Deployment Guide
July-2015 rev. A

Deploying Array Networks APV Series Application Delivery Controllers with VMware Horizon View

1 Introduction

This guide details the configuration of Array Networks APV Series application delivery controllers for deployment with VMware Horizon View. It includes details of ports/services that must be load balanced, topology considerations for the various VMware Horizon View servers, and steps on how to configure the appliances.

For an introduction to setting up an APV Series appliance, as well as more technical information, please refer to our quick-start guides and full administration manuals for the appliance's WebUI.

1.1 VMware Horizon View

VMware Horizon View (formerly VMware View) is a virtual desktop infrastructure solution that simplifies desktop management and provides users with access when needed, regardless of their location. For high availability and scalability, VMware recommends that multiple View Servers be deployed in a load-balanced cluster.

Please refer to the following VMware link for additional Horizon View architecture and planning information.

https://pubs.vmware.com/horizon-view-60/topic/com.vmware.ICbase/PDF/horizon-view-60-architecture-planning.pdf

1.2 Array Networks APV Series Appliances

Array Networks' APV Series provides a strategic point of control of optimizing the availability, security and performance of enterprise applications, IP data services and data center equipment. Leveraging robust and powerful distribution algorithms, health check mechanisms and failover capabilities, the APV Series maintains connections, ensures persistence, directs traffic away from failed data centers, and intelligently distributes application services between multiple nodes and locations for optimized performance and availability.

APV Series ensures that both end users and administrators obtain the optimal user experience by creating a highly available and scalable platform that achieves the highest levels of reliability through network optimization.

The APV Series is available as a dedicated hardware appliance or as the vAPV virtual application delivery controller.

1.3 Prerequisites & Assumptions

It is assumed that the reader of this deployment guide is a network administrator or a person otherwise familiar with networking and general computer terminology. Software versions supported:

VMware Horizon View: View Connection Server v5.2, v5.3, v6.x and later

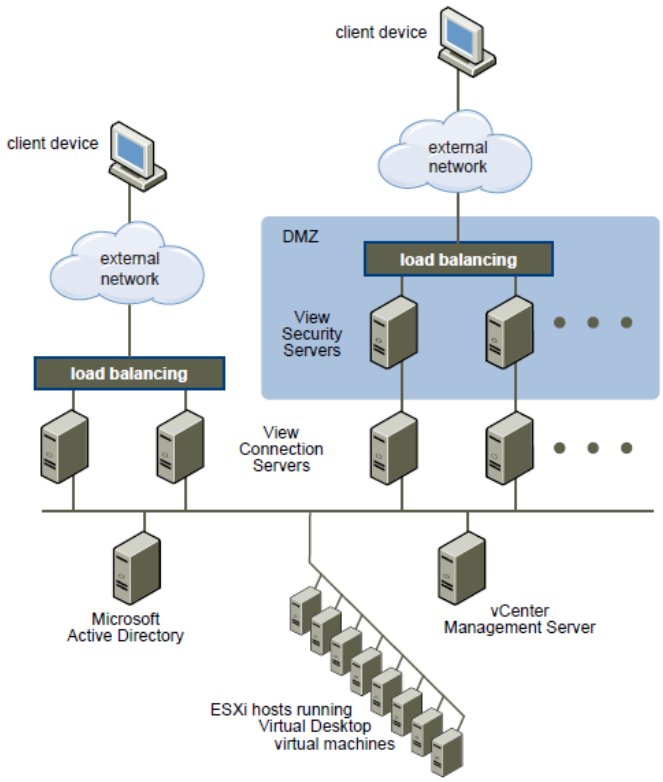
ArrayOS APV 8.4.0.x, 8.5.0.x and later

Verify that each View Connection Server instance or security server has a security certificate that can be fully verified by using the host name that you enter in the browser.

In this example, the View clients are running the Windows 7 Operating System.

2 VMware View Load Balancing

To support VMware Horizon View high availability, the best practice is to load balance two Security Servers or Connection Servers.



2.1 VMware View Servers

VMware Horizon View supports two types of servers:

Connection Server

The View Connection Server acts as a broker for client connections. It authenticates users through Windows Active Directory and directs the requests to the appropriate virtual machine, physical or blade PC, or Windows Terminal Services server. The Connection Server can be the gateway for the View Client to access the virtual desktop machine.

Security Server (optional, for external access)

A View Security Server is a special instance of a View Connection Server that runs a subset of View Connection Server functions. A Security Server is used to provide an additional layer of security between the Internet and the internal network. A Security Server resides within a DMZ and acts as a proxy host for connections inside the trusted network. Each Security Server is paired with an instance of View Connection Server and forwards all traffic to that instance.

2.2 Port Protocol Uses

- 443 TCP HTTPS

- 4172 TCP PCoIP
- 4172 UDP PCoIP
- 8443 TCP Blast (HTML Access)

2.3 View Client Connection Process

VMware Horizon View clients have two connection stages to access the View Desktops. They are:

First Connection: Initial connection, access the portal, logon and authentication, obtain the session data (including Virtual Desktop access information), etc. We refer as to this as portal access (HTTPS/443). This type of connection is always load balanced by the APV Series.

Second Connection: The client connects to the Virtual Desktop machine (per session data). It can be RDP (HTTPS/443), Blast (TCP/8443), or PCoIP (UDP/TCP, port 4172). Depending upon the View Servers' (or Security Server) configuration, the second connection can bypass or NAT through the APV Series.

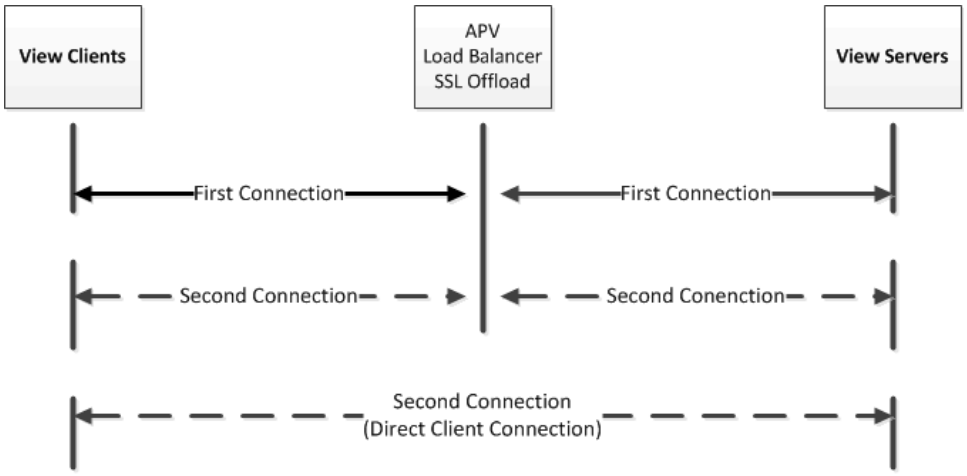
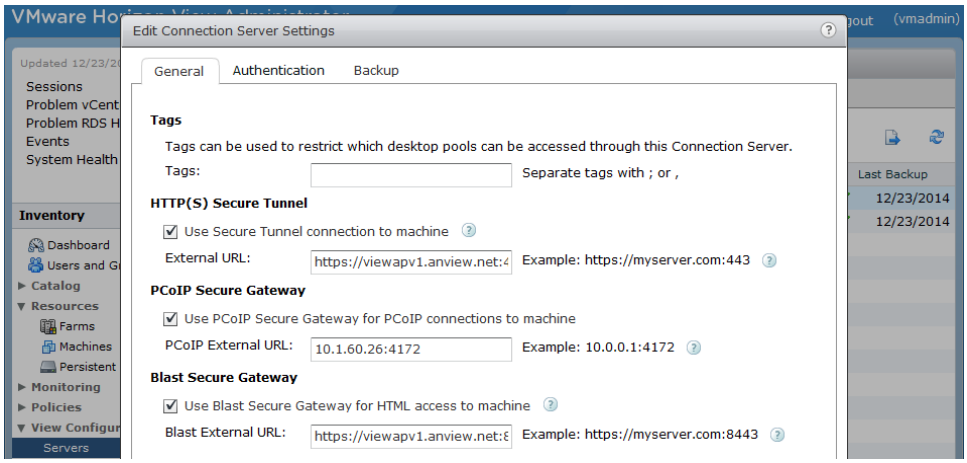


Figure 1: View Client Connection Process

The point at which the second View Client connection connects is controlled by the View Server (or Security Server External URL) Settings. It can be:

- Direct access to the Virtual Desktop machine, bypassing the APV and View Servers. This is the default for View Servers; the settings are no HTTP(S) Secure Tunnel, no PCoIP Secure Gateway, and no Blast Secure Gateway.
- Use the View Server as the proxy for the View Clients. This option requires configuring an external URL for the Connection Server. For example, if 10.1.60.26:4172 is used, the external firewall (or APV Series) would NAT 10.1.60.26 to the Connection Server.



- Persistence (aka Server Affinity). This requires that View client requests are forwarded to the same View Server for the duration of the session. This can be achieved using either source IP persistence or application cookie (JSESSIONID or insert cookie) persistence for HTTP/HTTPS. Source IP persistence can incur an uneven load in a mega proxy scenario, since one IP is used by many clients. The application cookie method is better for load distribution, but requires SSL offloading to see clear text traffic (see below).
- SSL Offloading (option, required by L7). In this method, View Clients must use HTTPS to connect to View Manager. If your View Clients connect to load balancers or other intermediate servers that pass on the connections to View Connection Server instances or Security Servers, you can offload SSL to the intermediate servers.

To learn how to configure View Servers for SSL offload, please see the following VMware link:

https://pubs.vmware.com/view-51/index.jsp?topic=%2Fcom.vmware.view.administration.doc%2FGUID-FBEBF977-6955-4A7D-8438-AD82C5AD9077.html

Technical Note

Per VMware, if View Clients use smart card authentication, the clients must make HTTPS connections directly to the View Connection Server or Security Server. SSL offloading is not supported with smart card authentication.

3 Deployment Overview

There are many options to deploy View Servers and the APV Series load balancer. Basically the options can be either internal or external clients (with or without View Security Server, or IP usage). Additional options include server persistence, with or without SSL offloading or bridging, and additional health checks for the View Servers.

3.1 Internal Client Access: Load Balancing Connection Servers

3.1.1 Scenario 1 – L7 Load Balance the First Connection, with Session Persistence

In this scenario, in which the APV Series is load balancing View Connection Servers, the Connection Server is not gateway enabled (or enabled without an external URL). For the first connection, the View client will access the APV Series, then the APV appliance selects a Connection Server for login based on the JSESSIONID cookie. Or it can select an available Connection Server per load balancing algorithm for new a session. For the second connection, the View client bypasses the APV Series, and directly connects to the Virtual Desktop machine (or Connection Server).

This scenario requires a single Virtual Service, SSL offload, with cookie persistence for the View Client to the same Connection Server (the latter allows load distribution among View Servers to be more even compared with persistent IP). For the second connection, the client directly accesses (or NATs through the APV to) the Connection Server or Virtual Desktop machines for fast access. In this scenario the APV load is reduced since for the second connection, Virtual Desktop display traffic bypasses the APV. However, this uses multiple IPs for each Virtual Desktop machine.

3.1.2 Scenario 2 – L4 Load Balance All View Connections with IP Persistence

This scenario provides better security, access control and management by not allowing View clients to directly access Virtual Desktop machines by using a single IP for all View traffic. The Connection Server acts as the Gateway for View traffic and external URLs are configured to utilize the APV virtual services for load balancing.

In this scenario, the APV uses a single IP with different ports/protocols for multiple Virtual Services and uses the client IP to ensure that View clients connect to the same Connection Server for the duration of the session for both the first and second connections. The Connection Server has its external URL configured to direct View client traffic to the APV Series.

3.2 External Client Access; Load Balancing Security Servers

3.2.1 Scenario 3 – L4 Load Balance all View Connections with IP Persistence

In this scenario, a single IP with multiple Virtual Services with different ports/protocols is used to conserve public IP usage for external clients' access. This scenario also uses IP persistency to ensure that clients connect to the same Security Server for the duration of the session.

The View Security Server external URLs are pointed to the APV virtual services. The first and second connections both go through the APV virtual services to access the

Security Server. The clients need to be persistent to the same Security Server, so IP persistency is used.

In addition, in this scenario if the paired connection is down, the Security Server needs to be marked as down as well.

4 Configuration Steps

Please ensure 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 the Array Networks Pilot Login, click **Login** to enter (default is no password enabled).

4.1 Scenario 1 – L7 Load Balance the First Connection, with Session Persistence

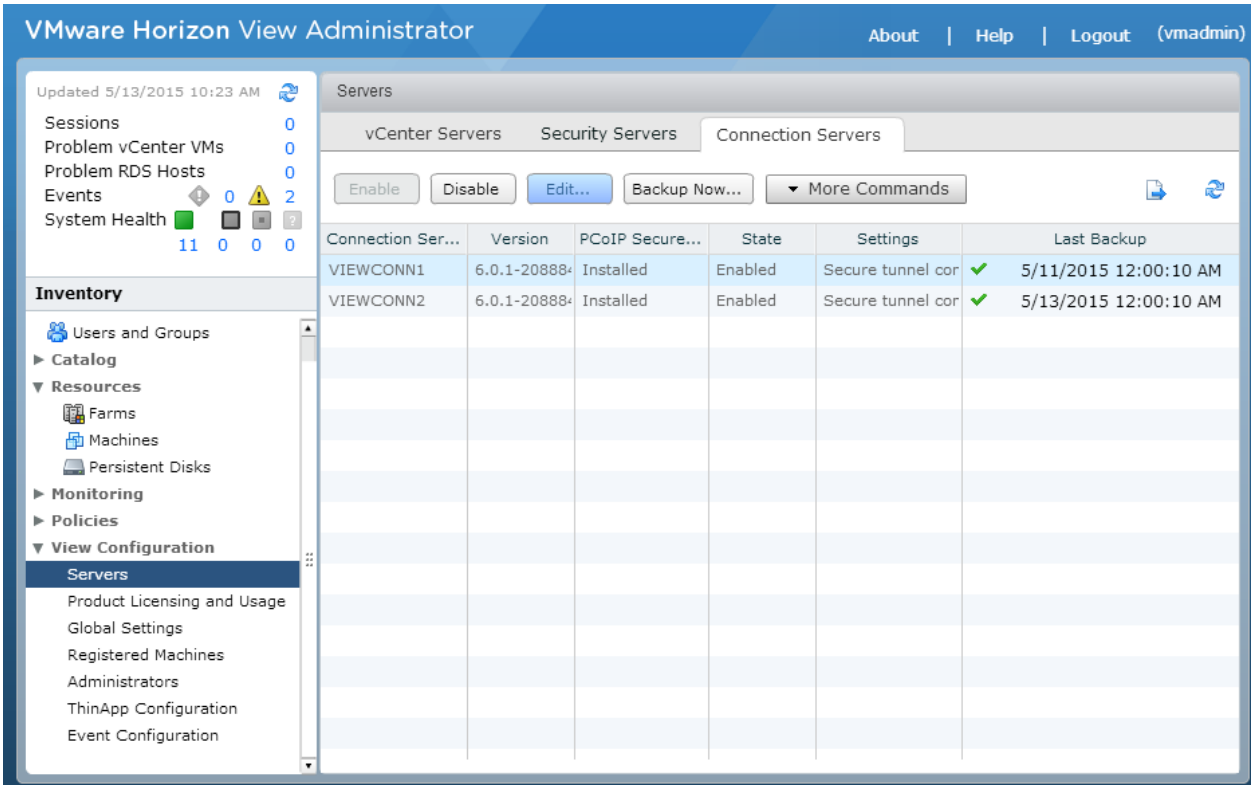
This scenario uses APV Series load balancing for the first View client connection, with SSL offload via cookie for server persistence for better load distribution. The second connections will bypass the APV with different FQDNs or IPs.

4.1.1 View Server Configuration

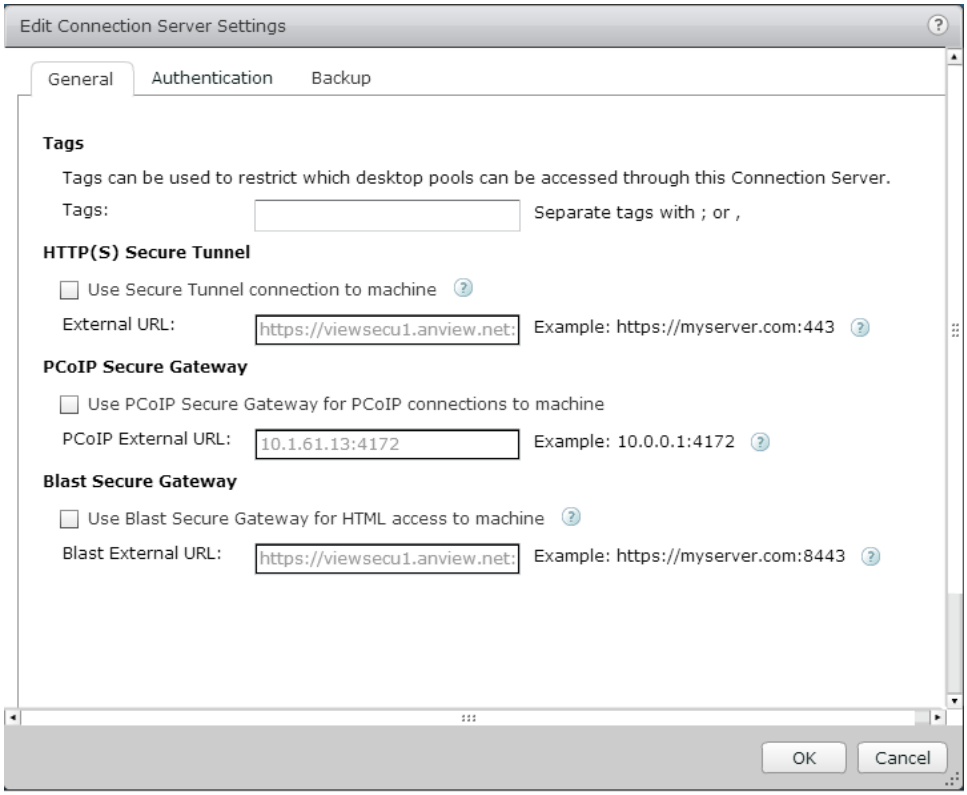
The Connection Server will let View Clients directly access Virtual Desktop machines or Connection Servers (Gateways).

VMware Horizon View configuration:

View Configuration > **Servers** > **Connection Servers** > **Edit**.



Uncheck all so that View clients can directly access the Virtual Desktop machine.



4.1.2 APV Configuration

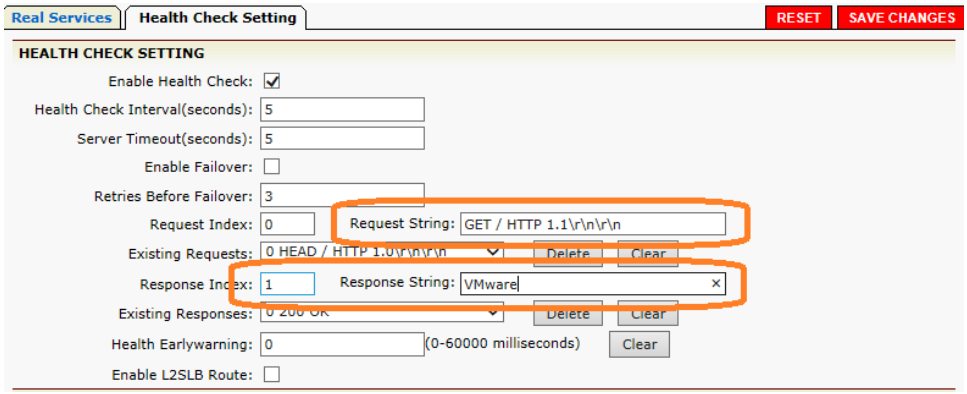
Define the Application Health Check

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

Request Index	Request String	Response Index	Response String
0	GET HTTP 1.1\r\n\r\n	1	VMware

To configure the content-based Health Check, enter WebUI, Mode: **Config**.

1. Select **Real Services** from the sidebar. Click the **Health Check Setting** tab. The **HEALTH CHECK SETTING** screen opens.
2. For Request Index: 0, enter "**GET / HTTP 1.1\r\n\r\n**" and for Response Index: 1, enter "**VMware**". Then click **SAVE CHANGES**.



If the View servers have other options to report their health condition, enter the URL and expected content into the Health Check Request/Response Table.

Create Real Services – Connection Server, Secure Tunnel

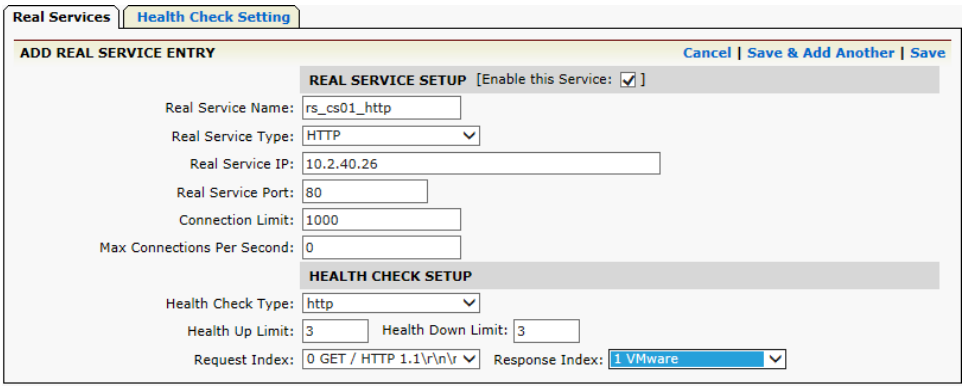
On the APV Series, the Real Services are two View Connection Servers. The Connection Server is SSL offloading to the APV, so the secured tunnel is via port 80/HTTP. Following is the summary of all Real Services that need to be added to the APV configuration.

Real Service Name (Connection Server)	Real Service Type	Real Service IP	Real Service Port	Health Check Type(index)
rs_cs01_http	HTTP	10.2.40.26	80	HTTP (0/1)
rs_cs02_http	HTTP	10.2.40.28	80	HTTP (0/1)

Table 1 - Real Services for Connection Servers

To configure the Real Services, 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 servers. Enter a unique name for the Real Service Name (***rs_cs01_http***). From the Real Service Type pulldown, select "**HTTP**". Enter the Real Service IP/Port (**10.2.40.26/80**) which is used by Connection Server 1.
3. Select **http** as the Health Check Type. For the Request Index and Response Index, pull down the selection and select the corresponding entry (Request Index: 0, Response Index: 1) as in the above table. Then click **Save** to add the Real Service.



4. Repeat steps 1-3 as above: add all Real Services according to Table 1 – Real Services for Connection Servers.

Create the Group

The APV Server Load Balancing (SLB) Group defines the load balancing method and the set of servers in the group. The following table contains all group information that needs to be entered into the APV system. Using the application session cookie method is recommended to achieve better load distribution.

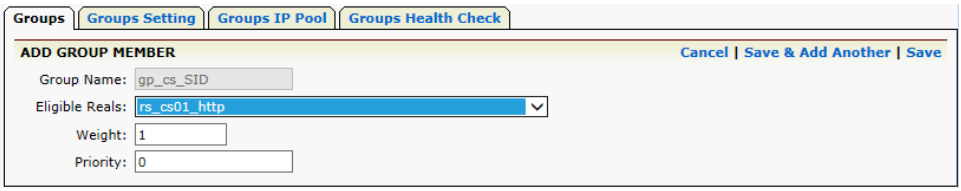
Group Name	Group Method	Group Member
gp_cs_SID	Persistence (Cookie: JSESSIONID)	rs_cs01_http
		rs_cs02_http

Table 2 - SLB Group for Connection Servers

To create a 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 we used "**gp_cs_SID**". From the Group Method pull down menu, select the "**Persistence**", Session Type: **string**, First Choice: **Least Connections**. Click **Add** to create the SLB group.

3. To add Real Services to the SLB group, open the **GROUPS LIST** by double clicking on the SLB Group (**gp_cs_SID**). The **GROUP INFORMATION** screen opens.
4. Under the "**GROUP MEMBERS**" section, click on "**Add**", and the **ADD GROUP MEMBER** screen opens.
5. From the Eligible Reals pull down menu, select "**rs_cs01_http**", click **Save & Add Another** and select "**rs_cs02_http**". Then click "**Save**".



6. To add the persistence cookie information, select the group **gp_cs_SID**, then pull down to access the **PERSISTENCE LIST**. Click **Add**, and the **ADD ENTRY PERSISTENCE** screen opens.

7. For both **request and response Modes**, select Type: **cookie** and Field Name: **JSESSIONID**. Click **Save** to enter the cookie information.

Create the Virtual Service

Following is the one-arm Virtual Service information that used for this example. For a two-arm configuration, the SLB Virtual Service and the Connection Servers are on different network segments. If the View clients need to be NATed through the APV appliance, see Appendix: 6.1 Configure Static NAT for Server Access.

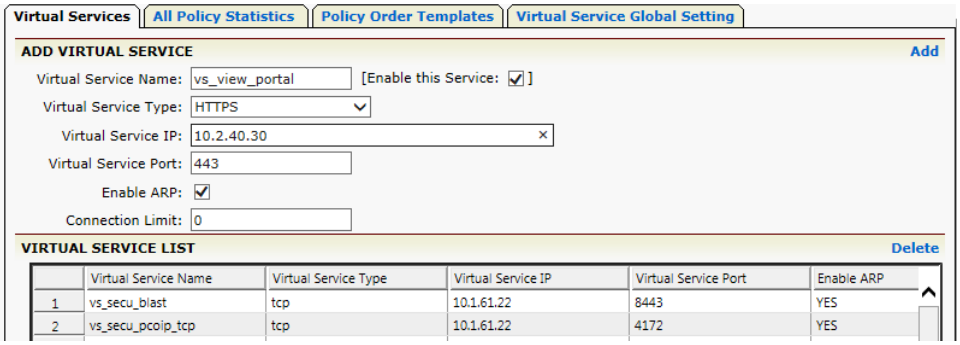
Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	SLB Policy	Associate Groups
vs_view_portal	HTTPS	10.2.40.30	443	Default	gp_cs_SID

Table 3 - Virtual Service for Connection Server

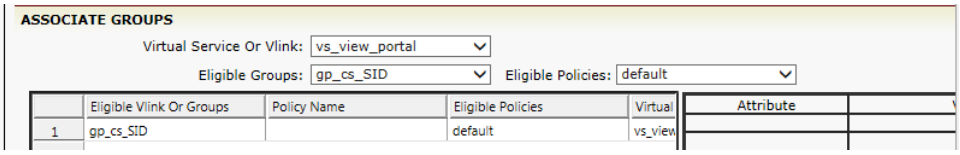
To create a new SLB Virtual Service, enter WebUI, Mode: **Config**.

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

2. Enter a unique name for the Virtual Service Name (**vs_view_portal**). Use the check box to enable the virtual service. From the Virtual Service Type pull down menu, select "HTTPS". Enter the Virtual Service IP and Port (**10.2.40.30/443**). 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.

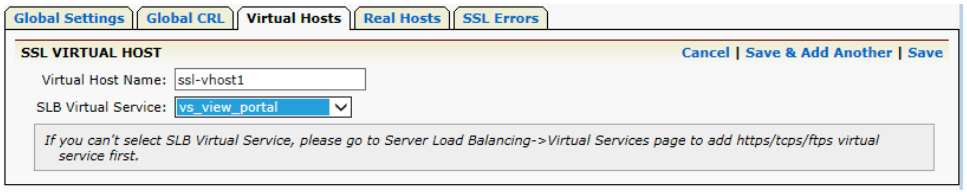


3. Select the Virtual Service (**vs_view_portal**) on the **VIRTUAL SERVICE LIST** by double clicking on it. The **VIRTUAL SERVICE INFORMATION** screen opens with a new series of tabs for completing the virtual services configuration.
4. Pull down to the **ASSOCIATE GROUPS** section, and from the **Eligible vLink or Groups** pull down menu select "**gp_cs_SID**" and in the **Eligible Policies** pull down menu, select "**default**". Click **Add** to associate the Group with the Virtual Service.

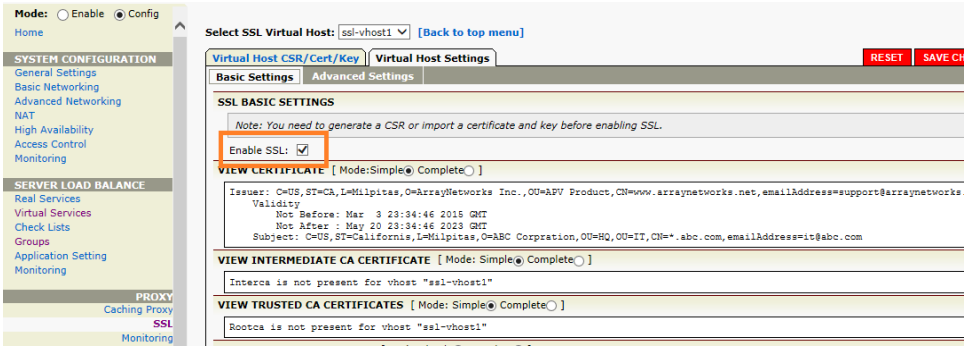


Because the Virtual Service type is HTTPS, we need to associate an SSL Virtual Host – if the SSL Virtual Host was not created previously, see Appendix: 6.2 Configure SSL Virtual Host.

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



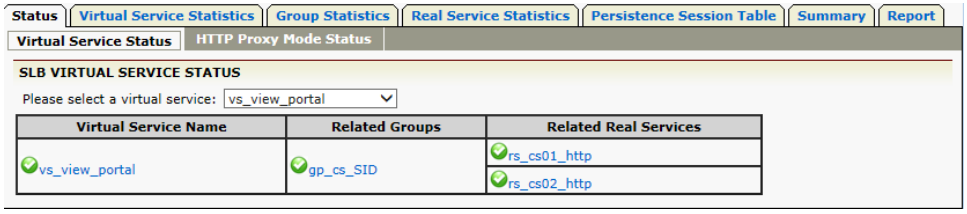
7. If SSL Virtual Host is not enabled, we need to enable it. To enable it, select **"SSL"** from the sidebar. Click **Virtual Hosts.** Double click the SSL Virtual Host on the list (**ssl-vhost1**). Then click **Virtual Host Settings**.
8. Under **SSL BASIC SETTNGS**, check the **Enable SSL** box if it is not already checked. Then click **SAVE CHANGES** to enable the SSL.



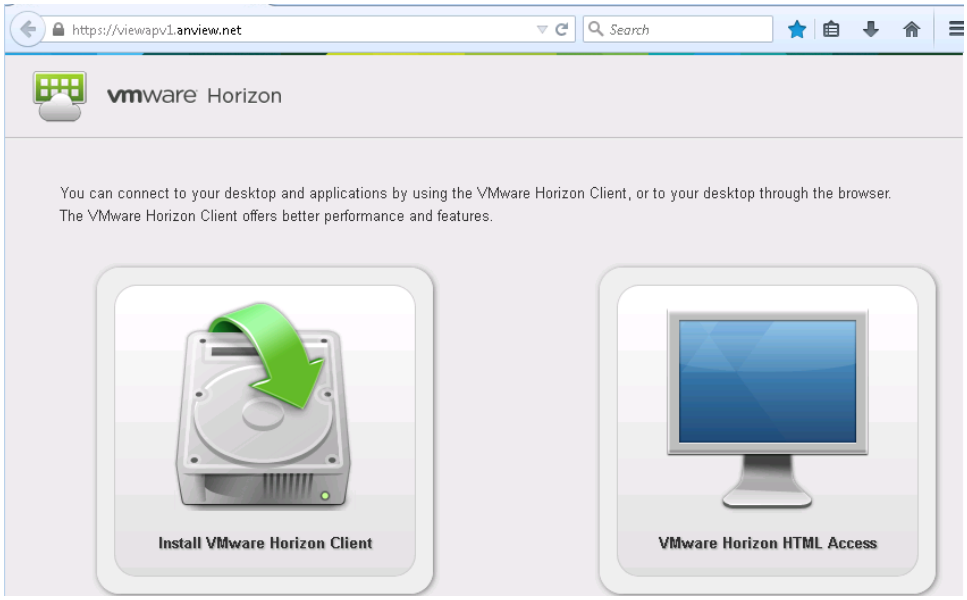
4.1.3 Validate the Configuration & Application

Validate that the basic configuration is functioning correctly:

1. From WebUI, **SERVER LOAD BALANCE**, **Monitoring** -> **Status** -> **Virtual Service Status**. Select "**vs_view_portal**" 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.



To verify that the View client works properly with the APV Series, from View Clients, enter the URL/IP to access the View portal.

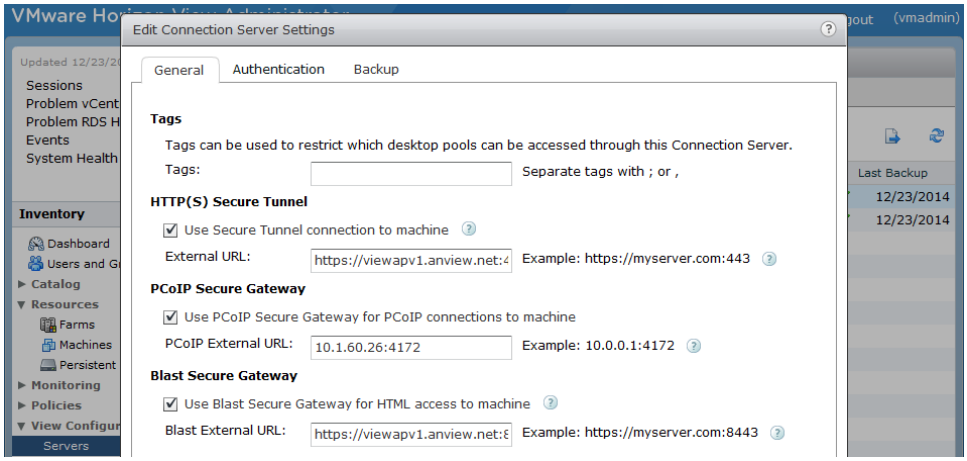


4.2 Scenario 2 – L4 Load Balance All View Connections with IP Persistence

For this scenario, all View traffic to the Connection Server will pass through the APV appliance.

4.2.1 View Server Configuration

Enable HTTP(S) Secure tunnel, PCoIP Secure Gateway, and Blast Secure Gateway. Set the external URLs to the APV Virtual Services.



4.2.2 APV Configuration

The APV system needs to be configured with multiple Virtual and Real Services to proxy all View traffic via a single IP.

Define Application Health Check

For the HTTP content application health check, the request/response configuration can be the same as Section 4.1.2.

Create Real Services

Real Services are two Connection Servers. The Connection Server will gateway all View traffic, so we need include secure tunnel, PCoIP and Blast support as Real Services.

Following is the summary of all Real Services need add to the APV configuration. The **rs_cs01_http** and **rs_cs02_http** configuration are the same as 4.1.2; however we need add additional real services.

Real Service Name (Connection Server)	Real Service Type	Real Service IP	Real Service Port	Health Check Type
rs_cs01_http	HTTP	10.2.40.26	80	HTTP (0/1)
rs_cs01_blast	**TCP**	**10.2.40.26**	**8443**	**TCP**
rs_cs01_pcoip_tcp	**TCP**	**10.2.40.26**	**4172**	**TCP**
rs_cs01_pcoip_udp	**UDP**	**10.2.40.26**	**4172**	**ICMP**
rs_cs02_http	HTTP	10.2.40.28	80	HTTP (0/1)
rs_cs02_blast	**TCP**	**10.2.40.28**	**8443**	**TCP**
rs_cs02_pcoip_tcp	**TCP**	**10.2.40.28**	**4172**	**TCP**
rs_cs02_pcoip_udp	**UDP**	**10.2.40.28**	**4172**	**ICMP**

Table 4 - Real Services for Connection Servers

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

1. Select **Real Services** from the sidebar. Click **Add**. The **ADD REAL SERVICE ENTRY** screen opens.
2. Enter a unique name for the Real Service Name; in our example, we entered "**rs_cs01_blast**". Select **TCP** as the Real Service Type, enter IP addresses/Port "**10.2.40.26/8443**" which is used by the Connection Server 1 Blast service.
3. Select **TCP** as the Health Check Type.
4. Repeat steps 1 through 3 to enter all Real Services, using the default health setup for TCP/UDP.

Optional: Additional Health Check

A Connection Server hosts multiple services; if one of the services is down, we need to mark the whole server as down, so the APV can divert new View client access to other, healthy, Connection Servers. For example, if Blast or PCoIP are down, the APV can utilize the Additional Health Check to mark the portal access as down for a Connection Server.

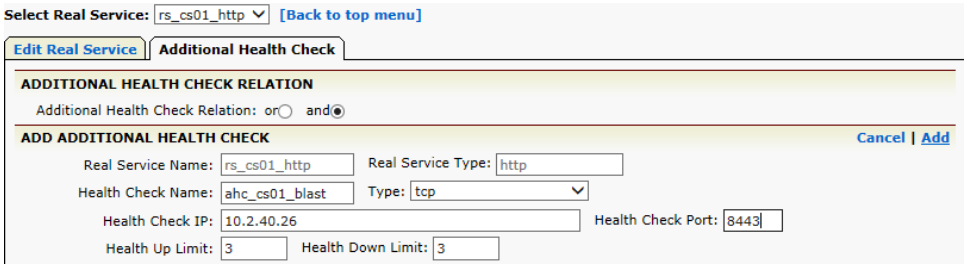
Additional Health Check Name	Real Service Name	Health Check IP	Health Check Port	Health Check Type
ahc_cs01_blast	rs_cs01_http	10.2.40.26	8443	TCP
ahc_cs01_pcoip	rs_cs01_http	10.2.40.26	4172	TCP
ahc_cs02_blast	rs_cs02_http	10.2.40.28	8443	TCP
ahc_cs02_pcoip	rs_cs02_http	10.2.40.28	4172	TCP

Table 5 - Additional Health Checks for Connection Servers

To configure the additional health checks as a Real Service, enter WebUI, Mode: **Config**.

1. Select **Real Services** from sidebar; double click the Real Service (rs_cs01_http), and then click **Additional Health Check**.

2. Under **ADD ADDITIONAL HEALTH CHECK,** enter a unique name for the **Health Check Name** (ahc_cs01_blast in the example). Select the type (tcp), and enter the target Health Check IP and Port (10.2.40.26/8443). Click **Add**.



3. Repeat steps 1 and 2 to enter all additional health checks from Table 5 – Additional Health Checks.

Create Groups

The following table shows the groups that are used in the example. Since View Clients need get to the same Connection Server for different View services, we are using "HASH IP" for this example. As there are multiple groups for a server, we need Real Service names for a server in sync (sorted with the same position) among all groups.

Group Name	Group Method	Group Member
gp_cs_http	Hash IP	rs_cs01_http
		rs_cs02_http
gp_cs_blast	Hash IP	rs_cs01_blast
		rs_cs02_blast
gp_cs_pcoip_tcp	Hash IP	rs_cs01_pcoip_tcp
		rs_cs02_pcoip_tcp
gp_cs_pcoip_udp	Hash IP	rs_cs01_pcoip_udp
		rs_cs02_pcoip_udp

Table 6 - Group

To create an SLB Group, enter 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 we used "**gp_cs_http**". From Group Method pull down menu, select "**Hash IP**". Click **Add** to create the SLB group.
3. To add Real Services to the SLB group, on the **GROUPS LIST** double click to select the SLB Group (**gp_cs_http**). The **GROUP INFORMATION** screen opens.
4. Under the "**GROUP MEMBERS**" section, click "**Add**". The **ADD GROUP MEMBER** screen opens.
5. From the Eligible Reals pull down menu, select "**rs_cs01_http**", click **Save & Add Another** and select "**rs_cs02_http**" and "**Save**".

6. Repeat steps 1 through 5 for all other groups and members.

Create Virtual Services

The following table lists all Virtual Services for the scenario:

Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	SLB Policy	Associate Groups
vs_view_portal	HTTPS	10.2.40.30	443	Default	gp_cs_http
vs_view_blast	**TCP**	**10.2.40.30**	**8443**	**Default**	**gp_cs_blast**
vs_view_pcoip_tcp	**TCP**	**10.2.40.30**	**4172**	**Default**	**gp_cs_pcoip_tcp**
vs_view_pcoip_udp	**UDP**	**10.2.40.30**	**4172**	**Default**	**gp_cs_pcoip_udp**

Table 7 - Virtual Services

Virtual Service **vs_view_portal** is the same as in Scenario 1. For detailed configuration steps, please refer Section 4.1.2.

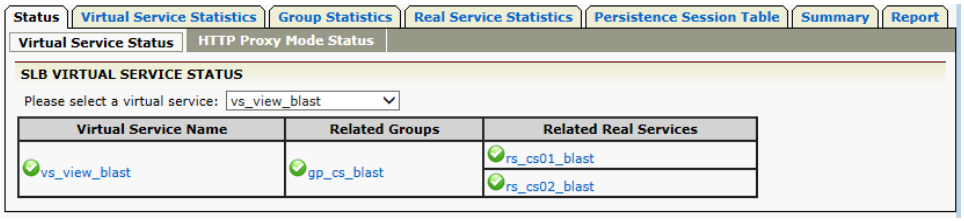
To create additional SLB Virtual Services, enter WebUI, Mode: **Config.**

1. Select **Virtual Services** from the sidebar. The "**ADD VIRTUAL SERVICE**" screen opens.
2. Enter a unique name for the Virtual Service Name (**vs_view_blast**). 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 (**10.2.40.30/8443**). Click "**Add**" to create the new SLB Virtual Service.
3. Select the Virtual Service (**vs_view_blast**) on the **VIRTUAL SERVICE LIST** by double clicking on it. The Virtual Service Information screen opens with a new series of tabs for completing the virtual services configuration.
4. Scroll down to **ASSOCIATE GROUPS**, from the Eligible vLink or Groups pull down menu; select "**gp_cs_blast**" and on the Eligible Policies pull down menu select "**default**". Click **Add** to associate the Group with the Virtual Service.
5. Repeat steps 1 through 4 to add all remaining Virtual Services listed on Table 7 – Virtual Services.

4.2.3 Validate the Configuration

Validate that the basic configuration is functioning correctly:

1. From WebUI, **SERVER LOAD BALANCE**, **Monitoring -> Status -> Virtual Service Status**, select "**vs_view_portal**", "**vs_view_blast**", "**vs_view_pcoip_tcp**" and "**vs_view_pcoip_udp**" as the virtual services.
2. Verify that the configuration is as intended and that all "**Service Status**" icons are green.



4.3 Scenario 3 - L4 Load Balance All View Connections with IP Persistence

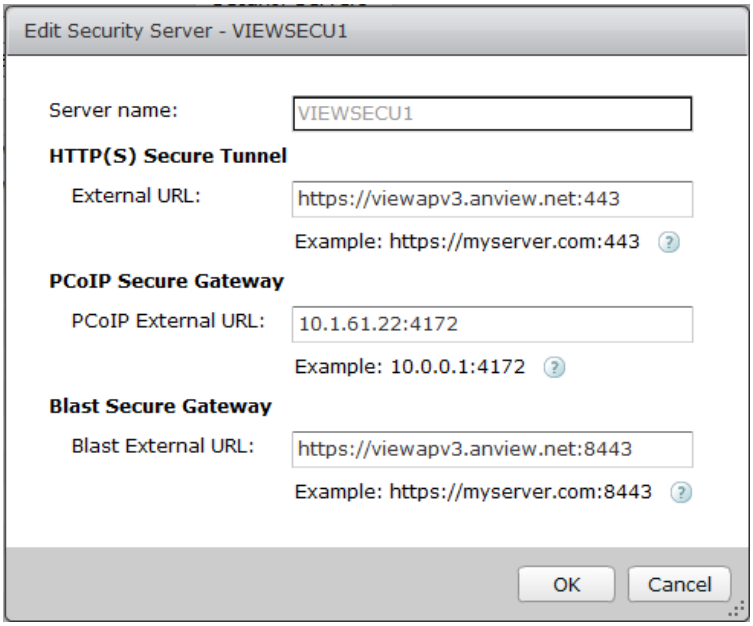
For external client access, an APV can be deployed with single IP to load balance all View traffic to the Security Server.

4.3.1 View Security Server Configuration

Each Security Server is paired with a Connection Server. All communications to the Security Server are encrypted. Only one IP is used for all View services.

On the Security Server, fill out all external URLs and IP addresses as below.

In the VMware Horizon View Administrator's interface, go to **View Configuration > Servers>Security Servers>Edit.**



4.3.2 APV Configuration

The APV Series is using L4 with IP persistence to load balance multiple Security Servers. No SSL processing is performed on the APV Series.

Additional health checks are needed for the paired Connection Server. In this scenario if the Connection Server is down, the front Security Server should be marked as down as well; otherwise, View clients will not be able to access the Virtual Desktop via the downed Connection Server.

Define Application Health Check

For this example, the default protocol checks are used.

Create Real Services

The following table shows the Security Server ports that need to be load balanced as the Real Services.

Real Service Name (Security Server)	Real Service Type	Real Service IP	Real Service Port	Health Check Type
rs_ss01_portal	TCP	10.2.40.27	443	TCP
rs_ss01_blast	TCP	10.2.40.27	8443	TCP
rs_ss01_pcoip_tcp	TCP	10.2.40.27	4172	TCP
rs_ss01_pcoip_udp	UDP	10.2.40.27	4172	ICMP
rs_ss02_portal	TCP	10.2.40.29	443	TCP
rs_ss02_blast	TCP	10.2.40.29	8443	TCP
rs_ss02_pcoip_tcp	TCP	10.2.40.29	4172	TCP
rs_ss02_pcoip_udp	UDP	10.2.40.29	4172	ICMP

Table 8 - Real Services for Security Servers

To configure the Real Services; 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 servers. Enter a unique name for the Real Service Name (**rs_ss01_portal**). From the Real Service Type pull down, select "**TCP**". Enter the Real Service IP/Port (**10.2.40.27/443**) which are used by Security Server 1.

3. Select **TCP** as the Health Check Type. Then click **Save** to create the Real Service.

4. Repeat steps 1-3 as above to add all Real Services according to Table 8 – Real Services for Security Servers.

Optional: Additional Health Check

Make sure the paired Connection Server is up. We paired Security Server 1 with Connection Server 1, and Connection Server 2 with the second Security Server. Following are the additional health checks needed for the Security Server main portal service.

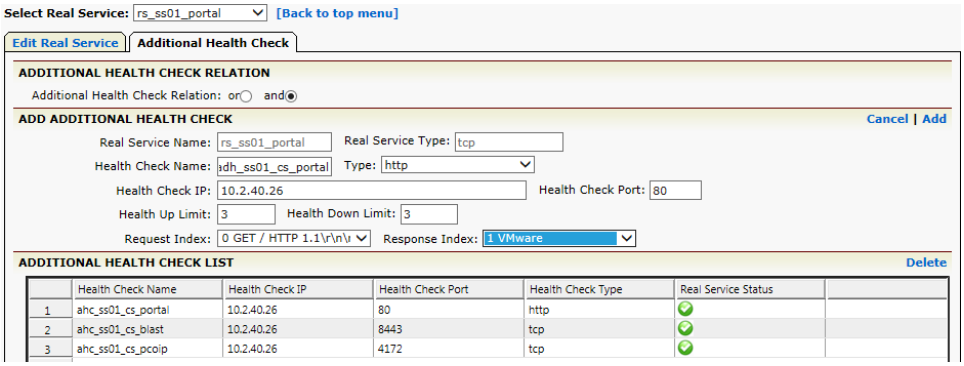
Additional Health Check Name	Real Service Name	Health Check IP	Health Check Port	Health Check Type
ahc_ss01_cs_portal	rs_ss01_portal	10.2.40.26	80	HTTP (0/1)
ahc_ss01_cs_blast	rs_ss01_portal	10.2.40.26	8443	TCP
ahc_ss01_cs_pcoip	rs_ss01_portal	10.2.40.26	4172	TCP
ahc_ss02_cs_portal	rs_ss02_portal	10.2.40.28	80	HTTP (0/1)
ahc_ss02_cs_blast	rs_ss02_portal	10.2.40.28	8443	TCP
ahc_ss02_cs_pcoip	rs_ss02_portal	10.2.40.28	4172	TCP

Table 9 – Additional Health Checks for Security Servers

To configure the additional health checks as Real Services, enter WebUI, Mode: **Config**.

1. Select **Real Services** from sidebar; double click the Real Service (**rs_ss01_portal**), and then click **Additional Health Check**.

2. Under "**ADD ADDITIONAL HEALTH CHECK",** enter a unique name for the "Health Check Name" (***ahc_ss01_cs_portal***). Select the type (http), and enter the target Health Check IP and Port (10.2.40.26/80). Click **Add**.



3. Repeat steps 1 and 2 to enter all additional health checks from Table 9 – Additional Health Checks for Security Servers

Create Groups

The following table shows the groups that are used for the example. Since View Clients need get to the same Connection Server for different View services, we are using "HASH IP" for this example.

Group Name	Group Method	Group Member
gp_ss_portal	Hash IP	rs_ss01_portal
		rs_ss02_portal
gp_ss_blast	Hash IP	rs_ss01_blast
		rs_ss02_blast
gp_ss_pcoip_tcp	Hash IP	rs_ss01_pcoip_tcp
		rs_ss02_pcoip_tcp
gp_ss_pcoip_udp	Hash IP	rs_ss01_pcoip_udp
		rs_ss02_pcoip_udp

Table 10 – Groups for Security Servers

To create SLB Groups, 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 we used "***gp_ss_portal***". From the Group Method pull down menu, select "**Hash IP**". Click **Add** to create the SLB group.

3. To add Real Services to the SLB group, on the **GROUPS LIST** double click on the SLB Group (**gp_ss_portal**). The **GROUP INFORMATION** screen opens.

4. Under the “**GROUP MEMBERS**” section, click “**Add**”, and the **ADD GROUP MEMBER** screen opens.

5. From the Eligible Reals pull down menu, select “**rs_ss01_portal**”, click **Save & Add Another** and select “**rs_ss02_portal**” and “**Save**”**.**

6. Repeat steps 1 through 5 for all other groups and members.

Create Virtual Services

The following table shows all Virtual Services used in this example.

Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	SLB Policy	Associate Groups
vs_secu_portal	TCP	10.1.61.22	443	Default	gp_ss_http
vs_secu_blast	TCP	10.1.61.22	8443	Default	gp_ss_blast
vs_secu_pcoip_tcp	TCP	10.1.61.22	4172	Default	gp_ss_pcoip_tcp
vs_secu_pcoip_udp	UDP	10.1.61.22	4172	Default	gp_ss_pcoip_udp

Table 11 - Virtual Services for Security Servers

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

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

2. Enter a unique name for the Virtual Service Name (**vs_secu_portal**). 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 (**10.1.61.22/443**). 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.

3. Select the Virtual Service (**vs_secu_portal**) on the **VIRTUAL SERVICE LIST** by double clicking on it. The Virtual Service Information screen opens with a new series of tabs for completing the virtual services configuration.

4. Go down to the **Associate Groups** section, from the **Eligible vLink or Groups** pull down menu select “**gp_ss_http**” and on the **Eligible Policies** pull down menu select “**default**”. Click **Add** to associate the Group with the Virtual Service.

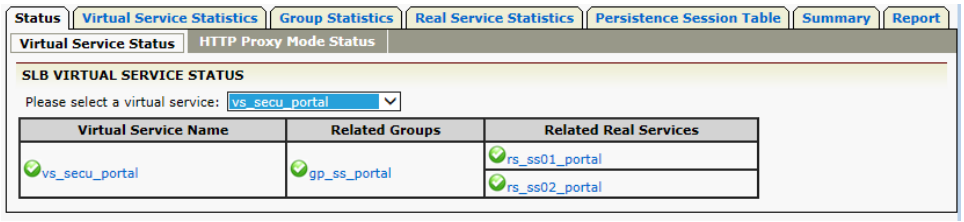
5. Repeat steps 1 through 4 for all other Virtual Services.

4.3.3 Validate the Configuration

Validate that the basic configuration is functioning correctly:

1. From WebUI, **SERVER LOAD BALANCE, Monitoring** -> **Status** -> **Virtual Service Status**. Select “**vs_secu_portal**”, "**vs_secu_blast**", "**vs_secu_pcoip_tcp**" and "**vs_secu_pcoip_udp**" as the virtual services.

2. Verify that each of the configurations is as intended and that all “**Service Status**” icons are green.



5 Summary

This concludes the Array Networks APV deployment guide for VMware Horizon View. Array Networks APV Series application delivery controllers provide Layer 2 to 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 VMware View Server deployments.

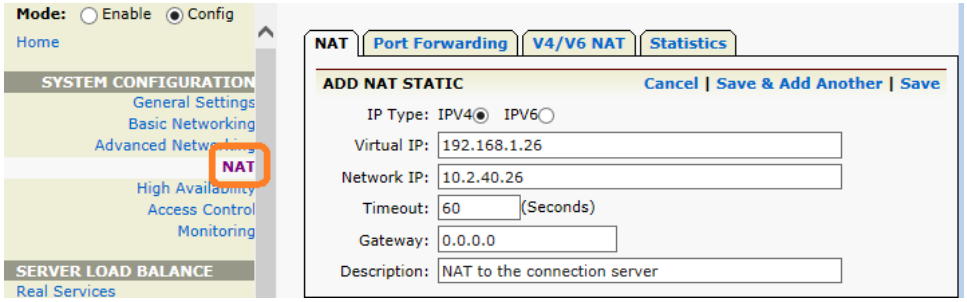
6 Appendix:

6.1 Configure Static NAT for Server Access.

With a two-arm network setup, in order to access individual servers the external clients need to NAT through the APV system. "NAT static" can be configured to facilitate the access. NAT static maps one external network IP on the APV to one internal server IP.

To create a NAT static, from WebUI Mode: **Config**:

1. Select **"NAT"** from the sidebar. From NAT STATIC CONFIGURATION, click **Add NAT Static**. The **ADD NAT STATIC** screen opens.
2. Enter a Virtual IP (**192.168.1.26**) as the public IP for the client-facing interface on the APV, and a Network IP (**10.2.40.26**) for the internal server to be NATed. Then click **Save.**



3. Repeat steps 1 and 2 to create more NAT static entries as needed.

6.2 Configure SSL Virtual Host

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

On the APV Series, SSL setup includes 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 to use the SSL Virtual Host (if available). Then click **Save.**
3. From the **SSL VIRTUAL HOSTS** screen, double click the newly created SSL Virtual Host **ssl-vhost1** to manage its Private Key and Certificate.

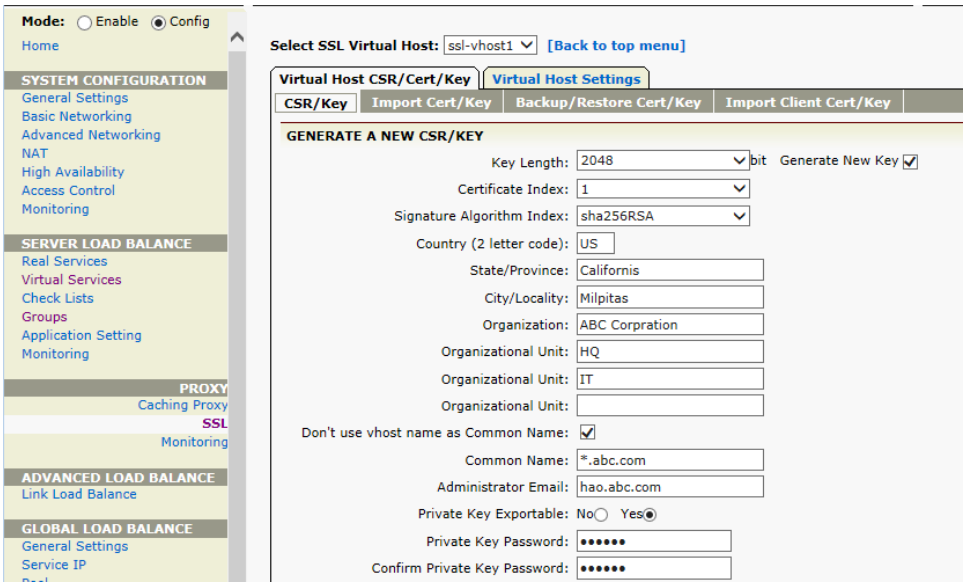
There are two options to add or update Private Key/Certificate to the SSL Virtual Host:

Option 1: Generate a CSR, Self-Signed Certificate and Private Key

Option 2: Import an existing Private Key and Certificate

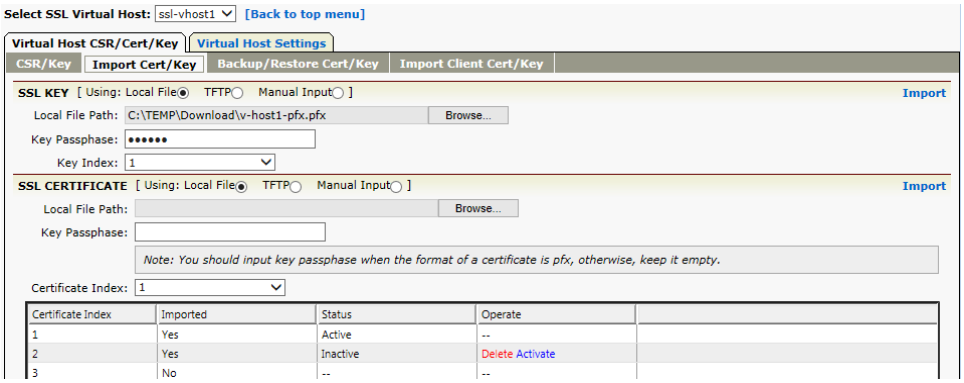
Option 1 - For a newly created **ssl-vhost1** SSL Virtual Host that does not have a Certificate and Private Key:

1. Under **CSR/Key** tab, 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 (this can be used for testing but is not intended for production use).



Option 2 - Import an existing Certificate and Key:

1. Click "**Import Cert/Key**".
2. In **SSL KEY**, select **Local File**; browse to locate the local PFX file on your disk, enter the **Key Passphase** 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.



3. In **SSL CERTIFICATE**, select **Local File**; browse to locate the local PFX file on your disk, enter the **Key Passphase** and **1** for **Key Index**, and click **Import** to import the corresponding certificate from the PFX file.

Technical Notes:

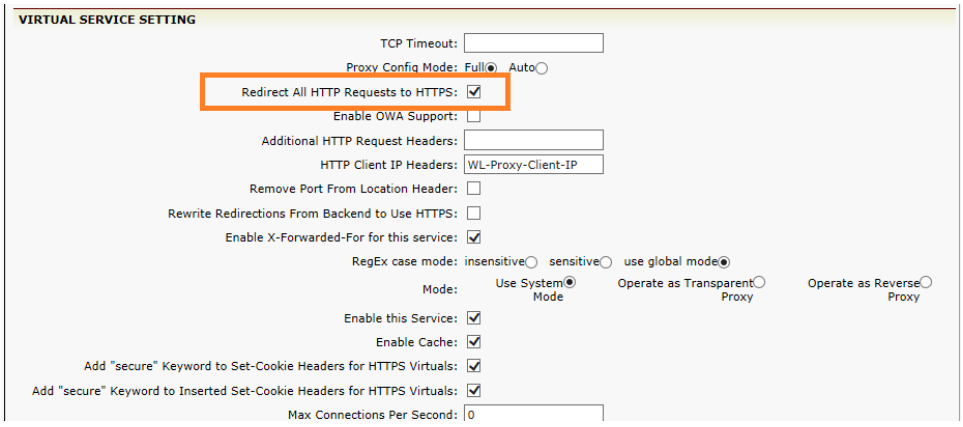
- In a scenario in which the application has multiple FQDNs on a single IP address, you can utilize a certificate with a wildcard or multiple Subject Alternative Names. Microsoft IIS 6 and Apache are both able to Virtual Host HTTPS sites using Unified Communications SSL, also known as SAN certificates.
- 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 an SSL Key/Certificate, you can use the OpenSSL tool to convert the PFX file to the unencrypted PEM format, then manually import to the APV system.
- On the APV, each SSL Virtual Host can have three sets of Keys/Certificates configured. This is to facilitate quick switchover when renewing certificates.

6.3 Configure HTTP to HTTPS Redirect

A user may accidentally type “http://...” (unsecured) instead of https://... (secured), or type just the domain name to access a secured View Virtual Desktop, which would normally cause the View client to wait until timeout without serving any content. To make this more user friendly, the APV appliance can be configured with another Virtual Service for port 80 (HTTP) to automatically redirect HTTP requests to HTTPS.

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

1. Select **Virtual Services** from the sidebar; double click the Virtual Service listed on port 80 (HTTP) to select it.
2. Check the box for “**Redirect All HTTP Requests to HTTPS**”, then click **SAVE CHANGES.**

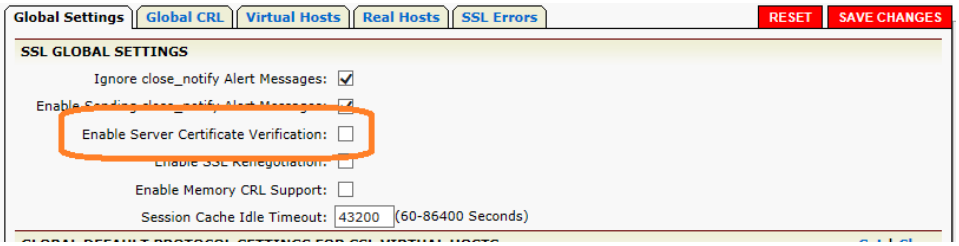


6.4 Disable Server Certificate Check

This is used for APV and View Servers that communicate with HTTPS/TCPS (including health checks). In standard SSL/TLS communication, the View Server will send its certificate to the APV (as a client). If the certificate is not signed by a trusted CA known to the APV, the server certificate validation will fail and the connection will be dropped. You will need import the intermediate and root CA to the APV. For quick testing, we can disable the server certificate validation on APV.

To disable the server certificate validation, enter WebUI, Mode: **Config**.

1. Select **SSL** from sidebar; the **Global Setting** screen opens.
2. Uncheck the box for Enable Server Certificate Verification; click **SAVE CHANGES**.



6.5 Sample APV CLI Configuration

Scenario 1:

```
health request 0 "GET / HTTP 1.1\r\n\r\n"
health response 1 "VMware"

slb real http "rs_cs01_http" 10.2.40.26 80 1000 http 3 3
slb real http "rs_cs02_http" 10.2.40.28 80 1000 http 3 3
health server "rs_cs01_http" 0 1
health server "rs_cs02_http" 0 1

slb group method "gp_cs_SID" persistence string rr
slb group member "gp_cs_SID" "rs_cs01_http" 1 0
slb group member "gp_cs_SID" "rs_cs02_http" 1 0
slb group persistence request cookie "gp_cs_SID" "JSESSIONID"
slb group persistence response cookie "gp_cs_SID" "JSESSIONID"

slb virtual https "vs_view_portal" 10.2.40.30 443 arp 0
slb policy default "vs_view_portal" "gp_cs_SID"

ssl host virtual "ssl-vhost1" "vs_view_portal"
```

Scenario 2:

```
slb real http "rs_cs01_http" 10.2.40.26 80 1000 http 3 3
slb real http "rs_cs02_http" 10.2.40.28 80 1000 http 3 3

slb real tcp "rs_cs01_blast" 10.2.40.26 8443 1000 tcp 3 3
```

```
slb real tcp "rs_cs01_pcoip_tcp" 10.2.40.26 4172 1000 tcp 3 3
slb real udp "rs_cs01_pcoip_udp" 10.2.40.26 4172 1000 3 3 60 icmp
slb real tcp "rs_cs02_blast" 10.2.40.28 8443 1000 tcp 3 3
slb real tcp "rs_cs02_pcoip_tcp" 10.2.40.28 4172 1000 tcp 3 3
slb real udp "rs_cs02_pcoip_udp" 10.2.40.28 4172 1000 3 3 60 icmp

[optional – addition health check]
slb real health "ahc_cs01_http_blast" "rs_cs01_http" 10.2.40.26 8443 tcp 3 3
slb real health "ahc_cs01_http_pcoip" "rs_cs01_http" 10.2.40.26 4172 tcp 3 3
slb real health "ahc_cs02_http_blast" "rs_cs02_http" 10.2.40.28 8443 tcp 3 3
slb real health "ahc_cs02_http_pcoip" "rs_cs02_http" 10.2.40.28 4172 tcp 3 3

[Group]
slb group method "gp_cs_blast" hi 32
slb group method "gp_cs_http" hi 32
slb group method "gp_cs_pcoip_tcp" hi 32
slb group method "gp_cs_pcoip_udp" hi 32

slb group member "gp_cs_blast" "rs_cs01_blast" 1 0
slb group member "gp_cs_blast" "rs_cs02_blast" 1 0
slb group member "gp_cs_http" "rs_cs01_http" 1 0
slb group member "gp_cs_http" "rs_cs02_http" 1 0
slb group member "gp_cs_pcoip_tcp" "rs_cs01_pcoip_tcp" 1 0
slb group member "gp_cs_pcoip_tcp" "rs_cs02_pcoip_tcp" 1 0
slb group member "gp_cs_pcoip_udp" "rs_cs01_pcoip_udp" 1 0
slb group member "gp_cs_pcoip_udp" "rs_cs02_pcoip_udp" 1 0

slb virtual tcp "vs_view_blast" 10.2.40.30 8443 arp 0
slb virtual tcp "vs_view_pcoip_tcp" 10.2.40.30 4172 arp 0
slb virtual udp "vs_view_pcoip_udp" 10.2.40.30 4172 arp 0

[same as previous example]
slb virtual https "vs_view_portal" 10.2.40.30 443 arp 0

slb policy default "vs_view_blast" "gp_cs_blast"
slb policy default "vs_view_pcoip_tcp" "gp_cs_pcoip_tcp"
slb policy default "vs_view_pcoip_udp" "gp_cs_pcoip_udp"
slb policy default "vs_view_portal" "gp_cs_http”

ssl host virtual "ssl-vhost1" "vs_view_portal"

slb virtual http "vs_view_portal" 10.2.40.30 80 arp 0
```

Scenario 3:

```
[Real Service]
slb real tcp "rs_ss01_portal" 10.2.40.27 443 1000 tcp 3 3
slb real tcp "rs_ss02_portal" 10.2.40.29 443 1000 tcp 3 3
slb real tcp "rs_ss01_blast" 10.2.40.27 8443 1000 tcp 3 3
slb real tcp "rs_ss01_pcoip_tcp" 10.2.40.27 4172 1000 tcp 3 3
slb real tcp "rs_ss02_blast" 10.2.40.29 8443 1000 tcp 3 3
```

```
slb real tcp "rs_ss02_pcoip_tcp" 10.2.40.29 4172 1000 tcp 3 3
slb real udp "rs_ss01_pcoip_udp" 10.2.40.27 4172 1000 3 3 60 icmp
slb real udp "rs_ss02_pcoip_udp" 10.2.40.29 4172 1000 3 3 60 icmp

[Simple Additional Health Check, for step 1, make sure connection server is up]
slb real health "ahc_ss01_cs_portal" "rs_ss01_portal" 10.2.40.26 80 http 3 3
slb real health "ahc_ss02_cs_portal" "rs_ss02_portal" 10.2.40.28 80 http 3 3
slb real health "ahc_ss01_cs_blast" "rs_ss01_portal" 10.2.40.26 8443 tcp 3 3
slb real health "ahc_ss02_cs_blast" "rs_ss02_portal" 10.2.40.28 8443 tcp 3 3
slb real health "ahc_ss01_cs_pcoip" "rs_ss01_portal" 10.2.40.26 4172 tcp 3 3
slb real health "ahc_ss02_cs_pcoip" "rs_ss02_portal" 10.2.40.28 4172 tcp 3 3

[Group]
slb group method "gp_ss_portal" hi 32
slb group method "gp_ss_blast" hi 32
slb group method "gp_ss_pcoip_tcp" hi 32
slb group method "gp_ss_pcoip_udp" hi 32

slb group member "gp_ss_portal" "rs_ss01_portal" 1 0
slb group member "gp_ss_portal" "rs_ss02_portal" 1 0
slb group member "gp_ss_blast" "rs_ss01_blast" 1 0
slb group member "gp_ss_blast" "rs_ss02_blast" 1 0
slb group member "gp_ss_pcoip_tcp" "rs_ss01_pcoip_tcp" 1 0
slb group member "gp_ss_pcoip_tcp" "rs_ss02_pcoip_tcp" 1 0
slb group member "gp_ss_pcoip_udp" "rs_ss01_pcoip_udp" 1 0
slb group member "gp_ss_pcoip_udp" "rs_ss02_pcoip_udp" 1 0

[Virtual Service]
slb virtual tcp "vs_secu_portal" 10.1.61.22 443 arp 0
slb virtual tcp "vs_secu_blast" 10.1.61.22 8443 arp 0
slb virtual tcp "vs_secu_pcoip_tcp" 10.1.61.22 4172 arp 0
slb virtual udp "vs_secu_pcoip_udp" 10.1.61.22 4172 arp 0

slb policy default "vs_secu_portal" "gp_ss_portal"
slb policy default "vs_secu_blast" "gp_ss_blast"
slb policy default "vs_secu_pcoip_tcp" "gp_ss_pcoip_tcp"
slb policy default "vs_secu_pcoip_udp" "gp_ss_pcoip_udp"
```

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

July-2015 rev. a