

**[Download Full Version NSE4\\_FGT-7.0 Exam Dumps\(Updated in March/2023\)](#)**

- C. Add user accounts to the FortiGate group filter.
- D. Add user accounts to the Ignore User List.

**Correct Answer: D**

**QUESTION 33**

A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and the file can be downloaded. What is the reason for the failed virus detection by FortiGate?

- A. Application control is not enabled
- B. SSL/SSH Inspection profile is incorrect
- C. Antivirus profile configuration is incorrect
- D. Antivirus definitions are not up to date

**Correct Answer: B**

**QUESTION 34**

An administrator must disable RPF check to investigate an issue. Which method is best suited to disable RPF without affecting features like antivirus and intrusion prevention system?

- A. Enable asymmetric routing, so the RPF check will be bypassed.
- B. Disable the RPF check at the FortiGate interface level for the source check.
- C. Disable the RPF check at the FortiGate interface level for the reply check.
- D. Enable asymmetric routing at the interface level.

**Correct Answer: B**

**QUESTION 35**

Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

- A. Log downloads from the GUI are limited to the current filter view
- B. Log backups from the CLI cannot be restored to another FortiGate.
- C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
- D. Log downloads from the GUI are stored as LZ4 compressed files.

**Correct Answer: AB**

**QUESTION 36**

When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

- A. Log ID
- B. Universally Unique Identifier
- C. Policy ID
- D. Sequence ID

**Correct Answer: B**

**QUESTION 37**

Which feature in the Security Fabric takes one or more actions based on event triggers?

- A. Fabric Connectors
- B. Automation Stitches
- C. Security Rating
- D. Logical Topology

**Correct Answer: B**

**QUESTION 38**

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scanning of application traffic to the DNS protocol only.
- B. It limits the scanning of application traffic to use parent signatures only.
- C. It limits the scanning of application traffic to the browser-based technology category only.
- D. It limits the scanning of application traffic to the application category only.

**Correct Answer: C**

**QUESTION 39**

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

- A. FortiManager
- B. Root FortiGate
- C. FortiAnalyzer
- D. Downstream FortiGate

**Correct Answer: B**

**QUESTION 40**

Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

- A. Source defined as Internet Services in the firewall policy.
- B. Destination defined as Internet Services in the firewall policy.
- C. Highest to lowest priority defined in the firewall policy.
- D. Services defined in the firewall policy.
- E. Lowest to highest policy ID number.

**Correct Answer: ABD**

**QUESTION 41**

Which three methods are used by the collector agent for AD polling? (Choose three.)

- A. FortiGate polling
- B. NetAPI
- C. Novell API
- D. WMI
- E. WinSecLog

**Correct Answer:** BDE

**QUESTION 42**

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy. Which two other security profiles can you apply to the security policy? (Choose two.)

- A. Antivirus scanning
- B. File filter
- C. DNS filter
- D. Intrusion prevention

**Correct Answer:** AD

**QUESTION 43**

Which two statements are true about collector agent advanced mode? (Choose two.)

- A. Advanced mode uses Windows convention--NetBios: Domain\Username.
- B. FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate
- C. Advanced mode supports nested or inherited groups
- D. Security profiles can be applied only to user groups, not individual users.

**Correct Answer:** BC

**QUESTION 44**

If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

- A. The Services field prevents SNAT and DNAT from being combined in the same policy.
- B. The Services field is used when you need to bundle several VIPs into VIP groups.
- C. The Services field removes the requirement to create multiple VIPs for different services.
- D. The Services field prevents multiple sources of traffic from using multiple services to connect to a single computer.

**Correct Answer:** C

**QUESTION 45**

Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

- A. Subject Key Identifier value
- B. SMMIE Capabilities value
- C. Subject value
- D. Subject Alternative Name value

**Correct Answer:** A

**QUESTION 46**

If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

- A. A CRL
- B. A person
- C. A subordinate CA
- D. A root CA

**Correct Answer:** D

**QUESTION 47**

Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

- A. The public key of the web server certificate must be installed on the browser.
- B. The web-server certificate must be installed on the browser.
- C. The CA certificate that signed the web-server certificate must be installed on the browser.
- D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

**Correct Answer:** C

**QUESTION 48**

Which three statements are true regarding session-based authentication? (Choose three.)

- A. HTTP sessions are treated as a single user.
- B. IP sessions from the same source IP address are treated as a single user.
- C. It can differentiate among multiple clients behind the same source IP address.
- D. It requires more resources.
- E. It is not recommended if multiple users are behind the source NAT

**Correct Answer:** ACD

**QUESTION 49**

In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

- A. The IP version of the sources and destinations in a firewall policy must be different.
- B. The Incoming Interface, Outgoing Interface, Schedule, and Service fields can be shared with both IPv4 and IPv6.
- C. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
- D. The IP version of the sources and destinations in a policy must match.
- E. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

**Correct Answer:** BDE

**QUESTION 50**

What is the primary FortiGate election process when the HA override setting is disabled?

- A. Connected monitored ports > System uptime > Priority > FortiGate Serial number
- B. Connected monitored ports > HA uptime > Priority > FortiGate Serial number