

Demo Questions

CompTIA SY0-601 Exam

CompTIA Security+ 2021

Thank you for downloading SY0-601 Exam PDF

Question #1 Topic 1

SIMULATION -

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

INSTRUCTIONS -

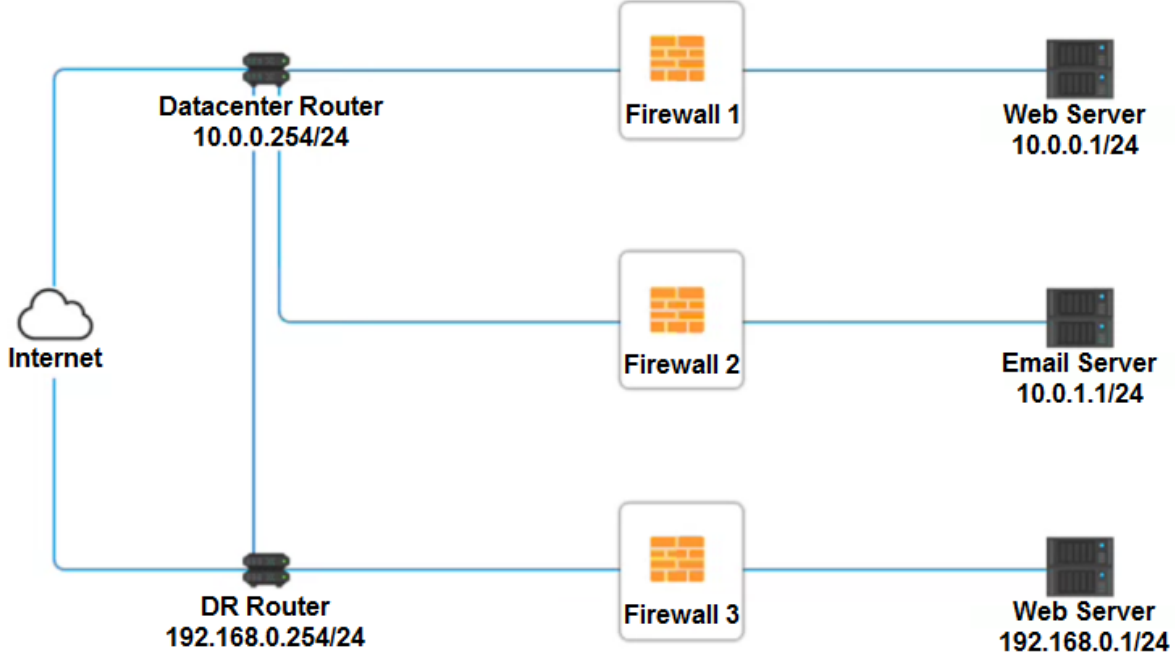
Click on each firewall to do the following:

1. Deny cleartext web traffic.
2. Ensure secure management protocols are used.
3. 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



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

Reset Answer

Save

Close

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

Reset Answer

Save

Close

Firewall 3



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

Reset Answer

Save

Close

Correct Answer: See explanation below.

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: No changes should be made to this firewall

Firewall 3:

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 Topic 1

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.

Select and Place:

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

Correct Answer:

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

Question #3 Topic 1

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.

Hot Area:

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

Correct Answer:

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

Question #4 Topic 1

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

Correct Answer: DF

Question #5 Topic 1

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

Correct Answer: C