Vendor: Cisco

Exam Code: 300-210

Exam Name: Implementing Cisco Threat Control Solutions (SITCS)

Version: Demo

QUESTION 1
Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?

A. cloud web services
B. network AMP
C. private cloud
D. public cloud

Correct Answer: C

QUESTION 2
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

Correct Answer: C

QUESTION 3
Which type of policy do you configure if you want to look for a combination of events using Boolean logic?

A. correlation
B. application detector
C. traffic profile
D. access control
E. intrusion

Correct Answer: A

QUESTION 4
In which two places can thresholding settings be configured? (Choose two.)

A. globally, per intrusion policy
B. globally, within the network analysis policy
C. on each access control rule
D. on each IPS rule
E. per preprocessor, within the network analysis policy

Correct Answer: CD

QUESTION 5
Which SSL traffic decryption feature is used when decrypting traffic from an external host to a server on your network?

A. Decrypt by stripping the server certificate.
B. Decrypt by resigning the server certificate
C. Decrypt with a known private key
D. Decypt with a known public key

Correct Answer: B

QUESTION 6
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

Correct Answer: C

QUESTION 7
A system administrator wants to know if the email traffic from a remote partner will active special treatment message filters that are created just for them. Which tool on the Cisco Email Security gateway can you use to debug and emulate the flow that a message takes through the work queue?

A. the trace tool
B. centralized or local message tracking
C. the CLI findevent command
D. the CLI grep command
E. the message tracker interface

Correct Answer: A

QUESTION 8
Which two routing options are valid with cisco firePOWER threat Defense version 6.0? (Choose two)

A. ECMP with up to three equal cost paths across multiple interfaces
B. BGPv6
C. BGPv4 with nonstop forwarding
D. BGPv4 unicast address family
E. ECMP with up to four equal cost paths

Correct Answer: AD

QUESTION 9
Which two options are the basic parts of a Snort rule? (Choose two)

A. rule policy
B. rule header
C. Rule assignment and ports
D. rule options
E. Rule footer

Correct Answer: BD

QUESTION 10
With Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two.)

A. Speed
B. Duplex
C. Media Type
D. Redundant Interface
E. EtherChannel

Correct Answer: AB

QUESTION 11
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

Correct Answer: D

QUESTION 12
An engineer is configuring a Cisco Email Security Appliance (ESA) and chooses "Preferred" as the settings for TLS on a HAT Mail Flow Policy. Which result occurs?.

A. TLS is allowed for outgoing connections to MTAs. Connection to the listener require encrypted Simple Mail Transfer Protocol conversations
B. TLS is allowed for incoming connections to the listener from MTAs, even after a STARTTLS command received
C. TLS is allowed for incoming connections to the listener from MTAs. Until a STARTTLS command received, the ESA responds with an error message to every command other than No Option, EHLO, or QUIT.
D. TLS is allowed for outgoing connections to the listener from MTAs. Until a STARTTLS command received, the ESA responds with an error message to every command other than No Option (NOOP), EHLO, or QUIT.

Correct Answer: D

QUESTION 13
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.

Correct Answer: B

QUESTION 14
Which two ports does the ISR G2 connector for CWS support redirection of HTTP traffic? (Choose two)

A. TCP port 65535
B. UDP port 8080
C. TCP port 88
D. TCP port 80
E. UDP port 80

Correct Answer: AD

QUESTION 15
Which policy must you edit to make changes to the Snort preprocessors?

A. access control policy
B. network discovery policy
C. intrusion policy
D. file policy
E. network analysis policy

Correct Answer: A

QUESTION 16
Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the Host Access Table Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance. Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the four multiple choice questions.

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

Correct Answer: D

QUESTION 17
Which Cisco FirePOWER setting is used to reduce the number of events received in a period of time and avoid being overwhelmed?

A. thresholding
B. rate-limiting
C. limiting
D. correlation

Correct Answer: D

QUESTION 18
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

Correct Answer: C

QUESTION 19
Which two TCP ports can allow the Cisco Firepower Management Center to communication with FireAMP cloud for file disposition information? (Choose two.)

A. 8080
B. 22
C. 8305
D. 32137
E. 443

Correct Answer: DE
Explanation:
http://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp- private-cloud-virtual-appliance/118336-configure-fireampprivatecloud-00html?referring_site=RE&pos=2&page=
http://www.cisco.com/c/en/us/support/docs/securi ty/sourcefire-amp-appliances/118121-technote-sourcefire-00.html

QUESTION 20
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.

Correct Answer: C

QUESTION 21
Which option lists the minimum requirements to deploy a managed device inline?

A. passive interface, security zone, MTU, and link mode.
B. passive interface, MTU, MDI/MDIX, and link mode.
C. inline interfaces, MTU, MDI/MDIX, and link mode.
D. inline interfaces, security zones, MTU, and link mode.

Correct Answer: A

QUESTION 22
A customer is concerned with their employee's internet usage and has asked for more web traffic control. Which two features of the cisco web security appliance help with issue? (Choose two)

A. Advanced Malware Protection
B. Dynamic ARP Inspection
C. DHCP spoofing Protection
D. Network Address Translation
E. Application Visibility and Control

Correct Answer: AE

QUESTION 23
An engineer must architect an AMP private cloud deployment. What is the benefit of running in air-gaped mode?

A. Internet connection is not required for disposition.
B. Database sync time is reduced.
C. Disposition queries are done on AMP appliances.
D. A dedicated server is needed to run amp-sync.

Correct Answer: D

QUESTION 24
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

Correct Answer: B