# Latest Version: 31.0

## 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:

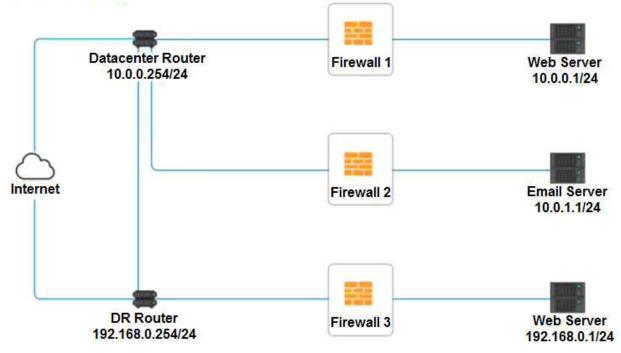
Deny cleartext web traffic.

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 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	V 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	V PERMIT DENY
Reset Answer			Save	Close

Firewall 3 ×				
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

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:
No changes should be made to this firewall

## No changes should be made to this firewall 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		192.158.0.1/24	•	HTTPS	,	PERMIT	
HTTP Inbound	ANY	•	192.168.0.1/24	•	НТТР		DENY	
Roset Artswar			s	ave			Close	2
Reset Answer Introduction date Trans Firewall 3			5	10.00			Close	
Firewall 3	Source		10000	10.00	Service		Close Action	
ine modified due train Firewall 3 Rule Name	Source 10.0.0.1/24		1 paretoan a -	10.00	Service DNS			
Firewall 3 Rule Name		*	Destination		1200/2		Action	
Firewall 3 Rule Name DNS Rule	10.0.0.1/24	x x x	Destination	•	DNS		Action	
be modified due to ' w	10.0.0.1/24 192.168.0.1/24		Destination Any Any	•	DNS HTTPS	•	Action PERMIT PERMIT	
Ine modified due to a v Firewall 3 Rule Name DNS Rule HTTPS Outbound Management	10.0.0.1/24 192.168.0.1/24 ANY		Destination ANY ANY 192/168.0.1/24	•	DNS HTTPS SSH	•	Action PERMIT PERMIT PERMIT	

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	SSH Client
chmod 644 ~/.ssh/ld_rsa	0
chmod 777 ~/_ssh/authorized_keys	
scp/.ssh/id_rsa.user@server:.ssh/authorized_keys	
ssh rootigiserver	
ssh-keygen –t rsa	
ssh-copy-ld ⊣/.ssh/ld_risa.pub user@server	
ssh—i.~/.ssh/id_rsa user@server	

**Answer:** 



## **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 Act
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
			Update the cryptographic algorithms
		Virus	
		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 establishes a connection, which allows	User	Botnet	Enable DDoS protection
remote commands to be executed.		RAT	Patch vulnerable systems
		Contraction and the second second	
		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
		and the second second second second	
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
The official is call composition and compositions of			
The attack is self propagating and compromises a SQL database using well-known credentials as it	Database server	•	·
	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
		A DEPARTMENT OF THE REAL MADE	Update the cryptographic algorithms
		Virus	
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing
			Implement a host-based IPS
		Keylogger	
		Phishing	Disable remote access services
The attacker uses hardware to remotely monitor a	Executive		
user's input activity to harvest credentials.	LYACOUAA	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
		CARESSEN EL MANAGE	
		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	*	
	, appreciation	Botnet	Enable DDoS protection
account login.		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
			Update the cryptographic algorithms
		Virus	
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing
		Transon ware	
		Koulogaas	Implement a host bacod IDS
		Keylogger Phishing	Implement a host-based IPS Disable remote access services

Answer:

Attack Description	Target	Attack Identi	fied	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	۲	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 humanmanagement

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: A

Explanation:

https://www.hexnode.com/blogs/what-is-containerization-and-why-is-it-important-for-your-business/