Deployment Guide
Nov-2016 rev. a

Deploying Array Networks APV Series Application Delivery Controllers with Microsoft Exchange 2016

Microsoft Partner

Introduction 3

1.1 Microsoft Exchange 2016 3
1.2 Exchange 2016 Load Balancing Options 4
1.3 Deployment Overview and Prerequisites 5
1.3.1 APV SSL Offloading/Acceleration 5
1.4 APV Application Delivery Controller Benefits 6

2 Configure L4 Load Balancing for Exchange 2016 8

2.1 Configuration Steps 8
2.1.1 Define the Application Health Check 8
2.1.2 Create the Real Services – L4 MBX 8
2.1.3 Create the Group – L4 MBX 9
2.1.4 Create the SLB Virtual Services – L4 Exchange 10
2.2 Validate Configuration and Service 11

3 Configure L7 QoS URL SLB + SSL Offload for Exchange 13

3.1 Configuration Steps 13
3.1.1 Define the Application Health Check – per Exchange Protocol 13
3.1.2 Create the Real Services – L7 MBX with individual protocol 15
3.1.3 Create the Group – L7 MBX 16
3.1.4 Create the Virtual Service – L7 Exchange with SSL Offload+ QoS URL 17
3.2 Validate Configuration and Service 18

4 Configure L7 QoS URL SLB + SSL Bridge for Exchange 19

4.1 Configuration Steps 19
4.1.1 Define the Application Health Check – per Exchange Protocol 19
4.1.2 Create the Real Services – MBX HTTPS with multiple protocols 19
4.1.3 Create the Group – L7 MBX 20
4.1.4 Create the Virtual Service – Exchange with SSL + L7 QoS URL 20
4.2 Validate Configuration and Service 20

5 Configure Other APV Features for Exchange 21

5.1 HTTP Rewrite/Redirect 21
5.2 HTTP Compression 21
5.3 Create the SSL Virtual Hosts 22
5.4 Advanced SSL Virtual Host Setting – Disable SSLv3 23

6 Conclusion..... 25

Appendix:..... 26

CLI Configuration Example 1 – L4 Load Balancing for Exchange 2016 26

CLI Configuration Example 2 – L7 QoS URL SLB + SSL Offload 27

CLI Configuration Example 3 – L7 QoS URL SLB + SSL Bridge 29

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 2016

For Microsoft Exchange 2016, changes from Exchange 2010/2013 are far less complex than previous releases; however, there have been major architectural changes to the Exchange server roles. In Exchange 2016, the number of server roles have been reduced to one:

- **MBX 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.

Following is the Exchange 2016 network architecture. The real server for the load balancer (APV/vAPV) are the Exchange Mail Box servers.

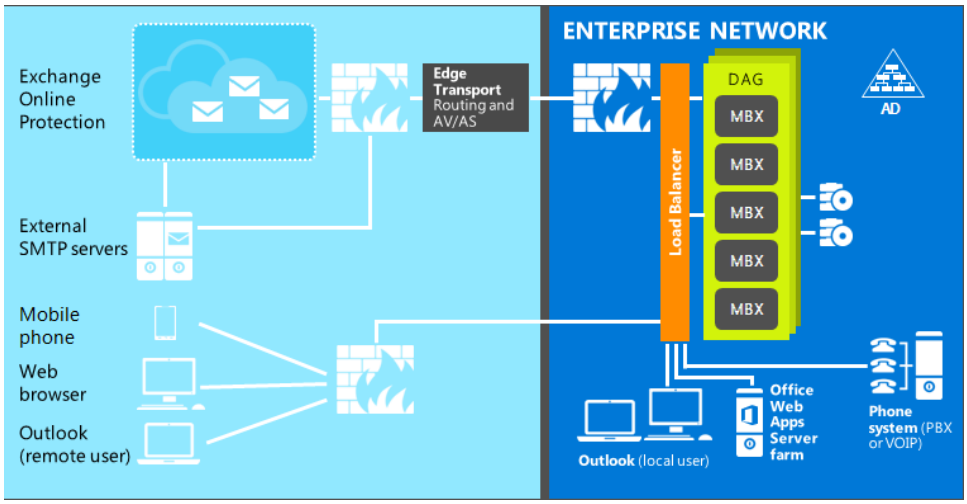


Figure 1: Exchange Server 2016 Architecture

For Exchange 2016, OWA/Outlook/EAS/EAC/PowerShell can be accessed via the same HTTPS/HTTP that MBX IIS service supports. IMAP/POP, SMTP and UM are accessed by their own services. Following is the Exchange 2016 Mailbox Protocol Architecture (Figure 2).

Because the Mailbox HTTP Proxy can proxy client connections to another MBX server that has the actual client mailbox database loaded (the "correct" destination end point), server affinity is not required for load balancing.

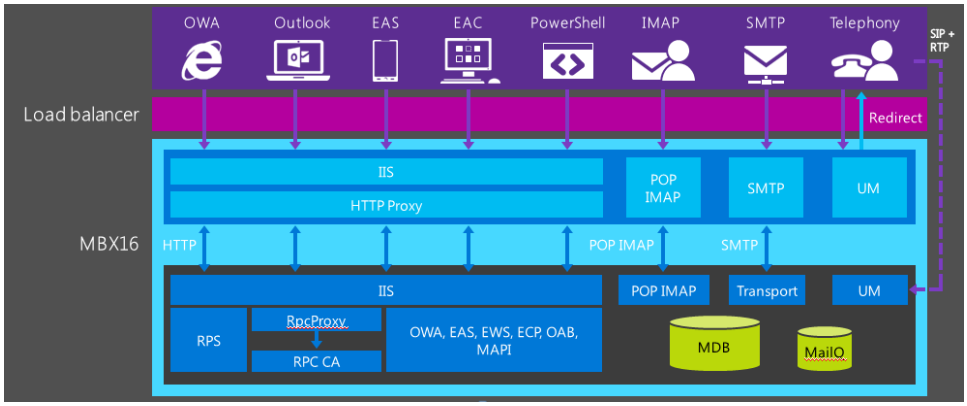


Figure 2: Exchange 2016 MBX Protocol Architecture

1.2 Exchange 2016 Load Balancing Options

For Mail namespace options, public IP availability affects load balancing requirements of different mail services with the same HTTP/HTTPS protocol. Each has its pros and cons.

1. Single Namespace/Layer 4 (single IP/port, single Virtual Service)
2. Multiple Namespace/Layer 4 (multiple IP/Ports, multiple Virtual Services)
3. Multiple Namespace/Layer 7 (single IP/Port, single Virtual Service, L7 Content Routing)

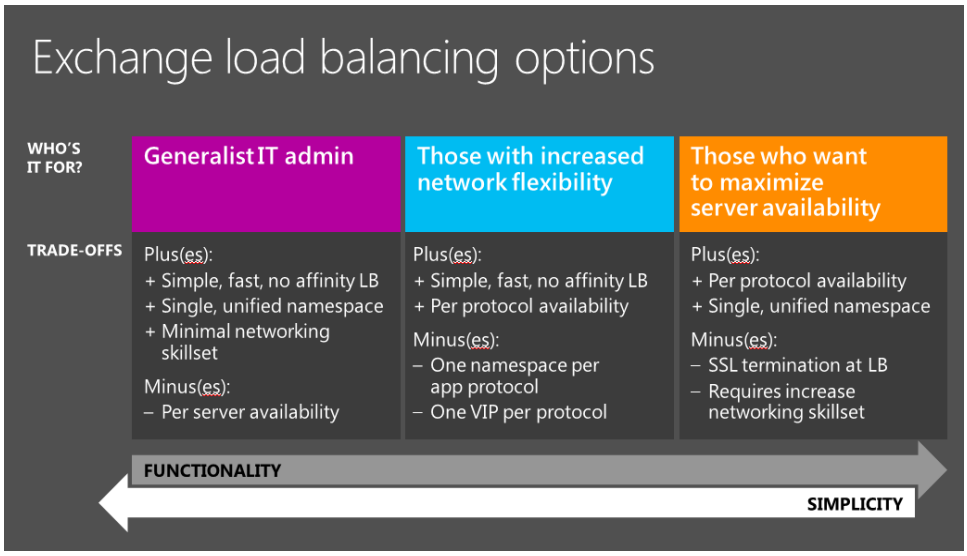


Figure 3: Exchange 2016 Load Balancing Options

Each deployment model has its own pros and cons. The deployment model can be selected based on the actual requirements of the organization. For an APV deployment with L7 content switching (SLB policy per mail protocol) and SSL termination (also called SSL bridging), a single IP can be used to easily maximize server availability.

1.3 Deployment Overview and Prerequisites

APV appliances are flexible to support all load balancing needs for Exchange 2016 through capabilities such as full reverse proxy, transparent mode, 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 MBX 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 MBX servers. These connections are then load balanced across the MBX servers to distribute the load according to the load balancing algorithm selected on the APV Series.

In this example, the APV/vAPV appliance is running version ArrayOS™ 8.x or later. Configuration steps given are for the old APV WebUI, which you may access through https://<apv_ip>:8889. 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.

1.3.1 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 to simplify certificate/key management, reduce server load, and accelerate SSL with high-performance hardware. Following are typical ways to use 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 on 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 open network) to be encrypted. In this case, APV Series is the SSL client, so there is no need for it to store SSL certificate and keys. The Exchange Servers needs store the certificates and keys. However, the APV Series expects a valid certificate from the Exchange Server.

3. SSL Bridge (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.

1.4 APV Application Delivery Controller Benefits

The Array Networks 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, 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 helps scale the capacity of the Exchange MBX 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 MBX 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 2016

For Exchange 2016 single namespace/L4 Load Balancing, all Exchange 2016 traffic is directed to APV Virtual Services and spread to multiple Mailbox Servers that use the same VIP and different TCP ports (protocols). The port numbers are mapped to all the Exchange 2016 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”.

Prior to APV 8.6, which includes Array’s Pilot Login/Enable Password, the default is no password. Just click Login to enter 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 MBX server availability. No additional configuration is required.

2.1.2 Create the Real Services – L4 MBX

Real Services are the two Exchange 2016 MBX servers (MBX01, MBX02). . The MBX is set up by default with SSL. Following is the summary of all Exchange 2016 Real Services that need to be added to the APV configuration.

IP	Real Service Name	Protocol	Port	HC Type	Req/Rep
MBX01 (10.2.40.180)	**rs_mbx01_https**	TCP	443	TCP	None
	rs_mbx01_smtp	TCP	25	TCP	None
	rs_mbx01_pop3s	TCP	995	TCP	None
	rs_mbx01_imaps	TCP	993	TCP	None
MBX02 (10.2.40.181)	**rs_mbx02_https**	TCP	443	TCP	None
	rs_mbx02_smtp	TCP	25	TCP	None
	rs_mbx02_pop3s	TCP	995	TCP	None
	rs_mbx02_imaps	TCP	993	TCP	None

Table 1 - L4 Real Services Configuration

Add each MBX 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_mbx01_https**). From the

Real Service Type pull down, select "**TCP**". Enter the Real Service IP/Port (10.2.40.180/443) that is used by the Exchange MBX Server 1.

3. For **HEALTH CHECK SETUP**, from the **Health Check Type** pull-down menu select "**tcp**". Click **Save & Add Another** to add more Real Services.
4. Follow the same steps as above: add all Real Services according to Table 1 – L4 MBX 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 systems 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.

2.1.3 Create the Group – L4 MBX

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_mbx_https	Least Connection	**rs_mbx01_https**
		rs_mbx02_https
gp_mbx_smtp	Least Connection	rs_mbx01_smtp
		rs_mbx02_smtp
gp_mbx_pop3s	Least Connection	rs_mbx01_pops
		rs_mbx02_pops
gp_mbx_imaps	Least Connection	rs_mbx01_imaps
		rs_mbx02_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_mbx_https"**. From the Group Method pull down menu; select **"Least Connections"**. Click **"Add"** to create the SLB group.

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.

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_mbx_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 pull down menu, select "**rs_mbx01_https**". Click **Save & Add Another** and select "**rs_mbx02_https**" and "**Save**"**.**

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 appliance 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_mbx_https
vs_smtp	tcp/25	default	None	None	None	gp_mbx_smtp
vs_pop3s	tcp/995	default	None	None	None	gp_mbx_pop3s
vs_imaps	tcp/993	default	None	None	None	gp_mbx_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 pull down 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.

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

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** pull down menu, select "***gp_mbx_https***" and from the **Eligible Policies** pull down menu, select "***default"***. Click **Add** to complete the Virtual Service configuration.
3. Repeat the same steps for all Virtual Services.

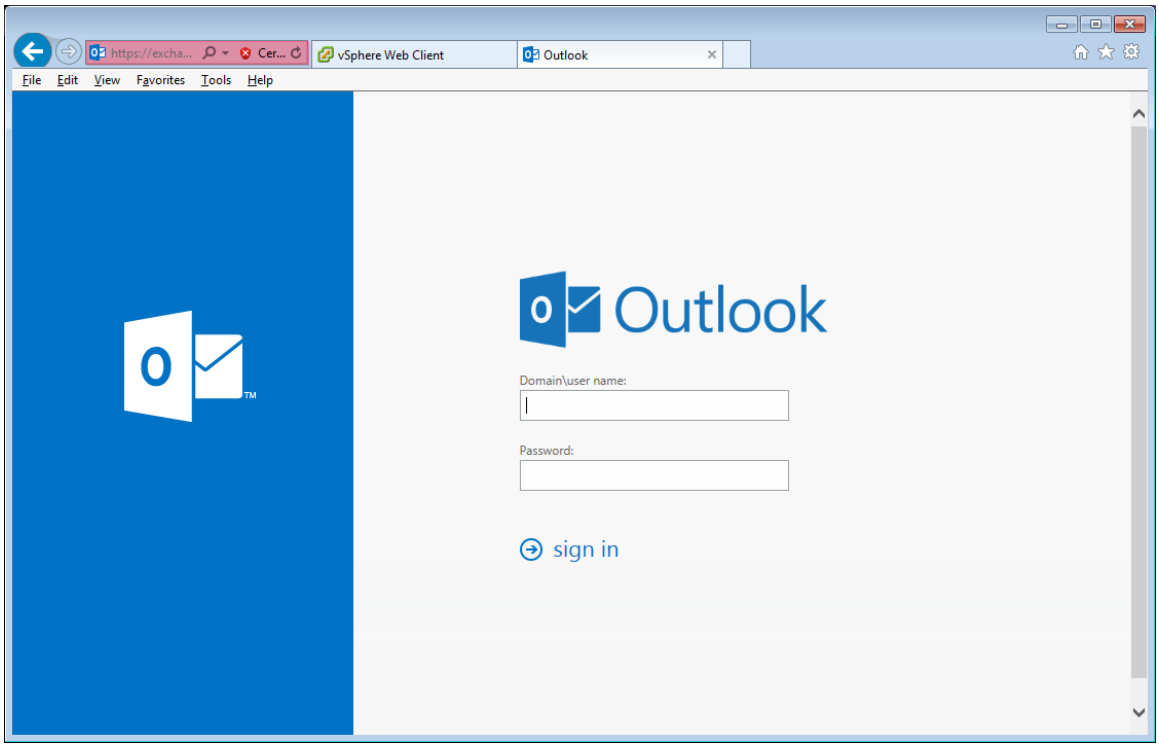
Note: On APV, the default TCP Idle timeout is 300 seconds. For Exchange, connections may stay up longer and keep alive may need to be more than 300 seconds. To extend the TCP idle timeout, use the CLI command:

slb timeout <virtual_service> <timeout_second>

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 all "**Service Status**" icons are green.
4. Launch the Web browser and navigate to the VIP address
5. Input the required Username and Password to login to Exchange 2016.


https://excha...
Cer...
vSphere Web Client
Outlook
File Edit View Favorites Tools Help
Outlook
Domain\user name:
Password:
sign in

3 Configure L7 QoS URL SLB + SSL Offload for Exchange

When the Exchange 2016 Mailbox Servers are configured with SSL Offloading (by the APV appliance), the SSL offload reduces the Mailbox server load and memory usage which in turn speed up the mailbox operation. With SSL offload on the APV, the APV can perform L7-based content routing/rewrite, security scan etc.

Another SSL offloading advantage can be simplified certificate management. Rather than having the SSL certificate(s) imported to multiple Mailbox Servers, the SSL certificate is imported to a single APV appliance, which simplifies certificate deployment and updates.

For an APV dedicated appliance with SSL hardware, SSL processing is accelerated greatly.

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 the Array Networks Pilot Login available in APV 8.6 and later, the default is no enable password. Just click Login to enter WebUI.

Note: The SMTP, POP, and IMAP setup is the same as for L4.

3.1.1 Define the Application Health Check – per Exchange Protocol

As each MBX HTTP interface supports multiple Exchange protocols, without differential protocols, if any one of the protocols is down it may render the entire MBX HTTP protocol down. Per the Microsoft Exchange 2013/2016 Health Probe Checking recommendation (see the following link), Exchange 2013/2016 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 2013/2016 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 MBX server that Managed Availability has marked as offline, load balancer health probes must be configured to check the responder.

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 MBX server. As a result, the load balancer should also consider that end point down and remove the MBX 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
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
AutoDiscover	GET /Autodiscover/HealthCheck.htm HTTP/1.0 \r\n\r\n	200	15	15
Active Sync	GET /Microsoft-Server-ActiveSync/HealthCheck.htm HTTP/1.0 \r\n\r\n	200	16	16

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**". **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**.
3. Repeat step 2 for all health check settings (for request index 11 to 16 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.

3.1.2 Create the Real Services – L7 MBX 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 on top of HTTP to share TCP port 80, such as OWA (Outlook Web Access), Outlook (RPC/MAPI), ActiveSync, etc. Those Exchange services sharing the same 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 previously defined application health checks for the respective services.

IP	Real Service Name	Protocol	Port	HC Type	Req/Rep
MBX01 (10.2.40.180)	rs_mbx01_owa	HTTP	80	HTTP	10/10
	rs_mbx01_rpc	HTTP	80	HTTP	12/12
	rs_mbx01_ews	HTTP	80	HTTP	14/14
	rs_mbx01_autodiscover	HTTP	80	HTTP	16/16
	rs_mbx01_ActiveSync	HTTP	80	HTTP	17/17
MBX02 (10.2.40.181)	rs_mbx02_owa	HTTP	80	HTTP	10/10
	rs_mbx02_rpc	HTTP	80	HTTP	12/12
	rs_mbx02_ews	HTTP	80	HTTP	14/14
	rs_mbx02_autodiscover	HTTP	80	HTTP	16/16
	rs_mbx02_ActiveSync	HTTP	80	HTTP	17/17

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_mbx01_owa*****"**. Select "**HTTP**" as the Real Service Type, enter IP address "**10.2.40.180**" and port "**80**" which is used by the MBX01 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.

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

3.1.3 Create the Group – L7 MBX

The APV Series' SLB Group defines the load balancing method and the set of servers in the group. Per Microsoft, Exchange 2013/2016 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_mbx01_ActiveSync
		rs_mbx02_ActiveSync
gp_autodiscover	Least Connection	rs_mbx01_autodiscover
		rs_mbx02_autodiscover
gp_ews	Least Connection	rs_mbx01_ews
		rs_mbx02_ews
gp_imap	Least Connection	rs_mbx01_imap
		rs_mbx02_imap
gp_owa	Least Connection	rs_mbx01_owa
		rs_mbx02_owa

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 pull down menu. Click **"Add"** to create the SLB group.
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.

4. To add Real Services to the SLB group, access the **GROUPS LIST** by double clicking on it, or by 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_mbx01_ActiveSync**", click **Save & Add Another** and select "**rs_mbx02_ActiveSync**" and "**Save**"**.**
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 HTTP (once decrypted) access to different Groups (Exchange services) based on the URL request string (similar to the content-based health check).

Note: the QoS URL string is to be matched from client that is configurable on the Exchange 2016.

Note: APV 8.6+ added Regular Expression support, for the URL String, we may configure "<regex>/(owa|ecp|ECP)" to qualify multiple match strings. See the CLI Handbook.

Virtual Service	Protocol/ Port	SLB Policy				Group
		Type	Name	URL String	Rank	
vs-mail-https	https/443	qos_url	p_owa	/owa	100	gp_owa
			p_rpc	/rpc	120	gp_rpc
			p_ews	/ews	140	gp_ews
			p_ecp	/ecp	150	gp_owa
			p_autodiscover	/Autodiscover	160	gp_autodiscover
			p_activesync	/Microsoft-Server-ActiveSync	170	gp_activesync

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.
3. If needed, 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**.

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:

1. Select the Virtual Service to work on: doubleclick ”**vs_mail_https**” on the **VIRTUAL SERVICE LIST**. The **VIRTUAL SERVICE INFORMATION** screen opens.
2. 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.**
3. Do the same as step 5 for all “qos url” policies with different URL String/Groups and Precedence as defined by Table 7.

Technical Notes:

- If for some reason there is no match with the client URL, we can set a default group (gp_owa) for the virtual service. The default group members can be any one of the MBX L7 real services.

The SLB configuration is completed. The next step is enable SSL termination with the SLB Virtual Service. If the SSL Virtual Host needs to be created, go to section 5.4.

To enable SSL/TLS termination for an SLB Virtual Service,

1. Navigate to ***SSL*** -> ***Virtual Hosts***; click Add. Enter the SSL Virtual Host Name (ssl-vhost1), and "**vs_mail_https**" for SLB Virtual Service. The click **Save**.
2. The SSL Virtual Host may be disabled. To enable the SSL Virtual Host, from the **SSL VIRTUAL HOSTS** display, double click the SSL Virtual Host with the SLB Virtual Host.
3. Click on the ***Virtual Host Settings*** tab and select **Enable SSL** under the **SSL BASIC SETTINGS**. Click ***SAVE CHANGES*** to enable SSL.

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 “**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 all “**Service Status**” icons are green.

Launch the Web browser and navigate to the VIP address. Input the required Username and Password to login to Exchange 2016.

4 Configure L7 QoS URL SLB + SSL Bridge for Exchange

The Exchange 2016 Mailbox Servers by default include SSL. Without disabling the Exchange SSL, the APV still can perform L7 load balancing with the SSL Bridge function. SSL Bridge is terminates the client SSL on the APV, and APV receives clear text. Then the APV as an SSL client re-encrypts the text send to the Exchange 2016 Mailbox.

The SSL bridge has advantages in simplifying Exchange server setup, by using the default Exchange settings. And this method allows you to use L7 content routing and health check to better utilize MBX server resources.

4.1 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 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 password enabled, just click Login to enter the WebUI.

4.1.1 Define the Application Health Check – per Exchange Protocol

Follow the same configuration and steps as 3.1.1.

4.1.2 Create the Real Services – MBX HTTPS with multiple protocols

Follow the same steps as 3.1.2 but the Exchange 2016 Services are changed to port 443 with protocol HTTPS. See the following –

IP	Real Service Name	Protocol	Port	HC Type	Req/Rep
MBX01 (10.2.40.180)	rs_mbx01_owa	HTTPS	443	HTTP	10/10
	rs_mbx01_rpc	HTTPS	443	HTTP	12/12
	rs_mbx01_ews	HTTPS	443	HTTP	14/14
	rs_mbx01_autodiscover	HTTPS	443	HTTP	16/16
	rs_mbx01_ActiveSync	HTTPS	443	HTTP	17/17
MBX02 (10.2.40.181)	rs_mbx02_owa	HTTPS	443	HTTP	10/10
	rs_mbx02_rpc	HTTPS	443	HTTP	12/12
	rs_mbx02_ews	HTTPS	443	HTTP	14/14
	rs_mbx02_autodiscover	HTTPS	443	HTTP	16/16
	rs_mbx02_ActiveSync	HTTPS	443	HTTP	17/17

To enable the APV (as an SSL client) to communicate to MBX services with the SSL protocol, the APV SSL Real Host needs to be used to associate with each MBX service.

To enable the APV SSL/TLS client function for each SLB Real Service from WebUI:

1. Navigate to ***SSL*** -> ***Real Hosts***; click Add (in Config mode). Enter the SSL Real Host Name (ssl-rhost1), and "**rs_mbx01_owa**" for the Real Virtual Service. Then click **Save & Another** for all the Exchange services that use port 443 and HTTPS protocol.
2. Check to see if the SSL Real Host has been disabled. To enable the SSL Real Host, from the **SSL REAL HOSTS** display, double click the SSL Virtual Hosts with the SLB Virtual Host.
3. Click on the ***Real Host Settings*** tab and select **Enable SSL** under the **SSL BASIC SETTINGS**. Click ***SAVE CHANGES*** to enable the SSL Real Host.

Note: APV as an SSL client, when making the SSL connection to the backend server, will validate the backend SSL certificate. In the case of an invalid certificate, such as a self-signed certificate, the SSL connection will fail. To disable Server Certificate Verification, de-select the Enable Server Certificate Verification check box from SSL Global Settings.

4.1.3 Create the Group – L7 MBX

Follow the same configuration and steps as 3.1.3.

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

Follow the same configuration and steps as 3.1.4.

4.2 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 all "**Service Status**" icons are green.

Launch the Web browser and navigate to the VIP address. Input the required Username and Password to login to Exchange 2016

5 Configure Other APV Features for Exchange

5.1 HTTP Rewrite/Redirect

Typically, client Exchange access is via HTTPS for privacy and security considerations. However, the client may accidentally 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, from WebUI:

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. The **VIRTUAL SERVICE INFORMATION** screen opens.
3. Check the box for "**Redirect ALL HTTP Requests to HTTPS**" and **SAVE CHANGES**.

5.2 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.
3. Note: By default, the following MIME types are compressed by the APV appliance for all browsers (User-Agent):
    a. Text (text/plain)
    b. HTML (text/HTML)
    c. 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.

1. Click the ***Compression Type*** tab. The **COMPRESSION MIME TYPES** screen opens.
    a. Depending on the WebUI you are using, click **Apply Tested User Agents** or other label. More compression types are added to the screen.
    b. For each **Add MIME Type**, enter **Mozilla** for the User Agent and add "JS", "CSS", and "PDF" to complete.

Note: To view compression statistics, from **WebUI, 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**.

5.3 Create the SSL Virtual Hosts

To terminate SSL communication from the client, the APV needs an SSL Virtual Host to support SSL/TLS communication. Each SSL Virtual Host has its own SSL Private Key, SSL Certificate, and SSL/TLS parameters. One SSL Virtual Host can serve multiple SLB Virtual Services, which may have different application types (on top of SSL/TLS), such as TCPS, HTTPS, FTPS, POPS, SMTPS, or IMAPS. Additional SSL/TLS protocol/cipher options and error handling can be configured for each SSL Virtual Host 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 (optional) select the SLB Virtual Service (**vs_mail_https**). Then click **Save.**
3. Repeat steps 1 and 2 for all the SLB Virtual Services that need the same SSL termination.

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

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 the Certificate/Key for the SSL Virtual Host:

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

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.

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 convert the PFX file to the unencrypted PEM format, and 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 Host. 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).

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

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 displayed if no certificate chain from a trusted root CA can be established. The new root and intermediate certificates can be imported by using the “ssl import rootca” and “ssl import interca <vhostname>” commands, or WebUI.

5.4 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, **Config Mode**.

1. Navigate to **SSL** -> **Virtual Hosts** -> and double click **SSL Virtual Hosts** to select it.

2. From **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.

6 Conclusion

This concludes the Array Networks APV deployment guide for Microsoft Exchange 2016. Array Networks APV/vAPV 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 Exchange server deployments.

Appendix:

CLI Configuration Example 1 – L4 Load Balancing for Exchange 2016

```
slb real tcp "rs_mbx01_https" 10.2.40.180 443 1000 tcp 3 3
slb real tcp "rs_mbx01_imaps" 10.2.40.180 993 1000 tcp 1 1
slb real tcp "rs_mbx01_pop3s" 10.2.40.180 995 1000 tcp 1 1
slb real tcp "rs_mbx01_smtp" 10.2.40.180 25 1000 tcp 1 1
slb real tcp "rs_mbx02_https" 10.2.40.181 443 1000 tcp 3 3
slb real tcp "rs_mbx02_imaps" 10.2.40.181 993 1000 tcp 1 1
slb real tcp "rs_mbx02_pop3s" 10.2.40.181 995 1000 tcp 3 3
slb real tcp "rs_mbx02_smtp" 10.2.40.181 25 1000 tcp 3 3

slb group method "gp_mbx_https" lc 32 no
slb group method "gp_mbx_imaps" lc 32 no
slb group method "gp_mbx_pop3s" lc 32 no
slb group method "gp_mbx_smtp" lc 32 no
slb group member "gp_mbx_https" "rs_mbx01_https" 1 0
slb group member "gp_mbx_https" "rs_mbx02_https" 1 0
slb group member "gp_mbx_imaps" "rs_mbx01_imaps" 1 0
slb group member "gp_mbx_imaps" "rs_mbx02_imaps" 1 0
slb group member "gp_mbx_pop3s" "rs_mbx01_pop3s" 1 0
slb group member "gp_mbx_pop3s" "rs_mbx02_pop3s" 1 0
slb group member "gp_mbx_smtp" "rs_mbx01_smtp" 1 0
slb group member "gp_mbx_smtp" "rs_mbx02_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_mbx_https"
slb policy default "vs_mail_imaps" "gp_mbx_imaps"
slb policy default "vs_mail_pop3s" "gp_mbx_pop3s"
slb policy default "vs_mail_smtp" "gp_mbx_smtp"
```

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

```
health request 10 "GET /owa/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 14 "GET /EWS/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"

slb real http "rs_mbx01_ActiveSync" 10.2.40.180 80 1000 http 3 3
slb real http "rs_mbx01_autodiscover" 10.2.40.180 80 1000 http 3 3
slb real http "rs_mbx01_ews" 10.2.40.180 80 1000 http 3 3
slb real http "rs_mbx01_owa" 10.2.40.180 80 1000 http 3 3
slb real http "rs_mbx01_rpc" 10.2.40.180 80 1000 http 3 3
slb real http "rs_mbx02_ActiveSync" 10.2.40.181 80 1000 http 3 3
slb real http "rs_mbx02_autodiscover" 10.2.40.181 80 1000 http 3 3
slb real http "rs_mbx02_ews" 10.2.40.181 80 1000 http 3 3
slb real http "rs_mbx02_owa" 10.2.40.181 80 1000 http 3 3
slb real http "rs_mbx02_rpc" 10.2.40.181 80 1000 http 3 3

health server "rs_mbx01_autodiscover" 16 16
health server "rs_mbx01_ews" 14 14
health server "rs_mbx01_owa" 10 10
health server "rs_mbx01_rpc" 12 12
health server "rs_mbx01_ActiveSync" 17 17
health server "rs_mbx02_autodiscover" 16 16
health server "rs_mbx02_ews" 14 14
health server "rs_mbx02_owa" 11 11
health server "rs_mbx02_owa" 10 10
health server "rs_mbx02_rpc" 12 12
health server "rs_mbx02_ActiveSync" 17 17

slb group method "gp_activesync" lc 32 no
slb group method "gp_autodiscover" lc 32 no
slb group method "gp_owa" lc 32 no
slb group method "gp_ews" lc 32 no
slb group method "gp_rpc" lc 32 no

slb group member "gp_activesync" "rs_mbx01_ActiveSync" 1 0
slb group member "gp_activesync" "rs_mbx02_ActiveSync" 1 0
slb group member "gp_autodiscover" "rs_mbx01_autodiscover" 1 0
slb group member "gp_autodiscover" "rs_mbx02_autodiscover" 1 0
slb group member "gp_ews" "rs_mbx01_ews" 1 0
slb group member "gp_ews" "rs_mbx02_ews" 1 0
slb group member "gp_owa" "rs_mbx01_owa" 1 0
slb group member "gp_owa" "rs_mbx02_owa" 1 0
slb group member "gp_rpc" "rs_mbx01_rpc" 1 0
slb group member "gp_rpc" "rs_mbx02_rpc" 1 0
```

```
slb virtual https "vs_mail_https" 10.1.61.13 443 arp 0

slb policy qos url "p_owa" "vs_mail_https" "gp_owa" "/owa" 100
slb policy qos url "p_rpc" "vs_mbail_https" "gp_rpc" "/rpc" 120
slb policy qos url "p_ews" "vs_mail_https" "gp_ews" "/ews" 140
slb policy qos url "p_ews" "vs_mail_https" "gp_owa" "/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_mail_https"  "gp_owa"

ssl host virtual "ssl_vhost_1" "vs_mail_https"
ssl start "ssl_vhost_1"
```

CLI Configuration Example 3 – L7 QoS URL SLB + SSL Bridge

```
health request 10 "GET /owa/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 14 "GET /EWS/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"

slb real https "rs_mbx01_ActiveSync" 10.2.40.180 443 1000 http 3 3
slb real https "rs_mbx01_autodiscover" 10.2.40.180 443 1000 http 3 3
slb real https "rs_mbx01_ews" 10.2.40.180 443 1000 http 3 3
slb real https "rs_mbx01_owa" 10.2.40.180 443 1000 http 3 3
slb real https "rs_mbx01_rpc" 10.2.40.180 443 1000 http 3 3
slb real https "rs_mbx02_ActiveSync" 10.2.40.181 443 1000 http 3 3
slb real https "rs_mbx02_autodiscover" 10.2.40.181 443 1000 http 3 3
slb real https "rs_mbx02_ews" 10.2.40.181 443 1000 http 3 3
slb real https "rs_mbx02_owa" 10.2.40.181 443 1000 http 3 3
slb real https "rs_mbx02_rpc" 10.2.40.181 443 1000 http 3 3

health server "rs_mbx01_autodiscover" 16 16
health server "rs_mbx01_ews" 14 14
health server "rs_mbx01_owa" 10 10
health server "rs_mbx01_rpc" 12 12
health server "rs_mbx01_ActiveSync" 17 17
health server "rs_mbx02_autodiscover" 16 16
health server "rs_mbx02_ews" 14 14
health server "rs_mbx02_owa" 11 11
health server "rs_mbx02_owa" 10 10
health server "rs_mbx02_rpc" 12 12
health server "rs_mbx02_ActiveSync" 17 17

slb group method "gp_activesync" lc 32 no
slb group method "gp_autodiscover" lc 32 no
slb group method "gp_owa" lc 32 no
slb group method "gp_ews" lc 32 no
slb group method "gp_rpc" lc 32 no

slb group member "gp_activesync" "rs_mbx01_ActiveSync" 1 0
slb group member "gp_activesync" "rs_mbx02_ActiveSync" 1 0
slb group member "gp_autodiscover" "rs_mbx01_autodiscover" 1 0
slb group member "gp_autodiscover" "rs_mbx02_autodiscover" 1 0
slb group member "gp_ews" "rs_mbx01_ews" 1 0
slb group member "gp_ews" "rs_mbx02_ews" 1 0
slb group member "gp_owa" "rs_mbx01_owa" 1 0
slb group member "gp_owa" "rs_mbx02_owa" 1 0
slb group member "gp_rpc" "rs_mbx01_rpc" 1 0
slb group member "gp_rpc" "rs_mbx02_rpc" 1 0
```

```
slb virtual https "vs_mail_https" 10.1.61.13 443 arp 0

slb policy qos url "p_owa" "vs_mail_https" "gp_owa" "/owa" 100
slb policy qos url "p_rpc" "vs_mbail_https" "gp_rpc" "/rpc" 120
slb policy qos url "p_ews" "vs_mail_https" "gp_ews" "/ews" 140
slb policy qos url "p_ews" "vs_mail_https" "gp_owa" "/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_mail_https"  "gp_owa"

ssl globals verifycert off
ssl host virtual "ssl_vhost_1" "vs_mail_https"
ssl start "ssl_vhost_1"
ssl host real "ssl_real_1" "rs_https_mbx01_ActiveSync"
ssl host real "ssl_real_1" "rs_https_mbx01_autodiscover"
ssl host real "ssl_real_1" "rs_https_mbx01_ews"
ssl host real "ssl_real_1" "rs_https_mbx01_owa"
ssl host real "ssl_real_1" "rs_https_mbx01_rpc"
ssl host real "ssl_real_1" "rs_https_mbx02_ActiveSync"
ssl host real "ssl_real_1" "rs_https_mbx02_autodiscover"
ssl host real "ssl_real_1" "rs_https_mbx02_ews"
ssl host real "ssl_real_1" "rs_https_mbx02_owa"
ssl host real "ssl_real_1" "rs_https_mbx02_rpc"
ssl settings protocol "ssl_real_1" "TLSv1"
ssl start "ssl_real_1"
```

About Array Networks

Array Networks is a global leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore® software, Array application delivery, WAN optimization and secure access solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is headquartered in Silicon Valley, is backed by over 250 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

Nov 2016 Rev. A