KillTest

높은 품질, 더 나은 서비스



연습 문제

https://www.killtest.kr

1년간 무료 업데이트 제공

Exam : **642-502**

Title : Securing Networks with Cisco Routers and Switches Exam(SNRS)

Version : DEMO

1.What are the two functions that crypto ACLs perform on outbound traffic? Choose two.

A.bypasses outbound traffic that should be protected by IPSec

B.selects inbound traffic that should be protected by IPSec

C.selects outbound traffic that should be protected by IPSec

D.sends outbound traffic that should not be protected by IPSec as clear text

E.discards outbound traffic that should not be protected by IPSec

F.discards outbound traffic that requires protection by IPSec

Correct:C D

2.Refer to the exhibit. An administrator cannot telnet to the router. The administrator is not prompted for a username or password and cannot ping the router. After reviewing the output of a show running-config command, what do you determine?

```
username cisco password 0 cisco
aaa new-model
aaa authentication login vty_in local
aaa authentication login con_in group tacacs+ local
aaa session-id common
interface FastEthernet0/0
 ip address 10.0.2.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.30.2.2 255.255.255.0
 duplex auto
 speed auto
accesslist 101 permit tcp any any eq 80
 line con 0
  login authentication con_in
 line aux 0
 line vty 0 4
  password cisco
  login authentication vty_in
```

A.AAA is not enabled.

B.Everything is configured correctly (the problem must be caused by something else).

C.An access control list is blocking traffic.

D.The wrong passwords are being used.

E.The TACACS server must be unreachable.

F.The wrong authentication method is applied to lines.

Correct:B

3.Which three thresholds does CBAC on the Cisco IOS Firewall provide against DoS attacks? Choose three.

A.number of half-open sessions based upon time

B.total number of half-open TCP or UDP sessions

C.number of fully open sessions based upon time

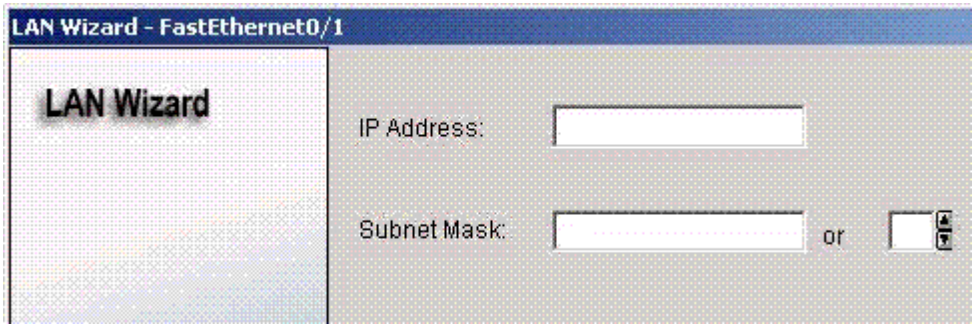
D.number of half-open TCP-only sessions per host

E.total number of fully open TCP or UDP sessions

F.number of fully open TCP-only sessions per host

Correct:A B D

4.Refer to the LAN Wizard screen in the exhibit. How many bits would you input to configure this host for a subnet consisting of two hosts on subnet 172.26.26.0?



A.3

B.4

C.24

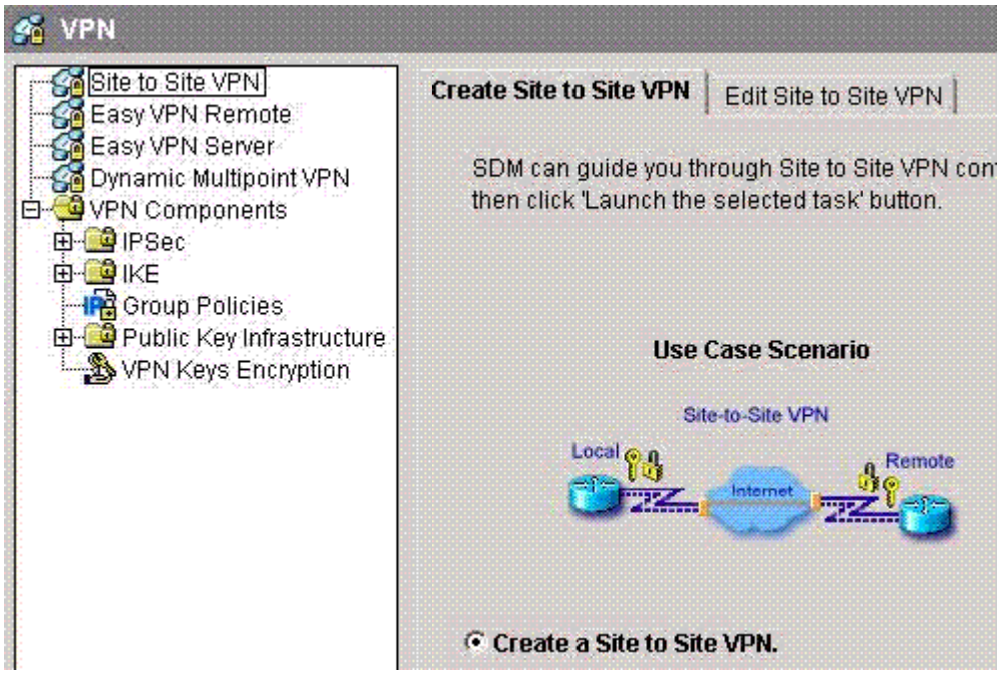
D.30

E.128

F.255

Correct:D

5.Refer to the Cisco Router and Security Device Manager page in the exhibit. What would be the result of clicking the "Launch the selected task" button in the VPN configuration screen?



A.to start the GRE site-to-site VPN connection configuration

B.to edit the site-to-site VPN connection

C.to start the security audit

D.to start the Easy VPN Server configuration

E.to start the default site-to-site VPN connection configuration

F.to start the Easy VPN Remote configuration

Correct:E

6.Where are access profiles stored with the authentication proxy features of the Cisco IOS Firewall?

A.PIX Firewall
B.Cisco router
C.Cisco VPN Concentrator
D.Cisco Secure ACS authentication server

Correct:D

7.Choose the correct command to allow IKE to establish the IPSec security associations.

A.crypto map 10 isakmp
B.crypto map 10 manual
C.crypto map MYMAP ipsec-isakmp
D.crypto map MYMAP ipsec-manual
E.crypto map MYMAP 10 ipsec-isakmp
F.crypto map MYMAP 10 ipsec-manual

Correct:E

8.Choose the correct command to generate two RSA key pairs for use with certificate authority.

A.key generate rsa general-keys
B.key generate rsa usage-keys
C.crypto key generate rsa general-keys
D.crypto key generate rsa usage-keys
E.enable crypto key generate rsa general-keys
F.enable crypto key generate rsa usage-keys

Correct:D

9.Which command is required to specify the authorization protocol for authentication proxy?

A.auth-proxy group tacacs+
B.aaa auth-proxy default group tacacs+
C.authorization auth-proxy default group tacacs+
D.aaa authorization auth-proxy default group tacacs+
E.aaa authorization auth-proxy group tacacs+
F.aaa authorization auth-proxy default group

Correct:D

10.Which Cisco Catalyst IOS command can be used to mitigate a CAM table overflow attack?

A.switch(config-if)# port-security maximum 1
B.switch(config)# switchport port-security
C.switch(config-if)# port-security
D.switch(config-if)# switchport port-security maximum 1
E.switch(config-if)# switchport access
F.switch(config-if)# access maximum 1

Correct:D