A. on each IPS rule
B. globally, within the network analysis policy
C. globally, per intrusion policy
D. on each access control rule
E. per preprocessor, within the network analysis policy

**Correct Answer:** AC

**QUESTION 32**
A company has many Cisco FTD devices managed by a Cisco FMC. The security model requires that access control rule logs be collected for analysis. The security engineer is concerned that the Cisco FMC will not be able to process the volume of logging that will be generated. Which configuration addresses this concern?

A. Send Cisco FTD connection events and security events directly to SIEM system for storage and analysis.
B. Send Cisco FTD connection events and security events to a cluster of Cisco FMC devices for storage and analysis.
C. Send Cisco FTD connection events and security events to Cisco FMC and configure it to forward logs to SIEM for storage and analysis.
D. Send Cisco FTD connection events directly to a SIEM system and forward security events from Cisco FMC to the SIEM system for storage and analysis.

**Correct Answer:** C

**QUESTION 33**
An organization does not want to use the default Cisco Firepower block page when blocking HTTP traffic. The organization wants to include information about its policies and procedures to help educate the users whenever a block occurs. Which two steps must be taken to meet these requirements? (Choose two.)

A. Modify the system-provided block page result using Python.
B. Create HTML code with the information for the policies and procedures.
C. Edit the HTTP request handling in the access control policy to customized block.
D. Write CSS code with the information for the policies and procedures.
E. Change the HTTP response in the access control policy to custom.
**Correct Answer:** BE

**QUESTION 34**
Which two actions can be used in an access control policy rule? (Choose two.)

A. Block with Reset
B. Monitor
C. Analyze
D. Discover
E. Block ALL

**Correct Answer:** AB

**QUESTION 35**

When creating a report template, how can the results be limited to show only the activity of a specific subnet?

A. Create a custom search in Firepower Management Center and select it in each section of the report.
B. Add an Input Parameter in the Advanced Settings of the report, and set the type to Network/IP.
C. Add a Table View section to the report with the Search field defined as the network in CIDR format.
D. Select IP Address as the X-Axis in each section of the report.

**Correct Answer:** B

**QUESTION 36**
Which Cisco Firepower rule action displays an HTTP warning page?

A. Monitor
B. Block
C. Interactive Block
D. Allow with Warning

**Correct Answer:** C

**QUESTION 37**
An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events filing the database and overloading the Cisco FMC. A monitored NAT device is executing multiple updates of its operating system in a short period of time. What configuration change must be made to alleviate this issue?

A. Leave default networks.
B. Change the method to TCP/SYN.
C. Increase the number of entries on the NAT device.
D. Exclude load balancers and NAT devices.

**Correct Answer:** D

**QUESTION 38**
An engineer is using the configure manager add <FMC IP> Cisc402098527 command to add a new Cisco FTD device to the Cisco FMC; however, the device is not being added. Why Is this occurring?

A. The NAT ID is required since the Cisco FMC is behind a NAT device.
B. The IP address used should be that of the Cisco FTD. not the Cisco FMC.
C. DONOTRESOLVE must be added to the command
D. The registration key is missing from the command

**Correct Answer:** A

**QUESTION 39**
In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.)

A. Traffic inspection can be interrupted temporarily when configuration changes are deployed.

B. The system performs intrusion inspection followed by file inspection.
C. They can block traffic based on Security Intelligence data.
D. File policies use an associated variable set to perform intrusion prevention.
E. The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters.

**Correct Answer:** AC

**QUESTION 40**
Which object type supports object overrides?

A. time range
B. security group tag
C. network object
D. DNS server group

**Correct Answer:** C

**QUESTION 41**
A company is in the process of deploying intrusion prevention with Cisco FTDs managed by a Cisco FMC. An engineer must configure policies to detect potential intrusions but not block the suspicious traffic. Which action accomplishes this task?

A. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the "Drop when inline" option.
B. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the "Drop when inline" option.
C. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the "Drop when inline" option.
D. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the "Drop when inline" option.

**Correct Answer:** A
**QUESTION 42**
Which two types of objects are reusable and supported by Cisco FMC? (Choose two.)

A. dynamic key mapping objects that help link HTTP and HTTPS GET requests to Layer 7 application protocols.
B. reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists
C. network-based objects that represent IP address and networks, port/protocols pairs, VLAN tags, security zones, and origin/destination country
D. network-based objects that represent FQDN mappings and networks, port/protocol pairs, VXLAN tags, security zones and origin/destination country
E. reputation-based objects, such as URL categories

**Correct Answer:** BC

**QUESTION 43**
Which Firepower feature allows users to configure bridges in routed mode and enables devices to perform Layer 2 switching between interfaces?

A. FlexConfig
B. BDI
C. SGT
D. IRB

**Correct Answer:** D

**QUESTION 44**
An organization is using a Cisco FTD and Cisco ISE to perform identity-based access controls. A network administrator is analyzing the Cisco FTD events and notices that unknown user traffic is being allowed through the firewall. How should this be addressed to block the traffic while allowing legitimate user traffic?

A. Modify the Cisco ISE authorization policy to deny this access to the user.
B. Modify Cisco ISE to send only legitimate usernames to the Cisco FTD.
C. Add the unknown user in the Access Control Policy in Cisco FTD.
D. Add the unknown user in the Malware & File Policy in Cisco FTD.

**Correct Answer:** C

**QUESTION 45**
Which two routing options are valid with Cisco Firepower Threat Defense? (Choose two.)

A. BGPv6
B. ECMP with up to three equal cost paths across multiple interfaces
C. ECMP with up to three equal cost paths across a single interface
D. BGPv4 in transparent firewall mode
E. BGPv4 with nonstop forwarding

**Correct Answer:** AC

**QUESTION 46**
A network administrator reviews the file report for the last month and notices that all file types, except exe. show a disposition of unknown. What is the cause of this issue?

A. The malware license has not been applied to the Cisco FTD.
B. The Cisco FMC cannot reach the Internet to analyze files.
C. A file policy has not been applied to the access policy.
D. Only Spero file analysis is enabled.

**Correct Answer:** D

**QUESTION 47**
Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)

A. OSPFv2 with IPv6 capabilities
B. virtual links
C. SHA authentication to OSPF packets
D. area boundary router type 1 LSA filtering
E. MD5 authentication to OSPF packets