

AWS BEST PRACTICES

High Availability Setup and Automating Route Table Change for an Active-Passive FortiGate Next Generation Firewall Deployment Q3 2017

PROBLEM STATEMENT

AWS best practice is to architect redundant Availability Zones (AZ) in each VPC for failover redundancy and maximum uptime in the event of an instance failure. However, there are manual steps required to maintain security redundancy. Fortinet has an automated solution to address this and create a truly automated failover and reversion.

SOLUTION

- In an Active-Passive FortiGate HA environment in AWS, if the Active firewall has an issue and cannot process the traffic, a manual change is necessary for the route table to go through the Secondary Firewall. This is not ideal and might increase the outage time.
- To work around this, a python script can be used to automate the process. The python script monitors the primary firewall, and if the primary firewall goes down, it makes the appropriate API calls to automate the route table changes needed to move to the secondary firewall.
- When the primary firewall is restored, the python script will make the API calls to AWS to change the route table back to the primary firewall.
- HA example:

FORTIGATE HA SETUP: VPC_CFT STEPS

Step 1. Download the CloudFormation template. <u>https://s3.amazonaws.com/fortigatetemplates/FortiGate-</u> HAtemplate5.4.5_ondemand.template

Step 2. Log in to AWS Management Console using your AWS login credentials. https://aws.amazon.com

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





Step 4. Click on Create Stack.

Create Stack Actions -	Design template		C	0
ilter: Active - By Name:		Shi	owing 0	stac
	Design a template Templates tell AWS CloudFormation which AWS resources to provision and how to provision them. When you create a CloudFormation stack, you must submit a template. To build and view templates, you can use the drag-and-drop tool called AWS CloudFormation Designer. You drag-and-drop the resources that you want to add to your template and drag lines between resources to create connections. To use Designer to create a template or to open and modify a template, choose Design template. Design template			
	Create a Stack AWS CloudFormation allows you to quickly and easily deploy your infrastructure resources and applications on AWS. You can use one of the templates we provide to get started quickly with applications like WordPress or Drupal, one of the many sample			

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.

Select Template	Select Template									
Specify Details Options Review	Select the template that descrit	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 Ino file selected Specify an Amazon S3 template URL								
		Cancel	Next							
Create stack Select Template Specify Details	Select Template	Cancel	Next							
Create stack Select Template Specify Details Options Review	Select Template Select the template that descrit	Cancel	Next							
Create stack Select Template Specify Details Options Review	Select Template Select the template that descrit Design a template	Cancel bes the stack that you want to create. A stack is a group of related resources that you manage as a single unit. Use AWS CloudFormation Designer to create or modify an existing template. Learn more. Design template	Next							
Create stack Select Template Specify Details Options Review	Select Template Select the template that descrit Design a template Choose a template	Cancel bes the stack that you want to create. A stack is a group of related resources that you manage as a single unit. Use AWS CloudFormation Designer to create or modify an existing template. Learn more. Design 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 https://s3-external-1.amazonaws.com/cf-templates-tkt28gk View/Edit template in Designer	Next							



Step 6. Create a stack name to identify the CloudFormation stack.

Step 7. Choose the appropriate values for the parameters listed in the parameter section. There are some default values, but these can be changed according to deployment needs. A short description for each parameter is provided to summarize what the parameter is used for and what value 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.

Parameters		
VPC Configuration		
Please enter the VPC specific details here	10.0.016	Enter the VPC COR that you want to use
FortiGate Instance Config	guration	
FortiGateInstanceType	må large	 Enter the Instance type and size that you want for the Fort/Gates
CIDRForFortiGateAcces 8	0.0.0.0	Errar the CDR from which FortiGate instances needs to be accessed
Primary FortiGate Instanc	te Interface Configuration	
Public1Subnet	10.0.024	Enter the value of the Public1 submet
Private 15ubnet	10.0.1.0/24	Enter the value of the Privatel subset
Public1IP		Enter the IP address for the external interface of the FortGate (IP from Public1Subnet)
PrivaterlinternaliP		Enter the IP address for the internal interface of the FontGate (IP from Private ISubnet)
Backup FortiGate Instanc	te Interface Configuration	
Backup FortiGate Instanc Public2Subnet	10.0.2.0.24	Enter the value of the Public2 subnet
Backup FortiGate Instanc Public2Subnet Private2Subnet	10.02.024	Enter the value of the Public2 subvet. Enter the value of the Public1 subvet.
Backup FortiGate Instano Public2Subnet Private2Subnet Public2P	9 Interface Configuration	Enter the value of the Public2 subnet. Enter the value of the Public1 subnet. Enter the VP address for the external interface of the ForQuate1(P from Public1Subnet)
Backup Forti Gate Instanc Public2Subnet Private2Subnet Public2P Private2InternalIP	e Interface Configuration 10.0.2.0.04 10.0.3.0.04	Enter the value of the Public2 submet. Enter the value of the Public1 submet. Enter the IP address for the external interface of the FontGase1(IP from Public1Submet) Enter the IP address for the internal interface of the FontGase1(IP from Public1Submet)
Baokup FortiGate Instanc Public2Subnet Private2Subnet Public2P Private2InternaliP Worker Node Instance C	Iterace Configuration Ite22024 Ite23024 Ite23024 Itease Interface Configuration	Enter the value of the Public2 submet. Enter the value of the Public2 submet. Enter the Value of the Public3 submet. Enter the IP address for the external interface of the FortQuate(IP from Public3Submet) Enter the IP address for the internal interface of the FortQuate(IP from Public3Submet)
Backup FortiGate Instance Public2Subnet Private2Subnet Public2P Private2InternalP Worker Node Instance C CIDRFort/Shocese	Interface Configuration 10.02.004 10.02.004 10.03.004 10.03.004 10.03.004 10.03.004 10.03.004	Enter the value of the Public2 submet: Enter the value of the Public2 submet: Enter the Value of the Public3 submet: Enter the IP address for the external interface of the FortGate(IP from Public15Jubme) Enter the IP address for the internal interface of the FortGate(IP from Public15Jubme) Enter the CDR from which AS instance needs to be accessed
Backup FortiGate Instance Public2Subnet Private2Subnet Public2P Private2InternaliP Worker Node Instance C CIDRFortSAccess RouteS3 Configuration	IL02004 IL0200	Enter the value of the Public2 subnet: Enter the value of the Public2 subnet: Enter the V address for the external interface of the FortGate(IP from Public15Jubnet) Enter the IP address for the internal interface of the FortGate2(IP from Public15Jubnet) Enter the COR from which AS instance meeds to be accessed
Backup FortGate Instance Public2Subnet Public2Dubnet Public2IP Private2DiternalIP Worker Node Instance D CIDIFFortGAccess RouteG3 Configuration DomainName	Interface Configuration Iso22024 Iso23024 Iso33024	Enter the value of the Public2 submet. Enter the value of the Public2 submet. Enter the Value of the Public2 submet. Enter the Values for the external interface of the FortGate1(P from Public1Submet) Enter the Values for the internal interface of the FortGate2(P from Public1Submet) Enter the Values for the internal interface of the FortGate2(P from Public1Submet) Enter the COR from which AS Instance medis to be accessed Enter the COR from which AS Instance medis to be accessed Enter the Comain Name In which the DNS Record Sets would be created
Backup FortiGate Instance Public2Subnet Private2Subnet Public2P Private2InternaliP Worker Node Instance C CIDRFork5Access Route53 Configuration DomainName DNSPhefix	Ital2004	Etter the value of the Public2 submet. Enter the value of the Public2 submet. Enter the Value of the Public3 submet. Etter the P address for the enternal interface of the FortQuate(IP from Public3Submet) Etter the P address for the internal interface of the FortQuate(IP from Public3Submet) Etter the P address for the internal interface of the FortQuate(IP from Public3Submet) Etter the CORP from which AS Instance meds to be accessed Etter the CORP from which AS Instance meds to be accessed Etter the Domain Name in which the DNS Record Sets would be created Etter the Paths for the DNS Record Set that would be created for the two instances
Backup FortiCate Instance Public2Subnet Private2Subnet Public2P Private2DiternaliP Worker Node Instance C CDDRFortSAccess Route53 Configuration DomainName DNSPrefix Other parameters	Ital2004	Enter the value of the Public2 submet Enter the value of the Public2 submet Enter the Value of the Public2 submet Enter the IP address for the external interface of the FonGuate(IP from Public1Submet) Enter the IP address for the external interface of the FonGuate(IP from Public1Submet) Enter the IP address for the internal interface of the FonGuate(IP from Public1Submet) Enter the ID address for the internal interface of the FonGuate(IP from Public1Submet) Enter the ID address for the internal interface of the FonGuate(IP from Public1Submet) Enter the ID address for the internal interface of the FonGuate(IP from Public1Submet) Enter the ID address for the internal interface of the FonGuate(IP from Public1Submet) Enter the ID address for the internal interface of the FonGuate(IP from Public1Submet) Enter the ID address for the internal interface of the FonGuate(IP from Public1Submet) Enter the ID address for the internal interface of the FonGuate(IP from Public1Submet) Enter the ID address for the internal interface of the internal internal interface of the internal internal interface of the internal int
Backup FortiGate Instance Public2Subnet Public2Dubnet Public2P Private2DitermaliP Worker Node Instance C CIDRFortSAccess RouteS3 Configuration DomainName DISPrefix Other parameters AZForFirewall	ILIU2004 IL	Enter the value of the Public2 submet: Enter the value of the Public2 submet: Enter the IP address for the external interface of the FonGland(IP from Public1Subme) Enter the IP address for the external interface of the FonGland(IP from Public1Subme) Enter the IP address for the internal interface of the FonGland(IP from Public1Subme) Enter the ID address for the external interface of the FonGland(IP from Public1Subme) Enter the ID address for the external interface of the FonGland(IP from Public1Subme) Enter the ID address for the external interface of the FonGland(IP from Public1Subme) Enter the ID address for the external interface of the FonGland(IP from Public1Subme) Enter the ID address for the external interface of the FonGland(IP from Public1Subme) Enter the ID address for the internal interface of the FonGland(IP from Public1Subme) Enter the ID address for the internal interface of the FonGland(IP from Public1Subme) Enter the ID address for the internal interface of the FonGland(IP from Public1Subme) Enter the ID address for the internal interface of the FonGland(IP from Public1Subme) Enter the ID address for the internal interface of the internal interface of the ID address for the internal internal interface of the ID address for the internal internal interface of the ID address for the internal i
Backup FortGate Instance Public2Subnet Public2Dubnet Public2P Private2DatemailP Worker Node Instance Cl CIDIPFortSAccess RouteG3 Configuration DomainName DINSPrefix Other parameters AZForFrewall	I I I I I I I I I I I I I I I I I I I	
Backup FortiGate Instance Public2Subnet Private2Subnet Public2P Private2InternaliP Worker Node Instance C CIDRFortSAccess RouteS3 Configuration DomainName DINSPrefix Other parameters AZForFrewalt2	Interface Configuration Itil02.004 Iti	Bree the value of the Rabic2 sabre: Bree the Values for the internal interface of the FonDast(IP from Rabic1Sabre) Bree the Values for the internal interface of the FonDast(IP from RisexISabre) Bree the CDR from which AS Instance meets to be accessed Bree the CDR from which AS Instance meets to be accessed Bree the Rabic for the DINS Record Sets would be created Bree the Rabic for the DINS Record Set the would be created for the two instances

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 pain) for resources in your stack. You can add up to 10 unique key-value pains for each stack. Learn more.								
	Key (127 characters maximum) T Advanced You can set additional options for your stack, like notification options and a stack policy. Li	Value (255 characters maximum)							
			Cancel Previous Next						



Step 9. Click Create.

Create stack										
Select Template	Review									
Specify Details	Templete									
Course -	TE T I I I I I I I I I I I I I I I I I I									
Heview	Template URL Description Estimate cost	https://s3-external-1.amazonaws.com/cf-templates-ixt28gkesmp-us-east-1/2016175x5h-FortiGate-template5.4.1.template AWS CloudFormation Template to launch VPC with a FortiGate protecting the resources in the private subnet. Cost								
	Details									
	Stack name	FortDemo								
	VPC and Subnets Informatio	n								
	VPCCIDR	10.0.016								
	PublicSubnet	10.0.024								
	PrivateSubnet	10.1.024								
	FortiGate Instance Configura	alion								
	FortiGateInstanceType	egaLEm								
	CIDRForFortiGateAcces	00.0.0								
	5									
	A2ForFirewall KeyPoir	UP-0057-10 24. Vervin								
	rispr as	re_repres								
	IP Configuration for the Fort	Gate Interfaces								
	PublicIP	10.0.254								
	Private Internal P	10.0.1254								
	Create two resources	no								
	Options									
	Tags									
	No tags provided									
	Advanced									
	Notification									
	Timeout	none								
	Rollback on failure	Yes								
		Caroat Previous Constr								

Step 10. Wait for the CloudFormation service to finish creating all the resources. The "**events**" tab should list the information the template is creating. The "**resources**" tab should list the resources as they are created.

Create Stack Actions -	Design template			C
Filter: Active - By Name:				Showing 1 sta
Stack Name	Created Time	Status	Description	
r, FortiDemo	2016-06-23 08:51:18 UTC-0700	CREATE_IN_PROGRESS	AWS CloudFormation Template to I	unch VPC with a FortiGate protecting the resources in the private subnet
Overview Outputs Res	ources Events Template	Parameters Tags	Stack Policy Change Sets	80
016-06-23 Status	Type		Logical ID	Status reason
	- ALL 20200000 ALL 2	Se Cometer Charle	FactDama	

Step 11. Once the stack is created, the Output section has the login information for the Firewall and the Worker Node.

								(
Create Stack Actions -	Design template							C O
Filter: Active - By Name:	· · · · · · · · · · · · · · · · · · ·							Showing 1 stack
Stack Name	Created Time Status	is Descript	ion					
r, FortiDemo	2016-06-23 08:51:18 UTC-0700 CREA	TE_IN_PROGRESS AWS CIO	udFormation Template to launch	VPC with a FortiGate protecting the n	sources in the private	subnet		
Overview Outputs Rer	sources Events Template Pa	arameters Tags Stack Pr	licy Change Sets					880
016-06-23 Status	Time		vical ID Sta	tus masson				
+ 08:51:24 UTC-0700 CREAT	TE_N_PROGRESS AWS:EC2.VP	PC V	PC Re	source creation Initiated				
08:51:24 UTC-0700 CREAT	TE_N_PROGRESS AWS:EC2.int	ternetGateway Is	ternetGateway Re	source creation Initiated				
08:51:23 UTC-0700 CREAT	TE_N_PROGRESS AWS:EC2.:VP	PC v ternetGateway lit	PC ternetGateway					
+ 08:51:18 UTC-0700 CREAT	TE_N_PROGRESS AWS: CloudFo	ormation: Stack F	ortiDemo Us	er Initiated				
Crete Stack Actions -	Design template							C O
								Chaulan Lateri
Filter: Active - By Name								anowing I stack
Stack Name	Created Time Statu	us Descrip	bon					
Overview Outputs Re	esources Events Template Pa	arameters Tags Stack P	olicy Change Sets					880
Logical ID	Physical ID			Туре		Status	Status Reason	
InternetGateway	igw-884b1bec			AWS: EC2: InternetGateway		CREATE_COMPLETE		
VPC	vpc-c00dbaa7			AWS::EC2::VPC		CREATE_COMPLETE		
Filter: Active - By Name	æ							Showing 1 stack
Stack Name	Created Time	Status	Description					
9 Fortinet1	2016-07-22 14:21:48 UTC-0700	CREATE_COMPLETE	AWS CloudFormation Ter	nplate to launch VPC with Two Subn	ets and Two instance	in a VPC.		

Overview	Outputs	Hesources	Events	rempiate	Parameters	raga	stack Policy Change sets		880
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	
Usemame							admin	Username to Access Fortigate	
Password							i-2d301798	Password to login Fortigate is the primary instance id	

Step 12. Log in to the Firewall through ssh/https; configure the Firewall with your required security features.

				52.2.95.	42 Č				Ô	Ø
FortiGate VM64-AWS	OND	EMAND FGTAWS00FAD	D9F66			0	31	?	53	admin -
ℜ Dashboard ▲ FortiView	☆ >	System Information							0	x -
 Network System Policy & Objects Security Profiles VPN User & Device WiFi & Switch Controller IL log & Report Monitor 	> > > > > > > >	HA Status: Host Name: Serial Number: Operation Mode: Inspection Mode: System Time: Firmware Version: System Configuration: Current Administrator: Uptime: Virtual Domain:	S F F T T T V V C C C	GTAWS GTAWS GTAWS NAT Proxy-ba Proxy-ba NAT (5.4.1,ba Backup) admin [C D day(s) (Disabled	ine [Configure] 500FADD9F66 [Change] 500FADD9F66 ased [Change] 23 09:04:12 2016 (FortiGuard) [Change] aild1064 (GA) [Update] [Restore] [Revisions] Change Password] /2 in Total [Details] 0 hour(s) 11 min(s) [[Enable]					
		License Information	Registration		O Not Registered				R	egister
۹			IPS & Application Con AntiVirus	trol	C Licensed (Expires 2021-01-01)	+ Add	Widget	CR	eset Da	shboard

Step 13. Log in 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 an Amazon Linux AMI that has the scripts required to monitor the FortiGates.

```
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EC2_GetStarted.html#ec2-connect-to-instance-linux
Example screenshot of the command to log in and how it looks after login.
```

```
🕨 📄 Keypairs — ec2-user@ip-10-0-0-168:~ — ssh -i Nortcalkeypair.pem.txt ec2-user@52.52.49.144 — 109×24
[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

Step 15. Execute the python script fortigateha.py with the runtime variable stack name. python fortigateha.py

Once this is done, FortiGate HA setup is complete.



```
🖲 😑 📒 Keypairs — ec2-user@ip-10-0-0-168:~/fortigateha — ssh -i Nortcalkeypair.pem.txt ec2-user@52.52.49.144 — 109...
                                                                                                               18
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 ~]$ cd fortigateha/
[ec2-user@ip-10-0-0-168 fortigateha]$
```

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:

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

```
Ē
[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
```

Congratulations: You have created an active:passive automated HA architecture in your AWS VPC.



GLOBAL HEADQUARTERS Fortinet Inc. 899 Kifer Road Sunnyvale, CA 94086 United States Tel: +1.408.235.7700 www.fortinet.com/sales EMEA SALES OFFICE 905 rue Albert Einstein 06560 Valbonne France Tel: +33.4.8987.0500 APAC SALES OFFICE 300 Beach Road 20-01 The Concourse Singapore 199555 Tel: +65,6513,3730 LATIN AMERICA HEADQUARTERS Sawgrass Lakes Center 13450 W. Sunrise Blvd., Suite 430 Sunrise, FL 33323 Tel: +1,954,368,9990

Copyright © 2017 Fortinet, Inc. All rights reserved. FortiGate®, FortiGate®, FortiGate®, 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 metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other 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 performance in the same ideal conditions and a fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet disclaims in full any covenants, nepresentations, and guarantees pursuant hereto, whether express or implied. Fortinet respress the ight to change, modify, transfer, or otherwise revise this publication shall be applicable.