FIT5037 Final Assessment

Student ID: 33948941

Project Hash:

```
gns3@gns3vm:/opt/gns3/projects$ sha1sum Monash_5.tar.gz
a8a1f715345c472383ed947ba7dad261bfdb36e9  Monash_5.tar.gz
gns3@gns3vm:/opt/gns3/projects$
```

Fig 1: Hash

Q4: Secure Network Design and Implementation:

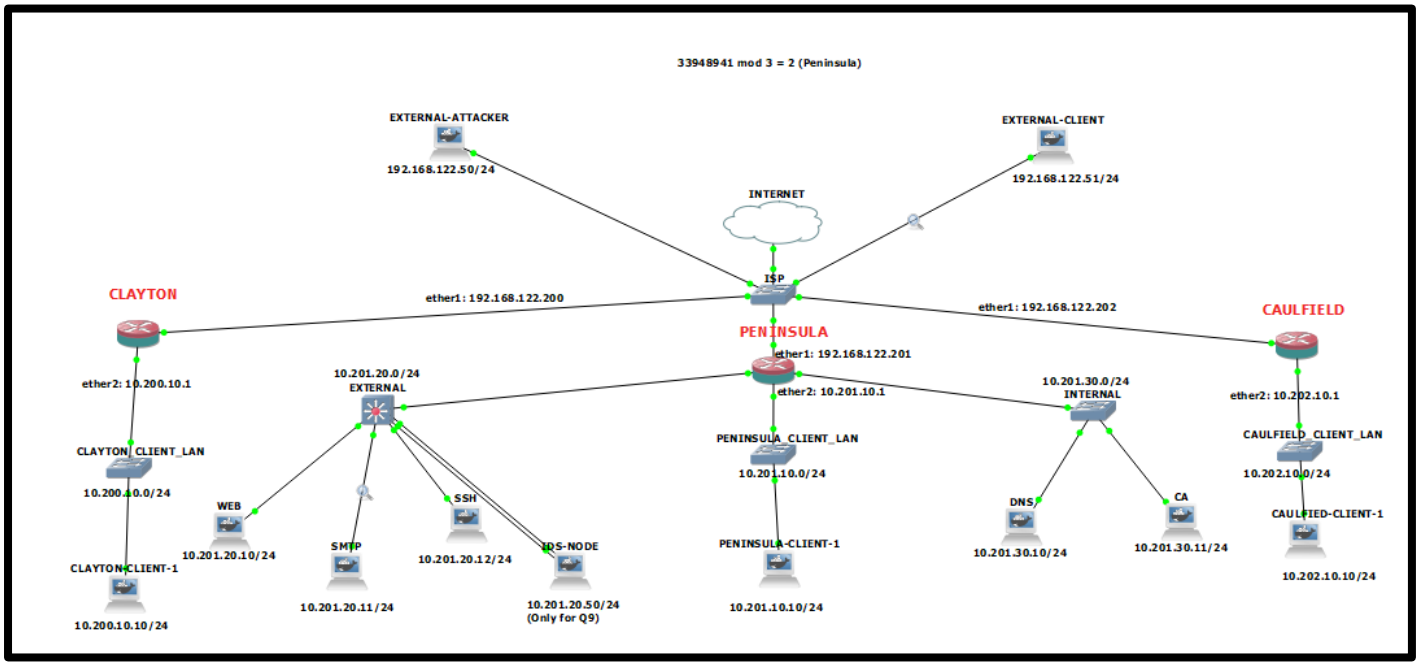

Fig 2- Topology

Q5: BGP:

(Please Refer to the video for the live demonstration of the attack and countermeasure)

Q6: VPN:

Site-to-Site VPN:

```
Flags: H - hw-aead, A - AH, E - ESP
 0  E spi=0xE665A13 src-address=192.168.122.200 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="09b94dee3a9aeae6a873113017de48c2975760869978504e086b3829f10a5da1137ffbc5"
      add-lifetime=6h24m7s/8h9s replay=128

 1  E spi=0x260197 src-address=192.168.122.200 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="61bc1aa79110e76130060c3d014d19406865ba040d2af2b069bd3ed6ed87989746e26f4f"
      add-lifetime=6h24m17s/8h22s replay=128

 2  E spi=0x1C7BD67 src-address=192.168.122.201 dst-address=192.168.122.200 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="76c2f9ab32601803e62e573ce1daba1ee16e6cde2cab12203e90861560f210ec2322e879"
      add-lifetime=6h24m17s/8h22s replay=128

 3  E spi=0x10BFAE6 src-address=192.168.122.201 dst-address=192.168.122.200 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="92d8ed2ec68126a8c13ed71c6ce237a9e57f4dbea9cdedce778b5868e7d7b62eb8f74778"
      add-lifetime=6h24m7s/8h9s replay=128

 4  E spi=0xA43A1D5 src-address=192.168.122.200 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="98658a62e26ee77827999eaad99921a6c5e28459088a911930f8395cb58fd3d079479d7f"
      addtime=nov/07/2025 02:50:45 expires-in=6h15m22s add-lifetime=6h24m9s/8h12s current-bytes=3864
      current-packets=46 replay=128

 5  E spi=0x50DD536 src-address=192.168.122.201 dst-address=192.168.122.200 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="c65d015821a3c24f3902532d69f41afa881ce3961925330d27836a0051e919dd1d5c6bd2"
      addtime=nov/07/2025 02:50:45 expires-in=6h15m22s add-lifetime=6h24m9s/8h12s current-bytes=3780
      current-packets=45 replay=128

 6  E spi=0xF8D80CC src-address=192.168.122.202 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="fdc879c91029bd5ce8d46339b370f973d861d570584f6a7cbd1a6137064b942a4eb2c5ff"
      add-lifetime=6h24m16s/8h20s replay=128

 7  E spi=0xFC7B19 src-address=192.168.122.201 dst-address=192.168.122.202 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="b6057767fb9639295ebc5875f17dd441c533ab05e463f7e925a25eeb5c9de1788480f636"
      add-lifetime=6h24m16s/8h20s replay=128

 8  E spi=0xD50CB9F src-address=192.168.122.202 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
-- [Q quit|D dump|down]
```

Fig 3: Peninsula Part 1

```
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="92d8ed2ec68126a8c13ed71c6ce237a9e57f4dbea9cdedce778b5868e7d7b62eb8f74778"
      add-lifetime=6h24m7s/8h9s replay=128

 4  E spi=0xA43A1D5 src-address=192.168.122.200 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="98658a62e26ee77827999eaad99921a6c5e28459088a911930f8395cb58fd3d079479d7f"
      addtime=nov/07/2025 02:50:45 expires-in=6h15m22s add-lifetime=6h24m9s/8h12s current-bytes=3864
      current-packets=46 replay=128

 5  E spi=0x50DD536 src-address=192.168.122.201 dst-address=192.168.122.200 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="c65d015821a3c24f3902532d69f41afa881ce3961925330d27836a0051e919dd1d5c6bd2"
      addtime=nov/07/2025 02:50:45 expires-in=6h15m22s add-lifetime=6h24m9s/8h12s current-bytes=3780
      current-packets=45 replay=128

 6  E spi=0xF8D80CC src-address=192.168.122.202 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="fdc879c91029bd5ce8d46339b370f973d861d570584f6a7cbd1a6137064b942a4eb2c5ff"
      add-lifetime=6h24m16s/8h20s replay=128

 7  E spi=0xFC7B19 src-address=192.168.122.201 dst-address=192.168.122.202 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="b6057767fb9639295ebc5875f17dd441c533ab05e463f7e925a25eeb5c9de1788480f636"
      add-lifetime=6h24m16s/8h20s replay=128

 8  E spi=0xD50CB9F src-address=192.168.122.202 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="9ca759f379887aabdc9a94628e1e7d93db0b53a6995c216f2da9f8abff079befd3874e99"
      add-lifetime=6h24m13s/8h17s replay=128

 9  E spi=0xECB8589 src-address=192.168.122.201 dst-address=192.168.122.202 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="479318971a2a3b82bdbc9d1a7278f9a3ee8ad684e14af7b5ac5a3dba2b4a08b2f0ad3260"
      add-lifetime=6h24m13s/8h17s replay=128

10  E spi=0x44C284C src-address=192.168.122.202 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="49a1132fd0be22d89a9185d9298a2656222197f47f4b0448b7a6f5cc5c378e1f5f2c0143"
      add-lifetime=6h24m21s/8h27s replay=128

11  E spi=0x6FD950F src-address=192.168.122.201 dst-address=192.168.122.202 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="48187dca584e48be6a4e118748eab834d7bea529de6251f30a640eaa9acad0b832602663"
      add-lifetime=6h24m21s/8h27s replay=128
-- [Q quit|D dump|up|down]
```

Fig 4: Peninsula Part 2

```
[admin@MikroTik] > /ip ipsec installed-sa print
Flags: H - hw-aead, A - AH, E - ESP
 0  E spi=0x10BFAE6 src-address=192.168.122.201 dst-address=192.168.122.200 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="92d8ed2ec68126a8c13ed71c6ce237a9e57f4dbea9cdedce778b5868e7d7b62eb8f74778"
      add-lifetime=6h24m1s/8h2s replay=128

 1  E spi=0xE665A13 src-address=192.168.122.200 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="09b94dee3a9aeae6a873113017de48c2975760869978504e086b3829f10a5da1137ffbc5"
      add-lifetime=6h24m1s/8h2s replay=128

 2  E spi=0x1C7BD67 src-address=192.168.122.201 dst-address=192.168.122.200 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="76c2f9ab32601803e62e573ce1daba1ee16e6cde2cab12203e90861560f210ec2322e879"
      add-lifetime=6h24m2s/8h3s replay=128

 3  E spi=0x260197 src-address=192.168.122.200 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="61bc1aa79110e76130060c3d014d19406865ba040d2af2b069bd3ed6ed87989746e26f4f"
      add-lifetime=6h24m2s/8h3s replay=128

 4  E spi=0x50DD536 src-address=192.168.122.201 dst-address=192.168.122.200 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="c65d015821a3c24f3902532d69f41afa881ce3961925330d27836a0051e919dd1d5c6bd2"
      addtime=nov/07/2025 02:50:47 expires-in=6h16m15s add-lifetime=6h24m17s/8h22s
      current-bytes=3780 current-packets=45 replay=128

 5  E spi=0xA43A1D5 src-address=192.168.122.200 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="98658a62e26ee77827999eaad99921a6c5e28459088a911930f8395cb58fd3d079479d7f"
      addtime=nov/07/2025 02:50:48 expires-in=6h16m16s add-lifetime=6h24m17s/8h22s
      current-bytes=4788 current-packets=57 replay=128

 6  E spi=0x96400A2 src-address=192.168.122.202 dst-address=192.168.122.200 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="e8e797d659d4638c2c096c626e8fd489999fc2ca27f81d5dd1964ecdc2f3a29814ab64c6"
      add-lifetime=6h24m4s/8h5s replay=128

 7  E spi=0xAF8DB98 src-address=192.168.122.200 dst-address=192.168.122.202 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="492638b5919a82d427b96bb9715a663d2f1dba2155f294a4c1bda327de2abfb5d5d18aad"
      add-lifetime=6h24m4s/8h5s replay=128
[admin@MikroTik] >
```

Fig 5: Clayton

```
[admin@MikroTik] > /ip ipsec installed-sa print
Flags: H - hw-aead, A - AH, E - ESP
 0  E spi=0xAF8DB98 src-address=192.168.122.200 dst-address=192.168.122.202 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="492638b5919a82d427b96bb9715a663d2f1dba2155f294a4c1bda327de2abfb5d5d18aad"
      add-lifetime=6h24m/8h replay=128

 1  E spi=0x96400A2 src-address=192.168.122.202 dst-address=192.168.122.200 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="e8e797d659d4638c2c096c626e8fd489999fc2ca27f81d5dd1964ecdc2f3a29814ab64c6"
      add-lifetime=6h24m/8h replay=128

 2  E spi=0xFC7B19 src-address=192.168.122.201 dst-address=192.168.122.202 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="b6057767fb9639295ebc5875f17dd441c533ab05e463f7e925a25eeb5c9de1788480f636"
      add-lifetime=6h24m19s/8h24s replay=128

 3  E spi=0xF8D80CC src-address=192.168.122.202 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="fdc879c91029bd5ce8d46339b370f973d861d570584f6a7cbd1a6137064b942a4eb2c5ff"
      add-lifetime=6h24m19s/8h24s replay=128

 4  E spi=0xECB8589 src-address=192.168.122.201 dst-address=192.168.122.202 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="479318971a2a3b82bdbc9d1a7278f9a3ee8ad684e14af7b5ac5a3dba2b4a08b2f0ad3260"
      add-lifetime=6h24m20s/8h25s replay=128

 5  E spi=0xD50CB9F src-address=192.168.122.202 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="9ca759f379887aabdc9a94628e1e7d93db0b53a6995c216f2da9f8abff079befd3874e99"
      add-lifetime=6h24m20s/8h25s replay=128

 6  E spi=0x6FD950F src-address=192.168.122.201 dst-address=192.168.122.202 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="48187dca584e48be6a4e118748eab834d7bea529de6251f30a640eaa9acad0b832602663"
      add-lifetime=6h24m22s/8h28s replay=128

 7  E spi=0x44C284C src-address=192.168.122.202 dst-address=192.168.122.201 state=mature
      enc-algorithm=aes-gcm enc-key-size=288
      enc-key="49a1132fd0be22d89a9185d9298a2656222197f47f4b0448b7a6f5cc5c378e1f5f2c0143"
      add-lifetime=6h24m22s/8h28s replay=128
[admin@MikroTik] >
```

Fig 6: Caulfield

Remote-Access VPN:

```
 GNU nano 7.2                                  /etc/ipsec.conf

config setup
        # strictcrlpolicy=yes
        # uniqueids = no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed
#       leftsubnet=10.1.0.0/16
#       leftcert=selfCert.der
#       leftsendcert=never
#       right=192.168.0.2
#       rightsubnet=10.2.0.0/16
#       rightcert=peerCert.der
#       auto=start

#conn sample-with-ca-cert
#       leftsubnet=10.1.0.0/16
#       leftcert=myCert.pem
#       right=192.168.0.2
#       rightsubnet=10.2.0.0/16
#       rightid="C=CH, O=Linux strongSwan CN=peer name"
#       auto=start



conn peninsula-vpn
    keyexchange=ikev2
    ike=aes256-sha256-modp2048!
    esp=aes256-sha256-modp2048,aes256gcm16-modp2048
    left=%defaultroute
    leftsourceip=%config
    leftauth=psk
    right=192.168.122.201
    rightauth=psk
    rightsubnet=10.201.0.0/16
    auto=start

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark     M-] To Bracket   M-Q Previous     ^B Back          ^Left Prev Word
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy         ^Q Where Was     M-W Next         ^F Forward       ^Right Next Word
```

Fig 7: External Client Configuration of VPN

Q7: Firewall Configuration

```
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; STATEFUL
      chain=forward action=accept connection-state=established,related

 1    ;;; ICMP
      chain=forward action=accept protocol=icmp

 2    ;;; DNS-PENINSULA
      chain=forward action=accept protocol=udp src-address=10.201.10.0/24 dst-address=10.201.30.10
      dst-port=53

 3    ;;; DNS-CAULFIELD
      chain=forward action=accept protocol=udp src-address=10.202.10.0/24 dst-address=10.201.30.10
      dst-port=53

 4    ;;; DNS-CLAYTON
      chain=forward action=accept protocol=udp src-address=10.200.10.0/24 dst-address=10.201.30.10
      dst-port=53

 5    ;;; DNS-REMOTE-VPN
      chain=forward action=accept protocol=udp src-address=172.16.10.0/24 dst-address=10.201.30.10
      dst-port=53

 6    ;;; DNS-OUTBOUND
      chain=forward action=accept protocol=udp src-address=10.201.30.10 out-interface=ether1
      dst-port=53

 7    ;;; DNS-RESPONSES
      chain=forward action=accept protocol=udp src-address=10.201.30.10 src-port=53

 8    ;;; SSH-REMOTE-VPN-ONLY
      chain=forward action=accept protocol=tcp src-address=172.16.10.0/24 dst-address=10.201.20.12
      dst-port=22

 9    ;;; SSH-OUTBOUND
      chain=forward action=accept protocol=tcp src-address=10.201.20.12 out-interface=ether1

10    ;;; WEB-PENINSULA
      chain=forward action=accept protocol=tcp src-address=10.201.10.0/24 dst-address=10.201.20.10
      dst-port=80,443

11    ;;; WEB-CLAYTON
      chain=forward action=accept protocol=tcp src-address=10.200.10.0/24 dst-address=10.201.20.10
      dst-port=80,443
```

Fig 8: Peninsula Part 1

```
12    ;;; WEB-CAULFIELD
      chain=forward action=accept protocol=tcp src-address=10.202.10.0/24 dst-address=10.201.20.10
      dst-port=80,443

13    ;;; WEB-EXTERNAL
      chain=forward action=accept protocol=tcp dst-address=10.201.20.10 in-interface=ether1
      out-interface=ether3 dst-port=80,443

14    ;;; WEB-OUTBOUND
      chain=forward action=accept protocol=tcp src-address=10.201.20.10 out-interface=ether1

15    ;;; SMTP-CAULFIELD-Q7
      chain=forward action=accept protocol=tcp src-address=10.202.10.0/24 dst-address=10.201.20.11
      dst-port=25,587,465

16    ;;; SMTP-EXTERNAL
      chain=forward action=accept protocol=tcp dst-address=10.201.20.11 in-interface=ether1
      out-interface=ether3 dst-port=25,587,465

17    ;;; SMTP-OUTBOUND
      chain=forward action=accept protocol=tcp src-address=10.201.20.11 out-interface=ether1

18    ;;; INTERNET-PENINSULA
      chain=forward action=accept src-address=10.201.10.0/24 out-interface=ether1

19    ;;; DENY-SMTP-REMOTE-VPN
      chain=forward action=drop protocol=tcp src-address=172.16.10.0/24 dst-address=10.201.20.11
      dst-port=25,587,465

20    ;;; DENY-SSH-CLAYTON
      chain=forward action=drop protocol=tcp src-address=10.200.10.0/24 dst-address=10.201.20.12
      dst-port=22

21    ;;; DENY-SSH-CAULFIELD
      chain=forward action=drop protocol=tcp src-address=10.202.10.0/24 dst-address=10.201.20.12
      dst-port=22

22    ;;; DENY-SSH-PENINSULA
      chain=forward action=drop protocol=tcp src-address=10.201.10.0/24 dst-address=10.201.20.12
      dst-port=22

23    ;;; DENY-SMTP-CLAYTON-Q7
      chain=forward action=drop protocol=tcp src-address=10.200.10.0/24 dst-address=10.201.20.11
      dst-port=25,587,465
-- [Q quit|D dump|up|down]
```

Fig 9: Peninsula Part 2

```
23    ;;; DENY-SMTP-CLAYTON-Q7
      chain=forward action=drop protocol=tcp src-address=10.200.10.0/24 dst-address=10.201.20.11
      dst-port=25,587,465

24    ;;; DENY-SMTP-PENINSULA
      chain=forward action=drop protocol=tcp src-address=10.201.10.0/24 dst-address=10.201.20.11
      dst-port=25,587,465

25    ;;; VPN-TO-CLAYTON
      chain=forward action=accept src-address=10.201.0.0/16 dst-address=10.200.10.0/24

26    ;;; VPN-FROM-CLAYTON
      chain=forward action=accept src-address=10.200.10.0/24 dst-address=10.201.0.0/16

27    ;;; VPN-TO-CAULFIELD
      chain=forward action=accept src-address=10.201.0.0/16 dst-address=10.202.10.0/24

28    ;;; VPN-FROM-CAULFIELD
      chain=forward action=accept src-address=10.202.10.0/24 dst-address=10.201.0.0/16

29    ;;; VPN-CLAYTON-CAULFIELD
      chain=forward action=accept src-address=10.200.10.0/24 dst-address=10.202.10.0/24

30    ;;; VPN-CAULFIELD-CLAYTON
      chain=forward action=accept src-address=10.202.10.0/24 dst-address=10.200.10.0/24

31    ;;; VPN-TO-REMOTE
      chain=forward action=accept src-address=10.201.0.0/16 dst-address=172.16.10.0/24

32    ;;; VPN-FROM-REMOTE
      chain=forward action=accept src-address=172.16.10.0/24 dst-address=10.201.0.0/16

33    ;;; DENY-ALL-FORWARD
      chain=forward action=drop

34    ;;; INPUT-STATEFUL
      chain=input action=accept connection-state=established,related

35    ;;; INPUT-ICMP
      chain=input action=accept protocol=icmp

36    ;;; INPUT-IKE
      chain=input action=accept protocol=udp dst-port=500,4500

-- [Q quit|D dump|up|down]
```

Fig 10: Peninsula Part 3

```
35    ;;; INPUT-ICMP
      chain=input action=accept protocol=icmp

36    ;;; INPUT-IKE
      chain=input action=accept protocol=udp dst-port=500,4500

37    ;;; INPUT-ESP
      chain=input action=accept protocol=ipsec-esp

38    ;;; INPUT-BGP
      chain=input action=accept protocol=tcp dst-port=179

39    ;;; INPUT-PENINSULA
      chain=input action=accept src-address=10.201.0.0/16

40    ;;; INPUT-CLAYTON
      chain=input action=accept src-address=10.200.10.0/24

41    ;;; INPUT-CAULFIELD
      chain=input action=accept src-address=10.202.10.0/24

42    ;;; INPUT-REMOTE-VPN
      chain=input action=accept src-address=172.16.10.0/24

43    ;;; DENY-ALL-INPUT
      chain=input action=drop

44    ;;; OUTPUT-STATEFUL
      chain=output action=accept connection-state=established,related

45    ;;; OUTPUT-IKE
      chain=output action=accept protocol=udp dst-port=500,4500

46    ;;; OUTPUT-ESP
      chain=output action=accept protocol=ipsec-esp

47    ;;; OUTPUT-BGP
      chain=output action=accept protocol=tcp dst-port=179

48    ;;; OUTPUT-ALLOW-ALL
      chain=output action=accept

49    ;;; DENY-ALL-OUTPUT
      chain=output action=drop
-- [Q quit|D dump|up|down]
```

Fig 11: Peninsula part 4

```
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; STATEFUL
      chain=forward action=accept connection-state=established,related

 1    ;;; ICMP
      chain=forward action=accept protocol=icmp

 2    ;;; DNS-TO-PENINSULA
      chain=forward action=accept protocol=udp src-address=10.200.10.0/24 dst-address=10.201.30.10
      dst-port=53

 3    ;;; DNS-RESPONSES
      chain=forward action=accept protocol=udp src-address=10.201.30.10 dst-address=10.200.10.0/24
      src-port=53

 4    ;;; DNS-OUTBOUND
      chain=forward action=accept protocol=udp src-address=10.201.30.10 out-interface=ether1
      dst-port=53

 5    ;;; WEB-TO-PENINSULA
      chain=forward action=accept protocol=tcp src-address=10.200.10.0/24 dst-address=10.201.20.10
      dst-port=80,443

 6    ;;; WEB-OUTBOUND
      chain=forward action=accept protocol=tcp src-address=10.201.20.10 out-interface=ether1

 7    ;;; SMTP-OUTBOUND
      chain=forward action=accept protocol=tcp src-address=10.201.20.11 out-interface=ether1

 8    ;;; SSH-OUTBOUND
      chain=forward action=accept protocol=tcp src-address=10.201.20.12 out-interface=ether1

 9    ;;; INTERNET
      chain=forward action=accept src-address=10.200.10.0/24 out-interface=ether1

10    ;;; DENY-SSH
      chain=forward action=drop protocol=tcp src-address=10.200.10.0/24 dst-address=10.201.20.12
      dst-port=22

11    ;;; DENY-SMTP-Q7
      chain=forward action=drop protocol=tcp src-address=10.200.10.0/24 dst-address=10.201.20.11
      dst-port=25,587,465

12    ;;; VPN-TO-PENINSULA
      chain=forward action=accept src-address=10.200.10.0/24 dst-address=10.201.0.0/16
-- [Q quit|D dump|down]
```

Fig 12: Clayton Part 1

```
13    ;;; VPN-FROM-PENINSULA
      chain=forward action=accept src-address=10.201.0.0/16 dst-address=10.200.10.0/24

14    ;;; VPN-TO-CAULFIELD
      chain=forward action=accept src-address=10.200.10.0/24 dst-address=10.202.10.0/24

15    ;;; VPN-FROM-CAULFIELD
      chain=forward action=accept src-address=10.202.10.0/24 dst-address=10.200.10.0/24

16    ;;; DENY-ALL-FORWARD
      chain=forward action=drop

17    ;;; INPUT-STATEFUL
      chain=input action=accept connection-state=established,related

18    ;;; INPUT-ICMP
      chain=input action=accept protocol=icmp

19    ;;; INPUT-IKE
      chain=input action=accept protocol=udp dst-port=500,4500

20    ;;; INPUT-ESP
      chain=input action=accept protocol=ipsec-esp

21    ;;; INPUT-BGP
      chain=input action=accept protocol=tcp dst-port=179

22    ;;; INPUT-PENINSULA
      chain=input action=accept src-address=10.201.0.0/16

23    ;;; INPUT-CAULFIELD
      chain=input action=accept src-address=10.202.10.0/24

24    ;;; INPUT-CLAYTON
      chain=input action=accept src-address=10.200.10.0/24

25    ;;; DENY-ALL-INPUT
      chain=input action=drop

26    ;;; OUTPUT-STATEFUL
      chain=output action=accept connection-state=established,related

27    ;;; OUTPUT-IKE
      chain=output action=accept protocol=udp dst-port=500,4500
-- [Q quit|D dump|up|down]
```

Fig 13: Clayton Part 2

```
17    ;;; INPUT-STATEFUL
      chain=input action=accept connection-state=established,related

18    ;;; INPUT-ICMP
      chain=input action=accept protocol=icmp

19    ;;; INPUT-IKE
      chain=input action=accept protocol=udp dst-port=500,4500

20    ;;; INPUT-ESP
      chain=input action=accept protocol=ipsec-esp

21    ;;; INPUT-BGP
      chain=input action=accept protocol=tcp dst-port=179

22    ;;; INPUT-PENINSULA
      chain=input action=accept src-address=10.201.0.0/16

23    ;;; INPUT-CAULFIELD
      chain=input action=accept src-address=10.202.10.0/24

24    ;;; INPUT-CLAYTON
      chain=input action=accept src-address=10.200.10.0/24

25    ;;; DENY-ALL-INPUT
      chain=input action=drop

26    ;;; OUTPUT-STATEFUL
      chain=output action=accept connection-state=established,related

27    ;;; OUTPUT-IKE
      chain=output action=accept protocol=udp dst-port=500,4500

28    ;;; OUTPUT-ESP
      chain=output action=accept protocol=ipsec-esp

29    ;;; OUTPUT-BGP
      chain=output action=accept protocol=tcp dst-port=179

30    ;;; OUTPUT-ALLOW-ALL
      chain=output action=accept

31    ;;; DENY-ALL-OUTPUT
      chain=output action=drop
-- [Q quit|D dump|up|down]
```

Fig 14: Clayton Part 3

```
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; STATEFUL
      chain=forward action=accept connection-state=established,related

 1    ;;; ICMP
      chain=forward action=accept protocol=icmp

 2    ;;; DNS-TO-PENINSULA
      chain=forward action=accept protocol=udp src-address=10.202.10.0/24 dst-address=10.201.30.10
      dst-port=53

 3    ;;; DNS-RESPONSES
      chain=forward action=accept protocol=udp src-address=10.201.30.10 dst-address=10.202.10.0/24
      src-port=53

 4    ;;; DNS-OUTBOUND
      chain=forward action=accept protocol=udp src-address=10.201.30.10 out-interface=ether1
      dst-port=53

 5    ;;; WEB-TO-PENINSULA
      chain=forward action=accept protocol=tcp src-address=10.202.10.0/24 dst-address=10.201.20.10
      dst-port=80,443

 6    ;;; WEB-OUTBOUND
      chain=forward action=accept protocol=tcp src-address=10.201.20.10 out-interface=ether1

 7    ;;; SMTP-AUTHORIZED-Q7
      chain=forward action=accept protocol=tcp src-address=10.202.10.0/24 dst-address=10.201.20.11
      dst-port=25,587,465

 8    ;;; SMTP-OUTBOUND
      chain=forward action=accept protocol=tcp src-address=10.201.20.11 out-interface=ether1

 9    ;;; SSH-OUTBOUND
      chain=forward action=accept protocol=tcp src-address=10.201.20.12 out-interface=ether1

10    ;;; INTERNET
      chain=forward action=accept src-address=10.202.10.0/24 out-interface=ether1

11    ;;; DENY-SSH
      chain=forward action=drop protocol=tcp src-address=10.202.10.0/24 dst-address=10.201.20.12
      dst-port=22

12    ;;; VPN-TO-PENINSULA
      chain=forward action=accept src-address=10.202.10.0/24 dst-address=10.201.0.0/16
-- [Q quit|D dump|down]
```

Fig 15: Caulfield Part 1

```
13    ;;; VPN-FROM-PENINSULA
      chain=forward action=accept src-address=10.201.0.0/16 dst-address=10.202.10.0/24

14    ;;; VPN-TO-CLAYTON
      chain=forward action=accept src-address=10.202.10.0/24 dst-address=10.200.10.0/24

15    ;;; VPN-FROM-CLAYTON
      chain=forward action=accept src-address=10.200.10.0/24 dst-address=10.202.10.0/24

16    ;;; DENY-ALL-FORWARD
      chain=forward action=drop

17    ;;; INPUT-STATEFUL
      chain=input action=accept connection-state=established,related

18    ;;; INPUT-ICMP
      chain=input action=accept protocol=icmp

19    ;;; INPUT-IKE
      chain=input action=accept protocol=udp dst-port=500,4500

20    ;;; INPUT-ESP
      chain=input action=accept protocol=ipsec-esp

21    ;;; INPUT-BGP
      chain=input action=accept protocol=tcp dst-port=179

22    ;;; INPUT-PENINSULA
      chain=input action=accept src-address=10.201.0.0/16

23    ;;; INPUT-CLAYTON
      chain=input action=accept src-address=10.200.10.0/24

24    ;;; INPUT-CAULFIELD
      chain=input action=accept src-address=10.202.10.0/24

25    ;;; DENY-ALL-INPUT
      chain=input action=drop

26    ;;; OUTPUT-STATEFUL
      chain=output action=accept connection-state=established,related

27    ;;; OUTPUT-IKE
      chain=output action=accept protocol=udp dst-port=500,4500

-- [Q quit|D dump|up|down]
```

Fig 16: Caulfield Part 2

```
17    ;;; INPUT-STATEFUL
      chain=input action=accept connection-state=established,related

18    ;;; INPUT-ICMP
      chain=input action=accept protocol=icmp

19    ;;; INPUT-IKE
      chain=input action=accept protocol=udp dst-port=500,4500

20    ;;; INPUT-ESP
      chain=input action=accept protocol=ipsec-esp

21    ;;; INPUT-BGP
      chain=input action=accept protocol=tcp dst-port=179

22    ;;; INPUT-PENINSULA
      chain=input action=accept src-address=10.201.0.0/16

23    ;;; INPUT-CLAYTON
      chain=input action=accept src-address=10.200.10.0/24

24    ;;; INPUT-CAULFIELD
      chain=input action=accept src-address=10.202.10.0/24

25    ;;; DENY-ALL-INPUT
      chain=input action=drop

26    ;;; OUTPUT-STATEFUL
      chain=output action=accept connection-state=established,related

27    ;;; OUTPUT-IKE
      chain=output action=accept protocol=udp dst-port=500,4500

28    ;;; OUTPUT-ESP
      chain=output action=accept protocol=ipsec-esp

29    ;;; OUTPUT-BGP
      chain=output action=accept protocol=tcp dst-port=179

30    ;;; OUTPUT-ALLOW-ALL
      chain=output action=accept

31    ;;; DENY-ALL-OUTPUT
      chain=output action=drop
-- [Q quit|D dump|up|down]
```

Fig 17: Caulfield Part 3

Firewall Rules Template:

Firewall	Chain	Source Interface	Destination Interface	Source IP	Destination IP	Destination Port and Protoco	Comments
Caulfield	forward						STATEFUL - Allow established/related connections
Caulfield	forward					ICMP	Allow ICMP
Caulfield	forward			10.202.10.0/24	10.201.30.10	UDP 53	DNS queries to Peninsula DNS
Caulfield	forward			10.201.30.10	10.202.10.0/24	UDP 53	DNS responses from Peninsula
Caulfield	forward		ether1	10.201.30.10		UDP 53	DNS queries outbound
Caulfield	forward			10.202.10.0/24	10.201.20.10	TCP 80,443	Web access to Peninsula
Caulfield	forward		ether1	10.201.20.10			Web server outbound
Caulfield	forward			10.202.10.0/24	10.201.20.11	TCP 25,587,465	SMTP to Peninsula (authorized Q7)
Caulfield	forward	ether1	ether3	10.201.20.11		TCP 25,587,465	SMTP external access
Caulfield	forward		ether1	10.201.20.11			SMTP server outbound
Caulfield	forward		ether1	10.201.20.12			SSH server outbound
Caulfield	forward		ether1			10.202.10.0/24	Internet access for Caulfield
Caulfield	forward			10.202.10.0/24	10.201.20.12	TCP 22	Block SSH to Peninsula
Caulfield	forward			10.202.10.0/24	10.201.20.11	TCP 25,587,465	Block SMTP to Peninsula (for Clayton Q7)
Caulfield	forward			10.201.10.0/24	10.201.20.12	TCP 22	Block SSH from Peninsula to SSH server
Caulfield	forward			10.202.10.0/24	10.201.20.11	TCP 25,587,465	Block SMTP from Peninsula (for Clayton Q7)
Caulfield	forward			10.200.10.0/24	10.202.10.0/24		VPN to Caulfield
Caulfield	forward			10.202.10.0/24	10.200.10.0/24		VPN from Caulfield to Clayton
Caulfield	forward			10.201.0.0/16	10.202.10.0/24		VPN from Peninsula to Caulfield
Caulfield	forward			10.202.10.0/24	10.201.0.0/16		VPN to Peninsula from Caulfield
Caulfield	forward			10.200.10.0/24	10.202.10.0/24		VPN Clayton to Caulfield
Caulfield	forward			10.202.10.0/24	10.200.10.0/24		VPN Caulfield to Clayton
Caulfield	forward						DENY-ALL-FORWARD - Drop all other forward traffic
Caulfield	input						INPUT-STATEFUL - Allow established/related
Caulfield	input					ICMP	Allow ICMP input
Caulfield	input					UDP 500,4500	Allow IKE input
Caulfield	input					IPsec-ESP	Allow ESP input
Caulfield	input					TCP 179	Allow BGP input
Caulfield	input			10.201.0.0/16			Accept input from Peninsula
Caulfield	input			10.202.10.0/24			Accept input from Caulfield network
Caulfield	input			10.200.10.0/24			Accept input from Clayton network
Caulfield	input						DENY-ALL-INPUT - Drop all other input
Caulfield	output						OUTPUT-STATEFUL - Allow established/related
Caulfield	output					UDP 500,4500	Allow IKE output
Caulfield	output					IPsec-ESP	Allow ESP output
Caulfield	output					TCP 179	Allow BGP output
Caulfield	output						OUTPUT-ALLOW-ALL - Allow all output
Caulfield	output						DENY-ALL-OUTPUT - Drop (not reached due to allow-all)
Clayton	forward						STATEFUL - Allow established/related connections
Clayton	forward					ICMP	Allow ICMP

Fig 18: Firewall rule Part 1

Clayton	forward					ICMP	Allow ICMP
Clayton	forward			10.200.10.0/24	10.201.30.10	UDP 53	DNS queries to Peninsula
Clayton	forward			10.201.30.10	10.200.10.0/24	UDP 53	DNS responses from Peninsula
Clayton	forward			10.201.30.10		UDP 53	DNS outbound to external
Clayton	forward			10.200.10.0/24	10.201.20.10	TCP 80,443	Web access to Peninsula
Clayton	forward			10.201.20.10			Web outbound
Clayton	forward			10.201.20.11			SMTP outbound
Clayton	forward			10.201.20.12			SSH outbound
Clayton	forward		ether1	10.200.10.0/24			Internet access
Clayton	forward			10.200.10.0/24	10.201.20.12	TCP 22	Block SSH from Clayton
Clayton	forward			10.200.10.0/24	10.201.20.11	TCP 25,587,465	Block SMTP from Clayton (for Caulfield Q7)
Clayton	forward			10.201.0.0/16	10.200.10.0/24		VPN to Clayton from Peninsula
Clayton	forward			10.200.10.0/24	10.201.0.0/16		VPN from Clayton to Peninsula
Clayton	forward			10.202.10.0/24	10.200.10.0/24		VPN to Clayton from Caulfield
Clayton	forward			10.200.10.0/24	10.202.10.0/24		VPN from Clayton to Caulfield
Clayton	forward						DENY-ALL-FORWARD
Clayton	input						INPUT-STATEFUL - Allow established/related
Clayton	input					ICMP	Allow ICMP input
Clayton	input					UDP 500,4500	Allow IKE input
Clayton	input					IPsec-ESP	Allow ESP input
Clayton	input					TCP 179	Allow BGP input
Clayton	input			10.201.0.0/16			Accept from Peninsula
Clayton	input			10.200.10.0/24			Accept from Clayton network
Clayton	input			10.202.10.0/24			Accept from Caulfield
Clayton	input						DENY-ALL-INPUT
Clayton	output						OUTPUT-STATEFUL - Allow established/related
Clayton	output					UDP 500,4500	Allow IKE output
Clayton	output					IPsec-ESP	Allow ESP output
Clayton	output					TCP 179	Allow BGP output
Clayton	output						OUTPUT-ALLOW-ALL
Clayton	output						DENY-ALL-OUTPUT
Peninsula	forward						STATEFUL - Allow established/related connections
Peninsula	forward					ICMP	Allow ICMP
Peninsula	forward			10.201.10.0/24	10.201.30.10	UDP 53	DNS queries from Peninsula network
Peninsula	forward			10.202.10.0/24	10.201.30.10	UDP 53	DNS from Caulfield
Peninsula	forward			10.200.10.0/24	10.201.30.10	UDP 53	DNS from Clayton
Peninsula	forward			172.16.10.10-172.16.10.50	10.201.30.10	UDP 53	DNS from Remote VPN (172.16.10.10-172.16.10.50)
Peninsula	forward			10.201.30.10		UDP 53	DNS outbound
Peninsula	forward			10.201.30.10		UDP 53	DNS responses
Peninsula	forward			172.16.10.10-172.16.10.50	10.201.20.12	TCP 22	SSH from remote VPN only (172.16.10.10-172.16.10.50)
Peninsula	forward			10.201.20.12			SSH outbound

Fig 19: Firewall Rule Part 2

Peninsula	forward			10.201.10.0/24	10.201.20.10	TCP 80,443	Web from Peninsula
Peninsula	forward			10.200.10.0/24	10.201.20.10	TCP 80,443	Web from Clayton
Peninsula	forward			10.202.10.0/24	10.201.20.10	TCP 80,443	Web from Caulfield
Peninsula	forward	ether1	ether3	10.201.20.10		TCP 80,443	Web external
Peninsula	forward		ether1	10.201.20.10			Web outbound
Peninsula	forward			10.202.10.0/24	10.201.20.11	TCP 25,587,465	SMTP from Caulfield (Q7)
Peninsula	forward	ether1	ether3	10.201.20.11		TCP 25,587,465	SMTP external
Peninsula	forward		ether1	10.201.20.11			SMTP outbound
Peninsula	forward		ether1	10.201.10.0/24			Internet access for Peninsula
Peninsula	forward			172.16.10.10-172.16.10.50	10.201.20.11	TCP 25,587,465	Block SMTP from remote VPN (172.16.10.10-172.16.10.50)
Peninsula	forward			10.200.10.0/24	10.201.20.12	TCP 22	Block SSH from Clayton
Peninsula	forward			10.202.10.0/24	10.201.20.12	TCP 22	Block SSH from Caulfield
Peninsula	forward			10.201.10.0/24	10.201.20.12	TCP 22	Block SSH from Peninsula network
Peninsula	forward			10.200.10.0/24	10.201.20.11	TCP 25,587,465	Block SMTP from Clayton (for Caulfield Q7)
Peninsula	forward			10.201.0.0/16	10.200.10.0/24		VPN to Clayton
Peninsula	forward			10.200.10.0/24	10.201.0.0/16		VPN from Clayton
Peninsula	forward			10.201.0.0/16	10.202.10.0/24		VPN to Caulfield
Peninsula	forward			10.202.10.0/24	10.201.0.0/16		VPN from Caulfield
Peninsula	forward			10.200.10.0/24	10.202.10.0/24		VPN Clayton-Caulfield
Peninsula	forward			10.202.10.0/24	10.200.10.0/24		VPN Caulfield-Clayton
Peninsula	forward			10.201.0.0/16	172.16.10.10-172.16.10.50		VPN to Remote (172.16.10.10-172.16.10.50)
Peninsula	forward			172.16.10.10-172.16.10.50	10.201.0.0/16		VPN from Remote (172.16.10.10-172.16.10.50)
Peninsula	forward						DENY-ALL-FORWARD
Peninsula	input						INPUT-STATEFUL - Allow established/related
Peninsula	input					ICMP	Allow ICMP input
Peninsula	input					UDP 500,4500	Allow IKE input
Peninsula	input					IPsec-ESP	Allow ESP input
Peninsula	input					TCP 179	Allow BGP input
Peninsula	input			10.201.0.0/16			Accept from Peninsula
Peninsula	input			10.200.10.0/24			Accept from Clayton
Peninsula	input			10.202.10.0/24			Accept from Caulfield
Peninsula	input			172.16.10.10-172.16.10.50			Accept from Remote VPN (172.16.10.10-172.16.10.50)
Peninsula	input						DENY-ALL-INPUT
Peninsula	output						OUTPUT-STATEFUL - Allow established/related
Peninsula	output					UDP 500,4500	Allow IKE output
Peninsula	output					IPsec-ESP	Allow ESP output
Peninsula	output					TCP 179	Allow BGP output
Peninsula	output						OUTPUT-ALLOW-ALL
Peninsula	output						DENY-ALL-OUTPUT

Fig 20: Firewall Rule Part 3

Q8: Security Analysis

Part 1: Firewall Bypass Analysis (4 Marks)

Can the Firewall Configuration Be Bypassed?

YES, the current firewall configuration has several vulnerabilities that can be exploited to bypass security controls:

1. Egress Filtering Weakness (Critical)

Bypass Method:

- The firewall can be used to exfiltrate data to external destinations without restriction
- Malware on the firewall can establish C2 (Command & Control) channels freely

Counter Measures:

- Implement egress filtering on output chain: only allow firewall management traffic (NTP, syslog, DNS, BGP, IPsec)

- Replace OUTPUT-ALLOW-ALL with OUTPUT-DENY-ALL and explicitly permit only necessary protocols

2. DNS Tunneling (High Risk)

Bypass Method:

- Attackers can encode data in DNS queries/responses to exfiltrate information
- Tools like iodine or dnscat2 can create tunnels over DNS

Counter Measures:

- Implement DNS Security (DNSSEC) to validate DNS responses
- Add rule to block DNS queries to external servers from internal hosts (force all DNS through 10.201.30.10 only)

Part 2: Network Security Improvements (8 Marks)

1. Intrusion Prevention System (IPS) - Inline Deployment

What It Is: Active security device that analyzes network traffic in real-time, detects threats using signatures and anomaly detection, and automatically blocks malicious traffic.

Where to Integrate:

- **Peninsula:** Place inline between Peninsula firewall (ether2: 10.201.10.1) and internal switch
    - Traffic flow: Peninsula clients → Firewall ether2 → **IPS** → Internal switch → Servers
- **Clayton/Caulfield:** Deploy at Internet edge
    - Traffic flow: ISP → Firewall ether1 → **IPS** → Firewall ether2 → Internal network

How It Strengthens Infrastructure:

- Blocks exploit attempts targeting servers (10.201.20.10/11/12) before reaching them
- Complements existing Snort IDS (10.201.20.50) by taking automated action

2. Web Application Firewall (WAF) - Reverse Proxy Mode

What It Is: Layer 7 firewall specifically designed to inspect, filter, and protect HTTP/HTTPS traffic by understanding web application protocols and common attack patterns.

Where to Integrate:

- Deploy on Peninsula network: **New WAF node at 10.201.20.9**
- Position: Between firewall and web server
    - Traffic flow: External → Peninsula FW → **WAF (10.201.20.9)** → Web Server (10.201.20.10)

How It Strengthens Infrastructure:

- Blocks SQL injection: ' OR '1'='1 in HTTP parameters before reaching web application
- Specific to your network: Protects the web server (10.201.20.10) which all three campuses + external clients access

3. Secure Email Gateway (SEG) at Peninsula

What It Is: Specialized email security appliance that filters inbound/outbound email for spam, phishing, malware, and data loss prevention.

Where to Integrate:

- Deploy at Peninsula: **New SEG node at 10.201.20.13**
- Position: Inline with SMTP server
    - Inbound: External SMTP → Peninsula FW → **SEG (10.201.20.13)** → SMTP (10.201.20.11) → Mailboxes
    - Outbound: Clients → SMTP (10.201.20.11) → **SEG (10.201.20.13)** → Peninsula FW → Internet
- Update firewall rules to redirect port 25/587/465 traffic through SEG first

How It Strengthens Infrastructure:

- Blocks phishing emails before reaching users (CEO fraud, credential harvesting)
- Detects malware attachments (ransomware, trojans) using sandboxing
- Specific to your network: Currently Caulfield can send SMTP (Q7 authorization), SEG ensures outbound emails don't leak sensitive data

4. Network Access Control (NAC) at Each Campus

What It Is: System that enforces security policy compliance before allowing devices to access the network. Checks device health, authentication, and posture.

Where to Integrate:

- **Peninsula:** NAC controller at 10.201.30.12, inline between firewall ether2 and client LAN switch
- **Clayton:** NAC at 10.200.30.1 (new subnet for infrastructure)
- **Caulfield:** NAC at 10.202.30.1
- 802.1X authentication on switch ports

How It Strengthens Infrastructure:

- Prevents unauthorized devices from connecting (stolen laptops, rogue devices)
- Quarantines non-compliant devices (missing patches, no antivirus) to remediation VLAN
- Specific to your network: Prevents compromised device at 10.202.10.x (Caulfield) from freely accessing Peninsula servers

5. DNS Security Service (DNSSEC + DNS Filtering)

What It Is: DNSSEC provides cryptographic authentication of DNS responses. DNS filtering blocks access to malicious domains.

Where to Integrate:

- Upgrade existing Peninsula DNS server (10.201.30.10)
- Enable DNSSEC validation for all responses
- Deploy DNS filter/firewall: integrate with threat intelligence feeds
- Configure DNS sinkhole for known malicious domains

How It Strengthens Infrastructure:

- Prevents DNS cache poisoning attacks (attacker cannot forge DNS responses)
- Example: User clicks malicious link in email → DNS query to 10.201.30.10 → DNS filter blocks evil.com → Connection refused

- Protects all three campuses since all DNS queries route to 10.201.30.10

6. Security Information and Event Management (SIEM)

What It Is: Centralized log aggregation, correlation, and analysis platform that provides real-time security monitoring and threat detection.

Where to Integrate:

- Deploy at Peninsula: **SIEM server at 10.201.30.20** (new management subnet 10.201.30.0/24)
- Collect logs from all firewalls (Caulfield, Clayton, Peninsula), IDS (10.201.20.50), servers
- Agents on all servers forward logs via syslog (UDP 514) or secure syslog (TCP 6514)

How It Strengthens Infrastructure:

- Correlates events across distributed infrastructure: detects if attacker pivots Clayton → Caulfield → Peninsula
- Alerts on suspicious patterns: 100 failed SSH attempts from 10.200.10.5 → potential brute force
- Specific to your network: Currently remote VPN users (172.16.10.10-50) have direct SSH access to 10.201.20.12; bastion adds additional authentication layer

8. Network Segmentation - DMZ and Server VLANs

Where to Integrate: Peninsula server network subdivision:

- **DMZ Zone (VLAN 20):** 10.201.20.0/24 - Public-facing servers (WEB: 10.201.20.10)
- **Internal Services Zone (VLAN 21):** 10.201.21.0/24 - Move SMTP (→10.201.21.11), SSH (→10.201.21.12)
- **Management Zone (VLAN 30):** 10.201.30.0/24 - DNS (10.201.30.10), CA (10.201.30.11), SIEM (10.201.30.20)
- **Client Zone (VLAN 10):** 10.201.10.0/24 - Unchanged

How It Strengthens Infrastructure:

- Specific to your network: Currently all servers in 10.201.20.0/24 are equally accessible; segmentation means compromised web server cannot pivot to SSH server directly

Q9: IDS

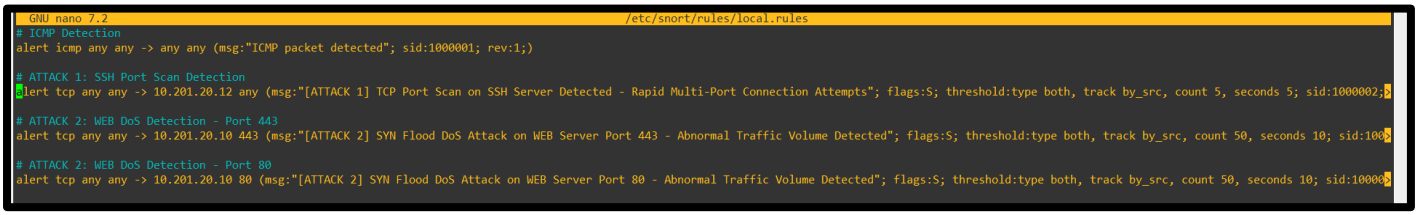

Fig 21: IDS Rules