

Cisco

300-210

Implementing Cisco Threat Control Solutions (SITCS)

For More Information – Visit link below:

<http://www.examsboost.com/>

Product Version

Question: 1

Which three operating systems are supported with Cisco AMP for Endpoints? (Choose three.)

- A. Windows
- B. AWS
- C. Android
- D. Cisco IOS
- E. OS X
- F. ChromeOS

Answer: A, C, E

Explanation:

Reference:

<http://www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html>

Question: 2

Which Cisco Web Security Appliance feature enables the appliance to block suspicious traffic on all of its ports and IP addresses?

- A. explicit forward mode
- B. Layer 4 Traffic Monitor
- C. transparent mode
- D. Secure Web Proxy

Answer: B

Question: 3

Which feature requires the network discovery policy for it to work on the Cisco Next Generate fusion Prevent-on System,

- A. impact flags
- B. URL filtering
- C. security intelligence
- D. health monitoring

Answer: A

Question: 4

Which CLI command is used to register a Cisco FirePOWER sensor to Firepower Management Center?

- A. configure system add <host> <key>
- B. configure manager <key> add host
- C. configure manager delete
- D. configure manger add <host> <key>

Answer: A

Explanation:

Reference:

http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_appendix_01011110.html#ID-2201-00000005

Question: 5

In WSA , which two pieces of information are required to implement transparent user identification using Context Directory Agent? (Choose two.)

- A. the server name where Context Directory Agent is installed
- B. the server name of the global catalog domain controller
- C. the backup Context Directory Agent
- D. the shared secret
- E. the syslog server IP address

Answer: AE

Question: 6

Which three protocols are required when considering firewall rules email services using a Cisco Email Security Appliance?

- A. HTTP
- B. SMTP
- C. TFTP
- D. FTP
- E. DNS
- F. SNMP

Answer: ABE

Question: 7

What are two arguments that can be used with the show content-scan command in Cisco IOS software? (Choose two.)

- A. data
- B. session
- C. buffer
- D. statistics
- E. verbose

Answer: BD

Question: 8

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

- A. system support ssl-debug
- B. system support firewall-engine-debug
- C. system support capture-traffic
- D. system support platform

Answer: C

Question: 9

What is difference between a Cisco Content Security Management virtual appliance and a physical appliance?

- A. Migration between virtual appliance of varying sizes is possible, but physical appliances must be of equal size.
- B. The virtual appliance requires an additional license to run on a host.
- C. The virtual appliance requires an additional license to activate its adapters.
- 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.

Answer: B

Question: 10

Which Cisco technology secures the network through malware filtering, category-based control, and reputation-based control?

- A. Cisco ASA 5500 Series appliances
- B. Cisco IPS
- C. Cisco remote-access VPNs
- D. Cisco WSA

Answer: D

Question: 11

When using Cisco AMP for Networks, which feature copies a file to the Cisco AMP cloud for analysis?

- A. Spero analysis
- B. dynamic analysis
- C. sandbox analysis
- D. malware analysis

Answer: B

Question: 12

Which type of server is required to communicate with a third-party DLP solution?

- A. an ICAP-capable proxy server
- B. a PKI certificate server
- C. an HTTP server
- D. an HTTPS server

Answer: A

Question: 13

Which detection method is also known as machine learning on Network-based Cisco Advanced Malware Protection?

- A. custom file detection

- B. hashing
- C. Spero engine
- D. dynamic analysis

Answer: D

Question: 14

Which policy is used to capture host information on the Cisco Next Generation Intrusion Prevention System?

- A. network discovery
- B. correlation
- C. intrusion
- D. access control

Answer: C

Question: 15

Which Cisco Firepower rule action displays a HTTP warning page and resets the connection of HTTP traffic specified in the access control rule ?

- A. Interactive Block with Reset
- B. Block
- C. Allow with Warning
- D. Interactive Block

Answer: D

Explanation:

Reference:

<http://www.cisco.com/c/en/us/td/docs/security/piresight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html>

Question: 16

With Cisco AMP for Endpoints on Windows, which three engines are available in the connector? (Choose three.)

- A. Ethos
- B. Tetra

- C. Annos
- D. Spero
- E. Talos
- F. ClamAV

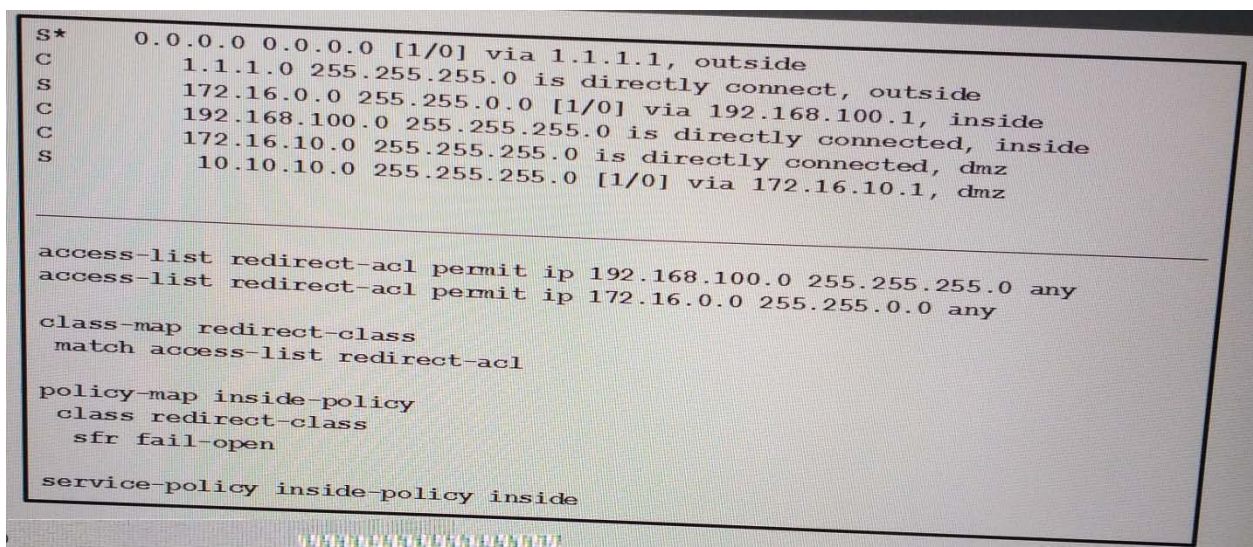
Answer: ABD

Explanation:

Reference:

<http://www.cisco.com/c/en/us/products/collateral/security/fireamp-private-cloud-virtual-appliance/datasheet-c78-733180.html>

Question: 17



Refer to the exhibit. Which option is a result of this configuration?

- A. All ingress traffic on the inside interface that matches the access list is redirected.
- B. All egress traffic on the outside interface that matches the access list is redirected.
- C. All TCP traffic that arrives on the inside interface is redirected.
- D. All ingress and egress traffic is redirected to the Cisco FirePOWER module.

Answer: C

Question: 1

What are two requirements for configuring a hybrid interface in FirePOWER? (Choose two)

- A. virtual network
- B. virtual router
- C. virtual appliance

- D. virtual switch
- E. virtual context

Answer: BD

Explanation:

Reference:

http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Hybrid_Interfaces.html

Question: 2

Which type of policy is used to define the scope for applications that are running on hosts?

- A. access control policy.
- B. application awareness policy.
- C. application detector policy.
- D. network discovery policy.

Answer: C

Question: 3

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

- A. rootkit detection
- B. spam scanning
- C. APT detection
- D. antivirus scanning
- E. URL filtering

Answer: BD

Question: 4

Which protocols can be specified in a Snort rule header for analysis?

- A. TCP, UDP, ICMP, and IP
- B. TCP, UDP, and IP
- C. TCP, UDP, and ICMP
- D. TCP, UDP, ICMP, IP, and ESP

E. TCP and UDP

Answer: A

Question: 5

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

- A. WHITELIST
- B. BLACKLIST
- C. UNKNOWNLIST
- D. SUSPECTLIST

Answer: B

Question: 6

With Cisco FirePOWER Threat Defense software, which interface mode do you configure for an IPS deployment, where traffic passes through the appliance but does not require VLAN rewriting?

- A. inline set
- B. passive
- C. inline tap
- D. routed
- E. transparent

Answer: E

Question: 7

How does the WSA policy trace tool make a request to the Proxy to emulate a client request?

- A. explicitly
- B. transparently
- C. via WCCP
- D. via policy-based routing

Answer: D

Question: 8

With Cisco AMP for Endpoints, which option shows a list of all files that have been executed in your environment?

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

Answer: C

Question: 9

When the WSA policy trace tool is used to make a request to the proxy, where is the request logged?

- A. proxy logs
- B. access logs
- C. authentication logs
- D. The request is not logged

Answer: B

Question: 10

When using Cisco FirePOWER Services for ASA, how is traffic directed from based Cisco ASA to the CiscoPOWER Services?

- A. SPAN port on a Cisco Catalyst switch.
- B. WCCP on the ASA.
- C. inline interface pair on the Cisco FirePOWER module.
- D. service policy on the ASA.

Answer: A

Question: 11

In a Cisco FirePOWER intrusion policy, which two event actions can be configured on a rule? (Choose two.)

- A. drop packet
- B. drop and generate

- C. drop connection
- D. capture trigger packet
- E. generate events

Answer: B

Question: 12

Which object can be used on a Cisco FirePOWER appliance, but not in an access control policy rule on Cisco FirePOWER services running on a Cisco ASA?

- A. URL
- B. security intelligence
- C. VLAN
- D. geolocation

Answer: C

Question: 13

Which two appliances support logical routed interfaces? (Choose two.)

- A. FirePOWER services for ASA-5500-X
- B. FP-4100-series
- C. FP-8000-series
- D. FP-7000-series
- E. FP-9300-series

Answer: D

Thank You for Trying Our Product

For More Information – **Visit link below:**

<http://www.examsboost.com/>

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



WE ACCEPT

