Exam : **642-637**

Title : Securing Networks with Cisco Routers and Switches (SECURE) v1.0

Version : DEMO

1.Refer to the exhibit.

```
Router# debug crypto isakmp
*ISAKMP (1009): received packet from 192.168.2.2 dport 500 sport 500 Global (I)
MM_KEY_EXCH
ISAKMP:(1009): processing ID payload. message ID = 0
ISAKMP (1009): ID payload
        next-payload : 8
        type         : 1
        address      : 192.168.2.2
        protocol     : 17
        port         : 500
        length       : 12
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1009): processing HASH payload. message ID = 0
ISAKMP:(1009):SA authentication status:         authenticated
ISAKMP:(1009):SA has been authenticated with 192.168.2.2
```

Given the partial output of the debug command, what can be determined?

A. There is no ID payload in the packet, as indicated by the message ID = 0.

B. The peer has not matched any offered profiles.

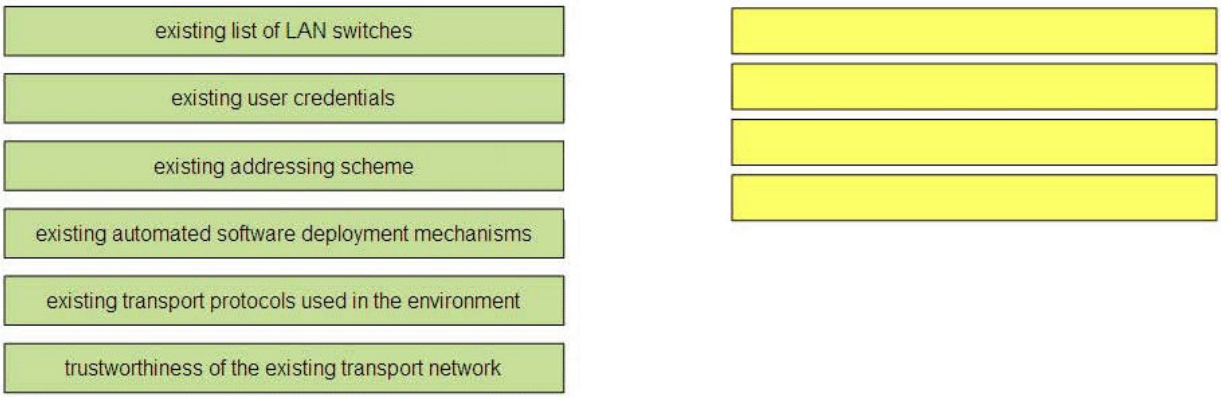
C. This is an IKE quick mode negotiation.

D. This is normal output of a successful Phase 1 IKE exchange.

Answer: D

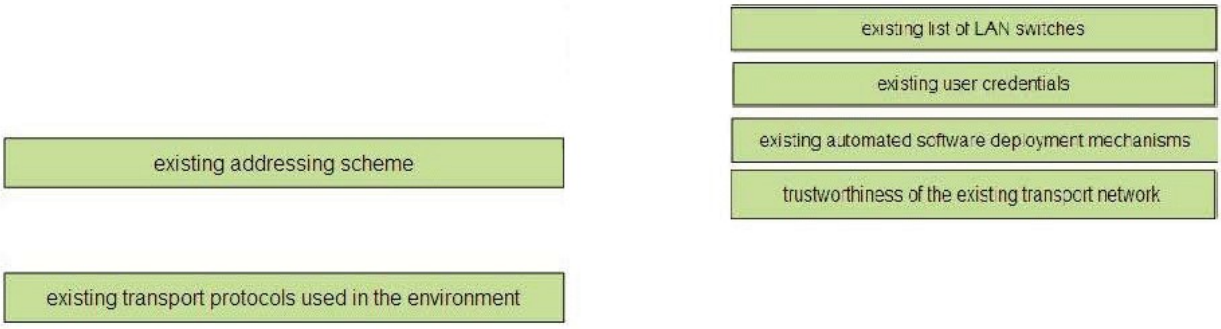
2.DRAG DROP

Drag the items on the left to the boxes on the right that identify important information you should collect prior to deploying 802.1X authentication in a Cisco IBNS environment. Not all items will be used.



Answer:

Drag the items on the left to the boxes on the right that identify important information you should collect prior to deploying 802.1X authentication in a Cisco IBNS environment. Not all items will be used.



3.Refer to the exhibit.

```
webvpn context MY-WEBVPN
 policy group GROUP-POLICY
   functions svc-enabled
   svc keep-client-installed
   svc address-pool MY-POOL
   svc default-domain cisco.com
   svc dns-server primary 10.10.1.1
   svc split dns domain.com
   svc split include 10.0.0.0 255.0.0.0
   filter tunnel FILTER-ACL
```

Which two Cisco IOS WebVPN features are enabled with the partial configuration shown? (Choose two.)
A. The end-user Cisco AnyConnect VPN software will remain installed on the end system.
B. If the Cisco AnyConnect VPN software fails to install on the end-user PC, the end user cannot use other modes.
C. Client based full tunnel access has been enabled.
D. Traffic destined to the 10.0.0.0/8 network will not be tunneled and will be allowed access via a split tunnel.
E. Clients will be assigned IP addresses in the 10.10.0.0/16 range.
Answer: A,D

4.Which two of these are benefits of implementing a zone-based policy firewall in transparent mode? (Choose two.)
A. Less firewall management is needed.
B. It can be easily introduced into an existing network.
C. IP readdressing is unnecessary.

D. It adds the ability to statefully inspect non-IP traffic.
E. It has less impact on data flows.
Answer: B,C

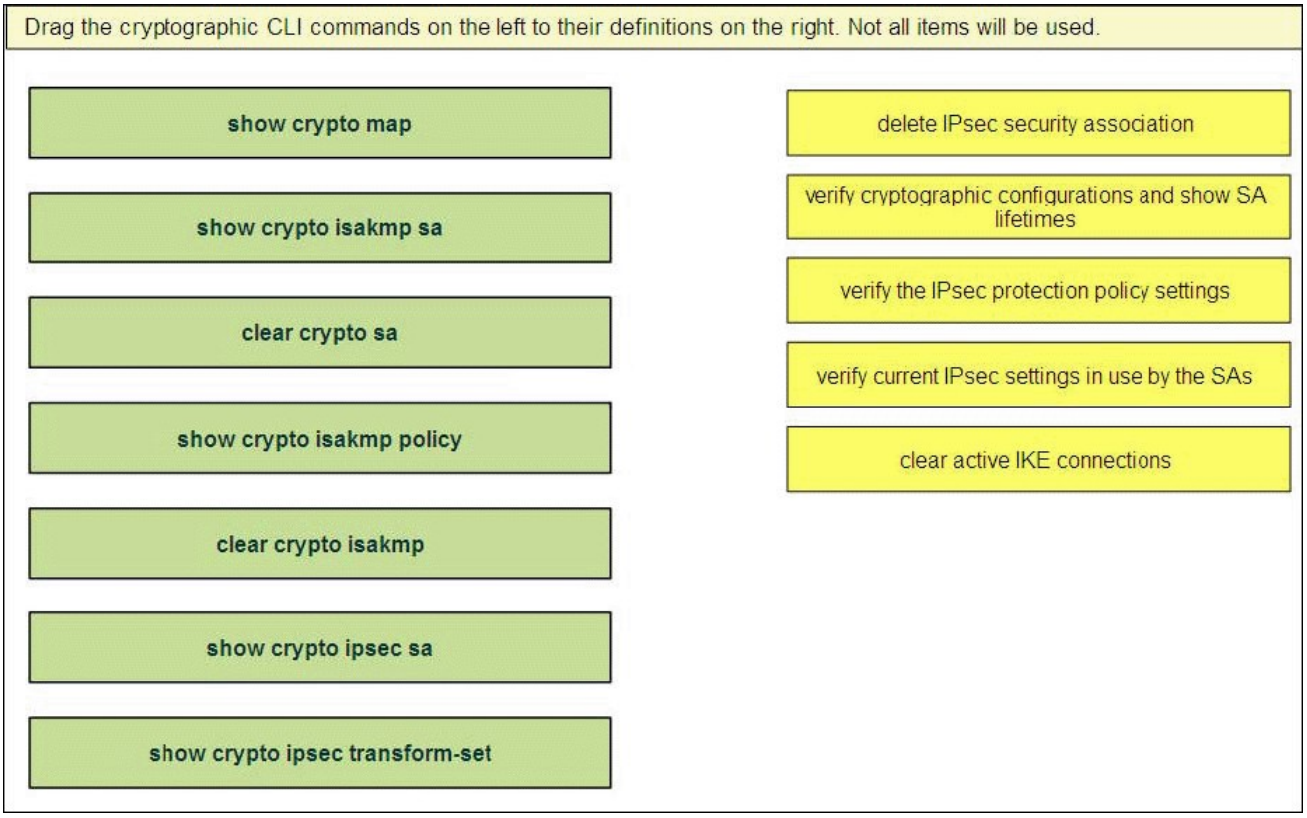
5.When configuring a zone-based policy firewall, what will be the resulting action if you do not specify any zone pairs for a possible pair of zones?
A. All sessions will pass through the zone without being inspected.
B. All sessions will be denied between these two zones by default.
C. All sessions will have to pass through the router "self zone" for inspection before being allowed to pass to the destination zone.
D. This configuration statelessly allows packets to be delivered to the destination zone.
Answer: B

6.Refer to the exhibit.
What can be determined from the output of this show command?

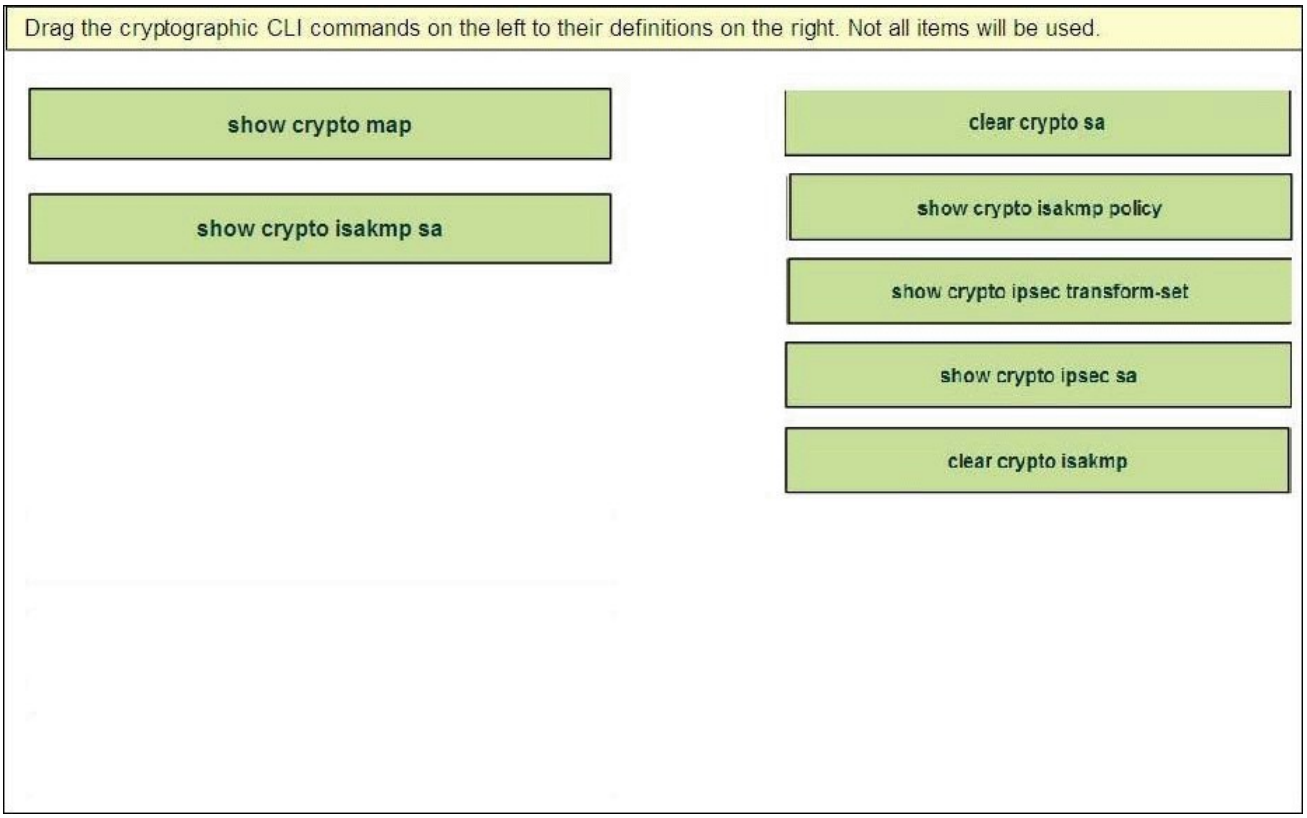
```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.1.1     192.168.2.1      QM_IDLE           1002 ACTIVE
```

A. The IPsec connection is in an idle state.
B. The IKE association is in the process of being set up.
C. The IKE status is authenticated.
D. The ISAKMP state is waiting for quick mode status to authenticate before IPsec parameters are passed between peers
E. IKE Quick Mode is in the idle state, indicating a problem with IKE phase 1.
Answer: C

7.DRAG DROP



Answer:



8.You are running Cisco IOS IPS software on your edge router. A new threat has become an issue. The Cisco IOS IPS software has a signature that can address the new threat, but you previously retired the

signature. You decide to unretire that signature to regain the desired protection level.
How should you act on your decision?
A. Retired signatures are not present in the routers memory. You will need to download a new signature package to regain the retired signature.
B. You should re-enable the signature and start inspecting traffic for signs of the new threat.
C. Unretiring a signature will cause the router to recompile the signature database, which can temporarily affect performance.
D. You cannot unretire a signature. To avoid a disruption in traffic flow, it's best to create a custom signature until you can download a new signature package and reload the router.
Answer: C

9.Which statement best describes inside policy based NAT?
A. Policy NAT rules are those that determine which addresses need to be translated per the enterprise security policy
B. Policy NAT consists of policy rules based on outside sources attempting to communicate with inside endpoints.
C. These rules use source addresses as the decision for translation policies.
D. These rules are sensitive to all communicating endpoints.
Answer: A

10.Refer to the exhibit.
What can be determined about the IPS category configuration shown?

```
ip ips signature-category
 category all
  enabled false
  retired true
 category os ios
  enabled true
  retired false
  event-action produce-alert reset-tcp-connection
```

A. All categories are disabled.
B. All categories are retired.
C. After all other categories were disabled, a custom category named "os ios" was created
D. Only attacks on the Cisco IOS system result in preventative actions.
Answer: D

11.When Cisco IOS IPS is configured to use SDEE for event notification, how are events managed?
A. They are stored in the router's event store and will allow authenticated remote systems to pull events from the event store.
B. All events are immediately sent to the remote SDEE server.
C. Events are sent via syslog over a secure SSUTLS communications channel.
D. When the event store reaches its maximum configured number of event notifications, the stored events are sent via SDEE to a remote authenticated server and a new event store is created.

Answer: A

12.Which two of these will match a regular expression with the following configuration parameters? [a-zA-Z][0-9][a-z] (Choose two.)
A. Q3h
B. B4Mn
C. aaB132AA
D. c7lm
E. BBpjnrIT
Answer: A,D

13.Which of these is a configurable Cisco IOS feature that triggers notifications if an attack attempts to exhaust critical router resources and if preventative controls have been bypassed or are not working correctly?
A. Control Plane Protection
B. Management Plane Protection
C. CPU and memory thresholding
D. SNMPv3
Answer: C

14.Which Cisco IOS IPS feature allows to you remove one or more actions from all active signatures based on the attacker and/or target address criteria, as well as the event risk rating criteria?
A. signature event action filters
B. signature event action overrides
C. signature attack severity rating
D. signature event risk rating
Answer: A

15.You are troubleshooting reported connectivity issues from remote users who are accessing corporate headquarters via an IPsec VPN connection.
What should be your first step in troubleshooting these issues?
A. issue a show crypto isakmp policy command to verify matching policies of the tunnel endpoints
B. ping the tunnel endpoint
C. run a traceroute to verify the tunnel path
D. debug the connection process and look for any error messages in tunnel establishment
Answer: B

16.Which of these is correct regarding the configuration of virtual-access interfaces?
A. They cannot be saved to the startup configuration.
B. You must use static routes inside the tunnels.
C. DVTI interfaces should be assigned a unique IP address range.
D. The Virtual-Access 1 interface must be enabled in an up/up state administratively
Answer: A

17.Refer to the exhibit. The INSIDE zone has been configured and assigned to two separate router interfaces. All other zones and interfaces have been properly configured.
Given the configuration example shown, what can be determined?

```
ip access-list extended INTRA_ZONE_ACL
  permit tcp 10.10.10.0 0.0.0.255 10.10.10.0 0.0.0.255 eq ssh
!
class-map type Inspect INTRAZONE_CLASS
  match access-group name INTRA_ZONE_ACL
!
policy-map type inspect INTRAZONE_POLICY
  class type inspect INTRAZONE_CLASS
   inspect
  class class-default
   drop log
!
zone-pair security INTRAZONE source INSIDE destination INSIDE
 service-policy type inspect INTRAZONE_POLICY
```

A. Hosts in the INSIDE zone, with addresses in the 10.10.10.0/24 network, can access any host in the 10.10.10.0/24 network using the SSH protocol.
B. If a host in the INSIDE zone attempts to communicate via SSH with another host on a different interface within the INSIDE zone, communications must pass through the router self zone using the INTRAZONE policy.
C. This is an illegal configuration. You cannot have the same source and destination zones.
D. This policy configuration is not needed, traffic within the same zone is allowed to pass by default.
Answer: A

18.Which action does the command private-vlan association 100,200 take?
A. configures VLANs 100 and 200 and associates them as a community
B. associates VLANs 100 and 200 with the primary VLAN
C. creates two private VLANs with the designation of VLAN 100 and VLAN 200
D. assigns VLANs 100 and 200 as an association of private VLANs
Answer: B

19.Which of these allows you to add event actions globally based on the risk rating of each event, without having to configure each signature individually?
A. event action summarization
B. event action filter
C. event action override
D. signature event action processor
Answer: C

20.When using Cisco Easy VPN, what are the three options for entering an XAUTH username and password for establishing a VPN connection from the Cisco Easy VPN remote router? (Choose three.)
A. using an external AAA server
B. entering the information via the router crypto ipsec client ezvpn connect CLI command in privileged EXEC mode

C. using the router local user database
D. entering the information from the PC via a browser
E. storing the XAUTH credentials in the router configuration file
Answer: B,D,E