AWS Deployment Guide

FortiIsolator 2.4.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

October 25, 2022
FortiIsolator 2.4.0 AWS Deployment Guide
51-240-809800-20221025

TABLE OF CONTENTS

Change log

Date	Change Description
2022-10-25	Initial version of document.

About FortiIsolator VM on AWS

This document provides information about deploying a FortiIsolator VM in the Amazon Web Services (AWS) environment. This includes how to configure the virtual hardware settings of the virtual appliance. This guide presumes that the reader has a thorough understanding of virtualization servers.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For that information, see the FortiIsolator Administration Guide.

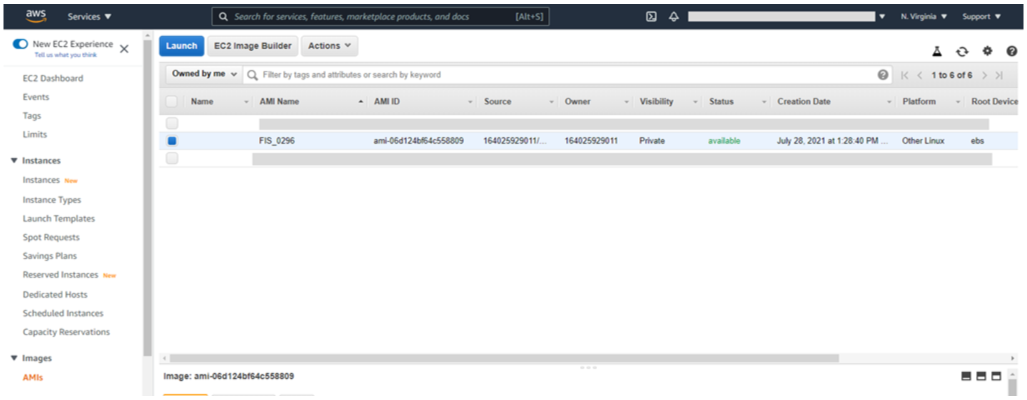
Deploying FortiIsolator on AWS

The deployment of FortiIsolator on AWS includes three steps:

- Step 1: Install FortiIsolator on AWS
- Step 2: Accessing to FortiIsolator CLI via Ubuntu
- Step 3: Browsing sites through FortiIsolator

Step 1: Install FortiIsolator on AWS

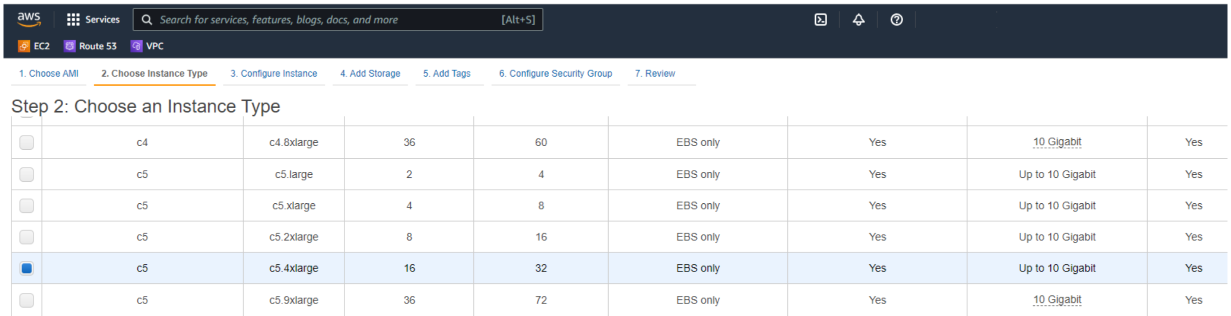
1. Verify the file has been uploaded in *AWS: EC2 > Images > AMIs*.



	Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date	Platform	Root Device
☐										
■		FIS_0296	ami-06d124bf64c558809	164025929011/...	164025929011	Private	available	July 28, 2021 at 1:28:40 PM ...	Other Linux	ebs
☐										

Image: ami-06d124bf64c558809

2. Create instance from the file.
   - Select an instance type:

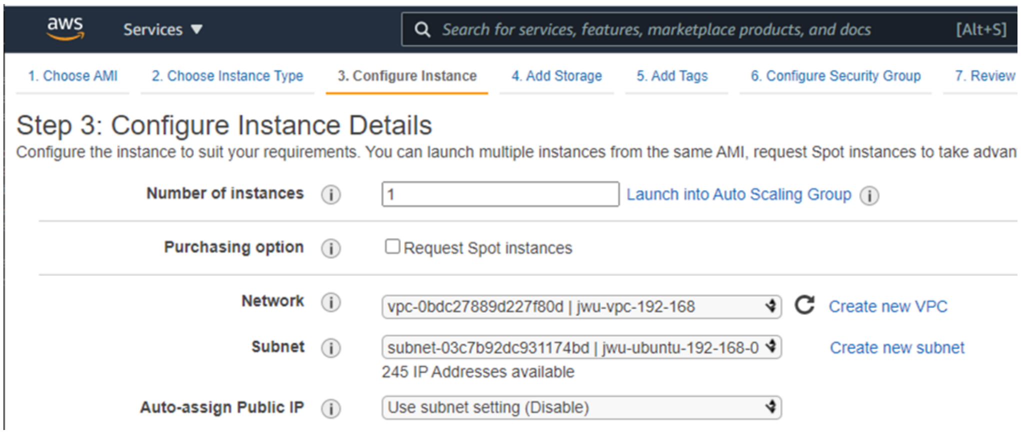


Step 2: Choose an Instance Type

☐	c4	c4.8xlarge	36	60	EBS only	Yes	10 Gigabit	Yes
☐	c5	c5.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes
☐	c5	c5.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
☐	c5	c5.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes
■	c5	c5.4xlarge	16	32	EBS only	Yes	Up to 10 Gigabit	Yes
☐	c5	c5.9xlarge	36	72	EBS only	Yes	10 Gigabit	Yes

FortiIsolator High Availabilities (HA) have to run on AWS Instances that are built on the Nitro System.

- Select VPC and Subnets:



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advan

Number of instances: 1 — Launch into Auto Scaling Group

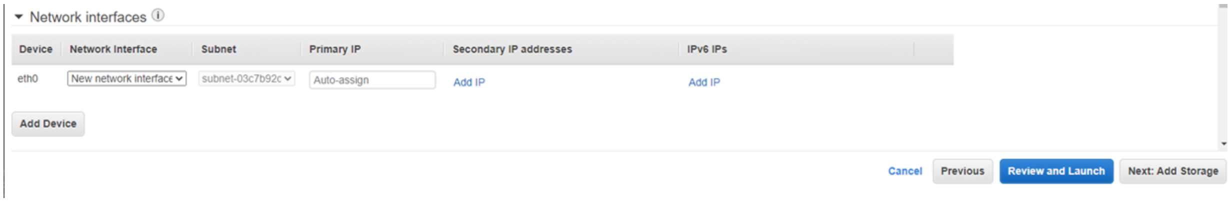
Purchasing option: □ Request Spot instances

Network: vpc-0bdc27889d227f80d | jwu-vpc-192-168 — Create new VPC

Subnet: subnet-03c7b92dc931174bd | jwu-ubuntu-192-168-0 — Create new subnet
245 IP Addresses available

Auto-assign Public IP: Use subnet setting (Disable)

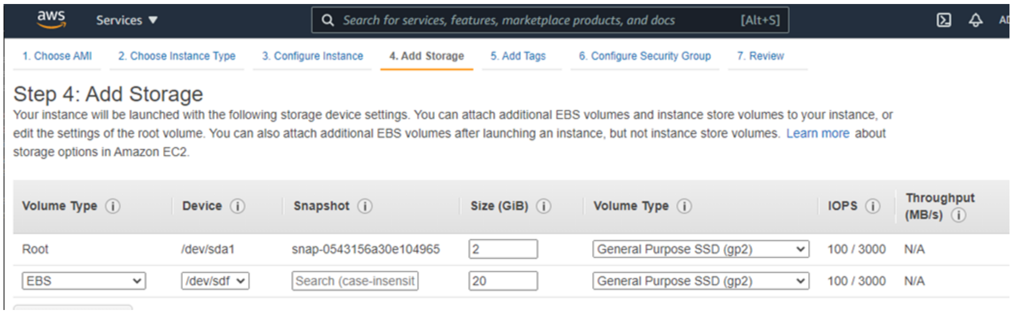
- Verify network interface, and click *Next: Add Storage*:



Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-03c7b92c	Auto-assign	Add IP	Add IP

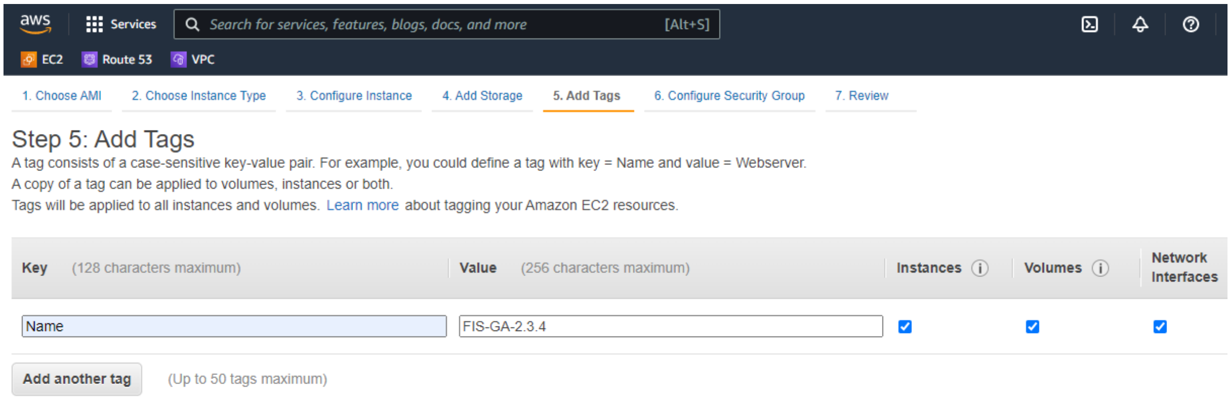
- Select */dev/sdf*, and assign size (GiB):



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)
Root	/dev/sda1	snap-0543156a30e104965	2	General Purpose SSD (gp2)	100 / 3000	N/A
EBS	/dev/sdf	Search (case-insensit	20	General Purpose SSD (gp2)	100 / 3000	N/A



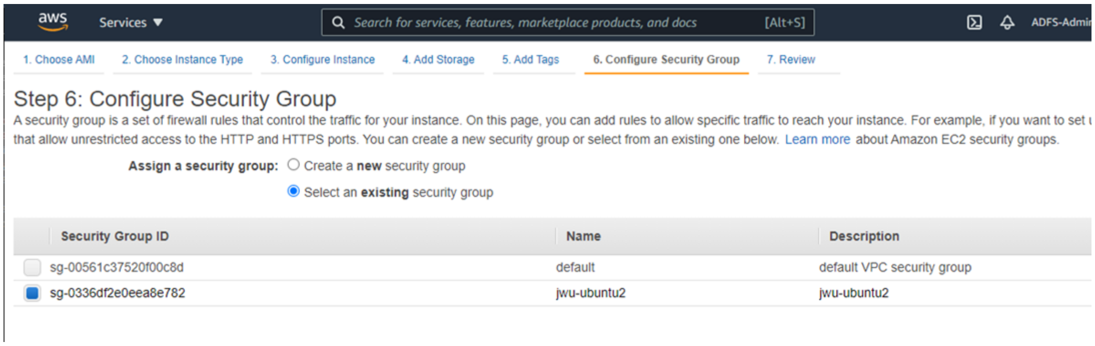
Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces
Name	FIS-GA-2.3.4	☑	☑	☑

(Up to 50 tags maximum)

- Select the security group that was created in the previous steps.

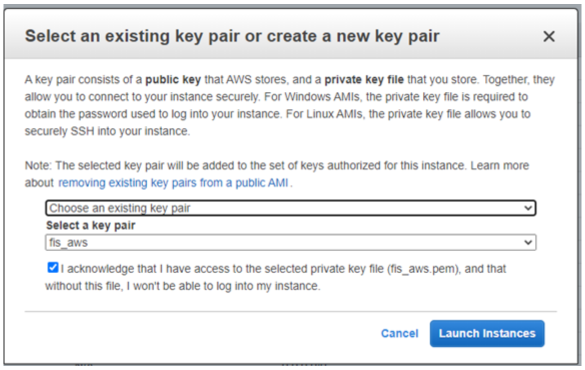


Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set u that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

	Security Group ID	Name	Description
□	sg-00561c37520f00c8d	default	default VPC security group
■	sg-0336df2e0eea8e782	jwu-ubuntu2	jwu-ubuntu2



Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Choose an existing key pair

Select a key pair

fis_aws

☑ I acknowledge that I have access to the selected private key file (fis_aws.pem), and that without this file, I won't be able to log into my instance.

After clicking *Launch Instance*, stop the process, and go add another three interfaces. Make sure FortiIsolator has four interfaces:

- Internal Interface: 192.168.0.0/24
- External Interface: 192.168.2.0/24
- Management Interface: 192.168.1.0/24
- HA Interface: 192.168.3.0/24

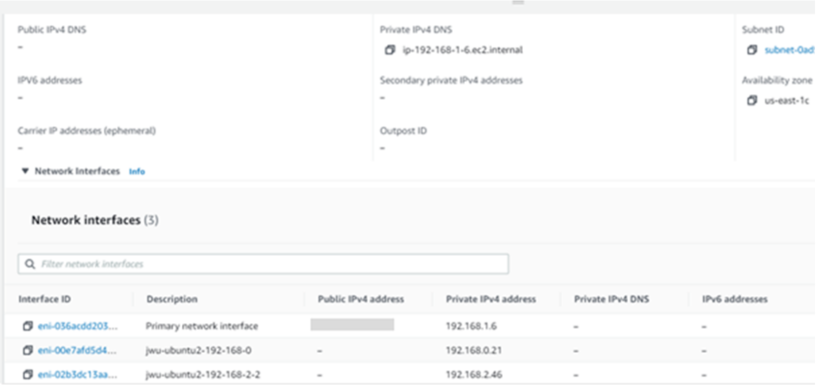
- Verify the interfaces are in this order.

Settings the third interface as `192.168.1.0/24` subnet allows you to access default management IP `192.168.1.99`.

Step 2: Accessing FortiIsolator CLI via Ubuntu

Pre-requisites

- You need an Ubuntu in AWS that has same subnets as FortiIsolator
- You need an associated EIP as the public IP to the Ubuntu on `192.168.1.0/24` subnet.



Public IPv4 DNS
-

Private IPv4 DNS
ip-192-168-1-6.ec2.internal

Subnet ID
subnet-0ad

IPV6 addresses
-

Secondary private IPv4 addresses
-

Availability zone
us-east-1c

Carrier IP addresses (ephemeral)
-

Outpost ID
-

▼ Network Interfaces Info

Network interfaces (3)

Filter network interfaces

Interface ID	Description	Public IPv4 address	Private IPv4 address	Private IPv4 DNS	IPv6 addresses
eni-036acdd203...	Primary network interface	[redacted]	192.168.1.6	-	-
eni-00e7afd5d4...	jwu-ubuntu2-192-168-0	-	192.168.0.21	-	-
eni-02b3dc13aa...	jwu-ubuntu2-192-168-2-2	-	192.168.2.46	-	-

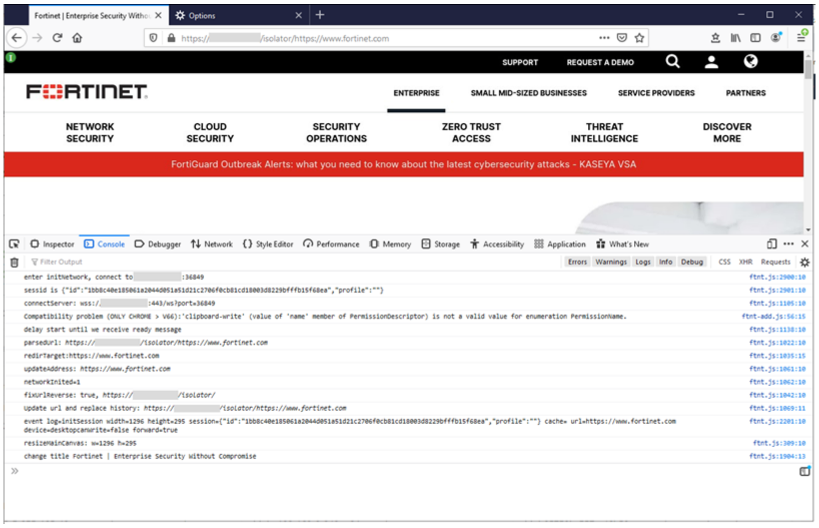
1. Connect to Ubuntu:
   ```
   > ssh -i "fis_aws.pem" ubuntu@public_ip(EIP)
   ```
2. From Ubuntu SSH to FIS via Mgmt Interface pre-defined IP (`192.168.1.99`).
   ```
   > ssh admin@192.168.1.99
   ```
3. Set Internal IP:
   ```
   > set internal-ip 192.168.0.99/24
   ```
4. Set DNS:
   ```
   > set dns 192.168.0.2 192.168.0.2
   ```
5. Set IP Mapping on FIS to public IP:
   ```
   > set fis-ipmap 443 443 public_ip
   ```
6. Overview:

   e.g.
   ```
   > set internal-ip 192.168.0.99/24
   > set internal-gw 0.0.0.0/0 192.168.0.2
   > set dns 192.168.0.2
   > set fis-ipmap 443 443 public_ip
   ```

Step 3: Browsing sites through FortiIsolator

IP Forwarding:

`https://<public_ip>/isolator/https://www.fortinet.com/`

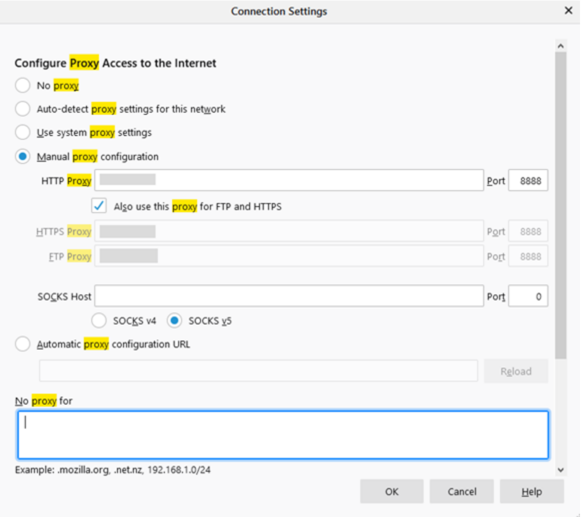


```
enter initNetwork, connect to [redacted]:36849                                                          ftnt.js:2900:10
sessid is {"id":"1bb8c40e185061a2044d051a51d21c2706f0cb81cd18003d8229bfffb15f68ea","profile":""}        ftnt.js:2901:10
connectServer: wss:/[redacted]:443/ws?port=36849                                                        ftnt.js:1105:10
Compatibility problem (ONLY CHROME > V66):'clipboard-write' (value of 'name' member of PermissionDescriptor) is not a valid value for enumeration PermissionName.   ftnt-add.js:56:15
delay start until we receive ready message                                                              ftnt.js:1138:10
parsedUrl: https://[redacted]/isolator/https://www.fortinet.com                                         ftnt.js:1022:10
redirTarget:https://www.fortinet.com                                                                    ftnt.js:1035:15
updateAddress: https://www.fortinet.com                                                                 ftnt.js:1061:10
networkInited=1                                                                                         ftnt.js:1062:10
fixUrlReverse: true, https://[redacted]/isolator/                                                       ftnt.js:1042:10
Update url and replace history: https://[redacted]/isolator/https://www.fortinet.com                    ftnt.js:1069:11
event log=initSession width=1296 height=295 session={"id":"1bb8c40e185061a2044d051a51d21c2706f0cb81cd18003d8229bfffb15f68ea","profile":""} cache= url=https://www.fortinet.com   ftnt.js:2201:10
device=desktopcanwrite=false forward=true
resizeMainCanvas: w=1296 h=295                                                                          ftnt.js:309:10
change title Fortinet | Enterprise Security Without Compromise                                          ftnt.js:1904:13
```

Proxy:

Browser Setting:

```
> HTTP Proxy: public_ip port 8888
```



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy [redacted] Port 8888

☑ Also use this proxy for FTP and HTTPS

HTTPS Proxy [redacted] Port 8888

FTP Proxy [redacted] Port 8888

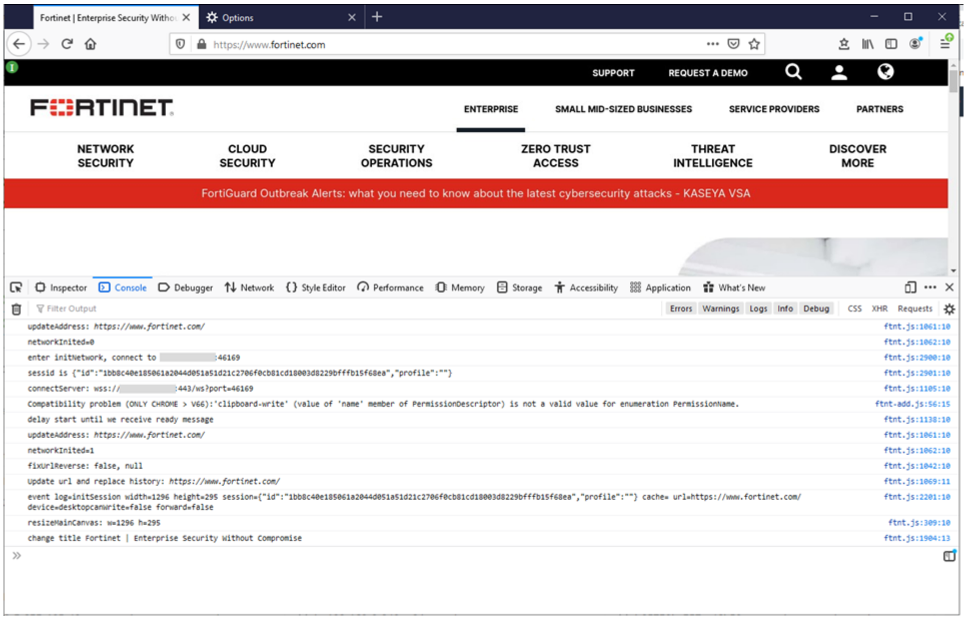
SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24



```
updateAddress: https://www.fortinet.com/                                          ftnt.js:1061:10
networkInited=0                                                                   ftnt.js:1062:10
enter initNetwork, connect to [redacted]:46169                                    ftnt.js:2900:10
sessid is {"id":"1bb8c40e185061a2044d051a51d21c2706f0cb81cd18003d8229bfffb15f68ea","profile":""}    ftnt.js:2901:10
connectServer: wss://[redacted]:443/ws?port=46169                                 ftnt.js:1105:10
Compatibility problem (ONLY CHROME > V66):'clipboard-write' (value of 'name' member of PermissionDescriptor) is not a valid value for enumeration PermissionName.    ftnt-add.js:56:15
delay start until we receive ready message                                        ftnt.js:1138:10
updateAddress: https://www.fortinet.com/                                          ftnt.js:1061:10
networkInited=1                                                                   ftnt.js:1062:10
fixUrlReverse: false, null                                                        ftnt.js:1042:10
Update url and replace history: https://www.fortinet.com/                         ftnt.js:1069:11
event log=initSession width=1296 height=295 session={"id":"1bb8c40e185061a2044d051a51d21c2706f0cb81cd18003d8229bfffb15f68ea","profile":""} cache= url=https://www.fortinet.com/    ftnt.js:2201:10
device=desktopcanWrite=false forward=false
resizeMainCanvas: w=1296 h=295                                                    ftnt.js:309:10
change title Fortinet | Enterprise Security Without Compromise                    ftnt.js:1904:13
```

FORTINET®

www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.