

Purpose	4
POC Setup	4
Network Diagram	5
Traffic Flows	5
Deployment With Terraform:	6
Verify the routing reachability	7
Activate fortiadc license with TFTP server	8
Deploy Manually	9
Create VPC fortiADC VM	10
vswitches	10
Route table	10
Create FortiADC VM	11
Build fortiadc custom image	11
Create instance with custom image ID	13
Add Tag	13
VM in FortiADC VPC	14
Create HUBVPC	14
HUBVPC	15
vSwitches	15
internal vswitch	15
external vswitch	15
TR-landing vswitch	15
Routing Tables	16
TR-landing routing table	17
custom routing table	17
Create Fortigate instance	19
Create Fortigate with image from the marketplace.	19
ENI ports	19
Create Client-VM	20
Add Tag	20
VMs in HUBVPC	21
Create ACK1VPC	22
Create VPC for ACK1	22
CIDR: 10.0.0.0/8	22
Vswitch	22
ACK1 VPC route table	22

Component created by ACK	27
install kubectl on client VM	28
Deploy application on ACK1	29
Create ACK2	31
Create and Config CEN-TR	31
TR Connections	32
Route Table- defaul-north-south	32
route table association	32
Remove Route Propagation	33
route entry	33
Route Table east-west	34
route table association	34
Enable Route Propagation	34
The route Entry	35
Config Fortigate VIP for access FortiADC	36
GUI access VIP mapping	36
Firewall Policy	36
Create a policy to allow this traffic	36
SSH access VIP mapping	37
Firewall Policy	38
Config Fortigate VIP for access client-VM	39
Firewall policy	40
Config Fortigate Routing	40
Config static Route	40
Config Firewall Policy for East-west traffic and ACK egress traffic to internet	41
Verify the reachability	43
ACK1 to ACK2	43
ACK1 POD and Node IP	44
ACK2 POD and Node IP	44
Ping Result	44
FortiGate View	46
enable security feature for egress traffic.	46
Config FortiADC as Ingress controller	47
Config FortiADC to connect ACK1 and ACK2	48
Create ServiceAccount on both ACK	48
config k8s sdn connector on fortiADC	49
Create ingress rule for ACK1 nodeport service	52
Create a Real Server Pool on FortiADC	52
Create Layer 7 Ingress Rule with RealServer Pool	54
Associate with WAF profile	56

Enable Monitoring	56
Verify the result	57
Access via fortiadc internal IP address (from client-vm)	57
access via fortiadc external IP	58
Access via Fortigate public IP if fortiadc has no public IP associated	58
Create a Virtual IP on fortigate	59
create virtual IP 0.0.0.0:8080 to map to 10.0.11.11:8080	59
Verify the result	60
scale out the node on ACK1	61
simulate the attack to nodeport service via ingress entry	61
Config FortiGate K8s Connector	62
Config K8S Connector	63
get the cluster IP and SA secret from ACK1 and ACK2	63
Config k8s connector on fortigate	65
Create Firewall Policy based on dynamic object	67
Define the Address object	67
create firewall policy	68

Purpose

Enterprises often want to have a central control to all traffic including both VM and Container traffic. and may also like to deploy or reuse existing fortiADC appliance/vm as ingress controller or load balancer for both ACK and VM workload.

Below POC shows Fortinet leverages Next Generation Firewall Fortigate and Application Controller FortiADC to secure Enterprise ACK workload. In the Setup, FortiGate L3-L7 packet inspection for East-West and North-South traffic , Fortigate k8s SDN connector, FortiADC k8s SDN connector, FortiADC L7 LB as Ingress controller feature are detailed.

POC Setup

Here are the all components that are used in this POC Setup.

VPCs : 4

Public IP : 2 (one for fortigate, one for fortiadvc)

ACK : 2

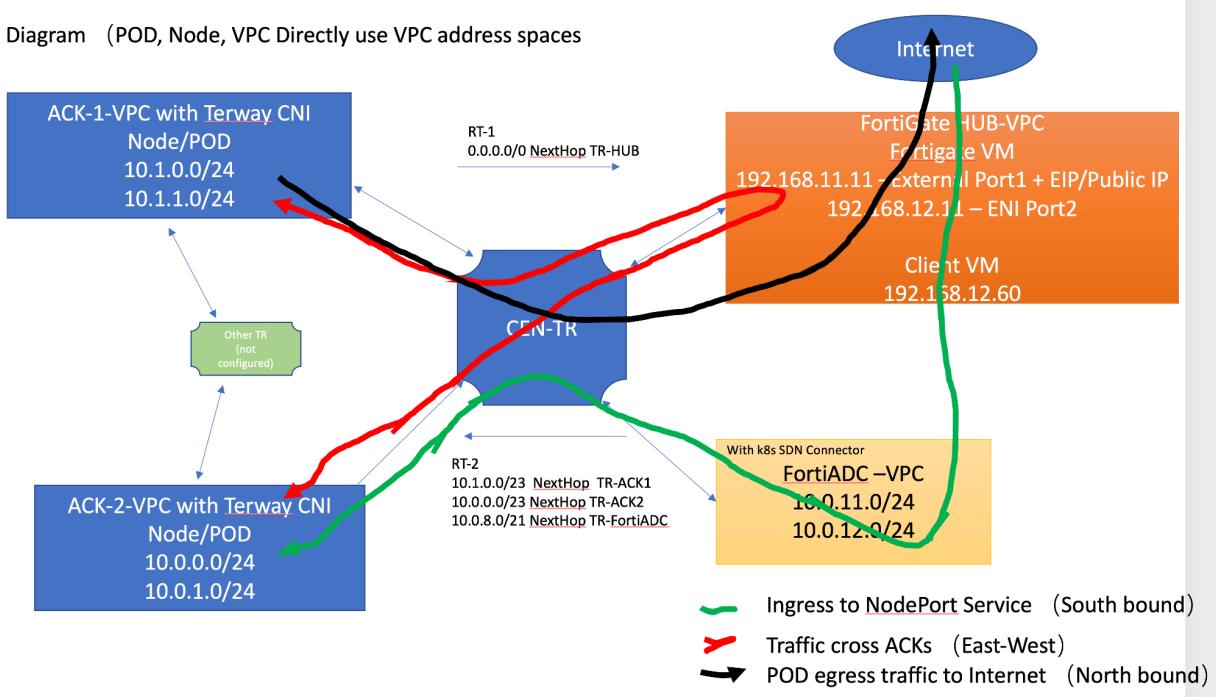
Alibaba SLB : 2 (created as part of each ACK, for ACK API access)

FortiADC VM : 1

Ubuntu Client VM :1

CEN-TR: 1 (attached to all 4 VPCs)

Network Diagram



Traffic Flows

CEN-TR0:

CEN-TR is attached to all 4 VPCs and as a central router to route the traffic between VPCs (East-West) and Internet bound traffic (North-South).

East-West Traffic :

Traffic between POD1 in ACK1 and POD2 in ACK2 is routed through FortiGate in HubVPC via CEN-TR0.

POD egress traffic:

All POD egress traffic is routed through Fortigate via CEN-TR0.

ACK1 ,ACK2 ingress Traffic:

Ingress to ACK1 and ACK2 service is via FortiADC Ingress controller for internal visit and external visit (when fortiadc associated a public IP) ,
FortiGate is used to take external traffic to ACK1, ACK2 , DNAT to FortiADC then to ACK Cluster when FortiADC does not have a public IP associated.

L7 Firewall Policy on Fortigate is used to inspect traffic between POD1 and POD2 (across VPCs). as well as POD egress traffic to the Internet. Fortigate is the central point for inspect traffic across ACKs and North-South traffices.

FortiADC is used as Ingress controller ,Layer 7 Ingress rule is configured on FortiADC to take ingress traffic to NodePort Type service on ACK1 and ACK2.

Traffic within ACK1 and ACK2 is subject to control by Alibaba Terway CNI with Network Policy.

Deploy With Terraform:

```
git clone git@github.com:yagosys/fortinet_alibaba.git
cd securehub_ack
terraform apply
```

follow the instructions in the README file.

after deployment, you shall see following similar output at the console

Outputs:

```
FortigateAdminGUI_PORT = "8443"
PrimaryFortigateAvailability_zone = "cn-hongkong-b"
PrimaryFortigateID = "i-j6c8ukmv8inb7eul5ik5"
PrimaryFortigatePrivateIP = "192.168.11.11"
PrimaryFortigatePublicIP = "47.242.124.76"
PrimaryFortigateport2IP = "192.168.12.11"
ack1_worknode_ip = tolist([
    "10.1.0.164",
    "10.1.0.163",
])
ack2_worknode_ip = tolist([
    "10.0.0.250",
    "10.0.0.251",
])
client-vm = "192.168.12.60"
client-vm-password = "Welcome.123"
client-vm-ssh-port = "2022"
fortiadc_gui_https_port = 9443
```

```
fortiadc_instance_id = "i-j6c8ukmv8inb7eul5ik6"
fortiadc_private_ip = "10.0.11.11"
fortiadc_public_ip = "47.243.181.129"
fortiadc_ssh_port = 6022
```

Verify the routing reachability

client-vm shall be able to ping all endpoints in the topology. which include fortigate internal IP, fortiadc IP, ack1 and ack2 worker-node IP.

```
(base) i@ecs-148531:~/fortinet/cen-tr-ack$ ssh root@47.242.124.76 -p 2022
Warning: Permanently added '[47.242.124.76]:2022' (ECDSA) to the list of
known hosts.
root@47.242.124.76's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Super-optimized for small spaces - read how we shrank the memory
 footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation
New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

Welcome to Alibaba Cloud Elastic Compute Service !

```
Last login: Tue Feb 22 16:17:02 2022 from 192.168.12.11
root@iZj6cg0w474i2p8oykt7kqZ:~# ping 192.168.11.11 -c 1
PING 192.168.11.11 (192.168.11.11) 56(84) bytes of data.
64 bytes from 192.168.11.11: icmp_seq=1 ttl=255 time=0.358 ms

--- 192.168.11.11 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
```

```
rtt min/avg/max/mdev = 0.358/0.358/0.358/0.000 ms
root@iZj6cg0w474i2p8oykt7kqZ:~# ping 10.1.0.164 -c 1
PING 10.1.0.164 (10.1.0.164) 56(84) bytes of data.
64 bytes from 10.1.0.164: icmp_seq=1 ttl=63 time=1.59 ms

--- 10.1.0.164 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.593/1.593/1.593/0.000 ms
root@iZj6cg0w474i2p8oykt7kqZ:~# ping 10.1.0.163 -c 1
PING 10.1.0.163 (10.1.0.163) 56(84) bytes of data.
64 bytes from 10.1.0.163: icmp_seq=1 ttl=63 time=1.49 ms

--- 10.1.0.163 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.496/1.496/1.496/0.000 ms
root@iZj6cg0w474i2p8oykt7kqZ:~# ping 10.0.0.250 -c 1
PING 10.0.0.250 (10.0.0.250) 56(84) bytes of data.
64 bytes from 10.0.0.250: icmp_seq=1 ttl=63 time=1.65 ms

--- 10.0.0.250 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.651/1.651/1.651/0.000 ms
root@iZj6cg0w474i2p8oykt7kqZ:~# ping 10.0.0.251 -c 1
PING 10.0.0.251 (10.0.0.251) 56(84) bytes of data.
64 bytes from 10.0.0.251: icmp_seq=1 ttl=63 time=1.86 ms

--- 10.0.0.251 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.861/1.861/1.861/0.000 ms
root@iZj6cg0w474i2p8oykt7kqZ:~# ping 10.0.11.11 -c 1
PING 10.0.11.11 (10.0.11.11) 56(84) bytes of data.
64 bytes from 10.0.11.11: icmp_seq=1 ttl=63 time=1.39 ms

--- 10.0.11.11 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.393/1.393/1.393/0.000 ms
root@iZj6cg0w474i2p8oykt7kqZ:~#
```

Activate fortiadc license with TFTP server

The Fortigate has already applied with License and configuration file, however, the terraform script does not support fortiadc cloud init, therefore, we have to manually apply license to fortiadc. There are two ways to activate the fortiadc license, use command line or use GUI. If we use the command line, a TFTP server is required which our client-VM has already configured as a TFTP server. so we can use clientVM as a tftp server to configure the license.

```
(base) i@ecs-148531:~/fortinet/cen-tr-ack$ ssh admin@47.242.124.76 -p 6022
Warning: Permanently added '[47.242.124.76]:6022' (ECDSA) to the list of
known hosts.
admin@47.242.124.76's password:
You are forced to change your password, please input a new password.
New Password: *****
Confirm Password: *****
FortiADC-ALI # execute vm license up
<Enter>

FortiADC-ALI # execute vm license tftp FADLICENSE.lic 192.168.12.60
This operation will replace the current vmware license and reload the
system!
Do you want to continue? (y/n)y

Connect to tftp server 192.168.12.60 ...
Please wait...

Get vmware license file from tftp server OK.
Connection to 47.242.124.76 closed by remote host.
```

Deploy Manually

Below is for how to manually provision entire infrastructure without using terraform

Create VPC and fortiADC VM

FortiADC VPC has CIDR block 10.0.0.0/8 and two vswitches with subnet 10.0.12.0/24 and 10.0.11.0/24 , FortiADC VM is on vswitch 10.0.11.0/24. vswitch 10.0.12.0/24 is created for attach to CEN-TR purpose. as CEN-TR requires minimal 2 vswitch attachment.

VPC / VPCs / vpc-j6cfzg9nxbu4506rzsy

← vpc-j6cfzg9nxbu4506rzsy

Information Resources CIDs Authorize Cross Account Attach CEN Advanced Features

VPC Details

ID	vpc-j6cfzg9nxbu4506rzsy Copy	Name	fortiadc-qccy Edit
IPv4 CIDR Block	10.0.0.0/16 (Primary)	Created At	Feb 22, 2022, 15:45:06
IPv6 CIDR Block	Enable IPv6 CIDR Block	Status	✓ Available
Tags	-	Description	- Edit
Default VPC	No	Instance Attachment Details	CEN ID:cen-wjow07frhq7t266ws Owner Account:1671278556116611 Status:attached
Region	China (Hong Kong)	Resource Group	默认资源组
Owner Account UID	Current Account		

vRouter Basic Information

ID	vrt-j6c719qpapp2s7kewpy02 Copy	Name	- Edit
Created At	Feb 22, 2022, 15:45:06	Description	- Edit

vswitches

VPC / vSwitch

vSwitch

Create vSwitch VPC ID vpc-j6cfzg9nxbu4506rzsy [Create](#) [Q](#) Filter by Tag

Instance ID/Name	VPC	Tags	Status	IPv4 CIDR Block	Available IP Addresses	IPv6 CIDR Block	Default vSwitch	Zone	Route Table
vsw-j6c1y0eds8xmfplst7719 fortiadc_vswitch2_in...	vpc-j6cfzg9nxbu4506rzsy fortiadc-qccy		✓ Available	10.0.12.0/24	251	Enable IPv6 CIDR Block	No	Hong Kong Zone C	vtb-j6chc7mr06zjos8scx4df
vsw-j6cc1z61pdhqzb77aii fortiadc_vswitch1_in...	vpc-j6cfzg9nxbu4506rzsy fortiadc-qccy		✓ Available	10.0.11.0/24	250	Enable IPv6 CIDR Block	No	Hong Kong Zone B	vtb-j6chc7mr06zjos8scx4df

Route table

FortiADC VPC has one system default routing table with default route point to CEN-TR.

The screenshot shows the Alibaba Cloud VPC Route Tables interface. At the top, there's a search bar with 'VPC ID' set to 'vpc-j6cfzg9nxbu4506rzsy' and a 'Filter by Tag' button. Below the search bar is a table with columns: Instance ID/Name, VPC, Tags, vRouter ID, Route Table Type, and Associate Resource. One row is selected, showing 'vtb-j6chc7mr06zjos8scx4df' as the instance ID, 'vpc-j6cfzg9nxbu4506rzsy' as the VPC, and 'fortiadc-gpv' as the tag. The 'Route Table Type' is 'System' and the 'Associate Resource' is 'vSwitch vsw-j6cl1y0eds8xmfpfa7719.vsw-j6cc1z81pdhqzbb77ai'. There's also a 'Configure Tags' button.

Below the table, the URL is 'VPC / Route Tables / vtb-j6chc7mr06zjos8scx4df'. A back arrow and the route table name 'vtb-j6chc7mr06zjos8scx4df' are displayed.

The 'Route Table Details' section shows the following information:

- Route Table ID:** vtb-j6chc7mr06zjos8scx4df [Copy](#)
- Name:** [Edit](#)
- Tags:** [Edit](#)
- Created At:** Feb 22, 2022, 15:45:06
- VPC ID:** vpc-j6cfzg9nxbu4506rzsy [Copy](#)
- Route Table Type:** System
- Associated Resource Type:** vSwitch
- Description:** [Edit](#)

Below this, there are tabs for 'Route Entry List' and 'Associated vSwitch'. The 'Custom Route' tab is selected, showing a table with columns: Destination CIDR Block, Status, Next Hop, Type, and Description. One entry is listed: '0.0.0.0/0 tf-default_to_tr' with status 'Available', next hop 'tr-attach-wecgg6d2egyyz49tdw' (with a 'Delete' link), type 'Custom Route', and description '-'.

Create FortiADC VM

FortiADC is not available on alibaba marketplace, therefore, build a custom image for fortiadc on alibaba cloud is required.

Build fortiadc custom image

official document

<https://docs.fortinet.com/document/fortiadc-public-cloud/latest/alibaba-cloud-deployment-guide>

you must have an existing Alibaba Cloud Account to enable you to use Alibaba Cloud products. Get a released image from Fortinet <https://support.fortinet.com/Download/FirmwareImages.aspx> with file name something like "XXX.FORTINET.out.ali.zip", then unzip this file to get boot.vpc

FAD_ALI-V700-build0014-FORTINET.out	117,854	2022-02-01 09:02:57	2022-02-01 09:02:10	HTTPS Checksum
FAD_ALI-V700-build0014-FORTINET.out.ali.zip	117,513	2022-02-01 09:02:21	2022-02-01 09:02:32	HTTPS Checksum

Upload boot.vpc file to OSS and obtain the URL for download

Object Storage Service / Buckets / **fortiweb-for-sap** / Files

View Details

Preview is not available for this format.

File Name: boot.vpc

ETag: 8704D7EED793AD6E7097BF76FA23EA59

Validity Period (Seconds): 300

HTTPS:

URL: <https://fortiweb-for-sap.oss-cn-hongkong.aliyuncs.com/fortiadc/boot.vpc?Expires=164506457&OSSAccessKeyId=TmP-39uL8p-2oVrG-CxLyVQjUmNkmbfTcaesExd47dTBe64W-3WNaDwASa2B72EfZz75fY-CRA1Ymc2GFMBc73qBfAxCjQ2BhoSH8&Signature=g3sTy5NpM3RNH2xdflsJx6mgIg%3D>

Storage Class: application/octet-stream

File ACL: Inherited from Bucket

Set HTTP Header

Set ACL

Storage Class: Standard

Server-side Encryption: None

Import Image from URL

Import Image

Before you import or export an image, take note of the following items:

1. Perform the following: [Activate OSS](#)
2. Make sure that an OSS bucket has been created in the region where the image is to be exported.
3. Make sure that you have authorized ECS to access your OSS resources. [Verify](#)
4. Before you import or export an image, the requirements must be met as described in [Requirements for custom images](#)
5. Note: Community-supported FreeBSD kernel versions are compatible only with 4th-generation or earlier ECS instance types. You can patch the images of community-supported FreeBSD kernel versions to make the images compatible with all ECS instance types before you import the images. [Learn More](#)

Region of Image: China (Hong Kong)

OSS Object Address: <https://fortiweb-for-sap.oss-cn-hongkong.aliyuncs.com/fortiadc/boot.vpc?Expires=164506457>

Image Family: [Create Image](#) [Create Now](#) [U](#)

Custom Image [Public Image](#)

Image Name: fortiadc7.0

Operating System/Platform: Linux [CentOS](#)

System Architecture: x86_64

System Disk (GiB): 50

Image Format: VHD

License Type: Auto

Description: Enter keywords

Add Data Disk Image

Resource Group: Select

you will got the image after a few minutes

The screenshot shows the AWS Lambda console interface. At the top, there are tabs for 'Custom Image', 'Public Image', 'Shared Image', 'Marketplace Images', and 'Community Image'. The 'Custom Image' tab is selected. On the left, there's a sidebar with 'Image Family' and a search bar. The main area has a table with columns: ID/Name, Image Family, Tag, Operating System, Platform, Bit Size of OS, Status(All), Progress, Creation Time, and Actions. One row is visible: 'm-j6ce5v0kaxlyrw1vvoup' (ID/Name), 'Not Specified' (Tag), 'CentOS' (Operating System), '64bit' (Bit Size of OS), 'Available' (Status), '100%' (Progress), 'Feb 17, 2022, 10:20:38' (Creation Time), and 'Actions' (Create Instance, Copy Image, Share Image).

Create instance with custom image ID

The screenshot shows the AWS Lambda instance configuration page for 'fortiadc-qcpy'. The instance is running with the ID 'i-j6c8ukmv8inb7eul5ik6'. It is located in the 'China (Hong Kong)' region, 'Hong Kong Zone B', with a public IP of '47.243.181.129'. The instance was created on 'Feb 22, 2022, 15:45:00'. Configuration options include 'Connect', 'Convert to EIP', 'Add to Security Group', 'Modify Instance Description', 'Reinitialize Disks', 'Modify Hostname', 'Release', 'Create Custom Image', and 'Change Pay-as-you-go Instance Bandwidth'. Under 'CPU and Memory', it shows '4Cores 8 GiB'. Under 'Operating System', it shows 'CentOS_64'. Under 'Type', it shows 'ecs.c4.xlarge'. Under 'Instance Family', it shows 'High Clock Compute Optimized'. In the 'Tags' section, there is a single tag named 'Name : terraform_created'. The 'Network Information' section lists VPC ('vpc-j6cfzg9nbxbu4506rzsy'), VSwitch ('vsw-j6cc1261pdhqzb77aii'), EIP ID ('-'), and Secondary Private IP Address ('-').

For this POC, only one ENI is required.

VM in FortiADC VPC

Create HUBVPC

HUBVPC uses CIDR 192.168.0.0/16. 3 Paires of Vswitches is required, one Vswitch is for external Internet access, Fortigate Port1 is on this vswitch, one Vswitch is for internal traffic, an ENI is created on this vswitch and attached to the fortigate as Port2. The cross VPCs traffic will be routed to this vSwitch so traffic can go into Fortigate VM. one pair of Vswitch for CEN-TR landing is required for landing TR traffic into this vswitch.

HUBVPC

ID	Name	Created At
vpc-j6cxbp2cfsux8i8k0icu	HUBVPC-qcpcv	Feb 22, 2022, 15:45:06

ID	Name	Description
vr1-j6cbhrfwqcsxwhp18qxnz	-	-

vSwitches

internal vswitch

VSwitch for internal traffic, fortigate Port 2 (corresponding to ECS ENI Port2) is on this vswitch.

external vswitch

VSwitch for External traffic, fortigate Port 1 is on this vswitch to accept traffic from external. Port1 will be associated with a public IP or EIP

TR-landing vswitch

a Pair of VSwitch for TR-Landing, when CEN-TR connects to this HUBVPC, the TR-Landing vswitch will take the traffic. since CEN-TR requires minimal two VSwitch to attach for redundancy purposes. therefore. two VSwitch is required. each one is a separated zone.

vSwitch										
Create vSwitch		VPC ID	Instance ID/Name	VPC	Tags	Status	IPv4 CIDR Block	Available IP Addresses	IPv6 CIDR Block	Default vSwitch
<input type="checkbox"/>	vsw-j6c4svip7tnrcp11nu9r internal_a_0	vpc-j6cbp2cfslue8:8k0icu HUBVPC-qcpv				Available	192.168.12.0/24	250	Enable IPv6 CIDR Block	No
<input type="checkbox"/>	vsw-j6c89q4p82jwoxnywh external_b_1	vpc-j6cbp2cfslue8:8k0icu HUBVPC-qcpv				Available	192.168.21.0/24	252	Enable IPv6 CIDR Block	No
<input type="checkbox"/>	vsw-j6cd19d0tix7ky64w43 landing_for_cen_a_0	vpc-j6cbp2cfslue8:8k0icu HUBVPC-qcpv				Available	192.168.13.0/24	251	Enable IPv6 CIDR Block	No
<input type="checkbox"/>	vsw-j6cyj3xdlnm83cp08hqj landing_for_cen_1	vpc-j6cbp2cfslue8:8k0icu HUBVPC-qcpv				Available	192.168.23.0/24	251	Enable IPv6 CIDR Block	No
<input type="checkbox"/>	vsw-j6cb7ev7bzgqlf37vdm internal_b_0	vpc-j6cbp2cfslue8:8k0icu HUBVPC-qcpv				Available	192.168.22.0/24	252	Enable IPv6 CIDR Block	No
<input type="checkbox"/>	vsw-j6cm7rq2xkxxfnqlbf3 external_a_0	vpc-j6cbp2cfslue8:8k0icu HUBVPC-qcpv				Available	192.168.11.0/24	251	Enable IPv6 CIDR Block	No
<button>Configure Tag</button>										

Routing Tables

In this VPC, 3 Routing Tables are required.

VPC / Route Tables

Route Tables

Create Route Table	VPC ID	vpc-j6cxbp2cfusu8l8k0icu	Filter by Tag			
<input type="checkbox"/>	Instance ID/Name	VPC	Tags	vRouter ID	Route Table Type	Associate Resource
<input type="checkbox"/>	vtb-j6c7v0ia97q57tssgcrv HUBVPC-internal_for...	vpc-j6cxbp2cfusu8l8k0icu HUBVPC-qcpv		vrt-j6cbhrfwqcswxhp@qxnz	Custom	vSwitch vsw-j6c4vijg7mrcp11nu9r;
<input type="checkbox"/>	vtb-j6c7qj0q9dk927h8aq9bh Tr-landing-qcpv-0	vpc-j6cxbp2cfusu8l8k0icu HUBVPC-qcpv		vrt-j6cbhrfwqcswxhp@qxnz	Custom	vSwitch vsw-j6cdz9d0xvnx7jky64w43yzsw-j6cy3xdlmn89cp08hqq;
<input type="checkbox"/>	vtb-j6c7ksqteehlbdw2pz10w	vpc-j6cxbp2cfusu8l8k0icu HUBVPC-qcpv		vrt-j6cbhrfwqcswxhp@qxnz	System	vSwitch vsw-j6c89dg4p82woxnywh;vsw-j6ctb7ev7bzgxqf37vdm;vien
Configure Tags						

The default route is point to default IGW. and associated with external vswitch, IGW can be replaced with NAT GW as well.

VPC / Route Tables / vtb-j6c7ksqteehlbdw2pz10w

[← vtb-j6c7ksqteehlbdw2pz10w](#)

Route Table Details

Route Table ID	vtb-j6c7ksqteehlbdw2pz10w Copy	VPC ID	vpc-j6cxbp2cfusu8l8k0icu Copy
Name	- Edit	Route Table Type	System
Tags		Associated Resource	vSwitch
Created At	Feb 22, 2022, 15:45:06	Type	
Route Entry List		Description	- Edit
Associated vSwitch			

<input type="checkbox"/>	vSwitch	Status	Destination CIDR Block
<input type="checkbox"/>	vsw-j6c89dg4p82woxnywh external_b_1		192.168.21.0/24
<input type="checkbox"/>	vsw-j6ctb7ev7bzgxqf37vdm internal_b_1		192.168.22.0/24
<input type="checkbox"/>	vsw-j6cm7rq2xjvxvofnqlbf3 external_a_0		192.168.11.0/24
<input type="checkbox"/>	Unbind		

TR-landing routing table

TR-landing is for traffic from TR Router and associated with TR-landing vswitch, where the nexthop will be sent to ECS VM via ENI Port 2. A default route with next hop to ENI port 2 is configured in this routing table. all traffices that from TR arriving to this vswitch will be routed to Fortigate VM via ENI Port 2.

VPC / Route Tables / vtb-j6c16qi8r9k27fv8aq98h

← vtb-j6c16qi8r9k27fv8aq98h

Route Table Details

Route Table ID	vtb-j6c16qi8r9k27fv8aq98h Copy	VPC ID	vpc-j6cbp2cfsux8i8k0icu Copy
Name	Tr-landing-qcpy-0 Edit	Route Table Type	Custom
Tags	Edit	Associated Resource	vSwitch

Created At Feb 22, 2022, 15:47:36

Route Entry List	Associated vSwitch
----------------------------------	------------------------------------

Associate vSwitch

vSwitch	Status	Destination CIDR Block
vsw-j6cdz9d0xitx7jky64w43 landing_for_cen_0	✓ Available	192.168.13.0/24
vsw-j6cy3x0dlmn89cp08hqj landing_for_cen_1	✓ Available	192.168.23.0/24
Unbind		

VPC / Route Tables / vtb-j6c16qi8r9k27fv8aq98h

← vtb-j6c16qi8r9k27fv8aq98h

Route Table Details

Route Table ID	vtb-j6c16qi8r9k27fv8aq98h Copy	VPC ID	vpc-j6cbp2cfsux8i8k0icu Copy
Name	Tr-landing-qcpy-0 Edit	Route Table Type	Custom
Tags	Edit	Associated Resource	vSwitch

Created At Feb 22, 2022, 15:47:36

Route Entry List	Associated vSwitch
----------------------------------	------------------------------------

System Route Dynamic Route Custom Route

Add Route Entry

Destination CIDR Block	Status	Next Hop	Type	Description
0.0.0.0/0 eni-j6cj0m6157grme9...	✓ Available	eni-j6cj0m6157grme99m4u	Delete	Custom Route -

custom routing table

to_VPC_ACK_1_2_ADC custom routing table is attached with internal vswitch, so when traffic exit from ENI Port 2 (as it is on internal vswitch), this routing table will be looked up , it will use nexthop TR router to reach VPC ACK-1 and VPC ACK-2 and FortiADC VPC.

VPC / Route Tables / vtb-j6ctv0ia97q57tzsxgcry

← vtb-j6ctv0ia97q57tzsxgcry

Route Table Details

Route Table ID	vtb-j6ctv0ia97q57tzsxgcry Copy	VPC ID	vpc-j6cxbp2cfusu8i8k0icu Copy
Name	HUBVPC-internal_fort... Edit	Route Table Type	Custom
Tags	Edit	Associated Resource Type	vSwitch
Created At	Feb 22, 2022, 15:51:05	Description	hubvpc internal rout... Edit
Route Entry List	Associated vSwitch		
Associate vSwitch			
<input type="checkbox"/> vSwitch	Status	Destination CIDR Block	
<input type="checkbox"/> vsw-j6c4svigr7mrcp1lnu9r internal_a_0	✓ Available	192.168.12.0/24	
<input type="checkbox"/> Unbind			

VPC / Route Tables / vtb-j6ctv0ia97q57tzsxgcry

← vtb-j6ctv0ia97q57tzsxgcry

Route Table Details

Route Table ID	vtb-j6ctv0ia97q57tzsxgcry Copy	VPC ID	vpc-j6cxbp2cfusu8i8k0icu Copy
Name	HUBVPC-internal_fort... Edit	Route Table Type	Custom
Tags	Edit	Associated Resource Type	vSwitch
Created At	Feb 22, 2022, 15:51:05	Description	hubvpc internal rout... Edit
Route Entry List	Associated vSwitch		
System Route	Dynamic Route	Custom Route	
Add Route Entry			
Destination CIDR Block	Status	Next Hop	Type
0.0.0.0/0 eni-j6cjom6i157grme9...	✓ Available	eni-j6cjom6i157grme99m4u	Delete Custom Route
10.0.8.0/21 tf-to_foriadc_vpc_v...	✓ Available	tr-attach-nlfbdhij5azhoay75	Delete Custom Route
10.1.0.0/23 tf-to_ack1_vpc_via_t...	✓ Available	tr-attach-nlfbdhij5azhoay75	Delete Custom Route
10.0.0.0/23 tf-to_ack2_vpc_via_t...	✓ Available	tr-attach-nlfbdhij5azhoay75	Delete Custom Route

FortiGate is in HUBVPC where all North-South traffic and Cross ACK traffic will be routed into this VPC via CEN-TR. Also Fortigate is located in this VPC. so this VPC will require internet access. FortiGate in this VPC will be associated with a public IP or EIP.

Create Fortigate instance

Create Fortigate with image from the marketplace.

The screenshot shows the 'Instance Details' page for an Alibaba Cloud instance named 'HUBVPC-Primary-FortiGate-qcpy'. The instance is currently running and has the following specifications:

- Region:** China (Hong Kong)
- Zone:** Hong Kong Zone B
- Public IP:** 47.242.124.76 (Public) | 192.168.11.11 (Private)
- Instance Type:** ecs.hfc6.large (2 vCPU, 4 GiB, I/O Optimized)
- Bandwidth:** 100Mbps (Peak Value)
- Creation Date:** February 22, 2022, 16:45
- Status:** Running

The 'Basic Information' tab is selected, showing details like Instance ID (i-6c8ukmv8inb7eul5ik5), Resource Group (-), Security Group (sg-j6cegovff561pdg48wi1), and Description (-). It also lists CPU and Memory (2Cores 4 GiB), Operating System (CentOS_64), and Instance Family (ecs.hfc6).

The 'Network Information' tab is partially visible at the bottom, showing VPC (vpc-j6cxbp2cfsux8i8k0icu), VSwitch (vsw-j6cm7rq2xjkvxofnqlbf3), and EIP ID (-).

ENI ports

ENI Port with IP 192.168.12.11 is map to fortigate Port2.
Primary Port with IP 192.168.11.11 is map to fortigate Port1.

Instance Details										Old Version		
ENIs										Buy Same Type	Refresh	All Operations
Bind Secondary ENI												
ID/Name	Tag	VSwitch/VPC	Zone	Security Group ID	Public IP Address	Private IP Address	Type/MAC Address(All)	Status/Creation Time(All)	Actions			
eni-j6c0m6157grme99m4u HUBVPC-Primary-Internal-ENI-qcpy	vsw-j6c4svjg... vpc-j6cxbp2c...	Hong Kong Zone B	sg-j6ceg...		192.168.12.11 (Primary)	Secondary 00:16:3e:02:85:e3	InUse February 22, 2022, 15:45		Modify Unbind Delete Manage Secondary Private IP Address Check Security Group Rules			
eni-j6CBf6B8jw0dunbye	vsw-j6cm7rq2... vpc-j6cxbp2c...	Hong Kong Zone B	sg-j6ceg...		192.168.11.11 (Primary)	Primary 00:16:3e:06:d7:7e	InUse February 22, 2022, 15:45		Modify Unbind Delete Manage Secondary Private IP Address Check Security Group Rules			

Create Client-VM

Create a Ubuntu VM in HUBVPC as a kubectl client. You can also create this VM in a dedicated VPC or any other VPCs as long as it has a route to reach all other components you want to manage. in this POC setup. We just use HUB VPC.

This Ubuntu VM does not need a public IP address associated , We will use Fortigate do a DNAT to access this VM, To to add, We need to add an Tag for this VM , so fortigate can automatically locate this VM via Tag when Fortigate configured with SDN connector to alibaba Cloud.

You can also attach a Public IP for this client VM temporarily for external SSH access if Fortigate has not ready yet. after you config a VIP/DNAT on fortigate for this client VM, you can detach its public IP.

You will need to install kubectl on this client VM to manage ACK1 and ACK2.

ECS / Instance / Instance Details

← client-ubuntu-qcpv ▾

Instance Details	Monitoring	Security Groups	Cloud Disk	Snapshot-consistent Groups	Snapshot	ENIs	Remote Commands/Files	Operation Records	Health Check	Events																																																															
<div style="display: flex; justify-content: space-between;"> Basic Information Instance Troubleshooting ... Start Restart Stop Configure Security Group Rule Reset Password ⋮ </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="flex: 1;"> client-ubuntu-qcpv Running </div> <div style="flex: 1; text-align: right;"> Connect </div> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Instance ID i-j6cg0w474i2p8oykt7kq</td> <td style="width: 30%;">Region China (Hong Kong)</td> </tr> <tr> <td>Resource Group -</td> <td>Zone Hong Kong Zone B</td> </tr> <tr> <td>Public IP -</td> <td>Hostname iJ6cg0w474i2p8oykt7kq2</td> </tr> <tr> <td>Security Group sg-j0cegovf561pdg4bw1</td> <td>Bind ENP Add to Security Group</td> <td style="text-align: right;">Modify Hostname</td> </tr> <tr> <td>Description -</td> <td>Created At Feb 22, 2022, 15:54:00</td> <td style="text-align: right;">Auto Release Time -</td> </tr> <tr> <td></td> <td>Modify Instance Description</td> <td style="text-align: right;">Release</td> </tr> <tr> <td colspan="3"><hr/></td> </tr> <tr> <td>CPU and Memory 2Cores 4 GiB</td> <td>Cloud Disk 1</td> <td style="text-align: right;">Reinitialize Disks</td> </tr> <tr> <td>Operating System Ubuntu 18.04 64-bit</td> <td>Snapshot 0</td> <td></td> </tr> <tr> <td>Type ecs.hfc6.large</td> <td>Image ID ubuntu_18_04_x64_20G_alibase_20200521.vhd</td> <td style="text-align: right;">Create Custom Image</td> </tr> <tr> <td>Instance Family ecs.hfc6</td> <td>Current Bandwidth 0Mbps (Maximum Bandwidth)</td> <td style="text-align: right;">Change Pay-as-you-go Instance Bandwidth</td> </tr> <tr> <td colspan="3"><hr/></td> </tr> <tr> <td colspan="3">Tags</td> </tr> <tr> <td colspan="3" style="text-align: right;">Edit Tags</td> </tr> <tr> <td colspan="3" style="text-align: center;">Name : Terraform-clientvm</td> </tr> <tr> <td colspan="3"><hr/></td> </tr> <tr> <td colspan="3"> Network Information </td> </tr> <tr> <td colspan="3" style="text-align: right;"> Bind Secondary ENI Change VPC ⋮ </td> </tr> <tr> <td>Network Type VPC</td> <td>VPC vpc-j6cxbp2cfusxe8i8k0icu ...</td> <td></td> </tr> <tr> <td>ENI eni-j6cg0w474i2p8oyzv56</td> <td>VSwitch vsw-j6c4svjgr7tnrcp11nu0r ...</td> <td></td> </tr> <tr> <td>Primary Private IP Address 192.168.12.60</td> <td>EIP ID -</td> <td></td> </tr> <tr> <td>IPv6 Address -</td> <td>Secondary Private IP Address -</td> <td></td> </tr> </table>											Instance ID i-j6cg0w474i2p8oykt7kq	Region China (Hong Kong)	Resource Group -	Zone Hong Kong Zone B	Public IP -	Hostname iJ6cg0w474i2p8oykt7kq2	Security Group sg-j0cegovf561pdg4bw1	Bind ENP Add to Security Group	Modify Hostname	Description -	Created At Feb 22, 2022, 15:54:00	Auto Release Time -		Modify Instance Description	Release	<hr/>			CPU and Memory 2Cores 4 GiB	Cloud Disk 1	Reinitialize Disks	Operating System Ubuntu 18.04 64-bit	Snapshot 0		Type ecs.hfc6.large	Image ID ubuntu_18_04_x64_20G_alibase_20200521.vhd	Create Custom Image	Instance Family ecs.hfc6	Current Bandwidth 0Mbps (Maximum Bandwidth)	Change Pay-as-you-go Instance Bandwidth	<hr/>			Tags			Edit Tags			Name : Terraform-clientvm			<hr/>			Network Information			Bind Secondary ENI Change VPC ⋮			Network Type VPC	VPC vpc-j6cxbp2cfusxe8i8k0icu ...		ENI eni-j6cg0w474i2p8oyzv56	VSwitch vsw-j6c4svjgr7tnrcp11nu0r ...		Primary Private IP Address 192.168.12.60	EIP ID -		IPv6 Address -	Secondary Private IP Address -	
Instance ID i-j6cg0w474i2p8oykt7kq	Region China (Hong Kong)																																																																								
Resource Group -	Zone Hong Kong Zone B																																																																								
Public IP -	Hostname iJ6cg0w474i2p8oykt7kq2																																																																								
Security Group sg-j0cegovf561pdg4bw1	Bind ENP Add to Security Group	Modify Hostname																																																																							
Description -	Created At Feb 22, 2022, 15:54:00	Auto Release Time -																																																																							
	Modify Instance Description	Release																																																																							
<hr/>																																																																									
CPU and Memory 2Cores 4 GiB	Cloud Disk 1	Reinitialize Disks																																																																							
Operating System Ubuntu 18.04 64-bit	Snapshot 0																																																																								
Type ecs.hfc6.large	Image ID ubuntu_18_04_x64_20G_alibase_20200521.vhd	Create Custom Image																																																																							
Instance Family ecs.hfc6	Current Bandwidth 0Mbps (Maximum Bandwidth)	Change Pay-as-you-go Instance Bandwidth																																																																							
<hr/>																																																																									
Tags																																																																									
Edit Tags																																																																									
Name : Terraform-clientvm																																																																									
<hr/>																																																																									
Network Information																																																																									
Bind Secondary ENI Change VPC ⋮																																																																									
Network Type VPC	VPC vpc-j6cxbp2cfusxe8i8k0icu ...																																																																								
ENI eni-j6cg0w474i2p8oyzv56	VSwitch vsw-j6c4svjgr7tnrcp11nu0r ...																																																																								
Primary Private IP Address 192.168.12.60	EIP ID -																																																																								
IPv6 Address -	Secondary Private IP Address -																																																																								

VMs in HUBVPC

Elastic Compute Service / Instances

Instances

Create Instance	<input type="button" value="VPC ID: Search by VPC ID"/>	<input type="button" value="Tags"/>						
Filters: Status: Running VPC ID: vpc-j6cxbp2cfusxe8i8k0icu Clear								
Instance ID/Name	Tag	Monitoring	Zone ⋮	IP Address	Status ⋮	Network Type ⋮	Specifications	Billing Method ⋮
i-j6cg0w474i2p8oykt7kq client-ubuntu-qcpv		Hong Kong Zone B	192.168.12.60 (Private)	Running	VPC	2 vCPU 4 GiB (IO Optimized) ecs.hfc6.large 0Mbps (Peak Value)	Pay-As-You-Go February 22, 2022, 15:54 Created
i-j68ukm8inb7eu5ik5 HUBVPC-Primary-FortGate-qcpv		Hong Kong Zone B	47.242.124.76 (Public) 192.168.11.11 (Private)	Running	VPC	2 vCPU 4 GiB (IO Optimized) ecs.hfc6.large 100Mbps (Peak Value)	Pay-As-You-Go February 22, 2022, 15:45 Created

Create ACK1VPC

Create VPC for ACK1

CIDR: 10.0.0.0/8

VPC / VPCs / vpc-j6c7lrz8o34leuiwcmuzs

← vpc-j6c7lrz8o34leuiwcmuzs

Information	Resources	CIDRs	Authorize Cross Account Attach CEN	Advanced Features
VPC Details				
ID	vpc-j6c7lrz8o34leuiwcmuzs	Copy	Name	ack1
IPv4 CIDR Block	10.1.0.0/16 (Primary)		Created At	Feb 22, 2022, 15:45:06
IPv6 CIDR Block	Enable IPv6 CIDR Block		Status	✓ Available
Tags	-		Description	Edit
Default VPC	No		Instance Attachment Details	CEN ID:cen-wjow07frthq7i266ws Owner Account:1671278556116611 Status:attached
Region	China (Hong Kong)		Resource Group	默认资源组
Owner Account UID	Current Account			
vRouter Basic Information				
ID	vrt-j6cayzs40azm2l08m9gmh	Copy	Name	Edit
Created At	Feb 22, 2022, 15:45:06		Description	Edit

Vswitch

10.1.1.0/24 and 10.1.0.0/24 subnet for both POD and ACK worknode.

VPC / vSwitch

vSwitch

Create vSwitch	VPC ID	vpc-j6c3z974rib7basotna0l	<input checked="" type="radio"/>	Filter by Tag						
Instance ID/Name	VPC	Tags	Status	IPv4 CIDR Block	Available IP Addresses	IPv6 CIDR Block	Default vSwitch	Zone	Route Table	Route Table Type
vsw-j6c53jqh0f6ppss3b3cme2 ack2-1	vpc-j6c3z974rib7basotna0l	ack2	✓ Available	10.1.0.0/24	251	Enable IPv6 CIDR Block	No	Hong Kong Zone C	vtb-j6cndjh4a9xmfs93mvf	System
vsw-j6c7izjx7co70gic4qs4 ack2-0	vpc-j6c3z974rib7basotna0l	ack2	✓ Available	10.0.0.0/24	235	Enable IPv6 CIDR Block	No	Hong Kong Zone B	vtb-j6cndjh4a9xmfs93mvf	System
Configure Tags										

ACK1 VPC route table

In ACK1 default route table, you may configure route all traffic to CEN-TR , where CEN-TR will send all traffic to HUB VPC fortigate for inspection and internet access.

VPC / Route Tables / vtb-j6c890nbfgtcqpg9nyd7u

← vtb-j6c890nbfgtcqpg9nyd7u

Route Table Details

Route Table ID	vtb-j6c890nbfgtcqpg9nyd7u	Copy	VPC ID	vpc-j6c7lrz8o34leuiwcmuzs	Copy
Name	-	Edit	Route Table Type	System	
Tags			Associated Resource Type	vSwitch	
Created At	Feb 22, 2022, 15:45:06		Description	-	Edit

Route Entry List Associated vSwitch

System Route Dynamic Route **Custom Route**

Add Route Entry

Destination CIDR Block	Status	Next Hop	Type	Description
0.0.0.0/0 tf-default_to_tr	✓ Available	tr-attach-wwwn3vd1vdayzsm96p	Custom Route	-

If you want POD egress to the internet use NAT Gateway, config 0.0.0.0/0 to NAT gateway, then configure specific route to CEN-TR.

Please be aware before you set up a fortigate for egress traffic to the internet, your ACK will not be able to reach the internet if you route all traffic to TR. you may configure 0.0.0.0/0 to NAT Gateway temporarily for internet access before Fortigate and CEN-TR are ready.

Create an ACK Cluster , In this POC, we choose a standard cluster. You can choose another model if you like.

Choose Terway as CNI as it will use VPC CIDR subnet for POD. also toggle Network-Policy option for network policy inside cluster. With Terway CNI, the POD will directly use the VPC CIDR address. no SNAT for POD is needed. POD , ACK nodes are directly using VPC CIDR.

Public access to ACK API is optional , as we will use client VM to access ACK with internal IP addresses. but you may toggle “Expose API with EIP” if you want.

You can choose not to install Ingress controller as we will use fortiadc as ingress controller. but you can install an ingress controller if you want to use both built-in ingress controller and FortiADC.

Cluster Name	ack-2022- ✓	The name must be 1 to 63 characters in length and can contain letters, Chinese characters, digits, and hyphens (-).								
Cluster Specification	<input checked="" type="radio"/> Professional	<input type="radio"/> Standard edition	🔗 Contrast	Professional Kubernetes clusters are developed based on managed Kubernetes clusters. This type of cluster provides higher reliability and security for workloads in large-scale production environments, and is covered by the service-level agreement (SLA) that includes compensation clauses. Learn More						
Region	China (Beijing)	China (Zhangjiakou)	China (Hohhot)	China (Ulanqab)	China (Hangzhou)	China (Shanghai)	China (Shenzhen)	China (Heyuan)		
🔗 How to select a region	China (Guangzhou)	China (Chengdu)	<input checked="" type="radio"/> China (Hong Kong)	Japan (Tokyo)	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	Philippines (Manila)		
Indonesia (Jakarta)	India (Mumbai)	US (Virginia)	US (Silicon Valley)	UK (London)	Germany (Frankfurt)					
Billing Method	<input checked="" type="radio"/> Pay-As-You-Go	<input type="radio"/> Subscription	🔗 Contrast							
Kubernetes Version	1.22.3-aliyun.1	1.20.11-aliyun.1	🔗 Release Notes							
Container Runtime	Containerd 1.4.8	Docker 19.03.15	Sandboxed-Container 2.2.0	🔗 How to choose the container runtime?						
VPC	VPC-ACK-1 (vpc-j6crkomejzxh81uyt4ia4, 10.0.0.... 🔗)									
	🔗 Create VPC 🔗 Plan Kubernetes CIDR blocks in VPC networks									
Network Plug-in	<input checked="" type="radio"/> Flannel	<input type="radio"/> Terway	🔗 How to select a network plug-in for a Kubernetes cluster							
	<input type="checkbox"/> IPVLAN This feature combines IPVLAN and eBPF to enable NIC virtualization and sharing. Only Alibaba Cloud Linux 2 is supported.									
	<input checked="" type="checkbox"/> Support for NetworkPolicy Policy-based network traffic control is provided.									
vSwitch	Select 1~5 vSwitches. We recommend that you select vSwitches in different zones to ensure high availability for the cluster.									
	🔗 Name	ID	Zone	CIDR	Available IP Addresses					
	<input checked="" type="checkbox"/> ACK-1-10-1-1	vsw-j6co50qducn3jawn7nkvk	China (Hong Kong) ZoneC	10.1.1.0/24	248					
	<input checked="" type="checkbox"/> ACK-1-10-1-0-0	vsw-j6cns9z7kgj71mppcpor	China (Hong Kong) ZoneB	10.1.0.0/24	236					
	🔗 Create vSwitch									
Pod vSwitch	All	ZoneC (1 / 1)	ZoneB (1 / 1)							
	🔗 Name	ID	Zone	CIDR	Supported Pods					
	<input checked="" type="checkbox"/> ACK-1-10-1-1	vsw-j6co50qducn3jawn7nkvk	China (Hong Kong) ZoneC	10.1.1.0/24	252					
	<input checked="" type="checkbox"/> ACK-1-10-1-0-0	vsw-j6cns9z7kgj71mppcpor	China (Hong Kong) ZoneB	10.1.0.0/24	252					
	🔗 Create vSwitch									
Service CIDR	192.168.0.0/16 ✓ Recommended Value: 192.168.0.0/16									
	Valid values: 10.0.0.0/16~24, 172.16~31.0.0/16~24, and 192.168.0.0/16~24.									
	The specified CIDR block cannot overlap with that of the VPC 10.0.0.0/8 or those of the ACK clusters that are deployed in the VPC. The CIDR block cannot be modified after the cluster is created.									
Configure SNAT	<input type="checkbox"/> Configure SNAT for VPC 🔗 Recommended									
	Nodes and applications in the cluster do not have Internet access. To enable Internet access for nodes and application after the cluster is created, you must manually create and configure a NAT gateway for the VPC. For more information, see Manually enable SNAT .									
Access to API Server	slb.s2.small	🔗 SLB Instance Specifications	By default, an internal-facing SLB instance is created for the API server. You can modify the specification of the SLB instance. If you delete the SLB instance, you cannot access the API server.							
	<input type="checkbox"/> Expose API Server with EIP ⚠ Note									
	If this option is disabled, you cannot access the cluster API server through the Internet.									
RDS Whitelist	Select RDS Instance									
	We recommend that you go to the RDS console to add the CIDR blocks of the specified nodes and specified pods to a whitelist of the RDS instance. Otherwise, if the RDS instance is not in the running state, the node pool cannot be scaled out.									
Security Group	Create Basic Security Group	Create Advanced Security Group	By default, advanced security groups that are automatically created allow the communication between IP addresses within the VPC. You can ALSO manually modify security group rules based on your requirements. Security group overview							
Deletion Protection	<input type="checkbox"/> Enable									
	Cluster Cannot Be Deleted in Console or by Calling API									
Resource Group	Not Selected	🔗	To create a resource group, click here .							

[All Clusters / ack-2022-1](#)

ack-2022-1

- [Overview](#)
- Basic Information**
- [Connection Information](#)
- [Cluster Resources](#)
- [Cluster Logs](#)

Basic Information

Cluster ID: c65494ca24a8d48e7a571c853e3cc0ce1	Running	Region: China (Hong Kong)	Time Zone: Asia/Shanghai
---	---------	---------------------------	--------------------------

Cluster Information

API Server Public Endpoint	EIP
API Server Internal Endpoint	https://10.1.99.6443 Set access control Troubleshoot connection issues
Service CIDR	192.168.0.0/16
Testing Domain	*.c65494ca24a8d48e7a571c853e3cc0ce1.cn-hongkong.alicontainer.com Rebind Domain Name
Kube-proxy Mode	ipvs
Network Plug-in	terway-enlip
Custom Certificate SANs	Update
Labels	ack.aliyun.com: c65494ca24a8d48e7a571c853e3cc0ce1

[Create Cluster](#) [Managed Kubernetes](#) [Dedicated Kubernetes](#) [Serverless Kubernetes](#) [Managed Edge Kubernetes](#) [Register Cluster](#) [Cluster Templates](#) [Back](#)

1 Cluster Configurations **2 Node Pool Configurations** **3 Component Configurations** **4 Confirm Order**

Node Pool Name: default-nodepool

The name must be 1 to 63 characters in length and can contain letters, Chinese characters, digits, and hyphens (-). If you want to add existing ECS instances, add them to node pools of the cluster after the cluster is created.

Instance Type: Current Generation All Generations

Architecture: x86-Architecture Heterogeneous Computing ECS Bare Metal Instance Super Computing Cluster

Category	All	General Purpose	Compute Optimized	Memory Optimized	Big Data	Local SSD	High Clock Speed	Shared	Enhanced	Recommended
Instance Family	ecs.hf6.xlarge	ecs.hf6.xlarge	4 vCPU	8 GiB	B D	3	One ENI for Multi-Pod(20)	Up to 5 Gbit/s	500000 I	
Compute Optimized Type with High Clock Speed hf6	ecs.hf6.xlarge	4 vCPU	8 GiB	B D	3	One ENI for Multi-Pod(20)	Up to 5 Gbit/s	500000 I		
General Purpose Type with High Clock Speed hf7	ecs.hf7.xlarge	4 vCPU	16 GiB	B D	3	One ENI for Multi-Pod(30)	Up to 10 Gbit/s	1000000 C		
Enhanced Compute Type c6e	ecs.c6e.xlarge	4 vCPU	8 GiB	B D	4	One ENI for Multi-Pod(45)	Up to 10 Gbit/s	1000000 C		
General Purpose Type with Enhanced Network Performance sn2ne	ecs.sn2ne.xlarge	4 vCPU	16 GiB	B C	3	One ENI for Multi-Pod(20)	1.5 Gbps	500000 I		
Enhanced General Purpose Type g6e	ecs.g6e.xlarge	4 vCPU	16 GiB	B D	4	One ENI for Multi-Pod(45)	Up to 10 Gbit/s	1000000 C		
Compute Optimized Type c7	ecs.c7.xlarge	4 vCPU	8 GiB	B D	4	One ENI for Multi-Pod(45)	Up to 10 Gbit/s	1000000 C		

Selected Types: You can select multiple instance types. Nodes are created based on the order of the instance types in the above list. If one instance type is unavailable, the next instance type is used. The actual instance types used to create nodes are subject to inventory availability.

Quantity: 1 unit(s) Nodes will be evenly assigned to your selected VSswitches. A standard managed cluster can contain up to 100 nodes. To use a larger cluster, create a professional managed cluster.

Nodes will be evenly assigned to your selected VSswitches. A standard managed cluster can contain up to 100 nodes. To use a larger cluster, create a professional managed cluster.

System Disk: ESSD Disk 120 GB Performance Level PL 1 (Up to 50,000 IOPS per D...)

Mount Data Disk: You have selected 0 disks and can select 10 more.

Disk Parameters and Performance: Add Data Disk Recommended

Operating System: Alibaba Cloud Linux 2.1903 Use the container-optimized operating system Alibaba Cloud Linux 2

Security Reinforcement: Disable Reinforcement based on classified protection CIS Reinforcement

Logon Type: Key Pair Password

Password: ***** The password must be 8 to 30 characters in length and contain at least three of the following four types of characters: uppercase letters, lowercase letters, digits, and special characters.

Confirm Password: *****

Show Advanced Options

Create Cluster [Managed Kubernetes](#) [Dedicated Kubernetes](#) [Serverless Kubernetes](#) [Managed Edge Kubernetes](#) [Register Cluster](#)

Cluster Configurations **Node Pool Configurations** **Component Configurations**

Ingress	<input type="radio"/> Do Not Install	<input type="radio"/> Nginx Ingress	<input type="radio"/> ALB Ingress	
Service Discovery	<input checked="" type="checkbox"/> Install NodeLocal DNSCache Runs a DNS caching agent on nodes to improve the performance of DNS resolution. Learn More .			
Volume Plug-in	<input type="radio"/> CSI	<input type="radio"/> Flexvolume	How to select the volume plug-in	
	<input checked="" type="checkbox"/> Dynamically Provision Volumes by Using the Default NAS File Systems and CNFS View Details			
	5 GiB of Capacity NAS space or 1 GB of Performance NAS space is offered free of charge to each ACK cluster for 12 months. For more information, see Pricing Details			
Monitoring Agents	<input type="checkbox"/> Install CloudMonitor Agent on ECS Instance Recommended <input type="checkbox"/> Enable Prometheus Monitoring Recommended Pricing Details Provides basic monitoring and alerts for Kubernetes clusters free of charge. Details			
Alerts	<input type="checkbox"/> Use Default Alert Rule Template ACK Default Alert Configurations After the cluster is created, you can go to the details page of the cluster and choose Operations > Alerts to manage alert rules.			
Log Service	<input type="checkbox"/> Enable Log Service Note Pricing Details The cluster auditing function is unavailable if Log Service is not activated.			
Log Collection for Control Plane Components	<input type="checkbox"/> Enable If you select this check box, logs of control plane components, including kube-apiserver, kube-controller-manager, and kube-scheduler, are collected to Log Service. Details			

Create Cluster [Managed Kubernetes](#) [Dedicated Kubernetes](#) [Serverless Kubernetes](#) [Managed Edge Kubernetes](#) [Register Cluster](#)

Cluster Configurations **Node Pool Configurations** **Component Configurations** **Confirm Order**

Selected Configurations	Product	Configuration	Quantity	Billing Method	Subscription Duration	Price
Generate API Request		Region: China (Hong Kong) Kubernetes Version: 1.22.3-almyun.1 VPC: vpc-1234567890123456 vSwitch: vswitch-00c050d4b3037hnkv vsw-0c0e932f919d71mpsoar Container Runtime: containerd 1.4.8 Pod CIDR Block: Service CIDR: 192.168.0.0/16	1	None	None	
Parameters						
ACK Cluster		Network Plug-interway Volume Plug-iscsi-plugin		None	None	
ECS Instance - Worker		ecs-hf6c-xlarge System Disk: ESSD Disk - 120G	1	Pay-As-You-Go	None	¥ 1.936 / Hours
SLB Instance - API Server		Instance Type:slb.s2.small Instance type: internal-facing	1	Pay-As-You-Go	None	¥ 0.380 / Hours
ENIs		Create one or two ENIs based on the cluster configuration.	1-2	None	None	
ROS		Automatically create a resource stack with the name prefixed with k8s-for-ecs.	1	None	None	
Auto Scaling		Use a scaling group to create worker nodes.	1	None	None	
Security Group			1	None	None	
RAM			1	None	None	

Dependency Check	Item	Status	Details
	ACK activation check	Passed	
	Account Status Check	Passed	
	RAM Role Authorization Check	Passed	
	Dependent Service Activation Status	Passed	
	Auto Scaling Status Check	Passed	
	Service Quota Check	Passed	
	System Disk Size Check	Passed	
	Data Disk Size Check	Passed	
	Account Balance Check	Passed	

Terms of Service

- During the cluster creation process, the following operations may be performed depending on cluster configurations:
- Create ECS instances, configure a public key to enable SSH login from master nodes to other nodes, and configure the Kubernetes cluster through Cloudinit.
 - Create a security group that allows access to the VPC network over ICMP.
 - Create VPC routing rules.
 - Create a RAM gateway and Elastic IP addresses.
 - Create a RAM role and grant it the following permissions: query, create, and delete ECS instances, create and delete cloud disks, and all permissions on SLB instances, CloudMonitor, VPC, Log Service, and NAS. The Kubernetes cluster dynamically creates SLB instances, cloud disks, and VPC routing rules based on your settings.
 - Create an internal SLB instance and open port 6443.
 - When you use a dedicated or managed Kubernetes cluster, the system collects log and monitoring information about control components on master nodes to help ensure cluster stability.
 - If the cluster creation fails, the created resources will be charged. We recommend that you delete unused resources at the earliest opportunity.

I have read and understand the preceding statement. I also have read and accept the [Terms of Service](#) and [Disclaimer](#).

An internal SLB is created for access to k8s API server , the SLB has IP:PORT pair 10.1.1.99:6443 in this POC. We can directly copy the kubeconfig context into client-VM kubeconfig file.

```

apiVersion: v1
clusters:
- cluster:
  server: https://10.1.1.99:6443
  certificate-authority-data:
LS0tLS1CRUUETiB0RUUUSUJZQ0PFURS0tLS0tCk1JSURPeKNQWIPZ0f3SUJBZ0tCQURBTkJna3Fpa2lHOXcwQFrCzBRRErTVNjg0R3QWRUVFLRdobiXNW4KZW1odmRUQVCCz05WQkFvVERXRnNhV0pwW1F21kyehZkV1F4RpBUJnTlZCQU1UQ
210MVLtVnL1iDVyWtInNdwPQ-J0tQfNNNGNtppWvGz1BakExTpBe16RXdexDeUzTgNYIJNnhkeKFQmD0WkB1R0R2h0cA1JZD2hRzxTUJRRExVUdVeE10Wd44FC1tRnLzU0,jYkc5MVpERVNRQkVHQTFRUfATUHM1zWtLkGD
pUMwK73pQ0QFT5XeUEUlkSz29s5whZY5B0UVQ1LBGRgnrVBREND0VfQ2dnRU529N9ckx6QlpNmwsxGtV0YFSApMTNRZtBxd1pkejVsdl35mJz0StraJSSmVmWksVTLEn1ZQ5kU2eU9jdskRvWhucvfcKvKl0t2b2w
2dVNUSPFLQ0UWmZveINn001A0MeX0WtuazRQwLveXdaRTJjd0h4ew1TGfsqzc3Um4KR0BaTnTJA1SmZMWEFLrnLbMktOrEhJTuPChNrBc93SHLKEpSMELN0Ewzcn1PSVp#TwFeDA3K3l0MjZTbdq5RXE3RBVUkFK0j1vUjFrd1V
ZjRjVTNUU31xkb2RKZl2j3eXjZ01MfTBRRGx0dW1qVXhpEtXb191a1f0a1BTCl1dqZ204akd0bTg5UnJrMhnCUEptRGFIIVN5TH2bGwIM3Z5bndPTEVNmWzRz1LzzVzYp)1kKydgkVED1VHQKWRz00F3RFUByU507UVd8dRmURMUjB0QVFl0jBU

```

Component created by ACK

Resource Type	Resource Name
Resource Orchestration Service (ROS)	k8s-for-cs-c65494ca24a8d48e7a571c853e3cc0ce1
VPC	vpc-j6crkomejzxh81uyt4ia4
Pod vSwitch	vsw-j6co50qducn3jawn7nkvk
Security Group	sg-j6cd6w5lquavxd4e02ew
Worker RAM Role	KubernetesWorkerRole-ef50b8e2-627a-4baf-a83b-a6b2b9ff0b99
Scaling Group	asg-j6ccaiydlxk3qau1dyp
APIServer SLB	lb-j6ccud84b7kmxkbsw
Node Pools	Go to Node Pool

1 VPC, two Vswitch (the POD and Node can be in both of these vswitch subnet, so when you create route entry in CEN-TR and Fortigate , do not forget add both), a APIServer SLB for k8s API server, a Node Pools

install kubectl on client VM

ssh into client VM by using fortigate public IP (after you configure VIP for client-VM on fortigate).

login into client-VM to install kubectl

<https://kubernetes.io/docs/tasks/tools/?spm=5176.2020520152.0.0.1c6e61b1ojKsuW>

```
(base) i@ecs-148531:~/fortinet/cen-tr-ack$ ssh root@47.242.124.76 -p 2022
root@iZj6cg0w474i2p8oykt7kqZ:~# head /root/.kube/config_ack1

apiVersion: v1
clusters:
- cluster:
  server: https://10.1.0.160:6443
  certificate-authority-data:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURPeKNDQW1PZ0F3SUJBZ01CQURBTkJna3F
oa21HOXcwQkFRc0ZBRErTVNjd0R3WURWUVFLRXdob1lXNW4KZW1odmRUQVVCZ05WQkFvVERXRn
NhV0poWw1FZ1kyeHZkV1F4RXpBUkJnT1ZCQU1UQ210MV1tVnlibVYwWlhNdwpJQmNOTWpJd01qs
X1NRGMwT1RVM1doZ1BNakExTwpBeU1UVXd0e1ExT1RkYU1ENHhKekFQQmd0VkJBb1RDR2hoCmJt
ZDZhRzkxTUJRR0ExVUVDaE10WVd4cFltRmlZU0JqYkc5MVPERVRNQkVHQTFVRUF4TUthM1ZpWlh
KdVpYUmwKY3pDQ0FTSXdEUV1KS29aSWh2Y05BUUVCQ1FBRGdnRVBBRENDQVFvQ2dnRUJBTGx6T1
JncG11K11Nd2FVZ010dApLcjY5c0UxRWhWMUdETVdiUEEZUFNJaDYvV29UNTJ1V3JLTxptQTThHW
UVyU1JjQmJwTxoxUjNwVEZ0eC9oYVU2CjNIbmNLdHdQeC9KOXVmVmF1S1hadk1HcEhMWFFjWVdp
ZXplbG9vdUp2dTfhbGdiR2pCZjdoU1FhRjVjNHFreGwKTTNwekN4RTloZ1hYV11HM1hRRkM3SEJ
3VTFsbn9IWU1mRhoxdX1EOThsYUhOVW1WMWcrNkovYk1SzzrN1RQVApiBudmWEnoaFRqeHdxQ2
xUUmxBc0tLbW91RXNETWRndXExc21ZbmRSaEx2Y0F5Mm4wbXJUNThDMnozbXRiRGNZCkNrWXY5S
nRvM3JGbHJWMMmk1dEs4N1RjL2NIS0pWZ1pxWDdVQ1U3VmRsanJSU2pvUUNXOGd0L2FuTXhuQ3RT
VkmKUUQwQ0F3RUFBYU5DTUVBd0RnWURWUjBQQVFILOJBURBZ0trTUE4R0ExVWRFd0VCL3dRRk1
BTUJBZjh3SFFZRapWUjBPQkJZRUZKWTZ4a0xEdw1MdWN2SjJGcWhSK3dzV1JaTXZNQTBHQ1NxR1
NJYjNEUUVCQ3dVQUE0SUJBUNmCndRa3Q2cnJSTE9LTE1sU01uODJMWTh1RW9NVHRBL1ZmRWpsN
XdYaFJ4K0kxWGFGRE9iRnUrY3V3SWN60VBOYUMKemFrSwpZdWN5NWd1NmZnQRFVzNOL0RDR1dP
WEJFNTh6N3R2a0V0U2N5bGV5cEdjV0U3Z1ZKeWtjVU1NcThyaQo1T1I0WXBoTjRJN1MvbGtHeTE
5c0J6NzI3STFqSGwyR31SQV1XZ1hkQnZUeUV4WFo5MU1pZmNVWUVBMUJBQkJ3C1d2WGzaK3Mxb3
g2dTNFaUFOZGV1ukNXeS9yWis1NTg5TFRzVUtsQ3BMTTFhT1hHRjhiQjZFMW1kdERqNGVxMmsKY
ndnbVFEWTAYW1JSsCVJQVHBWR1J1TXdpZytGSmRPWU41Q1FnQzc0T1pUTnVJQ0F2aTZDRUcvNUI4
NktpOWJyWQp3L2ov0VFaNW9pa11vVmVyY3pyTgotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg=
=
  name: kubernetes
contexts:
- context:
  cluster: kubernetes
```

you shall be able to use kubectl get the node information.

```
root@iZj6cg0w474i2p8oykt7kqZ:~# kubectl get node  
--kubeconfig=/root/.kube/config_ack1 -o wide  
NAME           STATUS   ROLES      AGE     VERSION  
INTERNAL-IP   EXTERNAL-IP  OS-IMAGE             KERNEL-VERSION  
CONTAINER-RUNTIME  
cn-hongkong.10.1.0.163  Ready    <none>    147m   v1.22.3-aliyun.1  
10.1.0.163     <none>     CentOS Linux 7 (Core)  
3.10.0-1160.15.2.el7.x86_64  containerd://1.4.8  
cn-hongkong.10.1.0.164  Ready    <none>    147m   v1.22.3-aliyun.1  
10.1.0.164     <none>     CentOS Linux 7 (Core)  
3.10.0-1160.15.2.el7.x86_64  containerd://1.4.8
```

Deploy application on ACK1

```
root@iZj6cg0w474i2p8oykt7kqZ:~# cat simple-deployment.yaml  
apiVersion: apps/v1  
kind: Deployment  
metadata:  
  name: nginx-deployment  
  labels:  
    app: nginx  
spec:  
  replicas: 2  
  selector:  
    matchLabels:  
      app: nginx  
  template:  
    metadata:  
      labels:  
        app: nginx  
    spec:  
      containers:  
      - name: nginx  
        image: nginx:1.14.2  
        ports:
```

```

    - containerPort: 80

root@iZj6cd1vfw01yb6cq9jsqyZ:~# kubectl apply -f simple-deployment.yaml
root@iZj6cg0w474i2p8oykt7kqZ:~# cat k8s_svc_nginx.yaml
kind: Service
apiVersion: v1
metadata:
  name: nginx-30163
spec:
  # Expose the service on a static port on each node
  # so that we can access the service from outside the cluster
  type: NodePort

  # When the node receives a request on the static port (30163)
  # "select pods with the label 'app' set to 'echo-hostname'"
  # and forward the request to one of them
  selector:
    app: nginx

ports:
  # Three types of ports for a service
  # nodePort - a static port assigned on each the node
  # port - port exposed internally in the cluster
  # targetPort - the container port to send requests to
  - nodePort: 30163
    port: 80
    targetPort: 80

root@iZj6cd1vfw01yb6cq9jsqyZ:~# kubectl apply -f k8s_svc_nginx.yaml

root@iZj6cg0w474i2p8oykt7kqZ:~# kubectl get svc
--kubeconfig=/root/.kube/config_ack1
NAME      TYPE      CLUSTER-IP      EXTERNAL-IP      PORT(S)      AGE
kubernetes   ClusterIP   172.21.0.1    <none>        443/TCP      153m
nginx-30163   NodePort    172.21.8.187   <none>        80:30163/TCP  135m
root@iZj6cg0w474i2p8oykt7kqZ:~#

```

Create ACK2

Do the same as ACK1 . except it has a different vswitch IP address, so POD and NODE have different IP address subnets.

```
root@iZj6cg0w474i2p8oykt7kqZ:~# kubectl get deployment  
--kubeconfig=/root/.kube/config_ack2  
NAME          READY   UP-TO-DATE   AVAILABLE   AGE  
nginx-deployment   2/2     2           2           136m  
root@iZj6cg0w474i2p8oykt7kqZ:~# kubectl get svc  
--kubeconfig=/root/.kube/config_ack2  
NAME      TYPE      CLUSTER-IP      EXTERNAL-IP      PORT(S)      AGE  
kubernetes   ClusterIP    172.21.0.1    <none>        443/TCP      154m  
nginx-30163   NodePort    172.21.14.153  <none>        80:30163/TCP  136m
```

Create and Config CEN-TR

A CEN-TR is required to attach ACK1 ,ACK2 , HUBVPC VPC as well as fortiADC VPC.

Two Routing Tables in CEN-TR are required, one is the default Routing Table, other one is custom Routing table for HUVPC route traffic to ACK1 , ACK2, and fortiADC VPC.
default Routing table is for ACK1,ACK2, fortiADC VPC to reach HUBVPC where it has only one 0.0.0.0/0 route with nexthop set to TR router.

The screenshot shows the AWS Cloud Enterprise Network Instances page. On the left, there's a sidebar with 'Cloud Enterprise Network' and a 'Instances' tab selected. Below the tabs are 'Bandwidth Plans', 'Health Check', and 'Quotas'. The main area has a heading 'Instan...' and a note about submitting compliance information for Express Connect. It includes a 'Create CEN Instance' button and a search bar. A table lists the instance 'cen-kt2p4Dy7s63gphe' with ID 'ACK2022-1'. The table columns are: Instance ID/Name, Tag, Status, Transit Router, Number of Connections, Bandwidth Plans, Description, and Actions. The instance is listed as 'Ready' with 1 transit router, 4 connections, and 0 bandwidth plans assigned.

so, this CEN TR router will have 4 Connections, and 2 Route Tables.

TR Connections

← tr-j6crst8fnz42zwlwseayo(China (Hong Kong)) [View Other Instances](#) [Create Connection](#)

Basic Settings	Intra-region Connections	Cross-region Connections	Route Table	Network Instance Route Table	PrivateZone	Cloud Services	Flow Logs		
Create Connection <input type="text" value="Search by instance name or instance ID."/> ⚙️ 🌐									
Instance ID/Name	Network Instance	Monitor	Metering	Network Type	Associated Route Table	Account ID	Attach Time	Status	Actions
tr-attach-kv415kdy244234a6ds ACK-POD1-10-0-0	vpc-j6cu59pud998cfm595h VPC-ACK-2			VPC	vtb-j6cu55vhdbq3ncnca13 default-north-south	1671278556116611	Feb 7, 2022, 09:27:00		Attached Detach
tr-attach-7yvblgtw36pkxho4a HUBVPC-FOT	vpc-j6c929gihkeyx11sqy62			VPC	vtb-j6ch8s48hqj21gab4si74 east-west	1671278556116611	Feb 7, 2022, 13:45:00		Attached Detach
tr-attach-x4szze2sn53g5ekpv ACK-POD2-10-1-0	vpc-j6corkejmezjh81uyt4ia4 VPC-ACK-1			VPC	vtb-j6cu55vhdbq3ncnca13 default-north-south	1671278556116611	Feb 7, 2022, 15:27:00		Attached Detach
tr-attach-g7yirgtx8es93yuk8u FortiADC-VPC-CLIENT-...	vpc-j6cu1jnekjxg19ywrmkz forti-twye			VPC	vtb-j6cu55vhdbq3ncnca13 default-north-south	1671278556116611	Feb 7, 2022, 17:35:00		Attached Detach

Route Table- default-north-south

default north-south route table is for north-south traffic (ACK to internet and ACK to FortiADC, fortiADC to ACK etc)

Cloud Enterprise Network / Instances / cen-k42p40y7i63gzphve / tr-j6crst8fnz42zwlwseayo [Product Update](#) [Documentation](#) [Create Connection](#)

← tr-j6crst8fnz42zwlwseayo(China (Hong Kong)) [View Other Instances](#)

Basic Settings	Intra-region Connections	Cross-region Connections	Route Table	Network Instance Route Table	PrivateZone	Cloud Services	Flow Logs																
<input style="width: 100px; margin-right: 10px;" type="text" value="Enter"/> Delete 🌐																							
Route Table Details (vtb-j6cu55vhdbq3ncnca13)																							
Basic Settings																							
ID	vtb-j6cu55vhdbq3ncnca13 Copy	Name	default-north-south Edit																				
Status		Type	System																				
Description	default-north-south Edit	Number of Routes	2,000																				
Route Entry Route Table Association Route Propagation Route Maps																							
Add Route Entry Export CIDR Block <input type="text" value="Search by keyword"/>																							
<table border="1"> <thead> <tr> <th>Name</th> <th>Destination CIDR Block</th> <th>Next Hop</th> <th>Type</th> <th>Route Type</th> <th>Route Status</th> <th>Description</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>rte-y2ycvui3blnxkb4v default</td> <td>0.0.0.0/0</td> <td>tr-attach-7yvblgtw36pkxho4a HUBVPC-FOT</td> <td>Network Instance</td> <td>Static Routes</td> <td></td> <td>Available</td> <td>Delete</td> </tr> </tbody> </table>								Name	Destination CIDR Block	Next Hop	Type	Route Type	Route Status	Description	Actions	rte-y2ycvui3blnxkb4v default	0.0.0.0/0	tr-attach-7yvblgtw36pkxho4a HUBVPC-FOT	Network Instance	Static Routes		Available	Delete
Name	Destination CIDR Block	Next Hop	Type	Route Type	Route Status	Description	Actions																
rte-y2ycvui3blnxkb4v default	0.0.0.0/0	tr-attach-7yvblgtw36pkxho4a HUBVPC-FOT	Network Instance	Static Routes		Available	Delete																

route table association

default-north-south route table is associated with ACK1, ACK2 and FortiADC-Client VPC.

← tr-j6crst8fzn42zwlwseayo(China (Hong Kong)) View Other Instances

Create Connection

Basic Settings	Intra-region Connections	Cross-region Connections	Route Table	Network Instance Route Table	PrivateZone	Cloud Services	Flow Logs
----------------	--------------------------	--------------------------	-------------	------------------------------	-------------	----------------	-----------

Q Enter

+ Create Route Table

vbt-j6cu55vhdbvq3ncnca3 Copy

default-north-south

vbt-j6ch8s48hg21gab4s74
east-west

Route Entry Route Table Association Route Propagation Route Maps

Create Association Q Search by keyword

Instance ID	Next Hop ID	Next Hop Type	Status	Actions
tr-attach-ku425k4yz44234s6ds ACK-POD1-10-0-0	vpc-j6c6p1udj996cf1n59h VPC-ACK-2	VPC	Available	Delete
tr-attach-x4szw2snr53g5ekpv ACK-POD2-10-1-0	vpc-j6crkomejzh8luyt4ia4 VPC-ACK-1	VPC	Available	Delete
tr-attach-g7yigtxbeis93yuk6u FortiADC-VPN-CLIENT-VM	vpc-j6cu1jnekkxj19ywrmkz forti-twye	VPC	Available	Delete

Remove Route Propagation

but it will not enable Route propagation from those VPCs, it only need default route to reach HUBVPC. so route propagation from ACK1,ACK2,FortiADC-Client VPC must be removed.

← tr-j6crst8fzn42zwlwseayo(China (Hong Kong)) View Other Instances

Create Connection

Basic Settings	Intra-region Connections	Cross-region Connections	Route Table	Network Instance Route Table	PrivateZone	Cloud Services	Flow Logs
----------------	--------------------------	--------------------------	-------------	------------------------------	-------------	----------------	-----------

Q Enter

+ Create Route Table

vbt-j6cu55vhdbvq3ncnca3 Copy

default-north-south

vbt-j6ch8s48hg21gab4s74
east-west

Route Entry Route Table Association Route Propagation Route Maps

Enable Route Propagation Q Search by keyword

Instance ID	Next Hop ID	Next Hop Type	Status	Actions
No data available.				

route entry

a default route 0.0.0.0/0 with nexthop to TR-attach to HUBVPC must be configured. so all traffic from ACK1,ACK2,FortiADC-Client VPC will be sent to TR to reach HUBVPC.

[← tr-j6crst8fzn42zwlwseayo\(China \(Hong Kong\)\)](#) [View Other Instances](#) [Create Connection](#)

Basic Settings	Intra-region Connections	Cross-region Connections	Route Table	Network Instance Route Table	PrivateZone	Cloud Services	Flow Logs
<input type="text"/> Enter							
Route Table Details (vtb-j6cu55vhdbq3ncnca3)							
Basic Settings							
ID	vtb-j6cu55vhdbq3ncnca3 Copy	Name	default-north-south Edit				
Status	✓ Available	Type	System				
Description	default-north-south Edit	Number of Routes: 2,000					
Route Entry							
Add Route Entry Export CIDR Block <input type="text"/> Search by keyword							
Name	Destination CIDR Block	Next Hop	Type	Route Type	Route Status	Description	Actions
rte-y2ycvui3blnxfbk4v default	0.0.0.0/0	tr-attach-7vvlgltw36pkxho4a HUBVPC-FGT	Network Instance	Static Routes	✓ Available	defaulttofortigatevp...	Delete

Route Table east-west

Route table east-west is for ACK cross VPC traffic, the traffic between ACKs VPC. those traffic subject be inspected by HUBVPC fortigate , Fortigate must learn ACK1 ,ACK2, FortiADC-clientVM subnet , so HUBVPC know where to send packet back to ACK1, ACK2, FortiADC after it done the inspection.

route table association

this route table is only associated with HUBVPC.

[Cloud Enterprise Network / Instances / cen-k12p40y7is63gzphve / tr-j6crst8fzn42zwlwseayo\(China \(Hong Kong\)\)](#) [View Other Instances](#) [Create Connection](#)

Basic Settings	Intra-region Connections	Cross-region Connections	Route Table	Network Instance Route Table	PrivateZone	Cloud Services	Flow Logs
<input type="text"/> Enter							
Route Table Details (vtb-j6ch8s48hqj21gab4si74)							
Basic Settings							
ID	vtb-j6ch8s48hqj21gab4si74 Copy	Name	east-west Edit				
Status	✓ Available	Type	Custom				
Description	- Edit	Number of Routes: 2,000					
Route Entry							
Create Association <input type="text"/> Search by keyword							
Instance ID	Next Hop ID	Next Hop Type	Status	Actions			
tr-attach-7vvlgltw36pkxho4a HUBVPC-FGT	vpc-j6c92sgihkeyx1sqy62 HUBVPC	VPC	Available	Delete			

Enable Route Propagation

Route Propagation from ACK1,ACK2, fortiADC-client must be enabled. for HUBVPC know how to route traffic.

Cloud Enterprise Network / Instances / cen-k12p40y7ie63gphe / tr-j6crst8fzn42zwlwseayo

← tr-j6crst8fzn42zwlwseayo(China (Hong Kong)) View Other Instances ▾

Product Update Documentation Create Connection

Basic Settings	Intra-region Connections	Cross-region Connections	Route Table	Network Instance Route Table	PrivateZone	Cloud Services	Flow Logs
----------------	--------------------------	--------------------------	--------------------	------------------------------	-------------	----------------	-----------

Route Table Details (vtb-j6ch8s48hql21gab4si74)

Basic Settings

ID: vtb-j6ch8s48hql21gab4si74 [Copy](#)

Status: Available

Description: east-west

Name: east-west [Edit](#)

Type: Custom

Number of Routes: 2,000

Route Entry **Route Table Association** **Route Propagation** **Route Maps**

Route Propagation Search by keyword

Instance ID	Next Hop ID	Next Hop Type	Status	Actions
tr-attach-ku4z5k4yz44234s6ds ACK-POD1-10-0-0	vpc-j6c6p1ud996cfini595h VPC-ACK-2	VPC	Available	Delete
tr-attach-x4szzw2snr53g5ekpv ACK-POD2-10-1-0	vpc-j6crkomejzxh81uy14a4 VPC-ACK-1	VPC	Available	Delete
tr-attach-g7irgtx8es93yuk6u FortiADC-VPC-CLIENT-VM	vpc-j6cu1jnekxg19ywrzmk2 forti-twye	VPC	Available	Delete

The route Entry

← tr-j6crst8fzn42zwlwseayo(China (Hong Kong)) View Other Instances ▾

Create Connection

Basic Settings	Intra-region Connections	Cross-region Connections	Route Table	Network Instance Route Table	PrivateZone	Cloud Services	Flow Logs
----------------	--------------------------	--------------------------	--------------------	------------------------------	-------------	----------------	-----------

Route Table Details (vtb-j6ch8s48hql21gab4si74)

Basic Settings

ID: vtb-j6ch8s48hql21gab4si74 [Copy](#)

Status: Available

Description: east-west

Name: east-west [Edit](#)

Type: Custom

Number of Routes: 2,000

Route Entry **Route Table Association** **Route Propagation** **Route Maps**

Add Route Entry **Export** **CIDR Block** Search by keyword

Name	Destination CIDR Block	Next Hop	Type	Route Type	Route Status	Description	Actions
-	10.0.0.0/24	tr-attach-ku4z5k4yz44234s6ds ACK-POD1-10-0-0	Network Instance	Propagated Routes	Available	-	
-	10.0.1.0/24	tr-attach-ku4z5k4yz44234s6ds ACK-POD1-10-0-0	Network Instance	Propagated Routes	Available	-	
-	10.0.11.0/24	tr-attach-g7irgtx8es93yuk6u FortiADC-VPC-CLIENT-VM	Network Instance	Propagated Routes	Available	-	
-	10.0.12.0/24	tr-attach-g7irgtx8es93yuk6u FortiADC-VPC-CLIENT-VM	Network Instance	Propagated Routes	Available	-	
-	10.1.0.0/24	tr-attach-x4szzw2snr53g5ekpv ACK-POD2-10-1-0	Network Instance	Propagated Routes	Available	-	
-	10.1.1.0/24	tr-attach-x4szzw2snr53g5ekpv ACK-POD2-10-1-0	Network Instance	Propagated Routes	Available	-	

a total of six routes from ACK1, ACK2, fortiADC VPC will be populated in this routing table.

if the Access key/secret from Alicloud is not available for the fortigate to use. Therefore configuring the SDN connector on fortigate to retrieve client-VM and fortiADC VM is not possible, you will need to get the IP address of client VM and fortiADC VM, then create static entry on fortigate with Virtual IP to access client VM and fortiadvc instead use SDN connector.

Config Fortigate VIP for access FortiADC

If FortiADC sits behind fortigate and does not have a public IP, we can config a VIP on Fortigate to access fortiadc. below we config a GUI access to fortiadc via VIP:Port on FortiGate and a SSH access to fortiadc.

GUI access VIP mapping

The screenshot shows the FortiGate VM64-ALI interface. The left sidebar is titled "Policy & Objects" and includes sections for Firewall Policy, IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, and Virtual IPs. The "Virtual IPs" section is currently selected. The main pane displays the "Edit Virtual IP" configuration for a VIP named "fortiadc-vm-9443". The configuration includes:

- VIP type:** IPv4
- Name:** fortiadc-vm-9443
- Comments:** Write a comment... (0/255)
- Color:** Change
- Network:**
 - Interface:** public (port1)
 - Type:** Static NAT
 - External IP address/range:** 0.0.0.0
 - Mapped IP address/range:** 10.0.11.11
- Optional Filters:** (disabled)
- Port Forwarding:** (selected)
 - Protocol:** TCP (selected)
 - External service port:** 9443
 - Map to port:** 443

At the bottom right are "OK" and "Cancel" buttons.

Firewall Policy

Create a policy to allow this traffic

The screenshot shows the 'Edit Policy' screen for a firewall rule named 'ingress_to_fortiadc_vm_9443'. The rule is configured to accept traffic from the 'public (port1)' interface to the 'private (port2)' interface, for the 'fortiadc-vm-9443' destination, always, and for all services. The action is set to 'ACCEPT'. The inspection mode is 'Flow-based'. Firewall / Network Options include NAT (disabled), IP Pool Configuration (using outgoing interface address), and various security profiles like AntiVirus, Web Filter, DNS Filter, Application Control, IPS, and File Filter, all disabled. SSL Inspection is set to 'no-inspection'. On the right side, there is a summary panel showing statistics: ID 5, Last used 5 minute(s) ago, First used 1 hour(s) ago, Hit count 142, Active sessions 1, Total bytes 9.00 MB, and Current bandwidth 0 B/s. Documentation links for Online Help, Video Tutorials, and Consolidated Policy Configuration are also present.

SSH access VIP mapping

Edit Virtual IP

VIP type: IPv4
 Name: fortadc-vm-6022
 Comments: Write a comment...
 Color: Change

Network
 Interface: public (port1)
 Type: Static NAT
 External IP address/range: 0.0.0.0
 Mapped IP address/range: 10.0.11.11

Optional Filters

Port Forwarding
 Protocol: TCP
 External service port: 6022
 Map to port: 22

OK **Cancel**

Firewall Policy

Edit Policy

Name: ingress_to_fortadc_vm_6022
 Incoming Interface: public (port1)
 Outgoing Interface: private (port2)
 Source: all
 Destination: fortadc-vm-6022
 Schedule: always
 Service: ALL
 Action: **ACCEPT**

Inspection Mode: Flow-based

Firewall / Network Options
 NAT: **On**
 IP Pool Configuration: Use Outgoing Interface Address, Use Dynamic IP Pool
 Preserve Source Port: **Off**
 Protocol Options: PROT default

Security Profiles
 AntiVirus: **Off**
 Web Filter: **Off**
 DNS Filter: **Off**
 Application Control: **Off**
 IPS: **Off**
 File Filter: **Off**
 SSL Inspection: **SSL no-inspection**

OK **Cancel**

Config Fortigate VIP for access client-VM

SSH access VIP mapping

The screenshot shows the FortiGate VM64-ALI configuration interface. The left sidebar navigation menu includes: Dashboard, Security Fabric, Network (selected), System, Policy & Objects (selected), Firewall Policy, IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs (selected), IP Pools, Protocol Options, Traffic Shapers, Traffic Shaping Policy, Traffic Shaping Profile, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, and Log & Report.

The main content area displays the "Edit Virtual IP" dialog for a new entry named "client-vm-2022". The dialog fields are as follows:

- VIP type:** IPv4
- Name:** client-vm-2022
- Comments:** Write a comment... (empty)
- Color:** Change (button)
- Network:**
 - Interface:** public (port1)
 - Type:** Static NAT
 - External IP address/range:** 0.0.0.0
 - Mapped IP address/range:** 192.168.12.60
- Optional Filters:** (radio button)
- Port Forwarding:** (radio button selected)
 - Protocol:** TCP (selected)
 - External service port:** 2022
 - Map to port:** 22

At the bottom right of the dialog are the "OK" and "Cancel" buttons.

Firewall policy

The screenshot shows the FortiGate VM64-ALI configuration interface for a Firewall Policy. The policy is named "ingress_to_client_vm_2022". It has the following settings:

- Name:** ingress_to_client_vm_2022
- Incoming Interface:** public (port1)
- Outgoing Interface:** private (port2)
- Source:** all
- Destination:** client-vm-2022
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (selected)
- Inspection Mode:** Flow-based

Firewall / Network Options:

- NAT: Enabled
- IP Pool Configuration: Use Outgoing Interface Address
- Preserve Source Port: Off
- Protocol Options: PROT default

Security Profiles:

- AntiVirus: Off
- Web Filter: Off
- DNS Filter: Off
- Application Control: Off
- IPS: Off
- File Filter: Off

SSL Inspection: SSL no-inspection

Logging Options: None

Statistics:

- ID: 3
- Last used: 30 minute(s) ago
- First used: 2 hour(s) ago
- Hit count: 20
- Active sessions: 0
- Total bytes: 50.63 MB
- Current bandwidth: 0 B/s

Documentation:

- Online Help
- Video Tutorials
- Consolidated Policy Configuration

Buttons: OK, Cancel

Config Fortigate Routing

Config static Route

On the fortigate, route entry to ACK-1 , ACK-2, fortADC subnet is needed. When traffic from TR reaches the fortigate (via TR-landing vswitch), the fortigate needs to lookup the VM inside the routing table to make a decision where to route the traffic. in this POC, the traffic will be sent back to port2.

FortiGate VM64-ALI all-fgt-active

The screenshot shows the FortiGate interface for managing static routes. The left sidebar has a 'Network' section with 'Static Routes' selected. The main area displays a table of static routes:

Destination	Gateway IP	Interface	Status
0.0.0.0/0	192.168.11.253	public (port1)	Enabled
192.168.0.0/16	192.168.12.253	private (port2)	Enabled
10.1.0.0/23	192.168.12.253	private (port2)	Enabled
10.0.0.0/23	192.168.12.253	private (port2)	Enabled
10.0.8.0/21	192.168.12.253	private (port2)	Enabled

Config Firewall Policy for East-west traffic and ACK egress traffic to internet

Two Firewall policies are required. One is for traffic from ACKs to the internet. Another one is for traffic from ACK1 to ACK2 as well as ACK1,ACK2 to fortiADC VM.

FortiGate VM64-ALI all-fgt-active

The screenshot shows the FortiGate interface for managing Firewall Policies. The left sidebar has a 'Policy & Objects' section with 'Firewall Policy' selected. The main area displays a table of firewall policies:

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
port2_port2	all	all	always	ALL	ACCEPT	Disabled	no-inspection	All 19.01 MB
port2_port1	all	all	always	ALL	ACCEPT	Enabled	default WLB monitor-all APP default IPF default SSL certificate-inspection	All 830.21 MB

◀ ▶ C Not Secure | https://47.242.124.76:8443/ng/firewall/policy/policy/standard/edit/1

FortiGate VM64-ALI all-fgt-active

Dashboard

Security Fabric

Network

System

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shapers

Traffic Shaping Policy

Traffic Shaping Profile

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

Log & Report

Edit Policy

Name: port2_port2

Incoming Interface: private (port2)

Outgoing Interface: private (port2)

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ✓ ACCEPT

Inspection Mode: Flow-based

Firewall / Network Options

NAT: off

Protocol Options: PROT default

Security Profiles

AntiVirus: off

Web Filter: off

DNS Filter: off

Application Control: off

IPS: off

File Filter: off

SSL Inspection: SSL no-inspection

Logging Options

Log Allowed Traffic: on

Security Events: All Sessions

ID: 1

Last used: 12 second(s) ago

First used: 2 hour(s) ago

Hit count: 998

Active sessions: 2

1 minute(s) ago now

Total bytes: 19.17 MB

Current bandwidth: 0 B/s

Documentation

Online Help

Video Tutorials

Consolidated Policy Configuration

OK Cancel

This screenshot shows the 'Edit Policy' dialog box for a standard firewall policy on a FortiGate VM64-ALI device. The policy is named 'port2_port2'. It has 'private (port2)' as both the incoming and outgoing interfaces. The source and destination are set to 'all'. The schedule is 'always' and the service is 'ALL'. The action is set to 'ACCEPT'. The inspection mode is 'Flow-based'. Under 'Firewall / Network Options', NAT is disabled. Protocol options are set to 'default'. Security profiles include AntiVirus, Web Filter, DNS Filter, Application Control, IPS, and File Filter, all of which are turned off. SSL inspection is set to 'SSL no-inspection'. Logging options log all sessions. The policy has an ID of 1, was last used 12 seconds ago, and first used 2 hours ago. It has a hit count of 998 and 2 active sessions. The total bytes processed is 19.17 MB and current bandwidth is 0 B/s. The interface also includes links to documentation, online help, video tutorials, and consolidated policy configuration.

Edit Policy

Name: port2_port1

Incoming Interface: private (port2)

Outgoing Interface: public (port1)

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ✓ ACCEPT

Inspection Mode: Flow-based

Firewall / Network Options:

- NAT: Off
- IP Pool Configuration: Use Outgoing Interface Address
- Preserve Source Port: Off
- Protocol Options: PROT default
- Security Profiles:

 - AntiVirus: AV default
 - Web Filter: WEB monitor-all
 - DNS Filter: Off
 - Application Control: APP default
 - IPS: IPS default
 - File Filter: Off
 - SSL Inspection: SSL certificate-inspection

Logging Options:

OK | **Cancel**

ID: 2

Last used: 29 second(s) ago

First used: 2 hour(s) ago

Hit count: 2,647

Active sessions: 4

1 minute(s) ago now

Total bytes: 830.21 MB

Current bandwidth: 0 B/s

Documentation:

- Online Help
- Video Tutorials
- Consolidated Policy Configuration

Verify the reachability

ACK1 to ACK2

POD1 to POD2 and PODs to Node IP

ACK1 POD and Node IP

Name	Status	Max. Retries	Pod IP	Nodes	Created At	Number of CPU Cores	Memory (Mi)
nginx-deployment-675d985b45-8fkvn	Running	0	10.1.0.176	cn-hongkong-10.1.0.176 cn-hongkong-10.1.0.164	Feb 22, 2022, 16:03:38 UTC+8	0	1.496 Mi
nginx-deployment-675d985b45-10zqg	Running	0	10.1.0.176	cn-hongkong-10.1.0.163 cn-hongkong-10.1.0.164	Feb 22, 2022, 16:03:38 UTC+8	0	1.504 Mi

ACK2 POD and Node IP

Name	Status	Max. Retries	Pod IP	Nodes	Created At	Number of CPU Cores	Memory (Mi)
nginx-deployment-675d985b45-8fkvn	Running	0	10.0.0.11	cn-hongkong-10.0.0.251 cn-hongkong-10.0.0.251	Feb 22, 2022, 16:03:38 UTC+8	0	1.426 Mi
nginx-deployment-675d985b45-10zqg	Running	0	10.0.0.10	cn-hongkong-10.0.0.250 cn-hongkong-10.0.0.250	Feb 22, 2022, 16:03:38 UTC+8	0	1.477 Mi

Ping Result

ACK1 POD1 can successfully ping ACK2 POD2 and is also able to access the internet . and traffic can also be inspected by fortigate.

```
root@iZj6cg0w474i2p8oykt7kqZ:~# kubectl exec -it
po/nginx-deployment-675d985b45-8fkvn -- sh
Defaulted container "nginx" out of: nginx, netshoot
# apt update
Hit:1 http://security.debian.org/debian-security stretch/updates InRelease
Ign:2 http://deb.debian.org/debian stretch InRelease
Hit:3 http://deb.debian.org/debian stretch-updates InRelease
Hit:4 http://deb.debian.org/debian stretch Release
Reading package lists... Done
Building dependency tree
Reading state information... Done
32 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
# apt install iutils-ping
Reading package lists... Done
Building dependency tree
Reading state information... Done
iutils-ping is already the newest version (3:20161105-1).
0 upgraded, 0 newly installed, 0 to remove and 32 not upgraded.
# ping 10.0.0.10 -c 1
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=59 time=3.25 ms

--- 10.0.0.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.256/3.256/3.256/0.000 ms
# ping 10.0.0.11 -c 1
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data.
64 bytes from 10.0.0.11: icmp_seq=1 ttl=59 time=3.53 ms

--- 10.0.0.11 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.530/3.530/3.530/0.000 ms
# ping 10.1.0.176 -c 1
PING 10.1.0.176 (10.1.0.176) 56(84) bytes of data.
64 bytes from 10.1.0.176: icmp_seq=1 ttl=64 time=0.029 ms

--- 10.1.0.176 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.029/0.029/0.029/0.000 ms
# ping 10.1.0.175 -c 1
PING 10.1.0.175 (10.1.0.175) 56(84) bytes of data.
64 bytes from 10.1.0.175: icmp_seq=1 ttl=62 time=0.304 ms

--- 10.1.0.175 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.304/0.304/0.304/0.000 ms
#
```

FortiGate View

The screenshot shows the FortiGate VM64-ALI interface. On the left, the navigation menu includes: Dashboard, Security Fabric, Network, System, Policy & Objects (selected), Firewall Policy, IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shapers, Traffic Shaping Policy, Traffic Shaping Profile, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, and Log & Report.

In the main content area, a summary of a selected policy (port2_port2 (1)) is displayed. The policy details are: Policy Type: Firewall, Source Interface: private (port2), Destination Interface: private (port2), Bytes: 54.10 kB, Sessions: 4, Bandwidth: 4.77 kbps. Below this, a table titled "Sessions" lists traffic flows between various IP addresses. One entry shows traffic from 10.1.0.176 to 10.0.0.175, and another shows traffic from 10.1.0.176 to 10.0.0.10.

Source	Device	Destination	Application	Protocol	Source Port	Destination Port	Bytes	Packets	Duration (seconds)
10.1.0.176		10.0.0.175	ICMP/8	ICMP	508	8	1.18 kB I	14 I	13s
10.1.0.176		10.0.0.10	ICMP/8	ICMP	497	8	48.22 kB	574	4m 47s
10.1.0.176		10.0.0.11	ICMP/8	ICMP	506	8	2.35 kB I	28 I	13s
10.1.0.176		10.0.0.10	ICMP/8	ICMP	507	8	2.35 kB I	28 I	13s

you can see the traffic between POD (10.1.0.176) and other POD
10.0.0.175, 10.0.0.10, 10.0.0.11, 10.0.0.10 etc

enable security feature for egress traffic.

to fine control what traffic allows to egress to the internet, you can enable fortigate builtin Layer 7 security feature.

The screenshot shows the "Edit Policy" dialog for a Firewall Policy. The policy configuration includes:

- Incoming Interface:** private (port2)
- Outgoing Interface:** public (port1)
- Source:** all
- Destination:** all
- Schedule:** always
- Action:** ACCEPT (selected)
- Inspection Mode:** Flow-based
- Firewall / Network Options:**
 - NAT: Enabled
 - IP Pool Configuration: Use Outgoing Interface Address
 - Preserve Source Port: Off
 - Protocol Options: PROT default
- Security Profiles:**
 - AntiVirus: AV default
 - Web Filter: WEB monitor-all
 - DNS Filter: Off
 - Application Control: APP block-high-risk
 - IPS: IPS default
 - File Filter: Off
 - SSL Inspection: SSL certificate-inspection

On the right side of the dialog, there are status metrics: ID 1, Last used 1 minute(s) ago, First used 9 hour(s) ago, Hit count 2,170, Active sessions 9, Total bytes 655.72 MB, and Current bandwidth 0 B/s. At the bottom are "OK" and "Cancel" buttons.

Firewall Policy	private (port2) → public (port1) 1
IPv4 DoS Policy	
Addresses	
Internet Service Database	
Services	
	public (port1) → private (port2) 5

After that, by default, you will see more detailed traffic information as well as you can see some suspicious traffic is dropped by default policy.

The screenshot shows the FortiGate VM64-ALI interface. On the left, the navigation menu is expanded under 'Policy & Objects' to show 'Firewall Policy'. A specific policy named 'port2_port1 (2)' is selected. The main pane displays a 'FortiView Policies by Bytes' chart for this policy. The chart shows a single data series for 'Bytes Sent' over a 1-hour period, with a total of 8.93 MB transferred across 153 sessions. Below the chart is a table of application-level traffic details:

Application	Category	Risk	Bytes	Sessions
Ubuntu.Update	Update	Low	8.47 MB	4
Apt-Get	Update	Low	447.25 kB	2
NTP	Network.Service	Low	13.30 kB	146
SSL	Network.Service	Low	4.48 kB	1

This screenshot is identical to the one above, showing the same policy configuration and traffic analysis. The chart shows 8.93 MB transferred over 133 sessions. The application traffic table remains the same, listing Ubuntu.Update, Apt-Get, NTP, and SSL traffic.

Config FortiADC as Ingress controller

FortiADC has a built-in k8s connector which can dynamically pull ACK SVC information and use that as a real server as target to create Layer 4 Load Balancer or Layer 7 Ingress Rule.

Config FortiADC to connect ACK1 and ACK2

Create ServiceAccount on both ACK

in the terraform script, create a Service Account already included. this step only required if you choose manually to deploy infrastructure .

```
root@iZj6cd1vfw01yb6cq9jsqyZ:~# kubectl cluster-info
Kubernetes control plane is running at https://10.0.0.221:6443
metrics-server is running at
https://10.0.0.221:6443/api/v1/namespaces/kube-system/services/heapster/proxy
KubeDNS is running at
https://10.0.0.221:6443/api/v1/namespaces/kube-system/services/kube-dns:dns/proxy

To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
root@iZj6cd1vfw01yb6cq9jsqyZ:~#
```

```
root@iZj6cd1vfw01yb6cq9jsqyZ:~# kubectl -n kube-system create
serviceaccount ftntconnector
serviceaccount/ftntconnector created
```

```
root@iZj6cd1vfw01yb6cq9jsqyZ:~# kubectl create clusterrolebinding
service-admin --clusterrole=cluster-admin
--serviceaccount=kube-system:ftntconnector
clusterrolebinding.rbac.authorization.k8s.io/service-admin created
```

```
root@iZj6cd1vfw01yb6cq9jsqyZ:~# kubectl describe secrets ftntconnector -n kube-system
Name:         ftntconnector-token-r2zrt
Namespace:    kube-system
Labels:       <none>
Annotations: kubernetes.io/service-account.name: ftntconnector
              kubernetes.io/service-account.uid:
              b22929da-808c-462b-97aa-441054631fa4
Type:        kubernetes.io/service-account-token

Data
=====
namespace:  11 bytes
token:
eyJhbGciOiJSUzI1NiIsImtpZCI6I1l6RTk0STNuME9feHBNNkhhT1poMDRhbjI1ZzBkN29HeEN
KbHprVWM1dE0ifQ.eyJpc3MiOiJrdWJlcmb5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXR
1cy5pby9zZXJ2aWN1YWNNjb3VudC9uYW1lc3BhY2UiOijrdWJ1LXN5c3R1bSIsImt1YmVybmv0ZX
Muaw8vc2VydmljZWfjY291bnQvc2VjcmV0Lm5hbWUiOijmdG50Y29ubmVjdG9yLXRva2VuLXIye
nJ0Iiwia3ViZXJuZXR1cy5pby9zZXJ2aWN1YWNNjb3VudC9zZXJ2aWN1LWFjY291bnQubmFtZSI6
ImZ0bnRjb25uZWN0b3IiLCJrdWJlcmb5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWN
jb3VudC51aWQiOijimjI5Mj1kYS04MDhjLTQ2MmItOTdhYS00NDEwNTQ2MzFmYTQiLCJzdWIiOij
JzeXN0ZW06c2VydmljZWfjY291bnQ6a3ViZS1zeXN0ZW06ZnRudGNvbm51Y3Rvcij9.N_77kMHu
8SEjAtgeDtzISGlaaFUY51Ek0Y1jrES1Wpt8sjxhhipYGrdyqFPfq12UyAlqDeI3W9Lnuf8_uWF
FJywhoF2o8v209bTZ_SJ5F4_mnlFjx8JhcNXRyCdy5aiuzpIKyi4UBJ6MoyMgx1FBJJ5UzpVhsr
fhCC87fOCL5f8vtmcz5NDbSzmpacwbcn1UDhXeKWamn1Y15UgkBY8WGqZesBmbtxnPPR5eeq4
s-PLwyRrtDNA9cakxKveLHQCPZCQKmRxEs_BZBrwloJnDLPC6-ZBSCK12neo6jBAKDzUdBVSGHx
wlTxxyb-HHIshfBFwsghblrTGdI-IyNbyQ
ca.crt:      1180 bytes

root@iZj6cd1vfw01yb6cq9jsqyZ:~#
```

config k8s sdn connector on fortiADC

```
root@iZj6cd1vfw01yb6cq9jsqyZ:~# ssh admin@10.0.11.11
admin@10.0.11.11's password:
FortiADC-ALI # config system sdn-connector
```

```
FortiADC-ALI (sdn-connector) # edit ack1

FortiADC-ALI (ack1) # set server 10.1.0.160

FortiADC-ALI (ack1) # set server-port 6443

FortiADC-ALI (ack1) # set secret-token
eyJhbGciOiJSUzI1NiIsImtpZCI6I1dTLUVKbkNoakNhLUQ3dExSY2tKeW1LR09VVVJZN1VYd1B
HU0N3elFJc28ifQ.eyJpc3MiOiJrdWJ1cm51dGVzL3N1cnZpY2VhY2NvdW50Iiwia3ViZXJuZXR
1cy5pb9zZXJ2aN1YWNjb3VudC9uYW1l1c3BhY2Ui0iJrdWJ1LN5c3R1bS1sImt1YmVybmV0ZX
Muaw8vc2VydmljZWfjY291bnQvc2VjcmV0Lm5hbWUi0iJmdG50Y29ubmVjdG9yLXRva2VuLXc3Z
mJyIiwia3ViZXJuZXR1cy5pb9zZXJ2aN1YWNjb3VudC9zZXJ2aN1LWFjY291bnQubmFtZSI6
ImZ0bnRjb25uZWN0b3IiLCJrdWJ1cm51dGVzLmlvL3N1cnZpY2VhY2NvdW50L3N1cnZpY2UtYWN
jb3VudC51awQi0iJyYTQzYzNjZi0zNzg5LTQzYjQtODRiYy1iMjM4MzMbhMDNiNTciLCJzdWIiOi
JzeXN0ZW06c2VydmljZWfjY291bnQ6a3ViZS1zeXN0ZW06ZnRudGNvbm51Y3Rvcij9.1LQhahSo
OMTkEqQFX77bep7yxV3hoxEdt6R8Rj3dhdJLSA05k70Wh9s6GsJ6KU6j70owYdC2XVJUbJi8v2p
dv80k5rS2LH1k4iSNLDVHjQhNdz-us0G3JA109zAseqyG_XBYfhNtebK5LFJOK1zrwL7r5SaIJ
3fRsElgXYFqZCdio3f-6_-QirL_MwQ5Uv6XSj8joc803TGp472deixwzwMwMHpTa3U1IJtNUqd
Y0xnFYqE56YkQMM7sqaUR85SbHSgFf8kYgU21iFQQltpsM1BLow7IvViZ_xEf1IvSGm8uFrRe01
430mJ4vT1VvGVvCXsFAb-o5ew5CI0CtufA

FortiADC-ALI (ack1) # next

FortiADC-ALI (sdn-connector) # end

FortiADC-ALI # config system sdn-connector

FortiADC-ALI (sdn-connector) # edit ack2

FortiADC-ALI (ack2) # set server 10.0.0.247

FortiADC-ALI (ack2) # set server-port 6443

FortiADC-ALI (ack2) # set secret-token
eyJhbGciOiJSUzI1NiIsImtpZCI6I1B0Q3JuWlhvRU9NVXloVVpzQm150VEyZjZJSDFwTk1YZXN
ueHJZS2ZRS1EifQ.eyJpc3MiOiJrdWJ1cm51dGVzL3N1cnZpY2VhY2NvdW50Iiwia3ViZXJuZXR
1cy5pb9zZXJ2aN1YWNjb3VudC9uYW1l1c3BhY2Ui0iJrdWJ1LN5c3R1bS1sImt1YmVybmV0ZX
Muaw8vc2VydmljZWfjY291bnQvc2VjcmV0Lm5hbWUi0iJmdG50Y29ubmVjdG9yLXRva2VuLWd6d
3o0Iiwia3ViZXJuZXR1cy5pb9zZXJ2aN1YWNjb3VudC9zZXJ2aN1LWFjY291bnQubmFtZSI6
ImZ0bnRjb25uZWN0b3IiLCJrdWJ1cm51dGVzLmlvL3N1cnZpY2VhY2NvdW50L3N1cnZpY2UtYWN
jb3VudC51awQi0iIyMDQ1MTMwMy02YmYxLTQ1MGQtYTVkNi0wMGE4NDU1ZTAzzjYiLCJzdWIiOi
JzeXN0ZW06c2VydmljZWfjY291bnQ6a3ViZS1zeXN0ZW06ZnRudGNvbm51Y3Rvcij9.YE48oJo-
cvIFzeUj7kSjzGJprY7aw3o6RLv9npizXGe17SfVb_nJaqc3DBVCge4CdM0fAhd0FA81RkiQi2W
```

```
LLFk6ya4C1sjowYP6wviOpxAwBDMK7qyfrKOJJj9ipyjtRIMWDz4b8MiYuzJxsNyRfxg1U1pNDf  
LzSrJPKbeSzAN8pUci3KGgiyCZM8G06EEMFOPWyKSUTk0HQDLibMrFi60Pj1D9LW9-CQWfh-FC  
yp9zu2husdHB17itHxhsI17KwVlu_7fu5zkB0n3mnw0XuzT8EY8h2pn1Xzsan6sCahIcNkyNCSk  
P3Ny7fkXI9MCTsac7M_Y9JxBoSn2m_sw-A
```

```
FortiADC-ALI (ack2) # end
```

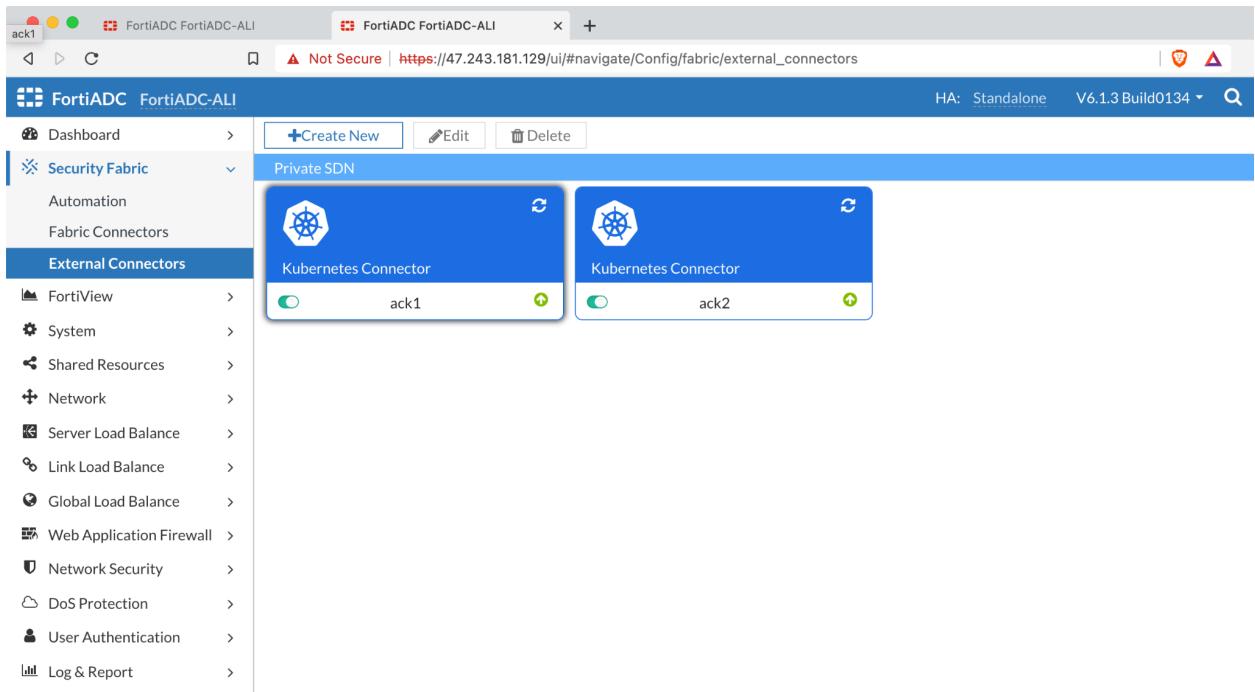
```
FortiADC-ALI #
```

once done. on the fortiADC console. You will see below, an green icon indicating the success connection between FortiADC and both ACKs.

you can use the browser to logon fortiadc GUI to take a look.

The fortiadc GUI can be accessed via fortigate VIP:9443 or fortiadc public IP:443 (if configured).

The screenshot shows the FortiADC FortiADC-ALI interface. The left sidebar has a navigation menu with items like Dashboard, Security Fabric (which is currently selected), External Connectors, and various system and network-related options. The main content area is titled "Private SDN" and displays two entries for "Kubernetes Connector". Each entry has a blue card with a white gear icon, the text "Kubernetes Connector", and a name (either "ack1" or "ack2"). To the right of each name is a green circular icon with a white checkmark, indicating a successful connection. There are also edit and delete buttons above the list.



Create ingress rule for ACK1 nodeport service

Create a Real Server Pool on FortiADC

Real Server Pool

Name: ack1_nginx_nodeport_30163
Type: Static
SDN Connector: ack1
Service: K8S_ServiceName=nginx-30163
Health Check: LB_HLTHCK_ICMP

Health Check Relationship

Selected Items: LB_HLTHCK_ICMP
Available Items: Create New, LB_HLTHCK_HTTP, LB_HLTHCK_HTTPS, LB_HLTHCK_TCP_ECHO

Health Check List

Double-click to deselect. Drag to reorder.

Direct Route Mode

Real Server SSL Profile: NONE

Member

<input type="checkbox"/>	ID	Name	Address	Health Check	Port	<input type="checkbox"/>
<input type="checkbox"/>	1	ack1_cn-hongkong.10.1.0.163	10.1.0.163	inherited	30163	<input type="checkbox"/>
<input type="checkbox"/>	2	ack1_cn-hongkong.10.1.0.164	10.1.0.164	inherited	30163	<input type="checkbox"/>

Show 1 to 2 of 2 entries Show 25 entries Previous 1 Next

Save Cancel

After clicking Save, the Member will be automatically populated.

Do same for nginx on ACK2

The screenshot shows the FortiADC FortiADC-ALI interface. The left sidebar navigation includes: Dashboard, Security Fabric, FortiView, System, Shared Resources, Network, Server Load Balance (selected), Virtual Server, Application Resources, Application Optimization, Real Server Pool (selected), Scripting, SSL-FP Resources, Link Load Balance, Global Load Balance, Web Application Firewall, Network Security, DoS Protection, User Authentication, and Log & Report.

The main panel displays the "Real Server Pool" configuration for a K8S service. The "Name" field is set to "ack2_nginx_nodeport_30163". The "Type" is "Static". The "SDN Connector" is "ack2". The "Service" is "K8S_ServiceName=nginx-30163". The "Health Check" section shows an "AND" relationship with "Selected Items" including "LB_HLTHCK_ICMP". The "Available Items" list includes "Create New", "LB_HLTHCK_HTTP", "LB_HLTHCK_HTTPS", and "LB_HLTHCK_TCP_ECHO". The "Health Check List" section allows double-clicking to deselect or reorder items. The "Direct Route Mode" is off. The "Real Server SSL Profile" is "NONE". The "Member" section lists two members: "ack2_cn-hongkong.10.0.0.250" and "ack2_cn-hongkong.10.0.0.251", both with "inherited" health checks, port 30163, and address 10.0.0.250/251. The "Save" and "Cancel" buttons are at the bottom.

Create Layer 7 Ingress Rule with RealServer Pool

The screenshot shows the FortiADC FortiADC-ALI interface. The left sidebar navigation includes: Dashboard, Security Fabric, FortiView, System, Shared Resources, Network, Server Load Balance (selected), Virtual Server (selected), Application Resources, Application Optimization, Real Server Pool, Scripting, SSL-FP Resources, Link Load Balance, Global Load Balance, Web Application Firewall, Network Security, DoS Protection, User Authentication, and Log & Report.

The main panel displays the "Virtual Server" configuration. The "Basic" tab is selected. The "Name" is "nginxonack1", "Type" is "Layer 7", "Status" is "Enable", "Address Type" is "IPv4", "Traffic Group" is "default", and "Comments" is "Specify the comments". The "Specifics" section includes "Schedule Pool", "Content Routing", and "Content Rewriting". The "NAT Source Pool List" section shows "Selected Items" including "Create New" and "10-0-11-12". The "Transaction Rate Limit" is set to "0". The "Save" and "Cancel" buttons are at the bottom.

Choose Layer 7 ingress.

FortiADC FortiADC-ALI

HA: Standalone V6.1.3 Build0134

The Server IP is fortiADC interface IP address; you can also choose another secondary IP once that IP has been added to fortiADC ECS. The port is set to 8080. The Profile uses LB_PROF_HTTPS which is default for HTTPS and also chooses the default Client SSL Profile and in the RealServer Pool , selects the correct real server pool.

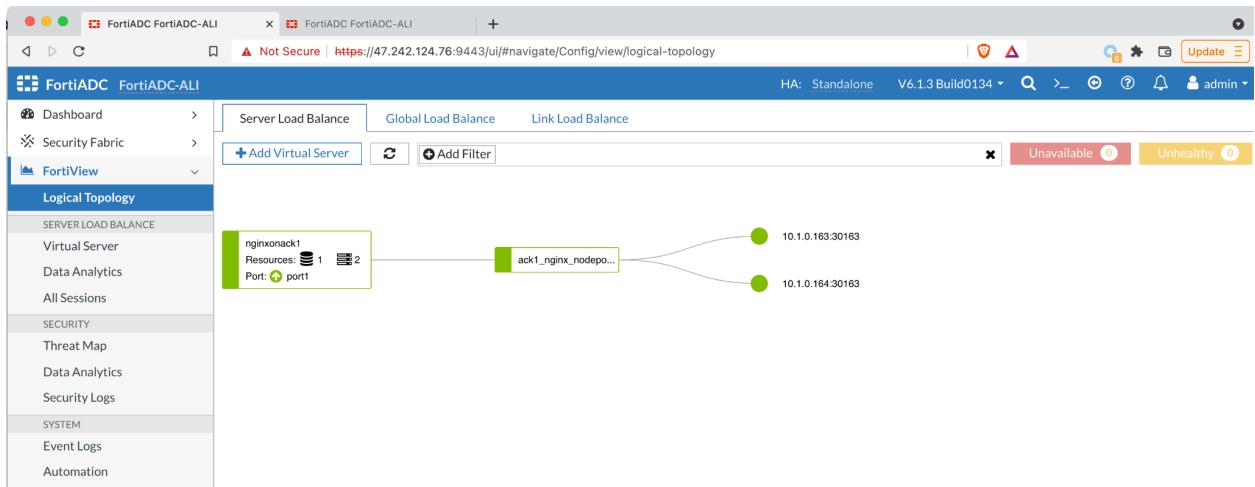
Associate with WAF profile

The screenshot shows the FortiADC interface for managing a Virtual Server. The left sidebar is collapsed, and the main area is titled 'Virtual Server'. The 'Security' tab is selected. Under 'WAF Profile', 'High-Level-Security' is chosen. Other dropdowns for 'AV Profile', 'DoS Protection Profile', and 'Captcha Profile' are set to 'Click to select' and 'LB_CAPTCHA_PROFILE_DEFAULT' respectively. At the bottom right are 'Save' and 'Cancel' buttons.

Enable Monitoring

The screenshot shows the FortiADC interface for managing a Virtual Server. The left sidebar is collapsed, and the main area is titled 'Virtual Server'. The 'Monitoring' tab is selected. Under 'Traffic Log', a green switch icon indicates it is enabled. A tooltip explains: 'Traffic logging should be used mainly for debugging; traffic logging will consume extensive memory and CPU resources. Please disable traffic logging after debugging is complete.' Under 'FortiView', a green switch icon indicates it is enabled. Under 'WCCP', a grey switch icon indicates it is disabled. At the bottom right are 'Save' and 'Cancel' buttons.

after that, you will see a ingress rule has been created for nodeport service on ACK1



Verify the result

Access via fortiadc internal IP address (from client-vm)

```
root@iZj6cd1vfw01yb6cq9jsqyZ:~# curl -k https://10.0.11.11:8080
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
body {
    width: 35em;
    margin: 0 auto;
    font-family: Tahoma, Verdana, Arial, sans-serif;
}
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

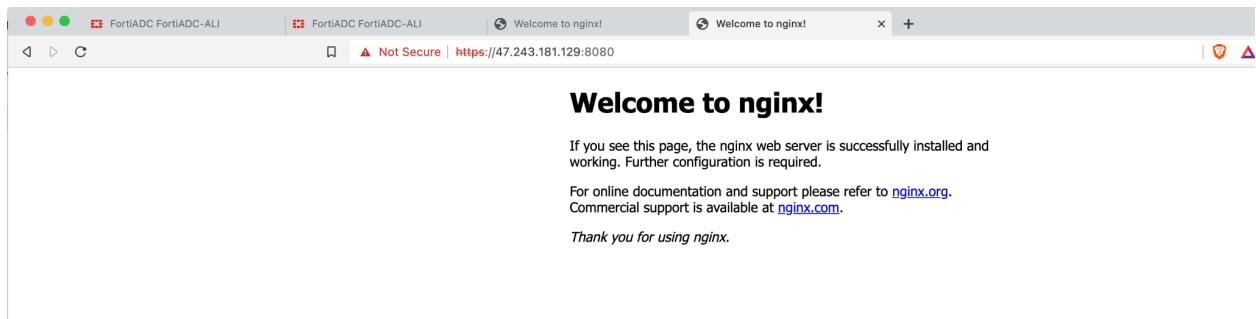
<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
```

```
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
root@iZj6cd1vfw01yb6cq9jsqyZ:~#
```

access via fortiadc external IP

If we have a public IP or EIP assigned to fortiadc , we can also use public IP to access nginx instead of using internal IP.



Access via Fortigate public IP if fortiadc has no public IP associated

The ingress for nginx nodeport service is configured with an internal IP address on fortiadc, what if we want to give external access to this nodeport service ? We can create a Layer 4 Entry on Fortigate for that with a VIP/DNAT entry. This portion of config has already been included in the terraform script. Below is only required if created manually.

Create a Virtual IP on fortigate

create virtual IP 0.0.0.0:8080 to map to 10.0.11.11:8080

The screenshot shows the FortiGate VM64-ALI interface with the title bar "FortiGate VM64-ALI all-fgt-active". The left sidebar has a green highlighted section for "Virtual IPs". The main content area is titled "Edit Virtual IP" and contains the following configuration:

- VIP type:** IPv4
- Name:** nginxonack1
- Comments:** Write a comment... 0/255
- Color:** Change
- Network:**
 - Interface:** public (port1)
 - Type:** Static NAT
 - External IP address/range:** 0.0.0.0
 - Mapped IP address/range:** 10.0.11.11
- Optional Filters:** (radio button)
- Port Forwarding:** (radio button, selected)
- Protocol:** TCP (selected), UDP, SCTP, ICMP
- External service port:** 8080
- Map to port:** 8080

At the bottom right are "OK" and "Cancel" buttons.

Create a Firewall Policy to enable this traffic and apply security policy such as IPS policy etc.,

Verify the result

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com.

Thank you for using nginx.

scale out the node on ACK1

let's scale out the ACK worknode from 2 to 3.

The screenshot shows two identical pages from the Alibaba Cloud console, both titled "Node Pools" under the "Cluster Information" section. The left page shows a single node pool named "default-nodepool" with 3 nodes, labeled as "Scaling Out". The right page shows the same node pool after scaling, now with 3 nodes, labeled as "Active". Both pages include filters for "Name", "Type", "Instance Type", "Status", "Nodes", "Operating System", and "Updated At". Buttons for "Create Node Pool", "Sync Node Pool", and "Configure Auto Scaling" are visible at the top right. The bottom right of each page shows pagination controls and a link to "Help Documentation".

FortiADC will automatically update the real server

The screenshot shows the FortiADC interface with the "Logical Topology" tab selected. On the left, there's a sidebar with "Dashboard", "Security Fabric", "FortiView", "Logical Topology", "SERVER LOAD BALANCE", "SECURITY", and "Data Analytics". The main area displays a logical topology diagram. A green box labeled "nginxonack1" contains "Resources: 1" and "Port: port1". An arrow points from this box to a green box labeled "ack1_nginx_nodepo...". From this second box, three arrows point to three green circles representing IP addresses: "10.1.0.163:30163", "10.1.0.164:30163", and "10.1.0.177:30163". The top status bar indicates "Not Secure | https://47.242.124.76:9443/ui/#navigate/Config/view/logical-topology". The top right shows "HA: Standalone", "V6.1.3 Build0134", and various navigation icons.

simulate the attack to nodeport service via ingress entry

```
root@iZj6cd1vfw01yb6cq9jsqyZ:~# curl -k -H "User-Agent: () { :; }; /bin/ls"
https://10.0.11.11:8080
<html><body><h1>
403 Forbidden</h1>
Request forbidden by administrative rules.
</body></html>
```

```
root@iZj6cd1vfw01yb6cq9jsqyZ:~#
```

you can see the attack to the ingress has been administratively forbidden . You can also check the fortiADC security log for that detail (after enabling security log in log setting). FortiADC has captured it's ShellShock attack and action accordingly .

The screenshot shows the FortiADC FortiADC-ALI interface. The left sidebar has a 'Log & Report' section with 'Security Log' selected. The main area displays a table of security logs. One log entry is expanded to show detailed information:

Date	Time	WAF Subcategory	Severity	Source	Destination	Action	Details
2022-02-22	01:09:46	Attacks(Signature)	high	192.168.12.60	10.0.11.11	deny	<pre>Date: 2022-02-22 Time: 01:09:46 Log ID: 0202006004 Log Level: alert Message ID: 45 Signature ID: 1002014010 Severity: high Service: https VS Name: nginxonstack1 Source: 192.168.12.60 Source Port: 55882 Destination: 10.0.11.11 Destination Port: 8080 Source Country: Reserved Destination Country: Reserved Type: attack Sub Type: waf WAF Subcategory: Attacks(Signature) Vdom: root OWASP Top10: A9:2017-Using Components with Known Vulnerabilities Action: deny HTTP URL: / HTTP Host: 10.0.11.11:8080 Message: "Attack ID: 1002014010 Desc: "This rule prevents attackers from executing arbitrary commands by GNU Bash Shellshock vulnerability." Module: "Known Exploits" Check Type: "Generic Exploit" Packet Header: Accept: */* User-Agent: () ; ; /bin/ls HTTP Method: GET User Agent: () ; ; /bin/ls Example: GET /index.html HTTP/1.1 Host: www.example.com Connection: keep-alive User-Agent: () ; ; /bin/bash -c cat /etc/passwd Accept: text/html,application/xhtml+xml,application/xml Accept-Encoding: gzip, deflate, br Matched Part: none</pre>

Config FortiGate K8s Connector for refined control

Config K8S Connector

To refine the control of K8S objects, for example, down to individual pods based on Label or based on service name. We can configure the K8S Connector on Fortigate to communicate with ACK to retrieve k8s objects dynamically.

get the cluster IP and SA secret from ACK1 and ACK2

```
root@iZj6cg0w474i2p8oykt7kqZ:~# kubectl cluster-info  
--kubeconfig=/root/.kube/config_ack1  
  
Kubernetes control plane is running at https://10.1.0.160:6443  
metrics-server is running at  
https://10.1.0.160:6443/api/v1/namespaces/kube-system/services/heapster/proxy  
KubeDNS is running at  
https://10.1.0.160:6443/api/v1/namespaces/kube-system/services/kube-dns:dns/proxy
```

To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.

```
root@iZj6cg0w474i2p8oykt7kqZ:~# kubectl describe secret ftntconnector -n kube-system --kubeconfig=/root/.kube/config_ack1
```

```
Name:          ftntconnector-token-w7fbr  
Namespace:    kube-system  
Labels:        <none>  
Annotations:   kubernetes.io/service-account.name: ftntconnector  
               kubernetes.io/service-account.uid:  
               ca43c3cf-3789-43b4-84bc-b23830a03b57
```

```
Type:  kubernetes.io/service-account-token
```

```
Data
```

```
====
```

```
ca.crt:      1180 bytes  
namespace:  11 bytes  
token:  
eyJhbGciOiJSUzI1NiIsImtpZCI6IldTLUVKbkNoakNhLUQ3dExSY2tKeWlLR09VWVJZN1VYd1B
```

```
HU0N3e1FJc28ifQ.eyJpc3MiOiJrdWJlcmb5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXR  
1cy5pb9zZXJ2aWN1YWNgjb3VudC9uYW1lc3BhY2UiOiJrdWJ1LXN5c3R1bSIsImt1YmVybmV0ZX  
Muaw8vc2VydmljZWfjY291bnQvc2VjcmV0Lm5hbWUiOiJmdG50Y29ubmVjdG9yLXRva2VuLXc3Z  
mJyIiwia3ViZXJuZXR1cy5pb9zZXJ2aWN1YWNgjb3VudC9zZXJ2aWN1LWFjY291bnQubmFtZSI6  
ImZ0bnRjb25uZWN0b3IiLCJrdWJlcmb5ldGVzLm1vL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWN  
jb3VudC51aWQiOijYTQzYzNjZi0zNzg5LTQzYjQtODRiYy1iMjM4MzMbhMDNiNTciLCJzdWIiOi  
JzeXN0ZW06c2VydmljZWfjY291bnQ6a3ViZS1zeXN0ZW06ZnRudGNvbm51Y3Rvcij9.1LQhahSo  
OMTkEqQFX77bep7yxV3hoxEdt6R8Rj3dhJLSA05k70Wh9s6GsJ6KU6j70owYdC2XVJUbJi8v2p  
dV80k5rS2LH1k4iSNLDVHjQhNdnz-us0G3JA109zAseqyG_XBYfhNtebK5LFJ0K1zrwL7r5SaIJ  
3fRsElgXYFqZCdio3f-6_-QirL_MwQ5Uv6XSj8joc803TGp472deixwzwnMwMHpTa3U1IJtNUqd  
Y0xnFYqE56YkQMM7sqaUR85SbHSgFf8kYgU21iFQQ1tpsM1BLow7IvViZ_xEf1IvSGm8uFrRe01  
430mJ4vT1VvGVvCXsFAb-o5ew5CI0Ctufa
```

```
root@iZj6cg0w474i2p8oykt7kqZ:~# kubectl cluster-info  
--kubeconfig=/root/.kube/config_ack2  
Kubernetes control plane is running at https://10.0.0.247:6443  
metrics-server is running at  
https://10.0.0.247:6443/api/v1/namespaces/kube-system/services/heapster/proxy  
KubeDNS is running at  
https://10.0.0.247:6443/api/v1/namespaces/kube-system/services/kube-dns:dns/proxy
```

To further **debug and** diagnose cluster problems, use '**kubectl cluster-info dump**'.

```
root@iZj6cg0w474i2p8oykt7kqZ:~# kubectl describe secret ftntconnector -n  
kube-system --kubeconfig=/root/.kube/config_ack2  
Name:          ftntconnector-token-gzwz4  
Namespace:    kube-system  
Labels:        <none>  
Annotations:   kubernetes.io/service-account.name: ftntconnector  
               kubernetes.io/service-account.uid:  
20451303-6bf1-450d-a5d6-00a8455e03f6
```

Type: kubernetes.io/service-account-token

```
Data  
=====  
ca.crt:      1180 bytes  
namespace:  11 bytes  
token:  
eyJhbGciOiJSUzI1NiIsImtpZCI6IlBOQ3JuWlhvRU9NVXloVVpzQm150VEyZjZJSDFwTk1YZXN  
ueHJZS2ZRS1EifQ.eyJpc3MiOiJrdWJlcmb5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXR
```

```
1cy5pb9zZXJ2aWN1YWNjb3VudC9uYW1lc3BhY2Ui0iJrdWJ1LXN5c3R1bSIsImt1YmVybmV0ZX
Muaw8vc2VydmljZWFjY291bnQvc2VjcmV0Lm5hbWUi0iJmdG50Y29ubmVjdG9yLXRva2VuLwd6d
3o0Iiwi3ViZXJuZXR1cy5pb9zZXJ2aWN1YWNjb3VudC9zZXJ2aWN1LWFjY291bnQubmFtZSI6
ImZ0bnRjb25uZWN0b3IiLCJrdWJ1cm5ldGVzLmlvL3N1cnZpY2vhY2NvdW50L3N1cnZpY2UtYWN
jb3VudC51aWQi0iIyMDQ1MTMwMy02YmYxLTQ1MGQtYTVkNi0wMGE4NDU1ZTAzZjYiLCJzdWIi0i
JzeXN0ZW06c2VydmljZWFjY291bnQ6a3ViZS1zeXN0ZW06ZnRudGNvbm51Y3Rvcij9.YE48oJo-
cvIFzeUj7kSjzGJprY7aw3o6RLv9npizXGe17sfVb_nJaqc3DBVCge4CdMOfAhd0FA81RkiQi2W
LLFk6ya4C1sjoWYP6wvi0pxAWBDMK7qyfrKOJJj9ipyjtRIMWDz4b8MiYuzJxsNyRfxglU1pNDF
LzSrJPKbeSzAN8pUci3KGgiyCZM8G06EEMFOPWyKSUTk0HQDLibMrFi60PJj1D9LW9-CQWfh-FC
yp9zu2husdHB17itHxhsI17KwVlu_7fu5zkB0n3mnw0XUzT8EY8h2pn1Xzsan6sCahIcNkyNCSk
P3Ny7fkXI9MCTsac7M_Y9JxBoSn2m_sw-A
```

root@iZj6cg0w474i2p8oykt7kqZ:~#

Config k8s connector on fortigate

Fill in ACK1 and ACK2 cluster IP and SA account token.

The screenshot shows the FortiGate VM64-ALI interface with the title "Edit External Connector". The left sidebar is titled "Security Fabric" and includes sections for Physical Topology, Logical Topology, Security Rating, Automation, Fabric Connectors, and External Connectors. Under External Connectors, there are Network, System, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, and Log & Report. The main content area is titled "Edit External Connector" and shows a "Private SDN" section with a "Kubernetes" icon. The "Connector Settings" section contains a "Name" field set to "ack1", a "Status" field with "Enabled" checked, and an "Update Interval" field with "Use Default" selected. The "Kubernetes Connector" section includes an "IP" field set to "10.1.0.160", a "Port" field with "Use Default" selected, and a "Secret token" field containing "*****". On the right side, there are "Status" (Up), "Available Filters" (73), and "Public SDN Connector Setup Guides" for AWS, Google Cloud Platform, Microsoft Azure, and Oracle Cloud Infrastructure. Below that are "Private SDN Connector Setup Guides" for Cisco Application Centric Infrastructure, Nuage Virtualized Services Platform, OpenStack Connector, and VMware NSX. At the bottom are links for Documentation, Online Help, and Video Tutorials.

FortiGate VM64-ALI ali-fgt-active

Dashboard > Edit External Connector

Security Fabric

- Physical Topology
- Logical Topology
- Security Rating
- Automation
- Fabric Connectors

External Connectors

- + Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
- WiFi & Switch Controller
- Log & Report

Kubernetes

Private SDN

Connector Settings

Name: ack2
Status: Enabled
Update Interval: Use Default

Kubernetes Connector

IP: 10.0.0.247
Port: Use Default
Secret token: *****

OK Cancel

Status: Up

Available Filters: 73 View

Public SDN Connector Setup Guides

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Oracle Cloud Infrastructure

Private SDN Connector Setup Guides

- Cisco Application Centric Infrastructure
- Nuage Virtualized Services Platform
- OpenStack Connector
- VMware NSX

Documentation

- Online Help
- Video Tutorials

once successful, you shall see

FortiGate VM64-ALI ali-fgt-active

Dashboard > + Create New Edit Delete

Security Fabric

- Physical Topology
- Logical Topology
- Security Rating
- Automation
- Fabric Connectors

External Connectors

- + Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
- WiFi & Switch Controller
- Log & Report

Private SDN

Kubernetes Connector

ack1

Kubernetes Connector

ack2

Create Firewall Policy based on dynamic object

Now we have the k8s connector configured, the fortigate can dynamically pull the k8s object and use it in the firewall policy.

Define the Address object

The screenshot shows the FortiGate VM64-ALI configuration interface. The left sidebar navigation includes Dashboard, Security Fabric, Network, System, Policy & Objects (selected), Firewall Policy, IPv4 DoS Policy, Addresses (selected), Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shapers, Traffic Shaping Policy, Traffic Shaping Profile, Virtual Servers, Health Check, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, and Log & Report. The main panel shows the 'Edit Address' configuration for a 'Dynamic' SDN Connector named 'ack2'. The 'SDN address type' is set to 'Private'. The 'Filter' dropdown displays a list of K8s objects, with 'K8S_Label.app=nginx' highlighted. At the bottom right are 'OK' and 'Cancel' buttons.

On the Filter Dropbox, we can see K8s Object ,can be filtered by use namespace, Label, Service,Node, PODname etc.,

Once done, the ip address of the dynamic object will be obtained.

Name	Details	Interface
FABRIC_DEVICE	0.0.0.0	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0	0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root) 2
all	0.0.0.0	8
client-vm	192.168.12.60/32	0
fortiadc-vm	10.0.11.11/32	0
none	0.0.0.0/32	0

FQDN	Address	nginx-app-by-label
gmail.com		gmail.com
login.microsoft.com		login.microsoft.com
login.microsoftonline.com		login.microsoftonline.com
login.windows.net		login.windows.net
*dropbox.com		*dropbox.com
*google.com		*google.com

Address Group	nginx-app-by-label
G Suite	gmail.com, wildcard.google.com
Microsoft Office 365	login.microsoftonline.com, login.microsoft.com, login.windows.net

then We can use the address object in firewall policy. Once the object changes on k8s , for example, due to scale out, as long as the filter does not change, the new ip will be dynamically updated on the fortigate side.

create firewall policy

FortiGate VM64-ALI ali-fgt-active
[Logout](#)

Dashboard
>
New Policy

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shapers

Traffic Shaping Policy

Traffic Shaping Profile

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

Log & Report

Name:

Incoming Interface:

Outgoing Interface:

Source:

Destination:

Schedule:

Service:

Action:

Inspection Mode:

Firewall / Network Options

NAT:

IP Pool Configuration:

Preserve Source Port:

Protocol Options:

Security Profiles

AntiVirus:

Web Filter:

DNS Filter:

Application Control:

IPS:

File Filter:

SSL Inspection:

Logging Options

Log Allowed Traffic: Security Events All Sessions

Generate Logs when Session Starts:

Address:

Type: Dynamic

Sub Type: Fabric Connector Address

SDN Connector:

Filter: K8S_Label.app=nginx

Interface:

Resolved To: 10.0.0.10 10.0.0.11

References: 0

[Edit](#)

[OK](#)
[Cancel](#)

then a more fine grained policy for POD that with label nginx is created.

This gives you the grainer control to the k8s object.

