



# RC0-501<sup>Q&As</sup>

CompTIA Security+ Recertification Exam

## Pass CompTIA RC0-501 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/rc0-501.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



**QUESTION 1**

An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient. Which of the following capabilities would be MOST appropriate to consider implementing in response to the new requirement?

- A. Transitive trust
- B. Symmetric encryption
- C. Two-factor authentication
- D. Digital signatures
- E. One-time passwords

Correct Answer: D

---

**QUESTION 2**

A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system. Which of the following methods should the security administrator select the best balances security and efficiency?

- A. Temporarily permit outbound internet access for the pac so desktop sharing can be set up
- B. Have the external vendor come onsite and provide access to the PACS directly
- C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing
- D. Set up a web conference on the administrator's pc; then remotely connect to the pac

Correct Answer: C

---

**QUESTION 3**

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

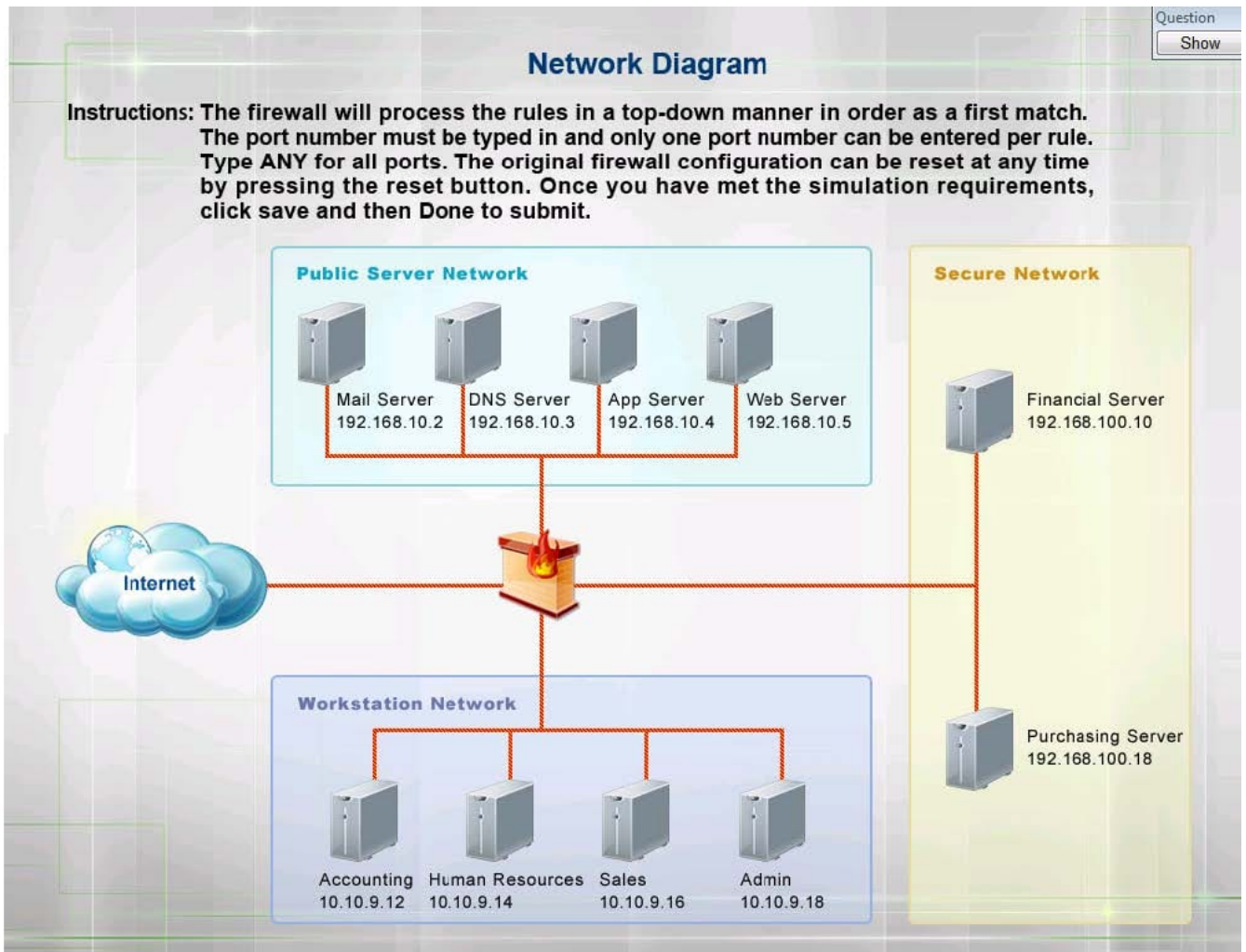
3.



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. 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.





Firewall Rules						
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action	
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

Hot Area:



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

Correct Answer:





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



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

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 and 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](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

#### QUESTION 4

A company wants to host a publicity available server that performs the following functions:

Evaluates MX record lookup

Can perform authenticated requests for A and AAA records Uses RRSIG

Which of the following should the company use to fulfill the above requirements?

- A. LDAPS
- B. DNSSEC
- C. SFTP
- D. nslookup
- E. dig

Correct Answer: A

#### QUESTION 5



A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

- A. LDAP services
- B. Kerberos services
- C. NTLM services
- D. CHAP services

Correct Answer: B

Only Kerberos that can do Mutual Auth and Delegation. <https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authenticationoverview>

[Latest RC0-501 Dumps](#)

[RC0-501 Practice Test](#)

[RC0-501 Study Guide](#)