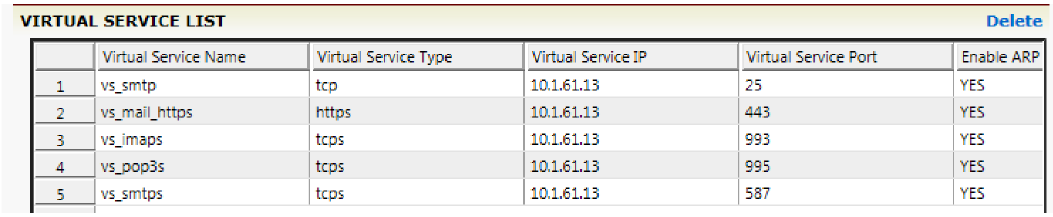
Virtual Host Name: ssl-vhost1

SLB Virtual Service: vs_mail_https

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.

3. Repeat step 1 and 2 for all the Exchange SLB Virtual Services that need SSL termination.

All SSL Virtual Hosts and their associated SLB Virtual Services should appear on the **SSL VIRTUAL HOSTS** list.



VIRTUAL SERVICE LIST

	Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	Enable ARP
1	vs_smtp	tcp	10.1.61.13	25	YES
2	vs_mail_https	https	10.1.61.13	443	YES
3	vs_imaps	tcps	10.1.61.13	993	YES
4	vs_pop3s	tcps	10.1.61.13	995	YES
5	vs_smtps	tcps	10.1.61.13	587	YES

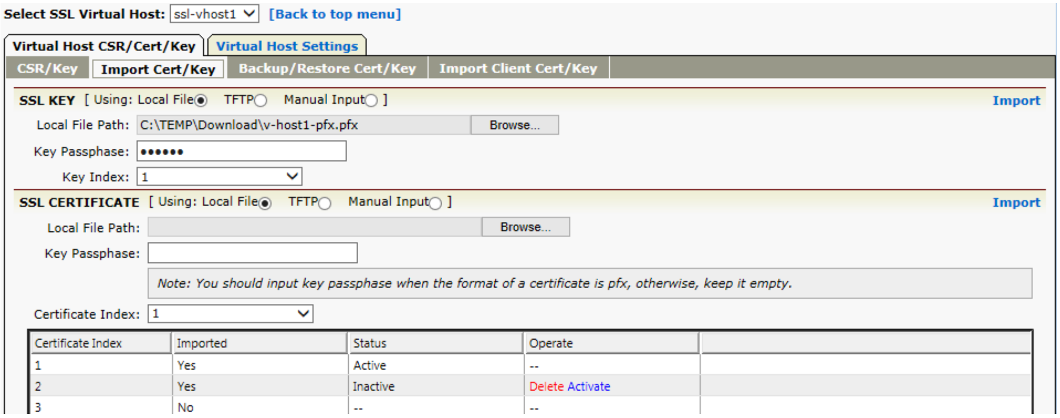
The SSL server requires a Certificate (and Private Key) for SSL/TLS handshake so that the client knows it is connected to the intended server with security. There are two options to add/update Certificate/Key to the SSL Virtual Host:

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

Option A: Import an Existing SSL Certificate and Key to the APV

To import an existing SSL key and certificate from a PFX local file, 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 Key and Certificate.
2. Click **"Import Cert/Key"**.
3. In **SSL KEY**, select **Local File**: Browse to locate the local PFX file on your disk, enter the **Key Passphrase** and **1** for **Key Index**, and click **Import** to import the private key from the PFX file. The following example is using a local disk file "**v-host1-pfx.pfx**" which is password protected.



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

SSL KEY [Using: Local File ● TFTP ○ Manual Input ○]

Local File Path: C:\TEMP\Download\v-host1-pfx.pfx

Key Passphase: ••••••

Key Index: 1

SSL CERTIFICATE [Using: Local File ● TFTP ○ Manual Input ○]

Local File Path:

Key Passphase:

Note: You should input key passphase when the format of a certificate is pfx, otherwise, keep it empty.

Certificate Index: 1

Certificate Index	Imported	Status	Operate	
1	Yes	Active	--	
2	Yes	Inactive	Delete Activate	
3	No	--	--	

4. In **SSL CERTIFICATE**, select **Local File**: Browse to locate the local PFX file on your disk, enter the **Key Passphrase** and **1** for **Key Index**, and click **Import** to import the corresponding certificate from the PFX file.

Technical Notes:

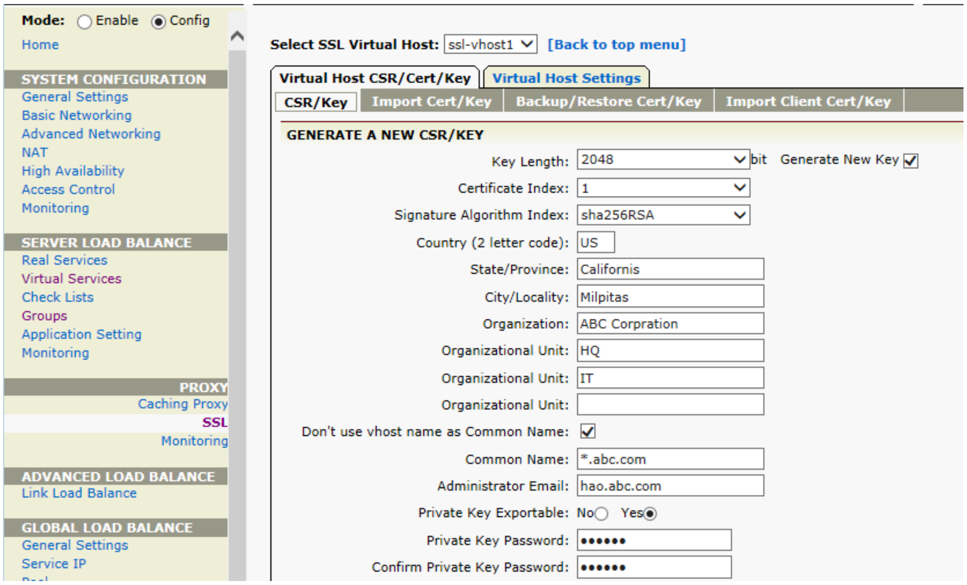
- PFX files are PKCS#12 Personal Information Exchange Syntax Standard files. They can include an arbitrary number of private keys with accompanying X.509 certificates (public keys) and a Certificate Authority Chain.
- To manually import the SSL Key/Certificate, you can use the OpenSSL tool to covert the PFX file to the unencrypted PEM format, then manually import it to the APV appliance.
- On the APV appliance, each SSL Virtual Host can have three sets of Keys/Certificates configured. This is to facilitate quick switchover when renewing a certificate.

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

This option is for quick testing, or when applying for a new certificate. The APV appliance can generate a new private key, self-signed certificate and a CSR (Certificate Signing Request) for the CA to create your SSL certificate. To generate the CSR and a self-signed certificate, enter WebUI, **Mode: Config**:

1. Navigate to **SSL** -> **Virtual Hosts** and double click the newly created SSL Virtual Hosts. Under **Virtual Host CSR/Cert/Key -> CSR/Key.** As the new SSL Virtual host does not have a key, the **GENERATE A NEW CSR/KEY** screen opens.

2. 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

Select SSL Virtual Host: ssl-vhost1

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 Corpration
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:	••••••

Technical Notes:

You can cut/paste and email the CSR to a trusted CA and pay for it. Once you have received the certificate you can import it into the SSL subsystem. To perform this task from the CLI or WebUI via manual input, simple cut from "-----BEGIN CERTIFICATE ----" line down to the "----END CERTIFICATE-----".

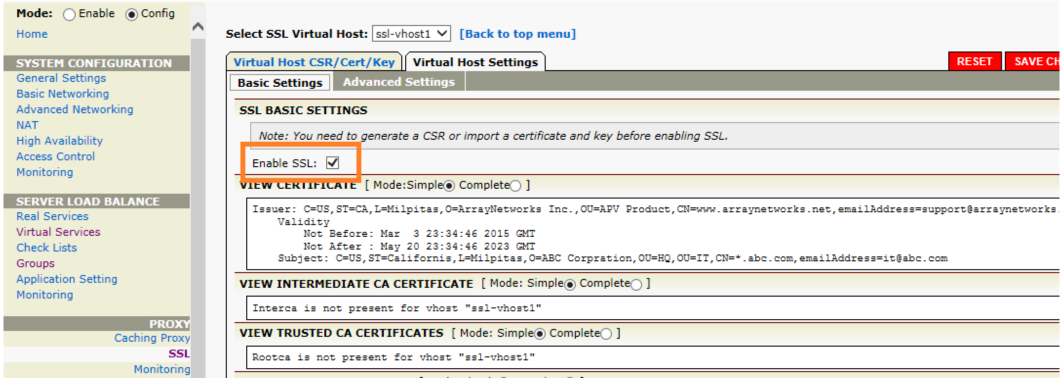
Once the Private Key/Certificate is available for the SSL Virtual Host, we can enable the SSL Virtual Host to process encrypted traffic by the following steps:

Enable SSL Virtual Host

Enter WebUI, **Mode: Config**:

1. Navigate to ***SSL*** -> ***Virtual Hosts***; double click **SSL Virtual Hosts**.

2. Click on the **Virtual Host Settings** tab and select **Enable SSL** under the **SSL BASIC SETTINGS**. Click **SAVE CHANGES** to enable the SSL.



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

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.
    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 Corpration,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"
```

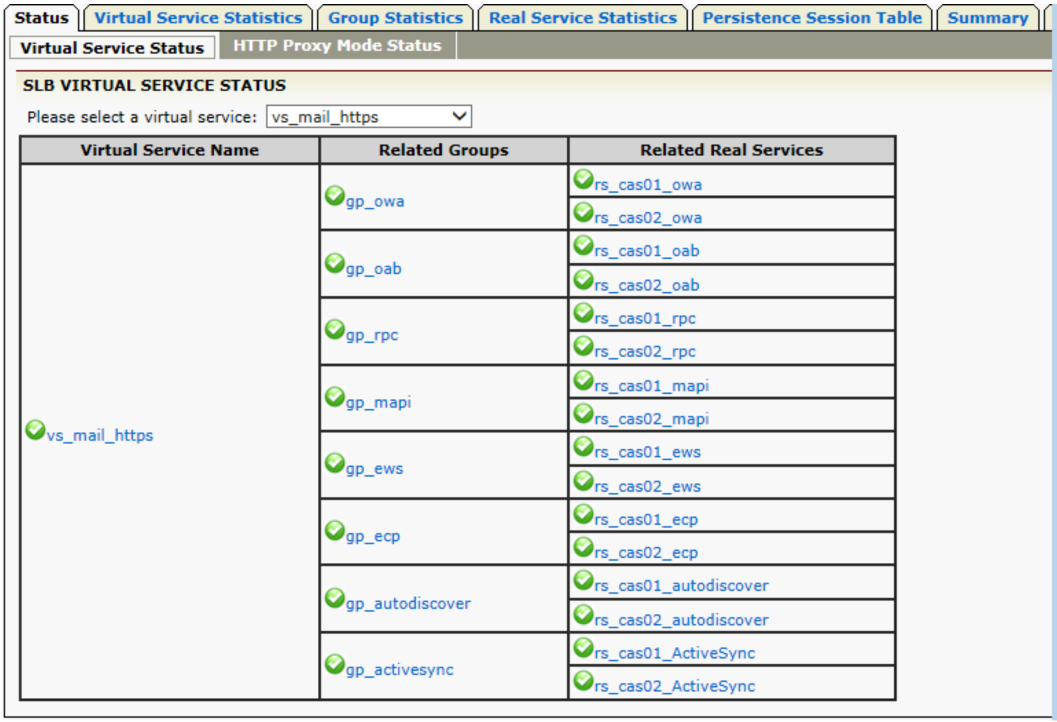
Technical Notes:

When Enable is selected, the APV system will validate the certificate chain for the SSL virtual host. A warning message, stating that the certificate chain is incomplete, will be printed if no certificate chain from a trusted root CA can be established. These new root and intermediate certificates can be imported by using the “ssl import rootca” and “ssl import interca <vhostname>” commands, or WebUI.

3.2 Validate Configuration and Service

Validate that the basic configuration is functioning correctly:

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



SLB VIRTUAL SERVICE STATUS

Please select a virtual service: vs_mail_https

Virtual Service Name	Related Groups	Related Real Services
✓vs_mail_https	✓gp_owa	✓rs_cas01_owa
		✓rs_cas02_owa
	✓gp_oab	✓rs_cas01_oab
		✓rs_cas02_oab
	✓gp_rpc	✓rs_cas01_rpc
		✓rs_cas02_rpc
	✓gp_mapi	✓rs_cas01_mapi
		✓rs_cas02_mapi
	✓gp_ews	✓rs_cas01_ews
		✓rs_cas02_ews
	✓gp_ecp	✓rs_cas01_ecp
		✓rs_cas02_ecp
	✓gp_autodiscover	✓rs_cas01_autodiscover
		✓rs_cas02_autodiscover
	✓gp_activesync	✓rs_cas01_ActiveSync
		✓rs_cas02_ActiveSync

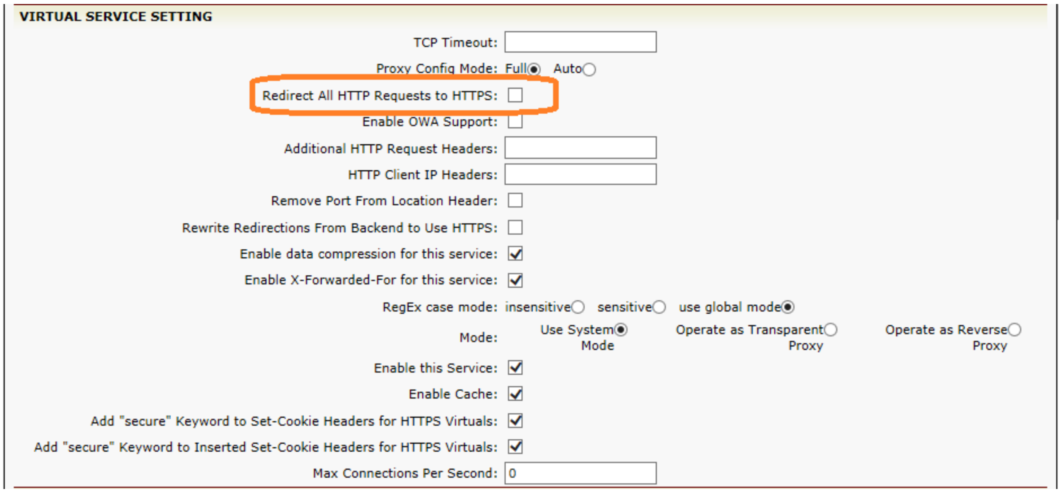
4 Configure Other APV Features for Exchange

4.1 HTTP Rewrite/Redirect

In normal operation for secured Exchange access, only HTTPS access to the Exchange services would be allowed. However, the end-user may inadvertently type http://...(unsecured) rather than https://...(secured) in attempting to access the secured Exchange service. Rather than waiting for timeout, to make this more user friendly the APV system can be configured to auto-redirect http requests to https.

To configure the HTTP-to-HTTPS redirection:

1. Add a new Virtual Service ”**vs_mail_http**” with the same IP as for “vs_mail_https” and virtual service port ”**80**” for HTTP.
2. Select the Virtual Service “**vs_mail_http**” to edit it. The **VIRTUAL SERVICE INFORMATION** screen opens.
3. Check the box for “**Redirect ALL HTTP Requests to HTTPS**” and **SAVE CHANGES**.



VIRTUAL SERVICE SETTING

TCP Timeout:	
Proxy Config Mode:	Full● Auto○
Redirect All HTTP Requests to HTTPS:	□
Enable OWA Support:	□
Additional HTTP Request Headers:	
HTTP Client IP Headers:	
Remove Port From Location Header:	□
Rewrite Redirections From Backend to Use HTTPS:	□
Enable data compression for this service:	☑
Enable X-Forwarded-For for this service:	☑
RegEx case mode:	insensitive○ sensitive○ use global mode●
Mode:	Use System Mode● Operate as Transparent Proxy○ Operate as Reverse Proxy○
Enable this Service:	☑
Enable Cache:	☑
Add "secure" Keyword to Set-Cookie Headers for HTTPS Virtuals:	☑
Add "secure" Keyword to Inserted Set-Cookie Headers for HTTPS Virtuals:	☑
Max Connections Per Second:	0

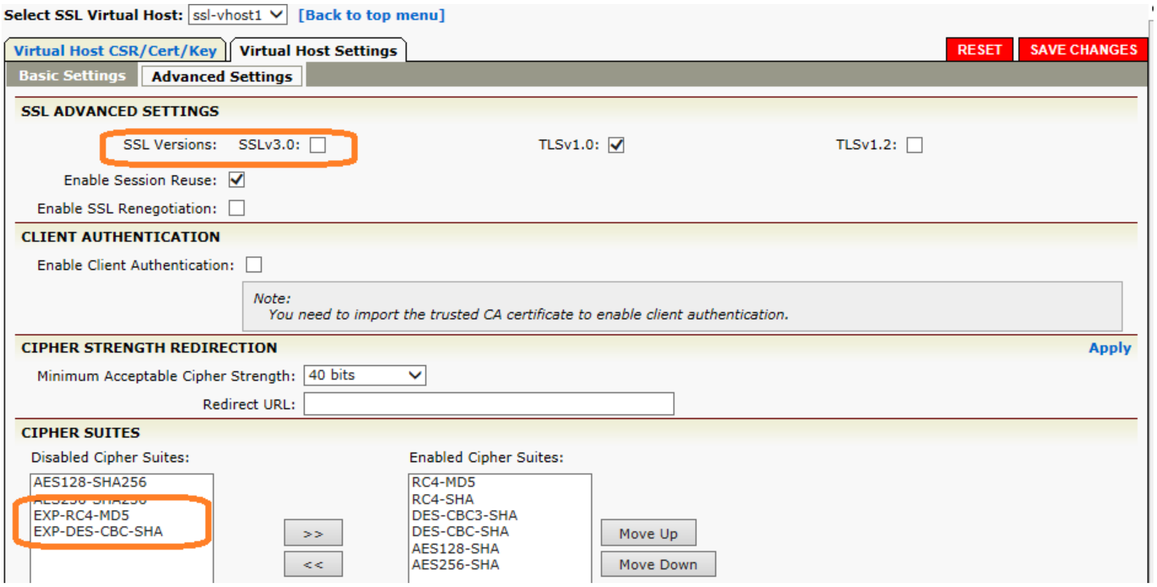
4.2 Advanced SSL Virtual Host Setting – Disable SSLv3

The APV appliance’s SSL Virtual Host has many options. For example, SSLv3 has many known vulnerabilities. If no backward compatibility is needed, we suggest disabling SSLv3.

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

1. Navigate to **SSL** -> **Virtual Hosts** -> and double click **SSL Virtual Hosts** to select it.
2. Navigate 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,** which are only supported by SSL3.0.

4. Uncheck SSLv3.0, and click **SAVE CHANGES** to store the change.



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

Minimum Acceptable Cipher Strength: 40 bits

Redirect URL:

CIPHER SUITES

Disabled Cipher Suites:	Enabled Cipher Suites:
AES128-SHA256	RC4-MD5
AES256-SHA256	RC4-SHA
EXP-RC4-MD5	DES-CBC3-SHA
EXP-DES-CBC-SHA	DES-CBC-SHA
	AES128-SHA
	AES256-SHA

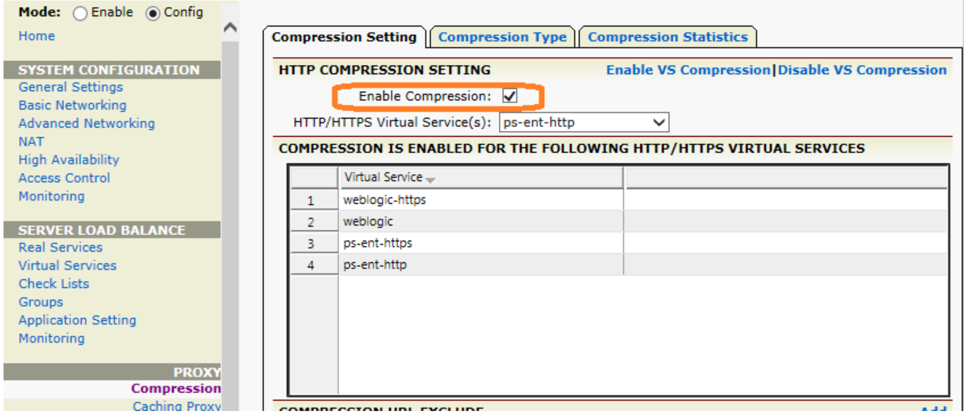
4.3 HTTP Compression

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 for HTTP compression. Individual Virtual Services can be selected and disabled.



HTTP COMPRESSION SETTING

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	

COMPRESSION URL EXCLUDE

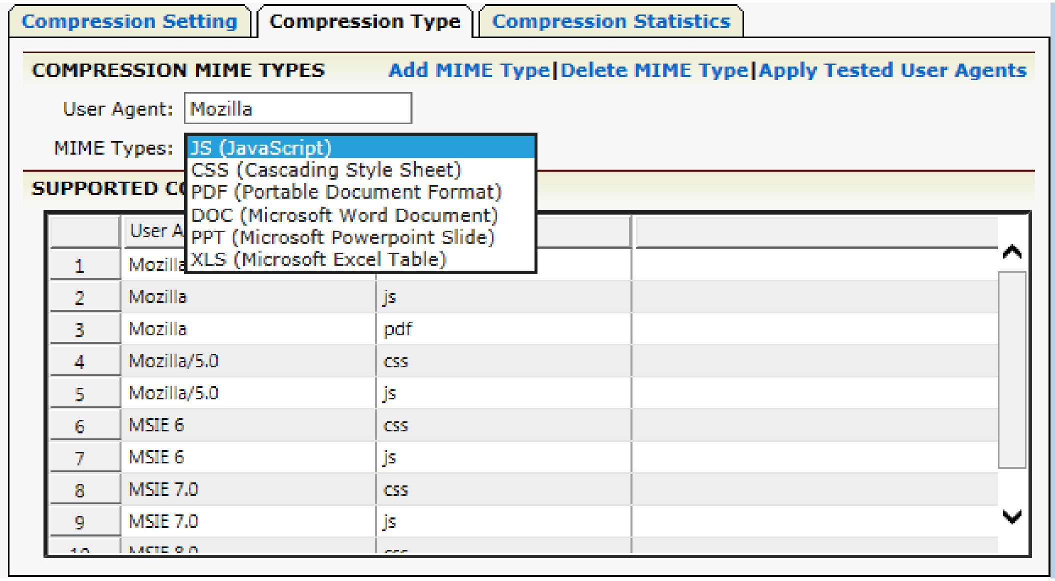
Note: By default, the following MIME types are compressed by the APV appliance for all browsers (User-Agent):

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

- XML (text/XML)

Due to compatibility issues, not all MIME types are supported on all types of browsers. 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 are added to the screen.
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
Add MIME Type
Delete MIME Type
Apply Tested User Agents
JS (JavaScript)
CSS (Cascading Style Sheet)
PDF (Portable Document Format)
DOC (Microsoft Word Document)
PPT (Microsoft Powerpoint Slide)
XLS (Microsoft Excel Table)

COMPRESSION MIME TYPES

User Agent: Mozilla

MIME Types: JS (JavaScript)

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 8.0	css	

Note: To view compression statistics, from WebUI, navigate to **Compression** -> **Compression Statistics**.

Note: In certain circumstances, a certain HTTP object might have an issue with compression. To exclude the particular HTTP object from compression, go to **Compression** -> **Compression Setting**, and add the URL to the **URL EXCLUDE LIST**.

5. Conclusion

This concludes the Array Networks APV deployment guide for Microsoft Exchange 2013. Array Networks APV/vAPV Series application delivery controllers provide Layer 7 server load balancing, high availability, Layer 7 SSL acceleration and offloading, DDoS protection, and TCP connection multiplexing, caching and compression to improve the performance, scalability, availability and security for Exchange server deployments.

Appendix:

Configuration Example 1 – Basic L4 SLB

```
slb real tcp "rs_cas01_https" 10.2.40.180 443 1000 tcp 3 3
slb real tcp "rs_cas01_imaps" 10.2.40.180 993 1000 tcp 1 1
slb real tcp "rs_cas01_pop3s" 10.2.40.180 995 1000 tcp 1 1
slb real tcp "rs_cas01_smtp" 10.2.40.180 25 1000 tcp 1 1
slb real tcp "rs_cas02_https" 10.2.40.181 443 1000 tcp 3 3
slb real tcp "rs_cas02_imaps" 10.2.40.181 993 1000 tcp 1 1
slb real tcp "rs_cas02_pop3s" 10.2.40.181 995 1000 tcp 3 3
slb real tcp "rs_cas02_smtp" 10.2.40.181 25 1000 tcp 3 3

slb group method "gp_cas_https" lc 32 no
slb group method "gp_cas_imaps" lc 32 no
slb group method "gp_cas_pop3s" lc 32 no
slb group method "gp_cas_smtp" lc 32 no
slb group member "gp_cas_https" "rs_cas01_https" 1 0
slb group member "gp_cas_https" "rs_cas02_https" 1 0
slb group member "gp_cas_imaps" "rs_cas01_imaps" 1 0
slb group member "gp_cas_imaps" "rs_cas02_imaps" 1 0
slb group member "gp_cas_pop3s" "rs_cas01_pop3s" 1 0
slb group member "gp_cas_pop3s" "rs_cas02_pop3s" 1 0
slb group member "gp_cas_smtp" "rs_cas01_smtp" 1 0
slb group member "gp_cas_smtp" "rs_cas02_smtp" 1 0

slb virtual tcp "vs_mail_https" 10.1.61.41 443 arp 0
slb virtual tcp "vs_mail_imaps" 10.1.61.41 993 arp 0
slb virtual tcp "vs_mail_pop3s" 10.1.61.41 995 arp 0
slb virtual tcp "vs_mail_smtp" 10.1.61.41 25 arp 0

slb policy default "vs_mail_https" "gp_cas_https"
slb policy default "vs_mail_imaps" "gp_cas_imaps"
slb policy default "vs_mail_pop3s" "gp_cas_pop3s"
slb policy default "vs_mail_smtp" "gp_cas_smtp"
```

Configuration Example 2 – L7 SLB + SSL Offload + QoS URL

```
slb real tcp "rs_cas01_imap" 10.2.40.180 143 1000 tcp 1 1
slb real tcp "rs_cas01_pop3" 10.2.40.180 110 1000 tcp 1 1
slb real tcp "rs_cas01_smtp" 10.2.40.180 25 1000 tcp 1 1
slb real tcp "rs_cas02_imap" 10.2.40.181 143 1000 tcp 1 1
slb real tcp "rs_cas02_pop3" 10.2.40.181 110 1000 tcp 3 3
slb real tcp "rs_cas02_smtp" 10.2.40.181 25 1000 tcp 3 3
slb real http "rs_cas01_ActiveSync" 10.2.40.180 80 1000 http 3 3
slb real http "rs_cas01_autodiscover" 10.2.40.180 80 1000 http 3 3
slb real http "rs_cas01_ecp" 10.2.40.180 80 1000 http 3 3
slb real http "rs_cas01_ews" 10.2.40.180 80 1000 http 3 3
slb real http "rs_cas01_mapi" 10.2.40.180 80 1000 http 3 3
slb real http "rs_cas01_oab" 10.2.40.180 80 1000 http 3 3
slb real http "rs_cas01_owa" 10.2.40.180 80 1000 http 3 3
slb real http "rs_cas01_rpc" 10.2.40.180 80 1000 http 3 3
slb real http "rs_cas02_ActiveSync" 10.2.40.181 80 1000 http 3 3
slb real http "rs_cas02_autodiscover" 10.2.40.181 80 1000 http 3 3
slb real http "rs_cas02_ecp" 10.2.40.181 80 1000 http 3 3
slb real http "rs_cas02_ews" 10.2.40.181 80 1000 http 3 3
slb real http "rs_cas02_mapi" 10.2.40.181 80 1000 http 3 3
slb real http "rs_cas02_oab" 10.2.40.181 80 1000 http 3 3
slb real http "rs_cas02_owa" 10.2.40.181 80 1000 http 3 3
slb real http "rs_cas02_rpc" 10.2.40.181 80 1000 http 3 3

slb group method "gp_activesync" lc 32 no
slb group method "gp_autodiscover" lc 32 no
slb group method "gp_ecp" lc 32 no
slb group method "gp_ews" lc 32 no
slb group method "gp_imap" lc 32 no
slb group method "gp_mapi" lc 32 no
slb group method "gp_oab" lc 32 no
slb group method "gp_owa" lc 32 no
slb group method "gp_pop3" lc 32 no
slb group method "gp_rpc" lc 32 no
slb group method "gp_smtp" lc 32 no
slb group member "gp_activesync" "rs_cas01_ActiveSync" 1 0
slb group member "gp_activesync" "rs_cas02_ActiveSync" 1 0
slb group member "gp_autodiscover" "rs_cas01_autodiscover" 1 0
slb group member "gp_autodiscover" "rs_cas02_autodiscover" 1 0
slb group member "gp_ecp" "rs_cas01_ecp" 1 0
slb group member "gp_ecp" "rs_cas02_ecp" 1 0
slb group member "gp_ews" "rs_cas01_ews" 1 0
slb group member "gp_ews" "rs_cas02_ews" 1 0
slb group member "gp_imap" "rs_cas01_imap" 1 0
slb group member "gp_imap" "rs_cas02_imap" 1 0
slb group member "gp_mapi" "rs_cas01_mapi" 1 0
slb group member "gp_mapi" "rs_cas02_mapi" 1 0
slb group member "gp_oab" "rs_cas01_oab" 1 0
slb group member "gp_oab" "rs_cas02_oab" 1 0
slb group member "gp_owa" "rs_cas01_owa" 1 0
slb group member "gp_owa" "rs_cas02_owa" 1 0
slb group member "gp_pop3" "rs_cas01_pop3" 1 0
slb group member "gp_pop3" "rs_cas02_pop3" 1 0
slb group member "gp_rpc" "rs_cas01_rpc" 1 0
slb group member "gp_rpc" "rs_cas02_rpc" 1 0
slb group member "gp_smtp" "rs_cas01_smtp" 1 0
slb group member "gp_smtp" "rs_cas02_smtp" 1 0

slb virtual tcp "vs_smtp" 10.1.61.13 25 arp 0
slb virtual https "vs_mail_https" 10.1.61.13 443 arp 0
slb virtual tcps "vs_imaps" 10.1.61.13 993 arp 0
slb virtual tcps "vs_pop3s" 10.1.61.13 995 arp 0
slb virtual tcps "vs_smtps" 10.1.61.13 587 arp 0

slb policy qos url "p_owa" "vs_mail_https" "gp_owa" "/owa" 100
slb policy qos url "p_oab" "vs_mail_https" "gp_oab" "/oab" 110
slb policy qos url "p_rpc" "vs_mail_https" "gp_rpc" "/rpc" 120
slb policy qos url "p_mapi" "vs_mail_https" "gp_mapi" "/mapi" 130
slb policy qos url "p_ews" "vs_mail_https" "gp_ews" "/ews" 140
slb policy qos url "p_ecp" "vs_mail_https" "gp_ecp" "/ecp" 150
slb policy qos url "p_autodiscover" "vs_mail_https" "gp_autodiscover" "/autodiscover" 160
slb policy qos url "p_activesync" "vs_mail_https" "gp_activesync" "/Microsoft-Server-ActiveSync" 170
slb policy default "vs_smtp" "gp_smtp"
slb policy default "vs_imaps" "gp_imap"
slb policy default "vs_pop3s" "gp_pop3"

health request 10 "GET /owa/HealthCheck.htm HTTP/1.0 \r\n\r\n"
health request 11 "GET /OAB/HealthCheck.htm HTTP/1.0 \r\n\r\n"
health request 12 "GET /RPC/HealthCheck.htm HTTP/1.0 \r\n\r\n"
health request 13 "GET /MAPI/HealthCheck.htm HTTP/1.0 \r\n\r\n"
health request 14 "GET /EWS/HealthCheck.htm HTTP/1.0 \r\n\r\n"
health request 15 "GET /ECP/HealthCheck.htm HTTP/1.0 \r\n\r\n"
health request 16 "GET /Autodiscover/HealthCheck.htm HTTP/1.0 \r\n\r\n"
health request 17 "GET /Microsoft-Server-ActiveSync/HealthCheck.htm HTTP/1.0 \r\n\r\n"

health server "rs_cas01_autodiscover" 16 16
health server "rs_cas01_ecp" 15 15
health server "rs_cas01_ews" 14 14
health server "rs_cas01_mapi" 13 13
health server "rs_cas01_oab" 11 11
health server "rs_cas01_owa" 10 10
health server "rs_cas01_rpc" 12 12
health server "rs_cas02_ActiveSync" 17 17
health server "rs_cas02_autodiscover" 16 16
health server "rs_cas02_ecp" 15 15
health server "rs_cas02_ews" 14 14
health server "rs_cas02_mapi" 13 13
health server "rs_cas02_oab" 11 11
health server "rs_cas02_owa" 10 10
health server "rs_cas02_rpc" 12 12
health server "rs_cas01_ActiveSync" 17 17
```

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