

CompTIA


# Security+

SY0-301 SY0-301 SY0-301 SY0-301 SY0-301 SY0-301 SY0-301

PRINTABLES

## PRINTABLE PRACTICE QUESTIONS

QUESTIONS, ANSWERS, AND  
DETAILED EXPLANATIONS IN AN  
EASY-TO-USE PRINTABLE FORMAT

 LearnSmart™

## Chapter 1

# Network Security

1. Why are web security gateways an important part of the enterprise security landscape? Select the best answer.
- A. They prevent users from successful privilege escalations.
  - B. They prevent cross-site scripting and SQL injection attacks.
  - C. They block malicious URLs, spyware, botnets, and viruses.
  - D. They prevent social engineering attacks.

[Find the Answer](#) p. 131

2. What is the purpose of using a VPN concentrator on a large scale corporate network? Select the best answer.
- A. To establish a business continuity mechanism that supports corporate policy.
  - B. To establish a secure central chokepoint through which IPSec and/or SSL traffic may pass.
  - C. To establish a failover platform that supports disaster recovery objectives.
  - D. To establish an audit trail used to correlate events for criminal investigations.

[Find the Answer](#) p. 131

3. How do network administrators intercept, interpret, and analyze traffic at the packet level? Select the best answer.
- A. System logs.
  - B. Port scanner.
  - C. Vulnerability scanner.
  - D. Network sniffer.

[Find the Answer](#) p. 131



4. How can organizations stop unsolicited email from reaching end-users? Select the best answer.
- A. Through various Bayesian spam filters that analyze and trap suspicious content.
  - B. Port scanner.
  - C. Network sniffer.
  - D. Vulnerability scanner.

[Find the Answer](#) p. 131

5. What is the purpose of an application firewall? Select the best answer.
- A. To establish a failover platform that supports disaster recovery objectives.
  - B. To establish a secure central chokepoint through which IPSec and/or SSL traffic may pass.
  - C. To control access and input/output between specific applications or services.
  - D. To establish an audit trail used to correlate events for criminal investigations.

[Find the Answer](#) p. 131

6. How is a network firewall different from an application firewall? Select the best answer.
- A. It monitors specific application or service traffic.
  - B. It establishes a secure central chokepoint through which IPSec and/or SSL traffic may pass.
  - C. It analyzes connection states and client-server or client-client relationships to identify legitimate and illegitimate traffic patterns.
  - D. To establish a failover platform that supports disaster recovery objectives.

[Find the Answer](#) p. 131



## Answers: Chapter 1

1. <b>C</b>	<a href="#">Review Question</a> p. 2	<a href="#">Detailed Explanation</a> p. 151
2. <b>B</b>	<a href="#">Review Question</a> p. 2	<a href="#">Detailed Explanation</a> p. 151
3. <b>D</b>	<a href="#">Review Question</a> p. 2	<a href="#">Detailed Explanation</a> p. 151
4. <b>A</b>	<a href="#">Review Question</a> p. 3	<a href="#">Detailed Explanation</a> p. 152
5. <b>C</b>	<a href="#">Review Question</a> p. 3	<a href="#">Detailed Explanation</a> p. 152
6. <b>C</b>	<a href="#">Review Question</a> p. 3	<a href="#">Detailed Explanation</a> p. 153
7. <b>B</b>	<a href="#">Review Question</a> p. 4	<a href="#">Detailed Explanation</a> p. 153
8. <b>C</b>	<a href="#">Review Question</a> p. 4	<a href="#">Detailed Explanation</a> p. 154
9. <b>A, D</b>	<a href="#">Review Question</a> p. 5	<a href="#">Detailed Explanation</a> p. 154
10. <b>B</b>	<a href="#">Review Question</a> p. 5	<a href="#">Detailed Explanation</a> p. 154
11. <b>A</b>	<a href="#">Review Question</a> p. 6	<a href="#">Detailed Explanation</a> p. 155
12. <b>A</b>	<a href="#">Review Question</a> p. 6	<a href="#">Detailed Explanation</a> p. 155
13. <b>A, B</b>	<a href="#">Review Question</a> p. 6	<a href="#">Detailed Explanation</a> p. 156
14. <b>A</b>	<a href="#">Review Question</a> p. 7	<a href="#">Detailed Explanation</a> p. 156
15. <b>A, D</b>	<a href="#">Review Question</a> p. 7	<a href="#">Detailed Explanation</a> p. 156
16. <b>A</b>	<a href="#">Review Question</a> p. 7	<a href="#">Detailed Explanation</a> p. 157
17. <b>B</b>	<a href="#">Review Question</a> p. 8	<a href="#">Detailed Explanation</a> p. 157
18. <b>C</b>	<a href="#">Review Question</a> p. 8	<a href="#">Detailed Explanation</a> p. 158
19. <b>D</b>	<a href="#">Review Question</a> p. 8	<a href="#">Detailed Explanation</a> p. 158
20. <b>B, C</b>	<a href="#">Review Question</a> p. 9	<a href="#">Detailed Explanation</a> p. 158
21. <b>A</b>	<a href="#">Review Question</a> p. 9	<a href="#">Detailed Explanation</a> p. 159
22. <b>D</b>	<a href="#">Review Question</a> p. 9	<a href="#">Detailed Explanation</a> p. 159
23. <b>B, C</b>	<a href="#">Review Question</a> p. 10	<a href="#">Detailed Explanation</a> p. 160

## Explanations: Chapter 1

1. [Review Question](#) p. 2

**Answers: C**

**Explanation A.** Incorrect. Privilege escalation prevention typically occurs on individual systems, not as part of the intermediate gateway filtering process.

**Explanation B.** Incorrect. Cross-Site Scripting (XSS) and SQL Injections (SQLi) are typically handled through secure coding practices at the application layer, rather than through a network gateway.

**Explanation C.** Correct. A web security gateway complements antivirus solutions by providing advanced features such as reputation analysis, browser code scanning, data fingerprinting, and content classification.

**Explanation D.** Incorrect. Social engineering attempts to deceive users into revealing confidential or sensitive information, an attack that cannot be prevented by gateway devices.

PrepLogic Question: [13085-1000](#)

2. [Review Question](#) p. 2

**Answers: B**

**Explanation A.** Incorrect. Business continuity practices and processes ensure continued operations in the event of disruption or interruption to business operations.

**Explanation B.** Correct. As the name implies, a VPN concentrator centralizes traffic to a specific point on the network for tighter control, monitoring, and security enforcement.

**Explanation C.** Incorrect. Disaster recovery planning and procedures establish a fallback plan in the event of catastrophic disaster that destroys critical business operations.

**Explanation D.** Incorrect. System and network logs directly support audit trails that help correlate events for the investigation of criminal computer activity.

PrepLogic Question: [13085-1001](#)

3. [Review Question](#) p. 2

**Answers: D**



**Explanation A.** Incorrect. System logs provide audit trails that support troubleshooting and investigation of system-related events.

**Explanation B.** Incorrect. A port scanner provides network service enumeration so that analysts can inventory which systems run what services.

**Explanation C.** Incorrect. A vulnerability scanner enumerates service banners so that analysts can identify which systems are susceptible to known attacks and aren't updated to the most current patch or version levels.

**Explanation D.** Correct. A network sniffer can capture and monitor network transmissions to provide insight into network-related activities.

PrepLogic Question: [13085-1002](#)

4. [Review Question](#) p. 3

**Answers: A**

**Explanation A.** Correct. Bayesian spam filters use classifiers and statistics to identify and quarantine suspicious email patterns that associate with spam.

**Explanation B.** Incorrect. A port scanner provides network service enumeration so that analysts can inventory which systems run what services.

**Explanation C.** Incorrect. A network sniffer can capture and monitor network transmissions to provide insight into network-related activities.

**Explanation D.** Incorrect. A vulnerability scanner enumerates service banners so that analysts can identify which systems are susceptible to known attacks and aren't updated to the most current patch or version levels.

PrepLogic Question: [13085-1003](#)

5. [Review Question](#) p. 3

**Answers: C**

**Explanation A.** Incorrect. Disaster recovery planning and procedures establish a fallback plan in the event of catastrophic disaster that destroys critical business operations.

**Explanation B.** Incorrect. A VPN concentrator centralizes IPsec and SSL traffic to a specific point on the network for tighter control, monitoring, and security enforcement.

**Explanation C.** Correct. An application firewall controls input, output, and access to or



from network applications and services (at OSI layer 7).

**Explanation D.** Incorrect. System and network logs directly support audit trails that help correlate events for the investigation of criminal computer activity.

PrepLogic Question: [13085-1004](#)

6. [Review Question](#) p. 3

**Answers: C**

**Explanation A.** Incorrect. An application firewall specifically focuses on application or service traffic sent to or from a host.

**Explanation B.** Incorrect. A VPN concentrator centralizes IPsec and SSL traffic to a specific point on the network for tighter control, monitoring, and security enforcement.

**Explanation C.** Correct. Network firewalls are "big picture" oriented in that they monitor and maintain relationships between endpoints across the network.

**Explanation D.** Incorrect. Disaster recovery planning and procedures establish a fallback plan in the event of catastrophic disaster that destroys critical business operations.

PrepLogic Question: [13085-1005](#)

7. [Review Question](#) p. 4

**Answers: B**

**Explanation A.** Incorrect. Network firewalls selectively pass or block traffic from entering or exiting the network based on predefined rules.

**Explanation B.** Correct. Content filtering concentrates on content; it can filter out unwanted traffic based on the nature of messages or messages sourced from known-bad hosts.

**Explanation C.** Incorrect. A host-based intrusion prevention system is suitable for preventing end-users from running unwanted applications on a system.

**Explanation D.** Incorrect. A network-based intrusion prevention system uses signatures and heuristics to analyze application protocol traffic for anomalous or abusive patterns.

PrepLogic Question: [13085-1006](#)

