

CompTIA Sy0-601

QUESTIONS AND ANSWERS

FREE VERSION

(LIMITED CONTENT)

Thank you for downloading our reliable exam questions for more exams you can visit:

https://www.pass4it.com/all-vendors

Dumps Questions sy0-601

Exam Name: CompTIA Security+ 2021

Certification Provider: CompTIA

Exam: CompTIA Security+ 2021

Question #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 -

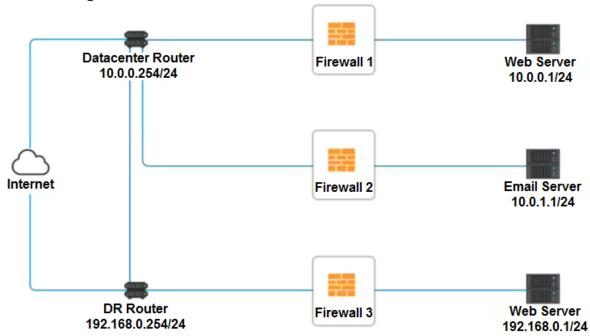
Click on each firewall to do the following:

- 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

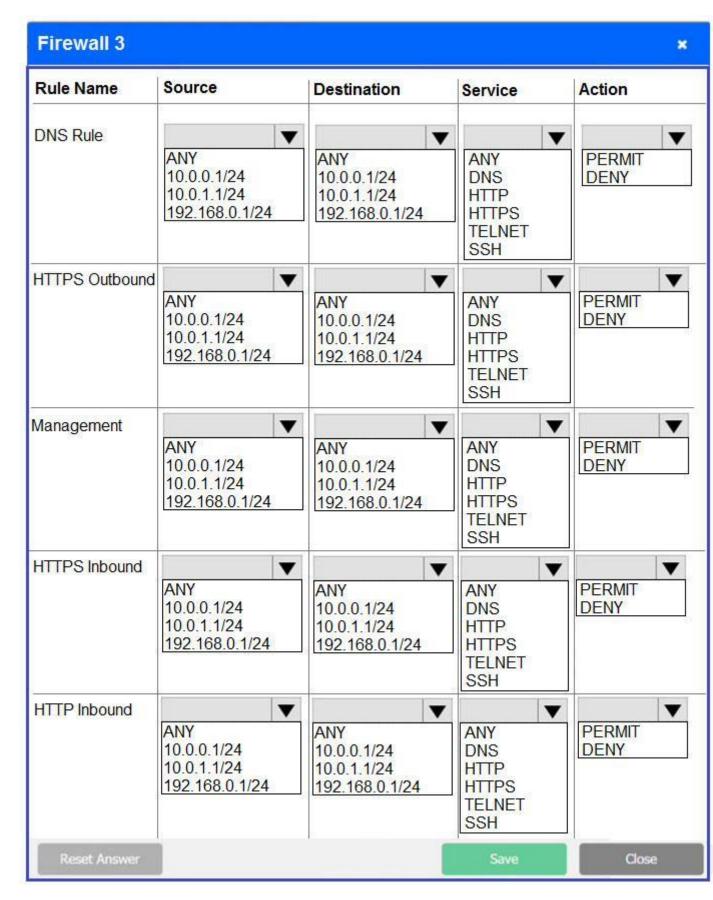


Firewall 1		
EIFOWAII 1		
I II C W CIII I		

rirewali i					
Rule Name	Source	Destination	Service	Action	
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY	
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY	
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY	
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY	
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY	
Reset Answer			Save	Close	

Firewall 2 ×

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT 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

DRAG DROP -

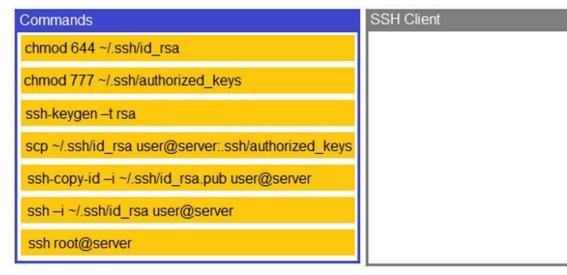
A security engineer is setting up passwordless authentication for the first time.

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:



Correct

Answer:

CommandsSSH Clientchmod 644 ~/.ssh/id_rsassh-keygen -t rsachmod 777 ~/.ssh/authorized_keysssh-copy-id -i ~/.ssh/id_rsa.pub user@serverssh-keygen -t rsachmod 644 ~/.ssh/id_rsascp ~/.ssh/id_rsa user@server:.ssh/authorized_keysssh root@serverssh-copy-id -i ~/.ssh/id_rsa.pub user@serverssh root@serverssh -i ~/.ssh/id_rsa user@serverssh root@server

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.

Hot Area:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation A
An attacker sends multiple SYN packets from			-
multiple sources.	Web server		E 11 55 6 1 1
multiple sources.		Botnet	Enable DDoS protection
		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
he attack establishes a connection, which allows	5900	•	
remote commands to be executed.	User	Botnet	Enable DDoS protection
emote commands to be executed.		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it	Database same		
2000 (1906) 150 (1906) 150 (1906) 150 (1906) 150 (1906) 150 (1906) 150 (1906) 150 (1906) 150 (1906) 1	Database server	Botnet	Enable DDoS protection
noves through the network.		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
he attacker uses hardware to remotely monitor a	LUCTURE SECURITION OF THE SECU		
ser's input activity to harvest credentials.	Executive	Detect	Enable DDoS protection
iser's input activity to rial vest credentials.		Botnet	
		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
he attacker embeds hidden access in an			
nternally developed application that bypasses	Application	7	Enable DDeC contesting
account login.	- ppinearion	Botnet	Enable DDoS protection
ccount login.		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS Disable remote access services

Correct Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation A
An attacker sends multiple SYN packets from			
	Web server		
multiple sources.		Botnet	Enable DDoS protection
		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		100000000000000000000000000000000000000	
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
he attack establishes a connection, which allows	NAME	•	
	User	Botnet	Enable DDoS protection
emote commands to be executed.		RAT	Patch vulnerable systems
		Compile Land	Disable vulnerable services
		Logic Bomb	
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		- 10-10-00-00-0	
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
The attack is self propagating and compromises a	100		
SQL database using well-known credentials as it	Database server	•	5 11 55 6 1
있는데 1000 HTM : 1000 HTM	Database server	Botnet	Enable DDoS protection
noves through the network.		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
			Disable remote access services
		Phishing	Disable remote access services
he attacker uses hardware to remotely monitor a	Executive	•	
user's input activity to harvest credentials.	LACCULAC	Botnet	Enable DDoS protection
		RAT	Patch vulnerable systems
		1000	
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		100000000000000000000000000000000000000	
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
The attacker embeds hidden access in an			
nternally developed application that bypasses	Application		
[[[[[[[[[[[[[[[[[[[[гирисалоп	Botnet	Enable DDoS protection
account login.		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	
			Update the cryptographic algorithms
		Spyware	Change the default application password
			Implement 2FA using push notification
		Spyware	
		Spyware Worm Adware	Implement 2FA using push notification Conduct a code review
		Spyware Worm Adware Ransomware	Implement 2FA using push notification Conduct a code review Implement application fuzzing
		Spyware Worm Adware	Implement 2FA using push notification Conduct a code review