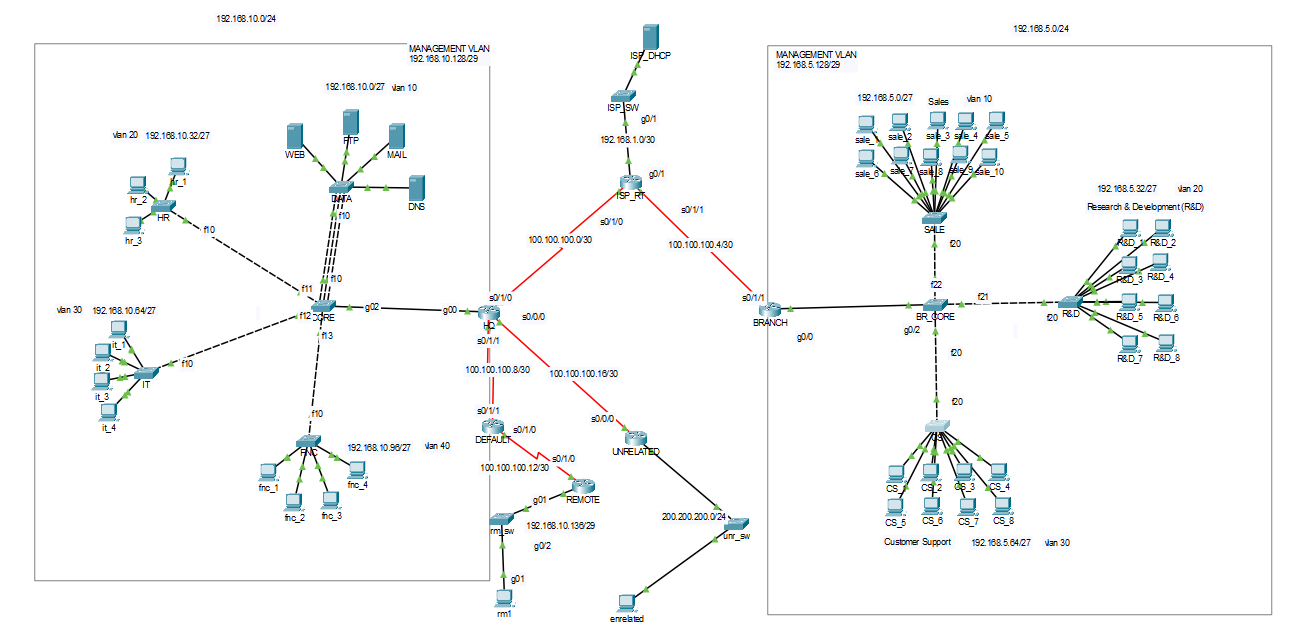
SECURITY POLICY SUMMARY



Firstly, I should mention the architecture of the company system. There are headquarters addressed as a HQ and branch. According to company policy company decided:

This company made a request to get 192.168.10.0/24 and 192.168.5.0/24 to use their device. And made their mind on that 192.168.10.0 would be HQ and 192.168.5.0 would be BRANCH. And get an DHCP server to serve internet as a trail and also make branch use.

The company structured should be required:

-All user included internet can reach web server  
-Reaching FTP SERVER was just allowed by head of vlan(like hr\_1, it\_1, r&d\_1 and so on..)  
-No one from outside can sent mail

-Branch devices can send mail to hq

-Every switch and router belongs to office should have password

-Remote users are not allowed to connect headquarters without vpn

-DNS Server is given permission to serve pc in headquarters and remote users

What security policy applied after those restriction:

1-NAT both side  
2-Give every router and swich in company network

3-For remote user create VPN

4-Write ACL required interfaces to give access to certain device for smtp and ftp

5-Use MAC Violation to provide security in company

6-Configure servers without unnecessary service (ex: http ,telnet…)

\*Detail of configuration is explained in Report