PASSTCERT
QUESTION & ANSWER

Higher Quality
Better Service!

We offer free update service for one year
HTTP://WWW.PASSTCERT.COM

Exam : **642-504**

Title : Securing Networks with Cisco Routers and Switches

Version : DEMO

1. Which two are technologies that secure the control plane of the Cisco router? (Choose two.)

A. Cisco IOS Flexible Packet Matching

B. uRPF

C. routing protocol authentication

D. CPPr

E. BPDU protection

F. role-based access control

Answer: CD

2. What are the two category types associated with 5.x signature use in Cisco IOS IPS? (Choose two.)

A. basic

B. advanced

C. 128MB.sdf

D. 256MB.sdf

E. attack-drop

F. built-in

Answer: AB

3. Refer to the exhibit.

Which optional AAA or RADIUS configuration command is used to support 802.1X guest VLAN functionality?

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa accounting system default start-stop group radius
radius-server host 10.1.1.1 auth-port 1812 acct-port 1813
radius-server key cisco123
```

A. aaa authentication dot1x default group radius

B. aaa authorization network default group radius

C. aaa accounting dot1x default start-stop group radius

D. aaa accounting system default start-stop group radius

E. radius-server host 10.1.1.1 auth-port 1812 acct-port 1813

Answer: B

4. Which is an advantage of implementing the Cisco IOS Firewall feature?

A. provides self-contained end-user authentication capabilities

B. integrates multiprotocol routing with security policy enforcement

C. acts primarily as a dedicated firewall device

D. is easily deployed and managed by the Cisco Adaptive Security Device Manager

E. provides data leakage protection capabilities

Answer: B

5. Which three statements correctly describe the GET VPN policy management? (Choose three.)

A. A central policy is defined at the ACS (AAA) server.

B. A local policy is defined on each group member.

C. A global policy is defined on the key server, and it is distributed to the group members.

D. The key server and group member policy must match.

E. The group member appends the global policy to its local policy.

Answer: BCE

6. The CPU and Memory Threshold Notifications of the Network Foundation Protection feature protects which router plane?

A. control plane

B. management plane

C. data plane

D. network plane

Answer: B

7. In DMVPN, the NHRP process allows which requirement to be met?

A. dynamic physical interface IP address at the spoke routers

B. high-availability DMVPN designs

C. dynamic spoke-to-spoke on-demand tunnels

D. dynamic routing over the DMVPN

E. dual DMVPN hub designs

Answer: A

8. Which is correct regarding the Management Plane Protection feature?

A. By default, Management Plane Protection is enabled on all interfaces.

B. Management Plane Protection provides for a default management interface.

C. Only SSH and SNMP management will be allowed on nondesignated management interfaces.

D. All incoming packets through the management interface are dropped except for those from the allowed management protocols.

Answer: D

9. What are the two enrollment options when using the SDM Certificate Enrollment wizard? (Choose two.)

A. SCEP

B. LDAP

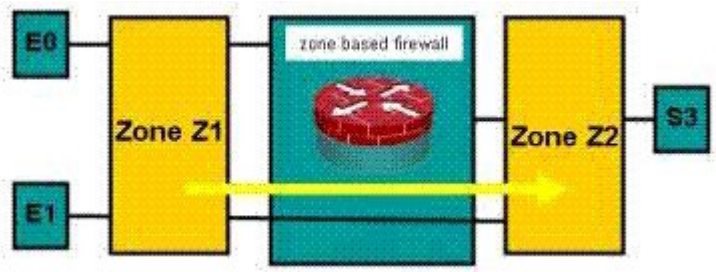
C. OCSP

D. Cut-and-Paste/Import from PC

Answer: AD

10. Refer to the exhibit.

Which two configuration commands are used to apply an inspect policy map for traffic traversing from the E0 or E1 interface to the S3 interface? (Choose two.)



A. zone-pair security test source Z1 destination Z2

B. interface E0

C. policy-map myfwpolicy

class class-default

inspect

D. ip inspect myfwpolicy out

E. ip inspect myfwpolicy in

F. service-policy type inspect myfwpolicy

Answer: AF

11. Cisco IOS Firewall supports which three of the following features? (Choose three.)

A. alerts

B. audit trails

C. multicontext firewalling

D. active/active stateful failover

E. DoS attacks protection

Answer: ABE

12. Refer to the exhibit.

What is correct based on the partial configuration shown?

```
crypto isakmp policy 101
        encr 3des
        hash sha-1
        authentication rsa-sig
        group 2
        lifetime 864000
```

A. The policy is configured to use an authentication key of 'rsa-sig'.

B. The policy is configured to use Diffie-Hellman group sha-1.

C. The policy is configured to use Triple DES IPsec encryption.

D. The policy is configured to use digital certificates.

E. The policy is configured to use access list 101 to identify the IKE-protected traffic.

Answer: D

13. When enabling Cisco IOS IPS using 5.x signatures, which required item can be downloaded from Cisco.com?

A. SDF files (128MB.sdf, 256MB.sdf, attack.drop.sdf)

B. public key

C. built-in signatures

D. Signature Micro-Engines

E. IME

Answer: B

14. Which information will be shown by entering the command show zone-pair security?

A. zone descriptions and assigned interfaces

B. all service policy maps

C. source and destination zones, and attached policy

D. physical interface members of the zone pair

Answer: C

15. Cisco IOS SSL VPN thin-client mode has which two characteristics? (Choose two.)

A. uses a Java applet

B. supports TCP and UDP applications that use static port(s)

C. provides full tunnel access like the IPsec VPN software client

D. requires the use of browser plug-ins

E. provides TCP port forwarding capabilities

Answer: AE

16. Refer to the exhibit.

What will result from this zone-based firewall configuration?

```
class-map type inspect match-all myprotocols
 match protocol http
 match protocol dns
!
policy-map type inspect myfwpolicy
 class type inspect myprotocols
  inspect
!
zone security private
zone security public
!
interface fastethernet 0/0
 zone-member security private
!
interface fastethernet 0/1
 zone-member security public
!
zone-pair security priv-to-pub source private destination public
 service-policy type inspect myfwpolicy
```

A. All traffic from the private zone to the public zone will be dropped.

B. All traffic from the private zone to the public zone will be permitted but not inspected.

C. All traffic from the private zone to the public zone will be permitted and inspected.

D. All traffic from the public zone to the private zone will be permitted but not inspected.

E. Only HTTP and DNS traffic from the private zone to the public zone will be permitted and inspected.

F. Only HTTP and DNS traffic from the public zone to the private zone will be permitted and inspected.

Answer: A

17. Cisco Easy VPN Server pushes parameters such as the client internal IP address, DHCP server IP address, and WINS server IP address to the Cisco Easy VPN Remote client during which of these phases?

A. IKE Phase 1 first-message exchange

B. IKE Phase 2 last-message exchange

C. IKE mode configuration

D. IKE XAUTH

E. IKE quick mode

Answer: C

18. Which two are capabilities of the Cisco IOS Firewall Feature Set? (Choose two.)

A. protects against worms, malicious users, and denial of service

B. provides intrusion protection capabilities

C. when combined with application inspection, performs as an advanced application layer firewall gateway

D. interoperates with Network Address Translation to conserve and simplify network address use

E. provides for secure connectivity between branch offices

Answer: AD

19. Which two commands are used to allow only SSH traffic to the router Eth0 interface and deny other management traffic (BEEP, FTP, HTTP, HTTPS, SNMP, Telnet, TFTP) to the router interfaces? (Choose two.)

A. interface eth0

B. control-plane host

C. policy-map type port-filter policy-name

D. service-policy type port-filter input policy-name

E. management-interface eth0 allow ssh

F. line vty 0 5

transport input ssh

Answer: BE

20. Cisco IOS IPS uses which alerting protocol with a pull mechanism for getting IPS alerts to the network management application?

A. HTTPS

B. SMTP

C. SNMP

D. syslog

E. SDEE

F. POP3

Answer: E