Report on Establishing a Network Plan

25/05/2023

Group Members

* Gianni
* Malika
* Quincy

This is the report file of our project to establish a network plan. In this document you can find a detailed explanation on the decisions we made, the tools we used and how exactly we approached this project.

Components

1. Active Directory (AD) Server: Manages user accounts and network resources.
2. DNS Server: Resolves domain names to IP addresses.
3. DHCP Server: Assigns IP addresses dynamically to network devices.
4. DMZ: Acts as a demilitarized zone with firewall and proxy servers.
5. Storage Server (iSCSI): Provides centralized storage for the network.
6. Switches: Connect various devices within each sector and to the central infrastructure.

IP Addresses and Connections

Subnet mask : 255.255.255.0

1. DMZ:
    * iSCSI Storage Server: IP - 192.168.1.1, Connection - Gigabit
    * DNS Server: IP - 192.168.1.2, Connection - Gigabit EthernetEthernet
2. Internal Servers:
    * AD Server: IP - 192.168.2.1, Connection - Gigabit Ethernet
    * DHCP Server: IP - 192.168.2.1, Connection - Gigabit Ethernet
3. Management Sector:
    * Switch: Connection - Gigabit Ethernet
    * 5 Management PCs: IP Range - 192.168.3.1 to 192.168.3.5
4. Study Sector:
    * Switch: Connection - Gigabit Ethernet
    * 8 Study PCs: IP Range - 192.168.4.1 to 192.168.4.8
5. Production Sector:
    * Switch: Connection - Gigabit Ethernet

    * 10 Production PCs: IP Range - 192.168.5.1 to 192.168.5.10
6. Support Sectors (Support1 and Support2):
    * Switch (Support1): Connection - Gigabit Ethernet
    * Switch (Support2): Connection - Gigabit Ethernet
    * Support1 PCs: IP Range - 192.168.6.1 to 192.168.6.30
    * Support2 PCs: IP Range - 192.168.6.31 to 192.168.6.60

Security Measurements:
* Proxy Server: IP - 192.168.10.2, Connection - Gigabit Ethernet

Topology

The computers inside the internal network are connected with a star topology and each server as well.
The actual cables used are Gigabit Ethernet cables to provide up to 1 Gigabit per second.

Firewalls & Proxy

We host a main firewall at the entry point of our network. Here we have the IPS & IDS. The proxy server (acting as proxy and firewall) acts as a central point where all traffic from clients go through. We also run a dedicated firewall for our internal servers. And there are firewalls in place to create the DMZ.

DMZ

Inside our DMZ we host the storage server so that people working from home don’t have access to the internal network. This is an extra security measurement. Traffic coming from outside requesting access to the servers inside this zone stays in the demilitarized zone. Servers hosted in this zone run on their own network range

Servers

Our servers for internal use are hosted behind a dedicated server firewall. The servers used for external traffic are put in a DMZ.

DHCP Server

The DHCP server is the part of the network that assigns the network parameters to the client devices such as IP addresses and default gateways. This server is for internal use only so it is **not** placed inside the DMZbut in the internal network.

For the DHCP server we chose a dedicated DHCP server instead of using switches or routers. We did this for the following reasons:

* Dedicated server provides IPAM (logging and management interface)
    * Important for:
        * address tracking
        * security forensics
        * scope utilization
* Supports IPv6 / DHCPv6
* Redundancy & increased availability
* Supports lager number of clients
    * scalability
* Dynamic DNS
* Easier to configure
    * time and resource efficient
* Faster processing

All of the above are not available if we would run the DHCP server on a switch or router.

Conclusion

To build a sizable network that is connected to the internet there are certain security aspects you need to take into consideration when it comes to traffic from the outside. A main firewall and a proxy firewall are a must for any decently sized network, to make sure internal files cannot be accessed. Inside of networks that work with sensitive data, a DMZ is also a must to keep the traffic coming from the outside separated from the internal traffic.

Depending on how many computers and servers there are inside of your network, different topologies provide different results. In our case the star topology made the most sense. But depending on your wants and needs, different considerations apply. Most topologies in larger networks nowadays are probably hybrid however.

Depending on the size of the network, different ways of IP addressing apply as well. In our case, for such a small network, a class C IP address suffices. With a maximum of 254 hosts, there are enough addresses to allocate.
Depending on how secure you want your network to be, you can use subnetting to get the exact amount of hosts you need for each section of your network. If certain departments for example don't have a need for many computers, you can limit the amount of hosts inside of the subnet.

Tools used for this project:

* Cisco Packet Tracer to build diagram and simulate the network
* VS Code & NotePad++ for note taking and reporting
* Discord for team communication
* ChatGPT & Youtube for intel gathering

List of sources:

* [What is a DHCP server?](https://www.infoblox.com/glossary/dhcp-server/)
* [How to set up a business network](https://www.techtarget.com/searchnetworking/answer/Guidelines-to-set-up-a-new-business-network)
* [Small business network tour video](https://www.youtube.com/watch?v=hwvywTzyqsY)
* [What is subnet mask?](https://www.ipxo.com/blog/what-is-subnet-mask/)
* [Secure Network Architecture Design](https://www.youtube.com/watch?v=nABcOxWQ1RA)
* [Configuring DHCP server using Cisco ios](https://www.youtube.com/watch?v=GCaR8e-16bs)
* [What is a dmz](https://www.youtube.com/watch?v=dqlzQXo1wqo)
* [What is a proxy](https://www.fortinet.com/resources/cyberglossary/proxy-server)
* [Subnet Mask](https://www.youtube.com/watch?v=s_Ntt6eTn94)