

**Exam : Cisco 642-502**

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

**Update :** 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**

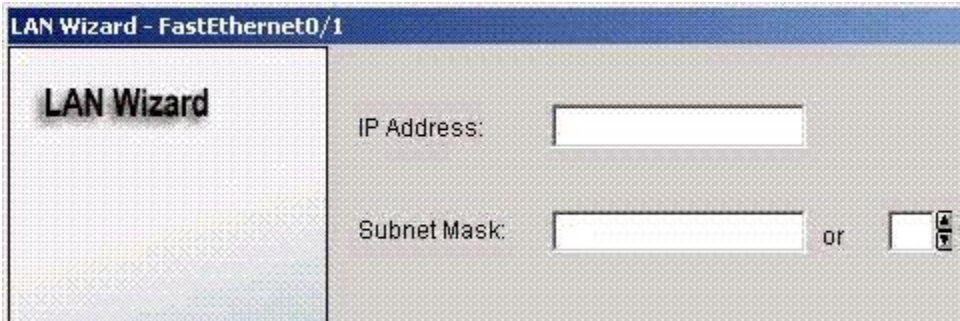
**3.Which three thresholds does CBAC on the Cisco IOS Firewall provide against DoS attacks? Choose three.**

- 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**

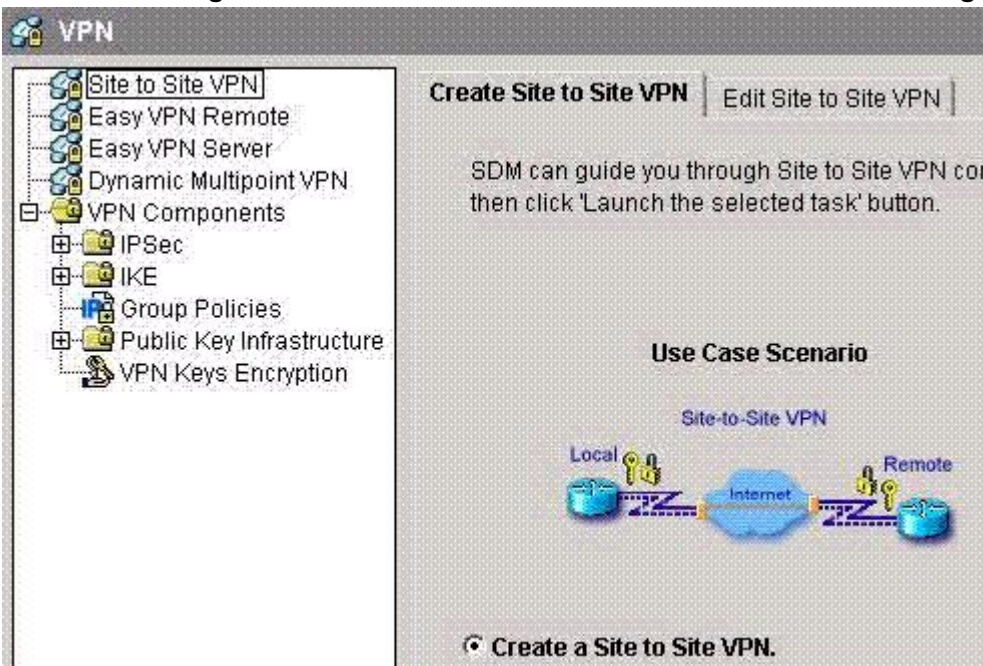
**4. Refer to the LAN Wizard screen in the exhibit. How many bits would you input to configure this host for a subnet consisting of two hosts on subnet 172.26.26.0?**



- 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**

**11.An authentication attempt to a Cisco Secure ACS for Windows server failed, yet no log entries are in the reports. What are two possible causes of this problem? (Choose two.)**

- 
- A.user is not defined
  - B.user belongs to the wrong group
  - C.CSAUTH service is down on the Cisco Secure ACS server
  - D.password has expired
  - E.user entered an incorrect password
  - F.communication path between the NAS and Cisco Secure ACS server is down

**Correct:C F**

**12.What are three main components of the Cisco IOS Firewall feature set? (Choose three.)**

- A.Context-based Access Control
- B.port security
- C.authentication proxy
- D.authentication, authorization, and accounting
- E.Intrusion Prevention System
- F.neighbor router authentication

**Correct:A C E**

**13.The SDF uses which type of file format, with a definition of each signature along with relevant configurable actions?**

- A.ASCII
- B.HTML
- C.JPEG
- D.Word
- E.text
- F.XML

**Correct:F**

**14.Which two are typical Layer 2 attacks? (Choose two.)**

- A.MAC spoofing
- B.CAM table overflow
- C.route poisoning
- D.DHCP Starvation
- E.ARP Starvation
- F.spam

**Correct:A B**

**15.What kind of signatures trigger on a single packet? (Choose one.)**

- A.regenerative
- B.cyclical
- C.atomic
- D.dynamic
- E.compound

**Correct:C**

**16.What does authentication proxy on the Cisco IOS Firewall do?**

- A.creates specific authorization policies for each user with Cisco Secure ACS, dynamic, per-user security and authorization
- B.provides additional visibility at intranet, extranet, and Internet perimeters

---

C.creates specific security policies for each user with Cisco Secure ACS, dynamic, per-user authentication and authorization

D.provides secure, per-application access control across network perimeters

**Correct:C**

**17.Select the two protocols used to provide secure communications between SDM and the target router. (Choose two.)**

A.HTTPS

B.RCP

C.Telnet

D.SSH

E.HTTP

F.AES

**Correct:A D**

**18.Which one of the following actions is used to send SDM generated commands to the target router?**

A.Refresh

B.Save

C.Deliver

D.Download

E.Copy-config

**Correct:C**

**19.Select the maximum number of routers SDM can manage simultaneously?**

A.1

B.5

C.50

D.100

E.1000

F.determined by router model

**Correct:A**

**20.Drag Drop question**

You have entered configuration mode on your VPN router in order to create an ISAKMP policy using pre-shared keys, 3DES encryption, and Diffie-Hellman Group 2. Click and drag the five necessary commands to the ordered steps.

crypto ike enable	Step 1
crypto isakmp enable	Step 2
crypto isakmp policy	Step 3
crypto isakmp policy 1	Step 4
pre-share	Step 5
authentication pre-share	
3DES	
encryption 3des	
group 2	

**Correct:**

Green choice2---->Yellow Choice1

Green choice4---->Yellow Choice2

Green choice6---->Yellow Choice3

Green choice8---->Yellow Choice4

Green choice9---->Yellow Choice5

**21.The Cisco Identity-Based Networking Services (IBNS) solution is based on which two standard implementations? (Choose two.)**

- A.TACACS+
- B.RADIUS
- C.802.11
- D.802.1x
- E.802.1q
- F.IPSec

**Correct:B D**

**22.Which module is audited first when packets enter an IOS Firewall IDS and match a specific audit rule?**

- A.TCP
- B.ICMP
- C.IP
- D.application level
- E.UDP

**Correct:C**

**23.How does the user trigger the authentication proxy after the idle timer expires?**

- A.authenticates the user

- 
- B. initiates another HTTP session
  - C. enters a new username and password
  - D. enters a valid username and password

**Correct: B**

**24. Refer to the exhibit. Given the output of the show crypto ipsec sa command, which encryption algorithm is being used?**

```
R2#sh crypto ipsec sa
```

```
interface: FastEthernet0/1
```

```
  Crypto map tag: MYMAP, local addr 172.30.2.2
```

```
protected vrf: (none)
```

```
local ident(addr/mask/proto/port): (172.30.2.2/255.255.255.255/0/0)
```

```
remote ident(addr/mask/proto/port): (172.30.7.2/255.255.255.255/0/0)
```

```
current_peer 172.30.7.2 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
```

```
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 1, #recv errors 0
```

```
local crypto endpt.: 172.30.2.2, remote crypto endpt.: 172.30.7.2
```

```
path mtu 1500, ip mtu 1500
```

```
current outbound spi: 0x5FAA1A55(1604983381)
```

```
inbound esp sas:
```

```
spi: 0x2831CBC6(674352070)
```

```
  transform: esp-des ,
```

```
  in use settings = { Tunnel, }
```

```
  conn id: 2001, flow_id: 1, crypto map: MYMAP
```

```
  sa timing: remaining key lifetime (k/sec): (4511705/3537)
```

```
  IV size: 8 bytes
```

```
  replay detection support: N
```

```
  Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcpsas:
```

```
outbound esp sas:
```

```
spi: 0x5FAA1A55(1604983381)
```

```
  transform: esp-des ,
```

```
  in use settings = { Tunnel, }
```

```
  conn id: 2002, flow_id: 2, crypto map: MYMAP
```

```
  sa timing: remaining key lifetime (k/sec): (4511705/3524)
```

```
  IV size: 8 bytes
```

```
  replay detection support: N
```

```
  Status: ACTIVE
```

- A.PCP
- B.ESP
- C.DES
- D.3DES

- E.AH
- F.HMAC

**Correct:C**

**25.Which Cisco Catalyst IOS command is used to mitigate a MAC spoofing attack?**

- A.switch(config-if)# port-security mac-address 0000.ffff.aaaa
- B.switch(config)# switchport port-security mac-address 0000.ffff.aaaa
- C.switch(config-if)# switchport port-security mac-address 0000.ffff.aaaa
- D.switch(config)# port-security mac-address 0000.ffff.aaaa
- E.switch(config-if)# mac-address 0000.ffff.aaaa
- F.switch(config)# security mac-address 0000.ffff.aaaa

**Correct:C**

**26.Which three keywords are used with the dot1x port-control command? (Choose three.)**

- A.enable
- B.force-authorized
- C.force-unauthorized
- D.authorized
- E.unauthorized
- F.auto

**Correct:B C F**

**27.Refer to the exhibit. After reviewing the running-config file, what do you determine?**

```
!
username cisco password 0 cisco
memory-size iomem 10
clock timezone EDT -5
no network-clock-participate slot 1
no network-clock-participate wic 0
no aaa new-model
ip subnet-zero

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
!
line con 0
login local
line aux 0
line vty 0 4
password cisco
login
```

- A.No one will be able to log in.
- B.No one will be able to console in.
- C.The wrong authentication method is applied to lines.

- 
- D.Users will use the local database to log in to console.
  - E.Users will use the password cisco to log in to console.
  - F.Users will use the local database to log in to vty.

**Correct:D**

**28.Which one of the following actions is used to prevent newly configured SDM commands from being sent to a target router?**

- A.Delete
- B.Remove
- C.Undo
- D.Clear-commands
- E.Refresh

**Correct:E**

**29.Choose the correct command that will load the SDF into a router and merge the new signatures with those that are already loaded in the router.**

- A.copy flash ips-sdf
- B.copy url ips-sdf
- C.copy ips-sdf url
- D.write flash ips-sdf
- E.write ips-sdf url
- F.write url ips-sdf

**Correct:B**

**30.Choose the correct command to disable signature 1000 in the SDF file.**

- A.1000 disable
- B.no ip ips signature 1000
- C.no ip ips signature 1000 enable
- D.ip ips signature 1000 disable
- E.ip signature 1000 disable
- F.signature 1000 disable

**Correct:D**