**CISCO NETWORKING PROJECT**

**The project involves designing and implementing a Cisco-based networking secure and reliable infrastructure that connects two physical locations (Site A and Site B) of a company. The network will include endpoints such as PCs, servers, printers, VoIP, cable structure, and configurations of network devices to communicate with each other through a secure IPsec VPN connection, and installing a surveillance camera system. The network will use logical addressing and will be connected using physical cables. The surveillance camera system will be connected to the network for remote monitoring and recording.**

**Equipment Required:**

* **Cisco routers and switches**
* **VPN concentrator**
* **Ethernet cables**
* **Surveillance camera system**
* **Power-over-Ethernet (PoE) switch**
* **Network interface cards**
* **PCs**
* **Servers**
* **Printers**
* **Software**
* **Etc…**

**Implementing a secure and reliable networking infrastructure**

**We Identify the requirements, by determine the scope of the network and what services will be required in terms of speed, capacity, availability, security, and scalability. This will help us select the appropriate networking equipment based on our requirements and budget, the type of equipment needed, such as switches, routers, firewalls, a variety of endpoint devices, such as PCs, servers, printers, software, and wireless access points etc… Cisco offers a wide range of switches, routers, and other devices, with different features and capabilities to meet your needs.**

**We’ll also Decide on the network topology that best meets the needs of the organization, including how devices will be connected, how data will be routed, and how different segments of the network will be isolated from each other.**

**IN TERMS OF SECURITY**

**Once we have the equipment in place, configure them according to the network requirements and security needs, Configure Cisco devices based on best practices, including strong passwords, proper SNMP configuration, and the latest software and firmware updates. This is important for keeping the network secure and up to date. We Implement network segmentation to create separate, user groups, types of data, network service and device type for secure and efficiency, secure zones for different types of traffic, such as management, voice, data, and internet traffic. This has been achieved through the use of VLANs, ACLs, and firewall policies. Identify the types of threats that the network may face and the level of security needed to protect against them. This include configuring firewalls, VPNs, and intrusion detection systems (IDS).**

**Establishing access policies that require authentication and authorization which ensure that only authorized users are allowed to access the network. Using Cisco's Software Defined Access (SDA) via Identity Services Engine (ISE) help to enforce such policies and integrated with various authentication protocols such as RADIUS, TACACS+. Consider the latest security features and capabilities. Continuously update the security infrastructure of the network, by regularly applying security patches, staying informed about the latest vulnerabilities and implementing the necessary protections. Perform periodic security assessments to identify and address potential vulnerabilities in the network. This can help ensure that the network remains secure over time. Finally, network monitoring and management tools such as Cisco's Prime Infrastructure and DNA Center, to allow real-time network visibility and help quickly identify and respond to security threats, outages, and performance issues.**

**Logical addressing & Equipment configurations**

**The network will use logical addressing (IP addresses) to identify and communicate with each device on the network. This will involve designing and assigning IP addresses to each endpoint, and configuring routing protocols to enable communication between the two sites.**

**Logical IP addressing with Variable Length Subnet Masking (VLSM) is a method of IP addressing that allows for more efficient use of IP address space. VLSM, allows for the use of different subnet masks within a network, which means that subnets of different sizes can be created, allowing for more efficient use of IP address space. This allows for easy identification of the location or department to which a particular device or user belongs. It helping me to conserve IP address space and ensure optimal network performance.**

**Logical IP addressing Table**

**The network will use Cisco networking equipment, including routers, switches, and firewalls. These devices will be configured to ensure the security and reliability of the network. This will involve configuring access control lists (ACLs), virtual private network (VPN) tunnels, and other security features. The list of tasks is exhausting here are some relevant tasks.**

* **Configure basic settings: Set the hostname, domain name, and IP address of the device. Etc...**
* **Set up security: Configure password authentication for console and remote access, and enable any necessary security features such as SSH Etc…**
* **Configure routing: Set up dynamic routing protocols such as EIGRP to enable the device to forward traffic between networks etc…**
* **Configure VLANs: Set up virtual LANs (VLANs) to segment the network into different logical domains, and assign interfaces to the appropriate VLANs etc…**
* **Configure services: Configure any necessary services such as DHCP, NAT, QoS to provide network functionality etc…**

**List of some used PROTOCOLS**

* **Spanning Tree Protocol (STP)**
* **Dynamic Host Configuration Protocol (DHCP)**
* **Domain Name System (DNS)**
* **Simple Network Management Protocol (SNMP)**
* **Enhanced Interior Gateway Routing Protocol (EIGRP)**
* **Hot Standby Router Protocol (HSRP)**
* **Internet Group Management Protocol (IGMP)**
* **Internet Protocol Security (IPsec)**
* **Secure Shell (SSH)**
* **Network Address Translation (NAT)**
* **Virtual Local Area Network (VLAN)**
* **Quality of Service (QoS)**
* **Link Aggregation Control Protocol (LACP)**
* **Cisco Discovery Protocol (CDP)**
* **Link Layer Discovery Protocol (LLDP)**

**System Surveillance Camera**

**To incorporate a system surveillance camera into your VPN network, we use IP cameras that connect to the network via Ethernet cables. Here are some relevant steps to set up a surveillance camera:**

* **Install the cameras at strategic locations on each site, such as entrances, exits, and common areas.**
* **Connect the cameras to the network using Ethernet cables.**
* **Configure the cameras to send video streams over the network. This involves setting up the IP address, port number, and other parameters.**
* **Install a video management system (VMS) software on a server or computer on your network. The VMS software will allow you to view and manage the video streams from the cameras.**
* **Set up access controls to ensure that only authorized personnel can view the video streams. This can include setting up user accounts and passwords or using two-factor authentication.**

I remember throughout this project I struggle with a lot of pressure, with whole night no sleep because I lost the network equipement configuration's after almost done, and I had to present the project with a short amount of time. But it's worth the pain and to be honnest I loved spending whole night no sleep by configuring, troubleshooting,

I find it awesome!! because I'm a passionnate of what I do. I gain lot of understanding throughout this project

In order to achieved this project I designed it like this:

In the network I implement:

All the basics configurations like: renamed, encryption, SSH etc...

A virtual local area network (VLAN) I used it to segment the network into smaller segments.

It's help me to improve network security and performance, provide easier management, as well

as ensuring network flexibility. I ordered the Vlans like this : Native VLAN, Voice VLAN,

Management VLAN, Data VLAN.

Spanning Tree Protocol (STP) I Specifically Rapid spanning tree (RSTP) to help me prevent bridge looping

on LANs that include redundant links. Without RSTP, it would be difficult for me to implement that redundancy

and still avoid network looping.

VLAN Trunking Protocol (VTP) - To simplify the configurations, I configure all the access switches as VTP client and the

switches layer 3 int the middle as VTP Client.

Link Aggregation Control Protocol(LACP) - Even though I'm using only CISCO equipement I did'nt use PAgP for the

etherchannel because if I have to change an equipement other than CISCO. PAGP is a cisco-proprietary protocol and LACP

is quite the opposite, Defined within IEEE 802.3ad Besides, LACP can support cross-stack, while PAGP does not since

it does not support participating interfaces on different physical switches.For the purpose of load balancing,

I'm able to balance the traffic load across the links and improves the efficient use of bandwidth.

Port Security to help me secure the network by preventing unknown devices from forwarding packets.

Once a device connected the switch learn his MAC address, if someone put another devices on that specific

port, immediately that specific port will shutdown. I shutdown every unused ports on the switches,

I also used a radius server for the WIFI signal. that's how I secure the network from unknown devices

For the Network redundancy I'm providing multiple paths for traffic, so that data can keep flowing even in the

event of a failure. for me redundancy equals more reliability.

EIGRP - I used on routers and Layer 3 switches to share routes with other routers, I could use

OSPF but I personnaly love EIGRP for his simplicity and it's a CISCO protocols so!!

For communication Purpose between I use in the simulation VPN with GRE but in real life it's VPN with IPsec with the

cisco ASA 5525 firewall which I experienced before in real life through the competences fair.

In real life it's dual ISPs I mean failover but because of packet tracer bugs and unvaillable features. in the simulation

for testing purpose I configured with one ISP.

for the simulation purpose I used a server for the IP-camera and configure a Router as a VoIP server. But

in real life it will a server for VoIP rather than a router and for the IP-camera a NVR rather the a server.

To simplify the IP configuration I used DHCP servers for PCs, Cameras, Servers, Printers etc..