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

Exam Questions 300-207
SITCS Implementing Cisco Threat Control Solutions (SITCS)
NEW QUESTION 1
What command alters the SSL ciphers used by the Cisco Email Security Appliance for TLS sessions and HTTPS access?

A. sslconfig
B. sgciphers
C. tlsconifg
D. certconfig

Answer: A

NEW QUESTION 2
The Web Cache Communication Protocol (WCCP) is a content-routing protocol that can facilitate the redirection of traffic flows in real time. Your organization has deployed WCCP to redirect web traffic that traverses their Cisco Adaptive Security Appliances (ASAs) to their Cisco Web Security Appliances (WSAs).

The simulator will provide access to the graphical user interfaces of one Cisco ASA and one Cisco WSA that are participating in a WCCP service. Not all aspects of the GUIs are implemented in the simulator. The options that have been implemented are sufficient to determine the best answer to each of the questions that are presented.

Your task is to examine the details available in the simulated graphical user interfaces and select the best answer.
Which of the following is true with respect to the version of WCCP configured on the Cisco ASA and the Cisco WSA?

A. Both are configured for WCCP v1.
B. Both are configured for WCCP v2.
C. Both are configured for WCCP v3.
D. There is a WCCP version mismatch between the Cisco WSA and the Cisco ASA.

Answer: B

Explanation:
ASA version shows as version 2.0:

WSA also shows version 2 is being used:
NEW QUESTION 3
Which commands are required to configure SSH on router? (Choose two.)

A. Configure domain name using `ip domain-name` command
B. Generate a key using `crypto key generate rsa`
C. Configure a DHCP host for the router using `dhcpena#configure terminal`
D. Generate enterprise CA self-sign certificate

Answer: AB

Explanation:
Here are the steps:
1. Configure a hostname for the router using these commands. `yourname#configure terminal`  
   Enter configuration commands, one per line. End with CNTL/Z. `yourname (config)#hostname LabRouter`  
   `LabRouter(config)#hostname CiscoLab.com`
2. Configure a domain name with the `ip domain-name` command followed by whatever you would like your domain name to be. I used `CiscoLab.com`.  
   `LabRouter(config)#ip domain-name CiscoLab.com`  
   We generate a certificate that will be used to encrypt the SSH packets using the `crypto key generate rsa` command.
   Take note of the message that is displayed right after we enter this command: "The name for the keys will be: LabRouter.CiscoLab.com" – it combines the hostname of the router along with the domain name we configured to get the name of the encryption key generated; this is why it was important for us to, first of all, configure a hostname then a domain name before we generated the keys.
References: [https://www.pluralsight.com/blog/tutorials/configure-secure-shell-ssh-on-cisco-router](https://www.pluralsight.com/blog/tutorials/configure-secure-shell-ssh-on-cisco-router)

NEW QUESTION 4
Which two options are known limitations in deploying an IPS sensor in promiscuous mode versus inline mode? (Choose two).

A. It is less effective in stopping email viruses and automated attackers such as worms.
B. It requires less of an operational response because the attacks are blocked automatically without operational team support.
C. Sensors in this deployment cannot stop the trigger packet and are not guaranteed to stop a connection.
D. A sensor failure affects network functionality.
E. It does not see the same traffic.

Answer: AC

NEW QUESTION 5
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 6
Which Cisco Security IntelliShield Alert Manager Service component mitigates new botnet, phishing, and web-based threats?

A. the IntelliShield Threat Outbreak Alert
B. IntelliShield Alert Manager vulnerability alerts
C. the IntelliShield Alert Manager historical database
D. the IntelliShield Alert Manager web portal
E. the IntelliShield Alert Manager back-end intelligence engine

Answer: A

NEW QUESTION 7
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:** AB

**NEW QUESTION 8**
Which statement about Cisco IPS Manager Express is true?

A. It provides basic device management for large-scale deployments.
B. It provides a GUI for configuring IPS sensors and security modules.
C. It enables communication with Cisco ASA devices that have no administrative access.
D. It provides greater security than simple ACLs.

**Answer:** B

**NEW QUESTION 9**
CORRECT TEXT

<table>
<thead>
<tr>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your organization has subscribed to the Cisco Cloud Web Security (CWS) service. You have been assigned the task of configuring the CWS connector on the ISR-G2 router at a branch office. Details of the configuration requirements include:</td>
</tr>
<tr>
<td>- Content scanning should be enabled for traffic outbound from FastEthernet0/1</td>
</tr>
<tr>
<td>- Explicitly specify 8080 for both the http and the https ports</td>
</tr>
<tr>
<td>- The primary CWS proxy server is proxy-a scansafe.net</td>
</tr>
<tr>
<td>- The secondary CWS proxy server is proxy-b scansafe.net</td>
</tr>
<tr>
<td>- The unencrypted license key is 0123456789abcdef</td>
</tr>
<tr>
<td>- If the CWS proxy servers are not available, web traffic from the branch office should be denied</td>
</tr>
<tr>
<td>- After configuration, use show commands to verify connectivity with the CWS service and scan activity</td>
</tr>
</tbody>
</table>

You can access the console of the ISR at the branch office using the icon on the topology display. The enable password is Cisco23.
A. Review the explanation part for full solution.

Explanation:
We need to define the parameter map, specifying port 8080 for http and https and define the servers and the license:
Branch-ISR(config)# parameter-map type content-scan global
Branch-ISR(config-profile)# server scansafe primary name proxy-a.scansafe.net port http 8080 https 8080
Branch-ISR(config-profile)# server scansafe secondary name proxy-b.scansafe.net port http 8080 https 8080
Branch-ISR(config-profile)# license 0 0123456789abcdef
If the CWS proxy servers are not available, we traffic should be denied. This is done by the following configuration:
Branch-ISR(config-profile)# server scansafe on-failure block-all
Now we need to apply this to the fastethernet 0/1 interface outbound:
Branch-ISR(config)# interface Fastethernet 0/1
Branch-ISR(config-if)# content-scan outbound
Branch-ISR(config-if)# exit
Branch-ISR(config)# exit
Finally, we can verify out configuration by using the "show content-scan summary command:
Branch-ISR# show content-scan summary Primary: 72.37.244.203(Up)*
Secondary: 70.39.231.99 (Up) Interfaces: Fastethernet0/1

NEW QUESTION 10
In addition to the CLI, what is another option to manage a Cisco IPS?

A. SDEE
B. Cisco SDM
C. Cisco IDM
D. Cisco ISE

Answer: C

NEW QUESTION 11
CORRECT TEXT
A.

Answer: Steps are in explanation below:

Explanation:
First, enable the Gig 0/0 and Gig 0/1 interfaces:

Second, create the pair under the "interface pairs" tab.
Then, apply the HIGHRISK action rule to the newly created interface pair:

Then apply the same for the MEDIUMRISK traffic (deny attacker inline)

Finally, Log the packets for the LOWRISK event:
NEW QUESTION 12
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
NEW QUESTION 13
Which technique is deployed to harden network devices?
A. port-by-port router ACLs
B. infrastructure ACLs
C. transmit ACLs
D. VLAN ACLs

Answer: B

NEW QUESTION 14
Which three statements about Cisco CWS are true? (Choose three.)
A. It provides protection against zero-day threats.
B. Cisco SIO provides it with threat updates in near real time.
C. It supports granular application policies.
D. Its Roaming User Protection feature protects the VPN from malware and data breaches.
E. It supports local content caching.
F. Its Cognitive Threat Analytics feature uses cloud-based analysis and detection to block threats outside the network.

Answer: ABC

NEW QUESTION 15
Within Cisco IPS anomaly detection, what is the default IP range of the external zone?
A. 0.0.0.0 0.0.0.0
B. 0.0.0.0 - 255.255.255.255
C. 0.0.0.0/8
D. the network of the management interface

Answer: B

NEW QUESTION 16
Refer to the following.
Router (config) #username admin secret cisco Router (config) #no service password-encryption
How is the “cisco” password stored?
A. As Type 0
B. As Type 7
C. As Clear Text

Answer: A

NEW QUESTION 17
Refer to the following. Which description of the result of this configuration is true?
Router(config)#line vty 5 15
Router(config-line)#access-class 23 in
A. Only clients denied in access list 23 can manage the router.
B. Only telnet access (TCP) is allowed on the VTY lines of this router.
C. Only clients permitted in access list 23 can manage the router.
D. Only SSH access (TCP 23) is allowed on the VTY lines of this router.

Answer: C

NEW QUESTION 18
Which Cisco technology secures the network through malware filtering, category-based control, and reputation-based control?
A. Cisco ASA 5500 Series appliances
B. Cisco remote-access VPNs
C. Cisco IronPort WSA
D. Cisco IPS

Answer: C

NEW QUESTION 19
Which two conditions must you configure in an event action rule to match all IPv4 addresses in the victim range and filter on the complete subsignature range? (Choose two.)
A. Disable event action override.
B. Leave the victim address range unspecified.
C. Set the subsignature ID-range to the default.
D. Set the deny action percentage to 100.
E. Set the deny action percentage to 0.

Answer: BC

NEW QUESTION 20
What Event Action in an IPS signature is used to stop an attacker from communicating with a network using an access-list?
A. Request Block Host
B. Deny Attacker Inline
C. Deny Connection Inline
D. Deny Packet Inline
E. Request Block Connection

Answer: A

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