Free Questions for 300-730 by dumpssheet

Shared by Sosa on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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 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?

Options:

A- Specify the trace using the -T option after the capture-traffic command

B- Perform the trace within the Cisco FMC GUI instead of the Cisco FMC CLI

C- Use the verbose option as a part of the capture-traffic command

D- Use the capture command and specify the trace option to get the required information

B) Performing the trace within the Cisco FMC GUI instead of the Cisco FMC CLI is not a valid option, because the FMC GUI does not support packet capture or tracing on the FTD device. You can only use the FMC GUI to view and export captures that are taken on the FTD CLI1.

C) Using the verbose option as a part of the capture-traffic command is not a valid option, because there is no verbose option for this command. The verbose option is only available for the capture command, which is used to capture packets on the LINA engine domain of the FTD device1.

D) Using the capture command and specifying the trace option to get the required information is not a valid option, because the capture command does not have a trace option. The capture command allows you to capture packets on the LINA engine domain of the FTD

device, but it does not show the Snort detection actions. The trace option is only available for the packet-tracer command, which is used to simulate a packet going through the FTD device and show its processing steps1.

Answer:

A

Explanation:

The correct answer is A. Specify the trace using the -T option after the capture-traffic command. According to the document Use Firepower Threat Defense Captures and Packet Tracer, the capture-traffic command allows you to capture packets on the Snort engine domain of the FTD device. However, by default, it only shows the packet headers and does not include the Snort detection actions. To see the Snort detection actions, you need to use the -T option, which enables tracing. For example:

capture-traffic -T

This will show the packet headers along with the Snort verdicts, such as allow, block, or replace. You can also use other options to filter or save the capture output1.

Question 2

Question Type: MultipleChoice

A network administrator is deploying a Cisco IPS appliance and needs it to operate initially without affecting traffic flows. It must also collect data to provide a baseline of unwanted traffic before being reconfigured to drop it. Which Cisco IPS mode meets these requirements?

Options:

A- failsafe

B- inline tap

C- promiscuous

D- bypass

A) failsafe mode is a feature that determines how the appliance behaves when a hardware or software failure occurs. It does not affect the normal traffic flow or analysis3. B. inline tap mode is a variation of inline mode that allows the appliance to pass traffic without inspection in case of a power failure or a software crash. It does not allow the appliance to collect data without affecting traffic4. D. bypass mode is a feature that enables the appliance to bypass traffic without inspection when it is overloaded or under maintenance. It does not allow the appliance to analyze traffic and generate alerts.

1: How the Sensor Functions 2: Cisco ASA IPS Module Quick Start Guide 3: Failsafe Mode 4: Inline Tap Mode : Bypass Mode

Answer:

C

Explanation:

The correct answer is C. promiscuous mode. In promiscuous mode, the Cisco IPS appliance operates as a passive device that monitors a copy of the network traffic and analyzes it for malicious activity. The appliance does not affect the traffic flow, but it can generate alerts, logs, and reports based on the configured security policy. Promiscuous mode is useful for initial deployment and baseline analysis, as well as for monitoring low-risk segments of the network12.

Question 3

Question Type: **MultipleChoice**

Which two protocols does DMVPN leverage to build dynamic VPNs to multiple destinations? (Choose two.)

Options:

A- IKEv2

B- NHRP

C- mGRE

D- mBGP

E- GDOI

Answer:

B, C

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

```
<snip>
Tunnel Group: VPNPhone, Client Cert Auth Success.
WebVPN: CSD data not sent from client
http_remove_auth_handle(): handle 24 not found!
<snip>
```

A network administrator is setting up a phone VPN on a Cisco AS

Options:

A- The phone cannot connect and the error is presented in a debug on the Cisco ASA. Which action fixes this issue?

A- Enable web-deploy of the posture module so that the module can be downloaded from the Cisco ASA to an IP phone.

B- Configure the Cisco ASA to present an RSA certificate to the phone for authentication.

C- Disable Cisco Secure Desktop under the connection profile VPNPhone.

D- Install the posture module on the Cisco ASA.

Answer:

C

Explanation:

CSD and IP phones: Currently, IP phones do not support Cisco Secure Desktop (CSD) and do not connect when CSD is enabled for the tunnel group or globally in the ASA.

Question 5

Question Type: **MultipleChoice**

An engineer is implementing the FlexVPN solution on a Cisco IOS router. The router must only terminate VPN requests and must not initiate them. Additionally, the interface must support VPNs from other routers and Cisco AnyConnect connections. Which interface type must be configured to meet these requirements?

Options:

A- point-to-point GRE tunnel interface

B- multipoint GRE tunnel interface

C- static virtual tunnel interface

D- virtual template interface

Answer:

D

Explanation:

The correct interface type to meet these requirements is the virtual template interface. This interface allows for the creation of multiple virtual access interfaces, which can be used for various types of remote access VPN connections, including site-to-site and AnyConnect VPNs. The virtual template interface can be configured to terminate VPN requests from other routers and allow for dynamic creation of VPN sessions, while also supporting AnyConnect VPN connections.

Question 6

Question Type: MultipleChoice

Which command must be configured on the tunnel interface of a FlexVPN spoke to receive a dynamic IP address from the hub?

Options:

A- ip address negotiated

B- ip unnumbered

C- ip address dhcp

D- ip address pool

Answer:

A

Explanation:

https://integratingit.wordpress.com/2018/03/31/configuring-flexvpn-external-aaa-with-radius/

interface Tunnel0

ip address negotiated

tunnel source GigabitEthernet1

tunnel mode ipsec ipv4

tunnel destination 1.1.1.5

tunnel protection ipsec profile IPSEC_PROFILE

Question 7

Question Type: **MultipleChoice**

An administrator is setting up Cisco AnyConnect on a Cisco ASA with the requirement that AnyConnect automatically establishes a VPN when a company-owned laptop is connected to the internet outside of the corporate network. Which configuration meets these requirements?

Options:

A- SBL with user certificate authentication

B- TND with machine certificate authentication

C- SBL with machine certificate authentication

D- TND with user certificate authentication

Answer:

B

Explanation:

Trusted Network Detection (TND) gives you the ability to have AnyConnect automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network).
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect41/administration/guide/b_AnyConnect_Administrator_Guide_4-1/configure-vpn.html#id_100236

Question 8

Question Type: MultipleChoice

An engineer is requesting an SSL certificate for a VPN load-balancing cluster in which two Cisco ASAs provide clientless SSLVPN access. The FQDN that users will enter to access the clientless VPN is asa.example.com, and users will be redirected to either asa1.example.com or asa2.example.com. The cluster FQDN and individual Cisco ASAs FQDNs resolve to IP addresses 192.168.0.1, 192.168.0.2, and 192.168.0.3 respectively. The issued certificate must be able to be used to validate the identity of either ASA in the cluster without returning any certificate validation errors. Which fields must be included in the certificate to meet these requirements?

Options:

A- CN=*.example.com, SAN=asa.example.com

B- CN=192.168.0.1, SAN=asa1.example.com, asa2.example.com

C- CN=asa.example.com, SAN=asa.example.com, asa1.example.com, asa2.example.com

D- CN=192.168.0.1, SAN=192.168.0.1, 192.168.0.2, 192.168.0.3

Answer:

C

Explanation:

https://integratingit.wordpress.com/2020/03/14/asa-vpn-load-balancing/