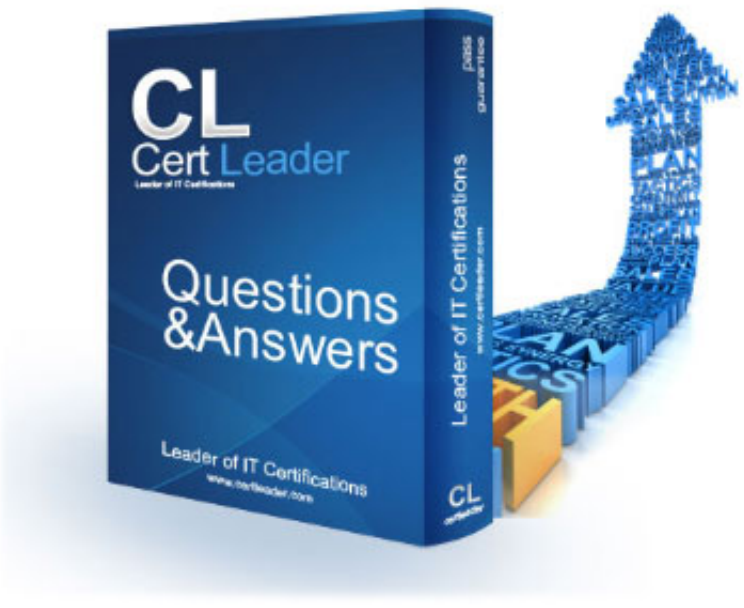
300-710 Dumps

Securing Networks with Cisco Firepower (SNCF)

https://www.certleader.com/300-710-dumps.html



NEW QUESTION 1
- (Exam Topic 5)
An administrator Is setting up a Cisco PMC and must provide expert mode access for a security engineer. The engineer Is permitted to use only a secured out-of-band network workstation with a static IP address to access the Cisco FMC. What must be configured to enable this access?

A. Enable SSH and define an access list.
B. Enable HTTP and define an access list.
C. Enable SCP under the Access List section.
D. Enable HTTPS and SNMP under the Access List section.

Answer: A

NEW QUESTION 2
- (Exam Topic 5)
An engineer integrates Cisco FMC and Cisco ISE using pxGrid. Which role is assigned for Cisco FMC?

A. controller
B. publisher
C. client
D. server

Answer: C

NEW QUESTION 3
- (Exam Topic 5)
A security engineer is configuring an Access Control Policy for multiple branch locations These locations share a common rule set and utilize a network object called INSIDE_NET which contains the locally significant internal network subnets at each location What technique will retain the policy consistency at each location but allow only the locally significant network subnet within the applicable rules?

A. utilizing policy inheritance
B. utilizing a dynamic ACP that updates from Cisco Talos
C. creating a unique ACP per device
D. creating an ACP with an INSIDE_NET network object and object overrides

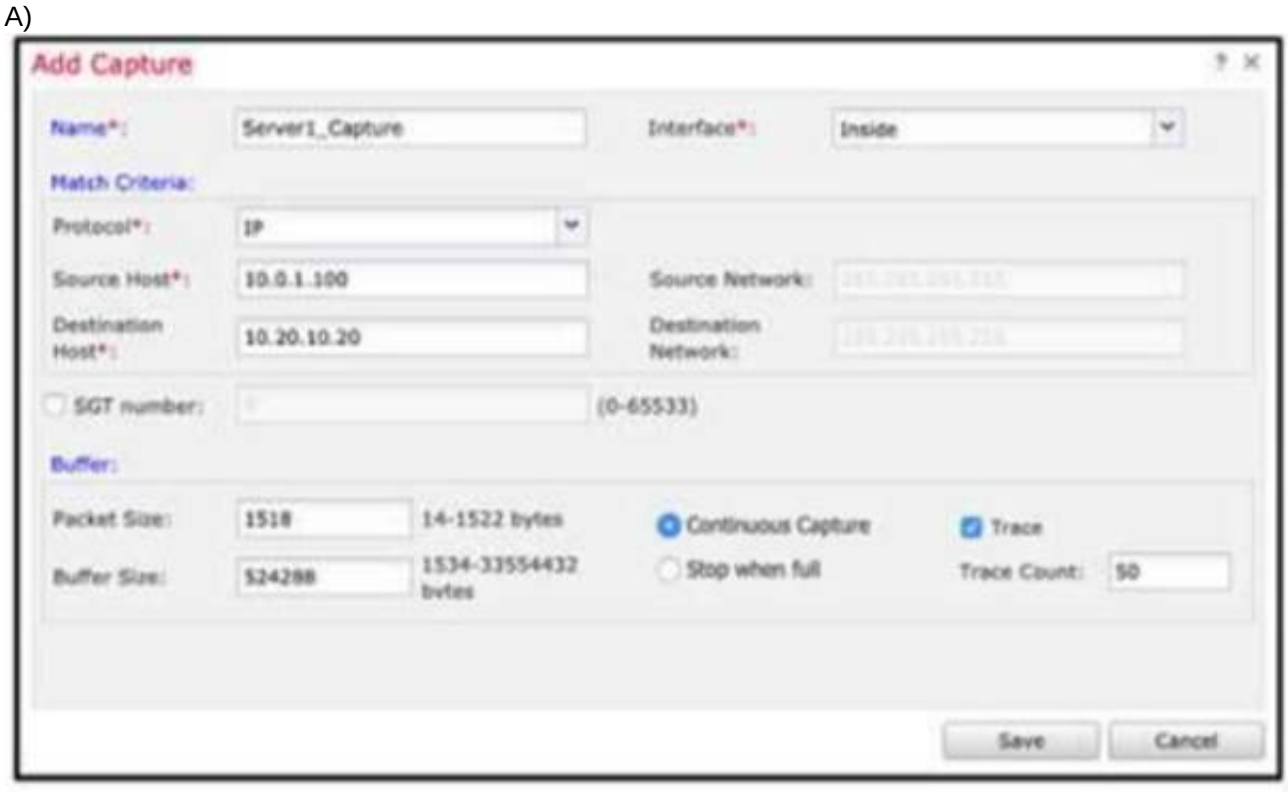
Answer: D

NEW QUESTION 4
- (Exam Topic 5)
Due to an Increase in malicious events, a security engineer must generate a threat report to include intrusion events, malware events, and security intelligence events. How Is this information collected in a single report?

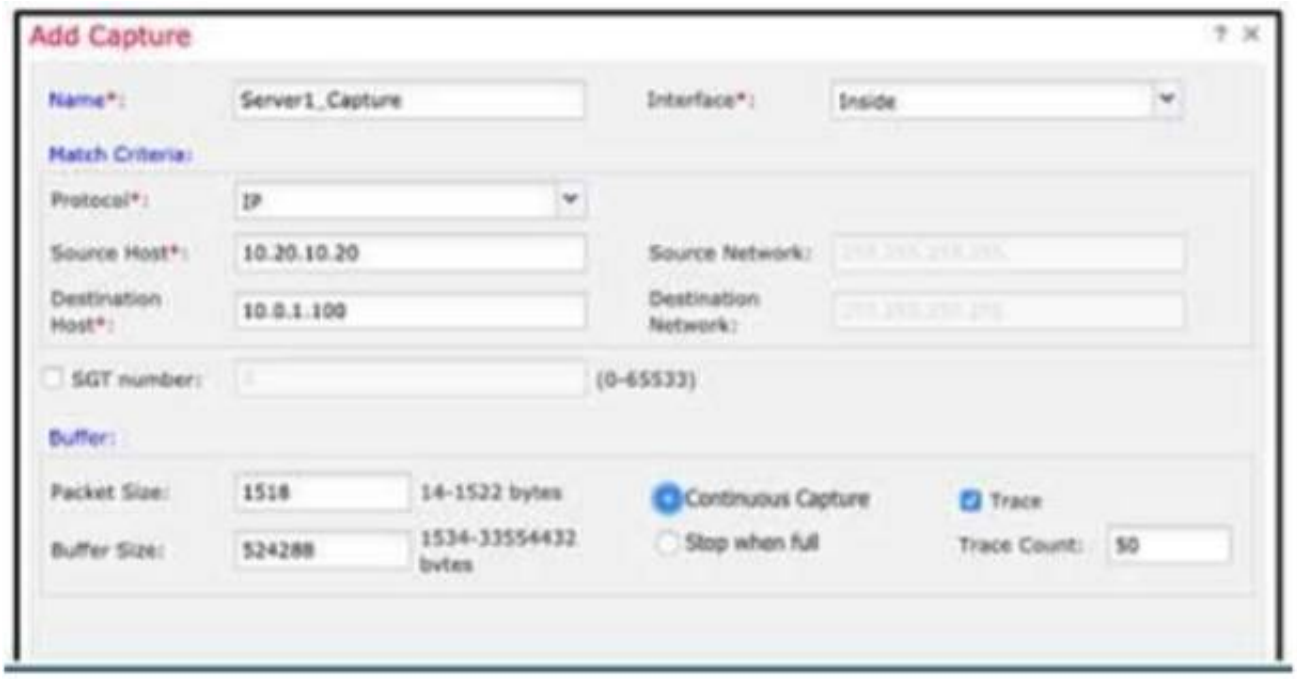
A. Run the default Firepower report.
B. Export the Attacks Risk report.
C. Generate a malware report.
D. Create a Custom report.

Answer: D

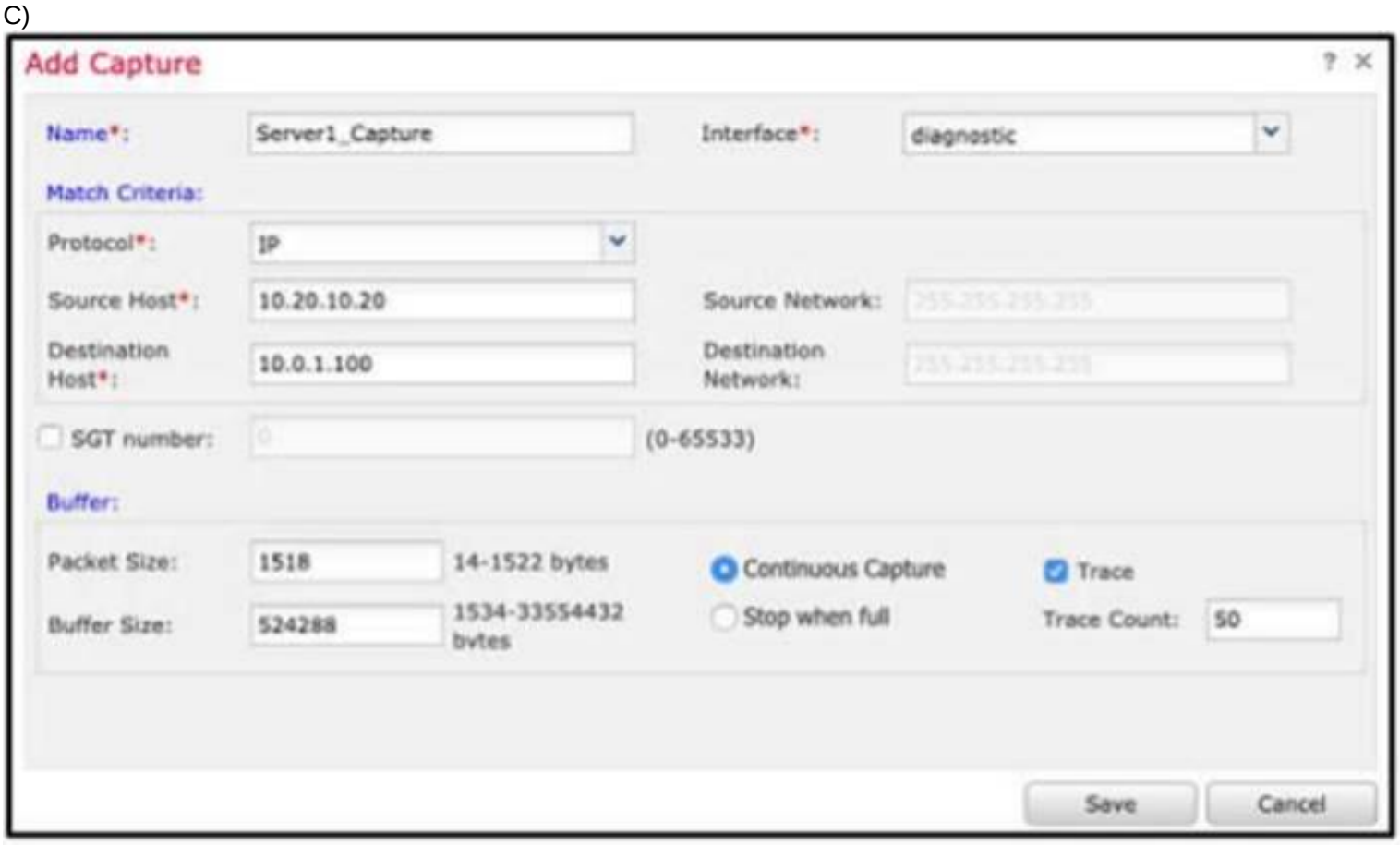
NEW QUESTION 5
- (Exam Topic 5)
An engineer is troubleshooting a device that cannot connect to a web server. The connection is initiated from the Cisco FTD inside interface and attempting to reach 10.0.1.100 over the non-standard port of 9443 The host the engineer is attempting the connection from is at the IP address of 10.20.10.20. In order to determine what is happening to the packets on the network, the engineer decides to use the FTD packet capture tool Which capture configuration should be used to gather the information needed to troubleshoot this issue?
A)



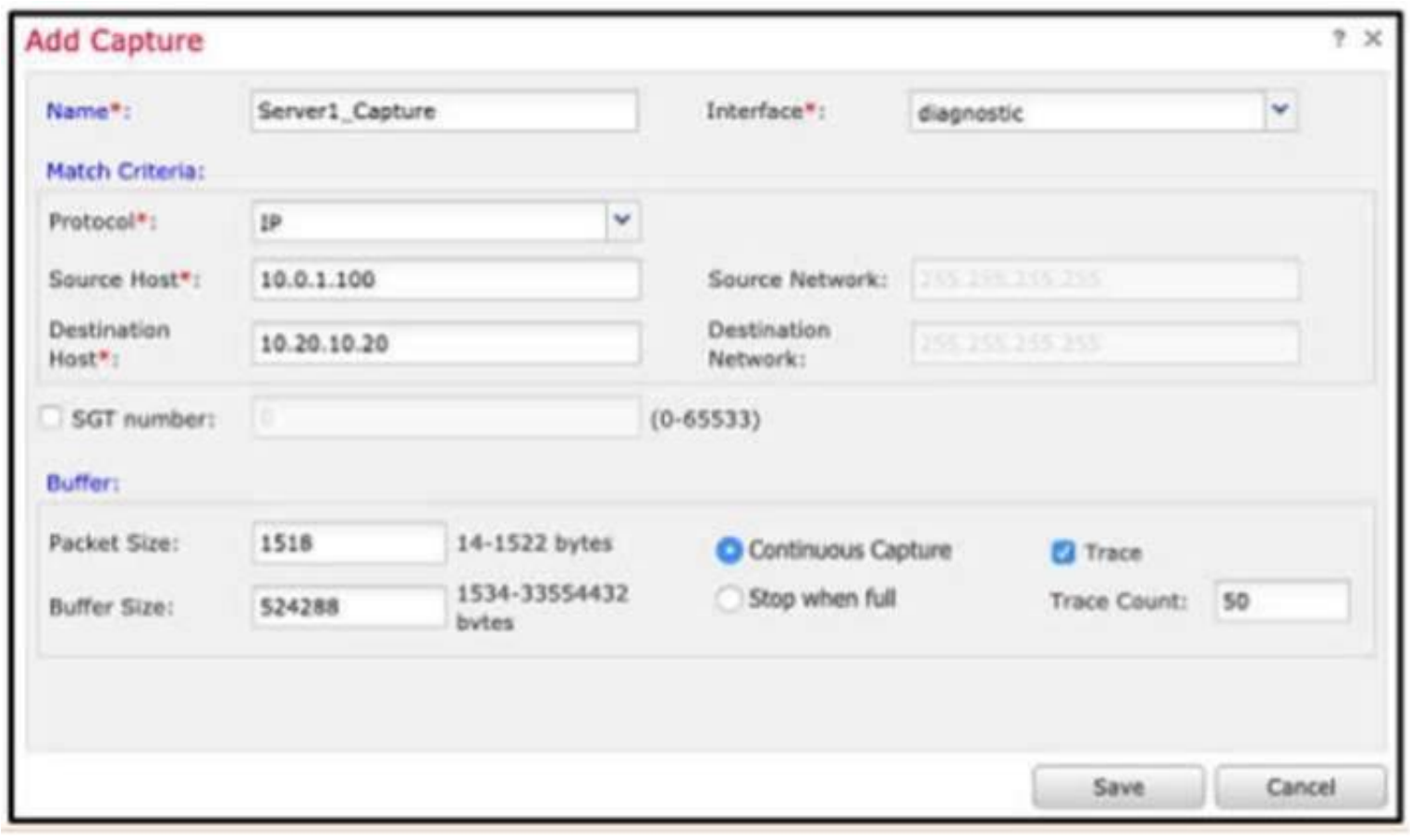
B)



C)



D)



A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 6
- (Exam Topic 5)
Which feature is supported by IRB on Cisco FTD devices?

A. redundant interface
B. dynamic routing protocol
C. EtherChannel interface
D. high-availability cluster

Answer: B

NEW QUESTION 7
- (Exam Topic 5)
An organization is configuring a new Cisco Firepower High Availability deployment. Which action must be taken to ensure that failover is as seamless as possible to end users?

A. Set up a virtual failover MAC address between chassis.
B. Use a dedicated stateful link between chassis.
C. Load the same software version on both chassis.
D. Set the same FQDN for both chassis.

Answer: B

NEW QUESTION 8
- (Exam Topic 5)
An administrator is configuring their transparent Cisco FTD device to receive ERSPAN traffic from multiple switches on a passive port, but the Cisco FTD is not processing the traffic. What is the problem?

A. The switches do not have Layer 3 connectivity to the FTD device for GRE traffic transmission.
B. The switches were not set up with a monitor session ID that matches the flow ID defined on the CiscoFTD.
C. The Cisco FTD must be in routed mode to process ERSPAN traffic.
D. The Cisco FTD must be configured with an ERSPAN port not a passive port.

Answer: C

NEW QUESTION 9
- (Exam Topic 5)
An engineer configures an access control rule that deploys file policy configurations to security zones or tunnel zones, and it causes the device to restart. What is the reason for the restart?

A. Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.
B. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.
C. Source or destination security zones in the source tunnel zone do not match the security zones that are associated with interfaces on the target devices.
D. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.

Answer: A

NEW QUESTION 10
- (Exam Topic 5)
An organization must be able to ingest NetFlow traffic from their Cisco FTD device to Cisco Stealthwatch for behavioral analysis. What must be configured on the Cisco FTD to meet this requirement?

A. interface object to export NetFlow
B. security intelligence object for NetFlow
C. flexconfig object for NetFlow
D. variable set object for NetFlow

Answer: C

NEW QUESTION 10
- (Exam Topic 5)
A network administrator configured a NAT policy that translates a public IP address to an internal web server IP address. An access policy has also been created that allows any source to reach the public IP address on port 80. The web server is still not reachable from the Internet on port 80. Which configuration change is needed?

A. The intrusion policy must be disabled for port 80.
B. The access policy rule must be configured for the action trust.
C. The NAT policy must be modified to translate the source IP address as well as destination IP address.
D. The access policy must allow traffic to the internal web server IP address.

Answer: D

NEW QUESTION 13
- (Exam Topic 5)
Remote users who connect via Cisco AnyConnect to the corporate network behind a Cisco FTD device report that they get no audio when calling between remote users using their softphones. These same users can call internal users on the corporate network without any issues. What is the cause of this issue?

A. The hairpinning feature is not available on FTD.
B. Split tunneling is enabled for the Remote Access VPN on FTD
C. FTD has no NAT policy that allows outside to outside communication
D. The Enable Spoke to Spoke Connectivity through Hub option is not selected on FTD.

Answer: A

NEW QUESTION 18
- (Exam Topic 5)
When a Cisco FTD device is configured in transparent firewall mode, on which two interface types can an IP address be configured? (Choose two.)

A. Diagnostic
B. EtherChannel
C. BVI
D. Physical
E. Subinterface

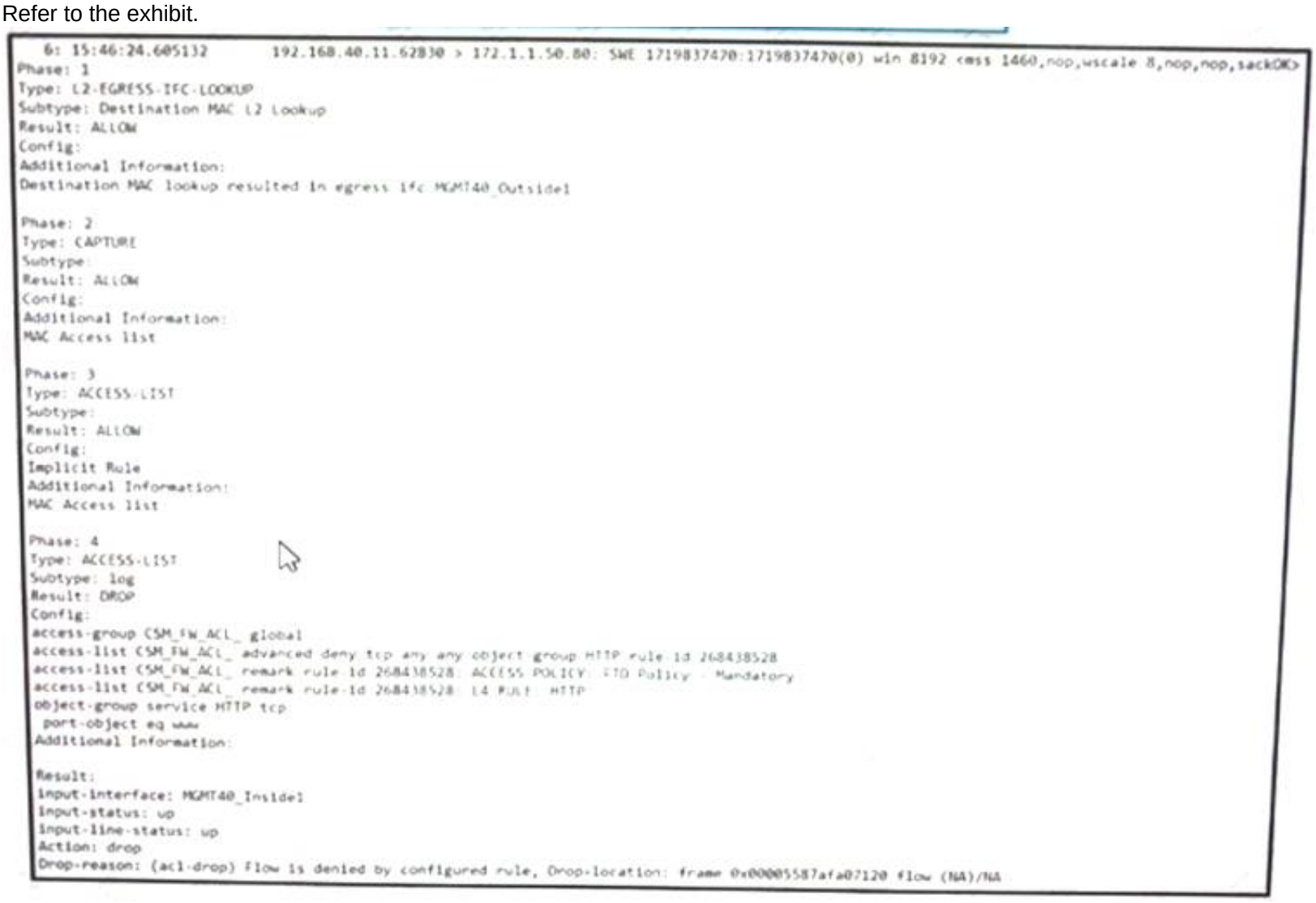
Answer: AC

NEW QUESTION 19
- (Exam Topic 5)
A security analyst must create a new report within Cisco FMC to show an overview of the daily attacks, vulnerabilities, and connections. The analyst wants to reuse specific dashboards from other reports to create this consolidated one. Which action accomplishes this task?

A. Create a new dashboard object via Object Management to represent the desired views.
B. Modify the Custom Workflows within the Cisco FMC to feed the desired data into the new report.
C. Copy the Malware Report and modify the sections to pull components from other reports.
D. Use the import feature in the newly created report to select which dashboards to add.

Answer: D

NEW QUESTION 22
- (Exam Topic 5)
Refer to the exhibit.



What must be done to fix access to this website while preventing the same communication to all other websites?

A. Create an intrusion policy rule to have Snort allow port 80 to only 172.1.1 50.
B. Create an access control policy rule to allow port 80 to only 172.1.1 50.
C. Create an intrusion policy rule to have Snort allow port 443 to only 172.1.1.50
D. Create an access control policy rule to allow port 443 to only 172.1.1 50

Answer: B

NEW QUESTION 25
- (Exam Topic 5)
A hospital network needs to upgrade their Cisco FMC managed devices and needs to ensure that a disaster recovery process is in place. What must be done in order to minimize downtime on the network?

A. Configure a second circuit to an ISP for added redundancy
B. Keep a copy of the current configuration to use as backup
C. Configure the Cisco FMCs for failover
D. Configure the Cisco FMC managed devices for clustering.

Answer: B

NEW QUESTION 28
- (Exam Topic 5)
An organization has seen a lot of traffic congestion on their links going out to the internet There is a Cisco Firepower device that processes all of the traffic going to the internet prior to leaving the enterprise. How is the congestion alleviated so that legitimate business traffic reaches the destination?

A. Create a flexconfig policy to use WCCP for application aware bandwidth limiting
B. Create a VPN policy so that direct tunnels are established to the business applications
C. Create a NAT policy so that the Cisco Firepower device does not have to translate as many addresses
D. Create a QoS policy rate-limiting high bandwidth applications

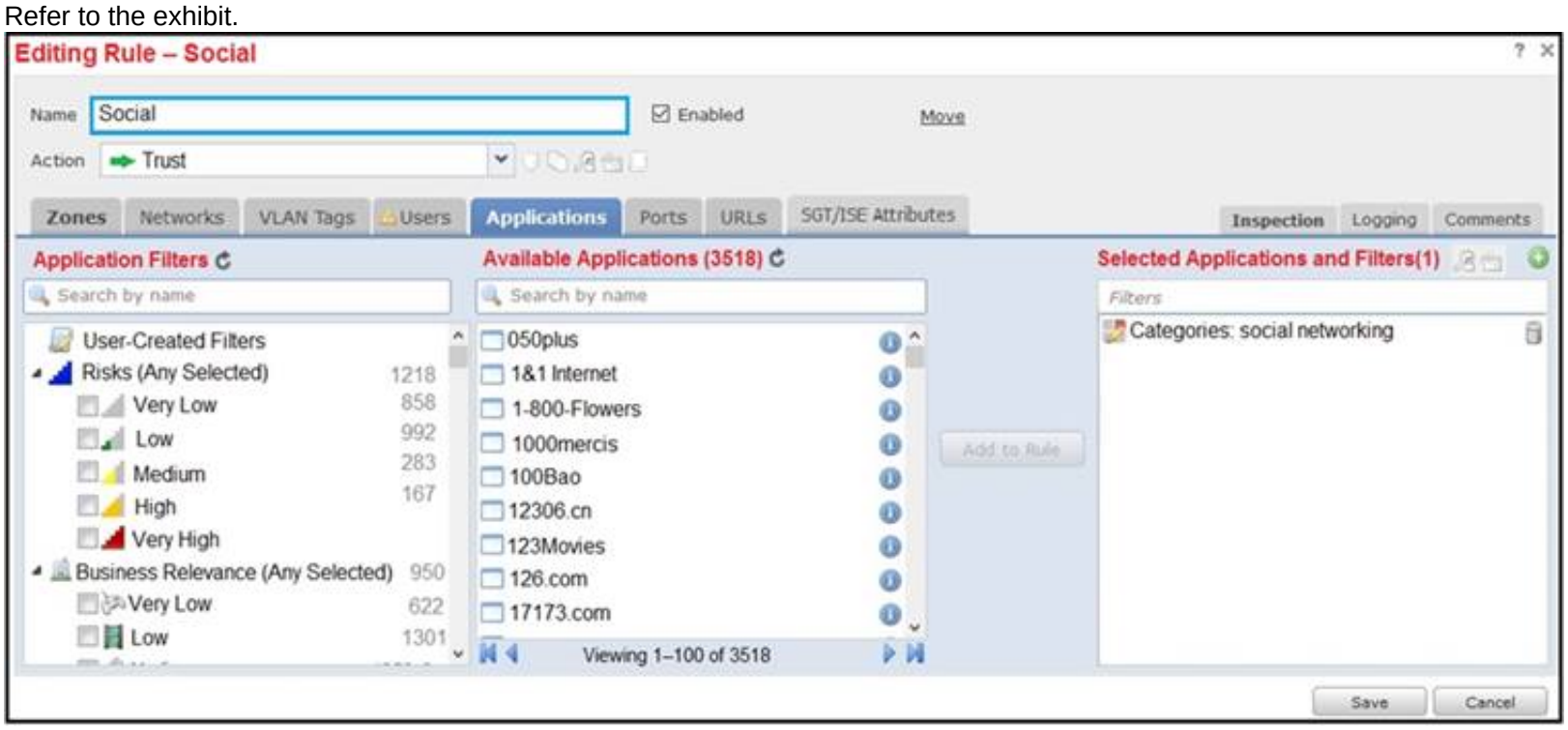
Answer: D

NEW QUESTION 33
- (Exam Topic 5)
An engineer must configure a Cisco FMC dashboard in a multidomain deployment Which action must the engineer take to edit a report template from an ancestor domain?

A. Add it as a separate widget.
B. Copy it to the current domain
C. Assign themselves ownership of it
D. Change the document attributes.

Answer: B

NEW QUESTION 36
- (Exam Topic 5)
Refer to the exhibit.



An organization has an access control rule with the intention of sending all social media traffic for inspection After using the rule for some time, the administrator notices that the traffic is not being inspected, but is being automatically allowed What must be done to address this issue?

A. Modify the selected application within the rule
B. Change the intrusion policy to connectivity over security.
C. Modify the rule action from trust to allow
D. Add the social network URLs to the block list

Answer: A

NEW QUESTION 39
- (Exam Topic 5)
A network administrator has converted a Cisco FTD from using LDAP to LDAPS for VPN authentication. The Cisco FMC can connect to the LDAPS server, but the Cisco FTD is not connecting. Which configuration must be enabled on the Cisco FTD?

A. SSL must be set to a use TLSv1.2 or lower.
B. The LDAPS must be allowed through the access control policy.
C. DNS servers must be defined for name resolution.
D. The RADIUS server must be defined.

Answer: B

NEW QUESTION 42

- (Exam Topic 5)
A network administrator notices that inspection has been interrupted on all non-managed interfaces of a device. What is the cause of this?

A. The value of the highest MTU assigned to any non-management interface was changed.
B. The value of the highest MSS assigned to any non-management interface was changed.
C. A passive interface was associated with a security zone.
D. Multiple inline interface pairs were added to the same inline interface.

Answer: A

NEW QUESTION 44
- (Exam Topic 5)
An administrator is adding a new URL-based category feed to the Cisco FMC for use within the policies. The intelligence source does not use STIX. but instead uses a .txt file format. Which action ensures that regular updates are provided?

A. Add a URL source and select the flat file type within Cisco FMC.
B. Upload the .txt file and configure automatic updates using the embedded URL.
C. Add a TAXII feed source and input the URL for the feed.
D. Convert the .txt file to STIX and upload it to the Cisco FMC.

Answer: A

NEW QUESTION 47
- (Exam Topic 5)
A network administrator is configuring a Cisco AMP public cloud instance and wants to capture infections and polymorphic variants of a threat to help detect families of malware. Which detection engine meets this requirement?

A. RBAC
B. Tetra
C. Ethos
D. Spero

Answer: C

NEW QUESTION 48
- (Exam Topic 5)
A network engineer must provide redundancy between two Cisco FTD devices. The redundancy configuration must include automatic configuration, translation, and connection updates. After the initial configuration of the two appliances, which two steps must be taken to proceed with the redundancy configuration? (Choose two.)

A. Configure the virtual MAC address on the failover link.
B. Disable hellos on the inside interface.
C. Configure the standby IP addresses.
D. Ensure the high availability license is enabled.
E. Configure the failover link with stateful properties.

Answer: AC

NEW QUESTION 50
- (Exam Topic 5)
A network engineer is extending a user segment through an FTD device for traffic inspection without creating another IP subnet How is this accomplished on an FTD device in routed mode?

A. by leveraging the ARP to direct traffic through the firewall
B. by assigning an inline set interface
C. by using a BVI and create a BVI IP address in the same subnet as the user segment
D. by bypassing protocol inspection by leveraging pre-filter rules

Answer: C

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/trans

NEW QUESTION 55
- (Exam Topic 5)
In a multi-tennent deployment where multiple domains are in use. which update should be applied outside of the Global Domain?

A. minor upgrade
B. local import of intrusion rules
C. Cisco Geolocation Database
D. local import of major upgrade

Answer: B

NEW QUESTION 59
- (Exam Topic 5)
With Cisco FTD software, which interface mode must be configured to passively receive traffic that passes through the appliance?

A. ERSPAN
B. IPS-only
C. firewall
D. tap

Answer: A

NEW QUESTION 62
- (Exam Topic 5)
Refer to the exhibit.

```
Phase: 16
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Firewall: starting rule matching, zone 4 -> 1, geo 0 -> 0, vlan 0, sgt 0, src sgt type 0, dest_sgt_tag 0, dest sgt type 0, username 'No Authentication Required', , icmpType 8, icmpCode 0
Firewall: block rule, 'Ping' , drop
Snort: processed decoder alerts or actions queue, drop
Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST, Blocked by Firewall
Snort Verdict: (black-list) black list this flow

Result:
input-interface: ACCESS41_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame 0x000055d2b0f8b7e0 flow (NA)/NA
```

A systems administrator conducts a connectivity test to their SCCM server from a host machine and gets no response from the server. Which action ensures that the ping packets reach the destination and that the host receives replies?

A. Create an access control policy rule that allows ICMP traffic.
B. Configure a custom Snort signature to allow ICMP traffic after Inspection.
C. Modify the Snort rules to allow ICMP traffic.
D. Create an ICMP allow list and add the ICMP destination to remove it from the implicit deny list.

Answer: A

NEW QUESTION 65
- (Exam Topic 5)
A network administrator is migrating from a Cisco ASA to a Cisco FTD. EIGRP is configured on the Cisco ASA but it is not available in the Cisco FMC.
Which action must the administrator take to enable this feature on the Cisco FTD?

A. Configure EIGRP parameters using FlexConfig objects.
B. Add the command feature eigrp via the FTD CLI.
C. Create a custom variable set and enable the feature in the variable set.
D. Enable advanced configuration options in the FMC.

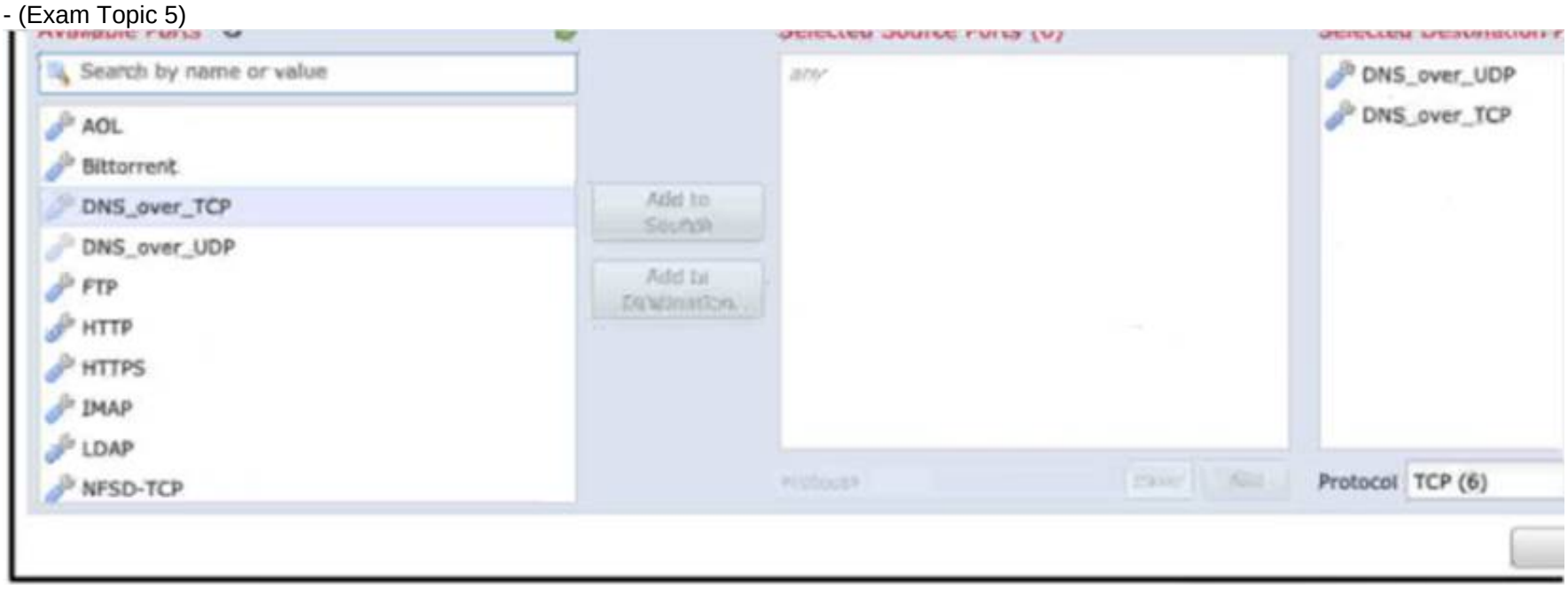
Answer: A

NEW QUESTION 67
- (Exam Topic 5)
An engineer is implementing Cisco FTD in the network and is determining which Firepower mode to use. The organization needs to have multiple virtual Firepower devices working separately inside of the FTD appliance to provide traffic segmentation Which deployment mode should be configured in the Cisco Firepower Management Console to support these requirements?

A. multiple deployment
B. single-context
C. single deployment
D. multi-instance

Answer: D

NEW QUESTION 71
- (Exam Topic 5)



Refer to the exhibit An engineer is modifying an access control pokey to add a rule to inspect all DNS traffic that passes through the firewall After making the change and deploying the pokey they see that DNS traffic is not bang inspected by the Snort engine What is the problem?

A. The rule must specify the security zone that originates the traffic
B. The rule must define the source network for inspection as well as the port
C. The action of the rule is set to trust instead of allow.
D. The rule is configured with the wrong setting for the source port

Answer: C

NEW QUESTION 75
- (Exam Topic 5)
Which two routing options are valid with Cisco FTD? (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

Answer: AC

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config- guide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

NEW QUESTION 76
- (Exam Topic 5)
An organization has noticed that malware was downloaded from a website that does not currently have a known bad reputation. How will this issue be addresses globally in the quickest way possible and with the least amount of impact?

A. by denying outbound web access
B. Cisco Talos will automatically update the policies.
C. by Isolating the endpoint
D. by creating a URL object in the policy to block the website

Answer: D

NEW QUESTION 81
- (Exam Topic 5)
An engineer must investigate a connectivity issue and decides to use the packet capture feature on Cisco FTD. The goal is to see the real packet going through the Cisco FTD device and see the Snort detection actions as a part of the output. After the capture-traffic command is issued, only the packets are displayed. Which action resolves this issue?

A. Use the verbose option as a part of the capture-traffic command
B. Use the capture command and specify the trace option to get the required information.
C. Specify the trace using the -T option after the capture-traffic command.
D. Perform the trace within the Cisco FMC GUI instead of the Cisco FTD CLI.

Answer: B

NEW QUESTION 84
- (Exam Topic 5)
What is the RTC workflow when the infected endpoint is identified?

A. Cisco ISE instructs Cisco AMP to contain the infected endpoint.
B. Cisco ISE instructs Cisco FMC to contain the infected endpoint.
C. Cisco AMP instructs Cisco FMC to contain the infected endpoint.
D. Cisco FMC instructs Cisco ISE to contain the infected endpoint.

Answer: D

NEW QUESTION 89
- (Exam Topic 5)
An engineer has been asked to show application usages automatically on a monthly basis and send the information to management What mechanism should be used to accomplish this task?

A. event viewer
B. reports
C. dashboards
D. context explorer

Answer: B

NEW QUESTION 91
- (Exam Topic 4)
What is a valid Cisco AMP file disposition?

A. non-malicious
B. malware
C. known-good
D. pristine

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Reference_a_wrapper_Chapter_topic_here.html

NEW QUESTION 96
- (Exam Topic 4)
Which action should you take when Cisco Threat Response notifies you that AMP has identified a file as malware?

A. Add the malicious file to the block list.
B. Send a snapshot to Cisco for technical support.
C. Forward the result of the investigation to an external threat-analysis engine.
D. Wait for Cisco Threat Response to automatically block the malware.

Answer: A

NEW QUESTION 100
- (Exam Topic 5)
An engineer must define a URL object on Cisco FMC. What is the correct method to specify the URL without performing SSL inspection?

A. Use Subject Common Name value.
B. Specify all subdomains in the object group.
C. Specify the protocol in the object.
D. Include all URLs from CRL Distribution Points.

Answer: B

NEW QUESTION 103
- (Exam Topic 3)
How many report templates does the Cisco Firepower Management Center support?

A. 20
B. 10
C. 5
D. unlimited

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Working_with_Reports.html

NEW QUESTION 108
- (Exam Topic 3)
Within Cisco Firepower Management Center, where does a user add or modify widgets?

A. dashboard
B. reporting
C. context explorer
D. summary tool

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Using_Dashboards.html

NEW QUESTION 109
- (Exam Topic 3)
Which command must be run to generate troubleshooting files on an FTD?

A. system support view-files
B. sudo sf_troubleshoot.pl
C. system generate-troubleshoot all
D. show tech-support

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote- SourceFire-00.html

NEW QUESTION 110
- (Exam Topic 4)
In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

A. unavailable
B. unknown
C. clean
D. disconnected

Answer: A

NEW QUESTION 111
- (Exam Topic 4)
Which two features of Cisco AMP for Endpoints allow for an uploaded file to be blocked? (Choose two.)

A. application blocking
B. simple custom detection
C. file repository
D. exclusions
E. application whitelisting

Answer: AB

NEW QUESTION 113
- (Exam Topic 3)
Which limitation applies to Cisco Firepower Management Center dashboards in a multidomain environment?

A. Child domains can view but not edit dashboards that originate from an ancestor domain.
B. Child domains have access to only a limited set of widgets from ancestor domains.
C. Only the administrator of the top ancestor domain can view dashboards.
D. Child domains cannot view dashboards that originate from an ancestor domain.

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Using_Dashboards.html

NEW QUESTION 114
- (Exam Topic 3)
Which group within Cisco does the Threat Response team use for threat analysis and research?

A. Cisco Deep Analytics
B. OpenDNS Group
C. Cisco Network Response
D. Cisco Talos

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits

NEW QUESTION 118
- (Exam Topic 3)
Which CLI command is used to control special handling of ClientHello messages?

A. system support ssl-client-hello-tuning
B. system support ssl-client-hello-display
C. system support ssl-client-hello-force-reset
D. system support ssl-client-hello-enabled

Answer: A

NEW QUESTION 120
- (Exam Topic 3)
Which Cisco Firepower feature is used to reduce the number of events received in a period of time?

A. rate-limiting
B. suspending
C. correlation
D. thresholding

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa- firepower-module-user-guide-v541/Intrusion-Global-Threshold.html

NEW QUESTION 124
- (Exam Topic 3)
What is a behavior of a Cisco FMC database purge?

A. User login and history data are removed from the database if the User Activity check box is selected.
B. Data can be recovered from the device.
C. The appropriate process is restarted.
D. The specified data is removed from Cisco FMC and kept for two weeks.

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/management_center_database_purge.pdf

NEW QUESTION 127
- (Exam Topic 3)
Which command-line mode is supported from the Cisco Firepower Management Center CLI?

A. privileged
B. user
C. configuration
D. admin

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config- guide-v66/command_line_reference.pdf

NEW QUESTION 130
- (Exam Topic 2)
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.

Answer: A

NEW QUESTION 131
- (Exam Topic 2)
Which Cisco Firepower rule action displays an HTTP warning page?

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

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System- UserGuide-v5401/AC-Rules-Tuning-Overview.html#76698

NEW QUESTION 133
- (Exam Topic 2)
What is the disadvantage of setting up a site-to-site VPN in a clustered-units environment?

A. VPN connections can be re-established only if the failed master unit recovers.
B. Smart License is required to maintain VPN connections simultaneously across all cluster units.
C. VPN connections must be re-established when a new master unit is elected.
D. Only established VPN connections are maintained when a new master unit is elected.

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster- solution.html#concept_g32_yml_y2b

NEW QUESTION 137
- (Exam Topic 2)
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

Answer: BC

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/reusable_objects.html#ID-2243-00000414

NEW QUESTION 139
- (Exam Topic 1)
On the advanced tab under inline set properties, which allows interfaces to emulate a passive interface?

A. transparent inline mode
B. TAP mode
C. strict TCP enforcement
D. propagate link state

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config- guide-v64/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

NEW QUESTION 140
- (Exam Topic 1)
Which firewall design allows a firewall to forward traffic at layer 2 and layer 3 for the same subnet?

A. Cisco Firepower Threat Defense mode
B. transparent mode
C. routed mode
D. integrated routing and bridging

Answer: B

NEW QUESTION 143
- (Exam Topic 1)
Within an organization's high availability environment where both firewalls are passing traffic, traffic must be segmented based on which department it is destined for. Each department is situated on a different LAN. What must be configured to meet these requirements?

A. span EtherChannel clustering
B. redundant interfaces
C. high availability active/standby firewalls
D. multi-instance firewalls

Answer: D

NEW QUESTION 146
- (Exam Topic 1)
A network security engineer must replace a faulty Cisco FTD device in a high availability pair. Which action must be taken while replacing the faulty unit?

A. Shut down the Cisco FMC before powering up the replacement unit.
B. Ensure that the faulty Cisco FTD device remains registered to the Cisco FMC.
C. Unregister the faulty Cisco FTD device from the Cisco FMC
D. Shut down the active Cisco FTD device before powering up the replacement unit.

Answer: C

NEW QUESTION 147
- (Exam Topic 1)
Which Cisco Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two.)

A. Redundant Interface
B. EtherChannel
C. Speed
D. Media Type
E. Duplex

Answer: CE

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm- interfaces.html

NEW QUESTION 149

- (Exam Topic 1)
What are two application layer preprocessors? (Choose two.)

A. CIFS
B. IMAP
C. SSL
D. DNP3
E. ICMP

Answer: BC

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Applic

NEW QUESTION 152
- (Exam Topic 1)
Which protocol establishes network redundancy in a switched Firepower device deployment?

A. STP
B. HSRP
C. GLBP
D. VRRP

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/firepower_threat_defense_high_availability.html

NEW QUESTION 156
- (Exam Topic 1)
When deploying a Cisco ASA Firepower module, an organization wants to evaluate the contents of the traffic without affecting the network. It is currently configured to have more than one instance of the same device on the physical appliance Which deployment mode meets the needs of the organization?

A. inline tap monitor-only mode
B. passive monitor-only mode
C. passive tap monitor-only mode
D. inline mode

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config/access Inline tap monitor-only mode (ASA inline)—In an inline tap monitor-only deployment, a copy of the traffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode lets you see what the ASA FirePOWER module would have done to traffic, and lets you evaluate the content of the traffic, without impacting the network. However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.

NEW QUESTION 157
- (Exam Topic 1)
What are the minimum requirements to deploy a managed device inline?

A. inline interfaces, security zones, MTU, and mode
B. passive interface, MTU, and mode
C. inline interfaces, MTU, and mode
D. passive interface, security zone, MTU, and mode

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config- guide-v65/ips_device_deployments_and_configuration.html

NEW QUESTION 161
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 300-710 Exam with Our Prep Materials Via below:

https://www.certleader.com/300-710-dumps.html