

Exam4Test 350-018 Exams

Cisco CCIE Pre-Qualification Test for Security



Practice Exam: 350-018

Exam Number/Code: 350-018

Exam Name: CCIE Pre-Qualification Test for Security

Questions and Answers: 199 Q&As

Exam Description

Order : [350-018 Exam](#)

1. Exam4Test offer free update service for three month.

After you purchase our product, we will offer free update in time for three month.

2. High quality and Value for the 350-018 Exam.

Exam4Test **Practice Exams** for 350-018 are written to the highest standards of technical accuracy, provided by our certified subject matter experts and published authors for development.

3. 100% Guarantee to Pass Your **CCIE** exam and get your **CCIE Certification**.

We guarantee your success in the first attempt. If you do not pass the **CCIE** "350-018" (CCIE Pre-Qualification Test for Security) on your first attempt, send us the official result. We will give you a FULLY REFUND of your purchasing fee and send you another same value product for free.

4. Exam4Test CCIE 350-018 Exam Downloadable.

Our PDF or Testing Engine Preparation Material of CCIE 350-018 exam provides everything which you need to pass your exam. The CCIE Certification details are researched and produced by our Professional Certification Experts who are constantly using industry experience to produce precise, and logical. You may get "350-018 exam" questions from different websites or books, but logic is the key. Our Product will help you not only pass in the first CCIE Pre-Qualification Test for Security(CCIE) exam try, but also save your valuable time.

Comprehensive questions with complete details about 350-018 exam.

350-018 exam questions accompanied by exhibits. Verified Answers Researched by Industry Experts and almost 100% correct.

Drag and Drop questions as experienced in the Real CCIE exam. 350-018 exam questions updated on regular basis. Like actual CCIE Certification exams, 350-018 exam preparation is in multiple-choice questions (MCQs). Tested by many real CCIE exams before publishing.

Try free CCIE exam demo before you decide to buy it in <http://www.Exam4Test.com>

High quality and Valued for the 350-018 Exam: 100% Guarantee to Pass Your 350-018 exam and get your CCIE Certification. Come to <http://www.Exam4Test.com> The easiest and quickest way to get your CCIE Certification.

Exam4Test professional provides CCIE 350-018 the newest Q&A, completely covers 350-018 test original topic. With our completed CCIE resources, you will minimize your CCIE cost and be ready to pass your 350-018 test on Your First Try, 100% Money Back Guarantee included!

350-018 Exam Study Guide

350-018 exam is regarded as one of the most favourite [CCIE Certifications](#). Many IT professionals prefer to add 350-018 exam among their credentials. Exam4Test not only caters you all the information regarding the 350-018 exam but also provides you the excellent 350-018 study guide which makes the certification exam easy for you.

Exam4Test Engine Features

Comprehensive questions and answers about 350-018 exam

350-018 exam questions accompanied by exhibits

Verified Answers Researched by Industry Experts and almost 100% correct

350-018 exam questions updated on regular basis

Same type as the certification exams, 350-018 exam preparation is in multiple-choice questions (MCQs).

Tested by multiple times before publishing

Try free 350-018 exam demo before you decide to buy it in Exam4Test.com

Exam4Test Help You Pass Any IT Exam

[Exam4Test.com](#) offers incredible career enhancing opportunities. We are a team of IT professionals that focus on providing our customers with the most up to date material for any IT certification exam. This material is so effective that we Guarantee you will pass the exam or your money back.

Exam : Cisco 350-018

Title : CCIE Security Qualification Exam

1. 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

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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

8. 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

9. 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?

- A.
- B.
- C.
- D.
- E.

Answer: D

10. 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

11. 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

12. 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

13. 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

14. 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

15. 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

16. 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

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

- 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

19. 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

20. 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

[More 350-018 Information](#)

Related 350-018 Exams

[350-001](#) CCIE Cisco Certified Internetworking Expert

[350-018](#) CCIE Pre-Qualification Test for Security

[350-001-LAB](#) CCIE-ROUTING AND SWITCHING QUALIFICATION (Lab exam)

[350-029](#) CCIE SP Written Exam

[351-001](#) CCIE Routing and Switching Written 3.0 Beta

[350-030](#) CCIE Voice Written

[350-018-LAB](#) CCIE Pre-Qualification Test for Security (Lab exam)

[350-040](#) CCIE Storage Networking

[350-050](#) CCIE Wireless Beta Written Exam

[350-020](#) CCIE SP Optical Qualification Exam

[350-022](#) CCIE Written, Service Provider: DSL

[350-027](#) CCIE Written: Metro Ethernet

[350-025](#) CCIE Service Provider Dial

[350-024](#) CCIE SP IP Telephony Qualification Exam

[350-021](#) CCIE SP Cable Qualification Exam

[351-018](#) Security 3.0 Beta

[350-023](#) CCIE Written: WAN Switching

[350-026](#) CCIE SP Content Networking ENU

[350-001GB2312-LAB](#) CCIE-Routing and Switching Written exam

Other Cisco Exams

[646-361](#) [640-801](#) [642-456](#) [352-001](#) [646-574](#) [646-230](#) [350-029](#) [642-444](#)

[642-504](#) [646-411](#) [350-001](#) [642-357](#) [350-021](#) [642-105](#) [646-222](#) [640-822](#)

[642-274](#) [640-553](#) [642-979](#) [642-091](#)