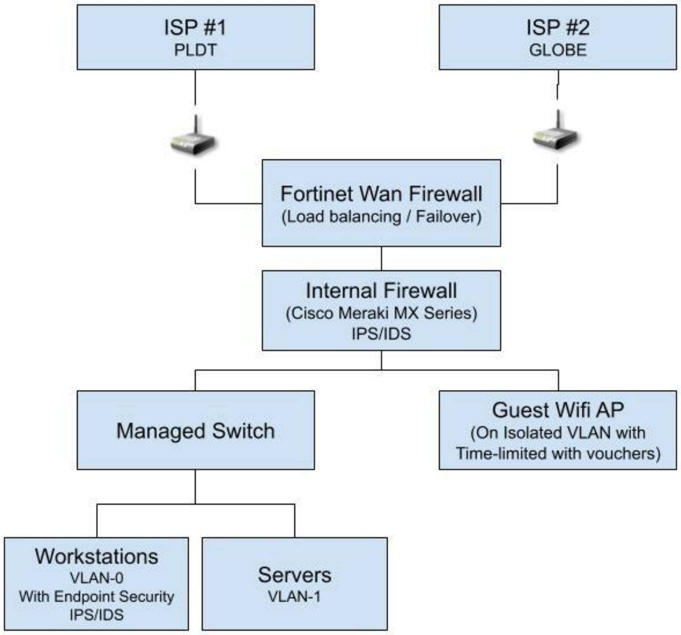
IT Protection and Security: MIT 264
Alden A. Quiñones
Activity 4: Designing a Secure Network

Secure Network Design for Small Office – 20 Users



1. Firewall and IDS/IPS Recommendation

To ensure both connectivity and robust security, it is recommended to deploy a Fortinet FortiGate 60F as the primary firewall. This model supports dual WAN connections, enabling load balancing and automatic failover between two internet service providers (ISPs). In the event one ISP experiences downtime, network connectivity will remain uninterrupted.

The FortiGate 60F also provides comprehensive security features, including deep packet inspection, application control, SSL inspection, and integrated IPS/IDS capabilities.

For enhanced intrusion detection and prevention, it is also advisable to incorporate a Cisco Meraki MX64 or MX67 device. The Meraki MX series offers cloud-managed security, including next-generation IDS/IPS, VPN support, content filtering, and real-time traffic analytics, all managed through an intuitive web dashboard.

2. Network Segmentation Strategy

To maintain a secure and efficient network, implement the following VLAN structure:

1. VLAN 0 – Personnel: For office employees. This VLAN will handle day-to-day user traffic such as desktop computers, shared printers, and access to internal applications.

2. VLAN 1 – Servers: Reserved for critical infrastructure such as file servers, application servers, and database systems. Access should be tightly controlled and monitored.
3. VLAN 3 – Guest Wi-Fi: Dedicated to guest users. This VLAN will provide internet-only access and will be completely isolated from the internal network (VLAN 0 and VLAN 1) to prevent unauthorized access to sensitive resources.

3. Guest Wi-Fi Policy

A secure and controlled guest Wi-Fi policy should be implemented with the following guidelines:

a) Guests must obtain a time-limited voucher to connect.
b) Voucher durations may vary (e.g., 1 hour, 3 hours, or full day)
c) Guests will be connected to a public-facing network with no access to internal systems or file shares.
d) Display a network usage policy disclaimer stating that the agency is not liable for any loss, damage, or compromise to personal devices or data while connected to the guest Wi-Fi network.