**Report**

**Design Concept**

The network security hierarchy will elaborate the security from all the concerns and parameters of an entire network security regarding to standards and policies we have design complete network architecture which we design as a segregated network wired and wireless and combination of and IT devices. Mainly we have 3 branches and one is head office (Ottawa). All sites are properly connected with each other and proper communicate with each other and all sites have the wired and wireless solution deployed. All these devices are connected with each other and communicate with each other. We use L3 devices for WAN connectivity on each site for Routing purpose and use L3 Switch which have the ability to route the traffic as well as switch the traffic on each site. And for all site we use L2 device (Switch) for Switching Purpose.

As per WAN Connectivity we use Point to Point links to connect all sites with HeadOffice (Ottawa) and then for communication we use RIP Protocol to interconnect all branches with HeadOffice (Ottawa) and All L3 devices is directly connected with Branch Edge Router on each site the we Connect LAN L2 Switches with L3. So if we observe the flow of Data So when some want to communicate with other site so LAN generate the traffic which is shifted to L3 and then L3 forward it to Branch Edge router and all edge routers are connected via Physical wires and also use RIP protocol so that every easily ping each other. On Wireless Area we have represent it as a Devices which is also do communicate within our LAN as well as communicate with other sites.

All of the procedures and standards will be applied to entire resources and Information Technology systems from Core Network Infrastructure to the trainings and awareness for employees. The scope is to secure all the computing devices connected to IT Infrastructure. All the physical security will also be covered along with the security of data and maintenance.

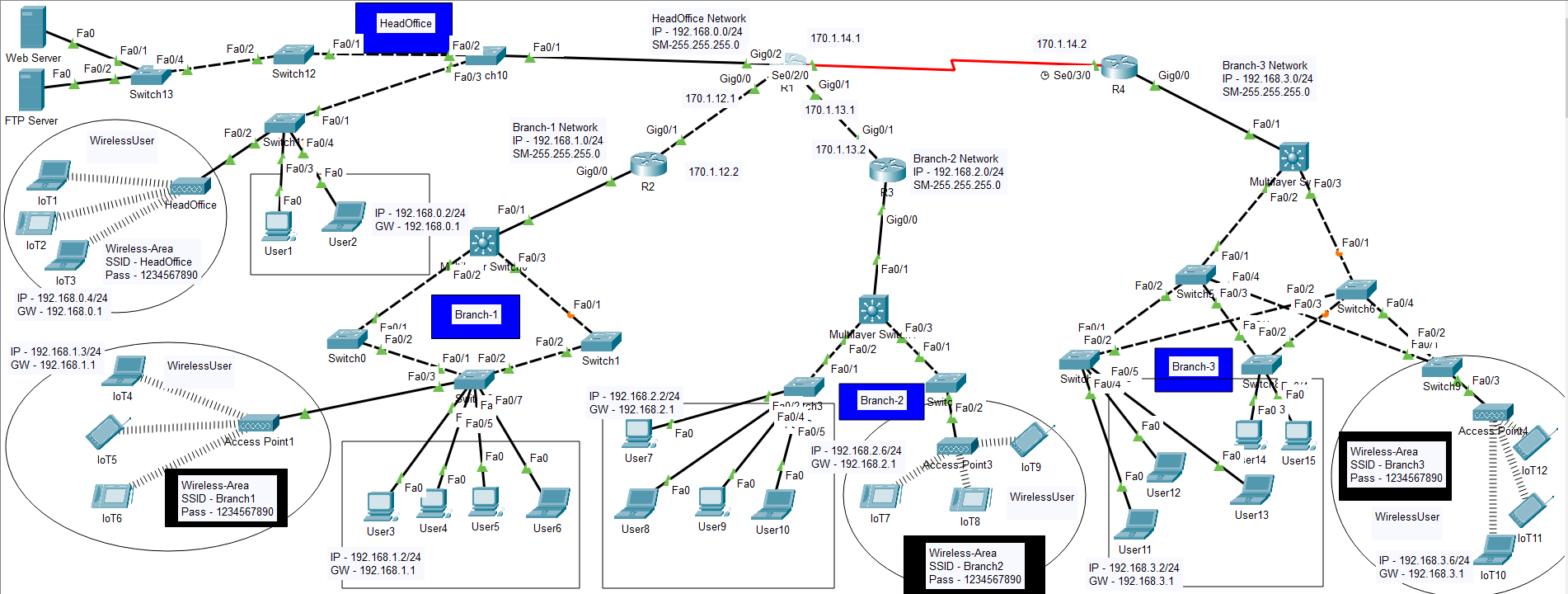
By considering the major objective of this Plan to secure the complete infrastructure the incident response team will be responsible for immediate threat identification, analysis of risks and take quick steps for risk mitigation to make sure the integrity of information systems and their Data resources.

**Managing the data**

The data management and controlling plan should be followed to make sure the data is valid and verified by the controlling department and integrity will also be assessed to make sure the data is correct and protection features are working properly. By applying data batch processing it is to make sure the data remain the same and the information resides in is accurate.

Data security policies should be applied from windows domain Servers or from the secure gateways against the data stealing from outside networks.

**Network Diagram**



**IP Configuration**

**Branches Connectivity**

HeadOffice (Ottawa) to Branch-1 (P2P Link) – 170.1.12.0/24

HeadOffice (Ottawa) to Branch-2 (P2P Link) – 170.1.13.0/24

HeadOffice (Ottawa) to Branch-3 (P2P Link) – 170.1.14.0/24

**Branches IP Networks**

HeadOffice (Ottawa) – 192.168.0.0/24 (Gateway – 192.168.0.1)

Branch 1 - 192.168.1.0/24 (Gateway – 192.168.1.1)

Branch 2 - 192.168.2.0/24 (Gateway – 192.168.2.1)

Branch 3 - 192.168.3.0/24 (Gateway – 192.168.3.1)

**Interface Connectivity & IP Assignment:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Gateway** |
| **R1(Ottawa)** | Gig 0/2 | 192.168.0.1 | 255.255.255.0 | - |
| Gig 0/0 | 170.1.12.1 | 255.255.255.0 | - |
| Gig 0/1 | 170.1.13.1 | 255.255.255.0 | - |
| Se 0/2/0 | 170.1.14.1 | 255.255.255.0 | - |
| **R2 ( Branch – 1)** | Gig 0/1 | 170.1.12.2 | 255.255.255.0 | - |
| Gig 0/0 | 192.168.1.1 | 255.255.255.0 | - |
| **R3 ( Branch – 2)** | Gig 0/1 | 170.1.13.2 | 255.255.255.0 | - |
| Gig 0/0 | 192.168.2.1 | 255.255.255.0 | - |
| **R4 ( Branch – 3)** | Gig 0/0 | 192.168.3.1 | 255.255.255.0 | - |
| Se 0/3/0 | 170.1.14.2 | 255.255.255.0 | - |
| **Web Server** | Eth0 | 192.168.0.9 | 255.255.255.0 | 192.168.0.1 |
| **FTP Server** | Eth0 | 192.168.0.10 | 255.255.255.0 | 192.168.0.1 |
| **User-1** | Eth0 | 192.168.0.3 | 255.255.255.0 | 192.168.0.1 |
| **User-2** | Eth0 | 192.168.0.2 | 255.255.255.0 | 192.168.0.1 |
| **User-3** | Eth0 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 |
| **User-4** | Eth0 | 192.168.1.4 | 255.255.255.0 | 192.168.1.1 |
| **User-5** | Eth0 | 192.168.1.5 | 255.255.255.0 | 192.168.1.1 |
| **User-6** | Eth0 | 192.168.1.6 | 255.255.255.0 | 192.168.1.1 |
| **User-7** | Eth0 | 192.168.2.2 | 255.255.255.0 | 192.168.2.1 |
| **User-8** | Eth0 | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 |
| **User-9** | Eth0 | 192.168.2.4 | 255.255.255.0 | 192.168.2.1 |
| **User-10** | Eth0 | 192.168.2.5 | 255.255.255.0 | 192.168.2.1 |
| **User-11** | Eth0 | 192.168.3.2 | 255.255.255.0 | 192.168.3.1 |
| **User-12** | Eth0 | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 |
| **User-13** | Eth0 | 192.168.3.4 | 255.255.255.0 | 192.168.3.1 |
| **User-14** | Eth0 | 192.168.3.5 | 255.255.255.0 | 192.168.3.1 |
| **User-15** | Eth0 | 192.168.3.7 | 255.255.255.0 | 192.168.3.1 |
| **User-1** | Wireless Port | 192.168.0.6 | 255.255.255.0 | 192.168.0.1 |
| **User-2** | Wireless Port | 192.168.0.5 | 255.255.255.0 | 192.168.0.1 |
| **User-3** | Wireless Port | 192.168.0.4 | 255.255.255.0 | 192.168.0.1 |
| **User-4** | Wireless Port | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| **User-5** | Wireless Port | 192.168.1.7 | 255.255.255.0 | 192.168.1.1 |
| **User-6** | Wireless Port | 192.168.1.8 | 255.255.255.0 | 192.168.1.1 |
| **User-7** | Wireless Port | 192.168.2.6 | 255.255.255.0 | 192.168.2.1 |
| **User-8** | Wireless Port | 192.168.2.7 | 255.255.255.0 | 192.168.2.1 |
| **User-9** | Wireless Port | 192.168.2.8 | 255.255.255.0 | 192.168.2.1 |
| **User-10** | Wireless Port | 192.168.3.6 | 255.255.255.0 | 192.168.3.1 |
| **User-11** | Wireless Port | 192.168.3.8 | 255.255.255.0 | 192.168.3.1 |
| **User-12** | Wireless Port | 192.168.3.9 | 255.255.255.0 | 192.168.3.1 |
|  |  |  |  |  |

**Equipment security consideration**

All the security measurements taken by any organization follow the rules and standards against the threats and vulnerabilities. Securing the data and information systems is the major concern of any environment. We has been proposed by the complete network infrastructure security. The infrastructure security and device hardening provide the facility against the vulnerabilities and threats. Cyber security plan blocks all the loopholes and backdoors in an environment to mitigate the risk of vulnerabilities and threats. Infrastructure security mechanism deployed in consideration of all the latest trends and technologies to ensure the network availability and data reliability. Advanced techniques are used from core to the user to present the business goals in a protected environment.

**Authentication\logging methods**

The data management and controlling plan should be followed to make sure the data is valid and verified by the controlling and integrity will also be assessed to make sure the data is correct and protection features are working properly. By applying data batch processing it is to make sure the data remain the same and the information resides in is accurate.

1. Password sharing will be strictly prohibited
2. Password expiry will occur within 60 days. All the users have to change the passwords of their accounts periodically.
3. Database accounts passwords will be expired after every 30 days
4. Whenever any person leave their roles their employee account and their data will be collected by Network Security departments.

**Wireless Settings**

In this topology we have configured wireless network on which we have connected different devices on all sites. We use Wireless standalone Access Point AP which spread the Wi-Fi signals and connected with Devices. This Wi-Fi work on 2.4 GHz range in a network. We have wired network which is part of LAN and Wireless Area is also part of our LAN but on Wi-Fi Area we represent it as . All system have a static IP Address as per subnet wise.

**Wi-Fi-Modules:**

The PT-REPEATER-NM-1CE features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.

The PT-REPEATER-NM-1FFE Module provides one Fast-Ethernet interface for use with fiber media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet.

**Wired & Wireless Users Internet Security:**

The Airport Infrastructure security team will follow the procedures and standards for response against the security incidents occurred according to the Airport IT and Data protection rules. Following steps must to be followed in case any incident occurred:

* Reporting incidents
* Incident Control
* Notifying Concerns
* Investigating against incident
* Final Reporting and recommendations against the incident.

**Users Credentials Security**

Separate policies should be applied with different privileges. Faculty and teaching staff will get the administrative privileges to the portals and Airport applications according to their job roles. All the users must to be follow WLV standards. All of the users should follow the below security best practices.

1. Password sharing will be strictly prohibited
2. Password expiry will occur within 60 days. All the users have to change the passwords of their accounts periodically.
3. Database accounts passwords will be expired after every 30 days
4. Whenever any person leave their roles their Airport account and their data will be collected by Airport Soc departments and will only reside under Airport custody

**Scalability of your design:**

* Using advance protocols and smart configurations
* Follow the IEEE standards of 2 tier architecture making network more scalable and available due to multiple links of aggregation.
* The modular switches and routers will be added for scenario base deployments
* Installing the less products and getting the maximum performance from them for what they actually designed for.
* To get the maximum availability of network the failover will be configured to eliminate the single point of failure concept.

**References**

|  |
| --- |
| W&L, "Information Security Plan," February 2017. [Online]. Available: https://my.wlu.edu/its/about-its/information-security-plan. [Accessed 14 May 2021]. |
| T. u. o. chicago, "GUIDELINES FOR THE SECURE MANAGEMENT OF IT INFRASTRUCTURE SYSTEMS THAT PROCESS, TRANSMIT, OR STORE CONFIDENTIAL INFORMATION," 2021. [Online]. Available: https://its.uchicago.edu/guidelines-secure-management-it-infrastructure-systems-process-transmit-or-store-confidential/. [Accessed 12 May 2021]. |
| O. o. i. security, "Infrastructure Security Policy," 26 February 2019. [Online]. Available: https://informationsecurity.wustl.edu/policies/infrastructure-security-policy/. [Accessed 13 May 2021]. |
| E. Dosal, "5 Critical Steps for Securing a Network Infrastructure," 28 June 2018. [Online]. Available: https://www.compuquip.com/blog/securing-network-infrastructure. [Accessed 12 5 2021].  **\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*** |