

FortiGate-AWS Deployment Guide



FortiGate-AWS Deployment Guide

September 25, 2014

01-500-252024-20140925

Copyright© 2014 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 resultsmay 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.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

I.	Overview
	Amazon Virtual Private Cloud (Amazon VPC)
	Components of Amazon VPC
	Network Information
	Video Walk-through
II.	Basic AWS Network Setup7
	Step 1 – Setting up your AWS account
	Step 2 – Create a Virtual Private Cloud (VPC)
	Step 2.1 – VPC Wizard
III.	FortiGate Provisioning11
	Step 3 – EC2 Launching virtual machines
	Step 3. 1 – Choosing an AMI
	Step 3.2 – Instance type
	Step 3.3 – Instance Details
	Step 3.4 – Instance Storage
	Step 3.5 – Instance Tags
	Step 3.6 – Security groups
	Step 3.7 – Key Pair and Launch Instance
IV.	Network Configuration17
	Step 4 – Configure AWS network settings
	Step 4.1 - Associate a public "elastic" IP to the FG-VM public interface
	Step 4.2 – Confirm the assigned Public address
	Step 4.3 – Setting up the default route for the private network.
	Step 4.4 – Disable Source / Destination check on the Private FG interface.
	Step 4.5 - Navigate to EC2 dash to review the Instance state
	Step 4.6 - Access the Virtual FortiGate
	Step 4.6 – SSH to the FortiGate
V.	Step 5.0 – Setup a Test VM24
	Step 5.1 – Provision a new AMI
	Step 5.2 – Select a VM Instance type
	Step 5.3 – Choose Instance settings
	Step 5.4 – VM Storage settings
	Step 5.5 – Assign any tags needed to the VM Instance
	Step 5.6 – VM Security Group Settings
	Step 5.7 – Review Instance Settings and Launch Instance
	Step 5.8 – Create key pair

VI.	Step 6.0 – FortiGate Configuration	. 30
	Step 6.1 - Update FortiGate Password	
	Step 6.2 – Confirm network settings	
	Step 6.3 – Setup basic policies	
VII.	Step 7 – Testing	.33
	Step 7.1 – Launch a RDP session to test	
	Step 7.2 – Retrieve your VM's password	
	Step 7.3 – Test Outbound access	
VIII.	Appendix	.36
	Regions and Availability Zones	
	Amazon EC2 Key Pairs	
	Additional info and links	

Change History

Version	Date	Author.	Changes
1.0	8-1-2014	Justin L. Wireman	Initial Document creation

Overview

This document is design to be a quick start walk-though in setting up a virtual Fortinet device utilizing the AWS services. We will start out reviewing some of the AWS concepts.

Amazon Virtual Private Cloud (Amazon VPC)

Amazon VPC lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can also create a Hardware Virtual Private Network (VPN) connection between your corporate datacenter and your VPC and leverage the AWS cloud as an extension of your corporate datacenter.

You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.



Components of Amazon VPC

Amazon VPC is comprised of a variety of objects that will be familiar to customers with existing networks:

- **A Virtual Private Cloud (VPC):** a logically isolated virtual network in the AWS cloud. You define a VPC's IP address space from a range you select.
- Subnet: a segment of a VPC's IP address range where you can place groups of isolated resources.
- Internet Gateway: the Amazon VPC side of a connection to the public Internet.
- **NAT Instance:** An EC2 instance that provides Port Address Translation for non-EIP instances to access the Internet via the Internet Gateway.
- Hardware VPN Connection: a hardware-based VPN connection between your Amazon VPC and your datacenter, home network, or co-location facility.
- Virtual Private Gateway: the Amazon VPC side of a VPN Connection.
- Customer Gateway: Your side of a VPN Connection.
- **Router:** Routers interconnect Subnets and direct traffic between Internet Gateways, Virtual Private Gateways, NAT instances and Subnets.
- **Peering Connection:** A peering connection enables you to route traffic via private IP addresses between two peered VPCs.

How do instances in a VPC access the Internet?

Elastic IP addresses (EIPs) give instances in the VPC the ability to both directly communicate outbound to the Internet and to receive unsolicited inbound traffic from the Internet (e.g., web servers)

How do instances without EIPs access the Internet?

Instances without EIPs can access the Internet in one of two ways:

Instances without EIPs can route their traffic through a NAT instance to access the Internet. These instances use the EIP of the NAT instance to traverse the Internet. The NAT instance allows outbound communication but doesn't enable machines on the Internet to initiate a connection to the privately addressed machines using NAT, and

For VPCs with a Hardware VPN connection, instances can route their Internet traffic down the Virtual Private Gateway to your existing datacenter. From there, it can access the Internet via your existing egress points and network security/monitoring devices.

Network Information

Figure #2 the default network design for a Public and Private VPC. We will be replacing much of the Router functionality with the FortiGate as pictured in figure 1.

- VPC Subnet 10.0.0/16
- Public Subnet 10.0.0/24
- Private Subnet 10.0.1.0/24



Figure 2 – Default Public / Private VPC design

Basic AWS Network Setup

Step 1 – Setting up your AWS account

For more information on AWS check out the getting started guide. <u>Click here</u>

You will need to provide billing information to setup an AWS

account. Once you have completed the basic account setup you will be presented with the AWS console.



Step 2 - Create a Virtual Private Cloud (VPC)

To allow VM instances access to more than one interface you need to create a VPC (virtual private cloud). You need to change dashboards to VPC and for our purpose start the VPC wizard.



Figure 4 - VPC Dashboard

It is important to note that like most multi-tenant environments AWS reserves the first 5 IP address of each network that is created for its own router / firewall and DHCP / DNS servers.

Step 2.1 - VPC Wizard

This next section is a visual walk-through of the VPC wizard. Select the Public and Private subnet option.

/PC with a Single Public Subnet	In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet, Instances in the counter whose carefulliate of the and constrained to be foremula the average.	Internet, SJ.
VPC with Public and Private Subgets	subnet using Network Address Translation (NAT).	DynamoDB, SNS. SOS. etc.
	A /16 network with two /24 subnets. Public subnet instances use Eastic IPs to access	
Provide Subnets and Iardware VPN Access	Transition (NAT) instance in the public subnet. (Hourly charges for NAT instances apply.)	Amazon Virtual Private Cloud
	Select	
PC with a Private Subnet Only and Hardware VPN Access		

Figure 5 - VPC Wizard

One item to double check on step 2 of the VPC wizard is to make sure that both subnets are in the <u>same</u> <u>availability zone</u>. Please see the <u>Appendix</u> for more information on availability zones.

🎁 Services 👻 Edit	*	Justin L Wireman -	Oregon +	Help +						
Step 2: VPC with Publ	Step 2: VPC with Public and Private Subnets									
IP CIDR block*										
VPC name:	Fort/VPC									
Public subnet:*	10.0.0/24 (251 IP addresses available)									
Availability Zone:*	us-west-2a =									
Public subnet name:	Public subnet									
Private subnet:*	10.0.1.0/24 (251 IP addresses available)									
Availability Zone:*	us-west-2a t									
Private subnet name:	Private subnet									
	You can add more subnets after AWS creates the VPC.									
Specify the details of your NAT inst	ance.									
Instance type:*	Small (m1.small) 1									
Key pair name:	No key pair 1									
	Note: Instance rates apply. View Rates.									
Enable DNS hostnames:*	⊛Yes No									
Hardware tenancy:*	Default :									
	Cance	and Exit Bac	k Creat	te VPC						

Figure 6 - VPC Wizard Subnets

Once you have verified the network setting, click create VPC and you will see the screen below.

Gervices - Edit	×							Justin L Wirer	nan +	Oregon +.	Help +
Step 2: VPC with Publ	ic and Privat	e Subnets	S								
IP CIDR block*	10.0.0/16	(65531 IP ad	dresses avail	(alcle							
VPC name:	ForsivPC	3									
Public subnet:*	10.0.0.0/24	Q51 IP addr	esses availab	leg .							
Availability Zone:*	us-west-2a ±										
Public subnet name:	Public subnet										
Private subnet:*	10.0.1.0/24	0251 IP addr	esses availab	let :							
Availability Zone:*	us-west-24 1										
Private subnet name:	Private subnet	1									
	You can add more a	subnets after Al	AS counters the	a VPC							
Specify the details of your NAT inst	ance.		-								
Instance type:*	Small (m1.small)		Puesies	.57	this may b						
Key pair name:	No key pair 1		few minu	ites)	e (inis may u	ino a					
	Note: Instance rates	apply. View R	atos.								
Enable DNS hostnames:*	eYes ⊖No										
Hardware tenancy:*	Default 2										
							Cance	l and Exit	Back	Creat	te VPC

Figure 7 - VPC Wizard

When the VPC setup has been completed you can review subnet and routing information on the VPC Dashboard. More on this later in the guide, as you will need to alter settings to route traffic through the FortiGate.

🎁 Services 🗸 Ed	dit v			Justin L Wireman 🗸 🛛	regon • Help •
VPC Dashboard Filter by VPC: vpc-da4fb7bf (10.0.0.0/. +	Create Subnet Delete Subnet	Modify Auto-Assign F propertie X	Public IP	K < 1 to 2 of 5	€ ♦ Ø 2 Subnets > > >
Virtual Private	Name	Subnet ID	- State	- VPC	CIDR
Cloud	Public subnet	subnet-81a571e4	available	vpc-da4fb7bf (10.0.0.0/16)	10.0.0/24
Your VPCs	Private subnet	subnet-86a571e3	available	vpc-da4fb7bf (10.0.0.0/16)	10.0.1.0/24
Subnets					
Route Tables					
Internet Gateways					
DHCP Options Sets					
Elastic IPs					
Peering Connections					
Figure 8					

FortiGate Provisioning

Step 3 - EC2 Launching virtual machines

Change dashboards to the EC2 dashboard. For time sake it is normally faster to get the VM provisioning started while setting up the network. Click Launch Instance on this screen.



Figure 9 - EC2 Dashboard

Step 3.1 - Choosing an AMI

🎁 Services 🗸 Edit	*				Justin L Wireman 🗸	Oregon - Help -
1. Choose AMI 2. Choose Instan	ice Type 3. Configu	ure Instance 4. Add Storage	5. Tag Instance	6. Configure Security Group	7. Review	
Step 1: Choose an A An AMI is a template that contains provided by AWS, our user comm	Amazon Ma s the software configurity, or the AWS M	chine Image (AM guration (operating system, a larketplace; or you can selec	l) pplication server, at one of your own	and applications) required to AMIs.	launch your instance. You c	Cancel and Exit
Quick Start	O Fortinat				< < 1 to 5 of	f 5 Products > >
My AMIs	C Fortinet	×				
AWS Marketplace	FORTIDET	FortiGate-VM				Select
Community AMIs		★★★★ (2) v5.0.5 Sold by Fo Bring Your Own License + AWS License (License) + AWS	rtinet Inc. usage fees pazon Machine Image (A	MD I Indated: 3/9/14		
 Categories All Categories Software Infrastructure (5) 		FortiGate virtual appliances a critical security controls withi More info	llow you to mitigate n your virtual infrast	blind spots and improve policy ucture	compliance by implementing	
 Operating System Clear Filter All Linux/Unix Other Linux (5) 	FCRTINET	Fortinet FortiAnalyzer-V ****** (0) v5.0.4 Sold by Fo Bring Your Own License + AWS Linux/Unix, Other v5.0.4 64-bit Am FortiAnalyzer Network Securit Fortinet Security Appliances.	Trinet Inc. usage fees nazon Machine Image (A y Logging, Analysis, A comprehensive su	MI) Updated: 11/10/13 and Reporting Appliances sec iite of easily	urely aggregate log data from	Select
 Software Pricing Plans 		More info				
☐ Hourly (1) ☐ Annual (1) ☐ Bring Your Own License (4)	F#BTINET	Fortinet FortiManager-V ***** (0) v5.0.4 Sold by Fo Bring Your Own License + AWS Linux/Unix, Other v5.0.4 64-bit Am	rtinet Inc. usage fees nazon Machine Image (A	Mi) Updated: 11/10/13		Select
 Region Current Region (5) All Regions (5) 		FortiManager Security Manag Security devices, from severa More info	ement appliances a al to thousands, incl	low you to centrally manage an uding FortiGate,	y number of Fortinet Network	
		Product Product Add				

Figure 10 - AMI Wizard

For this guide we have chosen the Bring your Own License version of the FortiGate VM.



Step 3.2 – Instance type

Choose the instance type that matches the license. For this example I have a 1 vCPU license file.

Î	Services ~	Edit 🗸	Justin L Wireman 🗸	Oregon 👻	Help 🕶

 1. Choose AMI
 2. Choose Instance Type
 3. Configure Instance
 4. Add Storage
 5. Tag Instance
 6. Configure Security Group
 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by:	All instance types	~	Current generation	~	Show/Hide Columns

Currently selected: m3.medium (3 ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon E5-2670v2, 3.75 GiB memory, 1 x 4 GiB Storage Capacity)

Note: The vendor recommends using a m3.xlarge instance (or larger) for the best experience with this product.

					Instance Channel (CD)	EDC Optimized	Natural Destances
	Family -	Туре –	vCPUs (j) 👻	Memory (GiB) 👻	i)	Available (j)	i
0	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
0	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
0	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High
	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes	High
	Compute optimized	c3.large	2	3.75	2 x 16 (SSD)	-	Moderate
	Compute optimized	c3.xlarge	4	7.5	2 x 40 (SSD)	Yes	Moderate
	Compute optimized	c3.2xlarge	8	15	2 x 80 (SSD)	Yes	High
	Compute optimized Compute optimized Compute optimized	c3.large c3.xlarge c3.2xlarge	2 4 8	3.75 7.5 15	2 x 16 (SSD) 2 x 40 (SSD) 2 x 80 (SSD)	- Yes Yes	Moderate Moderate High

Cancel Previous

Review and Launch

Next: Configure Instance Details

Step 3.3 – Instance Details

In this step you will choose the public subnet, assign IP addresses, and add the eth1 interface (private subnet).

1. Choose AMI 2. Choose Instance Type	3. Cor	nfigure Instance	4. Add Storage	5. Tag Instance	6. Config	ure Security Group	7. Review
Step 3: Configure Instar	ice D	etails					
Number of instances	(i)	1					
Purchasing option	(j)	Request Sp	ot Instances				
Network	(j)	vpc-da4fb7bf (1	0.0.0.0/16) FortiVP	c	÷ C	Create new VPC	
Subnet	(j)	subnet-81a571 250 IP Address	e4(10.0.0.0/24) Pub ses available	lic subnet us-west-	2 ‡	Create new subne	et
Auto-assign Public IP	()	Disable			÷		
IAM role	(j)	None			\$		
Shutdown behavior	i	Stop			\$		
Enable termination protection	i	Protect aga	inst accidental ter	mination			
Monitoring	(i)	Enable Clou Additional cha	dWatch detailed r rges apply.	nonitoring			
Tenancy	(j)	Shared tenancy Additional cha	(multi-tenant hardwa rges will apply for	re) dedicated tenanc	\$ y.		
 Network interfaces 							
Device Network Interface	Subnet	Pr	imary IP	Secondary IP	addresse	es	

201100				
eth0	New network interface \$	subnet-81a571e4 ‡	10.0.0.5	Add IP
eth1	New network interface \$	subnet-86a571e3 ‡	10.0.1.5	Add IP

Cancel Previous

Review and Launch

Step 3.4 – Instance Storage

If you are configuring this for demonstration purposes, you can change the highlighted storage size to create a larger disk size for logging / reporting.

()								Justin L Wire
1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Tag Instance	6. Configure Security Group	7. Review		
ur instance will edit the setting pout storage op	Id Storage Il be launched with the fo is of the root volume. You tions in Amazon EC2.	llowing storage device s u can also attach additio	ettings. You can a nal EBS volumes a	attach additional after launching a	EBS volumes and instance In instance, but not instance	store volumes to you store volumes. Lea	r instance, n more	
Type (i)	Device (i)	Snapshot (i)	Size (GiB) (i	Volume Ty	pe (i) IOPS (i)	Delete on Termina	tion (i) Encrypted (i)	
Root	/dev/sda1	snap-acbcb25d	2	General Pur	pose (SSD)		Not Encrypted	
EBS	¢ /dev/sdb ¢	Search (case-insensitive)	eþ	Magnetic	÷ N/A			\otimes
Add New Volu	ime							
Free tier	r eligible customers can g	get up to 30 GB of EBS (General Purpose (SSD) or Magneti	c storage. Learn more abo	ut free usage tier elig	ibility	
and dou	ge rectrictions.							

Figure 12

Step 3.5 – Instance Tags

It is valuable to create tags to quickly reference instance items in your AWS deployment. I have tagged a few items below as an example.

Justin L Wireman 👻 Oregon 👻 Help	•
Tag Instance 6. Configure Security Group 7. Review	
with key = Name and value = Webserver. Learn more about tagging your Amazon EC2	
Value (255 characters maximum)	
FortiGate-VM	×
10.0.0.5	\otimes
10.0.1.5	
	Justin L Wireman × Oregon × Help Tag Instance 6. Configure Security Group 7. Review with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 Value (255 characters maximum) FortiGate-VM 10.0.0.5

Figure 13 - Instance Tags

Step 3.6 – Security groups

Amazon by default has your VPC behind a basic firewall. Since we are going to be utilizing the FortiGate, I have created a Permit All security group and applied it to this instance.

🎁 Services 🗸 Edit 🗸				Justin L Wireman 🗸	Oregon - Help -
1. Choose AMI 2. Choose Instance Type	3. Configure Instance 4	. Add Storage 5. Tag Insta	6. Configure Security C	aroup 7. Review	
Step 6: Configure Security A security group is a set of firewall rules that want to set up a web server and allow Inter- group or select from an existing one below.	y Group It control the traffic for yo net traffic to reach your in Learn more about Ama:	ur instance. On this page, nstance, add rules that alk zon EC2 security groups.	you can add rules to allow s w unrestricted access to th	specific traffic to reach your instance le HTTP and HTTPS ports. You can	ce. For example, if you create a new security
Assign a security grou	p: • Create a new sec	urity group			
	Select an existing	security group			
Security group name	B: PermitAll				
Description	n: This security group v	vas generated by AWS Marketpl	ace and is based on recommende	ed setting	
Туре ()	Protocol (i)	Port	Range (i)	Source (i)	
All traffic \$	All	0 - 6	5535	Anywhere \$ 0.0.0.0/0	8
Add Rule					
Rules with source of 0.0.0.0/0 allow only.	w all IP addresses to acc	ess your instance. We rec	ommend setting security gr	oup rules to allow access from kno	wn IP addresses

Figure 14 - Security Groups

Step 3.7 - Key Pair and Launch Instance

- Choose proceed without a keypair and use the default FortiGate username / password.
- Click Launch Instance to begin the provisioning.



Step 4 – Configure AWS network settings

In this section you will be locating items such as the Network interface ENI on the EC2 dashboard and making IP and routing updates on the VPC dashboard.

Step 4.1 - Associate a public "elastic" IP to the FG-VM public interface

- On the EC2 Dashboard under the Network interface menu.
 - Locate the public interface ENI.
 - See step 4.3 figure 18 for a screenshot of this menu.
- On the VPC Dashboard under the Elastic IPs menu.
 - If the Public IP is associated with a default instance you will need to disassociate the Public IP before you can proceed.
 - Use the ENI of the public FortiGate interface as the object to associate the public IP.

🎁 Services 🗸 Ed	lit v	Justin L Wireman 🗸 Oregon 👻 Help 🗸
VPC Dashboard Filter by VPC:	Allocate New Address Release Address Associate Address Disassociate Address Filter VPC addresses ~ Q, Search Elastic IPs X	
Virtual Private Cloud	Ad Associate Address	Private Address
Your VPCs Subnets	Associate this IP address with an instance or a network interface.	
Route Tables Internet Gateways	Associate with Network Interface ‡ i Network Interface eni-3e4f165b ‡ i Private IP address 10.0.0.5 ÷ i	
Elastic IPs Peering Connections	54.200.77.	
Security	Address: 54.200.77.52 Network interface ID:	
Network ACLs Security Groups	Instance ID: Network interface owner: Scope: vpc Allocation ID: eipallor	c-e2db3187
VPN Connections Customer Gateways		
Virtual Private Gateways VPN Connections		



Step 4.2 – Confirm the assigned Public address

• Take note of the public IP address and DNS assigned. You will use these items in later steps.

📋 Services 🗸 Ed	ilit v			Justin	n L Wireman 👻 Ore	egon ≁	Help 🗸	
EC2 Dashboard Events Tags Reports Limits	Allocate New Address Rel Filter: All addresses Y Q	Associate Addresses Associate Search Addresses Instance	Address Disassoci	ate Address	< < 1 to 1 of 1 A	€ ddresses Public	✿ s → DNS	2
INSTANCES Instances Spot Requests Reserved Instances	54.200.77.52	i-64fb846f (FortiGate-VM)	10.0.0.5	vpc-da4fb7	rbf	ec2-54-	200-77-	·52.u
AMIs Bundle Tasks								
 ELASTIC BLOCK STORE Volumes Snapshots 								
NETWORK & SECURITY Security Groups Elastic IPs Placement Groups Load Balancers								
Key Pairs	Address: 54.200.77.52		000					
Network Interfaces AUTO SCALING Launch Configurations Auto Scaling Groups 	Public I Instanc Scop Public DN	p 54.200.77.52 e i-64fb846f (FortiGate-VM) vpc vpc s ec2-54-200-77-52.us-west- 2.compute.amazonaws.com	Netw	letwork interface ID Private IP address ork interface owner Allocation ID	eni-3e4f165b 10.0.0.5 138006460020 eipalloc-e2db3187			

Step 4.3 – Setting up the default route for the private network.

- On the EC2 Dashboard under the Network interface menu.
 - Locate the network interface ID (ENI-) of the private network and Copy the ID.
 - Change dashboards back to the VPC>Route Tables
 - Edit the default route (for the private subnet) to point to the FortiGate private network interface ID.
 - o Demonstrated in figures 19-20

•

🎁 Services 🗸 Ed	dit 🗸								Justin L Wireman 🗸	Oregon 🗸	Help 🗸	
EC2 Dashboard Events	Creat	te Network Interfa	Attach	Detach	Delete	Actions V				Ð	¢	0
Tags	Filter	All VPC network	k interfaces 🗸	Q Sear	ch Network	nterfaces	×	K	< 1 to 3 of 3 Netwo	k Interface	s >	>
Reports Limits		Name 💡	· · Network i	interfa - Su	bnet ID 🚽	VPC ID	- Zone	Ŧ	Security groups -	Descriptio	n –	Ins
INSTANCES			eni-96752	cf3 sub	onet-43ad7926	vpc-0e46be6b	us-west-2a		PermitALL	Primary net	wo	i-6
Instances			eni-00752	c65 sub	onet-43ad7926	vpc-0e46be6b	us-west-2a		default			i-9
Spot Requests Reserved Instances		Private FG Interfac	e eni-91752	cf4 sub	onet-40ad7925	vpc-0e46be6b	us-west-2a		PermitALL			i-6
IMAGES AMIs Bundle Tasks ELASTIC BLOCK STORE												
Volumes Snapshots												
NETWORK & SECURITY Security Groups Elastic IPs Placement Groups Load Balancers												
Key Pairs	Netwo	ork Interface: eni-	91752cf4			000				I		
Network Interfaces	Det											
Figure 18												
🧍 Services 🗸 E	dit 🗸								Justin L Wireman 🗸	Oregon	Hel	p •
VPC Dashboard	Crea	te Route Table	Delete Rou	te Table	Set As Main	Table				Ð	٠	Ø
None ‡	Qs	earch Route Tal	oles and thei	r proj 🗙					I< ≤ 1 to 2 of 2	Route Tab	les >	>
Virtual Private		Name	*	Route Table	ID	- Associate	ed With	-	N ain	· VPC	•	
Cloud				rtb-4601c523		1 Subnet		١	ю	vpc	-0e46be	6b (1I
Your VPCs				rtb-4701c522		0 Subnets		١	/es	vpc	-0e46be	6b (11
Subnets												
Route Tables												
Internet Gateways	rth_47	016522				7.7.7.7						
DUOD Ontinge Onte	rtD-47	010022										

DHCP Options Sets Elastic IPs Subnet Associations Route Propagation Summary Routes Tags Peering Connections Edit Destination Target Status Propagated Security 10.0.0/16 local Active No Network ACLs 0.0.0.0/0 eni-00752c65 / i-96d6a99d Active No Security Groups

rtb-4701c522					
Summary	Routes Subnet A	ssociation	Route F	ropagation	Tags
Cancel Save					
Destination	Target	Status	Propagated	Remove	
10.0.0/16	local	Active	No		
0.0.0/0	eni-91752cf4	Active	No	×	
	eni-91752cf4 Pri No results	vate FG	Interface	×	
Add another route					

Figure 20

• Associate the private subnet to the private routing entry you have been editing in the previous steps.

rtb-4701c52 Summa	2 ry Routes Subnet Associations	Route Pro	opagation Tags
Cancel	Save		
Associate	Subnet	CIDR	Current Route Table
	subnet-43ad7926 (10.0.0.0/24) Public subnet	10.0.0/24	rtb-4601c523
I	subnet-40ad7925 (10.0.1.0/24) Private subnet	10.0.1.0/24	Main

Step 4.4 – Disable Source / Destination check on the Private FG interface.

- On the EC2 Dashboard under the Network interface menu.
 - o Right click and select Change Source/Dest Check
 - o Select Disable and Save

育 Services 🗸 Ed	dit 🗸						
EC2 Dashboard Events	Create Network Interface	Attach	tach Delete	Actions ¥			
Tags	Filter: All VPC network inte	rfaces 👻 🔍	Search Network Inte	erfaces	×		K
Reports	.		0.1	1000	-	0	
Limits	Name Y ·	Network Interfa*	Subnet ID 🔹	VPC ID	* Zone	 Security groups 	*
INSTANCES	Public subnet	eni-b7b094d2	subnet-c16eb9a4	vpc-663ec403	us-west-2a	PermitALL	
Instances		5b094d0	subnet-c66eb9a3	vpc-663ec403	us-west-2a	PermitALL	
Spot Requests	Detach	cb69219	subnet-c16eb9a4	vpc-663ec403	us-west-2a	default	
Reserved Instances	Delete						
IMAGES	Manage Private IP Addresses	5					
AMIs	Associate Address						
Bundle Tasks	Disassociate Address						
ELASTIC BLOCK STORE	Change Termination Behavior						
Volumes	Change Security Groups						
Snapshots	Add/Edit Tags						
NETWORK & SECURITY	Change Description						
Security Groups		-					
Elastic IPs							
Placement Groups							
Load Balancers							
Key Pairs							
Network Interfaces							

Services 🗸 Edi	
EC2 Dashboard	Create Network Interface Attach Detach Delete Actions *
Tags	Filter: All VPC network interfaces × Q. Search Network Interfaces ×
Reports Limits	Name ♥ ▼ Network interfa▼ Subnet ID ▼ VPC ID ▼ Zone ▼ Security groups
INSTANCES	Public subnet eni-b7b094d2 subnet-c16eb9a4 vpc-663ec403 us-west-2a PermitALL
Instances	Private FG Interface eni-b5b094d0 subnet-c66eb9a3 vpc-663ec403 us-west-2a PermitALL
Spot Requests	eni-7cb69219 subnet-c16eb9a4 vpc-663ec403 us-west-2a default
Reserved Instances	
IMAGES	
AMIs	
Bundle Tasks	
ELASTIC BLOCK STORE	Change Source/Dest. Check ×
Volumes	
Snapshots	Network Interface eni-b5b094d0
NETWORK & SECURITY	Source/dest. check O Enabled
Security Groups	Disabled
Elastic IPs	
Placement Groups	Cancel Save
Load Balancers	
Key Pairs	
Network Interfaces	

Step 4.5 - Navigate to EC2 dash to review the Instance state

- Once confirming that the instance has finished provisioning and powering up check the following items.
 - o Public IP/DNS assigned
 - Confirm the correct security group is assigned.

🎁 Services 🗸 Ec	lit ¥		ıt	ustin L Wireman 👻 Oregon 👻 Help 👻
EC2 Dashboard Events	Launch Instance Connect	Actions v		ତ 🕈 🖗
Tags	Filter: All instances Y All inst	tance types 👻 🔍 i-64fb846f	×	$ \langle$ \langle 1 to 1 of 1 Instances \rangle $\rangle $
Reports Limits	■ Name ♀ - Instance ID	✓ Instance Type ✓ Availability Zone	- Instance State - Status	Checks Alarm Status Public DNS
INSTANCES	FortiGate-VM i-64fb846f	m3.medium us-west-2a	🥥 running 🛛 🛣 In	itializing None 🍖 ec2-54-200-7
Instances				
Spot Requests				
Reserved Instances				
IMAGES				
AMIs				
Bundle Tasks				
ELASTIC BLOCK STORE	Instance: i-64fb846f (FortiGate-	••••		880
Volumes				
Snapshots	Description Status Checks	Monitoring Tags		
NETWORK & SECURITY	Instance ID	i-64fb846f	Public DNS	ec2-54-200-77-52.us-west-
Security Groups				2.compute.amazonaws.com
Elastic IPs	Instance state	running m2 madium	Public IP	54.200.77.52
Placement Groups	Instance type		Elastic IP	54.200.77.52
Load Balancers	Fivale DN3	2.compute.internal	Availability 2011e	u5-w651-2.d
Key Pairs	Private IPs	10.0.0.5	Security groups	PermitAll . view rules
Network Interfaces	Secondary private IPs		Scheduled events	No scheduled events
AUTO SCALING	VPC ID	vpc-da4fb7bf	AMI ID	FortiGate-VM64-AWS build0252
Launch Configurations				AMI-e5936f4a-0d69-479f-919c-
Auto Scaling Groups				(ami-f8026dc8)
	Subnet ID	subnet-81a571e4	Platform	-
	Network interfaces	eth0	IAM role	-
		eth1		
	Source/dest. check	True	Key pair name	-
			Owner	138006460020

Step 4.6 - Access the Virtual FortiGate

- Open a HTTPS session to the public IP or DNS entry provided and login with the default username / password.
- Upload license file for BYOL. (See figure 22)
- The FortiGate will reboot after license install.

● ○ ○ / Install FortiGate-VM Licens	× Fortinet Service & Support ×
← → C ↑ 🖹 <u>kttps</u> ://54.200.77.52/index	
👯 Apps 📄 Popular 📄 Personal 📄 Fortinet	
	Install FortiGate-VM License File
License File: Choose File FGVM00000024667.lic	
	OK Cancel

Figure 22

Step 4.7 – SSH to the FortiGate

- SSH to the device using the DNS hostname
- Issue the following commands to test access
 - o Ping 8.8.8.8 to test connectivity
 - o Execute update-now
 - Execute formatlogdisk and reboot (Option step if you need disk logging)

```
FortiGate-VM64-AWS# Execute ping 8.8.8.8
FortiGate-VM64-AWS# Execute update-now
FortiGate-VM64-AWS# Execute formatlogdisk
```

Step 5.0 – Setup a Test VM

In this step we will setup a test windows VM on the private network and configure it to use the FortiGate for all access in and out of the private network. In this example we are going to setup remote access to the test VM as well.

Step 5.1 - Provision a new AMI

For this example we are using Windows Server 2012. Note that any OS version could be used for testing / demonstration purposes.

🎁 Services 🗸 Edit	✓ Justin L Wireman ✓	Oregon - Help -
1. Choose AMI 2. Choose Insta Step 1: Choose an Community AMIs	nce Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review Amazon Machine Image (AMI) Root device type: ebs Virtualization type: hvm	Cancel and Exit
\Box Free tier only ($\ensuremath{\hat{i}}$	Red Hat Enterprise Linux 7.0 (HVM) - ami-77d7a747 Red Hat Red Hat Enterprise Linux version 7.0 (HVM), EBS-backed Free ther eligible Root device type: ebs Virtualization type: hvm	Select 64-bit
	Suse Linux Enterprise Server 11 sp3 (HVM), SSD Volume Type - ami-7fd3ae4f Suse Linux Enterprise Server 11 Service Pack 3 (HVM), EBS General Purpose (SSD) Volume Type. Nvidia driver installs automatically during startup for GPU instances. Root device type: ebs Virtualization type: hvm	Select 64-bit
	Output Ubuntu Server 14.04 LTS (HVM), SSD Volume Type - ami-e7b8c0d7 Ubuntu Ubuntu Server 14.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services). Free tier eligible Not device type: ebs Virtualization type: hvm	Select 64-bit
	Microsoft Windows Server 2012 R2 Base - ami-57e29c67 Windows Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English] Free tier eligible Root device type: ebs Virtualization type: hvm	Select 64-bit
	Image: Windows Microsoft Windows Server 2012 R2 with SQL Server Express - ami-5be59b6b Windows Microsoft Windows Server 2012 R2 Standard edition, 64-bit architecture, Microsoft SQL Server 2014 Express edition. [English] Free tiar eligible Root device type: ebs Virtualization type: hvm	Select 64-bit

Step 5.2 – Select a VM Instance type

The default is the free tier general purpose type. This instance type is fine for basic testing.

Î	Services 🗸 Edit 🗸					Justin L Wirema	an • Oregon • Help •
1. Cho	ose AMI 2. Choose Instance T	ype 3. Configure	Instance 4. Add St	torage 5. Tag Instan	ce 6. Configure Security Grou	up 7. Review	
Step Amazon of CPU	D 2: Choose an Ins n EC2 provides a wide selectio , memory, storage, and networ v can meet your computing pro- ting pro- ting pro- section (1997)	tance Type on of instance types rking capacity, and eeds	s optimized to fit diff give you the flexibil	erent use cases. Inst ity to choose the app	ances are virtual servers tha propriate mix of resources for	t can run applications. They your applications. Learn m	have varying combinations ore about instance types and
Filter	by: All instance types 👻	Current gene	eration 👻 Show	v/Hide Columns			
Curre	ently selected: t2.micro (Varial	ble ECUs, 1 vCPUs	s, 2.5 GHz, Intel Xec	on Family, 1 GiB men	nory, EBS only)		
	Family ~	Type -	vCPUs (j) 👻	Memory (GiB) 🤟	Instance Storage (GB)	EBS-Optimized Available (j	Network Performance
	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High
	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes	High
	Compute optimized	c3.large	2	3.75	2 x 16 (SSD)	-	Moderate
	Compute optimized	c3.xlarge	4	7.5	2 x 40 (SSD)	Yes	Moderate
	Compute optimized	c3.2xlarge	8	15	2 x 80 (SSD)	Yes	High
	Compute optimized	c3 4xlarge	16	30	2 x 160 (SSD)	Yes	High

Cancel Previous Review and Launch Next: Configure Instance Details

Step 5.3 – Choose Instance settings

- It is important to select the private subnet to place this VM behind the FortiGate.
- I have also chosen to assign the IP address of 10.0.1.25. I have done this so I can setup port forwarding on the FortiGate while this VM is provisioned.

Ĩ	Services ~	Edit 🗸						Justin L Wireman 🗸	Oregon 🗸	Help 🕶
1. Cho	Dose AMI 2. Choo	se Instance Type	3. Configure Ins	tance 4. Add Storage	5. Tag Instance	6. Configure S	ecurity Group	7. Review		
Step	o 3: Configu	ure Instar	Details		_					
	Purc	hasing option	(i) 🗌 Requ	est Spot Instances						
		Network	() vpc-da4	fb7bf (10.0.0.0/16) FortiV	PC	÷ C Cre	ate new VPC			
		Subnet	i subnet- 250 IP /	86a571e3(10.0.1.0/24) Pri Addresses available	ivate subnet us-west	-: ÷ Cre	eate new subne	t		
	Auto-as	sign Public IP	(j) Use sub	net setting (Disable)		\$				
		IAM role	() None			\$				
	Shutd	lown behavior	(j) Stop			*				
	Enable terminati	on protection	(i) Prote	ct against accidental te	rmination					
		Monitoring	i 🛛 Enab	le CloudWatch detailed	monitoring					
			Addition	al charges apply.						
		Tenancy	i Shared Addition	enancy (multi-tenant hardw al charges will apply for	vare) r dedicated tenanc	÷ y.				
▼ Ne	etwork interfac	es								
Devic	ce Network Inte	erface	Subnet	Primary IP	Secondary IF	addresses				
eth0	New network i	nterface ‡	subnet-86a571e3	10.0.1.25	Add IP					
Add	Device									
► Ac	dvanced Detail	s								
						Cano	Previous	Review and Launch	Next: Ad	d Storage

Figure 25

l

Step 5.4 – VM Storage settings

Adjust the default storage setting as appropriate for our virtual machine. If you are deploying this machine for basic testing the default should suffice.

🎁 Services 🗸 Edit 🗸	Justin L Wireman 🗸
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6.	Configure Security Group 7. Review
Step 4: Add Storage Your instance will be launched with the following storage device settings. You can attach additional EBS or edit the settings of the root volume. You can also attach additional EBS volumes after launching an in- about storage options in Amazon EC2.	volumes and instance store volumes to your instance, stance, but not instance store volumes. Learn more
Type (i) Device (i) Snapshot (i) Size (GiB) (i) Volume Type (i)	IOPS (1) Delete on Termination (1) (1)
Root /dev/sda1 snap-435fe5b7 60 General Purpose (SSD) ÷	90 / 3000 🗹 Not Encrypted
Add New Volume	
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic sto and usage restrictions.	brage. Learn more about free usage tier eligibility

Figure 26

Step 5.5 – Assign any tags needed to the VM Instance

This is an optional step.

Step 5.6 – VM Security Group Settings

Assign the same "Permit All" security group you created during the step 3.6.

Ũ	Services 🗸 Edit 🗸				Justin L Wireman 👻 O	regon 👻 Help 👻				
1. Ch	oose AMI 2. Choose Instance Type	3. Configure Instance 4. Add Storage	5. Tag Instance	6. Configure Security Group	7. Review					
A secu want to group	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 up a web server and allow Internet traffic to reach your instance, add rules 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 grou	up: OCreate a new security group								
		 Select an existing security gro 	oup							
	Security Group ID	Name		Description		Actions				
	sg-636feb06	default		default VPC secu	rity group	Copy to new				
	sg-4d69ed28	PermitAll		This security grou	up was generated by AWS M	Copy to new				
	Warning Rules with source of 0.0.0.0/0 allo only.	w all IP addresses to access your ins	tance. We recomme	nd setting security group rule	es to allow access from known I	P addresses				

Step 5.7 – Review Instance Settings and Launch Instance

🚺 Servic	es v	Edit 🗸					Justin L Wi	reman 👻 Ore	egon 🕶	Help 🕶
1. Choose AMI	2. Choose	Instance Type	3. Configure I	nstance 4. Add Store	age 5. Tag Instance 6	6. Configure Security Group	7. Review			
Step 7: Re	view I	nstance launch details	Launch s. You can go	back to edit changes	for each section. Click La	aunch to assign a key pair	r to your instance and	d complete the	e launch	process.
Your instance configuration is not eligible for the free usage tier To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about free usage tier eligibility and usage restrictions.										
Your inst Your can groups	e your in tance may also open	stance's sec be accessible additional por	from any IP a ts in your secu	security group, Per address. We recomme urity group to facilitate	rmitAll, is open to the end that you update your a e access to the application	world. security group rules to alk n or service you're runnin	ow access from knov g, e.g., HTTP (80) for	vn IP addresse web servers.	es only. Edit sec	surity
AMI Detail	s									Edit AMI
Free tier eligible Ro	licrosoft Will	Windows Ser ndows 2012 R2 pe: ebs Virtualia	ver 2012 R2 Standard editio	Base - ami-57e29cl on with 64-bit architectu	67 Ire. [English]			F	dit insta	ancetype
Instance T	ype	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized	d Available	Network Pe	rformar	nce
t2.micro		Variable	1	1	EBS only	-		Low to Mode	erate	
- Security G	iroups							Edit	t securi	ty groups
Security	Nam	e Descri	ption							
sg-4d69ed2	28 Perm	nitAll This se	curity group w	as generated by AWS	6 Marketplace and is base	ed on recommended settin	ngs for FortiGate-VM	version v5.0.5	provide	d by Fortin
All selected	eacurity /	aroune inhour	nd rulae				c	Cancel Pre	vious	Launch

Step 5.8 – Create key pair

If you already have a key pair you can use an existing one. If not choose to create a new key pair and download it. You will need this file to login to the VM.

Important - If you lose the key pair, you cannot connect to your Amazon EC2 instances.

For more information on Key Pairs see the Appendix

🎁 Services 🗸 Edit 🗸	Justin	i L Wireman 👻 Oregon 👻 Help 🗸
1. Choose AMI 2. Choose Instance Step 7: Review Instan	Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review	
 AMI Details 		Edit AMI
Microsoft Window Free tier Microsoft Windows 20 Root Device Type: ebs	vs Server 2012 R2 Base - ami-57e29c67 112 R2 Standard edition with 64-bit architecture. [English] Virtualization type: hvm	
 Instance Type 	Select an existing key pair or create a new key pair \times	Edit instance type
Instance Type ECUs t2.micro Variat	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.	Network Performance Low to Moderate
Security Groups	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. Create a new key pair	Edit security groups
sg-4d69ed28 PermitAll	Key pair name	/M version v5.0.5 provided by Fortine
All selected security groups	Download Key Pair	
Security Group ID sg-4d69ed28	You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.	Source (i) 0.0.0.0/0
Instance Details Storage	Cancel Launch Instances	Edit instance details Edit storage
▶ Tags		Cancel Previous Launch

Figure 29 - Key Pair

Step 6.0 – FortiGate Configuration

While the Windows VM is being provisioned you can finish the FortiGate configuration.

Step 6.1 - Update FortiGate Password

Update the FortiGate password as there are many bots that attempt to log in to newly provisioned devices on AWS subnets.



Step 6.2 – Confirm network settings

Set the port2 interface IP address settings (private subnet)

← → C ↑ kettps://ec2-54-200-77-52.us-west-2.compute.amazonaws.com/index									C Cther Bookmarks	
FortiGate VM64-	AWS					(2) Help	Wizard	Logout	F	
System Subsection Status - * Top Sources	FortiGate VMe	ET. 1 3 5 7 2 4 6								
Top Destinations	Creater	V Name	⊤Туре	▼IP/Netmask	Ţ	Access		▼ Administrat	tive Status	▼ Link Status
Traffic History	port1	(outside)	Physical	10.0.0.5 255.255.255.0	PING, HTTPS	, SSH, FMG	-Access	0		O 1000Mbps/Full Dup
Threat History	port2	(inside)	Physical	10.0.1.5 255.255.255.0	PING,	HTTPS, SS	н	0		O 1000Mbps/Full Dup
Retwork	port3		Physical	0.0.0.0 0.0.0.0				0		0
Interfaces	port4		Physical	0.0.0.0 0.0.0.0				0		0
	port5		Physical	0.0.0.0 0.0.0.0				0		0
	port6		Physical	0.0.0.0 0.0.0.0				0		0
	port7		Physical	0.0.0.0 0.0.0.0				0		0
	mesh.roo	ot (& SSID: fortinet.mesh.root)	WiFi	0.0.0.0 0.0.0.0				0		
Monitor										

Step 6.3 – Setup basic policies

For this example we are going to create the following policies. (Samples below)

- NAT & allow outbound access
 - (Optional) You can apply any additional policies if you want to demonstrate features such as Web-filtering, DLP, etc.

- Port forwarding port 3389 to the Windows server
- Any required logging for troubleshooting

```
config firewall policy
```

```
edit 1
set srcintf "port2"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set logtraffic all
set av-profile "default"
set ips-sensor "default"
set profile-protocol-options "default"
set nat enable
next
```

```
edit 2
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "Windows-RDP"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set logtraffic all
        set av-profile "AV-flow"
        set ips-sensor "default"
        set profile-protocol-options "default"
   next
end
config firewall vip
   edit "Windows-RDP"
       set extintf "port1"
        set portforward enable
        set mappedip 10.0.1.25
        set extport 3389
        set mappedport 3389
   next
end
```

Step 7 – Testing

Step 7.1 – Launch a RDP session to test

Remote Desktop Connection	
Remote Desktop Connection	
Computer: 3-40-99 us-west-2 compute amazonaws com	
User name: None specified You will be asked for credentials when you connect.	
Options Connect Help	
	1

Step 7.2 - Retrieve your VM's password

On the EC2 Dashboard, Right click your test VM instance and select Get Windows Password

🎁 Services 🗸 Edit	*	
EC2 Dashboard Events	Launch Instance Connect Actions *	
Tags	Filter: All instances Y All instance types Y Q Search Instances	×
Reports Limits	Name ♥ ▼ Instance ID ▲ Instance Type ▼ Availability Zone	Instance State Status Checks ·
INSTANCES	i-580d4d53 m1.small us-west-2a	running Ø 2/2 checks
Instances	Fortigate-VM i-e90f4fe2 m3.medium us-west-2a	running Ø 2/2 checks
Spot Requests	Windows2 Instance Management pro us-west-2a	running Ø 2/2 checks
Reserved Instances	Launch More Like This	
IMAGES	Add/Edit Tags	
AMIs	Change Instance Type	
Bundle Tasks	Create Image	
	Bundle Instance (instance store AMI)	
ELASTIC BLOCK STORE	Change Termination Protection	
Volumes	View/Change User Data	
Snapshots	Change Shutdown Behavior	
NETWORK & SECURITY	Get Windows Password	
Security Groups	Get System Log	
Elastic IPs	Networking	
Placement Groups	Change Security Groups	
Load Balancers Figure 32	Attach Network Interface	

• You will be asked for the key pair you created to decypt the administrotr password.

Retrieve Default Windows Administrator Password X
To access this instance remotely (e.g. Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.
To decrypt your password, you will need your key pair for this instance. Browse to your key pair, or copy and paste the contents of your private key file into the text area below, then click Decrypt Password.
The following Key Pair was associated with this instance when it was created.
Key Name justinkey01
In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:
Key Pair Path Choose File No file chosen
Or you can copy and paste the contents of the Key Pair below:
Paste contents of private key file here
Cancel Decrypt Password

Figure 33

Retrieve Default Windows Administrator Password

×

Password Decryption Successful

The password for instance i-fa1959f1 (Windows2012-Test01) was successfully decrypted.

Password change recommended

We recommend that you change your default password. Note: If a default password is changed, it cannot be retrieved through this tool. It's important that you change your password to one that you will remember.

You can connect remotely using this information:

Private IP10.0.1.25User nameAdministratorPasswordk(nac;=K@w&



Step 7.3 - Test Outbound access

For testing purposes I have attempted to download a file from eicar.org to show that the FortiGate is inline for outbound traffic. See Figures 34-35.



Appendix

Regions and Availability Zones

Region and Availability Zone Concepts

Each region is completely independent. Each Availability Zone is isolated, but the Availability Zones in a region are connected through low-latency links. The following diagram illustrates the relationship between regions and Availability Zones.



You can list the Availability Zones that are available to your account. For more information, see Describing Your Regions and Availability Zones. When you launch an instance, you can select an Availability Zone or let us choose one for you. If you distribute your instances across multiple Availability Zones and one instance fails, you can design your application so that an instance in another Availability Zone can handle requests.

Amazon EC2 resources are either global, tied to a region, or tied to an Availability Zone. For more information, see AWS documentation for the complete article.

Amazon EC2 Key Pairs

Amazon EC2 uses public–key cryptography to encrypt and decrypt login information. Public–key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data. The public and private keys are known as a *key pair*.

To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. Linux/Unix instances have no password, and you use a key pair to log in using SSH. With Windows instances, you use a key pair to obtain the administrator password and then log in using RDP.

Creating a Key Pair

You can use Amazon EC2 to create your key pair. For more information, see <u>Creating Your Key Pair Using</u> <u>Amazon EC2</u>. Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see <u>Importing Your Own Key Pair to Amazon EC2</u>.

Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt your login information, so it's important that you store your private keys in a secure place.

The keys that Amazon EC2 uses are 1024-bit SSH-2 RSA keys. You can have up to five thousand key pairs per region.

Launching and Connecting to Your Instance

When you launch an instance, you should specify the name of the key pair you plan to use to connect to the instance. If you don't specify the name of an existing key pair when you launch an instance, you won't be able to connect to the instance. When you connect to the instance, you must specify the private key that corresponds to the key pair you specified when you launched the instance. Amazon EC2 doesn't keep a copy of your private key; therefore, if you lose your private key, there is no way to recover it. If you lose the private key for an instance store-backed instance, you can't access the instance; you should terminate the instance and launch another instance using a new key pair. If you lose the private key for an EBS-backed instance, you can regain access to your instance. For more information, see <u>Connecting to Your Instance if You Lose Your Private Key</u>.

Detailed VPC Diagram



Figure 36

Additional info and links

http://aws.amazon.com/documentation/vpc/

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC Introduction.html