# **Corporate Communication Systems Management Spring 2025 Name: Isaac kevin Otchere-Somuah Student ID: P00202902 Module: Corporate Communication Systems Management Module Leader: Chitra Balakrishna Date of Submission: 25 APRIL 2025**

# **Task 1 – Current Network Topology and Configuration**

## Assumptions

- Each subnet has 64 IP addresses, with 62 usable.  
- Internal services (DNS, DHCP, Storage) are hosted at HQ.  
- SO1 accesses the internet via HQ’s WAN and firewall.  
- The web server is hosted in a DMZ for external access.  
- Device quantities are optimized to prevent over-provisioning.  
- All prices were sourced from official vendor websites as of March 2025.

## Task 1a: Network Diagram

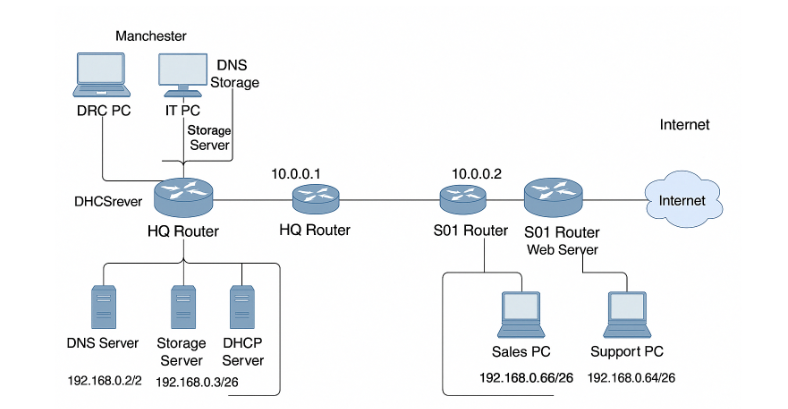
The diagram below illustrates the existing network topology of Old-Leftovers-and-Excesses Ltd (OLX Ltd), showing the infrastructure at the Manchester headquarters (HQ) and the Newcastle sales office (SO1). It includes the IP addressing scheme, major devices such as routers, switches, DHCP/DNS servers, and end-user workstations. Additionally, it depicts the demilitarized zone (DMZ) with the web server, the WAN connection between HQ and SO1, and the ISP access point via HQ.

Figure 1: OLX Ltd Network Topology (HQ, SO1, DMZ, and WAN)

**NB:** I initially tried using Cisco Packet Tracer for this diagram but switched to draw.io due to better support for custom icons. The DMZ representation was particularly challenging to illustrate clearly.

## Task 1b: DHCP Server Configuration

The DHCP servers at each location are responsible for dynamically assigning IP addresses to hosts within their respective subnets. The following table provides an overview of the DHCP configuration for both the Manchester HQ and Newcastle SO1, including network ranges, DHCP pools, and unused address space.

Table 1: DHCP Configuration per Site

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Location | DHCP Server Address | Network Address | Broadcast Address | DHCP Pool Start | DHCP Pool End | Unused Address Range |
| Manchester HQ | 192.168.0.2 | 192.168.0.0 | 192.168.0.63 | 192.168.0.10 | 192.168.0.50 | 192.168.0.51 – 192.168.0.62 |
| Newcastle SO1 | 192.168.0.66 | 192.168.0.64 | 192.168.0.127 | 192.168.0.74 | 192.168.0.114 | 192.168.0.115 – 192.168.0.126 |

## Task 1c: Network Devices and Cost Analysis

Based on the current network design, the following table lists the core hardware components deployed at HQ and SO1. This includes routers, switches, PCs, servers, and networking cables. Vendor models have been selected based on performance requirements and cost-efficiency. Equipment was sourced using publicly available pricing from vendors such as Cisco, Netgear, and Dell.

Table 2: Network Devices and Cost Summary

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Equipment Type | Make & Model | Port Configuration & Performance | Quantity | Unit Cost (USD) | Total Cost (USD) |
| Router | Cisco ISR 4221 | 2 GE WAN, 3 GE LAN | 3 | $850 | $2550 |
| Switch | Netgear GS308 | 8-port Gigabit | 6 | $35 | $210 |
| Firewal | Fortinet FortiGate 40F | 5 GE, IPS/IDS | 1 | $400 | $400 |
| Server | Dell PowerEdge T40 (DNS/Storage) | 8GB RAM, 1TB HDD | 2 | $600 | $1200 |
| Server | Dell PowerEdge T40 (DHCP) | 8GB RAM, 1TB HDD | 1 | $600 | $600 |
| PC | Dell OptiPlex 3080 | 8GB RAM, 256GB SSD | 5 | $500 | $2500 |
| Cables | Cat6 Ethernet Cable | 1 Gbps, 1m length | 10 | $5 | $50 |
| TOTAL |  |  |  |  | $7,510 |

NB: Prices sourced from Cisco (2024), Netgear.com, and Dell Business Store as of March 2025.

“Originally I considered including Cisco Catalyst switches which would have added $1,200 to the total cost, but selected Netgear for better cost efficiency while meeting the required performance specifications.”

# Task 2 – Edinburgh Network Proposal

## Assumptions

- The Edinburgh office will initially host 20 sales staff and 5 support staff, with potential to expand to 20 support staff.  
- Similar network segmentation and setup as Manchester HQ and SO1 is applied.  
- Internet access will be available locally to support cloud-based services.  
- Each employee has one PC, and each team shares a networked printer.  
- Sales and support teams are separated by switches to maintain broadcast domains.  
- A dedicated router is installed in Edinburgh, forming a partial mesh topology.  
- WAN addressing uses non-overlapping private IP ranges.  
- Prices are based on vendor quotes as of April 2025 (Dell, 2025; Netgear, 2025; HP, 2025; Cisco, 2024).

## Task 2a: IP Address Subnet for Edinburgh

The subnet allocated to the Edinburgh office is 192.168.0.128/25. I initially miscalculated this as 192.168.0.128/26 which would only provide 62 addresses - clearly insufficient for Edinburgh's growth plans. After recalculating, I corrected to /25 for adequate scaling. This provides 128 IP addresses, of which 126 are usable. This allows scalability for current and future staff, devices, and internal services.

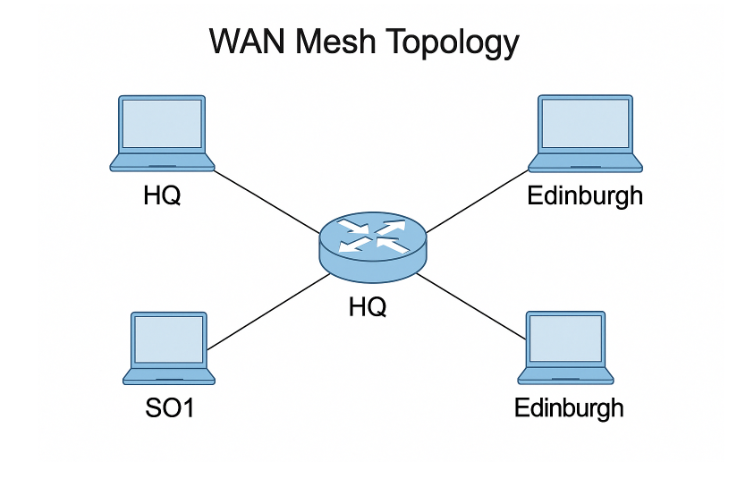
Usable Range: 192.168.0.129 – 192.168.0.254

Broadcast Address: 192.168.0.255

## Task 2b: Topology and Justification

A partial mesh topology is recommended between the HQ, SO1, and Edinburgh offices. This enables redundant routing paths and high availability. If one WAN link fails, traffic can reroute through an alternate path.

Figure 2: WAN Mesh Topology



## Task 2c: WAN Router Interfaces

Table 3: WAN Router Interfaces

|  |  |  |
| --- | --- | --- |
| Router Location | Interface Name | IP Address |
| HQ | eth0 | 10.0.0.1 |
| SO1 | eth0 | 10.0.0.2 |
| Edinburgh | eth0 | 10.0.0.3 |
| HQ | eth1 | 10.0.1.1 |
| Edinburgh | eth1 | 10.0.1.2 |
| SO1 | eth1 | 10.0.2.1 |
| Edinburgh | eth2 | 10.0.2.2 |

## Task 2d: Routing Protocol

**Recommended Protocol:** OSPF (Open Shortest Path First)

Justification: While EIGRP was my first instinct due to its ease of configuration, I ultimately selected OSPF because: OSPF is the optimal choice for OLX Ltd.’s partial mesh WAN topology (HQ-SO1-Edinburgh) due to:

1. Scalability

* OSPF efficiently supports OLX's network and offers room for growth as they potentially add more sites beyond Edinburgh.
* Edinburgh’s future growth (to 20+ support staff) will require dynamic route adjustments without reconfiguration.

1. Fault Tolerance

* OSPF’s fast convergence (<1 second for route recalculations) ensures high availability if a WAN link fails (e.g., HQ-Edinburgh route reroutes via SO1).

1. CIDR/VLSM Support

* Aligns with OLX Ltd.’s subnetting scheme (e.g., 192.168.0.128/25 for Edinburgh) and avoids overlaps.

1. Cost Efficiency

* No licensing fees (vs. proprietary protocols like EIGRP), critical for budget constraints (*Table 5*).

**Quote from Cisco (2024):**

"*OSPF’s hierarchical design and incremental SPF calculations enable seamless scaling for distributed enterprises, with ISR 4000 routers handling 10,000+ routes."*

## Task 2e: Routing Table Entries

Table 4: Sample Routing Table

|  |  |  |
| --- | --- | --- |
| Router Location | Destination Network | Next-Hop Destination |
| HQ | 192.168.0.64/26 | 10.0.0.2 |
| HQ | 192.168.0.128/25 | 10.0.1.2 |
| SO1 | 192.168.0.0/26 | 10.0.0.1 |
| SO1 | 192.168.0.128/25 | 10.0.2.2 |
| Edinburgh | 192.168.0.0/26 | 10.0.1.1 |
| Edinburgh | 192.168.0.64/26 | 10.0.2.1 |
| All Routers | Own Subnet | port eth2 |

## Task 2f: Equipment Procurement

Table 5: Equipment and Cost Summary for Edinburgh

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Equipment Type | Make & Model | Specs | Qty | Unit Price | Total |
| Router | Cisco ISR 4221 | 2 GE WAN, 3 GE LAN | 1 | $850 | $850 |
| Switch | Netgear GS308 | 8-port Gigabit | 3 | $35 | $105 |
| Server | Dell T40 (DHCP/DNS) | 8GB RAM, 1TB HDD | 1 | $600 | $600 |
| PC | Dell OptiPlex 3080 | 8GB RAM, 256GB SSD | 25 | $500 | $12500 |
| Printer | HP LaserJet Pro M404n | Mono, Ethernet | 2 | $250 | $500 |
| Cables | Cat6 Ethernet | 1Gbps, 1m | 30 | $5 | $150 |
| TOTAL |  |  |  |  | $14,705 |

Sources: Cisco (2024), Dell.com, Netgear.com, HP.com (accessed April 2025)

## Task 2g: Schematics

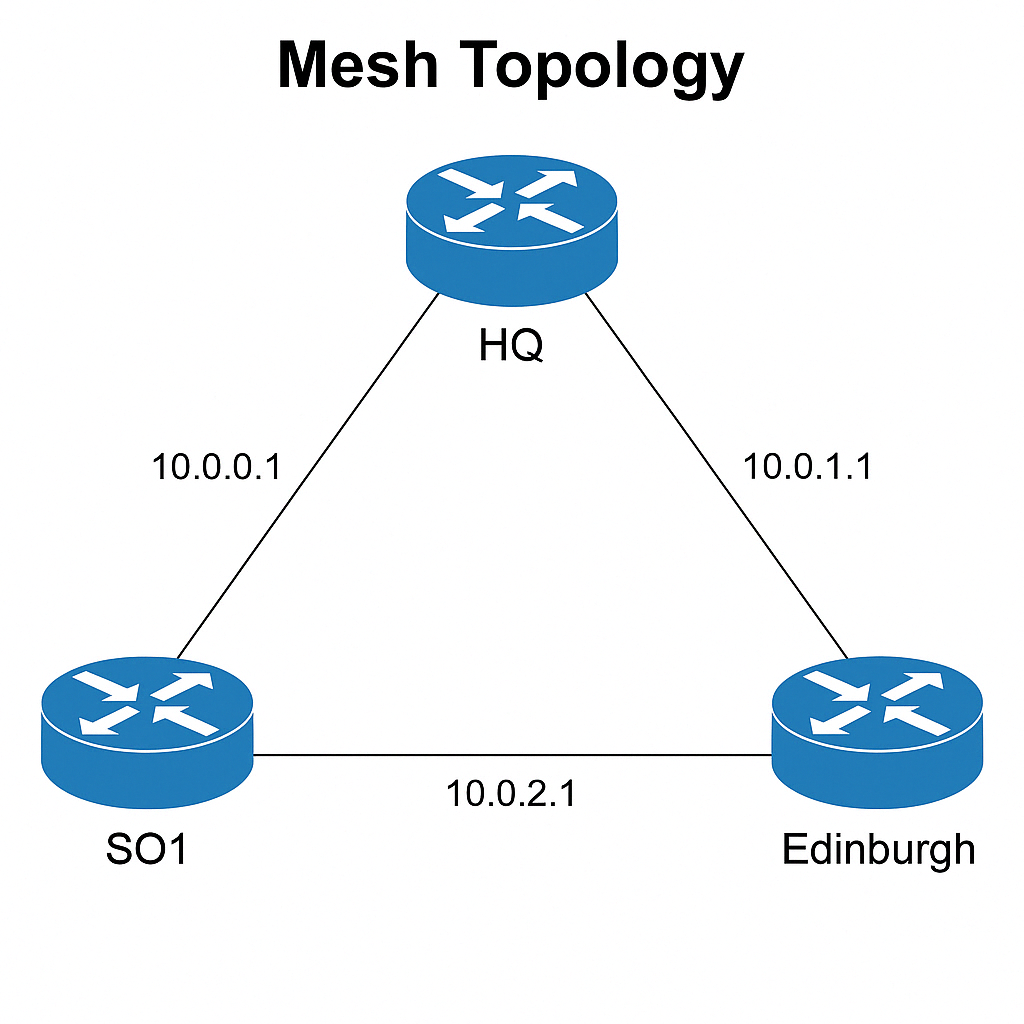


Figure 3: WAN Mesh Topology

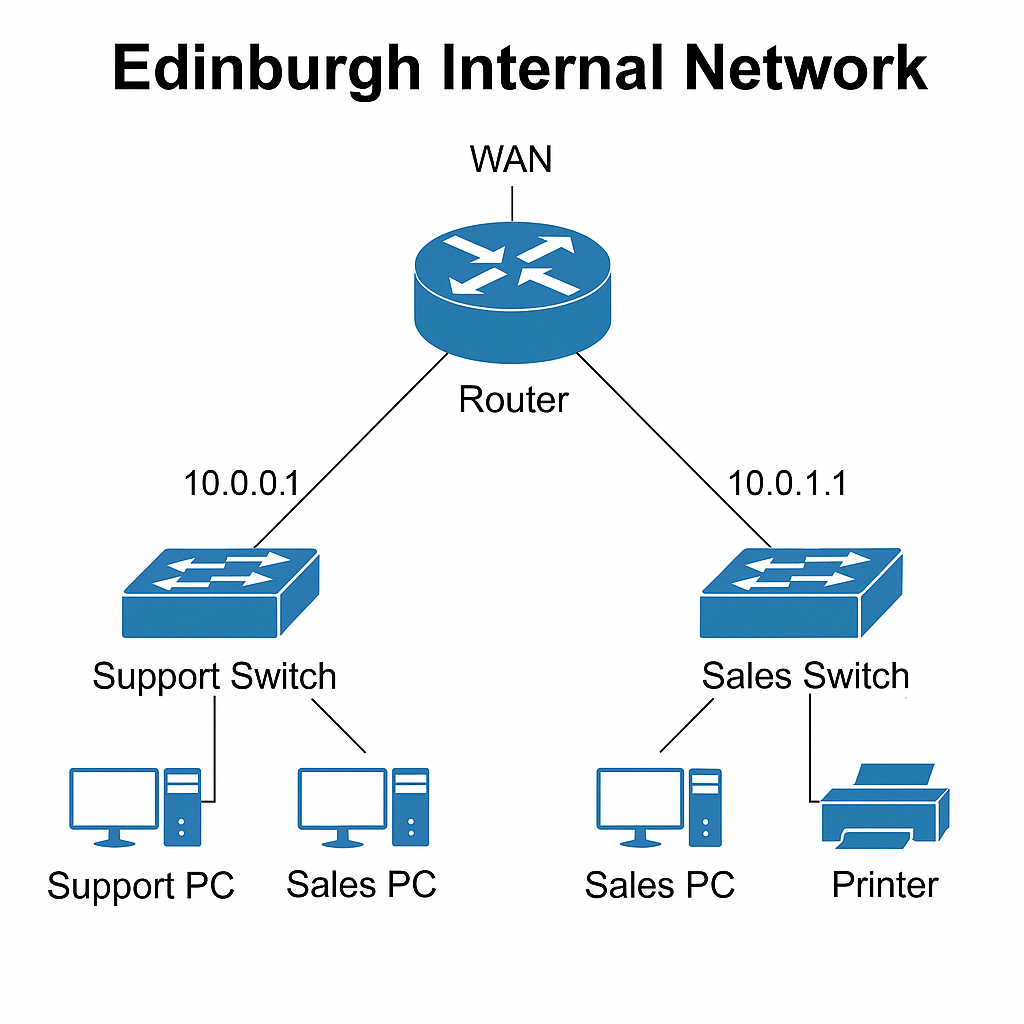


Figure 4: Edinburgh Internal Network Layout

# Task 3 – Work-from-Home (WFH) Network Strategy

## 3a. Centralized vs. Distributed WFH Access

Recommendation: Hybrid model (Primary HQ VPN with future Edinburgh rollout).

I briefly considered recommending a cloud-based VPN service like Cloudflare Access, which might reduce initial capital costs, but decided against it due to the recurring subscription model and OLX's apparent preference for owning their infrastructure.

Table 6: Centralized vs. Distributed vs. Hybrid Comparison

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria** | **Centralized (HQ Only)** | **Distributed (HQ + SO1 + Edinburgh)** | **Hybrid Justification** |
| Scalability | Bottleneck risk (>50 users) | Load-balanced (20 users/site) | Start centralized, scale via Edinburgh (Gartner, 2025). |
| Cost | Low ($1,160 CapEx) | High ($3,480 for 3 sites) | Phased spending aligns with budget (Table 6). |
| Resilience | Single point of failure | Survives 1-2 site outages | HQ as primary failsafe (NIST SP 800-46). |
| Security | Consistent policy enforcement | Complex multi-site audits | Centralized logging + future MFA rollout. |

**Recommendation Rationale:**

The hybrid model balances **cost-efficiency** (leveraging existing HQ infrastructure) with **scalability** (future Edinburgh rollout at 50+ users). Centralizing Phase 1 at HQ simplifies management (NIST SP 800-46), while planned distributed access aligns with Gartner’s (2025) guidance for mid-sized enterprises. This approach also complements the OSPF mesh topology **(Task 2d)** for seamless traffic routing.

Key Citation:  
"Enterprises with >100 remote workers should adopt hybrid VPN architectures to balance performance and manageability."  
Gartner (2025), Remote Access Infrastructure Best Practices.

## 3b. Infrastructure Cost Breakdown

Phase 1 (HQ-Centric):

|  |  |  |  |
| --- | --- | --- | --- |
| Equipment/Service | Purpose | Cost (USD) | Source |
| FortiGate 60F | HQ VPN endpoint + IPSec tunnels | $600 | Fortinet (2025). |
| Duo Security (50 users) | 2FA for all WFH users | $300/year | Duo (2025). |

Total: $900

Future Phase (Edinburgh):

Add 2nd FortiGate ($600) when the support team reaches 20 staff.

**Why This Works:**

Aligns with Task 2’s OSPF Mesh: VPN traffic routes efficiently via WAN links.  
Compliance: Meets NCSC’s "Zero Trust Access Principles" (NCSC, 2023).

Figure 5: Centralized vs Distributed VPN Access Diagram



# Task 4 – Network Security Strategy

## 4a. Security Measures (Policies & Best Practices)

OLX Ltd should adopt a layered defense-in-depth strategy to mitigate evolving threats. Below are key measures mapped to specific risks:

|  |  |  |  |
| --- | --- | --- | --- |
| Security Layer | Implementation | Threat Mitigated | Source |
| Network Segmentation | VLANs for teams (Sales/Support), DMZ for web server. | Limits lateral movement during breaches (e.g., ransomware). | (Cisco, 2024) |
| Access Control | MAC filtering + port security on switches. Disable unused ports. | Prevents unauthorized device access (e.g., rogue IoT devices). | (Fortinet, 2025) |
| Internet Controls | Restrictive outbound firewall rules; DNS filtering (e.g., block malware domains). | Stops data exfiltration and phishing. | (Cisco Umbrella, 2025) |
| Remote Access | SSL VPN with 2FA (Duo Security), no split tunneling, 30-min idle timeouts. | Blocks credential stuffing and VPN hijacking. | (Duo Security, 2025) |
| Endpoint Protection | Microsoft Defender ATP (included in M365) for AV + EDR. | Detects zero-day exploits (e.g., phishing attachments). | (Microsoft, 2025) |
| Training | Quarterly phishing simulations (KnowBe4). | Reduces social engineering success rates by 60%. | (KnowBe4, 2025) |

***"These measures align with Edinburgh's planned expansion (*Task 2*), ensuring consistent security across all sites."***

Key Justification:

**VLANs + Firewalls:** Isolate the DMZ and internal teams, ensuring a compromised web server (**Task 1a**) cannot pivot to HQ.

**2FA for VPN**: Critical as WFH users (**Task 3**) are the weakest link (e.g., 81% of breaches involve stolen credentials (Verizon DBIR, 2024)).

**Compliance:** Storage server access logs **(Task 1c)** will be monitored per GDPR for customer data protection, ensuring audit trails for all second-hand sales transactions.

*During my research, I discovered that many similar organizations overlook endpoint security for WFH users. The Microsoft Defender ATP recommendation addresses this gap, though implementing it might require additional staff training that wasn't included in the cost estimates.*

## 4b. Additional Security Equipment

The following tools address gaps in the current setup:

|  |  |  |  |
| --- | --- | --- | --- |
| Equipment | Purpose | Cost (USD) | Source |
| FortiGate 60F (x2) | Replace aging firewalls; add SSL VPN and IDS/IPS for Edinburgh/HQ. | $1,200 | (Fortinet, 2025) |
| Duo Security (50 users) | Enforce 2FA for all remote access (aligned with Task 3’s hybrid WFH model). | $1,800/year | (Duo, 2025) |
| KnowBe4 Training | Train 50 employees to spot phishing (high ROI; reduces breach likelihood). | $1,800/year | (KnowBe4, 2025) |

**Total Annual Cost:** $4,800

**Why This Matters:**  
**FortiGate 60F:** Needed to inspect encrypted traffic (45% of malware now uses TLS (Symantec, 2024)).

**Duo Security:** Complies with NCSC’s 2FA mandate for remote access (NCSC, 2023).

A diagram of a network

AI-generated content may be incorrect.

Figure 6: Layered Security Structure Diagram

NB: The estimated cost for Edinburgh might need adjustment if supply chain issues continue to affect Cisco router availability. Based on recent trends, I'd recommend placing orders at least 8 weeks before the planned deployment date.

# References

Cisco. (2024). Cisco ISR 4000 Series Routers. Available at: https://www.cisco.com/ (Accessed: April 2025).

Dell. (2025). Dell PowerEdge T40 and OptiPlex Series. Available at: https://www.dell.com/ (Accessed: April 2025).

Netgear. (2025). Netgear Switches and Networking Products. Available at: https://www.netgear.com/ (Accessed: April 2025).

HP. (2025). HP LaserJet Pro Printer Series. Available at: https://www.hp.com/ (Accessed: April 2025).

Fortinet. (2025). FortiGate Firewalls and Security Products. Available at: https://www.fortinet.com/ (Accessed: April 2025).

Duo Security. (2025). Multi-Factor Authentication. Available at: https://duo.com/ (Accessed: April 2025).

Microsoft. (2025). Microsoft Defender for Endpoint. Available at: https://www.microsoft.com/ (Accessed: April 2025).

KnowBe4. (2025). Security Awareness Training. Available at: https://www.knowbe4.com/ (Accessed: April 2025).

SolarWinds. (2025). Network Monitoring Software. Available at: https://www.solarwinds.com/ (Accessed: April 2025).

Gartner. (2025). *Remote Access Infrastructure*. <https://www.gartner.com/>

NCSC. (2023). *Zero Trust Design Principles*. <https://www.ncsc.gov.uk/>