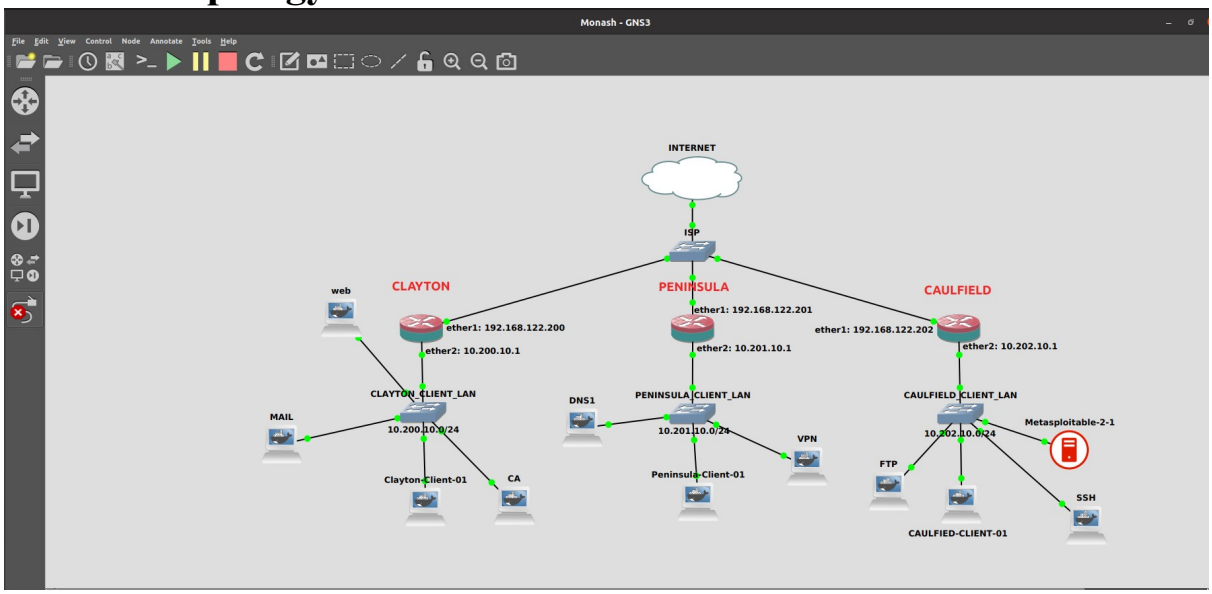
Secure Networking Report

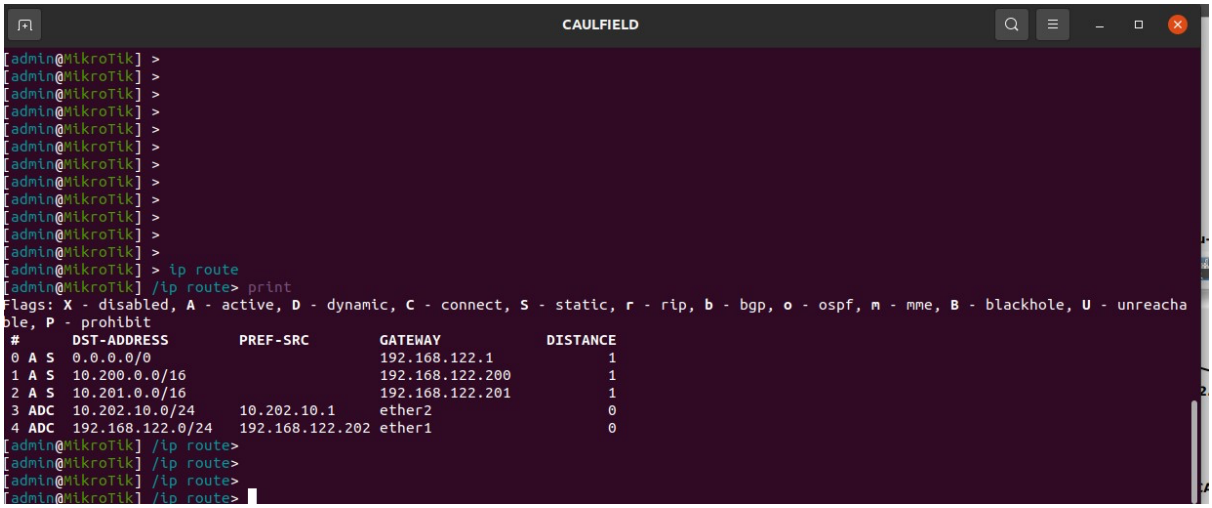
Secure Network Design and Implementation

Network Topology:



Clayton Router Routing table:

Caufield Router Routing table:



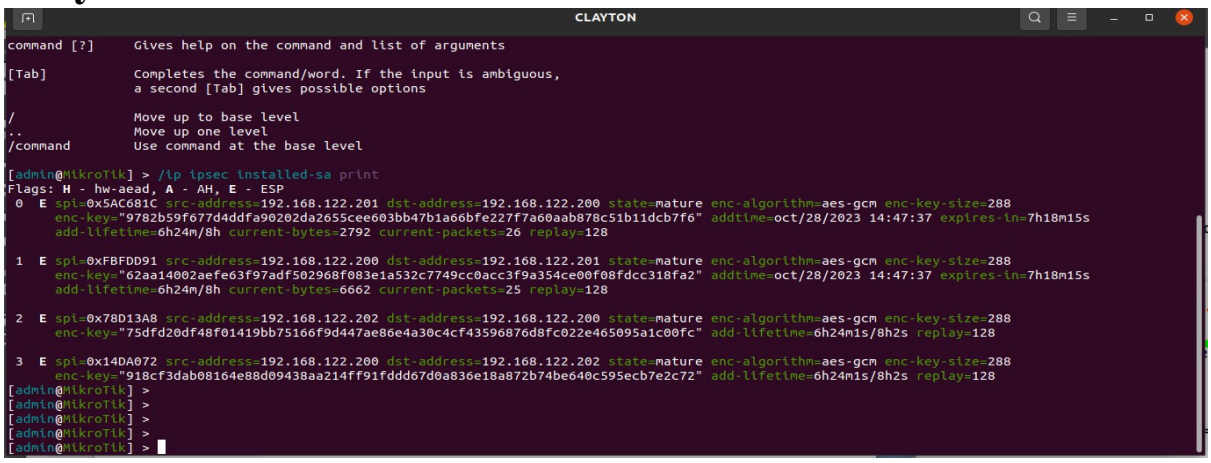
Peninsula Router Routing table:

Demonstration video:

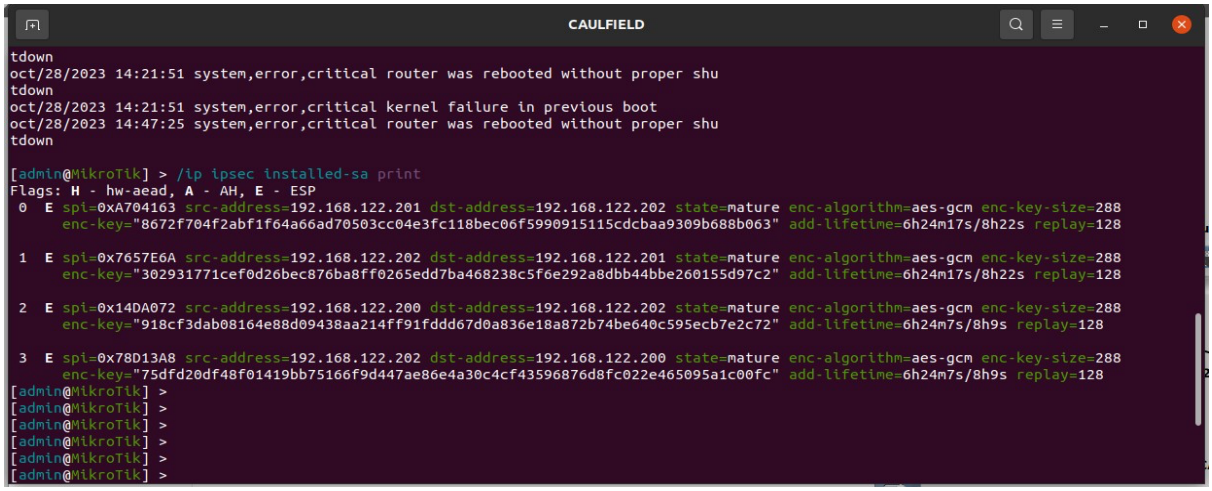
https://drive.google.com/file/d/1sTdf-F5_XE8TtDAjWYcQi5mhhd_GoZzN/view?usp=sharing

VPN

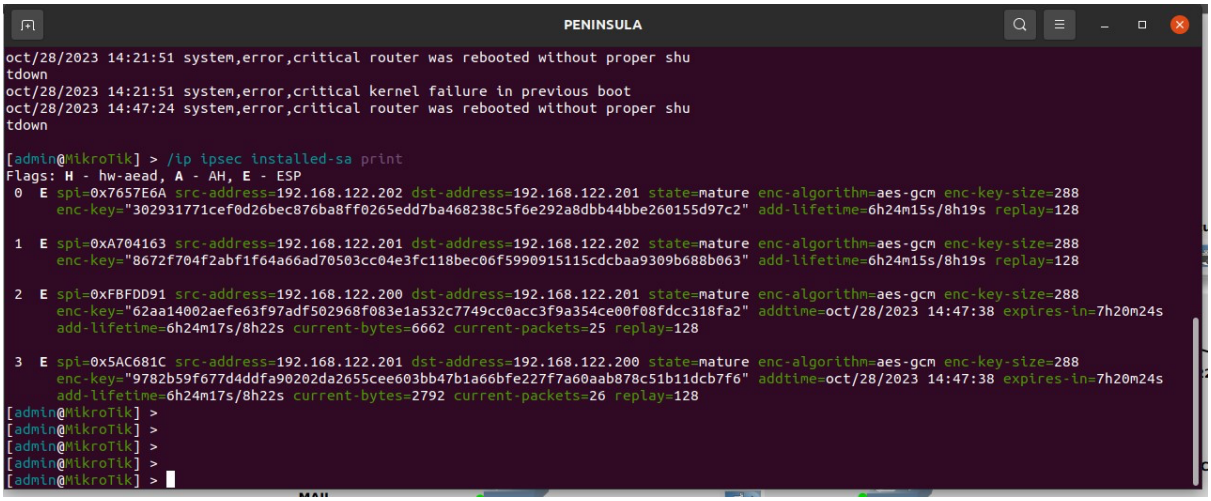
Clayton:



Caufield:



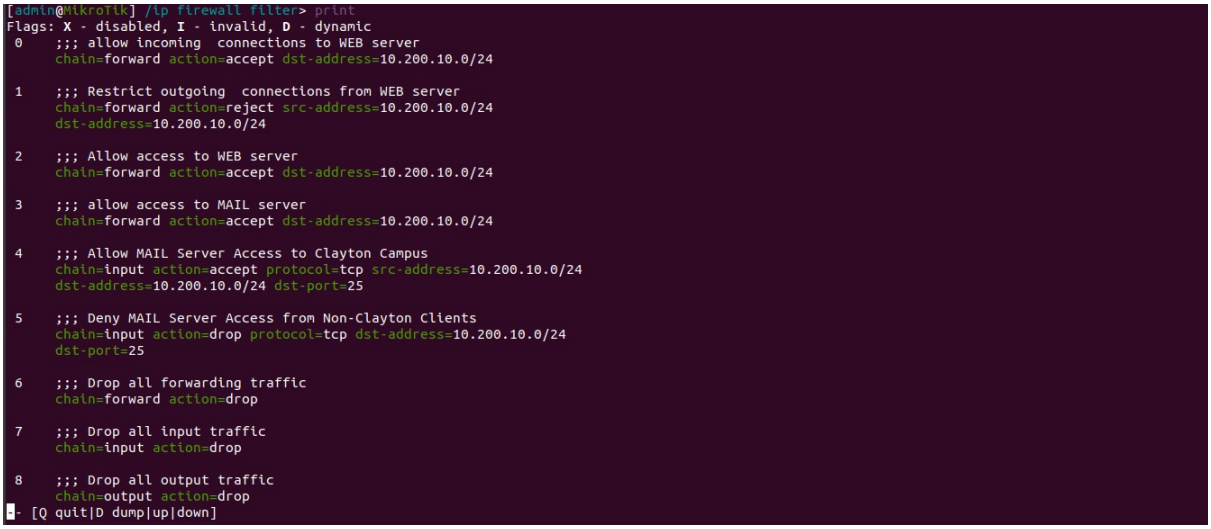
Peninsula:



Demonstration video showing esp packets:

https://drive.google.com/file/d/1sPb1k3nkLA0WhGdRl5UfF54IZ9Io6_vL/view?usp=sharing

Firewall:
Rules in each router: Clayton:



Caufield:

```
[admin@MikroTik] /ip firewall filter> print
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; Allow FTP Server Access to Caulfield Campus
      chain=input action=accept protocol=tcp src-address=10.202.10.0/24
      dst-address=10.202.10.0/24 dst-port=21

 1    ;;; Deny FTP Server Access from Non-Caulfield Clients
      chain=input action=drop protocol=tcp dst-address=10.202.10.0/24
      dst-port=21

 2    ;;; Drop all forwarding traffic
      chain=forward action=drop

 3    ;;; Drop all input traffic
      chain=input action=drop

 4    ;;; Drop all output traffic
      chain=output action=drop
[admin@MikroTik] /ip firewall filter>
```

Peninsula:

```
[admin@MikroTik] /ip firewall filter> print
Flags: X - disabled, I - invalid, D - dynamic
0     ;;; Allow access to DNS server froom internal clients only
      chain=forward action=reject src-address=10.201.10.0/24
      dst-address=10.201.10.0/24

1     ;;; Restrict outgoing connections from  VPN server
      chain=forward action=reject src-address=10.201.10.0/24
      dst-address=10.201.10.0/24

2     ;;; Allow access to VPN server
      chain=forward action=accept dst-address=10.201.10.0/24

3     ;;; Allow SSH Server Access to Peninsula Campus
      chain=input action=accept protocol=tcp src-address=10.201.10.0/24
      dst-address=10.202.10.0/24 dst-port=22

4     ;;; Deny SSH Server Access from Non-Peninsula Clients
      chain=input action=drop protocol=tcp dst-address=10.202.10.0/24
      dst-port=22

5     ;;; Drop all forwarding traffic
      chain=forward action=drop

6     ;;; Drop all input traffic
      chain=input action=drop

7     ;;; Drop all output traffic
      chain=output action=drop
```

Demonstration Video:

https://drive.google.com/file/d/1FHvyUWV7x7H9GCDDGglJizc7fiKL15oz/view?usp=sharing

Security Analysis

Bypassing Firewall Configuration: Although the firewall configuration is an important security measure, it can still be gotten around by using vulnerabilities in services that are allowed or by insider threats. Strict escape filtering must be used, and firewall rules must be updated frequently, to reduce these risks. dividing the network would reduce the impact of any security breaches. The firewall can be strengthened by creating rules that ban all traffic by default and only permit services that are absolutely necessary.

Additional Security Solutions: Intrusion detection and prevention systems (IDPS) should be installed at important network entry points to improve security. To provide the best protection possible, make sure every server has a solid antivirus programme that is updated frequently. To enhance security protocols, integrate multi-factor authentication and setup a virtual private network (VPN) for safe and secure remote access. All of these precautions work together to strengthen the network's defences against possible attacks and protect confidential data from harm.

General Security Recommendations: All round security advice: vulnerability detection depends on frequent security inspections and penetration testing. It's critical to keep firmware and software updated with the newest security fixes. Use of data encryption for sensitive data, strict password regulations, and employee training on security protocols are all crucial. To monitor network activity and spot possible threats in real time, it's also advised to integrate a specialised security information and event management (SIEM) system.

IDS

Setting up a system that can identify when someone is attempting to use Metasploit to gain access to a computer system is known as creating an intrusion detection system (IDS) rule. Additionally, you should monitor specifics such as the ports it uses, the types of messages it sends, and the methods it applies to gain access to systems. Once you are aware of these things, you can create a rule that instructs your system to sound an alert whenever it notices any of these questionable activities taking place.
It's critical to maintain this rule current by routinely looking for any new methods or hacks that Metasploit might be utilising. It's also crucial to test the rule to make sure it functions properly and doesn't trigger too many false alarms. You can ensure that your system is more adept at spotting attempts to use Metasploit against your computer network by taking these steps.

Ethical Conduct

The expectations for staff and students with regard to acceptable network behaviour, restricted activities, and unethical behaviours are outlined in the following policy guidelines. Respecting the principles of responsible digital citizenship and academic integrity requires commitment to these guidelines.

Appropriate Use of Resources:
Faculty and students at Monash University are all expected to use the network resources in an appropriate manner. This includes using the

network in a responsible and professional manner, making sure that activities complement the academic and research missions of the university. Users must stay away from any actions that might restrict or interfere with other users' ability to access the network. Avoiding unnecessary or excessive use of network storage or bandwidth is part of this, as it may affect the functionality of the network for other authorised users.

Data Security and Privacy:
Maintaining data security and privacy is a core value of the university's network. It is important that users stay away from any unauthorized access to data or systems, including trying to violate security protocols or obtain sensitive data without the necessary authorization. It is the duty of every user to keep their accounts secure and to make sure that their login information and personal data are kept private.

Respect for Intellectual Property:
It is important to maintain the values of academic integrity and show respect for the rights of intellectual property. Users are asked to stay away from violating copyright in all forms and to avoid using software, multimedia, and academic works without permission. Every academic and research activity carried out over the network needs to follow copyright regulations and properly cite sources.

Network infrastructure protection:
It is important that users give maintenance and defence of the network infrastructure top priority. This involves avoiding from any actions that can compromise the network's security and stability, such as trying to alter network configurations without authorisation or interfering with normal operations. Users should notify the relevant IT authorities as soon as they discover any vulnerabilities or issues with the network infrastructure.

Education and Training Responsibilities:

Educational and Training Responsibilities: It is the users' responsibility to stay up to date on the best practices for digital security. The university will provide the instruction and training required to guarantee commitment to the policy. Participation in these educational initiatives is required for all staff members and students, who also have to apply the knowledge they gain to their everyday network usage.

Depending on the seriousness of the violation of this Ethical Network Usage Policy may result in disciplinary action, which may include account suspension, network access cancellation, academic penalties, and legal consequences. All users are expected to read these guidelines carefully and to use the Monash University network in a way that reflects the highest moral principles.

GNS3:

https://drive.google.com/file/d/1RqPxHRbwG3a5pTrI76991PslbauG23b/view?usp=sharing