Deployment Guide
Sep-2017 rev. a

vAWF Deployment Guide
for AVX Series Network Functions Platform

Table of Contents

Table of Contents **1**

1. About vAWF on AVX **2**

2. Deployment Requirements and Limitations **3**

2.1. Requirements 3

2.2. Limitations 3

3. Deploying the vAWF Instance on AVX **4**

3.1. Importing the vAWF Image to AVX 4

3.2. Creating a vAWF Instance on AVX 4

3.3. Adding Virtual Traffic Ports to the vAWF Instance 4

3.3.1. Assigning an SR-IOV Virtual Port to the vAWF Instance 5

3.3.2. Assigning a Virtio Virtual Port to the vAWF Instance 5

3.4. Starting the vAWF Instance 6

4. Completing the Initial Configuration for the vAWF Instance **7**

5. Loading a Valid License to the vAWF Instance **8**

6. Deployment Examples **9**

6.1. Supported Deployment Modes 9

6.1.1. vAWF in Proxy Mode 9

6.1.2. vAWF in Router Mode 10

6.1.3. vAWF in Bridge Mode 11

6.1.4. vAWF in Sniffer Mode 11

6.2. Configuration Examples 12

6.2.1. vAWF Configuration in One-arm Proxy Mode 12

6.2.2. vAWF Configuration in Inline Proxy Mode 14

6.2.3. vAWF Configuration in Router Mode 15

6.2.4. vAWF Configuration in Bridge Mode 16

6.2.5. vAWF Configuration in Sniffer Mode 17

7. Deploying vAWF Instances with High Availability **19**

1. About vAWF on AVX

Array Networks AVX Series network functions platforms offer a multi-tenant virtualized platform that supports deployment of multiple Virtual Appliance (VA) instances or Virtual Network Functions (VNFs) with guaranteed performance, which enables organizations to consolidate their data centers without sacrificing performance, stability and flexibility.

vAWF on AVX is a virtual version of the AWF product that provides the same feature set as the hardware AWF product. Array's AWF Series Web application firewalls extend beyond traditional firewalls and Intrusion Detection Systems (IDSs) to provide comprehensive protection for business-critical Web applications. The AWF Series not only detects the complex Web application attacks of today, but also blocks the attack traffic in real time without affecting the normal flow of business data traffic. In addition, the AWF Series provides extremely fine-grained attack detection and analysis capabilities while protecting against the most common Web application threats including SQL injection attacks, Website defacement, Website malicious code, and disclosure of sensitive information.

vAWF on AVX has the following advantages:

- AVX provides guaranteed performance for vAWF, in contrast to other common hypervisors.
- AVX provides high scalability for vAWF and allows a pay-as-you-grow license model.
- Multiple vAWFs can work with high availability on one AVX.
- vAWF and Array and other 3rd party networking and security products can be deployed as a service chain on one AVX.

Note: For the examples shown in the deployment guide, the AVX Series should run ArrayOS AVX 2.4.0.3 or later and vAWF should run ArrayOS 6.1.2.27178 version or later.

2. Deployment Requirements and Limitations

2.1. Requirements

You can deploy multiple instances of vAWF on the Array AVX platform. A vAWF instance is assigned a specific amount of AVX system resources, like the number of vCPUs, memory, and disk space. The amount of system resources assigned is determined by the AVX instance size.

Table 2-1 System Resource Requirements for vAWF on AVX

System Resource	Instance Size			
	Entry	**Small**	**Medium**	**Large**
Number of vCPUs	1	2	4	8
Memory	2GB	4GB	8GB	16GB
Disk Space	40GB	40GB	40GB	40GB

When you want to run a specific size of vAWF instance on the AVX, please ensure that the amount of free system resources bound to the instance size is adequate.

2.2. Limitations

The AVX does not provide a hardware bypass card. Therefore, the vAWF on AVX cannot support the hardware bypass function.

3. Deploying the vAWF Instance on AVX

Before deploying the vAWF virtual appliance on the AVX appliance, please contact Array Networks Customer Support to obtain the vAWF image package (such as vAWF_6.1.2.xxxxx_AVX.tgz), which contains a vawf.qocw2 disk file and a metadata.ini file.

Then, place the vAWF image package onto an HTTP or FTP server that is accessible by the AVX appliance.

For example: http://10.3.0.54/vAWF_6.1.2.xxxxx_AVX.tgz

3.1. Importing the vAWF Image to AVX

To import the vAWF image to AVX, execute the following command on the AVX:

va image <*image_name*> <*url*> *[format] [metadata_url]*

image_name: the name of the image.

url: the URL of the image.

format: the format of the image: qcow2, raw, vmdk or tgz.

metadata_url: the URL of the image's metadata file. If the image format is tgz and the tgz file contains a metadata file, this parameter does not need to be specified.

```
AN(config)#va image vAWF_6.1.2 http://10.3.0.54/vAWF_6.1.2.xxxxx_AVX.tgz tgz
```

3.2. Creating a vAWF Instance on AVX

After the vAWF image has been imported successfully, you can create the vAWF instance using the following command:

va pureinstance <*va_name*> <*va_size*> *[domain_id] [image_name]*

va_name: name of the VA instance.

va_size: size of the VA instance. The vAWF instance supports any instance size on the AVX.

domain_id: ID of the NUMA domain from which system resources are assigned.

image_name: name of the image.

```
AN(config)#va pureinstance vAWF medium 1 vAWF_6.1.2
```

3.3. Adding Virtual Traffic Ports to the vAWF Instance

The AVX assigns a virtual management port that is connected with the AVX's physical management port using a built-in virtual switch when the vAWF instance is created. It is recommended that the virtual management port be used for management purposes only.

To process data traffic, you need to assign virtual traffic ports to the vAWF instance according to the requirements of different deployment modes, as shown in the table below.

The AVX supports two types of virtual traffic port:

- SR-IOV virtual ports: SR-IOV Virtual Function (VF) of a 10G traffic port.
- Virtio virtual ports: virtio-type ports assigned by the virtual switch to the attached VA instance.

Deployment Mode	Requirements
Reverse proxy mode	Assign one or more SR-IOV virtual ports
Transparent proxy mode	Assign one or multiple pairs of virtio virtual ports
Bridge mode	Assign one or multiple pairs of virtio virtual ports
Sniffer mode	Assign one virtio virtual port

3.3.1. Assigning an SR-IOV Virtual Port to the vAWF Instance

With SR-IOV, one physical traffic port on the AVX can be virtualized as eight SR-IOV virtual ports.

To assign an SR-IOV virtual port, execute the following command:

va port <*va_name*> <*port_name*> <*vf_index*>

va_name: name of the VA instance.

port_name: name of the physical traffic port.

vf_index: Index of the SR-IOV VF to be assigned. The indexes of eight SR-IOV virtual ports under one physical traffic port are 1 to 8 respectively.

```
AN(config)#va port vAWF port1 1
```

3.3.2. Assigning a Virtio Virtual Port to the vAWF Instance

When you attach the vAWF instance to a virtual switch, the vAWF instance will be assigned a virtio virtual port. For external communication of the vAWF instance using a virtio virtual port, you also need to add a physical traffic port to the virtual switch. In this way, the virtio virtual port can send traffic to the network via the physical traffic port.

To create a virtual switch, execute the following command:

switch name <*virtual_switch_name*>

virtual_switch_name: name of the virtual switch

```
AN(config)#switch name switch1
```

To attach the vAWF instance to the virtual switch, execute the following command:

switch va <*virtual_switch_name*> <*va_name*> <*vport_name*> *[vlan_tag] [queue_number]*

virtual_switch_name: name of the virtual switch

va_name: name of the VA instance

vport_name: name of the virtual switch

vlan_tag: tag of the VLAN to which the virtio virtual port belongs.

queue_number: number of Rx/Tx queue pairs enabled for the virtio virtual port.

```
AN(config)#switch va switch1 vAWF vport1 0 4
```

Note: The AVX provides multi-queue support to maximize the network performance of the virtio virtual port as the number of vCPUs increases. Please enable a specified number of Rx/Tx queue pairs in the “queue_number” parameter according to the number of vCPUs assigned to the VA instance. For example, enable four queue pairs for a medium-size VA instance. Refer to Table 2-1 System Resource Requirements for vAWF on AVX to determine how many vCPUs are provided per instance size.

To add a traffic port to the virtual switch, execute the following command:

switch interface <*virtual_switch_name*> <*interface_name*>

virtual_switch_name: name of the virtual switch.

interface_name: name of the physical traffic port.

```
AN(config)#switch interface switch1 port1
```

Note: For the vAWF instance to support the bridge deployment mode, you need to create two virtual switches, attach the vAWF instance to both of them, and add two traffic ports to the two virtual switches respectively.

3.4. Starting the vAWF Instance

After the vAWF instance is created, you can start it using the “**va start** <*va_name*>” command.

```
AN(config)#va start vAWF
```

4. Completing the Initial Configuration for the vAWF Instance

When the vAWF instance is up, you can establish a console connection to the vAWF instance using the "**va console vAWF**" command.

1. Enter the default user name "admin" and the password "admin" to log into the vAWF instance.

2. Add a management IP address (10.3.0.75, for example) to the MngtBridge interface using the following command:

bridge -A/--add -v/--vname<Bridgename> -f/--ip<ipv4> -m/--mask <mask> -n/--mngt <y/n>

```
WAF>bridge -A -v MngtBridge -f 10.3.0.75 -m 255.255.255.0 -n y
```

Note: The management IP of the vAWF instance should be on the same subnet as that of the AVX.

3. Add the static route to the MngtBridge interface for the management subnet (such as 10.3.0.0/24) using the following command:

route -A/--add -i/--ip {ip} -m/--mask {mask} <[-g/--gateway {gateway}] [-n/--interface {interface}]> [-t {metric}]

```
WAF>route -A -i 10.3.0.0 -m 255.255.0.0 -g 10.3.0.1
```

4. Configure remote management rules to allow remote SSH and WebUI access using the following command:

remote -A/--add -t/--type<remote type> -i/--ip<ip address> -m/--mask<network mask>

```
WAF>remote -A -t web -i 10.3.0.0 -m 255.255.0.0
WAF>remote -A -t ssh -i 10.3.0.0 -m 255.255.0.0
WAF>remote -A -t ping -i 10.3.0.0 -m 255.255.0.0
```

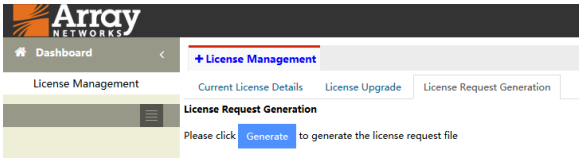
5. Loading a Valid License to the vAWF Instance

After the vAWF instance is created, it will be preinstalled with a trial license. The trial license will have a validity period of 30 days. With the trial license, the vAWF instance can provide a maximum of 200 Mbps throughput.

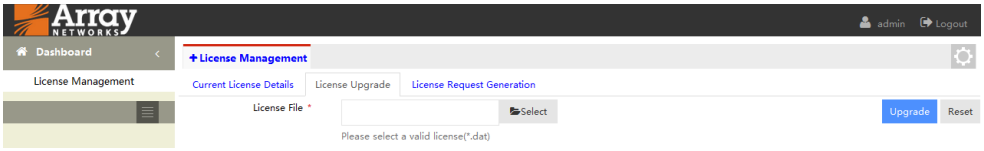
To make full use of functionality and performance of the vAWF instance, you need to purchase a valid formal license.

To purchase a valid license and load it to the vAWF instance, follow these steps:

1. Access the VA instance's WebUI (for example: https://10.3.0.75) after the initial configuration is completed.
2. Select **License Management > License Request Generation**, and click the **Generate** button to generate and save the license request file locally.



3. Send the license request file to Array Networks Customer Support.
4. After receiving the license file, select the **License Management > License Upgrade** tab, click the **Select** icon to select the license file and click the **Upgrade** button.



6. Deployment Examples

6.1. Supported Deployment Modes

The vAWF instance on AVX can support the same deployment modes as its hardware counterpart:

- Proxy mode
- Router mode
- Bridge mode
- Sniffer mode

For the configuration examples for these deployment modes, please refer to section 6.2 Configuration Examples.

6.1.1. vAWF in Proxy Mode

vAWF on AVX can support one-arm proxy and inline proxy modes. For the one-arm proxy mode, the vAWF instance only requires one SR-IOV virtual port. For the inline proxy mode, the vAWF instance needs two SR-IOV virtual ports to connect two network subnets.

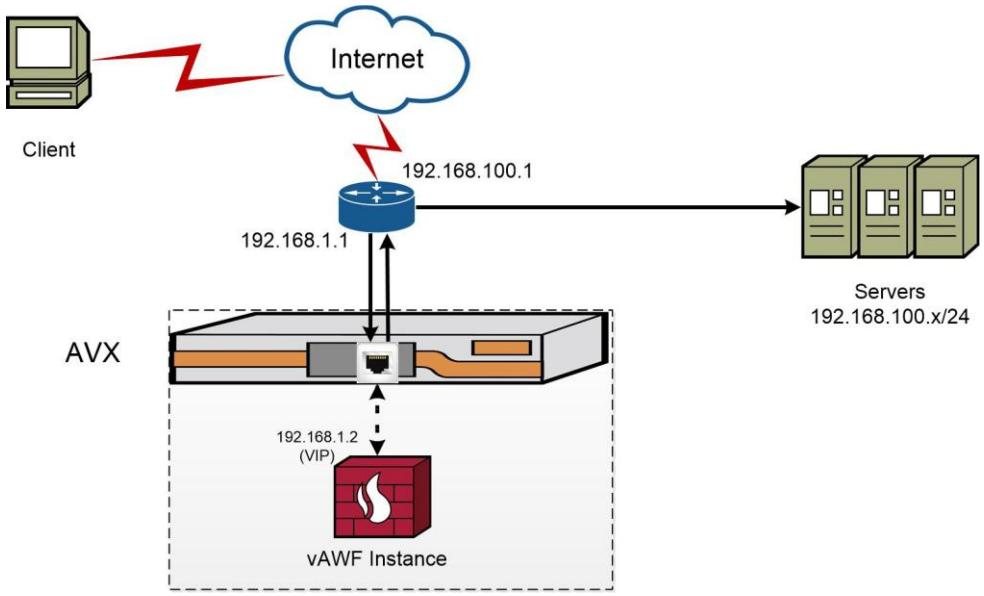


Figure 3–1 vAWF in One-arm Proxy Mode

In one-arm proxy deployment mode, the vAWF instance works as the proxy server for the backend servers.

The data flow in one-arm proxy deployment mode is as follows:

1. The client sends requests to the gateway (router) of the network.
2. The gateway forwards the requests to the VIP (192.168.1.2) of the vAWF instance based on NAT configurations.
3. After the vAWF instance processes the requests, it sends the requests to the gateway.

4. The gateway (router) forwards the requests processed by the vAWF instance to the backend server on another subnet.

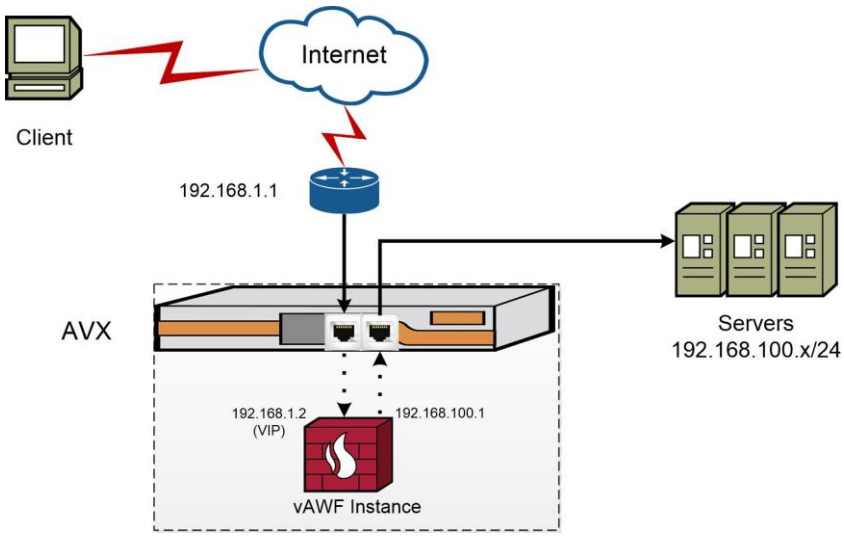


Figure 3–2 vAWF in Inline Proxy Mode

The data flow in inline proxy deployment mode is as follows:

1. The client sends requests to the gateway of the network.
2. The gateway forwards the requests to the VIP (192.168.1.2) of the vAWF instance based on NAT configurations.
3. After the vAWF instance processes the requests, it sends the requests to the backend servers through the interface (192.168.100.1).

6.1.2. vAWF in Router Mode

vAWF on AVX can support router mode. For router mode, the vAWF instance needs to use two or more SR-IOV virtual ports to connect different network subnets and function as the gateway for these network subnets.

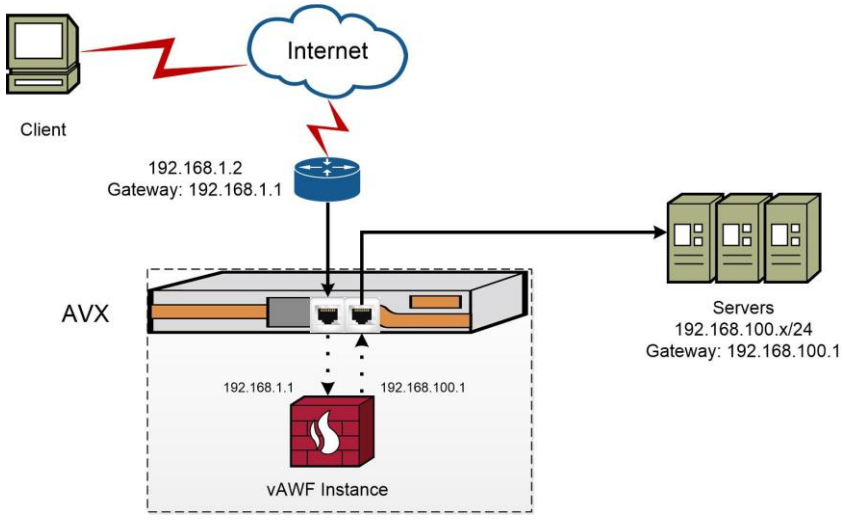


Figure 3–3 vAWF in Router Mode

The data flow in router deployment mode is as follows:

1. The client sends requests to the router.
2. The router forwards the requests destined for backend servers through the vAWF instance based on the routing table.
3. After the vAWF instance inspects the requests, it transparently forwards the requests to the backend servers through the interface (192.168.100.1) based on the routing table.

6.1.3. vAWF in Bridge Mode

vAWF on AVX can support bridge mode, which allows traffic to transparently pass through the vAWF instance. For bridge mode, the vAWF instance needs to use two virtio virtual ports (connected to two virtual switches) and the two ports should be added into a bridge interface within the vAWF instance.

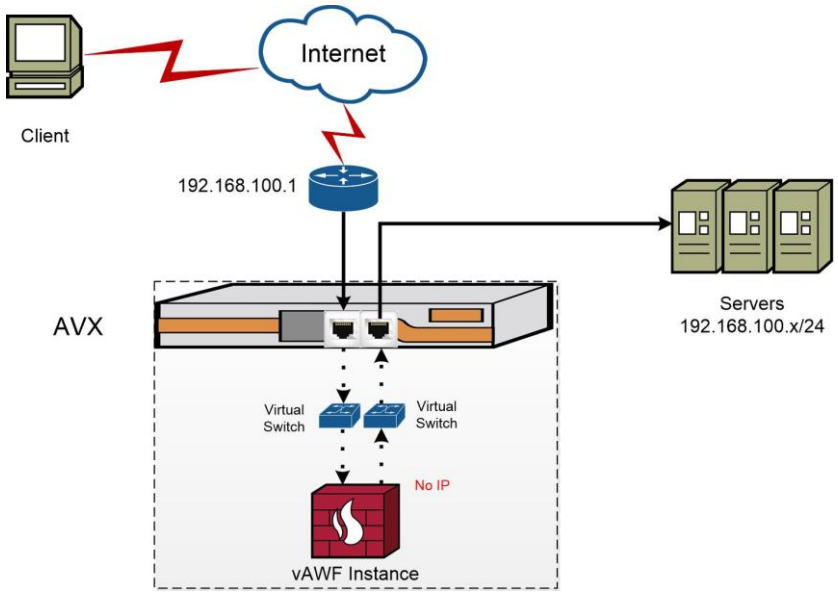


Figure 3–4 vAWF in Bridge Mode

The data flow in bridge deployment mode is as follows:

1. The client sends requests to the gateway of the network.
2. The gateway forwards the requests destined for backend servers to the first switch.
3. The first switch forwards the requests to the vAWF appliance transparently.
4. The vAWF instance inspects the requests and transparently forwards the requests to the backend servers through the second virtual switch.

6.1.4. vAWF in Sniffer Mode

vAWF on AVX can support sniffer mode when the data flow passes another VA instance on the AVX, such as a vAPV load balancing instance. For sniffer mode, the vAWF instance needs to use one virtio virtual port (connected to the virtual switch) and the virtio virtual port should be configured as the mirror port on the virtual switch to receive a copy of the traffic sent or received on the vAPV instance's interface connected to the same virtual switch.

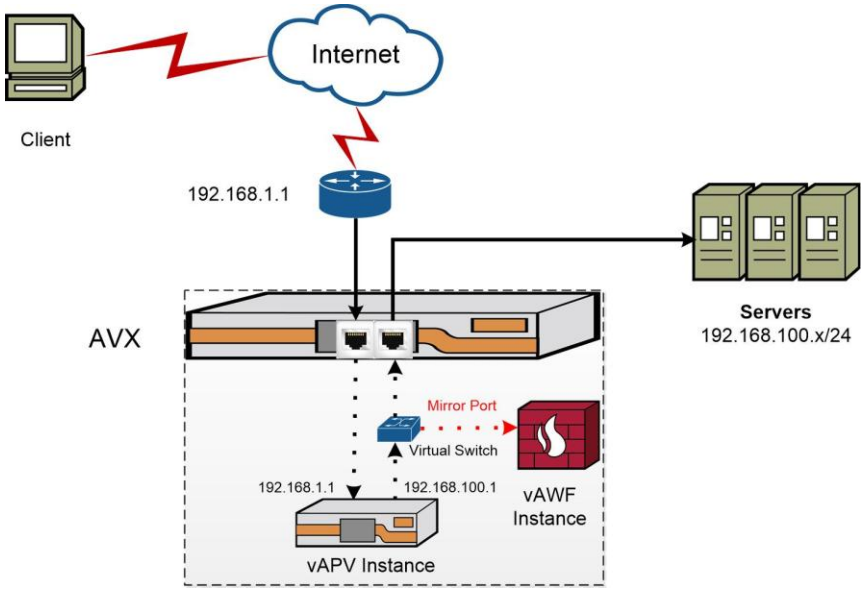


Figure 3–4 vAWF in Sniffer Mode

The data flow in sniffer deployment mode is as follows:

1. The client sends requests to the gateway of the network.
2. The gateway forwards the requests to the vAPV instance.
3. The vAPV instance transparently forwards the requests to the virtual switch.
4. The virtual switch forwards requests to the backend servers and sends a copy of request to the mirror port on the vAWF instance.

The responses to the requests will follow the reverse process, i.e. the vAWF instance will receive a copy of the responses sent to the vAPV instance by the virtual switch.

Note: To support sniffer mode, the vAWF instance should use another port to send RST packets to the client and servers on detection of attacks. You should ensure that the port can reach the client and backend servers. For example, you can assign an SR-IOV virtual port from the AVX traffic port that is connected to the backend servers.

6.2. Configuration Examples

This section provides vAWF configuration examples in different deployment modes.

6.2.1. vAWF Configuration in One-arm Proxy Mode

- **Prerequisites**

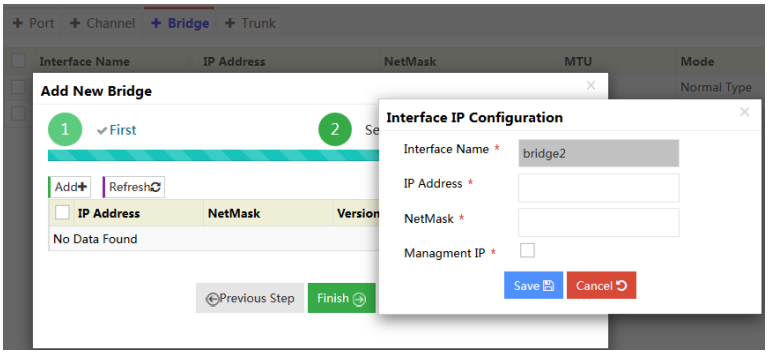
Before vAWF configuration, you need to assign an SR-IOV virtual port to the vAWF instance. Port1 of the vAWF instance is mapped to the SR-IOV virtual port of the traffic port port1.

On the AVX, Port1 is connected to the upstream gateway.

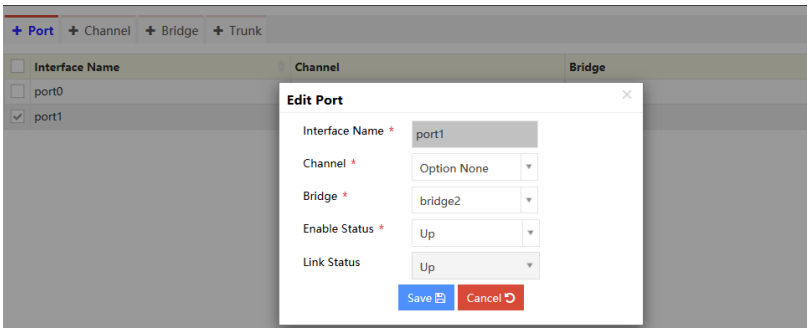
- **Configuration Steps**

1. Create a new bridge interface named bridge2 and add port1 to it.

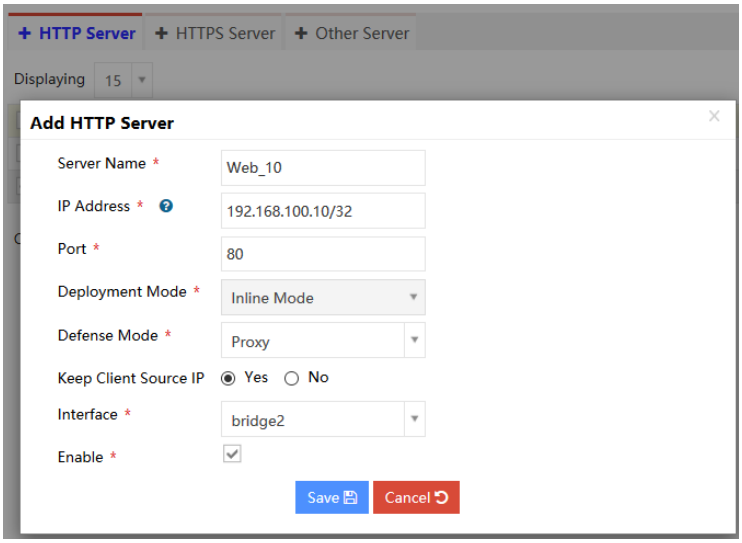
- Select **Network Management > Interface > Bridge**, and click the **Add** button. In the **Add New Bridge** window, specify the Bridge ID and other parameters and click the **Next Step** button.
- In the second step, click the **Add** button to add the virtual IP (for example, 192.168.1.2) to the bridge interface.



- Select **Network Management > Interface > Port**. Select the port1 interface entry and click the **Edit** button. In the **Edit Port** window, set the **Bridge** parameter to bridge2 and click the **Save** button to save the configuration.

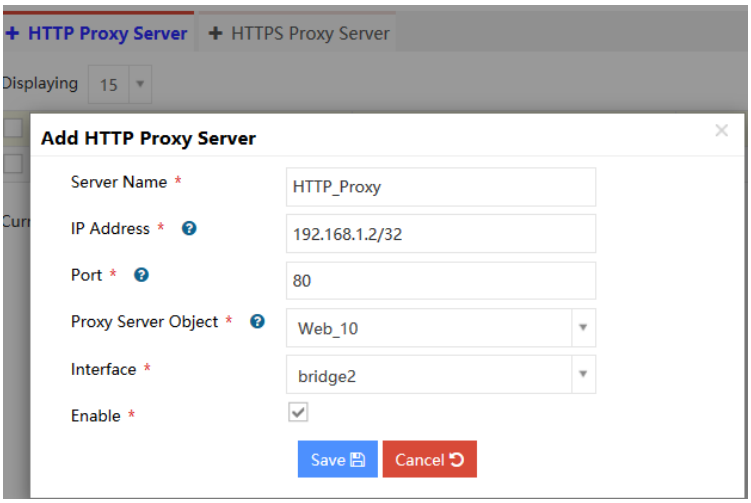


2. Define an HTTP Web server (for example, 192.168.100.10:80).
   - Select **Server Management > Normal Server > HTTP Server** and click the **Add** button. In the prompted window, specify the parameters, and click the **Save** button to save the configuration.

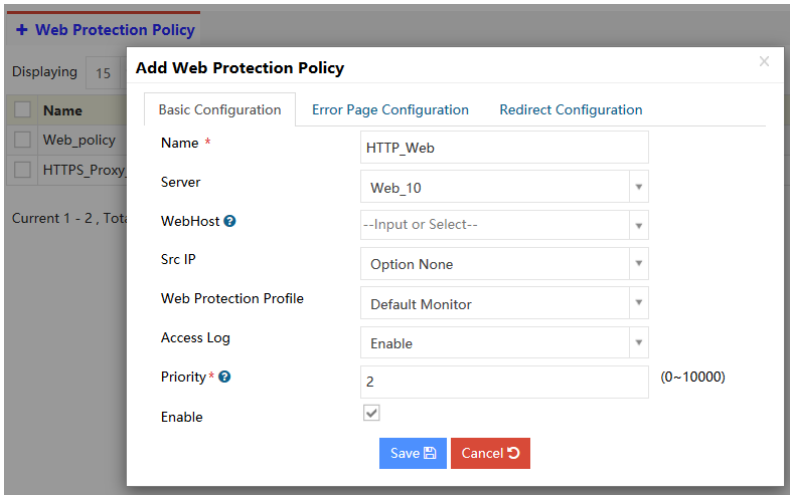


Note: In one-arm proxy mode, you still need to set the **Deployment Mode** parameter to Inline Mode.

3. Define an HTTP proxy server and associate it with the HTTP Web server.
   - **Select Server Management > Proxy Server > HTTP Proxy Server**, and click the **Add** button. In the prompted window, specify the parameters and click the **Save** button to save the configuration.



4. Configure a Web protection policy to associate a Web protection profile with the HTTP Web server.
   - Select **Web Protection > Web Protection Policy > Web Protection Policy** and click the **Add** button. In the prompted window, specify the parameters and click the **Save** button to save the configuration.



6.2.2. vAWF Configuration in Inline Proxy Mode

➢ **Prerequisites**

Before vAWF configuration, you need to assign two SR-IOV virtual ports to the vAWF instance. Port1 of the vAWF instance is mapped to the SR-IOV virtual port of the traffic port port1 and port2 of the vAWF instance is mapped to the SR-IOV virtual port of the traffic port port2.

On the AVX, port1 is connected to the upstream gateway while port2 is connected to backend Web servers.

➢ **Configuration Steps**

The configuration steps in inline proxy mode are similar to those in one-arm proxy mode. The only differences are that you need to define two bridge interfaces, bridge2 (192.168.1.2) and bridge3 (192.168.100.1), and add port1 and port2 to them respectively in step 1.

Note: In step 2, you still need to set the **Interface** parameter to bridge2 instead of bridge3.

6.2.3. vAWF Configuration in Router Mode

➢ **Prerequisites**

Before vAWF configuration, you need to assign two SR-IOV virtual ports to the vAWF instance. Port1 of the vAWF instance is mapped to the SR-IOV virtual port of the traffic port port1 and port2 of the vAWF instance is mapped to the SR-IOV virtual port of the traffic port port2.

On the AVX, port1 is connected to the upstream router while port2 is connected to backend Web servers.

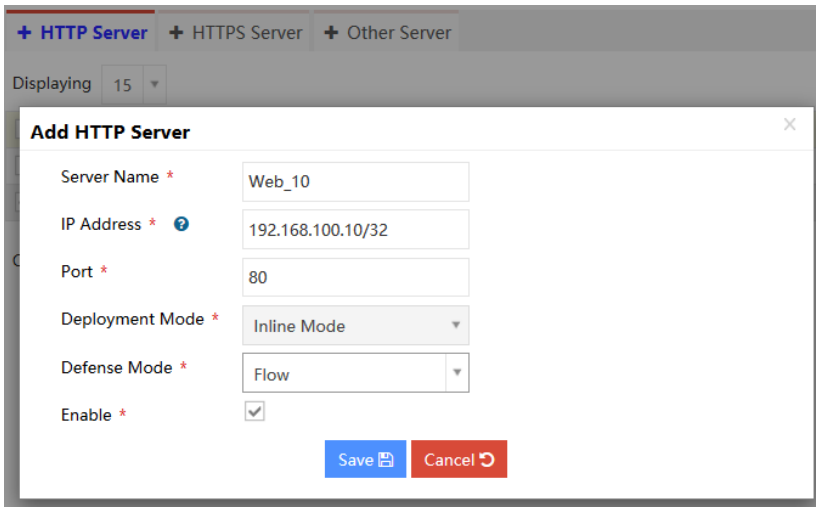
Note: You need to configure 192.168.1.1 as the gateway of the upstream router and 192.168.100.1 as the gateway of backend Web servers.

➢ **Configuration Steps**

1. Define two bridge interfaces bridge2 (192.168.1.1) and bridge3 (192.168.100.1) and add port1 and port2 to them respectively. For details, refer to step 1 in section 6.2.1 vAWF Configuration in One-arm Proxy Mode.

2. Define an HTTP Web server (for example, 192.168.100.10:80).

    - Select **Server Management > Normal Server > HTTP Server** and click the **Add** button. In the prompted window, specify the parameters, and click the **Save** button to save the configuration.



Note: In router mode, you need to set the **Deployment Mode** parameter to **Inline Mode** and the **Defense Mode** parameter to **Flow**.

3. Configure a Web protection policy to associate a Web protection profile with the HTTP Web server. For details, refer to step 4 in section 6.2.1 vAWF Configuration in One-arm Proxy Mode.

6.2.4. vAWF Configuration in Bridge Mode

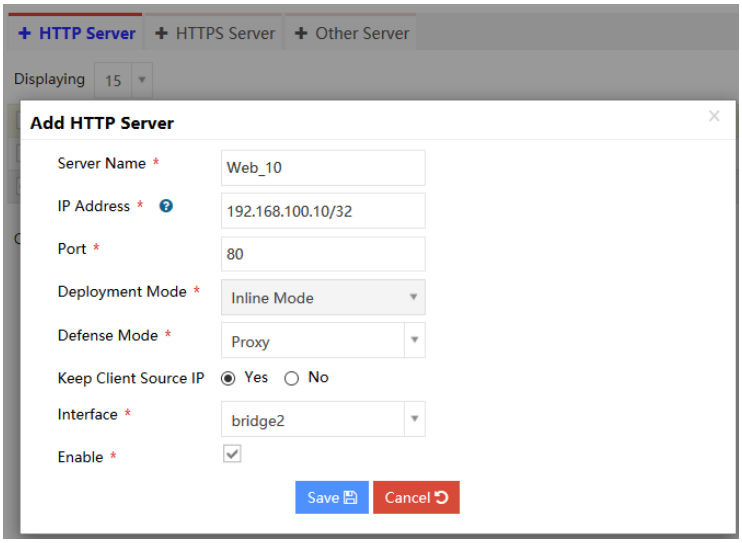
➢ **Prerequisites**

Before vAWF configuration, you need to create two virtual switches, attach the vAWF instance to them and add two traffic ports (port1 and port2) to them respectively. Port1 and port2 of the vAWF instance are mapped to vport1 and vport2 connected to the two virtual switches respectively.

On the AVX, port1 is connected to the upstream router while port2 is connected to backend Web servers.

➢ **Configuration Steps**

1. Create a bridge interface named bridge2 and add port1 and port2 to bridge2. For details, refer to step 1 in section 6.2.1 vAWF Configuration in One-arm Proxy Mode.
2. Define an HTTP Web server (for example, 192.168.100.10:80).
    - Select **Server Management > Normal Server > HTTP Server** and click the **Add** button. In the prompted window, specify the parameters, and click the **Save** button to save the configuration.



Note: In bridge mode, you need to set the **Deployment Mode** parameter to **Inline Mode**, the **Defense Mode** parameter to **Proxy** or **Flow**, and set the **Interface** parameter to bridge2.

3. Configure a Web protection policy to associate a Web protection profile with the HTTP Web server. For details, refer to step 4 in section 6.2.1 vAWF Configuration in One-arm Proxy Mode.

6.2.5. vAWF Configuration in Sniffer Mode

➢ **Prerequisites**

Before vAWF configuration, you need to create a VA instance (such as a vAPV instance named vAPV) that is assigned an SR-IOV virtual port from the traffic port port1 and a virtio virtual port (vport1) by attaching it to a virtual switch. The traffic port port2 on AVX is connected to the virtual switch.

On the AVX, port1 is connected to the upstream router while port2 is connected to backend Web servers.

In addition, you need to assign a virtio virtual port (vport2) to the vAWF instance by attaching it to the virtual switch and configured a port mirroring policy for the virtual switch to mirror traffic from vport1 to vport2. Port1 of the vAWF instance is mapped from the virtio virtual port vport2.

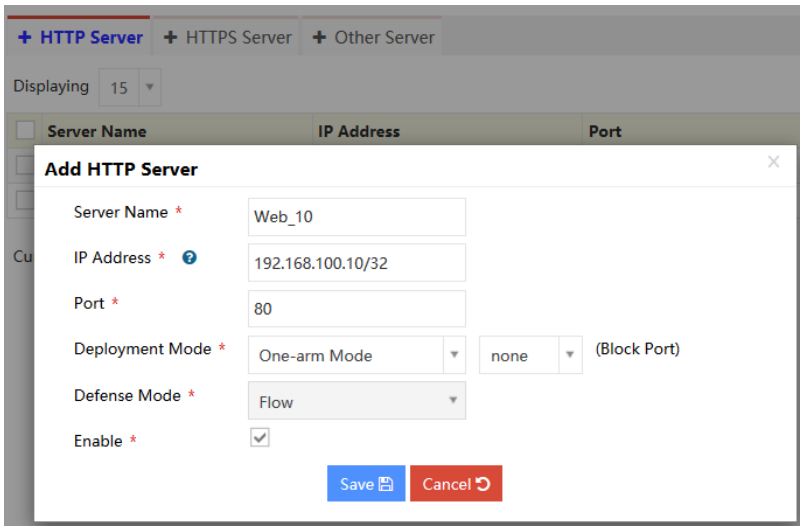
```
AN(config)#va pureinstance vAPV medium 1 default
AN(config)#va pureinstance vAWF medium 1 vAWF_6.1.2
AN(config)#va port vAPV port1 1
AN(config)#switch name switch1
AN(config)#switch interface switch1 port2
AN(config)#switch va switch1 vAPV vport1 0 4
AN(config)#switch va switch1 vAWF vport2 0 4
AN(config)#switch mirror switch1 vport2 vport1 0
```

➢ **Configuration Steps**

1. Create a bridge interface named bridge2 and added port1 to bridge2. For details, refer to step 1 in section 6.2.1 vAWF Configuration in One-arm Proxy Mode.

2. Define an HTTP Web server (for example, 192.168.100.10:80).

   - Select **Server Management > Normal Server > HTTP Server** and click the **Add** button. In the prompted window, specify the parameters, and click the **Save** button to save the configuration.



Note: In bridge mode, you need to set the **Deployment Mode** parameter to **One-arm Mode** and the **Defense Mode** parameter to **Flow**.

3. Configure a Web protection policy to associate a Web protection profile with the HTTP Web server. For details, refer to step 4 in section 6.2.1 vAWF Configuration in One-arm Proxy Mode.

7. Deploying vAWF Instances with High Availability

On one AVX, you can deploy multiple vAWF instances with high availability.

The following figure shows a deployment example of two vAWF instances with high availability.

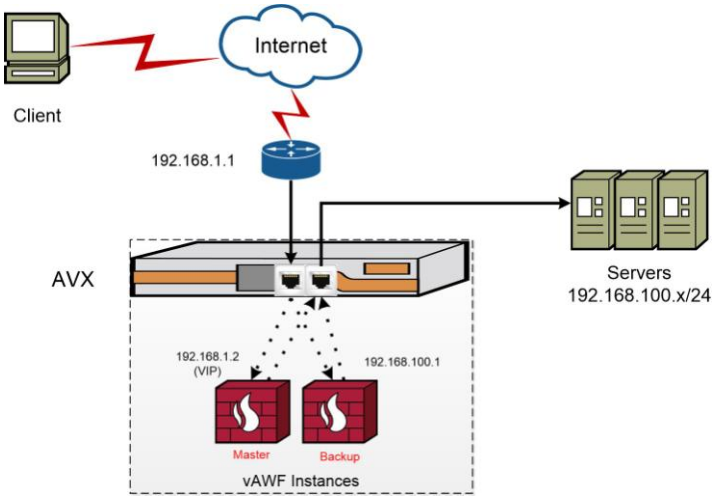


Figure 6-1 vAWF Instances with High Availability

In this figure, the vAWF instance vAWF1 works as the master node while vAWF2 works as a backup node. When vAWF1 becomes down, vAWF2 will automatically take over services and become the new master node. After vAWF1 is restored, it will preempt the master role back.

- **Configuration Example**

This section will use the inline proxy mode of vAWF instances as an example.

1. Deploy two vAWF Instances on the AVX.

```
AN(config)#va pureinstance vAWF1 medium 1 vAWF_6.1.2
AN(config)#va pureinstance vAWF2 medium 1 vAWF_6.1.2
AN(config)#va port vAWF1 port1 1
AN(config)#va port vAWF1 port2 1
AN(config)#va port vAWF2 port1 2
AN(config)#va port vAWF2 port2 2
```

2. Complete the initial configurations for two instances.

For vAWF1:

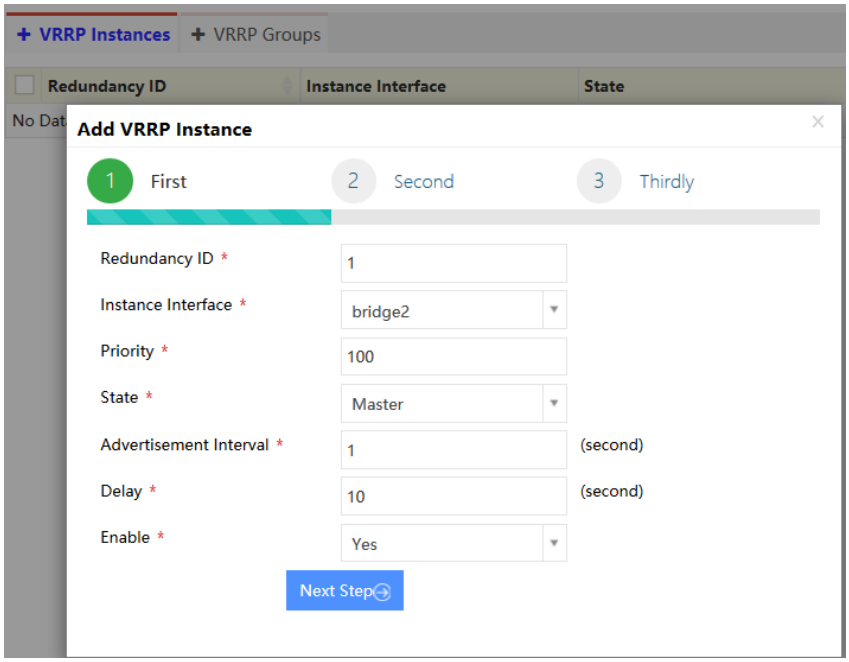
```
WAF>bridge -A -v MngtBridge -f 192.168.0.111 -m 255.255.255.0 -n y
WAF>route -A -i 192.168.0.0 -m 255.255.0.0 -g 192.168.0.1
WAF>remote -A -t web -i 192.168.0.0 -m 255.255.0.0
WAF>remote -A -t ssh -i 192.168.0.0 -m 255.255.0.0
WAF>remote -A -t ping -i 192.168.0.0 -m 255.255.0.0
```

For vAWF2:

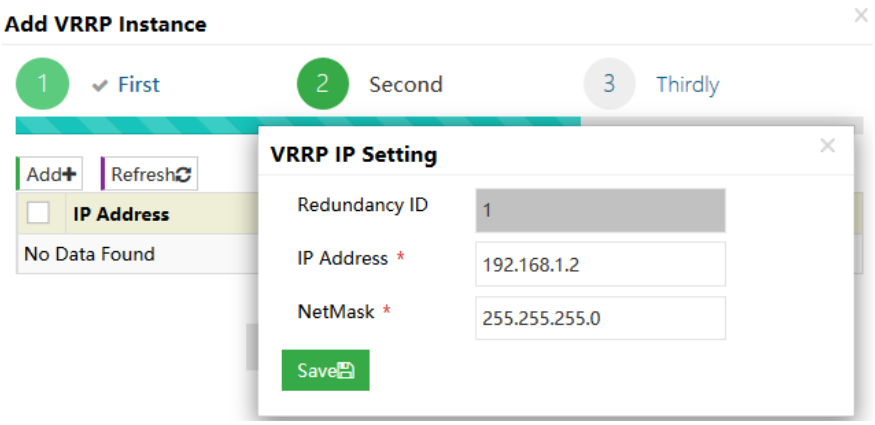
```
WAF>bridge -A -v MngtBridge -f 192.168.0.111 -m 255.255.255.0 -n y
WAF>route -A -i 192.168.0.0 -m 255.255.0.0 -g 192.168.0.1
WAF>remote -A -t web -i 192.168.0.0 -m 255.255.0.0
```

WAF>**remote -A -t ssh -i *192.168.0.0* -m 255.255.0.0**
WAF>**remote -A -t ping -i *192.168.0.0* -m 255.255.0.0**

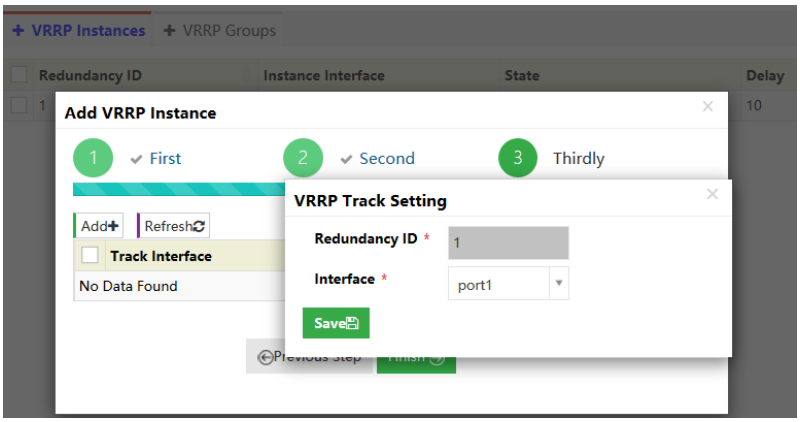
3. Load valid licenses to the two vAWF instances.
4. Complete the vAWF configuration on vAWF1 according to section 6.2.2 vAWF Configuration in Inline Proxy Mode.
5. Configure HA settings on vAWF1.
   - Create VRRP Instances (1 and 2) for bridge2 and bridge3.



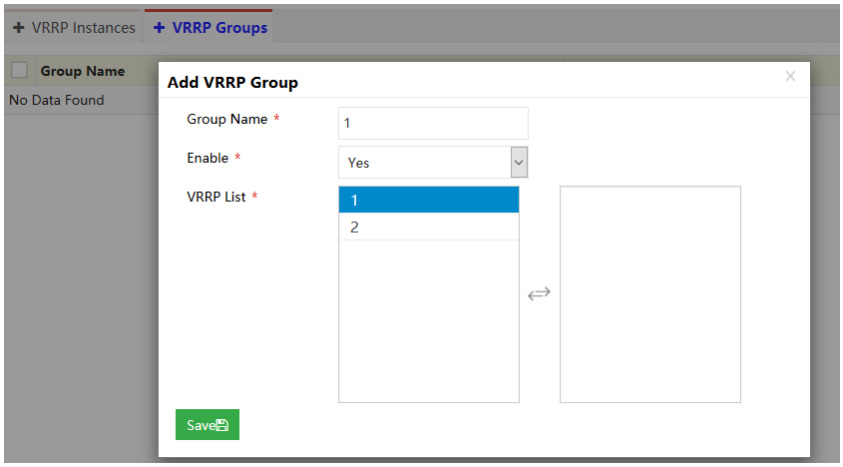
   - Add VRRP IPs (192.168.1.2 and 192.168.100.1) for the VRRP instances respectively.



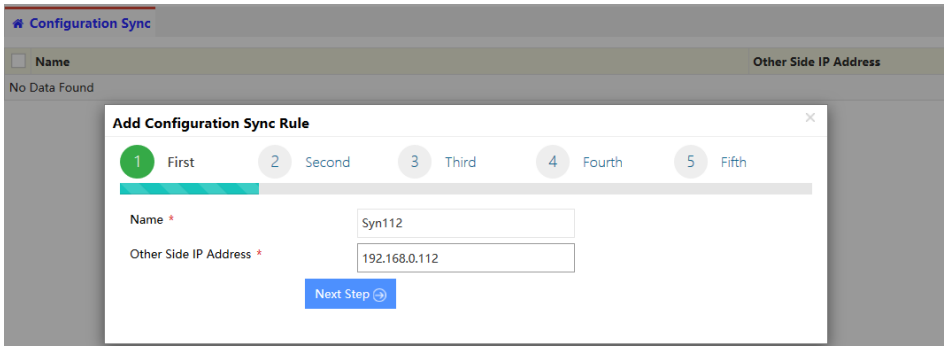
   - Associate the VRRP instances with port1 and port2 respectively.



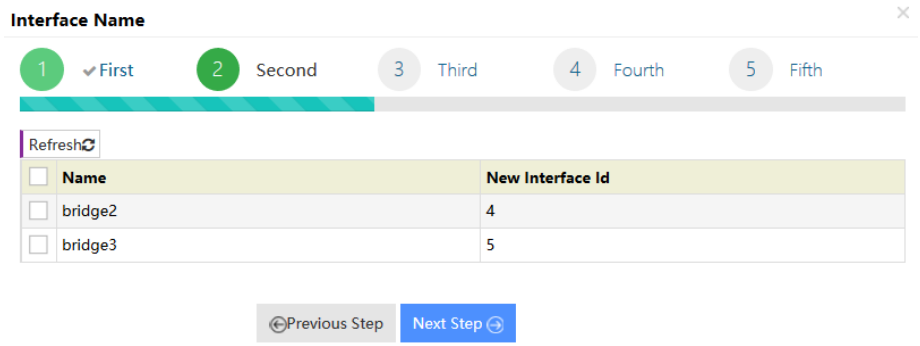
- Add the two VRRP instances into a VRRP group so that services on two VRRP instances can be switched simultaneously.



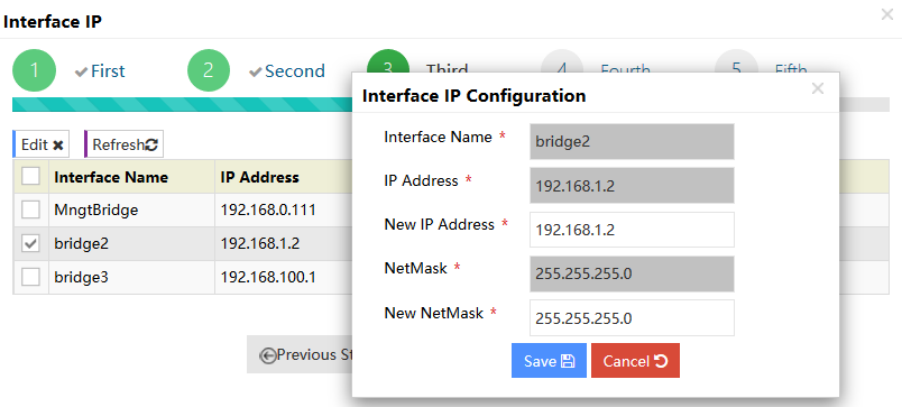
6. Synchronize the configurations of vAWF1 to vAWF2.
   - Define the name of the configuration sync rule and specify the peer IP address.



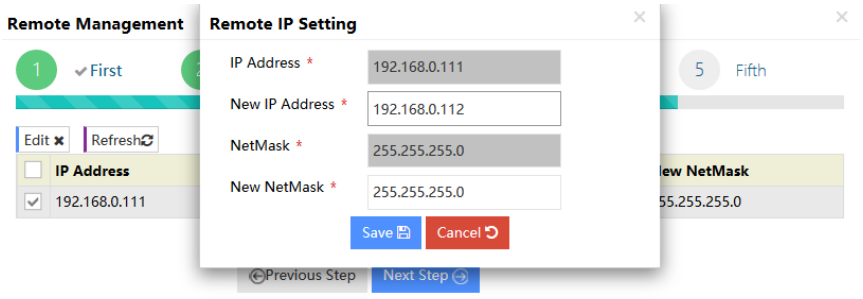
   - Set the IDs of the bridge interfaces on vAWF2.



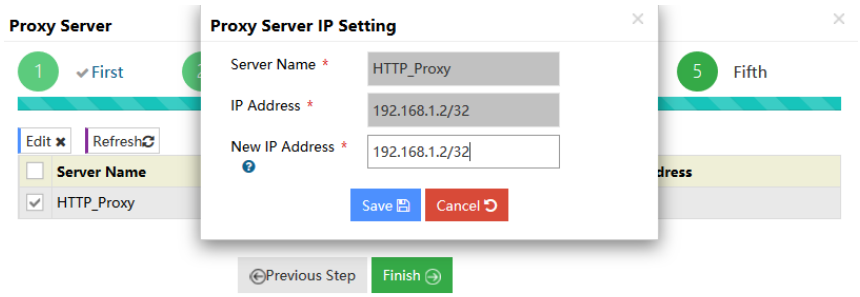
- Set the IP addresses for the bridge interfaces on vAWF2.



- Set the remote IP address for vAWF2.



- Set the IP address of the HTTP proxy server for vAWF2.



- Select the configuration sync rule and click **Apply** button to synchronize configurations to vAWF2.

About Array Networks

Array Networks, the network functions platform company, develops purpose-built systems for deploying virtual app delivery, networking and security functions with guaranteed performance. Headquartered in Silicon Valley, Array is backed by over 250 worldwide employees and is poised to capitalize on explosive growth in the areas of virtualization, cloud and software-centric computing. Proven at over 5000 worldwide customer deployments, Array is recognized by leading analysts, enterprises and service providers, for 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

May-2017 rev. a