DUMPSHQ

Free Questions for SY0-601 by dumpshq

Shared by Rodriguez on 07-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: DragDrop

An attack has occurred against a company.

INSTRUCTIONS

You have been tasked to do the following:

Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1).

Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server.

(Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Image not found or type unknown

Image not found or type unknown

Answer:

Question 2

Question Type: **MultipleChoice**

A172

given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

Options:

A) Nmapn

B) Heat maps

C) Network diagrams

D) Wireshark

Answer:

C

Question 3

Question Type: **MultipleChoice**

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:

Deny cleartext web traffic.

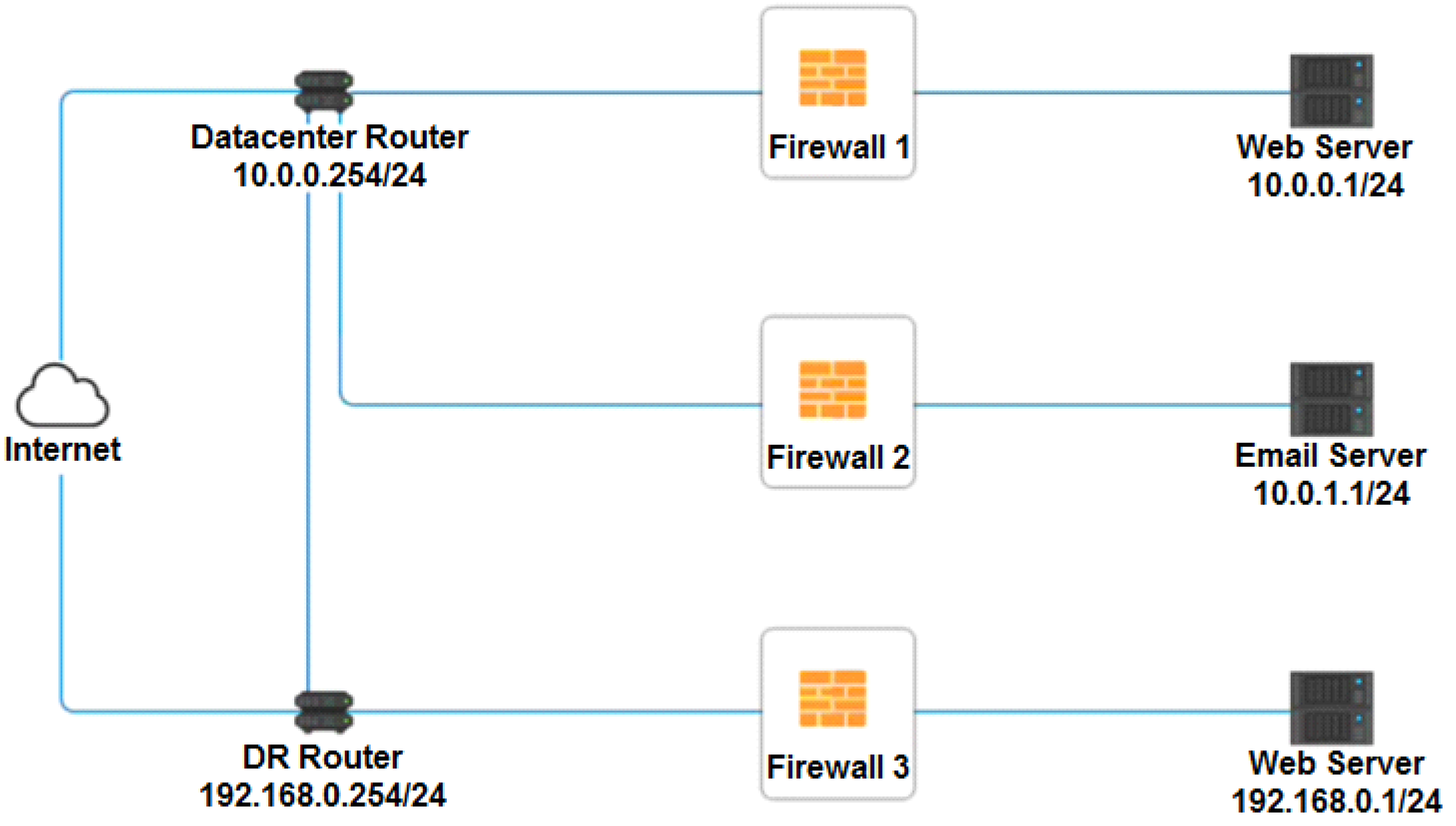
Ensure secure management protocols are used.

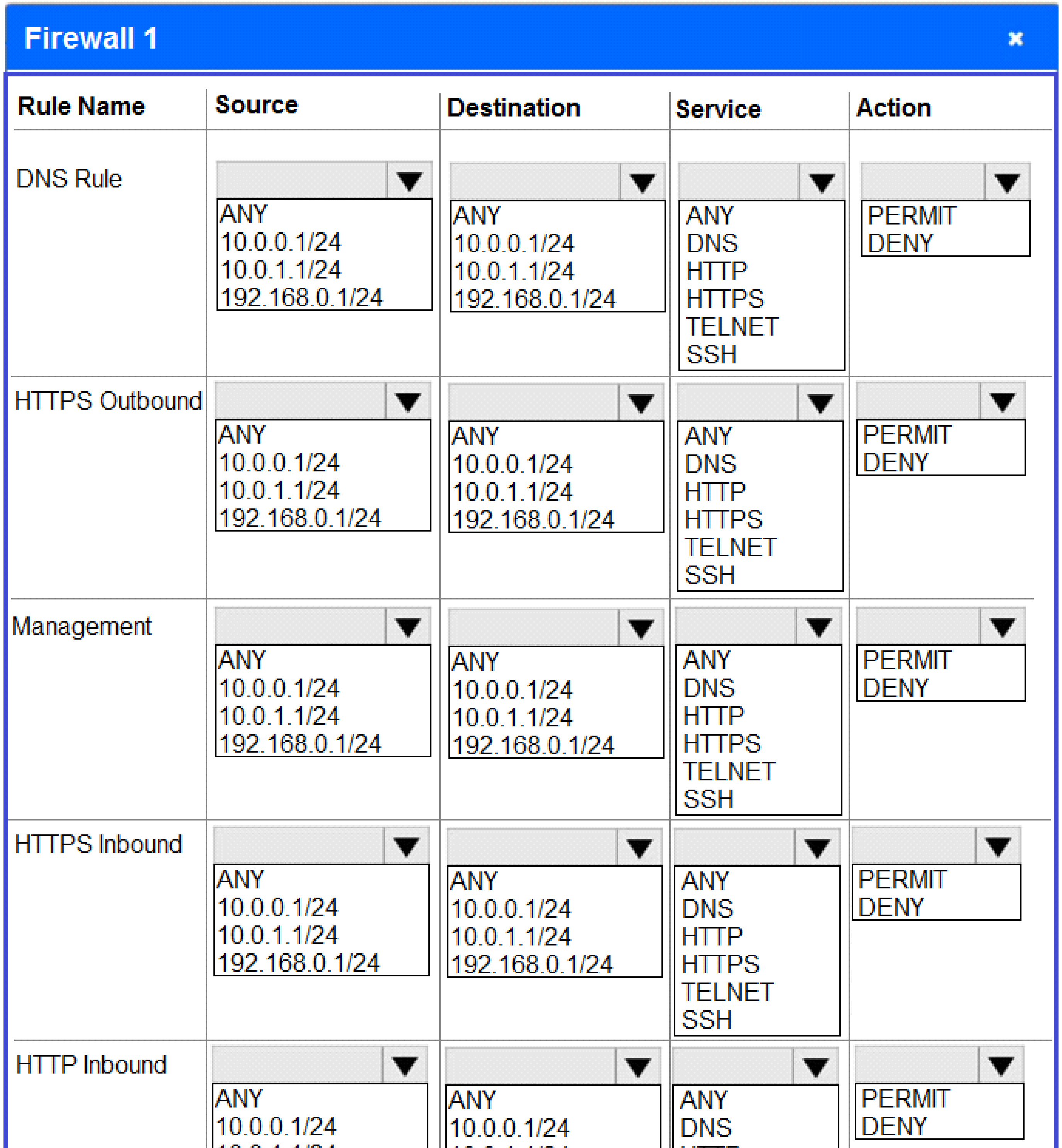
Resolve issues at the DR site.

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.

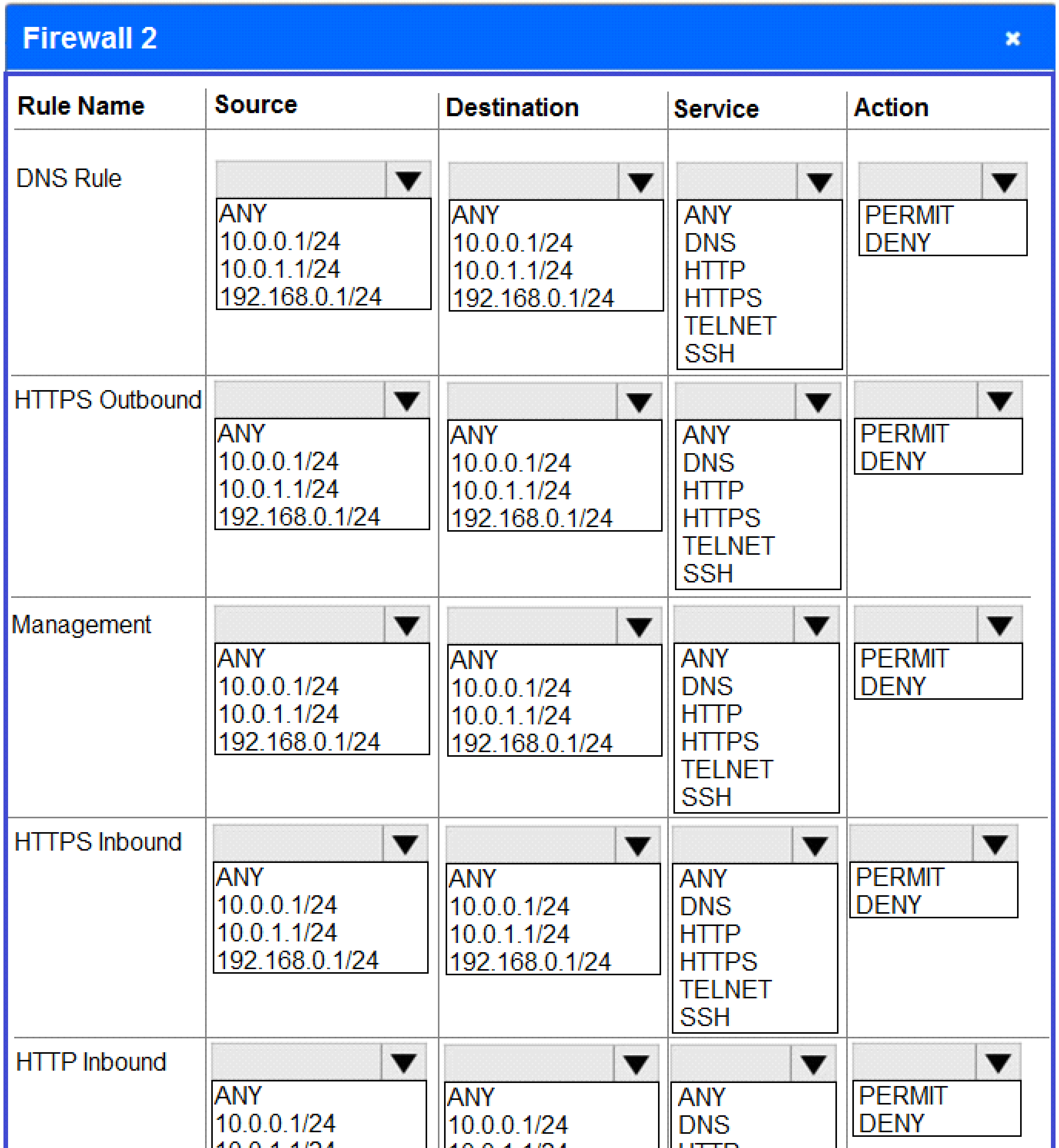
Network Diagram





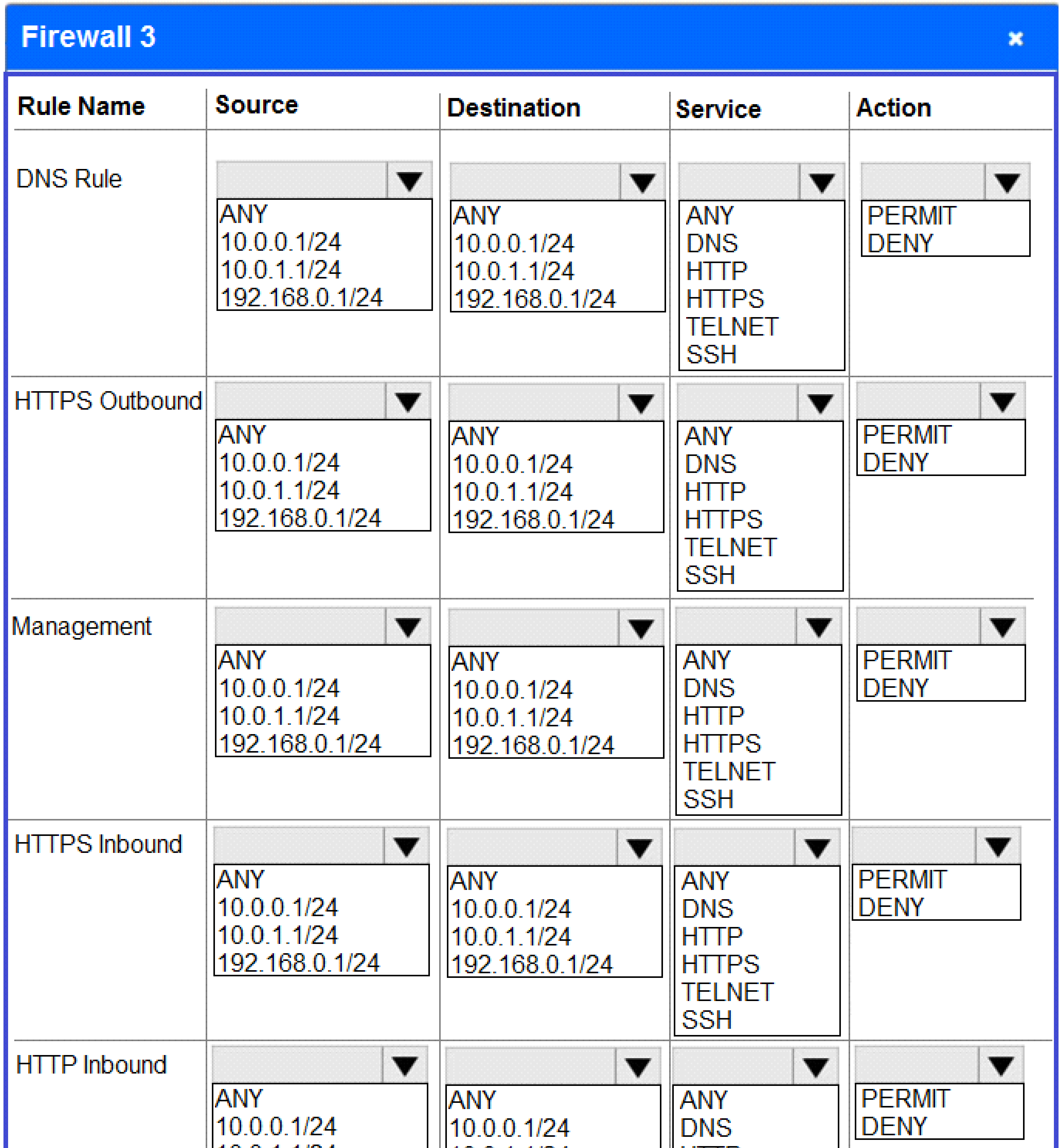
Firewall 1

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	ANY 10.0.0.1/24	ANY DNS	PERMIT DENY



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	ANY 10.0.0.1/24	ANY DNS	PERMIT DENY



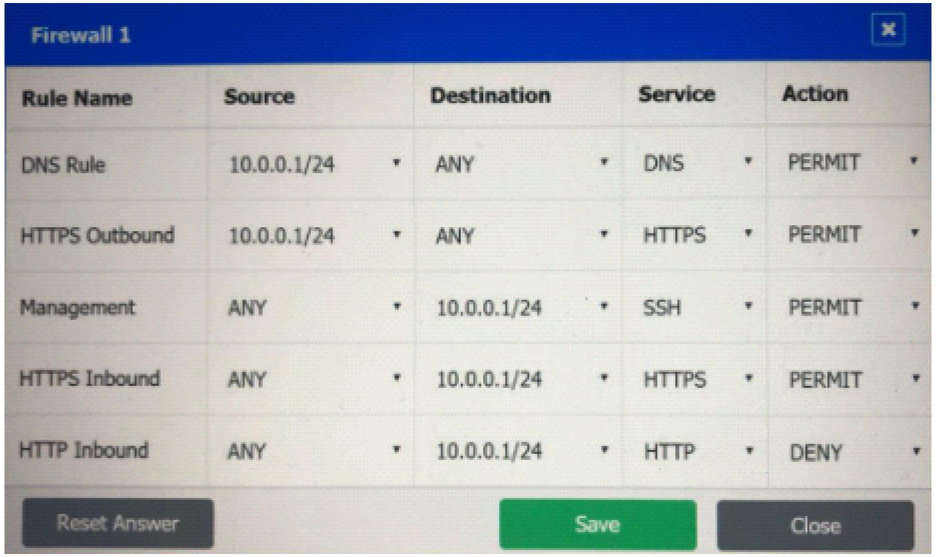
Firewall 3

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	ANY 10.0.0.1/24	ANY DNS	PERMIT DENY

Options:

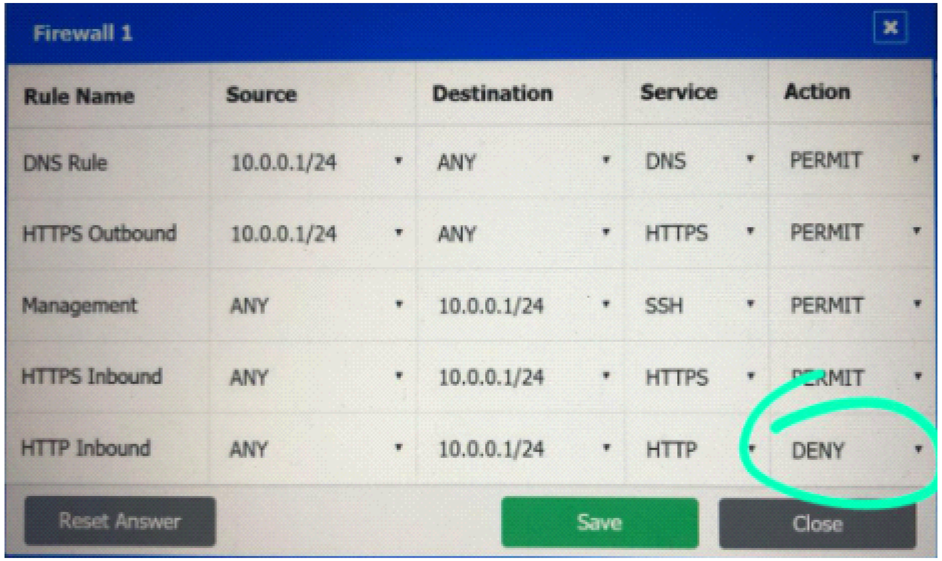
A) Explanation:

Firewall 1:



Firewall 1

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



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

DNS Rule -- ANY --> ANY --> DNS --> PERMIT

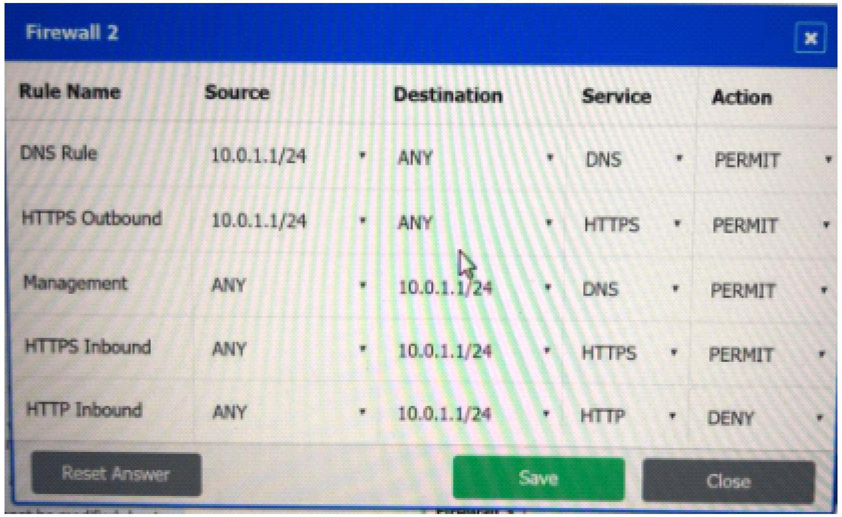
HTTPS Outbound -- 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT

Management -- ANY --> ANY --> SSH --> PERMIT

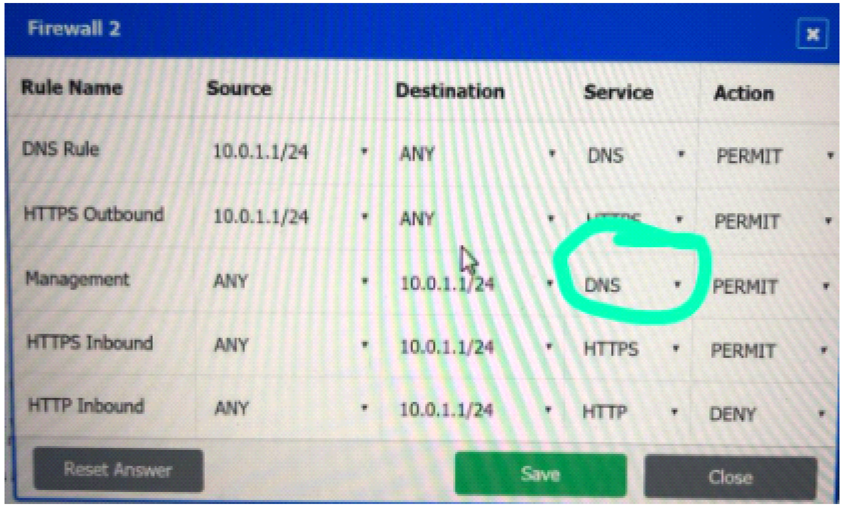
HTTPS Inbound -- ANY --> ANY --> HTTPS --> PERMIT

HTTP Inbound -- ANY --> ANY --> HTTP --> DENY

Firewall 2:

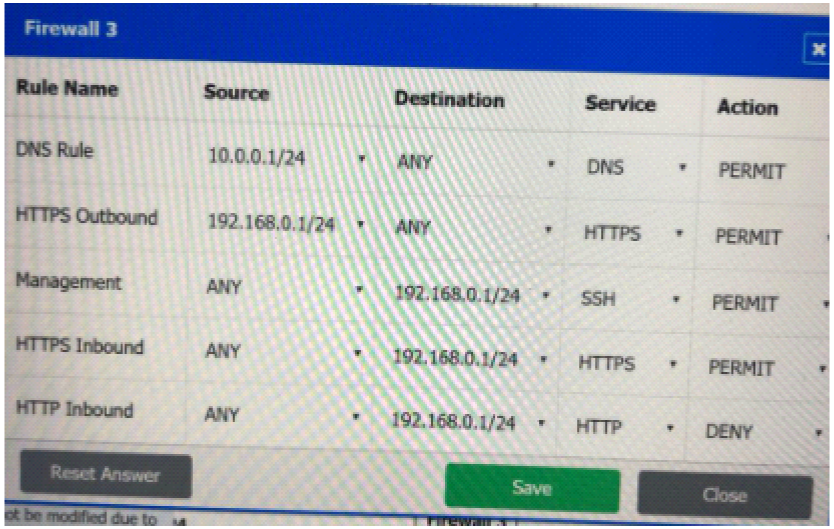


Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

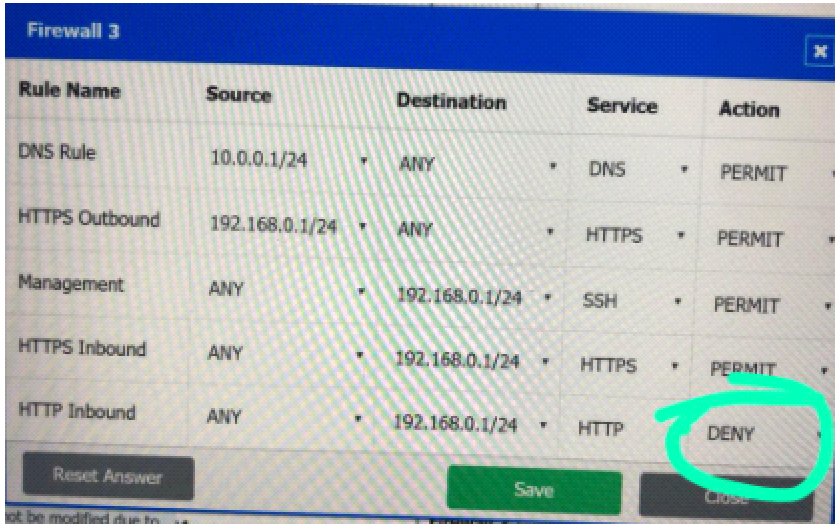


Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

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	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY



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	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

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

Answer:

A

Question 4

Question Type: **MultipleChoice**

The process of passively gathering information poor to launching a cyberattack is called:

Options:

A) tailgating

B) reconnaissance

C) pharming

D) prepending

Answer:

B

Question 5

Question Type: **MultipleChoice**

A157

is given the following, requirements?

* The solution must be inline in the network

* The solution must be able to block known malicious traffic

* The solution must be able to stop network-based attacks

Which of the following should the network administrator implement to BEST meet these requirements?

Options:

A) HIDS

B) NIDS

C) HIPS

D) NIPS

Answer:

D

Question 6

Question Type: **Hotspot**

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:

Deny cleartext web traffic.

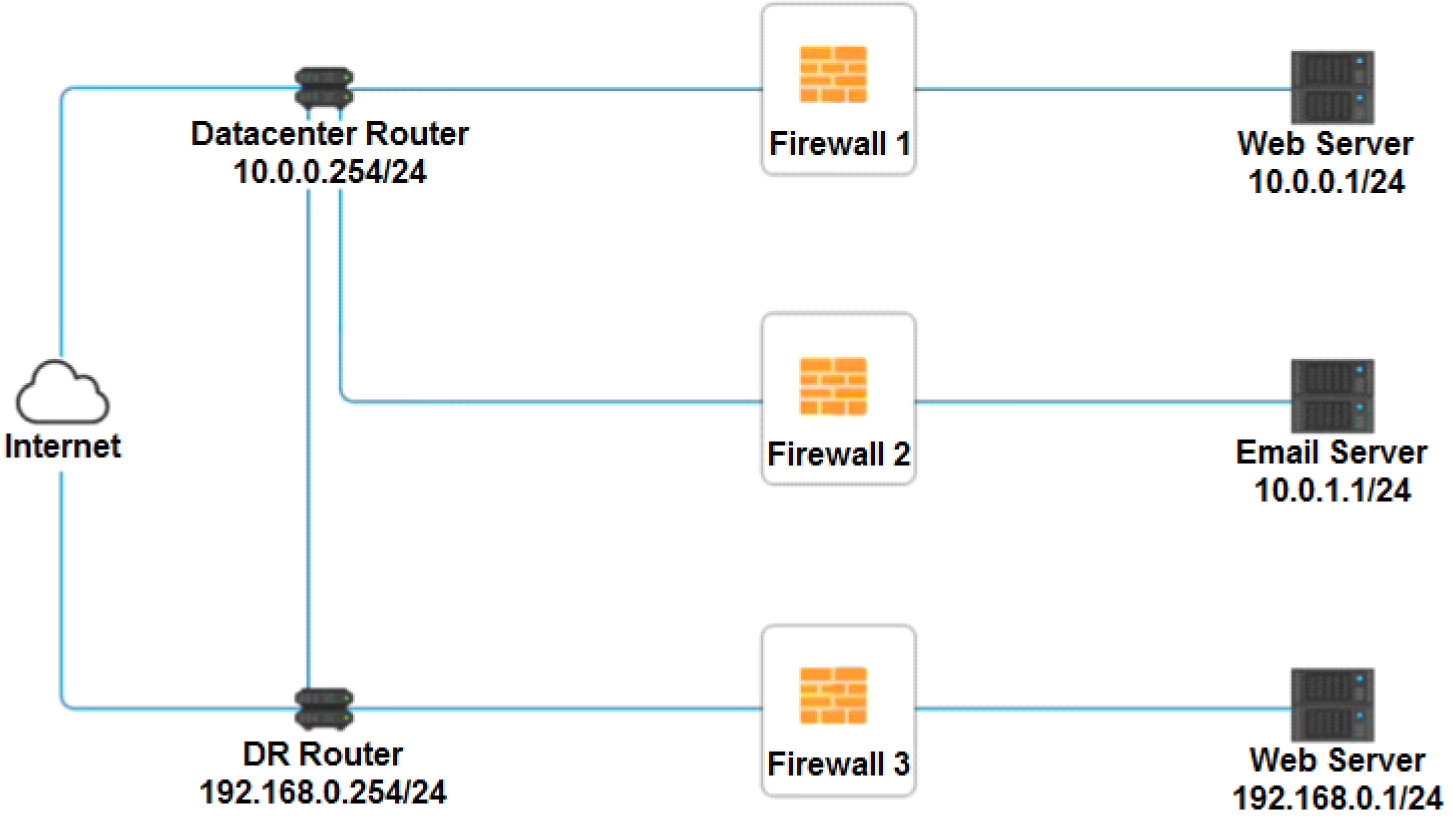
Ensure secure management protocols are used.

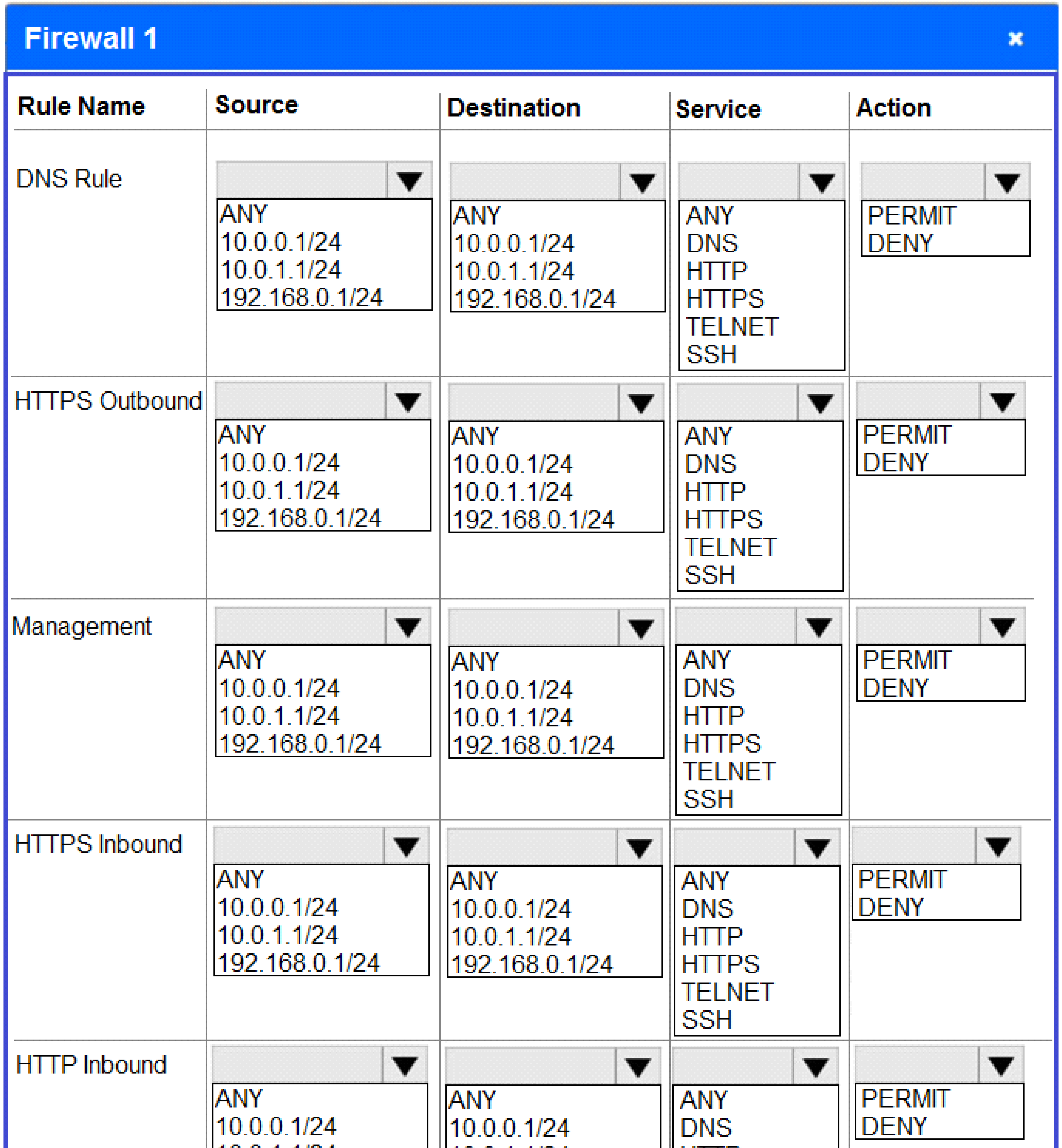
Resolve issues at the DR site.

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.

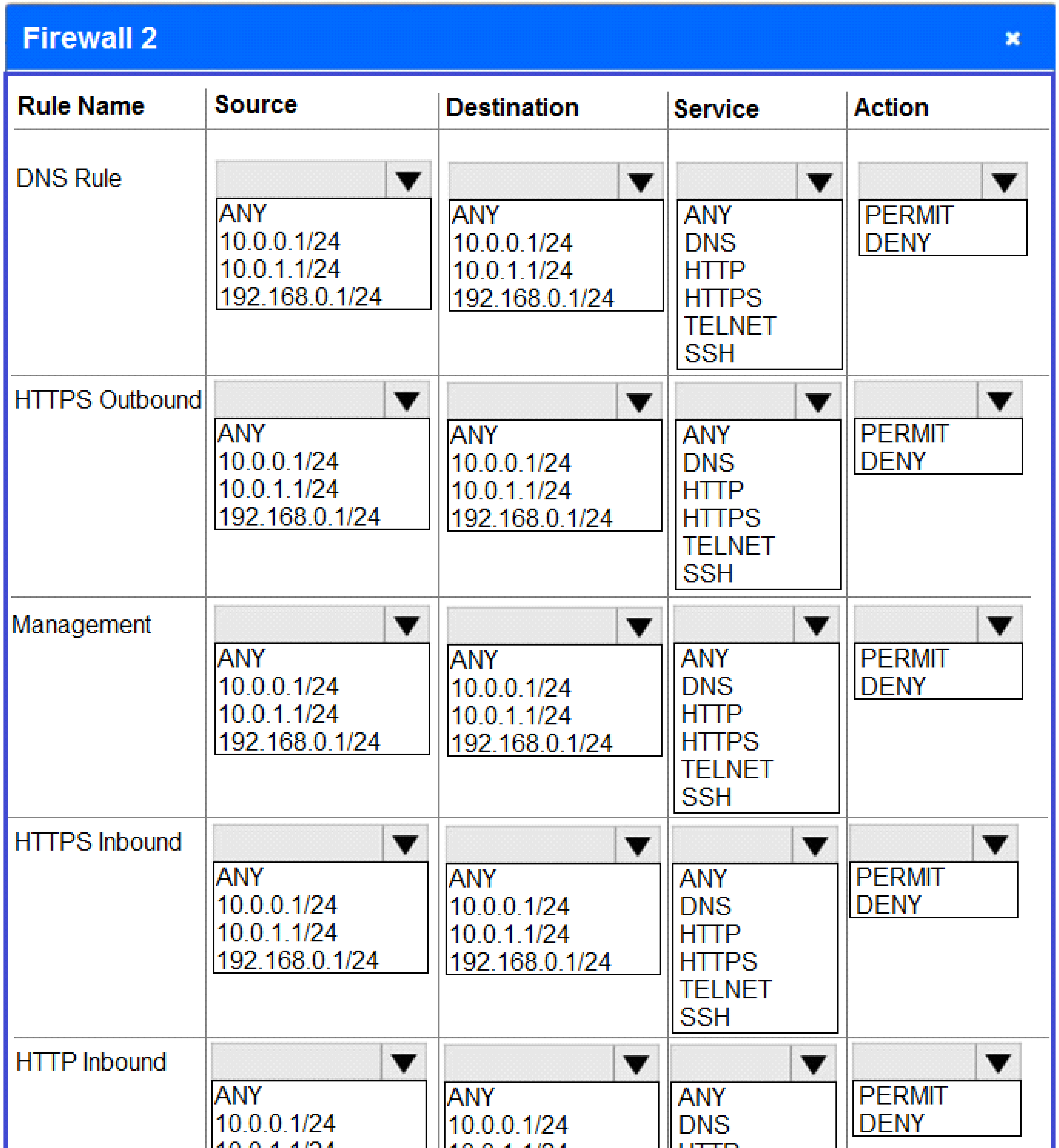
Network Diagram





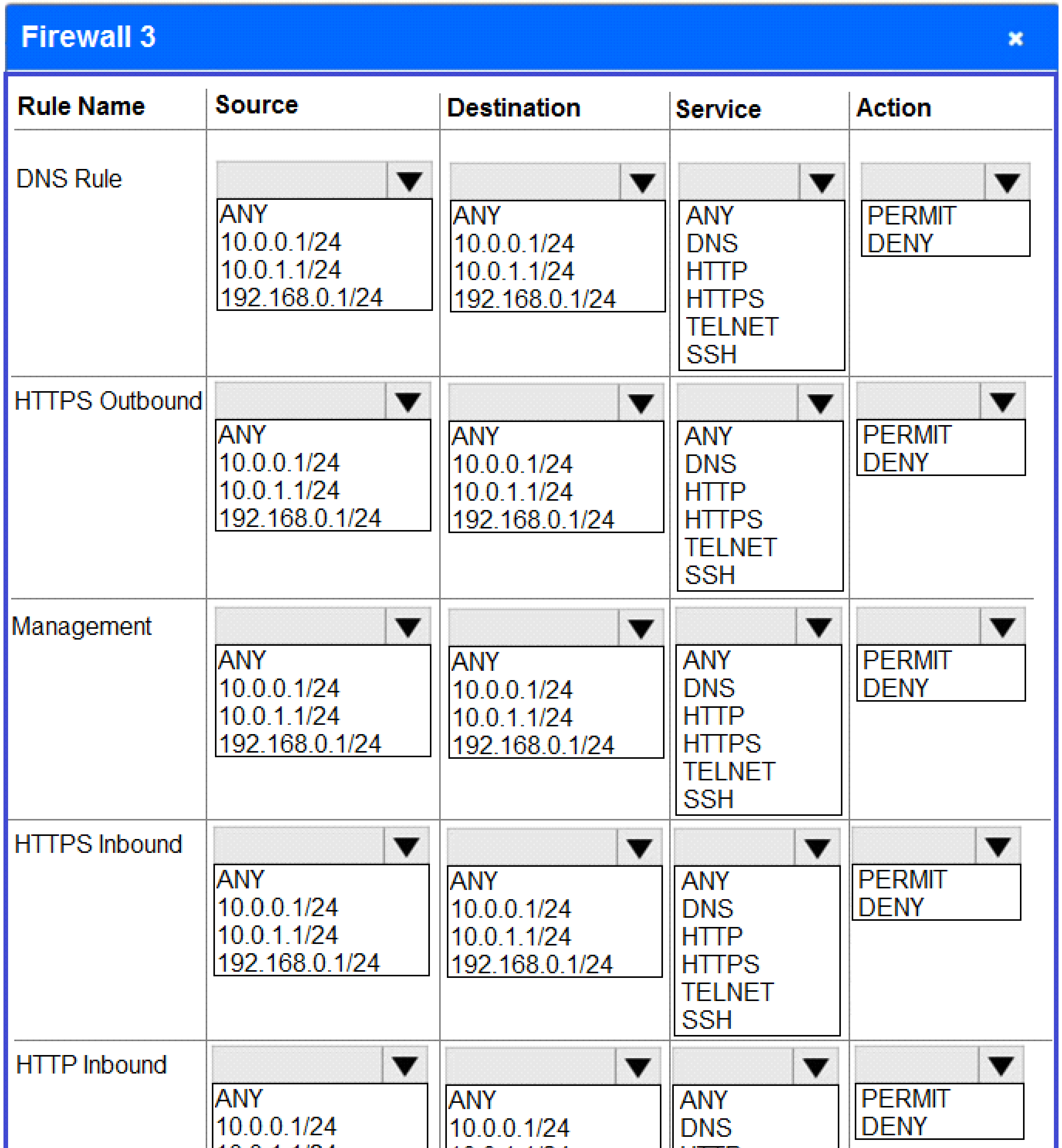
Firewall 1

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	▼ ANY 10.0.0.1/24	▼ ANY DNS	▼ PERMIT DENY



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	▼ ANY 10.0.0.1/24	▼ ANY DNS	▼ PERMIT DENY
]



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	ANY 10.0.0.1/24	ANY DNS	PERMIT DENY

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

Answer:

Question 7

Question Type: **MultipleChoice**

An attacker was easily able to log in to a company's security camera by performing a baste online search for a setup guide for that particular camera brand and model. Which of the following BEST describes the configurations the attacker exploited?

A Weak encryption

Options:

B) Unsecure protocols

C) Default settings

D) Open permissions

Answer:

C

Question 8

Question Type: MultipleChoice

n organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization

need to determine for this to be successful?

Options:

A) The baseline

B) The endpoint configurations

C) The adversary behavior profiles

D) The IPS signatures

Answer:

C

Question 9

Question Type: MultipleChoice

A Chief Executive Officer (CEO) is dissatisfied with the level of service from the company's new service provider. The service provider is preventing the CEO.

from sending email from a work account to a personal account. Which of the following types of service providers is being used?

Options:

A) Telecommunications service provider

B) Cloud service provider

C) Master managed service provider

D) Managed security service provider

Answer:

B

Question 10

Question Type: **MultipleChoice**

The security administrator has installed a new firewall which implements an implicit DENY policy by default.

Options:

A) INSTRUCTIONS:

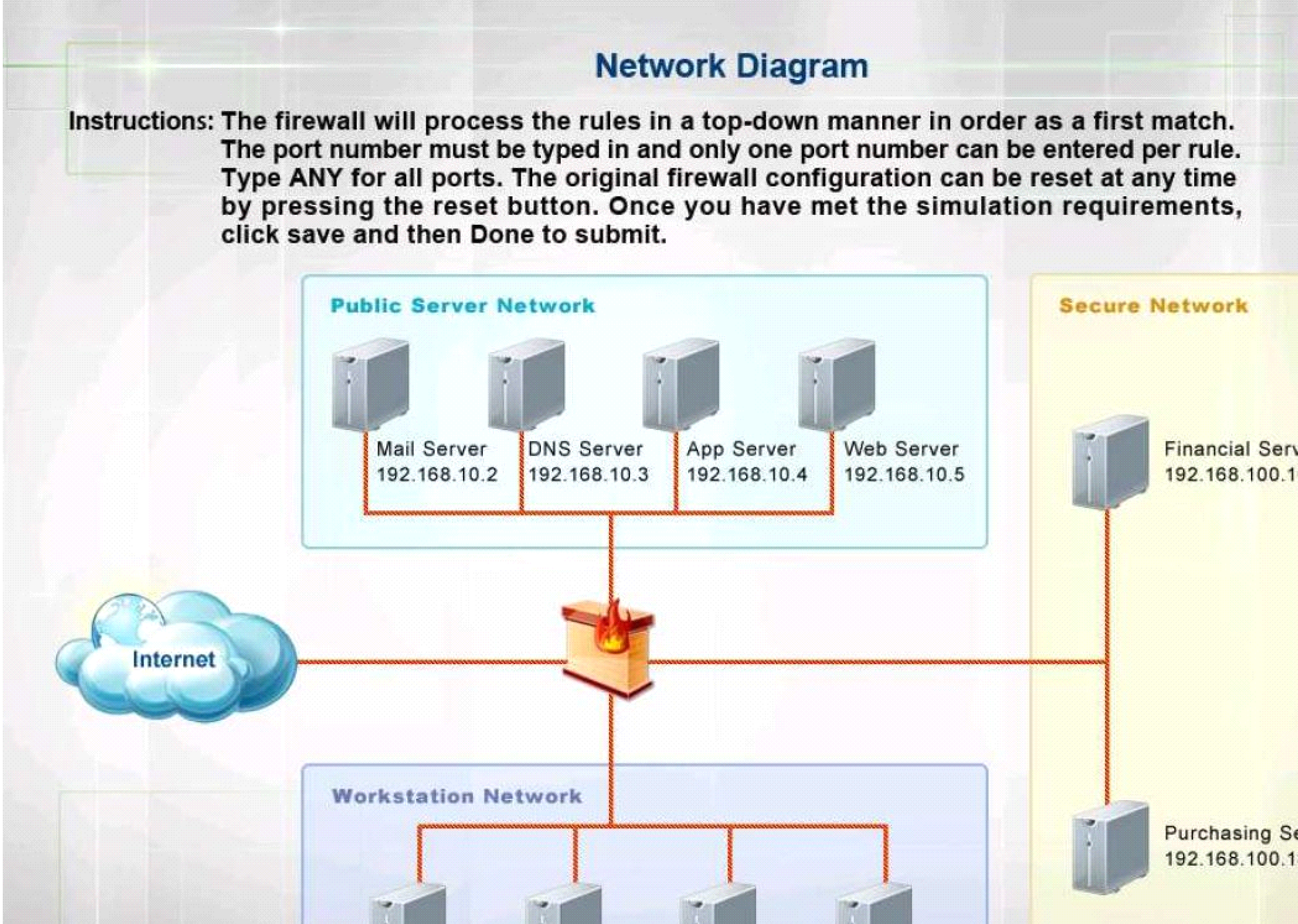
Click on the firewall and configure it to allow ONLY the following communication.

1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.

2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port

3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

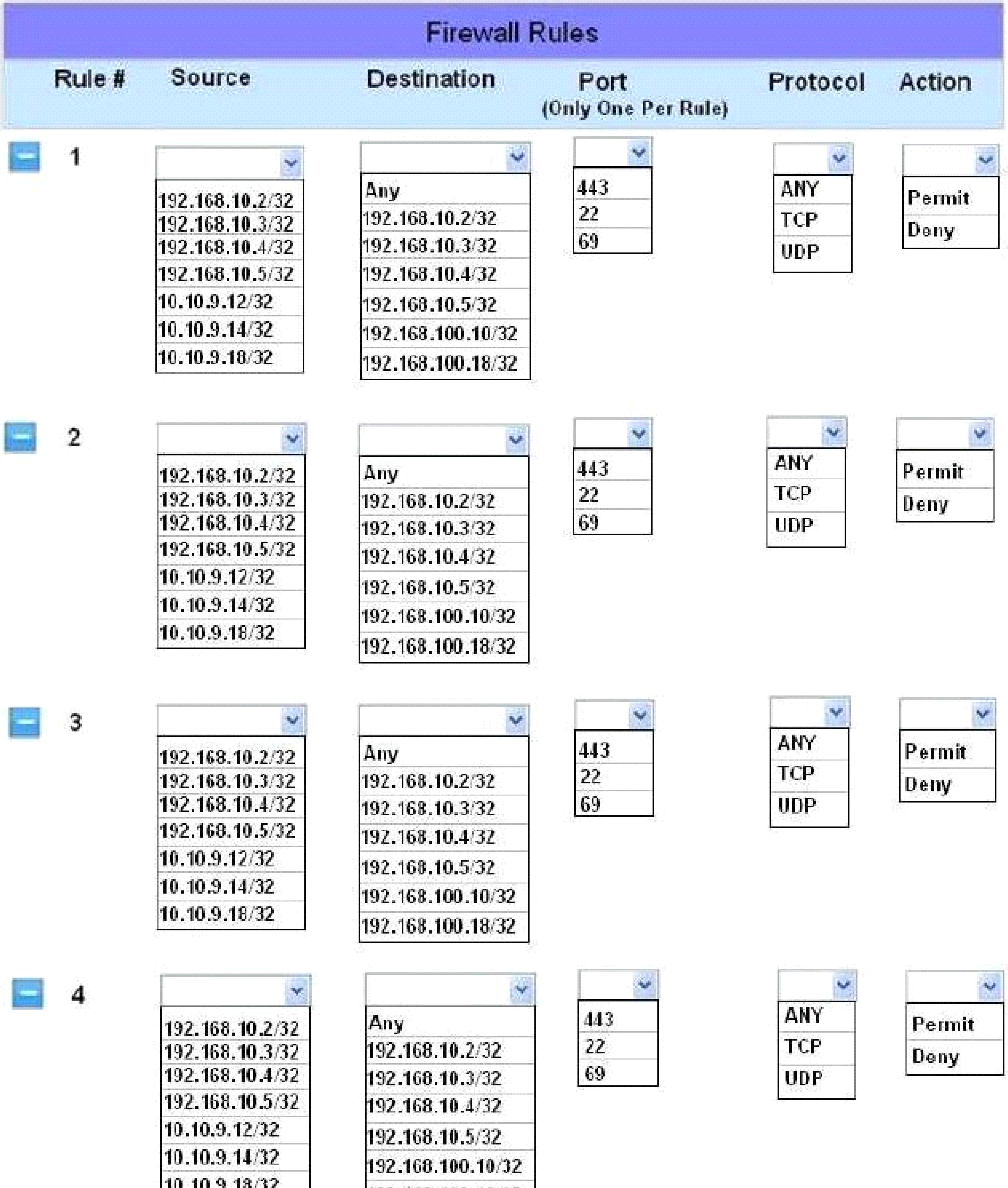
Instructions: The firewall will process the rules in a top-down manner in order as a first match The port number must be typed in and only one port number can be entered per rule Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.



Network Diagram

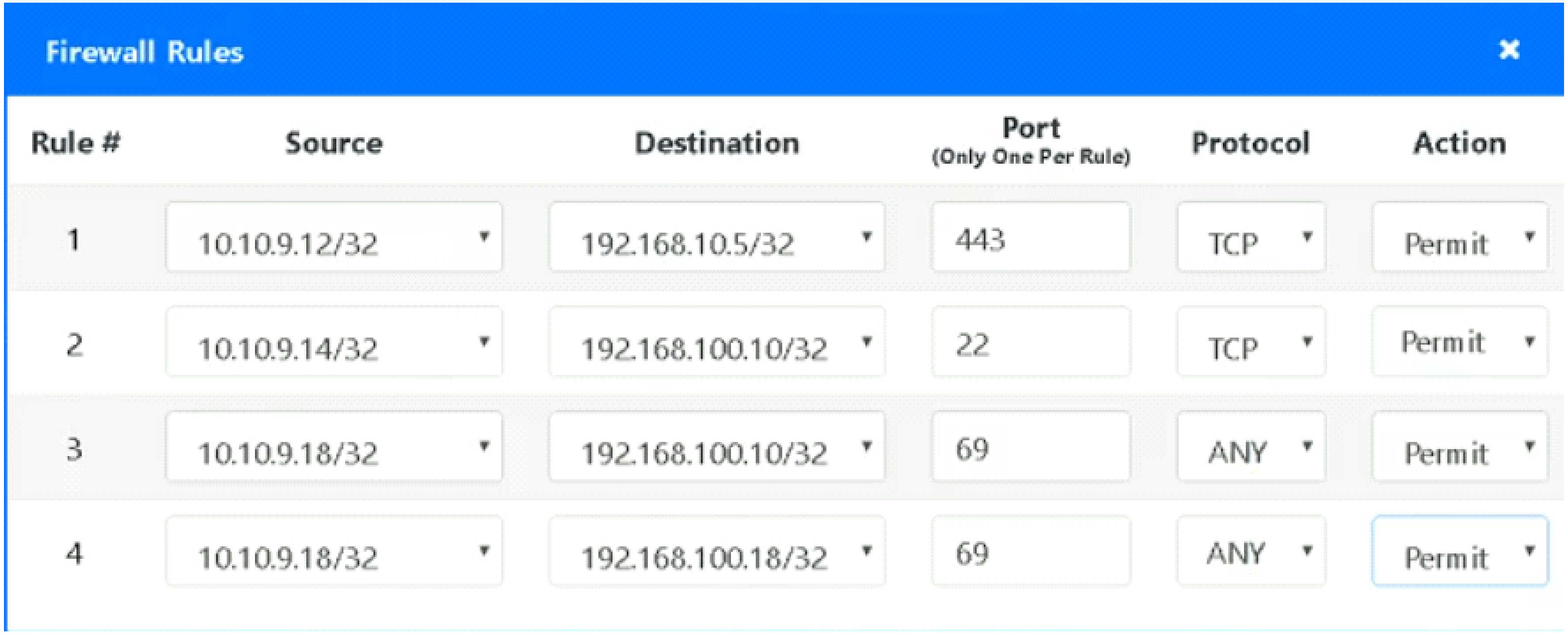
Instructions: The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.

Hot Area:



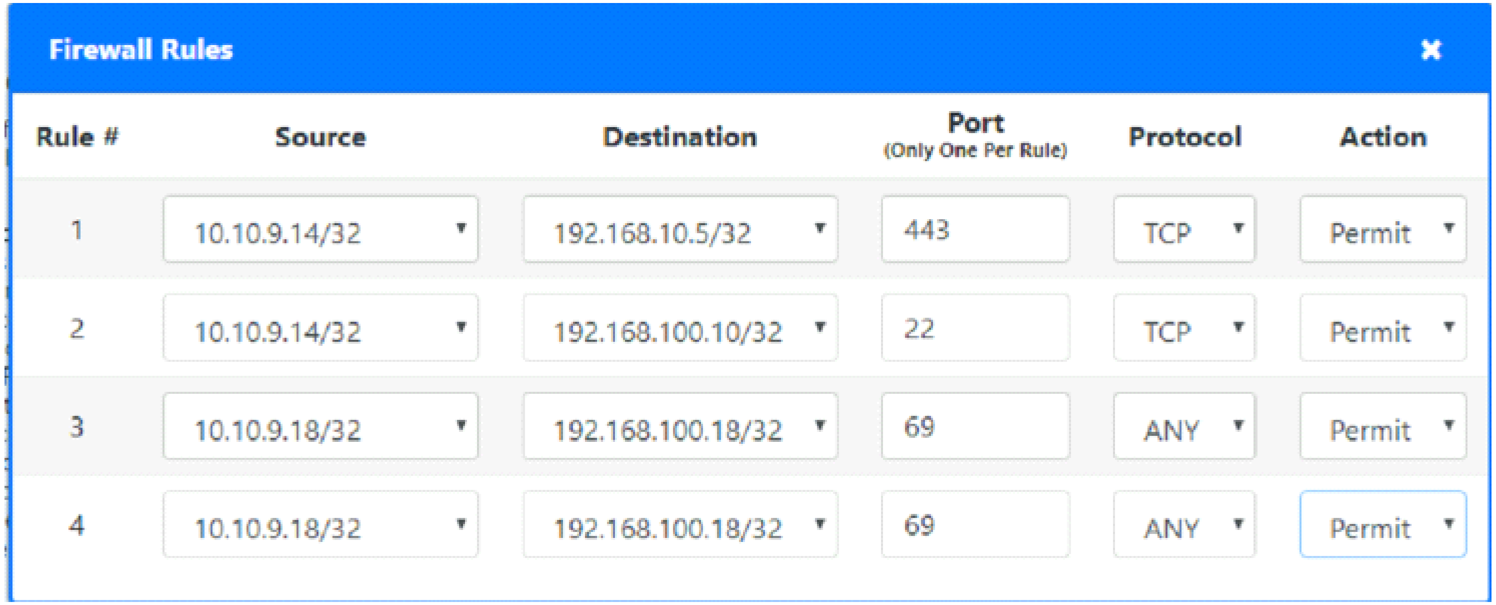
Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
2	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
3	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
4	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32	443 22 69	ANY TCP UDP	Permit Deny



Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	10.10.9.12/32	192.168.10.5/32	443	TCP	Permit
2	10.10.9.14/32	192.168.100.10/32	22	TCP	Permit
3	10.10.9.18/32	192.168.100.10/32	69	ANY	Permit
4	10.10.9.18/32	192.168.100.18/32	69	ANY	Permit



Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	10.10.9.14/32	192.168.10.5/32	443	TCP	Permit
2	10.10.9.14/32	192.168.100.10/32	22	TCP	Permit
3	10.10.9.18/32	192.168.100.18/32	69	ANY	Permit
4	10.10.9.18/32	192.168.100.18/32	69	ANY	Permit

Section: Network Security

Answer:

A

Explanation:

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default.

Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443.

Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port 22

Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69.

References: Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 26, 44
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

References: Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 26, 44
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Question 11

Question Type: **MultipleChoice**

organization's vulnerabilities. Which of the following would BEST meet this need?

Options:

A) CVE

B) SIEM

C) SOAR

D) CVSS

Answer:

D