Vendor: Cisco

Exam Code: 350-018

Exam Name: CCIE Security Written Exam v4.0

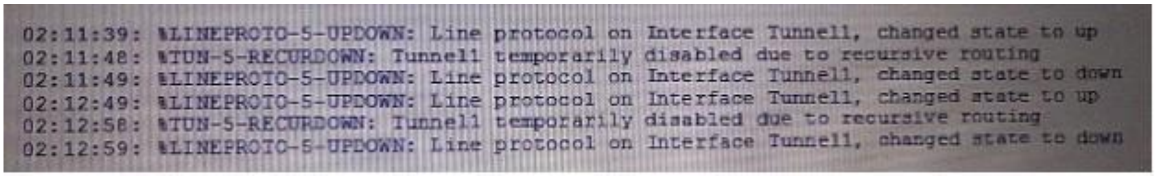
Version: Demo

QUESTION 1
Which two statements about attacks against IPV4 and IPv6 network are true? (Choose two)

A. Man-in-the-middle attacks are more common against IPv4 and IPv6
B. The multicast DHCPv6 replies on IPv6 network are easier to protect from attacks
C. Rogue devices provide more risk to IPv4 networks than IPv6 networks
D. It is easier to scan an IPv4 network than an IPv6 networks.
E. Data can be captured in transit across both network types.
F. Attacks performed at the application layer can compromise both types

Correct Answer: AF

QUESTION 2
Refer the exhibit. Two routers are connected using GRE through a WAN link. Your syslog server is logging the given error message. What is a possible reason for the errors?



```
02:11:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
02:11:48: %TUN-5-RECURDOWN: Tunnel1 temporarily disabled due to recursive routing
02:11:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
02:12:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
02:12:58: %TUN-5-RECURDOWN: Tunnel1 temporarily disabled due to recursive routing
02:12:59: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
```

A. The loopback interface is configured as the source of the tunnel
B. The connection is experiencing WAN link flapping
C. The tunnel key is misconfigured
D. Secondary addresses are being used on the physical interface
E. The tunnel source and destination are advertised through the tunnel itself

Correct Answer: E

QUESTION 3
What ASA feature can you use to restrict a user to a specific VPN group?

A. MPF
B. A Webtype ACL
C. group-lock
D. A VPN filter

Correct Answer: C

QUESTION 4
Which two statements about DNSSEC are true? (Choose two)

A. It support data confidentiality for DNS client
B. It can protect bulk data as is it transmitted between DNS servers.
C. It supports data integrity for DNS clients.
D. It supports spilt-horizon DNS to prevent attackers from enumerating the names in a zone
E. It can protect all types of data published in the DNS

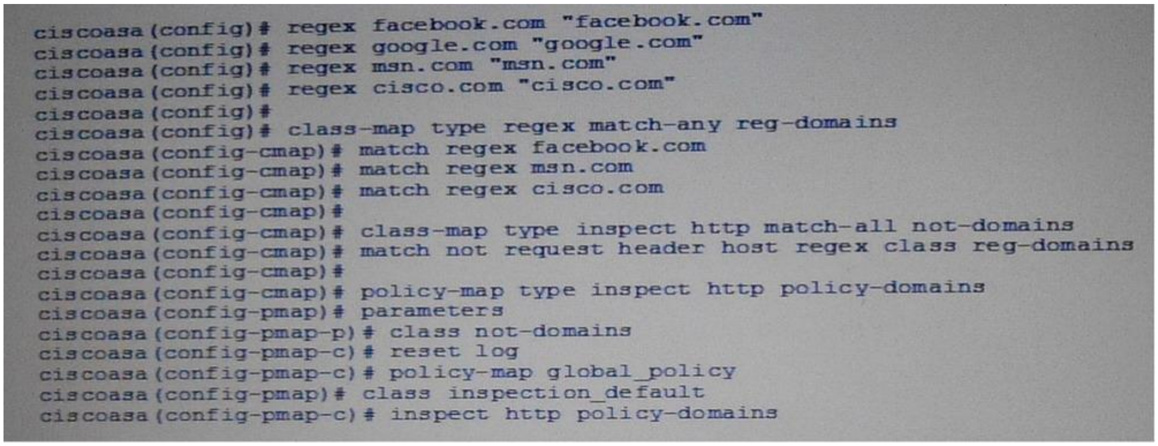
Correct Answer: CE

QUESTION 5
Which three statements about VRF-Aware Firewall are true? (Choose three)

A. It can run as more than one instance
B. It enables service providers to implement firewall on PE devices.
C. It can generate syslog message that are visible only to individual VPNs
D. It can support VPN network with overlapping address range without NAT
E. It supports both global and per-VRF commands and DoS parameters
F. It enables service providers to deploy firewall on customer device.

Correct Answer: ABC

QUESTION 6
Refer to the exhibit. What is the effect of the given service policy configuration?



```
ciscoasa(config)# regex facebook.com "facebook.com"
ciscoasa(config)# regex google.com "google.com"
ciscoasa(config)# regex msn.com "msn.com"
ciscoasa(config)# regex cisco.com "cisco.com"
ciscoasa(config)#
ciscoasa(config)# class-map type regex match-any reg-domains
ciscoasa(config-cmap)# match regex facebook.com
ciscoasa(config-cmap)# match regex msn.com
ciscoasa(config-cmap)# match regex cisco.com
ciscoasa(config-cmap)#
ciscoasa(config-cmap)# class-map type inspect http match-all not-domains
ciscoasa(config-cmap)# match not request header host regex class reg-domains
ciscoasa(config-cmap)#
ciscoasa(config-cmap)# policy-map type inspect http policy-domains
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# class not-domains
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http policy-domains
```

A. It blocks cisco.com, msn.com, and facebook.com and permits all other domains.
B. It blocks all domains except facebook.com, msn.com, cisco.com and google.com
C. It blocks all domains except cisco.com, msn.com, and facebook.com
D. It blocks facebook.com, msn.com, cisco.com and google.com, and permits all other domains

Correct Answer: B

QUESTION 7
What is an RFC 2827 recommendation for protecting your network against DoS attacks with IP address spoofing?

A. Advertise only assigned global IP addresses to the internet
B. Use ingress traffic filtering to limit traffic from a downstream network to known advertised prefixes.
C. Use the TLS protocol to secure the network against eavesdropping
D. Brower-based applications should be filtered on the source to protect your network from know advertised prefix

Correct Answer: B

QUESTION 8
Which two statements about the IPv6 OSPFv3 authentication Trailer are true (choose two)

A. The AT-bit resides in the OSPFv3 Header field
B. The IPv6 Payload length includes the length of the authentication Trailer
C. It Provide an alternative option to OSPFv3 IPsec authentication
D. The AT-bit must be set only in OSPFv3 Hello packets that include an Authentication Trailer
E. The AT-bit must be set only in OSPFv3 Database Description packets that include an Authentication Trailer
F. The OSPFv3 packet length includes the length of the Authentication Trailer

Correct Answer: DE

QUESTION 9
Which two statements about Cisco MQC are true? (Choose two)

A. It can classify Layer 2 Packets from legacy protocols
B. By default, its uses match-any matching
C. A packet can match only one traffic class within an individual traffic policy
D. It allows you to link multiple traffic policies to a single traffic class.
E. Unclassified traffic is queued in a FIFO queue to be managed by the match not command configuration
F. It can handle Layer2 packets from legacy protocol without classifying them.

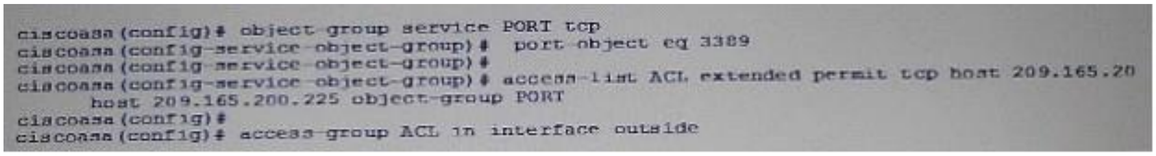
Correct Answer: EF

QUESTION 10
Which two statements about DNSSEC are true? (Choose two)

A. It support data confidentiality for DNS client
B. It can protect bulk data as is it transmitted between DNS servers.
C. It supports data integrity for DNS clients.
D. It supports spilt-horizon DNS to prevent attackers from enumerating the names in a zone
E. It can protect all types of data published in the DNS

Correct Answer: CE

QUESTION 11
Refer to the exhibit. Which two statements about the given configuration are true? (Choose two)



```
ciscoasa(config)# object-group service PORT tcp
ciscoasa(config-service-object-group)#  port-object eq 3389
ciscoasa(config-service-object-group)#
ciscoasa(config-service-object-group)# access-list ACL extended permit tcp host 209.165.20
      host 209.165.200.225 object-group PORT
ciscoasa(config)#
ciscoasa(config)# access-group ACL in interface outside
```

A. It will allow 202.165.200.225 to connect to 209.165.202.129 on a VNC port.
B. It will allow 209.165.202.129 to connect to 202.165.200.225 on a IMAP port
C. It will allow 209.165.202.129 to connect to 202.165.200.225 on a RDP port
D. It is an inbound policy

E. It is an outbound policy
F. It will allow 202.165.200.225 to connect to 209.165.202.129 on a RDP port

Correct Answer: CD

QUESTION 12
Which statement about ACS rule-based policies is true?

A. The permissions for rule-based policies are defined in authentication profile.
B. Permission for rule-bases polices are associated with user group.
C. Rule-based polices can apply different permission to the same user under different condition
D. TACACS+ is one of the attributes included in the authorization profile

Correct Answer: B

QUESTION 13
What are the three probes supported by Cisco ISE profiling services? (Choose three)

A. NetFlow (NetFlow Probe)
B. DHCP (DHCP Probe)
C. DHCP SPAN (DHCP SPAN Probe)
D. HTTP (HTTP Probe)
E. HTTP SPAN (HTTP SPAN Probe)
F. RADIUS (RADIUS Probe)
G. Network Scan (Network Scan Probe)
H. DNS (DNS Probe)
I. SNMP Query (SNMP Query Probe)
J. SNMP Trap (SNMP Trap Probe)

Correct Answer: ABD

QUESTION 14
Which two statements about Flexible Packet Matching are true? (Choose two)

A. It is supported by CSM management applications
B. It can classify traffic at the bit level
C. It can detected and filter malicious traffic
D. It provides stateful classification for Layer 2 to Layer 7 traffic
E. It can inspect non-IP protocol

Correct Answer: BC

QUESTION 15
Which three statements about Cisco Secure Desktop are true? (Choose three)

A. It is interpretable with Clientless SSL VPN, AnyConnect, and the IPSec VPN client.
B. Its supports shared network folder
C. It validate PKI certificates
D. It supports multiple prelogin checks, including IP address, certificate and OS

E. It supports unlimited CSD locations.
F. It can be pre-installed to reduce download time.

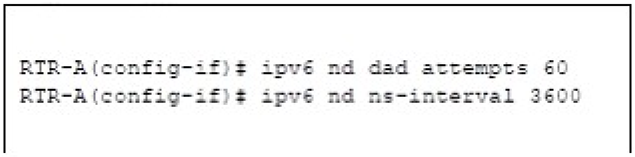
Correct Answer: BCE

QUESTION 16
What is an example of a stream cipher?

A. RC4
B. DES
C. Blowfish
D. RC6

Correct Answer: A

QUESTION 17
Refer to the exhibit. What is the effect of the given configuration?



```
RTR-A(config-if)# ipv6 nd dad attempts 60
RTR-A(config-if)# ipv6 nd ns-interval 3600
```

A. It sets the number of neighbor solicitation message to 60 and sets the retransmission interval to 3600 milliseconds
B. It sets the number of duplicate address detection attempts to 60 and sets the duplicate address detection interval to 3600 milliseconds
C. It sets the duplicate address detection interval to 60 seconds and sets the IPv6 neighbor solicitation interval to 3600 milliseconds
D. It sets the duplicate address detection interval 60 seconds and the IPv6 neighbor reachable time to 3600 milliseconds
E. It sets the number of neighbor solicitation message to 60 and sets the duplicate address detection interval to 3600 seconds

Correct Answer: C

QUESTION 18
Which two statements about router advertisement message are true? (Choose two)

A. Message are sent to the multicast address FF02::1
B. Local link prefixes are shared automatically
C. Flag settings are shared in the message and retransmitted on the link
D. Router solicitation message are sent in response to Router Advertisement message
E. It support a configurable number of retransmission attempt for neighbor solicitation message
F. Each prefix included in the advertisement carrier's lifetime information for that prefix

Correct Answer: BD

QUESTION 19
What is the most common use of Scavenger-Class QoS?

A. Mitigating DoS attacks
B. Mitigating SQL injection attacks
C. traffic shaping
D. prioritizing traffic

Correct Answer: A

QUESTION 20
Which statement about the Cisco AnyConnect web Security module is true?

A. It is VPN client software that works over the SSL protocol
B. It is deployment on endpoints to route HTTP traffic to ScanSafe
C. It is an endpoint component that is used with smart tunnels in a clientless SSL VPN
D. It operates as an NAC Agent when it is configured with AnyConnect VPN client

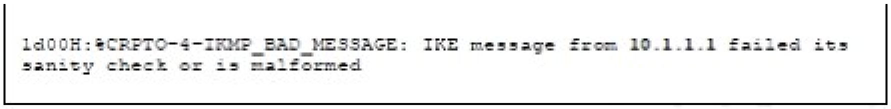
Correct Answer: B

QUESTION 21
Which three statements about Cisco IPS Manager Express are true? (Choose three)

A. It can provision policies based on Risk Ratings
B. It uses vulnerability-focused signature to protect against zero-day attacks
C. It can provision policies based on signatures
D. It can provision policies based on IP address and ports.
E. It provides a customizable view of event statistics
F. it support up to 10 sensors

Correct Answer: AEF

QUESTION 22
Refer to the exhibit. What is the meaning of the given error message?



```
1d00H:%CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 10.1.1.1 failed its
sanity check or is malformed
```

A. The PFS groups are mismatched
B. IKE is disabled on the remote peer
C. The mirrored crypto ACLs are mismatched.
D. The pre-shared keys are mismatched

Correct Answer: D