South Brokers Zrt. project English presentation

Our task was to build a complete network for a fictional environment including mandatory and custom elements. In our case this environment is an investment company called South Brokers, and we are the IT employees of it. With the help of Cisco Packet Tracer, I will explain the different sites on the topology map. The company has four sites, and a guest Wi-Fi network. The green area is our main office, all the employees work here. The end-devices are separated by VLANs which are operated by VTP on our four switches. We have also scripted a python program to change VTP passwords easily. These switches are also configured with LACP and Rapid STP for increased redundancy, port-security and DHCP Snooping for better security. We have two routers, therefore two exit points from this site. These two routers are configured with dynamic NAT and ACLs for security and HSRP for proper traffic priority. This is due to the fact, that our main servers are in a data centre which is represented by the orange area. The main exit route is through the South Brokers\_Main router, and is protected by IPsec, which authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. The secondary exit route is through the ISP and is protected by PPP technology with CHAP authentication. For a dynamic routing protocol, we chose EIGRP version two and three since we operate with both IPv4 and IPv6 addresses.

In this data centre we have three Linux Debian Servers. The first one is our Domain Controller, which also provides Active Directory, DNS, and DHCP. In the event of a malfunction in the first server, we have a Secondary Domain Controller, which takes over the responsibilities. Our third Linux server is used for a private email service, virtual private network, and printer sharing for the internal network. Besides the Linux servers we also have a 2019 Windows GUI Server. This provides certification for our responsive website which uses URL rewrite to redirect from HTTP to a secure HTTPS connection. Besides this, for remote file transfer, we use a secure sFTP which is also certificated. Our local workers have shared and personal internal storage to store data.

The blue area represents the local bank where we store our client’s confidential data. We used a high-performance Cisco ASA firewall in order to maximize the protection.

The pink area is the wireless network provided at our main office for up to 200 guests.

The last area, yellow, represents the company’s home office workers. They can only access the internal network via VPN service.

All in all, this is how our investment company works in essence, but we are still open for suggestions. Thank you for your attention!