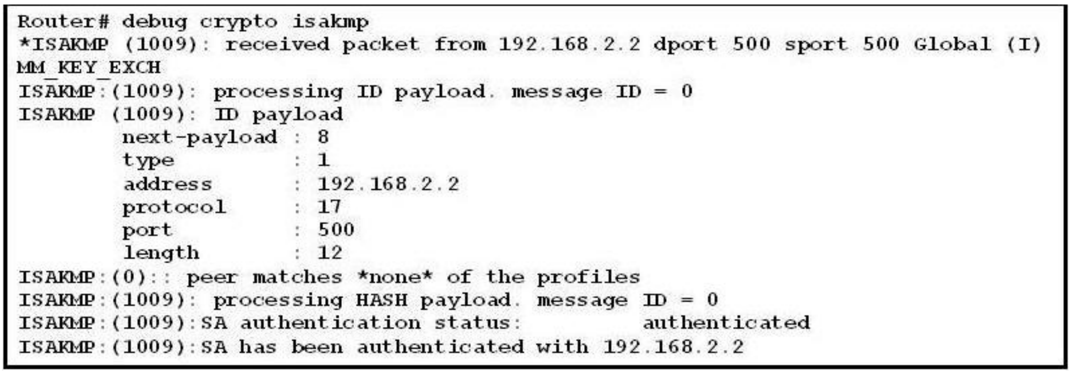
Cisco 642-637

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

Version: 8.3

QUESTION NO: 1

Refer to the exhibit. Given the partial output of the debug command, what can be determined?

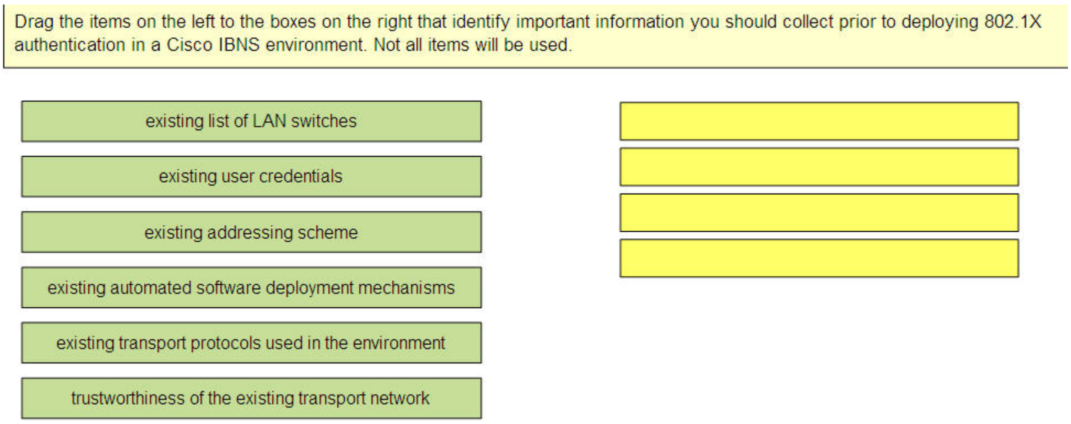


```
Router# debug crypto isakmp
*ISAKMP (1009): received packet from 192.168.2.2 dport 500 sport 500 Global (I)
MM_KEY_EXCH
ISAKMP:(1009): processing ID payload. message ID = 0
ISAKMP (1009): ID payload
        next-payload : 8
        type         : 1
        address      : 192.168.2.2
        protocol     : 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
```

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: B
Explanation:
Although the authentication of IKe phase 1 is authenticated, the exhibit question says “Given the partial output of the “debug command”, what can be determined? 2 is best for the peer has not matched any offered profiles.

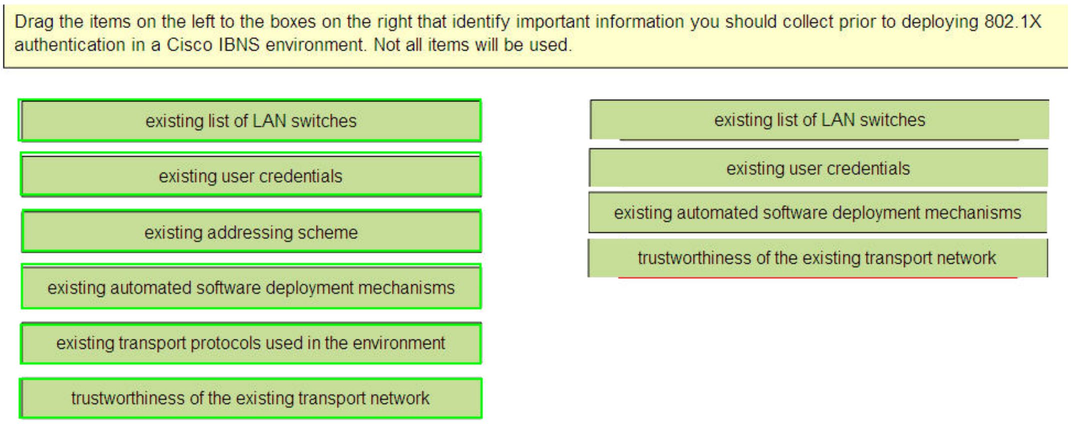
QUESTION NO: 2 DRAG DROP



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.

existing list of LAN switches
existing user credentials
existing addressing scheme
existing automated software deployment mechanisms
existing transport protocols used in the environment
trustworthiness of the existing transport network

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.

existing list of LAN switches

existing user credentials

existing addressing scheme

existing automated software deployment mechanisms

existing transport protocols used in the environment

trustworthiness of the existing transport network

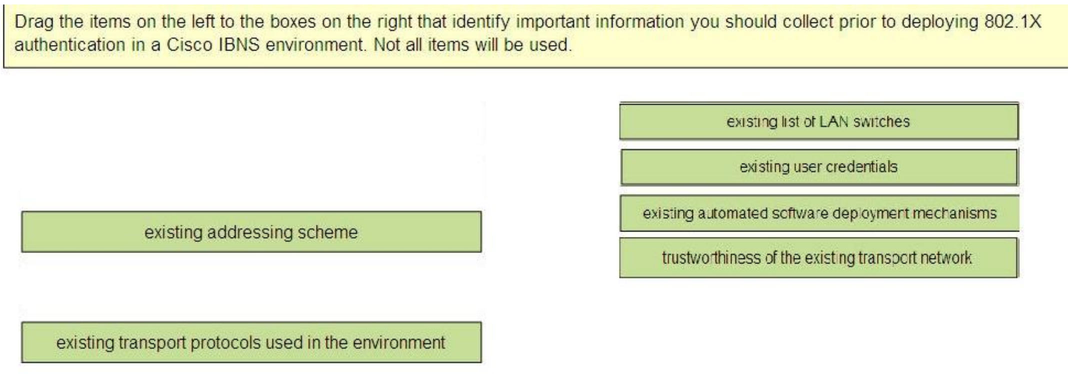
existing list of LAN switches

existing user credentials

existing automated software deployment mechanisms

trustworthiness of the existing transport network

Explanation:



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.

existing addressing scheme

existing transport protocols used in the environment

existing list of LAN switches

existing user credentials

existing automated software deployment mechanisms

trustworthiness of the existing transport network

Page 113 of the CCNP Secure guide

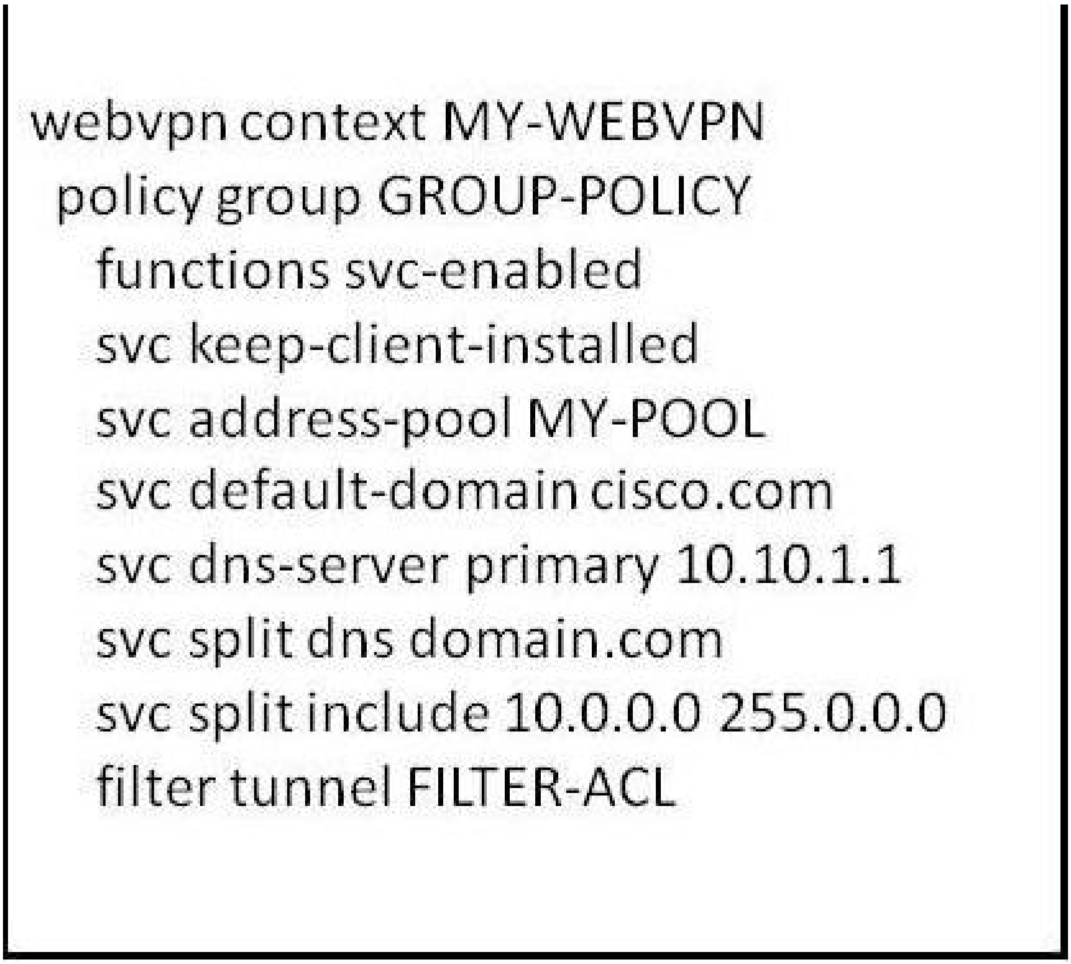
Gathering Input Parameters

Because 802.1X authentication requires several technologies to work together, up-front planning helps ensure the success of the deployment.

Part of this planning involves gathering important input information:

QUESTION NO: 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,C
Explanation:

QUESTION NO: 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

Explanation:

QUESTION NO: 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

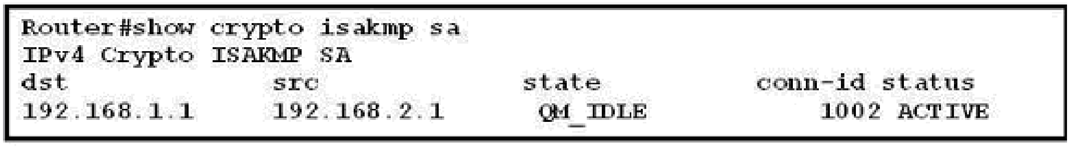
Explanation:

Zone Pair Configuration

The configuration of the zone pair is important because its configuration dictates the direction in which traffic is allowed to flow. As stated previously, a zone pair is unidirectional and is the part of the configuration that controls traffic between zones; this is referred to as interzone. If no zone pair is defined, traffic will not flow between zones

QUESTION NO: 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.

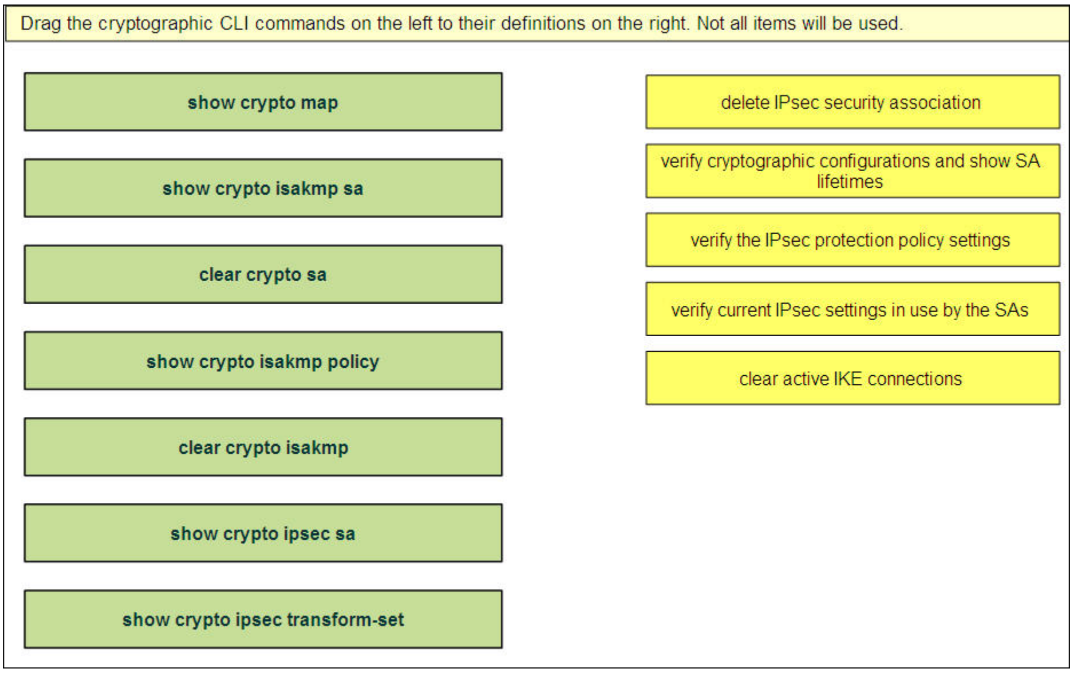
Answer: C

Explanation:

Verify Local IKE Sessions

Use the show crypto isakmp sa command to display the current IKE Security Associations (SA) on the local router. The QM_IDLE status indicates successful establishment of the IKE SA, meaning that the ISAKMP process is idle after having successfully negotiated and established SAs. Example 15-5 shows the output of the show crypto isakmp sa command.

QUESTION NO: 7 DRAG DROP



Drag the cryptographic CLI commands on the left to their definitions on the right. Not all items will be used.

show crypto map

show crypto isakmp sa

clear crypto sa

show crypto isakmp policy

clear crypto isakmp

show crypto ipsec sa

show crypto ipsec transform-set

delete IPsec security association

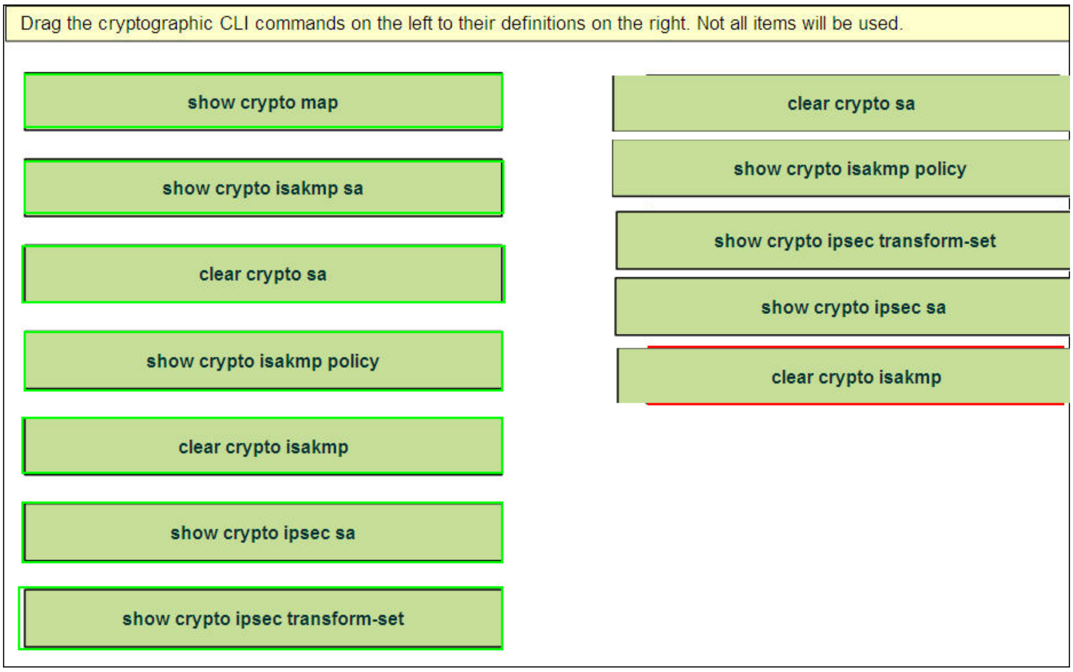
verify cryptographic configurations and show SA lifetimes

verify the IPsec protection policy settings

verify current IPsec settings in use by the SAs

clear active IKE connections

Answer:



Drag the cryptographic CLI commands on the left to their definitions on the right. Not all items will be used.

show crypto map

show crypto isakmp sa

clear crypto sa

show crypto isakmp policy

clear crypto isakmp

show crypto ipsec sa

show crypto ipsec transform-set

clear crypto sa

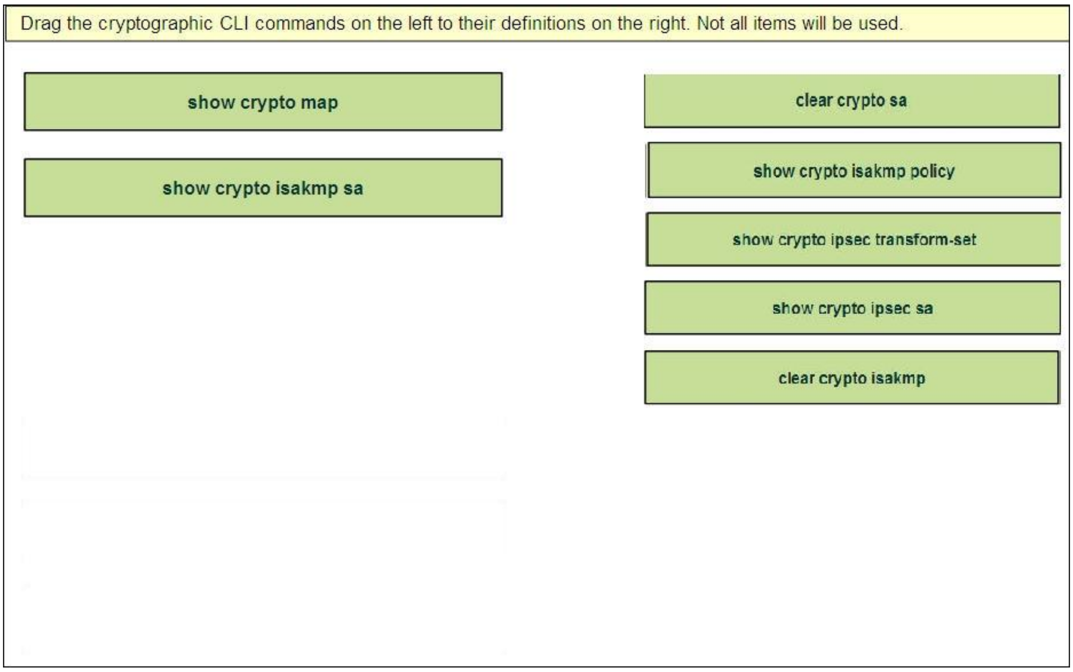
show crypto isakmp policy

show crypto ipsec transform-set

show crypto ipsec sa

clear crypto isakmp

Explanation:



Drag the cryptographic CLI commands on the left to their definitions on the right. Not all items will be used.

show crypto map

show crypto isakmp sa

clear crypto sa

show crypto isakmp policy

show crypto ipsec transform-set

show crypto ipsec sa

clear crypto isakmp

Verify cryptographic configs

router# show crypto isakmp policy

rotection suite priority 15

ncryption algorithm: DES - Data Encryption Standard (56 bit keys)

ash algorithm: Message Digest 5

uthentication method: Rivest-Shamir-Adleman Signature

iffie-Hellman Group: #2 (1024 bit)

ifetime: 5000 seconds, no volume limit

rotection suite priority 20

ncryption algorithm: DES - Data Encryption Standard (56 bit keys)

ash algorithm: Secure Hash Standard authentication method: preshared Ke

QUESTION NO: 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
Explanation:
Some signatures can be retired. This signature is not present in the router's memory. Unretiring a retired signature requires that the router recompile the signature database.
This can temporarily affect performance and take a long time with a large signature database.

QUESTION NO: 9

Which statement best describes inside policy based NAT?

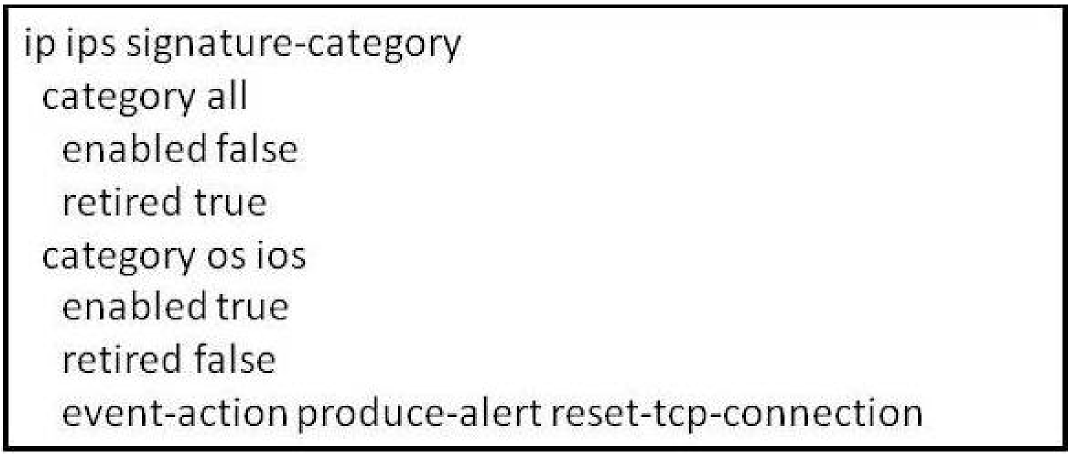
A. Policy NAT rules are those that determine which addresses need to be translated per the enterprise security policy
B. Policy NAT consists of policy rules based on outside sources attempting to communicate with inside endpoints.
C. These rules use source addresses as the decision for translation policies.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

Answer: A
Explanation:
The original dump had this option:

A) Policy NAT rules are those that determine which addresses need to be translated per the enterprise security policy
The newer dump did not so no sure the answer is still A)
http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/nat_overview.html#wp1088419

QUESTION NO: 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

Explanation:

This configuration task is completed by entering the signature category configuration mode using the ip ips signature-category command. See Example 13-3 for the relevant configuration. First, retire and disable all signatures because only the desired signatures will be enabled. This is achieved using the category all command. Then, use the retired true and enabled false commands to disable and retire all signatures by default. Next, enable all signatures that are designed to prevent attacks against Cisco IOS Software devices and assign a preventative action to them. Enter the category that comprises these signatures using the category os ios command and enable them by using the retired false and enabled true commands. Use the event-action produce-alert deny-packet-inline command to enable these signatures to generate an alert and drop the offending packets when they trigger.

QUESTION NO: 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
Explanation:
SDEE uses a pull communication model for event messages. This allows management consoles to pull alerts from the Cisco IPS sensors over an HTTPS connection.
When Cisco SDEE notification is enabled, by default, 200 events can be stored in the local event store. This number can be increased to hold a maximum of 1000. All stored events are lost if SDEE notifications are disabled, and a new local event store is allocated when the notification feature is enabled again.

QUESTION NO: 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
Explanation:

QUESTION NO: 13