Question 1
Which IPS signature engine inspects the IP protocol packets and the Layer TCP?
A. String TCP
B. Atomic TCP
C. Service HTTP
D. Atomic IP
Correct Answer: D
Explanation/Reference:

Question 2
Which command applies WCCP redirection on the inside interface of a Cisco ASA 5500-x firewall?
A. wccp interface inside 90 redirect in
B. web-cache interface inside 90 redirect in
C. wccp interface inside redirect out
D. wccp web-cache
Correct Answer: A
Explanation/Reference:

Question 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
Correct Answer: A
Explanation/Reference:

Question 4
Refer to the exhibit:
A. Traffic denied in prefix-list 80 is redirected to the Cisco WSA
B. The default “cisco” password is configured on the Cisco WSA
C. Traffic permitted in access-list 80 is redirected to the Cisco WSA
D. Traffic using TCP port 80 is redirected to the Cisco WSA
Correct Answer: C
Explanation/Reference:

Question 5
The Cisco Email Security Appliance will reject messages from which domains?
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 federated domains: SenderBase has records for one sender from each of these domains. The list provides the domain name and the SenderBase Reputation Score for the domain's sender.

- Ver. 300 red public, 4
- Ver. 300 orange public, 4
- Ver. 300 yellow public, 2
- Ver. 300 green public, 2
- Ver. 300 blue public, 8
- Ver. 300 violet public, 5

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 Score.

Instructions

Access the configuration of the Cisco Email Security Appliance using the Mail Flow/Policies tab. Within the GUI, you can navigate between the Mail Flow/Policies 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 federated domains when answering the 5 multiple-choice questions.

- Red public, 4
- Orange public, 4
- Yellow public, 2
- Green public, 2
- Blue public, 8
- Violet public, 5

THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.

Click on the Mail Flow/Policies 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 four multiple-choice questions with the task. Be sure to answer all four questions before selecting the Next button.

---

### Mail Flow Policies

**Policies (Listeners: SummaryMail 172.16.16.25:25, etc.)**

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Behavior</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCEPTED</td>
<td>Accept</td>
<td></td>
</tr>
<tr>
<td>BLOCKED</td>
<td>Reject</td>
<td></td>
</tr>
<tr>
<td>RELATED</td>
<td>Relay</td>
<td></td>
</tr>
<tr>
<td>THROTTLED</td>
<td>Accept</td>
<td></td>
</tr>
<tr>
<td>TRUSTED</td>
<td>Accept</td>
<td></td>
</tr>
</tbody>
</table>

---

Copyright © 2013-2019 Cisco Systems, Inc. All rights reserved. | Privacy Statement

---

http://www.aoowe.com/practice-300-207-3145.html
## HAT Overview

### Find Senders
Find Senders that Contain this Text:

### Sender Groups (List: IncomingMail (172.16.16.0/25 \(\cdot\) ))

<table>
<thead>
<tr>
<th>Order</th>
<th>Sender Group</th>
<th>Sender Reputation Score</th>
<th>Mail Flow Policy</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RELAYLIST</td>
<td></td>
<td>RELAYED</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>WHITELIST</td>
<td></td>
<td>TRUSTED</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>BLACKLIST</td>
<td></td>
<td>BLOCKED</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SUSPECTLIST</td>
<td></td>
<td>THROTTLED</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>UNKNOWNLIST</td>
<td></td>
<td>ACCEPTED</td>
<td></td>
</tr>
<tr>
<td>ALL</td>
<td></td>
<td></td>
<td>ACCEPTED</td>
<td></td>
</tr>
</tbody>
</table>

### Additional Features
- Email Security Manager
- Outgoing Mail Policies
- Outgoing Content Filters
- Mail Flow Policies
- Exception Table
- Address Lists
- Domain Keys
- Verification Profiles
- Signing Profiles
- Signing Keys
- Test Resources
- Dictionaries

---

Copyright © 2000-2013 Cisco Systems, Inc. All rights reserved. Privacy Statement

http://www.cisco.com
### Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25

#### Edit Policy Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>BLOCKED</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Behavior</strong></td>
<td>Reject</td>
</tr>
<tr>
<td>Max. Messages Per Connection</td>
<td>Use Default (10)</td>
</tr>
<tr>
<td>Max. Recipient Per Message</td>
<td>Use Default (50)</td>
</tr>
<tr>
<td>Max. Message Size</td>
<td>Use Default (10MB) (add a trailing \n for long messages)</td>
</tr>
<tr>
<td>Max. Concurrent Connections from a Single IP</td>
<td>Use Default (10)</td>
</tr>
<tr>
<td><strong>SMTP</strong></td>
<td></td>
</tr>
<tr>
<td>Custom SMTP Banner Code</td>
<td>Use Default (554)</td>
</tr>
<tr>
<td>Custom SMTP Banner Text</td>
<td>Use Default ()</td>
</tr>
<tr>
<td>Override SMTP Banner Hostname</td>
<td>Use Hostname from Interface</td>
</tr>
<tr>
<td><strong>Mail Flow Limits</strong></td>
<td></td>
</tr>
<tr>
<td>Rate LIMIT OF Hosts</td>
<td>Max. Recipients Per Hour</td>
</tr>
<tr>
<td>Max. Recipients Per Hour Code</td>
<td>Use Default (452)</td>
</tr>
</tbody>
</table>
The Cisco Email Security Appliance will reject messages from which domains?

A. red.public
B. red.public and orange.public
C. red.public, orange.public and yellow.public
D. orange.public
E. violet.public and blue.public
F. None of the listed domains

Correct Answer: G

Explanation/Reference:

The BLOCKED policy rejects messages as shown below:

http://www.aoowe.com/practice-300-207-3145.html

http://www.aoowe.com/practice-300-207-3145.html

http://www.aoowe.com
The BLOCKED policy is assigned to the BLACKLIST sender group, and here we see that no senders have been applied to this group:

**Question 6**
What is the maximum message size that the Cisco Email Security Appliance will accept from the violet.public domain?
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: SenderBase has records for one sender from each of these domains. The list provides the domain name and the SenderBase Reputation Score for the domain's sender.

- VC20 red public: 4
- orange public: 4
- yellow public: 2
- green public: 2
- blue public: 8
- violet public: 8

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.

Instructions

Access the configuration of the Cisco Email Security Appliance using the Mail Flow Policies tab. Within the GUI, you can navigate between the BAF Overview and Mail Flow Policies pages. 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 fictional domains when answering the 5 multiple-choice questions.

- red public: 4
- orange public: 4
- yellow public: 2
- green public: 2
- blue public: 8
- violet public: 8

**This Task Does Not Require Device Configuration.**

Click on the Mail Flow Policies 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 four multiple-choice questions with the task. Be sure to answer all four questions before selecting the next button.

---

**Mail Flow Policies**

<table>
<thead>
<tr>
<th>Policies (Listener Port: 7155-7165 - 25)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td><strong>ADD Policy</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Policy Name</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>ACCEPTED</td>
</tr>
<tr>
<td>BLOCKED</td>
</tr>
<tr>
<td>RELAYED</td>
</tr>
<tr>
<td>THROTTLED</td>
</tr>
<tr>
<td>TRUSTED</td>
</tr>
</tbody>
</table>

---

Copyright © 2013-2019 Cisco Systems, Inc. All rights reserved. | Privacy Statement
### Sender Group: SUSPECTLIST - IncomingMail 172.16.16.25:25

**Sender Group Settings**

<table>
<thead>
<tr>
<th>Name</th>
<th>SUSPECTLIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>4</td>
</tr>
<tr>
<td>Comments</td>
<td>Suspicious senders are throttled</td>
</tr>
<tr>
<td>Policy</td>
<td>TCP TTL=20</td>
</tr>
<tr>
<td>BRRS (Status)</td>
<td>OOS 3.9</td>
</tr>
<tr>
<td>DNS Lists (Status)</td>
<td>None</td>
</tr>
</tbody>
</table>

**Find Senders**

Find Senders that contain this text: 

**Sender List: Display All Items in List**

<table>
<thead>
<tr>
<th>Sender</th>
<th>Comment</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:nym@nym.co.doc">nym@nym.co.doc</a></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sender</th>
<th>Comment</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:nym@nym.co.doc">nym@nym.co.doc</a></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sender</th>
<th>Comment</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:nym@nym.co.doc">nym@nym.co.doc</a></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2007-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

http://www.aoowe.com/practice-300-207-3145.html

http://www.aoowe.com/practice-300-207-3145.html
300-207 200 Questions Implementing Cisco Threat Control Solutions (SI TCS)

http://www.aoowe.com/practice-300-207-3145.html

http://www.aoowe.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

Correct Answer: D

Explanation/Reference:

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.

By clicking on the ACCEPTED policy we see that max message size has been set to the default value of 10M:
Question 7
What is the maximum number of recipients per hour that the Cisco Email Security Appliance will accept from the green public domain?
### Mail Flow Policies

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Behavior</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCEPTED</td>
<td>Accept</td>
<td></td>
</tr>
<tr>
<td>BLOCKED</td>
<td>Reject</td>
<td></td>
</tr>
<tr>
<td>RELAYED</td>
<td>Relay</td>
<td></td>
</tr>
<tr>
<td>THROTTLLED</td>
<td>Accept</td>
<td></td>
</tr>
<tr>
<td>TRUSTED</td>
<td>Accept</td>
<td></td>
</tr>
</tbody>
</table>

**Default Policy Parameters**

---

### HAT Overview

- Email Security Manager
- Incoming Mail Policies
- Incoming Content Filters
- Outgoing Mail Policies
- Outgoing Content Filters
- Mail Access Table (HAT)
- HAT Overview
- Mail Flow Policies
- Exception Table
- Address Lists

**Sender Groups (List)**

<table>
<thead>
<tr>
<th>Order</th>
<th>Sender</th>
<th>Domain Keys</th>
<th>Verification Profiles</th>
<th>Signature Keys</th>
<th>Signing Keys</th>
<th>Test Resources</th>
<th>Distribution List</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RELAY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>WHITEL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>BLACKL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SUSPEC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>UNKNOWN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Import HAT**

- HAT: 1
- Mail Flow Policy: ACCEPTED
- Delete: 1

---

Copyright © 2013-2014 Cisco Systems, Inc. All rights reserved. | Privacy Statement
### Mail Flow Policy: ACCEPTED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

- **Name:** ACCEPTED

**Connection Behavior**

- **Max. Messages Per Connection:**
  - Use Default (30)  
  - Unlimited

- **Max. Recipients Per Message:**
  - Use Default (50)  
  - Unlimited

- **Max. Message Size:**
  - Use Default (10MB)  
  - Unlimited

- **Max. Concurrent Connections From a Single IP:**
  - Use Default (20)  
  - Unlimited

**SMTP**

- **Custom SMTP Banner Code:**
  - Use Default (220)

- **Custom SMTP Banner Text:**
  - Use Default ()

- **Override SMTP Banner Hostname:**
  - Use Default (Use Hostname from Interface)

**Mail Flow Limits**

- **Rate Limit for Hosts:**
  - Use Default (Unlimited)

- **Max. Recipients Per Hour:**
  - Use Default (Unlimited)

- **Max. Recipients Per Hour Code:**
  - Use Default (452)
### Sender Group: BLACKLIST - IncomingMail 172.16.16.25:25

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>BLACKLIST</td>
</tr>
<tr>
<td>Order</td>
<td>3</td>
</tr>
<tr>
<td>Comment</td>
<td>Spammers are rejected</td>
</tr>
<tr>
<td>Policy</td>
<td>BLOCKED</td>
</tr>
<tr>
<td>SBRS (Optional)</td>
<td>10.0 to -3.9</td>
</tr>
<tr>
<td>DNS Lists (Optional)</td>
<td>None</td>
</tr>
<tr>
<td>Connecting Host DNS Verification</td>
<td>None loaded</td>
</tr>
</tbody>
</table>

#### Find Senders
- Find Senders that Contain This Text: [Submit]

#### Sender List: Display All Items to List
- Add Sender... [Add]

There are no senders.

---

http://www.aoowe.com/practice-300-207-3145.html
### Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25

<table>
<thead>
<tr>
<th>Field</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>BLOCKED</td>
</tr>
<tr>
<td>Connection Behavior</td>
<td>Reject</td>
</tr>
<tr>
<td>Max. Messages Per Connection</td>
<td>Use Default (10)</td>
</tr>
<tr>
<td>Max. Recipients Per Message</td>
<td>Use Default (50)</td>
</tr>
<tr>
<td>Max. Message Size</td>
<td>Use Default (10MB)</td>
</tr>
<tr>
<td>Max. Concurrent Connections From a Single IP</td>
<td>Use Default (150)</td>
</tr>
<tr>
<td>SMTP Banner Code</td>
<td>Use Default (594)</td>
</tr>
<tr>
<td>SMTP Banner Text</td>
<td>Use Default ()</td>
</tr>
<tr>
<td>Override SMTP Banner Hostname</td>
<td>Use Default (Use Hostname from Interface)</td>
</tr>
</tbody>
</table>

### Mail Flow Limits

<table>
<thead>
<tr>
<th>Field</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. Recipients Per Hour</td>
<td>Use Default (Unlimited)</td>
</tr>
<tr>
<td>Max. Recipients Per Hour</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Rate Limit for Hosts</td>
<td>Use Default (45)</td>
</tr>
<tr>
<td>Host Access Table (HAT)</td>
<td></td>
</tr>
<tr>
<td>Exception Table</td>
<td></td>
</tr>
<tr>
<td>Address List</td>
<td></td>
</tr>
<tr>
<td>Recipient Access Table (RAT)</td>
<td></td>
</tr>
<tr>
<td>Recipient Exception Table (RET)</td>
<td></td>
</tr>
<tr>
<td>Originator Address List (OAT)</td>
<td></td>
</tr>
<tr>
<td>Recipient Verification</td>
<td></td>
</tr>
<tr>
<td>Data Protection (DLP)</td>
<td></td>
</tr>
<tr>
<td>Content Filtering (CTF)</td>
<td></td>
</tr>
<tr>
<td>CLP Policy Manager</td>
<td></td>
</tr>
<tr>
<td>Blacklist Actions</td>
<td></td>
</tr>
<tr>
<td>SMTP Banner Code</td>
<td>Use Default (594)</td>
</tr>
<tr>
<td>SMTP Banner Text</td>
<td>Use Default ()</td>
</tr>
<tr>
<td>Override SMTP Banner Hostname</td>
<td>Use Default (Use Hostname from Interface)</td>
</tr>
</tbody>
</table>

---

**Sender Group: RELAYLIST - IncomingMail 172.16.16.25:25**

| **Sender Group Settings** | **Name:** RELAYLIST  
| **Order:** 1  
| **Comment:** Only select hosts can relay from this box  
| **Policy:** RELAYED  
| **SBRS (Optional):** Not in use  
| **DNS Lists (Optional):** None  
| **Connecting Host DNS Verification:** None Included |

**Find Senders**

Find Senders that Contain this Text: 

| **Sender List: Display All Items in List** | **Items per page:** 20  
| **Sender:**  
| **Comment:**  
| **Delete** |

**Sender List: Display All Items in List**

| **Sender:** none.mail,maroon.public  
| **Comment:** None  
| **Delete** |

**Sender Group: RELAYLIST - IncomingMail 172.16.16.25:25**

| **Host Access Table (HAT)** | **Recipient Access Table (RAT)**  
| **Cutoff Policies:**  
| **Exception Table:**  
| **Address Lists:**  
| **Destination Controls:**  
| **Bounce Verification:**  

**Find Senders**

Find Senders that Contain this Text: 

| **Sender List: Display All Items in List** | **Items per page:** 20  
| **Sender:**  
| **Comment:**  
| **Delete** |

**Sender List: Display All Items in List**

| **Sender:** none.mail,maroon.public  
| **Comment:** None  
| **Delete** |

---

http://www.aoowe.com/practice-300-207-3145.html
### Mail Flow Policy: THROTTLED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

**Name:** THROTTLED

**Connection Behavior:**

- **Max. Messages Per Connection:**
  - Use Default (10) [ ]
  - 1 [ ]

- **Max. Recipients Per Message:**
  - Use Default (50) [ ]
  - 50 [ ]

- **Max. Message Size:**
  - Use Default (1MB) [ ]
  - 10485760 [ ]
  - (add a trailing K for kilobytes; M for megabytes)

- **Max. Concurrent Connections from a Single IP:**
  - Use Default (10) [ ]
  - 1 [ ]

**SMTP:**

- **Custom SMTP Banner Code:**
  - Use Default (200) [ ]
  - TCC [ ]

- **Custom SMTP Banner Text:**
  - [ ]

- **Override SMTP Banner Hostname:**
  - Use Default (Use Hostname from Interface) [ ]
  - Use Hostname from Interface [ ]

**Mail Flow Limits**

- **Rate Limit for Hosts:**
  - Max. Recipients Per Hour:
    - Use Default (Unlimited) [ ]
    - Unlimited [ ]
    - 20 [ ]

  - Max. Recipients Per Hour Code:
    - Use Default (452) [ ]

---

### Mail Flow Policy: IncomingMail 172.16.16.25:25

**Edit Policy Settings**

**Name:**

**Connection Behavior:**

- **Max. Messages Per Connection:**
  - Use Default (10) [ ]
  - 1 [ ]

- **Max. Recipients Per Message:**
  - Use Default (50) [ ]
  - 50 [ ]

- **Max. Message Size:**
  - Use Default (1MB) [ ]
  - 10485760 [ ]
  - (add a trailing K for kilobytes; M for megabytes)

- **Max. Concurrent Connections from a Single IP:**
  - Use Default (10) [ ]
  - 1 [ ]

**SMTP:**

- **Custom SMTP Banner Code:**
  - Use Default (200) [ ]
  - TCC [ ]

- **Custom SMTP Banner Text:**
  - [ ]

- **Override SMTP Banner Hostname:**
  - Use Default (Use Hostname from Interface) [ ]
  - Use Hostname from Interface [ ]

**Mail Flow Limits**

- **Rate Limit for Hosts:**
  - Max. Recipients Per Hour:
    - Use Default (Unlimited) [ ]
    - Unlimited [ ]
    - 20 [ ]

  - Max. Recipients Per Hour Code:
    - Use Default (452) [ ]
What is the maximum number of recipients per hour that the Cisco Email Security Appliance will accept from the green public domain?

A. 0
B. 1
C. 20
D. 25
E. 50
F. 5000
G. Unlimited

Correct Answer: C

Explanation/Reference:
Explanation:
From the instructions we know that the green.public domain has been assigned a reputation score of 2. From below we know that a reputation score of 2 belongs to the SUSPECTLIST, which has a policy of “THROTTLED”.

By clicking on the THROTTLED policy we see that the max recipients per hour has been set to 20:

Question 8
For which domains will the Cisco Email Security Appliance allow up to 5000 recipients per message?
### Mail Flow Policy: ACCEPTED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**
- **Name:** ACCEPTED
- **Connection Behavior:** Accept
  - **Max. Messages Per Connection:** Use Default (30)
  - **Max. Recipients Per Message:** Use Default (50)
  - **Max. Message Size:** Use Default (20M)
    - (add a trailing k for kilobytes; M for megabytes)
  - **Max. Concurrent Connections From a Single IP:** Use Default (10)
- **SNMP**
  - **Custom SNMP Banner Code:** Use Default (220)
  - **Custom SNMP Banner Text:** Use Default (2)
  - **Override SNMP Banner Hostname:** Use Default (Use Hostname from Interface)
- **Mail Flow Limits**
  - **Rate Limit for Hosts:** Unlimited
  - **Max. Recipients Per Hour:** Unlimited
  - **Max. Recipients Per Hour Code:** Use Default (42)

---

### Mail Flow Policy: incomingMail 172.16.16.25:25

**Edit Policy Settings**
- **Host Access Table (HAT)**
- **NAT Overview**
- **Connection Filter**
  - **Mail Flow Policies**
  - **Address Usages**
  - **Recipient Access Table (RAT)**
  - **Destination Context**
  - **Header Verification**
  - **Data Loss Prevention (DLP)**
  - **UDP Policy Manager**
  - **UDP Message Actions**
- **Domain Keys**
  - **Verification Profiles**
  - **Signing Profiles**
  - **Signing Keys**
- **Text Resources**
  - **Dictionaries**
- **Mail Flow Limits**
  - **Rate Limit for Hosts:** Unlimited
  - **Max. Recipients Per Hour:** Unlimited
  - **Max. Recipients Per Hour Code:** Use Default (42)

---

http://www.aoowe.com/practice-300-207-3145.html
### Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25

#### Edit Policy Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>BLOCKED</td>
</tr>
<tr>
<td>Connection Behavior</td>
<td>Reject</td>
</tr>
<tr>
<td>Max. Messages Per Connection</td>
<td>Use Default (10)</td>
</tr>
<tr>
<td>Max. Recipients Per Message</td>
<td>Use Default (50)</td>
</tr>
<tr>
<td>Max. Message Size</td>
<td>Use Default (L)</td>
</tr>
<tr>
<td>Max. Concurrent Connections From a Single IP</td>
<td>Use Default (10)</td>
</tr>
<tr>
<td>SMTP: Custom SMTP Banner Text</td>
<td>Not configured</td>
</tr>
<tr>
<td>SMTP: Custom SMTP Banner Code</td>
<td>Not configured</td>
</tr>
<tr>
<td>Override SMTP Banner Hostname</td>
<td>Use Default (Use Hostname from Interface)</td>
</tr>
</tbody>
</table>

#### Mail Flow Limits

<table>
<thead>
<tr>
<th>Limit</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limit for Hosts: Max. Recipients Per Hour</td>
<td>Use Default (Unlimited)</td>
</tr>
<tr>
<td>Rate Limit for Hosts: Max. Recipients Per Hour Code</td>
<td>Use Default</td>
</tr>
</tbody>
</table>

---

### Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25

#### Edit Policy Settings
- **Name:** RELAYED

#### Connection Behavior
- **Max. Messages Per Connection:**
  - Use Default (10)
  - Use Default (50)
  - Use Default (LIM)

- **Max. Recipients Per Message:**
  - Use Default (10)
  - Use Default (50)
  - Use Default (LIM)

- **Max. Message Size:**
  - Use Default (10)
  - Use Default (50)
  - Use Default (LIM)

- **Max. Concurrent Connections From a Single IP:**
  - Use Default (10)
  - Use Default (50)
  - Use Default (LIM)

#### SMTP
- **Custom SMTP Banner Code:**
  - Use Default (220)

- **Custom SMTP Banner Text:**
  - Use Default

- **Override SMTP Banner Hostname:**
  - Use Default (Use Hostname from Interface)
  - Use Hostname from Interface

#### Mail Flow Limits
- **Rate Limit for Hosts:**
  - Max. Recipients Per Hour:
    - Use Default (Unlimited)
    - Unlimited

- **Max. Recipients Per Hour Code:**
  - Use Default (482)
Sender Group: RELAYLIST - IncomingMail 172.16.16.25:25

Sender Group Settings
Name: RELAYLIST
Order: 1
Comment: Only select hosts can relay from this box
Policy: RELAYED
SBRS (Optional): Not in use
DNS Lists (Optional): None
Connecting Host DNS Verification: None

Senders

Find Senders
Find Senders that Contain this Text:

Sender List: Display All Items in List
Add Sender:
Sender: to-mail.maron.public
Comment: None

Delete

Items per page 20

http://www.aoowe.com/practice-300-207-3145.html
http://www.aoowe.com/practice-300-207-3145.html
### Mail Flow Policy: THROTTLED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**
- **Name:** THROTTLED

**Connection Behavior**
- **Max. Messages Per Connection:**
  - Use Default (10)
  - 1

**SMTP**
- **Custom SMTP Banner Code:**
  - Use Default (220)
  - USE220

**Mail Flow Limits**
- **Rate Limit for Hosts:**
  - **Max. Recipients Per Hour:**
    - Use Default (Unlimited)
    - Unlimited
    - 50

---

### Mail Flow Policy: IncomingMail 172.16.16.25:25

**Edit Policy Settings**
- **Name:**

**Host Access Table (HAT)**
- **Max. Recipients Per Connection:**
  - Use Default (10)
  - 1

**SMTP Banner Code:**
- **Use Default (220):**
  - USE220

**Mail Flow Limits**
- **Rate Limit for Hosts:**
  - **Max. Recipients Per Hour:**
    - Use Default (Unlimited)
    - Unlimited
    - 50
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

Correct Answer: E

Explanation/Reference:

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.

By clicking on the WHITELIST sender group we can see that orange.public is listed as the sender.
Question 9
SIMULATION

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:

- Content scanning should be enabled for traffic outbound from FastEthernet0/1
- Explicitly specify 8080 for both the http and the https ports
- The primary CWS proxy server is proxy-a.sansafe.net
- The secondary CWS proxy server is proxy-b.sansafe.net
- The username/license key is 912548597696abdef
- If the CWS proxy servers are not available, web traffic from the branch office should be denied

After configuration, use show commands to verify connectivity with the CWS service and scan activity. You can access the console of the ISR at the branch office using the login of JohnDoe. The enable password is Cisco23.
Correct Answer: Review the explanation part for full solution

Explanation/Reference:

We need to define the parameter map, specifying port 8080 for http and https and define the servers and the license:

```yaml
Branch-ISR(config)
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, the traffic should be denied. This is done by the following configuration:

```yaml
Branch-ISR(config-profile)#server scansafe on-failure block-all
```

Now we need to apply this to the fastethernet 0/1 interface outbound:

```yaml
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 our configuration by using the "show content-scan summary" command:

```yaml
Branch-ISR#show content-scan summary
Primary: 72.37.244.203 (Up)*
Secondary: 70.39.231.99 (Up)
Interfaces: Fastethernet0/1
```

**Question 10**

**SIMULATION**

**SIMULATION**

Your organization is deploying the ASA CX software module in the ASA. You connect the organization’s internal network to the Internet. A colleague has configured the policy in the CX module. Your task is to configure the ASA to forward the appropriate traffic to the CX module for processing.

Currently, there are no policies configured for the inside interface. Your goal is to match all traffic which traverses the inside interface using the system default schedule, and send that traffic to the CX module. The CX will use active authentication. Also in the event of a CX module failure, no traffic should be allowed.

Access to the console of the ASA by clicking on the icon in the topology map. The enable password is Cisco23.

Use inside policy as the name of the policy map that will configure after you have successfully applied the policy map to the inside interface, verify that it is active using an appropriate show command.
We need to create a policy map named inside-policy and send the traffic to the CXSC blade:

```
ASA-FW# config t
ASA-FW(config)# policy-map inside-policy
ASA-FW(config-pmap)# class class-default
ASA-FW(config-pmap-c)# cxsc fail-close auth-proxy
ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit
```

The fail-close is needed as per instructions that if the CX module fails, no traffic should be allowed. The auth-proxy keyword is needed for active authentication.

Next, we need to apply this policy map to the inside interface:

```
ASA-FW(config)# service-policy inside-policy interface inside.
```

Finally, verify that the policy is active:

```
ASA-FW# show service-policy interface inside
Interface inside:
Service-policy: inside-policy
Class-map: class-default
Default Queuing CXSC: card status Up, mode fail-close, auth-proxy enabled
Packet input 181, packet output 183, drop 0, reset-drop 0, proxied 0
```

Configuration guidelines can be found at this reference link:


**Question 11**
Which interface on the Cisco Email Security Appliance has HTTP and SSH enabled by default?

A. data 1
B. data 2
C. management 1
D. all interfaces

Correct Answer: A

**Explanation/Reference:**

**Question 12**
Which two options are the correct URL and credentials used to access the Cisco Web Security Appliance for the first time? (Choose two.)

A. admin/password
B. http://192.168.1.1:8080
C. ironport/ironport
D. http://192.168.42.42:8080
E. admin/ironport
F. http://192.168.42.42:8443

Correct Answer: DE

**Explanation/Reference:**

**Question 13**
Which platform has message tracking enabled by default?

A. C670
B. C370
C. Virtual ESA
D. It is not enabled by default on any platform.

Correct Answer: D

**Explanation/Reference:**

**Question 14**
When centralized message tracking is enabled on the Cisco ESA, over which port does the communication to the SMA occur by default?

When centralized message tracking is enabled on the Cisco ESA, over which port does the communication to the SMA occur by default?
A. port 2222/TCP  
B. port 443/TCP  
C. port 25/TCP  
D. port 22/TCP  

Correct Answer: D  
Explanation/Reference:

Question 15  
Which four methods are used to deploy transparent mode traffic redirection?  
Which four methods are used to deploy transparent mode traffic redirection? (Choose four.)  
A. PAC files  
B. Web Cache Communication Protocol  
C. policy-based routing  
D. Microsoft GPO  
E. Layer 4 switch  
F. DHCP server  
G. Layer 7 switch  
H. manual browser configuration  

Correct Answer: BCEG  
Explanation/Reference:

Question 16  
When a user receives an encrypted email from a Cisco ESA, which technology is used to retrieve the key to open the email?  
When a user receives an encrypted email from a Cisco ESA, which technology is used to retrieve the key to open the email?  
A. trusted certificate authority  
B. private certificate authority  
C. Cisco Registered Envelope Service  
D. Simple Certificate Enrollment Protocol  

Correct Answer: C  
Explanation/Reference:

Question 17  
Where should an operator navigate to determine the running software image on the Cisco WSA?  
Using the Cisco WSA GUI, where should an operator navigate to determine the running software image on the Cisco WSA?  
A. Systems Administration > System Upgrade  
B. Systems Administration > Feature Keys  
C. Systems Administration > General  
D. Admin > System Info  

Correct Answer: A  
Explanation/Reference:

Question 18  
Which option describes how the native VLAN is set up on an IPS sensor when VLAN groups are used in an inline deployment of the sensor?  
Which option describes how the native VLAN is set up on an IPS sensor when VLAN groups are used in an inline deployment of the sensor?  
A. The sensor looks at the native VLAN setup on the switch to determine the correct native VLAN to use.  
B. The sensor does not care about VLANs.  
C. A default VLAN variable must be associated with each physical interface on the sensor.  
D. There is no way to set this, so you need to tag all traffic.  
E. ISL links are only supported.  

Correct Answer: C  
Explanation/Reference:

Question 19  
Which two options are known limitations in deploying an IPS sensor in promiscuous mode versus inline mode?  
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.  

Correct Answer: AC  
Explanation/Reference:

Question 20  
Which option describes a customer benefit of the Cisco Security IntelliShield Alert Manager?  
Which option describes a customer benefit of the Cisco Security IntelliShield Alert Manager?  
A. It provides access to threat and vulnerability information for Cisco related products only.  
B. It consolidates vulnerability information from an internal Cisco source, which allows security personnel to focus on remediation and proactive protection versus research.  
C. It provides effective and timely security intelligence via early warnings about new threats and technology vulnerabilities.  
D. It enhances the efficiency of security staff with accurate, noncustomizable threat intelligence, critical remediation information, and easy-to-use workflow tools.  

Correct Answer: C  
Explanation/Reference:
Question 21
Which three categories of the seven major risk management categories are covered in the Cyber Risk Reports?

Which three categories of the seven major risk management categories are covered in the Cyber Risk Reports? (Choose three.)
A. vulnerability
B. risk rating
C. legal
D. confidence level
E. geopolitical
F. global reputation

Correct Answer: ACE
Explanation/Reference:

Question 22
Which solution must a customer deploy to prioritize traffic to a cloud-based contact management application while still allowing employees access to the Internet for business and personal use?

Which solution must a customer deploy to prioritize traffic to a cloud-based contact management application while still allowing employees access to the Internet for business and personal use?
A. Cisco Application Visibility and Control
B. Cisco Intrusion Prevention Services
C. Cisco NetFlow
D. policy-based routing

Correct Answer: A
Explanation/Reference:

Question 23
Which option is a benefit of deploying Cisco Application Visibility and Control?

Which option is a benefit of deploying Cisco Application Visibility and Control?
A. It ensures bandwidth availability and performance of mission-critical applications in a data- and media-rich environment.
B. It performs deep packet inspection of mission-critical applications in a data- and media-rich environment.
C. It encrypts mission-critical applications in a data- and media-rich environment.
D. It securely tunnels mission-critical applications in a data- and media-rich environment.

Correct Answer: A
Explanation/Reference:

Question 24
Which technology is used to improve business-critical application performance?

Which technology is used to improve business-critical application performance?
A. Application Visibility and Control
B. Intrusion Prevention Services
C. Advanced Malware Protection
D. TrustSec

Correct Answer: A
Explanation/Reference:

Question 25
Which option is a benefit of Cisco hybrid email security?

Which option is a benefit of Cisco hybrid email security?
A. on-premises control of outbound data
B. advanced malware protection
C. email encryption
D. message tracking

Correct Answer: A
Explanation/Reference:

Question 26
Which option is a benefit of Cisco Email Security virtual appliance over the Cisco ESA appliance?

Which option is a benefit of Cisco Email Security virtual appliance over the Cisco ESA appliance?
A. reduced space and power requirements
B. outbound message protection
C. automated administration
D. global threat intelligence updates from Talos

Correct Answer: A
Explanation/Reference:

Question 27
Which feature of the Cisco Hybrid Email Security services enables you to create multiple email senders on a single Cisco ESA?

Which feature of the Cisco Hybrid Email Security services enables you to create multiple email senders on a single Cisco ESA?
A. Virtual Gateway
B. Sender Groups
C. Mail Flow Policy Connector
D. Virtual Routing and Forwarding
E. Email Marketing Connector

Correct Answer: A
Explanation/Reference:
Question 28
Which Cisco Web Security Appliance feature enables the appliance to block suspicious traffic on all of its ports and IP addresses?
A. Layer 4 Traffic Monitor
B. Secure Web Proxy
C. explicit forward mode
D. transparent mode
Correct Answer: A
Explanation/Reference:

Question 29
What is a difference between a Cisco Content Security Management virtual appliance and a physical appliance?
A. The virtual appliance requires an additional license to run on a host.
B. The physical appliance requires an additional license to activate its adapters.
C. Migration between virtual appliances of varying sizes is possible, but physical appliances must be of equal size.
D. The physical appliance is configured with a DHCP-enabled management port to receive an IP address automatically, but you must assign the virtual appliance an IP address manually in your management subnet.
Correct Answer: A
Explanation/Reference:

Question 30
What is the function of the Web Proxy Auto-Discovery protocol?
A. It enables a web client to discover the URL of a configuration file.
B. It enables a web client to download a script or configuration file that is named by a URL.
C. It enables a web client’s traffic flows to be redirected in real time.
D. It enables web clients to dynamically resolve hostname records.
Correct Answer: A
Explanation/Reference:

Question 31
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
Correct Answer: C
Explanation/Reference:

Question 32
What are three arguments that can be used with the show content-scan command in Cisco IOS software?
A. session
B. data
C. verbose
D. buffer
E. summary
F. statistics
Correct Answer: AEF
Explanation/Reference:

Question 33
Which website can be used to validate group information about connections that flow through Cisco CWS?
A. whoami.scansafe.net
B. policytrace.scansafe.net
C. whoami.scansafe.com
D. policytrace.scansafe.com
Correct Answer: B
Explanation/Reference:

Question 34
What is a valid search parameter for the Cisco ESA find event tool?
A. Envelope Origination
B. Envelope Type
C. Message ID
D. Download Type
Correct Answer: C
Explanation/Reference:
Question 35
Which piece of information is required to perform a policy trace for the Cisco WSA?
A. the URL to trace
B. the source IP address of the trace
C. authentication credentials to make the request
D. the destination IP address of the trace

Correct Answer: A
Explanation/Reference:

Question 36
Which action can be taken to correct the problem?
You ran the ssh generate-key command on the Cisco IPS and now administrators are unable to connect. Which action can be taken to correct the problem?
A. Replace the old key with a new key on the client.
B. Run the ssh host-key command.
C. Add the administrator IP addresses to the trusted TLS host list on the IPS.
D. Run the ssh authorized-keys command.

Correct Answer: A
Explanation/Reference:

Question 37
Which additional configuration must you perform to enable the switch to pass traffic?
You have configured a VLAN pair that is connected to a switch that is unable to pass traffic. If the IPS is configured correctly, which additional configuration must you perform to enable the switch to pass traffic?
A. Configure access ports on the switch.
B. Configure the trunk port on the switch.
C. Enable IP routing on the switch.
D. Enable ARP inspection on the switch.

Correct Answer: A
Explanation/Reference:

Question 38
Which feature does Acceptable Use Controls use to implement Cisco AVC?
A. ISA
B. Cisco Web Usage Controls
C. Cisco WSA
D. Cisco ESA

Correct Answer: B
Explanation/Reference:

Question 39
Which type of server is required to communicate with a third-party DLP solution?
A. an HTTPS server
B. an HTTP server
C. an ICAP-capable proxy server
D. a PKI certificate server

Correct Answer: C
Explanation/Reference:

Question 40
Which of the following is true with respect to the version of WCCP configured on the Cisco ASA and the Cisco WSA?
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.

Correct Answer: B

Explanation/Reference:
ASA version shows as version 2.0:
WSA also shows version 2 is being used:
What is true with respect to redirected ports?
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.

### Question 41

What is true with respect to redirected ports?

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.

#### Transparent Redirection

<table>
<thead>
<tr>
<th>Transparent Redirection Device</th>
<th>Type: WCCP v2 Router</th>
</tr>
</thead>
</table>

#### WCCP v2 Services

<table>
<thead>
<tr>
<th>Service Profile Name</th>
<th>Service ID</th>
<th>Router IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebTrafficFromASA</td>
<td>10</td>
<td>10.10.1.1</td>
</tr>
</tbody>
</table>
Between the Cisco ASA configuration and the Cisco WSA configuration, what is true with respect to redirected ports?

A. Both are configured for port 80 only.
B. Both are configured for port 443 only.
C. Both are configured for both port 80 and 443.
D. Both are configured for ports 80, 443 and 3128.
E. There is a configuration mismatch on redirected ports.

Correct Answer: C

Explanation/Reference:
This can be seen from the WSA Network tab shown below:
Question 42

What traffic is not redirected by WCCP?

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.
What traffic is not redirected by WCCP?

A. Traffic destined to public address space
B. Traffic sent from public address space
C. Traffic destined to private address space
D. Traffic sent from private address space

Correct Answer: B

Explanation/Reference:

From the screenshot below we see the WCCP-Redirection ACL is applied, so all traffic from the Private IP space to any destination will be redirected.

Question 43

How many Cisco ASAs and how many Cisco WSAs are participating in the WCCP service?

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.
How many Cisco ASAs and how many Cisco WSAs are participating in the WCCP service?

A. One Cisco ASA or two Cisco ASAs configured as an Active/Standby failover pair, and one Cisco WSA.
B. One Cisco ASA or two Cisco ASAs configured as an Active/Active failover pair, and one Cisco WSA.
C. One Cisco ASA or two Cisco ASAs configured as an Active/Standby failover pair, and two Cisco WSAs.
D. One Cisco ASA or two Cisco ASAs configured as an Active/Active failover pair, and two Cisco WSAs.
E. Two Cisco ASAs and one Cisco WSA.
F. Two Cisco ASAs and two Cisco WSAs.

Correct Answer: A
Explanation/Reference:
We can see from the output that the number of routers (ASA's) is 1, so there is a single ASA or an active/standby pair being used, and 1 Cache Engine.
If the ASA's were in a active/active role it would show up as 2 routers.

Question 44
What is the function of the Cisco Context Adaptive Scanning Engine in Cisco Hybrid Email Security services?

A. It uses real-time traffic threat assessment to identify suspicious email senders and messages.
B. It provides a preventive defense against viruses by scanning messages before they enter the network.
C. It analyzes message content and attachments to protect an organization's intellectual property.
D. It protects against blended threats by using human-like logic to review and evaluate traffic.

Correct Answer: D
Explanation/Reference:

Question 45
Which Cisco ESA component receives connections from external mail servers?

A. MTA
B. public listener
C. private listener
D. recipient acceptable table
E. SMTP incoming relay agent

Correct Answer: B
Explanation/Reference:

Question 46
Which Cisco Cloud Web Security Connector feature allows access by all of an organization’s users while applying Active Directory group policies?

A. a company authentication key
B. a group authentication key
C. a PAC file
D. proxy forwarding
E. a user authentication key

Correct Answer: A
Explanation/Reference:

http://www.aoowe.com/practice-300-207-3145.html
A. no fail-open  
B. fail-close  
C. fail-close auth-proxy  
D. auth-proxy  
Correct Answer: B  
Explanation/Reference:

Question 48  
What is a primary difference between the web security features of the Cisco WSA and the Cisco ASA NGFW?  
What is a primary difference between the web security features of the Cisco WSA and the Cisco ASA NGFW?  
A. Cisco WSA provides URL filtering, while Cisco ASA NGFW does not.  
B. Cisco ASA NGFW provides caching services, while Cisco WSA does not.  
C. Cisco WSA provides web reputation filtering, while Cisco ASA NGFW does not.  
D. Cisco ASA NGFW provides application visibility and control on all ports, while Cisco WSA does not.  
Correct Answer: D  
Explanation/Reference:

Question 49  
Which two statements about devices within a Cisco ESA cluster are true?  
Which two statements about devices within a Cisco ESA cluster are true? (Choose two.)  
A. Clustered systems must consist of devices in the same hardware series.  
B. Clustered devices can communicate via either SSH or Cluster Communication Service.  
C. Clustered devices can communicate only with Cluster Communication Service.  
D. In-the-cloud devices must be in a separate cluster from on-premise devices.  
E. Clustered devices can run different versions of AsyncOS.  
Correct Answer: AB  
Explanation/Reference:

Question 50  
Which two statements about devices within a Cisco ESA cluster are true?  
Which two statements about devices within a Cisco ESA cluster are true? (Choose two.)  
A. A cluster must contain exactly one group.  
B. A cluster can contain multiple groups.  
C. Clusters are implemented in a client/server relationship.  
D. The cluster configuration must be managed by the cluster administrator.  
E. The cluster configuration can be created and managed through either the GUI or the CLI.  
Correct Answer: BE  
Explanation/Reference:

Question 51  
Which role does Passive Identity Management play in the Cisco Cloud Web Security architecture?  
Which role does Passive Identity Management play in the Cisco Cloud Web Security architecture?  
A. It provides user-level information that is received from Active Directory.  
B. It enables the administrator to control web access for users and user groups.  
C. It defines a standard for exchanging authentication and authorization data.  
D. It controls content that passes into and out of the network.  
Correct Answer: A  
Explanation/Reference:

Question 52  
Which sensor deployment mode does Cisco recommend when interface capacity is limited and you need to increase sensor functionality?  
Which sensor deployment mode does Cisco recommend when interface capacity is limited and you need to increase sensor functionality?  
A. inline interface pair mode  
B. inline VLAN pair mode  
C. inline VLAN group mode  
D. VLAN group mode  
Correct Answer: C  
Explanation/Reference:

Question 53  
What is a side effect?  
If inline-TCP-evasion-protection-mode on a Cisco IPS is set to asymmetric mode, what is a side effect?  
A. Packet flow is normal.  
B. TCP requests are throttled.  
C. Embryonic connections are ignored.  
D. Evasion may become possible.  
Correct Answer: D  
Explanation/Reference:

Question 54  
When a Cisco IPS is deployed in fail-closed mode, what are two conditions that can result in traffic being dropped?  
When a Cisco IPS is deployed in fail-closed mode, what are two conditions that can result in traffic being dropped? (Choose two.)  
A. The signature engine is undergoing the build process.  
B. The SDF failed to load.
C. The built-in signatures are unavailable.
D. An ACL is configured.

Correct Answer: AB
Explanation/Reference:

Question 55
Which Cisco IPS deployment mode is best suited for bridged interfaces?
Which Cisco IPS deployment mode is best suited for bridged interfaces?
A. inline interface pair mode
B. inline VLAN pair mode
C. inline VLAN group mode
D. inline pair mode

Correct Answer: B
Explanation/Reference:

Question 56
Which IPS feature allows you to aggregate multiple IPS links over a single port channel?
Which IPS feature allows you to aggregate multiple IPS links over a single port channel?
A. UDLD
B. ECLB
C. LACP
D. PAgP

Correct Answer: B
Explanation/Reference:

Question 57
What are three features of the Cisco Security Intellishield Alert Manager Service?
What are three features of the Cisco Security Intellishield Alert Manager Service? (Choose three.)
A. validation of alerts by security analysts
B. custom notifications
C. complete threat and vulnerability remediation
D. vendor-specific threat analysis
E. workflow-management tools
F. real-time threat and vulnerability mitigation

Correct Answer: ABE
Explanation/Reference:

Question 58
What is a value that Cisco ESA can use for tracing mail flow?
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

Correct Answer: A
Explanation/Reference:

Question 59
Which centralized reporting function of the Cisco Content Security Management Appliance aggregates data from multiple Cisco ESA devices?
Which centralized reporting function of the Cisco Content Security Management Appliance aggregates data from multiple Cisco ESA devices?
A. message tracking
B. web tracking
C. system tracking
D. logging

Correct Answer: A
Explanation/Reference:

Question 60
Which three administrator actions are used to configure IP logging in Cisco IME?
Which three administrator actions are used to configure IP logging in Cisco IME? (Choose three.)
A. Select a virtual sensor.
B. Enable IP logging.
C. Specify the host IP address.
D. Set the logging duration.
E. Set the number of packets to capture.
F. Set the number of bytes to capture.

Correct Answer: ACD
Explanation/Reference:

Question 61
When you create a new server profile on the Cisco ESA, which subcommand of the ldapconfig command configures spam quarantine end-user authentication?
When you create a new server profile on the Cisco ESA, which subcommand of the ldapconfig command configures spam quarantine end-user authentication?
A. isqauth
B. isqalias
C. test
D. server

Correct Answer: A
Explanation/Reference:

**Question 62**
Which command disables SSH access for administrators on the Cisco ESA?

Which command disables SSH access for administrators on the Cisco ESA?
A. interfaceconfig
B. sshconfig
C. sslconfig
D. systemsetup

Correct Answer: A
Explanation/Reference:

**Question 63**
Which Cisco ESA predefined sender group uses parameter-matching to reject senders?

Which Cisco ESA predefined sender group uses parameter-matching to reject senders?
A. BLACKLIST
B. WHITELIST
C. SUSPECTLIST
D. UNKNOWNLIST

Correct Answer: A
Explanation/Reference:

**Question 64**
When you configure the Cisco ESA to perform blacklisting, what are two items you can disable to enhance performance? (Choose two.)

When you configure the Cisco ESA to perform blacklisting, what are two items you can disable to enhance performance? (Choose two.)
A. spam scanning
B. antivirus scanning
C. APT detection
D. rootkit detection

Correct Answer: AB
Explanation/Reference:

**Question 65**
Which command can change the HTTPS SSL method on the Cisco ESA?

Which command can change the HTTPS SSL method on the Cisco ESA?
A. sslconfig
B. strictssl
C. sshconfig
D. adminaccessconfig

Correct Answer: A
Explanation/Reference:

**Question 66**
Which command allows the administrator to access the Cisco WSA on a secure channel on port 8443?

Which command allows the administrator to access the Cisco WSA on a secure channel on port 8443?
A. strictssl
B. adminaccessconfig
C. ssl
D. ssh

Correct Answer: A
Explanation/Reference:

**Question 67**
Which action can be taken to correct the problem?

You ran the ssh generate-key command on the Cisco IPS and now administrators are unable to connect. Which action can be taken to correct the problem?
A. Replace the old key with a new key on the client.
B. Run the ssh host-key command.
C. Add the administrator IP addresses to the trusted TLS host list on the IPS.
D. Run the ssh authorized-keys command.

Correct Answer: A
Explanation/Reference:

**Question 68**
Which Cisco technology provides spam filtering and email protection?

Which Cisco technology provides spam filtering and email protection?
A. IPS
B. ESA
C. WSA
D. CX

Correct Answer: B
Question 69
What can you use to access the Cisco IPS secure command and control channel to make configuration changes?
A. SDEE
B. the management interface
C. an HTTP server
D. Telnet
Correct Answer: B

Question 70
What is a possible reason for this behavior?
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.
Correct Answer: A

Question 71
Which three statements about threat ratings are true? (Choose three.)
A. A threat rating is equivalent to a risk rating that has been lowered by an alert rating.
B. The largest threat rating from all actioned events is added to the risk rating.
C. The smallest threat rating from all actioned events is subtracted from the risk rating.
D. The alert rating for deny-attacker-inline is 45.
E. Unmitigated events do not cause a threat rating modification.
F. The threat rating for deny-attacker-inline is 50.
Correct Answer: ADE

Question 72
In which way are packets handled when the IPS internal zone is set to “disabled”?
A. All packets are dropped to the external zone.
B. All packets are dropped to the internal zone.
C. All packets are ignored in the internal zone.
D. All packets are sent to the default external zone.
Correct Answer: D

Question 73
Which statement about the knowledge base is true?
If learning accept mode is set to “auto” and the knowledge base is loaded only when explicitly requested on the IPS, which statement about the knowledge base is true?
A. The knowledge base is set to load dynamically.
B. The knowledge base is set to “save only.”
C. The knowledge base is set to “discarded.”
D. The knowledge base is set to load statically.
Correct Answer: B

Question 74
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.
Correct Answer: BC

Question 75
When you deploy a sensor to send connection termination requests, which additional traffic-monitoring function can you configure the sensor to perform?
When you deploy a sensor to send connection termination requests, which additional traffic-monitoring function can you configure the sensor to perform?
A. Monitor traffic as it flows to the sensor.
B. Monitor traffic as it flows through the sensor.
C. Monitor traffic from the Internet only.
D. Monitor traffic from both the Internet and the intranet.
Question 76
Which two conditions must you configure in an event action override to implement a risk rating of 70 or higher and terminate the connection on the IPS?
A. Configure the event action override to send a TCP reset.
B. Set the risk rating range to 70 to 100.
C. Configure the event action override to send a block-connection request.
D. Set the risk rating range to 0 to 100.
E. Configure the event action override to send a block-host request.
Correct Answer: AB

Question 77
Which type of signature is generated by copying a default signature and modifying its behavior?
A. meta
B. custom
C. atomic
D. normalized
Correct Answer: B

Question 78
Over the period of one day, several Atomic ARP engine alerts fired on the same IP address. You observe that each time an alert fired, requests on the IP address exceeded replies by the same number. Which configuration could cause this behavior?
A. The reply-ratio parameter is enabled.
B. MAC flip is enabled.
C. The inspection condition is disabled.
D. The IPS is misconfigured.
Correct Answer: A

Question 79
Which configuration mode enables a virtual sensor to monitor the session state for unidirectional traffic?
A. asymmetric mode
B. symmetric mode
C. loose mode
D. strict mode
Correct Answer: A

Question 80
Which method does Cisco recommend for collecting streams of data on a sensor that has been virtualized?
A. VACL capture
B. SPAN
C. the Wireshark utility
D. packet capture
Correct Answer: D

Question 81
Which three pieces of information are required to implement transparent user identification using Context Directory Agent?
A. the server name of the global catalog domain controller
B. the server name where Context Directory Agent is installed
C. the backup Context Directory Agent
D. the primary Context Directory Agent
E. the shared secret
F. the syslog server IP address
Correct Answer: BDE

Question 82
What are the two policy types that can use a web reputation profile to perform reputation-based processing?
A. profile policies
B. encryption policies
C. decryption policies
D. access policies
Question 83
What are two facts about the interface that you can determine from the given output?
Refer to the exhibit.

Correct Answer: CD
Explanation/Reference:

Question 84
Which three statements about Cisco CWS are true?
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.
Correct Answer: ABC
Explanation/Reference:

Question 85
What are two features of the Cisco ASA NGFW?
What are two features of the Cisco ASA NGFW? (Choose two.)
A. It can restrict access based on qualitative analysis.
B. It can restrict access based on reputation.
C. It can reactively protect against Internet threats.
D. It can proactively protect against Internet threats.
Correct Answer: BD
Explanation/Reference:

Question 86
Why did the Cisco Email Security gateway fail to do a spam scan on emails for [email protected]?
Refer to the exhibit.
The system administrator of mydomain.com was informed that one of the users in his environment received spam from an Internet sender. Message tracking shows that the emails for this user were not scanned by antispam. Why did the Cisco Email Security gateway fail to do a spam scan on emails for [email protected]?
A. The remote MTA activated the SUSPECTLIST sender group.
B. The Cisco Email Security gateway created duplicates of the message.
C. The user [email protected] matched an inbound rule with antispam disabled.
D. The user [email protected] matched an inbound rule with antispam disabled.
Correct Answer: C
Explanation/Reference:

Question 87
Which command sets the number of packets to log on a Cisco IPS sensor?
http://www.aoowe.com/practice-300-207-3145.html
Which command sets the number of packets to log on a Cisco IPS sensor?
A. ip-log-count number
B. ip-log-packets number
C. ip-log-bytes number
D. ip-log number
Correct Answer: B
Explanation/Reference:

Question 88
Who or what calculates the signature fidelity rating in a Cisco IPS?
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
Correct Answer: A
Explanation/Reference:

Question 89
Which three zones are used for anomaly detection in a Cisco IPS?
Which three zones are used for anomaly detection in a Cisco IPS? (Choose three.)
A. internal zone
B. external zone
C. illegal zone
D. inside zone
E. outside zone
F. DMZ zone
Correct Answer: ABC
Explanation/Reference:

Question 90
Which two statements regarding the basic setup of the Cisco CX for services are correct?
Which two statements regarding the basic setup of the Cisco CX for services are correct? (Choose two.)
A. The Packet capture feature is available for either permitted or dropped packets by default.
B. Public Certificates can be used for HTTPS Decryption policies.
C. Public Certificates cannot be used for HTTPS Decryption policies.
D. When adding a standard LDAP realm, the group attribute will be UniqueMember.
E. The Packet capture features is available for permitted packets by default.
Correct Answer: CE
Explanation/Reference:

Question 91
Which three sender reputation ranges identify the default behavior of the Cisco Email Security Appliance?
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 -10 and -4, the email is blocked
F. If it is between -10 and -3, the email is sent to the virus and spam engines for additional scanning
G. If it is between -10 and -4, the email is blocked
H. If it is between -10 and -4, the email is blocked
Correct Answer: ACF
Explanation/Reference:

Question 92
Which two design considerations are required to add the Cisco Email Security Appliance to an existing mail delivery chain?
Which two design considerations are required to add the Cisco Email Security Appliance to an existing mail delivery chain? (Choose two.)
A. Existing MX records should be maintained and policy routing should be used to redirect traffic to the ESA.
B. Update the MX records to point to the inbound listener interfaces on the ESA.
C. Update the MX records to point to the outbound listener interfaces on the ESA.
D. Different Listeners must be used to handle inbound and outbound mail handling.
E. The ESA should be connected to the same subnet as the Email Server because it maintains only a single routing table.
F. The ESA can be connected to a DMZ external to the Email Server but it maintains only a single routing table.
G. The ESA can be connected to a DMZ external to the Email Server but it maintains multiple routing tables.
H. Mail Listeners by default can share the same IP interface by defining the routes for sending and receiving.
Correct Answer: BG
Explanation/Reference:

Question 93
Which three protocols are required when considering firewall rules for email services using a Cisco Email Security Appliance?
Which three protocols are required when considering firewall rules for email services using a Cisco Email Security Appliance? (Choose three.)
A. SMTP
B. HTTP
C. DNS
D. SNMP
### Question 94
Which four rows exhibit the correct WCCP service to protocol assignments?
Refer to the exhibit.

<table>
<thead>
<tr>
<th>Option</th>
<th>WCCP Service</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>60</td>
<td>WAAS – reverse</td>
</tr>
<tr>
<td>2</td>
<td>61</td>
<td>WAAS – forward</td>
</tr>
<tr>
<td>3</td>
<td>62</td>
<td>FTP</td>
</tr>
<tr>
<td>4</td>
<td>70</td>
<td>HTTPS</td>
</tr>
<tr>
<td>5</td>
<td>88</td>
<td>CIFS-Cache WAAS</td>
</tr>
<tr>
<td>6</td>
<td>90-97</td>
<td>User Configurable</td>
</tr>
<tr>
<td>7</td>
<td>98</td>
<td>RTSPU</td>
</tr>
<tr>
<td>8</td>
<td>99</td>
<td>Reverse Proxy</td>
</tr>
</tbody>
</table>

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

Correct Answer: BDFH
Explanation/Reference:

### Question 95
Which four rows identify the switch behavior in correlation to the redirect method?
Refer to the exhibit.

<table>
<thead>
<tr>
<th>Option</th>
<th>Redirect Method</th>
<th>Assignment Method</th>
<th>Ingress/Egress Redirection</th>
<th>Switching Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>L2</td>
<td>Hash</td>
<td>Ingress</td>
<td>Software Processing</td>
</tr>
<tr>
<td>2</td>
<td>L2 (Recommended)</td>
<td>Mask</td>
<td>Ingress</td>
<td>Full Hardware Processing with ACL TCAM</td>
</tr>
<tr>
<td>3</td>
<td>L2</td>
<td>Hash</td>
<td>Egress</td>
<td>Software Processing</td>
</tr>
<tr>
<td>4</td>
<td>L2</td>
<td>Mask</td>
<td>Egress</td>
<td>Software Processing of initial packet</td>
</tr>
<tr>
<td>5</td>
<td>GRE (FPC3 or newer)</td>
<td>Hash</td>
<td>Ingress</td>
<td>Software Processing of Initial packet with Netflow Partial-Flow</td>
</tr>
<tr>
<td>6</td>
<td>GRE (FPC3 or newer)</td>
<td>Mask</td>
<td>Ingress</td>
<td>Full Hardware Processing with Netflow Full-Flow</td>
</tr>
<tr>
<td>7</td>
<td>GRE</td>
<td>Hash</td>
<td>Egress</td>
<td>Software Processing</td>
</tr>
<tr>
<td>8</td>
<td>GRE (FPC3 or newer)</td>
<td>Mask</td>
<td>Egress</td>
<td>Software Processing of initial packet</td>
</tr>
</tbody>
</table>

When designing the network to redirect web traffic utilizing the Catalyst 6500 to the Cisco Web Security Appliance, impact on the switch platform needs consideration. Which four rows identify the switch behavior in correlation to the redirect method? (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

Correct Answer: BCFG
Question 96
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.
Correct Answer: B

Question 97
Which two modes does Cisco recommend using to configure for this?
A. VLAN pair
B. interface pair
C. transparent mode
D. EtherChannel load balancing
E. promiscuous mode
Correct Answer: AD

Question 98
Which two commands are used to verify that CWS redirection is working on a Cisco ASA appliance?
A. show scansafe statistics
B. show webvpn statistics
C. show service-policy inspect scansafe
D. show running-config scansafe
E. show running-config webvpn
F. show url-server statistics
Correct Answer: AC

Question 99
Which command verifies that CWS redirection is working on a Cisco IOS router?
A. show content-scan session active
B. show content-scan summary
C. show interfaces stats
D. show sessions
Correct Answer: A

Question 100
Which tool on the Cisco Email Security gateway can you use to debug or emulate the flow that a message takes through the work queue?
A. the message tracker interface
B. centralized or local message tracking
C. the CLI findevent command
D. the trace tool
E. the CLI grep command
Correct Answer: D

Question 101
What is the likely cause of the intermittent delays?
Refer to the exhibit.
The system administrator of mydomain.com received complaints that some messages that were sent from sender [email protected] were delayed. Message tracking data on the sender shows that an email sample that was received was clean and properly delivered. What is the likely cause of the intermittent delays?

A. The remote MTA has a SenderBase Reputation Score of -1.0.
B. The remote MTA is sending emails from RFC 1918 IP addresses.
C. The remote MTA has activated the SUSPECTLIST sender group.
D. The remote MTA has activated the default inbound mail policy.

Correct Answer: C

Explanation/Reference:

---

### Question 102
Which five system management and reporting protocols are supported by the Cisco Intrusion Prevention System?

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

- SNMPv2c
- SNMPv1
- SNMPv2
- SNMPv3
- syslog
- SDEE
- SMTP

Correct Answer: ABCFG

Explanation/Reference:

---

### Question 103
Which two features must be enabled in order to record those connections in the mail log on the Cisco ESA?

Connections are being denied because of SenderBase Reputation Score. Which two features must be enabled in order to record those connections in the mail log on the Cisco ESA? (Choose two.)

- Rejected Connection Handling
- Domain Debug Logs
- Injection Debug Logs
- Message Tracking

Correct Answer: AD

Explanation/Reference:

---

### Question 104
Which feature of the Cisco Email Security Appliance provides this record?

The helpdesk was asked to provide a record of delivery for an important email message that a customer claims it did not receive. Which feature of the Cisco Email Security Appliance provides this record?

- Outgoing Mail Reports
- SMTP Routes
- Message Tracking
- Scheduled Reports
- System Administration

Correct Answer: C

Explanation/Reference:

---

### Question 105
When a Cisco Email Security Appliance joins a cluster, which four settings are inherited?

When a Cisco Email Security Appliance joins a cluster, which four settings are inherited? (Choose four.)

- IP address
- DNS settings
- SMTP routes
- HAT
- RAT
- hostnames
- certificates

Correct Answer: BCDE

Explanation/Reference:
Question 106
Which two steps must be performed?
In order to set up HTTPS decryption on the Cisco Web Security Appliance, which two steps must be performed? (Choose two.)
A. Enable and accept the EULA under Security Services > HTTPS Proxy.
B. Upload a publicly signed server certificate.
C. Configure or upload a certificate authority certificate.
Correct Answer: AC
Explanation/Reference:

Question 107
Which Cisco ESA command is used to edit the ciphers that are used for GUI access?
Which Cisco ESA command is used to edit the ciphers that are used for GUI access?
A. interfaceconfig
B. etherconfig
C. certconfig
D. sslconfig
Correct Answer: D
Explanation/Reference:

Question 108
Which command is used to enable strong ciphers on the Cisco Web Security Appliance?
Which command is used to enable strong ciphers on the Cisco Web Security Appliance?
A. interfaceconfig
B. strictssl
C. etherconfig
D. adminaccessconfig
Correct Answer: B
Explanation/Reference:

Question 109
Which four steps should Joe implement to accomplish this goal?
Joe was asked to secure access to the Cisco Web Security Appliance to prevent unauthorized access. Which four steps should Joe implement to accomplish this goal? (Choose four.)
A. Implement IP access lists to limit access to the management IP address in the Cisco Web Security Appliance GUI.
B. Add the Cisco Web Security Appliance IP address to the local access list.
C. Enable HTTPS access via the GUI/CLI with redirection from HTTP.
D. Replace the Cisco self-signed certificate with a publicly signed certificate.
E. Put the Cisco WSA Management interface on a private management VLAN.
F. Change the netmask on the Cisco WSA Management interface to a 32-bit mask.
G. Create an MX record for the Cisco Web Security Appliance in DNS.
Correct Answer: ACDE
Explanation/Reference:

Question 110
What command alters the SSL ciphers used by the Cisco Email Security Appliance for TLS sessions and HTTPS access?
What command alters the SSL ciphers used by the Cisco Email Security Appliance for TLS sessions and HTTPS access?
A. sslconfig
B. sslciphers
C. tlsconfig
D. certconfig
Correct Answer: A
Explanation/Reference:

Question 111
How does a user access a Cisco Web Security Appliance for initial setup?
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.
Correct Answer: C
Explanation/Reference:
Question 113
Which two options are characteristics of router-based IPS?
Which two options are characteristics of router-based IPS? (Choose two.)
A. It supports custom signatures
B. It supports virtual sensors.
C. It supports multiple VRFs.
D. It uses configurable anomaly detection.
E. Signature definition files have been deprecated.

Correct Answer: CE
Explanation/Reference:

Question 114
Which IPS engine detects ARP spoofing?
Which IPS engine detects ARP spoofing?
A. Atomic ARP Engine
B. Service Generic Engine
C. ARP Inspection Engine
D. AIC Engine

Correct Answer: A
Explanation/Reference:

Question 115
Which Cisco IPS CLI command shows the most fired signature?
Which Cisco IPS CLI command shows the most fired signature?
A. show statistics virtual-sensor
B. show event alert
C. show alert
D. show version

Correct Answer: A
Explanation/Reference:

Question 116
Which configuration option causes an ASA with IPS module to drop traffic matching IPS signatures and to block all traffic if the module fails?
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

Correct Answer: B
Explanation/Reference:

Question 117
Which three options are valid event actions for a Cisco IPS?
Which three options are valid event actions for a Cisco IPS? (Choose three.)
A. deny-packet-inline
B. deny-attack-reset
C. produce-verbose-alert
D. log-attacker-packets
E. deny-packet-internal
F. request-block-drop-connection

Correct Answer: ACD
Explanation/Reference:

Question 118
Which two Cisco IPS events will generate an IP log?
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.

Correct Answer: AB
Explanation/Reference:

Question 119
What is the default IP range of the external zone?
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

Correct Answer: B
Explanation/Reference:
Question 120
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

Correct Answer: A
Explanation/Reference:

Question 121
What Cisco ESA CLI command generated the output?
Refer to the exhibit.

What Cisco ESA CLI command generated the output?
A. smtproutes
B. tophosts
C. hoststatus
D. workqueuestatus

Correct Answer: B
Explanation/Reference:

Question 122
What is the default antispam policy for positively identified messages within the Cisco Email Security Appliance?
A. Drop
B. Deliver and Append with [SPAM]
C. Deliver and Prepend with [SPAM]
D. Deliver and Alternate Mailbox

Correct Answer: C
Explanation/Reference:

Question 123
Which Cisco Web Security Appliance deployment mode requires minimal change to endpoint devices?
A. Transparent Mode
B. Explicit Forward Mode
C. Promiscuous Mode
D. Inline Mode

Correct Answer: A
Explanation/Reference:

Question 124
Which three functions can Cisco Application Visibility and Control perform within Cisco Cloud Web Security? (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

Correct Answer: BDE
Explanation/Reference:

Question 125
Which three features does Cisco CX provide? (Choose three.)
A. HTTPS traffic decryption and inspection
B. Application Visibility and Control

http://www.aoowe.com/practice-300-207-3145.html
C. Category or reputation-based URL filtering
D. Email virus scanning
E. Application optimization and acceleration
F. VPN authentication

Correct Answer: ABC

Explanation/Reference:

Question 126
SIMULATION

Correct Answer: Steps are in Explanation below
Explanation/Reference:
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:
Question 127
What is the status of OS Identification?

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.

Correct Answer: D

Explanation/Reference:
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 mapping, which take precedence over learned OS mappings.

• Computation of attack relevance rating and risk rating.

Question 128
Which three statements about the Cisco IPS appliance configurations are true?
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.

Correct Answer: ABC

Explanation/Reference:

Question 129
Which two statements about Signature 1104 are true?

Correct Answer: C, D

Explanation/Reference:

http://www.aoowe.com/practice-300-207-3145.html
Which two statements about Signature 1104 are true? (Choose two.)

A. This is a custom signature.
B. The severity level is High.
C. This signature has triggered as indicated by the red severity icon.
D. Produce Alert is the only action defined.
E. This signature is enabled, but inactive, as indicated by the 0 to the follows the signature number.

Correct Answer: BD

Explanation/Reference:

Explanation:

This can be seen here where signature 1004 is the 5th one down:

http://www.aoowe.com/practice-300-207-3145.html
Question 130
To what extent will the Cisco IPS sensor contribute data to the Cisco SensorBase network?

Instructions
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.

Scenario
Using Cisco IPS Device Manager (CDM), answer the multiple choice questions.

http://www.aoowe.com/practice-300-207-3145.html
To what extent will the Cisco IPS sensor contribute data to the Cisco SensorBase network?

A. It will not contribute to the SensorBase network.
B. It will contribute to the SensorBase network, but will withhold some sensitive information.
C. It will contribute the victim IP address and port to the SensorBase network.
D. It will not contribute to Risk Rating adjustments that use information from the SensorBase network.

Correct Answer: B

Explanation/Reference:

To configure network participation, follow these steps:

Step 1: Log in to IDM using an account with administrator privileges.
Step 2: Choose Configuration > Policies > Global Correlation > Network Participation.
Step 3: To turn on network participation, click the Partial or Full radio button:
  • Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
  • Full—All data is contributed to the SensorBase Network.

In this case, we can see that this has been turned off as shown below:

Question 131
What action will the sensor take regarding IP addresses listed as known bad hosts in the Cisco SensorBase network?

Instructions:

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, drag the title bar and drag the window.

Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.
What action will the sensor take regarding IP addresses listed as known bad hosts in the Cisco SensorBase network?

A. Global correlation is configured in Audit mode for testing the feature without actually denying any hosts.
B. Global correlation is configured in Aggressive mode, which has a very aggressive effect on deny actions.
C. It will not adjust risk rating values based on the known bad hosts list.
D. Reputation filtering is disabled.

Correct Answer: D

Explanation/Reference:
Explanation:
This can be seen on the Global Correlation – Inspection/Reputation tab show below:
Question 132
Which signature definition is virtual sensor 0 assigned to use?

Instructions:
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.

Listing Cisco IPS Device Manager (CDM), answer the multiple choice questions.
Which signature definition is virtual sensor 0 assigned to use?
A. rules0
B. vs0
C. sig0
D. ad0
E. ad1
F. sig1
Correct Answer: C
Explanation/Reference:
This is the default signature.
You can create multiple security policies and apply them to individual virtual sensors. A security policy is made up of a signature definition policy, an event action rules policy, and an anomaly detection policy. Cisco IPS contains a default signature definition policy called sig0, a default event action rules policy called rules0, and a default anomaly detection policy called ad0. You can assign the default policies to a virtual sensor or you can create new policies.

Question 133
Which Cisco technology is a customizable web-based alerting service designed to report threats and vulnerabilities?
Which Cisco technology is a customizable web-based alerting service designed to report threats and vulnerabilities?
A. Cisco Security Intelligence Operations
B. Cisco Security IntellShld Alert Manager Service
C. Cisco Security Optimization Service
D. Cisco Software Application Support Service
Correct Answer: B
Explanation/Reference:

Question 134
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
Correct Answer: AC
Explanation/Reference:

Question 135
At which value do custom signatures begin?
At which value do custom signatures begin?
A. 1024
B. 10000
C. 1
D. 60000
Correct Answer: D
Explanation/Reference:

Question 136
Which three options are IPS signature classifications? (Choose three.)
A. tuned signatures  
B. response signatures  
C. default signatures  
D. custom signatures  
E. preloaded signatures  
F. designated signatures  
Correct Answer: ACD
Explanation/Reference:

Question 137
Which three user roles are partially defined by default in Prime Security Manager? 
Which three user roles are partially defined by default in Prime Security Manager? (Choose three.)
A. networkoperator  
B. admin  
C. helpdesk  
D. securityoperator  
E. monitoringadmin  
F. systemadmin  
Correct Answer: BCF
Explanation/Reference:

Question 138
Which IPS signature regular expression CLI command matches a host issuing a domain lookup for www.theblock.com?
Which IPS signature regular expression CLI command matches a host issuing a domain lookup for www.theblock.com? 
A. regex-string (x03[Tt][Hh][Ee]x05[Bb][Ll][Oo][Cc][Kk])  
B. regex-string (x0b[theblock.com])  
C. regex-string (x03[the]x05[block]0x3[com])  
D. regex-string (x03[T][H][E]x05[B][L][O][C][K][.][C][O][M]  
Correct Answer: A
Explanation/Reference:

Question 139
Which five system management protocols are supported by the Intrusion Prevention System? 
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  
Correct Answer: ABCFG
Explanation/Reference:

Question 140
Which are the two most likely reasons that the category is still being blocked for a faculty and staff user? 
The Web Security Appliance has identities defined for faculty and staff, students, and default access. The faculty and staff identity identifies users based on the source network and authenticated credentials. The identity for students identifies users based on the source network along with successful authentication credentials. The global identity is for guest users not authenticated against the domain. 
Recently, a change was made to the organization’s security policy to allow faculty and staff access to a social network website, and the security group changed the access policy for faculty and staff to allow the social networking category. 
Which are the two most likely reasons that the category is still being blocked for a faculty and staff user? (Choose two.)
A. The user is being matched against the student policy because the user did not enter credentials.  
B. The user is using an unsupported browser so the credentials are not working.  
C. The social networking URL was entered into a custom URL category that is blocked in the access policy.  
D. The user is connected to the wrong network and is being blocked by the student policy.  
E. The social networking category is being allowed but the AVC policy is still blocking the website.  
Correct Answer: CE
Explanation/Reference:

Question 141
Cisco AVC allows control of which three of the following?
Cisco AVC allows control of which three of the following? (Choose three.)
A. Facebook  
B. LWAPP  
C. IPv6  
D. MySpace  
E. Twitter  
F. WCCP  
Correct Answer: ADE
Explanation/Reference:

Question 142
During initial configuration, the Cisco ASA can be configured to drop all traffic if the ASA CX SSP fails by using which command in a policy-map? 
During initial configuration, the Cisco ASA can be configured to drop all traffic if the ASA CX SSP fails by using which command in a policy-map? 
A. exec fail
Question 143
Which three statements about Cisco ASA CX are true? (Choose three.)
A. It groups multiple ASAs as a single logical device.
B. It can perform context-aware inspection.
C. It provides high-density security services with high availability.
D. It uses policy-based interface controls to inspect and forward TCP- and UDP-based packets.
E. It can make context-aware decisions.
F. It uses four cooperative architectural constructs to build the firewall.
Correct Answer: BEF
Explanation/Reference:

Question 144
Which Cisco technology is a modular security service that combines a stateful inspection firewall with next-generation application awareness, providing near real-time threat protection?
A. Cisco ASA 5500 series appliances
B. Cisco ASA CX Context-Aware Security
C. WSA
D. Internet Edge Firewall / IPS
Correct Answer: B
Explanation/Reference:

Question 145
Which antispam technology assumes that email from server A, which has a history of distributing spam, is more likely to be spam than email from server B, which does not have a history of distributing spam?
A. Reputation-based filtering
B. Context-based filtering
C. Cisco ESA multilayer approach
D. Policy-based filtering
Correct Answer: A
Explanation/Reference:

Question 146
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
Correct Answer: C
Explanation/Reference:

Question 147
What are three benefits of the Cisco AnyConnect Secure Mobility Solution? (Choose three.)
A. It can protect against command-injection and directory-traversal attacks.
B. It provides Internet transport while maintaining corporate security policies.
C. It provides secure remote access to managed computers.
D. It provides seamless remote access to multiple network-based systems.
E. It enforces security policies, regardless of the user location.
F. It uses ACLs to determine best-route connections for clients in a secure environment.
Correct Answer: BCE
Explanation/Reference:

Question 148
Which version of AsyncOS for web is required to deploy the Web Security Appliance as a CWS connector?
A. AsyncOS version 7.7.x
B. AsyncOS version 7.5.x
C. AsyncOS version 7.5.7
D. AsyncOS version 7.5.0
Correct Answer: C
Explanation/Reference:
What CLI command generated the output? Refer to the exhibit.

What CLI command generated the output?
A. smtproutes
B. tophosts
C. hoststatus
D. workqueuestatus

Correct Answer: B
Explanation/Reference:

**Question 150**

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

Correct Answer: A
Explanation/Reference:

**Question 151**

What are two benefits of using SPAN with promiscuous mode deployment? (Choose two.)
A. SPAN does not introduce latency to network traffic.
B. SPAN can perform granular scanning on captures of per-IP-address or per-port monitoring.
C. Promiscuous Mode can silently block traffic flows on the IDS.
D. SPAN can analyze network traffic from multiple points.

Correct Answer: AD
Explanation/Reference:

**Question 152**

What set of commands changes the FTP client timeout when the sensor is communicating with an FTP server?

A. sensor# configure terminal sensor(config)# service sensor sensor(config-hos)# network-settings sensor(config-hos-net)# ftp-timeout 500
B. sensor# configure terminal sensor(config)# service host sensor(config-hos)# network-settings parameter ftp sensor(config-hos-net)# ftp-timeout 500
C. sensor# configure terminal sensor(config)# service host sensor(config-hos)# network-settings sensor(config-hos-net)# ftp-timeout 500
D. sensor# configure terminal sensor(config)# service network sensor(config-hos)# network-settings sensor(config-hos-net)# ftp-timeout 500

Correct Answer: C
Explanation/Reference:

**Question 153**

Which two practices are recommended for implementing NIPS at enterprise Internet edges? (Choose two.)
A. Integrate sensors primarily on the more trusted side of the firewall (inside or DMZ interfaces).
B. Integrate sensors primarily on the less trusted side of the firewall (outside interfaces).
C. Implement redundant IPS and make data paths symmetrical.
D. Implement redundant IPS and make data paths asymmetrical.
E. Use NIPS only for small implementations.

Correct Answer: AC
Explanation/Reference:

**Question 154**

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

Correct Answer: B
Explanation/Reference:
Question 155
A network engineer can assign IPS event action overrides to virtual sensors and configure which three modes?
A network engineer can assign IPS event action overrides to virtual sensors and configure which three modes? (Choose three.)
A. Anomaly detection operational mode
B. Inline TCP session tracking mode
C. Normalizer mode
D. Load-balancing mode
E. Inline and Promiscuous mixed mode
F. Fail-open and fail-close mode
Correct Answer: ABC
Explanation/Reference:

Question 156
Which Cisco Security IntelliShield Alert Manager Service component mitigates new botnet, phishing, and web-based threats?
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
Correct Answer: A
Explanation/Reference:

Question 157
Which three search parameters are supported by the Email Security Monitor?
Which three search parameters are supported by the Email Security Monitor? (Choose three.)
A. Destination domain
B. Network owner
C. MAC address
D. Policy requirements
E. Internal sender IP address
F. Originating domain
Correct Answer: ABE
Explanation/Reference:

Question 158
Which Cisco monitoring solution displays information and important statistics for the security devices in a network?
Which Cisco monitoring solution displays information and important statistics for the security devices in a network?
A. Cisco Prime LAN Management
B. Cisco ASDM Version 5.2
C. Cisco Threat Defense Solution
D. Syslog Server
E. TACACS+
Correct Answer: B
Explanation/Reference:

Question 159
Which two benefits are provided by the dynamic dashboard in Cisco ASDM Version 5.2?
Which two benefits are provided by the dynamic dashboard in Cisco ASDM Version 5.2? (Choose two.)
A. It configures system policies for NAC devices.
B. It forwards traffic to destination devices.
C. It provides statistics for device health.
D. It replaces syslog, RADIUS, and TACACS+ servers.
E. It automatically detects Cisco security appliances to configure.
Correct Answer: CE
Explanation/Reference:

Question 160
Which rate limit option specifies the maximum bandwidth for rate-limited traffic?
With Cisco IDM, which rate limit option specifies the maximum bandwidth for rate-limited traffic?
A. protocol
B. rate
C. bandwidth
D. limit
Correct Answer: B
Explanation/Reference:

Question 161
What three alert notification options are available in Cisco IntelliShield Alert Manager?
What three alert notification options are available in Cisco IntelliShield Alert Manager? (Choose three.)
A. Alert Summary as Text
B. Complete Alert as an HTML Attachment
C. Complete Alert as HTML
D. Complete Alert as RSS
Question 162
Which three parameters can they adjust to restrict alerts to specific product sets?
The security team needs to limit the number of e-mails they receive from the Intellishield Alert Service. Which three parameters can they adjust to restrict alerts to specific product sets? (Choose three.)
A. Vendor
B. Chassis/Module
C. Device ID
D. Service Contract
E. Version/Release
F. Service Pack/Platform
Correct Answer: AEF
Explanation/Reference:

Question 163
Which two GUI options display users’ activity in Cisco Web Security Appliance?
Which two GUI options display users’ activity in Cisco Web Security Appliance? (Choose two.)
A. Web Security Manager Identity Identity Name
B. Security Services Reporting
C. Reporting Users
D. Reporting Reports by User Location
Correct Answer: CD
Explanation/Reference:

Question 164
Which four statements are correct regarding management access to a Cisco Intrusion Prevention System?
Which four statements are correct regarding management access to a Cisco Intrusion Prevention System? (Choose four.)
A. The Telnet protocol is enabled by default
B. The Telnet protocol is disabled by default
C. HTTP is enabled by default
D. HTTP is disabled by default
E. SSH is enabled by default
F. SSH is disabled by default
G. HTTPS is enabled by default
H. HTTPS is disabled by default
Correct Answer: BDEG
Explanation/Reference:

Question 165
Which five system management protocols are supported by the Cisco Intrusion Prevention System?
Which five system management protocols are supported by the Cisco Intrusion Prevention System? (Choose five.)
A. SNMPv2c
B. SNMPv1
C. SNMPv2
D. SNMPv3
E. Syslog
F. SDEE
G. SMTP
Correct Answer: ABCFG
Explanation/Reference:

Question 166
Which command verifies that the correct CWS license key information was entered on the Cisco ASA?
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
Correct Answer: B
Explanation/Reference:

Question 167
Which Cisco WSA is intended for deployment in organizations of more than 6000 users?
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
Correct Answer: B
Explanation/Reference:
Question 168
Which Cisco WSA is intended for deployment in organizations of up to 1500 users?
A. WSA S370
B. WSA S670
C. WSA S370-2RU
D. WSA S170
Correct Answer: D
Explanation/Reference:

Question 169
Which Cisco technology combats viruses and malware with virus outbreak filters that are downloaded from Cisco SenderBase?
A. ASA
B. WSA
C. Secure mobile access
D. IronPort ESA
E. SBA
Correct Answer: D
Explanation/Reference:

Question 170
Which Cisco technology prevents targeted malware attacks, provides data loss prevention and spam protection, and encrypts email?
A. SBA
B. secure mobile access
C. IPv6 DMZ web service
D. ESA
Correct Answer: D
Explanation/Reference:

Question 171
Which port is used for CLI Secure shell access?
A. Port 23
B. Port 25
C. Port 22
D. Port 443
Correct Answer: C
Explanation/Reference:

Question 172
Which is the default IP address and admin port setting for https in the Cisco Web Security Appliance?
A. http://192.168.42.42:8080
Correct Answer: D
Explanation/Reference:

Question 173
What can Cisco Prime Security Manager (PRSM) be used to achieve?
A. Configure and monitor Cisco CX Application Visibility and Control, web filtering, access and decryption policies
B. Configure Cisco ASA connection limits
C. Configure TCP state bypass in Cisco ASA and IOS
D. Configure Cisco IPS signature and monitor signature alerts
E. Cisco Cloud Security on Cisco ASA
Correct Answer: A
Explanation/Reference:

Question 174
A Cisco Email Security Appliance uses which message filter to drop all executable attachments entering and leaving the Cisco Email Security Appliance?
A. drop-exe! if (attachment-filename =~ "\.*exe\="/ OR (attachment-filetype = "exe") { drop(); }
B. drop-exe! if (recv-listener = "InboundMail") AND (attachment-filename =~ ".\.*exe\="/ OR (attachment-filetype = "exe") { drop(); }
C. drop-exe! if (attachment-filename =~ ".\.*exe\="/ OR (attachment-filetype = "exe") { drop(); }
D. drop-exe! if (recv-listener = "InboundMail") AND (attachment-filename =~ ".\.*exe\="/ OR (attachment-filetype = "exe") { drop(); }
Correct Answer: A
Explanation/Reference:
What is the CLI command to create a new Message Filter in a Cisco Email Security Appliance?

A. filterconfig
B. filters new
C. messagefilters
D. policyconfig - inbound or outbound - filters

Correct Answer: B
Explanation/Reference:

Question 176
When learning accept mode is set to auto, and the action is set to rotate, when is the KB created and used?

A. It is created every 24 hours and used for 24 hours.
B. It is created every 24 hours, but the current KB is used.
C. It is created every 1 hour and used for 24 hours.
D. A KB is created only in manual mode.

Correct Answer: A
Explanation/Reference:

Question 177
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

Correct Answer: B
Explanation/Reference:

Question 178
Which three zones are used for anomaly detection? (Choose three.)

A. Internal zone
B. External zone
C. Illegal zone
D. Inside zone
E. Outside zone
F. DMZ zone

Correct Answer: ABC
Explanation/Reference:

Question 179
Who or what calculates the signature fidelity rating?

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

Correct Answer: A
Explanation/Reference:

Question 180
Which three best practices for a Cisco Intrusion Prevention System? (Choose three.)

A. Checking for new signatures every 4 hours
B. Checking for new signatures on a staggered schedule
C. Automatically updating signature packs
D. Manually updating signature packs
E. Group tuning of signatures
F. Single tuning of signatures

Correct Answer: BCE
Explanation/Reference:

Question 181
Which three options are characteristics of router-based IPS?

Which three options are characteristics of router-based IPS? (Choose three.)

A. It is used for large networks.
B. It is used for small networks.
C. It supports virtual sensors.
D. It supports multiple VRFs.
E. It uses configurable anomaly detection.
F. Signature definition files have been deprecated.

Correct Answer: BDF
Explanation/Reference:
Question 182
Which CLI command shows the most fired signature?
A new Cisco IPS device has been placed on the network without prior analysis. Which CLI command shows the most fired signature?
A. Show statistics virtual-sensor
B. Show event alert
C. Show alert
D. Show version

Correct Answer: A
Explanation/Reference:

Question 183
Which describes the correct configuration?
An ASA with an IPS module must be configured to drop traffic matching IPS signatures and block all traffic if the module fails. Which describes the correct configuration?
A. Inline Mode, Permit Traffic
B. Inline Mode, Close Traffic
C. Promiscuous Mode, Permit Traffic
D. Promiscuous Mode, Close Traffic

Correct Answer: B
Explanation/Reference:

Question 184
What CLI command configures IP-based access to restrict GUI and CLI access to a Cisco Email Security appliance’s administrative interface?
What CLI command configures IP-based access to restrict GUI and CLI access to a Cisco Email Security appliance’s administrative interface?
A. adminaccessconfig
B. sshconfig
C. sslconfig
D. ipaccessconfig

Correct Answer: A
Explanation/Reference:

Question 185
Which CLI command shows the most fired signature?
A new Cisco IPS device has been placed on the network without prior analysis. Which CLI command shows the most fired signature?
A. Show statistics virtual-sensor
B. Show event alert
C. Show alert
D. Show version

Correct Answer: A
Explanation/Reference:

Question 186
Which command establishes a virtual console session to a CX module within a Cisco Adaptive Security Appliance?
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

Correct Answer: E
Explanation/Reference:

Question 189
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

Correct Answer: C
Explanation/Reference:

Question 190
What is the authentication method for an encryption envelope that is set to medium security?
A. The recipient must always enter a password, even if credentials are cached.
B. A password is required, but cached credentials are permitted.
C. The recipient must acknowledge the sensitivity of the message before it opens.
D. The recipient can open the message without authentication.

Correct Answer: B
Explanation/Reference:

Question 191
Which two options are features of the Cisco Email Security Appliance? (Choose two.)
A. Cisco Anti-Replay Services
B. Cisco Destination Routing
C. Cisco Registered Envelope Service
D. Cisco IronPort SenderBase Network

Correct Answer: CD
Explanation/Reference:

Question 192
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

Correct Answer: BDE
Explanation/Reference:

Question 193
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

Correct Answer: D
Explanation/Reference:

Question 194
Which two statements about Cisco Cloud Web Security functionality are true? (Choose two.)
A. It integrates with Cisco Integrated Service Routers.
B. It supports threat avoidance and threat remediation.
C. It extends web security to the desktop, laptop, and PDA.
D. It integrates with Cisco ASA Firewalls.

Correct Answer: AD
Explanation/Reference:

Question 195
What step is required to enable HTTPS Proxy on the Cisco Web Security Appliance?
A. Web Security Manager HTTPS Proxy click Enable
B. Security Services HTTPS Proxy click Enable
C. HTTPS Proxy is enabled by default
D. System Administration HTTPS Proxy click Enable

Correct Answer: B
Explanation/Reference:
Question 196
Which Cisco Web Security Appliance design requires minimal change to endpoint devices?
A. Transparent Mode
B. Explicit Forward Mode
C. Promiscuous Mode
D. Inline Mode
Correct Answer: A
Explanation/Reference:

Question 197
A Cisco Web Security Appliance’s policy can provide visibility and control of which two elements?
A. Voice and Video Applications
B. Websites with a reputation between -100 and -60
C. Secure websites with certificates signed under an unknown CA
D. High bandwidth websites during business hours
Correct Answer: CD
Explanation/Reference:

Question 198
Cisco's ASA CX includes which two URL categories?
A. Proxy Avoidance
B. Dropbox
C. Hate Speech
D. Facebook
E. Social Networking
F. Instant Messaging and Video Messaging
Correct Answer: CE
Explanation/Reference:

Question 199
A network engineer may use which three types of certificates when implementing HTTPS decryption services on the ASA CX?
A. Self Signed Server Certificate
B. Self Signed Root Certificate
C. Microsoft CA Server Certificate
D. Microsoft CA Subordinate Root Certificate
E. LDAP CA Server Certificate
F. LDAP CA Root Certificate
G. Public Certificate Authority Server Certificate
H. Public Certificate Authority Root Certificate
Correct Answer: BDF
Explanation/Reference:

Question 200
During initial configuration, the Cisco ASA can be configured to drop all traffic if the ASA CX SSP fails by using which command in a policy-map?
A. cxsc fail
B. cxsc fail-close
C. cxsc fail-open
D. cxssp fail-close
Correct Answer: B
Explanation/Reference: