Cisco

Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

NEW QUESTION 1
- (Exam Topic 5)
An engineer is creating an URL object on Cisco FMC How must it be configured so that the object will match for HTTPS traffic in an access control policy?

A. Specify the protocol to match (HTTP or HTTPS).
B. Use the FQDN including the subdomain for the website
C. Define the path to the individual webpage that uses HTTPS.
D. Use the subject common name from the website certificate

Answer: B

NEW QUESTION 2
- (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 3
- (Exam Topic 5)
A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https://<FMC IP>/capture/CAPI/pcap/test.pcap. an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

A. Disable the HTTPS server and use HTTP instead.
B. Enable the HTTPS server for the device platform policy.
C. Disable the proxy setting on the browser.
D. Use the Cisco FTD IP address as the proxy server setting on the browser.

Answer: B

NEW QUESTION 4
- (Exam Topic 5)
An engineer is configuring a second Cisco FMC as a standby device but is unable to register with the active unit. What is causing this issue?

A. The primary FMC currently has devices connected to it.
B. The code versions running on the Cisco FMC devices are different
C. The licensing purchased does not include high availability
D. There is only 10 Mbps of bandwidth between the two devices.

Answer: B

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

NEW QUESTION 5
- (Exam Topic 5)
What is an advantage of adding multiple inline interface pairs to the same inline interface set when deploying an asynchronous routing configuration?

A. Allows the IPS to identify inbound and outbound traffic as part of the same traffic flow.
B. The interfaces disable autonegotiation and interface speed is hard coded set to 1000 Mbps.
C. Allows traffic inspection to continue without interruption during the Snort process restart.
D. The interfaces are automatically configured as a media-independent interface crossover.

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpm

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)
The administrator notices that there is malware present with an .exe extension and needs to verify if any of the systems on the network are running the executable file. What must be configured within Cisco AMP for Endpoints to show this data?

A. prevalence
B. threat root cause
C. vulnerable software
D. file analysis

Answer: A

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 is restoring a Cisco FTD configuration from a remote backup using the command restore remote-manager-backup location 1.1.1.1 admin /volume/home/admin BACKUP_Cisc394602314.zip on a
Cisco FMG. After connecting to the repository, an error occurred that prevents the FTD device from accepting the backup file. What is the problem?

A. The backup file is not in .cfg format.
B. The backup file is too large for the Cisco FTD device
C. The backup file extension was changed from tar to zip
D. The backup file was not enabled prior to being applied

Answer: C

NEW QUESTION 10
- (Exam Topic 5)
A network engineer sets up a secondary Cisco FMC that is integrated with Cisco Security Packet Analyzer What occurs when the secondary Cisco FMC synchronizes with the primary Cisco FMC?

A. The existing integration configuration is replicated to the primary Cisco FMC
B. The existing configuration for integration of the secondary Cisco FMC the Cisco Security Packet Analyzer is overwritten.
C. The synchronization between the primary and secondary Cisco FMC fails
D. The secondary Cisco FMC must be reintegrated with the Cisco Security Packet Analyzer after the synchronization

Answer: B

NEW QUESTION 10
- (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.

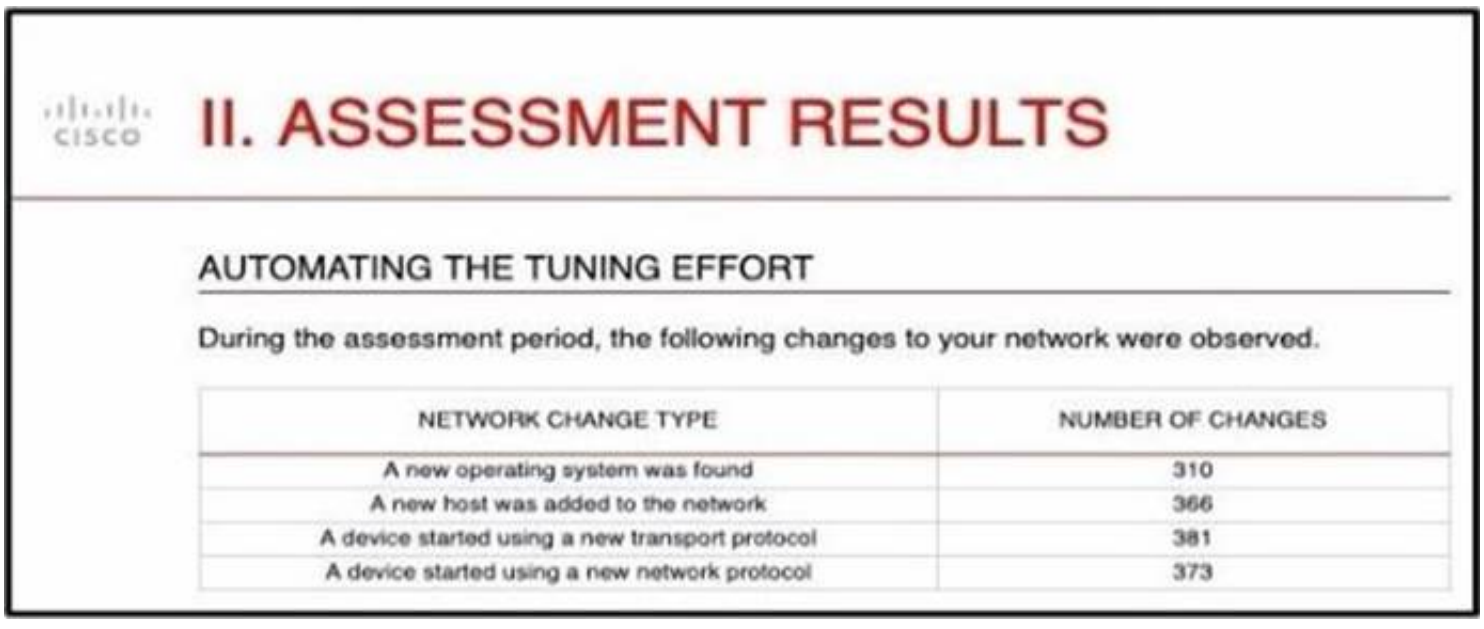
Answer: A

NEW QUESTION 11
- (Exam Topic 5)
A network engineer wants to add a third-party threat feed into the Cisco FMC for enhanced threat detection Which action should be taken to accomplish this goal?

A. Enable Threat Intelligence Director using STIX and TAXII
B. Enable Rapid Threat Containment using REST APIs
C. Enable Threat Intelligence Director using REST APIs
D. Enable Rapid Threat Containment using STIX and TAXII

Answer: A

NEW QUESTION 15
- (Exam Topic 5)
Refer to the exhibit.



And 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 16
- (Exam Topic 5)
Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC (Choose two).

A. Before re-adding the device In Cisco FMC, the manager must be added back.
B. The Cisco FMC web interface prompts users to re-apply access control policies.
C. Once a device has been deleted, It must be reconfigured before it is re-added to the Cisco FMC.
D. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re-apply the polices after registration is completed.
E. There is 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: BE

NEW QUESTION 20
- (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 25
- (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 Cisco0420l06525. 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 27
- (Exam Topic 5)
An administrator needs to configure Cisco FMC to send a notification email when a data transfer larger than 10 MB is initiated from an internal host outside of standard business hours. Which Cisco FMC feature must be configured to accomplish this task?

A. file and malware policy
B. application detector
C. intrusion policy
D. correlation policy

Answer: A

NEW QUESTION 30
- (Exam Topic 5)
The network administrator wants to enhance the network security posture by enabling machine learning tor malware detection due to a concern with suspicious Microsoft executable file types that were seen while creating monthly security reports for the CIO. Which feature must be enabled to accomplish this goal?

A. Spero
B. dynamic analysis
C. static analysis
D. Ethos

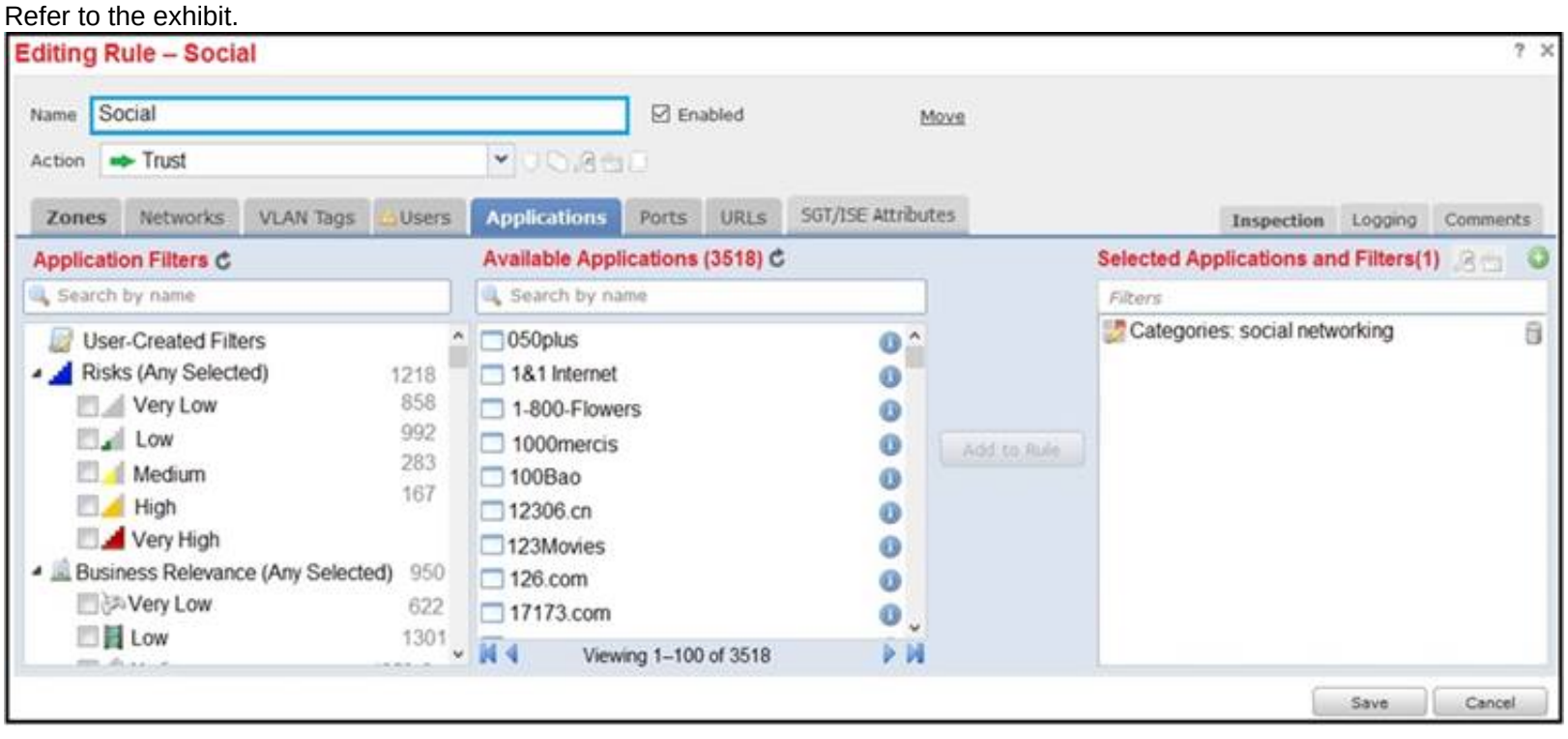
Answer: A

NEW QUESTION 32
- (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 35
- (Exam Topic 5)
Refer to the exhibit.

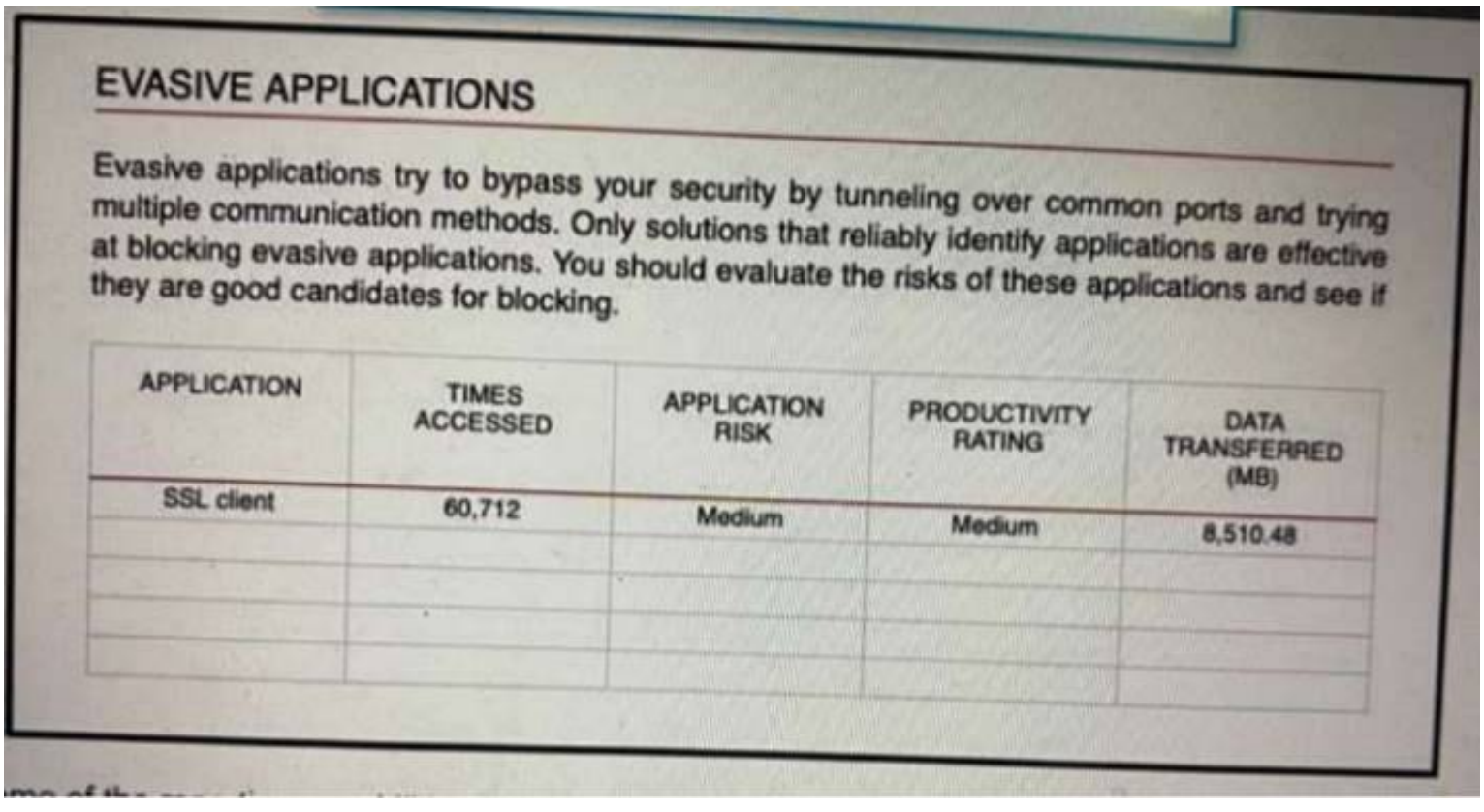


An organization has an access control rule with the intention of sending all social media traffic for inspection After using the rule for some time, the administrator notices that the traffic is not being inspected, but is being automatically allowed What must be done to address this issue?

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)
Refer to the exhibit.



EVASIVE APPLICATIONS

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
SSL client	60,712	Medium	Medium	8,510.48

An administrator is looking at some of the reporting capabilities for Cisco Firepower and noticed this section of the Network Risk report showing a lot of SSL activity that cloud be used for evasion. Which action will mitigate this risk?

A. Use SSL decryption to analyze the packets.
B. Use encrypted traffic analytics to detect attacks
C. Use Cisco AMP for Endpoints to block all SSL connection
D. Use Cisco Tetration to track SSL connections to servers.

Answer: A

NEW QUESTION 40
- (Exam Topic 5)
An engineer is working on a LAN switch and has noticed that its network connection to the mime 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 42
- (Exam Topic 5)
An organization has implemented Cisco Firepower without IPS capabilities and now wants to enable inspection for their traffic. They need to be able to detect protocol anomalies and utilize the Snort rule sets to detect malicious behaviour. How is this accomplished?

A. Modify the access control policy to redirect interesting traffic to the engine
B. Modify the network discovery policy to detect new hosts to inspect
C. Modify the network analysis policy to process the packets for inspection
D. Modify the intrusion policy to determine the minimum severity of an event to inspect.

Answer: D

NEW QUESTION 47
- (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 IFV4 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 52
- (Exam Topic 5)
What must be implemented on Cisco Firepower to allow multiple logical devices on a single physical device to have access to external hosts?

A. Add at least two container instances from the same module.
B. Set up a cluster control link between all logical devices
C. Add one shared management interface on all logical devices.
D. Define VLAN subinterfaces for each logical device.

Answer: C

NEW QUESTION 55
- (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 60
- (Exam Topic 5)
An engineer must deploy a Cisco FTD appliance via Cisco FMC to span a network segment to detect malware and threats. When setting the Cisco FTD interface mode, which sequence of actions meets this requirement?

A. Set to passive, and configure an access control policy with an intrusion policy and a file policy defined
B. Set to passive, and configure an access control policy with a prefilter policy defined
C. Set to none, and configure an access control policy with a prefilter policy defined
D. Set to none, and configure an access control policy with an intrusion policy and a file policy defined

Answer: A

NEW QUESTION 64
- (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 68
- (Exam Topic 5)
administrator is configuring SNORT inspection policies and is seeing failed deployment messages in Cisco FMC . What information should the administrator generate for Cisco TAC to help troubleshoot?

A. A Troubleshoot" file for the device in question.
B. A "show tech" file for the device in question
C. A "show tech" for the Cisco FMC.
D. A "troubleshoot" file for the Cisco FMC

Answer: A

NEW QUESTION 71
- (Exam Topic 5)
An engineer wants to connect a single IP subnet through a Cisco FTD firewall and enforce policy. There is a requirement to present the internal IP subnet to the outside as a different IP address. What must be configured to meet these requirements?

A. Configure the downstream router to perform NAT.
B. Configure the upstream router to perform NAT.
C. Configure the Cisco FTD firewall in routed mode with NAT enabled.
D. Configure the Cisco FTD firewall in transparent mode with NAT enabled.

Answer: C

NEW QUESTION 76
- (Exam Topic 5)
A Cisco FMC administrator wants to configure fastpathing of trusted network traffic to increase performance. In which type of policy would the administrator configure this feature?

A. Identity policy
B. Prefilter policy
C. Network Analysis policy
D. Intrusion policy

Answer: B

NEW QUESTION 78
- (Exam Topic 5)
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.

Answer: A

NEW QUESTION 79
- (Exam Topic 5)
A network administrator is configuring an FTD in transparent mode. A bridge group is set up and an access policy has been set up to allow all IP traffic. Traffic is not passing through the FTD. What additional configuration is needed?

A. The security levels of the interfaces must be set.
B. A default route must be added to the FTD.
C. An IP address must be assigned to the BVI.
D. A mac-access control list must be added to allow all MAC addresses.

Answer: C

NEW QUESTION 83
- (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 85
- (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 88
- (Exam Topic 5)
An engineer has been tasked with using Cisco FMC to determine if files being sent through the network are malware. Which two configuration tasks must be performed to achieve this file lookup? (Choose two).

A. The Cisco FMC needs to include a SSL decryption policy.
B. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.
C. The Cisco FMC needs to connect to the Cisco ThreatGrid service directly for sandboxing.
D. The Cisco FMC needs to connect with the FireAMP Cloud.
E. The Cisco FMC needs to include a file inspection policy for malware lookup.

Answer: BE

NEW QUESTION 93
- (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.

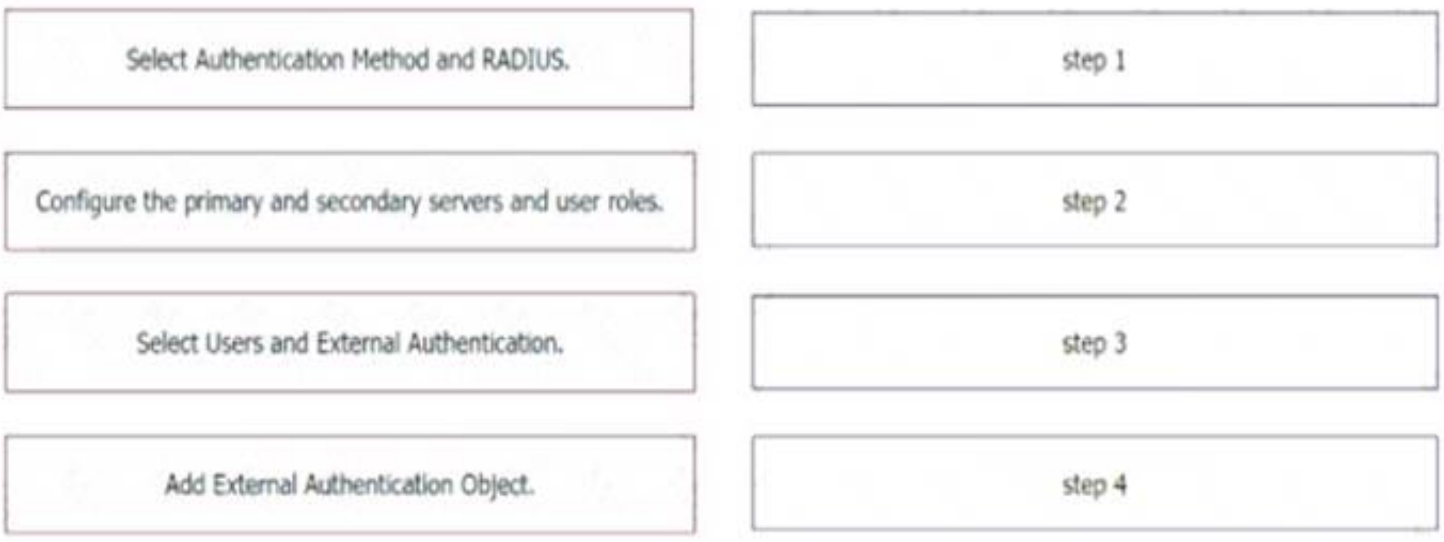
Answer: C

NEW QUESTION 94
- (Exam Topic 5)
A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface. What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

A. Only the UDP packet type is supported.
B. The output format option for the packet logs is unavailable.
C. The destination MAC address is optional if a VLAN ID value is entered.
D. The VLAN ID and destination MAC address are optional.

Answer: C

NEW QUESTION 97
- (Exam Topic 5)
Drag and drop the configuration steps from the left into the sequence on the right to enable external authentication on Cisco FMC to a RADIUS server.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
4, 1, 2, 3

NEW QUESTION 100
- (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 103
- (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 blockedtraffic.

Answer: A

NEW QUESTION 108
- (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 112
- (Exam Topic 5)
A network administrator is troubleshooting access to a website hosted behind a Cisco FTD device External clients cannot access the web server via HTTPS The IP address configured on the web server is 192 168 7.46 The administrator is running the command capture CAP interface outside match ip any 192.168.7.46 255.255.255.255 but cannot see any traffic in the capture Why is this occurring?

A. The capture must use the public IP address of the web server.
B. The FTD has no route to the web server.
C. The access policy is blocking the traffic.
D. The packet capture shows only blocked traffic

Answer: A

NEW QUESTION 117
- (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 118
- (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 121
- (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 122
- (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 125
- (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 129
- (Exam Topic 5)
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. generate events
B. drop packet
C. drop connection
D. drop and generate

Answer: B

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

NEW QUESTION 130
- (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

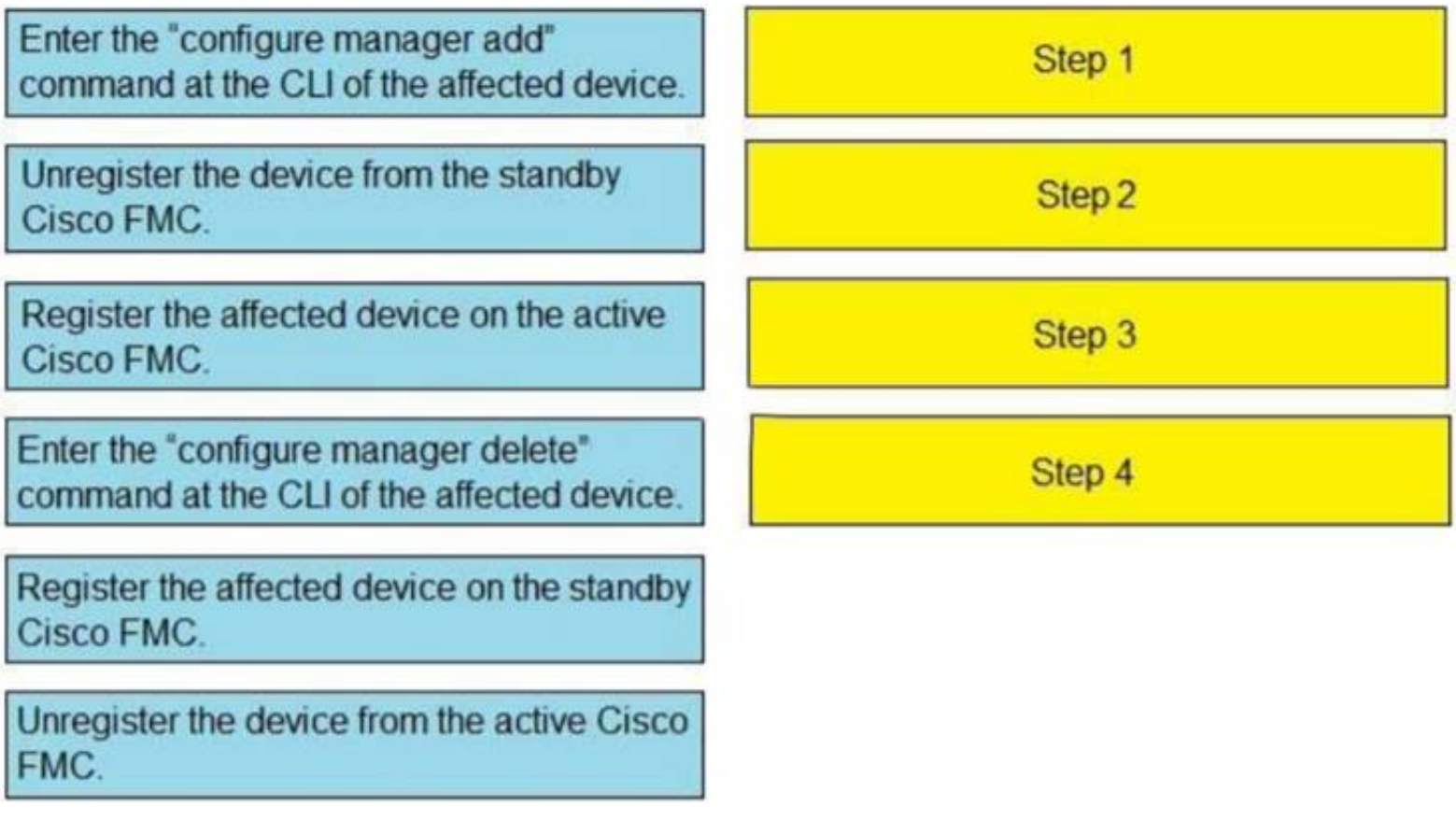
NEW QUESTION 134
- (Exam Topic 3)
Within Cisco Firepower Management Center, where does a user add or modify widgets?

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 137
- (Exam Topic 3)
Drag and drop the steps to restore an automatic device registration failure on the standby Cisco FMC from the left into the correct order on the right. Not all options are used.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/firepower_management_center_high_availability.html#id_32288

NEW QUESTION 142
- (Exam Topic 2)
Which two actions can be used in an access control policy rule? (Choose two.)

A. Block with Reset
B. Monitor
C. Analyze
D. Discover
E. Block ALL

Answer: AB

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa- firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html#71854

NEW QUESTION 145
- (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 148
- (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 153
- (Exam Topic 3)

Which CLI command is used to generate firewall debug messages on a Cisco Firepower?

A. system support firewall-engine-debug
B. system support ssl-debug
C. system support platform
D. system support dump-table

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212330-firepower- management-center-display-acc.html

NEW QUESTION 158
- (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 162
- (Exam Topic 2)
An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events filing 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)
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 169
- (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 173
- (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 178
- (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 181
- (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 184
- (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 187
- (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 188
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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