Table of Contents

[Introduction 2](#_Toc194326832)

[Discussion Solutions 2](#_Toc194326833)

[Conclusion 11](#_Toc194326834)

[References 11](#_Toc194326835)

# Introduction

In this task, we will be improving Acme's network security for their Southampton and Newbury offices .To do this I have implemented network improvement using packet tracer Our aim is to meet and achieve the company's requirements by focusing on key aspects of security, including user authentication, network device security, time synchronization, secure network traffic, and secure connections between sites as (Portnox, 2025) highlights, the needs for keeping data safe with encryption, and protecting against threats from within the network and securing data through encryption are critical to preventing unauthorized access and maintaining compliance. (Portnox, 2025) which I will be discussing about some of commands further below .

# Discussion Solutions

As for Figure 1 Implementing SSH with the commands crypto key generate rsa and figure 1.1 ip ssh version 2 sets up a secure, encrypted channel for remote device management. This encryption ensures that all communications between network devices and administrators are safeguarded against eavesdropping and man-in-the-middle attacks, directly enhancing network security as required by Acme's first and fourth security requirements. According to  (McAfee, 2025) using SSH version 2 is essential for preventing unauthorized access and ensuring data integrity across financial networks(McAfee, 2025)

Figure 1 commands to create RSA Key Generation for Secure Device Authentication on Southampton Router

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 1.1 Enabling SSH Version 2 for Secure Remote Access on Southampton router

A screenshot of a computer program

AI-generated content may be incorrect.

The following commands in figure 1.2 configured on the Southampton router for Acme aim to protect the network devices used by Acme Corporation from unauthorized access and potential security threats. Password protection is applied using encrypted values to secure both local and remote access, ensuring that only approved users can manage the router. By enforcing a minimum password length and blocking login attempts after repeated failures, Acme can add another layer of according to (Basic Security Configuration, n.d)defense against password guessing and brute-force attacks. (Basic Security Configuration, n.d) According to(Kanade, 2023)Secure remote access is set up using SSH, which encrypts all communication between administrators and the device. This prevents sensitive information such as usernames and commands from being intercepted over the network. (Kanade, 2023) By enforcing a minimum password length of around 4 characters and employing a login block mechanism, as demonstrated in the provided configuration commands, Acme can add another layer of defense against password guessing and brute-force attacks. The security passwords min-length 12 and login block-for 60 attempts 3 within 60 commands, when implemented, restrict password access to only those who meet the complexity requirements. These measures directly support Requirement 1 by establishing strong security controls on the router, and Requirement 2 by ensuring only authorized users can log in using their own usernames and passwords. In addition, limited user roles are created using privilege levels, allowing specific staff members to perform tasks such as restarting the router without giving them full control.

Figure 1.2

Configuring authentication and login protection on Southampton router  
A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

To meet Acme Company’s requirement 3 that all network events are logged on central servers, These commands in figure 2 configures the routers at Southampton and Newbury to send all log messages to the specified IP addresses, which are the Syslog servers at each site according to (Security, 2022) This ensures that all significant system and network events, such as login attempts, configuration changes, and system errors, are centrally collected and stored. (Security, 2022)Centralizing log data helps Acme's network security team quickly analyse and respond to potential security incidents. Based on the research (National Cyber Security Centre, n.d.) By having access to detailed logs, the team can detect patterns of malicious activity or operational problems much faster. (National Cyber Security Centre, n.d.) This is crucial for maintaining the integrity and availability of network resources, especially in environments dealing with sensitive financial and insurance information. This directly supports Requirement 3 from the case study, ensuring that all events are logged on a central (National Cyber Security Centre, n.d.) server for better as per the oversight and auditability. (National Cyber Security Centre, n.d.)

Figure 2

Commands for centralized syslog logging for event monitoring on Acme routers for Soton

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

As for figure 2.1 and 2.2 these commands for the ntp server ensures that all network devices across both locations maintain accurate and consistent system time. According to research (Sitechecker, 2023)Time synchronization is essential for ensuring that log entries are consistent across the network, which is critical for troubleshooting and security investigations . (Sitechecker, 2023) (Bodet, 2024)Proper time synchronization ensures that timestamps in security logs are accurate, which is critical when analyzing the events leading up to and following a security incident. According to (Bodet, 2024)This aids in forensic investigations and helps in establishing a precise timeline of events, which is vital for effective security measures. These fulfills Requirement 3 in the case study, enhancing Acme’s ability to synchronize time on network devices and ensuring the logs are accurately timestamped as shown on figure 2.1

Figure 2.1

NTP configuration and synchronization verification on Soton router

A screenshot of a computer

AI-generated content may be incorrect.

Figure 2.2 using ntp command for the server

A screenshot of a computer

AI-generated content may be incorrect.

The SNMP configuration commands for Acme in figure 2.3 and 2.4 address Requirement 6 by securing switches against unauthorized access. By using Access Control Lists and PERMIT-ADMIN, according to research (Priono, 2024)SNMP access is restricted to authorized devices within a specified IP range. These SNMP views and groups limit exposure to sensitive network information, allows only authenticated users to access essential data. (Priono, 2024) .Based on(Cisco, 2024) The use of SNMPv3 with SHA authentication and AES encryption ensures secure management communications, (Cisco, 2024) protecting against data breaches and unauthorized modifications. This is crucial for maintaining network integrity and safeguarding Acme's finance and insurance operations.

Figure 2.3 SNMPv3 Configuration on R1 with ACL-Based Access Control and Encrypted User Authentication

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 2.4 Configuring SNMPv3 User with Authentication and Encrypted Access on R1

A screenshot of a computer

AI-generated content may be incorrect.

Figure 3 of the commands shows to configure a (RADIUS) server specifically named "Southampton” for Acme’s Southampton office. The command radius server Southampton initiates the configuration, clearly naming this RADIUS instance for ease of management and identification. Subsequently, the command based on the research (Microsoft, 2024)address ipv4 192.168.10.1 explicitly defines the IP address of the central RADIUS authentication server. This ensures the router knows exactly where to send authentication requests. (Microsoft, 2024) The key Southampton-key command establishes according to(Adcock, 2023) a shared secret, essential for encrypting communication between the Southampton router for in this case Acme and the RADIUS server, thus protecting sensitive authentication data from interception or unauthorized access. (Adcock, 2023) Implementing these commands directly addresses Acme’s Requirement 2, which mandates centralized administrative authentication. By using a RADIUS server, Acme significantly enhances network security by centralizing user credential management. (McClure, 2024)This mitigates risks associated with manual or individual device configurations, such as inconsistent user accounts or outdated access permissions. (McClure, 2024) .Moreover, encrypted communication between the router and the RADIUS server prevents potential attackers from capturing login credentials, thereby safeguarding against unauthorized administrative access attempts and enhancing overall network security integrity

Figure 3 RADIUS server configuration on Southampton router

A screenshot of a computer error

AI-generated content may be incorrect.

Authentication is handled by the aaa authentication login default group radius local command. According to research (Cisco, 2014)This command configures the system to verify administrative credentials primarily through a central RADIUS server, with a local fallback option if the RADIUS server becomes unreachable. (Cisco, 2014) This approach directly addresses Requirement 2 of Acme's case study, which requires centralized administrative authentication to enhance security and control. In the other hand Authorization is managed through the aaa authorization (Cisco, 2016) exec default group radius command. This setting ensures that once users are authenticated, they can only execute commands or access resources as defined by policies stored on the RADIUS server. (Cisco, 2016) This helps maintain strict operational boundaries, preventing unauthorized activities and directly supporting Requirement 1, which focuses on basic security on routers and switches by enforcing controlled access to device configuration. Accounting is achieved with the aaa accounting exec default start-stop group radius command, which logs detailed information about each user session, from start to finish. (Cisco, 2014)This logging is essential for auditing and security monitoring, facilitating the detection and investigation of any potential security incidents. (Cisco, 2014)It addresses Requirement 3 in part by providing a robust mechanism for event logging, although time synchronization would need to be configured separately to fully meet this requirement.

Figure 3.1 Enabling AAA and configuring radius based Authentication, Authorization and Accounting on Southampton Router

A screenshot of a computer error

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

The commands shown in Figure 4 configure extended access control lists (ACLs) to filter traffic based on IP address and different protocol type. For example, according to (chiradeep-basumallick, 2024) they permit specific traffic between Acme’s internal subnets and deny anything that is not explicitly allowed. (chiradeep-basumallick, 2024) This provides fine-grained control over what data is allowed into or out of the network, helping to enforce security policies. This setup directly supports Requirement 4 as it requires the networks at both sites must be secured by access control lists and firewalls. By using extended ACLs, Acme ensures that only authorized users and systems can communicate, helping prevent unauthorized access and reduce exposure to external threats. According to (Heimdal Security Blog ,2024), ACLs are a critical line of defense against network-based attacks. They also support compliance with data protection regulations, (Heimdal Security Blog ,2024) especially important for a financial and insurance company like Acme

Figure 4 Extended ACLs applied on Southampton Router for Intranet and Newbury Host

A screen shot of a computer

AI-generated content may be incorrect.

These commands set up a Zone-Based Firewall (ZBF) on Acme’s router to control and inspect traffic between different parts of the network. As shown on Figure 5 Zones called NEWBURY1, NEWBURY2, and OUTSIDE are created to separate internal and external traffic. Access rules are defined using ACLs and class maps to match allowed traffic types like TCP, UDP, and ICMP. Policy maps are then used to inspect as shown in Figure 5.1 this traffic, and zone pairs are created to apply these policies between zones, such as from NEWBURY1 to OUTSIDE or from OUTSIDE to NEWBURY2. This setup directly meets requirement 4 from the Acme case study: *“The networks at both sites must be secured by access control lists and firewalls.”* Based on the source *(Cisco, 2014)* It protects Acme’s network by making sure only defined and inspected traffic can flow between zones, blocking anything not explicitly permitted (Cisco, 2014). According to  (Cisco, 2025) This reduces risks like unauthorized access, internal misuse, and attacks from outside the network.  (Cisco, 2025 ) Using ZBF gives Acme better visibility and control over traffic and strengthens the overall security of their infrastructure.

Figure 5 Creation of security zones in Newbury router for zone-based firewall configuration

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 5.1 Commands to create Class Map NEWBURY\_PROTOCOLS to Match TCP, UDP, and ICMP for Traffic

A screenshot of a computer program

AI-generated content may be incorrect.

These commands configure a secure VPN tunnel between Acme’s Newbury and Southampton offices, meeting requirement 5: “A secure encrypted link must be configured between the two sites.” The ISAKMP policy uses AES 256-bit encryption for strong data protection, pre-shared key authentication to ensure only trusted routers can connect, and Diffie-Hellman group 5 to securely exchange encryption keys. This protects Acme’s sensitive financial and customer data from being intercepted or altered during transmission. Once applied, the tunnel can be verified as active using the command (Cisco, 2018) show crypto isakmp sa, confirming that Phase 1 of the VPN is working. This solution aligns with Cisco’s security best practices for IPsec VPNs (Cisco, 2018) and helps Acme meet data security expectations, including protection against man-in-the-middle attacks and compliance with data protection standards

Figure 6.1Configuring ISAKMP policy for VPN setup with AES-256 encryption

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 6.2 crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac configures an IPsec transform set on Acme’s Newbury router. It defines how data will be protected in Phase 2 of the VPN connection with Southampton, using AES for encryption and SHA-HMAC for integrity. This helps Acme secure sensitive data in transit and ensures that it is not tampered with or intercepted. This setup meets requirement 5 by securing the encrypted link between the two offices. Once configured, (Cisco, 2018) the tunnel’s operation can be verified using show crypto ipsec sa, which displays the status of encrypted data flows. This approach follows Cisco’s recommended best practices for securing site-to-site VPNs with IPsec (Cisco, 2018)and provides Acme with strong protection against common threats such as man-in-the-middle attacks and data spoofing.

Figure 6.2 Setting up VPN for encryption

A screenshot of a computer program

AI-generated content may be incorrect.

This command applies the crypto map named VPN-MAP to the router’s outgoing interface at Acme’s Newbury office. This step is essential to activate the VPN configuration and ensure that traffic matching the VPN policy is encrypted and sent securely to the remote site for instance Southampton according to research (Cisco, 2018)without applying the crypto map to the correct interface, the VPN tunnel will not function, even if the rest of the configuration is correct. (Cisco, 2018)This directly supports requirement 5, which is to establish a secure encrypted link between the two offices. By enabling the VPN on the interface, Acme ensures that any sensitive business or customer data sent between the sites is automatically encrypted and protected from interception, fulfilling a key part of their network security plan.

Figure 6.3 Applying crypto map "VPN-MAP" to the interface on Newbury

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 7.3 display command enables DHCP snooping on Acme’s Switch5. (netseccloud.com, 2024) DHCP snooping is a Layer 2 security feature that helps prevent rogue DHCP servers from handing out false IP address information to devices on the network. (netseccloud.com, 2024) By enabling this feature, Acme ensures that only trusted DHCP servers can respond to client requests according to research (ManageEngine, 2025)This helps protect against man-in-the-middle attacks and network disruption, which could occur if an attacker introduces a rogue DHCP server to redirect or intercept traffic. (ManageEngine, 2025) This directly supports requirement 6, which states that *“Switches must be secured against threats on the LAN.”* So according to (netseccloud.com, 2024) Enabling DHCP snooping adds a strong security layer at the access switch level, (netseccloud.com, 2024) helping Acme maintain a more trustworthy and controlled internal network environment

Figure 7.3 Enabling dhcp snooping on Switch5 to prevent rogue dhcp server attacks

A black text on a white background

AI-generated content may be incorrect.

Figure 7.5 of the command ip dhcp snooping trust is applied to a specific interface on Acme’s Switch5 to mark it as trusted for DHCP traffic. This is necessary so that only the legitimate DHCP server, connected to that interface, is allowed to send IP address assignments to devices on the network. All other ports remain untrusted, (Cisco, n.d.) helping block any unauthorized DHCP responses from rogue devices. (Cisco, n.d.) This configuration directly supports because requirement 6 requires to protect the LAN from internal threats. After applying the command, the output of show ip dhcp snooping confirms that DHCP snooping is enabled and that the correct interface is listed as trusted port as you can see in figure 7.5 This shows that Acme’s switch is actively preventing DHCP spoofing attacks and only allowing IP assignments from approved sources, strengthening the internal security of the network.

Figure 7.5 Verifying DHCP Snooping Status by running the show ip dhcp command

A screenshot of a computer program

AI-generated content may be incorrect.

The commands shown on figure 8 configure extended access control lists (ACLs) on Acme’s firewall to control traffic between internal subnets and between sites. The ACL named ACL\_NEWBURY permits TCP traffic between defined network objects NEWBURY2 and NEWBURY3 in both directions. (Aakriti, 2023)These ACLs are then applied to interfaces INSIDE1, INSIDE2 etc using access-group commands, ensuring that the firewall only allows explicitly permitted traffic through each interface. (Aakriti, 2023) This configuration directly supports requirement 4 of the case study: *“The networks at both sites must be secured by access control lists and firewalls.”* By using (learncisco, n.d.)object-based rules and applying them per interface (learncisco, n.d.), Acme can reduce the attack surface and preventing unauthorized access between segments of the network. For instance (Wadhwa, 2024) These ACLs help mitigate risks such as lateral movement by attackers within the LAN, data leakage, and unmonitored access to sensitive systems. (Wadhwa, 2024)

Figure 8 Applying extended access control lists for Newbury and Southampton

A screenshot of a computer program

AI-generated content may be incorrect.

.

# Conclusion

In conclusion, I successfully addressed the requirement of safeguarding Acme's network by implementing various security measures at both the Southampton and Newbury offices. These measures included securing device access through SSH and password policies, managing administrative access with AAA and RADIUS, and utilizing extended ACLs and firewalls to control traffic and prevent unauthorized access. Additionally, I configured an IPsec VPN for secure site-to-site communication, enabled DHCP snooping to mitigate LAN-based threats, and set up NTP and Syslog for time synchronization and centralized event logging. Each solution was tested using verification commands and tailored to meet Acme's unique business needs within the finance and insurance sector.

# References

McAfee (2025). *SSH provides secure access over unsecured networks | McAfee*. [online] McAfee. Available at: <https://www.mcafee.com/learn/defend-your-network-with-secure-shell/>

Security, C.C. for C. (2022). *Network security logging and monitoring - ITSAP.80.085*. [online] Canadian Centre for Cyber Security. Available at: <https://www.cyber.gc.ca/en/guidance/network-security-logging-monitoring-itsap80085>

National Cyber Security Centre (n.d.). *Logging and protective monitoring*. [online] www.ncsc.gov.uk. Available at: <https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/logging-and-protective-monitoring>

Sitechecker. (2023). *What is an NTP Server? Implementation and Practical Use*. [online] Available at: <https://sitechecker.pro/what-is-ntp-server/>.

Bodet (2024). *What solutions are to be implemented for secure synchronisation?* [online] Bodet-time.com. Available at: <https://www.bodet-time.com/resources/blog/1936-best-practices-and-technical-vision-of-ntp.html>

Priono, A. (2024). *SNMP Monitoring: Definitions, Benefits, And Its Difference With SSH - NexaLab Blog*. [online] Nexa Lab. Available at: <https://nexalab.io/blog/what-is-snmp-monitoring/>

Cisco. (2024). *Harden IOS Devices*. [online] Available at: <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#toc-hId--834557961>

Adcock, C. (2023b). *RADIUS vs. TACACS+: A Comparative Breakdown*. [online] Portnox. Available at: <https://www.portnox.com/blog/network-access-control/radius-vs-tacacs-the-complete-breakdown-for-decision-makers/>

Microsoft (2024). *Configure RADIUS Clients*. [online] learn.microsoft.com. Available at: <https://learn.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-radius-clients-configure>

McClure, M. (2024). *What is RADIUS (Remote Authentication Dial-In User Service)?* [online] CBT Nuggets. Available at: <https://www.cbtnuggets.com/blog/technology/networking/what-is-radius>

chiradeep-basumallick (2024). *Access Control Lists: Working, Importance, and Best Practices*. [online] Spiceworks Inc. Available at: <https://www.spiceworks.com/tech/networking/articles/access-control-lists/>

Heimdal Security Blog. (2024). *What Is an Access Control List (ACL)? Definition, Types and Benefits*. [online] Available at: <https://heimdalsecurity.com/blog/what-is-an-access-control-list-acl/>.

Cisco. (2018). *Security for VPNs with IPsec Configuration Guide, Cisco IOS XE Gibraltar 16.10.x - Configuring Security for VPNs with IPsec [Cisco IOS XE Gibraltar 16.10.1]*. [online] Available at: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xe-16-10/sec-sec-for-vpns-w-ipsec-xe-16-10-book/sec-cfg-vpn-ipsec.html>

Cisco (2025). *Zone-Based Policy Firewall Design and Application Guide*. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html>

Cisco. (2014). *Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS XE Release 3S - Zone-Based Policy Firewalls [Support]*. [online] Available at: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book/sec-zone-pol-fw.html>

netseccloud.com (2024). *Why Implement DHCP Snooping? The Crucial Role in Network Security*. [online] Netseccloud.com. Available at: <https://netseccloud.com/implement-dhcp-snooping>

ManageEngine, communications@manageengine.com (2025). Switch Port & IP Address Management Software by ManageEngine OpUtils. [online] ManageEngine OpUtils. Available at: <https://www.manageengine.com/products/oputils/tech-topics/dhcp-snooping.html>

Cisco (n.d.). Configuring DHCP Snooping About DHCP Snooping. [online] Available at: <https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus3548/103x/configuration/security/cisco-nexus-3548-nx-os-security-configuration-guide-103x/m-configuring-dhcp-snooping.pdf>.

Wadhwa, P. (2024). *What Is a Access Control List (ACL)? (Implemention Guide)*. [online] Sprinto. Available at: <https://sprinto.com/blog/access-control-list/>

learncisco (n.d.). *Types of ACL - Standard and Extended ACLs | ICND1 100-105*. [online] www.learncisco.net. Available at: <https://www.learncisco.net/courses/icnd-1/acls-and-nat/type-of-acls.html>

Lab 4.6.1: Basic Security Configuration. (n.d.). Available at: <https://www.goldbeach.org.uk/askgeoff/LSWN/CCNA4/Lab%204.6.1.pdf>

Portnox. (2025). *Different Methods of Device Authentication*. [online] Available at: <https://www.portnox.com/cybersecurity-101/device-authentication/>

Cisco. (2014). Cisco 1000 Series Connected Grid Routers Security Software Configuration Guide - Configuring AAA. [online] Available at: <https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/security/security_Book/sec_aaa_cgr1000.html>

Cisco. (2016). RADIUS Configuration Guide - Configuring RADIUS [Cisco Cloud Services Router 1000V Series]. [online] Available at: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/xe-16/sec-usr-rad-xe-16-book/sec-cfg-radius.html>

‌