Fortinet Interview Questions and Answers

1. What do you know about Fortinet's FortiGate?
Ans: FortiGate is a firewall that was released by Fortinet. It enables protection against malware and automated visibility to stop attacks. It includes features like intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. FortiGate has also equipped with Artificial Intelligence (AI), which helps in proactive threat detection.

2. Tell me about Fortinet's history
Ans: Fortinet was founded in the year 2000 by Ken Xie and Michael Xie (siblings). They have released their first product, FortiGate, in the year 2002. Between the years 2000 and 2003, the company has raised $13 million in private funding and $30 million in financing. Over the last decade, the company has acquired many security-related software vendors. Fortinet recently released an AI-powered product, called FortiAI in February 2020.

3. What do you know about Fortinet as an organization?
Ans: Fortinet is an American MNC having over 7000 employees with its headquarters at Sunnyvale, California. Fortinet provides security-driven networking solutions such as firewalls, anti-spam, endpoint security, spyware, anti-virus, etc. Fortinet also announced a technical certification program called Network Security Expert (NSE) to enable more developers on cybersecurity.

4. What is Traditional Firewall?
Ans: A traditional firewall is a device that controls the flow of traffic that enters or exits the network. It either uses a stateless or stateful method to achieve this. It can only track the traffic on 2 to 4 layers.

5. What is the Next-Generation Firewall?
Ans: The Next-Generation Firewall (NGFW) acts as a deep-packet inspection firewall. It includes all the functionalities of a traditional firewall. Additionally, it provides application awareness, Integrated Intrusion Protection System (IPS), Secure Sockets Layer (SSL) inspection, and Shell (SSH) control.

6. Explain the differences between a Next-Generation Firewall and a Traditional Firewall
Ans: Following are the main differences between the traditional firewall and Next-Generation firewall,

The NGFW can find the identity of a user, whereas the traditional firewall can't.
A traditional firewall can only track the traffic based on 2 to 4 layers. The NGFW tracks the traffic through 5 to 7 layers.
A traditional firewall only looks at the header, footer, source, and destination of the incoming packets. The NGFW will also look at the data of the incoming packet.

7. What is UTM?
Ans: Unified Threat Management (UTM) protects users from security threats. It provides a variety of security features in a single platform that can be used by IT teams to address security challenges. It includes functionalities like anti-virus, content filtering, unapproved website access, spyware, etc.

8. Explain about integrated threat management

Ans: Integrated threat management is an approach used to face malware such as blended threats, spam, etc. It protects from intrusion at both gateway and endpoint levels. It enables simplified administration by protecting from all threats for every component in a heterogeneous and integrated environment.

9. What is Security Fabric?

Ans: The Fortinet Security Fabric has defined as a broad, integrated, and automated cybersecurity platform. It provides seamless protection through expanding attack surface, the profusion of endpoints across multiple environments, etc. It increases the speed of operation by linking different tools through a single console and eliminates security gaps.

10. Name the different encryption mechanisms available in Fortigate Firewall

Ans: FortiGate uses AES and DES symmetric-key algorithms for encrypting and decrypting data. Some of the algorithms supported by FortiGate are,

des-md5
des-sha1
des-sha256
des-sha384
des-sha512
aes128-md5
aes128-sha1

11. What do you mean by 'Aware' in Fortinet Security fabric?

Ans: Security Fabric provides situational awareness to management and enables continuous improvement. It will establish awareness throughout the network, which means understanding threats. It focuses on understanding the flow of data or information across the network. It controls which packet gets to where and to whom.

12. Explain about 'Actionable' in Fortinet Security Fabric

Ans: Security Fabric provides a unified view of the distributed attack surface. It has a common set of threat intelligence and centralized orchestration. So it correlates global threat intelligence with local network data and delivers actionable threat intelligence to every security device in your network.

13. Explain the 'Scalable' feature in Fortinet Fabric?

Ans: Security should be provided end-to-end at a deep inspection level. Security Fabric's software not only scales within the environment, but it also scales seamlessly tracking data from IoT and endpoints. It protects the packet data across distributed networks from IoT to the Cloud.

14. How does the security feature of Fortinet Security Fabric benefit us?

Ans: In an organization, security has to be provided for the tools and services across the network. Security Fabric acts like a single collaborative entity by allowing individual device elements to share global and local threat intelligence and threat mitigation information.

15. What are open APIs in Fortinet Security Fabric?
Ans: An organization might have multiple security devices that serve different purposes. Security Fabric provides open APIs that have to be used to include these devices from technology to an integrated Fortinet security solution. It allows interaction points such as a hypervisor, the SDN orchestration controller, cloud, sandbox, etc.

16. How is Fortinet's Fabric-Ready Partner program different from the other partner programs?
Ans: Fortinet Fabric-Ready partner program expands openness by providing integration through open APIs and a variety of scripts using DevOps tools. Fabric connectors allow integration with Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, VMWare NSX, etc. It enables automation of workflows, security policies, and application deployments.

17. What is a Fortinet Firewall?
Ans: Fortinet firewalls are nothing but purpose-built with security processors mainly used to enable the industry's best threat protection and performance for SSL-encrypted traffic in an organization. This Fortinet Firewall mainly offers the following usages such as granular visibility of applications, user data protection, and secured IoT devices. These types of appliance firewalls are designed to track any kind of to track the issues.

18. How can we configure FortiIOS to turn on global strong encryption?
Ans: Global encryption means to allow only strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS, SSH, and SSL/TLS. We can use the below command to configure FortIOS:

19. Which back-end servers can be used to provide recipient verification?
Ans: LDAP servers and SMTP servers are the two server types that are used to provide recipient verification.

20. How can you send logs to FortiAnalyzer/ FortiManager in an encrypted format by using GUI?
Ans: Steps are as follows;

Go to Select log & Report ->then select Log settings and configure Remote Logging to FortiAnalyzer/ FortiManager (or Select Encrypt log transmission button).

21. What does a FortiMail unit do in a transparent mode?
Ans: The FortiMail unit acts as a proxy and does the following operations,

Intercepts email messages.
Scans for viruses and spam.
It sends emails to the destination email server.
External MTAs connected to the FortiMail unit.

22. What are the points that should be considered while mounting a Fortinet firewall (Hardware) in the rack?
Ans: Below are important points which explain how to perform molding Fortinet firewalls;

First set the room temperature -> this should be equal to the range of ambient temperature which is given by the original equipment manufacturer system management(OEM).
Using a mechanism like reliable power earthing
Firewalls Adequate system airflow used for safe operations
firewalls Adequate system precautions used for overcurrent management and supply wiring.

23. Why do we have to deploy a FortiMail unit in transparent mode?
Ans: If the FortiMail unit is operating in transparent mode, then the administrator doesn't have to configure DNS records for protected domain names.

24. What actions can be taken against a source IP address generating spam or invalid email messages when using a sender reputation?
Ans: FortiMail unit calculates a sender reputation score and performs actions based on the threshold,

If the score is less than the threshold, the sender can send emails without restrictions
If the score lies between the threshold and a reject threshold, the FortiMail unit will send a temporary failure code while delaying email delivery
If the score is greater than the threshold, the FortiMail unit will send a rejection code

25. What is the method does the FortiGate unit use to determine the availability of a web cache using Web cache communication protocol (WCCP)?
Ans: In the Fortigate, the Web cache mechanism sends a message like “I see you” which is later stored by the FortiGate unit.

26. What profile can be used to protect against denial-of-service attacks?
Ans: Session profile has to be used to protect against denial-of-service attacks.

27. What is the FGCP cluster?
Ans: FGCP stands for FortiGate Clustering Protocol. This is one of the proprietaries and popular high availability solutions offered by Fortinet firewall. FortiGate High Availability solution mainly contains two firewalls, which are used for configuring the high availability operation.

28. What are the various steps that should be taken by any user before performing up-gradation of the firmware of the Fortinet security Firewall?
Ans: The steps are as follows;

Back up -> store the old configuration

Back up the copy -> then the old Fortinet firmware can be executed. This is one of the worst-case scenarios.
Now the user needs to Read NOTE command which is released by the manufacturer. This may consist of firewall mechanisms useful information related to debugging fixation, and test the performance, etc.
Finally upgrade the system.

29. How to take a backup of the Fortinet firewall configuration?
Ans: Here you can follow the given CLI commands for the backup configuration;

Execute backup config management- station

Execute backup config USD < Filename-backup> []

For FTP;

Execute backup config ftp [] [] [].

For TFTP;

Execute backup config tftp .

30. What happens if the disk logging is disabled in the FortiGate unit?
Ans:If the hard disk logging is disabled, then the logs are written to flash memory. Constant rewrites to flash drives will reduce the lifetime and efficiency of the memory.

31. How to perform disable activities involved in administrative access management from the internet?
Ans: User can disable the administrative activity access from the outside world through GUI (user interface) AND CLI through CLI;

Config system interface
Edit
Unset allow access
End.
Via:

Network -> interfaces, edit external interface and disable five protocols: HTTPS, PING, HTTP, SSH, and TELNET under administrative access.

32. Write the important CLI command to disable or deactivate auto USB installation?
Ans: The following is the important CLI code snippet to disable or deactivate USB installation;

Config system auto-install
Set auto-install-config disable

Set auto-install-image-disable
End.

33. How Fortinet provides support in case of any difficulty or issue faced by any network administrator?

Ans: Below are the important options available to resolve any issue;

Knowledge base system
Fortinet document library management
Training and Certification provided by communities
Fortinet Video library usage
Discussion forums maintenance
Technical Contact support availability.

34. WAN optimization is, Configured in active or passive mode, when will the remote peer accept an attempt to initiate a tunnel?

Ans: The attempt will be accepted when there is a matching WAN optimization passive rule.

35. An e-mail message, received by the Fortinet unit is subject to the bounce verification, Antispam check, under which circumstances?

Ans: The envelop MAIL FROM field contains a null reverse-path when a bounce verification key is created and activated.

36. In the local storage structure of the Fortimail Unit, what does the flash memory contain?

Ans: The flash memory contains firmware images along with system configuration and certificates.

37. Which SMTP sessions are defined As Incoming?

Ans: SMTP sessions for the protected domain.

Fortinet Interview Questions and Answers

1. What is your opinion of Fortinet's FortiGate Firewall?

Ans: The rising tendency towards all-in-one products sounds a good marketing idea, but when it comes to performance, there is a big gap. It is believed that when it comes to security there should be no negotiation and concession. With all in one box, perfectly synchronized with each other working synergistically, the product is bound to be appreciated. FortiOS released by Fortinet with its range of appliances offers good routing and encryption features by enhancing support for RIP I & II and OSPF.

2. What is UTM?

Ans: Unified threat management (UTM) is a move toward security management that allows a network administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console. UTM appliances not only combines firewall, gateway anti-virus, and intrusion detection and prevention capabilities into a single platform but also works within themselves interdependently just like a piece of fabric.

3. What is Security fabric?

Ans: Security Fabric uses FortiTelemetry to connect different security sensors and tools together to collect, coordinate, and respond to malicious behavior anywhere it occurs on the network in real-time. The core of a security fabric is an upstream FortiGate located at the edge of the network, with several FortiGates functioning as Internet Segmentation Firewalls (ISFWs).

A security fabric is used to coordinate with the behavior of other Fortinet products in the network, including FortiAnalyzer, FortiManager, FortiClient, FortiClient EMS, FortiWeb, FortiSwitch, and FortiAP.

3. What is Threat Management?
Ans: Integrated threat management is a complete approach to network security issues that address multiple types of malwares, as well as blended threats and spam, and protects from invasion not only at the gateway but also at the endpoint levels.

4. What is a Next-Generation Firewall?
Ans: Next-Generation Firewall (NGFW) is the part of the third generation in firewall technology, combining a traditional firewall with other network device filtering functionalities, such as an application firewall using an in-line deep packet inspection system (DPI), an intrusion prevention system (IPS).

Other techniques might also be employed, such as TLS/SSL encrypted traffic examination, website filtering, QoS/bandwidth management, antivirus scrutiny, and third-party identity management integration (i.e. LDAP, RADIUS, Active Directory)

5. What is the difference between a Next-Generation Firewall vs. Traditional Firewall?
Ans: NGFWs includes typical functions of traditional firewalls such as packet filtering, network and port address translation (NAT), stateful monitoring, with virtual private network (VPN) support. The aim of next-generation firewalls is to include more layers of the OSI model, improving the filtering of network traffic that is dependent on the packet contents.

NGFWs perform deeper inspection compared to stateful inspection executed by the first and second-generation firewalls. NGFWs use a more thorough inspection approach, checking packet payloads and matching the signatures for harmful activities such as exploitable attacks and malware.

6. Do you know about Fortinet as an Organization?
Ans: Fortinet is an American MNC with its headquarters in Sunnyvale, California. It develops and markets cybersecurity software, appliances, and services, such as firewalls, anti-virus, intrusion prevention, and endpoint security, among others. It is the fourth-largest network security company by revenue.

7. Tell us something about Fortinet's history
Ans: Ken and Michael Xie, each other's siblings, founded Fortinet in 2000. Fortinet raised about $93 million in funding by 2004 and introduced ten FortiGate appliances. That same year was the beginning of a recurring patent dispute between Fortinet and Trend Micro.

The company went public in 2009, raising $156 million through an initial public offering. Throughout the 2000s, Fortinet expanded its product lines, by adding products for wireless access points, sandboxing, and messaging security, among others.

8. When inspecting and delivering email messages, what does a FortiMail unit do in a transparent mode?
Ans: First, inspect viruses, then Inspect the content of the message payload, then Inspect for spam, followed by performing a routing lookup to decide the next hop in MTA.

9. What are the benefits of the Scalable feature in Fortinet Fabric?
Ans: Fortinet Security Fabric protects any organization from IoT to the Cloud. A complete security strategy needs both in-depth performances and in deep inspection along with the breadth i.e. end to end. Security not only needs to scale to meet volume and performance demands, it needs to scale itself up laterally, seamlessly tracking and securing data from IoT and endpoints, across the distributed network and data center, and into the cloud.

Fortinet Security Fabric provides seamless, protection across the distributed Enterprise, as well as inspection of packet data, application protocols, and deep analysis of unstructured content at wire speeds.

10. What does Aware mean in Fortinet Security fabric?
Ans: Security Fabric behaves as a single entity from a Policy and Logging perspective, enabling end-to-end segmentation in order to lessen the risk from advanced threats. We not only need to see data that flows into and out of the network but how that data pass through the network once it is inside the perimeter.

Fortinet Security Fabric enables end-to-end network segmentation for deep visibility and inspection of traffic traveling the network, and controls who and what gets to go where thereby minimizing the risk from advanced threats.

11. What is the method FortiGate unit usess to determine the availability of a web cache using wccp? (web cache communication protocol)
Ans: The web cache sends an “I see you” message, being fetched by the FortiGate unit.

12. WAN optimization is, configured in active or passive mode, when will the remote peer accept an attempt to initiate a tunnel?
Ans: The attempt will be accepted when there is a matching WAN optimization passive rule.

13. How does FortiMail Administrator Retrieve Email Account Information from a LDAP server instead of configuring this data manually on the unit?
Ans: The Configure of the LDAP profile sections “User query options” and “Authentication” then associates the profile to the domain, which is locally configured.

14. When using a sender reputation on a FortiMail unit, which actions can be taken against a source IP address generating spam or invalid E-mail messages?
Ans:

1. FortiMail Delays the email messages from that source IP address with a temporary failure.
2. FortiMail Rejects the email messages from that source IP address with a permanent failure.
3. FortiMail Quarantines all the email messages from that source IP address

15. What does the security feature of Fortinet Security Fabric benefit us?
Ans: Global and local risk intelligence and lessening information can be shared across individual products to decrease time to protect. Not only does security need to include powerful security tools for the various places and functions in the network, but true visibility and control needs these distinct elements work together as an integrated security system.

Fortinet's Security Fabric behaves as a single collaborative entity from a policy and logging perspective, allowing individual product elements to share global and local risk intelligence and risk mitigation information.

16. What do we mean by Actionable in Fortinet Security Fabric?
Ans: Big Data cloud systems correlate risk information and network data to deliver into Actionable Threat Intelligence in real-time. It is not enough to sense bad traffic or block malware using distinct security devices. Network administrators need a common set of risk intelligence and centralized orchestration that allows the security to dynamically adapt as a risk is revealed anywhere, not just in our network, but also anywhere in the world.

Fortinet's Big Data cloud systems centralize and correlate risk information and network data and provide actionable threat intelligence to each and every single security device in the network's security fabric in real-time.

17. What do we understand by Open APIs in Fortinet Security Fabric?
Ans: Well defined, open APIs allow leading technology partners to become part of the fabric. Of course, a true security fabric lets us maximize our existing investment in security technologies. That is why Fortinet has developed a series of well defined, open APIs that allow technology partners to become a part of the Fortinet Security Fabric. Combined, the Fortinet Security Fabric is able to quickly adapt to the evolving network architecture as well as changing the threat landscape.

18. Why is the idea of a security fabric so important to network security in this current environment?
Ans: In this futuristic era, companies have to deal with a growing list of issues that put incredible strain on their security capabilities, including the Internet of Things, virtualization, SDN, a growing portfolio of interactive applications, and transitioning to cloud-based networking.

They also have professionals who expect to be able to access work applications and data from anywhere, at any time, and on the same device, they use to manage their professional lives. Networks have evolved to accommodate these new requirements, becoming more complex, flexible, and powerful. At the same time, securing them has become a lot more complex as well.

19. What distinguishes Fortinet's security fabric approach from other vendors' attempts at an integrated platform?

Ans: Fortinet distinguishes with other vendors with intentionally designed integration beginning with a unified operating system, highly optimized hardware and software processing with unmatched zero-day discovery, and a detection approach that combines behavioral detection, machine learning, and hardware virtualization.

This allows the Fortinet Security Fabric to go beyond what is possible with a traditional signature-based approach to risk protection, or with siloed security technologies that vendors have begun to apparently stitch together using an overlay "platform" method.

20. How does Fortinet's Security Fabric benefit Fortinet's global partner network of distributors and solution providers?

Ans: Because of its significant and complex character, security continues to be one of the largest opportunities for the channel. Partners that can plan, design, deploy and optimize an integrated security system are finding a growing demand for their skills. By combining the traditional security devices and emerging technologies together into an integrated security fabric, associates can help their customers collect and respond to intelligence that is more actionable, synchronize risk responses, and centralize the creation, distribution, and orchestration of their security management and further investigation.

This wide visibility and open-standards approach offered by the Fortinet Security Fabric allows the solution providers to implement more automation to focus on the alerts, which matters the most in today's world.

21. How is Fortinet's Fabric-Ready Partner program different from the partner programs we see other vendors promoting?

Ans: Like many other partner programs, Fortinet's Fabric-Ready Partner Program brings together best-in-class technology alliance partners. Unlike other approaches, Fortinet's approach actually allows the partners to deliver pre-integrated, end-to-end security offerings ready for deployment in any organization.

22. An e-mail message, received by the FortiMail unit is subject to the bounce verification, Antispam check, under which circumstances?

Ans: The envelope MAIL FROM field contains a null reverse-path when a Bounce Verification key is created and activated.

23. Network Administrator of a FortiMail Unit operating in server mode has been given the requirement to configure disk quotas for all the users of a specific domain. How can the administrator achieve this requirement?
Ans: Network Administrator needs to define a disk quota value in a resource profile.

24. Which operational mode allows the FortiMail unit to operate as a full-featured email server rather than just a mail relay agent?
Ans: In Server Mode, FortiMail, operate as a full-featured email server rather than just a mail relay agent

25. What is the one reason for deploying a FortiMail unit in transparent mode?
Ans: If the network administrator deploys the FortiMail unit in transparent mode then DNS records do not necessarily have to be modified.

26. Which SMTP Sessions is defined as incoming?
Ans: SMTP sessions for the protected domain are defined as incoming.

27. Which back-end servers can be used to provide recipient verification?
Ans: LDAP servers, and SMTP servers.

28. A System Administrator Is Concerned By The Amount Of Disk Space Being Used To Store Quarantine Email Messages For Non-existent Accounts. Which Techniques Can Be Used On A FortiMail Unit To Prevent Email Messages From Being Quarantined For Non-existent Accounts?
Ans: Recipient Address Verification should be adopted to prevent E-mail messages from being quarantined for non-existent accounts

29. In The Local Storage Structure Of The Fortimail Unit, What Does The Flash Memory Contain?
Ans: The Flash Memory Contain Firmware Image along with System Configuration and Certificates.