

vAPV/FortiGate VM Firewall Sandwich Deployment Guide for AVX Series Network Functions Platform

Table of Contents

Table of Contents	1
1. Introduction.....	2
2. Prerequisites.....	3
2.1. Array Networks AVX Network Functions Platform	3
2.2. Array Networks vAPV Series Application Delivery Controllers	3
2.3. Fortinet FortiGate VM virtual appliance	3
3. Network Topology	4
4. Deploying the vAPVs on AVX.....	5
4.1. Obtain the Image of the vAPV.....	5
4.2. Import the Image to the AVX appliance.....	5
4.3. Create a VA instance with the image on the AVX appliance	5
4.4. Assign Virtual Traffic ports to the VA instance.....	5
4.5. Start the VA instance	8
5. Deploying the FortiGate VM virtual appliances on AVX.....	9
5.1. Obtain the Image of the FortiGate VM.....	9
5.2. Import the Image to the AVX appliance.....	9
5.3. Create a VA instance with the image on the AVX appliance	9
5.4. Assign Virtual Traffic ports to the VA instance.....	9
5.5. Start the VA instance	12
6. Completing Initial Configuration for the vAPVs.....	13
7. Completing Initial Configuration for the FortiGate VM virtual appliances.....	18

1. Introduction

Array Networks AVX Series Network Functions Platforms host multiple Array and 3rd-party virtual appliances, providing the agility of cloud and virtualization with the guaranteed performance of dedicated appliances.

Array's AVX Series Network Functions Platform hosts up to 32 fully independent virtual appliances (VAs), including Array load balancing and SSL VPN as well as open-source VAs and 3rd-party VAs from leading networking and security vendors. Designed with managed service providers and enterprises in mind, the AVX Series enables data center consolidation without sacrificing the agility of cloud and virtualization or the performance of dedicated appliances. Uniquely capable of assigning dedicated CPU, SSL, memory and interface resources per VA, the AVX Series Network Functions Platform is the only solution to deliver guaranteed performance in shared environments.

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. A firewall sandwich is a deployment in which multiple firewalls are sandwiched between a pair of load balancers to improve availability, scalability, and manageability across the IT infrastructure.

The following sections will describe the steps required to deploy a firewall sandwich on the AVX Series Network Functions Platform.

The Array vAPV is a virtual application delivery controller that improves application availability, performance and security while enabling dynamic, flexible and elastic provisioning in cloud and virtual environments. The vAPV will be deployed on the AVX as a VA instance to provide firewall and server load balancing.

The Fortinet FortiGate Virtual Machine (VM) is a Next-Generation Firewall that offers flexible deployments from the network edge to the core, data center, internal segment, and the Cloud. FortiGate VM firewalls deliver scalable performance of advanced security services like Thread Protection, SSL inspection, and ultra-low latency for protecting internal segments and mission-critical environments. The FortiGate VM will be deployed on the AVX as a VA instance.

2. Prerequisites

The following are general prerequisites for this deployment guide.

2.1. Array Networks AVX Network Functions Platform

- One AVX Series 7600 Network Functions Platform running version ArrayOS 2.7.0.19 or later

The AVX appliance can be purchased from an authorized Array Networks reseller. For more information on deploying the AVX appliance, please refer to the AVX WebUI User Guide, which is accessible through the product's Web User Interface.

2.2. Array Networks vAPV Series Application Delivery Controllers

- One vAPV virtual appliance running version ArrayOS 8.6.1.80 or later for firewall load balancing
- One vAPV virtual appliance running version ArrayOS 8.6.1.80 or later for server load balancing

The vAPV appliances can be purchased from an authorized Array Networks reseller. For more information on deploying the vAPV appliance on the AVX appliance, please refer to the APV ArrayOS™ WebUI Guide, which is accessible through the product's Web User Interface.

2.3. Fortinet FortiGate VM virtual appliance

- Two FortiGate VM virtual appliances running version 6.0.2 or later. 2 x vCPU cores and (up to) 4 GB RAM

The FortiGate VM virtual appliances can be purchased from Fortinet. For more information on deploying the FortiGate VM for KVM, please visit <https://www.fortinet.com>.

Note: Assuming you have all these components, it should take roughly 2 hours to complete the entire configuration in this deployment guide.

3. Network Topology

Figure 1 shows a detailed configuration of the AVX/vAPV/Firewall Sandwich.

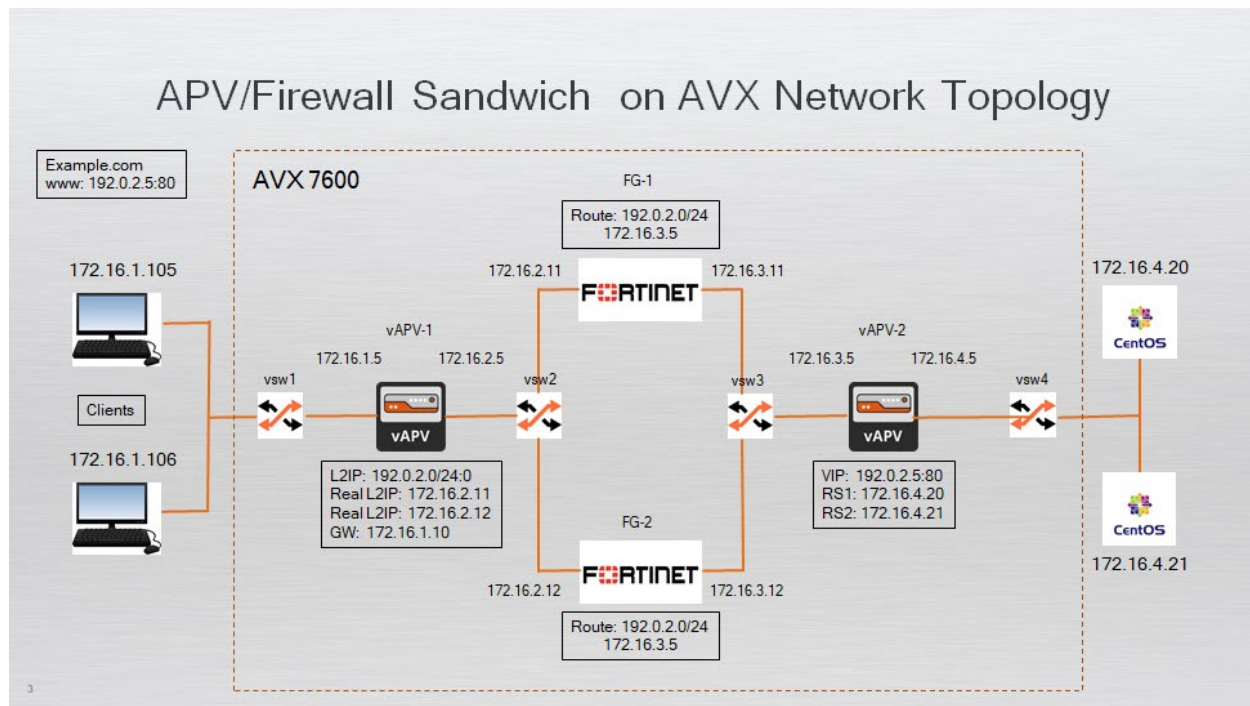


Figure 1 – Deployment Details

In this deployment, there are two vAPV load balancers, one (vAPV-1) to distribute traffic between the two firewalls and the other (vAPV-2) to distribute the client requests between the two web servers.

Since the firewall itself is not the intended destination of client connections, traffic must be transparently directed through the firewalls in both directions, inbound and outbound.

A virtual IP 192.0.2.5 on vAPV-2 is publicly known to the clients but all the real or private IP addresses for the web servers are masked.

The two vAPVs, two FortiGate VM virtual appliances and four AVX virtual switches are all deployed on the AVX appliance (see Figure 1 – the dotted lines represent the components inside the AVX7600).

Typical Traffic Flow: Inbound

The clients are Windows 10 machines external to the AVX. The web servers are CentOS machines external to the AVX.

The clients (on the left side) generate web server (on the right side) requests to the CentOS web servers via the firewall sandwich consisting of the firewall vAPV load balancer and the web server vAPV load balancer.

4. Deploying the vAPVs on AVX

To deploy the vAPVs on the AVX appliance, follow these steps:

1. Obtain the image of the vAPV
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

4.1. Obtain the Image of the vAPV

By default, the vAPV is already preloaded as a VA image on the AVX. If not, please contact Array Networks to obtain the image. Please consult the AVX Application Guide or AVX CLI Handbook for instructions on how to upload and create a VA instance.

Licenses are required for each VA instance. Please contact Array Networks Support or your authorized Array reseller to obtain licenses.

4.2. Import the Image to the AVX appliance

On the AVX WebUI, navigate to **VA Management > VA Image** to upload the vAPV image.

4.3. Create a VA instance with the image on the AVX appliance

On the AVX WebUI, navigate to **VA Management > VA** to create the VA instance using the vAPV image.

1. Create one vAPV VA instance named vAPV-1. vAPV-1 is the firewall load balancer.
2. Create a second vAPV VA instance named vAPV-2. vAPV-2 is the web server load balancer.

4.4. Assign Virtual Traffic ports to the VA instance

In this deployment, the AVX built-in virtual switches will be used to interconnect VAs. On the AVX WebUI, navigate to **Platform > Network > Virtual Switch** to create virtual switches.

1. Create a Virtual Switch named vsw1 and attach the vAPV-1 VA instance. Assign the Virtual Port Name to vport1. This port will represent the ingress port on vAPV-1.

Attach VA Instance to Virtual Switch

Virtual Switch Name
vsw1

VA Name
vAPV-1

Virtual Port Name
vport1

VLAN Tag
0

Enabled Queues
1

Save

2. Create a second Virtual Switch named vsw2 and attach the vAPV-1 VA instance. Assign the Virtual Port name to vport2. This port will represent the egress port on vAPV-1.

Attach VA Instance to Virtual Switch

Virtual Switch Name
vsw2

VA Name
vAPV-1

Virtual Port Name
vport2

VLAN Tag
0

Enabled Queues
1

Save

3. Create a third Virtual Switch named vsw3 and attach the vAPV-2 VA instance. Assign the Virtual Port name to vport3. This port will represent the ingress port on vAPV-2.

Attach VA Instance to Virtual Switch ×

Virtual Switch Name

vsw3

VA Name

vAPV-2

Virtual Port Name

vport3

VLAN Tag

0

Enabled Queues

1

Save

4. Create a fourth Virtual Switch named vsw4 and attach the vAPV-2 VA instance. Assign the Virtual Port name to vport4. This port will represent the egress port on vAPV-2.

Attach VA Instance to Virtual Switch ×

Virtual Switch Name

vsw4

VA Name

vAPV-2

Virtual Port Name

vport4

VLAN Tag

0

Enabled Queues













1

Save

4.5. Start the VA instance

On the AVX WebUI, navigate to **VA Management > VA** to start the VA instance.

1. Locate the VA instance named vAPV-1 and click on the ► symbol under the Action column to start the VA instance.
2. Locate the VA instance named vAPV-2 and click on the ► symbol under the Action column to start the VA instance.

VA Management										
No.	VA Name	IP Address	Product Name	Product Category	VA Size	Image	Vendor	Status	Boot Time	Action
	<input type="text" value="apv"/>	<input type="text" value="Search by IP"/>	<input type="text" value="Search by Product"/>	<input type="text" value="All"/>	<input type="text" value="/"/>	<input type="text" value="All"/>	<input type="text" value="All"/>	<input type="text" value="All"/>		
1	 vAPV-2	10.10.152.184	vAPV	 ADC	▪ entry	default	Array Networks	 Running	2018-12-14T00:13:54	
2	 vAPV-3	10.10.152.178	vAPV	 ADC	▪ entry	default	Array Networks	 Shutdown	N/A	
3	 vAPV-1	10.10.152.180	vAPV	 ADC	▪ entry	default	Array Networks	 Running	2018-12-19T00:20:39	

5. Deploying the FortiGate VM virtual appliances on AVX

To deploy the FortiGate VM virtual appliances on the AVX appliance, follow these steps:

1. Obtain the image of the FortiGate VM
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

Licenses are required for each VA instance. Please contact Fortinet to obtain licenses.

5.1. Obtain the Image of the FortiGate VM

Before deploying a FortiGate VM, please contact Fortinet to obtain the KVM image. KVM images can be directly uploaded to the AVX. Please consult the AVX Application Guide or AVX CLI Handbook for instructions on how to upload and create a VA instance.

Licenses are required for each VA instance. Please contact Fortinet to obtain licenses.

5.2. Import the Image to the AVX appliance

On the AVX WebUI, navigate to **VA Management > VA Image** to upload the FortiGate VM image.

5.3. Create a VA instance with the image on the AVX appliance

On the AVX WebUI, navigate to **VA Management > VA** to create the VA instance using the FortiGate VM image.

1. Create a FortiGate VM VA instance named FG-1. FG-1 is the first Firewall.
2. Create a second FortiGate VM VA instance named FG-2. FG-2 is the second Firewall.

5.4. Assign Virtual Traffic ports to the VA instance

The virtual switches were previously created in the “Deploying the vAPVs on AVX” section. In this section, virtual traffic ports need to be created and assigned to the FortiGate VM virtual appliances.

On the AVX WebUI, navigate to **Platform > Network > Virtual Switch**.

1. Click on the Virtual Switch named vsw2 and attach the FG-1 VA instance. Assign the Virtual Port Name to vport5. This port will represent the ingress port on FG-1.

×

Attach VA Instance to Virtual Switch

Virtual Switch Name

vsw2

VA Name

FG-1

Virtual Port Name

vport5

VLAN Tag

0

Enabled Queues

1

Save

- Click on the Virtual Switch named vsw2 and attach the FG-2 VA instance. Assign the Virtual Port Name to vport6. This port will represent the ingress port on FG-2.

×

Attach VA Instance to Virtual Switch

Virtual Switch Name

vsw2

VA Name

FG-2

Virtual Port Name

vport6

VLAN Tag

0

Enabled Queues

1

Save

- Click on the Virtual Switch named vsw3 and attach the FG-1 VA instance. Assign the Virtual Port Name to vport7. This port will represent the egress port on FG-1.

Attach VA Instance to Virtual Switch ×

Virtual Switch Name

VA Name

Virtual Port Name

VLAN Tag

Enabled Queues

- Click on the Virtual Switch named vsw3 and attach the FG-2 VA instance. Assign the Virtual Port Name to vport8. This port will represent the ingress port on FG-2.

×

Attach VA Instance to Virtual Switch

Virtual Switch Name

vsw3

VA Name

FG-2

Virtual Port Name

vport8

VLAN Tag

0

Enabled Queues







1

Save

5.5. Start the VA instance

On the AVX WebUI, navigate to **VA Management > VA** to start the VA instance.

1. Locate the VA instance named FG-1 and click on the ► symbol under the Action column to start the VA instance.
2. Locate the VA instance named FG-2 and click on the ► symbol under the Action column to start the VA instance.

VA Management										
<div> <div>↺</div> <div>+</div> </div>										
No.	VA Name	IP Address	Product Name	Product Category	VA Size	Image	Vendor	Status	Boot Time	Action
	FG	Search by IP	Search by Product	All	/	All	All	All		
1	 FG-2	10.10.152.182	XGFW	FW	* small	Fortigate-VA	Fortinet	 Running	2018-12-14T00:13:59	
2	 FG-1	10.10.152.186	XGFW	FW	* small	Fortigate-VA	Fortinet	 Running	2018-12-14T00:13:58	

6. Completing Initial Configuration for the vAPVs

After the vAPV VA instances are up, to complete the initial configuration, follow these steps:

1. Configure the IP address for the management interface (port1) on the firewall load balancer (vAPV-1) via the console.

```
# ip address port1 <your IP address> <your Netmask>
```

```
# ip route default <your Gateway IP>
```

2. Enable the WebUI access mode and save changes.

```
# webui on
```

```
# write memory
```

3. Configure the IP addresses for the ingress port (port2) as 172.16.1.5 and the egress port (port3) as 172.16.2.5 via the WebUI.

System Interface Bond Interface VLAN Interface MNET Interface Interface Configuration & Statistics

System Interface

Interface Name	Interface Type	Interface IP	Interface Status	Interface ID	MAC Address	MTU	Speed	Promiscuous Mode
port1	System	10.10.152.180	active	port1	fc:e1:fb:0a:a5:13	1500	autoselect (1000baseT <full-duplex >)	
port2	System	172.16.1.5	active	port2	fc:e1:fb:0a:a5:10	1500	10Gbase-T <full-duplex>	
port3	System	172.16.2.5	active	port3	fc:e1:fb:0a:a5:0f	1500	10Gbase-T <full-duplex>	

Show 10 entries

First Previous 1 Next Last

4. Configure the Default Route for the management interface (e.g. 10.10.152.1).

Default Route Static Route

Default Route

Gateway IP

IPv4

10.10.152.1

IPv6

5. Configure the SLB Virtual Service on vAPV-1 as follows:

```
# slb virtual l2ip "VS_HTTP_1" 172.16.1.5
```

SLB Virtual Service
SLB VLink

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	
L2 IP	VS_HTTP_1	N/A	172.16.1.5	N/A	More...

Show 10 entries

First Previous 1 Next Last

6. Configure the SLB Real Services on vAPV-1 as follows:

```
# slb real l2ip "RS_WEB_1" 172.16.2.11
```

```
# slb real l2ip "RS_WEB_2" 172.16.2.12
```

SLB Real Service
SLB Real Service Group
SLB Health Check
SLB Group Health Check
Database Server Health Check

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 Name	Real Service Type	Enable Real Service	Force Offline	IP/Domain Name	Port	Up/Down Status
RS_WEB_2	L2 IP	✓	N/A	172.16.2.12	N/A	✓
RS_WEB_1	L2 IP	✓	N/A	172.16.2.11	N/A	✓

Show 10 entries

First Previous 1 Next Last

7. Configure the SLB Real Service Group on vAPV-1 as follows:

```
# slb group method "GROUP_HTTP_1" chi direct default
```

```
# slb group member "GROUP_HTTP_1" "RS_WEB_1"
```

```
# slb group member "GROUP_HTTP_1" "RS_WEB_2"
```

SLB Real Service Group



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.

	ADD	DELETE	Clear HTTP2	Group Method	All	Search	
<input type="checkbox"/>	Group Name	Group Method	Number of Active Real Services	Enable Group	Protocol	Group Members	
<input type="checkbox"/>	GROUP_HTTP_1	Layer 2 Consistent Hash IP	0	<input checked="" type="checkbox"/>	l2ip	RS_WEB_1 RS_WEB_2	More...
Show 10 entries				First	Previous	1	Next Last

- Configure the SLB default Policy on vAPV-1 as follows:

```
# slb policy default "VS_HTTP_1" "GROUP_HTTP_1"
```

Policy



Policy establishes a mapping between the virtual service and the real service group.

	ADD	DELETE	Policy Type	All	Search	
<input type="checkbox"/>	Policy Type	Policy Name	Virtual Service	Associated Groups		
<input type="checkbox"/>	Default	Default Policy of VS_HTTP_1	VS_HTTP_1	GROUP_HTTP_1		
Show 10 entries				First	Previous	1 Next Last

- Configure the IP address for the management interface (port1) on the web server load balancer (vAPV-2) via the console.

```
# ip address port1 <your IP address> <your Netmask>
```

```
# ip route default <your Gateway IP>
```

- Enable the WebUI access mode and save changes.

```
# webui on
```

```
# write memory
```

- Configure the IP addresses for the ingress port (port2) as 172.16.3.5 and the egress port (port3) as 172.16.4.5.

System Interface

Interface Name	Interface Type	Interface IP	Interface Status	Interface ID	MAC Address	MTU	Speed	Promiscuous Mode
port1	System	10.10.152.184	active	port1	fc:e1:fb:0a:a5:12	1500	autoselect (1000baseT <full-duplex >)	
port2	System	172.16.3.5	active	port2	fc:e1:fb:0a:a5:0c	1500	10Gbase-T <full-duplex>	
port3	System	172.16.4.5	active	port3	fc:e1:fb:0a:a5:0b	1500	10Gbase-T <full-duplex>	

Show 10 entries

First Previous 1 Next Last

12. Configure the Default Route for the management interface (e.g. 10.10.152.1).

Default Route

Gateway IP

IPv4

10.10.152.1

IPv6

13. Configure the SLB Virtual Service on vAPV-2 as follows:

```
# slb virtual http "VS_HTTP_1" 192.0.2.5 80 arp 0
```

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	
HTTP	VS_HTTP_1	<input checked="" type="checkbox"/>	192.0.2.5	80	More...

Show 10 entries

First Previous 1 Next Last

14. Configure the SLB Real Service on vAPV-2 as follows:

```
# slb real http "RS_WEB_1" 172.16.4.20 80 1000 icmp 3 3
# slb real http "RS_WEB_2" 172.16.4.21 80 1000 icmp 3 3
```

SLB Real Service
SLB Real Service Group
SLB Health Check
SLB Group Health Check
Database Server Health Check

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 Name	Real Service Type	Enable Real Service	Force Offline	IP/Domain Name	Port	Up/Down Status	
RS_WEB_1	HTTP	✓	N/A	172.16.4.20	80	✓	More...
RS_WEB_2	HTTP	✓	N/A	172.16.4.21	80	✓	More...

Show 10 entries

First Previous 1 Next Last

15. Configure the SLB Real Service Group on vAPV-2 as follows:

```
# slb group method "GROUP_HTTP_1" rr
# slb group member "GROUP_HTTP_1" "RS_WEB_1" 1 0
# slb group member "GROUP_HTTP_1" "RS_WEB_2" 2 0
```

16. Configure the SLB default Policy on vAPV-2 as follows:

```
# slb policy default "VS_HTTP_1" "GROUP_HTTP_1"
```

Policy
Static Policy

Policy

Policy establishes a mapping between the virtual service and the real service group.

Policy Type	Policy Name	Virtual Service	Associated Groups
Default	Default Policy of VS_HTTP_1	VS_HTTP_1	GROUP_HTTP_1

Show 10 entries

First Previous 1 Next Last

7. Completing Initial Configuration for the FortiGate VM virtual appliances

After the FortiGate VM virtual appliances are up, to complete the initial configuration, follow these steps:

1. Login into the FG-1 console with the username “admin”. By default, there is no password. Just press **Enter**.
2. Configure the IP address for the management interface (port3) on FG-1.
3. Configure the network settings (ingress = port1, egress = port 2) as follows:

```
config system interface
  edit port1
    set ip 172.16.2.11 255.255.255.0
    set allowaccess ping https ssh http fgfm
  end
  edit port2
    set ip 172.16.3.11 255.255.255.0
    set allowaccess ping https ssh http fgfm
  end
  edit port3
    set ip 10.10.152.182 255.255.255.0
    set allowaccess ping https ssh http fgfm
  end
end
```

4. Login to the FG-1 WebUI and confirm the network settings for port1 and port2.

FortiGate VM64-KVM

FGVM02TM18000791

Dashboard
Security Fabric
FortiView
Network
Interfaces
DNS
Packet Capture
SD-WAN
Performance SLA
SD-WAN Rules
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System
Policy & Objects
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report
Monitor

Edit Interface

Interface Name
port1 (FC:E1:FB:0A:A5:08)
Alias
Link Status
Up
Type
Physical Interface

Estimated Bandwidth
0 kbps Upstream
0 kbps Downstream

Tags

Role
WAN

Add Tag Category

Address

Addressing mode
Manual DHCP
IP/Network Mask
172.16.2.11/255.255.255.0

Administrative Access

IPv4

☒ HTTPS
☒ HTTP
☒ PING
☒ FMG-Access
☐ CAPWAP
☒ SSH
☐ SNMP
☐ FTM
☐ RADIUS Accounting
☐ FortiTelemetry

Miscellaneous

Scan Outgoing Connections to Botnet Sites
Disable Block Monitor

Secondary IP Address

Status

Comments

Interface State
Enabled Disabled

OK

Cancel

FortiGate VM64-KVM

FGVM02TM18000791

Dashboard
Security Fabric
FortiView
Network
Interfaces
DNS
Packet Capture
SD-WAN
Performance SLA
SD-WAN Rules
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System
Policy & Objects
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report
Monitor

Edit Interface

Interface Name
port2 (FC:E1:FB:0A:A5:07)
Alias
Link Status
Up
Type
Physical Interface

Tags

Role
LAN

Add Tag Category

Address

Addressing mode
Manual DHCP Dedicated to FortiSwitch
IP/Network Mask
172.16.3.11/255.255.255.0

Administrative Access

IPv4

☒ HTTPS
☒ HTTP
☒ PING
☒ FMG-Access
☐ CAPWAP
☒ SSH
☐ SNMP
☐ FTM
☐ RADIUS Accounting
☐ FortiTelemetry

DHCP Server

Networked Devices

Device Detection
Active Scanning

Admission Control

Security Mode
None

Secondary IP Address

Status

OK

Cancel

©2019 Array Networks, Inc. All Rights Reserved.

19

5. Add the following Static Routes:

FortiGate VM64-KVM FGVMO2TM18000791			
Dashboard	+ Create New Edit Clone Delete		
Security Fabric			
FortiView			
Network			
Interfaces	0.0.0.0/0	172.16.2.5	port1
DNS	192.0.2.0/24	172.16.3.5	port2
Packet Capture	192.168.1.0/24	172.16.2.5	port1
SD-WAN	0.0.0.0/0	10.10.152.1	port3
Performance SLA			
SD-WAN Rules			
Static Routes			
Policy Routes			

6. Configure the IPv4 Policy for port1 (WAN) to port2 (LAN) traffic as follows:

FortiGate VM64-KVM FGVMO2TM18000791	
Dashboard	Edit Policy
Security Fabric	
FortiView	
Network	
System	
Policy & Objects	
IPv4 Policy	
IPv4 DoS Policy	
Addresses	
Wildcard FQDN Addresses	
Internet Service Database	
Services	
Schedules	
Virtual IPs	
IP Pools	
Traffic Shapers	
Traffic Shaping Policy	
Security Profiles	
VPN	
User & Device	
WiFi & Switch Controller	
Log & Report	
Monitor	

Name

WAN to LAN

Incoming Interface

port1

Outgoing Interface

port2

Source

all

Destination

all

Schedule

always

Service

ALL

Action

ACCEPT DENY

Firewall / Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address Use Dynamic IP Pool

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

SSL Inspection

Logging Options

Log Allowed Traffic

Generate Logs when Session Starts

Capture Packets

Security Events All Sessions

Comments

Write a comment...

OK

Cancel

7. Configure the IPv4 Policy for port2 (LAN) to port1 (WAN) traffic as follows:

The screenshot shows the FortiGate VM64-KVM web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects (selected), IPv4 Policy (selected), IPv4 DoS Policy, Addresses, Wildcard FQDN Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Traffic Shapers, Traffic Shaping Policy, Security Profiles, VPN, User & Device, WiFi & Switch Controller, Log & Report, and Monitor. The main content area is titled 'Edit Policy' and displays the configuration for a policy named 'LAN to WAN'. The configuration includes: Incoming Interface: port2, Outgoing Interface: port1, Source: all, Destination: all, Schedule: always, Service: ALL, and Action: ACCEPT (checked) and DENY (unchecked). Below the policy configuration, there are sections for Firewall / Network Options (NAT is checked, IP Pool Configuration is 'Use Outgoing Interface Address'), Security Profiles (Antivirus, Web Filter, DNS Filter, Application Control, IPS, and SSL Inspection are all unchecked), and Logging Options (Log Allowed Traffic is checked, Security Events and All Sessions are selected, Generate Logs when Session Starts is unchecked, and Capture Packets is unchecked). At the bottom, there is a 'Comments' field with the text 'Write a comment...' and a character count of 0/1023. The bottom right corner has 'OK' and 'Cancel' buttons.

8. Login into the FG-2 console with the username “admin”. By default, there is no password. Just press **Enter**.

9. Configure the IP address for the management interface (port3) on FG-2.

10. Configure the network settings (ingress = port1, egress = port 2) as follows:

```
config system interface
  edit port1
    set ip 172.16.2.12 255.255.255.0
    set allowaccess ping https ssh http fgfm
  end
  edit port2
    set ip 172.16.3.12 255.255.255.0
    set allowaccess ping https ssh http fgfm
  end
  edit port3
    set ip 10.10.152.186 255.255.255.0
    set allowaccess ping https ssh http fgfm
  end
end
```

11. Login to the FG-2 WebUI and confirm the network settings for port1 and port2.

FortiGate VM64-KVM FGVMM02TM18000878

Dashboard > **Edit Interface**

Security Fabric >

FortiView >

Network >

Interfaces ☆

DNS

Packet Capture

SD-WAN

Performance SLA

SD-WAN Rules

Static Routes

Policy Routes

RIP

OSPF

BGP

Multicast

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

WiFi & Switch Controller >

Log & Report >

Monitor >

Interface Name: port1 (FC:E1:FB:0A:A4:12)

Alias:

Link Status: Up

Type: Physical Interface

Estimated Bandwidth: kbps Upstream kbps Downstream

Tags

Role: WAN

Address

Addressing mode: **Manual** DHCP

IP/Network Mask:

Administrative Access

IPv4 ☒ HTTPS ☒ HTTP ☒ PING ☒ FMG-Access

☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM

☐ RADIUS Accounting ☐ FortiTelemetry

Miscellaneous

Scan Outgoing Connections to Botnet Sites: **Disable** Block Monitor

☐ Secondary IP Address

Status

Comments:

Interface State: **Enabled** Disabled

OK **Cancel**

FortiGate VM64-KVM FGVMM02TM18000878

Dashboard > **Edit Interface**

Security Fabric >

FortiView >

Network >

Interfaces ☆

DNS

Packet Capture

SD-WAN

Performance SLA

SD-WAN Rules

Static Routes

Policy Routes

RIP

OSPF

BGP

Multicast

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

WiFi & Switch Controller >

Log & Report >

Monitor >

Interface Name: port2 (FC:E1:FB:0A:A4:11)

Alias:

Link Status: Up

Type: Physical Interface

Tags

Role: LAN

Address

Addressing mode: **Manual** DHCP Dedicated to FortiSwitch

IP/Network Mask:

Administrative Access

IPv4 ☒ HTTPS ☒ HTTP ☒ PING ☒ FMG-Access

☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM

☐ RADIUS Accounting ☐ FortiTelemetry

☐ DHCP Server

Networked Devices

Device Detection:

Admission Control

Security Mode: None

☐ Secondary IP Address

Status

Comments:

OK **Cancel**

12. Add the following Static Routes:

FortiGate VM64-KVM FGVMO2TM18000878			
Dashboard	>	+ Create New Edit Clone Delete	
Security Fabric	>		
FortiView	>		
Network	>	0.0.0.0/0	172.16.2.5
Interfaces	>	192.0.2.0/24	172.16.3.5
DNS	>	192.168.1.0/24	172.16.2.5
Packet Capture	>	0.0.0.0/0	10.10.152.1
SD-WAN	>		
Performance SLA	>		
SD-WAN Rules	>		
Static Routes	>		
Policy Routes	>		

13. Configure the IPv4 Policy for port1 (WAN) to port2 (LAN) traffic as follows:

FortiGate VM64-KVM FGVMO2TM18000791	
Dashboard	> Edit Policy
Security Fabric	>
FortiView	>
Network	>
System	>
Policy & Objects	>
IPv4 Policy	>
IPv4 DoS Policy	>
Addresses	>
Wildcard FQDN Addresses	>
Internet Service Database	>
Services	>
Schedules	>
Virtual IPs	>
IP Pools	>
Traffic Shapers	>
Traffic Shaping Policy	>
Security Profiles	>
VPN	>
User & Device	>
WiFi & Switch Controller	>
Log & Report	>
Monitor	>

Name: WAN to LAN

Incoming Interface: port1

Outgoing Interface: port2

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT DENY

Firewall / Network Options

NAT: ON

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Security Profiles

AntiVirus: OFF

Web Filter: OFF

DNS Filter: OFF

Application Control: OFF

IPS: OFF

SSL Inspection: OFF

Logging Options

Log Allowed Traffic: ON Security Events All Sessions

Generate Logs when Session Starts: OFF

Capture Packets: OFF

Comments: Write a comment...

OK Cancel

14. Configure the IPv4 Policy for port2 (LAN) to port1 (WAN) traffic as follows:

FortiGate VM64-KVM

FGVM02TM18000791

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPv4 Policy

IPv4 DoS Policy

Addresses

Wildcard FQDN Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Traffic Shapers

Traffic Shaping Policy

Security Profiles

VPN

User & Device

WiFi & Switch Controller

Log & Report

Monitor

Edit Policy

Name

LAN to WAN

Incoming Interface

port2

Outgoing Interface

port1

Source

all

Destination

all

Schedule

always

Service

ALL

Action

ACCEPT

DENY

Firewall / Network Options

NAT

Use Outgoing Interface Address

Use Dynamic IP Pool

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

SSL Inspection

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Generate Logs when Session Starts

Capture Packets

Comments

Write a comment...

OK

Cancel

©2019 Array Networks, Inc. All Rights Reserved.

25

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