



**Vendor:** Cisco

**Exam Code:** 350-018

**Exam Name:** CCIE Security Written Exam v4.1

**Version:** DEMO

### QUESTION 1

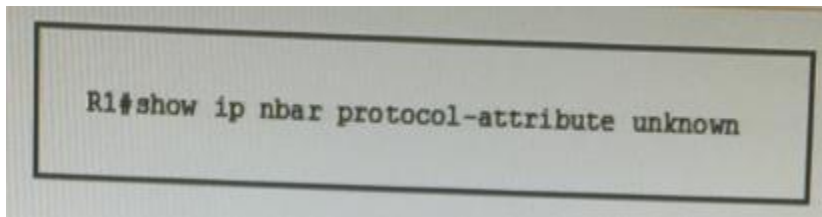
What protocol is responsible for issuing certificates?

- A. SCEP
- B. AH
- C. GET
- D. ESP
- E. DTLS

**Answer: A**

### QUESTION 2

Refer to the exhibit. Which statement about the effect of this command is true?



- A. It lists the current protocol-to-port mappings of NBAR.
- B. It lists traffic that is packet switched and bypassed by NBAR.
- C. It lists the number of packets processed for unknown and unclassified flows.
- D. It lists the attributes configured for unknown and unclassified flows.
- E. It displays the link age for unknown and unclassified flows.

**Answer: D**

### QUESTION 3

Which four of these attacks or wireless tools can the standard IDS signatures on a wireless LAN controller detect? (Choose four.)

- A. long HTTP request
- B. SYN flood
- C. Deauthorization flood
- D. NetStumbler
- E. Wellenreiter
- F. Association flood
- G. AirSnort
- H. Fragment Overlap attack

**Answer: CDEG**

### QUESTION 4

What Cisco IOS feature prevents an attacker from filling up the MTU cache for locally generated traffic when using path MTU discovery?

- A. Use NetFlow information to export data to a workstation.
- B. Force all traffic to send 1280-byte Packets by hard coding the MSS.
- C. Enable flow-label marking to track packet destination.
- D. Enable flow-label switching to track IPv6 packets in the MPLS cloud.
- E. Always use packets of 1500-byte size or larger.

**Answer: C**

#### QUESTION 5

What technology can you implement on your network to allow Independent applications to work with IPv6-capable applications?

- A. DS-Lite
- B. NAT-PT
- C. ISATAP
- D. NAT 6to4
- E. NAT64

**Answer: E**

#### QUESTION 6

Refer to the exhibit. What is the maximum number of hops from the device that generated the given output to its BGP neighbor at 4.4.4.4?

```
Router#show ip bgp neighbors 4.4.4.4
BGP neighbor is 4.4.4.4, remote AS 6504, external link
  BGP version 4, remote router ID 4.4.4.4
  BGP state = Established, up for 00:05:38
  Last read 00:00:38, last write 00:00:38, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

      Sent      Rcvd
  Opens:         1         1
  Notifications: 0         0
  Updates:       0         0
  Keepalives:    7         7
  Route Refresh: 0         0
  Total:         8         8
  Default minimum time between advertisement runs is 30 seconds

Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 252, Outgoing TTL 255
Local host: 3.3.3.3, Local port: 179
Foreign host: 4.4.4.4, Foreign port: 21122
Connection tableid (VRF): 0
```

- A. 3
- B. 252
- C. 5
- D. 255
- E. 2

F. 254

**Answer:** A

#### QUESTION 7

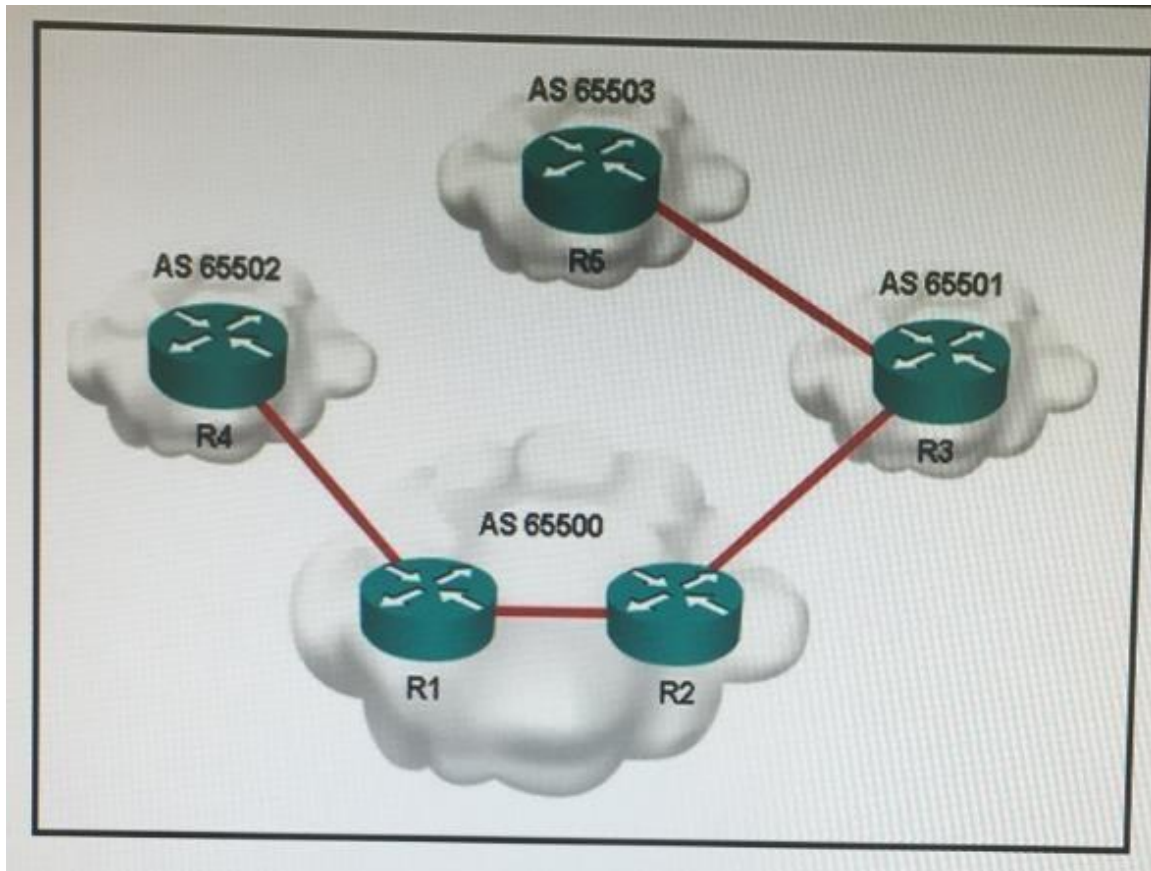
Which three of these statements about a zone-based policy firewall are correct? (Choose three.)

- A. An interface can be assigned to only one security zone.
- B. By default, all traffic to and from an interface that belongs to a security zone is dropped unless explicitly allowed in the zone-pair policy.
- C. Firewall policies, such as the pass, inspect, and drop actions, can only be applied between two zones.
- D. In order to pass traffic between two interfaces that belong to the same security zone, you must configure a pass action using class-default.
- E. Traffic cannot flow between a zone member interface and any interface that is not a zone member.

**Answer:** ACE

#### QUESTION 8

Refer to the exhibit. Which as-path access-list regular expression should be applied on R2 as a neighbor filter list to only allow updates with an origin of AS 65503?



- A. \_65503.?\$
- B. ^65503.\*
- C. 65503
- D. \_65503\_
- E. \_65503\$
- F. ^65503\$

**Answer: B**

#### QUESTION 9

If an ASA device is configured as a remote access IPsec server with RADIUS authentication and password management enabled, which type of authentication will it use?

- A. MS-CHAPV2
- B. MS-CHAPv1
- C. RSA
- D. NTLM
- E. PAP

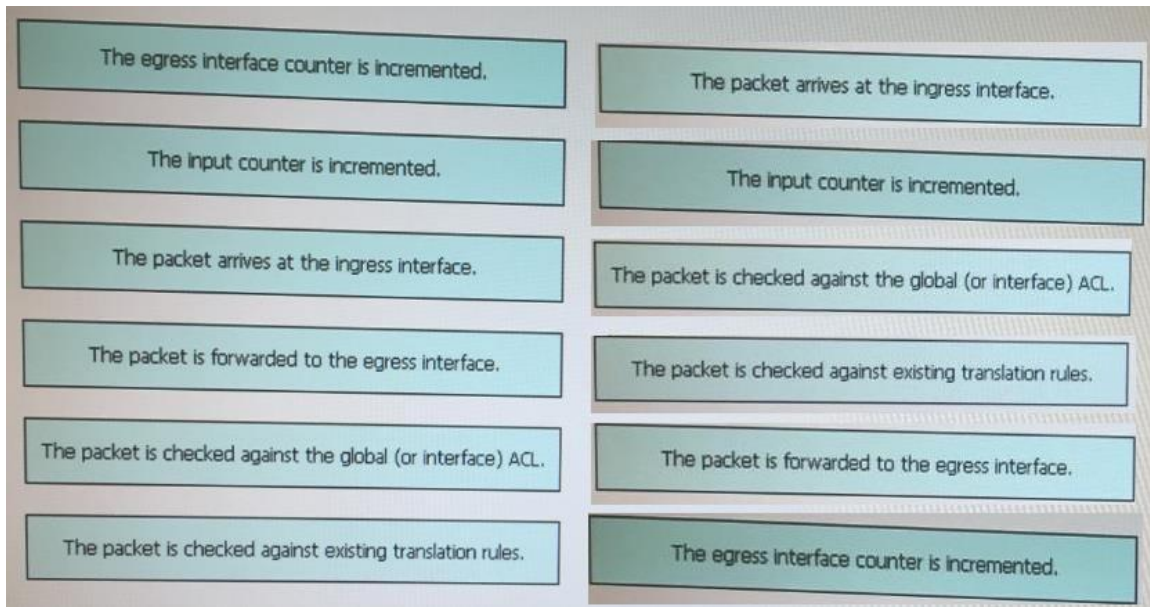
**Answer: E**

#### QUESTION 10

Drag and drop the step in the Cisco ASA packet processing flow on the left into the correct order of operations on the right.

The egress interface counter is incremented.	Step 1
The input counter is incremented.	Step 2
The packet arrives at the ingress interface.	Step 3
The packet is forwarded to the egress interface.	Step 4
The packet is checked against the global (or interface) ACL.	Step 5
The packet is checked against existing translation rules.	Step 6

**Answer:**



#### QUESTION 11

Which two statements about 802.1x authentication with port security are true? (Choose two.)

- A. If any client causes a security violation, the port is immediately placed in spanning-tree disabled mode.
- B. An entry is created in the secure host table for any client that is authenticated and manually configured for port security, even if the table is full.
- C. 802.1x manages network access for all authorized MAC addresses.
- D. If a client is authenticated and the port security table is full, the oldest client is aged out.
- E. If any host causes a security violation, the port is immediately error-disabled.

**Answer:** BE

#### QUESTION 12

Of which IPS application is Event Store a component?

- A. MainApp
- B. InterfaceApp
- C. AuthenticationApp
- D. NotificationApp
- E. SensorApp

**Answer:** A



## Thank You for Trying Our Product

### Braindump2go Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.braindump2go.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives<sup>®</sup>

**10% Discount Coupon Code: BDN2014**