FortiWeb

On OCB-FE

Installation and Deployment Guide

8th April 2019

Version 1.0

document control

date	version no.	author	change/addition
8-April-2019	1.0	Ahmad Samak	Creation

Table of contents

1 References

Reference	Description	Link to document
[2]	Fortinet Knowledge Base	http://cookbook.fortinet.com/fortiweb/
[3]	Technical Documentation	http://docs.fortinet.com
[4]	Video Tutorials	http://video.fortinet.com

2 What Is the Fortinet FortiWeb on OCB-FE?

Unprotected web applications are the easiest point of entry for hackers and vulnerable to a number of attack types. The multi-layered and correlated approach protects web apps from the Open Web Application Security Project (OWASP) Top 10 and more. Our Web Application Security Service from FortiGuard Labs uses information based on the latest application vulnerabilities, bots, suspicious URL and data patterns, and specialized heuristic detection engines to keep web applications safe from:

Malicious Sources

- Denial-of-service (DoS) attacks
- Sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, and cookie poisoning
- Malware uploads and application distributed denial-of-service (DDoS) and other attacks

It also includes Layer 7 load balancing and accelerated SSL offloading for more efficient application delivery.

The FortiWeb Web Application Firewall (WAF) provides nearly 100% protection from even the most sophisticated attacks with:

- Vulnerability scanning
- IP reputation, attack signatures, and antivirus powered by FortiGuard
- Behavioral attack detection, threat scanning, protection against botnets, DDoS, automated attacks, and more
- Integration with FortiSandbox for advanced threat protection (ATP) detection
- Tools to give you valuable insights on attacks
- Available in the Azure Marketplace

3 Why FortiWeb on OCB-FE?

Web Application Firewalls

3.1 Web Applications Are an Easy Target

Although Payment Card Industry Data Security Standard (PCI DSS) compliance is the main reason most organizations deploy web application firewalls (WAFs), many now realize that unprotected web applications are the easiest point of entry for even unsophisticated hackers. Externally facing web applications are vulnerable to attacks such as cross-site scripting, SQL injection, and Layer 7 DoS. Internal web applications are even easier to compromise if an attacker is able to gain access to an internal network where many organizations think they're protected by their perimeter network defenses. Custom code is usually the weakest link as development teams have the impossible task of staying on top of every new attack type. However, even commercial code is vulnerable as many organizations don't have the resources to apply patches and security fixes as soon as they're made available. Even if you apply every patch and have an army of developers to protect your systems, zero-day attacks can leave you defenseless and only able to respond after the attack has occurred.

3.2 Comprehensive Web Application Security with FortiWeb

Using an advanced multi-layered and correlated approach, FortiWeb provides complete security for your external and internal web-based applications from the OWASP Top 10 and many other threats. Using IP reputation services, botnets and other malicious sources are automatically screened out before they can do any damage. DoS detection and prevention keep your applications safe from being overloaded by Layer 7 DoS attacks. FortiWeb checks that the request hasn't been manipulated using HTTP RFC validation. Requests are checked against FortiWeb's signatures to compare them against known attack types to make sure they're clean. Any files, attachments, or code are scrubbed with FortiWeb's built-in antivirus and anti-malware services. FortiWeb's auto-learning behavioral detection engine reviews all requests that have passed the tests for known attacks. If the request is outside of user or automatic parameters, the request is blocked. Lastly, FortiWeb provides a correlation engine where multiple events from different security layers are correlated to make a more accurate decision and help protect against the most sophisticated attacks. This combination provides nearly 100% protection from any web application attacks, including zero-day threats that signature file-based systems can't detect.

3.3 Included Vulnerability Scanning

Only FortiWeb includes a web application vulnerability scanner in every appliance at no extra cost to help you meet PCI DSS compliance. FortiWeb's vulnerability scanning dives deep into all application elements and provides in-depth results of potential weaknesses in your applications. Vulnerability scanning is always up to date with regular updates from FortiGuard Labs.

3.4 Deep Integration with FortiGate and FortiSandbox

As the threat landscape evolves, many new threats require a multi-pronged approach for protecting web-based applications. Advanced persistent threats that target users can take many different forms than traditional single-vector attack types and can evade protections offered only by a single device. FortiWeb's integration with FortiGate and FortiSandbox extend basic WAF protections through synchronization and sharing of threat information to both deeply scan suspicious files and share infected internal sources. FortiWeb is one of many Fortinet products that provide integration with our FortiSandbox advanced threat detection platform. FortiWeb can be configured with FortiSandbox to share threat information and block threats as they're discovered in the sandboxing environment. Files uploaded to web servers can be sent to FortiSandbox and FortiSandbox Cloud for analysis. Alerts are sent immediately when malicious files are identified and future similar files are blocked immediately. Integration with FortiGate enables the sharing of quarantined IP addresses detected and maintained on the FortiGate firewall. Through regular polling of the FortiGate, FortiWeb is up to date with the latest list of internal sources that have or are suspected of being infected and blocks traffic from these devices to prevent more damage. Additionally, FortiGate users can now simplify the deployment of FortiWeb in a Fortinet-based network. Using the WCCP protocol, a FortiGate can be configured to direct HTTP traffic for inspection to a FortiWeb without having to manually configure routers or DNS services. Users can set up custom rules to route specific traffic using comprehensive, granular forwarding policies.

3.5 Advanced False Positive Mitigation Tools with User Scoring and Session Tracking

False positive detections can be very disruptive if a web application firewall isn't configured correctly. Although the installation of a WAF may take only minutes, fine-tuning it to minimize false positives can take days or even weeks. Plus, there's the regular ongoing adjustments for application and environmental changes. FortiWeb combats this problem with many sophisticated tools including alert tuning, white lists, automatic learning exceptions, correlated threat detection, and advanced code-based syntax analysis.

FortiWeb is the only WAF that employs user scoring and session tracking to further enhance our false positive mitigation tools. Administrators can attach threat levels to any of FortiWeb's WAF protections, then set trigger thresholds that can block, report, or monitor users that cross a combined multi-event violation score over the lifetime of their session. Never before has this level of customization and advanced correlation been available in a WAF, and it can dramatically reduce the number of false positive detections depending on the level of sensitivity set by the administrator.

3.6 FortiWeb User Tracking

FortiWeb monitors users authenticating to web applications and tracks all their subsequent activity. All traffic and attack logs are attached with the username, allowing rule enforcement and forensics at the user level.

3.7 Secured by FortiGuard

Fortinet’s award-winning FortiGuard Labs is the backbone for many of FortiWeb’s layers in its approach to application security. Offered as three separate options, you

can choose the FortiGuard services you need to protect your web applications. FortiWeb IP Reputation Service protects you from known attack sources like botnets,

spammers, anonymous proxies, and sources known to be infected with malicious software. FortiWeb Security Service is designed just for FortiWeb including items

such as application layer signatures, malicious robots, suspicious URL patterns, and web vulnerability scanner updates. Finally, FortiWeb offers FortiGuard’s top-rated

antivirus engine that scans all file uploads for threats that can infect your servers or other network elements.

3.8 Virtual Patching

FortiWeb provides integration with leading third-party vulnerability scanners including Acunetix, HP WebInspect, IBM AppScan, Qualys, and WhiteHat to provide dynamic virtual patches to security issues in application environments. Vulnerabilities found by the scanner are quickly and automatically turned into security rules by FortiWeb to protect the application until developers can address them in the application code.

3.9 Blazing Fast SSL Offloading

FortiWeb is able to process up to tens of thousands of web transactions by providing hardware-accelerated SSL offloading in most models. With near real-time decryption and encryption using ASIC-based chipsets, FortiWeb can easily detect threats that target secure applications.

3.10 Application Delivery and Authentication

FortiWeb provides advanced Layer 7 load balancing and authentication offload services. FortiWeb can easily expand your applications across multiple servers using intelligent, application-aware Layer 7 load balancing and can be combined with SSL offloading for load balancing secure application traffic. Using HTTP compression, FortiWeb can also improve bandwidth utilization and user response times for content-rich applications. Authentication offloading integrates with many authentication services including LDAP, NTLM, Kerberos, and RADIUS with two-factor authentication for RADIUS and RSA SecurID. Using these authentication services, you can easily publish websites and use single sign-on (SSO) for any web application including Microsoft applications such as Outlook Web Access and SharePoint. Finally, FortiWeb can improve application response times by caching often-used content to serve it to users faster than having to request the same information each time it is needed.

3.11 VM and Cloud Options

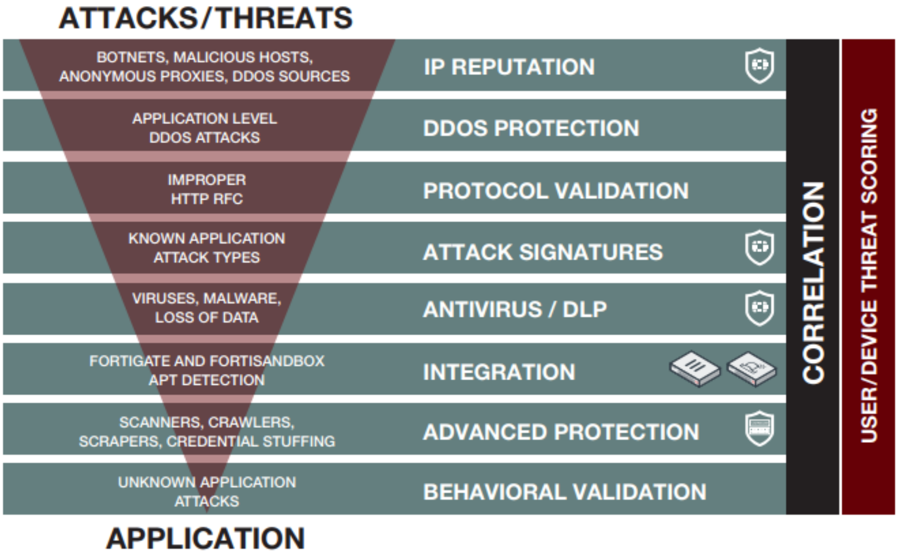
FortiWeb provides maximum flexibility in supporting your virtual and hybrid environments. The virtual versions of FortiWeb support all the same features as our hardware-based devices and work with all the top hypervisors including VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, and KVM. FortiWeb is also available for Amazon Web Services and Microsoft Azure.

3.12 Central Management and Reporting

FortiWeb offers the tools you need to manage multiple appliances and gain valuable insights on attacks that target your applications. From within a single management console you can configure and manage multiple FortiWeb gateways using our VMware-based central management utility. If you need an aggregated view of attacks across your network, FortiWeb easily integrates into our FortiWeb reporting appliances for centralized logging and report consolidation from multiple FortiWeb devices.

4 FortiWeb-VM For OCB-FE

FortiWeb is a web application firewall (WAF) that protects hosted web applications from attacks that target known and unknown exploits. Using multi-layered and correlated detection methods, FortiWeb defends applications from known vulnerabilities and from zero-day threats.


ATTACKS/THREATS
BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES
IP REPUTATION
APPLICATION LEVEL DDOS ATTACKS
DDOS PROTECTION
IMPROPER HTTP RFC
PROTOCOL VALIDATION
KNOWN APPLICATION ATTACK TYPES
ATTACK SIGNATURES
VIRUSES, MALWARE, LOSS OF DATA
ANTIVIRUS / DLP
FORTIGATE AND FORTISANDBOX APT DETECTION
INTEGRATION
SCANNERS, CRAWLERS, SCRAPERS, CREDENTIAL STUFFING
ADVANCED PROTECTION
UNKNOWN APPLICATION ATTACKS
BEHAVIORAL VALIDATION
CORRELATION
USER/DEVICE THREAT SCORING
APPLICATION

FortiWeb's layered and correlated approach to threat detection provides nearly 100% protection from known and unknown zero-day threats that target application vulnerabilities.

4.1 Features

4.1.1 Deployment options

- Reverse Proxy
- Inline Transparent
- True Transparent Proxy
- Offline Sniffing
- WCCP

4.1.2 Web Security

- Automatic profiling (white list)
- Web server and application signatures (black list)
- IP Reputation
- IP Geolocation
- HTTP RFC compliance
- Native support for HTTP/2

4.1.3 Application Attack Protection

- OWASP Top 10
- Cross Site Scripting
- SQL Injection

- Cross Site Request Forgery
- Session Hijacking
- Built-in Vulnerability Scanner
- Third-party scanner integration (virtual patching)
- File upload scanning with AV and sandbox

4.1.4 Security Services

- WWeb services signatures
- XML and JSON protocol conformance
- Malware detection
- Virtual patching
- Protocol validation
- Brute force protection
- Cookie signing and encryption
- Threat scoring and weighting
- Syntax-based SQLi detection
- HTTP Header Security
- Custom error message and error code handling
- Operating system intrusion signatures
- Known threat and zero-day attack protection
- L4 Stateful Network Firewall
- DoS prevention
- Advanced correlation protection using multiple security elements
- Data leak prevention
- Web Defacement Protection

4.1.5 Application Delivery

- Layer 7 server load balancing
- URL Rewriting
- Content Routing
- HTTPS/SSL Offloading
- HTTP Compression
- Caching

4.1.6 Authentication

- Active and passive authentication
- Site Publishing and SSO
- RSA Access for 2-factor authentication
- LDAP, RADIUS, and SAML support
- SSL client certificate support
- CAPTCHA and Real Browser Enforcement (RBE)

4.1.7 Management and Reporting

- Web user interface
- Command line interface
- FortiView graphical analysis and reporting tools
- Central management for multiple FortiWeb devices
- Active/Active HA Clustering

- REST API
- Centralized logging and reporting
- User/device tracking
- Real-time dashboards
- Bot dashboard
- Geo IP Analytics
- SNMP, Syslog and Email Logging/Monitoring
- Administrative Domains with full RBAC

4.1.8 Other

- IPv6 Ready
- HTTP/2 to HTTP 1.1 translation
- HSM Integration
- Seamless PKI integration
- Attachment scanning for ActiveSync and OWA applications
- High Availability with Config-sync for syncing across multiple active appliances
- Auto setup and default configuration settings for simplified deployment
- Setup Wizards for common applications and databases
- Preconfigured for common Microsoft applications; Exchange, SharePoint, OWA
- OpenStack support for FortiWeb VMs
- Predefined security policies for Drupal and Wordpress applications
- WebSockets support

4.2 Benefits

FortiWeb is designed specifically to protect web servers.
FortiWeb web application firewalls (WAF) provide specialized application layer threat detection and protection for many HTTP or HTTPS services, including:

- Apache Tomcat
- nginx
- Microsoft IIS
- JBoss
- IBM Lotus Domino
- Microsoft SharePoint
- Microsoft Outlook Web App (OWA)
- RPC and ActiveSync for Microsoft Exchange Server
- Joomla
- WordPress

FortiWeb’s integrated web vulnerability scanner can drastically reduce challenges associated with protecting regulated and confidential data by detecting your exposure to the latest threats, especially the OWASP Top 10.

In addition, FortiWeb’s XML firewall and denial-of-service (DoS) attack-prevention protect your Internet-facing web-based applications from attack and data theft. Using advanced techniques to provide bidirectional protection against sophisticated threats like SQL injection and cross-site scripting (XSS), FortiWeb helps you prevent identity theft, financial fraud, and corporate espionage. FortiWeb delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal security policies, including firewalling and patching requirements from PCI DSS.

FortiWeb’s application-aware firewalling and load balancing engine can:

- Secure HTTP applications that are often gateways into valuable databases
- Prevent and reverse defacement
- Improve application stability
- Monitor servers for downtime & connection load
- Reduces response times
- Accelerate SSL/TLS *
- Accelerate compression/decompression
- Rewrite content on the fly

* On VM models, acceleration is due to offloading the cryptography burden from the back-end server. On hardware models with ASIC chips, cryptography is also hardware-accelerated.

FortiWeb significantly reduces deployment costs by consolidating WAF, hardware acceleration, load balancing, and vulnerability scanning into a single device with no per-user pricing. Those features drastically reduce the time required to protect your regulated, Internet-facing data and eases the challenges associated with policy enforcement and regulatory compliance.

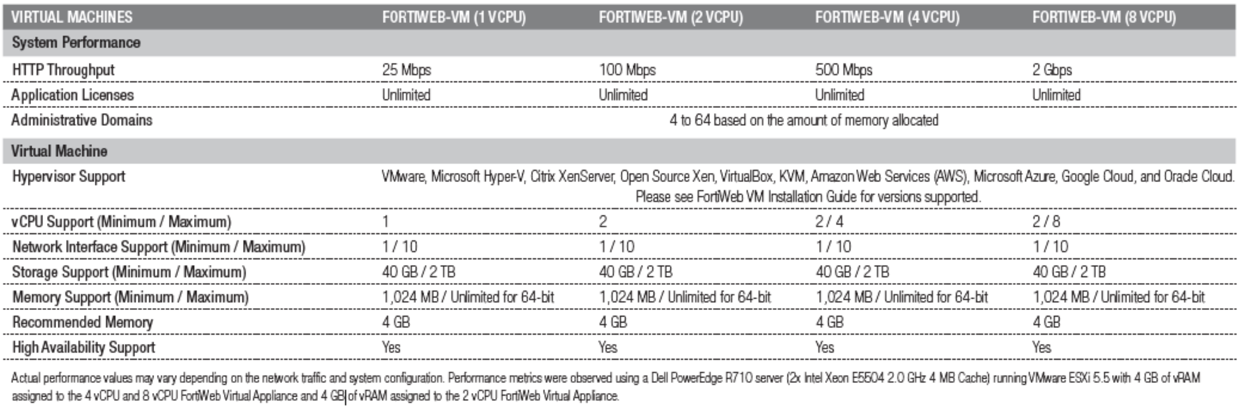
4.3 Licensing

Azure deployments require FortiWeb-VM licenses that specify the size of the virtual appliance you can deploy. In addition, you use the registration number that you use to obtain the license to register for FortiGuard services and technical support.

No trial license is available for FortiWeb-VM for OCB-FE.

FortiWeb-VM for OCB-FE licenses are available for the following sizes of virtual machine:

FortiWeb-VM models Compatible with OCB-FE

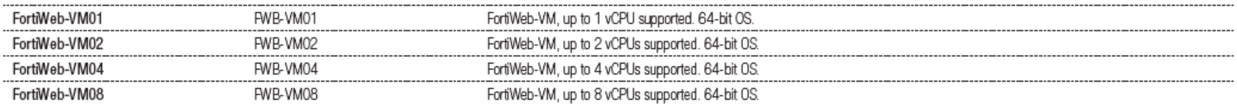


VIRTUAL MACHINES	FORTIWEB-VM (1 VCPU)	FORTIWEB-VM (2 VCPU)	FORTIWEB-VM (4 VCPU)	FORTIWEB-VM (8 VCPU)
System Performance				
HTTP Throughput	25 Mbps	100 Mbps	500 Mbps	2 Gbps
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	4 to 64 based on the amount of memory allocated			
Virtual Machine				
Hypervisor Support	VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and Oracle Cloud. Please see FortiWeb VM Installation Guide for versions supported.			
vCPU Support (Minimum / Maximum)	1	2	2 / 4	2 / 8
Network Interface Support (Minimum / Maximum)	1 / 10	1 / 10	1 / 10	1 / 10
Storage Support (Minimum / Maximum)	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB
Memory Support (Minimum / Maximum)	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit
Recommended Memory	4 GB	4 GB	4 GB	4 GB
High Availability Support	Yes	Yes	Yes	Yes

Actual performance values may vary depending on the network traffic and system configuration. Performance metrics were observed using a Dell PowerEdge R710 server (2x Intel Xeon E5504 2.0 GHz 4 MB Cache) running VMware ESXi 5.5 with 4 GB of vRAM assigned to the 4 vCPU and 8 vCPU FortiWeb Virtual Appliance and 4 GB of vRAM assigned to the 2 vCPU FortiWeb Virtual Appliance.

The maximum number of IP sessions and policies an instance can support is determined by the license and available vRAM, just as it does for hardware models.

4.4 Order Information



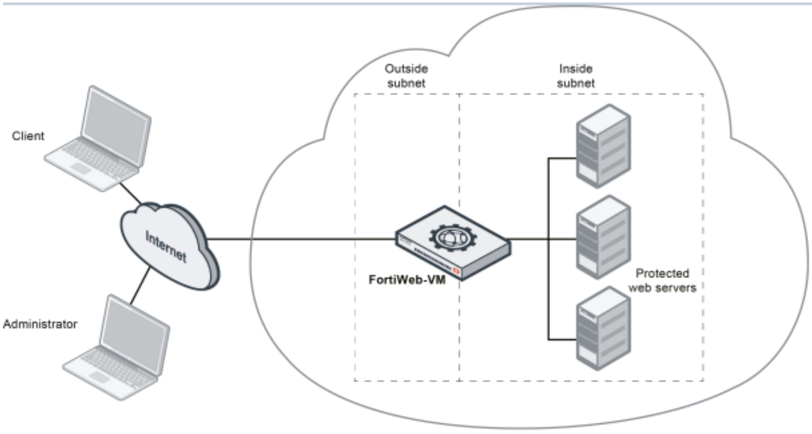
FortiWeb-VM01	FWB-VM01	FortiWeb-VM, up to 1 vCPU supported. 64-bit OS.
FortiWeb-VM02	FWB-VM02	FortiWeb-VM, up to 2 vCPUs supported. 64-bit OS.
FortiWeb-VM04	FWB-VM04	FortiWeb-VM, up to 4 vCPUs supported. 64-bit OS.
FortiWeb-VM08	FWB-VM08	FortiWeb-VM, up to 8 vCPUs supported. 64-bit OS.

5 FortiWeb-VM Deployment on OCB-FE

5.1 Architecture

You deploy FortiWeb-VM in the OCB-FE platform as part of a VPC.

FortiWeb-VM for OCB-FE



FortiWeb-VM for OCB-FE operates in reverse proxy mode only. It is positioned inline to intercept all incoming client connections on the public subnet and scan and redistribute them to servers on the private subnet.

In a typical deployment, the FortiWeb outgoing interface connects to the OCB-FE Load Balancer.

Once the virtual appliance is deployed, you can configure FortiWeb-VM via either its web UI (from a web browser) or CLI (from a terminal emulator).

5.2 System Requirements

To deploy FortiWeb-VM for OCB-FE, first ensure you have the following resources:

- A OCB-FE, which allows you to log in to the Flex Engine Portal.
- A FortiWeb-VM license.
- OCB-FE VPC and storage account..

5.3 Downloading the FortiWeb-VM license & registering with Technical Support

When you purchase FortiWeb-VM from your reseller, you receive an email that contains a registration number. Use this number to download your license and register for technical support.

Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration.

To register & download your FortiWeb-VM license

1. On your management computer, start a web browser.

2. Log in to the Fortinet Technical Support web site: https://support.fortinet.com/

3. In the Asset Management quadrant of the page, click Register/Renew.

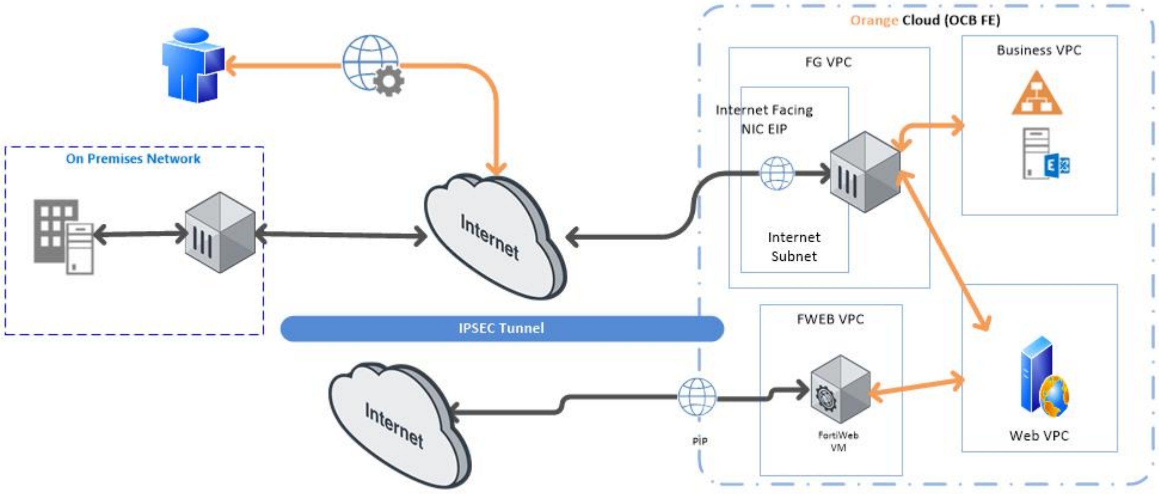
4. Provide the registration number that was emailed to you when you purchased the software. Registration numbers are a hyphenated mixture of 25 numbers and characters in groups of For example:
   12C45-AB3DE-678G0-F9HIJ-123B5
   A registration form is displayed.

5. Complete the form to register your ownership of FortiWeb-VM with Technical Support.
After you complete the form, a registration acknowledgement page is displayed.

6. Click the License File Download link.
Your browser downloads the .lic file that was purchased for that registration number.
You upload the license later, after you have deployed a FortiWeb instance in Azure.

5.4 Deployment Scenarios

5.4.1 FortiWeb (Reverse Proxy) in a hub-spoke network with no peering topology in OCB-FE

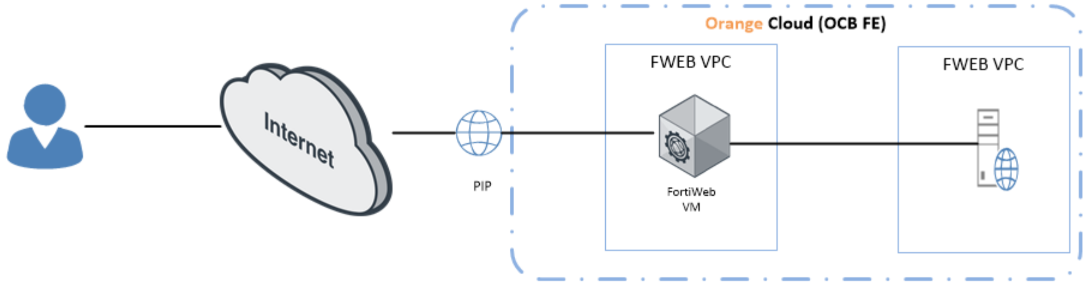


The hub is VPC on OCB-FE that acts as a central point of connectivity to your on-premises network. The spokes can be used to isolate workloads. Traffic flows between the on-premises datacenter and the hub through an ExpressRoute or VPN gateway connection.

The benefits of this topology include:

- Cost savings by centralizing services that can be shared by multiple workloads, such as network virtual appliances (NVAs) and DNS servers, in a single location.
- Separation of concerns between central IT (SecOps, InfraOps) and workloads (DevOps).

5.4.2 FortiWeb (Reverse Proxy) with no X Headers



DMZ Virtual Network where FortiWeb VM is Deployed.

Lab Subnet Virtual Network including the Webserver.

6 FortiWeb-VM Installation on OCB-FE

6.1 Create VPC

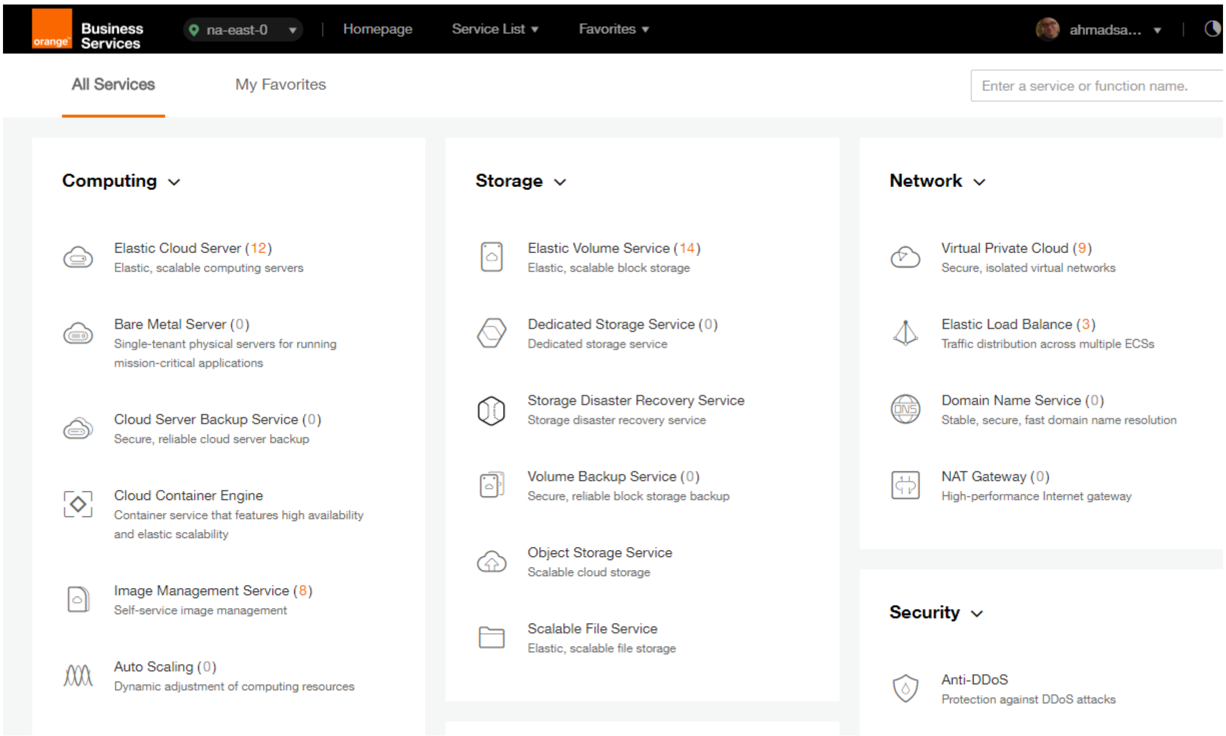
A VPC provides an isolated virtual network for ECSs. You can configure and manage the network as required.

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**.



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

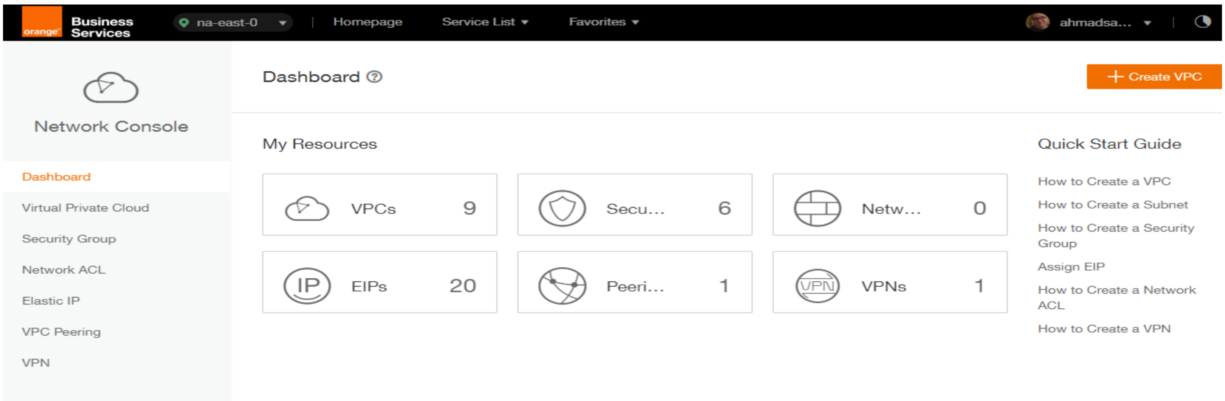
Domain Name Service (0)
Stable, secure, fast domain name resolution

NAT Gateway (0)
High-performance Internet gateway

Security

Anti-DDoS
Protection against DDoS attacks

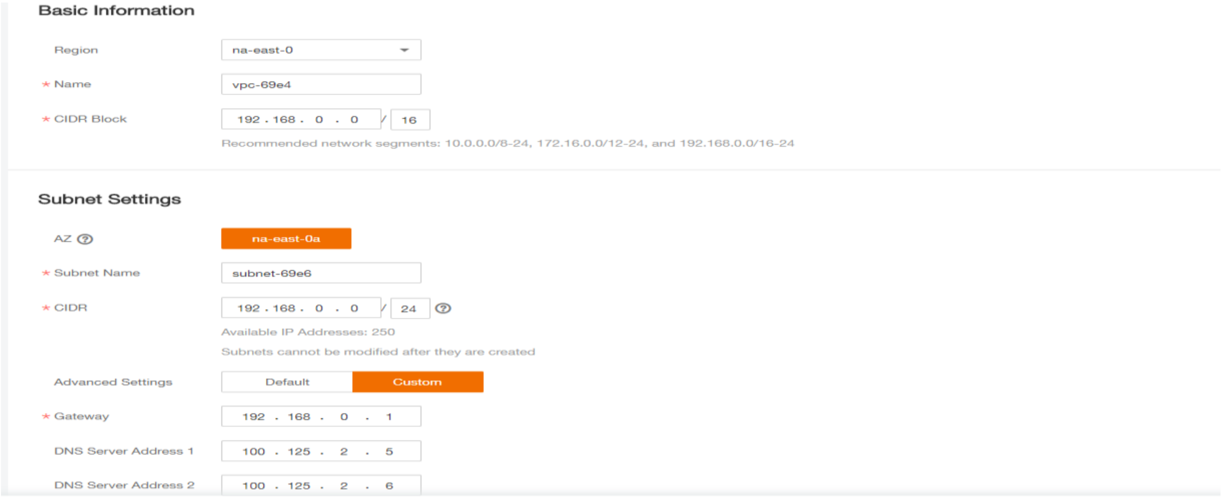
3. On the **Dashboard** page, click **Create VPC**.



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

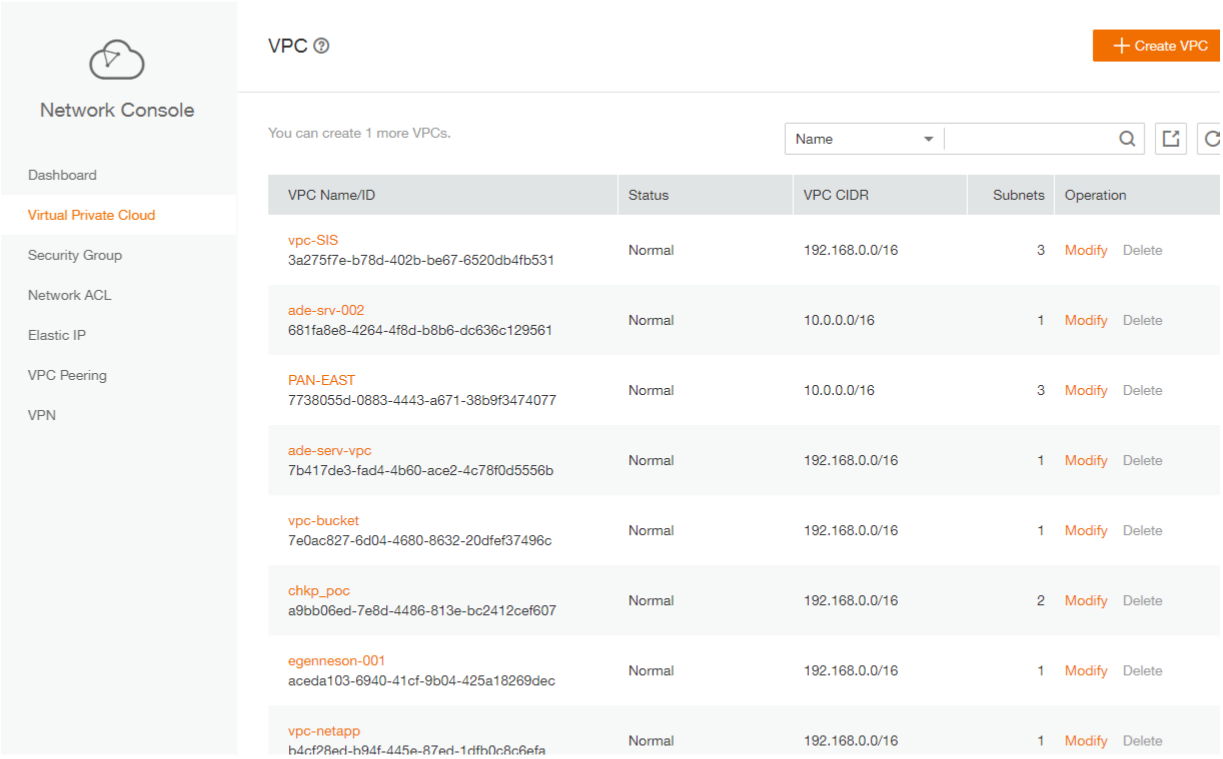
DNS Server Address 1: 100 . 125 . 2 . 5

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



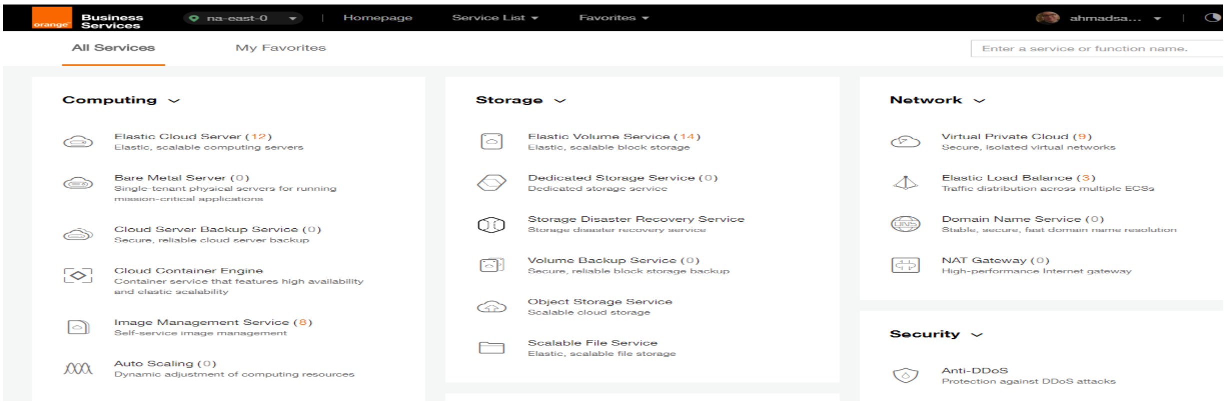
You can create 1 more VPCs.

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

6.2 Install FortiWEB 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**.



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

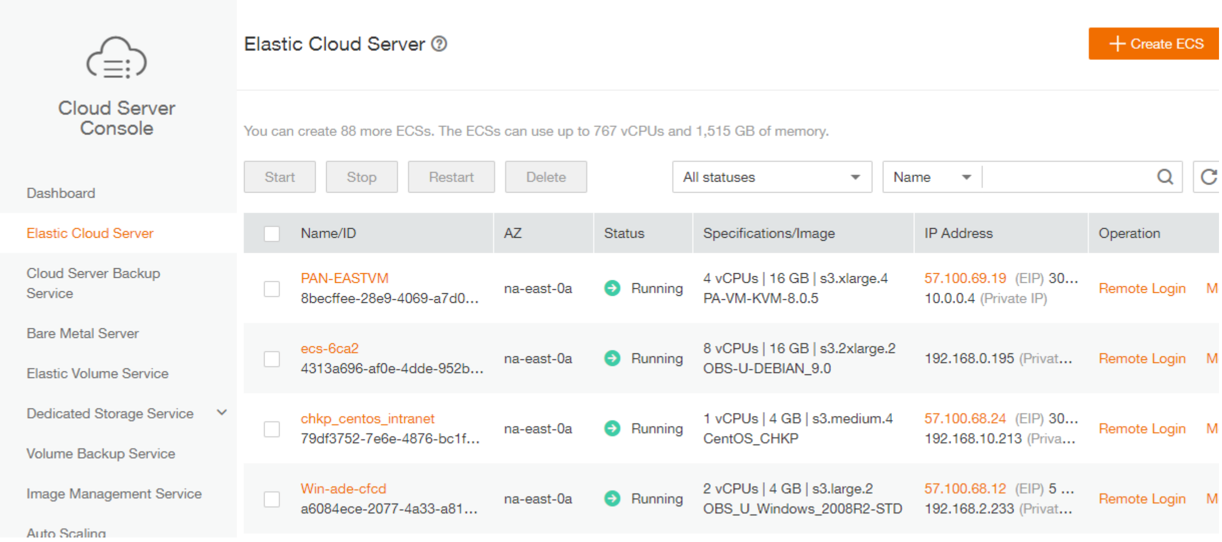
Domain Name Service (0)
Stable, secure, fast domain name resolution

NAT Gateway (0)
High-performance Internet gateway

Security

Anti-DDoS
Protection against DDoS attacks

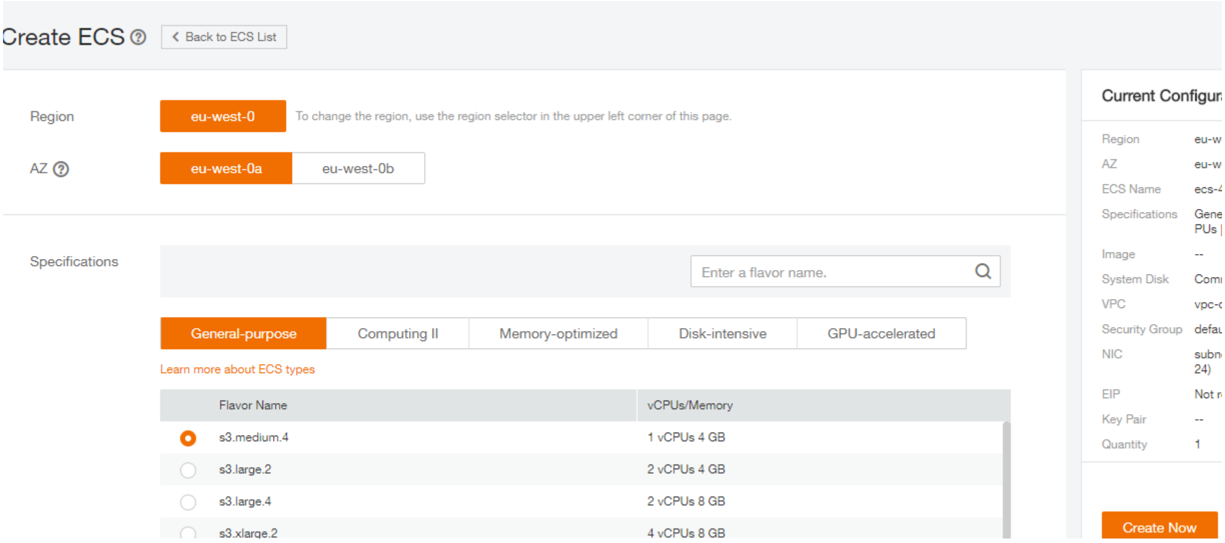
3. Click **Create ECS**.



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

□	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.



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.

	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	Com
VPC	vpc-c
Security Group	defau
NIC	subn 24)
EIP	Not r
Key Pair	--
Quantity	1

Very Important Notice:
Machine type to be chosen on OCB-FE should be General Purpose (S3)

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.

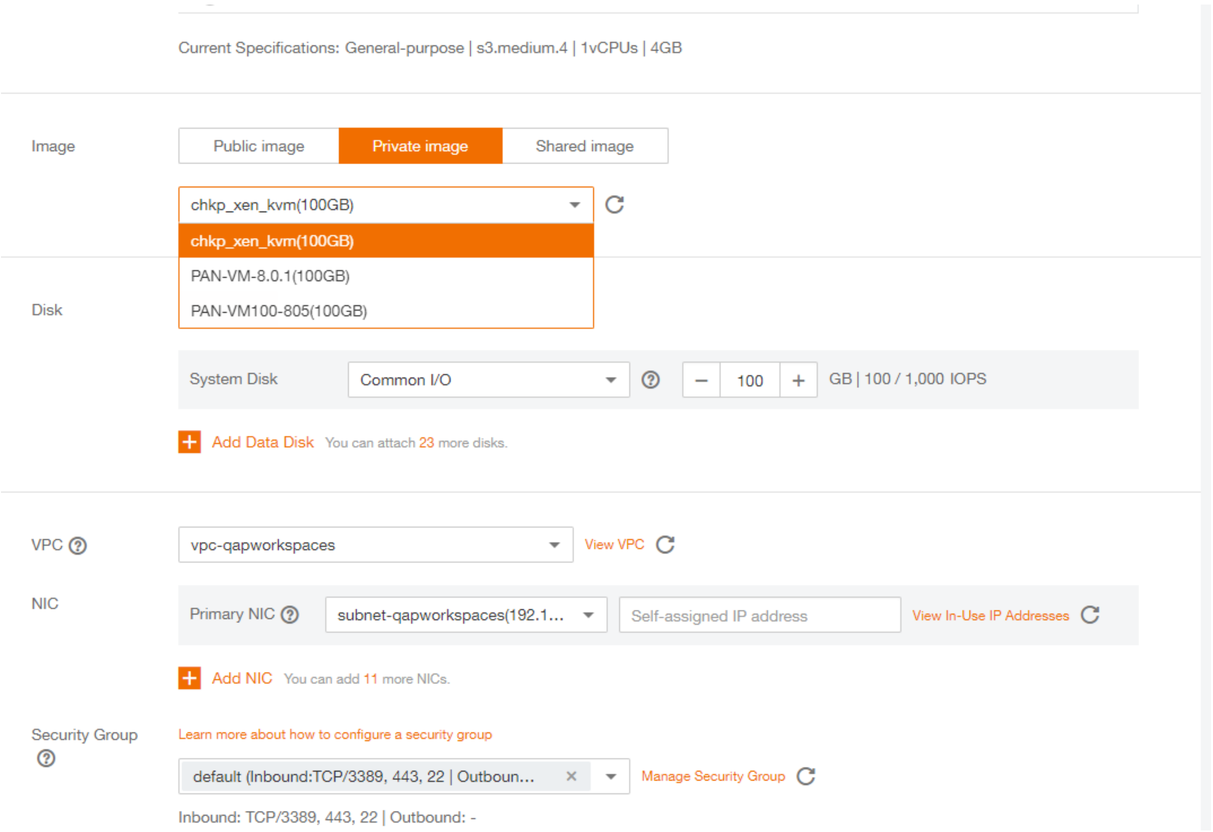
For example, if the Local Disk value is 3 x 1800 GB, three HDDs are attached to the ECS and the capacity of each HDD is 1800 GB.

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 FortiWeb 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. You should add a data disk of type SCSI for storing logs

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

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 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 three NIC cards one for the Management one for the internet facing Interface. The third NIC card is created as the inside (DMZ facing interface)
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

Table 2 Parameter descriptions

Parameter	Description
	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. ** In our scenario: We assigned 1 EIP for the management port

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 FortiWeb VM you can access it through **Https** using the EIP of the Management NIC. (username: admin / no password)

6.3 Connecting to FortiWeb's web UI & CLI

After you deploy FortiWeb-VM on OCB-FE, you use the public IP address displayed in the Azure instance information to access the web UI in a web browser or the CLI using an SSH connection.

To connect to the web UI

1. Enter the public IP address displayed in the Azure instance information in a web browser's address field.

2. Log in using the username and password you specified in the Azure virtual machine basic settings (**FortiWeb Administrative Username** and **FortiWeb Password**).

To connect to the CLI via SSH

These instructions connect to FortiWeb-VM for Azure using PuTTY terminal emulation software.

1. On your management computer, start PuTTY.

2. To ensure that your configuration does not use environment variables that can interfere with the connection, in the **Category** tree, expand **Connection**, and then click **Data.** Remove any environment variables.

3. Click **Session**, and for **Host Name (or IP Address)**, enter the public IP address of the FortiWeb-VM OCB-FE instance.

4. In Port, type 22.
5. For **Connection type**, select **SSH**.

6. Select **Open**.

   The SSH client connects to the FortiWeb appliance.
   The SSH client may display a warning if this is the first time you are connecting to the FortiWeb appliance and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiWeb appliance but it used a different IP address or SSH key.

7. Click **Yes** to verify the fingerprint and accept the FortiWeb appliance's SSH key. You cannot log in until you accept the key.
   The CLI displays a login prompt.

8. Enter the username you specified in the ECS basic settings (**FortiWeb Administrative Username**).

9. For password, enter the password you specified in the basic settings (**FortiWeb Password**).

If 3 incorrect login or password attempts occur in a row, FortiWeb temporarily blacklists your IP address from the GUI and CLI. This action protects the appliance from brute force login attacks. Wait 1 minute, and then attempt the login again.

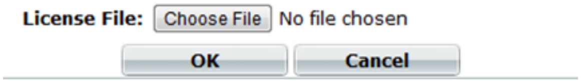
6.4 Uploading the license

You can upload the FortiWeb-VM license via a web browser connection to the web UI or the CLI. No maintenance period scheduling is required. The uploading process does not interrupt traffic or trigger an appliance reboot.

6.4.1 To upload the license via the web UI

1. Log in to the web UI using the public IP address for your FortiWeb-VM instance.
   On the status dashboard, the FortiGuard Information widget displays the current license status and provides the link you use to upload the license file.

2. By **VM License** , click **Update**.



3. Depending on your browser, either a Browse or Choose File button is displayed. Locate the license file (.lic) you downloaded earlier from Fortinet, then click OK.

   Your browser uploads the license file. Time required varies by the size of the file and the speed of the network connection. If you have uploaded a file that is not a license file, an error message is displayed:
   Uploaded file is not a license. Please upload a valid license.

   If you upload the right file type, FortiWeb connects to Fortinet to validate its license. Time required varies, but
   is usually only a few seconds. A message is displayed:
   License has been uploaded. Please wait for authentication with registration servers.

4. In the message box, click Refresh.

   If you uploaded a valid license, the following message is displayed:
   License has been successfully authenticated with registration servers.

   The web UI logs you out. The login dialog reappears.

5. Log in again.

6. To verify that the license was uploaded successfully, log in to the web UI again, then view the FortiGuard Information widget. The VM License row should say Valid.

   Also view the System Information widget. The Serial Number row displays the maximum number of vCPUs that you can allocate according to the FortiWeb-VM software license, such as FVVM040000003619 (where “VM04” indicates a limit of 2 vCPUs).

6.4.2 To upload the license via the CLI

1. Using an SSH client, log in to the CLI.

2. Enter the following command:

   execute restore vmlicense {ftp | tftp} <license-file_str> {<ftp_ipv4> | <user_ str>:<password_str>@<ftp_ipv4> | <tftp_ipv4>}

   where:

   {ftp | tftp} specifies whether to connect to the server using file transfer protocol (FTP) or trivial file transfer protocol (TFTP).
   <license-file_str> is the name of the license file.
   {<ftp_ipv4> is the IP address of the FTP server.
   <user_str> is the user name that FortiWeb uses to authenticate with the server.

<password_str> is the password for the account specified by <user_str>.
<tftp_ipv4> is the IP address of the TFTP server.

3. Confirm that you want to perform the license upload.

After the license is authenticated successfully, the following message is displayed:

*"*ATTENTION*: license registration status changed to 'VALID', please logout and relogin"*