Paloalto

VM-Series on OCB Flex Engine Installation and Deployment Guide

30th January 2021

Version 2.0

document control

date	version no.	author	change/addition
12 – September 2018	1.0	Ahmad Samak	Creation
30 January 2021	2.0	Ahmad Samak	Modification and update (Deployment of Palo Alto KVM release 9.1.3) Modification and update (Software Update of Palo Alto KVM release 9.1.3 to release 9.1.4)

table of contents

1 References

Reference	Description	Link to document
[1]	OCB FE Help Center	https://docs.prod-cloud-ocb.orange-business.com/en-us/index.html
[2]	VM-Series Deployment Guide	https://www.paloaltonetworks.com/documentation/81/virtualization/virtualization

2 Introduction

For new applications and service deployment, many organizations are moving to the public cloud. Instead of developing new applications and running them on their on-premises hardware, these organizations are increasingly using infrastructure hosted and maintained by remote vendors. These Infrastructure-as-a-Service (IaaS) environments, originally used by startups or niche purposes by enterprises, are increasingly being used for applications that provide business differentiation. Applications deployed in public cloud IaaS environments are becoming more prevalent because they offer several productivity and scale benefits to an organization.

Purpose of This Guide

Although IaaS providers are responsible for ensuring the security and availability of their infrastructure, ultimately, organizations are still responsible for the security of the applications and data. This reference architecture describes how an organization can use the Palo Alto Networks® VM-Series firewalls running PAN-OS to bring visibility, control, and protection to your applications built in Orange Flex Engine.

This document provides architectural guidance for solution architects and engineers who are familiar with the next-generation firewall but not Orange Flex Engine. It links the technical aspects of the Orange FE and Palo Alto Networks solution together before exploring the technical design models of the architecture. Use this guide as a roadmap for architectural discussions between Palo Alto Networks and your organization

3 Public Cloud and On-Premises Differences

Organizations generally move to the public cloud with the goals of increasing scale and reducing time to deployment. Achieving these goals requires application architectures built specifically for the public cloud. Before you can architect for the public cloud, you must understand how it is different from traditional on-premises environments.

3.1 Scaling Methods

Traditionally, organizations scale on-premises deployments through the purchase of devices that have increased performance capacity. Scaling up an on-premises deployment in this method makes sense because the devices are typically purchased to last year's requirements and must be sized to satisfy the performance requirements during their lifetime.

Public cloud environments focus on scaling out the deployment instead of scaling up. This architectural difference stems primarily from the capability of public cloud environments to dynamically increase or decrease the number of resources you have allocated. In the public cloud, infrastructure used to satisfy performance requirements can have a lifetime in minutes instead of years. Instead of purchasing extra capacity for use at some time in the future, the dynamic nature of the public cloud allows you to allocate just the right amount of resources required to service the application.

What this means in practice is that to architect an application for the cloud, you need to distribute functionality, and each functional area should be built to scale out as necessary. Typically, this means a load balancer distributes traffic across a pool of identically configured resources. When changes occur in the application traffic, the number of resources you have allocated to the pool can be increased or decreased dynamically. This design method provides scale and resiliency. However, the application architecture must take into account that the resources are transient. For example, the application state should not be stored in the networking infrastructure or in the frontend application servers. Instead, store state information on the client or persistent storage services.

The ability to scale a cloud architecture extends not only to the capacity of an application but also capacity to deploy applications globally. Scaling an application to a new region in a traditional on-premises deployment requires significant investment and planning. Public cloud architectures are location-agnostic and can be deployed globally in a consistent amount of time.

3.2 Reduced Time to Deployment

To achieve the goals of a reduced time to deployment you have to have a development and deployment process that is repeatable and reacts to changes quickly. DevOps workflows are the primary method for implementing this process. DevOps workflows are highly dependent on the ability to automate, as much as possible, the process of deploying a resource or application. In practice, this means the cloud infrastructure, as well as the resources running on it, needs to be able to be bootstrapped, configured, updated, and destroyed programmatically. Compared to traditional on-premises deployments where devices deployment, configuration, and operation happen manually, automated workflows in a public cloud environment can significantly reduce time to deployment.

In fact, automation is so core to cloud design that many cloud application architectures deploy new capabilities through the automated build-out of new resources instead of updating the existing ones. This type of cloud architecture provides a number of benefits, not the least of which is the ability phase in the changes to a subset of the traffic as well as the ability to quickly roll back the changes by redirecting traffic from the new resources to the old.

3.3 Security Integration

VM-Series firewalls enable you to securely implement scalable cloud architectures and reduce time to deployment. Capabilities of VM-Series firewalls leveraged to achieve this include:

- Application visibility—VM-Series firewalls natively analyze all traffic in a single pass to determine the application, content, and user identity. The application, content, and user are used as core elements of your security policy and for visibility, reporting, and incident investigation.

- Prevent advanced attacks at the application level—Attacks, much like many applications, can use any port, rendering traditional prevention mechanisms ineffective. VM-Series firewalls allow you to use Threat Prevention and the WildFire™ cloud-based threat analysis service to apply application-specific threat prevention policies that block exploits, malware, and previously unknown threats from infecting your cloud.

- Consistent policy and management—Panorama™ network security management enables you to manage your VM-Series deployments across multiple cloud environments, along with your physical security appliances, thereby ensuring policy consistency and cohesiveness. Rich, centralized logging and reporting capabilities provide visibility into virtualized applications, users, and content.

- Automation features to reduce time to deployment—VM-Series firewalls include management features that enable you to integrate security into your public cloud development projects. You can use bootstrapping to automatically provision a firewall with a working configuration, complete with licenses and subscriptions, and then auto-register itself with Panorama. Firewall performance metrics and health information can be published to Azure Application Insights, so you can create automate actions based on performance and usage patterns. To automate policy updates when workloads change, a fully documented XML API and dynamic address groups allow VM-Series firewalls to consume external data in the form of tags that can drive policy updates dynamically. The result is that new applications and next-generation security can be deployed simultaneously in an automated manner.

4 License Options

You can license VM-Series firewalls on OCB FE with licenses purchased through regular Palo Alto Networks channels.

Bring your own license (BYOL) and VM-Series ELA—A license that you purchase from a partner, reseller, or directly from Palo Alto Networks. VM-Series firewalls support all capacity, support, and subscription licenses in BYOL.

When using your own licenses, you license VM-Series firewalls like a traditionally deployed appliance, and you must apply a license authorization code. After you apply the code to the device, the device registers with the Palo Alto Networks support portal and obtains information about its capacity and subscriptions. Subscription licenses include Threat Prevention, PAN-DB URL Filtering, AutoFocus™, GlobalProtect, and WildFire.

To accelerate firewall deployment, the VM-Series enterprise licensing agreement (ELA) provides a fixed price licensing option allowing unlimited deployment of VM-Series firewalls with BYOL. Palo Alto Networks offers licenses in one and three-year term agreements with no true-up at the end of the term.

The VM-Series ELA includes four components:

- Your choice of single VM-Series model that you can deploy as many times as you want and in as many virtual environments as you want. All of your VM-Series ELA deployments use a single license authorization code, which allows for easier automation and simplifies the deployment of firewalls.

- Threat Prevention, WildFire, GlobalProtect and PAN-DB Subscriptions for every VM-Series firewall deployed as part of the VM-Series ELA.

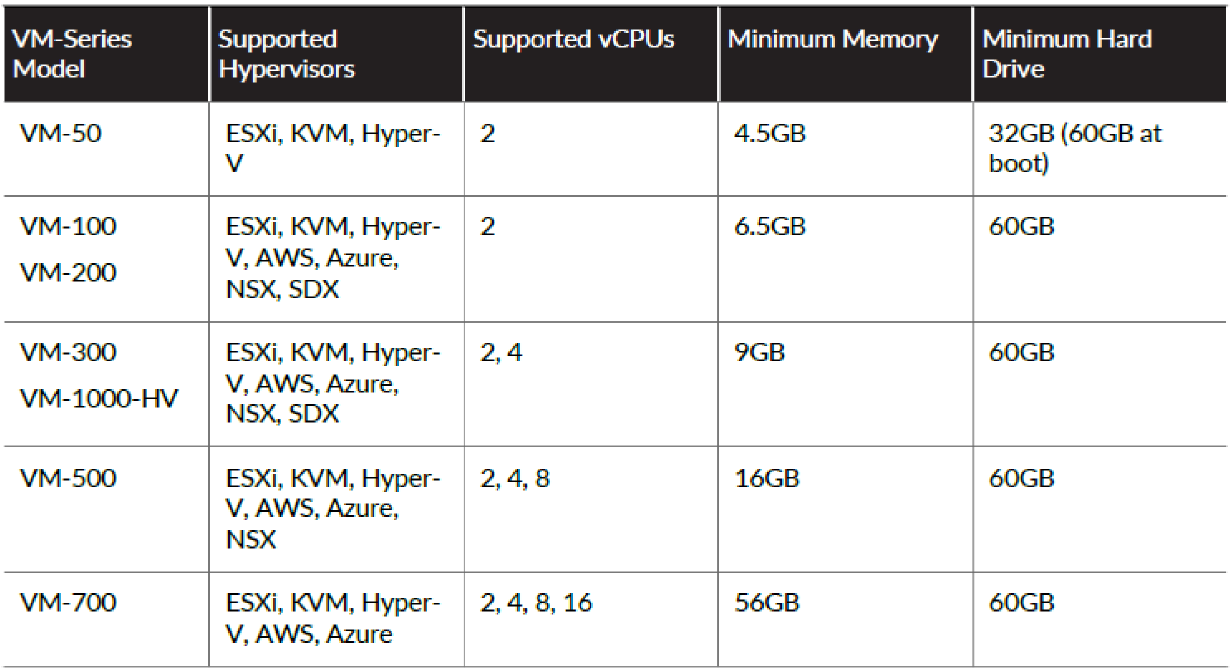
- Unlimited deployments of Panorama as a virtual appliance.

- Support that covers all the components deployed as part of the VM-Series ELA.

✓ Whichever licensing model you chose will be permanent. After you deploy them, VM-Series firewalls cannot switch between the PAYG and bring-your-own-license (BYOL) licensing models. Switching between licensing models requires deploying a new firewall and migrating the configuration. Migration between evaluation, a regular license, and ELA is possible because they are all part of the BYOL licensing model.

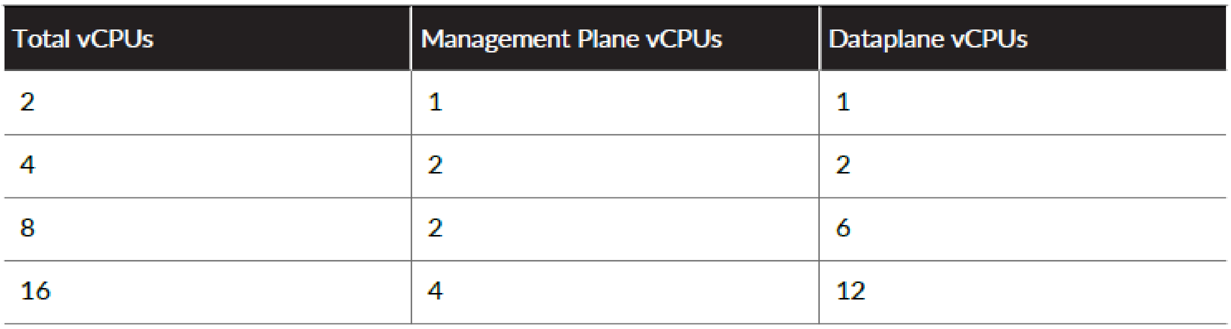
5 VM-Series System Requirements

Each instance of the VM-Series firewall requires a minimum resource allocation—number of CPUs, memory,and disk space, on its host server. Use the table below to verify that you allocate the necessary hardware resources for your VM-Series model.



VM-Series Model	Supported Hypervisors	Supported vCPUs	Minimum Memory	Minimum Hard Drive
VM-50	ESXi, KVM, Hyper-V	2	4.5GB	32GB (60GB at boot)
VM-100 VM-200	ESXi, KVM, Hyper-V, AWS, Azure, NSX, SDX	2	6.5GB	60GB
VM-300 VM-1000-HV	ESXi, KVM, Hyper-V, AWS, Azure, NSX, SDX	2, 4	9GB	60GB
VM-500	ESXi, KVM, Hyper-V, AWS, Azure, NSX	2, 4, 8	16GB	60GB
VM-700	ESXi, KVM, Hyper-V, AWS, Azure	2, 4, 8, 16	56GB	60GB

The number of vCPUs assigned to the management plane and those assigned to the dataplane differs depending on the total number of vCPUs assigned to the VM-Series firewall. If you assign more vCPUs than those officially supported by the license, any additional vCPUs are assigned to the management plane.



Total vCPUs	Management Plane vCPUs	Dataplane vCPUs
2	1	1
4	2	2
8	2	6
16	4	12

CPU Oversubscription

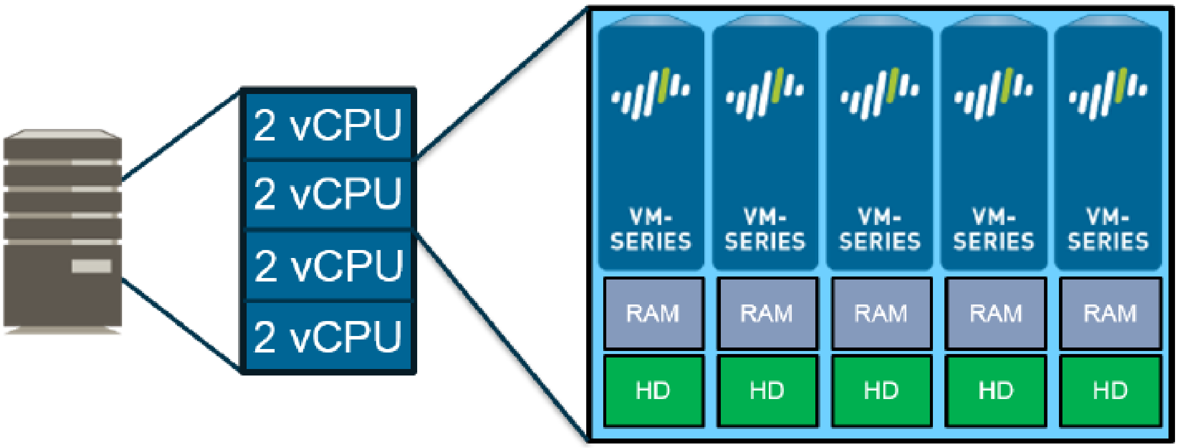
The VM-Series firewall supports CPU oversubscription on all models. CPU oversubscription allows you deploy a higher density of VM-Series firewalls on hypervisors running on x86 architecture. You can deploy two (2:1) to five (5:1) VM-Series firewalls per required allocation of CPUs. When planning your deployment, use the following formula to calculate the number of VM-Series firewalls your hardware can support.

(Total CPUs x Oversub Ratio)/CPUs per firewall = total number of VM-Series firewalls

For example, at a 5:1 ratio, a host machine with 16 physical CPU and at least 180GB of memory (40 × 4.5GB) can support up to 40 instances to the VM-50. Each VM-50 requires two vCPUs and five VM-50sb can be associated to each pair of vCPUs.

(16 CPUs x 5)/2 = 40 VM-50 firewalls

Beyond meeting the minimum VM-Series System Requirements, no additional configuration is required to take advantage of oversubscription. Deploy VM-Series firewalls normally and resource oversubscription occurs automatically. When planning your deployment, consider other functions, such as virtual switches, and guest machines on the host that require hardware resources of their own.

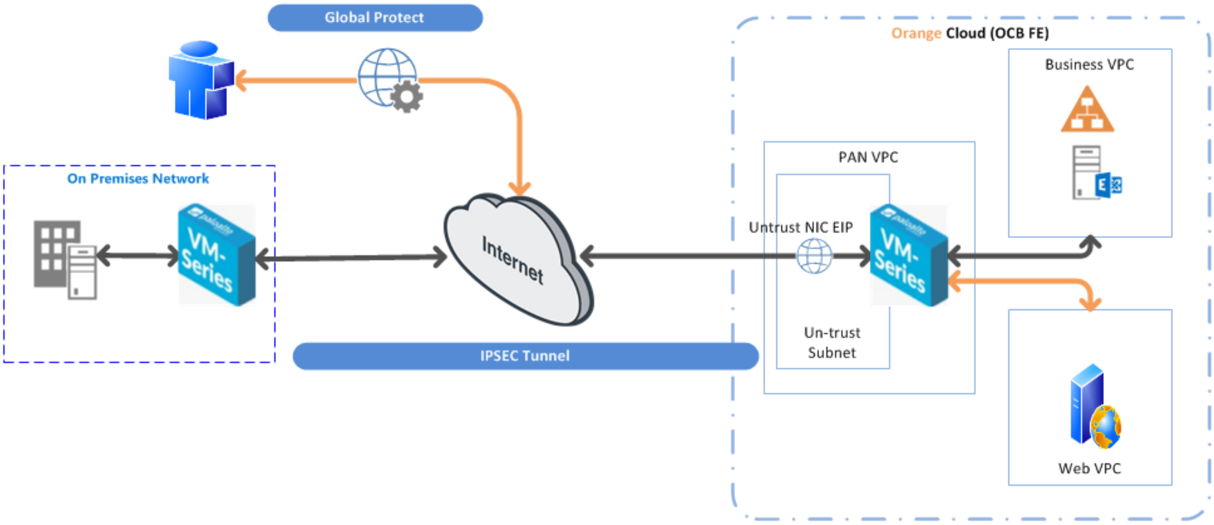


6 Deployment Methods

Use the VM-Series firewall on OCB FE to secure your network users in the following scenarios:

6.1 Hybrid and VPC to VPC

The VM-Series firewall on OCB FE allows you to securely extend your physical data center/private cloud into OCB FE using IPsec tunneling. To improve your data center security, if you have segmented your network and deployed your workloads in separate VPC's, you can secure traffic flowing between VPC's with an IPsec tunnel and application whitelisting policies.



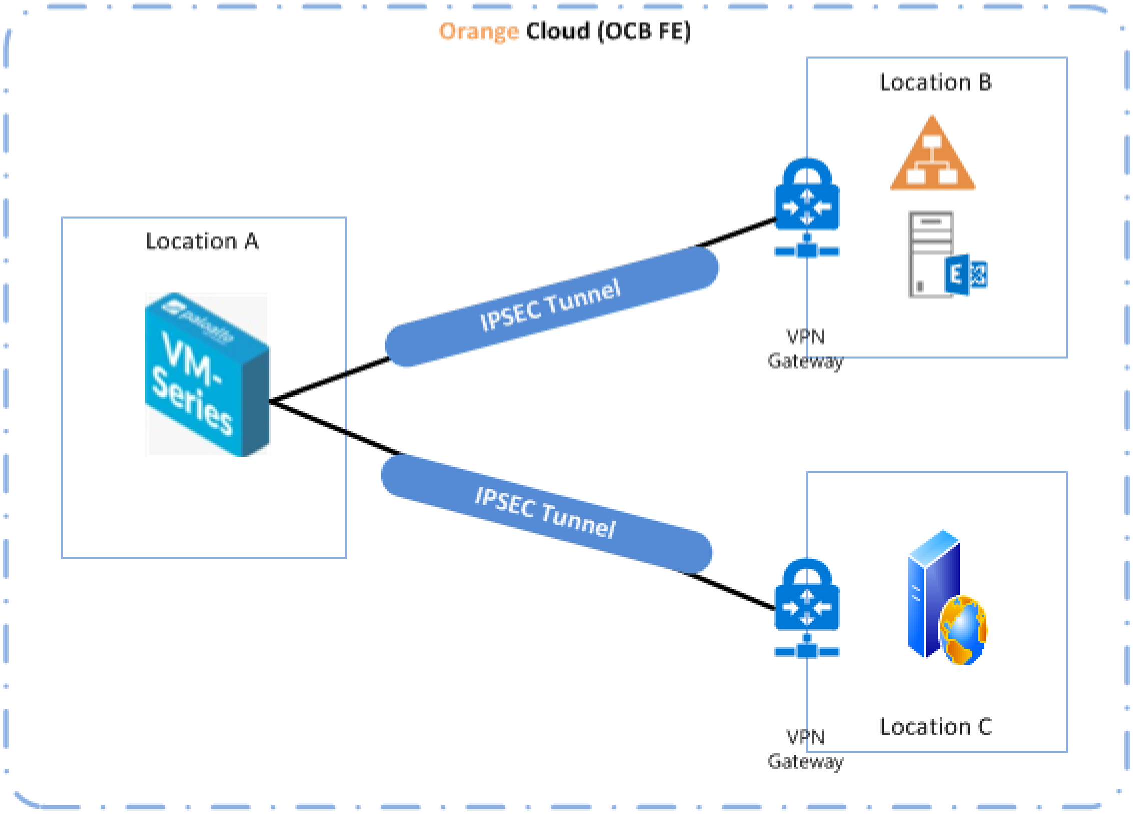
• Inter-Subnet —The VM-Series firewall can front your servers in a VPC and protects against lateral threats for inter-subnet traffic between applications in a multi-tier architecture.

• Gateway—The VM-Series firewall serves as the VPC gateway to protect Internet-facing deployments in the OCB FE (VPC). The VM-Series firewall secures traffic destined to the servers in the VPC and it also protects against lateral threats for inter-subnet traffic between applications in a multitier architecture.

• GlobalProtect—Use the OCB FE infrastructure to quickly and easily deploy the VM-Series firewall as GlobalProtect™ and extend your gateway security policy to remote users and devices, regardless of location.

6.2 On Cloud /On Cloud

The VM-Series firewall on OCB FE allows you to securely extend your multiple location cloud VPC's into OCB FE using IPsec tunneling.



- Inter-Subnet The VM-Series firewall can front your servers in a VPC and protects against lateral threats for inter-subnet traffic between applications in a multi-tier architecture.

- VPN Gateway A Virtual Private Network (VPN) provides an encrypted communication channel that enables users to remotely access VPCs.

- Multiple location VPC's with one subnet in each VPC.

7 Deploy the VM-Series Firewall on Orange Flex Engine

In our scenarios we have 3 VPC's

- PAN VPC that will host VM-Series Firewall
- Business VPC hosting active directory and exchange servers
- Web VPC hosting a webserver.

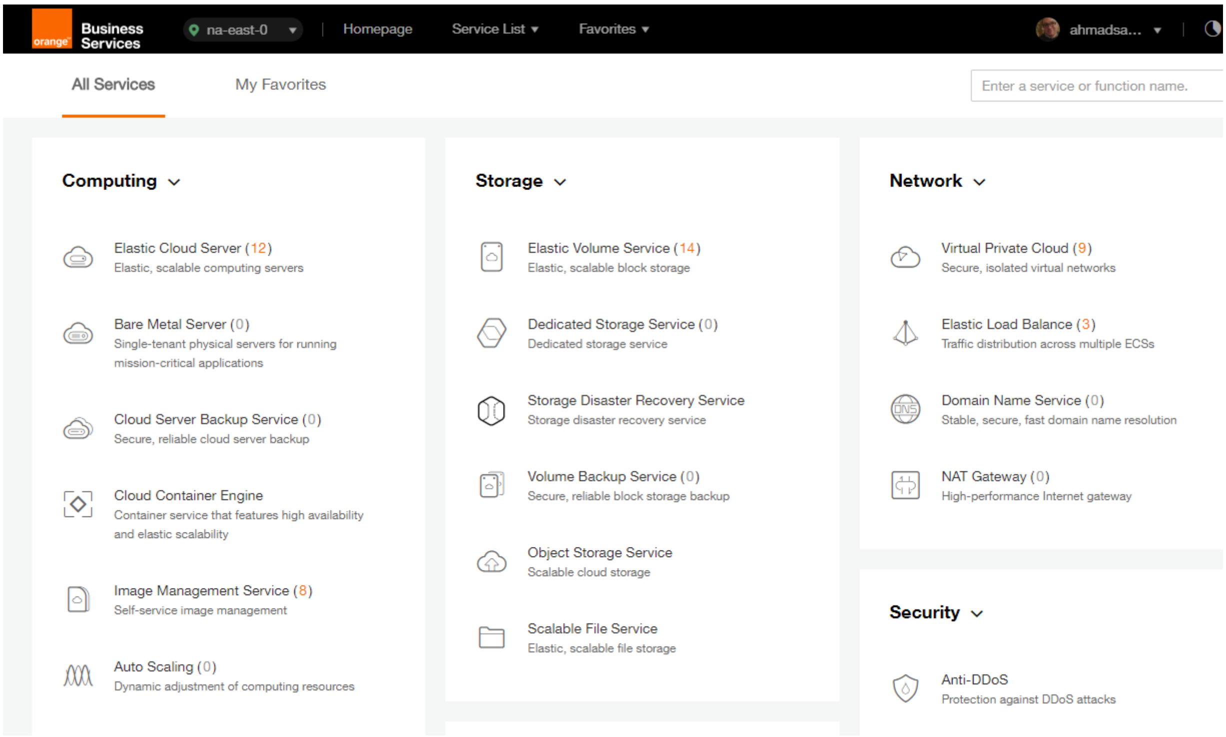
7.1 Create VPC

A VPC provides an isolated virtual network for ECSs. You can configure and manage the network as required.

To use a VPC, first create it by following the procedure provided in this section. Then, create subnets, security groups, and VPNs, and assign EIPs by following the procedure provided in subsequent sections based on your actual network requirements.

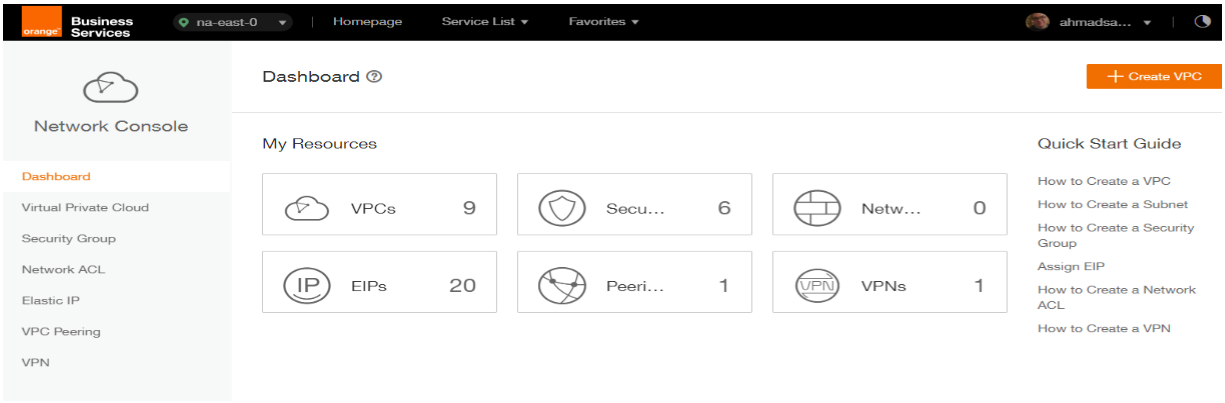
Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.



Business Services
na-east-0
Homepage
Service List
Favorites
ahmadsa...
All Services
My Favorites
Enter a service or function name.
Computing
Elastic Cloud Server (12)
Elastic, scalable computing servers
Bare Metal Server (0)
Single-tenant physical servers for running mission-critical applications
Cloud Server Backup Service (0)
Secure, reliable cloud server backup
Cloud Container Engine
Container service that features high availability and elastic scalability
Image Management Service (8)
Self-service image management
Auto Scaling (0)
Dynamic adjustment of computing resources
Storage
Elastic Volume Service (14)
Elastic, scalable block storage
Dedicated Storage Service (0)
Dedicated storage service
Storage Disaster Recovery Service
Storage disaster recovery service
Volume Backup Service (0)
Secure, reliable block storage backup
Object Storage Service
Scalable cloud storage
Scalable File Service
Elastic, scalable file storage
Network
Virtual Private Cloud (9)
Secure, isolated virtual networks
Elastic Load Balance (3)
Traffic distribution across multiple ECSs
Domain Name Service (0)
Stable, secure, fast domain name resolution
NAT Gateway (0)
High-performance Internet gateway
Security
Anti-DDoS
Protection against DDoS attacks

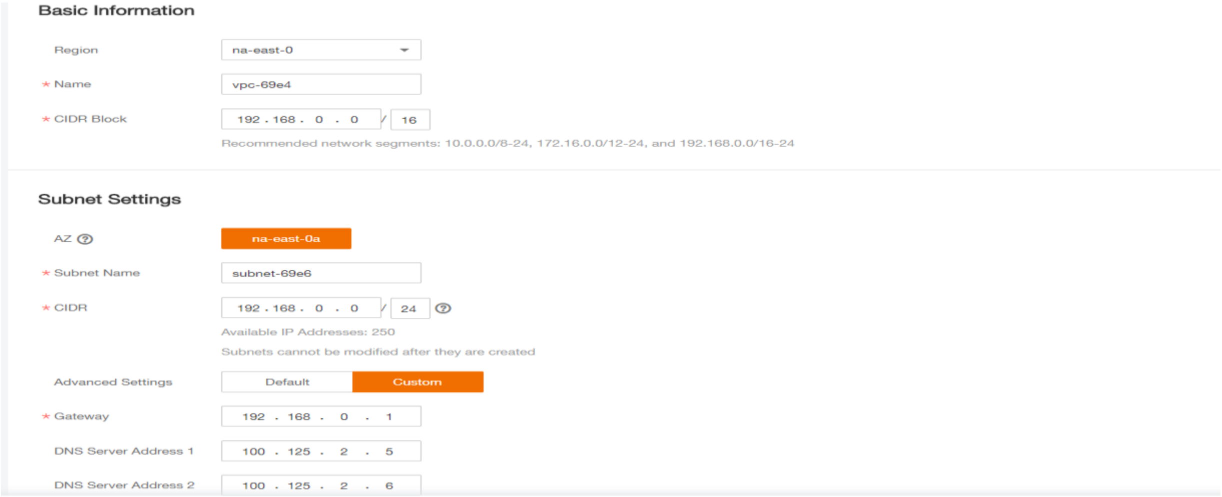
3. On the **Dashboard** page, click **Create VPC**.



On the displayed **Apply for VPC** page, set the parameters as prompted.

Table 1 Parameter description

Parameter	Description	Example Value
Name	Specifies the VPC name.	VPC-001
VPC CIDR	Specifies the Classless Inter-Domain Routing (CIDR) block for the VPC. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset (for multiple subnets in the VPC). The following CIDR blocks are supported: 10.0.0.0/8–24 172.16.0.0/12–24 192.168.0.0/16–24	192.168.0.0/16
Name	Specifies the subnet name.	Subnet-001
CIDR	Specifies the CIDR block for the subnet. This value must be within the VPC CIDR range.	192.168.0.0/24
Gateway	Specifies the gateway address of the subnet.	192.168.0.1



Basic Information

Region	na-east-0
* Name	vpc-69e4
* CIDR Block	192 . 168 . 0 . 0 / 16
	Recommended network segments: 10.0.0.0/8-24, 172.16.0.0/12-24, and 192.168.0.0/16-24

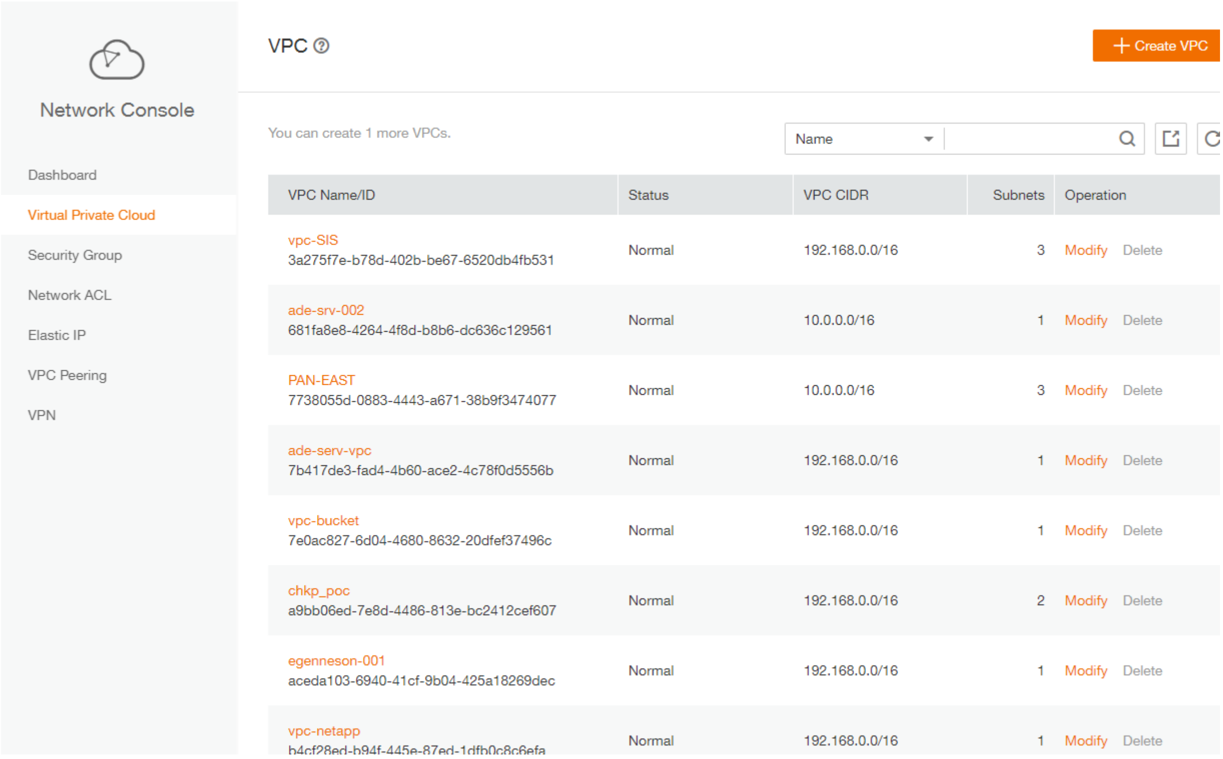
Subnet Settings

AZ	na-east-0a
* Subnet Name	subnet-69e6
* CIDR	192 . 168 . 0 . 0 / 24 Available IP Addresses: 250 Subnets cannot be modified after they are created
Advanced Settings	Default [✓ Custom]
* Gateway	192 . 168 . 0 . 1
DNS Server Address 1	100 . 125 . 2 . 5
DNS Server Address 2	100 . 125 . 2 . 6

4. The external DNS server address is used by default. If you need to change the DNS server address, click Show Advanced Settings and configure the DNS server addresses. You must ensure that the configured DNS server addresses are available.

5. Click Create Now.

The created VPC will be shown in the VPC List



You can create 1 more VPCs.

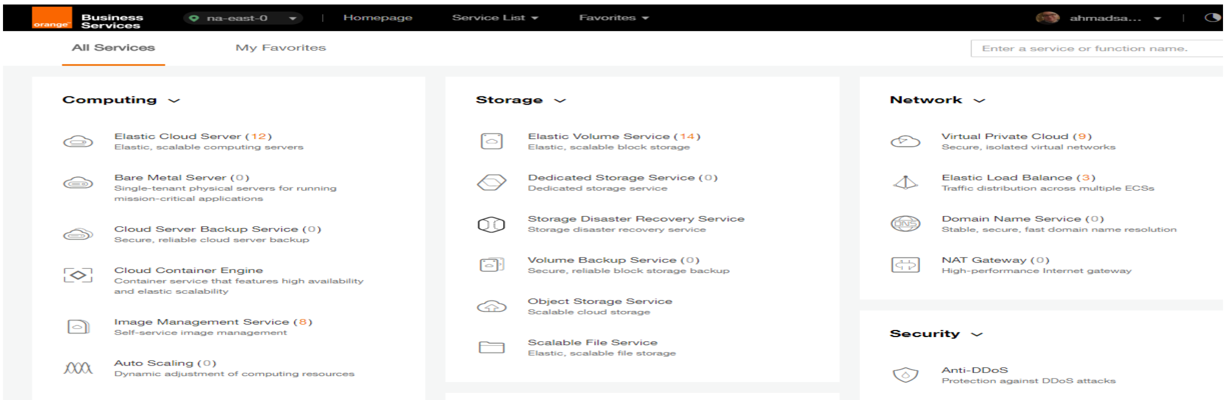
VPC Name/ID	Status	VPC CIDR	Subnets	Operation
vpc-SIS 3a275f7e-b78d-402b-be67-6520db4fb531	Normal	192.168.0.0/16	3	Modify Delete
ade-srv-002 681fa8e8-4264-4f8d-b8b6-dc636c129561	Normal	10.0.0.0/16	1	Modify Delete
PAN-EAST 7738055d-0883-4443-a671-38b9f3474077	Normal	10.0.0.0/16	3	Modify Delete
ade-serv-vpc 7b417de3-fad4-4b60-ace2-4c78f0d5556b	Normal	192.168.0.0/16	1	Modify Delete
vpc-bucket 7e0ac827-6d04-4680-8632-20dfef37496c	Normal	192.168.0.0/16	1	Modify Delete
chkp_poc a9bb06ed-7e8d-4486-813e-bc2412cef607	Normal	192.168.0.0/16	2	Modify Delete
egenneson-001 aceda103-6940-41cf-9b04-425a18269dec	Normal	192.168.0.0/16	1	Modify Delete
vpc-netapp b4cf28ed-b94f-445e-87ed-1dfb0c8c6efa	Normal	192.168.0.0/16	1	Modify Delete

7.2 Install Palo Alto VM on the VPC

ECSs are more cost-effective than physical servers. Within minutes, you can obtain ECS resources from the public cloud. ECS resources are flexible and on-demand. This section describes how to create an ECS.

1. Log in to the management console.

2. Under **Computing**, click **Elastic Cloud Server**.



orange Business Services | na-east-0 | Homepage | Service List | Favorites | ahmadsa...

All Services | My Favorites | Enter a service or function name.

Computing

Elastic Cloud Server (12)
Elastic, scalable computing servers

Bare Metal Server (0)
Single-tenant physical servers for running mission-critical applications

Cloud Server Backup Service (0)
Secure, reliable cloud server backup

Cloud Container Engine
Container service that features high availability and elastic scalability

Image Management Service (8)
Self-service image management

Auto Scaling (0)
Dynamic adjustment of computing resources

Storage

Elastic Volume Service (14)
Elastic, scalable block storage

Dedicated Storage Service (0)
Dedicated storage service

Storage Disaster Recovery Service
Storage disaster recovery service

Volume Backup Service (0)
Secure, reliable block storage backup

Object Storage Service
Scalable cloud storage

Scalable File Service
Elastic, scalable file storage

Network

Virtual Private Cloud (9)
Secure, isolated virtual networks

Elastic Load Balance (3)
Traffic distribution across multiple ECSs

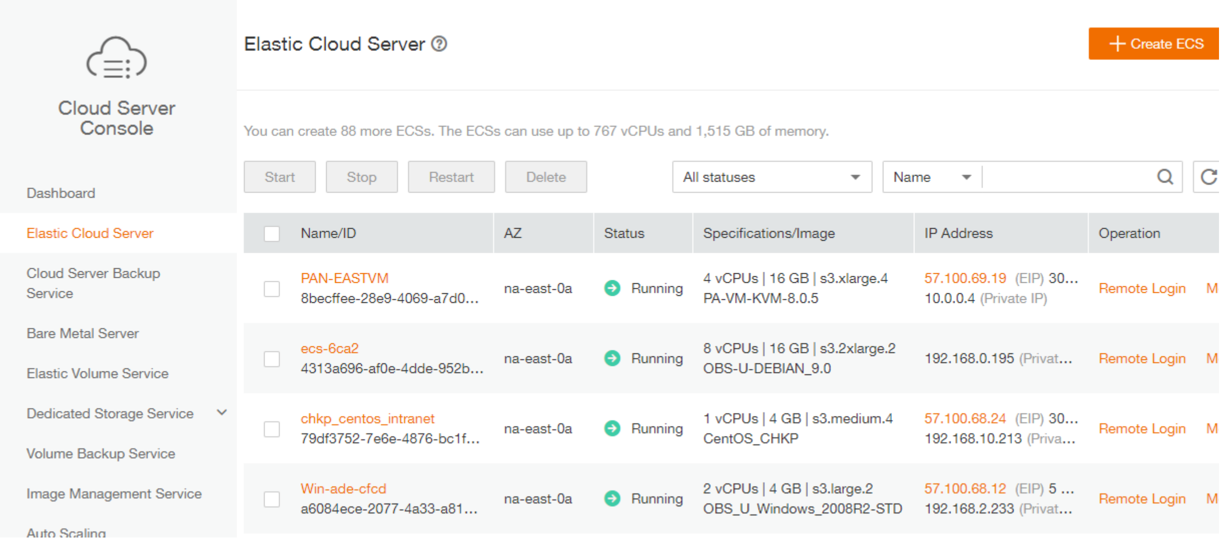
Domain Name Service (0)
Stable, secure, fast domain name resolution

NAT Gateway (0)
High-performance Internet gateway

Security

Anti-DDoS
Protection against DDoS attacks

3. Click **Create ECS**.



Cloud Server Console

Dashboard
Elastic Cloud Server
Cloud Server Backup Service
Bare Metal Server
Elastic Volume Service
Dedicated Storage Service
Volume Backup Service
Image Management Service
Auto Scaling

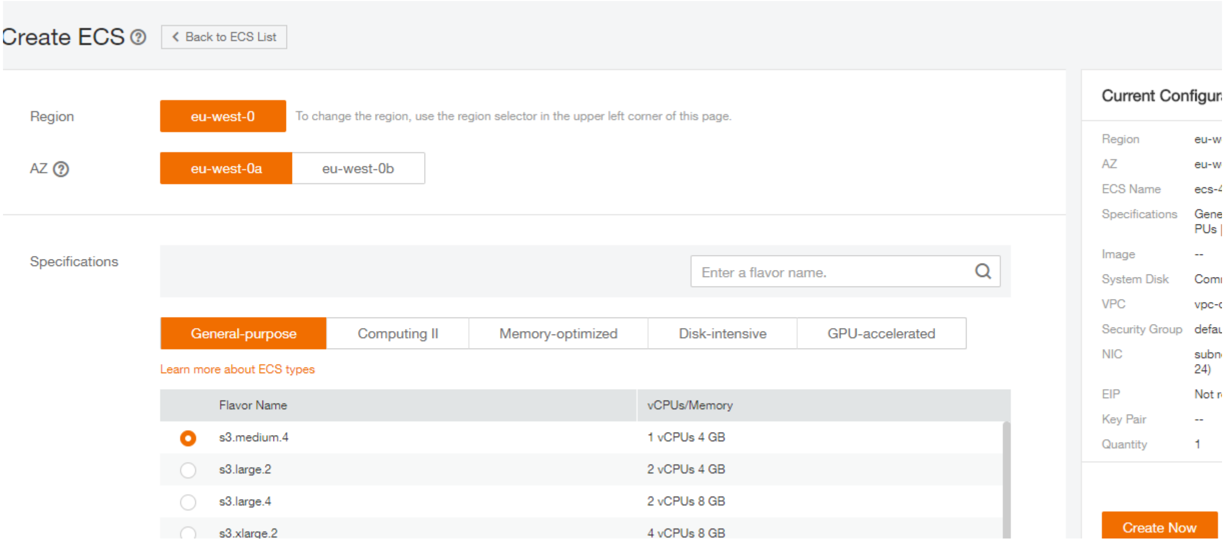
Elastic Cloud Server | + Create ECS

You can create 88 more ECSs. The ECSs can use up to 767 vCPUs and 1,515 GB of memory.

Start | Stop | Restart | Delete | All statuses | Name

□	Name/ID	AZ	Status	Specifications/Image	IP Address	Operation
□	PAN-EASTVM 8becffee-28e9-4069-a7d0...	na-east-0a	Running	4 vCPUs | 16 GB | s3.xlarge.4 PA-VM-KVM-8.0.5	57.100.69.19 (EIP) 30... 10.0.0.4 (Private IP)	Remote Login M
□	ecs-6ca2 4313a696-af0e-4dde-952b...	na-east-0a	Running	8 vCPUs | 16 GB | s3.2xlarge.2 OBS-U-DEBIAN_9.0	192.168.0.195 (Privat...	Remote Login M
□	chkp_centos_intranet 79df3752-7e6e-4876-bc1f...	na-east-0a	Running	1 vCPUs | 4 GB | s3.medium.4 CentOS_CHKP	57.100.68.24 (EIP) 30... 192.168.10.213 (Priva...	Remote Login M
□	Win-ade-cfcd a6084ece-2077-4a33-a81...	na-east-0a	Running	2 vCPUs | 4 GB | s3.large.2 OBS_U_Windows_2008R2-STD	57.100.68.12 (EIP) 5 ... 192.168.2.233 (Privat...	Remote Login M

The ECS creation page is displayed.



Create ECS ⓘ ‹ Back to ECS List

Region: eu-west-0 — To change the region, use the region selector in the upper left corner of this page.

AZ ⓘ: eu-west-0a | eu-west-0b

Specifications: Enter a flavor name.

General-purpose | Computing II | Memory-optimized | Disk-intensive | GPU-accelerated

Learn more about ECS types

	Flavor Name	vCPUs/Memory
●	s3.medium.4	1 vCPUs 4 GB
○	s3.large.2	2 vCPUs 4 GB
○	s3.large.4	2 vCPUs 8 GB
○	s3.xlarge.2	4 vCPUs 8 GB

Current Configur

Region	eu-w
AZ	eu-w
ECS Name	ecs-4
Specifications	Gene PUs |
Image	--
System Disk	Comi
VPC	vpc-c
Security Group	defau
NIC	subn 24)
EIP	Not r
Key Pair	--
Quantity	1

Create Now

4. Confirm the region.

If the region is incorrect, click ⊙ in the upper left corner of the page for correction.

5. Select an AZ.

An AZ is a physical region where power and networks are physically isolated. AZs in the same region can communicate with each other over an intranet.

1. To enhance application availability, create ECSs in different AZs.
2. To shorten network latency, create ECSs in the same AZ.

6. Click + to open the **Select Specifications** page. On the page, select an ECS type.

7. Set **Local-Disk**.

This parameter is optional and is automatically displayed when you use a local disk.

A local disk specifies the local storage for the physical host where the ECS is deployed. Only hard disk drives (HDDs) are supported. If you select the disk-intensive ECS type, the system automatically attaches local disks to the ECS.

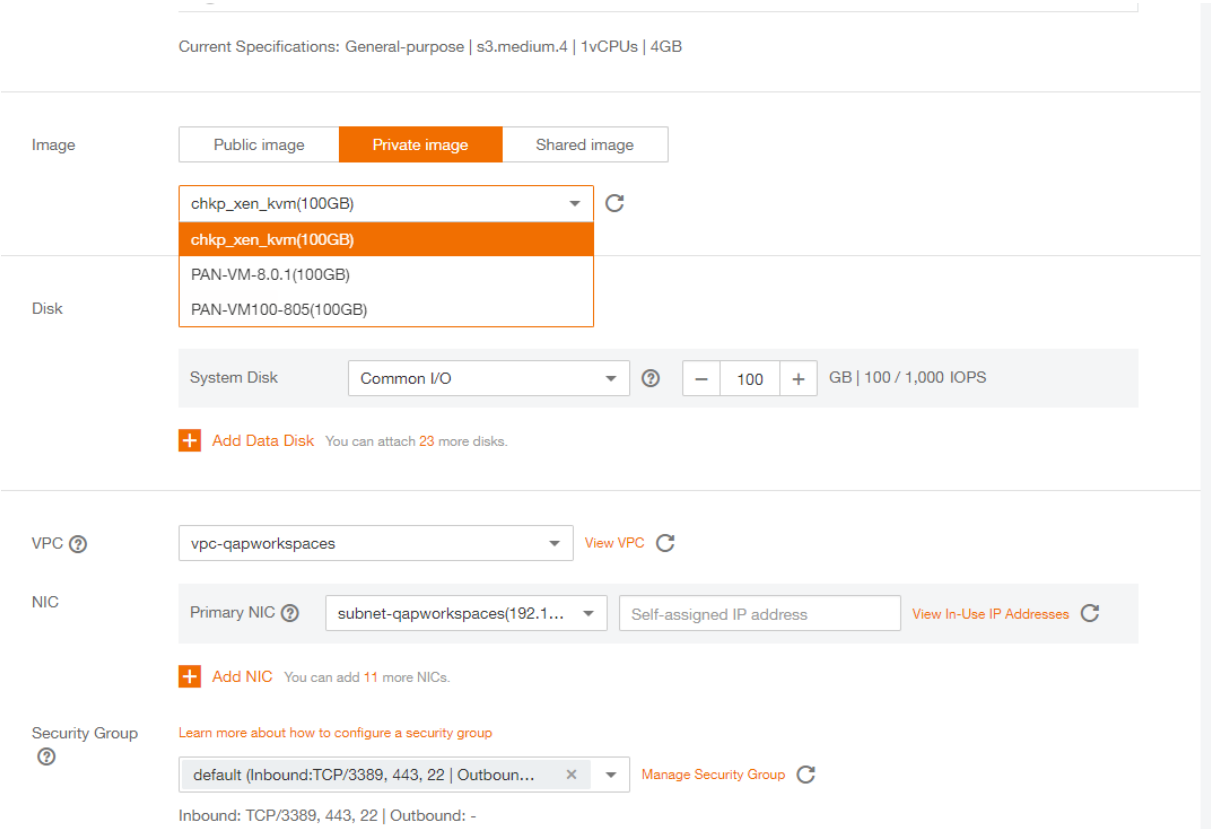
For example, if the Local Disk value is 3 x 1800 GB, three HDDs are attached to the ECS and the capacity of each HDD is 1800 GB.

8. Click **Image**.

Private Image

A private image is an image available only to the user who creates it. It contains an OS, preinstalled public applications, and the user's private applications. Using a private image to create ECSs removes the need to configure multiple ECSs repeatedly.

In our installation we previuosly uploaded a KVM image for PaloAlto VM . to check how to upload a private image to certain region please check the URL: https://docs.prod-cloud-ocb.orange-business.com/en-us/usermanual/ims/en-us_topic_0030713190.html



Current Specifications: General-purpose | s3.medium.4 | 1vCPUs | 4GB

Image: Public image | **Private image** | Shared image

chkp_xen_kvm(100GB)
- chkp_xen_kvm(100GB)
- PAN-VM-8.0.1(100GB)
- PAN-VM100-805(100GB)

Disk: System Disk: Common I/O, 100 GB | 100 / 1,000 IOPS

Add Data Disk You can attach 23 more disks.

VPC: vpc-qapworkspaces View VPC

NIC: Primary NIC: subnet-qapworkspaces(192.1... Self-assigned IP address View In-Use IP Addresses

Add NIC You can add 11 more NICs.

Security Group: Learn more about how to configure a security group

default (Inbound:TCP/3389, 443, 22 | Outboun... Manage Security Group

Inbound: TCP/3389, 443, 22 | Outbound: -

9. Set **Disk**.

A disk can be a system disk or a data disk. You can create multiple data disks for an ECS and customize their disk sizes.

10. Set network parameters, including **VPC**, **Security Group**, and **NIC**.

When you use VPC for the first time, the system automatically creates a VPC for you, including the security group and NIC.

Table 2 Parameter descriptions

Parameter	Description
VPC	Provides a network, including subnet and security group, for an ECS. You can select an existing VPC, or click **View VPC** and create a desired one. For more information about VPC, see *Virtual Private Cloud User*

Table 2 Parameter descriptions

Parameter	Description
	Guide. **NOTE:** DHCP must be enabled in the VPC to which the ECS belongs.
Security Group	Controls instance access within or between security groups by defining access rules. This enhances instance security. When creating an ECS, you can select multiple (recommended not more than five) security groups. In such a case, the access rules of all the selected security groups apply on the ECS. **NOTE:** Before initializing an ECS, ensure that the security group rule in the outbound direction meets the following requirements: • **Protocol**: **TCP** • **Port Range**: **80** • **Remote End**: **169.254.0.0/16** If you use the default security group rule in the outbound direction, the preceding requirements are met, and the ECS can be initialized. The default security group rule in the outbound direction is as follows: • **Protocol**: **ANY** • **Port Range**: **ANY** • **Remote End**: **0.0.0.0/16**
NIC	Consists of a primary NIC and one or more extension NICs. **MTU Settings**: optional If your ECS is of M2, large-memory, H1, or D1 type, you can click **MTU Settings** to configure the maximum transmission unit (MTU) for a to-be-added extension NIC for improving network performance. An MTU can only be a number, ranging from 1280 to 8888. ** In our scenario: We created only two NIC cards one for the Management and the Other is for the Untrust Interfaces. The other two NIC cards will be created using API request on the Business and Web VPC's then will be assigned to the Palo Alto VM **
EIP	A static public IP address bound to an ECS in a VPC. Using the EIP, the ECS provides services externally. The following options are provided: • **Do not use** Without an EIP, the ECS cannot access the Internet and is used only in the private network or cluster. • **Automatically assign** The system automatically assigns an EIP for the ECS. The EIP provides exclusive bandwidth that is configurable. • **Specify** An existing EIP is assigned for the ECS. When using an existing EIP, you cannot create ECSs in batches.

Table 2 Parameter descriptions

Parameter	Description
	** In our scenario: We assigned 2 EIP's one for the management NIC and the other for the Un trust NIC.

11. Set **ECS Name**.

    If you want to create multiple ECSs at a time, the system automatically sequences these ECSs.

12. Configure the number of ECSs to be created.

    After the configuration, click **Price Calculator** to view the ECS configuration fee.

13. Click **Create Now**.

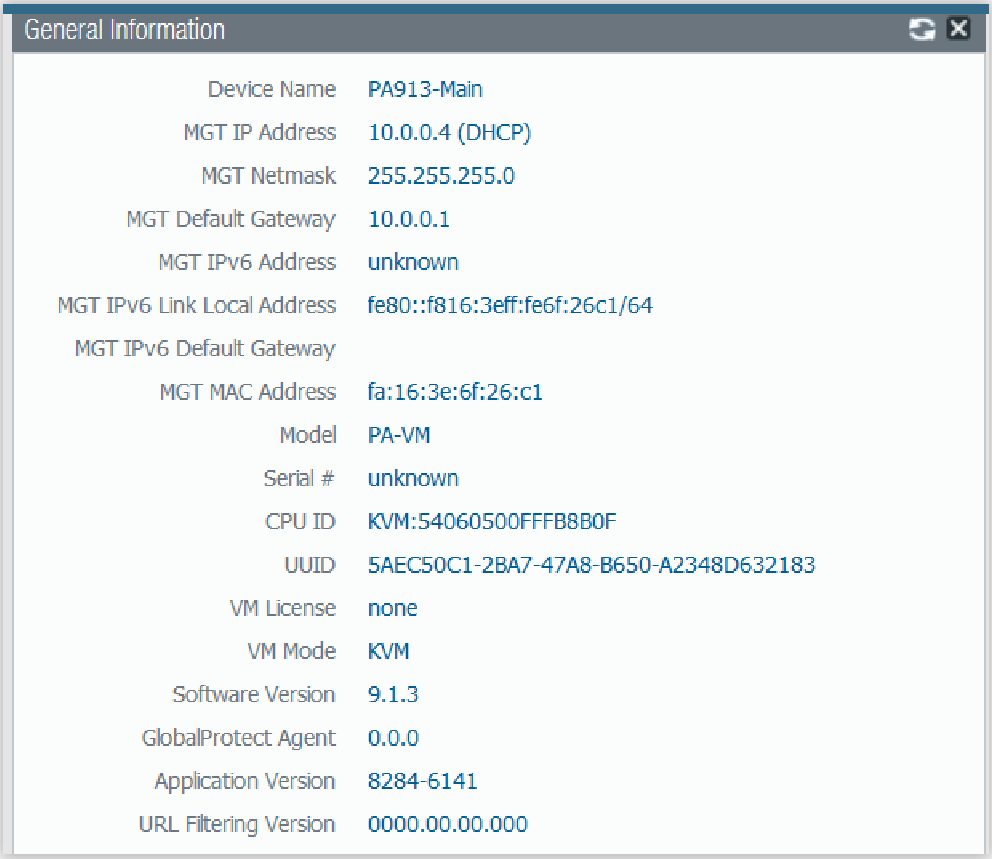
14. On the ECS specification confirmation page, confirm the ECS specifications and click **Submit**.

    After the ECS is created, you can view information about it on the **Elastic Cloud Server** page.

15. After creating the Palo Alto VM you can access it through **Https** using the EIP of the Management NIC. (username: admin / Password: admin)

7.3 Initial configuration for the primary Palo Alto VM

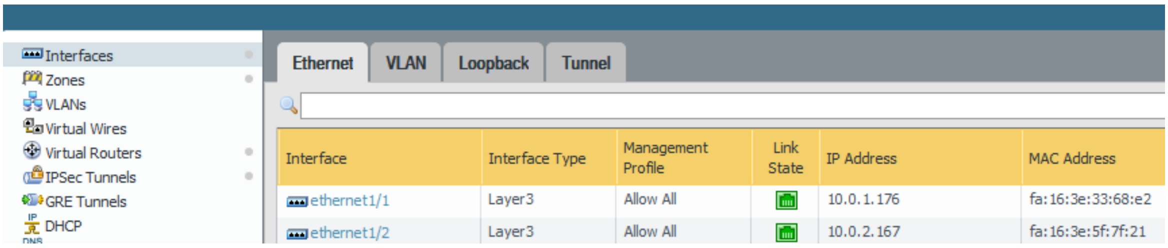
1. Login the primary Palo Alto VM using the management port EIP through https



General Information

Device Name	PA913-Main
MGT IP Address	10.0.0.4 (DHCP)
MGT Netmask	255.255.255.0
MGT Default Gateway	10.0.0.1
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::f816:3eff:fe6f:26c1/64
MGT IPv6 Default Gateway	
MGT MAC Address	fa:16:3e:6f:26:c1
Model	PA-VM
Serial #	unknown
CPU ID	KVM:54060500FFFB8B0F
UUID	5AEC50C1-2BA7-47A8-B650-A2348D632183
VM License	none
VM Mode	KVM
Software Version	9.1.3
GlobalProtect Agent	0.0.0
Application Version	8284-6141
URL Filtering Version	0000.00.00.000

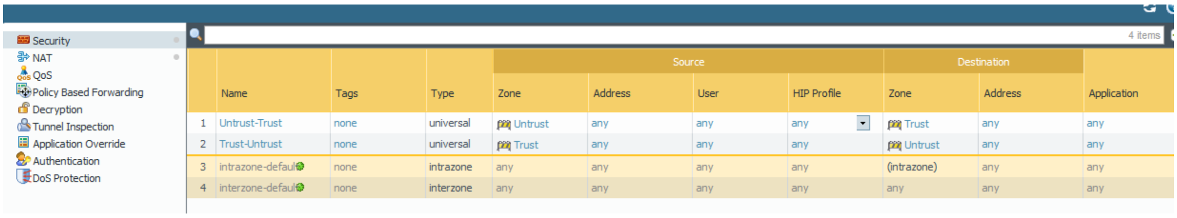
2. Got to Network > Interfaces and configure the untrust and trust ports by adding the Virtual IP’s you assigned on the Untrust and trust subnets.



Interface	Interface Type	Management Profile	Link State	IP Address	MAC Address
ethernet1/1	Layer3	Allow All	🟩	10.0.1.176	fa:16:3e:33:68:e2
ethernet1/2	Layer3	Allow All	🟩	10.0.2.167	fa:16:3e:5f:7f:21

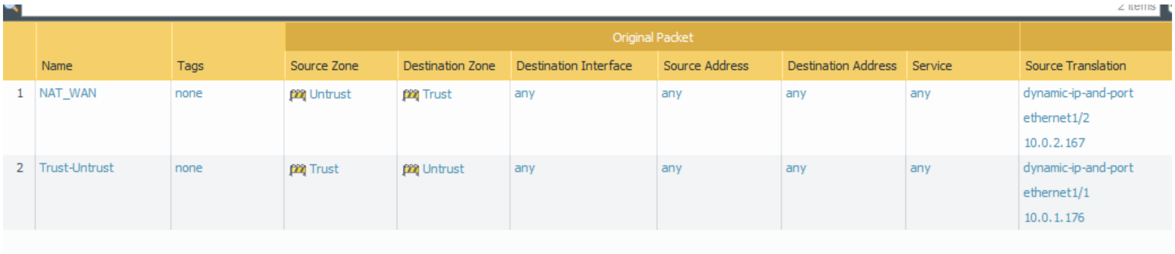
3. Commit

4. Go to Policies > Security > Add two policies between un-trust to trust and vice versa



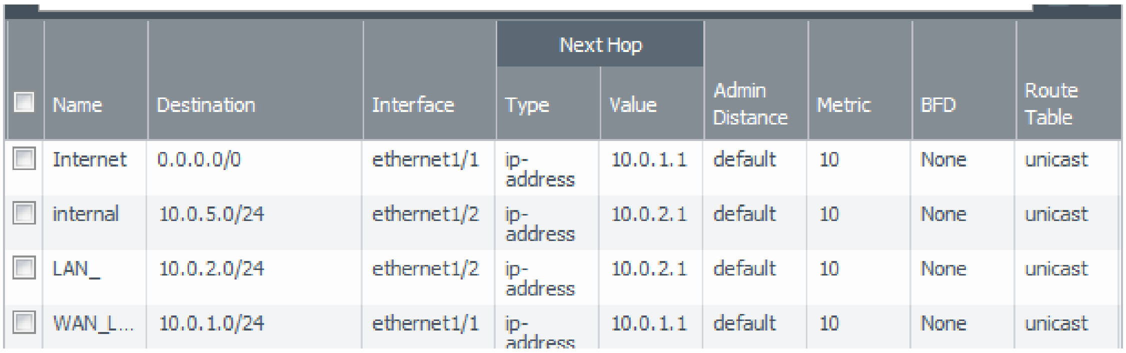
				Source				Destination		
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application
1	Untrust-Trust	none	universal	Untrust	any	any	any	Trust	any	any
2	Trust-Untrust	none	universal	Trust	any	any	any	Untrust	any	any
3	intrazone-defaul	none	intrazone	any	any	any	any	(intrazone)	any	any
4	interzone-defaul	none	interzone	any	any	any	any	any	any	any

5. Go to Policies > NAT > Add two NAT rules as shown below



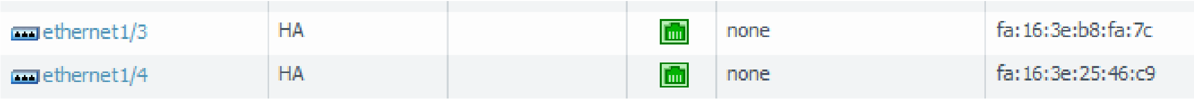
			Original Packet						
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation
1	NAT_WAN	none	Untrust	Trust	any	any	any	any	dynamic-ip-and-port ethernet1/2 10.0.2.167
2	Trust-Untrust	none	Trust	Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1 10.0.1.176

6. Add routes to enable traffic from untrust and protected zone and vice versa



				Next Hop					
□	Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD	Route Table
□	Internet	0.0.0.0/0	ethernet1/1	ip-address	10.0.1.1	default	10	None	unicast
□	internal	10.0.5.0/24	ethernet1/2	ip-address	10.0.2.1	default	10	None	unicast
□	LAN_	10.0.2.0/24	ethernet1/2	ip-address	10.0.2.1	default	10	None	unicast
□	WAN_L...	10.0.1.0/24	ethernet1/1	ip-address	10.0.1.1	default	10	None	unicast

7. Configure the High Availability Ports . In our scenario we have ports 3 and 4 .



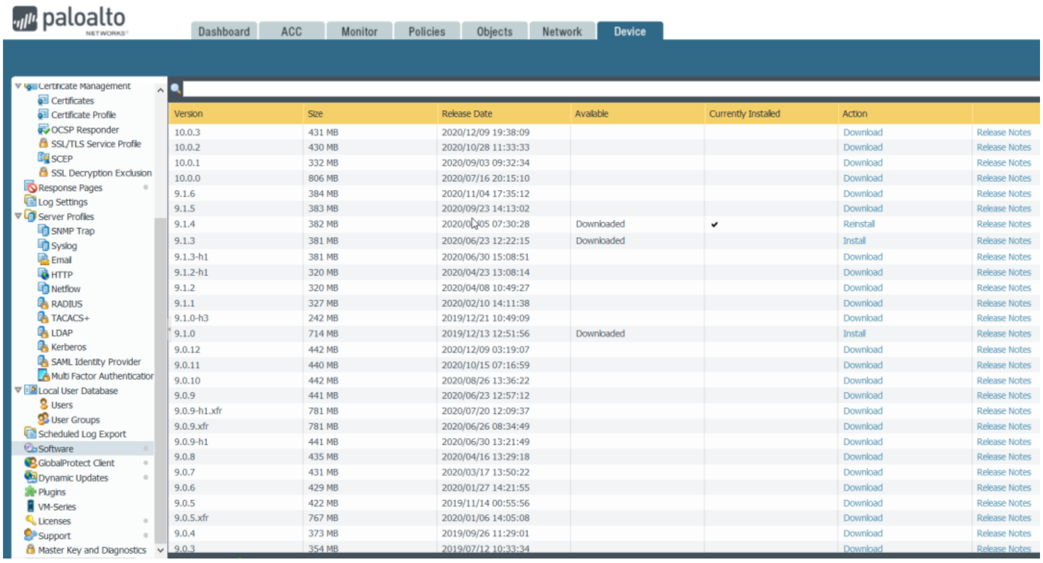
ethernet1/3	HA		🟩	none	fa:16:3e:b8:fa:7c
ethernet1/4	HA		🟩	none	fa:16:3e:25:46:c9

8. Perform the same configuration to the backup firewall and make sure that the two firewalls have the same software version and identical to each other.

9. Now we have the 2 firewalls identically configured . They are ready to start the high availability configuration and synchronize with each other.

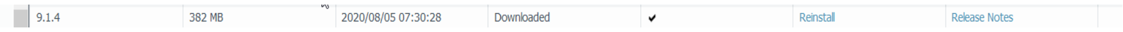
7.4 Firewall Software Update to release 9.1.4

From Device Tab > Choose Software



Version	Size	Release Date	Available	Currently Installed	Action	
10.0.3	431 MB	2020/12/09 19:38:09			Download	Release Notes
10.0.2	430 MB	2020/10/28 11:33:33			Download	Release Notes
10.0.1	332 MB	2020/09/03 09:32:34			Download	Release Notes
10.0.0	806 MB	2020/07/16 20:15:10			Download	Release Notes
9.1.6	384 MB	2020/11/04 17:35:12			Download	Release Notes
9.1.5	383 MB	2020/09/23 14:13:02			Download	Release Notes
9.1.4	382 MB	2020/08/05 07:30:28	Downloaded	✓	Reinstall	Release Notes
9.1.3	381 MB	2020/06/23 12:22:15	Downloaded		Install	Release Notes
9.1.3-h1	381 MB	2020/06/30 15:08:51			Download	Release Notes
9.1.2-h1	320 MB	2020/04/23 13:08:14			Download	Release Notes
9.1.2	320 MB	2020/04/08 10:49:27			Download	Release Notes
9.1.1	327 MB	2020/02/10 14:11:38			Download	Release Notes
9.1.0-h3	242 MB	2019/12/21 10:49:09			Download	Release Notes
9.1.0	714 MB	2019/12/13 12:51:56	Downloaded		Install	Release Notes
9.0.12	442 MB	2020/12/09 03:19:07			Download	Release Notes
9.0.11	440 MB	2020/10/15 07:16:59			Download	Release Notes
9.0.10	442 MB	2020/08/26 13:36:22			Download	Release Notes
9.0.9	441 MB	2020/06/23 12:57:12			Download	Release Notes
9.0.9-h1.xfr	781 MB	2020/07/20 12:09:37			Download	Release Notes
9.0.9.xfr	781 MB	2020/06/26 08:34:49			Download	Release Notes
9.0.9-h1	441 MB	2020/06/30 13:21:49			Download	Release Notes
9.0.8	435 MB	2020/04/16 13:29:18			Download	Release Notes
9.0.7	431 MB	2020/03/17 13:50:22			Download	Release Notes
9.0.6	429 MB	2020/01/27 14:21:55			Download	Release Notes
9.0.5	422 MB	2019/11/14 00:55:56			Download	Release Notes
9.0.5.xfr	767 MB	2020/01/06 14:05:08			Download	Release Notes
9.0.4	373 MB	2019/09/26 11:29:01			Download	Release Notes
9.0.3	354 MB	2019/07/12 10:33:34			Download	Release Notes

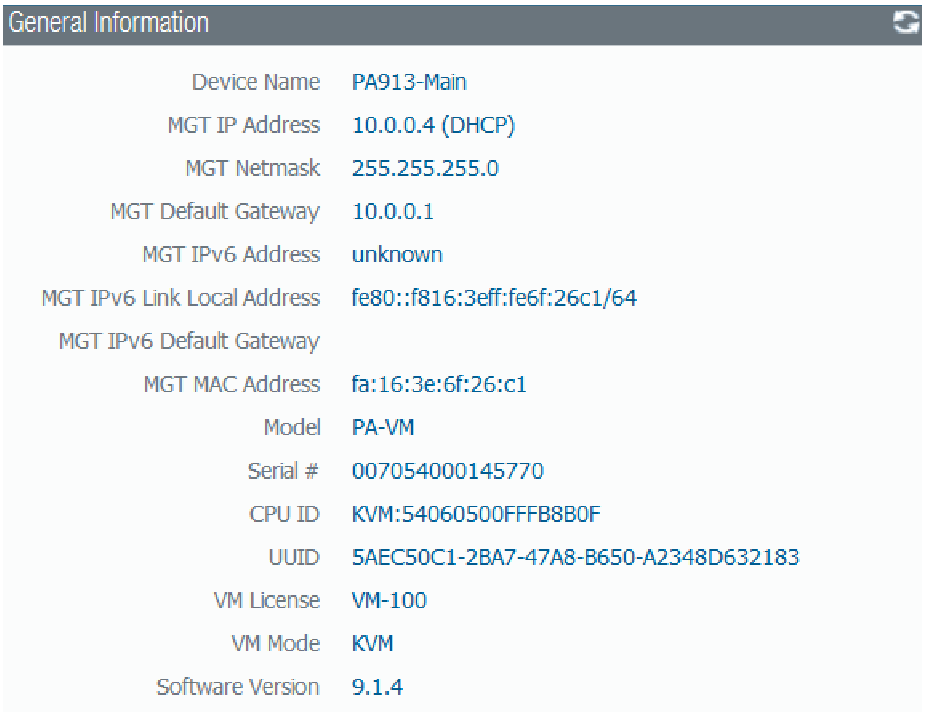
Choose release 9.1.4 update > then click Download



9.1.4	382 MB	2020/08/05 07:30:28	Downloaded	✓	Reinstall	Release Notes

The update will start to download after the download is finished . Click on install.

This will update the firwall software from 9.1.3 to 9.1.4



General Information

Device Name	PA913-Main
MGT IP Address	10.0.0.4 (DHCP)
MGT Netmask	255.255.255.0
MGT Default Gateway	10.0.0.1
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::f816:3eff:fe6f:26c1/64
MGT IPv6 Default Gateway	
MGT MAC Address	fa:16:3e:6f:26:c1
Model	PA-VM
Serial #	007054000145770
CPU ID	KVM:54060500FFFB8B0F
UUID	5AEC50C1-2BA7-47A8-B650-A2348D632183
VM License	VM-100
VM Mode	KVM
Software Version	9.1.4