300-710 Q&As

Securing Networks with Cisco Firepower (SNCF)

Pass Cisco 300-710 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/300-710.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A security engineer found a suspicious file from an employee email address and is trying to upload it for analysis, however the upload is failing. The last registration status is still active. What is the cause for this issue?

A. Cisco AMP for Networks is unable to contact Cisco Threat Grid on premise.

B. Cisco AMP for Networks is unable to contact Cisco Threat Grid Cloud.

C. There is a host limit set.

D. The user agent status is set to monitor.

Correct Answer: B

QUESTION 2

Which firewall design will allow it to forward traffic at layers 2 and 3 for the same subnet?

A. routed mode

B. Cisco Firepower Threat Defense mode

C. transparent mode

D. integrated routing and bridging

Correct Answer: D

QUESTION 3

An engineer is troubleshooting a file that is being blocked by a Cisco FTD device on the network. The user is reporting that the file is not malicious. Which action does the engineer take to identify the file and validate whether or not it is malicious?

A. Identify the file in the intrusion events and submit it to Threat Grid for analysis.

B. Use FMC file analysis to look for the file and select Analyze to determine its disposition.

C. Use the context explorer to find the file and download it to the local machine for investigation.

D. Right click the connection event and send the file to AMP for Endpoints to see if the hash is malicious.

Correct Answer: B

QUESTION 4

When using Cisco Threat Response, which phase of the Intelligence Cycle publishes the results of the investigation?

A. direction

B. dissemination

C. processing

D. analysis

Correct Answer: B

Explanation: Disseminate: The dissemination phase publishes the results of the investigation or threat hunt. This information is disseminated with a focus on the receivers of the information. At the tactical level, this information feeds back into the beginning of the F3EAD model, Find. Figure 3 illustrates the F3EAD model.

QUESTION 5

An engineer is using the configure manager add Cisc404225383 command to add a new Cisco FTD device to the Cisco FMC; however, the device is not being added. Why is this occurring?

A. DONOTRESOLVE must be added to the command

B. The IP address used should be that of the Cisco FTD, not the Cisco FMC

C. The registration key is missing from the command

D. The NAT ID is required since the Cisco FMC is behind a NAT device

Correct Answer: C

QUESTION 6

What is the result of specifying of QoS rule that has a rate limit that is greater than the maximum throughput of an interface?

A. The rate-limiting rule is disabled.

B. Matching traffic is not rate limited.

C. The system rate-limits all traffic.

D. The system repeatedly generates warnings.

Correct Answer: B

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

v62/quality_of_service_qos.pdf

QUESTION 7

Which Cisco AMP for Endpoints policy is used only for monitoring endpoint activity?

A. Windows domain controller

B. audit

C. triage

D. protection

Correct Answer: B

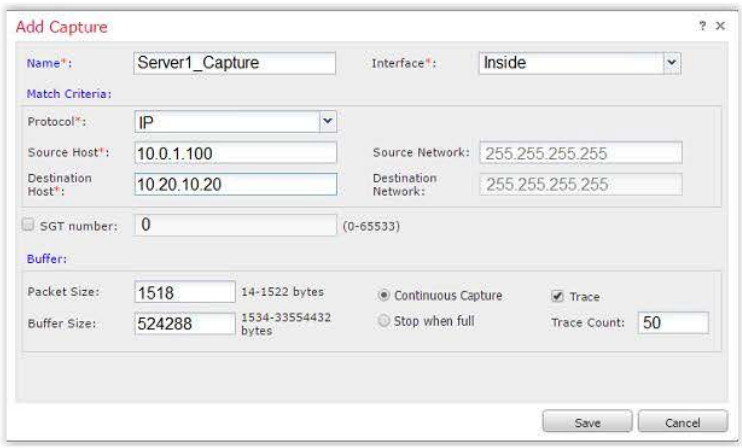
Reference: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214933-amp-for-endpoints-deployment-methodology.html

QUESTION 8

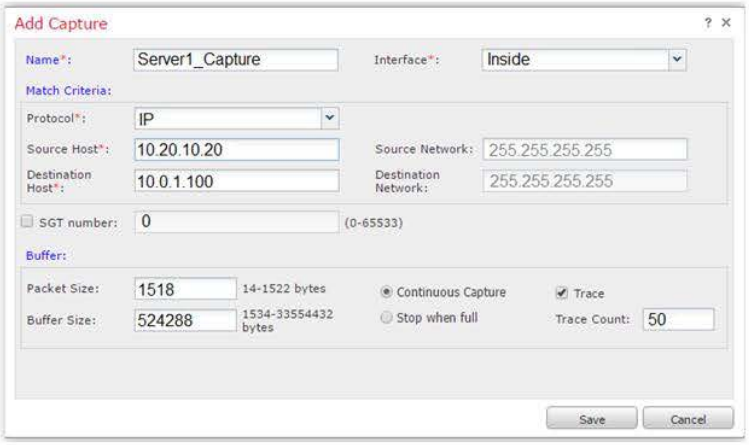
An engineer is troubleshooting a device that cannot connect to a web server. The connection is initiated from the Cisco FTD inside interface and attempting to reach 10.0.1.100 over the non-standard port of 9443. The host the engineer is attempting the connection from is at the IP address of 10.20.10.20. 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 the issue?

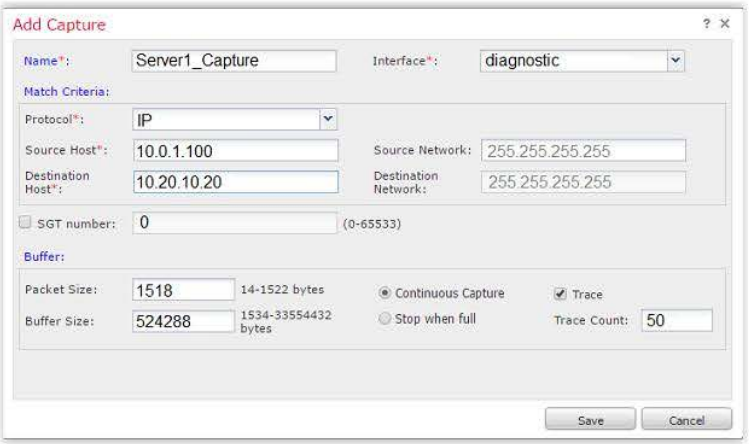
A.


Add Capture
Name*: Server1_Capture
Interface*: Inside
Match Criteria:
Protocol*: IP
Source Host*: 10.0.1.100
Source Network: 255.255.255.255
Destination Host*: 10.20.10.20
Destination Network: 255.255.255.255
SGT number: 0
(0-65533)
Buffer:
Packet Size: 1518
14-1522 bytes
Continuous Capture
Trace
Buffer Size: 524288
1534-33554432 bytes
Stop when full
Trace Count: 50
Save
Cancel

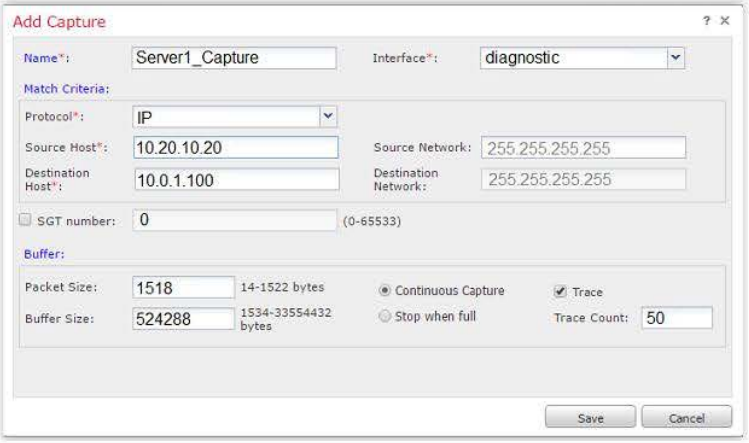
B.


Add Capture
Name*: Server1_Capture
Interface*: Inside
Match Criteria:
Protocol*: IP
Source Host*: 10.20.10.20
Source Network: 255.255.255.255
Destination Host*: 10.0.1.100
Destination Network: 255.255.255.255
SGT number: 0
(0-65533)
Buffer:
Packet Size: 1518
14-1522 bytes
Continuous Capture
Trace
Buffer Size: 524288
1534-33554432 bytes
Stop when full
Trace Count: 50
Save
Cancel

C.


Add Capture
Name*: Server1_Capture
Interface*: diagnostic
Match Criteria:
Protocol*: IP
Source Host*: 10.0.1.100
Source Network: 255.255.255.255
Destination Host*: 10.20.10.20
Destination Network: 255.255.255.255
SGT number: 0
(0-65533)
Buffer:
Packet Size: 1518
14-1522 bytes
Continuous Capture
Trace
Buffer Size: 524288
1534-33554432 bytes
Stop when full
Trace Count: 50
Save
Cancel

D.


Add Capture
Name*: Server1_Capture
Interface*: diagnostic
Match Criteria:
Protocol*: IP
Source Host*: 10.20.10.20
Source Network: 255.255.255.255
Destination Host*: 10.0.1.100
Destination Network: 255.255.255.255
SGT number: 0
(0-65533)
Buffer:
Packet Size: 1518
14-1522 bytes
Continuous Capture
Trace
Buffer Size: 524288
1534-33554432 bytes
Stop when full
Trace Count: 50
Save
Cancel

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

QUESTION 9

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 the same FQDN for both chassis.

B. Set up a virtual failover MAC address between chassis.

C. Load the same software version on both chassis.

D. Use a dedicated stateful link between chassis.

Correct Answer: D

QUESTION 10

Which limitation applies to Cisco FMC dashboards in a multi-domain environment?

A. Child domains are able to 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 is able to view dashboards.

D. Child domains are not able to view dashboards that originate from an ancestor domain.

Correct Answer: D

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

QUESTION 11

While integrating Cisco Umbrella with Cisco Threat Response, a network security engineer wants to automatically push blocking of domains from the Cisco Threat Response interface to Cisco Umbrella. Which API meets this requirement?

A. investigate

B. reporting

C. enforcement

D. REST

Correct Answer: C

QUESTION 12

Which function is the primary function of Cisco AMP threat Grid?

A. It analyzes copies of packets from the packet flow

B. The device is deployed in a passive configuration

C. If a rule is triggered the device generates an intrusion event.

D. The packet flow traverses the device

E. If a rule is triggered the device drops the packet

Correct Answer: AC

QUESTION 13

A company is in the process of deploying intrusion protection with Cisco FTDs managed by a Cisco FMC. Which action must be selected to enable fewer rules detect only critical conditions and avoid false positives?

A. Connectivity Over Security

B. Balanced Security and Connectivity

C. Maximum Detection

D. No Rules Active

Correct Answer: A