Certshared now are offering 100% pass ensure 300-207 dumps!
https://www.certshared.com/exam/300-207/ (242 Q&As)

Cisco

Exam Questions 300-207

SITCS Implementing Cisco Threat Control Solutions (SITCS)
NEW QUESTION 1
When https traffic is scanned, which component of the full URL does CWS log?

A. not log
B. only host host and query path and query

Answer: B

NEW QUESTION 2
Refer to the exhibit.

You can click the grey buttons at the bottom of this frame to view the different windows.

To minimize the window, click the [-]. To move the window, click the title bar and drag the window.

Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.
What is the status of OS Identification?

A. It is only enabled to identify "Cisco IOS" OS using statically mapped OS fingerprinting
B. OS mapping information will not be used for Risk Rating calculations.
C. It is configured to enable OS mapping and ARR only for the 10.0.0.0/24 network.
D. It is enabled for passive OS fingerprinting for all networks.

Answer: D

Explanation:
Understanding Passive OS Fingerprinting
Passive OS fingerprinting lets the sensor determine the OS that hosts are running. The sensor analyzes network traffic between hosts and stores the OS of these hosts with their IP addresses. The sensor inspects TCP SYN and SYNACK packets exchanged on the network to determine the OS type. The sensor then uses the OS of the target host OS to determine the relevance of the attack to the victim by computing the attack relevance rating component of the risk rating. Based on the relevance of the attack, the sensor may alter the risk rating of the alert for the attack and/or the sensor may filter the alert for the attack. You can then use the risk rating to reduce the number of false positive alerts (a benefit in IDS mode) or definitively drop suspicious packets (a benefit in IPS mode). Passive OS fingerprinting also enhances the alert output by reporting the victim OS, the source of the OS identification, and the relevance to the victim OS in the alert.

Passive OS fingerprinting consists of three components:
• Passive OS learning
  Passive OS learning occurs as the sensor observes traffic on the network. Based on the characteristics of TCP SYN and SYNACK packets, the sensor makes a determination of the OS running on the host of the source IP address.
• User-configurable OS identification
  You can configure OS host mappings, which take precedence over learned OS mappings.
• Computation of attack relevance rating and risk rating.

NEW QUESTION 3
Who or what calculates the signature fidelity rating in a Cisco IPS?

A. the signature author
B. Cisco Professional Services
C. the administrator
D. the security policy

Answer: A

NEW QUESTION 4
Which Cisco WSA is intended for deployment in organizations of more than 6000 users?

A. WSA S370
B. WSA S670
C. WSA S370-2RU
D. WSA S170

Answer: B

NEW QUESTION 5
Refer to the exhibit.
Which three statements about the Cisco IPS appliance configurations are true? (Choose three.)

A. The maximum number of denied attackers is set to 10000.
B. The block action duration is set to 3600 seconds.
C. The Meta Event Generator is globally enabled.
D. Events Summarization is globally disabled.
E. Threat Rating Adjustment is globally disabled.

Answer: ABC

NEW QUESTION 6
Which command verifies that the correct CWS license key information was entered on the Cisco ASA?

A. sh run scansafe server
B. sh run scansafe
C. sh run server
D. sh run server scansafe

Answer: B

NEW QUESTION 7
Refer to the exhibit.

What CLI command generated the output?

A. smtproutes
B. tophosts
C. hoststatus
D. workqueuestatus

Answer: B

NEW QUESTION 8
Which three functions can Cisco Application Visibility and Control perform? (Choose three.)

A. Validation of malicious traffic
B. Traffic control
C. Extending Web Security to all computing devices
D. Application-level classification
E. Monitoring
F. Signature tuning

Answer: BDE

NEW QUESTION 9
Which three sender reputation ranges identify the default behavior of the Cisco Email Security Appliance? (Choose three.)

A. If it is between -1 and +10, the email is accepted
B. If it is between +1 and +10, the email is accepted
C. If it is between -3 and -1, the email is accepted and additional emails from the sender are throttled
D. If it is between -3 and +1, the email is accepted and additional emails from the sender are throttled
E. If it is between -4 and +1, the email is accepted and additional emails from the sender are throttled
F. If it is between -10 and -3, the email is blocked
G. If it is between -10 and -4, the email is sent to the virus and spam engines for additional scanning
H. If it is between -10 and -4, the email is blocked

Answer: ACF

NEW QUESTION 10
Which configuration option causes an ASA with IPS module to drop traffic matching IPS signatures and to block all traffic if the module fails?

A. Inline Mode, Permit Traffic
B. Inline Mode, Close Traffic
C. Promiscuous Mode, Permit Traffic
D. Promiscuous Mode, Close Traffic

**Answer:** B

**NEW QUESTION 11**

Which five system management protocols are supported by the Intrusion Prevention System? (Choose five.)

A. SNMPv2c
B. SNMPv1
C. SNMPv2
D. SNMPv3
E. syslog
F. SDEE
G. SMTP

**Answer:** ABCFG

**NEW QUESTION 12**

What is a value that Cisco ESA can use for tracing mail flow?

A. the FQDN of the source IP address
B. the FQDN of the destination IP address
C. the destination IP address
D. the source IP address

**Answer:** A

**NEW QUESTION 13**

Which command establishes a virtual console session to a CX module within a Cisco Adaptive Security Appliance?

A. session 1 ip address
B. session 2 ip address
C. session 1
D. session ips console
E. session cxsc console

**Answer:** E

**NEW QUESTION 14**

What is the correct deployment for an IPS appliance in a network where traffic identified as threat traffic should be blocked and all traffic is blocked if the IPS fails?

A. Inline; fail open
B. Inline; fail closed
C. Promiscuous; fail open
D. Promiscuous; fail closed

**Answer:** B

**NEW QUESTION 15**

Which signature engine is responsible for ICMP inspection on Cisco IPS?

A. AIC Engine
B. Fixed Engine
C. Service Engine
D. Atomic IP Engine

**Answer:** D

**NEW QUESTION 16**

What is the access-list command on a Cisco IPS appliance used for?

A. to permanently filter traffic coming to the Cisco IPS appliance via the sensing port
B. to filter for traffic when the Cisco IPS appliance is in the inline mode
C. to restrict management access to the sensor
D. to create a filter that can be applied on the interface that is under attack

**Answer:** C

**NEW QUESTION 17**

Refer to the following. What type of password is “cisco”?

```
Router(config)#service password-encryption
Router(config)#username admin password cisco
```

A. CHAP
B. Type 7
C. Type 0

**Answer:** C
NEW QUESTION 18
Refer to the exhibit.

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. Senders BASE has records for one sender from each of these domains. The list provides the domain name and the Sender BASE Reputation Score for the domain’s sender.

- red public, 4
- orange public, 4
- yellow public, 2
- green public, 2
- blue public, 6
- violet public, 6

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 Sender BASE Reputation Score.

Consider the configuration and the Sender BASE Reputation Scores of the following fictional domains when answering the 5 multiple choice questions.

- red public, 4
- orange public, 4
- yellow public, 2
- green public, 2
- blue public, 6
- violet public, 6

THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.

Look at the MailFlowPolicies tab to access the device configuration. To access the multiple-choice questions, click on the numbered boxes on the left of the top panel. There are 5 multiple-choice questions with this task. You are to answer all five questions before selecting the Next button.
Certshared now are offering 100% pass ensure 300-207 dumps!
https://www.certshared.com/exam/300-207/ (242 Q&As)
Certshared now are offering 100% pass ensure 300-207 dumps!

https://www.certshared.com/exam/300-207/ (242 Q&As)

Guaranteed success with Our exam guides
visit - https://www.certshared.com
Certshared now are offering 100% pass ensure 300-207 dumps!
https://www.certshared.com/exam/300-207/ (242 Q&As)

Guaranteed success with Our exam guides
visit - https://www.certshared.com
Certshared now are offering 100% pass ensure 300-207 dumps!

https://www.certshared.com/exam/300-207/ (242 Q&As)

Guaranteed success with Our exam guides

visit - https://www.certshared.com
Certshared now are offering 100% pass ensure 300-207 dumps!
https://www.certshared.com/exam/300-207/ (242 Q&As)
Certshared now are offering 100% pass ensure 300-207 dumps!

https://www.certshared.com/exam/300-207/ (242 Q&As)
Certshared now are offering 100% pass ensure 300-207 dumps!
https://www.certshared.com/exam/300-207/ (242 Q&As)

Guaranteed success with Our exam guides
visit - https://www.certshared.com
For which domains will the Cisco Email Security Appliance allow up to 5000 recipients per message?

A. violet.public
B. violet.public and blue.public
C. violet.public, blue.public and green.public
D. red.public
E. orange.public
F. red.public and orange.public

Answer: E

Explanation:
Here we see that the TRUSTED policy is being throttled to 5000 recipients per message.

By looking at the HAT policy we see that the TRUSTED policy applies to the WHITELIST sender group.
NEW QUESTION 19
Which two commands are valid URL filtering commands? (Choose two.)

A. url-server (DMZ) vendor smartfilter host 10.0.1.1
B. url-server (DMZ) vendor url-filter host 10.0.1.1
C. url-server (DMZ) vendor n2h2 host 10.0.1.1
D. url-server (DMZ) vendor CISCO host 10.0.1.1
E. url-server (DMZ) vendor web host 10.0.1.1

Answer: AC

NEW QUESTION 20
What is the default antispam policy for positively identified messages?

A. Drop
B. Deliver and Append with [SPAM]
C. Deliver and Prepend with [SPAM]
D. Deliver and Alternate Mailbox

Answer: C

NEW QUESTION 21
......
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

300-207 Practice Exam Features:

* 300-207 Questions and Answers Updated Frequently
* 300-207 Practice Questions Verified by Expert Senior Certified Staff
* 300-207 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 300-207 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click Order The 300-207 Practice Test Here