Deployment Guide
Apr-2019 rev. a

Array Networks APV/vAPV Series ADCs and eClinicalWorks Application Servers

1 Introduction

This guide provides information on configuring the APV/vAPV Series application delivery controller for eClinicalWorks servers.

eClinicalWorks offers a variety of products including electronic health records, population health management, patient engagement, revenue cycle management and others.

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

1.1 Prerequisites and Assumptions

eClinicalWorks

This document is written with the assumption that you are familiar with eClinicalWorks (eCW) server products. For more information on planning and deploying the eClinicalWorks server please visit the eCW customer portal.

Array Networks APV Series

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

1.2 APV Series Application Delivery Controllers (ADCs) Benefits

The Array Networks APV Series delivers all required application delivery functions for optimizing application delivery for eCW environments, such as Layer 4 server load balancing, high availability, SSL acceleration and offloading, DDoS mitigation, TCP connection multiplexing, site proximity and failover – all in a single, easy-to-manage appliance.

Availability & Scalability

The APV Series' server load balancing (SLB) ensures maximum uptime for eCW services. Customers can scale their eCW environment to meet capacity and performance needs with APV server load balancers.

SSL Offloading and SSL Security

APV Series provides industry-leading performance and cost per SSL TPS for 2048-bit SSL, with advanced client certificate handling for secure application support and easy application integration. SSL acceleration reduces the number of servers required for secure applications, improves server efficiency and administration, and dramatically improves application performance. Offloading compute-intensive key exchange and bulk encryption, and delivering industry-leading client-certificate performance, APV Series SSL acceleration is ideal for scaling secure Software-as-a-Service (SaaS) services, e-commerce environments and business-critical applications requiring high-volume secure connectivity

Network and Server Protection

The APV appliance can protect eCW services from malicious network and server attacks like DDoS attacks, SYN floods, TCP port scans, UDP floods and UDP port scans, etc. The advanced rate limiting options can rate limit connections per user and advanced HTTP profiles can limit HTTP commands and parameters for Web applications.

Site Resilience

The APV's global server load balancing directs traffic away from failed data centers and intelligently distributes services between sites based on proximity, language, capacity, load and response times for maximum performance and availability.

TCP Connection Multiplexing

The APV appliance multiplexes several client TCP connections into fewer connections for HTTP- based services. The APV appliance also reuses existing server connections.

Cache Offload

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

2 Basic Installation

This section covers the basic installation and set-up of the APV appliance. If the APV appliance is already installed in the network with management IP, interface IP, VLANs, WebUI enabled and default gateway configured, you can skip this section and proceed to section 3: Advanced System Configuration (via WebUI).

2.1 Factory Defaults

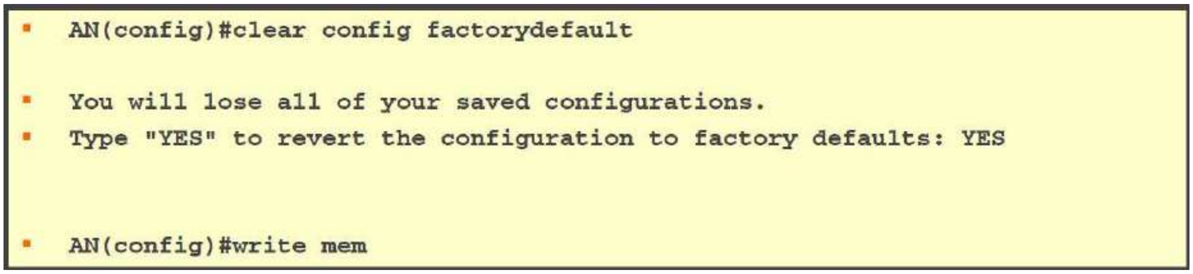
The Array APV ships with full factory defaults set. You will need to connect to the APV via its Serial Console port to assign an IP address and gain full access to the Administrative interface.

The unit ships with a DB9 to DB9 Serial Cable. Connect one end to the Console port of the Array appliance and the other end to a PC using a Virtual Terminal emulator. *Note, most new PCs will not have a serial DB9 connector. You will need a USB to DB9 connector in this case.*

Console Specifications	
Emulation:	VT100
Baud Rate:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1

2.2 Resetting Factory Defaults

If you need to reset the APV to factory defaults, type “configure terminal” or “conf t” for short at the enable prompt to enter configuration mode. Then use the following commands to clear the configuration and set the APV to factory default.



```
AN(config)#clear config factorydefault

You will lose all of your saved configurations.
Type "YES" to revert the configuration to factory defaults: YES


AN(config)#write mem
```

“write mem” commits the changes to the startup configuration.

2.3 Login for the First Time

Once connected to the APV via the serial console port, you will need to login using the default user name and passwords.

Default Login Admin Accounts	
Admin User Name:	Array
Admin Password:	Admin
Enable Password:	Not Set

When prompted for credentials, user the information above. Note that the enable password is not set by default. Simply type 'enable' and press ENTER at the password prompt. *We highly recommend that you secure your APV by setting the credentials to non-default passwords before placing it into production.*

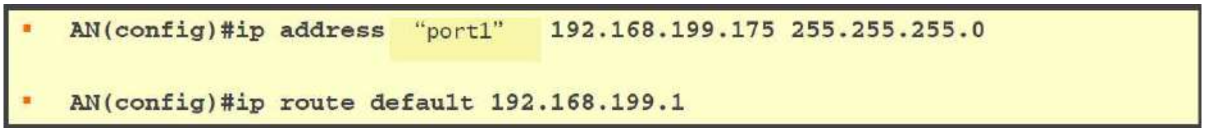
Note that once you are logged in, there are different configuration nodes needed in order to manage the Array APV.

Configuration Modes	
User Mode	The first level is User Mode. Here, the user is only authorized to execute some very basic operations and non-critical functions. The User Mode prompt appears as "AN>" in the CLI.
Enable Mode	The second level is Enable Mode. Users in this mode have access to a majority of view-only commands such as "show log config". Users in the Enable mode may execute commands from both the User and Enable modes. Users will know that they have been granted access to the Enable Mode when the CLI prompt changes from "AN>" to "AN#".
Config Mode	The final level is Config Mode. It is at this level that users can make changes to any part of the Array appliance configuration. No two users may access the Configuration mode at the same time. The CLI prompt will change from "AN#" to "AN(config)#".

2.4 IP Address and WebUI Settings

In order to make IP address changes, you must be in config mode.

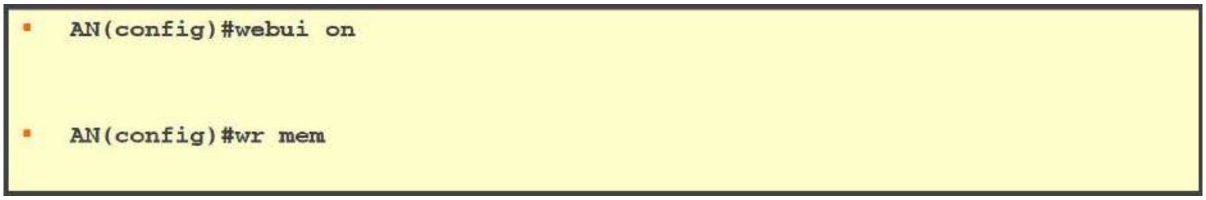
Note that interfaces are referenced as "port#" in the Array OS. All ports are labeled on the front of the appliance.



```
▪   AN(config)#ip address  "port1"   192.168.199.175 255.255.255.0

▪   AN(config)#ip route default 192.168.199.1
```

The Array APV has two administrative interfaces – the command line interface (CLI) can be accessed via the console port or over the network with an SSH client. The second administrative interface is a web-based user interface (WebUI), which can be accessed with a web browser using the IP address given to the APV and port 8888. This port number can be changed if necessary. To enable WebUI administration, type the commands below.



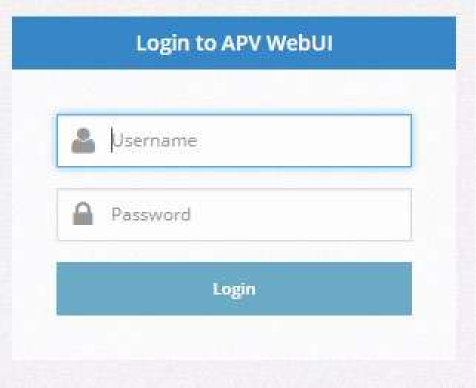
```
▪   AN(config)#webui on


▪   AN(config)#wr mem
```

2.4.1 Accessing the WebUI

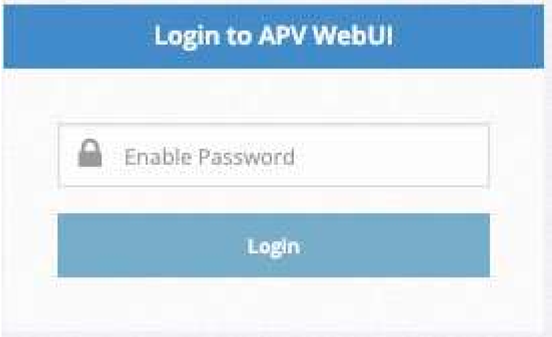
To access the WebUI, type "https://<ip_address_given>:8888 in the browser address bar. You will see a certificate error. This is because the APV has a self-signed certificate by default. Simply click 'Continue to this website (not recommended).' to go to the admin interface.

You will be prompted for your login credentials. These are the same credentials used to access the CLI. By default, the user name is array and the password is admin.



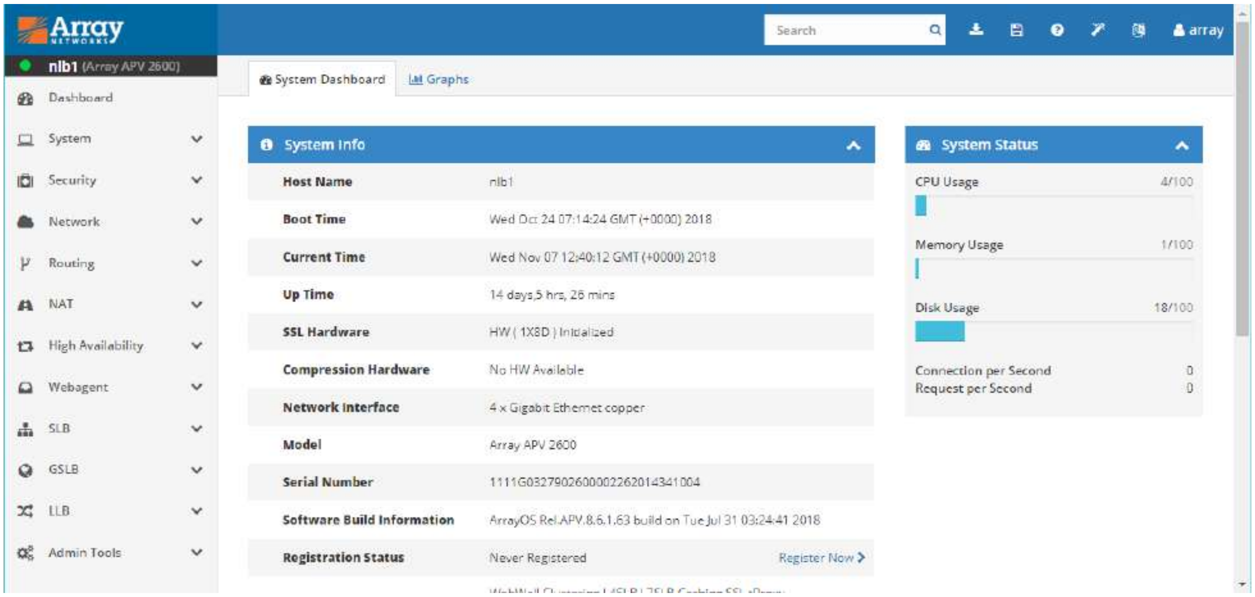
The admin login prompt as it appears in Google Chrome

After successfully logging in with your admin credentials, you may need to also enter the enable password to gain the ability to make configuration changes.



2.4.2 The WebUI

Once logged into the WebUI, you are in Config mode and can begin making configuration changes.



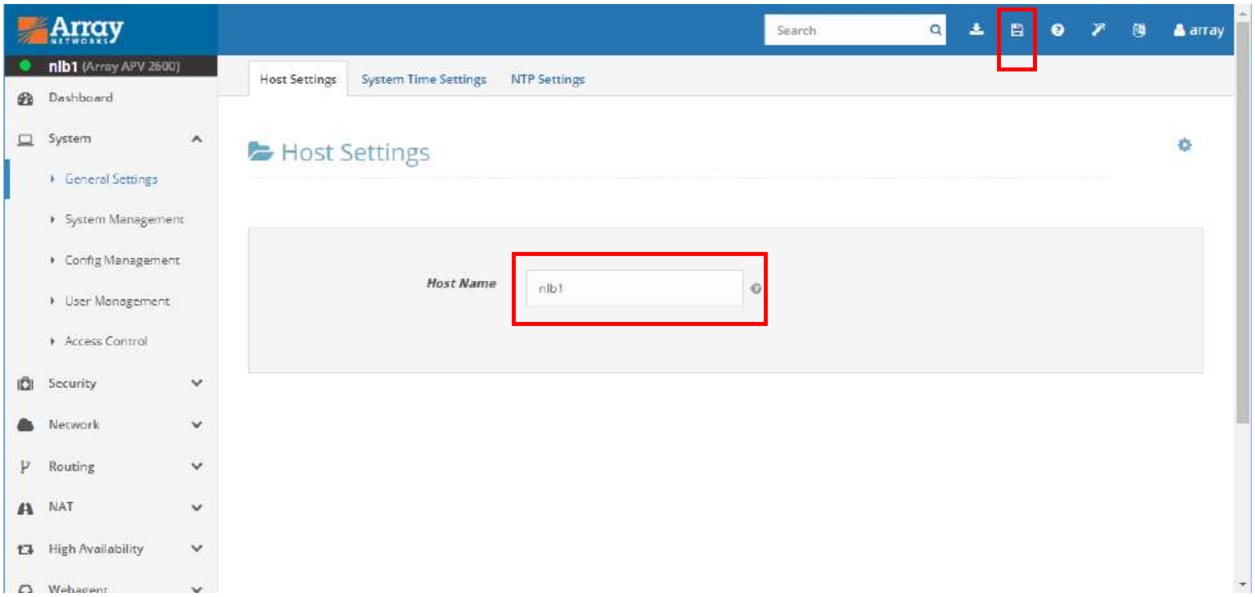
System Info	
Host Name	nlb1
Boot Time	Wed Oct 24 07:14:24 GMT (+0000) 2018
Current Time	Wed Nov 07 12:40:12 GMT (+0000) 2018
Up Time	14 days,5 hrs, 26 mins
SSL Hardware	HW (1X8D) Initialized
Compression Hardware	No HW Available
Network Interface	4 x Gigabit Ethernet copper
Model	Array APV 2600
Serial Number	1111G0327902600002262014341004
Software Build Information	ArrayOS Rel.APV.8.6.1.63 build on Tue Jul 31 03:24:41 2018
Registration Status	Never Registered

System Status	
CPU Usage	4/100
Memory Usage	1/100
Disk Usage	18/100
Connection per Second	0
Request per Second	0

2.4.2 Configure the Host Name

Click on General Settings under the System section and enter the name you would like to assign to this particular Array appliance. *Note: Using unique hostnames helps prevent accidental configurations to the incorrect appliance!*

As soon as you begin making changes, you will get the option to save those changes. Click on Save Changes (disk icon in the top blue bar) before moving on to another task, otherwise your changes will not be saved.

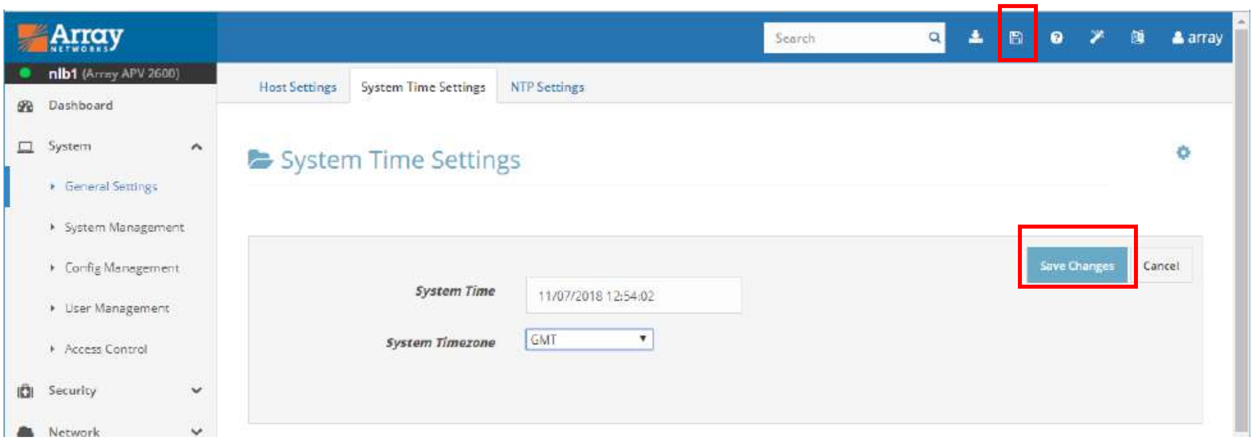


Host Settings

Host Name: nlb1

2.4.3 Save to the Startup Config

A special note about saving your configuration: As you make changes, you will be saving these changes to the running config. However, you must also save these changes to the startup config. To save to the startup config, click on the disk icon on the top right-hand side of the page. This is equivalent to entering "write mem" on the CLI. If the unit is rebooted, any configuration changes not saved to the startup config will be lost.



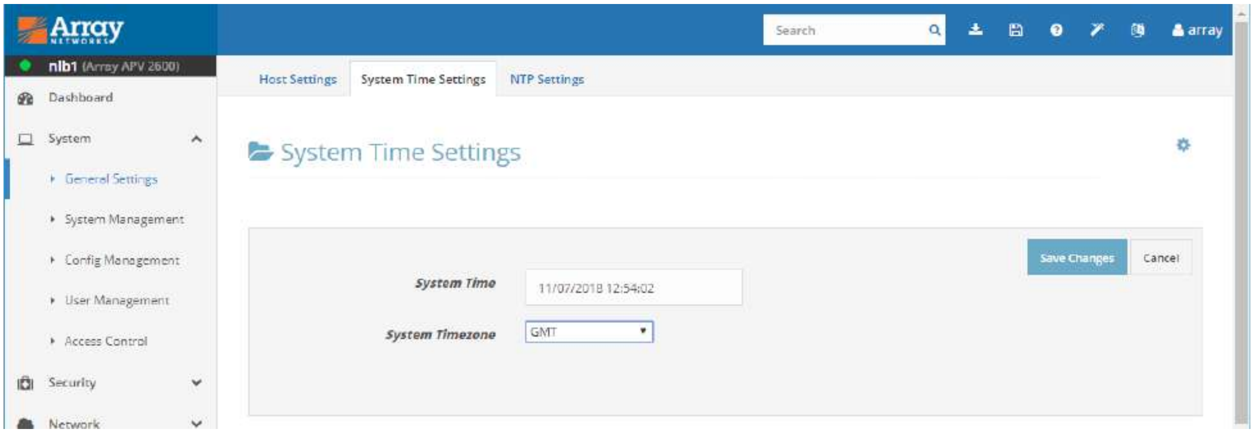
System Time Settings

System Time: 11/07/2018 12:54:02

System Timezone: GMT

2.4.4 Configure Date and Time

In the Date/Time tab, set the date and time. Uncheck the GTM check box and configure your time zone. Remember to Save Changes and Save Config.



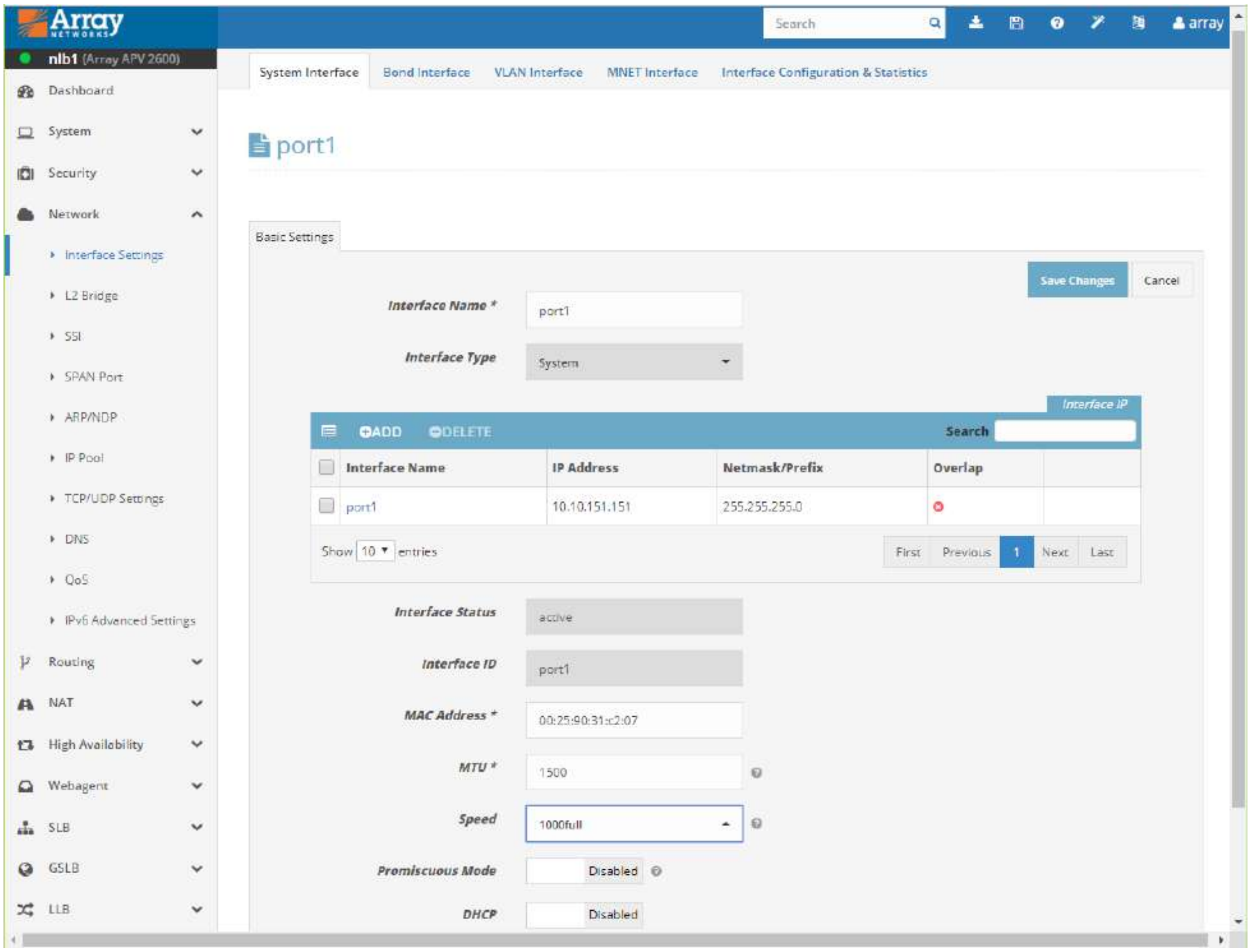
System Time Settings

System Time: 11/07/2018 12:54:02

System Timezone: GMT

2.4.5 Configure Interfaces

From the Network section, select the Interface Settings tab. The APV appliance performs best when its interfaces are forced to use a specific speed rather than setting them to Auto. Set the interface (Port) to 100full or 1000full, depending on the switch port to which it is connected. Save Changes and Save Config.



port1

Interface Name *: port1

Interface Type: System

Interface Name	IP Address	Netmask/Prefix	Overlap
port1	10.10.151.151	255.255.255.0	●

Interface Status: active

Interface ID: port1

MAC Address *: 00:25:90:31:c2:07

MTU *: 1500

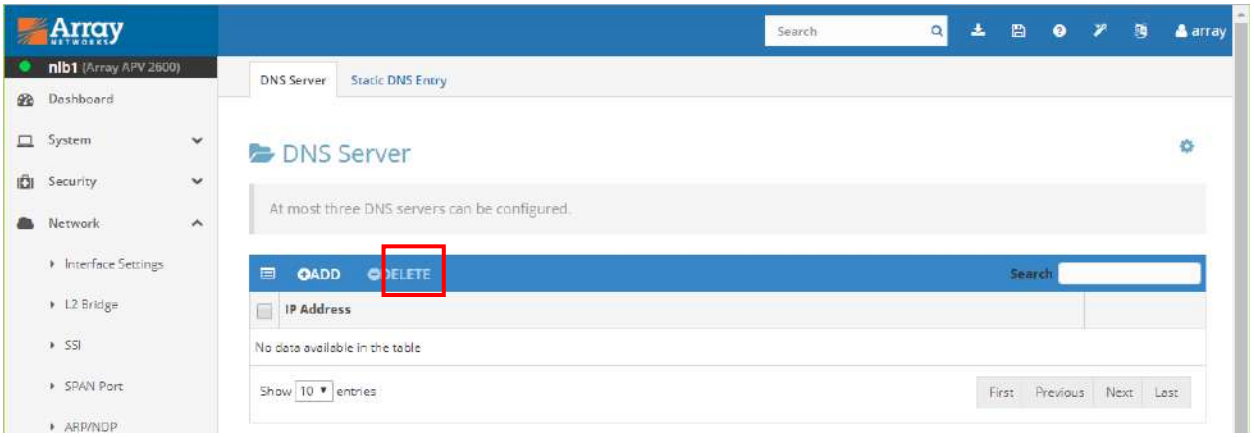
Speed: 1000full

Promiscuous Mode: Disabled

DHCP: Disabled

2.4.6 Configure DNS (optional)

Again, in the Network section, if you need to configure a DNS server for the Array appliance, click on the DNS link and then click on the Add link on the left.

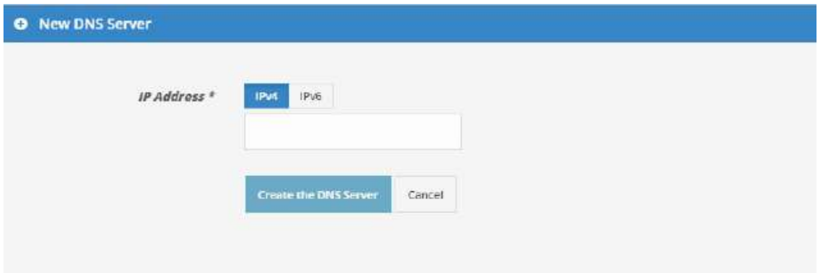


DNS Server

At most three DNS servers can be configured.

IP Address
No data available in the table

Enter the IP address of the DNS server and click Create the DNS Server, then Save. You can enter multiple DNS servers if necessary.



Basic setup is now complete.

3 Configuring Server Load Balancing

3.1 Server Load Balancing Configuration Components

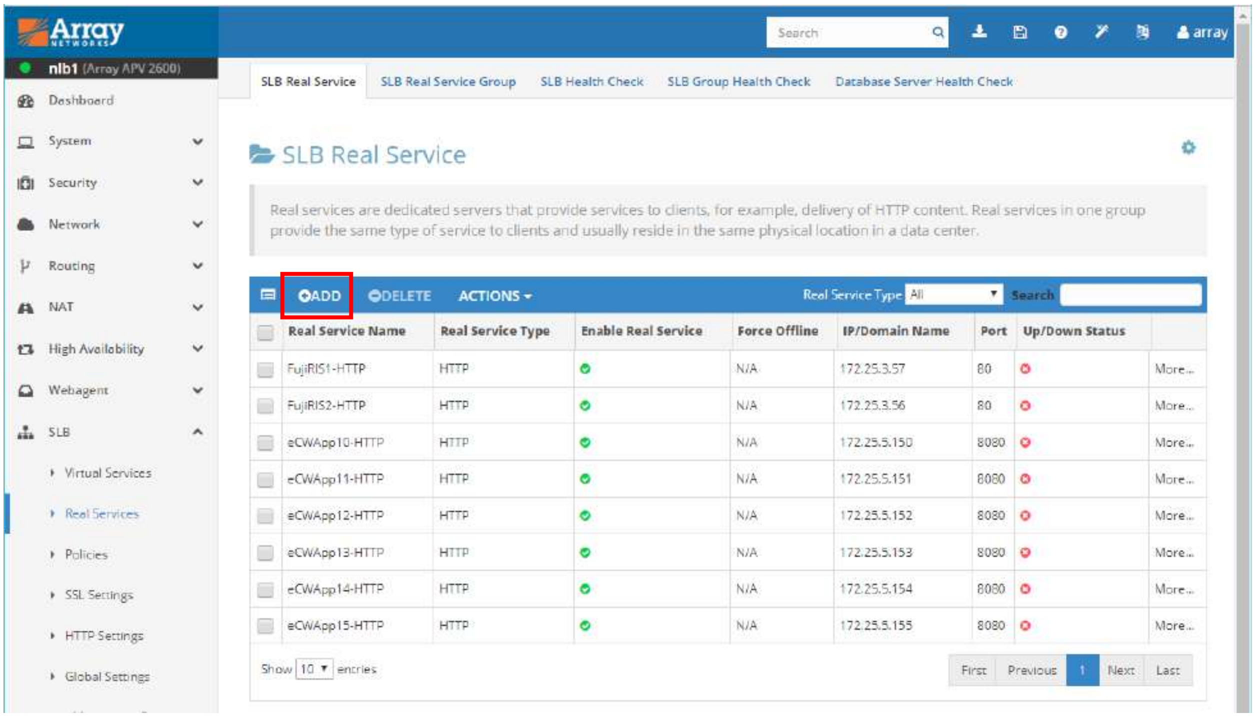
There are four main steps required to set up basic server load balancing:

1. **Add Real Services -** Real services are the individual application servers that will be grouped and accessed via one virtual IP (VIP) address.
2. **Add Group –** A Group is the logical grouping of servers and real services that serve the same application or service.
3. **Add Virtual Services –** A Virtual Service is the assignment of a virtual IP address which will be used to access a group.
4. **Configure SSL –** SSL Settings are used when you need to offload SSL encryption processing to the APV and away from your server.

3.2 Adding Real Services

To begin configuring Real Services:

1. Under the SLB section, click on Real Services.
2. In the SLB Real Service, click on Add at the left of the screen.



SLB Real Service

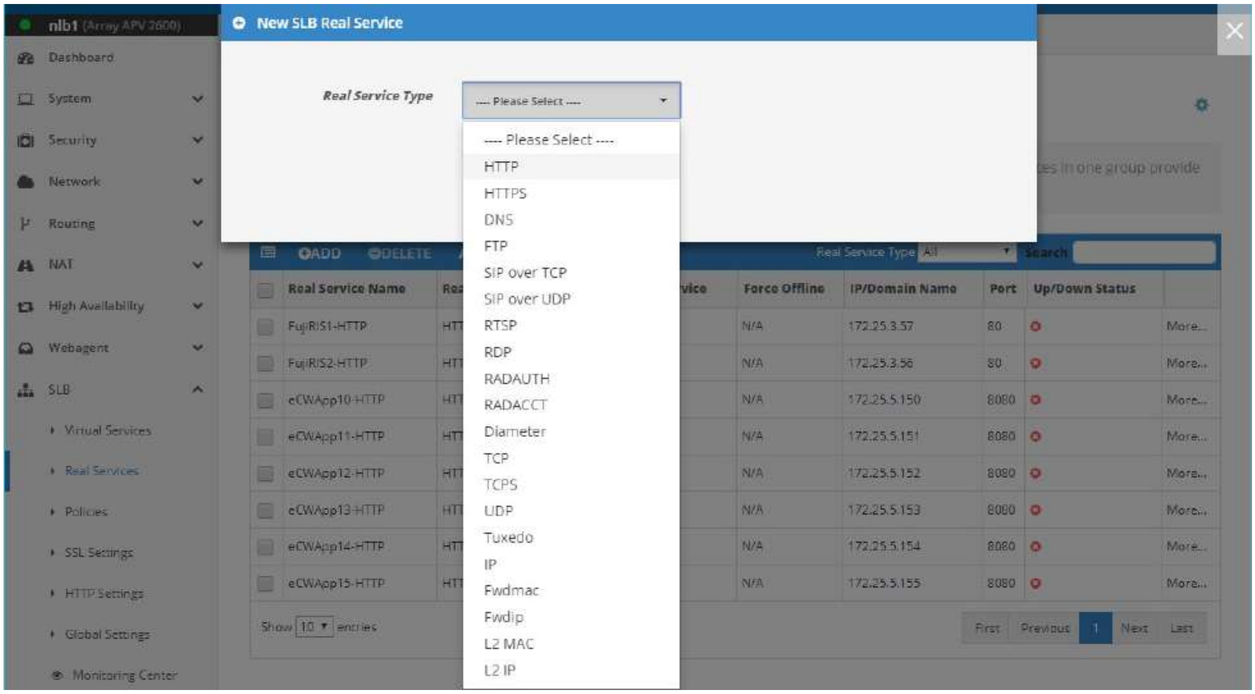
Real services are dedicated servers that provide services to clients, for example, delivery of HTTP content. Real services in one group provide the same type of service to clients and usually reside in the same physical location in a data center.

Real Service Type: All

□	Real Service Name	Real Service Type	Enable Real Service	Force Offline	IP/Domain Name	Port	Up/Down Status	
□	FujiRIS1-HTTP	HTTP	✓	N/A	172.25.3.57	80	✗	More...
□	FujiRIS2-HTTP	HTTP	✓	N/A	172.25.3.56	80	✗	More...
□	eCWApp10-HTTP	HTTP	✓	N/A	172.25.5.150	8080	✗	More...
□	eCWApp11-HTTP	HTTP	✓	N/A	172.25.5.151	8080	✗	More...
□	eCWApp12-HTTP	HTTP	✓	N/A	172.25.5.152	8080	✗	More...
□	eCWApp13-HTTP	HTTP	✓	N/A	172.25.5.153	8080	✗	More...
□	eCWApp14-HTTP	HTTP	✓	N/A	172.25.5.154	8080	✗	More...
□	eCWApp15-HTTP	HTTP	✓	N/A	172.25.5.155	8080	✗	More...

Show 10 entries

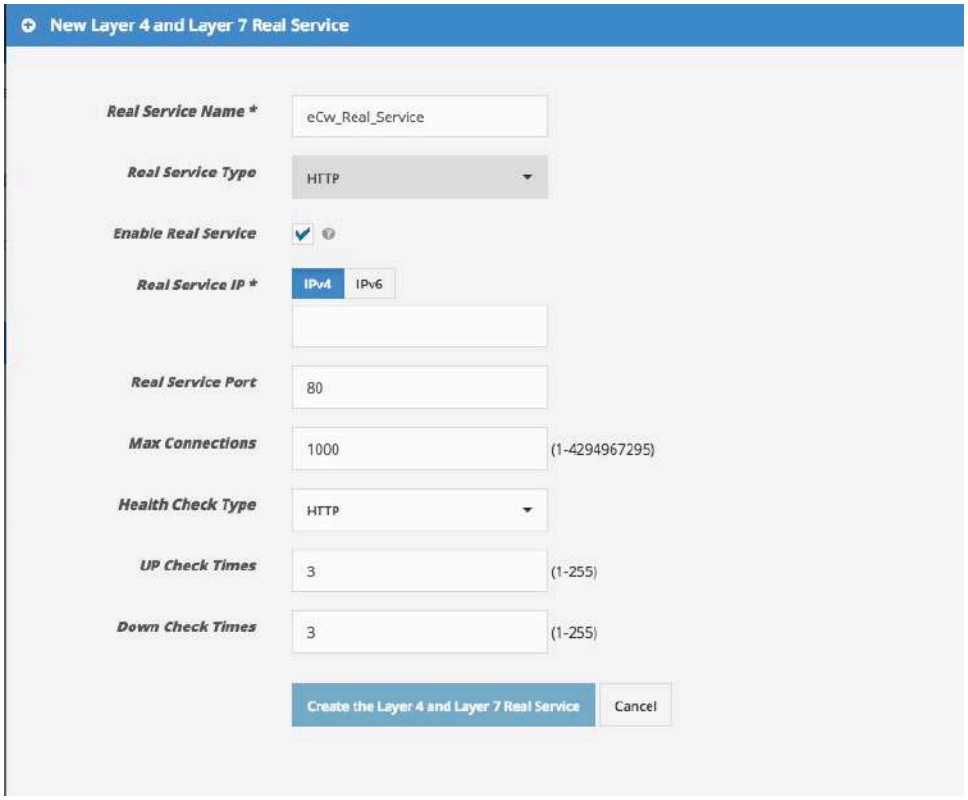
Select Real Service Type: HTTP



Real Service Type: ---- Please Select ----

Real Service Name	Rea	vice	Force Offline	IP/Domain Name	Port	Up/Down Status	
FujiRIS1-HTTP	HTT		N/A	172.25.3.57	80	○	More...
FujiRIS2-HTTP	HTT		N/A	172.25.3.56	80	○	More...
eCWApp10-HTTP	HTT		N/A	172.25.5.150	8080	○	More...
eCWApp11-HTTP	HTT		N/A	172.25.5.151	8080	○	More...
eCWApp12-HTTP	HTT		N/A	172.25.5.152	8080	○	More...
eCWApp13-HTTP	HTT		N/A	172.25.5.153	8080	○	More...
eCWApp14-HTTP	HTT		N/A	172.25.5.154	8080	○	More...
eCWApp15-HTTP	HTT		N/A	172.25.5.155	8080	○	More...

Give the Real Service an arbitrary name – it cannot contain spaces. Enter the Real Service IP address. Set the Health Check Type to “HTTP”.

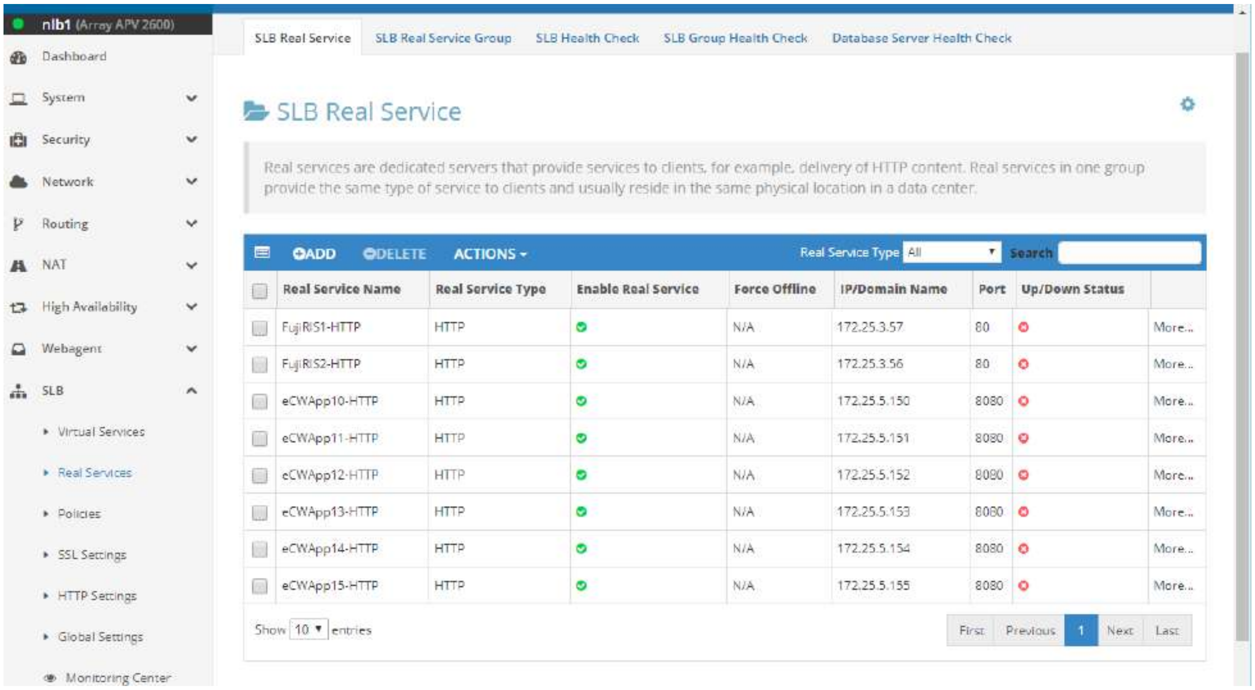

New Layer 4 and Layer 7 Real Service
Create the Layer 4 and Layer 7 Real Service
Cancel

Real Service Name *	eCw_Real_Service
Real Service Type	HTTP
Enable Real Service	☑
Real Service IP *	IPv4 IPv6
Real Service Port	80
Max Connections	1000 (1-4294967295)
Health Check Type	HTTP
UP Check Times	3 (1-255)
Down Check Times	3 (1-255)

Click “Create the Layer 4 and Layer 7 Real Services. Click “Add” to add another. Repeat until all Real Servers are defined. Save, then Save Config.

3.2.1 Real Service Status

The Real Services page displays the server up/down status. If the server is healthy and running, it displays a green check symbol. If the server is down or not responding, it displays a red X symbol.

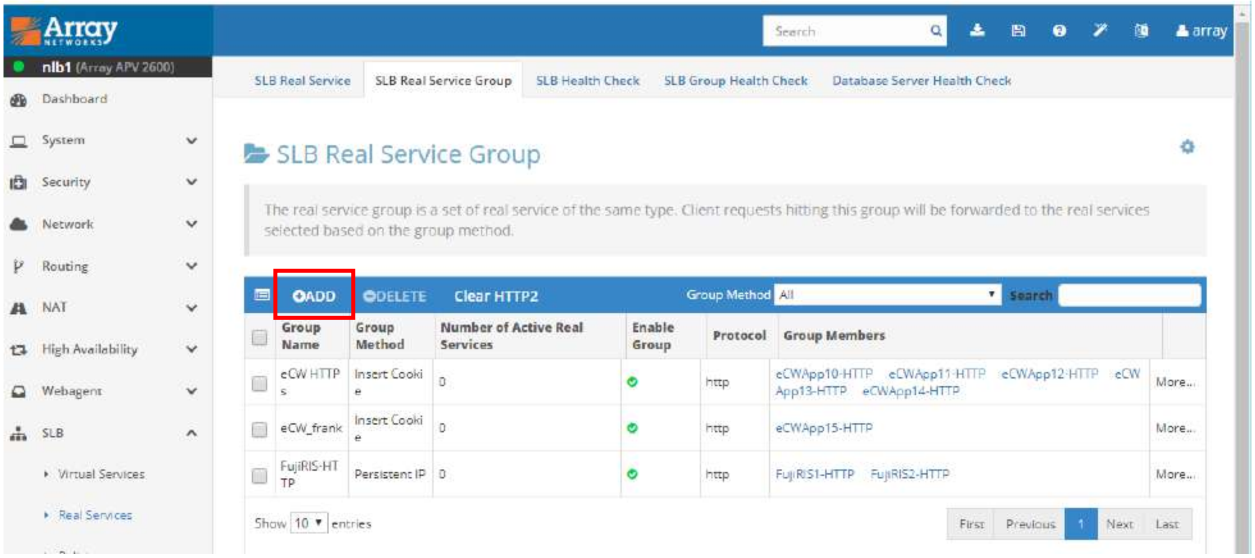


Real services are dedicated servers that provide services to clients, for example, delivery of HTTP content. Real services in one group provide the same type of service to clients and usually reside in the same physical location in a data center.

□	Real Service Name	Real Service Type	Enable Real Service	Force Offline	IP/Domain Name	Port	Up/Down Status	
□	FujiRIS1-HTTP	HTTP	✓	N/A	172.25.3.57	80	✗	More...
□	FujiRIS2-HTTP	HTTP	✓	N/A	172.25.3.56	80	✗	More...
□	eCWApp10-HTTP	HTTP	✓	N/A	172.25.5.150	8080	✗	More...
□	eCWApp11-HTTP	HTTP	✓	N/A	172.25.5.151	8080	✗	More...
□	eCWApp12-HTTP	HTTP	✓	N/A	172.25.5.152	8080	✗	More...
□	eCWApp13-HTTP	HTTP	✓	N/A	172.25.5.153	8080	✗	More...
□	eCWApp14-HTTP	HTTP	✓	N/A	172.25.5.154	8080	✗	More...
□	eCWApp15-HTTP	HTTP	✓	N/A	172.25.5.155	8080	✗	More...

3.2 Adding Groups

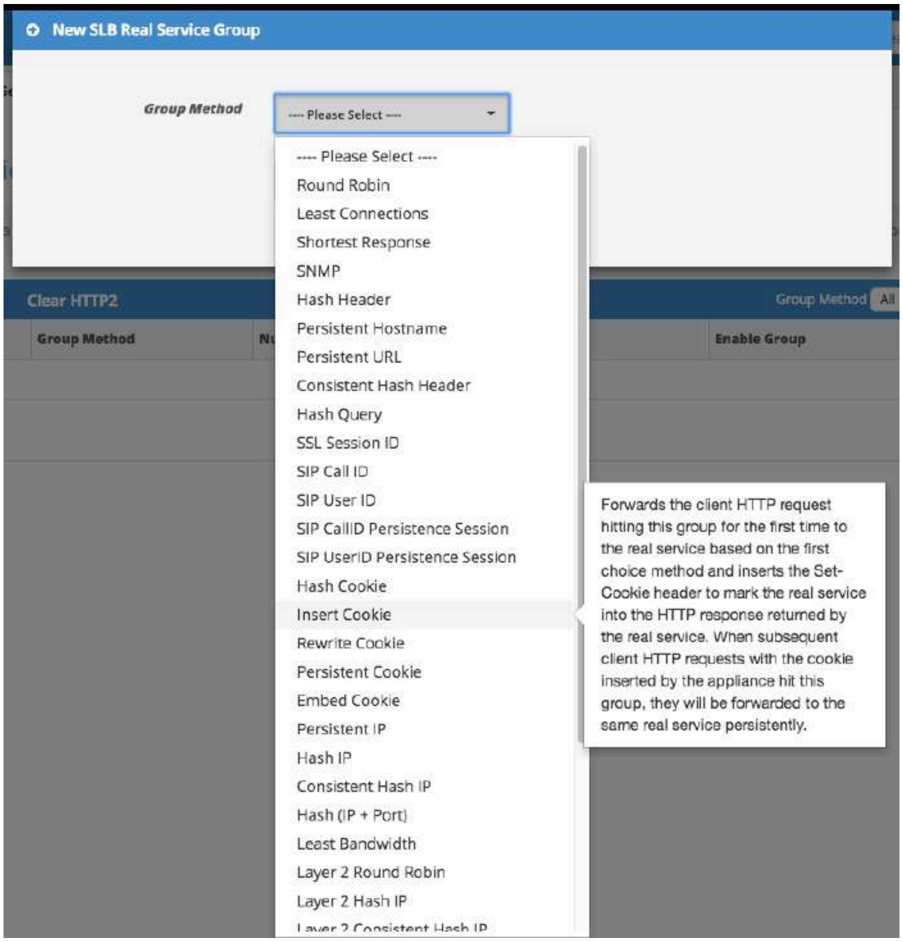
To begin configuring Groups, click on the SLB Real Service Group tab in the Real Services section, then select “Add”.



The real service group is a set of real service of the same type. Client requests hitting this group will be forwarded to the real services selected based on the group method.

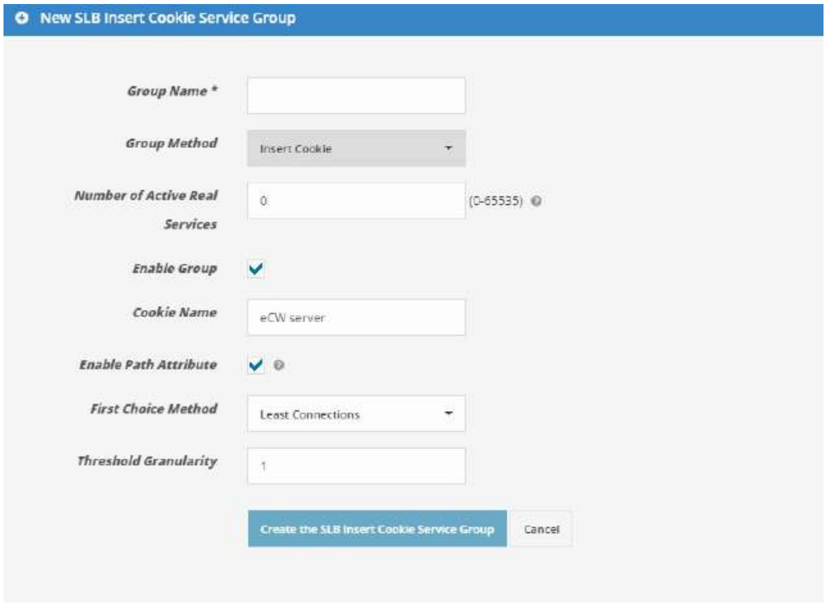
□	Group Name	Group Method	Number of Active Real Services	Enable Group	Protocol	Group Members	
□	eCW HTTPs	Insert Cookie	0	✓	http	eCWApp10-HTTP eCWApp11-HTTP eCWApp12-HTTP eCWApp13-HTTP eCWApp14-HTTP	More...
□	eCW_frank	Insert Cookie	0	✓	http	eCWApp15-HTTP	More...
□	FujiRIS-HTTP	Persistent IP	0	✓	http	FujiRIS1-HTTP FujiRIS2-HTTP	More...

Select “Insert Cookie” from the dropdown for the Group Method



Forwards the client HTTP request hitting this group for the first time to the real service based on the first choice method and inserts the Set-Cookie header to mark the real service into the HTTP response returned by the real service. When subsequent client HTTP requests with the cookie inserted by the appliance hit this group, they will be forwarded to the same real service persistently.

From the resulting dialog:



New SLB Insert Cookie Service Group

Group Name *

Group Method: Insert Cookie

Number of Active Real Services: 0 (0-65535)

Enable Group: ✓

Cookie Name: eCW server

Enable Path Attribute: ✓

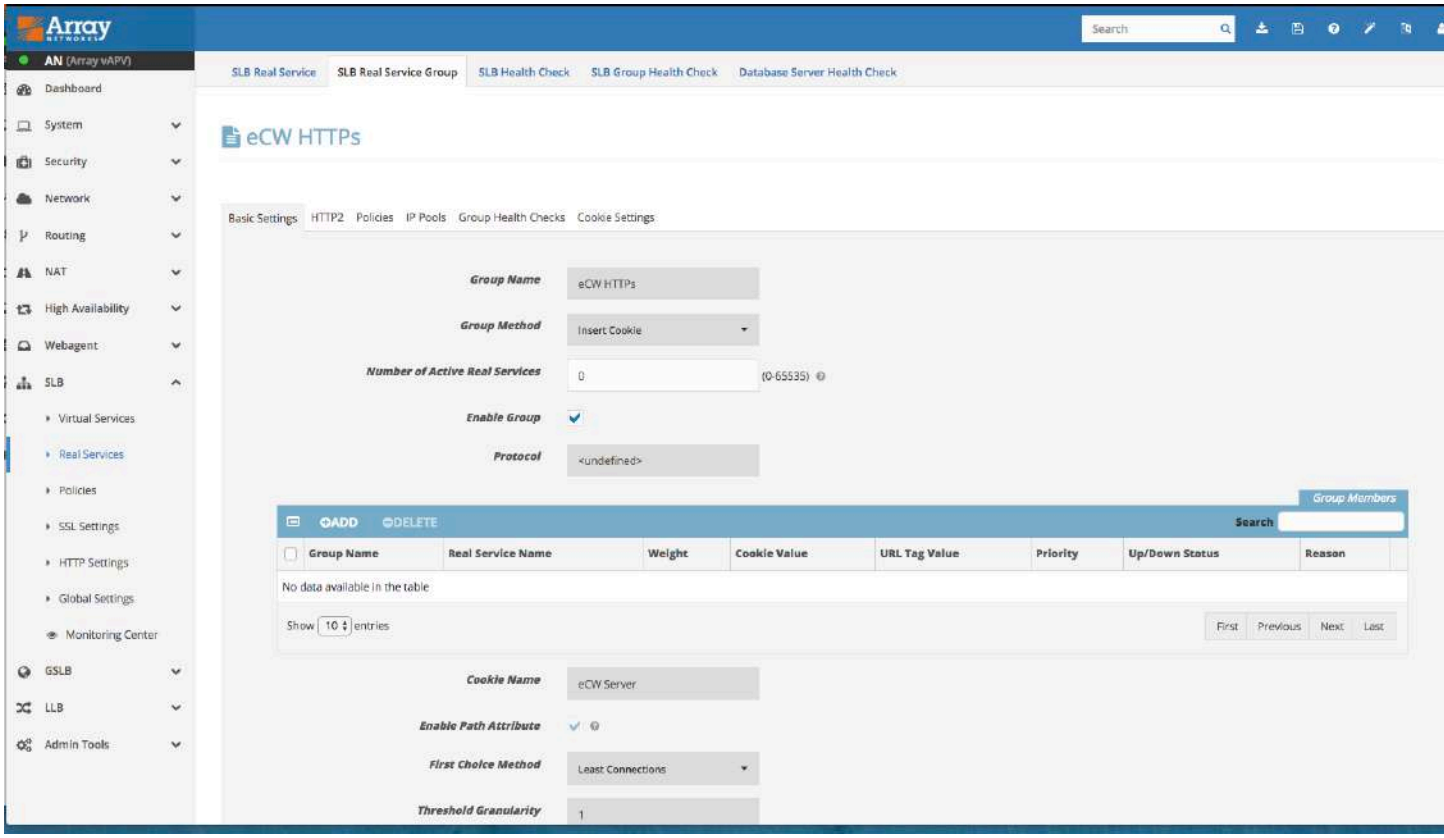
First Choice Method: Least Connections

Threshold Granularity: 1

1. Assign a Group Name (arbitrary)
2. Enable the group (make sure the checkbox is checked)
3. Assign a Cookie Name (arbitrary)
4. Enable Path Attribute (check the checkbox)
5. Select Least Connections from the dropdown for First Choice Method
6. Set the Threshold Granularity to “1”
7. Click Create the SLB Insert Cookie Service Group button. Save Config

3.2.1 Adding Real Services to a Group

Double-click on the Group Name to continue configuring the Group you just created.



eCW HTTPs

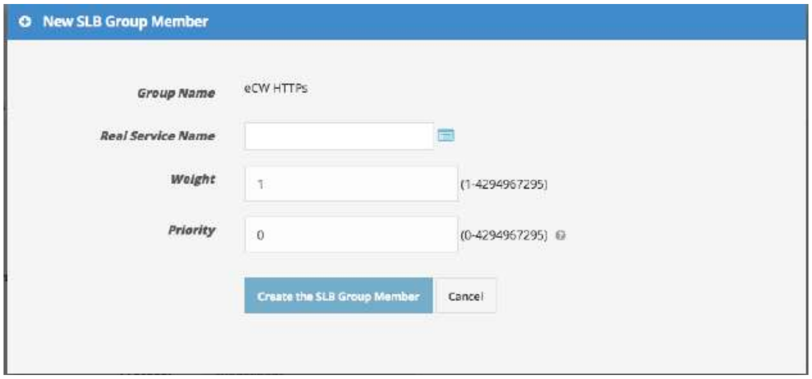
Group Name	eCW HTTPs
Group Method	Insert Cookie
Number of Active Real Services	0 (0-65535)
Enable Group	✓
Protocol	<undefined>

□	Group Name	Real Service Name	Weight	Cookie Value	URL Tag Value	Priority	Up/Down Status	Reason
No data available in the table								

Show 10 entries

Cookie Name	eCW Server
Enable Path Attribute	✓
First Choice Method	Least Connections
Threshold Granularity	1

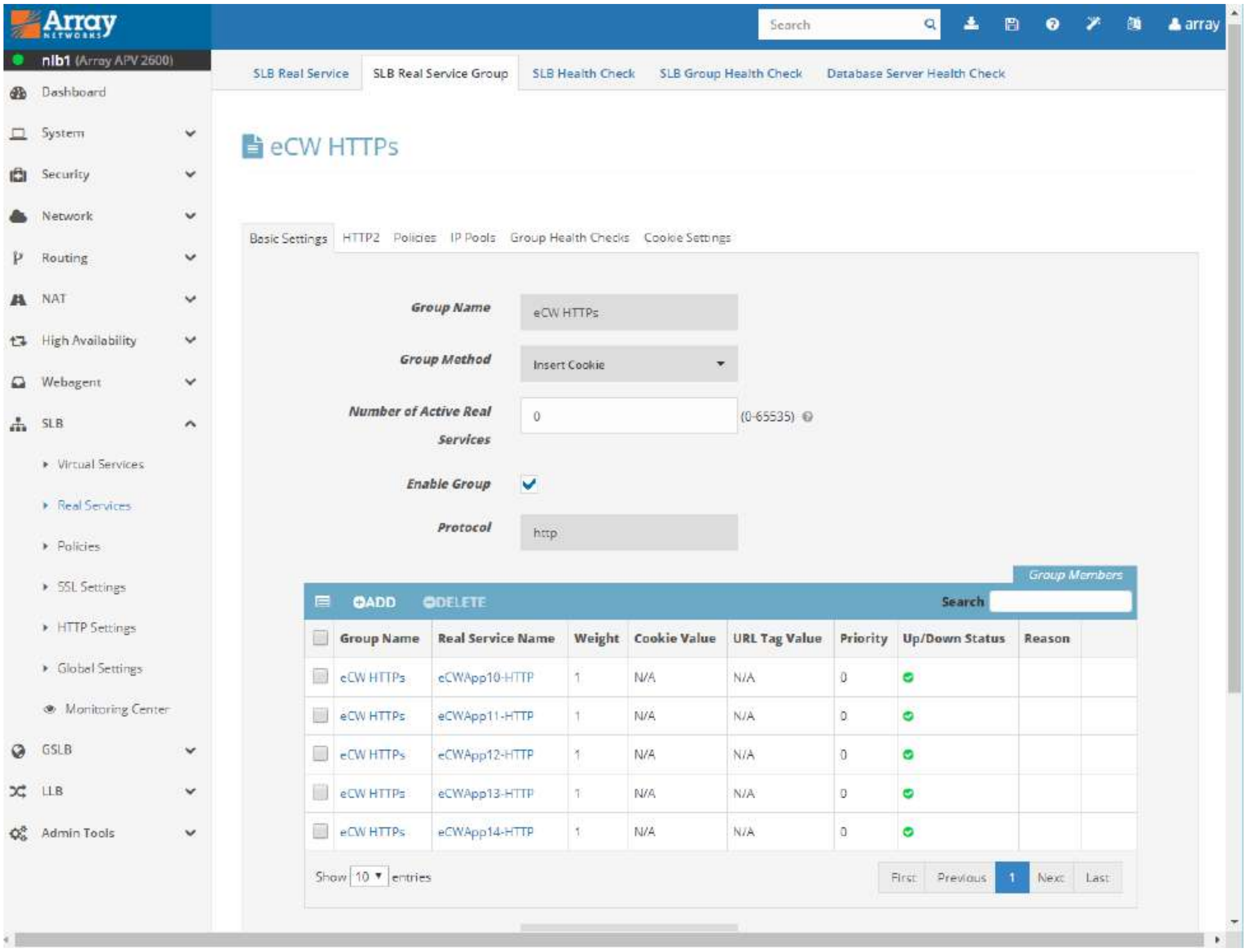
Click Add to add real services to the created service group.



New SLB Group Member

Group Name	eCW HTTPs
Real Service Name	
Weight	1 (1-4294967295)
Priority	0 (0-4294967295)

Click “Create the SLB Group Member” button.



eCW HTTPs

Group Name	eCW HTTPs
Group Method	Insert Cookie
Number of Active Real Services	0 (0-65535)
Enable Group	☑
Protocol	http

□	Group Name	Real Service Name	Weight	Cookie Value	URL Tag Value	Priority	Up/Down Status	Reason
□	eCW HTTPs	eCWApp10-HTTP	1	N/A	N/A	0	✓	
□	eCW HTTPs	eCWApp11-HTTP	1	N/A	N/A	0	✓	
□	eCW HTTPs	eCWApp12-HTTP	1	N/A	N/A	0	✓	
□	eCW HTTPs	eCWApp13-HTTP	1	N/A	N/A	0	✓	
□	eCW HTTPs	eCWApp14-HTTP	1	N/A	N/A	0	✓	

Scroll down to the Group Members section and select the Real Servers (from the Eligible Reals dropdown) that will be part of the group. You will need to click Add at the top of the Group Members table, select each Real Server individually, then click on Add to add another. When done adding servers, Save then Save Config.

3.2.2 Group Status

Verify the Real Service Status under Group Members, as shown above.

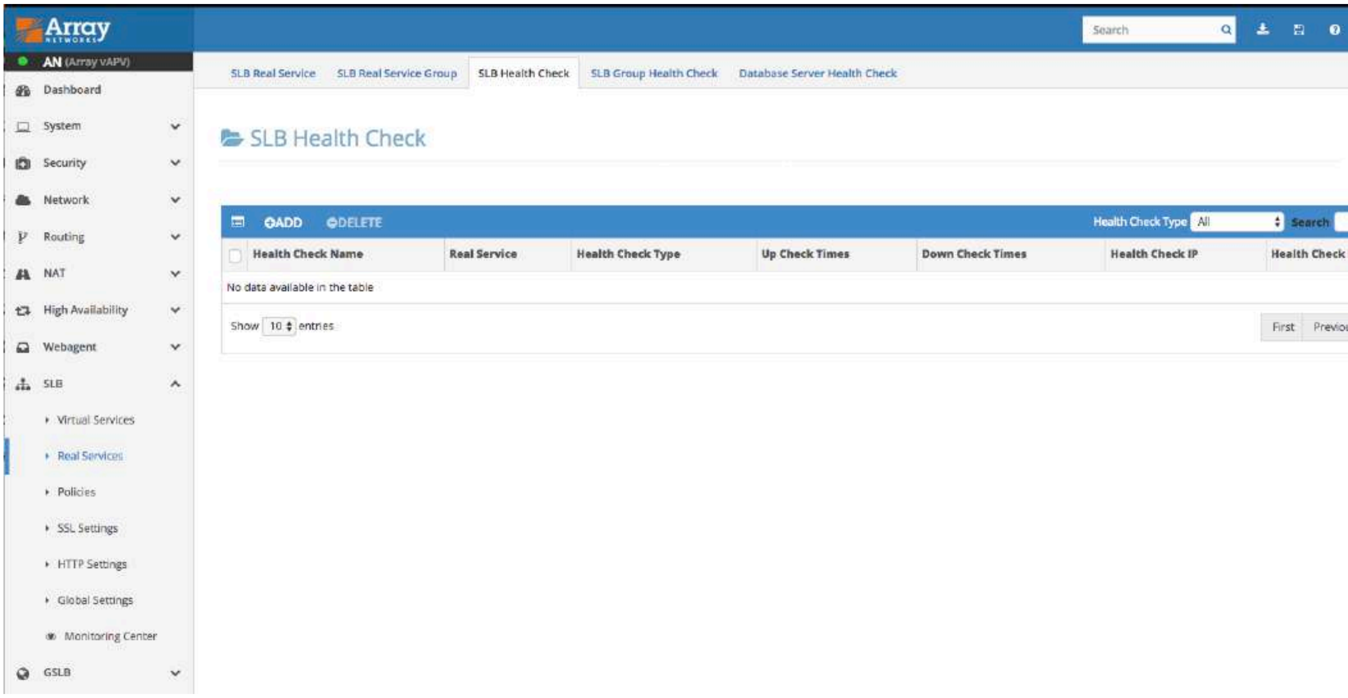
3.2 Health Check Settings

Next, configure the Health Check Settings for the eClinicalWorks application. The Health Check Settings are used by the APV to verify that the eCW application server is running.

If a real service is detected as down, the server is removed from rotation to ensure application availability. When the server is back up in operation, it automatically gets returned to the list of available servers.

3.2.1 Configuring Health Check Settings

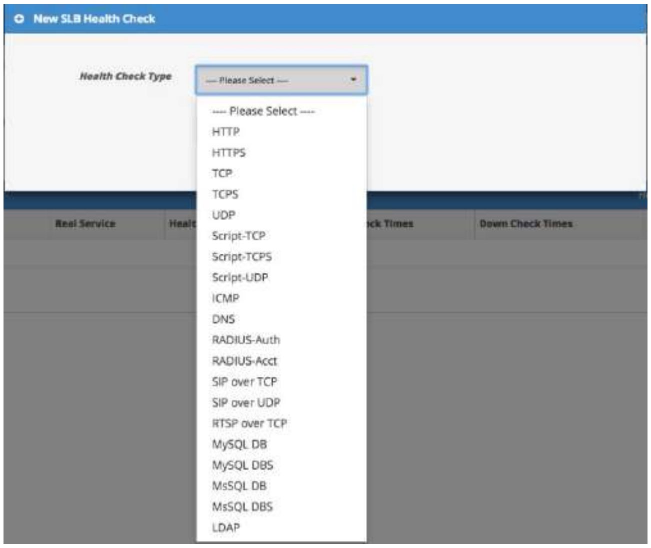
From the SLB section, select Real Services, then the SLB Health Check tab. Here we configure the health check settings that will be used to test the health of the eCW application servers. Please note that there will be default health checks here, but please follow along with the instructions below. Click on the Add link on the left.



□ Health Check Name	Real Service	Health Check Type	Up Check Times	Down Check Times	Health Check IP	Health Check
No data available in the table						

Show 10 entries

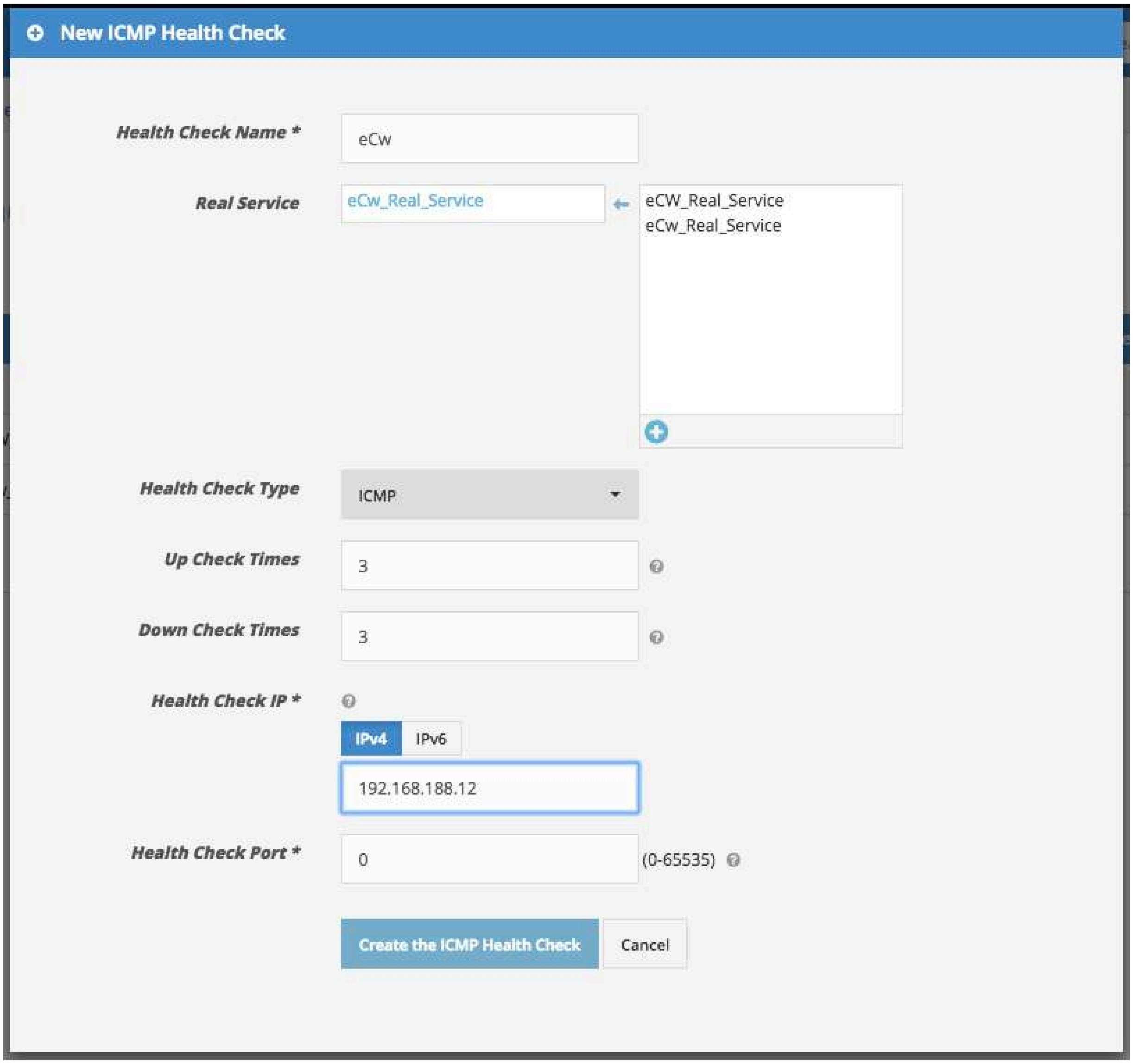
Choose “HTTP” from the Health Check Type drop down list:



Add the Health Check Name (arbitrary value).

Click the picker box ▤ and choose the real server you’d like checked.

Add the IP address and port you would like checked (leave the port set to “0” for ICMP health checks).



New ICMP Health Check

Health Check Name * eCw

Real Service eCw_Real_Service

eCW_Real_Service
eCw_Real_Service

Health Check Type ICMP

Up Check Times 3

Down Check Times 3

Health Check IP * IPv4 IPv6 192.168.188.12

Health Check Port * 0 (0-65535)

Once complete, click “Create the ICMP Health Check”. Create a health check for each, real server. Once complete, save the configuration.

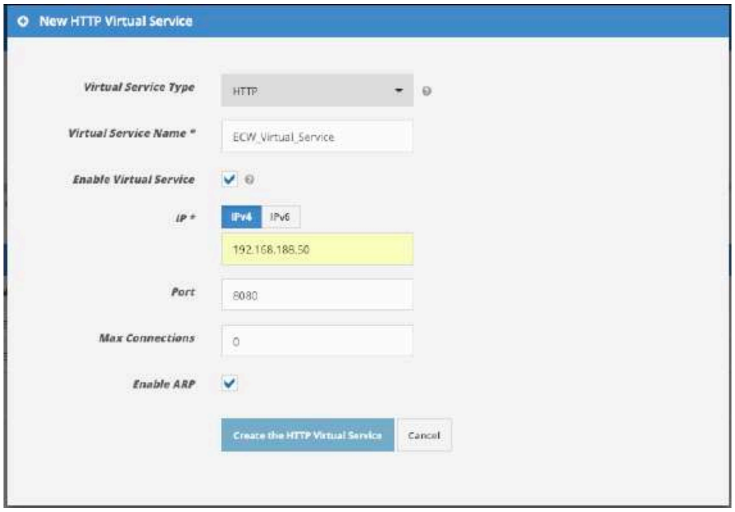
3.3a Add a Virtual HTTP Service

The next step is to create an SLB Virtual Service for the APV Series to allow the client to access these services. On the APV appliance, a Virtual Service is defined by a Virtual IP/Port and the protocol. External client requests will be terminated on it and the APV appliance will load balance the requests to different Real Services. Follow these steps to configure the Virtual Service for eCW:

From the SLB section, click on Virtual Services. Click Add to add a new Virtual Service.

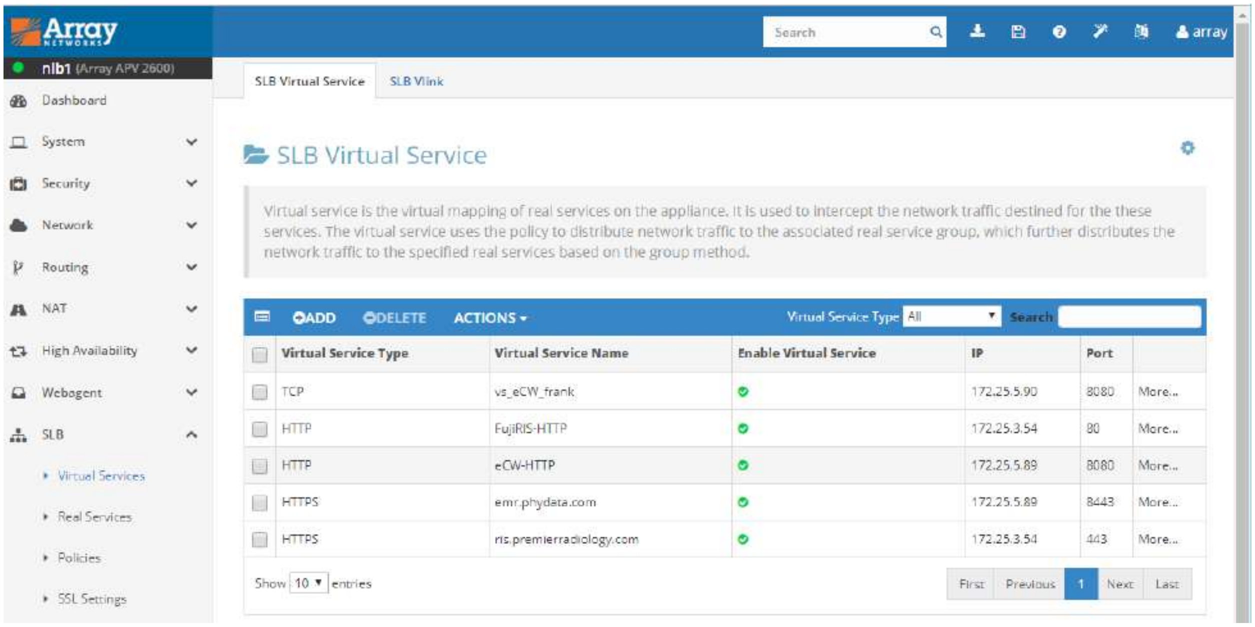
1. Set the Virtual Service Type to “HTTP” from the dropdown.
2. Add a Virtual Service name (arbitrary) and tick the checkbox to Enable this Service.

3. Configure the IP address for the Virtual Service.
4. Assign the Virtual Service Port (8080).
5. Click Create the HTTP Virtual Service to create the Virtual Service.



Virtual Service Type	HTTP
Virtual Service Name *	ECW_Virtual_Service
Enable Virtual Service	☑
IP *	IPv4 IPv6 192.168.188.50
Port	8080
Max Connections	0
Enable ARP	☑

Double-click on the Virtual Service name to continue making configuration settings.

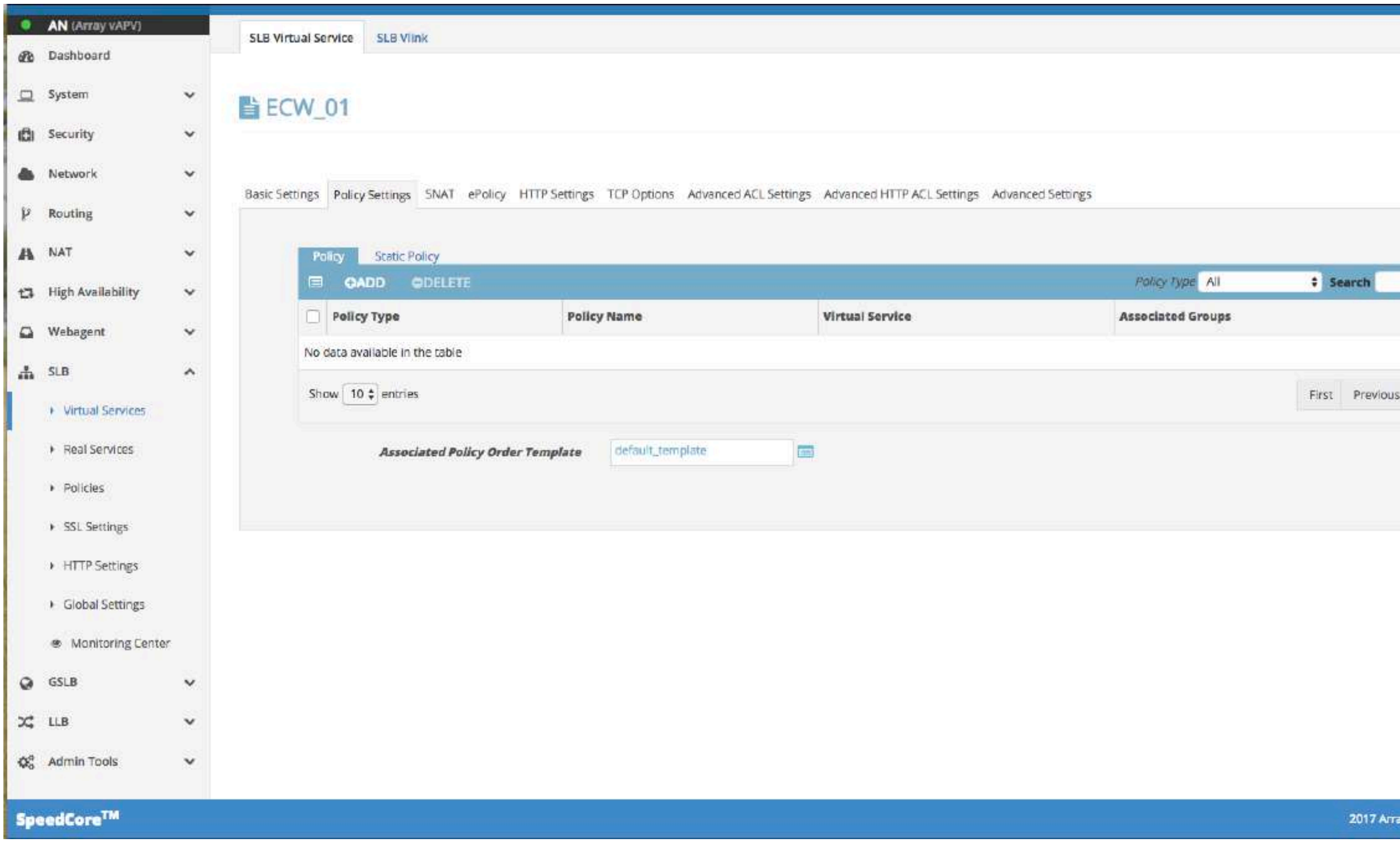


SLB Virtual Service

Virtual service is the virtual mapping of real services on the appliance. It is used to intercept the network traffic destined for the these services. The virtual service uses the policy to distribute network traffic to the associated real service group, which further distributes the network traffic to the specified real services based on the group method.

□	Virtual Service Type	Virtual Service Name	Enable Virtual Service	IP	Port	
□	TCP	vs_eCW_frank	✓	172.25.5.90	8080	More...
□	HTTP	FujiRIS-HTTP	✓	172.25.3.54	80	More...
□	HTTP	eCW-HTTP	✓	172.25.5.89	8080	More...
□	HTTPS	emr.phydata.com	✓	172.25.5.89	8443	More...
□	HTTPS	ris.premierradiology.com	✓	172.25.3.54	443	More...

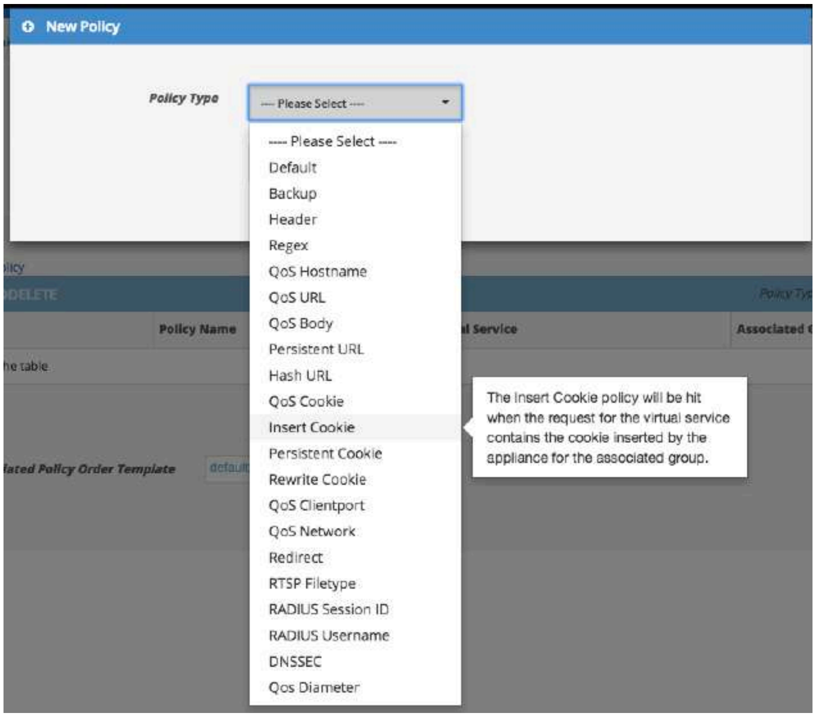
Choose the tab “Policy Settings” and click “Add”. A policy is needed to tie everything together (virtual service with real servers).



No data available in the table

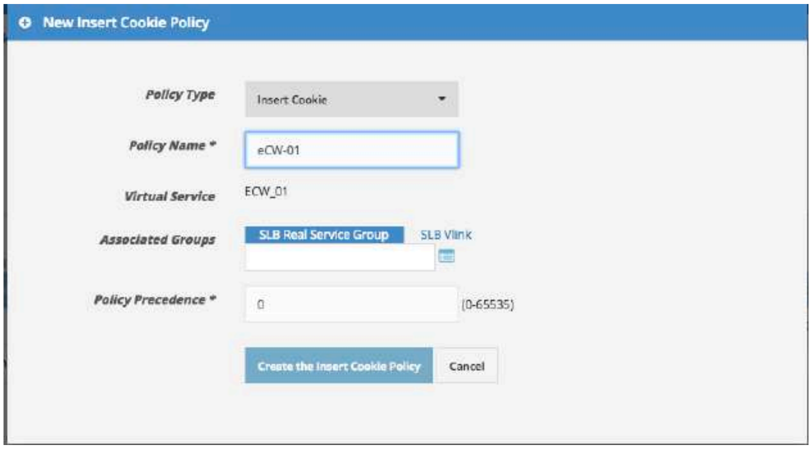
Associated Policy Order Template: default_template

Choose “Insert Cookie” from the Eligible Policies dropdown.



The Insert Cookie policy will be hit when the request for the virtual service contains the cookie inserted by the appliance for the associated group.

Assign a policy name (arbitrary).



New Insert Cookie Policy

Policy Type: Insert Cookie

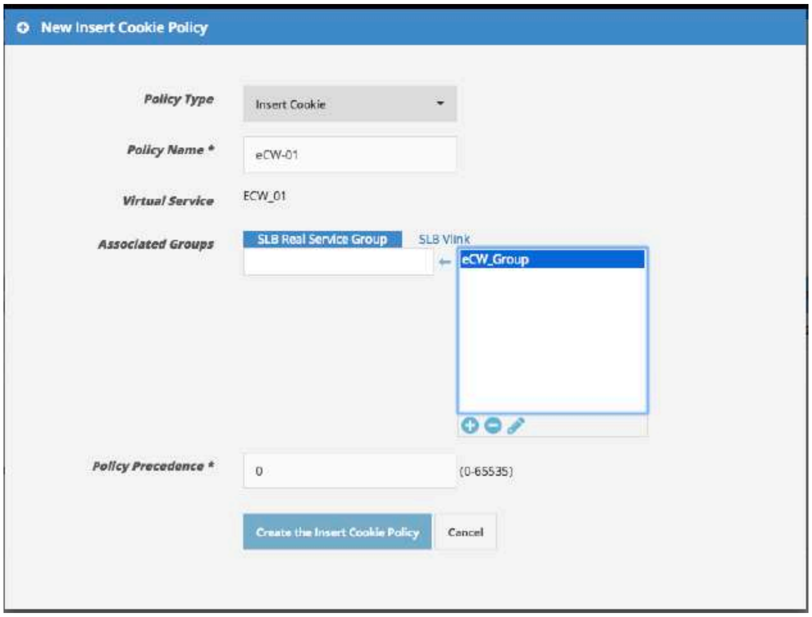
Policy Name *: eCW-01

Virtual Service: ECW_01

Associated Groups: SLB Real Service Group | SLB Vlink

Policy Precedence *: 0 (0-65535)

Click the picker box and choose the group you just created.



New Insert Cookie Policy

Policy Type: Insert Cookie

Policy Name *: eCW-01

Virtual Service: ECW_01

Associated Groups: SLB Real Service Group | SLB Vlink

eCW_Group

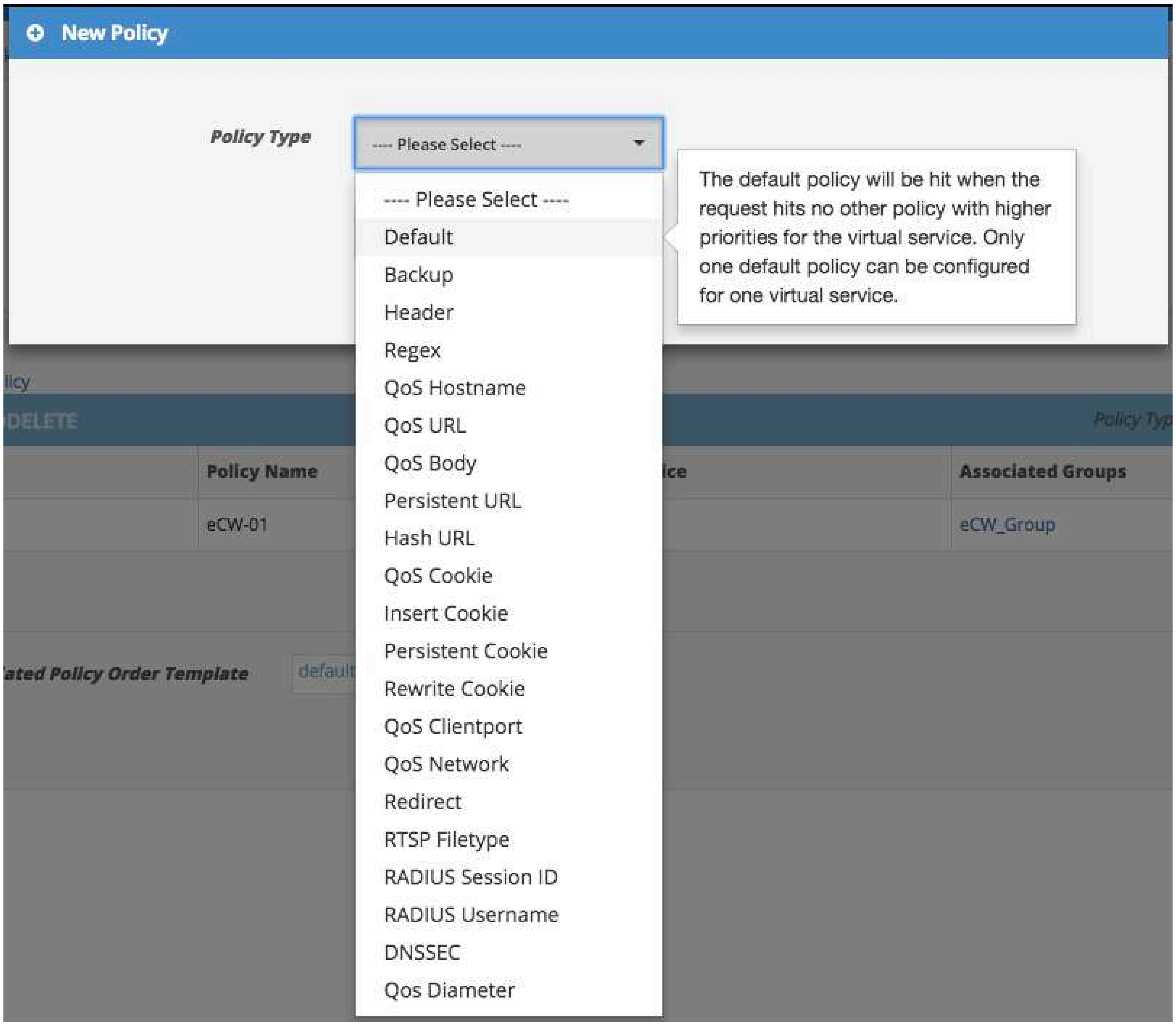
Policy Precedence *: 0 (0-65535)

Ensure “0” is selected for the Policy Precedence and click the “Create the Insert Cookie Policy” button to create the policy. Save the configuration.

3.3a.1 Virtual Service Default Policy

All Group associations must include a default policy (the policy that is executed if all prior policy conditions are not met/used). To set the default policy:

1. In the SLB > Virtual Services section, select the Policy Settings tab.
2. Click “Add” as above.
3. For policy type, choose “Default”.



The default policy will be hit when the request hits no other policy with higher priorities for the virtual service. Only one default policy can be configured for one virtual service.

4. Click the picker box and choose the group for which you just created the Insert Cookie policy.

5. Click “Create the Default Policy” and Save Config.

If the Virtual Service is HTTP, then you are done. At this point, your Virtual Service should be accessible.

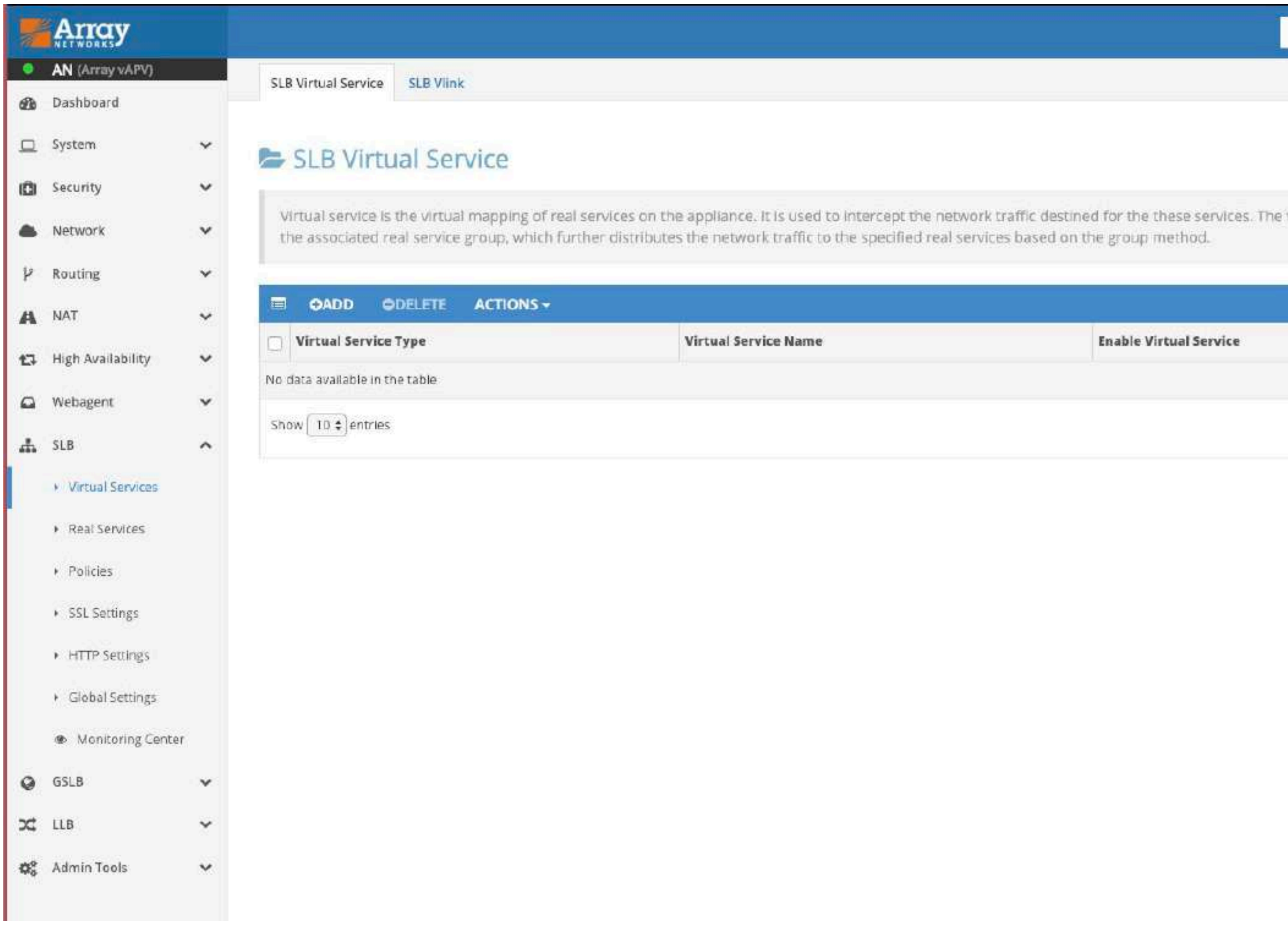
If the Virtual Service is HTTPS, go to the next section.

3.3b Add a Virtual HTTPS Service

When HTTPS service support is required, this is how you add it:

On the APV appliance, a Virtual is defined by a Virtual IP/Port and the protocol. External client requests will be terminated on it and the APV appliance will load balance the requests to different Real Services. Follow these steps to configure the Virtual Service for eCW:

From the SLB section, click on Virtual Services. Click Add to add a new Virtual Service.

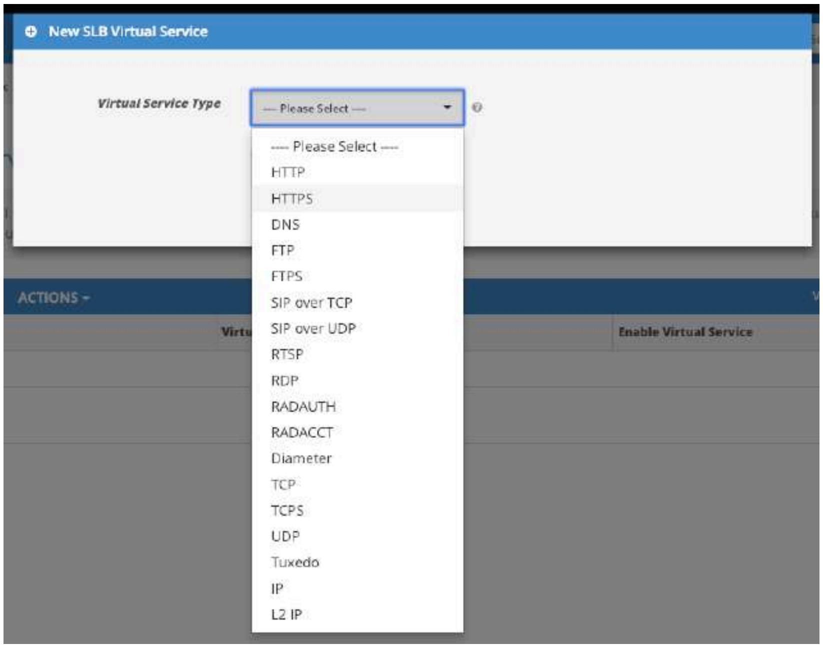


SLB Virtual Service

Virtual service is the virtual mapping of real services on the appliance. It is used to intercept the network traffic destined for the these services. The v
the associated real service group, which further distributes the network traffic to the specified real services based on the group method.

□ Virtual Service Type	Virtual Service Name	Enable Virtual Service
No data available in the table		

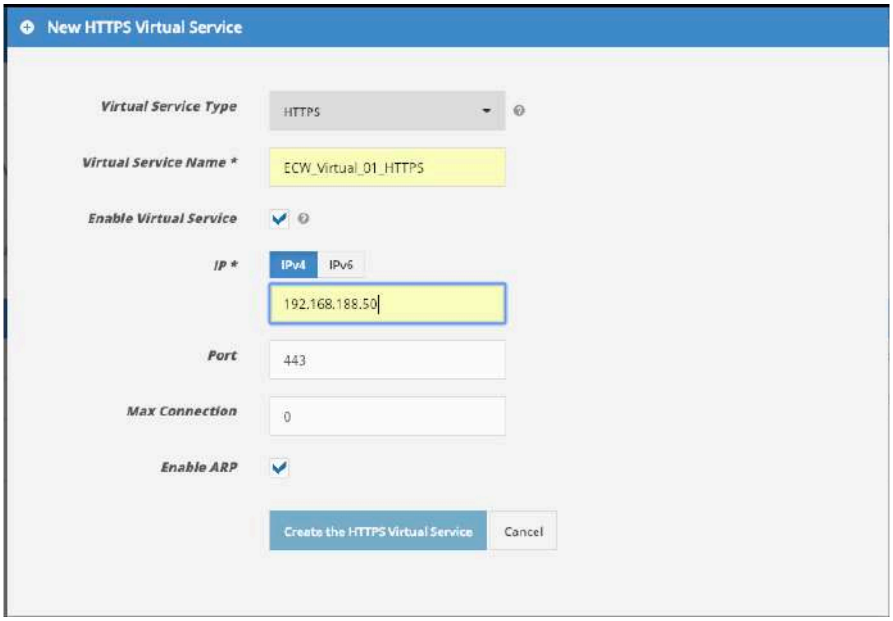
1. Set the Virtual Service Type to “HTTPS” from the dropdown.



2. Add a Virtual Service name (arbitrary) and tick the checkbox to Enable this Service.

3. Configure the IP address for the Virtual Service.

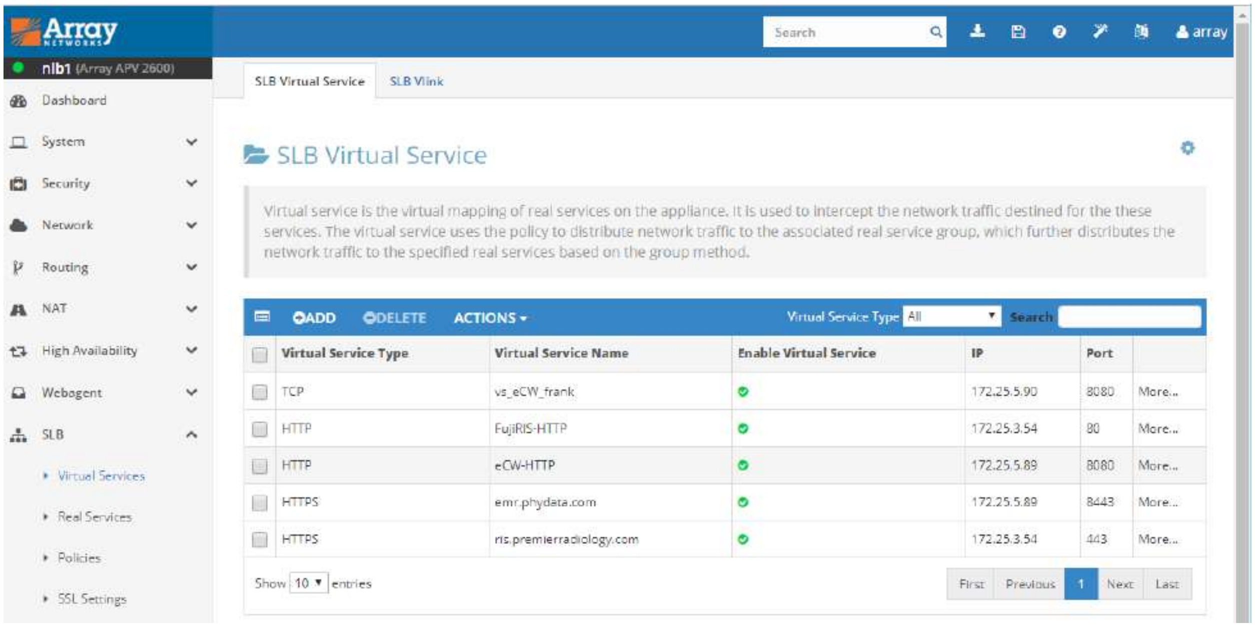
4. Leave the remaining items at their default values *(Port 443, Max Connections 0, and Enable ARP checked)*.
5. Click Create the HTTPS Virtual Service to create the Virtual Service.



New HTTPS Virtual Service

Virtual Service Type	HTTPS
Virtual Service Name *	ECW_Virtual_01_HTTPS
Enable Virtual Service	☑
IP *	IPv4 IPv6 192.168.188.50
Port	443
Max Connection	0
Enable ARP	☑

Double-click on the Virtual Service name to continue making configuration changes.

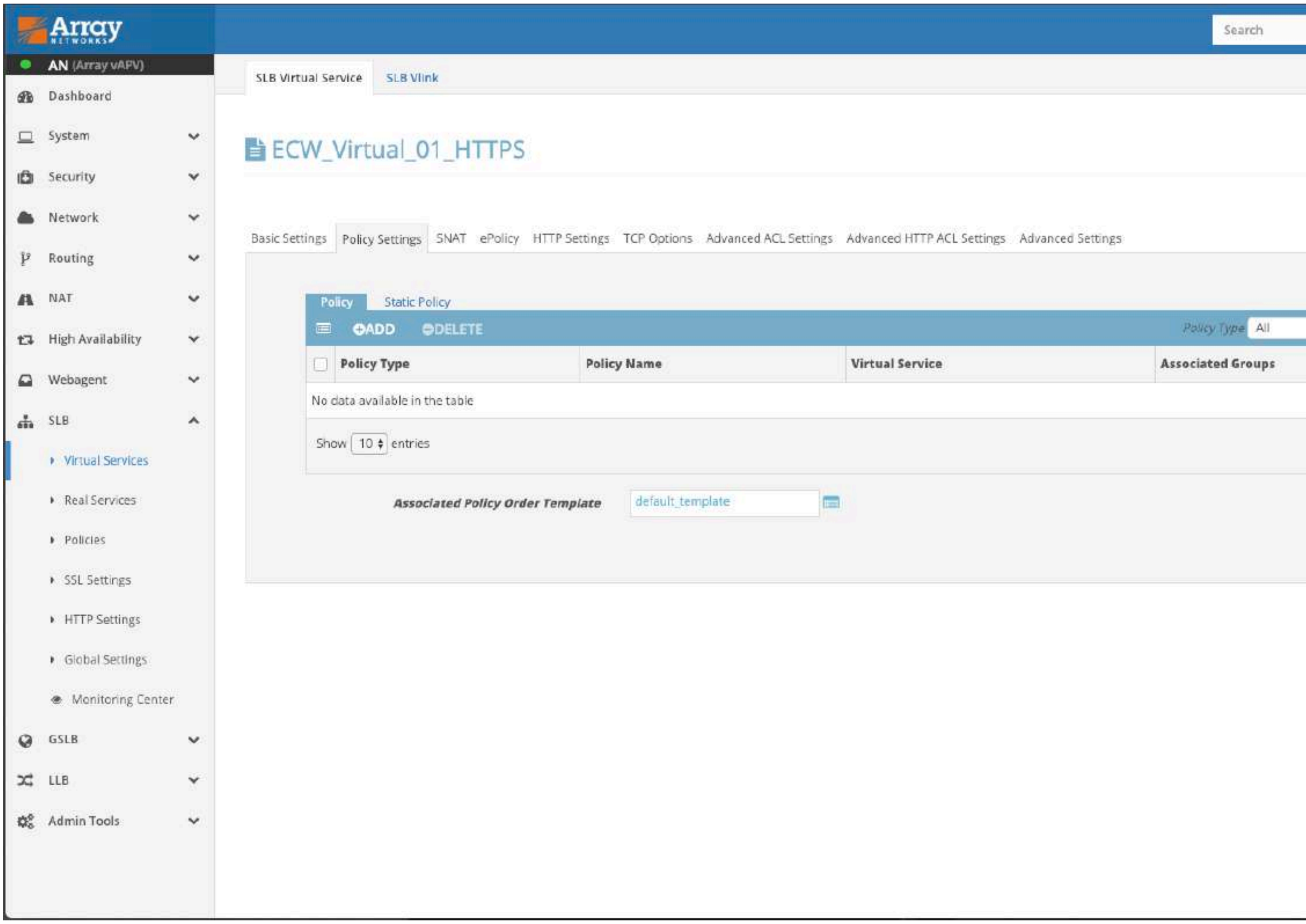


SLB Virtual Service

Virtual service is the virtual mapping of real services on the appliance. It is used to intercept the network traffic destined for the these services. The virtual service uses the policy to distribute network traffic to the associated real service group, which further distributes the network traffic to the specified real services based on the group method.

□	Virtual Service Type	Virtual Service Name	Enable Virtual Service	IP	Port	
□	TCP	vs_eCW_frank	✓	172.25.5.90	8080	More...
□	HTTP	FujiRIS-HTTP	✓	172.25.3.54	80	More...
□	HTTP	eCW-HTTP	✓	172.25.5.89	8080	More...
□	HTTPS	emr.phydata.com	✓	172.25.5.89	8443	More...
□	HTTPS	ris.premierradiology.com	✓	172.25.3.54	443	More...

Choose the tab "Policy Settings" and click "Add". A policy is needed to tie everything together (virtual service with real servers).



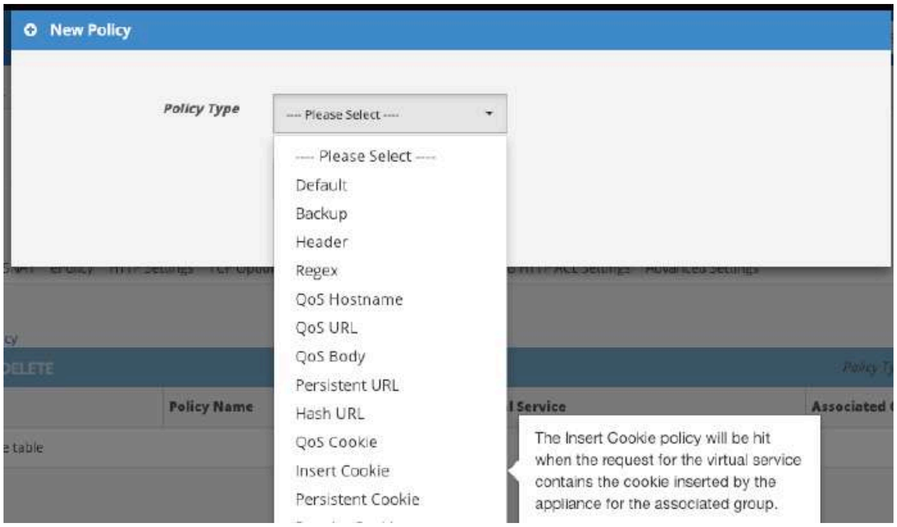
ECW_Virtual_01_HTTPS

Policy Type	Policy Name	Virtual Service	Associated Groups
No data available in the table			

Show 10 entries

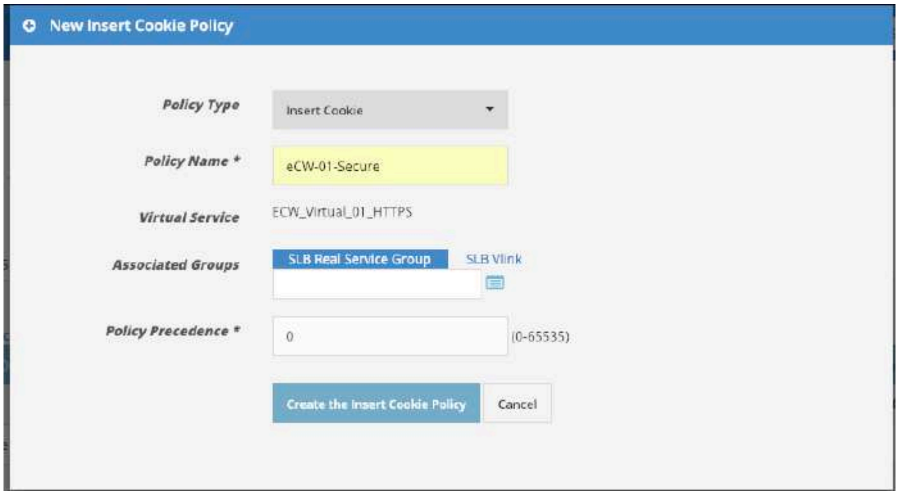
Associated Policy Order Template: default_template

Choose “Insert Cookie” from the Eligible Policies dropdown.



The Insert Cookie policy will be hit when the request for the virtual service contains the cookie inserted by the appliance for the associated group.

Assign a policy name (arbitrary).



New Insert Cookie Policy

Policy Type: Insert Cookie

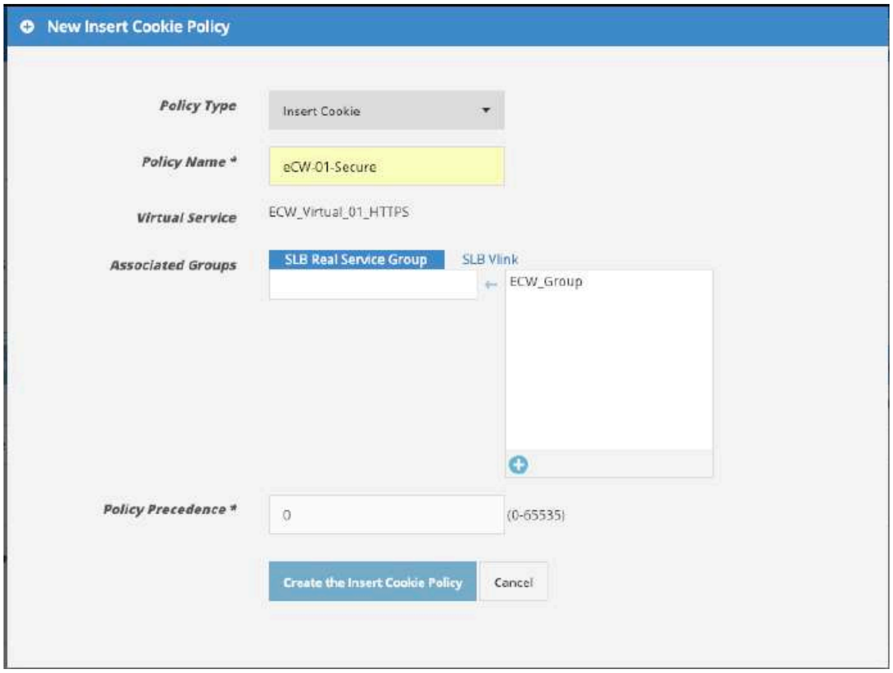
Policy Name *: eCW-01-Secure

Virtual Service: ECW_Virtual_01_HTTPS

Associated Groups: SLB Real Service Group | SLB Vlink

Policy Precedence *: 0 (0-65535)

Click the picker box ▤ and choose the group you just created. Then click the arrow.



New Insert Cookie Policy

Policy Type: Insert Cookie

Policy Name *: eCW-01-Secure

Virtual Service: ECW_Virtual_01_HTTPS

Associated Groups: SLB Real Service Group | SLB Vlink

ECW_Group

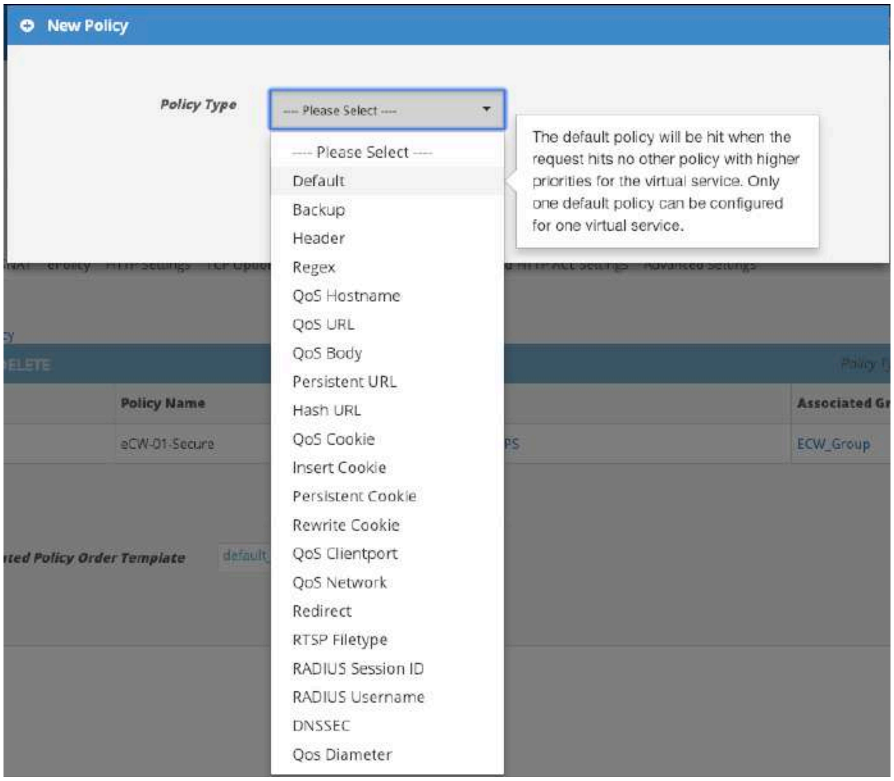
Policy Precedence *: 0 (0-65535)

Ensure “0” is selected for the Policy Precedence and click the “Create the Insert Cookie Policy” to create the policy. Save the configuration.

3.3b.1 Virtual Service Default Policy

All Group associations must include a default policy (the policy that is executed if all prior policy conditions are not met/used). To set the default policy:

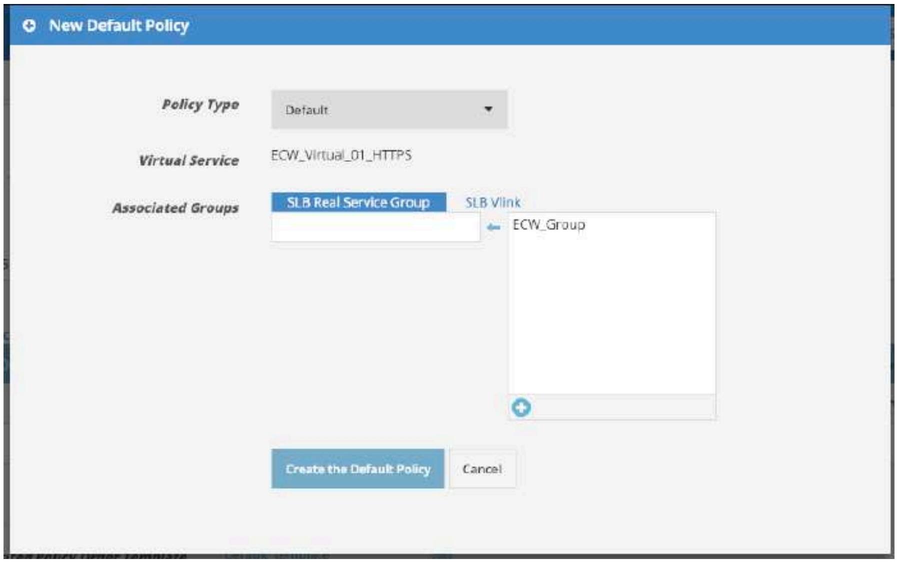
6. In the SLB > Virtual Services section, select the Policy Settings tab.
7. Click “Add” as above.
8. For policy type, choose “Default”.



Policy Type

The default policy will be hit when the request hits no other policy with higher priorities for the virtual service. Only one default policy can be configured for one virtual service.

9. Click the picker box ▤ and choose the group for which you just created the Insert Cookie policy. Then click the arrow.



Policy Type: Default

Virtual Service: ECW_Virtual_01_HTTPS

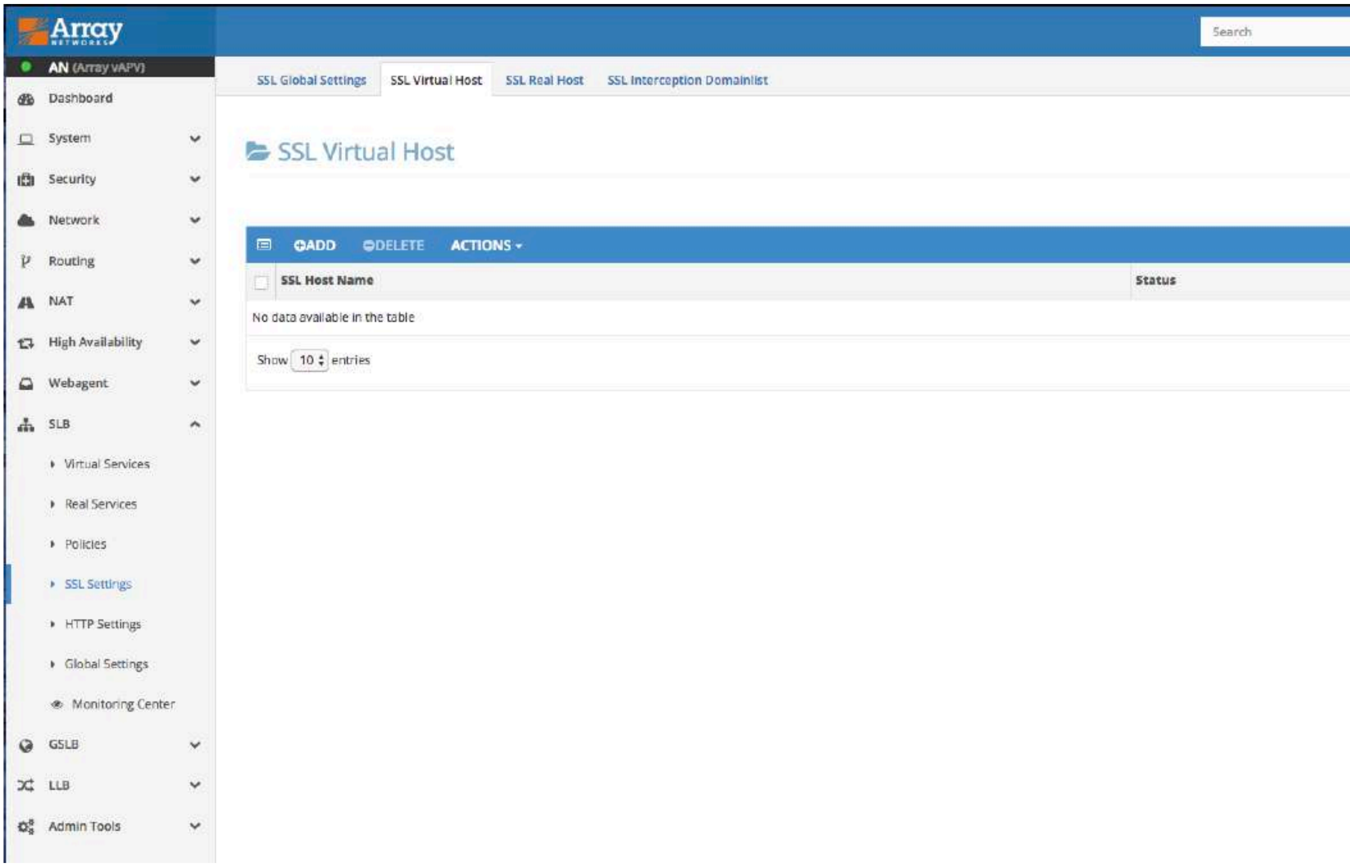
Associated Groups: ECW_Group

10. Click “Create the Default Policy” and Save Config.

3.3.2 Add an SSL Virtual Host

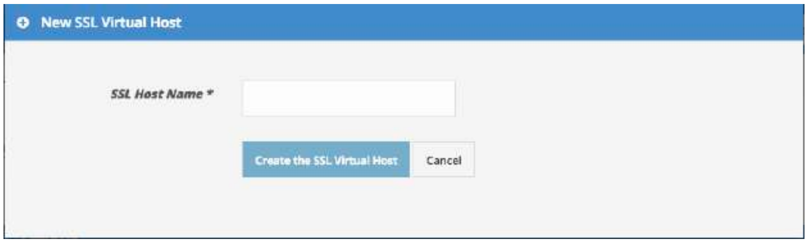
An SSL virtual host is required when you want to offload HTTPS traffic to the load balancer. This is usually done to reduce load on the backend servers, and your load balancer is specifically designed to handle these types of loads.

To begin configuring the SSL settings, go to SLB → SSL Settings. Click on the SSL Virtual Host tab.

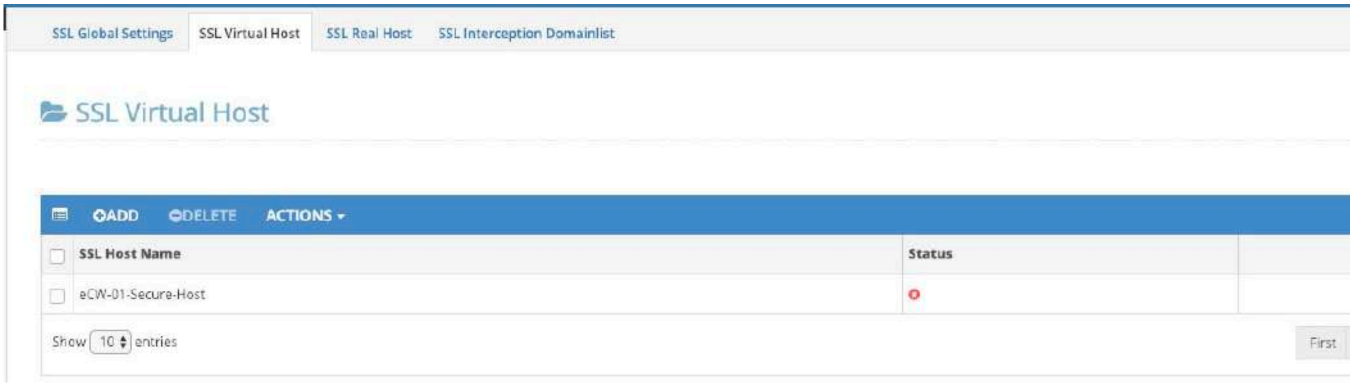


No data available in the table

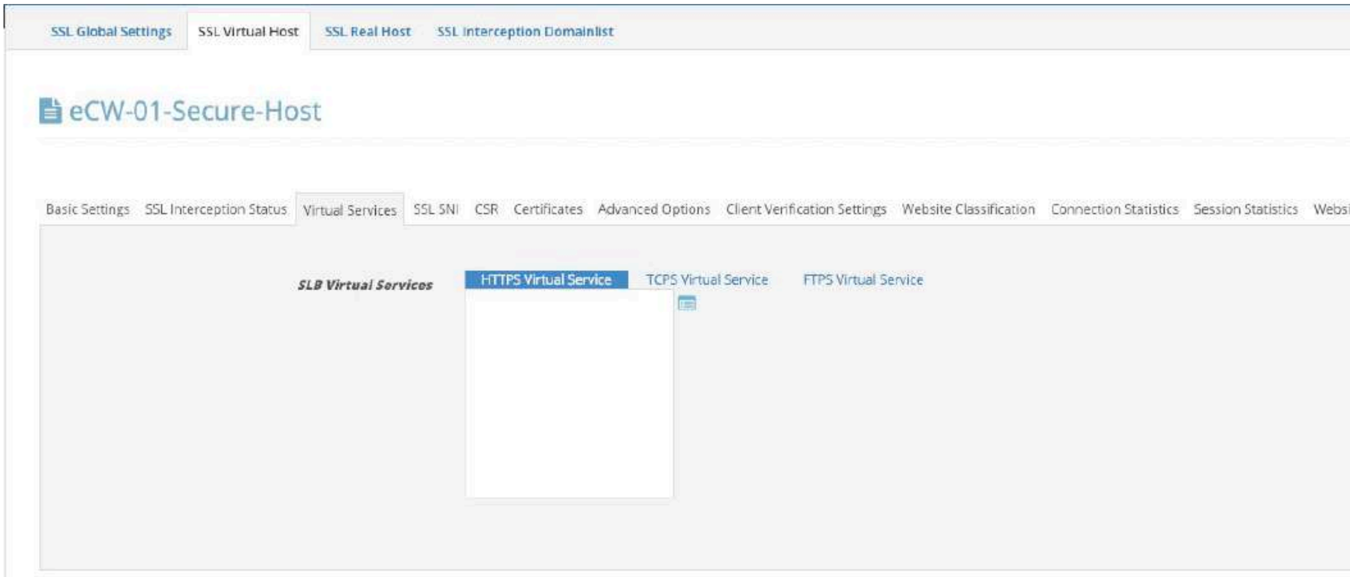
Once you are on the Virtual Hosts page, click on the “Add” link on the left of the window and in the Virtual Host Name field, assign a descriptive name to the Virtual Host you are creating. Note that neither spaces nor most special characters are allowed here.



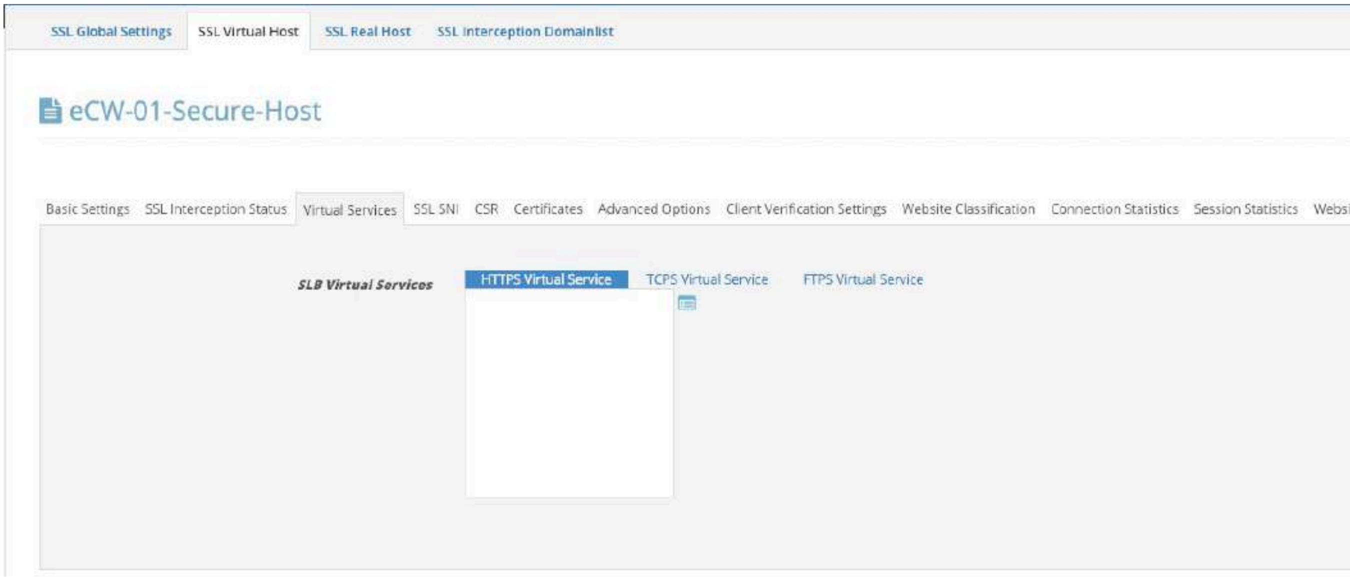
Next, double click the host name you just created and choose the virtual services tab, toward the middle of the resulting page.



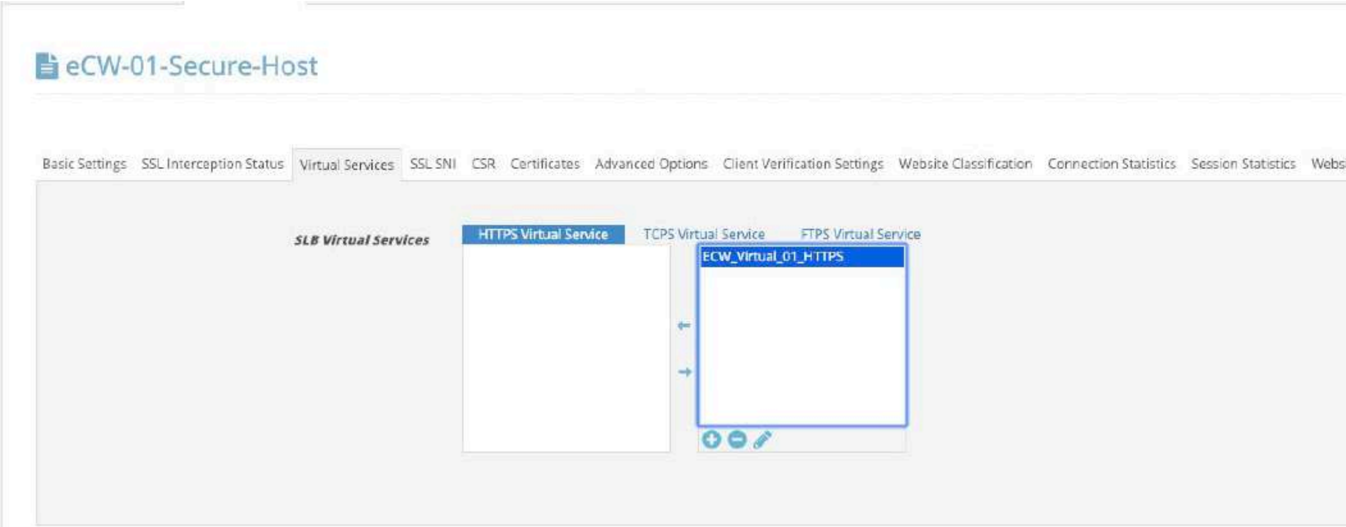
□	SSL Host Name	Status
□	eCW-01-Secure-Host	○



Click the picker box ▤ and choose the service for which you will be offloading SSL. Then click the arrow.



Click “Save Changes”.



SLB Virtual Services: ECW_Virtual_01_HTTPS

If you can't see the virtual service listed in the dropdown, it is probably because you have not configured it as type: HTTPS. Please go back to Virtual Services, and create a group with the type HTTPS.

3.3.3 Configure the SSL Virtual Host

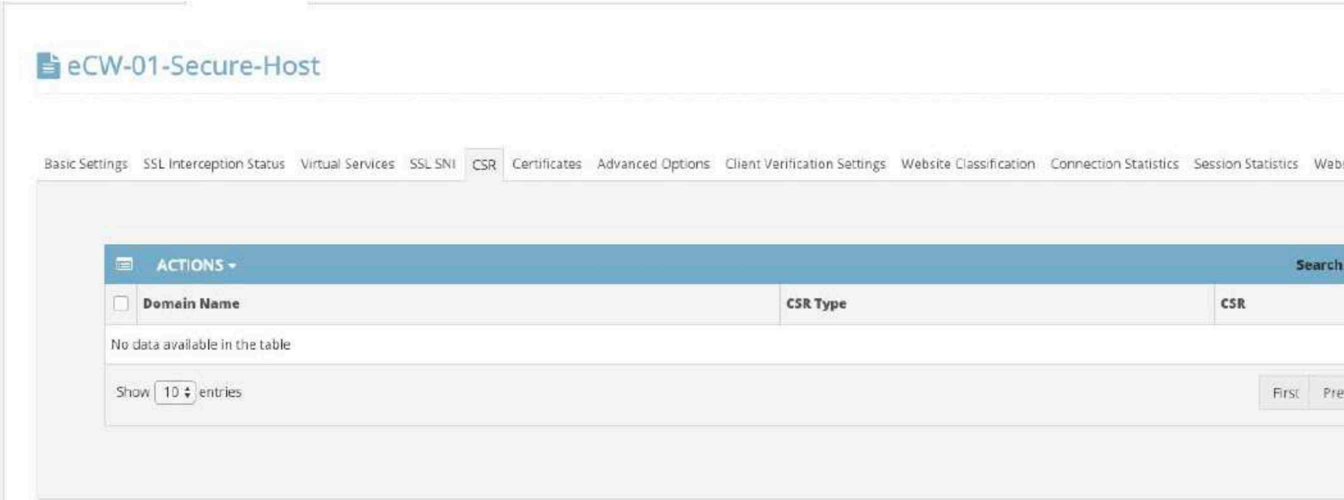
Instructions for importing and assigning an existing SSL certificate will follow, in this section. Generating a CSR (Certificate signing Request) is only necessary if you need to purchase an SSL Certificate.

All references to "SSL" should be considered to include SSL, TLS or any mixture of those technologies you wish to use.

We will go through the process of setting up a self-signed certificate so you can move forward with SSL.

Choose the "CSR" tab; this menu is reached by either clicking the tab in the menu after 3.3.2 (above), or choosing SSL Settings from the left menu, SSL Virtual Hosts from the tabs near the top, double-clicking the host for which you want to generate a certificate, and then choosing the "CSR" tab.

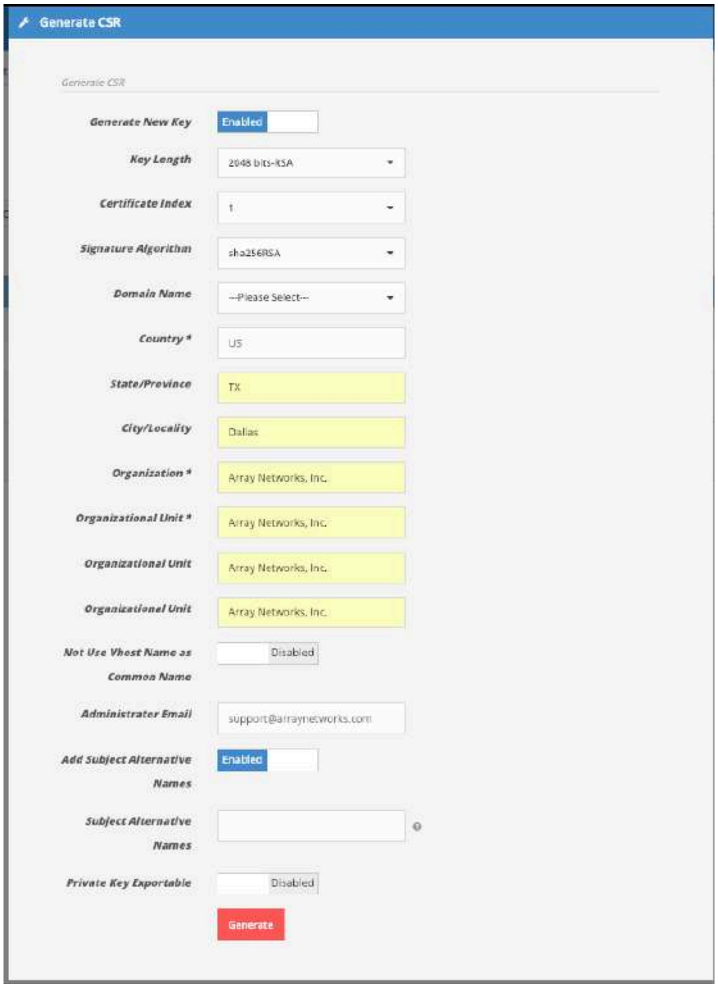
From the Actions menu, click Generate CSR.



□	Domain Name	CSR Type	CSR
No data available in the table			

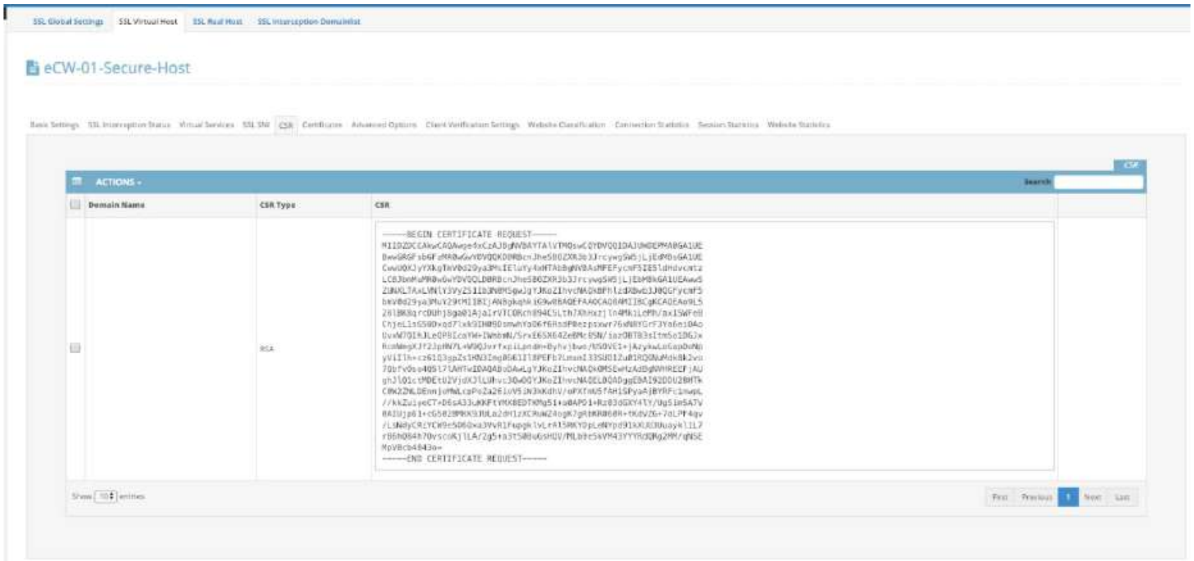
Show 10 ÷ entries

As the field data is explanatory, we will skip a line-by-line instruction. Please keep in mind that blanks with an asterisk are required information.



Generate New Key	Enabled
Key Length	2048 bits-RSA
Certificate Index	1
Signature Algorithm	sha256RSA
Domain Name	--Please Select--
Country *	US
State/Province	TX
City/Locality	Dallas
Organization *	Array Networks, Inc.
Organizational Unit *	Array Networks, Inc.
Organizational Unit	Array Networks, Inc.
Organizational Unit	Array Networks, Inc.
Not Use Vhost Name as Common Name	Disabled
Administrater Email	support@arraynetworks.com
Add Subject Alternative Names	Enabled
Subject Alternative Names	
Private Key Exportable	Disabled

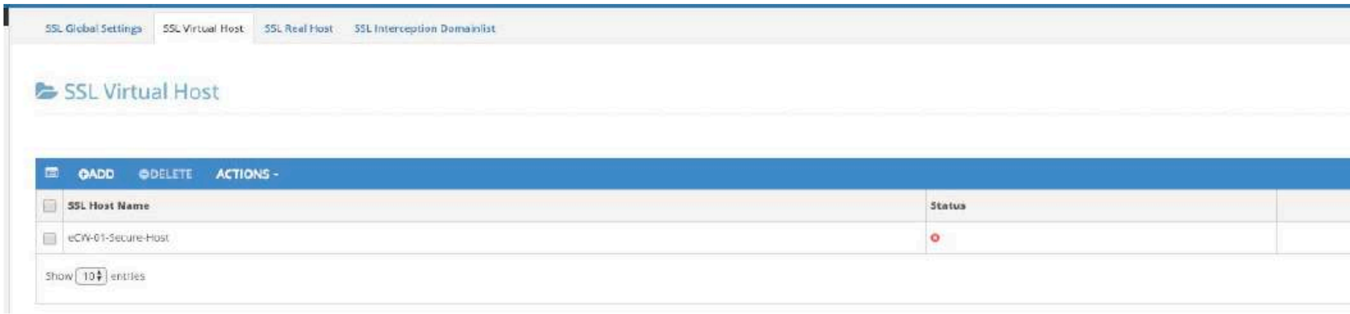
The result of properly filling the above information out is a page that looks like this:



eCW-01-Secure-Host

Domain Name	CSR Type	CSR
	RSA	-----BEGIN CERTIFICATE REQUEST----- [illegible] -----END CERTIFICATE REQUEST-----

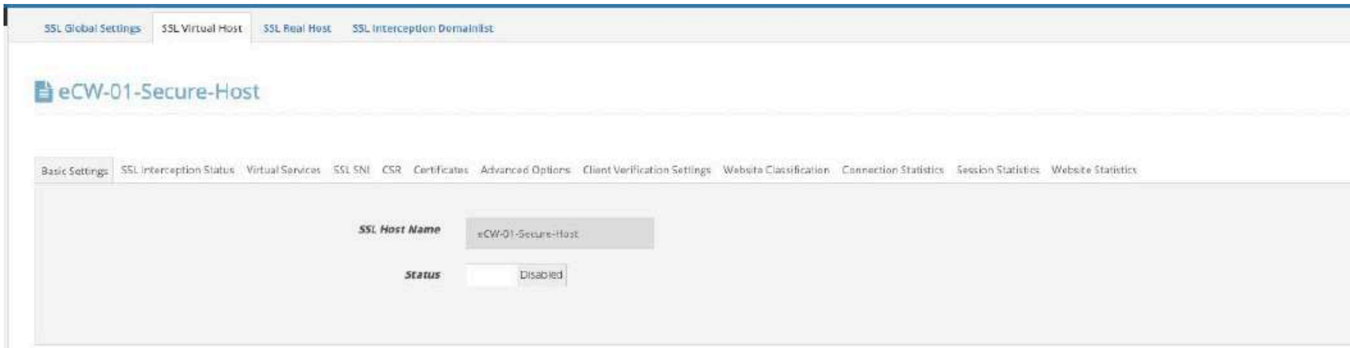
Lastly, you need to enable Status for your virtual host. Click “SSL Virtual Host” in the top tabs:



SSL Virtual Host

SSL Host Name	Status
eCW-01-Secure-Host	●

Double click the SSL Host Name for which SSL services need to be enabled:

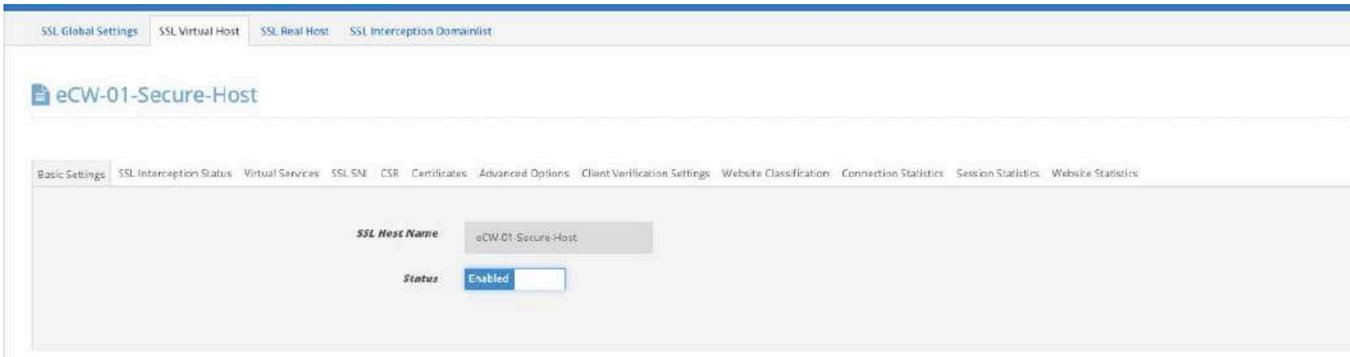


eCW-01-Secure-Host

SSL Host Name: eCW-01-Secure-Host

Status: Disabled

Lastly, click the “Disabled” slider to the “Enabled” status, click “Save Changes” and then save the configuration.



SSL Global Settings | SSL Virtual Host | SSL Real Host | SSL Interception Domainlist

eCW-01-Secure-Host

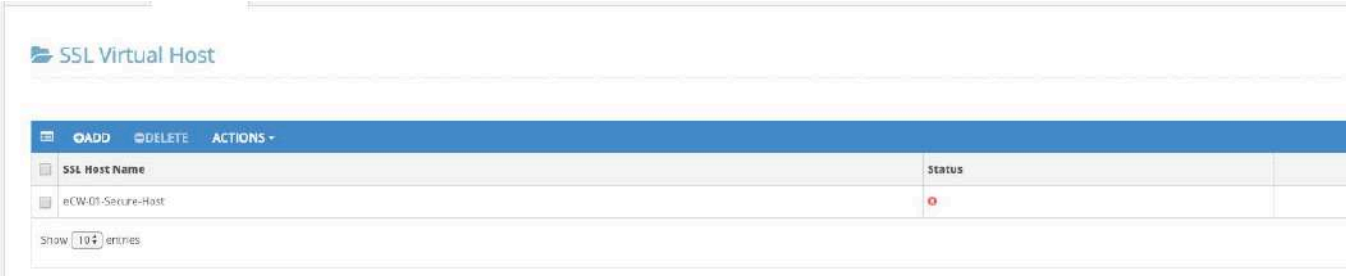
Basic Settings | SSL Interception Status | Virtual Services | SSL SNI | CSR | Certificates | Advanced Options | Client Verification Settings | Website Classification | Connection Statistics | Session Statistics | Website Statistics

SSL Host Name: eCW-01-Secure-Host

Status: Enabled

3.3.4 Import an Existing Certificate

Choose “SSL Settings” from the side menu, then choose the “SSL Virtual Host tab” at the top of the page. Then choose the SSL Virtual Host for which you want to import a certificate:

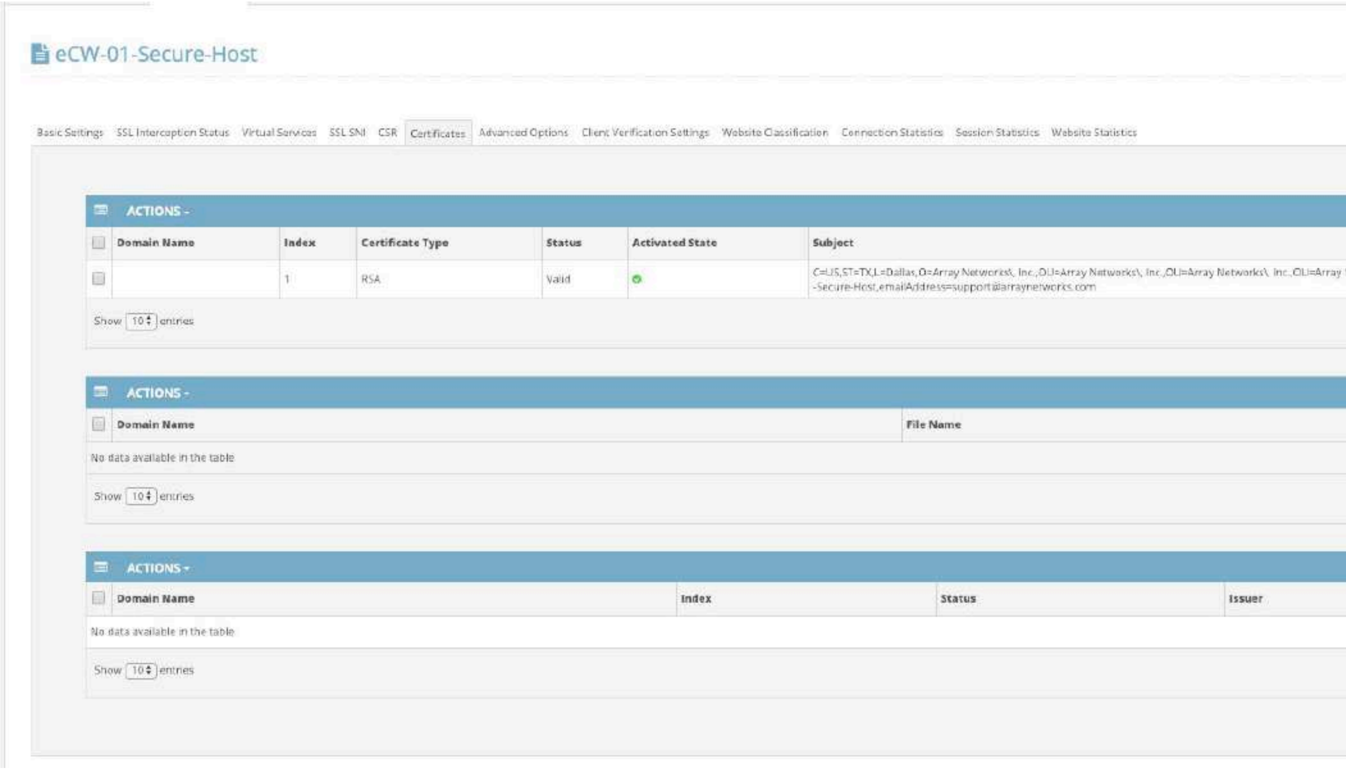


SSL Virtual Host

☐	SSL Host Name	Status
☐	eCW-01-Secure-Host	●

Show 10 entries

Choose the “Certificates” tab:



eCW-01-Secure-Host

Basic Settings | SSL Interception Status | Virtual Services | SSL SNI | CSR | Certificates | Advanced Options | Client Verification Settings | Website Classification | Connection Statistics | Session Statistics | Website Statistics

☐	Domain Name	Index	Certificate Type	Status	Activated State	Subject
☐		1	RSA	Valid	●	C=US,ST=TX,L=Dallas,O=Array Networks\, Inc.,OU=Array Networks\, Inc.,OU=Array Networks\, Inc.,OU=Array -Secure-Host,emailAddress=support@arraynetworks.com

Show 10 entries

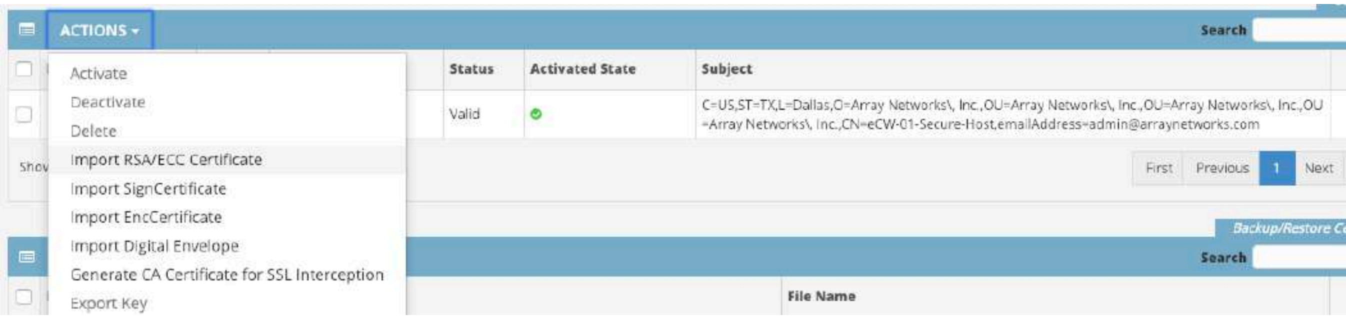
☐	Domain Name	File Name
No data available in the table		

Show 10 entries

☐	Domain Name	Index	Status	Issuer
No data available in the table				

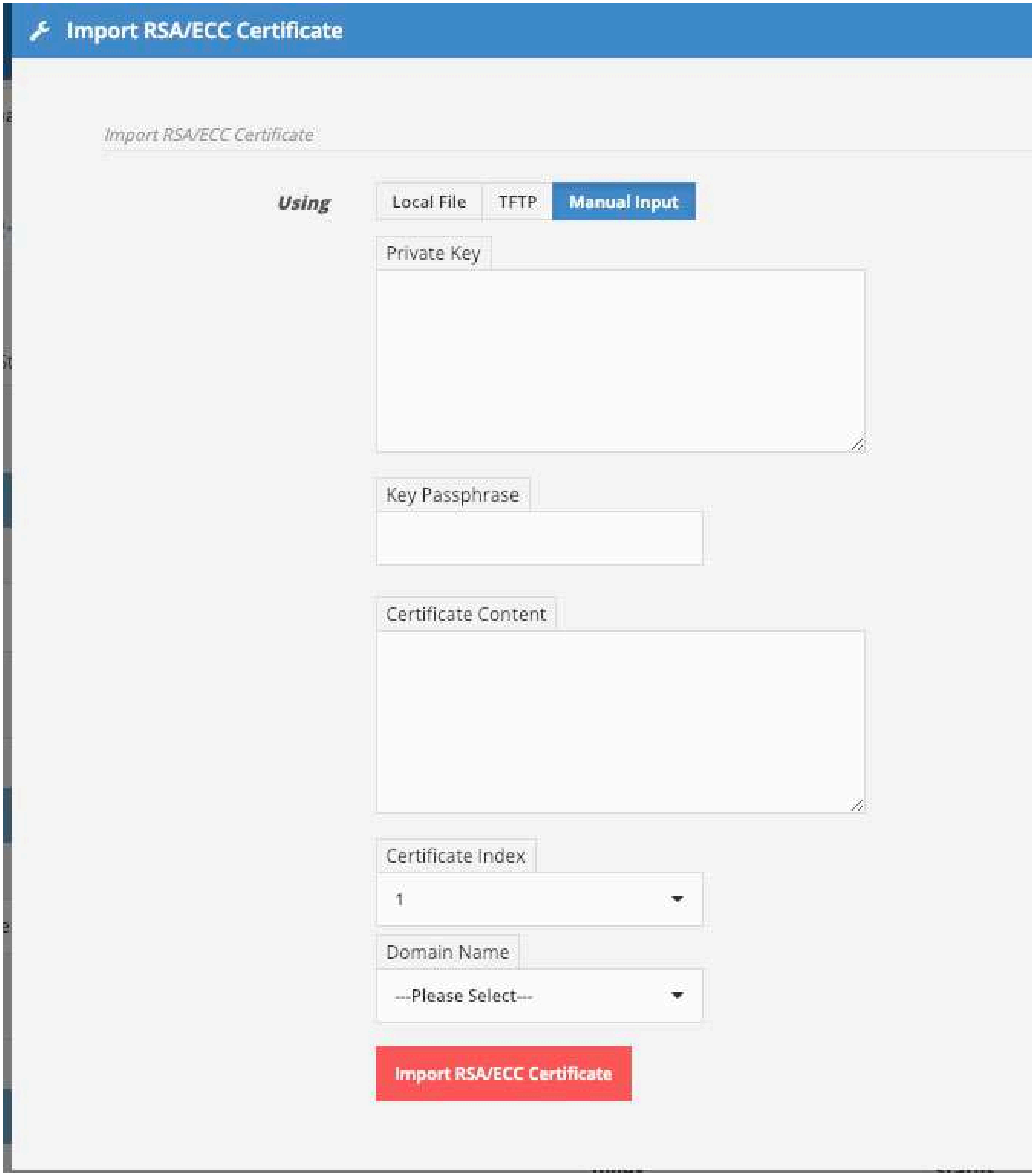
Show 10 entries

In the first section, choose the “Actions” dropdown, and then choose “Import RSA/ECC Certificate”:



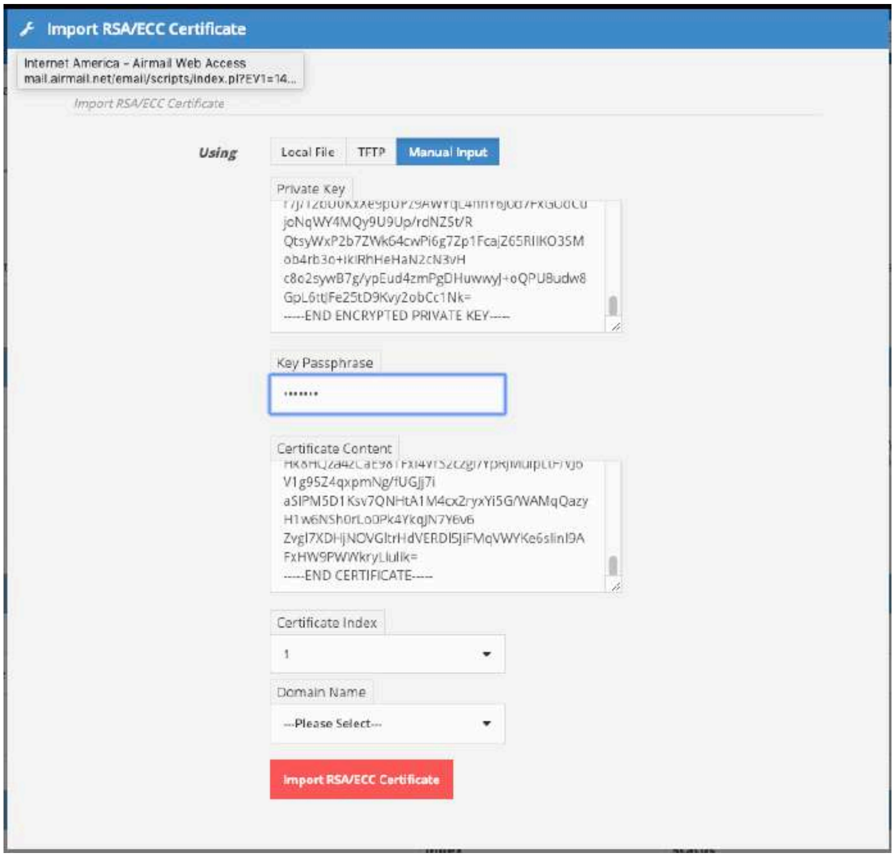
Status	Activated State	Subject
Valid	✓	C=US,ST=TX,L=Dallas,O=Array Networks\, Inc.,OU=Array Networks\, Inc.,OU=Array Networks\, Inc.,OU=Array Networks\, Inc.,CN=eCW-01-Secure-Host,emailAddress=admin@arraynetworks.com

Choose “Manual Input”



- Enter the private key for your existing SSL / TLS certificate
- Enter the passphrase
- Enter the certificate information
- Leave the Certificate index as-is

- Ignore the Domain Name.



Import RSA/ECC Certificate
Internet America - Airmail Web Access
mail.airmail.net/email/scripts/index.pl?EV1=14...
Import RSA/ECC Certificate
Local File
TFTP
Import RSA/ECC Certificate

Using: Manual Input

Private Key

```
joNqWY4MQy9U9Up/rdNZ5t/R
QtsyWxP2b7ZWk64cwPi6g7Zp1FcajZ65RIIKO35M
ob4rb3o+ikIRhHeHaN2cN3vH
c8o2sywB7g/ypEud4zmPgDHuwwyJ+oQPU8udw8
GpL6ttJFe25tD9Kvy2obCc1Nk=
-----END ENCRYPTED PRIVATE KEY-----
```

Key Passphrase: •••••••

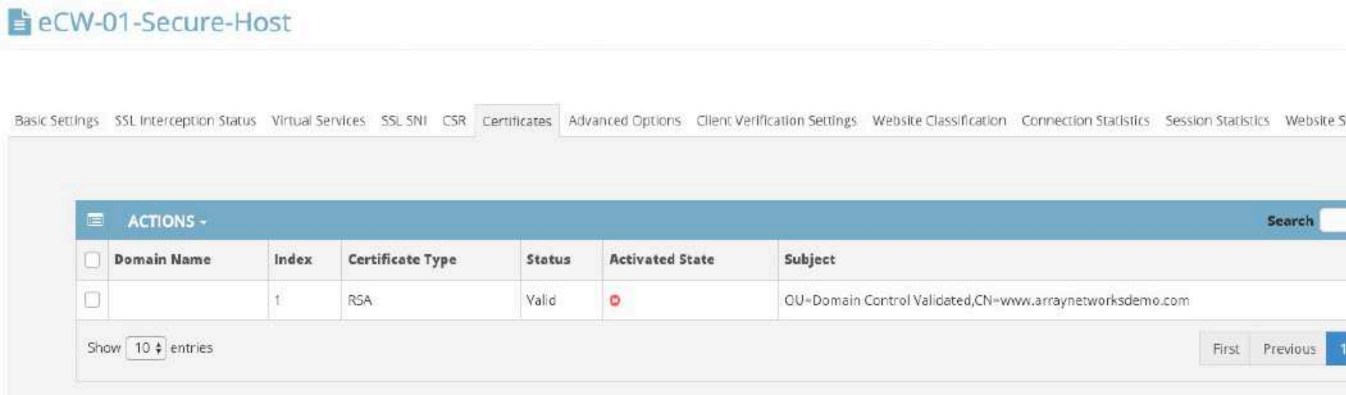
Certificate Content

```
V1g95Z4qxpmNg/fUGJj7i
aSIPM5D1Ksv7QNHtA1M4cx2ryxYi5G/WAMqQazy
H1w6NSh0rLo0Pk4YkqJN7Y6v6
ZvgI7XDHjNOVGltrHdVERDI5JiFMqVWYKe6sIinI9A
FxHW9PWWkryLIulIk=
-----END CERTIFICATE-----
```

Certificate Index: 1

Domain Name: ---Please Select---

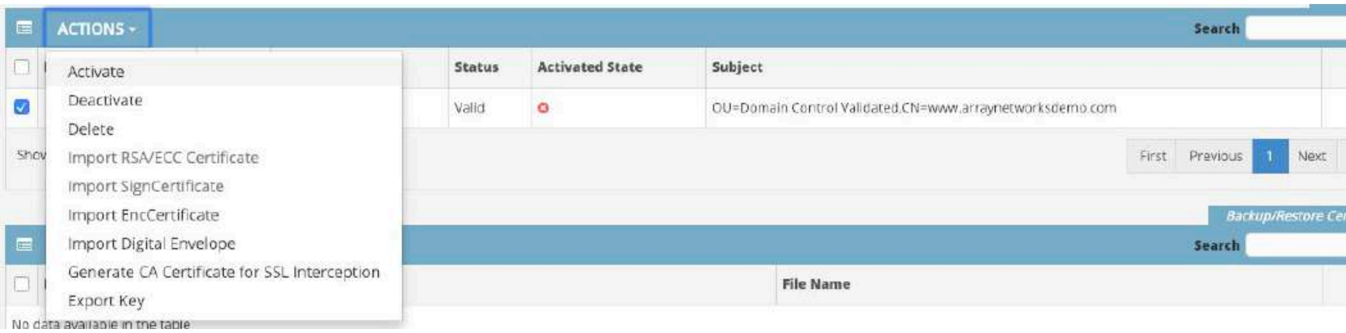
Click “Import RSA/ECC Certificate”



□	Domain Name	Index	Certificate Type	Status	Activated State	Subject
□		1	RSA	Valid	●	OU=Domain Control Validated,CN=www.arraynetworksdemo.com

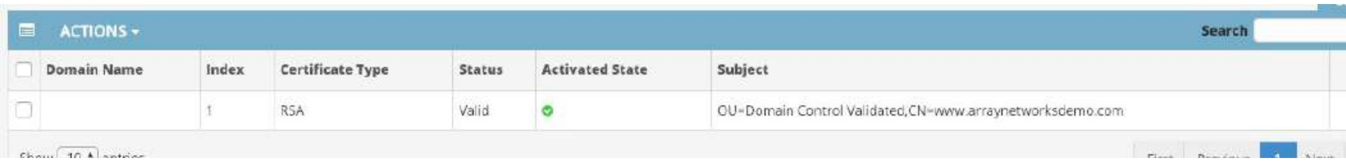
Show 10 entries

Lastly, choose the certificate you just added, and choose “Activate” from the Actions dropdown:



☐	Status	Activated State	Subject
☑	Valid	●	OU=Domain Control Validated,CN=www.arraynetworksdemo.com

The resulting green icon indicates success:



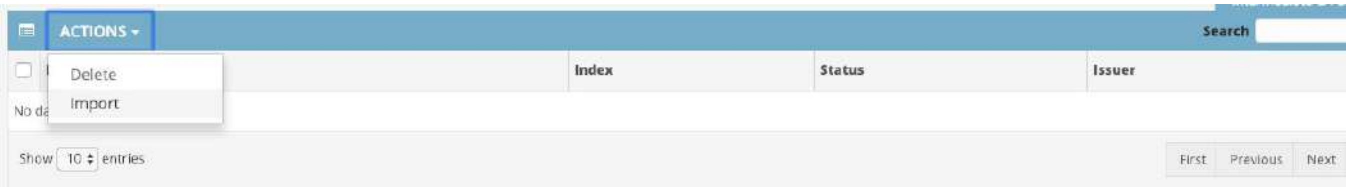
☐	Domain Name	Index	Certificate Type	Status	Activated State	Subject
☐		1	RSA	Valid	●	OU=Domain Control Validated,CN=www.arraynetworksdemo.com

Save the configuration.

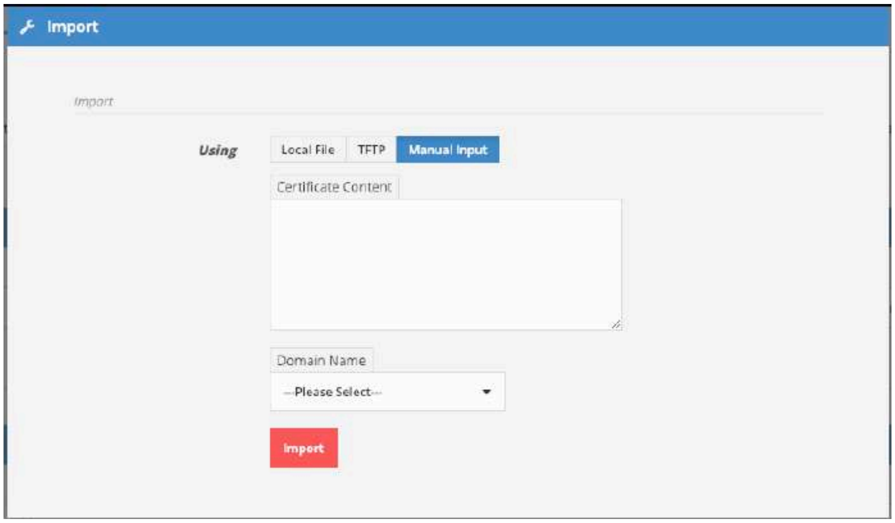
3.3.5 Import an Intermediate Certificate

If your certificate registry requires the use of an intermediate certificate, what follows are instructions on how to add an intermediate certificate. If you do not need an intermediate certificate, you may skip these instructions.

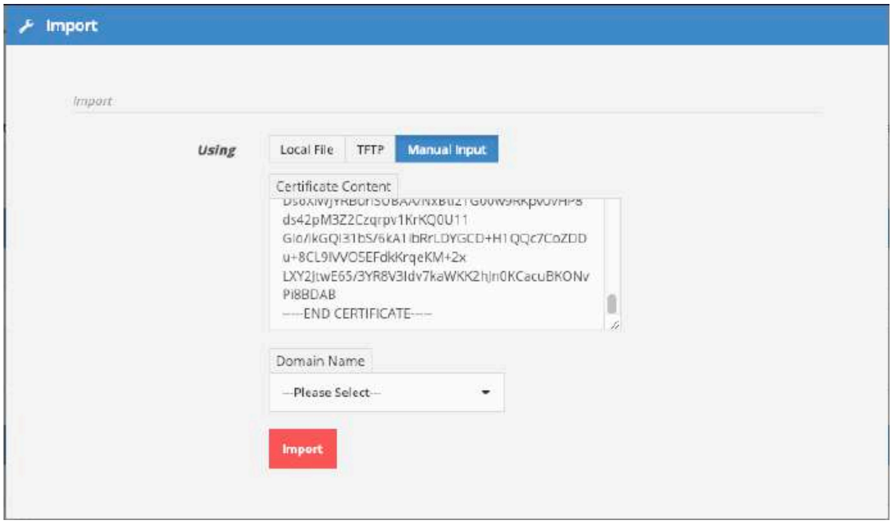
Choose "Import" from the "Intermediate CA Certificate" Actions dropdown menu:



Choose Manual Input in the resulting page:



Enter the intermediate certificate provided by your Certificate Authority:

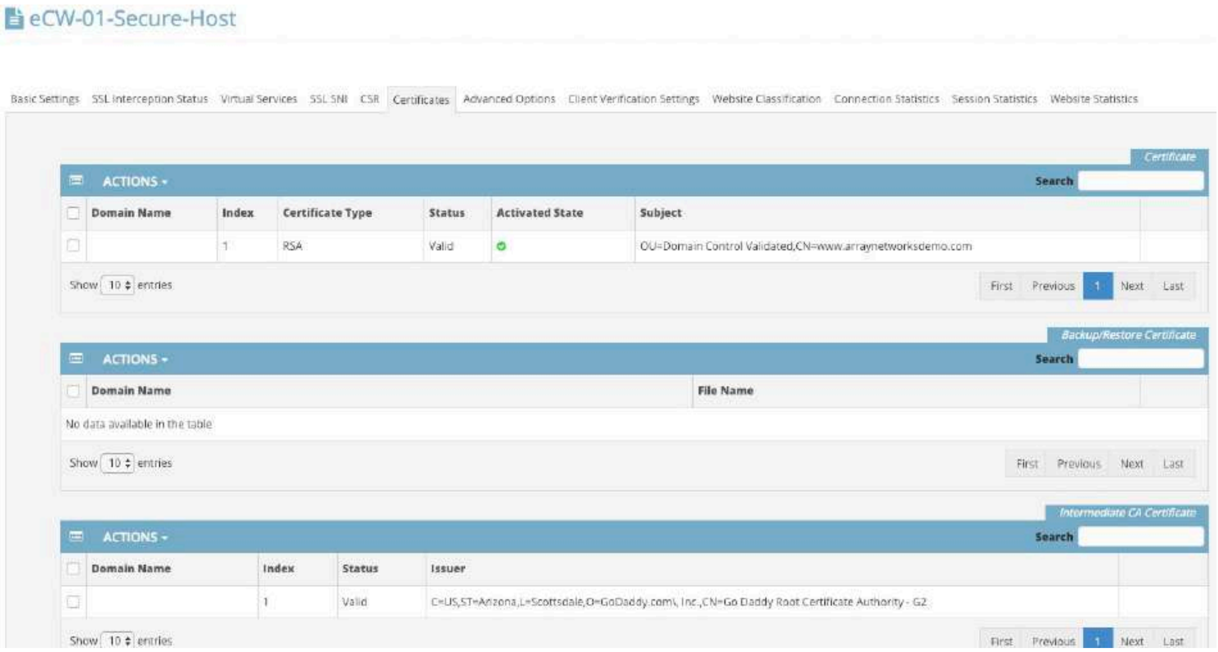


Certificate Content

```
ds42pM3Z2Czqrpv1KrKQ0U11
Glo/lkGQI31b5/6kA1IbRrLDYGCD+H1QQc7CoZDD
u+8CL9IVVO5EFdkKrqeKM+2x
LXY2JtwE65/3YR8V3Idv7kaWKK2hJn0KCacuBKONv
Pi8BDAB
-----END CERTIFICATE-----
```

Domain Name: --Please Select--

Click Import.



□	Domain Name	Index	Certificate Type	Status	Activated State	Subject
□		1	RSA	Valid	●	OU=Domain Control Validated,CN=www.arraynetworksdemo.com

□	Domain Name	File Name
No data available in the table		

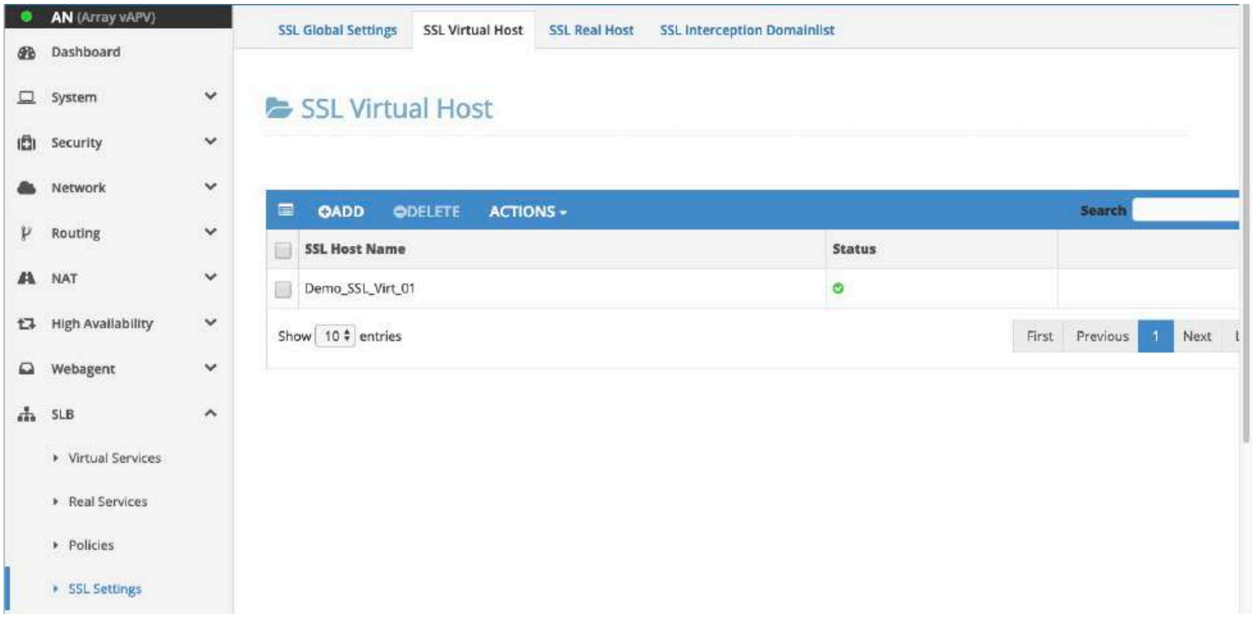
□	Domain Name	Index	Status	Issuer
□		1	Valid	C=US,ST=Arizona,L=Scottsdale,O=GoDaddy.com\, Inc.,CN=Go Daddy Root Certificate Authority - G2

3.3.5 Create an SSL Real Host (Optional)

In some cases you may be required to continue HTTPS protections from the client on the Internet all the way to the system serving traffic to said client. In these cases, you will need to configure your Array APV to send encrypted traffic to the real servers, and you will need to insure the real servers can encrypt/decrypt as necessary. For the purposes of this guide, we are only going to focus on how to configure the load balancer.

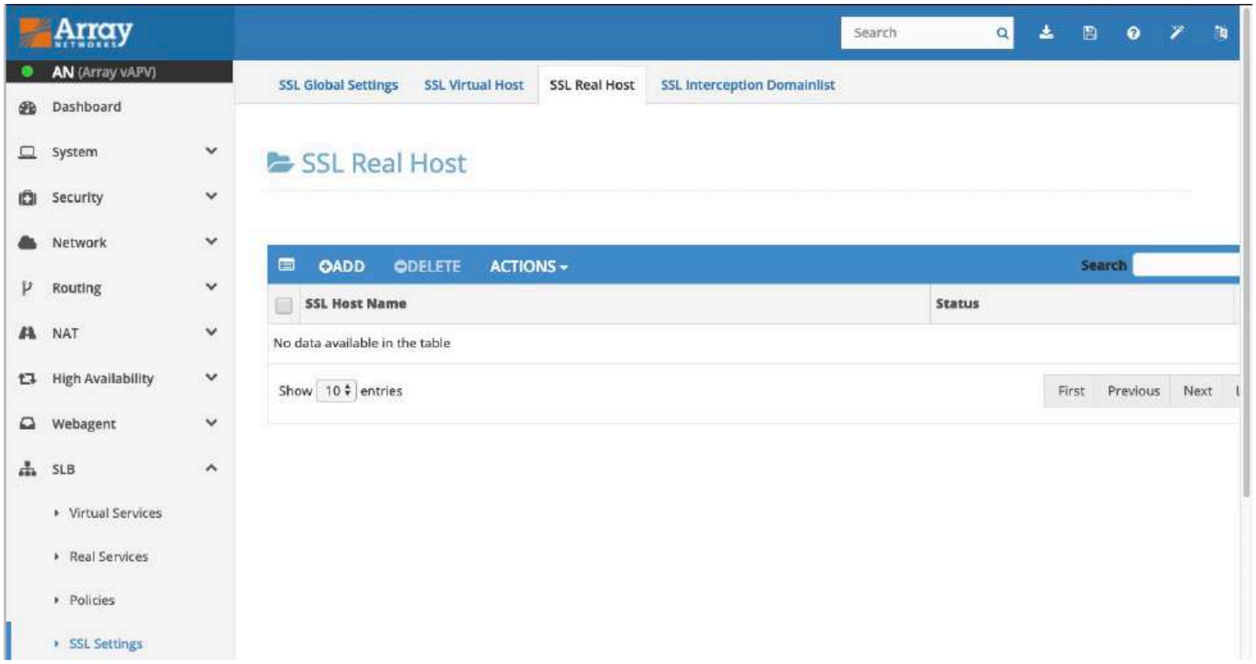
If you do not have an existing virtual host, please return to 3.3.2 and create the SSL Virtual Host.

Go to SLB (side menu) → SSL Settings (side, submenu) → SSL Virtual Host (tab toward the top of the page). Choose the existing SSL Virtual Host.



SSL Host Name	Status
Demo_SSL_Virt_01	●

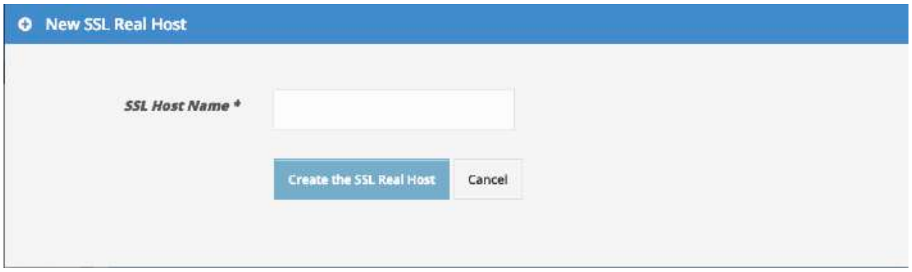
From the resulting page, choose “SSL Real Host” from the tabs at the top of the page:



SSL Host Name	Status
No data available in the table	

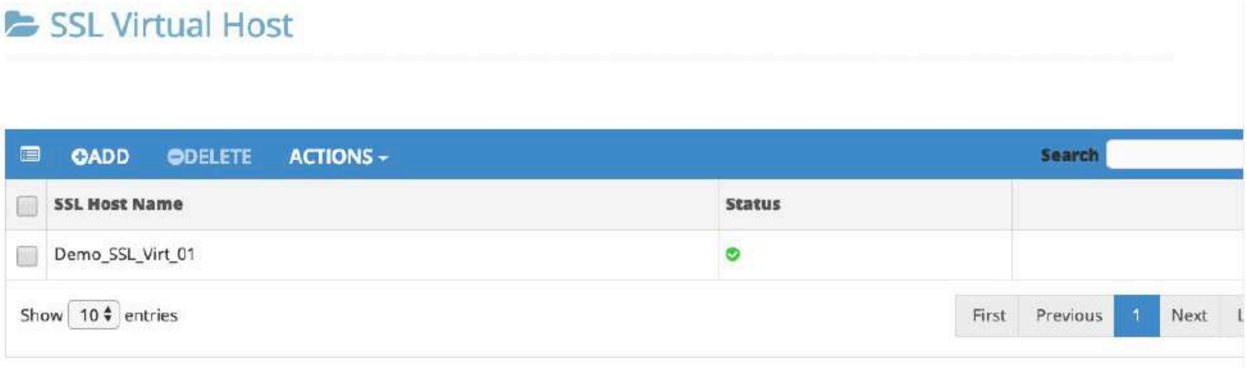
Choose Add from the preceding drop down

Enter a name for the SSL real host. Note that this is an arbitrary name – you may use anything you wish. Only use numbers, letters, underscore and hyphen in the blank. Once complete, click “Create the SSL Real Host” button



SSL Host Name *

Doubleclick the resulting service:



☐	SSL Host Name	Status
☐	Demo_SSL_Virt_01	✓

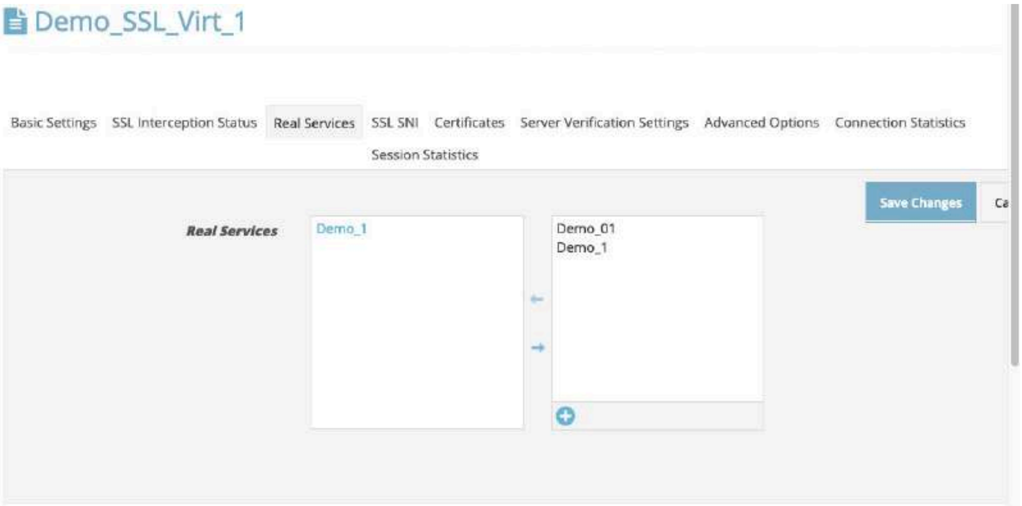
Show 10 entries

Choose the “Real Services” tab, from the tabs below the main tabs

Click the picker box and choose the real server

Click “Save Changes”.

Note: The real server you choose must be an HTTPS service.



Real Services: Demo_1

Demo_01
Demo_1

Complete this for each real server behind the load balancer which requires backend security (HTTPS).

About Array Networks

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

Corporate Headquarters
info@arraynetworks.com
408-240-8700
1 866 MY-ARRAY
www.arraynetworks.com

EMEA
rschmit@arraynetworks.com
+32 2 6336382

China
support@arraynetworks.com.cn
+010-84446688

France and North Africa
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

Apr-2019 rev. a