

Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

<https://www.2passeasy.com/dumps/300-710/>



NEW QUESTION 1

- (Exam Topic 5)

An organization wants to secure traffic from their branch office to the headquarter building using Cisco Firepower devices, They want to ensure that their Cisco Firepower devices are not wasting resources on inspecting the VPN traffic. What must be done to meet these requirements?

- A. Configure the Cisco Firepower devices to ignore the VPN traffic using prefilter policies
- B. Enable a flexconfig policy to re-classify VPN traffic so that it no longer appears as interesting traffic
- C. Configure the Cisco Firepower devices to bypass the access control policies for VPN traffic.
- D. Tune the intrusion policies in order to allow the VPN traffic through without inspection

Answer: C

Explanation:

When you configure the Cisco Firepower devices to bypass the access control policies for VPN traffic, the devices will not inspect the VPN traffic and thus will not waste resources on it. This is the best option to ensure that the VPN traffic is not wasting resources on the Cisco Firepower devices.

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the>

NEW QUESTION 2

- (Exam Topic 5)

A user within an organization opened a malicious file on a workstation which in turn caused a ransomware attack on the network. What should be configured within the Cisco FMC to ensure the file is tested for viruses on a sandbox system?

- A. Capacity handling
- B. Local malware analysis
- C. Spere analysis
- D. Dynamic analysis

Answer: D

NEW QUESTION 3

- (Exam Topic 5)

A network administrator is trying to convert from LDAP to LDAPS for VPN user authentication on a Cisco FTD. Which action must be taken on the Cisco FTD objects to accomplish this task?

- A. Add a Key Chain object to acquire the LDAPS certificate.
- B. Create a Certificate Enrollment object to get the LDAPS certificate needed.
- C. Identify the LDAPS cipher suite and use a Cipher Suite List object to define the Cisco FTD connection requirements.
- D. Modify the Policy List object to define the session requirements for LDAPS.

Answer: B

NEW QUESTION 4

- (Exam Topic 5)

A network administrator is seeing an unknown verdict for a file detected by Cisco FTD. Which malware policy configuration option must be selected in order to further analyse the file in the Talos cloud?

- A. Spero analysis
- B. Malware analysis
- C. Dynamic analysis
- D. Sandbox analysis

Answer: B

NEW QUESTION 5

- (Exam Topic 5)

An engineer is monitoring network traffic from their sales and product development departments, which are on two separate networks What must be configured in order to maintain data privacy for both departments?

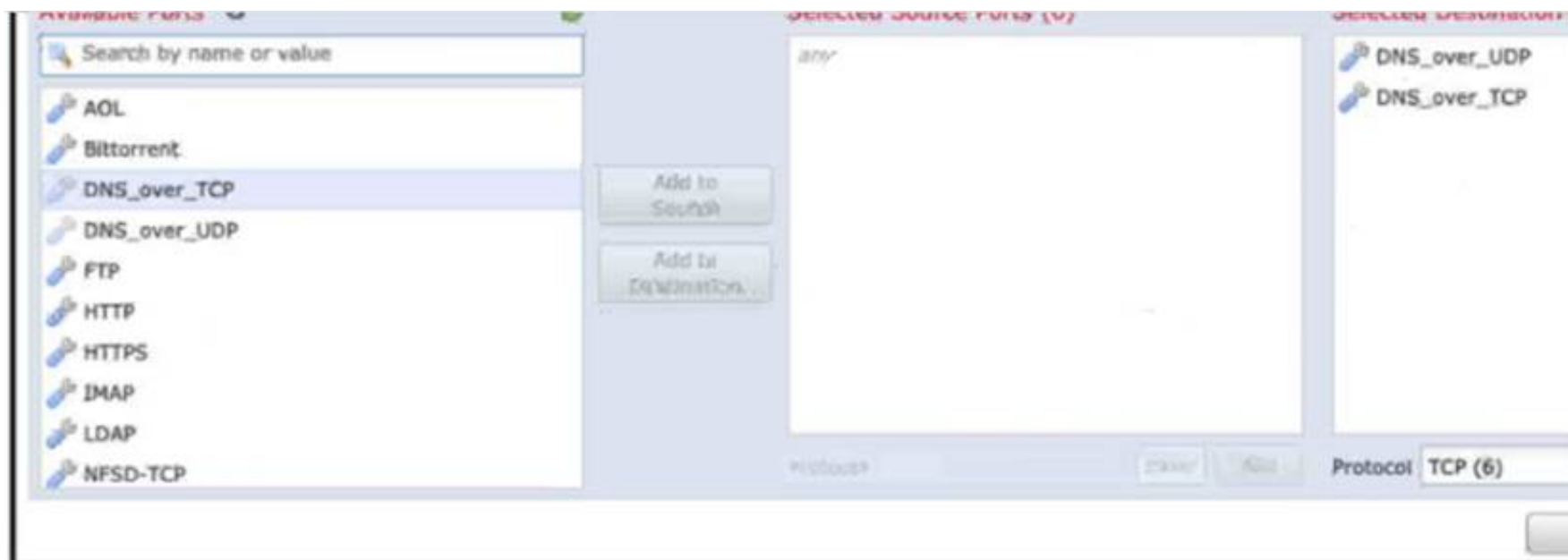
- A. Use a dedicated IPS inline set for each department to maintain traffic separation
- B. Use 802 1Q mime set Trunk interfaces with VLANs to maintain logical traffic separation
- C. Use passive IDS ports for both departments
- D. Use one pair of inline set in TAP mode for both departments

Answer: B

NEW QUESTION 6

- (Exam Topic 5)

Refer to the exhibit.



An engineer is modifying an access control policy to add a rule to inspect all DNS traffic that passes it making the change and deploying the policy, they see that DNS traffic is not being inspected by the Snort engine. What is.....

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

Answer: A

NEW QUESTION 7

- (Exam Topic 5)

A network administrator is implementing an active/passive high availability Cisco FTD pair. When adding the high availability pair, the administrator cannot select the secondary peer. What is the cause?

- A. The second Cisco FTD is not the same model as the primary Cisco FTD.
- B. An high availability license must be added to the Cisco FMC before adding the high availability pair.
- C. The failover link must be defined on each Cisco FTD before adding the high availability pair.
- D. Both Cisco FTD devices are not at the same software Version

Answer: A

NEW QUESTION 8

- (Exam Topic 5)

An engineer has been tasked with providing disaster recovery for an organization's primary Cisco FMC. What must be done on the primary and secondary Cisco FMCs to ensure that a copy of the original corporate policy is available if the primary Cisco FMC fails?

- A. Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device fails.
- B. Configure high-availability in both the primary and secondary Cisco FMCs.
- C. Connect the primary and secondary Cisco FMC devices with Category 6 cables of not more than 10 meters in length.
- D. Place the active Cisco FMC device on the same trusted management network as the standby device.

Answer: A

NEW QUESTION 9

- (Exam Topic 5)

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.

Answer: B

NEW QUESTION 10

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

Answer: A

NEW QUESTION 14

- (Exam Topic 5)

A security engineer is adding three Cisco FTD devices to a Cisco FMC. Two of the devices have successfully registered to the Cisco FMC. The device that is unable to register is located behind a router that translates all outbound traffic to the router's WAN IP address. Which two steps are required for this device to register to the Cisco FMC? (Choose two.)

- A. Reconfigure the Cisco FMC to use the device's private IP address instead of the WAN address.
- B. Configure a NAT ID on both the Cisco FMC and the device.
- C. Add the port number being used for PAT on the router to the device's IP address in the Cisco FMC.
- D. Reconfigure the Cisco FMC to use the device's hostname instead of IP address.
- E. Remove the IP address defined for the device in the Cisco FMC.

Answer: BE

NEW QUESTION 18

- (Exam Topic 5)

A network administrator cannot select the link to be used for failover when configuring an active/passive HA Cisco FTD pair. Which configuration must be changed before setting up the high availability pair?

- A. An IP address in the same subnet must be added to each Cisco FTD on the interface.
- B. The interface name must be removed from the interface on each Cisco FTD.
- C. The name Failover must be configured manually on the interface on each Cisco FTD.
- D. The interface must be configured as part of a LACP Active/Active EtherChannel.

Answer: A

NEW QUESTION 20

- (Exam Topic 5)

Refer to the exhibit.

II. ASSESSMENT RESULTS	
AUTOMATING THE TUNING EFFORT	
During the assessment period, the following changes to your network were observed.	
NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	310
A new host was added to the network	366
A device started using a new transport protocol	381
A device started using a new network protocol	373

An engineer is analyzing the Attacks Risk Report and finds that there are over 300 instances of new operating systems being seen on the network. How is the Firepower configuration updated to protect these new operating systems?

- A. Cisco Firepower automatically updates the policies.
- B. The administrator requests a Remediation Recommendation Report from Cisco Firepower.
- C. Cisco Firepower gives recommendations to update the policies.
- D. The administrator manually updates the policies.

Answer: C

Explanation:

Ref:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Tailor>

NEW QUESTION 22

- (Exam Topic 5)

An organization is implementing Cisco FTD using transparent mode in the network. Which rule in the default Access Control Policy ensures that this deployment does not create a loop in the network?

- A. ARP inspection is enabled by default.
- B. Multicast and broadcast packets are denied by default.

- C. STP BPDU packets are allowed by default.
- D. ARP packets are allowed by default.

Answer: B

NEW QUESTION 23

- (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 24

- (Exam Topic 5)

An administrator is setting up Cisco Firepower to send data to the Cisco Stealthwatch appliances. The NetFlow_Set_Parameters object is already created, but NetFlow is not being sent to the flow collector. What must be done to prevent this from occurring?

- A. Add the NetFlow_Send_Destination object to the configuration
- B. Create a Security Intelligence object to send the data to Cisco Stealthwatch
- C. Create a service identifier to enable the NetFlow service
- D. Add the NetFlow_Add_Destination object to the configuration

Answer: B

NEW QUESTION 29

- (Exam Topic 5)

An engineer defines a new rule while configuring an Access Control Policy. After deploying the policy, the rule is not working as expected and the hit counters associated with the rule are showing zero. What is causing this error?

- A. Logging is not enabled for the rule.
- B. The rule was not enabled after being created.
- C. The wrong source interface for Snort was selected in the rule.
- D. An incorrect application signature was used in the rule.

Answer: B

NEW QUESTION 30

- (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 32

- (Exam Topic 5)

An engineer is configuring two new Cisco FTD devices to replace the existing high availability firewall pair in a highly secure environment. The information exchanged between the FTD devices over the failover link must be encrypted. Which protocol supports this on the Cisco FTD?

- A. IPsec
- B. SSH
- C. SSL
- D. MACsec

Answer: A

NEW QUESTION 34

- (Exam Topic 5)

An administrator is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of NAT001 and a password of Cisco0420I06525. The private IP address of the FMC server is 192.168.45.45. which is being translated to the public IP address of 209.165.200.225/27. Which command set must be used in order to accomplish this task?

- A. configure manager add 209.165.200.225 <reg_key> <nat_id>
- B. configure manager add 192.168.45.45 <reg_key> <nat_id>
- C. configure manager add 209.165.200.225 255.255.255.224 <reg_key> <nat_id>
- D. configure manager add 209.165.200.225/27 <reg_key> <nat_id>

Answer: A

NEW QUESTION 37

- (Exam Topic 5)

An engineer wants to add an additional Cisco FTD Version 6.2.3 device to their current 6.2.3 deployment to create a high availability pair.

The currently deployed Cisco FTD device is using local management and identical hardware including the available port density to enable the failover and stateful links required in a proper high availability deployment. Which action ensures that the environment is ready to pair the new Cisco FTD with the old one?

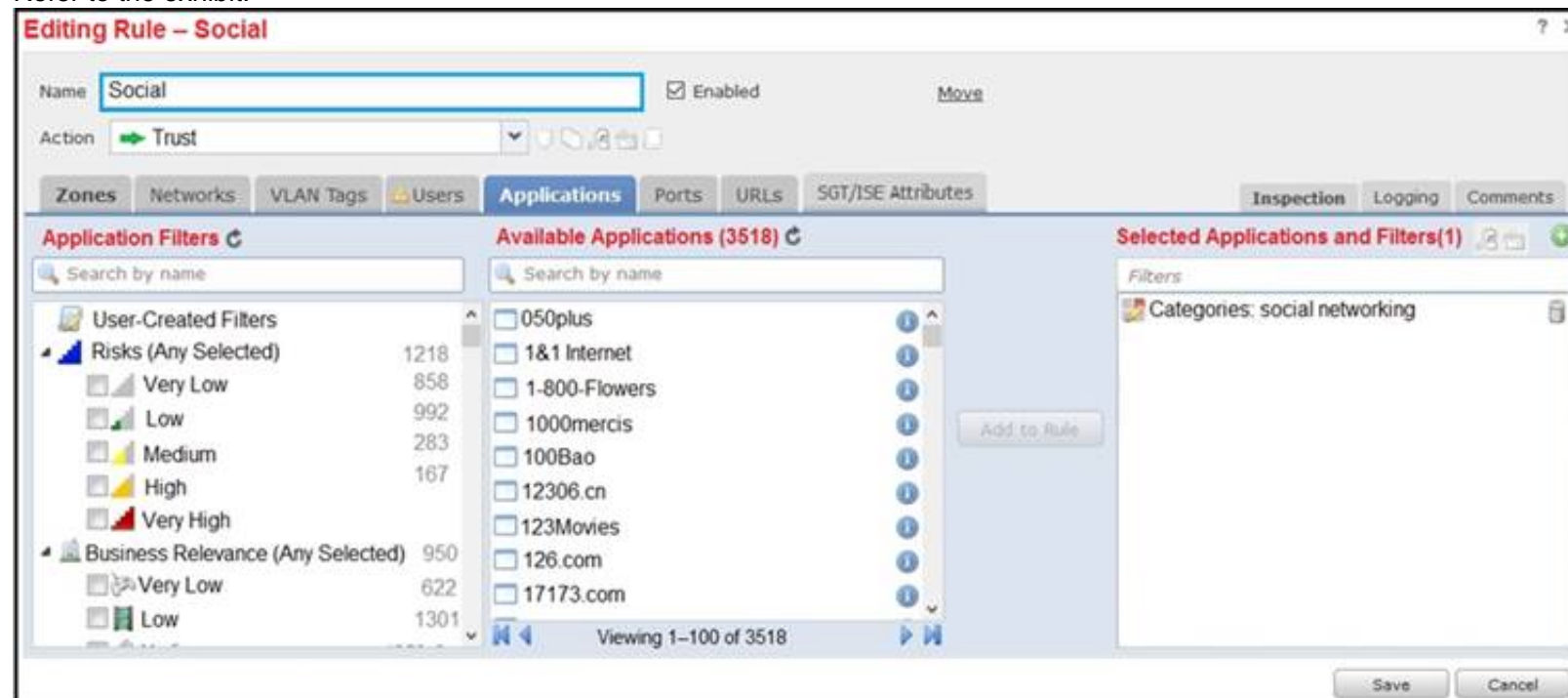
- A. Change from Cisco FDM management to Cisco FMC management on both devices and register them to FMC.
- B. Ensure that the two devices are assigned IP addresses from the 169.254.0.0/16 range for failover interfaces.
- C. Factory reset the current Cisco FTD so that it can synchronize configurations with the new Cisco FTD device.
- D. Ensure that the configured DNS servers match on the two devices for name resolution.

Answer: A

NEW QUESTION 40

- (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 42

- (Exam Topic 5)

An engineer needs to configure remote storage on Cisco FMC. Configuration backups must be available from a secure location on the network for disaster recovery. Reports need to back up to a shared location that auditors can access with their Active Directory logins. Which strategy must the engineer use to meet these objectives?

- A. Use SMB for backups and NFS for reports.
- B. Use NFS for both backups and reports.
- C. Use SMB for both backups and reports.
- D. Use SSH for backups and NFS for reports.

Answer: C

Explanation:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/syste> "You cannot send backups to one remote system and reports to another, but you can choose to send either to a remote system and store the other on the Firepower Management Center."

NEW QUESTION 46

- (Exam Topic 5)

An engineer is working on a LAN switch and has noticed that its network connection to the Cisco IPS has gone down. Upon troubleshooting, it is determined that the switch is working as expected. What must have been implemented for this failure to occur?

- A. The upstream router has a misconfigured routing protocol.
- B. Link-state propagation is enabled.
- C. The Cisco IPS has been configured to be in fail-open mode.
- D. The Cisco IPS is configured in detection mode.

Answer: D

NEW QUESTION 49

- (Exam Topic 5)

An engineer currently has a Cisco FTD device registered to the Cisco FMC and is assigned the address of 10.10.50.12. The organization is upgrading the addressing schemes and there is a requirement to convert the addresses to a format that provides an adequate amount of addresses on the network. What should the engineer do to ensure that the new addressing takes effect and can be used for the Cisco FTD to Cisco FMC connection?

- A. Delete and reregister the device to Cisco FMC
- B. Update the IP addresses from IPv4 to IPv6 without deleting the device from Cisco FMC
- C. Format and reregister the device to Cisco FMC.
- D. Cisco FMC does not support devices that use IPv4 IP addresses.

Answer: A

NEW QUESTION 50

- (Exam Topic 5)

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?

- A. failsafe
- B. inline tap
- C. promiscuous
- D. bypass

Answer: B

NEW QUESTION 52

- (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 57

- (Exam Topic 5)

An administrator is attempting to remotely log into a switch in the data centre using SSH and is unable to connect. How does the administrator confirm that traffic is reaching the firewall?

- A. by running Wireshark on the administrator's PC
- B. by performing a packet capture on the firewall.
- C. by running a packet tracer on the firewall.
- D. by attempting to access it from a different workstation.

Answer: B

NEW QUESTION 59

- (Exam Topic 5)

A network engineer is receiving reports of users randomly getting disconnected from their corporate applications which traverse the data center FTD appliance.

Network monitoring tools show that the FTD appliance utilization is peaking above 90% of total capacity. What must be done in order to further analyze this issue?

- A. Use the Packet Export feature to save data onto external drives
- B. Use the Packet Capture feature to collect real-time network traffic
- C. Use the Packet Tracer feature for traffic policy analysis
- D. Use the Packet Analysis feature for capturing network data

Answer: B

NEW QUESTION 63

- (Exam Topic 5)

An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighbouring Cisco devices or use multicast in their environment. What must be done to resolve this issue?

- A. Create a firewall rule to allow CDP traffic.
- B. Create a bridge group with the firewall interfaces.
- C. Change the firewall mode to routed.
- D. Change the firewall mode to transparent.

Answer: C

NEW QUESTION 65

- (Exam Topic 5)

An engineer is setting up a new Firepower deployment and is looking at the default FMC policies to start the implementation. During the initial trial phase, the organization wants to test some common Snort rules while still allowing the majority of network traffic to pass. Which default policy should be used?

- A. Maximum Detection

- B. Security Over Connectivity
- C. Balanced Security and Connectivity
- D. Connectivity Over Security

Answer: C

Explanation:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusio>

NEW QUESTION 67

- (Exam Topic 5)

After using Firepower for some time and learning about how it interacts with the network, an administrator is trying to correlate malicious activity with a user Which widget should be configured to provide this visibility on the Cisco Firepower dashboards?

- A. Custom Analysis
- B. Current Status
- C. Current Sessions
- D. Correlation Events

Answer: A

NEW QUESTION 70

- (Exam Topic 5)

What is the role of the casebook feature in Cisco Threat Response?

- A. sharing threat analysts
- B. pulling data via the browser extension
- C. triage automaton with alerting
- D. alert prioritization

Answer: A

Explanation:

The casebook and pivot menu are widgets available in Cisco Threat Response. Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables.

[https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide/esa_user_guide_13-5-1/b_ESA_Admin_Guide_ces_13-5-1/b_ESA_Admin_Guide_13-0_chapter_0110001.pdf](https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_13-5-1/b_ESA_Admin_Guide_ces_13-5-1/b_ESA_Admin_Guide_13-0_chapter_0110001.pdf)

NEW QUESTION 73

- (Exam Topic 5)

An engineer is reviewing a ticket that requests to allow traffic for some devices that must connect to a server over 8699/udp. The request mentions only one IP address, 172.16.18.15, but the requestor asked for the engineer to open the port for all machines that have been trying to connect to it over the last week. Which action must the engineer take to troubleshoot this issue?

- A. Use the context explorer to see the application blocks by protocol.
- B. Use the context explorer to see the destination port blocks
- C. Filter the connection events by the source port 8699/udp.
- D. Filter the connection events by the destination port 8699/udp.

Answer: D

NEW QUESTION 77

- (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 78

- (Exam Topic 5)

Which protocol is needed to exchange threat details in rapid threat containment on Cisco FMC?

- A. SGT
- B. SNMP v3
- C. BFD
- D. pxGrid

Answer: D

NEW QUESTION 79

- (Exam Topic 5)

A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?

- A. Use regular expressions to block the malicious file.
- B. Add the hash from the infected endpoint to the network block list.
- C. Add the hash to the simple custom detection list.
- D. Enable a personal firewall in the infected endpoint.

Answer: C

NEW QUESTION 82

- (Exam Topic 5)

The CEO ask a network administrator to present to management a dashboard that shows custom analysis tables for the top DNS queries URL category statistics, and the URL reputation statistics.

Which action must the administrator take to quickly produce this information for management?

- A. Run the Attack report and filter on DNS to show this information.
- B. Create a new dashboard and add three custom analysis widgets that specify the tables needed.
- C. Modify the Connection Events dashboard to display the information in a view for management.
- D. Copy the intrusion events dashboard tab and modify each widget to show the correct charts.

Answer: B

NEW QUESTION 83

- (Exam Topic 5)

Refer to the exhibit.



What is the effect of the existing Cisco FMC configuration?

- A. The remote management port for communication between the Cisco FMC and the managed device changes to port 8443.
- B. The managed device is deleted from the Cisco FMC.
- C. The SSL-encrypted communication channel between the Cisco FMC and the managed device becomes plain-text communication channel.
- D. The management connection between the Cisco FMC and the Cisco FTD is disabled.

Answer: D

NEW QUESTION 84

- (Exam Topic 5)

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 Connection Events dashboard to check the block reason and adjust the inspection policy as needed.
- B. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion 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.

Answer: A

NEW QUESTION 88

- (Exam Topic 5)

A company wants a solution to aggregate the capacity of two Cisco FTD devices to make the best use of resources such as bandwidth and connections per second. Which order of steps must be taken across the Cisco FTDs with Cisco FMC to meet this requirement?

- A. Configure the Cisco FTD interfaces, add members to FMC, configure cluster members in FMC, and create cluster in Cisco FMC.
- B. Add members to Cisco FMC, configure Cisco FTD interfaces in Cisco FM
- C. configure cluster members in Cisco FMC, create cluster in Cisco FM
- D. and configure cluster members in Cisco FMC.
- E. Configure the Cisco FTD interfaces and cluster members, add members to Cisco FM
- F. and create the cluster in Cisco FMC.
- G. Add members to the Cisco FMC, configure Cisco FTD interfaces, create the cluster in Cisco FMC, and configure cluster members in Cisco FMC.

Answer: D

NEW QUESTION 93

- (Exam Topic 5)

A security engineer must configure a Cisco FTD appliance to inspect traffic coming from the internet. The Internet traffic will be mirrored from the Cisco Catalyst 9300 Switch. Which configuration accomplishes the task?

- A. Set interface configuration mode to none.
- B. Set the firewall mode to transparent.
- C. Set the firewall mode to routed.
- D. Set interface configuration mode to passive.

Answer: D

NEW QUESTION 96

- (Exam Topic 5)

An analyst using the security analyst account permissions is trying to view the Correlations Events Widget but is not able to access it. However, other dashboards are accessible. Why is this occurring?

- A. An API restriction within the Cisco FMC is preventing the widget from displaying.
- B. The widget is configured to display only when active events are present.
- C. The widget is not configured within the Cisco FMC.
- D. The security analyst role does not have permission to view this widget.

Answer: C

NEW QUESTION 98

- (Exam Topic 5)

An engineer runs the command `restore remote-manager-backup location 2.2.2.2 admin /Volume/home/admin FTD408566513.zip` on a Cisco FMC. After connecting to the repository, the Cisco FTD device is unable to accept the backup file. What is the reason for this failure?

- A. The backup file is not in .cfg format.
- B. The wrong IP address is used.
- C. The backup file extension was changed from .tar to .zip.
- D. The directory location is incorrect.

Answer: C

Explanation:

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3455.pdf>

NEW QUESTION 102

- (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 103

- (Exam Topic 5)

A mid-sized company is experiencing higher network bandwidth utilization due to a recent acquisition The network operations team is asked to scale up their one Cisco FTD appliance deployment to higher capacities due to the increased network bandwidth. Which design option should be used to accomplish this goal?

- A. Deploy multiple Cisco FTD appliances in firewall clustering mode to increase performance.
- B. Deploy multiple Cisco FTD appliances using VPN load-balancing to scale performance.
- C. Deploy multiple Cisco FTD HA pairs to increase performance
- D. Deploy multiple Cisco FTD HA pairs in clustering mode to increase performance

Answer: A

NEW QUESTION 104

- (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 108

- (Exam Topic 5)

Which license type is required on Cisco ISE to integrate with Cisco FMC pxGrid?

- A. mobility
- B. plus
- C. base
- D. apex

Answer: B

NEW QUESTION 110

- (Exam Topic 5)

A network administrator is configuring a site-to-site IPsec VPN to a router sitting behind a Cisco FTD. The administrator has configured an access policy to allow traffic to this device on UDP 500, 4500, and ESP VPN traffic is not working. Which action resolves this issue?

- A. Set the allow action in the access policy to trust.
- B. Enable IPsec inspection on the access policy.
- C. Modify the NAT policy to use the interface PAT.
- D. Change the access policy to allow all ports.

Answer: B

NEW QUESTION 111

- (Exam Topic 5)

A network administrator notices that SI events are not being updated The Cisco FTD device is unable to load all of the SI event entries and traffic is not being blocked as expected. What must be done to correct this issue?

- A. Restart the affected devices in order to reset the configurations
- B. Manually update the SI event entries to that the appropriate traffic is blocked
- C. Replace the affected devices with devices that provide more memory
- D. Redeploy configurations to affected devices so that additional memory is allocated to the SI module

Answer: D

NEW QUESTION 115

- (Exam Topic 5)

An organization has a compliancy requirement to protect servers from clients, however, the clients and servers all reside on the same Layer 3 network Without readdressing IP subnets for clients or servers, how is segmentation achieved?

- A. Deploy a firewall in transparent mode between the clients and servers.
- B. Change the IP addresses of the clients, while remaining on the same subnet.
- C. Deploy a firewall in routed mode between the clients and servers
- D. Change the IP addresses of the servers, while remaining on the same subnet

Answer: A

NEW QUESTION 120

- (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 124

- (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 125

- (Exam Topic 3)

When do you need the file-size command option during troubleshooting with packet capture?

- A. when capture packets are less than 16 MB
- B. when capture packets are restricted from the secondary memory

- C. when capture packets exceed 10 GB
- D. when capture packets exceed 32 MB

Answer: D

Explanation:

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

NEW QUESTION 129

- (Exam Topic 3)

A network engineer is configuring URL Filtering on Firepower Threat Defense. Which two port requirements on the Firepower Management Center must be validated to allow communication with the cloud service? (Choose two.)

- A. outbound port TCP/443
- B. inbound port TCP/80
- C. outbound port TCP/8080
- D. inbound port TCP/443
- E. outbound port TCP/80

Answer: AE

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Securi>

NEW QUESTION 133

- (Exam Topic 3)

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

Answer: C

Explanation:

Reason: the command "capture-traffic" is used for SNORT Engine Captures. To capture a LINA Engine Capture, you use the "capture" command. Since the Lina Engine represents the actual physical interface of the device, "capture" is the only reasonable choice Reference:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-de>

The command is firepower# capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100 firepower# capture INSIDE interface inside trace detail match ip host 192.168.76.14 host 192.168.75.14

NEW QUESTION 137

- (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 140

- (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 144

- (Exam Topic 3)

Which two statements about deleting and re-adding a device to Cisco FMC are true? (Choose two.)

- A. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re- apply the policies after registration is completed.
- B. Before re-adding the device in Cisco FMC, you must add the manager back in the device.
- C. No option to delete and re-add a device is available in the Cisco FMC web interface.
- D. The Cisco FMC web interface prompts users to re-apply access control policies.
- E. No option to re-apply NAT and VPN policies during registration is available, so users need to re-apply the policies after registration is completed.

Answer: DE

Explanation:

Reference:

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

NEW QUESTION 146

- (Exam Topic 3)

What is the maximum bit size that Cisco FMC supports for HTTPS certificates?

A. A.-1024B.8192C.4096D.2048

Answer: C

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config- guide-v61/system_configuration.html

NEW QUESTION 151

- (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 152

- (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 156

- (Exam Topic 2)

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.

Answer: C

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-identity>

NEW QUESTION 161

- (Exam Topic 2)

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.

Answer: C

Explanation:

A file policy defines the actions that the Cisco Firepower Threat Defense (FTD) device should take when it encounters different types of files. The file policy is applied as part of an access control policy. If an access control policy does not include a file policy, the FTD device will not take any action on the files it encounters, resulting in a disposition of "unknown" for all file types except exe.

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the>

NEW QUESTION 164

- (Exam Topic 2)

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 FT
- C. not the Cisco FMC.
- D. DONOTRESOLVE must be added to the command
- E. The registration key is missing from the command

Answer: A

NEW QUESTION 166

- (Exam Topic 2)

An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events filling 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.

Answer: D

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Netwo>

NEW QUESTION 167

- (Exam Topic 2)

In which two places can thresholding settings be configured? (Choose two.)

- 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

Answer: AC

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.pdf>

NEW QUESTION 171

- (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 174

- (Exam Topic 2)

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.

Answer: C

NEW QUESTION 178

- (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 182

- (Exam Topic 1)

What is a result of enabling Cisco FTD clustering?

- A. For the dynamic routing feature, if the master unit fails, the newly elected master unit maintains all existing connections.
- B. Integrated Routing and Bridging is supported on the master unit.
- C. Site-to-site VPN functionality is limited to the master unit, and all VPN connections are dropped if the master unit fails.
- D. All Firepower appliances can support Cisco FTD clustering.

Answer: C

Explanation:

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

NEW QUESTION 184

- (Exam Topic 2)

Which command is run on an FTD unit to associate the unit to an FMC manager that is at IP address 10.0.0.10, and that has the registration key Cisco123?

- A. configure manager local 10.0.0.10 Cisco123
- B. configure manager add Cisco123 10.0.0.10
- C. configure manager local Cisco123 10.0.0.10
- D. configure manager add 10.0.0.10 Cisco123

Answer: D

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#id_106101

NEW QUESTION 185

- (Exam Topic 1)

Which policy rule is included in the deployment of a local DMZ during the initial deployment of a Cisco NGFW through the Cisco FMC GUI?

- A. a default DMZ policy for which only a user can change the IP addresses.
- B. deny ip any
- C. no policy rule is included
- D. permit ip any

Answer: C

NEW QUESTION 188

- (Exam Topic 1)

What is the difference between inline and inline tap on Cisco Firepower?

- A. Inline tap mode can send a copy of the traffic to another device.
- B. Inline tap mode does full packet capture.
- C. Inline mode cannot do SSL decryption.
- D. Inline mode can drop malicious traffic.

Answer: A

NEW QUESTION 192

- (Exam Topic 1)

A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?

- A. Specify the BVI IP address as the default gateway for connected devices.
- B. Enable routing on the Cisco Firepower
- C. Add an IP address to the physical Cisco Firepower interfaces.
- D. Configure a bridge group in transparent mode.

Answer: D

Explanation:

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place. Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw>.

NEW QUESTION 195

- (Exam Topic 1)

An organization is migrating their Cisco ASA devices running in multicontext mode to Cisco FTD devices. Which action must be taken to ensure that each context on the Cisco ASA is logically separated in the Cisco FTD devices?

- A. Add a native instance to distribute traffic to each Cisco FTD context.
- B. Add the Cisco FTD device to the Cisco ASA port channels.
- C. Configure a container instance in the Cisco FTD for each context in the Cisco ASA.
- D. Configure the Cisco FTD to use port channels spanning multiple networks.

Answer: C

NEW QUESTION 196

- (Exam Topic 1)

Which two dynamic routing protocols are supported in Firepower Threat Defense without using FlexConfig? (Choose two.)

- A. EIGRP
- B. OSPF
- C. static routing
- D. IS-IS
- E. BGP

Answer: BE

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-routing.html>

NEW QUESTION 198

- (Exam Topic 1)

An administrator is optimizing the Cisco FTD rules to improve network performance, and wants to bypass inspection for certain traffic types to reduce the load on the Cisco FTD. Which policy must be configured to accomplish this goal?

- A. prefilter
- B. intrusion
- C. identity
- D. URL filtering

Answer: A

NEW QUESTION 201

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-710 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-710 Product From:

<https://www.2passeasy.com/dumps/300-710/>

Money Back Guarantee

300-710 Practice Exam Features:

- * 300-710 Questions and Answers Updated Frequently
- * 300-710 Practice Questions Verified by Expert Senior Certified Staff
- * 300-710 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 300-710 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year