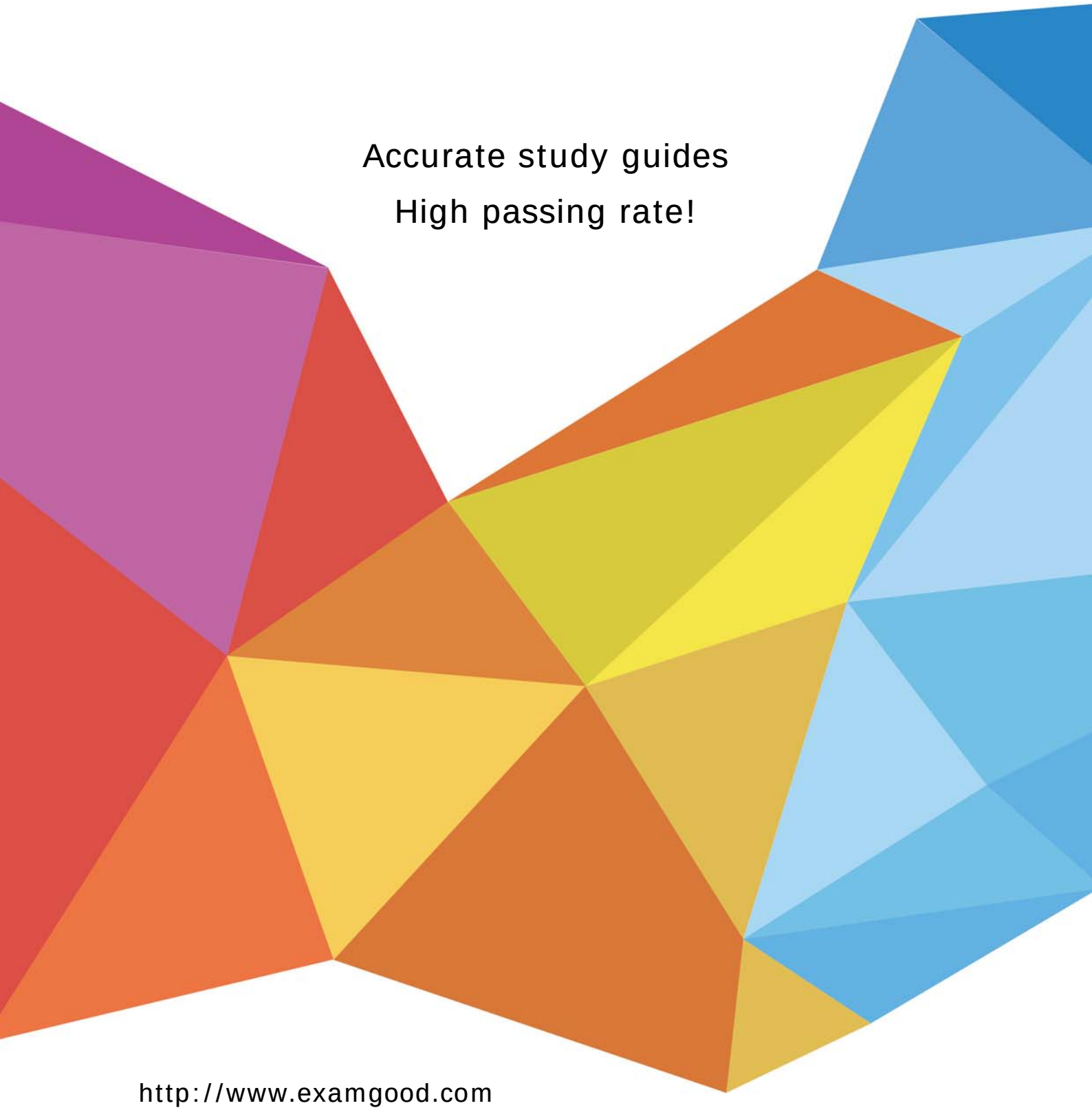
EXAMGOOD

QUESTION & ANSWER

Exam Good provides update free of charge in one year!



Accurate study guides

High passing rate!

http://www.examgood.com

Exam : **642-503**

Title : Securing Networks with Cisco Routers and Switches

Version : Demo

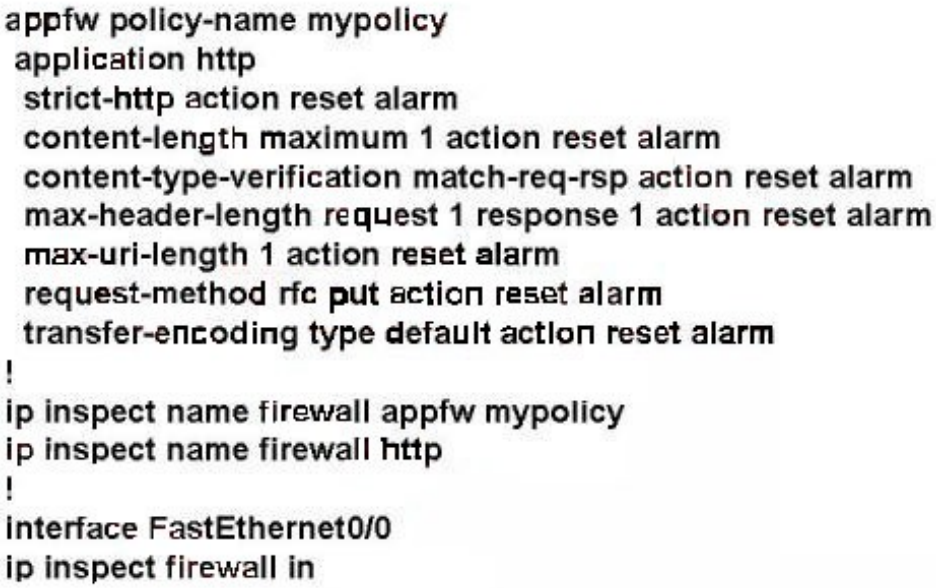
1. Which two statements are true regarding classic Cisco IOS Firewall configurations? (Choose two.)
A. You can apply the IP inspection rule in the inbound direction on the trusted interface.
B. You can apply the IP inspection rule in the outbound direction on the untrusted interface.
C. For temporary openings to be created dynamically by Cisco IOS Firewall, the access list for the returning traffic must be a standard ACL.
D. For temporary openings to be created dynamically by Cisco IOS Firewall, you must apply the IP inspectionrule to the trusted interface.
E. For temporary openings to be created dynamically by Cisco IOS Firewall, the inbound access list on the trustedinterface must be an extended ACL.
Answer: AB

2. Refer to the exhibit. Why is the Cisco IOS Firewall authentication proxy not working?

```
aaa new-model
aaa authentication login default group tacacs
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start stop group tacacs+
enable password TeSt_123
ip auth-proxy name pxy http
ip auth-proxy auth-proxy-banner
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
 ip auth-proxy pxy
no ip http server
tacacs-server host 192.168.123.14
tacacs-server key cisco
! Output omitted
```

A. The aaa authentication auth-proxy default group tacacs+ command is missing in the configuration.
B. The router local username and password database is not configured.
C. Cisco IOS authentication proxy only supports RADIUS and not TACACS+.
D. HTTP server and AAA authentication for the HTTP server is not enabled.
E. The AAA method lists used for authentication proxy should be named "pxy" rather than "default" to match the authentication proxy rule name.
Answer: D

3. Refer to the exhibit. What additional configuration is required for the Cisco IOS Firewall to reset the TCPconnection if any peer-to-peer, tunneling, or instant messaging traffic is detected over HTTP?



```
appfw policy-name mypolicy
 application http
  strict-http action reset alarm
  content-length maximum 1 action reset alarm
  content-type-verification match-req-rsp action reset alarm
  max-header-length request 1 response 1 action reset alarm
  max-uri-length 1 action reset alarm
  request-method rfc put action reset alarm
  transfer-encoding type default action reset alarm
!
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
interface FastEthernet0/0
ip inspect firewall in
```

A. class-map configuration for matching peer-to-peer, tunneling, and instant messaging traffic over HTTP, and a policy map specifying the reset action
B. the port-misuse default action reset alarm command in the HTTP application firewall policy configuration
C. the PAM configuration for mapping the peer-to-peer, tunneling, and instant messaging TCP ports to the HTTPapplication
D. the ip inspect name firewall im, ip inspect name firewall p2p, and ip inspect name firewall tunnel commands
E. the service default action reset command in the HTTP application firewall policy configuration
Answer: B

4. Refer to the exhibit. Why is the Total Active Signatures count zero?

```
R1#show ip ips all
Configured SDF Locations:
 flash:/128MB.sdf
Builtin signatures are enabled but not loaded
Last successful SDF load time: 00:50:03 UTC Aug 22 2006
IPS fail closed is disabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through SDEE is enabled
Total Active Signatures: 0
Total Inactive Signatures: 0
IPS Rule Configuration
 IPS name test
R1#
```

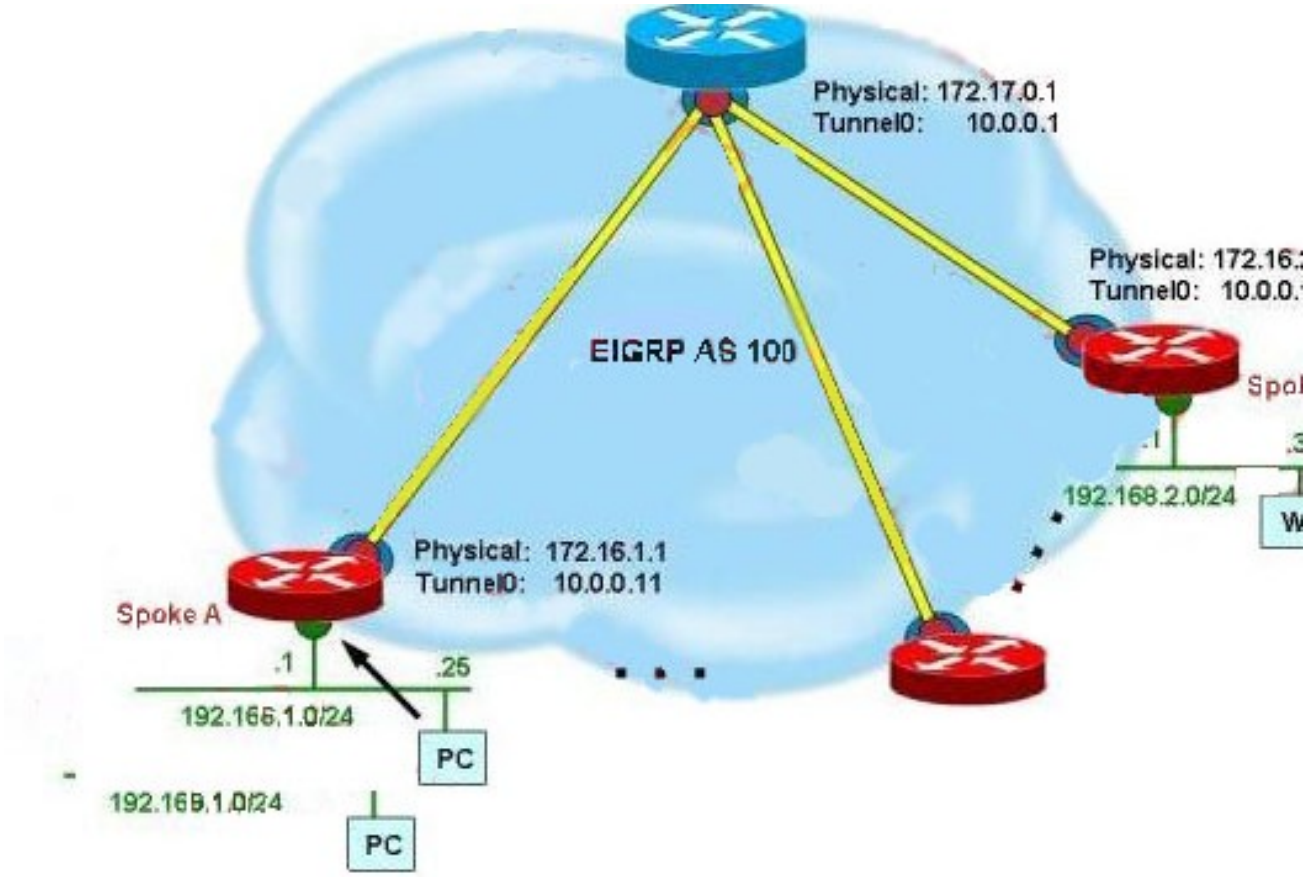
A. The 128MB.sdf file in flash is corrupted.
B. IPS is in fail-open mode.
C. IPS is in fail-closed mode.
D. IPS has not been enabled on an interface yet.
E. The flash:/128MB.sdf needs to be merged with the built-in signatures first.
Answer: D

5. Which three configurations are required to enable the Cisco IOS Firewall to inspect a user-defined application which uses TCP ports 8000 and 8001? (Choose three.)
A. access-list 101 permit tcp any any eq 8000 access-list 101 permit tcp any any eq 8001 class-map user-10 match access-group 101
B. policy-map user-10 class user-10 inspect
C. ip port-map user-10 port tcp 8000 8001 description "TEST PROTOCOL"
D. ip inspect name test appfw user-10
E. ip inspect name test user-10
F. int {type|number} ip inpsect name test in
Answer: CEF

6. What are two benefits of using an IPsec GRE tunnel? (Choose two.)
A. It allows dynamic routing protocol to run over the tunnel interface.

B. It has less overhead than running IPsec in tunnel mode.
C. It allows IP multicast traffic.
D. It requires a more restrictive crypto ACL to provide finer security control.
E. It supports the use of dynamic crypto maps to reduce configuration complexity.
Answer: AC

7. Refer to the DMVPN topology diagram in the exhibit. Which two statements are correct? (Choose two.)



A. The hub router needs to have EIGRP split horizon disabled.
B. At the Spoke A router, the next hop to reach the 192.168.2.0/24 network is 10.0.0.1.
C. Before a spoke-to-spoke tunnel can be built, the spoke router needs to send an NHRP query to the hub toresolve the remote spoke router physical interface IP address.
D. At the Spoke B router, the next hop to reach the 192.168.1.0/24 network is 172.17.0.1.
E. The spoke routers act as the NHRP servers for resolving the remote spoke physical interface IP address.
F. At the Spoke A router, the next hop to reach the 192.168.0.0/24 network is 172.17.0.1.
Answer: AC

8. Referring to a DMVPN hub router tunnel interface configuration, what can happen if the ip nhrp map multicastdynamic command is missing on the tunnel interface?
A. The NHRP request and response between the spoke router and hub router will fail.
B. The GRE tunnel between the hub router and the spoke router will be down.
C. The IPsec peering between the hub router and the spoke router will fail.
D. The dynamic routing protocol between the hub router and the spoke router will fail.

E. The NHRP mappings at the spoke routers will be incorrect.
F. The NHRP mappings at the hub router will be incorrect.
Answer: D

9. Which three of these statements are correct regarding DMVPN configuration? (Choose three.)
A. If running EIGRP over DMVPN, the hub router tunnel interface must have "next hop self" enabled: ip next-hop-self eigrp AS-Number
B. If running EIGRP over DMVPN, the hub router tunnel interface must have split horizon disabled: no ip split-horizon eigrp AS-Number
C. The spoke routers must be configured as the NHRP servers: ip nhrp nhs spoke-tunnel-ip-address
D. At the spoke routers, static NHRP mapping to the hub router is required: ip nhrp map hub-tunnel-ip-address hub-physical-ip-address
E. The GRE tunnel mode must be set to point-to-point mode: tunnel mode gre point-to-point
F. The GRE tunnel must be associated with an IPsec profile: tunnel protection ipsec profile profile-name
Answer: BDF

10. When you configure Cisco IOS WebVPN, you can use the port-forward command to enable which function?
A. web-enabled applications
B. Cisco Secure Desktop
C. full-tunnel client
D. thin clientE. CIFS
F. OWA
Answer: D