Creating a secure network for a Professional Environment

Yunus-Mehdi-Achraf
BECODE KAMKAR 2024

Table of Contents

Introduction

First of all, we would like to say that we are proud to present our network design in a professional environment. To do this, we have taken into account all the parameters requested by the customer in order to obtain an optimal architecture respecting needs such as scalability, financial and energy efficiency, not forgetting the main aspect, Security. The different departments are represented as follows:

Management / Secretariat: 5 computers

Support Sector 1: 10 computers Support

Sector 2: 10 computers

Production: 10 Computers

Study: 8 Computers

Materials and Equipments

2 Router

1 laptop for configuration + console cable

6switch 24-port Switches + cables

43 Ethernet cables

12 cables for EtherChannel connection

1 Storage server + 1 Ethernet cable

a server hosted on Microsoft's cloud computing platform called Microsoft Azure, ensuring optimal security and a backup in case of loss or error leading to data loss .

Installation of a Faraday cage in the sensitive departments to protect the equipment against electromagnetic interference and wave attacks, thus guaranteeing the security of the data and the continuity of operations.

Option: In case of a contract of more than 3 years, our company offers the camera surveillance system and non-reproducible access card.

General Design & IP Adressing Table

Our network does not strictly follow a star topology. It has a more complex structure, resembling a hierarchical tree topology, where multiple switches are interconnected, and different VLANs and servers are distributed. This design allows for better segmentation, more flexible traffic management, and stronger redundancies compared to a simple star topology.

VLAN	Hosts	Subnet	Subnet Mask	IP Address Range
Support Sector 2	10	192.168.0.0/28	255.255.255.240	192.168.0.1 to 192.168.0.14
Support Sector 1	10	192.168.0.16/28	255.255.255.240	192.168.0.17 to 192.168.0.30
Production	10	192.168.0.32/28	255.255.255.240	192.168.0.33 to 192.168.0.46
Study	8	192.168.0.48/28	255.255.255.240	192.168.0.49 to 192.168.0.62
Management/Secretariat	5	192.168.0.64/29	255.255.255.248	192.168.0.65 to 192.168.0.70

Choices and Explanations

Using VLANs and Why?

The use of VLANs (Virtual Local Area Networks) in a network like this offers many advantages, especially in complex corporate environments. Here are the main reasons why VLANs were implemented in this network:

1. **Network Segmentation for Security** VLANs allow the logical segmentation of the network into different parts. Each VLAN corresponds to a group of users or services (such as Production, Support, Study, etc.), isolating these groups from each other.
   This means users in one VLAN cannot directly access resources in another VLAN without going through a router (or inter-VLAN configuration). This reduces the risk of security breaches spreading from one group to another.

2. **Better Traffic and Bandwidth Management**
   By separating users into different VLANs, it becomes possible to control and optimize network traffic. For example, traffic generated by the Production department (which may have high network demands) is isolated from traffic from Support or Study departments, which may have lighter needs.
   This helps reduce congestion on the network and better manage priorities based on the specific needs of each group.

3. **Flexibility and Simplified Management**
   VLANs allow for quick and easy network reorganization without requiring physical changes (like moving cables). If a user switches departments, their VLAN can be updated via the switch without modifying the physical infrastructure.
   This also simplifies large-scale management since security and access policies are applied at the VLAN level, not to individual machines.

4. **Improved Internal Security** VLANs limit the scope of broadcast domains, meaning broadcast requests (which are sent to all devices on a network) are confined to their respective VLAN. This reduces network load and improves security by limiting resource visibility to each VLAN.
   If a security incident (such as a virus or attack) occurs in a specific VLAN, its impact is contained within that VLAN, preventing it from easily spreading to other parts of the network.

5. **Inter-VLAN Routing and Granular Control** Using VLANs with a router for inter-VLAN routing allows for the implementation of specific access control rules. For instance, the Production VLAN may be granted access to certain resources in the Support VLAN, but not vice versa.This enables fine-grained control over which groups or departments can access specific resources.

6. **Differentiated Access Policies** Each VLAN can have its own specific policies, such as traffic prioritization (for example, production data might have a higher priority than study data) or internet access restrictions, like blocking access to social media or streaming platforms.
   This allows network customization based on the needs of different departments.

7. **Improved Data Security** In this case, with the use of an Azure server for data backup and other measures like web server access filtering (represented by the "TIKTOK" server), VLANs add an extra layer of security. Each VLAN can have specific data backup and security policies, ensuring that only certain machines or users can access critical or sensitive resources.

And what about Scalability ?

VLANs also significantly improve the scalability of the network. As the company grows and new departments or services are added, VLANs allow for easy expansion without redesigning the entire network infrastructure. New VLANs can be created, and new users or devices can be assigned to them without affecting the existing setup. This ensures that the network can grow alongside the organization while maintaining optimal performance, security, and manageable complexity.

Protocols

We utilized several different protocols tailored to the client's needs. Here is an overview of the key protocols:

HSRP (Hot Standby Router Protocol)
HSRP allows configuring multiple routers and switches as a redundant default gateway for hosts on a local network.
This means if the main router/switch fails, a backup router/switch automatically takes over, ensuring uninterrupted service for users.
Routers/switches configured with HSRP agree on an "active" router/switch, which serves as the default gateway. A "standby" router/switch is also designated to take over in case the active one fails.
The routers/switches communicate regularly to ensure the configuration is working properly.

DHCP Snooping (to prevent man-in-the-middle attacks)

DHCP snooping is a feature that monitors and controls DHCP traffic on the network. It helps secure the network in several ways:

- **Prevent unauthorized DHCP servers:** DHCP snooping can detect and block unauthorized DHCP servers, preventing man-in-the-middle attacks by rogue DHCP servers.
- **Secure IP addresses:** DHCP snooping creates a list of IP addresses assigned by the legitimate DHCP server, verifying that IP addresses in use are valid and legitimate.
- **Logging and monitoring:** DHCP snooping logs information about the IP addresses assigned, which can be used to detect suspicious activity on the network.

OSPF (Open Shortest Path First)

OSPF is one of the most widely used dynamic routing protocols in enterprise networks.

It allows routers to communicate with each other to stay informed about available paths on the network, enabling them to automatically choose the best paths for traffic routing.

Key benefits of OSPF in an enterprise network include:

- **Fast convergence:** OSPF updates routing tables quickly when the network topology changes, ensuring better responsiveness in the event of network failures or changes.
- **Load balancing:** OSPF can distribute traffic across multiple equal-cost paths to the same destination, improving bandwidth utilization.
- **Network hierarchy:** OSPF allows the network to be structured into different areas, which simplifies management and scalability.
- **IP network support:** OSPF is specifically designed to work with the IP protocol, making it highly suited to modern enterprise networks.

EtherChannel

EtherChannel is a technique that combines multiple Ethernet cables into a single logical link. This increases bandwidth and improves redundancy between two switches or between a switch and a router.

Advantages of EtherChannel:

- **Increased bandwidth:** By combining multiple cables, EtherChannel increases the total connection capacity, allowing more data to be transferred faster.
- **Redundancy and reliability:** If one cable in the EtherChannel fails, the other cables continue to operate, ensuring a continuous and reliable connection. This reduces service interruptions and improves network availability.
- **Simplified management:** Instead of managing multiple individual cables, you manage a single logical link, simplifying network configuration and management.

- **Load balancing:** EtherChannel distributes network traffic evenly across the various cables, improving overall network performance.
  In summary, EtherChannel increases network speed and reliability by combining multiple Ethernet cables, offering better bandwidth, enhanced redundancy, and simplified management.

SSH (Secure Shell)

SSH is widely used in enterprise networks for several important reasons:

- **Enhanced security:** SSH allows secure and encrypted connections between network devices, preventing unauthorized access and protecting transmitted data from eavesdropping.
- **Strong authentication:** SSH uses robust authentication mechanisms, such as public/private key pairs, ensuring the identity of users and devices connecting to the network.

- **Secure remote access:** SSH enables secure remote access to network devices (servers, routers, switches, etc.), facilitating remote administration and troubleshooting.
- **Secure file transfer:** SSH includes secure file transfer features like SCP and SFTP, allowing confidential data to be transferred without the risk of interception.

Security

In addition to the physical layer of security, our team paid particular attention to network security by implementing the following parameters:

- **Network segmentation with VLANs**
- **Internet access filtering:** Represented as a server named “Tiktok,” this system blocks a list of websites such as social networks (Instagram, Facebook, TikTok) and other downloading and streaming platforms. This serves three main purposes: first, to avoid network overload; second, to ensure the network is used exclusively for professional purposes; and lastly, as an additional layer of protection against potential phishing threats or malware downloads.
  These restrictions apply across the various VLANs (e.g., Support VLAN, Study VLAN), ensuring that all departments adhere to this access restriction policy. For websites and messaging applications like Outlook, our group can also offer phishing awareness training to users.

- **Azure Backup Server:** The inclusion of an Azure backup server is an excellent measure for resilience and data protection. In the event of an attack, such as ransomware, data can be restored from the remote server.
  Using the cloud for backup also provides geographic redundancy, ensuring data is safe even in the event of a localized disaster (hardware failure, fire, etc.). Additionally, secure remote access for the administrator is maintained.
- **Access control with specific credentials (admin/user):** Differentiated access accounts (admin and user) are used to restrict access rights based on roles, minimizing the potential for errors or misuse.
  The use of distinct passwords and protecting administrator rights further strengthens the security of the network.

Admin Access:

- For unique administrator access, such as access to the server, we have implemented a daily password rotation protocol.
  For example, if the base password is

  #Be|C}ode_1

  then on Monday your password will be #Cf|D}pef_2.

If you log in at 00:01 on Saturday, your password will be

#Hl|j}uk_8.
If your password contains a "z," the rotation restarts from "A" as the first letter.

User Access: The entire system will be managed through **Windows Administrator** to simplify the assignment of access privileges.
For better security, we recommend employees use passwords with a minimum of 12 characters and change them every 30 days.

Where Are the Firewalls ?

We chose to implement **Extended ACLs** rather than relying solely on firewalls for several reasons:

1. Granular Internal Control:
Extended ACLs provide more precise control over internal traffic between different sectors of the network. While firewalls are generally used to manage traffic at the perimeter (between the internal network and external sources), ACLs allow us to enforce strict rules within the internal network, controlling communication between VLANs or specific devices. This level of internal control is essential for segmenting access between departments like Management, Support, and Production.

2. Performance Optimization:
Firewalls, while powerful, can introduce latency when dealing with a large volume of internal traffic due to the deep inspection they perform. By using Extended ACLs directly on network devices like switches or routers, we can filter traffic without needing to route everything through a firewall. This approach improves network performance, as ACLs operate at the router level and process packets more efficiently.

3. Specific Traffic Blocking:
Extended ACLs allow us to block specific traffic based on more detailed criteria, such as the source and destination IP address, protocol, or port number. For instance, if we need to block requests to certain sensitive internal resources or external sites from particular VLANs, ACLs provide a straightforward and flexible method to do this. This fine-tuned control is more effective for internal segmentation than using firewalls, which might require more complex configurations to achieve the same result.

4. Cost and Complexity Reduction:
Deploying firewalls at multiple points within the internal network could increase both the complexity and cost of the infrastructure. Firewalls require ongoing management, updates, and monitoring. By leveraging Extended ACLs on existing network devices, we reduce the need for additional hardware and streamline network management without compromising on security.

5. Complementary to Firewalls:
While we use firewalls to secure the external perimeter, the role of Extended ACLs complements this by providing internal protection. The ACLs help to prevent unauthorized access between departments or VLANs, while the firewalls focus on filtering and inspecting traffic that crosses the boundary between the internal network and external threats. This layered approach ensures comprehensive security coverage.