

FortiGate HA Setup in a VPC_CFT Steps

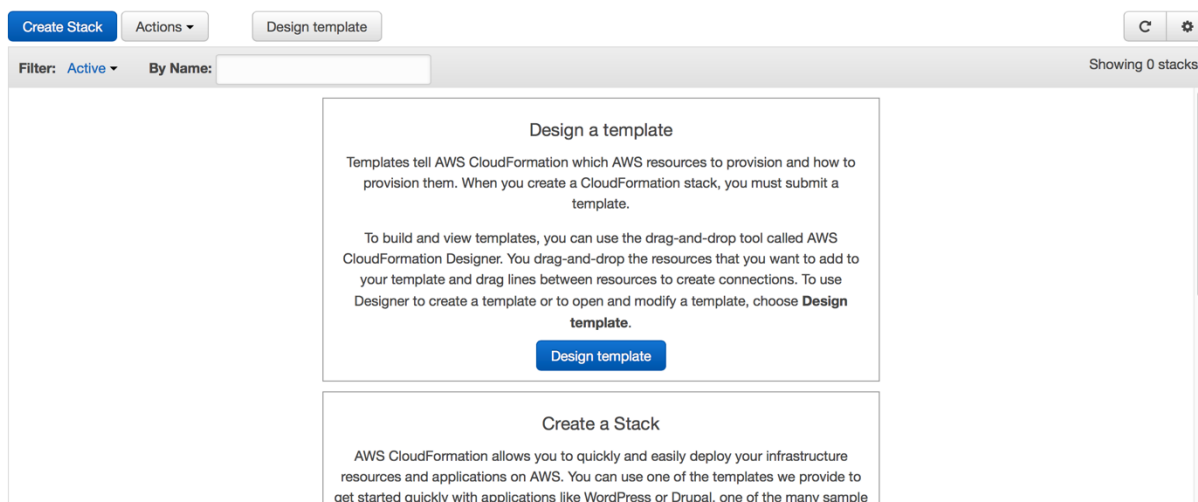
Step 1) Download the CloudFormation template here at <https://s3.amazonaws.com/fortigatetemplates/FortiGate-HAtemplate5.4.1.template>

Step 2) Login to AWS Management Console at <https://aws.amazon.com> using your AWS login credentials

Step 3) Navigate to CloudFormation service in the Management Tools Section of the Management Console.

The screenshot displays the AWS Management Console interface. On the left, there is a sidebar titled "Amazon Web Services" with a grid of service icons and their descriptions, categorized into Compute, Storage & Content Delivery, Database, Developer Tools, Management Tools, Security & Identity, Internet of Things, Game Development, Mobile Services, and Application Services. On the right, there is a section for "Resource Groups" with a "Learn more" link, a "Create a Group" button, and a "Tag Editor" button. Below this is the "Additional Resources" section, which includes links for "Getting Started", "AWS Console Mobile App", "AWS Marketplace", and "AWS re:Invent Announcements". At the bottom right, there is a "Service Health" section.

Step 4) Click on Create Stack



Step 5) Choose the option "Upload a template to Amazon S3", Click on "Choose File" and browse to the downloaded template from step 1). click Next

Create stack

Select Template

Specify Details

Options

Review

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. [Learn more.](#)

Design template

Choose a template A template is a JSON-formatted text file that describes your stack's resources and their properties. [Learn more.](#)

Select a sample template

Upload a template to Amazon S3

Choose File no file selected

Specify an Amazon S3 template URL

Cancel

Next

Create stack

Select Template

Specify Details

Options

Review

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. [Learn more.](#)

Design template

Choose a template A template is a JSON-formatted text file that describes your stack's resources and their properties. [Learn more.](#)

Select a sample template

Upload a template to Amazon S3

Choose File no file selected

Specify an Amazon S3 template URL

[View/Edit template in Designer](#)

Cancel

Next

Step 6) Here provide a stack name that to identify the CloudFormation stack

Step 7) Choose the appropriate values for all the parameters that is listed under the parameter section. There are some default values but can be changed according to the deployment needed. A short description for each parameter is provided to give some information on what the parameter is used for and what values to choose; /,.;]. The parameters are split into different sections for convenience. Make sure to provide information for all the parameters. The VPC CIDR cannot be greater than /16 and cannot be less than /28. For an AWS recommended fault tolerance, the AZ for each firewall1 and firewall2 should be different. The keypair would be the same keypair that would be used to create the firewalls and the worker node.

Stack name

Parameters

VPC Configuration

Please enter the VPC specific details here Enter the VPC CIDR that you want to use

FortiGate Instance Configuration

FortiGateInstanceType Enter the instance type and size that you want for the FortiGates

CIDRForFortiGateAccess Enter the CIDR from which FortiGate instances needs to be accessed

Primary FortiGate Instance Interface Configuration

Public1Subnet Enter the value of the Public1 subnet

Private1Subnet Enter the value of the Private1 subnet

Public1IP Enter the IP address for the external interface of the FortiGate1(IP from Public1Subnet)

Private1InternalIP Enter the IP address for the internal interface of the FortiGate1(IP from Private1Subnet)

Backup FortiGate Instance Interface Configuration

Public2Subnet Enter the value of the Public2 subnet

Private2Subnet Enter the value of the Private2 subnet

Public2IP Enter the IP address for the external interface of the FortiGate2(IP from Public2Subnet)

Private2InternalIP Enter the IP address for the internal interface of the FortiGate2(IP from Private2Subnet)

Worker Node Instance Configuration

CIDRForASAccess Enter the CIDR from which AS instance needs to be accessed

Route53 Configuration

DomainName Enter the Domain Name in which the DNS Record Sets would be created

DNSPrefix Enter the Prefix for the DNS Record Set that would be created for the two instances

Other parameters

AZForFirewall1 Enter the AZ for the primary firewall

AZForFirewall2 Enter the AZ for the backup firewall

KeyPair Enter the keypair that you want to associate with the launch of the test instances and worker node

Step 8) Click Next and provide a key name(optional)

Create stack

- Select Template
- Specify Details
- Options**
- Review

Options

Tags

You can specify tags (key-value pairs) for resources in your stack. You can add up to 10 unique key-value pairs for each stack. [Learn more.](#)

Key (127 characters maximum)	Value (255 characters maximum)
1 <input type="text"/>	<input type="text"/>

Advanced

You can set additional options for your stack, like notification options and a stack policy. [Learn more.](#)

Cancel Previous **Next**

Step 9) Click Create

Create stack

- Select Template
- Specify Details
- Options
- Review**

Review

Template

Template URL <https://s3-external-1.amazonaws.com/ct-templates-4c28gkesmp-us-east-1/2016175v5h-FortGate-template5.4.1.template>
Description AWS CloudFormation Template to launch VPC with a FortiGate protecting the resources in the private subnet
Estimate cost Cost

Details

Stack name FortiDemo

VPC and Subnets Information

VPCCIDR	10.0.0.0/16
PublicSubnet	10.0.0.0/24
PrivateSubnet	10.0.1.0/24

FortiGate Instance Configuration

FortiGateInstanceType	m3.large
CIDRForFortiGateAccess	0.0.0.0/0
AZForFirewall	us-east-1a
KeyPair	AS_Virginia

IP Configuration for the FortiGate Interfaces

PublicIP	10.0.0.254
PrivateInternalIP	10.0.1.254

Create IAM resources No

Options

Tags

No tags provided

Advanced

Notification	none
Timeout	none
Rollback on failure	Yes

Cancel Previous **Create**

Step 10) Wait for the CloudFormation service to finish creating all the resources. The events tab should the information on what the template is creating. The resources tab should have the information on what resources are created.

[Create Stack](#) [Actions](#) [Design template](#) Showing 1 stack

Filter: **Active** By Name:

Stack Name	Created Time	Status	Description
FortiDemo	2016-06-23 08:51:18 UTC-0700	CREATE_IN_PROGRESS	AWS CloudFormation Template to launch VPC with a FortiGate protecting the resources in the private subnet

[Overview](#) [Outputs](#) [Resources](#) [Events](#) [Template](#) [Parameters](#) [Tags](#) [Stack Policy](#) [Change Sets](#)

2016-06-23	Status	Type	Logical ID	Status reason
08:51:18 UTC-0700	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	FortiDemo	User Initiated

Step 11) Once the stack is created, the Output section would have the login information for the Firewall and also to the Worker Node.

[Create Stack](#) [Actions](#) [Design template](#) Showing 1 stack

Filter: **Active** By Name:

Stack Name	Created Time	Status	Description
FortiDemo	2016-06-23 08:51:18 UTC-0700	CREATE_IN_PROGRESS	AWS CloudFormation Template to launch VPC with a FortiGate protecting the resources in the private subnet

[Overview](#) [Outputs](#) [Resources](#) [Events](#) [Template](#) [Parameters](#) [Tags](#) [Stack Policy](#) [Change Sets](#)

2016-06-23	Status	Type	Logical ID	Status reason
08:51:24 UTC-0700	CREATE_IN_PROGRESS	AWS::EC2::VPC	VPC	Resource creation Initiated
08:51:24 UTC-0700	CREATE_IN_PROGRESS	AWS::EC2::InternetGateway	InternetGateway	Resource creation Initiated
08:51:23 UTC-0700	CREATE_IN_PROGRESS	AWS::EC2::VPC	VPC	
08:51:23 UTC-0700	CREATE_IN_PROGRESS	AWS::EC2::InternetGateway	InternetGateway	
08:51:18 UTC-0700	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	FortiDemo	User Initiated

Filter: Active By Name: Showing 1 stack

Stack Name	Created Time	Status	Description
FortiDemo	2016-06-23 08:51:18 UTC-0700	CREATE_IN_PROGRESS	AWS CloudFormation Template to launch VPC with a FortiGate protecting the resources in the private subnet

Overview Outputs Resources Events Template Parameters Tags Stack Policy Change Sets

Logical ID	Physical ID	Type	Status	Status Reason
InternetGateway	igw-684b1bec	AWS::EC2::InternetGateway	CREATE_COMPLETE	
VPC	vpc-c00bbaa7	AWS::EC2::VPC	CREATE_COMPLETE	

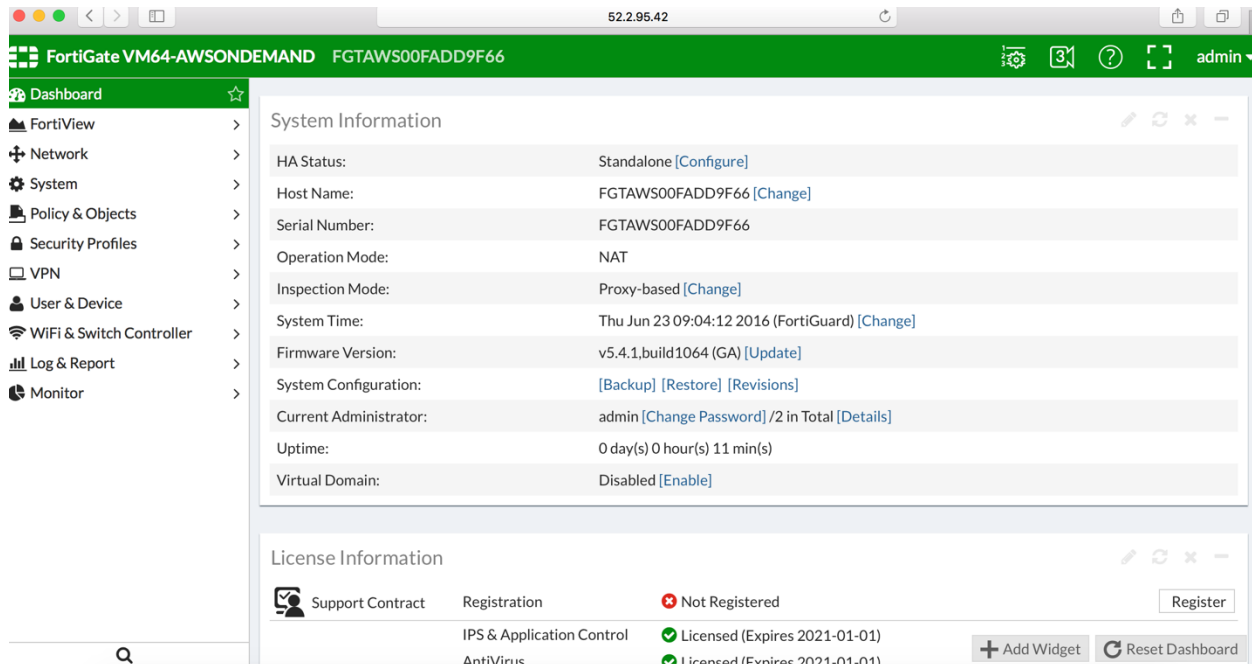
Filter: Active By Name: Showing 1 stack

Stack Name	Created Time	Status	Description
Fortinet1	2016-07-22 14:21:48 UTC-0700	CREATE_COMPLETE	AWS CloudFormation Template to launch VPC with Two Subnets and Two Instance in a VPC.

Overview Outputs Resources Events Template Parameters Tags Stack Policy Change Sets

Key	Value	Description
Fortigate	https://52.52.49.137	Connecting to the Active Fortigate
ASinstance	52.52.49.144	Connect to Amazon Linux Worker Node instance using ssh to this IP
Username	admin	Username to Access Fortigate
Password	I-2d301798	Password to login Fortigate is the primary instance id

Step 12) Login to the firewall through ssh/https and the firewall can be configured from there.



The screenshot shows the FortiGate web interface. The top navigation bar includes 'Dashboard', 'FortiView', 'Network', 'System', 'Policy & Objects', 'Security Profiles', 'VPN', 'User & Device', 'WiFi & Switch Controller', 'Log & Report', and 'Monitor'. The main content area is divided into two sections: 'System Information' and 'License Information'.

System Information:

HA Status:	Standalone [Configure]
Host Name:	FGTAW500FADD9F66 [Change]
Serial Number:	FGTAW500FADD9F66
Operation Mode:	NAT
Inspection Mode:	Proxy-based [Change]
System Time:	Thu Jun 23 09:04:12 2016 (FortiGuard) [Change]
Firmware Version:	v5.4.1,build1064 (GA) [Update]
System Configuration:	[Backup] [Restore] [Revisions]
Current Administrator:	admin [Change Password] /2 in Total [Details]
Uptime:	0 day(s) 0 hour(s) 11 min(s)
Virtual Domain:	Disabled [Enable]

License Information:

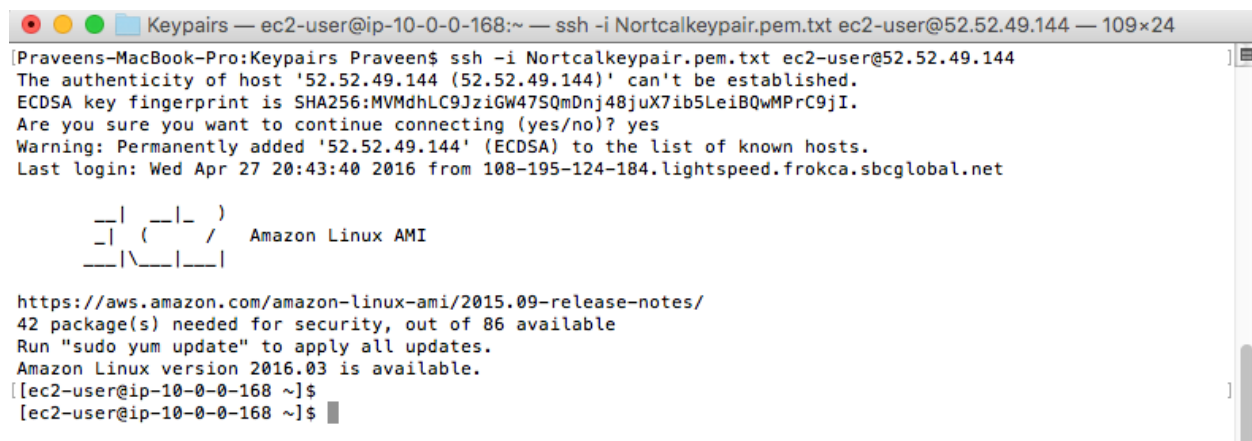
Support Contract	Registration	Status	Details
	IPS & Application Control	Not Registered	[Register]
	AntiVirus	Licensed (Expires 2021-01-01)	

Buttons: + Add Widget, Reset Dashboard

Step 13) Login to the Worker Node through ssh. The IP address of the Worker node is listed in the results section of the CloudFormation stack. The worker node is a Amazon Linux ami that has the scripts that are needed to monitor the FortiGates.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EC2_GetStarted.html#ec2-connect-to-instance-linux

Here is a screenshot of the command to login and how it looks like after login.



```
Praveens-MacBook-Pro:Keypairs Praveen$ ssh -i Nortcalkeypair.pem.txt ec2-user@52.52.49.144
The authenticity of host '52.52.49.144 (52.52.49.144)' can't be established.
ECDSA key fingerprint is SHA256:MVMdhLC9JziGW47SqmDnj48juX7ib5LeiBQwMPrc9jI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '52.52.49.144' (ECDSA) to the list of known hosts.
Last login: Wed Apr 27 20:43:40 2016 from 108-195-124-184.lightspeed.frokca.sbcglobal.net

  _ _ _ _ _
 _| ( _ _ /   Amazon Linux AMI
  _|\_ _ _ _ _

https://aws.amazon.com/amazon-linux-ami/2015.09-release-notes/
42 package(s) needed for security, out of 86 available
Run "sudo yum update" to apply all updates.
Amazon Linux version 2016.03 is available.
[ec2-user@ip-10-0-0-168 ~]$
[ec2-user@ip-10-0-0-168 ~]$
```


Step 14) Navigate to the folder fortigateha once you are logged into the worker node.
cd fortigateha

```
Praveens-MacBook-Pro:Keypairs Praveen$ ssh -i Nortcalkeypair.pem.txt ec2-user@52.52.49.144
The authenticity of host '52.52.49.144 (52.52.49.144)' can't be established.
ECDSA key fingerprint is SHA256:MVMdhLC9JziGW475QmDnj48juX7ib5LeiBQwMPrc9jI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '52.52.49.144' (ECDSA) to the list of known hosts.
Last login: Wed Apr 27 20:43:40 2016 from 108-195-124-184.lightspeed.frokca.sbcglobal.net

  _|  _|_ )
 _| (  _ /  Amazon Linux AMI
  _|\_|_|_|

https://aws.amazon.com/amazon-linux-ami/2015.09-release-notes/
42 package(s) needed for security, out of 86 available
Run "sudo yum update" to apply all updates.
Amazon Linux version 2016.03 is available.
[ec2-user@ip-10-0-0-168 ~]$
[ec2-user@ip-10-0-0-168 ~]$ cd fortigateha/
[ec2-user@ip-10-0-0-168 fortigateha]$
```

Step 15) Execute the python script fortigateha.py with the runtime variable of stack name.
python fortigateha.py stackname
Once this is done, FortiGate HA setup is complete.

```
Praveen — ec2-user@ip-10-0-0-168:~/fortigateha — ssh -i Desktop/Keypairs/Nortcalkeypair.pem.txt ec2-user@52.52.49...
[ec2-user@ip-10-0-0-168 fortigateha]$ python fortigateha.py Fortinet1
```

Step 16) Once the Script is started, the output will look like below.

```
Praveen — ec2-user@ip-10-0-0-168:~/fortigateha — ssh -i Desktop/Keypairs/Nortcalkeypair.pem.txt ec2-user@52.52.49...

[ec2-user@ip-10-0-0-168 fortigateha]$ python fortigateha.py Fortinet1
The Primary Instance is i-2d301798
The Backup Instance is i-e3117da6
The primary IP is 10.0.0.254
PING 10.0.0.254 (10.0.0.254) 56(84) bytes of data.
64 bytes from 10.0.0.254: icmp_seq=1 ttl=255 time=0.668 ms

--- 10.0.0.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.668/0.668/0.668/0.000 ms
The primary IP is 10.0.0.254
PING 10.0.0.254 (10.0.0.254) 56(84) bytes of data.
64 bytes from 10.0.0.254: icmp_seq=1 ttl=255 time=0.482 ms

--- 10.0.0.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.482/0.482/0.482/0.000 ms
The primary IP is 10.0.0.254
PING 10.0.0.254 (10.0.0.254) 56(84) bytes of data.
64 bytes from 10.0.0.254: icmp_seq=1 ttl=255 time=0.462 ms

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