

CompTIA

SY0-601 Exam

CompTIA Security+

**Questions & Answers
Demo**

Version: 28.1

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:

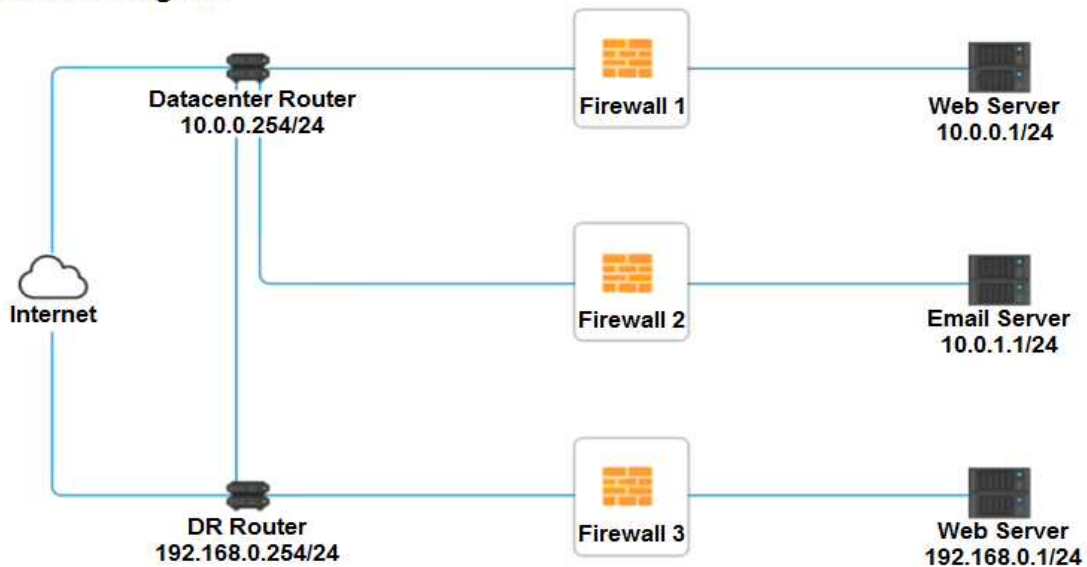
Deny cleartext web traffic.

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 2
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY DNS HTTP HTTPS TELNET SSH	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> PERMIT DENY
HTTPS Outbound	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY DNS HTTP HTTPS TELNET SSH	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> PERMIT DENY
Management	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY DNS HTTP HTTPS TELNET SSH	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> PERMIT DENY
HTTPS Inbound	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY DNS HTTP HTTPS TELNET SSH	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> PERMIT DENY
HTTP Inbound	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> ANY DNS HTTP HTTPS TELNET SSH	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">▼</div> PERMIT DENY

Reset Answer
Save
Close

Firewall 3
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> PERMIT DENY </div>
HTTPS Outbound	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> PERMIT DENY </div>
Management	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> PERMIT DENY </div>
HTTPS Inbound	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> PERMIT DENY </div>
HTTP Inbound	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: right; font-size: 0.8em;">▼</div> PERMIT DENY </div>

Reset Answer
Save
Close

Answer: See explanation below.

Explanation:
Firewall 1:

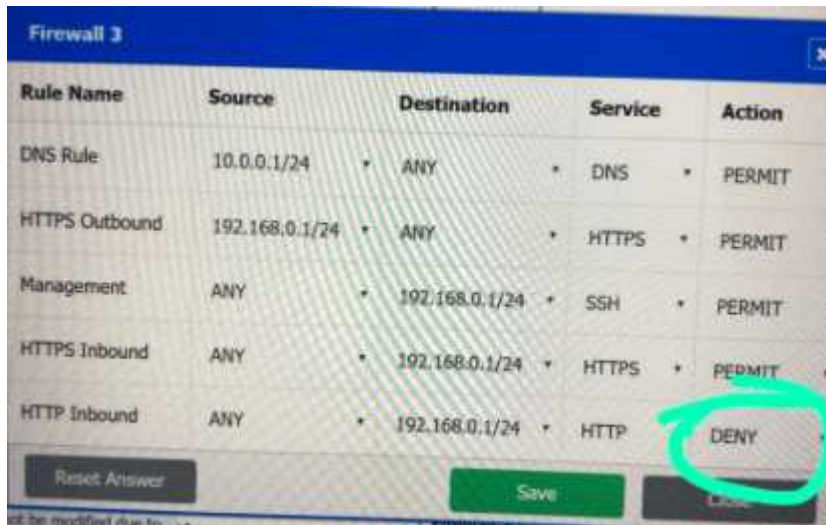
DNS Rule – ANY --> ANY --> DNS --> PERMIT
 HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT
 Management – ANY --> ANY --> SSH --> PERMIT
 HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT
 HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Firewall 2:

Firewall 3:

The screenshot shows a configuration window for 'Firewall 3' with a table of rules. The table has five columns: Rule Name, Source, Destination, Service, and Action. The rules listed are: DNS Rule (Source: 10.0.0.1/24, Destination: ANY, Service: DNS, Action: PERMIT), HTTPS Outbound (Source: 192.168.0.1/24, Destination: ANY, Service: HTTPS, Action: PERMIT), Management (Source: ANY, Destination: 192.168.0.1/24, Service: SSH, Action: PERMIT), HTTPS Inbound (Source: ANY, Destination: 192.168.0.1/24, Service: HTTPS, Action: PERMIT), and HTTP Inbound (Source: ANY, Destination: 192.168.0.1/24, Service: HTTP, Action: DENY). At the bottom of the window, there are buttons for 'Reset Answer', 'Save', and '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



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

DRAG DROP

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:



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

Question: 3

HOTSPOT

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
