South Brokers Zrt. project English presentation

Bendi:

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 PVST 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. **Now Laci will explain the rest of the topology.**

Laci:

The orange area represents the data center in which our main servers are located. The first server provides DNS,FTP,TFTP and WEB services, and is available through both IPv4 and IPv6. The second server is responsible for MAIL, SYSLOG and NTP services. For security we applied ACL restrictions so that only the administrator can ping the servers, but their services are accessible from outside.

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. With the help of multiple access points, the guest WiFi network is available in the whole area.

The last area, yellow, represents the company’s home office workers. They can only access the internal network via Cisco’s Anyconnect VPN service, and two factor authentication. **Now Bendi will explain our virtualized servers**

Gyula:

With the help of Oracle VirtualBox software, we were able to create the servers and services in a virtual environment. We have five Linux Debian Servers, and a Windows Server. The first Linux server 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. Our fourth one is an OpenVPN server, which hides our ip addresses. Our last Linux server is for 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.

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