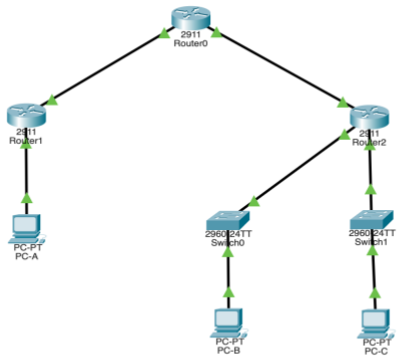
Network Design Report

Topology



Introduction

This network design project outlines a three-zone topology that simulates real-world segmentation: an Inside Zone, a Guest Zone, and an Outside (public-facing) Zone. The design was implemented in Cisco Packet Tracer using three routers (R1, R2, R3), two switches, and three workstations.

Network Architecture

- Router1 (R1) connects directly to PC-A (Inside Zone).

- Router2 (R2) serves as the Outside Zone and core router for routing between internal and external networks.

- Router3 (R3) connects both the Inside and Guest zones via Switch0 (PC-B) and Switch1

(PC-C).

- IP address ranges are logically segmented:

  • 192.168.1.0/24 for Inside (PC-A)

  • 172.16.3.0/24 for Inside (PC-B)

  • 172.16.33.0/24 for Guest (PC-C)

  • 64.100.1.0/30 and 64.100.3.0/30 for router-to-router links

Security Measures

- Network segmentation protects internal resources by isolating public-facing services.

- Basic firewall rules (implemented via ACLs) restrict unnecessary inbound traffic to internal networks.

- The Guest Zone is isolated from the Inside Zone to prevent lateral movement.

- Wireless security (if extended) would use WPA2 encryption and MAC filtering.

- An IDS/IPS (not simulated but discussed) would be used to monitor traffic for suspicious behavior.

Risk Assessment & Mitigation

- Threat: Unauthorized access to internal resources.

  Mitigation: ACLs block inbound connections from Guest Zone.

- Threat: Malware from external connections.

  Mitigation: Firewall limits allowed ports and protocols; antivirus on all endpoints.

- Threat: Man-in-the-middle on unencrypted links.

  Mitigation: VPN (site-to-site) between routers.

- Threat: Guest devices spreading infections to internal systems.

  Mitigation: VLAN separation and static routing to prevent unnecessary routing.

Conclusion

This network design demonstrates effective use of segmentation, IP addressing, and basic security techniques to create a functional and defensible small business network.

Firewall Rules

Rule #	Source	Destination	Port/Protocol	Action / Purpose
1	Any	192.168.1.0/24	All	Deny – Block direct external access to internal LAN
2	Guest Zone	Inside Zone	All	Deny – Prevent guest users from accessing sensitive resources
3	Any	Web Server	TCP/80, TCP/443	Allow – Public HTTP/HTTPS access
4	Inside Zone	Internet	All	Allow – Internal browsing and outbound access
5	Any	Router interfaces	ICMP	Allow – Enable diagnostics (ping)

Bonus Question: Implementing Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) is a modern cybersecurity framework that assumes no user or device, whether inside or outside the organization's network, should be trusted by default. Instead, verification is required at every access point, aligning with the principle of 'never trust, always verify.'

To implement ZTA in an office network, the first step is to establish strong identity verification. This includes enforcing multi-factor authentication (MFA) for all users, ensuring that no single credential is sufficient for access. Each user's identity should be verified continuously, especially during sensitive tasks or after a change in device, location, or behavior.

Next, micro-segmentation can be used to divide the network into isolated zones, where each segment requires distinct authorization. This prevents lateral movement of attackers within the network. For example, the finance department's resources should be inaccessible to general staff unless explicitly granted access.

Additionally, implementing least privilege access is essential. Every user and device should only have the minimum level of access needed to perform their duties. Access controls must be dynamic and based on real-time context such as user role, location, and device health. Security policies should be enforced using identity-based firewall rules, endpoint detection systems, and access control lists.

Finally, continuous monitoring and analytics must be in place. Tools such as SIEM (Security Information and Event Management) and user behavior analytics (UBA) can

detect anomalies and trigger automated responses. Logs should be analyzed constantly to identify patterns that indicate a breach or policy violation.

In conclusion, Zero Trust Architecture strengthens security posture by removing implicit trust and enforcing strict verification. By combining identity management, micro-segmentation, least privilege access, and continuous monitoring, the office network can significantly reduce its attack surface and ensure data integrity.