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.leads4pass.com/300-710.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An engineer is implementing a new Cisco Secure Firewall. The firewall must filler traffic between the three subnets:

1.

LAN 192.168.101.0724

2.

DMZ 192.168 200.0/24

3.

WAN 10.0.0.0/30

Which firewall mode must the engineer implement?

A. transparent

B. network

C. routed

D. gateway

Correct Answer: C

To filter traffic between multiple subnets, the engineer must implement the firewall in routed mode. In routed mode, the firewall operates as a Layer 3 device, capable of routing traffic between different IP subnets. This mode is appropriate for

filtering traffic between LAN, DMZ, and WAN subnets.

Steps to configure routed mode:

Access the firewall\\'s management interface.

Configure interfaces for each subnet (LAN, DMZ, WAN) with appropriate IP addresses and network masks.

Define security zones and apply access control policies to filter traffic as required. This ensures that the firewall can inspect and route traffic between the different subnets, providing the necessary security and control.

References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Routed Mode Configuration.

QUESTION 2

A network engineer is tasked with minimising traffic interruption during peak traffic limes. When the SNORT inspection engine is overwhelmed, what must be configured to alleviate this issue?

A. Enable IPS inline link state propagation

B. Enable Pre-filter policies before the SNORT engine failure.

C. Set a Trust ALL access control policy.

D. Enable Automatic Application Bypass.

Correct Answer: D

QUESTION 3

A network administrator notices that remote access VPN users are not reachable from inside the network. It is determined that routing is configured correctly, however return traffic is entering the firewall but not leaving it What is the reason for this issue?

A. A manual NAT exemption rule does not exist at the top of the NAT table.

B. An external NAT IP address is not configured.

C. An external NAT IP address is configured to match the wrong interface.

D. An object NAT exemption rule does not exist at the top of the NAT table.

Correct Answer: A

https://www.cisco.com/c/en/us/support/docs/security/firepower-management- center/212702-configure-and-verify-nat-on-ftd.html

QUESTION 4

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 5

Which two dynamic routing protocols are supported in FirePower Threat Defense v6.0? (Choose Two)

A. IS-IS

B. BGP

C. OSPF

D. static routing

E. EIGRP

Correct Answer: BC

QUESTION 6

An engineer is troubleshooting connectivity to the DNS servers from hosts behind a new Cisco FTD device. The hosts cannot send DNS queries to servers in the DMZ. Which action should the engineer take to troubleshoot this issue using the real DNS packets?

A. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion policy as needed

B. Use the Connection Events dashboard to check the block reason and adjust the inspection policy as needed

C. Use the packet tracer tool to determine at which hop the packet is being dropped

D. Use the show blocks command in the Threat Defense CLI tool and create a policy to allow the blocked traffic

Correct Answer: A

QUESTION 7

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. FTD has no NAT policy that allows outside to outside communication.

B. Split tunneling is enabled for the Remote Access VPN on FTD.

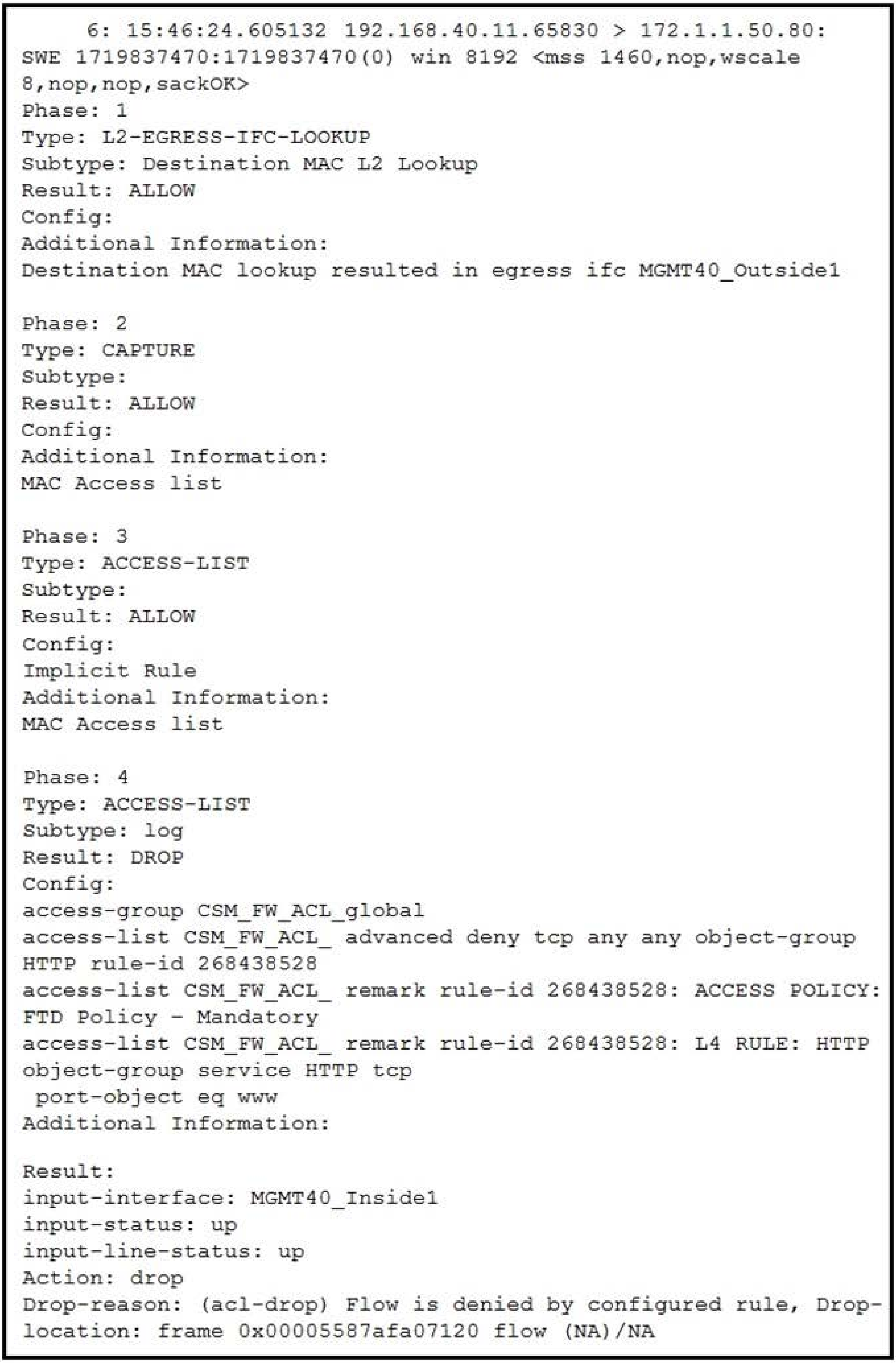
C. The hairpinning feature is not available on FTD.

D. The Enable Spoke to Spoke Connectivity through Hub option is not selected on FTD.

Correct Answer: A

QUESTION 8

Refer to the exhibit.



```
     6: 15:46:24.605132 192.168.40.11.65830 > 172.1.1.50.80:
SWE 1719837470:1719837470(0) win 8192 <mss 1460,nop,wscale
8,nop,nop,sackOK>
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC lookup resulted in egress ifc MGMT40_Outside1

Phase: 2
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_ advanced deny tcp any any object-group
HTTP rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY:
FTD Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: HTTP
object-group service HTTP tcp
 port-object eq www
Additional Information:

Result:
input-interface: MGMT40_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-
location: frame 0x00005587afa07120 flow (NA)/NA
```

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

Correct Answer: B

QUESTION 9

A security engineer must deploy a Cisco FTD appliance as a bump in the wire to detect intrusion events without disrupting the flow of network traffic. Which two features must be configured to accomplish the task? (Choose two.)

A. inline set pair

B. transparent mode

C. tap mode

D. passive interfaces

E. bridged mode

Correct Answer: AC

QUESTION 10

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.

Correct Answer: D

QUESTION 11

What is a limitation to consider when running a dynamic routing protocol on a Cisco FTD device in IRB mode?

A. Only link-stale routing protocols are supported.

B. Only distance vector routing protocols are supported.

C. Only EtherChannel interfaces are supposed.

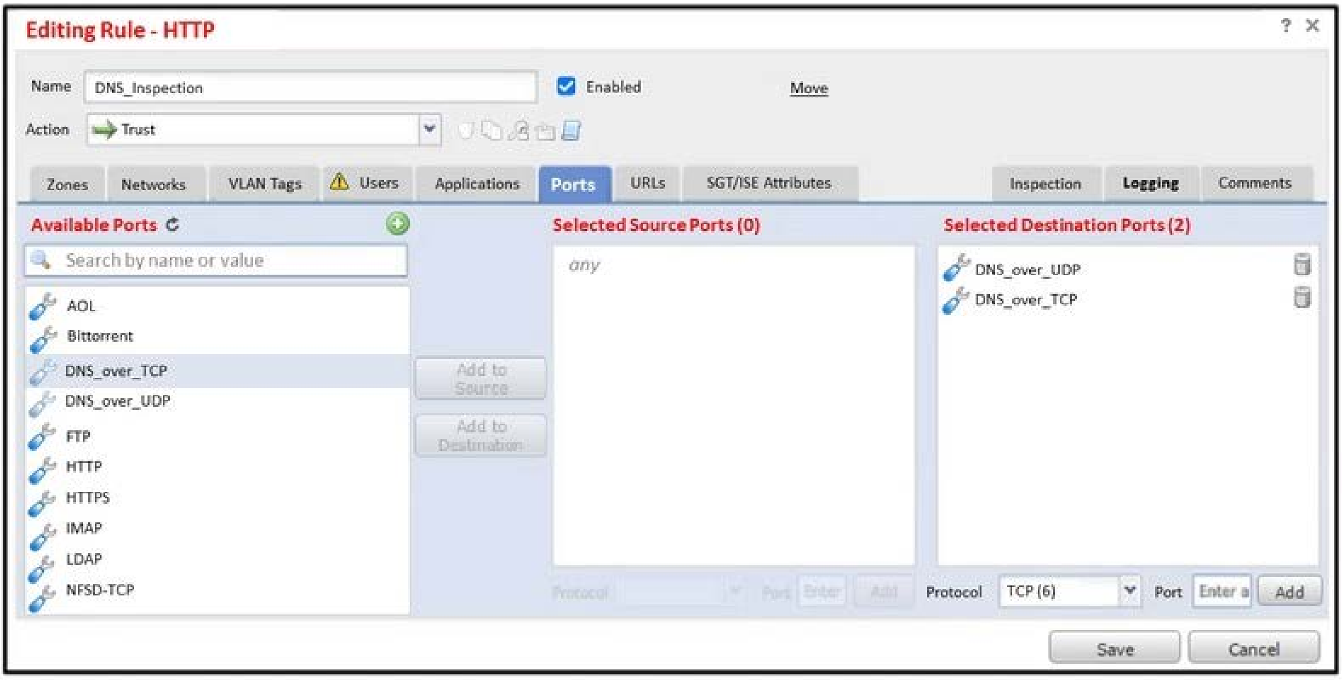
D. Only nonbridge interfaces are supported.

Correct Answer: D

Integrated routing and bridging (IRB) is a feature that allows you to route between different bridge groups on a Cisco FTD device. A bridge group is a logical interface that acts as a container for one or more physical or logical interfaces that belong to the same layer 2 broadcast domain. You can assign an IP address to a bridge group interface (BVI) and enable routing protocols on it, just like a regular routed interface. However, when you run a dynamic routing protocol on a Cisco FTD device in IRB mode, you can only use nonbridge interfaces as routing peers. You cannot use bridge group interfaces or bridge group member interfaces as routing peers2. This is because the routing protocol packets are sent and received on the nonbridge interfaces, and the bridge group interfaces are used only for forwarding data traffic3.

QUESTION 12

Refer to the exhibit



Editing Rule - HTTP

Name: DNS_Inspection

☑ Enabled

Action: Trust

Selected Source Ports (0)

any

Selected Destination Ports (2)

DNS_over_UDP

DNS_over_TCP

Protocol: TCP (6)

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 Is configured with the wrong setting for the source port.

C. The rule must define the source network for inspection as well as the port.

D. The action of the rule is set to trust instead of allow.

Correct Answer: D

QUESTION 13

The event dashboard within the Cisco FMC has been inundated with low priority intrusion drop events, which are overshadowing high priority events. An engineer has been tasked with reviewing the policies and reducing the low priority events. Which action should be configured to accomplish this task?

A. drop packet

B. generate events

C. drop connection

D. drop and generate

Correct Answer: A

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

QUESTION 14

A network engineer must configure IPS mode on a Secure Firewall Threat Defense device to inspect traffic and act as an IDS. The engineer already configured the passive-interface on the Secure Firewall Threat Defense device and SPAN on the switch. What must be configured next by the engineer?

A. intrusion policy on the Secure Firewall Threat Defense device

B. active SPAN port on the switch

C. DHCP on the switch

D. active interface on the Secure Firewall Threat Defense device

Correct Answer: A

To configure IPS mode on a Cisco Secure Firewall Threat Defense (FTD) device to inspect traffic and act as an IDS, the network engineer must configure an intrusion policy on the FTD device. The passive-interface and SPAN on the switch

have already been configured, which means the traffic is being mirrored to the FTD. The next step is to set up an intrusion policy that defines the rules and actions for detecting and responding to malicious traffic.

Steps:

In FMC, navigate to Policies > Intrusion.

Create a new intrusion policy or edit an existing one. Define the rules and actions for detecting threats. Apply the intrusion policy to the relevant interfaces or access control policies. This configuration enables the FTD to inspect the mirrored

traffic and take appropriate actions based on the defined intrusion policy.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Intrusion Policies.

QUESTION 15

Which command should be used on the Cisco FTD CLI to capture all the packets that hit an interface?

A. configure coredump packet-engine enable

B. capture-traffic

C. capture

D. capture WORD

Correct Answer: C