Exam Code: 642-825

Exam Name: ISCW - Implementing Secure Converged Wide Area Networks

Vendor: CISCO

Version: DEMO

Part: A

1: What are three methods of network reconnaissance? (Choose three.)

A.IP spoofing

B.one-time password

C.dictionary attack

D.packet sniffer

E.ping sweep

F.port scan

Correct Answers: D E F

2: Which three statements are correct about MPLS-based VPNs? (Choose three.)

A.Route Targets (RTs) are attributes attached to a VPNv4 BGP route to indicate its VPN membership.

B.Scalability becomes challenging for a very large, fully meshed deployment.

C.Authentication is done using a digital certificate or pre-shared key.

D.A VPN client is required for client-initiated deployments.

E.A VPN client is not required for users to interact with the network.

F.An MPLS-based VPN is highly scalable because no site-to-site peering is required.

Correct Answers: A E F

3: What are two steps that must be taken when mitigating a worm attack? (Choose two.)

A.Inoculate systems by applying update patches.

B.Limit traffic rate.

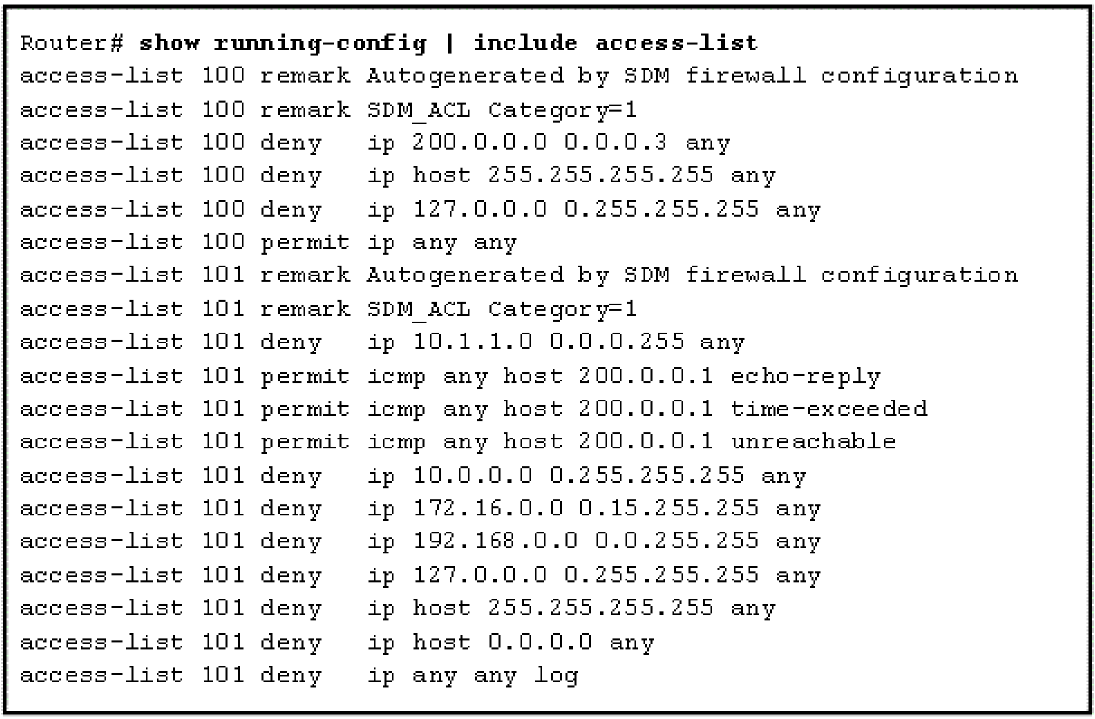
C.Apply authentication.

D.Quarantine infected machines.

E.Enable anti-spoof measures

Correct Answers: A D

4: Refer to the exhibit. What information can be derived from the SDM firewall configuration that is shown?



```
Router# show running-config | include access-list
access-list 100 remark Autogenerated by SDM firewall configuration
access-list 100 remark SDM_ACL Category=1
access-list 100 deny   ip 200.0.0.0 0.0.0.3 any
access-list 100 deny   ip host 255.255.255.255 any
access-list 100 deny   ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip any any
access-list 101 remark Autogenerated by SDM firewall configuration
access-list 101 remark SDM_ACL Category=1
access-list 101 deny   ip 10.1.1.0 0.0.0.255 any
access-list 101 permit icmp any host 200.0.0.1 echo-reply
access-list 101 permit icmp any host 200.0.0.1 time-exceeded
access-list 101 permit icmp any host 200.0.0.1 unreachable
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 deny   ip host 255.255.255.255 any
access-list 101 deny   ip host 0.0.0.0 any
access-list 101 deny   ip any any log
```

A.Access-list 100 was configured for the trusted interface, and access-list 101 was configured for the untrusted interface.

B.Access-list 101 was configured for the trusted interface, and access-list 100 was configured for the untrusted interface.

C.Access-list 100 was configured for the inbound direction, and access-list 101 was configured for the outbound direction on the trusted interface.

D.Access-list 100 was configured for the inbound direction, and access-list 101 was configured for the outbound direction on the untrusted interface.

Correct Answers: A

5: Which three statements about IOS Firewall configurations are true? (Choose three.)

A.The IP inspection rule can be applied in the inbound direction on the secured interface.

B.The IP inspection rule can be applied in the outbound direction on the unsecured interface.

C.The ACL applied in the outbound direction on the unsecured interface should be an extended ACL.

D.The ACL applied in the inbound direction on the unsecured interface should be an extended ACL.

E.For temporary openings to be created dynamically by Cisco IOS Firewall, the access-list for the returning traffic must be a standard ACL.

F.For temporary openings to be created dynamically by Cisco IOS Firewall, the IP inspection rule must be applied to the secured interface.

Correct Answers: A B D