# RC0-C02$^{\text{Q\&As}}$

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

## Pass CompTIA RC0-C02 Exam with 100% Guarantee

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

**QUESTION 1**

A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?

A. Insider threat

B. Network reconnaissance

C. Physical security

D. Industrial espionage

Correct Answer: C

If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office door. However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security. Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

**QUESTION 2**

ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).

A. Establish a list of users that must work with each regulation

B. Establish a list of devices that must meet each regulation

C. Centralize management of all devices on the network

D. Compartmentalize the network

E. Establish a company framework

F. Apply technical controls to meet compliance with the regulation

Correct Answer: BDF

Payment card industry (PCI) compliance is adherence to a set of specific security standards that were developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.

There are six main requirements for PCI compliance. The vendor must:

Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

To achieve PCI and SOX compliance you should:

Establish a list of devices that must meet each regulation. List all the devices that contain the sensitive data.

Compartmentalize the network. Compartmentalize the devices that contain the sensitive data to form a security boundary.

Apply technical controls to meet compliance with the regulation. Secure the data as required.

**QUESTION 3**

The Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router\\'s external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company\\'s external router\\'s IP which is 128.20.176.19:

11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 1400 11:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 1400 11:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 1400 11:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 1400 11:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400 Which of the following describes the findings the senior security engineer should report to the ISO and the BEST solution for service restoration?

A. After the senior engineer used a network analyzer to identify an active Fraggle attack, the company\\'s ISP should be contacted and instructed to block the malicious packets.

B. After the senior engineer used the above IPS logs to detect the ongoing DDOS attack, an IPS filter should be enabled to block the attack and restore communication.

C. After the senior engineer used a mirror port to capture the ongoing amplification attack, a BGP sinkhole should be configured to drop traffic at the source networks.

D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company\\'s external router to block incoming UDP port 19 traffic.

Correct Answer: A

The exhibit displays logs that are indicative of an active fraggle attack. A Fraggle attack is similar to a smurf attack in that it is a denial of service attack, but the difference is that a fraggle attack makes use of ICMP and UDP ports 7 and 19. Thus when the senior engineer uses a network analyzer to identify the attack he should contact the company\\'s ISP to block those malicious packets.

**QUESTION 4**

The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The following information is compiled: Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0 Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0 Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0 All callers are connected to the same switch and are routed by a router with five built-in interfaces. The upstream router interface\\'s MAC is 00-01-42-32-ab-1a A packet capture shows the following: 09:05:15.934840 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a) 09:06:16.124850 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a) 09:07:25.439811 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a) 09:08:10.937590 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2305, seq 1, length 65534 09:08:10.937591 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2306, seq 2, length 65534 09:08:10.937592 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2307, seq 3, length 65534 Which of the following is occurring on the network?

A. A man-in-the-middle attack is underway on the network.

B. An ARP flood attack is targeting at the router.

C. The default gateway is being spoofed on the network.

D. A denial of service attack is targeting at the router.

Correct Answer: D

The above packet capture shows an attack where the attacker is busy consuming your resources (in this case the router) and preventing normal use. This is thus a Denial Of Service Attack.

**QUESTION 5**

A system worth $100,000 has an exposure factor of eight percent and an ARO of four. Which of the following figures is the system\\'s SLE?

A. $2,000

B. $8,000

C. $12,000

D. $32,000

Correct Answer: B

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF) SLE = AV x EF = $100 000 x 8% = $ 8 000

References:

http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment

**QUESTION 6**

A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization\\'s customer database. The database will be accessed by both the company\\'s users and its customers. The procurement department has asked what security activities must be performed for the deal to proceed.

Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).

A. Physical penetration test of the datacenter to ensure there are appropriate controls.

B. Penetration testing of the solution to ensure that the customer data is well protected.

C. Security clauses are implemented into the contract such as the right to audit.

D. Review of the organizations security policies, procedures and relevant hosting certifications.

E. Code review of the solution to ensure that there are no back doors located in the software.

Correct Answer: CD

Due diligence refers to an investigation of a business or person prior to signing a contract. Due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance. Due diligence should verify the data supplied in the RFP and concentrate on the following: Company profile, strategy, mission, and reputation Financial status, including reviews of audited financial statements Customer references, preferably from companies that have outsourced similar processes Management qualifications, including criminal background checks Process expertise, methodology, and effectiveness Quality initiatives and certifications Technology, infrastructure stability, and applications Security and audit controls Legal and regulatory compliance, including any outstanding complaints or litigation Use of subcontractors Insurance Disaster recovery and business continuity policies

C and D form part of Security and audit controls.

**QUESTION 7**

Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the proprietary web application before launch. Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of the company\\'s purchased application? (Select TWO).

A. Code review

B. Sandbox

C. Local proxy

D. Fuzzer

E. Port scanner

Correct Answer: CD

C: Local proxy will work by proxying traffic between the web client and the web server. This is a tool that can be put to good effect in this case.

D: Fuzzing is another form of blackbox testing and works by feeding a program multiple input iterations that are specially written to trigger an internal error that might indicate a bug and crash it.

**QUESTION 8**

Several business units have requested the ability to use collaborative web-based meeting places with third party vendors. Generally these require user registration, installation of client-based ActiveX or Java applets, and also the ability for the user to share their desktop in read-only or read-write mode. In order to ensure that information security is not compromised, which of the following controls is BEST suited to this situation?

A. Disallow the use of web-based meetings as this could lead to vulnerable client-side components being installed, or a malicious third party gaining read-write control over an internal workstation.

B. Hire an outside consultant firm to perform both a quantitative and a qualitative risk- based assessment. Based on the outcomes, if any risks are identified then do not allow web-based meetings. If no risks are identified then go forward and allow for these meetings to occur.

C. Allow the use of web-based meetings, but put controls in place to ensure that the use of these meetings is logged and tracked.

D. Evaluate several meeting providers. Ensure that client-side components do not introduce undue security risks. Ensure that the read-write desktop mode can either be prevented or strongly audited.

Correct Answer: D

**QUESTION 9**

A Security Manager is part of a team selecting web conferencing systems for internal use. The system will only be used for internal employee collaboration. Which of the following are the MAIN concerns of the security manager? (Select THREE).

A. Security of data storage

B. The cost of the solution

C. System availability

D. User authentication strategy

E. PBX integration of the service

F. Operating system compatibility

Correct Answer: ACD

**QUESTION 10**

Ann, a systems engineer, is working to identify an unknown node on the corporate network. To begin her investigative work, she runs the following nmap command string: user@hostname:~$ sudo nmap ? 192.168.1.54 Based on the output, nmap is unable to identify the OS running on the node, but the following ports are open on the device: TCP/22 TCP/111 TCP/512-514 TCP/2049 TCP/32778 Based on this information, which of the following operating systems is MOST likely running on the unknown node?

A. Linux

B. Windows

C. Solaris

D. OSX

Correct Answer: C

TCP/22 is used for SSH; TCP/111 is used for Sun RPC; TCP/512-514 is used by CMD like exec, but automatic authentication is performed as with a login server, etc. These are all ports that are used when making use of the Sun Solaris operating system.

**QUESTION 11**

A company decides to purchase commercially available software packages. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?

A. Commercially available software packages are typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.

B. Commercially available software packages are often widely available. Information concerning vulnerabilities is often kept internal to the company that developed the software.

C. Commercially available software packages are not widespread and are only available in limited areas. Information concerning vulnerabilities is often ignored by business managers.

D. Commercially available software packages are well known and widely available. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

Correct Answer: B

Commercially available software packages are often widely available. Huge companies like Microsoft develop software packages that are widely available and in use on most computers. Most companies that develop commercial software make their software available through many commercial outlets (computer stores, online stores etc). Information concerning vulnerabilities is often kept internal to the company that developed the software. The large companies that develop commercial software packages are accountable for the software. Information concerning vulnerabilities being made available could have a huge financial cost to the company in terms of loss of reputation and lost revenues. Information concerning vulnerabilities is often kept internal to the company at least until a patch is available to fix the vulnerability.

**QUESTION 12**

Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP address. The company uses the following internal IP address ranges:

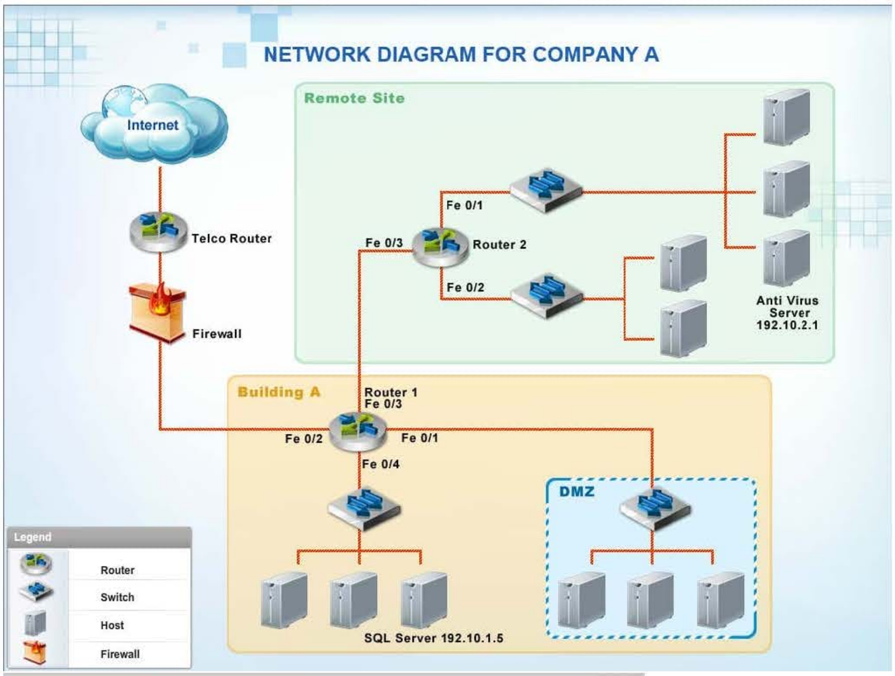
192.10.1.0/24 for the corporate site and 192.10.2.0/24 for the remote site. The Telco router interface uses the 192.10.5.0/30 IP range.

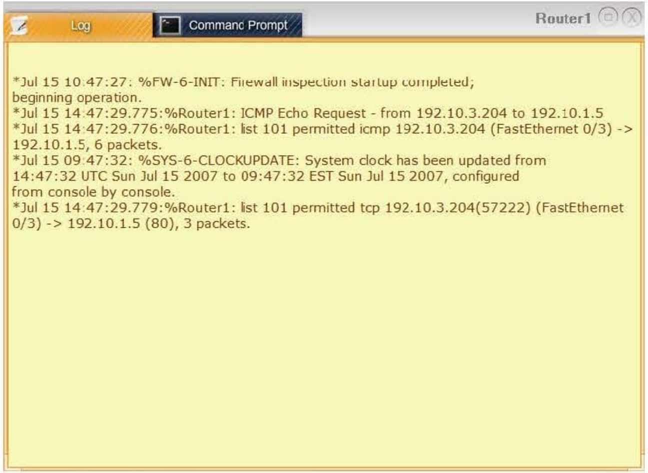
Instructions: Click on the simulation button to refer to the Network Diagram for Company A.

Click on Router 1, Router 2, and the Firewall to evaluate and configure each device.

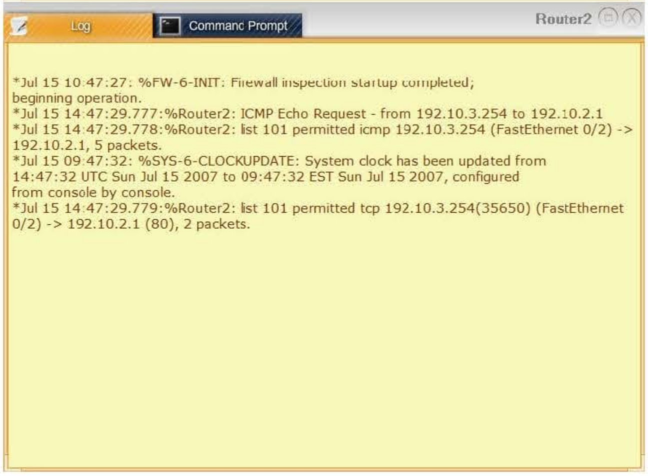
Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.

Task 2: Reconfigure the appropriate devices to prevent the attacks from continuing to target the SQL server and other servers on the corporate network.

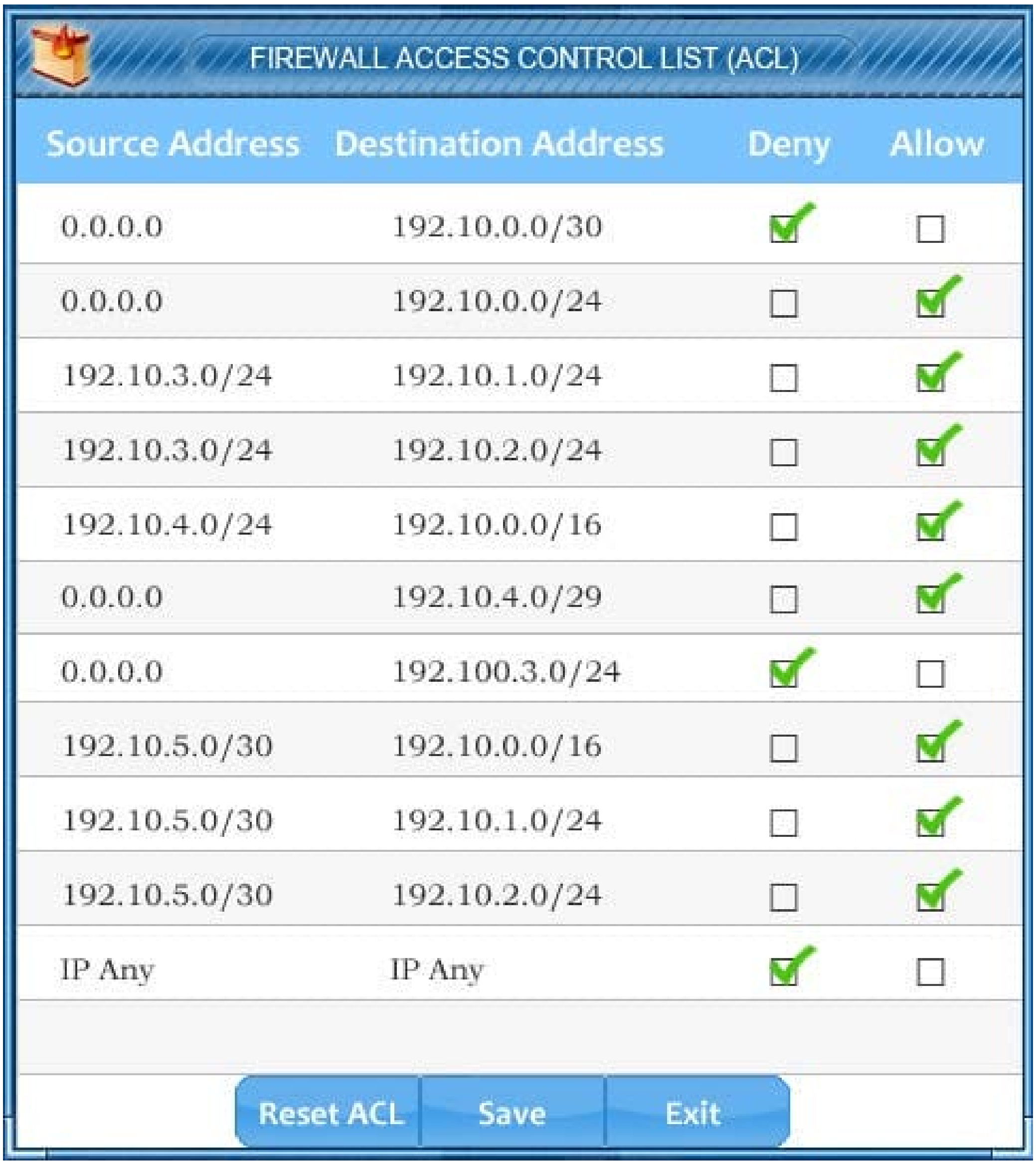




```
*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29.775:%Router1: ICMP Echo Request - from 192.10.3.204 to 192.10.1.5
*Jul 15 14:47:29.776:%Router1: list 101 permitted icmp 192.10.3.204 (FastEthernet 0/3) ->
192.10.1.5, 6 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router1: list 101 permitted tcp 192.10.3.204(57222) (FastEthernet
0/3) -> 192.10.1.5 (80), 3 packets.
```

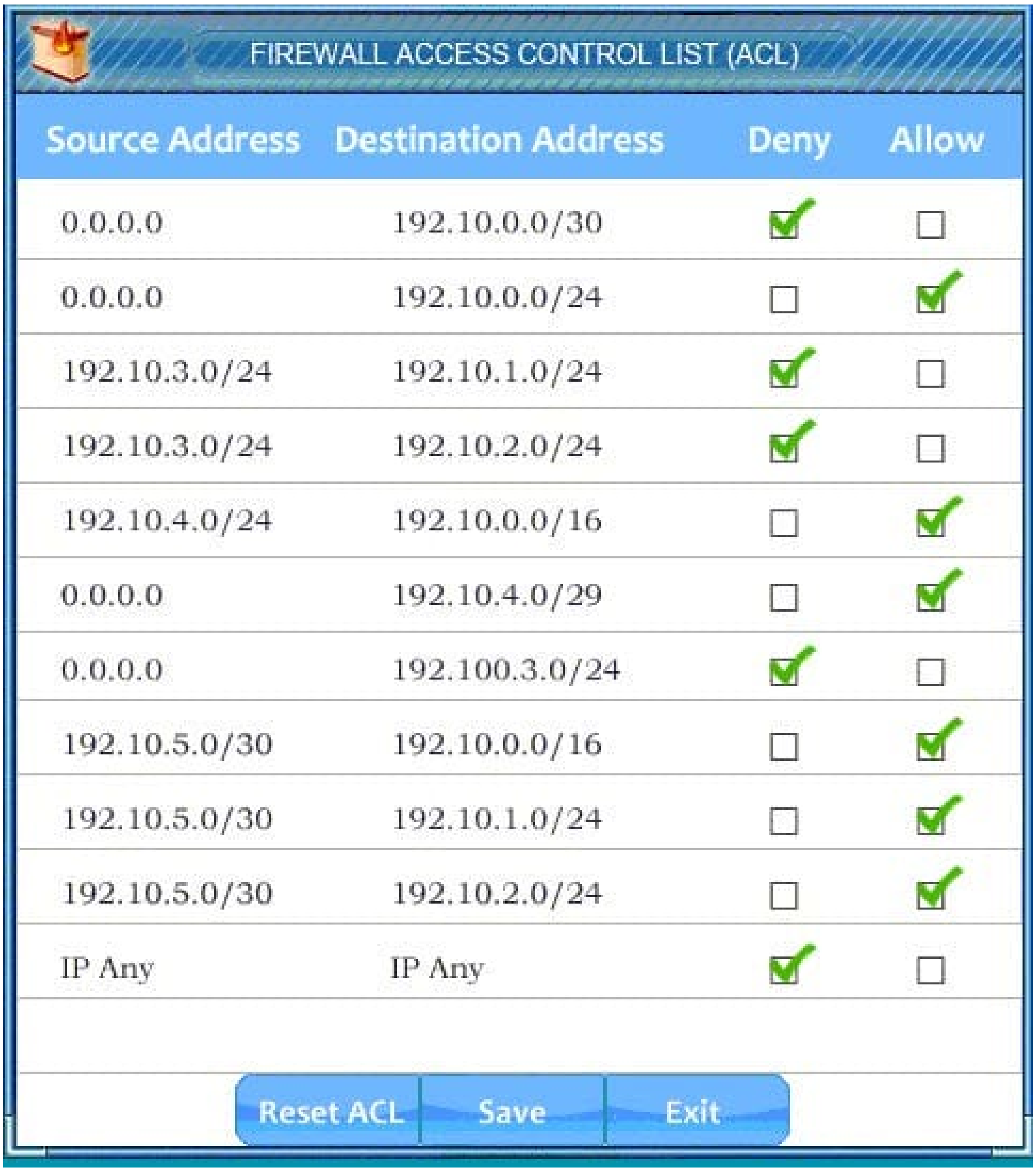


```
*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29.777:%Router2: ICMP Echo Request - from 192.10.3.254 to 192.10.2.1
*Jul 15 14:47:29.778:%Router2: list 101 permitted icmp 192.10.3.254 (FastEthernet 0/2) ->
192.10.2.1, 5 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router2: list 101 permitted tcp 192.10.3.254(35650) (FastEthernet
0/2) -> 192.10.2.1 (80), 2 packets.
```



| Source Address | Destination Address | Deny | Allow |
|---|---|---|---|
| 0.0.0.0 | 192.10.0.0/30 | ☑ | □ |
| 0.0.0.0 | 192.10.0.0/24 | □ | ☑ |
| 192.10.3.0/24 | 192.10.1.0/24 | □ | ☑ |
| 192.10.3.0/24 | 192.10.2.0/24 | □ | ☑ |
| 192.10.4.0/24 | 192.10.0.0/16 | □ | ☑ |
| 0.0.0.0 | 192.10.4.0/29 | □ | ☑ |
| 0.0.0.0 | 192.100.3.0/24 | ☑ | □ |
| 192.10.5.0/30 | 192.10.0.0/16 | □ | ☑ |
| 192.10.5.0/30 | 192.10.1.0/24 | □ | ☑ |
| 192.10.5.0/30 | 192.10.2.0/24 | □ | ☑ |
| IP Any | IP Any | ☑ | □ |

Correct Answer:



| Source Address | Destination Address | Deny | Allow |
|---|---|---|---|
| 0.0.0.0 | 192.10.0.0/30 | ☑ | □ |
| 0.0.0.0 | 192.10.0.0/24 | □ | ☑ |
| 192.10.3.0/24 | 192.10.1.0/24 | ☑ | □ |
| 192.10.3.0/24 | 192.10.2.0/24 | ☑ | □ |
| 192.10.4.0/24 | 192.10.0.0/16 | □ | ☑ |
| 0.0.0.0 | 192.10.4.0/29 | □ | ☑ |
| 0.0.0.0 | 192.100.3.0/24 | ☑ | □ |
| 192.10.5.0/30 | 192.10.0.0/16 | □ | ☑ |
| 192.10.5.0/30 | 192.10.1.0/24 | □ | ☑ |
| 192.10.5.0/30 | 192.10.2.0/24 | □ | ☑ |
| IP Any | IP Any | ☑ | □ |

We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.30.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:

**QUESTION 13**

An insurance company is looking to purchase a smaller company in another country. Which of the following tasks would the security administrator perform as part of the security due diligence?

A. Review switch and router configurations

B. Review the security policies and standards

C. Perform a network penetration test

D. Review the firewall rule set and IPS logs

Correct Answer: B

IT security professionals should have a chance to review the security controls and practices of a company targeted for acquisition. Any irregularities that are found should be reported to management so that expenses and concerns are properly identified.

**QUESTION 14**

A company is deploying a new iSCSI-based SAN. The requirements are as follows:

SAN nodes must authenticate each other.

Shared keys must NOT be used.

Do NOT use encryption in order to gain performance.

Which of the following design specifications meet all the requirements? (Select TWO).

A. Targets use CHAP authentication

B. IPSec using AH with PKI certificates for authentication

C. Fiber channel should be used with AES

D. Initiators and targets use CHAP authentication

E. Fiber channel over Ethernet should be used

F. IPSec using AH with PSK authentication and 3DES

G. Targets have SCSI IDs for authentication

Correct Answer: BD

CHAP (Challenge Handshake Authentication Protocol) is commonly used for iSCSI authentication.

Initiators and targets both using CHAP authentication is known as mutual CHAP authentication.

Another option is to use IPSec using AH with PKI certificates for authentication. One of the two core security protocols in IPSec is the Authentication Header (AH). This is another protocol whose name has been well chosen: AH is a protocol

that provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram. We can use PKI certificates for authentication rather than shared keys.

**QUESTION 15**

A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production. Which of the following development methodologies is the team MOST likely using now?

A. Agile

B. Waterfall

C. Scrum

D. Spiral

Correct Answer: B