N10-009$^{\text{Q\&As}}$

CompTIA Network+ Exam

Pass CompTIA N10-009 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/n10-009.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?

A. To encrypt sensitive data in transit

B. To secure the endpoint

C. To maintain contractual agreements

D. To comply with data retentin requirements

Correct Answer: A

The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user\\'s device and the corporate network, ensuring that data

is encrypted and protected from interception.

Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks. Data Protection: Essential for industries handling sensitive information, such as insurance

brokerages, to protect customer data and comply with regulatory requirements.

Security: Enhances overall network security by providing secure remote access for employees.

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Discusses the role of VPNs in securing data in transit.

Cisco Networking Academy: Provides training on VPN technologies and their importance in data security.

Network+ Certification All-in-One uide: Explains VPN usage and its benefits in protecting sensitive information.

QUESTION 2

A technician completed troubleshooting and was able to fix an issue. Which of the following is the BEST method the technician can use to pass along the exact steps other technicians should follow in case the issue arises again?

A. Use change management to build a database

B. Send an email stating that the issue is resolved.

C. Document the lessons learned

D. Close the ticket and inform the users.

Correct Answer: C

Documenting the lessons learned is the best method for passing along the exact steps other technicians should follow in case the issue arises again. Lessons learned are the knowledge and experience gained from completing a project or solving a problem. Documenting the lessons learned helps to capture the best practices, challenges, solutions, and recommendations for future reference and improvement. Documenting the lessons learned can also help to update the knowledge base, standard operating procedures, or policies related to the issue. References: [CompTIA Network+ Certification Exam Objectives], Lessons Learned: Definition and Examples for Project Managers

QUESTION 3

SIMULATION

You have been tasked with implementing an ACL on the router that will:

1.

Permit the most commonly used secure remote access technologies from the management network to all other local network segments

2.

Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.

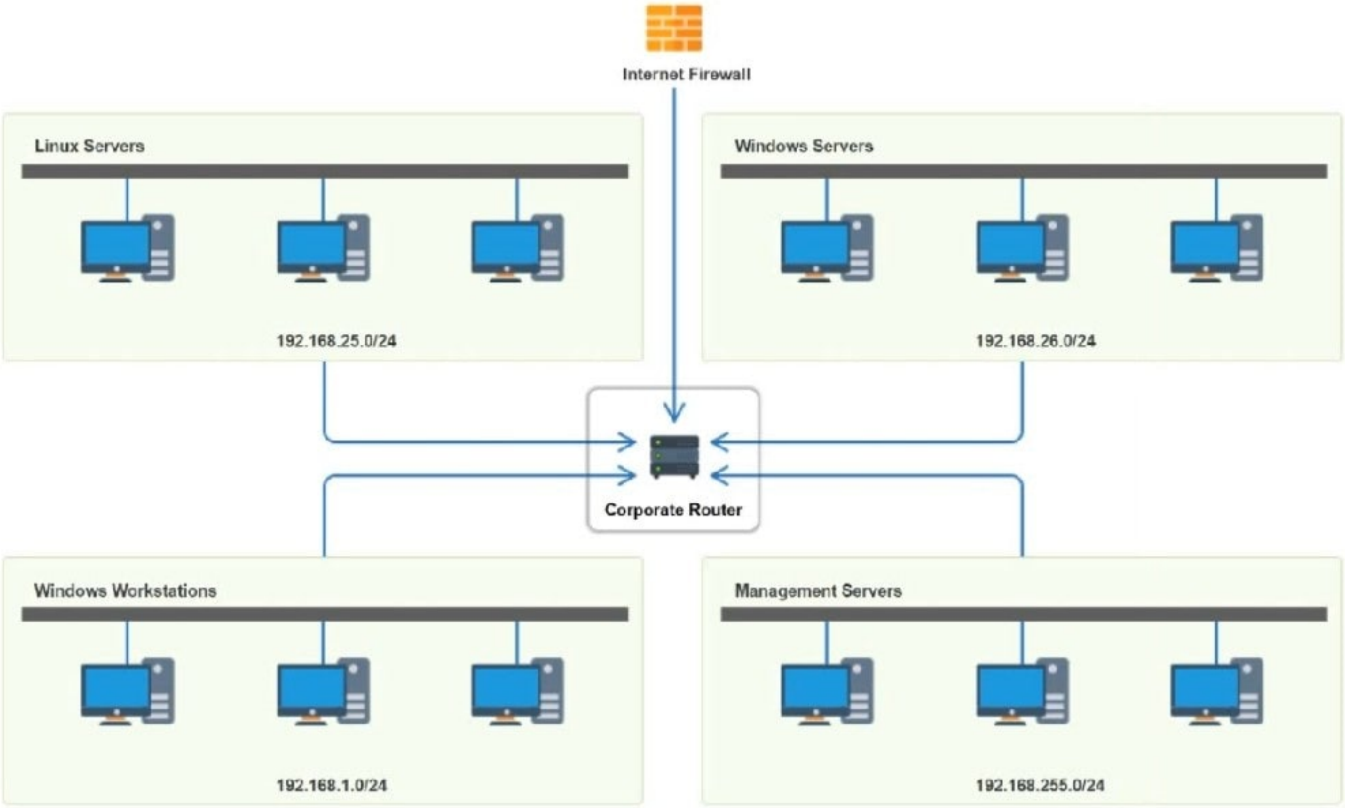
3.

Prohibit any traffic that has not been specifically allowed.

INSTRUCTIONS

Use the drop-downs to complete the ACL

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



A. See the answer and solution below.

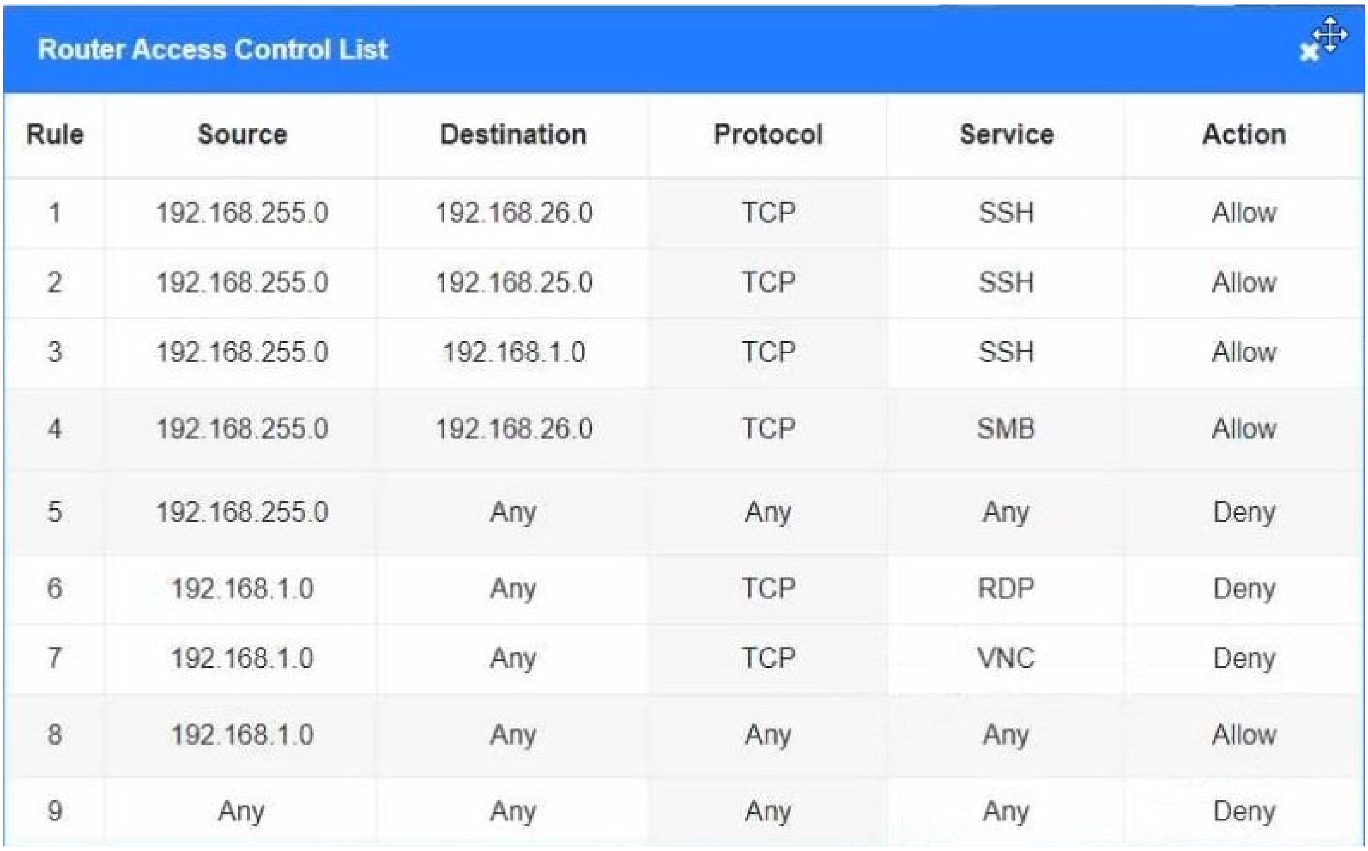
B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

Answer: See the answer and solution below.



Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.255.0	192.168.26.0	TCP	SSH	Allow
2	192.168.255.0	192.168.25.0	TCP	SSH	Allow
3	192.168.255.0	192.168.1.0	TCP	SSH	Allow
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0	Any	TCP	RDP	Deny
7	192.168.1.0	Any	TCP	VNC	Deny
8	192.168.1.0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

QUESTION 4

Users are connected to a switch on an Ethernet interface of a campus router. The service provider is connected to the serial 1 interface on the router. The output of the interfaces is: E1/0: 192.168.8.1/24 S1: 192.168.7.252/30

After router and device configurations are applied, internet access is not possible. Which of the following is the most likely cause?

A. The Ethernet interface was configured with an incorrect IP address.

B. The router was configured with an incorrect loopback address.

C. The router was configured with an incorrect default gateway.

D. The serial interface was configured with the incorrect subnet mask.

Correct Answer: D

QUESTION 5

Which of the following are environmental factors that should be considered when installing equipment in a building? (Select two).

A. Fire suppression system

B. UPS location

C. Humidity control

D. Power load

E. Floor construction type

F. Proximity to nearest MDF

Correct Answer: A

When installing equipment in a building, environmental factors are critical to ensure the safety and longevity of the equipment. A fire suppression system is essential to protect the equipment from fire hazards. Humidity control is crucial to prevent moisture-related damage, such as corrosion and short circuits, which can adversely affect electronic components. Both factors are vital for maintaining an optimal environment for networking equipment.References: CompTIA Network

+ study materials.

QUESTION 6

A network administrator for a small office is adding a passive IDS to its network switch for the purpose of inspecting network traffic. Which of the following should the administrator use?

A. SNMP trap

B. Port mirroring

C. Syslog collection

D. API integration

Correct Answer: B

Port mirroring, also known as SPAN (Switched Port Analyzer), is used to send a copy of network packets seen on one switch port (or an entire VLAN) to another port where the IDS is connected. This allows the IDS to passively inspect network traffic without interfering with the actual traffic flow. Port mirroring is an essential feature for implementing IDS in a network for traffic analysis and security monitoring.References: CompTIA Network+ study materials.

QUESTION 7

Which of the following technologies are X.509 certificates most commonly associated with?

A. PKI

B. VLAN tagging

C. LDAP

D. MFA

Correct Answer: A

X.509 certificates are most commonly associated with Public Key Infrastructure (PKI). These certificates are used for a variety of security functions, including digital signatures, encryption, and authentication. PKI: X.509 certificates are a

fundamental component of PKI, used to manage encryption keys and authenticate users and devices. Digital Certificates: They are used to establish secure communications over networks, such as SSL/TLS for websites and secure email

communication. Authentication and Encryption: X.509 certificates provide the means to securely exchange keys and verify identities in various applications, ensuring data integrity and confidentiality.

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Covers PKI and the role of X.509 certificates in network security.

Cisco Networking Academy: Provides training on PKI, certificates, and secure communications.

Network+ Certification All-in-One uide: Explains PKI, X.509 certificates, and their applications in securing network communications.

QUESTION 8

Which of the following requires network devices to be managed ustng a different set of IP addresses?

A. Console

B. Split tunnel

C. Jump box

D. Out of band

Correct Answer: D

Out of band management is a process for accessing and managing network devices and infrastructure at remote locations through a separate management plane from the production network. Out of band management requires network devices to be managed using a different set of IP addresses than the ones used for in-band management or data traffic. This provides a secure and dedicated alternate access method to administer connected devices and IT assets without using the corporate LAN.

QUESTION 9

Which of the following attacks utilizes a network packet that contains multiple network tags?

A. MAC flooding

B. VLAN hopping

C. DNS spoofing

D. ARP poisoning

Correct Answer: B

QUESTION 10

Which of the following disaster recovery metrics describes the average length of time a piece of equipment can be expected to operate normally?

A. RPO

B. RTO

C. MTTR

D. MTBF

Correct Answer: D

MTBF is the disaster recovery metric that describes the average length of time a piece of equipment can be expected to operate normally. MTBF stands for mean time between failures, which is a measure of the reliability and availability of a device or system. MTBF is calculated by dividing the total operating time by the number of failures that occurred during that time. MTBF indicates how often a device or system fails and how long it can run without interruption. A higher MTBF means a lower failure rate and a longer operational life span.

QUESTION 11

A network administrator needs to divide 192.168.1.0/24 into two equal halves. Which of the following subnet masks should the administrator use?

A. 255.255.0.0

B. 255.255.254.0

C. 255.255.255.0

D. 255.255.255.128

Correct Answer: D

Understanding Subnetting:

uk.co.certification.simulator.questionpool.PList@37532e05 Calculating Subnet Mask:

Verification:

Comparison with Other Options:

References:

CompTIA Network+ study materials on subnetting and IP addressing.

QUESTION 12

A customer connects a firewall to an ISP router that translates traffic destined for the internet. The customer can connect to the internet but not to the remote site. Which of the following will verify the status of NAT?

A. tcpdump

B. nmap

C. ipconfig

D. tracert

Correct Answer: A

tcpdump is a command-line tool that can capture and analyze network traffic on a given interface. tcpdump can verify the status of NAT by showing the source and destination IP addresses of the packets before and after they pass through the ISP router that translates traffic destined for the internet. tcpdump can also show the NAT protocol and port numbers used by the router. nmap, ipconfig, and tracert are not suitable tools for verifying the status of NAT, as they do not show the IP address translation process.

QUESTION 13

Which of the following is the most accurate NTP time source that is capable of being accessed across a network connection?

A. Stratum 0 device

B. Stratum 1 device

C. Stratum 7 device

D. Stratum 16 device

Correct Answer: B

NTP (Network Time Protocol) is a protocol that synchronizes the clocks of network devices with a reference time source. NTP uses a hierarchical system of time sources, called strata, to distribute the time information. A stratum 0 device is

the most accurate time source, such as an atomic clock or a GPS receiver, but it is not directly accessible across a network connection. A stratum 1 device is a network device that is directly connected to a stratum 0 device, such as a

dedicated NTP server or a router with a GPS antenna, and it acts as a primary time server for other network devices. A stratum 2 device is a network device that synchronizes its time with a stratum 1 device, and so on. The higher the stratum

number, the lower the accuracy and reliability of the time source. A stratum 16 device is a network device that has no valid time source and is considered unsynchronized.

References:

Part 1 of current page talks about how Bing is your AI-powered copilot for the web and provides various examples of how it can help you with different tasks, such as writing a joke, creating a table, or summarizing research. However, it does

not mention anything about NTP or time sources.

Part 2 of current page shows the search results for "ai powered search bing chat", which include web, image, and news results. However, none of these results seem to be relevant to the question, as they are mostly about Bing\\'s features,

products, or announcements, not about NTP or time sources.

Therefore, I cannot find the answer or the explanation from the current page. I have to use my own knowledge and information from other sources to verify the answer and provide a short but comprehensive explanation. I will cite these

sources using numerical references.

: CompTIA Network+ Certification Exam Objectives, Version 8.0, Domain 2.0:

Infrastructure, Objective 2.5: Given a scenario, implement network time synchronization, Subobjective 2.5.1: NTP, https://www.comptia.jp/pdf/comptia- network-n10-008-exam-objectives.pdf : Network Time Protocol (NTP), https://

www.cisco.com/c/en/us/about/press/internet-protocol-journal/back- issues/table-contents-58/154-ntp.html

: How NTP Works, https://www.meinbergglobal.com/english/info/ntp.htm

QUESTION 14

HOTSPOT

You have been tasked with implementing an ACL on the router that will:

1.

Permit the most commonly used secure remote access technologies from the management network to all other local network segments.

2.

Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.

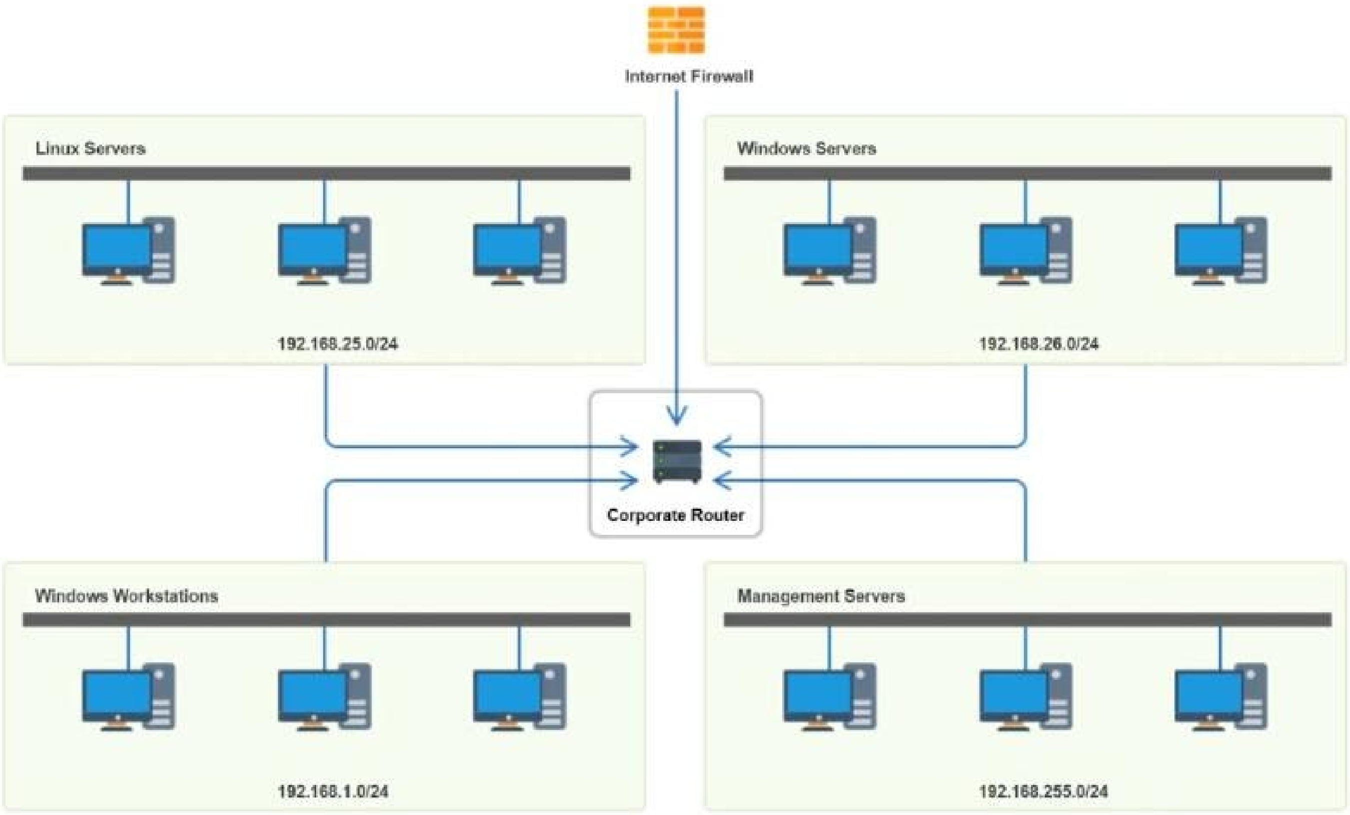
3.

Prohibit any traffic that has not been specifically allowed.

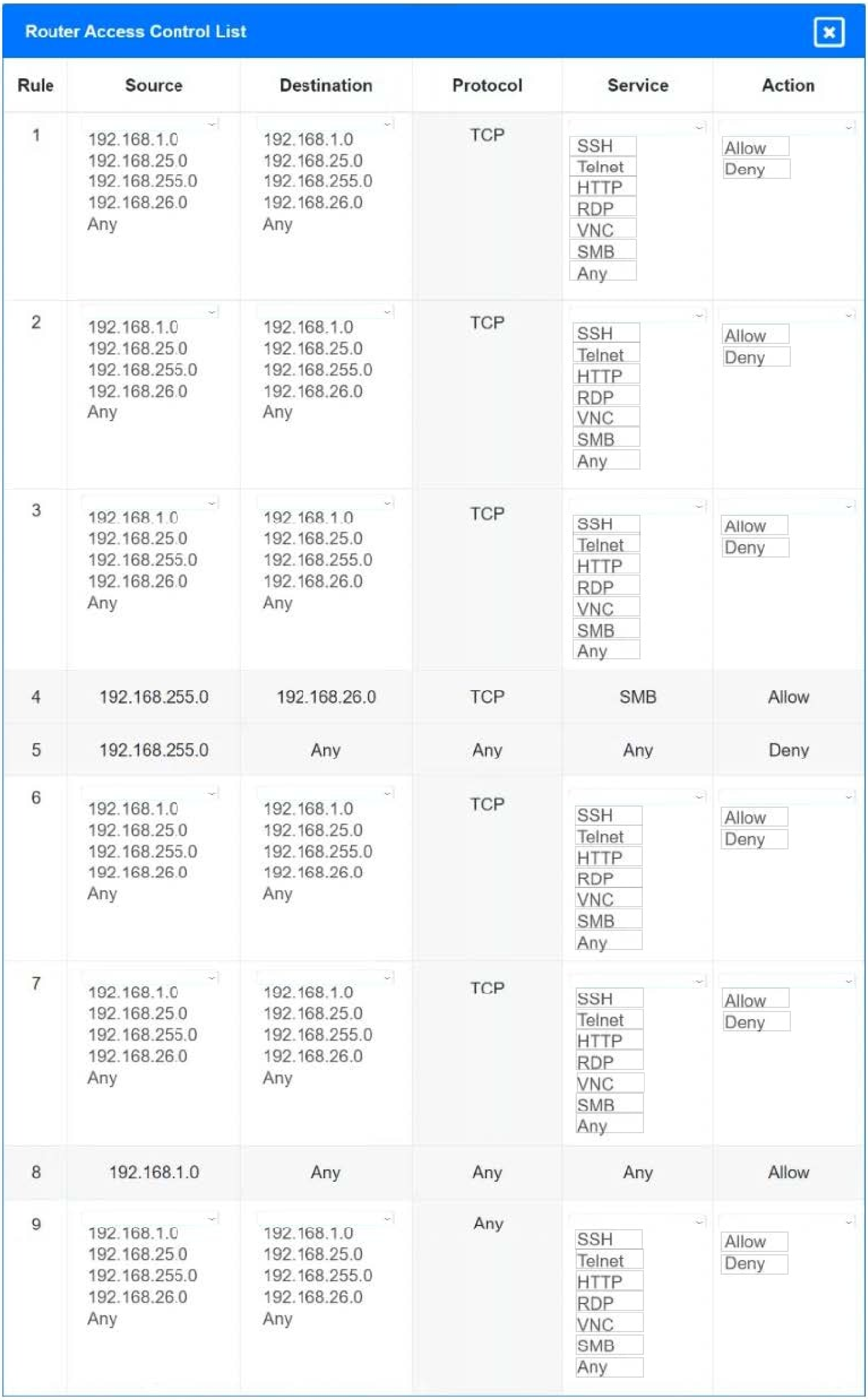
INSRUCTIONS

Use the drop-downs to complete the ACL.

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


Internet Firewall
Linux Servers
192.168.25.0/24
Windows Servers
192.168.26.0/24
Corporate Router
Windows Workstations
192.168.1.0/24
Management Servers
192.168.255.0/24

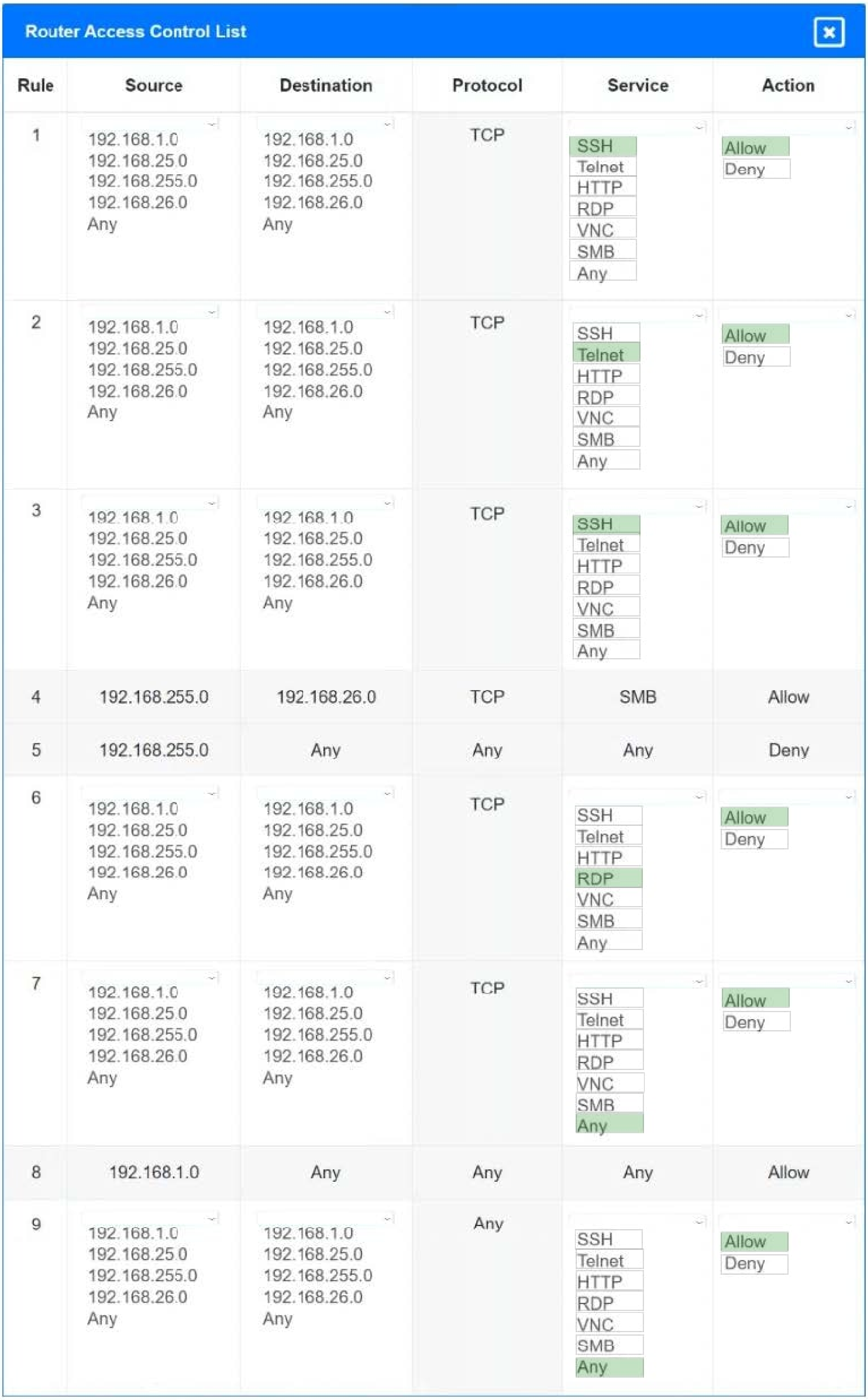
Hot Area:



Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny

Correct Answer:



Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	[✓ SSH] Telnet HTTP RDP VNC SMB Any	[✓ Allow] Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH [✓ Telnet] HTTP RDP VNC SMB Any	[✓ Allow] Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	[✓ SSH] Telnet HTTP RDP VNC SMB Any	[✓ Allow] Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP [✓ RDP] VNC SMB Any	[✓ Allow] Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB [✓ Any]	[✓ Allow] Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB [✓ Any]	[✓ Allow] Deny

QUESTION 15

A critical infrastructure switch is identified as end-of-support. Which of the following is the best next step to ensure security?

A. Apply the latest patches and bug fixes.

B. Decommission and replace the switch.

C. Ensure the current firmware has no issues.

D. Isolate the switch from the network.

Correct Answer: B

Understanding End-of-Support:

uk.co.certification.simulator.questionpool.PList@7662a7f2 Risks of Keeping an End-of-Support Device:

Best Next Step - Replacement:

Comparison with Other Options:

References:

CompTIA Network+ study materials on network maintenance and security best practices.

N10-009 Practice Test N10-009 Exam Questions N10-009 Braindumps