Exam Questions 300-210

SITCS Implementing Cisco Threat Control Solutions (SITCS)
NEW QUESTION 1
- (Exam Topic 1)
Which four parameters must be defined in an ISAKMP policy when creating an IPsec site-to-site VPN using the Cisco ASDM? (Choose four.)

A. encryption algorithm
B. hash algorithm
C. authentication method
D. IP address of remote IPsec peer
E. D-H group
F. perfect forward secrecy

Answer: ABCE

NEW QUESTION 2
- (Exam Topic 1)
With Cisco AMP for Endpoints on Windows, which three engines are available in the connector? (Choose three.)

A. Ethos
B. Tetra
C. Annos
D. Spero
E. Talos
F. ClamAV

Answer: ABD

Explanation:

NEW QUESTION 3
- (Exam Topic 1)
User wants to deploy your managed device in Layer 3 routed mode and must configure a virtual router and a routed interface. Which managed shows this configuration?

A. Cisco FirePOWER services on a Cisco ASA 5500x.
B. virtual NGIPS
C. Cisco FirePOWER module on a Cisco ASA 5585x.
D. Cisco FirePOWER appliance.

Answer: C

NEW QUESTION 4
- (Exam Topic 1)
Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the Host Access Table Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance.

Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the four multiple choice questions.

A. red.public, -6
B. orange.public, -4
C. yellow.public, -2
D. gree
E. .public, 2
F. blue.public, 6
G. violet.public, 8

Answer: D

NEW QUESTION 5
- (Exam Topic 1)
Which statement about the Cisco ASA botnet traffic filter is true?

A. The four threat levels are low, moderate, high, and very high.
B. By default, the dynamic-filter drop blacklist interface outside command drops traffic with a threat level of high or very high.
C. Static blacklist entries always have a very high threat level.
D. A static or dynamic blacklist entry always takes precedence over the static whitelist entry.

Answer: C

NEW QUESTION 6
- (Exam Topic 2)
Which two Cisco IPS events will generate an IP log? (Choose two.)

A. A signature had an event action that was configured with log packets.
B. A statically configured IP or IP network criterion was matched.
C. A dynamically configured IP address or IP network was matched.
D. An attack produced a response action.

Answer: A
NEW QUESTION 7
- (Exam Topic 2)
What command alters the SSL ciphers used by the Cisco Email Security Appliance for TLS sessions and HTTPS access?

A. sslcconfig
B. salciphers
C. tlcconfig
D. centconfig

Answer: A

NEW QUESTION 8
- (Exam Topic 2)
How does a user access a Cisco Web Security Appliance for initial setup?

A. Connect the console cable and use the terminal at 9600 baud to run the setup wizard.
B. Connect the console cable and use the terminal at 115200 baud to run the setup wizard.
C. Open the web browser at 192.168.42.42:8443 for the setup wizard over https.
D. Open the web browser at 192.168.42.42:443 for the setup wizard over https.

Answer: C

NEW QUESTION 9
- (Exam Topic 2)
What are the initial actions that can be performed on an incoming SMTP session by the workqueue of a Cisco Email Security Appliance?

A. Accept, Reject, Relay, TCPRefuse
B. LDAP Verification, Envelope Sender Verification, Bounce Verification, Alias Table Verification
C. Recipient Access Table Verification, Host DNS Verification, Masquerading, Spam Payload Check
D. SMTP Authentication, SBRS Verification, Sendergroup matching, DNS host verification

Answer: A

NEW QUESTION 10
- (Exam Topic 2)
Which Cisco Cloud Web Security tool provides URL categorization?

A. Cisco Dynamic Content Analysis Engine
B. Cisco ScanSafe
C. ASA Firewall Proxy
D. Cisco Web Usage Control

Answer: D

NEW QUESTION 11
- (Exam Topic 3)
An IPS is configured to fail-closed and you observe that all packets are dropped. What is a possible reason for this behavior?

A. Mainapp is unresponsive.
B. The global correlation update failed.
C. The IPS span session failed.
D. The attack drop file is misconfigured.

Answer: A

NEW QUESTION 12
- (Exam Topic 3)
In this simulation, you have access to the mail flow policies and sender groups configured on a Cisco Email Security Appliance. You are also provided the following list of fictional domains. SenderBases has records for one sender from each of these domains. The list provides the domain name and the SenderBase Reputation Score for the domains sender.

Your task is to review the configuration on the Cisco Email Security Appliance and then answer 5 multiple choice questions about the behavior of the Cisco Email Security Appliance given the configuration and the domain SenderBase Reputation Scores.

Answer: A
Certshared now are offering 100% pass ensure 300-210 dumps!
https://www.certshared.com/exam/300-210/ (494 Q&As)

Guaranteed success with Our exam guides
visit - https://www.certshared.com
Certshared now are offering 100% pass ensure 300-210 dumps!
https://www.certshared.com/exam/300-210/ (494 Q&As)

Guaranteed success with Our exam guides
visit - https://www.certshared.com
Certshared now are offering 100% pass ensure 300-210 dumps!
https://www.certshared.com/exam/300-210/ (494 Q&As)

Guaranteed success with Our exam guides
visit - https://www.certshared.com
Certshared now are offering 100% pass ensure 300-210 dumps!
https://www.certshared.com/exam/300-210/ (494 Q&As)

Guaranteed success with Our exam guides
visit - https://www.certshared.com
Guaranteed success with Our exam guides
visit - https://www.certshared.com
What is the maximum message size that the Cisco Email Security Appliance will accept from the violet.public domain?

A. 1 KB  
B. 100 KB  
C. 1 MB  
D. 10 MB  
E. 100 MB  
F. Unlimited  

Answer: D  

Explanation: From the instructions we know that the reputation score for the violet.public domain has been set to 8. From the HAT table shown below we know that a score of 8 belongs to the UNKNOWNLIST group, which is assigned the ACCEPTED policy.
NEW QUESTION 13
- (Exam Topic 3)
Refer to the exhibit.

Which four rows exhibit the correct WCCP service to protocol assignments? (Choose four.)

A. Row 1
B. Row 2
C. Row 3
D. Row 4
E. Row 5
F. Row 6
G. Row 7
H. Row 8

Answer: BDFH

NEW QUESTION 14
- (Exam Topic 3)
Which two pieces of information are required to implement transparent user identification using context Directory Agent? (Choose two.)
A. the shared secret
B. the server name where Context Directory Agent is installed
C. the server name of the global catalog domain controller
D. the syslog server IP address

Answer: AB

NEW QUESTION 15
- (Exam Topic 3)
For which task can PRSM be used?

A. To configure Cisco ASA CX firewalls
B. To monitor Cisco intelliShield
C. To monitor CWS traffic
D. To configure Cisco ESA

Answer: A

NEW QUESTION 16
- (Exam Topic 3)
Which step is required when you configure URL filtering to Cisco Cloud Web Security?

A. configure URL filtering policies in Cisco ScanCenter
B. install the ASA FirePOWER module on the Cisco ASA.
C. Implement Next Generation IPS intrusion rules.
D. Configure URL filtering criteria in the Cisco ASA FirePOWER access rules.

Answer: A

NEW QUESTION 17
- (Exam Topic 4)
Which option is omitted from a query on a ESA virtual appliance?

A. raidrable
B. FailoverHealthy
C. keyExpiration
D. CPUUtilizationExceeded

Answer: A

NEW QUESTION 18
- (Exam Topic 4)
Which action inspects packets in IPS?

A. Monitor
B. Trust
C. Block
D. Allow
E. Default Action

Answer: AE

NEW QUESTION 19
- (Exam Topic 4)
A customer has various external http resources available including Internet, External, and Internet, with the proxy configuration is running in explicit mode. Which method allows the client desktop browsers to be configured to select when to use the proxy?

A. Transparent mode
B. Bridge mode
C. Forward file
D. Pack file

Answer: D

NEW QUESTION 20
- (Exam Topic 4)
Upon receiving a digital certificate, what are three steps that a Cisco ASA will perform to authenticate the digital certificate? (Choose three.)

A. The identity certificate validity period is verified against the system clock of the Cisco ASA.
B. Identity certificates are exchanged during IPsec negotiations.
C. The identity certificate signature is validated by using the stored root certificate.
D. The signature is validated by using the stored identity certificate.
E. If enabled, the Cisco ASA locates the CRL and validates the identity certificate.

Answer: ACE
NEW QUESTION 21

Guaranteed success with Our exam guides
visit - https://www.certshared.com
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions
2nd - Questions and Answers in PDF Format

300-210 Practice Exam Features:

* 300-210 Questions and Answers Updated Frequently
* 300-210 Practice Questions Verified by Expert Senior Certified Staff
* 300-210 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 300-210 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 300-210 Practice Test Here