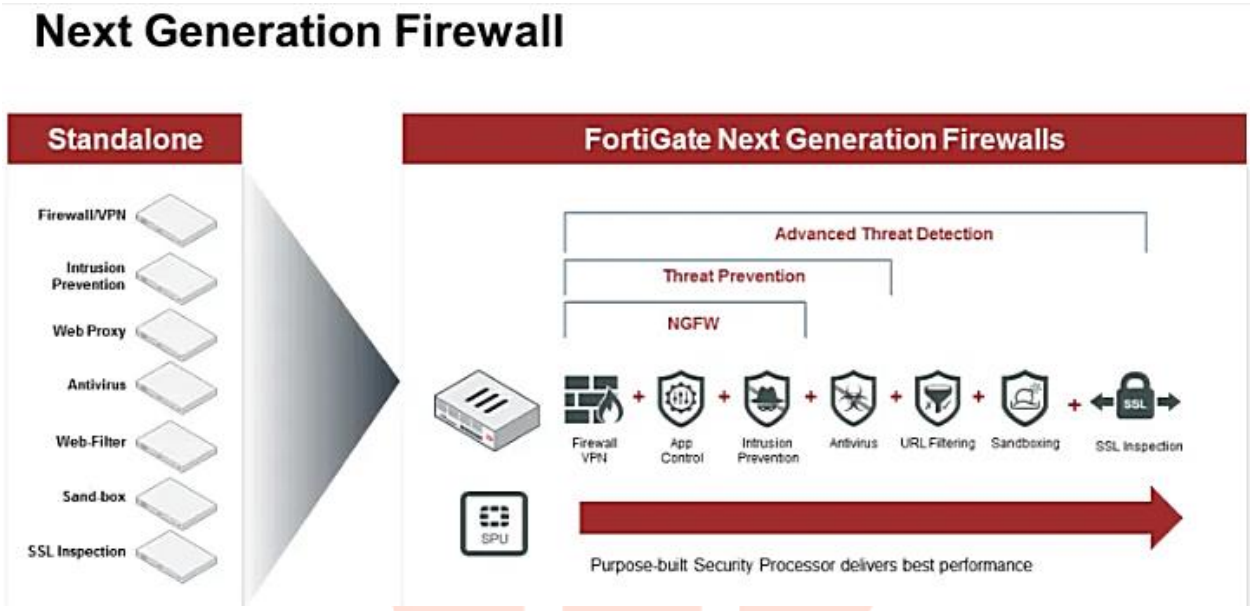
Q1: What is the Next Generation Firewall?

A: 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).

FortiGate Next Generation Firewall



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).

Q2. What are the different authentication and encryption mechanisms available in Fortigate Firewall?

Ans: I am listing below methods in order of strength for authentication and encryption:
WPA2 – Enterprise 802.1x/EAP (Personal pre-shared key of 8-63 characters)
WPA – Enterprise 802.1x/EAP (Personal pre-shared key of 8-63 characters)
WEP128 (26 Hexadecimal digit key)
WEP64 (10 Hexadecimal digit key)
None
It is advisable to use WPA2, which is the strongest method for authentication and encryption.

Q.3 Mention some points while configuring the network.

Ans:Don’t leave the backdoor to access the firewall.
Prepare network diagram consists of IP addressing, cabling, and network devices.

Q4. What is the command to power off the FortiGate unit via CLI?

Ans: To power off the FortiGate unit
execute shutdown

Q5. What are the points that should be considered while installing/mounting a Fortinet firewall (hardware) in the rack?

Ans: Below are the points of consideration while mounting a firewall:

The room temperature should be in the range of ambient temperature defined by the Original Equipment Manufacturer (OEM)
Reliable earthing mechanism
Adequate airflow provided for safe operation.
Adequate precautions for overcurrent and supply wiring

Q6. What is Security Fabric?

Ans: Security Fabric is a security solution to detect, monitor, block, and remediate cyber-attacks.

A: 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.

Q7. What are the steps that should take before each upgrade of firmware of the Fortinet firewall?

Ans:
Step 1: Backup and store old configuration.

Step 2: Back up a copy of the old firmware executable. This is for the worst-case scenario. If something bad happens, you have an option of rollback.

Step 3: Read the NOTE released by the manufacturer. It may contain useful information related to bug fixation, performance, etc.

Step 4: Upgrade.

Q8. Mention the steps for back up the FortiGate configuration via GUI.

Ans. Dashboard -> select Backup in System Information widget -> select drive for storing -> Encrypt configuration file –> Enter a password and select Backup –> save the configuration file

Q9. What is the backup configuration file format in the Fortinet firewall?

Ans: The configuration file will have a .conf extension.

Q10. How you take a backup of the configuration of a Fortinet firewall?

Ans: You can use below CLI commands for backup configuration:

execute backup config management-station <comment>

execute backup config usb <filename-backup> [<password-backup>]
For FTP

execute backup config ftp <filename-backup> <ftp_server> [<port>] [<username>] [<password>]
For TFTP

execute backup config tftp <filename-backup> <tftp_servers> <password>

Q11. How to disable administrative access from the internet?

Ans: You can disable administrative access from the outside world via GUI and CLI.
via CLI:
config system interface
edit <external-interface>
unset allowaccess
end
via GUI:

Network -> Interfaces, edit external interface, and disable five protocols: HTTPS, PING, HTTP, SSH, and TELNET under Administrative Access.

Q12. How to maintain short login timeouts while accessing the FortiGate firewall?

Ans: Below command can be used to short the login timeouts:

config system global
set admi timeout 5
end
Click here for more Firewall Interview Questions

Q13. How can you send logs to FortiAnalyzer/FortiManager in an encrypted format by using GUI?

Ans: Select Log & Report > Log Settings and configure Remote Logging to FortiAnalyzer/FortiManager (select Encrypt log transmission).

Q14. Write the CLI command to disable auto USB installation.

Ans: Below is the CLI code snippet to disable USB installation

```
config system auto-install
set auto-install-config disable
set auto-install-image disable
end
```

Q15. How Fortinet provide support in case of any difficulty face by a network administrator?

Ans: You can access the “Customer Service & Support” page on the Fortinet portal. Following options are available to resolve any issue:

Knowledge Base
Fortinet Document Library
Training & Certification
Fortinet Video Library
Discussion Forums
Contact Support

Q16. What is the FGCP cluster?

Ans: FGCP stands for FortiGate Clustering Protocol. It is a proprietary High Availability (HA) solution provided by Fortinet. Fortigate HA solution consists of a minimum of two firewalls configured for high availability operation.

Q17. How can we configure FortiOS to turn on global strong encryption?

Ans: Global strong 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:

```
config sys global
set strong-crypto enable
end
```

Related

Q18. When inspecting and delivering email messages, what does a FortiMail unit do in a transparent mode?

Ans: First inspect viruses, then Inspect content of the message payload, then Inspect for spam, followed by performing a routing lookup to decide the next hop in MTA.

Q19. What is the one reason for deploying a FortiMail unit in transparent mode?

Ans: If the network administrator deploys FortiMail unit in transparent mode then DNS records do not necessarily have to be modified.

Q20. How you can send logs to FortiAnalyzer/FortiManager in an encrypted format by using GUI?

Ans: Select Log & Report > Log Settings and configure Remote Logging to FortiAnalyzer/FortiManager (select Encrypt log transmission).

Q21. 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:
FortiMail Delays the email messages from that source IP address with a temporary failure.
FortiMail Rejects the email messages from that source IP address with a permanent failure.
FortiMail Quarantines all the email messages from that source IP address.

Q22. What are the points that should be considered while mounting a Fortinet firewall (hardware) in the rack?

Ans: Below are the points of consideration while mounting a firewall:

*The room temperature should be in the range of ambient temperature defined by Original Equipment Manufacturer (OEM)
*Reliable earthing mechanism
*Adequate airflow provided for safe operation
*Adequate precautions for overcurrent and supply wiring

Q23. What Is the Method Does the Fortigate Unit Use to Determine the Availability of A Web Cache Using Web Cache Communication Protocol (WCCP)?

Ans: The web cache sends an “I see you” message which is captured by the FortiGate unit.

Q24. 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 can quickly adapt to the evolving network architecture as well as changing the threat landscape.

Q26. 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.

Q27. 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.

Q28. When Inspecting And Delivering Mail Messages, Which Steps Could Be Taken By A Fortimail Unit Operating In Transparent Mode?

Ans:
Inspect for viruses.
Inspect the content of the message payload.
Inspect for spam.
Perform a routing lookup to decide the next-hop MTA.

Q28. Wan Optimization Is Configured in Active/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.

Q29. How Can a FortiMail Administrator Retrieve Email Account Information from An LDAP Server Instead of Configuring This Data Manually on The Unit?

Ans: Configure the LDAP profile sections “User query options” and “Authentication” then associate the profile to the domain that is locally configured.

Q30. Which Operational Mode Allows the FortiMail Unit to Operate as A Full-Featured Mail Server Rather Than Just a Mail Relay Agent?

Ans: Server Mode.

Q31. What Is One Reason for Deploying a FortiMail Unit in Transparent Mode?

Ans: DNS records do not necessarily have to be modified.

Q32. Which Profile Can Be Used to Protect against Denial-of-Service Attacks?

Ans: session profile.

Q33. Which Smtp Sessions Are Defined as Incoming?

Ans: SMTP sessions for the protected domain.

Q34. 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.

Q35. 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.

Q36. 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.

Q37. 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.

Q38. 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 behavioural 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.

Q39. 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.

Q40. 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.