First Test, First Pass!

Vendor: Cisco

Exam Code: 351-018

Exam Name: CCIE Security Written Beta Exam v4.0

Version: DEMO

QUESTION 1
Which two options represent definitions that are found in the syslog protocol (RFC 5426)? (Choose two.)

A. Syslog message transport is reliable.
B. Each syslog datagram must contain only one message.
C. IPv6 syslog receivers must be able to receive datagrams of up to 1180 bytes.
D. Syslog messages must be prioritized with an IP precedence of 7.
E. Syslog servers must use NTP for the accurate time stamping of message arrival.

Answer: BC

QUESTION 2
According to RFC-5426, syslog senders must support sending syslog message datagrams to which port?

A. TCP port 514
B. UDP port 514
C. TCP port 69
D. UDP port 69
E. TCP port 161
F. UDP port 161

Answer: B

QUESTION 3
In an 802.11 wireless network, what would an attacker have to spoof to initiate a deauthentication attack against connected clients?

A. the BSSID of the AP where the clients are currently connected
B. the SSID of the wireless network
C. the MAC address of the target client machine
D. the broadcast address of the wireless network

Answer: A

QUESTION 4
What is the commonly known name for the process of generating and gathering initialization vectors, either passively or actively, for the purpose of determining the security key of a wireless network?

A. WEP cracking
B. session hijacking
C. man-in-the-middle attacks
D. disassociation flood frames

Answer: A

QUESTION 5

According to RFC 4890, which four ICMPv6 types are recommended to be allowed to transit a firewall? (Choose four.)

A. Type 1 - destination unreachable
B. Type 2 - packet too big
C. Type 3 - time exceeded
D. Type 0 - echo reply
E. Type 8 - echo request
F. Type 4 - parameter problem

Answer: ABCF

QUESTION 6
Which action is performed first on the Cisco ASA appliance when it receives an incoming packet on its outside interface?

A. check if the packet is permitted or denied by the inbound ACL applied to the outside interface
B. check if the packet is permitted or denied by the global ACL
C. check if the packet matches an existing connection in the connection table
D. check if the packet matches an inspection policy
E. check if the packet matches a NAT rule
F. check if the packet needs to be passed to the Cisco ASA AIP-SSM for inspections

Answer: C

QUESTION 7
If an incoming packet from the outside interface does not match an existing connection in the connection table, which action will the Cisco ASA appliance perform next?

A. drop the packet
B. check the outside interface inbound ACL to determine if the packet is permitted or denied
C. perform NAT operations on the packet if required
D. check the MPF policy to determine if the packet should be passed to the SSM
E. perform stateful packet inspection based on the MPF policy

Answer: B

QUESTION 8
When you are configuring QoS on the Cisco ASA appliance, which four are valid traffic selection criteria? (Choose four.)

A. VPN group
B. tunnel group
C. IP precedence
D. DSCP
E. default-inspection-traffic
F. qos-group

Answer: BCDE

QUESTION 9
Which command is required in order for the Botnet Traffic Filter on the Cisco ASA appliance to function properly?

A. dynamic-filter inspect tcp/80
B. dynamic-filter whitelist
C. inspect botnet
D. inspect dns dynamic-filter-snoop

Answer: D

QUESTION 10
You have been asked to configure a Cisco ASA appliance in multiple mode with these settings:

(A) You need two customer contexts, named contextA and contextB.
(B) Allocate interfaces G0/0 and G0/1 to contextA.
(C) Allocate interfaces G0/0 and G0/2 to contextB.
(D) The physical interface name for G0/1 within contextA should be "inside".
(E) All other context interfaces must be viewable via their physical interface names.

A.
```
context contextA
config-url disk0:/contextA.cfg
allocate-interface GigabitEthernet0/0 visible
allocate-interface GigabitEthernet0/1 inside
context contextB
config-url disk0:/contextB.cfg
allocate-interface GigabitEthernet0/0 visible
allocate-interface GigabitEthernet0/2 visible
```
B.
```
context contexta
config-url disk0:/contextA.cfg
allocate-interface GigabitEthernet0/0 visible
allocate-interface GigabitEthernet0/1 inside
context contextb
config-url disk0:/contextB.cfg
allocate-interface GigabitEthernet0/0 visible
allocate-interface GigabitEthernet0/2 visible
```
C.
```
context contextA
config-url disk0:/contextA.cfg
allocate-interface GigabitEthernet0/0 invisible
allocate-interface GigabitEthernet0/1 inside
context contextB
config-url disk0:/contextB.cfg
allocate-interface GigabitEthernet0/0 invisible
allocate-interface GigabitEthernet0/2 invisible
```
D.
```
context contextA
config-url disk0:/contextA.cfg
allocate-interface GigabitEthernet0/0
allocate-interface GigabitEthernet0/1 inside
context contextB
config-url disk0:/contextB.cfg
allocate-interface GigabitEthernet0/0
```

```
    allocate-interface GigabitEthernet0/2
E.  context contextA
    config-url disk0:/contextA.cfg
    allocate-interface GigabitEthernet0/0 visible
    allocate-interface GigabitEthernet0/1 inside
    context contextB
    config-url disk0:/contextB.cfg
    allocate-interface GigabitEthernet0/1 visible
    allocate-interface GigabitEthernet0/2 visible
```

Answer: A

QUESTION 11

Which four configuration steps are required to implement a zone-based policy firewall configuration on a Cisco IOS router? (Choose four.)

A. Create the security zones and security zone pairs.
B. Create the self zone.
C. Create the default global inspection policy.
D. Create the type inspect class maps and policy maps.
E. Assign a security level to each security zone.
F. Assign each router interface to a security zone.
G. Apply a type inspect policy map to each zone pair.

Answer: ADFG

QUESTION 12

Which Cisco IPS appliance signature engine defines events that occur in a related manner, within a sliding time interval, as components of a combined signature?

A. Service engine
B. Sweep engine
C. Multistring engine
D. Meta engine

Answer: D