

CertsChief

Guaranteed Success with Accurate & Updated Questions.

Comptia

*SY0-601
CompTIA Security+ Exam 2021*

Questions & Answers PDF

For More Information - Visit:
<https://www.certschief.com/>

Product Full Version Features:

- ✓ 90 Days Free Updates
- ✓ 30 Days Money Back Guarantee
- ✓ Instant Download Once Purchased
- ✓ 24/7 Online Chat Support

Latest Version: 16.0

Question: 1

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

INSTRUCTIONS

Click on each firewall to do the following:

Deny cleartext web traffic.

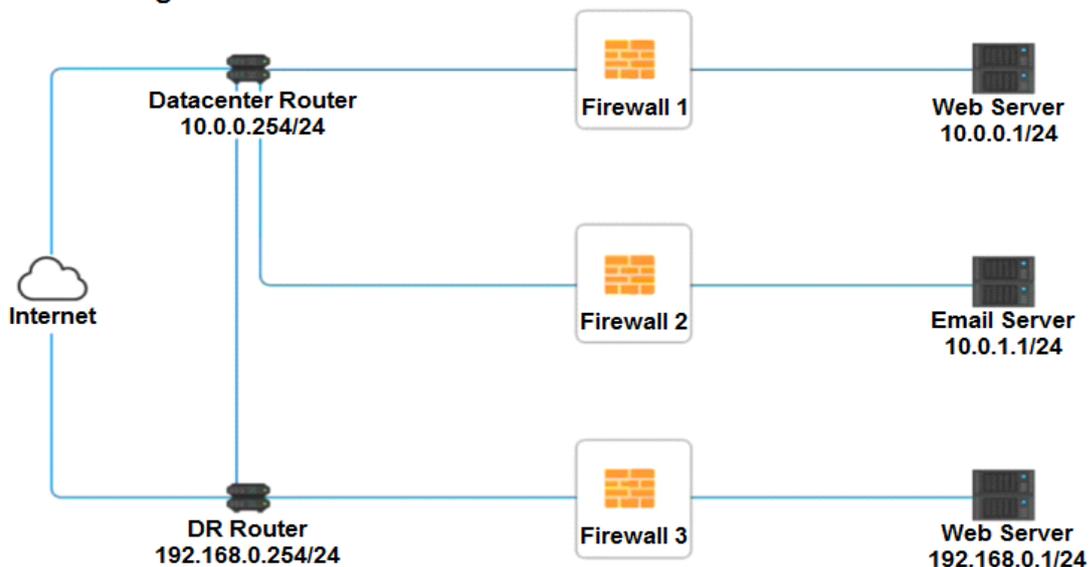
Ensure secure management protocols are used.

Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram



Firewall 1 [X]

Rule Name	Source	Destination	Services	Action
<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY	DNS Rule
<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY	HTTPS Outbound
<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY	Management
<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY	HTTPS Inbound
<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY	HTTP Inbound

Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY
HTTPS Outbound	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY
Management	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY
HTTPS Inbound	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY
HTTP Inbound	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY
HTTPS Outbound	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY
Management	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY
HTTPS Inbound	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY
HTTP Inbound	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text"/> ANY DNS HTTP HTTPS TELNET SSH	<input type="text"/> PERMIT DENY

Answer:

Explanation:
Firewall 1:

Firewall 1				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY

Reset Answer Save Close

Firewall 1				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY

Reset Answer Save Close

DNS Rule – ANY --> ANY --> DNS --> PERMIT
 HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT
 Management – ANY --> ANY --> SSH --> PERMIT
 HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT
 HTTP Inbound – ANY --> ANY --> HTTP --> DENY
 Firewall 2:

Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Reset Answer Save Close

Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Reset Answer Save Close

Firewall 3:

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

Reset Answer Save Close

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT

Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT

HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Question: 2

A security engineer is setting up passwordless authentication for the first time.

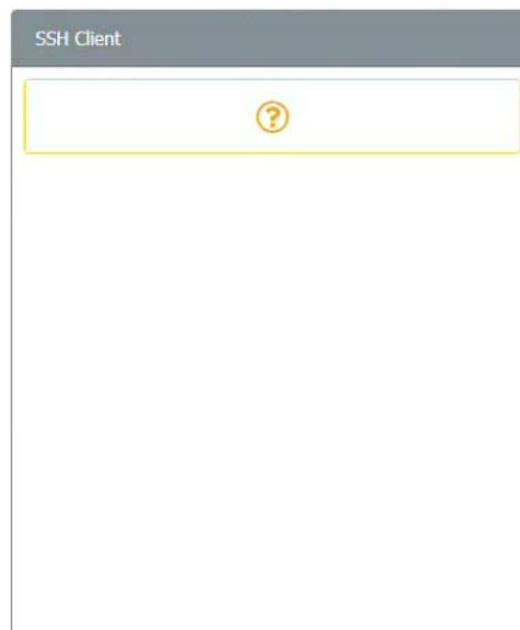
INSTRUCTIONS

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

```

Commands
-----
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
  
```



Answer:



Question: 3

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS

Not all attacks and remediation actions will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Patch vulnerable systems
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Conduct a code review

Question: 4

Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

- A. Cross-site scripting
- B. Data exfiltration
- C. Poor system logging
- D. Weak encryption
- E. SQL injection
- F. Server-side request forgery

Answer: DF

Question: 5

A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

- A. Containerization
- B. Geofencing
- C. Full-disk encryption
- D. Remote wipe

Answer: C

Question: 6

A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

- A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
- B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
- C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
- D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

Answer: D

Question: 7

A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

- A. Perform a site survey
- B. Deploy an FTK Imager
- C. Create a heat map

- D. Scan for rogue access points
- E. Upgrade the security protocols
- F. Install a captive portal

Answer: AC

Question: 8

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

- A. dd
- B. chmod
- C. dnsenum

D. logger

Answer: A

Question: 9

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

- A. SSAE SOC 2
- B. PCI DSS
- C. GDPR
- D. ISO 31000

Answer: C

Question: 10

Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

- A. DNSSEC and DMARC
- B. DNS query logging
- C. Exact mail exchanger records in the DNS
- D. The addition of DNS conditional forwarders

Answer: C

Question: 11

On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)

- A. Data accessibility
- B. Legal hold
- C. Cryptographic or hash algorithm
- D. Data retention legislation
- E. Value and volatility of data
- F. Right-to-audit clauses

Answer: EF

Question: 12

Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

- A. Investigation
- B. Containment
- C. Recovery
- D. Lessons learned

Answer: B

Question: 13

A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

- A. The scan results show open ports, protocols, and services exposed on the target host
- B. The scan enumerated software versions of installed programs
- C. The scan produced a list of vulnerabilities on the target host
- D. The scan identified expired SSL certificates

Answer: B

Question: 14

Which of the following BEST explains the difference between a data owner and a data custodian?

- A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
- B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
- C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
- D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Answer: B

Question: 15

A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

- A. Implement open PSK on the APs
- B. Deploy a WAF
- C. Configure WIPS on the APs
- D. Install a captive portal

Answer: D



CERTS CHIEF



Full Product includes:

- Money Back Guarantee
- Instant Download after Purchase
- 90 Days Free Updates
- PDF Format Digital Download
- 24/7 Live Chat Support
- Latest Syllabus Updates

For More Information - Visit:

<http://www.certschief.com/>

Discount Coupon Code:

CERTSCHIEF10

Visit us at

We Accept

PayPal