Latest 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:

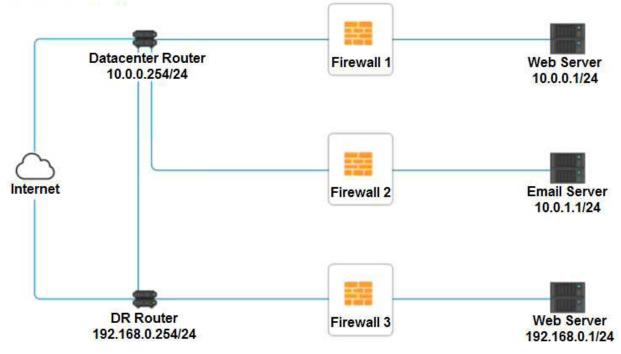
Deny cleartext web traffic.

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	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 3	rewall 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:

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	$\left \cdot \right $	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	
Reset Answer			S CONSIGNATION OF	200			Close	
the modified due to . w	Source		10000	10.04	Service			
Firewall 3	Source 10.0.0.1/24		1 Paretonan	10.04	Service		Close Action PERMIT	
In modified due to a v Firewall 3 Rule Name DNS Rule		* *	Destination	10.04	200/2		Action	
in modified due to a second se	10.0.0.1/24		Destination ANY	•	DNS		Action	
Firewall 3 Rule Name DNS Rule HTTPS Outbound	10.0.0.1/24 192.168.0.1/24	W.	Destination Any Any	•	DNS HTTPS	•	Action PERMIT PERMIT	
Internediated due to a Firewall 3 Rule Name ONS Rule HTTPS Outbound Management	10.0.0.1/24 192.168.0.1/24 ANY		Destination ANY ANY 197,168.0.1/24	•	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.

SSH Client
(?

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	1222.00		
multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password
		Virus Spyware Worm Adware Ransomware Keylogger Phishing	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	124	•	
remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger	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
		Phishing	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	• Botnet RAT	Enable DDoS protection Patch vulnerable systems
		Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	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	Executive		-
user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	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	Botnet RAT Logic Bomb	Enable DDoS protection Patch vulnerable systems Disable vulnerable services
		Backdoor Virus Spyware Worm Adware Ransomware	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
		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	٠	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: C