Network Design and Plan

Project Scenario

Corporation Techs provides remote and on-site support to small and mid-size businesses. Clients use Corporation Techs' services to solve problems involving malware removal, to manage data recovery and network issues, and to install hardware and software.

Due to recent developments, most technical representatives will begin working from home within the next six months. Because Corporation Techs provides 24/7 support, its systems and communications pathways must be fully operational at all times. In addition, the company has been experiencing unprecedented growth and is preparing to double its client-facing staff.

You are a junior network architect who is responsible for helping to plan and design network enhancements to create a more secure internal network, and to ensure secure remote access.

Objectives

- To plan and design network enhancements to create a more secure internal network, and to ensure secure remote access.

- Scalable network for the business that is preparing to double its client-facing staff to compensate fast growing business

Project Outline

- Project Part 1: Network Design
- Project Part 2: Firewall Selection & Placement
- Project Part 3: Remote Access and VPNs
- Project Part 4: Final Network Design Report

Methodology

Project Part 1: Network Design

Existing Network

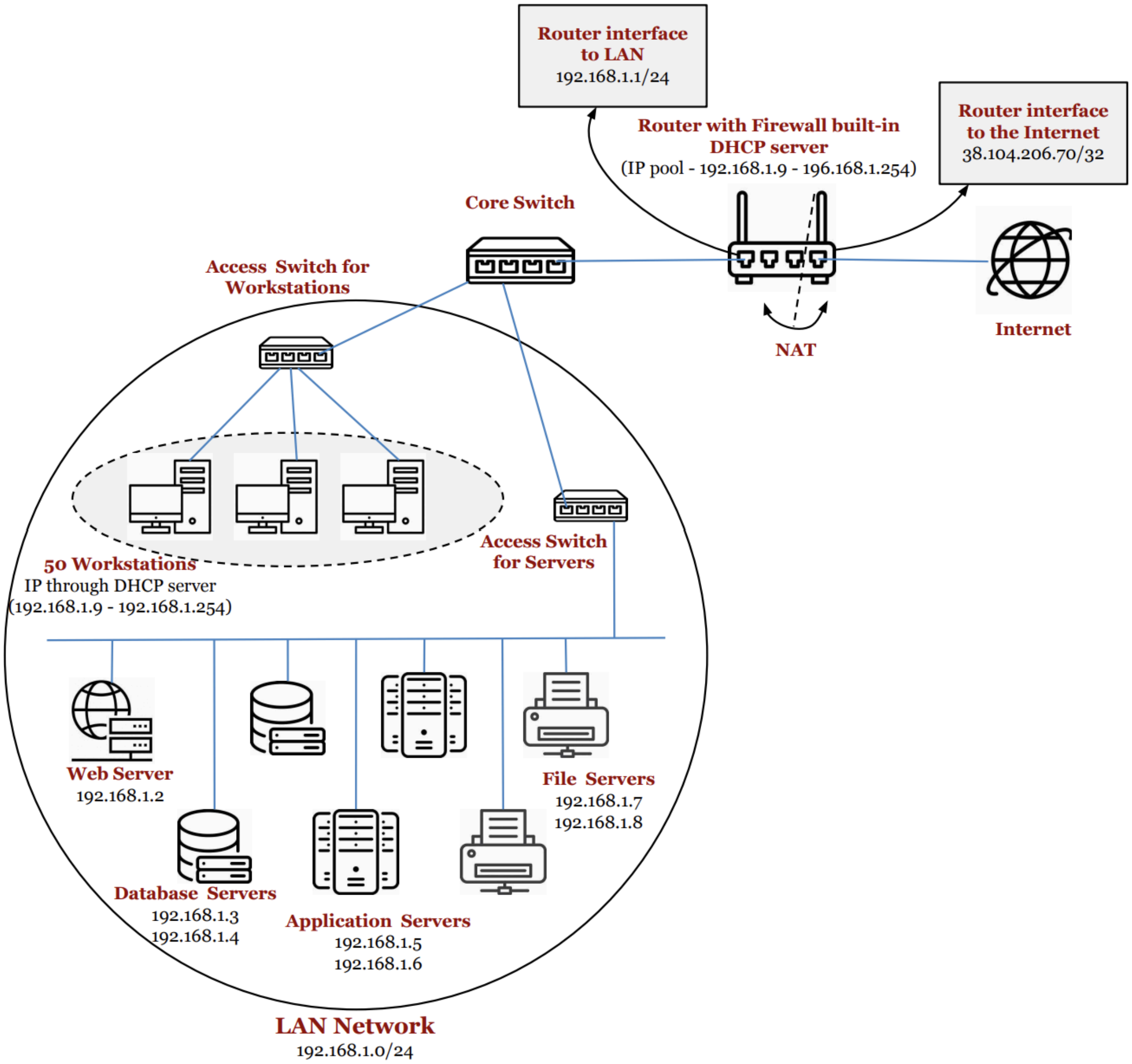
Infrastructure elements:

- 1 web server (accessible by the public) running Linux/Apache

- 2 application servers, 2 database servers, 2 file & print servers with Microsoft Windows Server

- 50 workstations that use Microsoft Windows

- Single border firewall



Network Outline

A private network (192.168.1.0/24) consists of 50 workstations and servers (a web server, 2 database servers, 2 application servers and 2 file & print servers).

Each server has a static IP ranging from 192.168.1.2 to 192.168.1.8 while the 50 workstations get their IP addresses from the DHCP server's available pool for dynamic addressing. The DHCP is provided by the gateway (192.168.1.1/24). The server group and the workstations are connected to their respective distributed switches to separate the user end devices from the servers.

These distributed switches are connected to a core switch which is in turn connected to a router incorporated with a built-in network layered firewall functionality for security with enabled Network Address Translation (NAT) to translate its public IP, 38.104.206.70/24 to internal IP addresses. The IP of the internal interface of the router is 192.168.1.1/24 and its public interface is 38.104.206.70/24. NAT rule and ACL are set to give access to the internal web server.

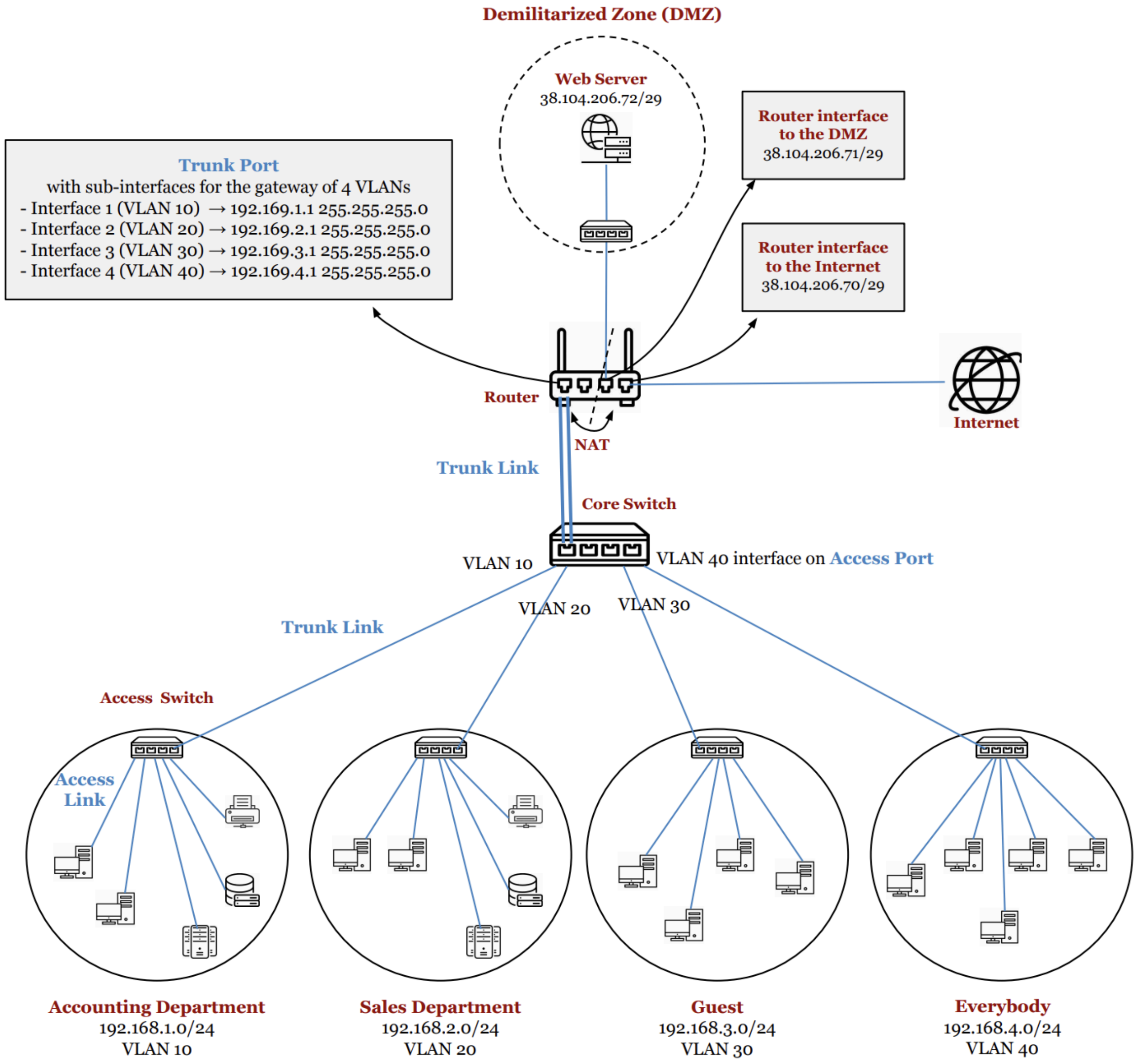
The router is connected to the Internet Service Provider (ISP) to access the internet for the whole network and for public access to the web server.

Proposed Design

- A logical topology that separates the Accounting and Sales departments
- Redundant communications
- Justification for continuing with IPv4 or upgrading to IPv6

For the corporate network, IPv4 can be continued to be used without changing to IPv6 because there are 50 workstations being used in the network currently, and together with servers, there are only around 60 IP addresses being occupied.

With a subnet mask of 255.255.255.0 (/24 in CIDR notation) there can be 254 hosts in the network. Since there are less than 70 hosts that are in use, it even allows 180 more hosts even if the company needs to add more endpoints, thus no issue regarding scalability.


Demilitarized Zone (DMZ)
Web Server
38.104.206.72/29
Router interface to the DMZ
38.104.206.71/29
Router interface to the Internet
38.104.206.70/29
Trunk Port
with sub-interfaces for the gateway of 4 VLANs
- Interface 1 (VLAN 10) → 192.169.1.1 255.255.255.0
- Interface 2 (VLAN 20) → 192.169.2.1 255.255.255.0
- Interface 3 (VLAN 30) → 192.169.3.1 255.255.255.0
- Interface 4 (VLAN 40) → 192.169.4.1 255.255.255.0
Router
NAT
Internet
Trunk Link
Core Switch
VLAN 10
VLAN 20
VLAN 30
VLAN 40 interface on Access Port
Trunk Link
Access Switch
Access Link
Accounting Department
192.168.1.0/24
VLAN 10
Sales Department
192.168.2.0/24
VLAN 20
Guest
192.168.3.0/24
VLAN 30
Everybody
192.168.4.0/24
VLAN 40

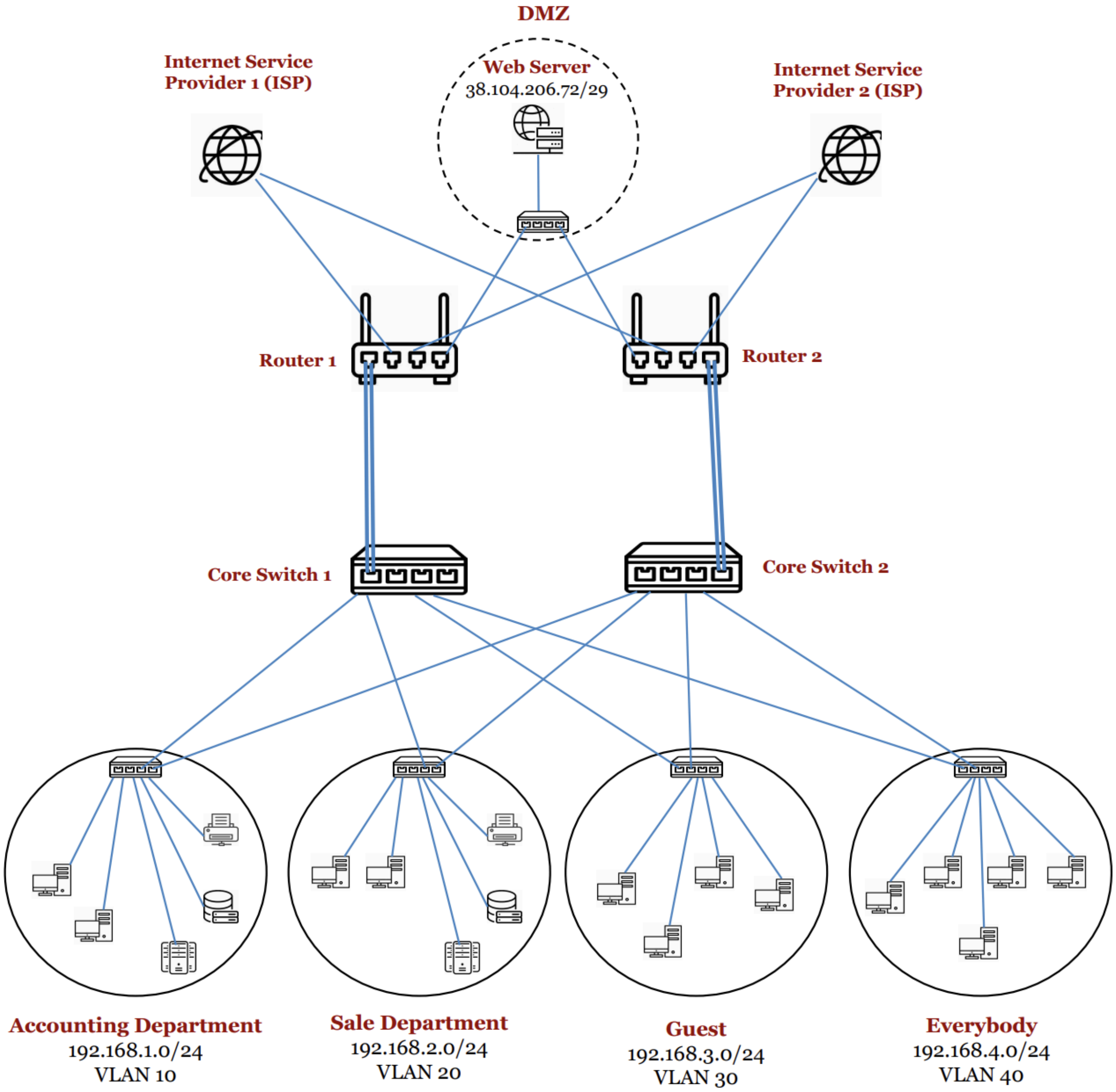
Network Outline

The departments are divided into different sub networks namely accounting department, sales department, guest and everyone. They are logically separated at layer 2 by applying VLAN (VLAN 10, 20, 30, 40 respectively) and at layer 3 (192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 and 192.168.4.0/24). The workstations and the servers that belong to the accounting and sales department are placed inside their subnet. All the IP of the endpoints dynamically come from the DHCP server that is deployed on the router. The servers can be manually configured to give static IP or dynamically from DHCP allocation.

The devices are then connected to their respective access switches via access links which are in turn attached to the interfaces of the core switch through trunk link. Each interface of the core switch is configured to belong to each VLAN of the subnet mask. The core switch is joined by the trunk link to the edge router. The accepting router port is structured to run sub-interfaces to receive the collection of different VLANs from one single port. The router is configured to run the DHCP server, NAT, NAT, ACL, and other services.

For the web server (38.104.206.72/29) to be visible to the public while securing the LAN, it is placed inside the demilitarized zone (DMZ) through an access switch as DMZ is less restrictive than the private network allowing public access to the web server while securing the internal network.

Proposed Design with High Redundancy

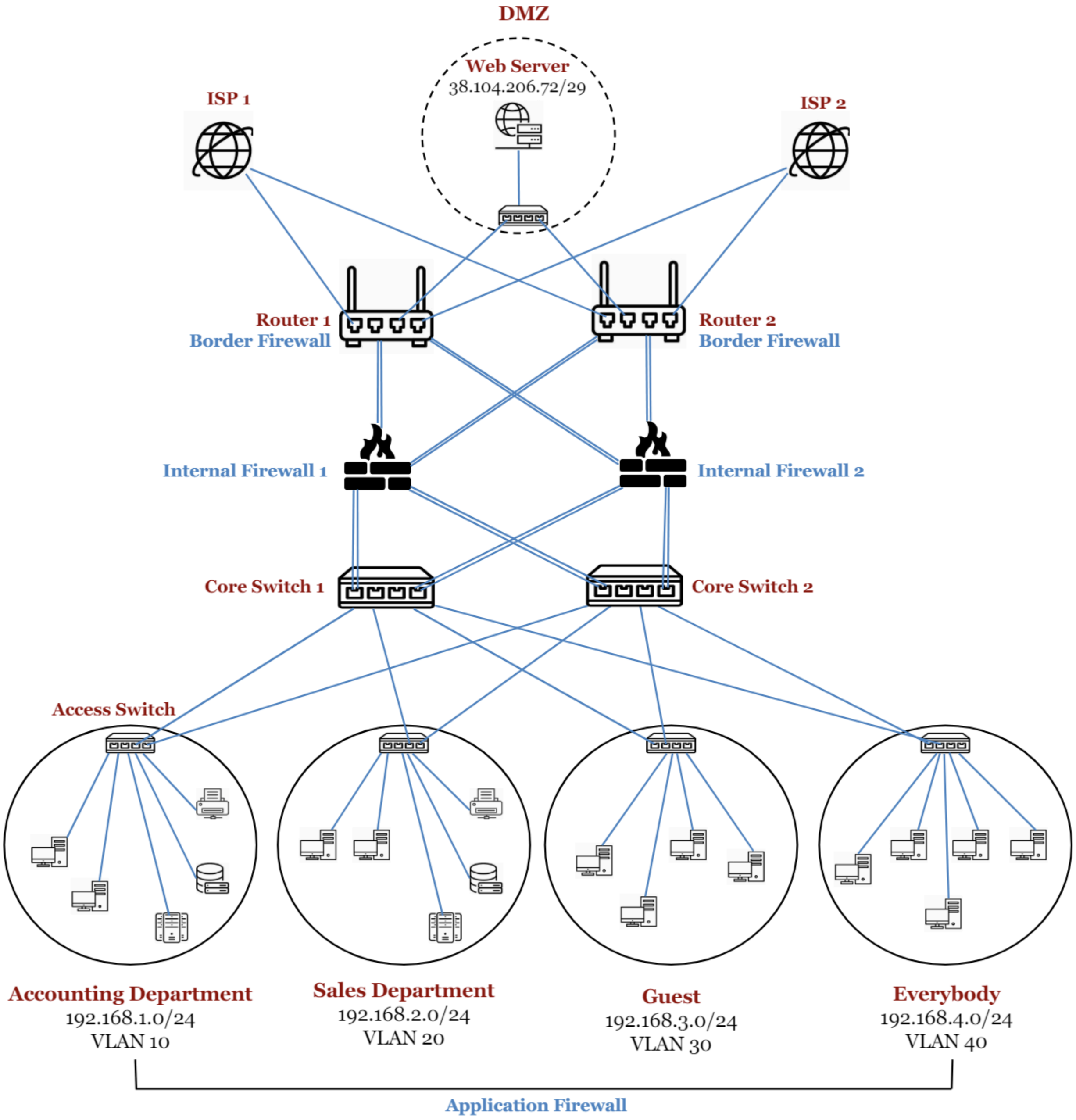


<u>Network Outline</u>

In order to incorporate high-level redundancy, ISP, router, core switches are doubled and are cross connected to each other to ensure the continuous communication 24/7 when one device fails or to divert the traffic when one is overloaded.

Project Part 2: Firewall Selection and Placement

- to research and select firewalls for the Corporation Techs network
- to place the firewalls for maximum effectiveness
- to create a high-level plan for secure authentication to internal network resources



<u>Network Outline</u>

The firewalls are deployed into the network to secure the network at different levels and segments. These are added as border firewalls, internal firewalls and application firewalls and are configured to meet the corporate’s requirement.

Border Firewall

The border firewall is configured on the edge router to filter the inbound traffic from the internet and the DMZ and the outbound communications from the internal LAN. Router Chassis with high port density can be used if there is a lot of traffic to connect to the router to support the high redundancy since it offers a large number of interfaces compared to traditional routers.

In addition to the functions of the router, Access Control List (ACL) and Network Access Control (NAC) functions are configured on it to effectively filter the traffic and to secure the network.

Access Control List (ACL)

ACL is a list of rules (tuples) that grant/deny access to the assets. These rules are obeyed according to the logical path, usually from top-to-bottom.

The rules to allow the traffic are administered in the ACL such as the allow any traffic to give access to the web server in the DMZ. All the rest of the unmatched traffic in the ACL must be denied by configuring “implicit deny” at the end of the list.

Network Access Control (NAC)

Access to the internal network is granted or denied by NAC which enforces rules and policies to determine who can access the network and to what level of access to enforce defense in depth. This involves authentication and authorization of the user such as 802.1x authentication, LDAP, etc as well as the posture assessment of the connecting device to ensure it is in good health performance and is clean.

NAC continuously monitors and reports the network traffic and devices behavior to inspect the traffic pattern, security incidents, policy violation and anonymous acts.

Internal Firewall

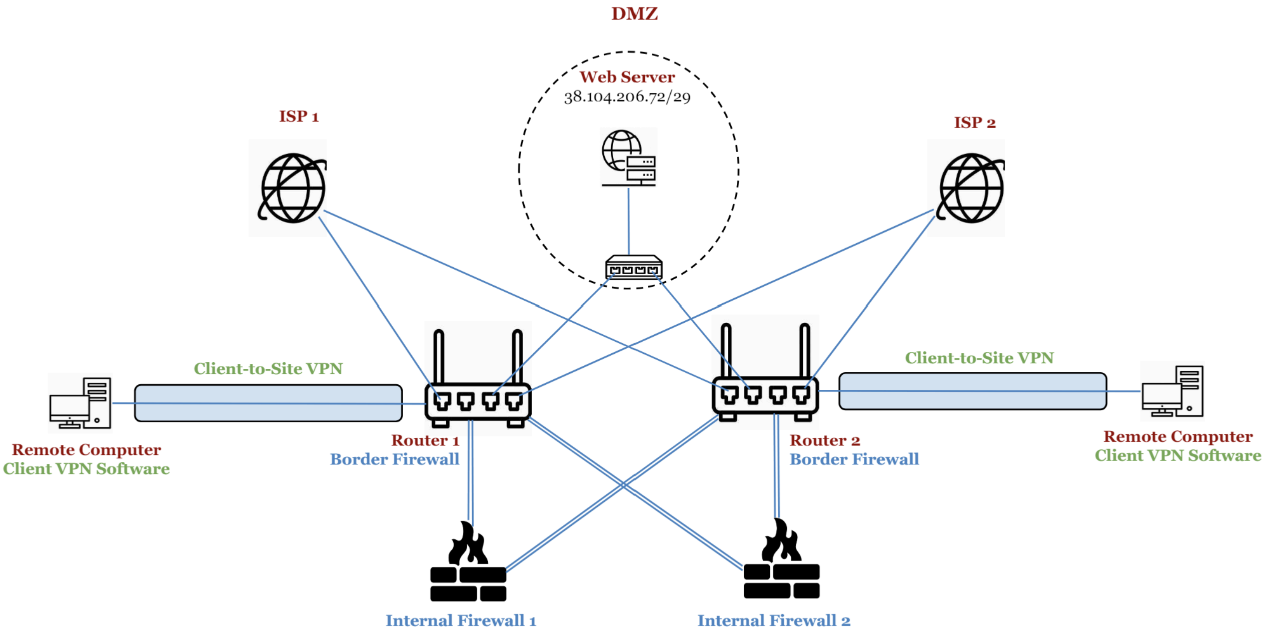
A hardware firewall is placed in the network between the router and the core switch to perform intense stateful inspection and filtering. ACLs are written on the firewall to provide centralized security enforcement for better and stricter security for the whole network.

Application Firewall

Host-based application firewalls are installed and used on each and every endpoint (workstations and servers) on the network. It hardens the devices and provides deep packet inspection to protect critical internal web applications and services especially from internal attacks. This also helps prevent lateral movement of the threats within the LAN.

Project Part 3: Remote Access and VPN

- to create a plan that will allow secure remote access to the internal network while preventing unauthorized access implementing VPN
- need of all information transferred between remote users and the organizational servers be protected against snooping



Network Outline

Client-to-site VPN is created to allow the employees to work remotely from their home. First, a client VPN software is installed on the remote computer to establish the VPN connection with the corporate's internal network. User authentication methods (username and password, digital certificate, etc.) are added to authenticate the user to the VPN gateway. After that, the VPN client and the gateway form a secure communication channel by negotiating the security associations. This includes agreeing on the encryption algorithm, protocol, integrity protection mechanisms and key exchange protocol. Once the pre-shared key is decided between the VPN client and the gateway, a secure tunnel is established where all the traffic inside it will be encrypted and invisible to the internet. The remote user can now access the corporate's network and the internal assets through this VPN tunnel.

Internet Protocol Security (IPsec) is recommended to use because of its ability to provide encryption and mutual authentication of both source and destination on layer 3, and with its tunnel mode, the data packet as well as the packet header is entirely encapsulated making it more secure. IPsec has 3 main components - Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE). IKE helps in managing the pre-shared key between the VPN client and the corporate's gateway, the edge router. AH provides authentication and integrity protection (through hash) while ESP can also encrypt the payload in addition, thus making it more favorable to use ESP. In order for the IPsec to work through NET, some of the ports must be opened on the VPN concentrator as follows:

- Internet Key Exchange (IKE) - User Datagram Protocol (UDP), port 500

- Encapsulating Security Payload (ESP) - IP protocol, port 50

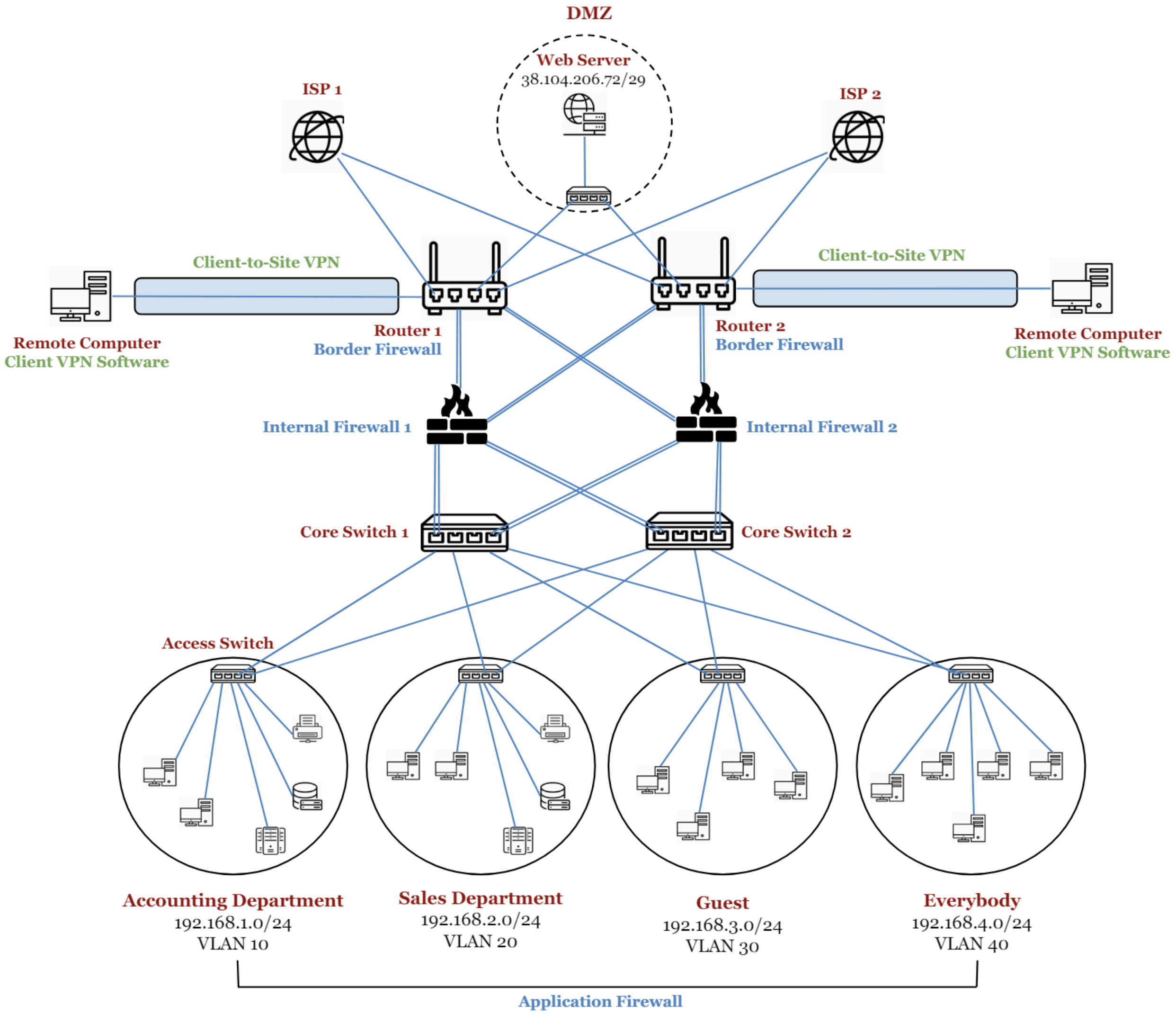
- Authentication Header (AH) - IP protocol, port 51

The remote computer is done with the preflight check before letting it connect to the VPN and after it lands off the VPN gateway, it is thoroughly inspected before granting access to the internal network. Once the permission is granted, the landing IP, a new trusted IP is allocated to the remote computer.

The alternative technology is SSL/TLS-based VPN that provides tunneling on layer 4-7. For this VPN connection, the client does not need to install a client VPN software on their computer. Instead they can just connect to the application on the corporate's network using the web browser. This method is less expensive, flexible, and easier network configuration while providing granular access control.

Project Part 4: Final Network Design Report

- to create a professional report that includes content from each draft report.
- details for all relevant information, persuasive justification for your recommendations, and methods to measure the success of each major network enhancement



Network Outline

The internal network is subdivided into different departments for clean physical network segmentation. VLAN and subnet is used for each department to logically separate them from each other. The endpoints in each department are connected to an access switch which is in turn connected to core switches, assigning VLAN on its interfaces. This is then connected to the firewall where it is set up so that diverse VLAN can be configured on one single interface on the firewall with the help of setting up subinterfaces. At the firewall, the traffic is inspected immensely to secure the whole network. Similarly, the traffic from the firewalls are sent to the router through trunk link, deploying subinterfaces for the VLANs. From the router, the traffic is routed to the internet or the DMZ which provides web service for the public. It also serves as the gateway for the VPN access of the remote users.

References

Stewart, J. M., & Kinsey, D. (2020). *Network Security, Firewalls, and VPNs*. Jones & Bartlett Learning, LLC.