NETWORK SECURITY

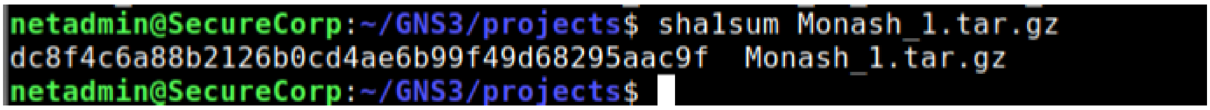
Project

NOVEMBER 1, 2024

MONISHRAJ MATHIVANAN

Contents

2. Hash of the gns3 Project file



```
netadmin@SecureCorp:~/GNS3/projects$ sha1sum Monash_1.tar.gz
dc8f4c6a88b2126b0cd4ae6b99f49d68295aac9f  Monash_1.tar.gz
netadmin@SecureCorp:~/GNS3/projects$ 
```

3. Scenario for the Assignment

For this assignment, the **primary data center (DC)** location is determined based on my **student ID (31942369)** using the following formula:

31942369 mod 3 = 1

Task 4: Secure Network Design and Implementation

This section outlines the secure network design across the three Monash campuses, implemented using **GNS3**. The **Primary Data Center (DC)** for this assignment is **Clayton**, as determined by my student ID (**31942369 mod 3 = 1**).

4.1 Network Topology

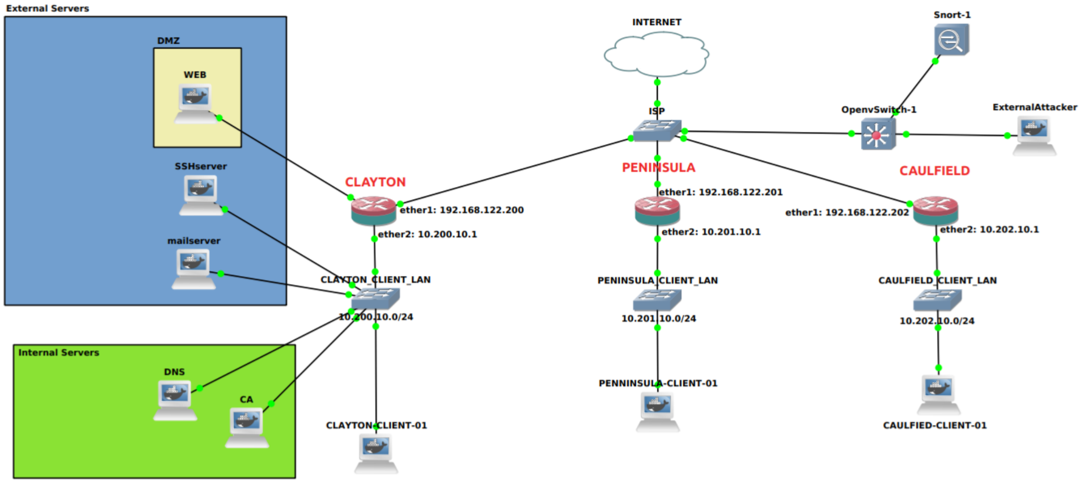


Figure 1: Above is the **GNS3 topology** showing the network layout

The network consists of:

- **Clayton (Primary DC)** hosting internal and external services.
- **Caulfield and Peninsula Campuses** connected via BGP routing with perimeter firewalls.

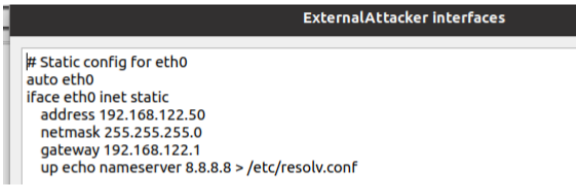
- **External-Attacker** connected to the ISP switch for testing purposes.
- **Web Server** placed in a **DMZ** for external access.

4.2 Campus Clients and IP Configuration

For campus clients, we used **auto-static IP assignment**. This simplifies IP configuration for end-users and makes it easier to manage devices connected to the network. Campus clients are on separate LANs per campus, and each router assigns static IPs within their respective subnets.

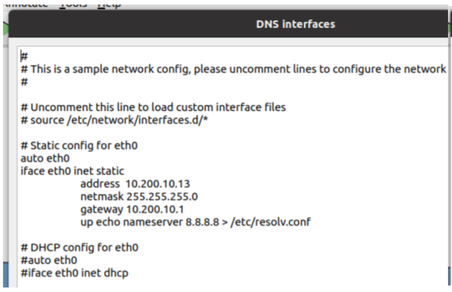
Campus	**Subnet**	**Device**	**IP Address**
Clayton	10.200.10.0/24	Clayton Router	10.200.10.1
		Clayton Client PC	10.200.10.10
Clayton DMZ (web)	10.200.20.0/24	Web server (external)	10.200.20.1
Caulfield	10.202.10.0/24	Caulfield Router	10.202.10.1
		Caulfield Client PC	10.202.10.10
Peninsula	10.201.10.0/24	Peninsula Router	10.201.10.1
		Peninsula Client PC	10.201.10.10

External attacker :



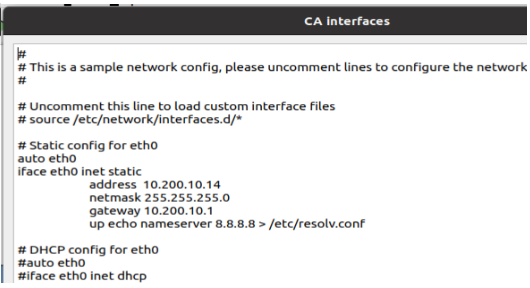
```
# Static config for eth0
auto eth0
iface eth0 inet static
   address 192.168.122.50
   netmask 255.255.255.0
   gateway 192.168.122.1
   up echo nameserver 8.8.8.8 > /etc/resolv.conf
```

Internal Servers in Clayton(Primary DC):



```
#
# This is a sample network config, please uncomment lines to configure the network
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
            address  10.200.10.13
            netmask 255.255.255.0
            gateway 10.200.10.1
            up echo nameserver 8.8.8.8 > /etc/resolv.conf

# DHCP config for eth0
#auto eth0
#iface eth0 inet dhcp
```

DNS

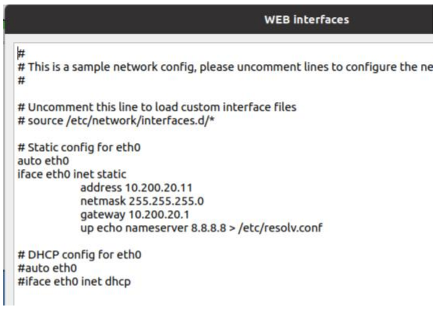


```
#
# This is a sample network config, please uncomment lines to configure the network
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
            address  10.200.10.14
            netmask 255.255.255.0
            gateway 10.200.10.1
            up echo nameserver 8.8.8.8 > /etc/resolv.conf

# DHCP config for eth0
#auto eth0
#iface eth0 inet dhcp
```

CA

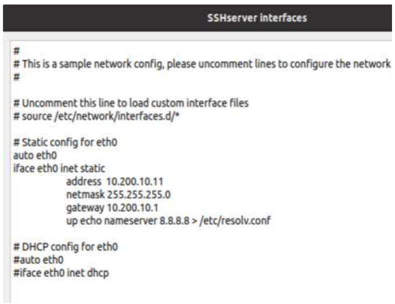
Internal Server	**Internal Server IP**
DNS server	10.200.10.13
CA server	10.200.10.14

External Servers in Clayton(Primary DC):



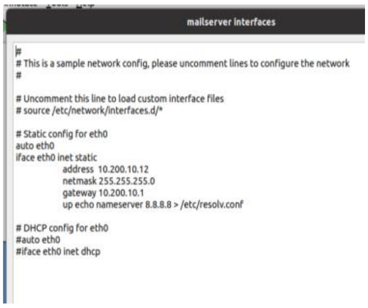
```
#
# This is a sample network config, please uncomment lines to configure the ne
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
            address 10.200.20.11
            netmask 255.255.255.0
            gateway 10.200.20.1
            up echo nameserver 8.8.8.8 > /etc/resolv.conf

# DHCP config for eth0
#auto eth0
#iface eth0 inet dhcp
```

WEB



```
#
# This is a sample network config, please uncomment lines to configure the network
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
            address  10.200.10.11
            netmask 255.255.255.0
            gateway 10.200.10.1
            up echo nameserver 8.8.8.8 > /etc/resolv.conf

# DHCP config for eth0
#auto eth0
#iface eth0 inet dhcp
```

SSH



```
#
# This is a sample network config, please uncomment lines to configure the network
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
            address  10.200.10.12
            netmask 255.255.255.0
            gateway 10.200.10.1
            up echo nameserver 8.8.8.8 > /etc/resolv.conf

# DHCP config for eth0
#auto eth0
#iface eth0 inet dhcp
```

Mailserver

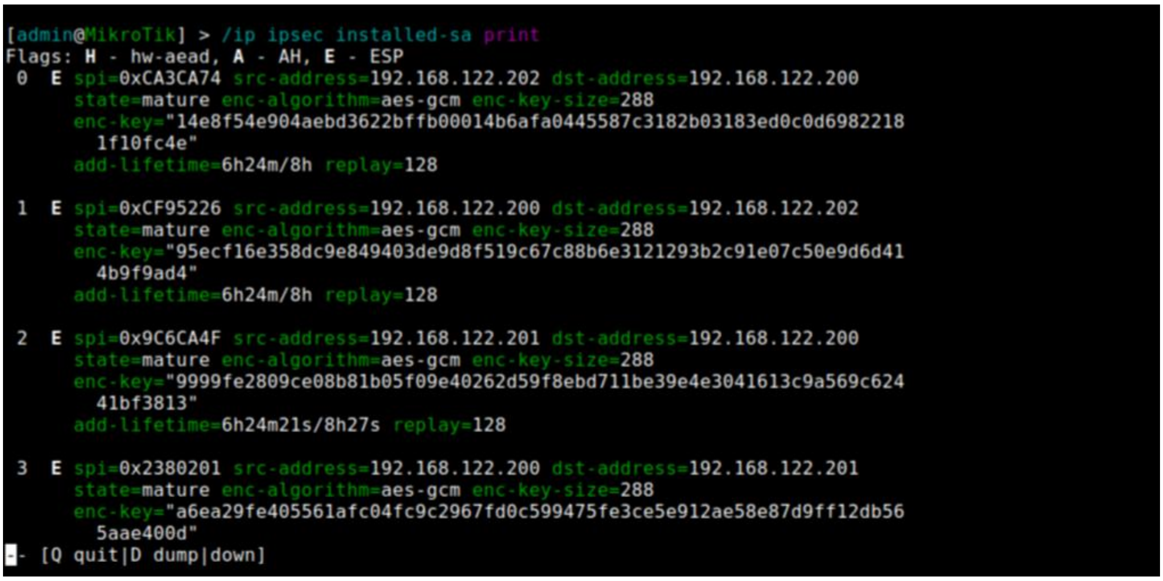
External Server	**External Server IP**
Web server	10.200.20.11
mailserver	10.200.10.12
SSH server	10.200.10.11

Task 5: BGP

A video has been recorded demonstrating the attack and the corresponding mitigation measures as required for this section.

Task 6: VPN

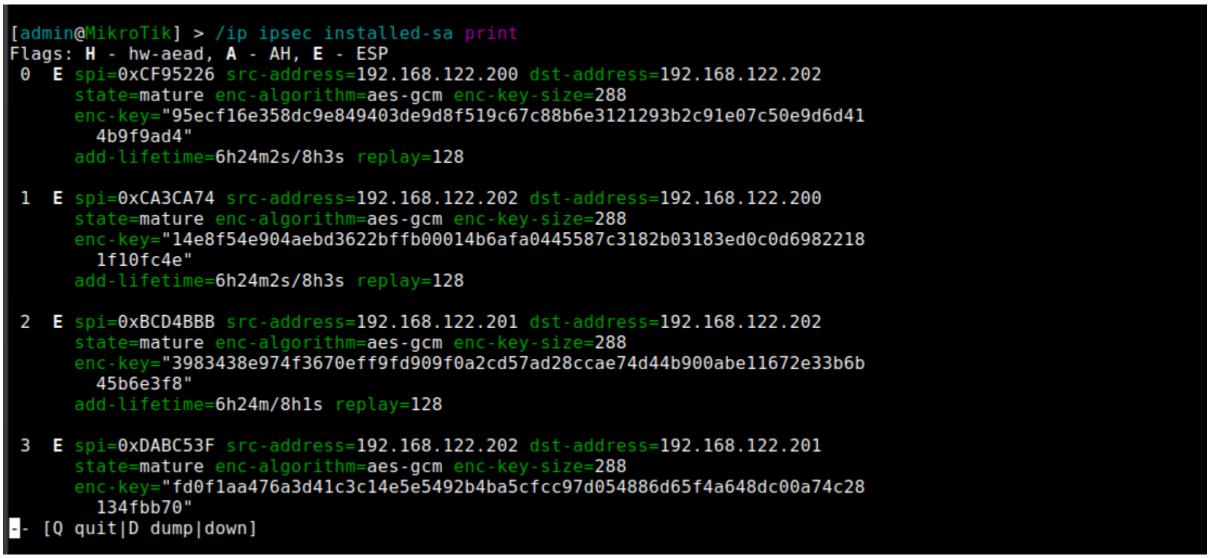
On clayton router:



```
[admin@MikroTik] > /ip ipsec installed-sa print
Flags: H - hw-aead, A - AH, E - ESP
 0  E spi=0xCA3CA74 src-address=192.168.122.202 dst-address=192.168.122.200
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="14e8f54e904aebd3622bffb00014b6afa0445587c3182b03183ed0c0d6982218
        1f10fc4e"
      add-lifetime=6h24m/8h replay=128

 1  E spi=0xCF95226 src-address=192.168.122.200 dst-address=192.168.122.202
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="95ecf16e358dc9e849403de9d8f519c67c88b6e3121293b2c91e07c50e9d6d41
        4b9f9ad4"
      add-lifetime=6h24m/8h replay=128

 2  E spi=0x9C6CA4F src-address=192.168.122.201 dst-address=192.168.122.200
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="9999fe2809ce08b81b05f09e40262d59f8ebd711be39e4e3041613c9a569c624
        41bf3813"
      add-lifetime=6h24m21s/8h27s replay=128

 3  E spi=0x2380201 src-address=192.168.122.200 dst-address=192.168.122.201
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="a6ea29fe405561afc04fc9c2967fd0c599475fe3ce5e912ae58e87d9ff12db56
        5aae400d"
-- [Q quit|D dump|down]
```

Figure 2: The command /ip ipsec installed-sa print shows active IPSec SAs on the Clayton router. AES encryption (288-bit) secures traffic between Clayton (.200), Caulfield (.202), and Peninsula (.201), with replay protection (128). All SAs are "mature," confirming active VPN connections.

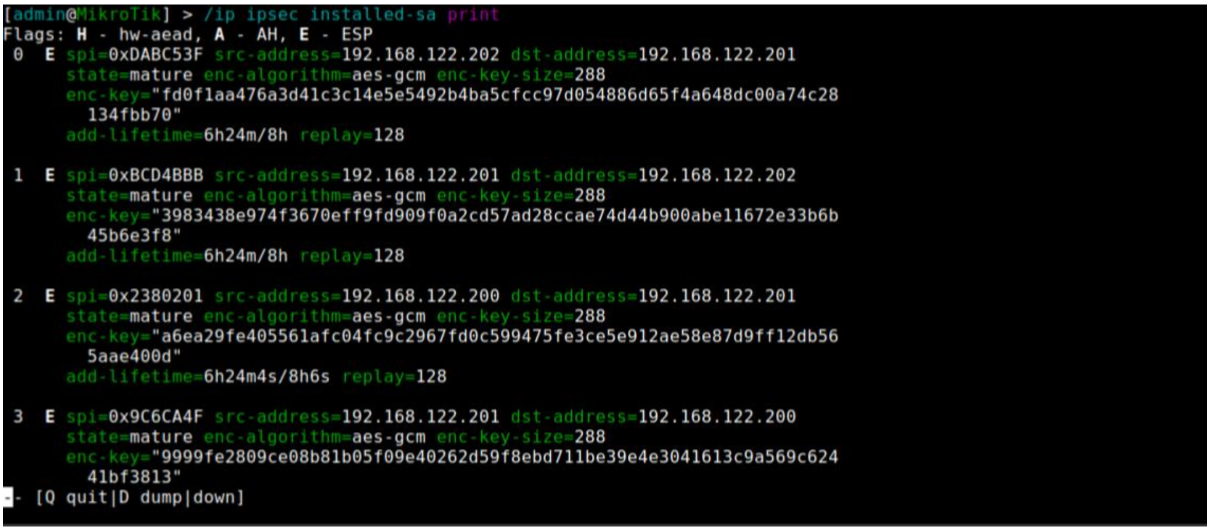
On Caulfield router:



```
[admin@MikroTik] > /ip ipsec installed-sa print
Flags: H - hw-aead, A - AH, E - ESP
 0  E spi=0xCF95226 src-address=192.168.122.200 dst-address=192.168.122.202
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="95ecf16e358dc9e849403de9d8f519c67c88b6e3121293b2c91e07c50e9d6d41
        4b9f9ad4"
      add-lifetime=6h24m2s/8h3s replay=128

 1  E spi=0xCA3CA74 src-address=192.168.122.202 dst-address=192.168.122.200
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="14e8f54e904aebd3622bffb00014b6afa0445587c3182b03183ed0c0d6982218
        1f10fc4e"
      add-lifetime=6h24m2s/8h3s replay=128

 2  E spi=0xBCD4BBB src-address=192.168.122.201 dst-address=192.168.122.202
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="3983438e974f3670eff9fd909f0a2cd57ad28ccae74d44b900abe11672e33b6b
        45b6e3f8"
      add-lifetime=6h24m/8h1s replay=128

 3  E spi=0xDABC53F src-address=192.168.122.202 dst-address=192.168.122.201
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="fd0f1aa476a3d41c3c14e5e5492b4ba5cfcc97d054886d65f4a648dc00a74c28
        134fbb70"
-- [Q quit|D dump|down]
```

Figure 3: The command /ip ipsec installed-sa print shows active IPSec SAs on the Caulfield router. AES-GCM encryption (288-bit) secures traffic between Caulfield (.202), Clayton (.200), and Peninsula (.201), with replay protection (128). All SAs are "mature," confirming active VPN connections.

On peninsula Router:



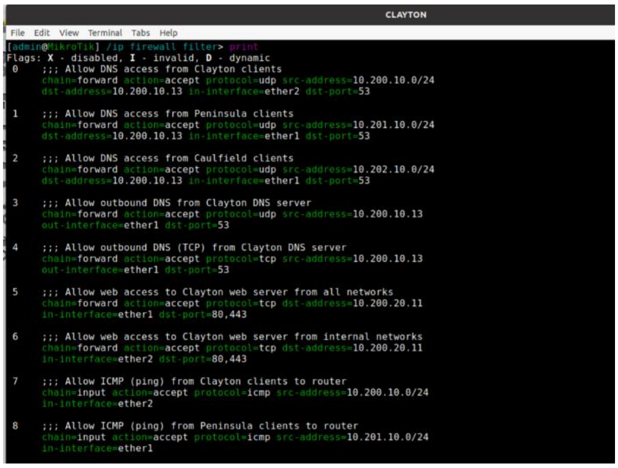
```
[admin@MikroTik] > /ip ipsec installed-sa print
Flags: H - hw-aead, A - AH, E - ESP
 0  E spi=0xDABC53F src-address=192.168.122.202 dst-address=192.168.122.201
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="fd0f1aa476a3d41c3c14e5e5492b4ba5cfcc97d054886d65f4a648dc00a74c28
        134fbb70"
      add-lifetime=6h24m/8h replay=128

 1  E spi=0xBCD4BBB src-address=192.168.122.201 dst-address=192.168.122.202
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="3983438e974f3670eff9fd909f0a2cd57ad28ccae74d44b900abe11672e33b6b
        45b6e3f8"
      add-lifetime=6h24m/8h replay=128

 2  E spi=0x2380201 src-address=192.168.122.200 dst-address=192.168.122.201
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="a6ea29fe405561afc04fc9c2967fd0c599475fe3ce5e912ae58e87d9ff12db56
        5aae400d"
      add-lifetime=6h24m4s/8h6s replay=128

 3  E spi=0x9C6CA4F src-address=192.168.122.201 dst-address=192.168.122.200
      state=mature enc-algorithm=aes-gcm enc-key-size=288
      enc-key="9999fe2809ce08b81b05f09e40262d59f8ebd711be39e4e3041613c9a569c624
        41bf3813"
-- [Q quit|D dump|down]
```

Figure 4: The command /ip ipsec installed-sa print shows active IPSec SAs on the Peninsula router. AES-GCM encryption (288-bit) secures traffic between Peninsula (.201), Caulfield (.202), and Clayton (.200), with replay protection (128). All SAs are "mature," confirming active VPN connections.

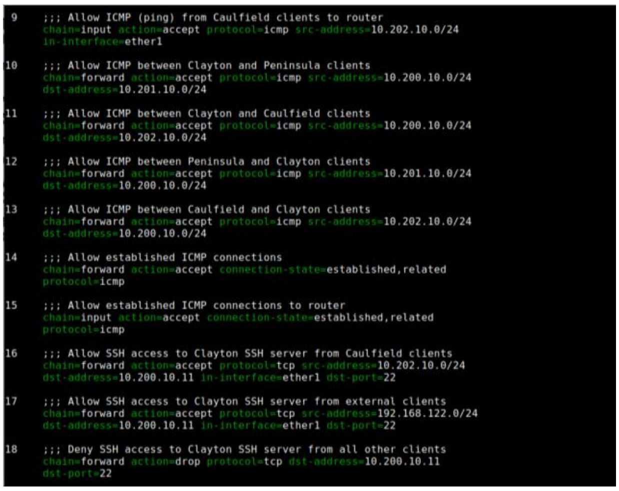
Task 7: Firewalls and Rules

Clayton firewall rules:

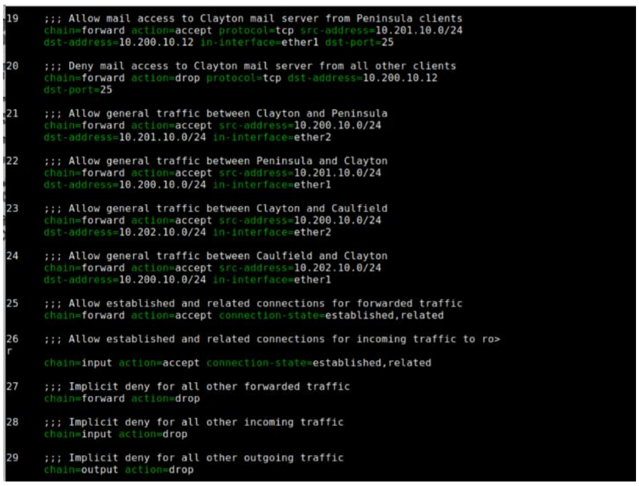
Allows DNS access from all campus clients and web access to the web server. Permits ICMP between subnets and to the router. Restricts SSH access to the SSH server to only Caulfield and external clients, and mail access to the mail server to only Peninsula clients. Enables inter-site traffic and allows established connections, with all other traffic denied.



```
[admin@MikroTik] /ip firewall filter> print
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; Allow DNS access from Clayton clients
      chain=forward action=accept protocol=udp src-address=10.200.10.0/24
      dst-address=10.200.10.13 in-interface=ether2 dst-port=53

 1    ;;; Allow DNS access from Peninsula clients
      chain=forward action=accept protocol=udp src-address=10.201.10.0/24
      dst-address=10.200.10.13 in-interface=ether1 dst-port=53

 2    ;;; Allow DNS access from Caulfield clients
      chain=forward action=accept protocol=udp src-address=10.202.10.0/24
      dst-address=10.200.10.13 in-interface=ether1 dst-port=53

 3    ;;; Allow outbound DNS from Clayton DNS server
      chain=forward action=accept protocol=udp src-address=10.200.10.13
      out-interface=ether1 dst-port=53

 4    ;;; Allow outbound DNS (TCP) from Clayton DNS server
      chain=forward action=accept protocol=tcp src-address=10.200.10.13
      out-interface=ether1 dst-port=53

 5    ;;; Allow web access to Clayton web server from all networks
      chain=forward action=accept protocol=tcp dst-address=10.200.20.11
      in-interface=ether1 dst-port=80,443

 6    ;;; Allow web access to Clayton web server from internal networks
      chain=forward action=accept protocol=tcp dst-address=10.200.20.11
      in-interface=ether2 dst-port=80,443

 7    ;;; Allow ICMP (ping) from Clayton clients to router
      chain=input action=accept protocol=icmp src-address=10.200.10.0/24
      in-interface=ether2

 8    ;;; Allow ICMP (ping) from Peninsula clients to router
      chain=input action=accept protocol=icmp src-address=10.201.10.0/24
      in-interface=ether1
```



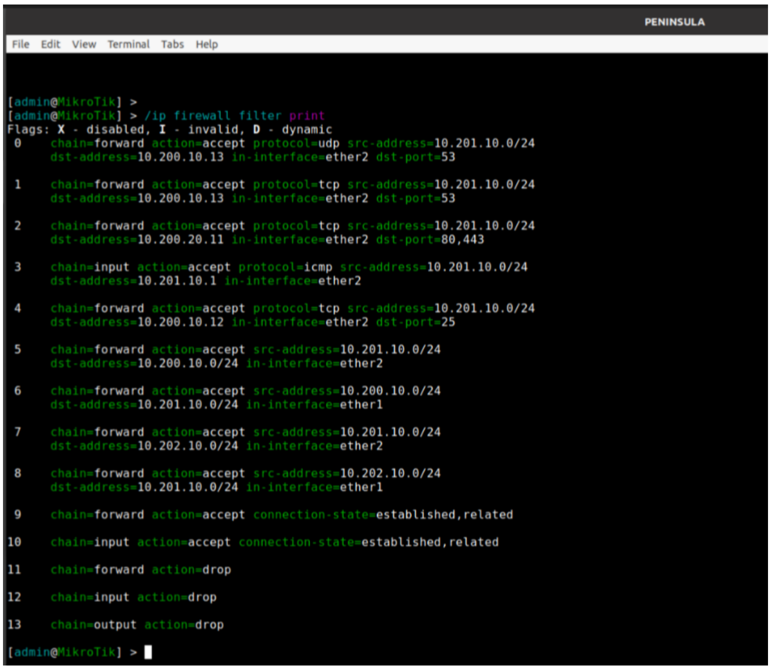
```
 9    ;;; Allow ICMP (ping) from Caulfield clients to router
      chain=input action=accept protocol=icmp src-address=10.202.10.0/24
      in-interface=ether1

10    ;;; Allow ICMP between Clayton and Peninsula clients
      chain=forward action=accept protocol=icmp src-address=10.200.10.0/24
      dst-address=10.201.10.0/24

11    ;;; Allow ICMP between Clayton and Caulfield clients
      chain=forward action=accept protocol=icmp src-address=10.200.10.0/24
      dst-address=10.202.10.0/24

12    ;;; Allow ICMP between Peninsula and Clayton clients
      chain=forward action=accept protocol=icmp src-address=10.201.10.0/24
      dst-address=10.200.10.0/24

13    ;;; Allow ICMP between Caulfield and Clayton clients
      chain=forward action=accept protocol=icmp src-address=10.202.10.0/24
      dst-address=10.200.10.0/24

14    ;;; Allow established ICMP connections
      chain=forward action=accept connection-state=established,related
      protocol=icmp

15    ;;; Allow established ICMP connections to router
      chain=input action=accept connection-state=established,related
      protocol=icmp

16    ;;; Allow SSH access to Clayton SSH server from Caulfield clients
      chain=forward action=accept protocol=tcp src-address=10.202.10.0/24
      dst-address=10.200.10.11 in-interface=ether1 dst-port=22

17    ;;; Allow SSH access to Clayton SSH server from external clients
      chain=forward action=accept protocol=tcp src-address=192.168.122.0/24
      dst-address=10.200.10.11 in-interface=ether1 dst-port=22

18    ;;; Deny SSH access to Clayton SSH server from all other clients
      chain=forward action=drop protocol=tcp dst-address=10.200.10.11
      dst-port=22
```



```
19    ;;; Allow mail access to Clayton mail server from Peninsula clients
      chain=forward action=accept protocol=tcp src-address=10.201.10.0/24
      dst-address=10.200.10.12 in-interface=ether1 dst-port=25

20    ;;; Deny mail access to Clayton mail server from all other clients
      chain=forward action=drop protocol=tcp dst-address=10.200.10.12
      dst-port=25

21    ;;; Allow general traffic between Clayton and Peninsula
      chain=forward action=accept src-address=10.200.10.0/24
      dst-address=10.201.10.0/24 in-interface=ether2

22    ;;; Allow general traffic between Peninsula and Clayton
      chain=forward action=accept src-address=10.201.10.0/24
      dst-address=10.200.10.0/24 in-interface=ether1

23    ;;; Allow general traffic between Clayton and Caulfield
      chain=forward action=accept src-address=10.200.10.0/24
      dst-address=10.202.10.0/24 in-interface=ether2

24    ;;; Allow general traffic between Caulfield and Clayton
      chain=forward action=accept src-address=10.202.10.0/24
      dst-address=10.200.10.0/24 in-interface=ether1

25    ;;; Allow established and related connections for forwarded traffic
      chain=forward action=accept connection-state=established,related

26    ;;; Allow established and related connections for incoming traffic to ro>
r
      chain=input action=accept connection-state=established,related

27    ;;; Implicit deny for all other forwarded traffic
      chain=forward action=drop

28    ;;; Implicit deny for all other incoming traffic
      chain=input action=drop

29    ;;; Implicit deny for all other outgoing traffic
      chain=output action=drop
```

Peninsula firewall rules :

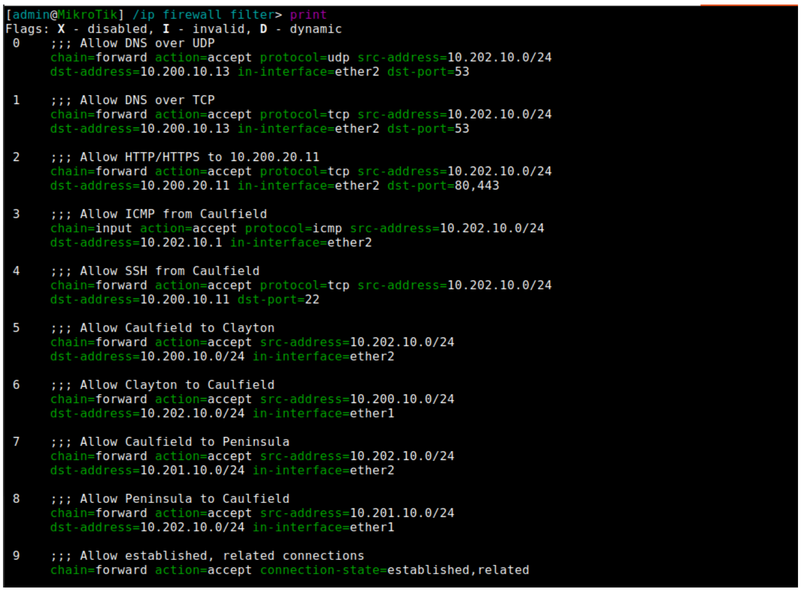
Allows DNS, web, and ICMP traffic, plus inter-site traffic with Clayton and Caulfield. All other traffic is denied.



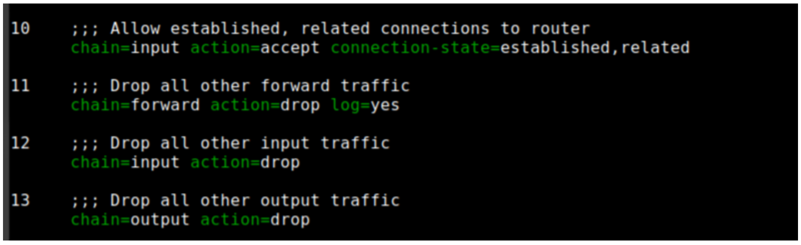
```
[admin@MikroTik] >
[admin@MikroTik] > /ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=accept protocol=udp src-address=10.201.10.0/24
      dst-address=10.200.10.13 in-interface=ether2 dst-port=53

 1    chain=forward action=accept protocol=tcp src-address=10.201.10.0/24
      dst-address=10.200.10.13 in-interface=ether2 dst-port=53

 2    chain=forward action=accept protocol=tcp src-address=10.201.10.0/24
      dst-address=10.200.20.11 in-interface=ether2 dst-port=80,443

 3    chain=input action=accept protocol=icmp src-address=10.201.10.0/24
      dst-address=10.201.10.1 in-interface=ether2

 4    chain=forward action=accept protocol=tcp src-address=10.201.10.0/24
      dst-address=10.200.10.12 in-interface=ether2 dst-port=25

 5    chain=forward action=accept src-address=10.201.10.0/24
      dst-address=10.200.10.0/24 in-interface=ether2

 6    chain=forward action=accept src-address=10.200.10.0/24
      dst-address=10.201.10.0/24 in-interface=ether1

 7    chain=forward action=accept src-address=10.201.10.0/24
      dst-address=10.202.10.0/24 in-interface=ether2

 8    chain=forward action=accept src-address=10.202.10.0/24
      dst-address=10.201.10.0/24 in-interface=ether1

 9    chain=forward action=accept connection-state=established,related

10    chain=input action=accept connection-state=established,related

11    chain=forward action=drop

12    chain=input action=drop

13    chain=output action=drop

[admin@MikroTik] >
```

Caulfield firewall rules:

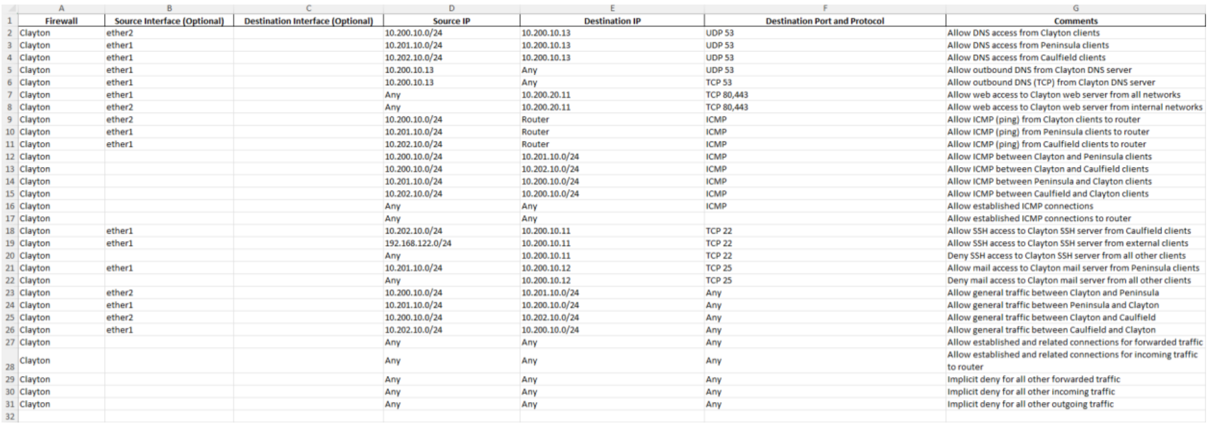
Allows DNS, web, and ICMP traffic, plus inter-site traffic with Clayton and Peninsula. All other traffic is denied.



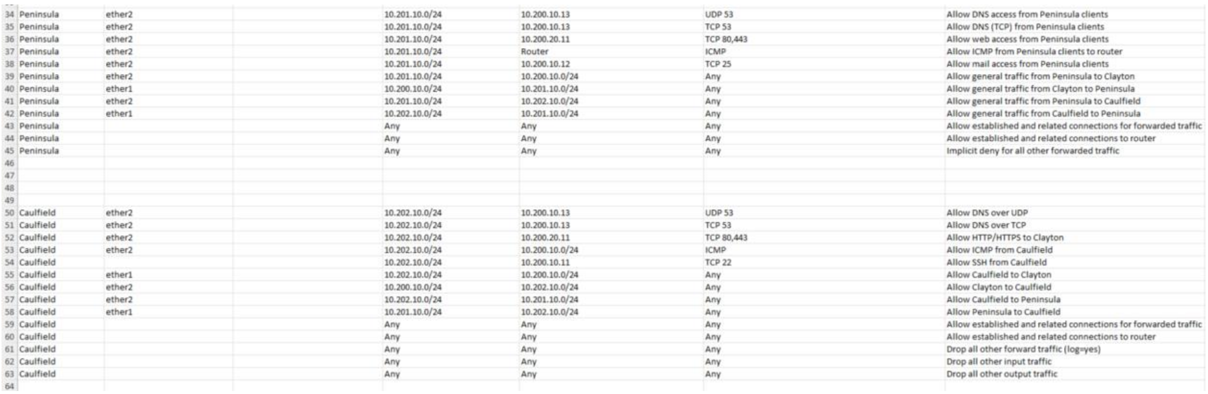
```
[admin@MikroTik] /ip firewall filter> print
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; Allow DNS over UDP
      chain=forward action=accept protocol=udp src-address=10.202.10.0/24
      dst-address=10.200.10.13 in-interface=ether2 dst-port=53

 1    ;;; Allow DNS over TCP
      chain=forward action=accept protocol=tcp src-address=10.202.10.0/24
      dst-address=10.200.10.13 in-interface=ether2 dst-port=53

 2    ;;; Allow HTTP/HTTPS to 10.200.20.11
      chain=forward action=accept protocol=tcp src-address=10.202.10.0/24
      dst-address=10.200.20.11 in-interface=ether2 dst-port=80,443

 3    ;;; Allow ICMP from Caulfield
      chain=input action=accept protocol=icmp src-address=10.202.10.0/24
      dst-address=10.202.10.1 in-interface=ether2

 4    ;;; Allow SSH from Caulfield
      chain=forward action=accept protocol=tcp src-address=10.202.10.0/24
      dst-address=10.200.10.11 dst-port=22

 5    ;;; Allow Caulfield to Clayton
      chain=forward action=accept src-address=10.202.10.0/24
      dst-address=10.200.10.0/24 in-interface=ether2

 6    ;;; Allow Clayton to Caulfield
      chain=forward action=accept src-address=10.200.10.0/24
      dst-address=10.202.10.0/24 in-interface=ether1

 7    ;;; Allow Caulfield to Peninsula
      chain=forward action=accept src-address=10.202.10.0/24
      dst-address=10.201.10.0/24 in-interface=ether2

 8    ;;; Allow Peninsula to Caulfield
      chain=forward action=accept src-address=10.201.10.0/24
      dst-address=10.202.10.0/24 in-interface=ether1

 9    ;;; Allow established, related connections
      chain=forward action=accept connection-state=established,related
```



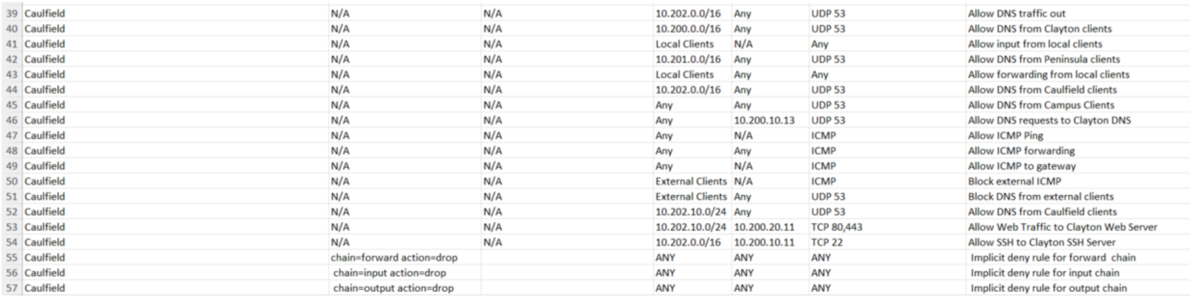
```
10    ;;; Allow established, related connections to router
      chain=input action=accept connection-state=established,related

11    ;;; Drop all other forward traffic
      chain=forward action=drop log=yes

12    ;;; Drop all other input traffic
      chain=input action=drop

13    ;;; Drop all other output traffic
      chain=output action=drop
```



	A	B	C	D	E	F	G
1	Firewall	Source Interface (Optional)	Destination Interface (Optional)	Source IP	Destination IP	Destination Port and Protocol	Comments
2	Clayton	ether2		10.200.10.0/24	10.200.10.13	UDP 53	Allow DNS access from Clayton clients
3	Clayton	ether1		10.201.10.0/24	10.200.10.13	UDP 53	Allow DNS access from Peninsula clients
4	Clayton	ether1		10.202.10.0/24	10.200.10.13	UDP 53	Allow DNS access from Caulfield clients
5	Clayton	ether1		10.200.10.13	Any	UDP 53	Allow outbound DNS from Clayton DNS server
6	Clayton	ether1		10.200.10.13	Any	TCP 53	Allow outbound DNS (TCP) from Clayton DNS server
7	Clayton	ether1		Any	10.200.20.11	TCP 80,443	Allow web access to Clayton web server from all networks
8	Clayton	ether2		Any	10.200.20.11	TCP 80,443	Allow web access to Clayton web server from internal networks
9	Clayton	ether2		10.200.10.0/24	Router	ICMP	Allow ICMP (ping) from Clayton clients to router
10	Clayton	ether1		10.201.10.0/24	Router	ICMP	Allow ICMP (ping) from Peninsula clients to router
11	Clayton	ether1		10.202.10.0/24	Router	ICMP	Allow ICMP (ping) from Caulfield clients to router
12	Clayton			10.200.10.0/24	10.201.10.0/24	ICMP	Allow ICMP between Clayton and Peninsula clients
13	Clayton			10.200.10.0/24	10.202.10.0/24	ICMP	Allow ICMP between Clayton and Caulfield clients
14	Clayton			10.201.10.0/24	10.200.10.0/24	ICMP	Allow ICMP between Peninsula and Clayton clients
15	Clayton			10.202.10.0/24	10.200.10.0/24	ICMP	Allow ICMP between Caulfield and Clayton clients
16	Clayton			Any	Any	ICMP	Allow established ICMP connections
17	Clayton			Any	Any		Allow established ICMP connections to router
18	Clayton	ether1		10.202.10.0/24	10.200.10.11	TCP 22	Allow SSH access to Clayton SSH server from Caulfield clients
19	Clayton	ether1		192.168.122.0/24	10.200.10.11	TCP 22	Allow SSH access to Clayton SSH server from external clients
20	Clayton			Any	10.200.10.11	TCP 22	Deny SSH access to Clayton SSH server from all other clients
21	Clayton	ether1		10.201.10.0/24	10.200.10.12	TCP 25	Allow mail access to Clayton mail server from Peninsula clients
22	Clayton			Any	10.200.10.12	TCP 25	Deny mail access to Clayton mail server from all other clients
23	Clayton	ether2		10.200.10.0/24	10.201.10.0/24	Any	Allow general traffic between Clayton and Peninsula
24	Clayton	ether1		10.201.10.0/24	10.200.10.0/24	Any	Allow general traffic between Peninsula and Clayton
25	Clayton	ether2		10.200.10.0/24	10.202.10.0/24	Any	Allow general traffic between Clayton and Caulfield
26	Clayton	ether1		10.202.10.0/24	10.200.10.0/24	Any	Allow general traffic between Caulfield and Clayton
27	Clayton			Any	Any	Any	Allow established and related connections for forwarded traffic
28	Clayton			Any	Any	Any	Allow established and related connections for incoming traffic to router
29	Clayton			Any	Any	Any	Implicit deny for all other forwarded traffic
30	Clayton			Any	Any	Any	Implicit deny for all other incoming traffic
31	Clayton			Any	Any	Any	Implicit deny for all other outgoing traffic
32							



34	Peninsula	ether2		10.201.10.0/24	10.200.10.13	UDP 53	Allow DNS access from Peninsula clients
35	Peninsula	ether2		10.201.10.0/24	10.200.10.13	TCP 53	Allow DNS (TCP) from Peninsula clients
36	Peninsula	ether2		10.201.10.0/24	10.200.20.11	TCP 80,443	Allow web access from Peninsula clients
37	Peninsula	ether2		10.201.10.0/24	Router	ICMP	Allow ICMP from Peninsula clients to router
38	Peninsula	ether2		10.201.10.0/24	10.200.10.12	TCP 25	Allow mail access from Peninsula clients
39	Peninsula	ether2		10.201.10.0/24	10.200.10.0/24	Any	Allow general traffic from Peninsula to Clayton
40	Peninsula	ether1		10.200.10.0/24	10.201.10.0/24	Any	Allow general traffic from Clayton to Peninsula
41	Peninsula	ether2		10.201.10.0/24	10.202.10.0/24	Any	Allow general traffic from Peninsula to Caulfield
42	Peninsula	ether1		10.202.10.0/24	10.201.10.0/24	Any	Allow general traffic from Caulfield to Peninsula
43	Peninsula			Any	Any	Any	Allow established and related connections for forwarded traffic
44	Peninsula			Any	Any	Any	Allow established and related connections to router
45	Peninsula			Any	Any	Any	Implicit deny for all other forwarded traffic
46							
47							
48							
49							
50	Caulfield	ether2		10.202.10.0/24	10.200.10.13	UDP 53	Allow DNS over UDP
51	Caulfield	ether2		10.202.10.0/24	10.200.10.13	TCP 53	Allow DNS over TCP
52	Caulfield	ether2		10.202.10.0/24	10.200.20.11	TCP 80,443	Allow HTTP/HTTPS to Clayton
53	Caulfield	ether2		10.202.10.0/24	10.200.10.0/24	ICMP	Allow ICMP from Caulfield
54	Caulfield			10.202.10.0/24	10.200.10.11	TCP 22	Allow SSH from Caulfield
55	Caulfield	ether1		10.202.10.0/24	10.200.10.0/24	Any	Allow Caulfield to Clayton
56	Caulfield	ether2		10.200.10.0/24	10.202.10.0/24	Any	Allow Clayton to Caulfield
57	Caulfield	ether2		10.202.10.0/24	10.201.10.0/24	Any	Allow Caulfield to Peninsula
58	Caulfield	ether1		10.201.10.0/24	10.202.10.0/24	Any	Allow Peninsula to Caulfield
59	Caulfield			Any	Any	Any	Allow established and related connections for forwarded traffic
60	Caulfield			Any	Any	Any	Allow established and related connections to router
61	Caulfield			Any	Any	Any	Drop all other forward traffic (log=yes)
62	Caulfield			Any	Any	Any	Drop all other input traffic
63	Caulfield			Any	Any	Any	Drop all other output traffic
64							



39	Caulfield	N/A	N/A	10.202.0.0/16	Any	UDP 53	Allow DNS traffic out
40	Caulfield	N/A	N/A	10.200.0.0/16	Any	UDP 53	Allow DNS from Clayton clients
41	Caulfield	N/A	N/A	Local Clients	N/A	Any	Allow input from local clients
42	Caulfield	N/A	N/A	10.201.0.0/16	Any	UDP 53	Allow DNS from Peninsula clients
43	Caulfield	N/A	N/A	Local Clients	Any	Any	Allow forwarding from local clients
44	Caulfield	N/A	N/A	10.202.0.0/16	Any	UDP 53	Allow DNS from Caulfield clients
45	Caulfield	N/A	N/A	Any	Any	UDP 53	Allow DNS from Campus Clients
46	Caulfield	N/A	N/A	Any	10.200.10.13	UDP 53	Allow DNS requests to Clayton DNS
47	Caulfield	N/A	N/A	Any	N/A	ICMP	Allow ICMP Ping
48	Caulfield	N/A	N/A	Any	Any	ICMP	Allow ICMP forwarding
49	Caulfield	N/A	N/A	Any	N/A	ICMP	Allow ICMP to gateway
50	Caulfield	N/A	N/A	External Clients	N/A	ICMP	Block external ICMP
51	Caulfield	N/A	N/A	External Clients	Any	UDP 53	Block DNS from external clients
52	Caulfield	N/A	N/A	10.202.10.0/24	Any	UDP 53	Allow DNS from Caulfield clients
53	Caulfield	N/A	N/A	10.202.10.0/24	10.200.20.11	TCP 80,443	Allow Web Traffic to Clayton Web Server
54	Caulfield	N/A	N/A	10.202.0.0/16	10.200.10.11	TCP 22	Allow SSH to Clayton SSH Server
55	Caulfield	chain=forward action=drop		ANY	ANY	ANY	Implicit deny rule for forward chain
56	Caulfield	chain=input action=drop		ANY	ANY	ANY	Implicit deny rule for input chain
57	Caulfield	chain=output action=drop		ANY	ANY	ANY	Implicit deny rule for output chain

Task 8: Security Analysis

In the configured network, which employs firewall configurations and IPSec VPN tunnels, several security considerations must be examined to assess the effectiveness of the current setup and explore potential improvements.

1. Can the Firewall Configuration Be Bypassed?

Firewalls are designed to restrict unauthorized access, yet they can potentially be bypassed through various techniques. One common method is IP spoofing, where an attacker sends packets from a forged IP address that the firewall considers trusted. Additionally, if proper stateful inspection is not implemented, attackers could exploit weaknesses in protocol handling to bypass controls.

To counter these risks, it is crucial to implement stringent rules, including:

- **Strict Source and Destination IP Filtering**: This ensures only verified IP addresses can access critical services. By maintaining a whitelist of allowed IP addresses, the likelihood of unauthorized access is significantly reduced.

- **Deep Packet Inspection (DPI)**: DPI analyzes packet content, preventing malicious payloads from passing through even if they originate from trusted IP addresses, adding an extra layer of scrutiny to incoming traffic.
- **Regular Updates and Patches**: Keeping firewall firmware up to date protects against newly discovered vulnerabilities, minimizing opportunities for attackers to exploit weaknesses.

Overall, a well-configured firewall with comprehensive rule sets and monitoring significantly reduces the risk of bypassing attempts.

2. Improving Network Security

To enhance network and server security, several strategies can be adopted:

- **Regular Vulnerability Assessments**: Conducting regular security assessments and penetration testing identifies weaknesses within the network and servers, allowing for timely remediation. This ongoing vigilance helps in recognizing and addressing potential threats before they are exploited.
- **Intrusion Detection and Prevention Systems (IDPS)**: Integrating IDPS provides real-time monitoring and alerts on suspicious activities, helping detect and mitigate threats before they escalate. Such systems can automatically respond to identified threats, enhancing security.
- **Network Segmentation**: Creating separate network segments for different departments or functions minimizes lateral movement within the network. For example, isolating the server infrastructure from client devices enhances security.
- **Enhanced Authentication Mechanisms**: Implementing multi-factor authentication (MFA) for accessing sensitive servers and applications adds an additional layer of verification beyond just usernames and passwords, improving security.
- **Logging and Monitoring**: Establishing robust logging and monitoring protocols for all network devices and servers provides critical insights into security incidents and aids forensic analysis.

In summary, while the current network configuration includes essential security measures, ongoing evaluations, protocol enhancements, employee awareness, and regular updates are vital to maintaining a strong security posture against evolving threats.

(Peltier, 2016)

Task 9:IDS

The video shows live attacks from an external attacker node and the real-time alerts generated by Snort. This below rule successfully detects specific network attacks while minimizing false positives. Custom IDS rules focused on patterns unique to malicious traffic ensure the IDS alerts only on relevant threats.

Rule 1: alert tcp any any -> any any (msg: "TCP Port Scan Detected"; flags: S; sid:1000001; rev:1;)

This above rule triggers an alert whenever a SYN packet is detected, which is a common characteristic of TCP port scans.

Rule 2: alert tcp any any -> 10.200.20.11 80 (msg: "DoS Attack Detected on Web Server"; flags: S; threshold: type threshold, track by_src, count 50, seconds 10; sid:1000002; rev:1;)

This above rule is triggered when 50 or more SYN packets are received on port 80 within 10 seconds from a single source, which indicates a possible SYN flood DoS attack.

Task 10:Ethical Network Usage Policy

In light of the suggested security improvements from Task 8, it is essential to establish an Ethical Network Usage Policy to mitigate potential unethical activities that may compromise the network's integrity. Unethical actions include unauthorized access to confidential data, misuse of network resources, and malicious behavior such as spreading malware.

Policy Guidelines:

1. **No Unauthorized Access:** Monash staff and students are strictly prohibited from accessing any servers, devices, or data not meant for their role or responsibilities within the network. Any attempt to bypass firewalls or access restricted services will be considered a breach of security.
2. **Prohibition of Attacks:** Activities such as Distributed Denial of Service (DDoS) attacks, packet sniffing, or any other form of network attack are strictly forbidden. These actions harm the integrity and security of the network.
3. **No Sharing of Credentials:** Users must not share their login details with others. Each user is responsible for maintaining the confidentiality of their credentials and any access granted under their account.
4. **Proper Use of Resources:** Network resources should only be used for approved academic or work-related purposes. Personal use that negatively affects the network performance or compromises security (such as installing unapproved software or visiting malicious websites) is strictly prohibited.

Consequences: Failure to follow to these guidelines may result in significant penalties, including suspension of network access, disciplinary action, or legal consequences, depending on the severity of the violation.

By following this policy, we can maintain a secure and efficient network environment conducive to learning and collaboration.

References:

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards*. Auerbach Publications. https://doi.org/10.1201/9780849390