# Table of Contents

- Setup Virtual Private Cloud (VPC) ................................................................. 3
- Subscribe to the Fortinet VM in marketplace .............................................. 6
- Start configuration of Fortinet Firewall ....................................................... 12
- Add ECS worker VMs for testing ................................................................. 14
- Verify the security capabilities of the Fortinet ......................................... 17
  - Demonstrate the Anti-Virus feature ......................................................... 17
  - Demonstrate the Application Control access feature ............................... 19
  - Enable NAT inbound protection in Fortinet ........................................... 21
- Conclusions ............................................................................................... 25
Setup Virtual Private Cloud (VPC)

1. Assume this is the new environment, now let's create the VPC first

   - The VPC named TP_FortiVPC

2. The VPC is created, click Next Step
4. We will need at least two VSwitches, one for the ECS and one for the FortiGate VM, let’s create the ECS VSwitch first.

5. Click Create More
6. And this is the VSwitch for keeping the FortiGate VM

7. Click Done to finish the VPC and VSwitches setup

8. The VPC is now ready, next section we will subscribe the FortiGate VM
Subscribe to the Fortinet VM in marketplace


10. If customer has their own FortiGate license they can choose the BYOL image, otherwise they can use On-Demand image offered
11. Click “Choose Your Plan” to continue.

12. In this case I’ll use PAYG, select Hong Kong and Zone B (where the VPC and VSwitches located), and then click the link “ECS Advance Purchase page” because I want to customize the Data disk and VPC information.
13. Add a data disk for the Log (Suggest to use SSD for better performance)

14. Choose the TP_FortiVPC and Forti_VSwitchFW in Network section, also assign the Public IP to the image

15. Continue and create the instance
16. Click Console and back to the ECS instance list

![Image of Activated message]

17. You will see the VM created, mark down the Public IP and the instance ID (this will be FortiGate default password) and you will use later

![Image of instance details]

18. First, we need to configure the default security group to allow 80 and 443 inbound

![Image of security group configuration]
19. Then we will be able to reach the Fortinet Web admin console by user admin/\textless instanceid\textgreater .

Also we need to add the route entry to Fortinet, this make sure all out-going traffic from ECS will go through Fortinet.
21. Click Add Route Entry

22. Add 0.0.0.0/0 and point to the FortiGate VM

23. This should be the result, this make sure ECS outbound traffic will goto Fortinet
24. You can change password here after logging in.

25. After logging in again by new password, you can change the time zone and language as well in System -> Settings.
26. Now we need to add the IPv4 Policy for the outbound traffic.

27. Specific the following “ToInternet” policy, let’s enabled the AntiVirus and Application Control here for Demo, also enabled All Sessions log too, then click “OK”.
Add ECS worker VMs for testing

28. Just create ECS as usual

29. Remember, **cannot use the same VSwitch of the Fortinet**, in this case I selected the ECS Vswitch. And don’t need to assign public IP because ECS with Public IP will not route through Fortinet.

30. Confirm and create the instance
31. Then reset the VNC password, login password and restart the instance.

32. Then connect to the VNC, login to the Windows.

33. You should find it is able to connect internet through the Fortinet.
34. You should also find the detail log information in the Fortinet as well!
Verify the security capabilities of the Fortinet

Demonstrate the Anti-Virus feature

35. In the ECS, visit the website http://metal.fortiguard.com/tests/

36. Click the run tests, if there is no Firewall Antivirus protection the test will fail.

37. As the ECS is protected by Fortinet, you will see it is blocked.

To have the best Anti-Virus scanning capabilities, make sure the anti-virus definition is up-to-update in Fortinet.
38. And we also can see the Threats in Fortinet console.
Demonstrate the Application Control access feature

39. Go to Security Profiles -> Application Control, let's select to block the Video/Audio and Social Media. And click Apply.

40. Then try to access facebook and youtube in the ECS, you will see they are not able to connect.
41. In the Fortinet console, we will see which clients trying to connect to facebook as well.
Enable NAT inbound protection in Fortinet

In this sample, I’ll try to enable the Fortinet to protect inbound RDP traffic, the same concept can be applied to HTTP/HTTPS and other services too, this is very useful because most customers want Fortinet to monitor both inbound and outbound traffic.

42. Setup the NAT and point to the RDP address of the ECS, Click Virtual IPs under Policy&Objects

43. We map the 3389 port of the Fortinet to the ECS 192.168.1.36
44. Can see the Virtual IP there now

45. Now we will configure the inbound policy for the RDP redirection

46. Name the rule and then choose the Virtual IP we created as the destination

47. Similarly, enable the security profiles you want, and then use All Sessions as Log allowed traffic for demo purpose.
48. The inbound rule is created successfully
49. And now you should be able to use the Fortinet Public IP address to RDP the ECS.

50. Logs and sessions information can also be viewed in Fortinet.
Conclusions

Fortinet is a powerful software that widely used by many international customers, financial and securities industries as well. By leveraging this VM, we should be able to strengthen the confidence of customer for using Cloud.