Deployment Guide
Oct-2017 rev. a

Hillstone CloudEdge Deployment Guide for AVX Series Network Functions Platform

Table of Contents

1. About Hillstone CloudEdge 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.

Hillstone Virtual Next-Generation Firewall, CloudEdge, embedded with the Hillstone Networks StoneOS operation system, is deployed as a virtual machine, and provides advanced security services for applications and users in any virtualized environment. It provides comprehensive security features including granular application identification and control, intrusion prevention, anti-virus, attack defense and cloud sandbox to fully keep a business secure and operational. It provides price- performance solutions for both public and private cloud customers, and can be rapidly provisioned and deployed at scale.

Hillstone CloudEdge can be deployed on Array's AVX appliance as a VA instance. CloudEdge supports the entry and small instance sizes provided by the AVX appliance. CloudEdge on AVX provides the following benefits:

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

Note: For this deployment guide, the AVX Series should run ArrayOS AVX 2.4.0.3 or later, and CloudEdge should run StoneOS 5.5R1 version or later.

For additional information about Hillstone SG6000 and CloudEdge, please visit http://docs.hillstonenet.com/en/Content/Home.htm.

2. Deploying CloudEdge on AVX

To deploy a CloudEdge instance on the AVX appliance, follow these steps:

1. Obtain the image of CloudEdge
2. Import the image to the AVX appliance
3. Create a VA Instance with the image on the AVX appliance
4. Assign virtual traffic ports to the VA instance
5. Start the VA Instance

Note: For different instance sizes, Hillstone provides different images: SG6000-CloudEdge-5.5R5-VM01.qcow2 for the entry size and SG6000-CloudEdge-5.5R5-VM02.qcow2 for the small size. If you want to create a specified size of CloudEdge, you should import the correct image.

2.1. Obtaining the Image of the CloudEdge VM

Before deploying a CloudEdge instance, contact Array Networks Customer Support to obtain the image (for example, SG6000-CloudEdge-5.5R5-VM02.qcow2) of the CloudEdge VM as well as the metadata file (metadata.ini) of the image.

Please place the image and the metadata file onto an HTTP server or FTP server that is accessible by the AVX appliance. For example, the URLs of the image and the metadata file are http://10.4.0.35/SG6000-CloudEdge-5.5R5-VM02.qcow2 and http://10.4.0.35/metadata.ini respectively.

2.2. Importing the Image to the AVX Appliance

To import the image to AVX, execute the following command on 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.

```
AN(config)#va image CloudEdge-image http://10.4.0.35/SG6000-CloudEdge-5.5R5-VM02.qcow2 qcow2 http://10.4.0.35/metadata.ini
```

2.3. Creating the CloudEdge VM with the Image on the AVX Appliance

After the image has been imported successfully, you can create the VA 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 size should match the used image. SG6000-CloudEdge-5.5R5-VM02.qcow2 can only be used to create the small size of CloudEdge VM while SG6000-CloudEdge-5.5R5-VM01.qcow2can only be used to create the entry size of CloudEdge VM.

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

image_name: name of the image.

```
AN(config)#va pureinstance CloudEdge-VM small 1 CloudEdge-image
```

The size of the VA instance determines the amount of system resources assigned to the VA instance.

Size	CPU	Memory
Entry	2 cores	2GB
Small	2 cores	4GB

2.4. Assign Virtual Traffic Ports to the CloudEdge VM

The AVX assigns a virtual management port that is connected with the AVX's physical management port using a built-in virtual switch when a CloudEdge VM is created. The virtual management port becomes the first interface (ethernet0/0) for the CloudEdge VM. 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 CloudEdge VM according to the requirements of different deployment modes, as shown in the table below.

The AVX appliance provides two types of virtual traffic ports for the CloudEdge VM:

- 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
Routing mode	Assign one or more SR-IOV virtual ports
Transparent mode	Assign one or multiple pairs of virtio virtual ports
Tap mode	Assign one virtio virtual port (tap interface) and assign one SR-IOV virtual port (control interface)

2.4.1. Assigning an SR-IOV Virtual Port to the CloudEdge VM

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 CloudEdge-VM port1 1
```

2.4.2. Assigning a Virtio Virtual Port to the CloudEdge VM

When you attach the CloudEdge VM to a virtual switch, the CloudEdge VM will be assigned a virtio virtual port. For external communication of the CloudEdge VM 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 CloudEdge VM 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 CloudEdge-VM vport1 0 2
```

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 two queue pairs for a small-size VA instance.

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 CloudEdge VM to support the transparent deployment mode, you need to create two virtual switches, attach the CloudEdge VM to both of them, and add two traffic ports to the two virtual switches respectively.

2.5. Starting the CloudEdge VM

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

```
AN(config)#va start CloudEdge-VM
```

3. Completing Initial Configuration for the CloudEdge VM

After the CloudEdge VM is up, you can establish a console connection to it using the "**va console** <*va_name* >" command.

```
AN(config)#va console CloudEdge-VM
```

Before you can connect to the CloudEdge VM's WebUI, you need to complete the initial configuration.

To complete the initial configuration, follow these steps:

1. Log into the console with the default username and password. The default username and password both are "hillstone".

2. Execute the following commands to enter the Config mode of the management interface.

```
SG-6000# configure
SG-6000(config)# interface ethernet0/0
SG-6000(config-if-eth0/0)#
```

3. Disable the Dynamic Host Configuration Protocol (DHCP) for the management interface and allocate a static IP address collected from the administrator.

```
SG-6000(config-if-eth0/0)# no ip address dhcp
SG-6000(config-if-eth0/0)# ip address 192.168.1.100/255.255.255.0
SG-6000(config-if-eth0/0)# manage ssh
SG-6000(config-if-eth0/0)# manage https
SG-6000(config-if-eth0/0)# manage snmp
SG-6000(config-if-eth0/0)# manage ping
SG-6000(config-if-eth0/0)# manage traceroute
SG-6000(config-if-eth0/0)# manage telnet
SG-6000(config-if-eth0/0)# exit
```

Note: If you have configured the DHCP function on the AVX appliance, you can enable the DHCP for the management interface so that the management interface will be automatically assigned an IP address. You can execute the "**show interface ethernet0/0**" command to view the assigned IP address.

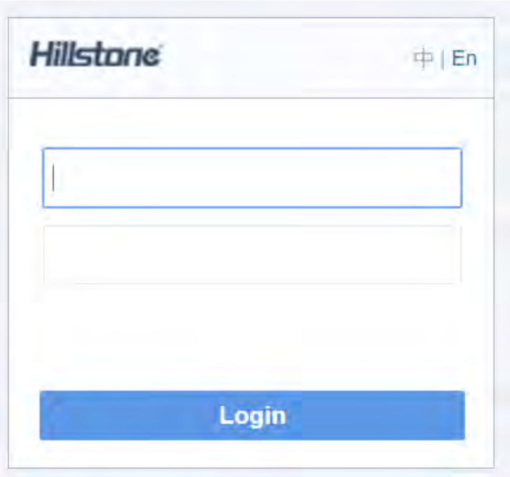
4. Configure the default route.

```
SG-6000(config)# ip vrouter trust-vr
SG-6000(config-vrouter)# ip route 0.0.0.0/0 192.168.1.1
SG-6000(config-if-eth0/0)# exit
```

5. Save the configurations.

```
SG-6000(config)# save
```

When the initial configuration is completed, you can access the CloudEdge VM's WebUI at https://<management_IP>, from which you can proceed with the configuration. The default username and password both are "hillstone".



Note: The CloudEdge VM’s WebUI is supported only by IE 11 and Chrome browsers.

For more information, please click the ⓘ icon to see the online help of the CloudEdge VM.

4. Loading a Formal License to the CloudEdge VM

4.1. License Models

Hillstone provides two CloudEdge-VM license models: CloudEdge-VM01 and CloudEdge-VM02.

Capacity	CloudEdge-VM01	CloudEdge-VM02
Core (min/max)	2/2	2/2
Memory	2G/4G	4G/8G
Storage (min)	4GB	4GB
Network Interfaces	10	10
Firewall Throughput (vNIC/SR-IOV)	2 Gbps/10 Gbps	4 Gbps/20 Gbps
IPS throughput (vNIC/SR-IOV)	1 Gbps/3 Gbps	2 Gbps/5 Gbps
AV throughput	800 Mbps/1 Gbps	1.6 Gbps/2 Gbps
IPSec throughput (vNIC/SR-IOV)	200 Mbps/400 Mbps	400 Mbps/800 Mbps
New Sessions/Second (vNIC/SR-IOV)	20K/40K	40K/120K
Maximum Concurrent Sessions	100K	500K
IPsec VPN Tunnels (Max)	50	500
SSL VPN Users (Max.)	50	250

4.2. Licensing CloudEdge-VM

4.2.1. Trial License

After the CloudEdge VM is created on the AVX appliance, it will be preinstalled with a trial license. With the trial license, the CloudEdge VM has the same features and capacity as the formal license, but the trial license is valid only for 30 days.

4.2.2. Formal License

To make full use of the capacity of the CloudEdge VM, you need to purchase and upload a valid formal license, which is Platform Base License. The Platform Base license provides firewall, VPN and other features in the listed capacities.

4.2.3. Default License

When the formal license or trial expires, the CloudEdge VM will use the Default License, which will be valid eternally. With the default license, the system can function normally, but cannot be upgraded to higher versions and change of configuration is not allowed. In addition, the default license provides the same features as the Platform Base license, but restricts capacities as below:

- Firewall throughput (1518 Bytes): 100 Mbps
- Firewall throughput (64 Bytes): 10 Mbps
- Maximum sessions: 1 K
- New sessions per second: 1 K
- IPSec throughput (512 Bytes): 10 Mbps
- IPSec VPN tunnels: 2

- SSL VPN users: 2
- Maximum policy rules: 50
- Maximum address entries: 100

4.2.4. Function License

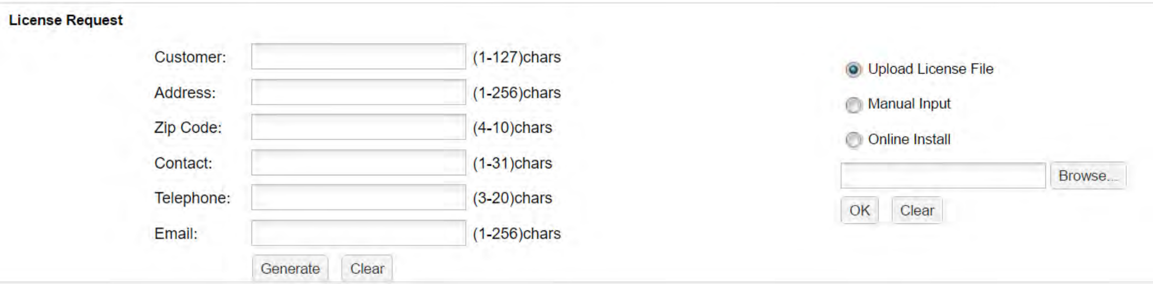
Some functions are only enabled when corresponding licenses are installed. The following function licenses are supported:

- **Intrusion Prevention System (IPS) License** IPS License provides IPS function and its signature database upgrade. IPS License has its own validity. When it expires, the IPS function works normally, but IPS signature database cannot be upgraded.
- **Anti-Virus (AV) License** AV License provides anti-virus function and its signature database upgrade. AV License has its own validity. When it expires, the anti-virus function works normally, but AV signature database cannot be upgraded.
- **Sandbox License** Sandbox License provides sandbox function, which controls the suspicious file quantity allowed to be uploaded to the cloud sandbox every day. It provides whitelist upgrade. Sandbox License has its own validity. When it expires, the cloud analysis is stopped and the whitelist cannot be upgraded. However, if the suspicious traffic still matches the analysis entries in the local cache, the sandbox function is still valid. After the system is restarted, the sandbox function will not be used.
- **URL DB License** URL DB License provides URL filter function and allows URL database to upgrade. URL DB License has its own validity. When it expires, the URL filter function works normally, but URL database cannot be upgraded.
- **APP DB License** APP DB License allows APP database to upgrade. APP DB license is issued with the platform license. There is no need to apply for it. The validity of APP DB License also follows platform license. When the platform license expires, APP signature database cannot be upgraded.
-

4.3. Loading the License

To upload a valid formal license, follow these steps:

1. Access the WebUI, select **System > License**.
2. Fill in the required fields under the **License Request** section and click the Generate button to generate the license application code.



License Request

Customer:		(1-127)chars
Address:		(1-256)chars
Zip Code:		(4-10)chars
Contact:		(1-31)chars
Telephone:		(3-20)chars
Email:		(1-256)chars

Generate Clear

● Upload License File

○ Manual Input

○ Online Install

Browse...

OK Clear

3. Contact Array Networks Customer Support to purchase a formal license by providing the license application code and the size of the VA instance.
4. Under the **License Request** section, choose one of the following two methods:
   - **Upload License File**: select this radio button and click **Browse**, select the license plain text file (.txt) to upload it to the system.
   - **Manual Input**: Select this radio button, and copy and paste license code into the text box.
5. Click **OK** to save the license.

5. Deployment Examples

5.1. Supported Operating Modes

The CloudEdge VM on AVX can support the same deployment modes as its hardware counterpart:

- Transparent Mode
- Routing Mode
- Tap Mode (Sniffer)

In addition, the CloudEdge VM can support the mixed mode of transparent, routing and tap at the same time.

5.1.1. Transparent Mode

Transparent mode is also known as bridge mode or transparent bridging mode. Transparent mode is used when the IT administrator does not wish to change its existing network layout, normally the existing network already has set up routers and switches. The CloudEdge VM will be used as a security device.

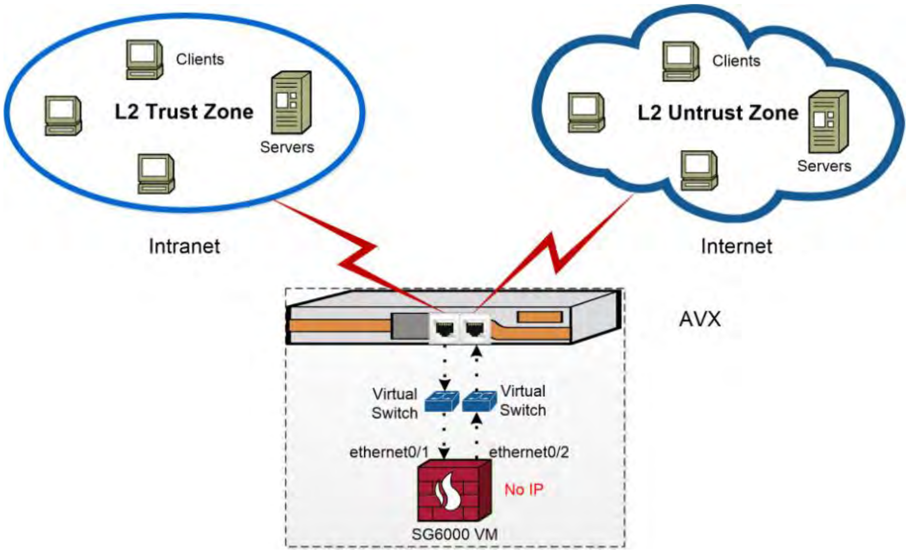
Transparent mode has the following advantages:

- No need to change IP addresses
- No need to set up Network Address Translation (NAT) rule

Under normal circumstances, the CloudEdge VM in the transparent mode is deployed between the router and switch of the protected network, or it is installed between Internet and a company's router. The internal network uses its old router to access Internet, and the firewall only provides security control features.

The transparent mode is realized by binding interfaces to Layer 2 zones and binding these Layer 2 zones to a virtual switch.

The following figure displays the deployment of the CloudEdge VM in transparent mode.

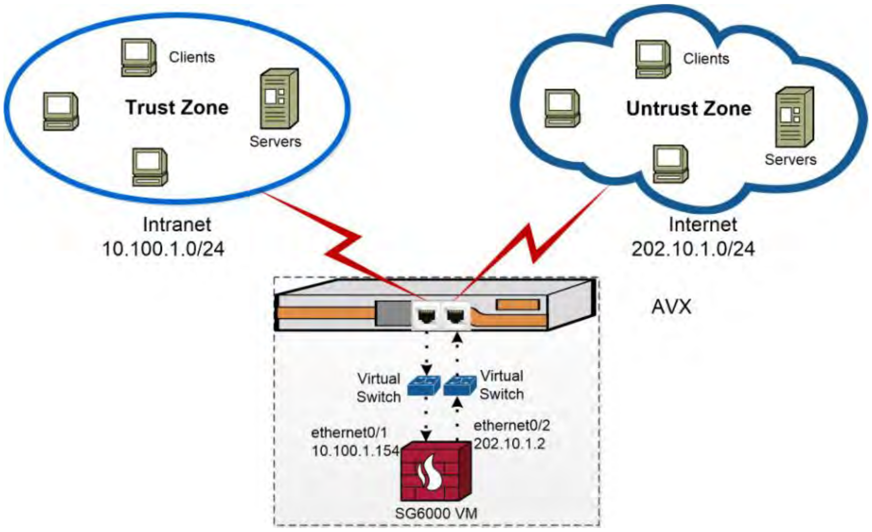


5.1.2. Routing Mode

Routing mode deployment often uses the NAT function as well, so it is also called NAT mode. In routing mode, each interface has its IP address which means interfaces are in the layer 3 zone. A firewall in routing mode can work as a router and a security device. Routing mode is mostly used when the firewall is installed between an internal network and Internet.

The routing mode is realized by binding interfaces to Layer 3 zones and binding these Layer 3 zones to a virtual router.

The following figure displays the deployment of the CloudEdge VM in routing mode.



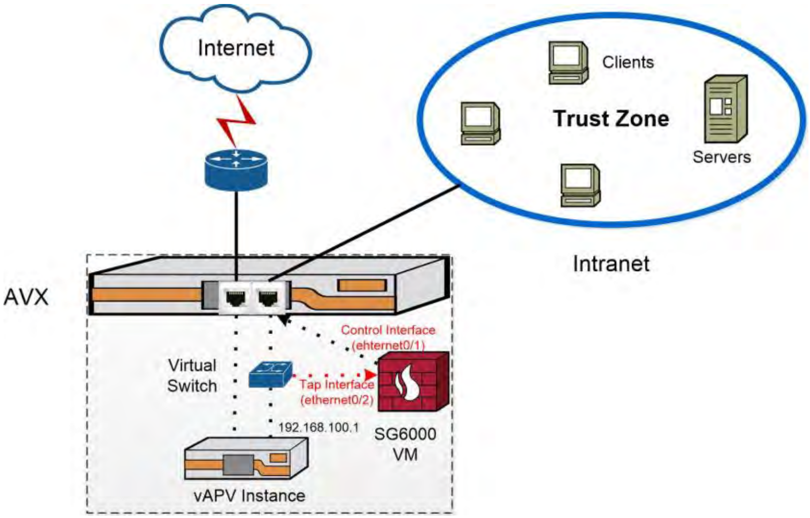
5.1.3. Tap Mode

In most cases, the CloudEdge VM is deployed within the network as an inline node. However, in some other scenarios, an IT administrator would just want auditing and statistical functions, like IPS, antivirus, and Internet behavior control. For these features, you just need to connect the CloudEdge VM to a mirrored interface of the trunk network. The traffic is mirrored to the CloudEdge VM for auditing and monitor.

The tap mode is realized by binding a physical interface to the Tap zone. Then the interface becomes a tap interface. The CloudEdge VM will monitor, scan, or record the traffic received in the tap interface.

After configuring IPS, AV, or network behavior control on the CloudEdge VM, if the CloudEdge VM detects network intrusions, virus, or illegal network behaviors, it will send TCP RST packets from the control interface to tell clients to reset the connections.

The following figure displays the deployment of the CloudEdge VM in tap mode.



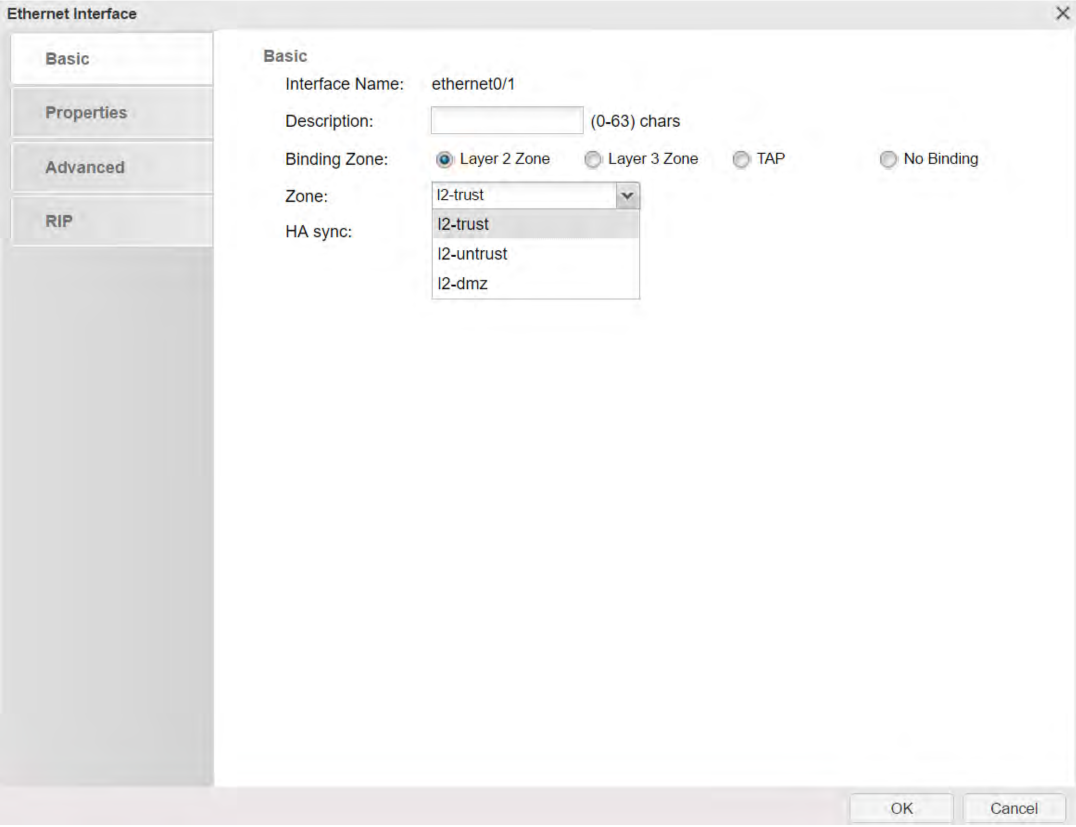
5.2. Configuration Example

5.2.1. Configuring the Transparent Mode

Assume that the ethernet0/1 is connected to the Intranet while ethernet0/2 is connected to the Internet.

To configure the transparent mode, follow these steps:

1. Access the WebUI of the CloudEdge VM (for example, https://192.168.1.100:8443).
2. Select **Network > Interface**, double-click ethernet0/1, set **Binding Zone** to **Layer 2 Zone** and **Zone** to **l2-trust**, and click **OK**.



Basic

Interface Name: ethernet0/1

Description: (0-63) chars

Binding Zone: ● Layer 2 Zone ○ Layer 3 Zone ○ TAP ○ No Binding

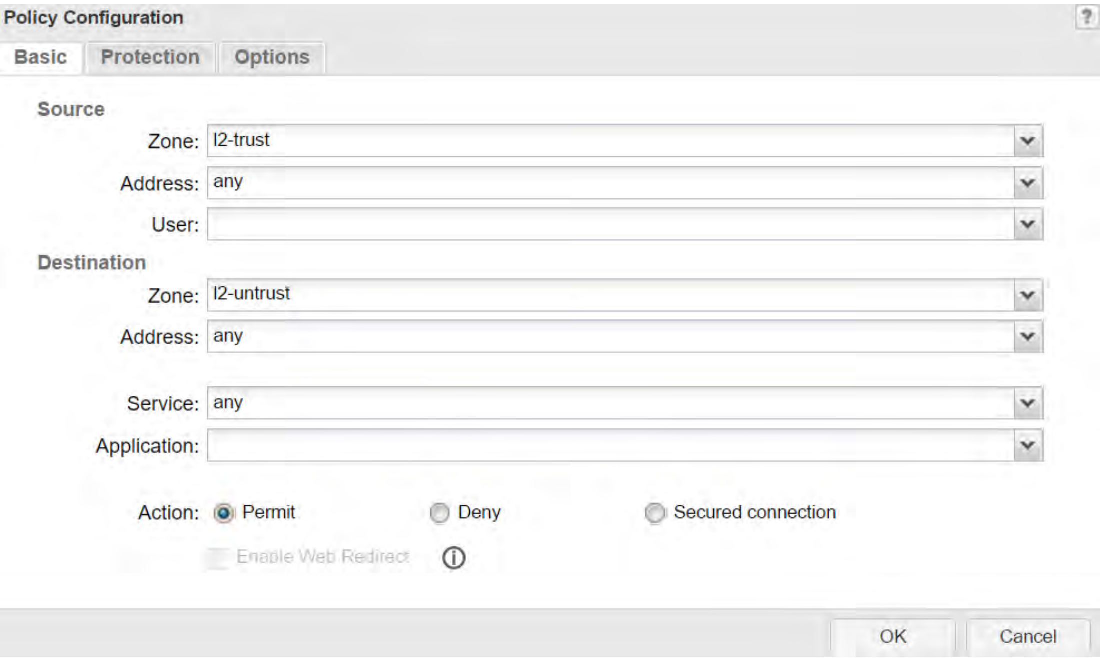
Zone: l2-trust

HA sync:

3. Double-click ethernet0/2, set **Binding Zone** to **Layer 2 Zone** and **Zone** to **l2-untrust**, and click **OK**.

Note: “l2-trust” and “l2-untrust” are predefined Layer 2 zones that are bound to the default virtual switch “vswitch1”. If you do not want to use the default zones or virtual switch, you can create a new virtual switch and two Layer 2 zones.

4. To configure a policy to allow the intranet to visit the internet, select **Policy > Security Policy** and click **New**. On the **Basic** tab page of the **Policy Configuration** window, set **Zone** in the **Source** section to **l2-trust**, set **Zone** in the **Destination** section to **l2-untrust**, set **Action** to **Permit** and click **OK**.



Source

Zone: l2-trust

Address: any

User:

Destination

Zone: l2-untrust

Address: any

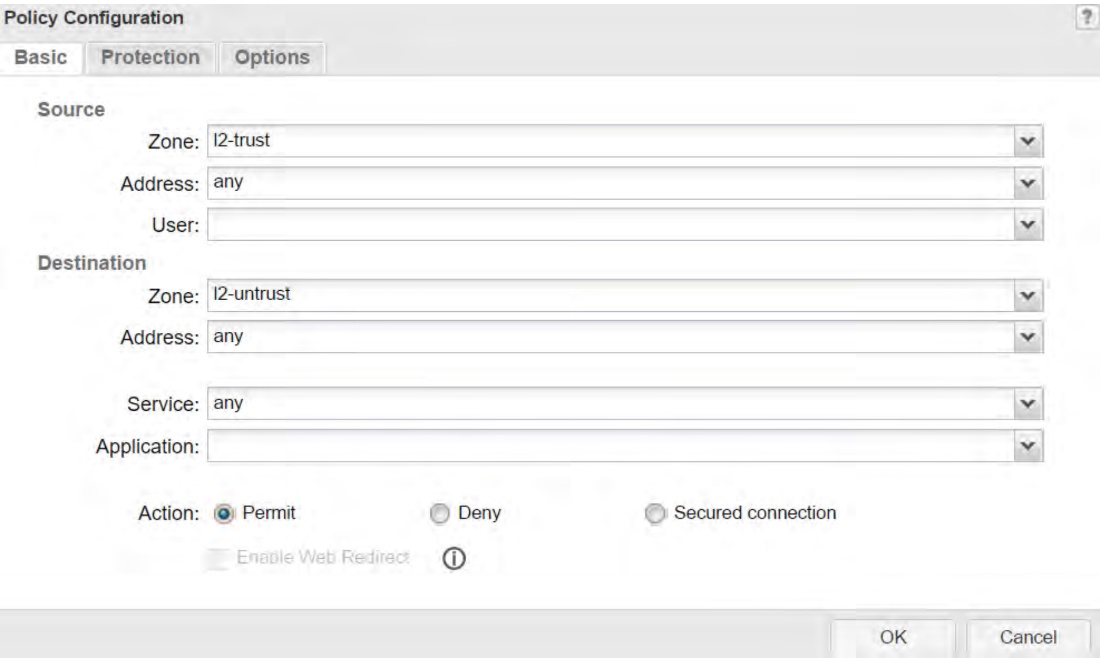
Service: any

Application:

Action: ● Permit ○ Deny ○ Secured connection

□ Enable Web Redirect ⓘ

5. To configure a policy to allow the internet to visit the private network, select **Policy > Security Policy** and click **New**. On the **Basic** tab page of the **Policy Configuration** window, set **Zone** in the **Source** section to **l2-untrust**, set **Zone** in the **Destination** section to **l2-trust**, set **Action** to **Permit** and click **OK**.



Source

Zone: l2-trust

Address: any

User:

Destination

Zone: l2-untrust

Address: any

Service: any

Application:

Action: ● Permit ○ Deny ○ Secured connection

□ Enable Web Redirect ⓘ

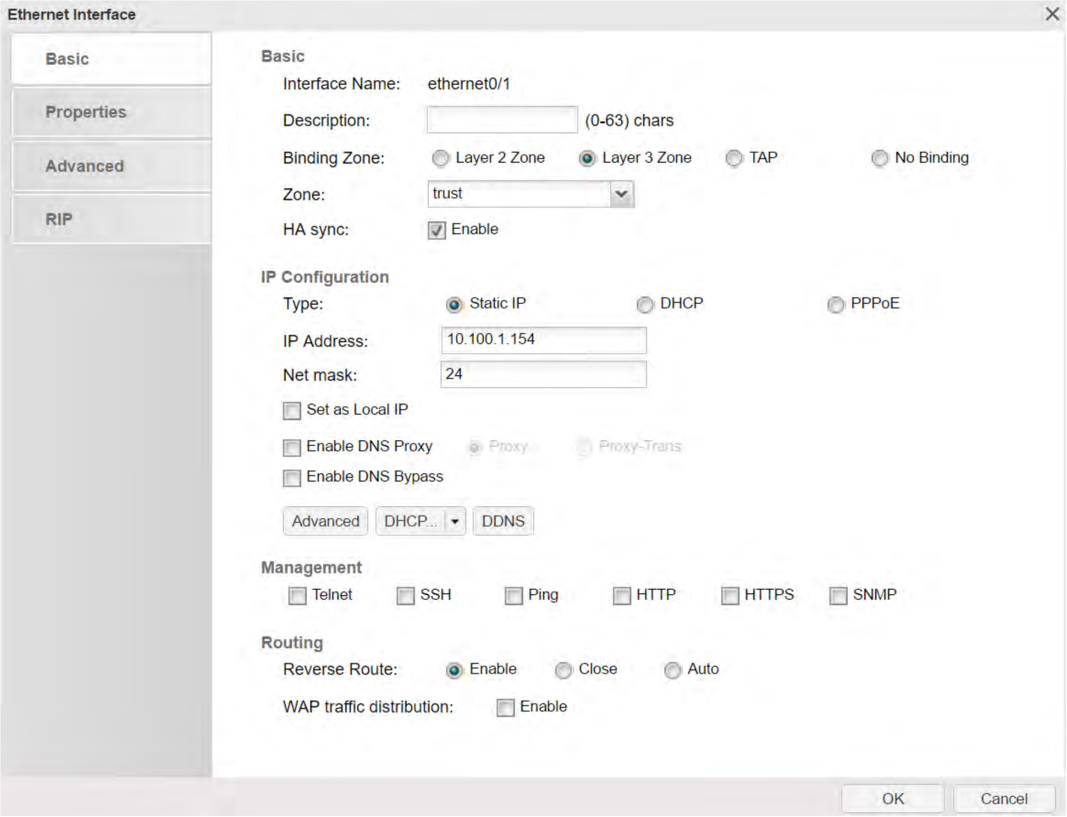
The transparent mode is now configured.

5.2.2. Configuring the Routing Mode

Assume that the ethernet0/1 is connected to the Intranet while ethernet0/2 is connected to the Internet.

To configure the routing mode, follow these steps:

1. Access the WebUI of the CloudEdge VM (for example, https://192.168.1.100:443).
2. Select **Network > Interface**, double-click ethernet0/1, set **Binding Zone** to **Layer 3 Zone** and **Zone** to **trust**, assign a private IP address, and click **OK**.



Ethernet Interface

Basic

Interface Name: ethernet0/1

Description: (0-63) chars

Binding Zone: ○ Layer 2 Zone ● Layer 3 Zone ○ TAP ○ No Binding

Zone: trust

HA sync: ☑ Enable

IP Configuration

Type: ● Static IP ○ DHCP ○ PPPoE

IP Address: 10.100.1.154

Net mask: 24

□ Set as Local IP

□ Enable DNS Proxy ● Proxy ○ Proxy-Trans

□ Enable DNS Bypass

Management

□ Telnet □ SSH □ Ping □ HTTP □ HTTPS □ SNMP

Routing

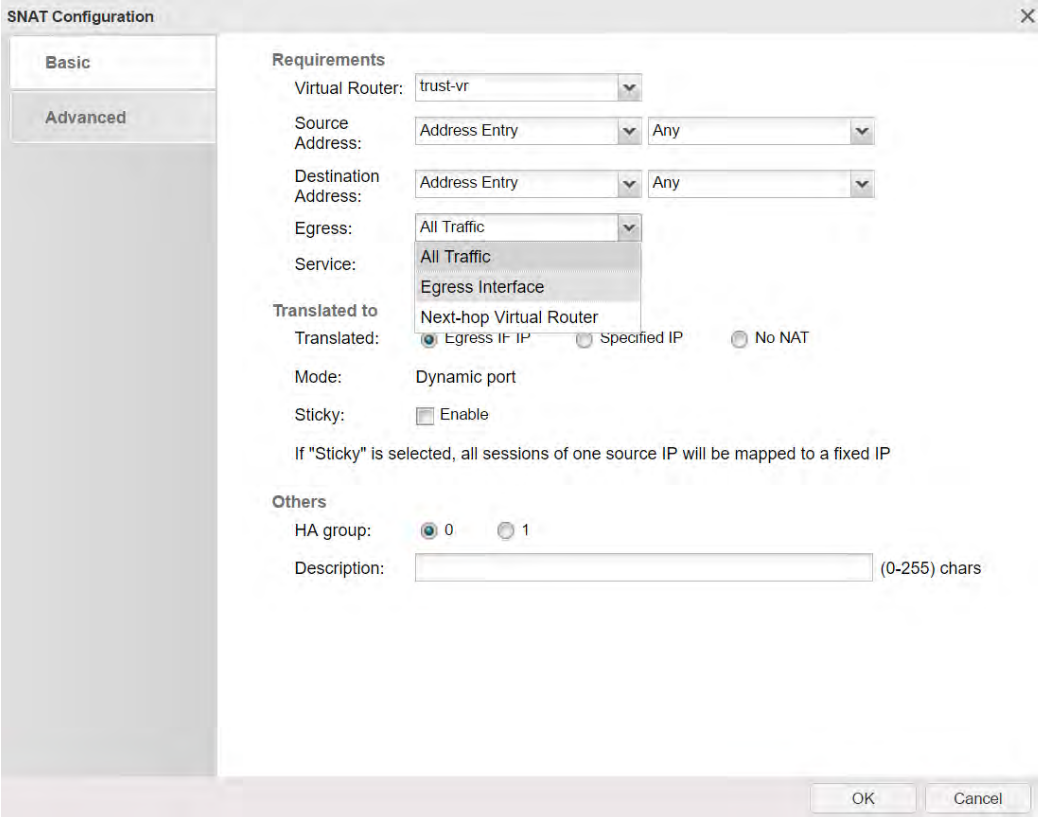
Reverse Route: ● Enable ○ Close ○ Auto

WAP traffic distribution: □ Enable

3. Double-click ethernet0/2, set **Binding Zone** to **Layer 3 Zone** and **Zone** to **untrust**, assign a public IP address and click **OK**.

Note: “trust” and “untrust” are predefined Layer 3 zones that are bound to the default virtual router “trust-vr”. If you do not want to use the default zones or virtual router, you can create a new virtual router and two Layer 3 zones.

4. To configure a NAT rule to translate the source IPs from the private IPs to the public IP, select **Policy > NAT > SNAT**, set **Virtual Router** to the one used in the preceding steps and click **New**. In the prompted **SNAT Configuration** window, set **Egress** to **Egress Interface** and choose the egress interface (ethernet0/2), set **Translated** to **Egress IF IP**, and click **OK**.



SNAT Configuration

Requirements

Virtual Router: trust-vr

Source Address: Address Entry · Any

Destination Address: Address Entry · Any

Egress: All Traffic

- All Traffic
- Egress Interface
- Next-hop Virtual Router

Service:

Translated to

Translated: ● Egress IF IP ○ Specified IP ○ No NAT

Mode: Dynamic port

Sticky: □ Enable

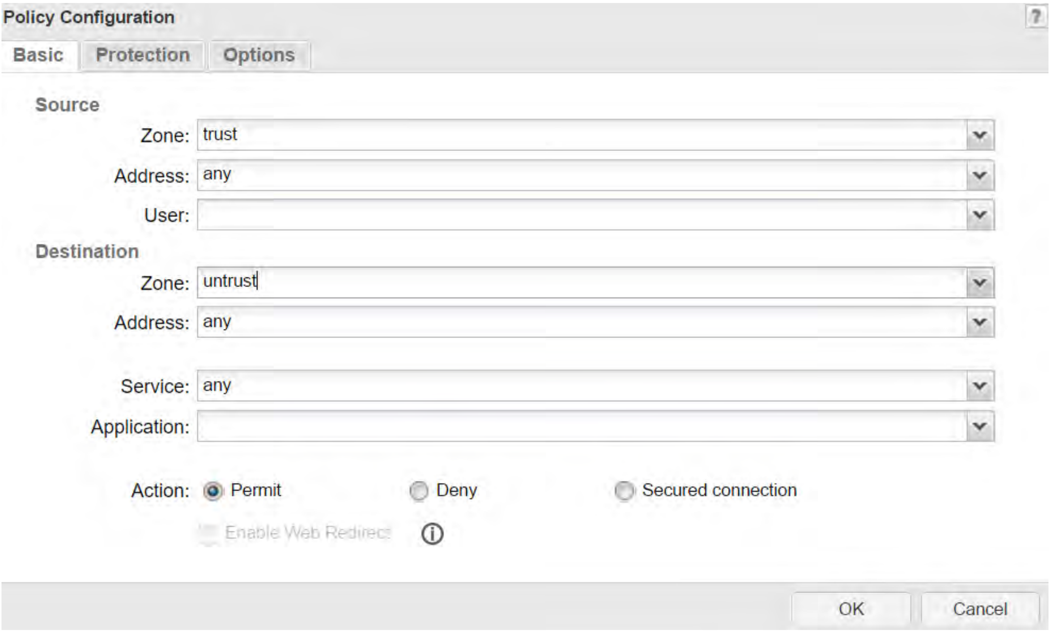
If "Sticky" is selected, all sessions of one source IP will be mapped to a fixed IP

Others

HA group: ● 0 ○ 1

Description: (0-255) chars

5. To configure a policy to allow internal users to visit the internet, select **Policy > Security Policy** and click **New**. On the **Basic** tab page of the **Policy Configuration** window, set **Zone** in the **Source** section to **trust**, set **Zone** in the **Destination** section to **untrust**, set **Action** to **Permit** and click **OK**.



Policy Configuration

Source

Zone: trust

Address: any

User:

Destination

Zone: untrust

Address: any

Service: any

Application:

Action: ● Permit ○ Deny ○ Secured connection

□ Enable Web Redirect ⓘ

The routing mode is now configured.

5.2.3. Configuring the Tap Mode

➢ **Prerequisites**

Before CloudEdge-VM configuration, you need to create another VA instance (such as a vAPV instance named vAPV) that is assigned an SR-IOV virtual port from the AVX's physical traffic port port1 and a virtio virtual port (vport1) by attaching it to a virtual switch. The physical 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 the internal network.

For the CloudEdge-VM, you need to assign an SR-IOV virtual port from the physical traffic port port2.

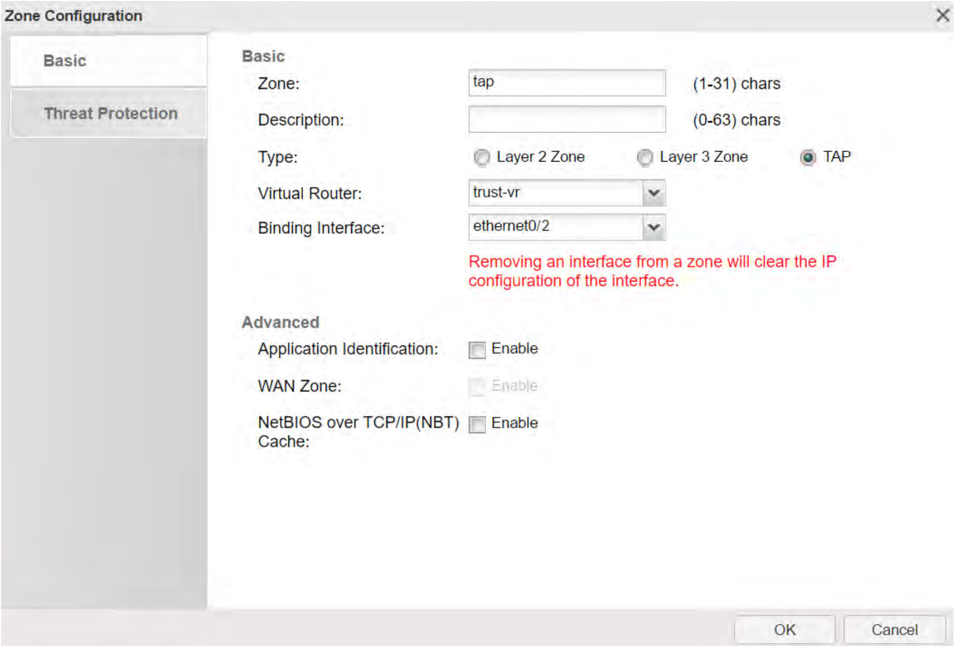
In addition, you need to assign a virtio virtual port (vport2) to the CloudEdge-VM by attaching it to the same virtual switch and configured a port mirroring policy for the virtual switch to mirror traffic from vport1 to vport2.

```
AN(config)#va pureinstance vAPV small 1 default
AN(config)#va pureinstance CloudEdge-VM small 1 CloudEdge-image
AN(config)#va port vAPV port1 1
AN(config)#va port CloudEdge-VM port2 1
AN(config)#switch name switch1
AN(config)#switch va switch1 vAPV vport1 0 2
AN(config)#switch va switch1 CloudEdge-VM vport2 0 2
AN(config)#switch mirror switch1 vport2 vport1 0
```

➢ **Configuration Steps**

Assume that the SR-IOV virtual port is mapped to the interface ethernet0/1 of the CloudEdge-VM and the virtio virtual port vport2 is mapped to the interface ethernet0/2 of the CloudEdge-VM.

1. Access the WebUI of the CloudEdge VM (for example, https://192.168.1.100:443).
2. Select **Network > Zone**, and click **New**. On the **Basic** tab page of the prompted **Zone configuration** window, specify the **Zone** field, set **Type** to **TAP** and **Binding Interface** to **ethernet0/2**, and click **OK**.



Zone Configuration

Basic

Zone: tap (1-31) chars

Description: (0-63) chars

Type: ○ Layer 2 Zone ○ Layer 3 Zone ● TAP

Virtual Router: trust-vr

Binding Interface: ethernet0/2

Removing an interface from a zone will clear the IP configuration of the interface.

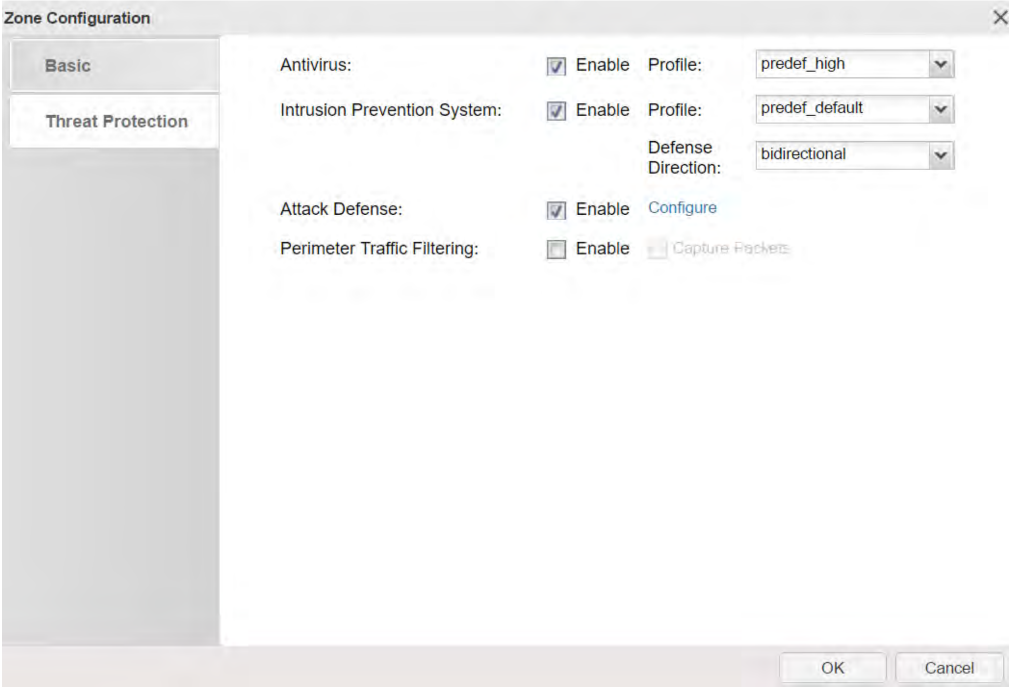
Advanced

Application Identification: □ Enable

WAN Zone: □ Enable

NetBIOS over TCP/IP(NBT) Cache: □ Enable

3. Click the **Threat Protection** tab, set **Antivirus** and **Intrusion Prevention System** to **Enable**, and select a profile for them and click **OK**.



Zone Configuration

Antivirus: ☑ Enable Profile: predef_high

Intrusion Prevention System: ☑ Enable Profile: predef_default

Defense Direction: bidirectional

Attack Defense: ☑ Enable Configure

Perimeter Traffic Filtering: □ Enable □ Capture Packets

Note: You can choose a predefined antivirus/IPS profile or a customized antivirus/IPS profile. To add a customized antivirus profile, go to **Object > Antivirus > Profile**. To add a customized IPS profile, go to **Object > Intrusion Prevention System > Profile**.

4. (Optional) To allow the CloudEdge-VM to block traffic when detecting network intrusions, virus or illegal network behaviors, configure the interface ethernet0/1 as the control interface in the Config mode of the tap interface via CLI.

```
SG-6000# configure
SG-6000(config)# interface ethernet0/2
SG-6000(config-if-eth0/2)# tap control-interface ethernet0/1
```

The tap mode is now configured.

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

Nov-2017 rev. a