

Exam : Cisco 350-018

**Title : CCIE Security Qualification
Exam**

Version : Demo

Important Note, Please Read Carefully

Other VisualExams products

[All visualexams IT Exam Products](#)

Our products of Offline Testing Engine

Use the offline Testing engine product to practice the questions in an exam environment.

Build a foundation of knowledge which will be useful also after passing the exam.

[visualexams Testing Engine](#)

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at VisualExams and update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to <http://www.visualexams.com/>
2. Log in the **User Center**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

Feedback

If you spot a possible improvement then please let us know. We always interested in improving product quality.

Feedback should be send to Visualexams@hotmail.com. You should include the following: Exam number, version, page number, question number, and your login Account.

Our experts will answer your mail promptly.

Explanations

This product does not include explanations at the moment. If you are interested in providing explanations for this exam, please contact Visualexams@hotmail.com.

Features

- Comprehensive questions with complete details
- Instant Downloadable in PDF form.
- Verified Answers Researched by Industry Experts
- Questions accompanied by exhibits.
- Drag and Drop questions as experienced in the Actual Exams.
- These questions and answers are backed by our GUARANTEE.
- Questions updated on regular basis.
- Like actual certification exams our product is in multiple-choice questions (MCQs)

Commitment to Your Success: At VisualTestExam.com, we are committed to your ongoing success. Our exams and questions are constantly being updated and compared to industry standards.

Want to earn a Microsoft certification like [MCSE](#), [MCSE 2003](#), [CCNA](#), [CCNP](#)? Thinking about getting an [A+](#) or [CCSP](#)?

A, [CCSP](#) or [Network+](#) Certification with less effort and time. You will be astonished at the theoretical and practical knowledge you will acquire in such a short period of time using our Certification Training Products. Our Study material will enable you to pass your [Microsoft](#), Your [Cisco](#) and any other certification on the very first attempt.

Guarantee

VisualExams provides the most competitive quality of all exams for the customers, we guarantee your success at the first attempt with only our Certification Question&Answers, if somehow you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

1. When initiating a new SSL/TLS session, the client receives the server SSL certificate and validates it. What does the client use the certificate for after validating it?

- A. The client and server use the key in the certificate to encrypt all data in the following SSL session.
- B. The server creates a separate session key and sends it to the client. The client has to decrypt the session key using the server public key from the certificate.
- C. The client creates a separate session key and encrypts it with the server public key from the certificate before sending it to the server.
- D. Nothing, the client and server switch to symmetric encryption using IKE to exchange keys.
- E. The client generates a random string, encrypts it with the server public key from the certificate, and sends it to the server. Both the client and server derive the session key from the random data sent by the client.

Answer: E

2. Which three of these statements describe how DNSSEC prevents DNS cache poisoning attacks from succeeding? (Choose three.)

- A. DNSSEC encrypts all records with domain-specific keys.
- B. DNSSEC eliminates caching and forces all answers to be authoritative.
- C. DNSSEC introduces KEY records that hold domain-specific public keys.
- D. DNSSEC deprecates CNAME records and replaces them with DS records.
- E. DNSSEC utilizes DS records to establish a trusted hierarchy of zones.
- F. DNSSEC signs all records with domain-specific keys.

Answer: CEF

3. Which two of the following statements describe why TACACS+ is more desirable from a security standpoint than RADIUS? (Choose two.)

- A. It uses UDP as its transport.
- B. It uses TCP as its transport.
- C. It encrypts the password field with a unique key between server and requester.
- D. Encrypting the whole data payload is optional.
- E. Authentication and authorization are combined into a single query for robustness.

Answer: BD

4. When using Cisco SDM to manage a Cisco IOS device, what configuration statements are necessary to be able to use Cisco SDM?

- A. ip http server
- B. ip http secure-server
- C. ip http server
sdm location X.X.X.X
- D. ip http secure-server
sdm location X.X.X.X
- E. ip http server
ip http secure-server

Answer: A

5. In regards to private address space, which three of the following statements are true? (Choose three.)

- A. Private address space is defined in RFC 1918.
- B. These IP addresses are considered private:
10.0.0.0
172.15.0.0
192.168.0.0
- C. Private address space is not supposed to be routed over the Internet.
- D. 127.0.0.1 is also considered part of private address space, according to the RFC.
- E. Using only private address space and NAT to the Internet is not considered as secure as having a stateful firewall.

Answer: ACE

6. A firewall administrator received this syslog message from his adaptive security appliance. What can the firewall administrator infer from the message?

| %ASA-6-201010: Embryonic connection limit exceeded 200/200 for inbound packet from 209.165.201.10/1026 to 10.1.1.20/80 on interface outside

- A. The server at 209.165.201.10 is under a smurf attack.

- B. The server at 10.1.1.20 is under a SYN attack.
- C. The client at 209.165.201.10 has been infected with a virus.
- D. The server at 10.1.1.20 is under a smurf attack.

Answer: B

7. Which two of the following statements are attributed to stateless filtering? (Choose two.)

- A. The first TCP packet in a flow must be a SYN packet.
- B. It must process every packet against the inbound ACL filter.
- C. It can look at sequence numbers to validate packets in flow.
- D. It must implement an idle timeout.
- E. It can be used in asymmetrical traffic flows.

Answer: BE

8. Which three of the following are attributes of the RADIUS protocol? (Choose three.)

- A. encrypts the password
- B. hashes the password
- C. uses UDP as the transport
- D. uses TCP as the transport
- E. combines authentication and authorization in a single request
- F. commonly used to implement command authorization

Answer: BCE

9. Which two of the following commands are required to implement a Cisco Catalyst 6500 Series FWSM?
(Choose two.)

- A. firewall multiple-vlan-interfaces
- B. firewall module x vlan-group y
- C. module x secure-traffic
- D. firewall vlan-group
- E. firewall module x secure-traffic

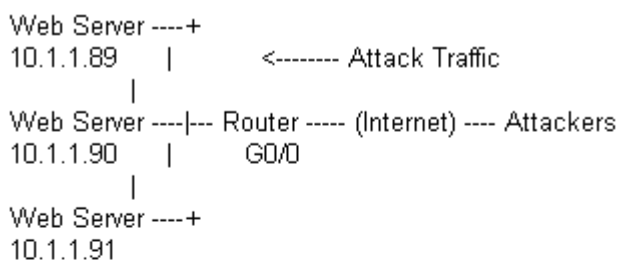
Answer: BD

10. If an administrator is unable to connect to a Cisco ASA or PIX security appliance via Cisco ASDM, which four of the following items should be checked? (Choose four.)

- A. The HTTPS server is enabled.
- B. The HTTP server is enabled.
- C. The user IP address is permitted in the interface ACL.
- D. The user IP address is permitted in the HTTP statement.
- E. The ASDM file resides in flash memory.
- F. The asdm image command exists in the configuration.

Answer: BDEF

11. Refer to the shown network diagram and configuration. You are hosting a web server at 10.1.1.90, which is under a denial of service attack. Use NBAR to limit web traffic to that server at 200 kb/s. Which of the following configurations is correct to complete the NBAR configuration?



```

class-map match-all DoS
match access-group 188
!
!
interface GigabitEthernet0/0
description Connection to ISP Router
ip address 192.168.1.1 255.255.255.0
service-policy input DoS-Attack
ip route-cache flow
load-interval 30
  
```

A.

```

policy-map drop
class DoS
police conform-action transmit exceed-action drop
  
```

B.

```
policy-map drop
  class DoS
    police cir 200000 bc 37500 be 75000
    conform-action transmit
    exceed-action drop
    violate-action drop
  !
access-list 188 permit tcp any host 10.1.1.90 eq www
```

C.

```
policy-map DoS-Attack
  class DoS
    police cir 200 bc 200 be 200
    conform-action transmit
    exceed-action drop
    violate-action drop
  !
access-list 188 permit tcp any host 10.1.1.90 eq www
```

D.

```
policy-map DoS-Attack
  class DoS
    police cir 200000 bc 37500 be 75000
    conform-action transmit
    exceed-action drop
    violate-action drop
  !
access-list 188 permit tcp any host 10.1.1.90 eq www
```

E.

```
policy-map DoS-Attack
  class drop
    police 200000 37500 75000 conform-action transmit exceed-action drop
  !
access-list 188 permit tcp any host 10.1.1.90 eq www
```

Answer: D

12. When designing the addressing scheme of the internal routers at a company, many security professionals choose to use RFC 1918 addresses. Which three of the following addresses are RFC 1918 addresses? (Choose three.)

- A. 0.0.0.0/8
- B. 10.0.0.0/8
- C. 172.16.0.0/12
- D. 172.16.0.0/16
- E. 192.168.0.0/16
- F. 192.168.0.0/24

Answer: BCE

13. How do TCP SYN attacks take advantage of TCP to prevent new connections from being established to a host under attack?

- A. sending multiple FIN segments, forcing TCP connection release
- B. filling up a host listen queue by failing to ACK partially opened TCP connections
- C. taking advantage of the host transmit backoff algorithm by sending jam signals to the host
- D. incrementing the ISN of each segment by a random number, causing constant TCP retransmissions
- E. sending TCP RST segments in response to connection SYN+ACK segments, forcing SYN retransmissions

Answer: B

14. What are two key characteristics of VTP? (Choose two.)

- A. VTP messages are sent out all switch-switch connections.
- B. VTP Layer 2 messages are communicated to neighbors using CDP.
- C. VTP manages addition, deletion, and renaming of VLANs 1 to 4094.
- D. VTP pruning restricts flooded traffic, increasing available bandwidth.
- E. VTPv2 can only be used in a domain consisting of VTPv2-capable switches.
- F. VTPv2 performs consistency checks on all sources of VLAN information.

Answer: DE

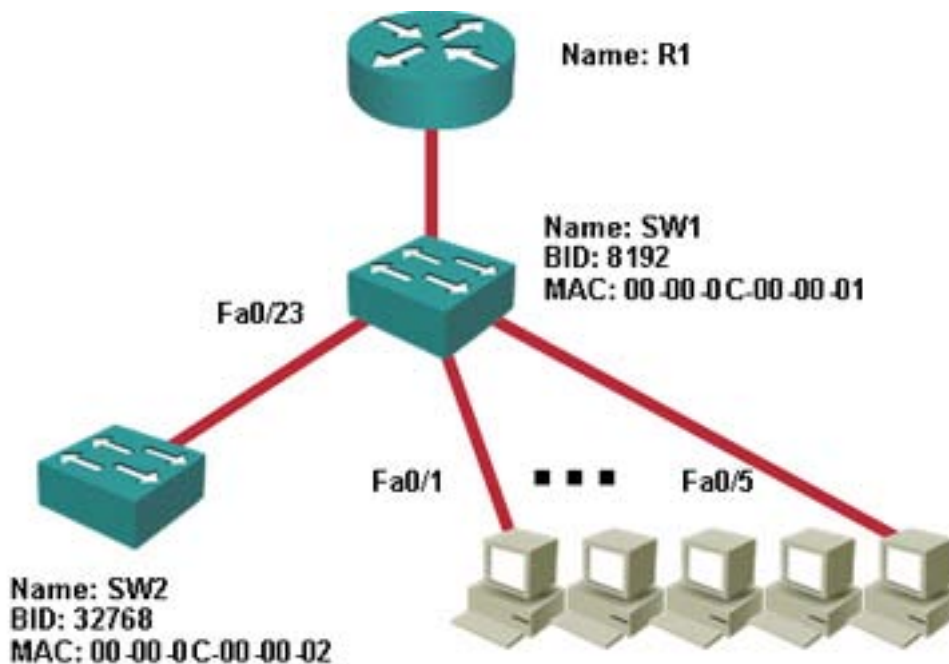
15. What are two important guidelines to follow when implementing VTP? (Choose two.)

- A. CDP must be enabled on all switches in the VTP management domain.
- B. All switches in the VTP domain must run the same version of VTP.
- C. When using secure-mode VTP, configure management domain passwords only on VTP servers.
- D. Enabling VTP pruning on a server will enable the feature for the entire management domain.
- E. Use of the VTP multidomain feature should be restricted to migration and temporary implementation.

Answer: BD

16. Refer to the exhibit. Switch SW2 has just been added to Fa0/23 on SW1. After a few seconds, interface

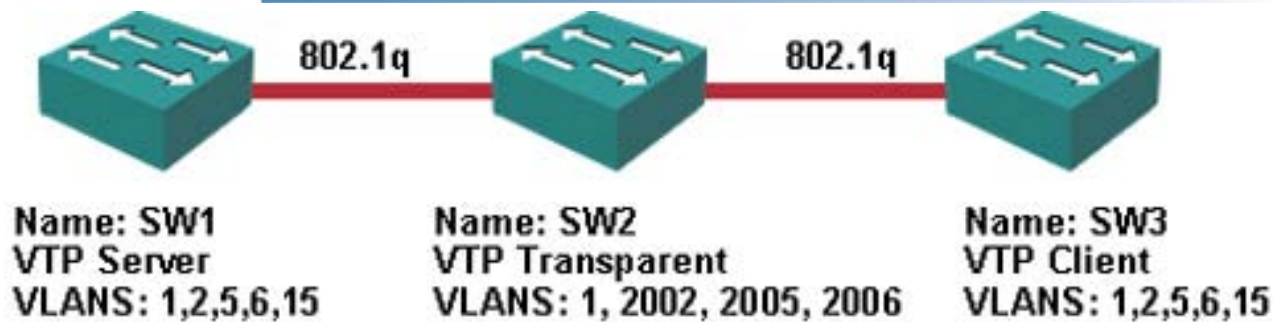
Fa0/23 on SW1 is placed in the error-disabled state. SW2 is removed from port 0/23 and inserted into SW1 port Fa0/22 with the same result. What is the most likely cause of this problem?



- A. The spanning-tree PortFast feature has been configured on SW1.
- B. BPDU filtering has been enabled either globally or on the interfaces of SW1.
- C. The BPDU guard feature has been enabled on the Fast Ethernet interfaces of SW1.
- D. The Fast Ethernet interfaces of SW1 are unable to autonegotiate speed and duplex with SW2.
- E. PAgP is unable to correctly negotiate VLAN trunk characteristics on the link between SW1 and SW2.

Answer: C

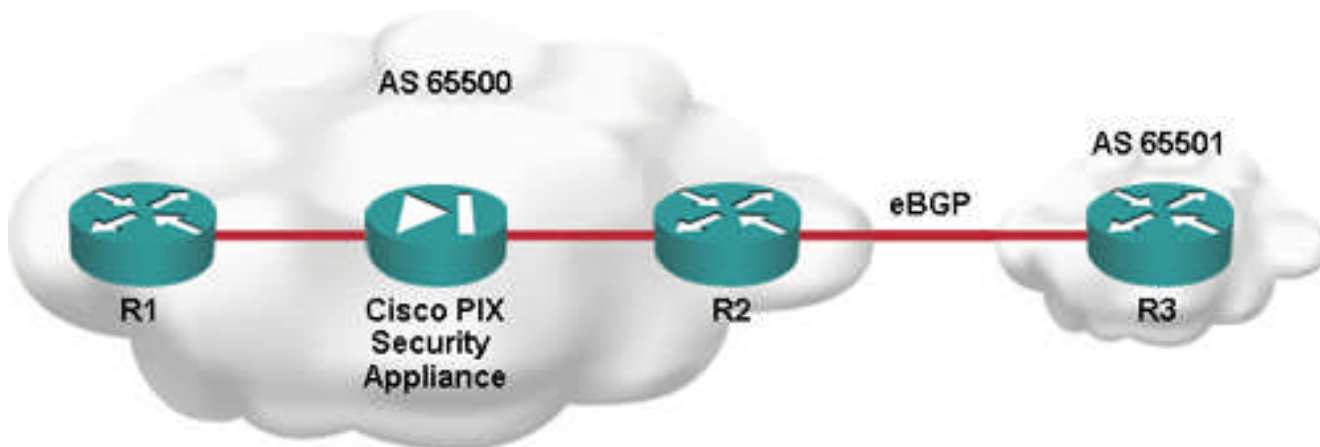
17. Refer to the exhibit. The Cisco IOS Software-based switches are configured with VTP and VLANs as shown. The network administrator wants to quickly add the VLANs defined on SW1 to the configuration of SW2. Therefore, the administrator copies the vlan.dat file from the flash memory on SW1 to the flash memory of SW2. After the file is copied to SW2, it is rebooted. What is the VLAN status of SW2 after the reboot?



- A. The VLAN information on SW2 will remain the same because it has been configured for transparent VTP mode.
- B. SW2 will clear the vlan.dat file and load its VLAN information from the configuration file stored in NVRAM.
- C. A VTP mode mismatch will occur, causing the VLANs in the startup configuration to be ignored and all VLANs above 1005 to be erased.
- D. The VLANs in the vlan.dat file will be copied to the running configuration and merged with the extended VLANs defined in the startup configuration.
- E. All VLANs will be erased and all ports will be moved into the default VLAN 1.

Answer: C

18. Refer to the exhibit. A Cisco security appliance has been inserted between routers R1 and R2 to enhance security and apply advanced protocol inspection. Unfortunately, BGP stopped working after the appliance was inserted in the network. Which three of these configuration tasks must be completed to restore BGP connectivity? (Choose three.)

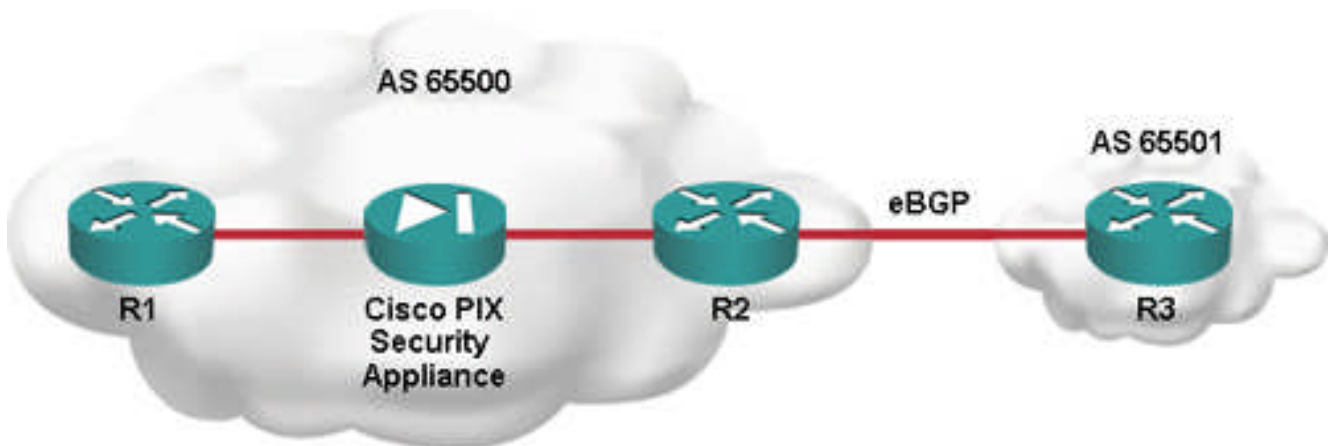


- A. Configure BGP on the security appliance as an IBGP peer to R1 and R2 in AS 65500.
- B. Configure a static NAT translation to allow inbound TCP connections from R2 to R1.
- C. Configure an ACL on the security appliance allowing TCP port 179 between R1 and R2.

- D. Configure a static route on R1 and R2 using the appliance inside and outside interfaces as gateways.
- E. Configure the BGP fixup feature on the security appliance to permit BGP TCP connections between R1 and R2.

Answer: BCD

19. Refer to the exhibit. A Cisco security appliance has been correctly configured and inserted between routers R1 and R2. The security appliance allows IBGP connectivity between R1 and R2 and BGP is fully functional. To increase security, MD5 neighbor authentication is correctly configured on R1 and R2. Unfortunately, BGP stops working after the MD5 configuration is added. Which configuration task must be completed on the security appliance to restore BGP connectivity?



- A. Configure authentication proxy on the security appliance.
- B. Configure the MD5 authentication key on the security appliance.
- C. Add the MD5 key to the security appliance BGP fixup configuration.
- D. Add norandomseq to the static NAT translation on the security appliance.
- E. Configure a GRE tunnel to allow authenticated BGP connections to traverse the security appliance.

Answer: D

20. According to RFC 3180, what is the correct GLOP address for AS 456?

- A. 224.0.4.86
- B. 224.4.86.0
- C. 233.1.200.0
- D. 239.2.213.0
- E. 239.4.5.6

Answer: C

Visualexams.com was founded in 2006. The safer,easier way to help you pass any IT Certification exams . We provide high quality IT Certification exams practice questions and answers(Q&A). Especially Adobe, Apple, Citrix, Comptia, EMC, HP, HuaWei, LPI, Nortel, Oracle, SUN, Vmware and so on. And help you pass any IT Certification exams at the first try.

Web site: <http://www.visualexams.com>

You can reach us at any of the email addresses listed below.

E-Mail: [visualexams \(at\) hotmail.Com](mailto:visualexams@hotmail.com)