

Cisco

300-206 Exam

Cisco Implementing Cisco Edge Network Security Solutions Exam



Thank you for Downloading 300-206 exam PDF Demo

You can also Buy our 300-206 Premium Full Version

<https://www.certkillers.net/Exam/300-206>

<https://www.certkillers.net>

Version: 17.0

Question: 1

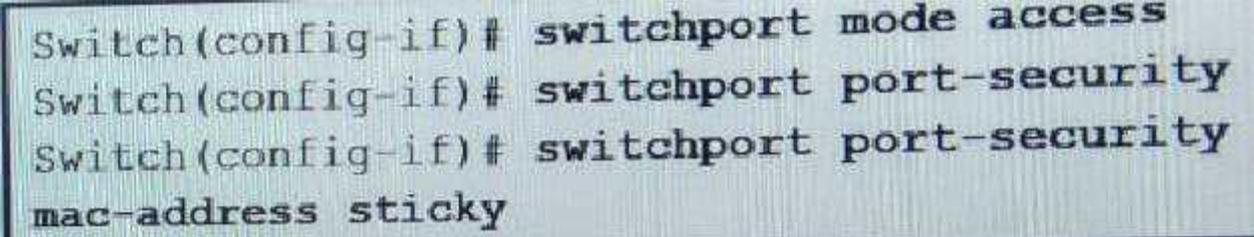
Which two user privileges does ASDM allow engineer to create? (Choose two)

- A. Full access
- B. admin
- C. read-write
- D. read-only
- E. write-only

Answer: CE

Question: 2

Refer to the exhibit.



```
Switch(config-if) # switchport mode access
Switch(config-if) # switchport port-security
Switch(config-if) # switchport port-security
mac-address sticky
```

Which two are true statements about the expected port security behavior? (Choose two)

- A. If a violation occurs, the switch port waits one minute to recover by default.
- B. Only one MAC address can be learned by default on the switch port.
- C. Up to five MAC addresses can be learned by default on the switch port.
- D. If a violation occurs, the switch port remains active, but the traffic is dropped.
- E. If a violation occurs, the switch port shuts down.

Answer: BE

Question: 3

An engineer is applying best practices to stop STP unauthorized changes from the user port. Which two actions help accomplish this task? (Choose two)

- A. Enable STP Guard
- B. Configure RSTP
- C. Disable STP
- D. Enable BPDU Guard
- E. Enable Root Guard

Answer: DE

Question: 4

When you enable IP source Guard on private VLAN ports, which additional action must you take for IP Source Guard to be effective?

- A. Enable DHCP snooping on the isolated VLAN
- B. Enable BPDU guard on the isolated VLAN.
- C. Enable BPDU guard on the primary VLAN.
- D. Enable DHCP snooping on the primary VLAN.

Answer: D

Question: 5

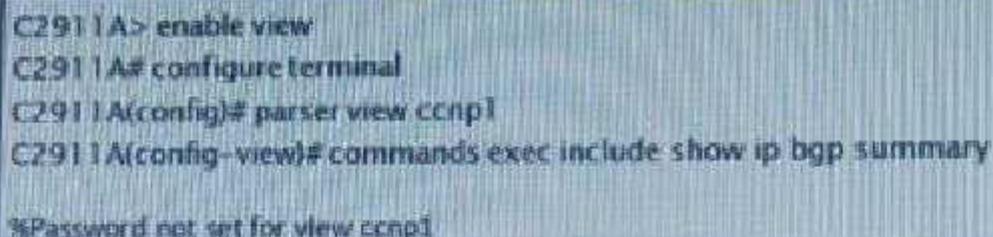
A network engineer wants to add new view to an IOS device configured with RBAC. Which privilege is required for that task?

- A. Level 16
- B. Level 15
- C. root view
- D. admin view

Answer: B

Question: 6

Refer to the exhibit.



```
C2911A> enable view
C2911A# configure terminal
C2911A(config)# parser view ccnp1
C2911A(config-view)# commands exec include show ip bgp summary
%Password not set for view ccnp1
```

An engineer is configuring IOS role based CLI access and is getting an error upon entering the command* exec include show ip bgp summary parser view command. Based on the console message received, which command would fix this error?

- A. enable secret <password>
- B. username <user> secret <password>
- C. password <password>
- D. secret 5 <encrypted password>

Answer: D

Question: 7

After a session has been secured with MACsec, which two types of traffic can be sent and received unencrypted?

- A. EAPOL-Start
- B. DHCP offer
- C. Cisco Discovery Protocol
- D. DHCP discover
- E. EAPOL-Logoff

Answer: AC

Question: 8

Which two main functions for application inspection on ASA are true?

- A. When services use dynamically assigned ports, the application inspection identifies dynamic port and permits data on these ports.
- B. When services embed IP addresses in the packet, the application inspection translates embedded addresses and updates the checksum.
- C. When services are operating on nonstandard ports, the application inspection identifies the nonstandard port and allows the service to run normally.
- D. When services need IP options to function, the application inspection keeps IP options during the packet transition through the appliance.
- E. When services use load balancing, the application inspection ensures that connections are load balanced across the servers equally.

Answer: AB

Question: 9

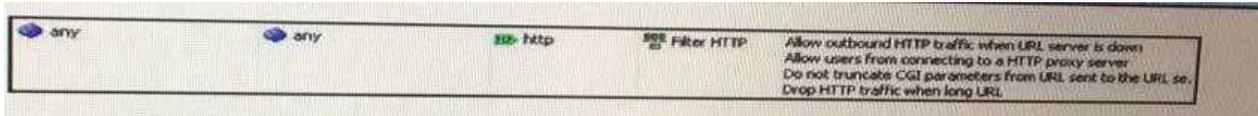
An engineer suspects that client workstations are experiencing extremely poor response time due to a man in middle attack. Which feature must be enabled and configured to provide relief from this type of attack?

- A. Internet Key Exchange
- B. Link Aggregation
- C. Reverse ARP
- D. Dynamic ARP Inspection
- E. private VLANs

Answer: D

Question: 10

Refer to the exhibit.



Which option describes the role of the filter rule on this Cisco ASA firewall?

- A. to discard http traffic destined to a proxy server
- B. to define allowed traffic when the URL filtering server is unavailable
- C. to perform deep packet inspection on all http traffic crossing the Cisco ASA
- D. to send http traffic to a defined URL filtering server

Answer: D

Question: 11

Which option is a consequence when an engineer changes the snmp server local engineID in router?

- A. The SNMP configuration that was created previously is invalid.
- B. The users that were created previously are invalid.
- C. The community that was created previously is invalid.
- D. The groups that were created previously are invalid

Answer: B

Question: 12

HTTPS server is configured on a router for management. Which command will change the router's listening port from 433 to 444?

- A. ip https secure-port 444
- B. ip http secure-server 444
- C. ip http server secure-port 444
- D. ip http secure-port 444

Answer: D

Question: 13

A security engineer is troubleshooting traffic across a Cisco ASA firewall using a packet tracer. When configuring the packet tracer, which option must be used first?

- A. interface
- B. protocol
- C. source

D. destination

Answer: A

Question: 14

Which two statements about the utilization of IPv4 and IPv6 addresses in the Cisco ASA 9.x firewall access list configuration are true? (Choose two.)

- A. Mixed IPv4 and IPv6 addresses cannot be used in the same access list entry
- B. Mixed IPv4 and IPv6 addresses can be used in the same access list entry
- C. Mixed IPv4 and IPv6 addresses can be used in the same access list for network object group
- D. Mixed IPv4 and IPv6 addresses cannot be used in the same access list
- E. Mixed IPv4 and IPv6 addresses cannot be used in the same access list for network object group

Answer: BC

Reference:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/acl_extended.pdf

Question: 15

A user is having trouble connecting to websites on the Internet. The network engineer proposes configuring a packet capture that captures only the HTTP response traffic on the Cisco Adaptive Security Appliance between the user's workstation and Internet. If the user's workstation IP address is 10.0.0.101, which ACE is needed to achieve this capture?

- A. access-list capture permit tcp host 10.0.0.101 eq 80 any
- B. access-list capture permit tcp host 10.0.0.101 any eq 80
- C. access-list capture permit tcp any eq 80 host 10.0.0.101
- D. access-list capture permit tcp any host 10.0.0.101 eq 80

Answer: D

Question: 16

Which two mandatory policies are needed to support a regular IPsec VPN in a Cisco Security Manager environment? (Choose two.)

- A. GRE modes
- B. IKE proposal
- C. group encryption
- D. server load balance

Answer: BC

Question: 17

DRAG DROP

An engineer must create an SSHv2 configuration for a remote user with a key size of 2048 on the inside network of 192.168.0.0/19 with a fully qualified domain name. Drag and drop the Cisco ASA commands on the left onto the matching function on the right.

ssh 192.168.0.0 255.255.224.0 inside	Create enable password to use SSH
domain-name <domain>	Define user and password to connect via SSH
aaa authentication ssh console LOCAL	Configure authentication mode
ssh version 2	Specify SSH protocol version
enable password <password>	Allow access from the inside interface
username <username> password <password>	Configure FQDN
crypto key generate rsa modulus 2048	Generate a key pair

Answer:

```
enable password <password>
```

```
username <username> password <password>
```

```
aaa authentication ssh console LOCAL
```

```
ssh version 2
```

```
ssh 192.168.0.0 255.255.224.0 inside
```

```
domain-name <domain>
```

```
crypto key generate rsa modulus 2048
```

Question: 18

Which statement about Cisco ASA botnet filtering is true?

- A. BTF takes the MD5 value and compares it against the dynamic database
- B. BTF checks if the domain name in a DNS reply matches a name in the BTF database
- C. BTF can rate-limit traffic to known botnet addresses
- D. BTF redirects DNS queries to a BTF server for further analysis

Answer: C

Question: 19

Which threat level is the default used in the Botnet Traffic Filter?

- A. high
- B. moderate to very-high
- C. high to very-high

D. very-high

Answer: B

Question: 20

An engineer has successfully captured data on an ASA (ip address 10.10.10.1) and wants to download the file to analyze offline. The filename is capin.

Which option must the engineer enter to accomplish this task?

- A. https://10.10.10.1/admin/capture/capin
- B. http://10.10.10.1/admin/capture/capin/pcap
- C. https://10.10.10.1/admin/capture/capin/pcap
- D. http://10.10.10.1/admin/capture/capin

Answer: C

Question: 21

An engineer has downloaded the database files for botnet traffic filtering on an AS

A. Where are these database files stored?

- A. flash memory
- B. SSD drive
- C. ROMMON
- D. running memory

Answer: A

Question: 22

Which benefit of using centralized management to manage a Cisco IronPort ESA is true?

- A. It reduces licensing cost
- B. It requires no initial setup
- C. It requires a light client on managed devices
- D. It reduces administration time

Answer: D

Question: 23

A company is concerned with valid time sources and has asked for NTP authentication to be configured.

Multiple NTP sources are on the network. Which configuration is required on the client device to authenticate and synchronize with an NTP source?

- A. trusted key
- B. stratum hash
- C. SSL
- D. certificate preshared key

Answer: A

Question: 24

Which statement about the behavior of the Cisco ASA firewall is true?

- A. The Cisco ASA is not seen as a router hop to connect devices in routed mode
- B. All Cisco ASA interfaces are on different subnets in transparent mode
- C. The Cisco ASA clears the running configuration when changing firewall modes
- D. The Cisco ASA blocks ARP inspection packets in transparent mode

Answer: C

Question: 25

An engineering team is working diligently to achieve the fastest possible throughput on a Cisco ASA deployment within the data center without sacrificing high availability or flexibility. Which type of architecture accomplishes this goal?

- A. multiple mode, transparent contexts
- B. single mode, transparent contexts
- C. multiple mode, routed contexts
- D. single mode, routed contexts

Answer: C

Thank You for trying 300-206 PDF Demo

To Buy our 300-206 Premium Full Version visit link below

<https://www.certkillers.net/Exam/300-206>

Start Your 300-206 Preparation

“”

Download and Pass Exam 300-206 Easily with CertKillers.net questions.

<https://www.certkillers.net>