300-206.examcollection.premium.exam.195q

Number: 300-206
Passing Score: 800
Time Limit: 120 min
File Version: 8.0

300-206

Implementing Cisco Edge Network Security Solutions

Version 8.0

Exam A

QUESTION 1
All 30 users on a single floor of a building are complaining about network slowness. After investigating the access switch, the network administrator notices that the MAC address table is full (10,000 entries) and all traffic is being flooded out of every port. Which action can the administrator take to prevent this from occurring?

A. Configure port-security to limit the number of mac-addresses allowed on each port
B. Upgrade the switch to one that can handle 20,000 entries
C. Configure private-vlans to prevent hosts from communicating with one another
D. Enable storm-control to limit the traffic rate
E. Configure a VACL to block all IP traffic except traffic to and from that subnet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A network printer has a DHCP server service that cannot be disabled. How can a layer 2 switch be configured to prevent the printer from causing network issues?

A. Remove the ip helper-address
B. Configure a Port-ACL to block outbound TCP port 68
C. Configure DHCP snooping
D. Configure port-security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A switch is being configured at a new location that uses statically assigned IP addresses. Which will ensure that ARP inspection works as expected?

A. Configure the ’no-dhcp’ keyword at the end of the ip arp inspection command

B. Enable static arp inspection using the command ’ip arp inspection static vlan vlan-number
C. Configure an arp access-list and apply it to the ip arp inspection command
D. Enable port security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following would need to be created to configure an application-layer inspection of SMTP traffic operating on port 2525?

A. A class-map that matches port 2525 and applying an inspect ESMTP policy-map for that class in the global inspection policy
B. A policy-map that matches port 2525 and applying an inspect ESMTP class-map for that policy
C. An access-list that matches on TCP port 2525 traffic and applying it on an interface with the inspect option
D. A class-map that matches port 2525 and applying it on an access-list using the inspect option

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which command is used to nest objects in a pre-existing group?

A. object-group
B. network group-object
C. object-group network
D. group-object

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which threat-detection feature is used to keep track of suspected attackers who create connections to too many hosts or ports?

A. complex threat detection
B. scanning threat detection
C. basic threat detection
D. advanced threat detection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
What is the default behavior of an access list on the Cisco ASA security appliance?

A. It will permit or deny traffic based on the access-list criteria.
B. It will permit or deny all traffic on a specified interface.
C. An access group must be configured before the access list will take effect for traffic control.
D. It will allow all traffic.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
What is the default behavior of NAT control on Cisco ASA Software Version 8.3?

A. NAT control has been deprecated on Cisco ASA Software Version 8.3.
B. It will prevent traffic from traversing from one enclave to the next without proper access configuration.
C. It will allow traffic to traverse from one enclave to the next without proper access configuration.
D. It will deny all traffic.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which three options are hardening techniques for Cisco IOS routers? (Choose three.)

A. limiting access to infrastructure with access control lists
B. enabling service password recovery
C. using SSH whenever possible
D. encrypting the service password
E. using Telnet whenever possible
F. enabling DHCP snooping

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which three commands can be used to harden a switch? (Choose three.)

A. switch(config-if)# spanning-tree bpdufilter enable
B. switch(config)# ip dhcp snooping
C. switch(config)# errdisable recovery interval 900
D. switch(config-if)# spanning-tree guard root
E. switch(config-if)# spanning-tree bpduguard disable
F. switch(config-if)# no cdp enable

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
What are three features of the Cisco ASA 1000V? (Choose three.)

A. cloning the Cisco ASA 1000V
B. dynamic routing
C. the Cisco VNMC policy agent
D. IPv6
E. active/standby failover
F. QoS

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
If the Cisco ASA 1000V has too few licenses, what is its behavior?

A. It drops all traffic.
B. It drops all outside-to-inside packets.
C. It drops all inside-to-outside packets.
D. It passes the first outside-to-inside packet and drops all remaining packets.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A network administrator is creating an ASA-CX administrative user account with the following parameters:

- The user will be responsible for configuring security policies on network devices.
- The user needs read-write access to policies.
- The account has no more rights than necessary for the job.

What role will the administrator assign to the user?

A. Administrator
B. Security administrator
C. System administrator
D. Root Administrator
E. Exec administrator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
What command alters the SSL ciphers used by the Cisco Email Security Appliance for TLS sessions and HTTPS access?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
What is the CLI command to enable SNMPv3 on the Cisco Web Security Appliance?

A. snmpconfig
B. snmpenable
C. configsnmp
D. enablesnmp

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
The Cisco Email Security Appliance can be managed with both local and external users of different privilege levels. What three external modes of authentication are supported? (Choose three.)

A. LDAP authentication
B. RADIUS Authentication
C. TACAS
D. SSH host keys
E. Common Access Card Authentication
F. RSA Single use tokens

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which tool provides the necessary information to determine hardware lifecycle and compliance details for deployed network devices?

A. Prime Infrastructure
B. Prime Assurance
C. Prime Network Registrar
D. Prime Network Analysis Module

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which three compliance and audit report types are available in Cisco Prime Infrastructure? (Choose three.)

A. Service

B. Change Audit
C. Vendor Advisory
D. TAC Service Request
E. Validated Design
F. Smart Business Architecture

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Cisco Security Manager can manage which three products? (Choose three.)

A. Cisco IOS
B. Cisco ASA
C. Cisco IPS
D. Cisco WLC
E. Cisco Web Security Appliance
F. Cisco Email Security Appliance
G. Cisco ASA CX
H. Cisco CRS

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which two web browsers are supported for the Cisco ISE GUI? (Choose two.)

A. HTTPS-enabled Mozilla Firefox version 3.x
B. Netscape Navigator version 9
C. Microsoft Internet Explorer version 8 in Internet Explorer 8-only mode
D. Microsoft Internet Explorer version 8 in all Internet Explorer modes

E. Google Chrome (all versions)

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
When a Cisco ASA is configured in multicontext mode, which command is used to change between contexts?

A. changeto config context
B. changeto context
C. changeto/config context change
D. changeto/config context 2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which statement about the Cisco Security Manager 4.4 NAT Rediscovery feature is true?

A. It provides NAT policies to existing clients that connect from a new switch port.
B. It can update shared policies even when the NAT server is offline.
C. It enables NAT policy discovery as it updates shared polices.
D. It enables NAT policy rediscovery while leaving existing shared polices unchanged.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
When you install a Cisco ASA AIP-SSM, which statement about the main Cisco ASDM home page is true?

A. It is replaced by the Cisco AIP-SSM home page.
B. It must reconnect to the NAT policies database.
C. The administrator can manually update the page.
D. It displays a new Intrusion Prevention panel.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which Cisco product provides a GUI-based device management tool to configure Cisco access routers?

A. Cisco ASDM
B. Cisco CP Express
C. Cisco ASA 5500
D. Cisco CP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which three options describe how SNMPv3 traps can be securely configured to be sent by IOS? (Choose three.)

A. An SNMPv3 group is defined to configure the read and write views of the group.
B. An SNMPv3 user is assigned to SNMPv3 group and defines the encryption and authentication credentials.
C. An SNMPv3 host is configured to define where the SNMPv3 traps will be sent.
D. An SNMPv3 host is used to configure the encryption and authentication credentials for SNMPv3 traps.
E. An SNMPv3 view is defined to configure the address of where the traps will be sent.
F. An SNMPv3 group is used to configure the OIDs that will be reported.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A network engineer is asked to configure NetFlow to sample one of every 100 packets on a router's fa0/0 interface. Which configuration enables sampling, assuming that NetFlow is already configured and running on the router's fa0/0 interface?

A. flow-sampler-map flow1
mode random one-out-of 100
interface fas0/0
flow-sampler flow1
B. flow monitor flow1
mode random one-out-of 100
interface fas0/0
ip flow monitor flow1
C. flow-sampler-map flow1
one-out-of 100
interface fas0/0
flow-sampler flow1
D. ip flow-export source fas0/0 one-out-of 100

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
What is the default log level on the Cisco Web Security Appliance?

A. Trace
B. Debug
C. Informational
D. Critical

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which command sets the source IP address of the NetFlow exports of a device?

A. ip source flow-export
B. ip source netflow-export
C. ip flow-export source
D. ip netflow-export source

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which two SNMPv3 features ensure that SNMP packets have been sent securely?" Choose two.

A. host authorization
B. authentication
C. encryption

D. compression

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which three logging methods are supported by Cisco routers? (Choose three.)

A. console logging
B. TACACS+ logging
C. terminal logging
D. syslog logging
E. ACL logging
F. RADIUS logging

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which three options are default settings for NTP parameters on a Cisco device? (Choose three.)

A. NTP authentication is enabled.
B. NTP authentication is disabled.
C. NTP logging is enabled.
D. NTP logging is disabled.
E. NTP access is enabled.
F. NTP access is disabled.

Correct Answer: BDE
Section: (none)
Explanation