Attack Description	Target	Attack Identified	BEST Preventative or Remediation Act
An attacker sends multiple SYN packets from	Web server	•	•
multiple sources.	VVCD 301V01	Botnet	Enable DDoS protection
		RAT	Patch vulnerable systems
		50-500000000000000000000000000000000000	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
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
The attack establishes a connection, which allows		•	•
remote commands to be executed.	User	Botnet	Enable DDoS protection
remote 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
			Implement application fuzzing
		Ransomware	
		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 server		·
	Database server	Botnet	Enable DDoS protection
moves 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
The attacker uses hardware to remotely monitor a	Executive	•	
user's input activity to harvest credentials.	2.000	Botnet	Enable DDoS protection
		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
			Change the default application password
		Spyware	Implement 2FA using push notification
		Worm	
		Adware	Conduct a code review
		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	Potent	Enable DDoS protection
		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
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Dancom	
		Ransomware	Implement application fuzzing
		Ransomware Keylogger Phishing	Implement application ruzzing Implement a host-based IPS Disable remote access services

Correct Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Act
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb	Enable DDoS protection I Patch vulnerable systems Disable vulnerable services
		Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	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	User	Botnet	Enable DDoS protection
remote commands to be executed.		RAT Logic Bomb Backdoor Virus	Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms
		Spyware Worm Adware Ransomware Keylogger Phishing	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-preparating and compressions a			
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb	Enable DDoS protection Patch vulnerable systems Disable vulnerable services
		Backdoor Virus Spyware Worm Adware	Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review
		Ransomware Keylogger Phishing	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.		Botnet RAT Logic Bomb Backdoor Virus Spyware	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password
		Worm Adware Ransomware Keylogger Phishing	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	Application	Retnet	Enable DDoS protection
account login.		Botnet RAT Logic Bomb	Patch vulnerable systems Disable vulnerable services
		Backdoor Virus	Change the default system password Update the cryptographic algorithms
		Spyware Worm Adware	Change the default application password Implement 2FA using push notification Conduct a code review
		Ransomware Keylogger	Implement application fuzzing Implement a host-based IPS
		Phishing	Disable remote access services

QUESTION 99

HOTSPOT

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

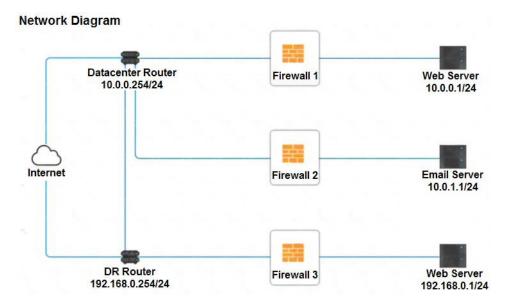
INSTRUCTIONS

Click on each firewall to do the following:

- Deny cleartext web traffic.
- Ensure secure management protocols are used. Please 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.



Firewall 1				×
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