**OUTCOMES OF THE PROJECT**

1. Built a hierarchical topology with departments required
   1. Departments were finance, HR, Marketing, software development and an additional for walk in customers.
   2. The walk in customers were provided internet access as shown in our topology.
   3. The websites they visit are monitored using Snort. Its intrusion detection system takes care of this.
   4. Blocking of websites can be done using Snort’s intrusion prevention system with keywords when and where required
2. Computer hardware requirements were met with i.e # of computers in departments.
3. Access constraints were met using Access Control Lists in Cisco packet tracer.
4. Security of on host devices is provided using Snort
   1. Snort’s intrusion prevention system takes care of this -> ip rules are configured the same for devices at the same security level
5. Common servers between marketing and software departments to ensure that the data between them is transparent.
6. Centralized printing is available for each department for each floor.
7. Centralized management is provided as shown in the upper half of our topology.
8. 3 9’s availability was not very hard to provide a normal topology was sufficient.
9. Initially classless addressing was used but later we shifted to classful as RIP did not provide its functionality to classless addressing.
10. Long term cost effectiveness was provided with the scalability features using the hierarchical model.

Additional features and their uses

1. **haproxy** load balancer : HAProxy is free, open source software that provides a high availability load balancer and proxy server for TCP and HTTP-based applications that spreads requests across multiple servers. It is written in C and has a reputation for being fast and efficient.
   1. Use : Increases the responsiveness and availability as we need 3 9’s

Another folder in the same contains a folder on how we implemented our load balancer and a video demonstrating it.

1. Snort : Snort is a free open source network intrusion detection system and intrusion prevention system.
   1. Use : Most of our security constraints such as blocking websites, malicious IP addresses are implemented using Snort.

Another folder in the same is dedicated to our exploration of Snort and the explanation for it.

Our topology is enclosed in the same folder for your reference

At the end of the project we felt that if taken to production it would make a decent job.