

Fortinet Certified Professional Public Cloud Security



Online Course



ZETLAN TECHNOLOGIES
www.zetlantech.com

Fortinet Certified Professional Public Cloud Security

Course Modules

NSE 6 – Cloud Security 7.0 for AWS

1. Fundamentals of securing AWS

- Explain AWS basic concepts and components
- Describe traffic flow in AWS

2. Fortinet solution for AWS

- Explain Fortinet solutions for AWS

3. Deploy Fortinet products in AWS

- Configure HA using Fortinet CloudFormation templates
- Configure the load balancer and autoscaling
- Configure and secure AWS cloud
- Configure FortiGate AWS SDN integration

NSE 6 – Cloud Security 7.0 for Azure

4. Fundamentals of securing Microsoft Azure

- Describe Azure basic concepts and components
- Explain networking in Azure



Fortinet Certified Professional Public Cloud Security

5. Fortinet solutions for Microsoft Azure

- Explain Fortinet solutions for Azure

6. Deploying Fortinet products in Azure

- Configure HA using Fortinet in Azure
- Configure load balancer and autoscaling
- Configure and secure Azure cloud
- Configure FortiGate Azure SDN integration

AWS Cloud Security 7.4 Administrator

7. Public cloud fundamentals

- Explain AWS public cloud concepts
- Identify Fortinet solutions to secure the cloud

8. AWS components

- Identify AWS networking components
- Apply AWS security components
- Describe traffic flow in AWS

9. Fortinet product deployment

- Integrate Fortinet solutions in AWS
- Deploy WAF in AWS



Fortinet Certified Professional Public Cloud Security

10. High availability

- Deploy HA in AWS
- Configure HA using Fortinet CloudFormation templates

11. Load balancers and Forti CNF

- Compare load balancer types in AWS
- Deploy FortiGate CNF

Azure Cloud Security 7.4 Administrator

12. Azure public cloud concepts

- Describe public cloud basic concepts and components
- Describe Azure basic concepts and components

13. Azure components

- Explain Azure components and networking elements
- Explain Azure security services

14. Fortinet product deployment

- Describe the Fortinet solutions in Azure
- Deploy a single FortiWeb instance
- Deploy a single FortiGate instance
- Configure FortiGate Azure SDN integration



Fortinet Certified Professional Public Cloud Security

15. High availability (HA)

- Configure HA using FortiGate in Azure
- Configure load balancing and autoscaling
- Explain Azure route server concepts
- Explain Azure route server use cases

16. VPN solutions in Azure

- Explain the site-to-site connection options in Azure
- Deploy connections between FortiGate and Azure VPN gateway
- Explain Azure virtual WAN concepts
- Deploy Azure virtual WAN

NSE 4 – FortiOS 7.2

17. Deployment and System Configuration

- Perform initial configuration
- Implement the Fortinet Security Fabric
- Configure log settings and diagnose problems using the logs
- Config VDOMs to split a FortiGate into multiple virtual devices
- Configure different operation modes for an FGCP HA cluster
- Diagnose resource and connectivity problems



Fortinet Certified Professional Public Cloud Security

18. Firewall and authentication

- Configure firewall policies
- Configure firewall policy NAT and central NAT
- Configure different methods of firewall authentication
- Explain how to deploy and configure FSSO

19. Content inspection

- Inspect encrypted traffic using certificates
- Identify FortiGate inspection modes and configure web filtering
- Config app control to monitor and control network applications
- Config antivirus scanning modes to neutralize malware threats
- Config IPS to protect network from threats and vulnerabilities

20. Routing

- Config and route packets using static and policy-based routes

21. VPN

- Configure and implement different SSL VPN modes
- Implement a meshed or partially redundant IPsec VPN
- Configure ZTNA to provide role-based application access



Fortinet Certified Professional Public Cloud Security

FortiGate 7.4 Administrator

22. Deployment and system configuration

- Perform initial configuration
- Implement the Fortinet Security Fabric
- Configure an FGCP HA cluster
- Diagnose resource and connectivity problems

23. Firewall policies and authentication

- Configure firewall policies
- Configure SNAT and DNAT options in firewall policies
- Configure different methods of firewall authentication
- Explain how to deploy and configure FSSO

24. Content inspection

- Explain and inspect encrypted traffic using certificates
- Identify FortiGate inspection modes and configure web filtering
- Config app control to monitor and control network applications
- Config antivirus scanning modes to neutralize malware threats
- Config IPS to protect networks from threats and vulnerabilities



Fortinet Certified Professional Public Cloud Security

25. Routing

- Configure and route packets using static routes
- SD-WAN to load balance traffic betwn multiple WAN links effct

26. VPN

- Config & implemnt different SSL VPNs to provide secure access
- Implement a meshed or partially redundant IPsec VPN

NSE 6 – Forti Mail 7.2

27. Initial deployment and basic configuration

- Describe the fundamentals of SMTP and email flow
- Complete basic setup of FortiMail operatn mode, system settgs
- Deploy FortiMail high-availability clusters
- Monitor and troubleshoot deployment and configuration issues

28. Email flow and authentication

- Enable and enforce authentication on FortiMail
- Configure secure MTA features
- Config and track access control rules, IP, and recipient policies
- Monitor and troubleshoot email flow and authentication issues



Fortinet Certified Professional Public Cloud Security

29. Email security

- Configure session-based email filtering
- Explain and apply spam filtering techniques
- Configure content-based email filtering and archiving
- Monitor and troubleshoot email security issues

30. Encryption

- Explain traditional SMTP encryption methods
- Configure identity-based encryption (IBE)
- Manage IBE users

31. Server mode and transparent mode

- Explain server mode specific features
- Deploy FortiMail in transparent mode

NSE 6 – Forti Web 6.4

32. Deployment and Configuration

- Identify FortiWeb deployment requirements
- Configure system settings
- Configure server pools, policies, and protected hostnames
- Configure FortiWeb HA
- Troubleshoot deployment and system related issues



Fortinet Certified Professional Public Cloud Security

33. Encryption, Authentication, and Compliance

- Mitigate web application vulnerabilities
- Configure various access control and tracking methods
- Mitigate attacks on authentication
- Configure SSL inspection and offloading
- Troubleshoot encryption and authentication related issues

34. Web Application Security

- Configure various threat mitigation features
- Configure machine learning and bot detection
- Configure API protection and bot mitigation
- Troubleshoot threat detection and mitigation related issues

35. Application Delivery

- Configure HTTP content routing, rewriting, and redirection
- Configure caching and compression
- Troubleshoot application delivery related issues



Fortinet Certified Professional Public Cloud Security

FortiWeb 7.4 Administrator

36. Deployment and configuration

- Identify FortiWeb deployment requirements
- Configure system settings
- Configure server pools, policies, and protected host names
- Configure FortiWeb high availability (HA)
- Troubleshoot deployment and system-related issues

37. Encryption, authentication, and compliance

- Mitigate web application vulnerabilities
- Configure various access control and tracking methods
- Mitigate attacks on authentication
- Configure SSL inspection and offloading
- Troubleshoot encryption and authentication-related issues

38. Web application security

- Configure various threat mitigation features
- Configure FortiWeb to block known attacks
- Troubleshoot threat detection and mitigation-related issues
- Configure API protection



Fortinet Certified Professional Public Cloud Security

For Enquiry: +91 8680961847

39. Machine learning (ML)

- Configure machine learning for anomalies
- Configure machine learning for bots
- Configure machine learning for APIs



Free Advice: +91 9600579474

www.zetlantech.com



**LEARN
REMOTELY!!**

The efficiency of online learning
in terms of time management,
flexibility, and the ability
to access resources anytime,
anywhere can be compelling.



ZETLAN TECHNOLOGIES
www.zetlantech.com

**For contact: +91 8680961847
+91 9600579474**

