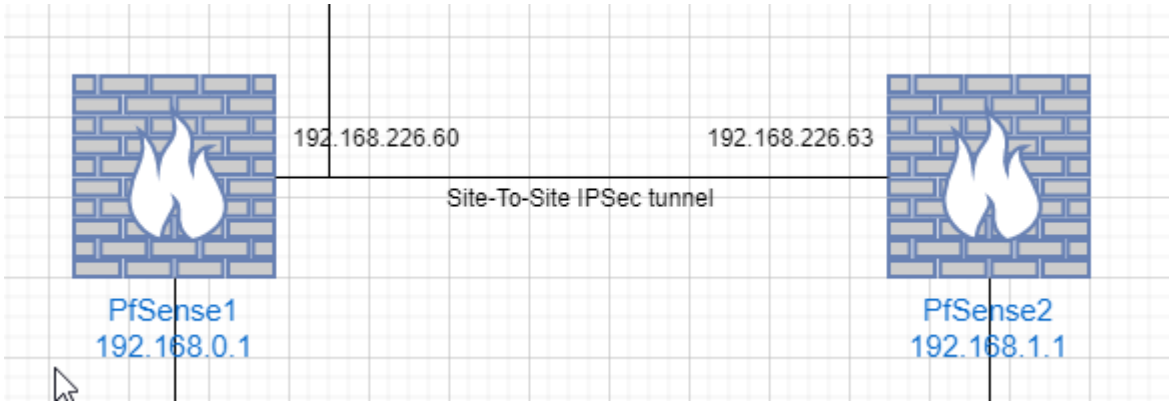
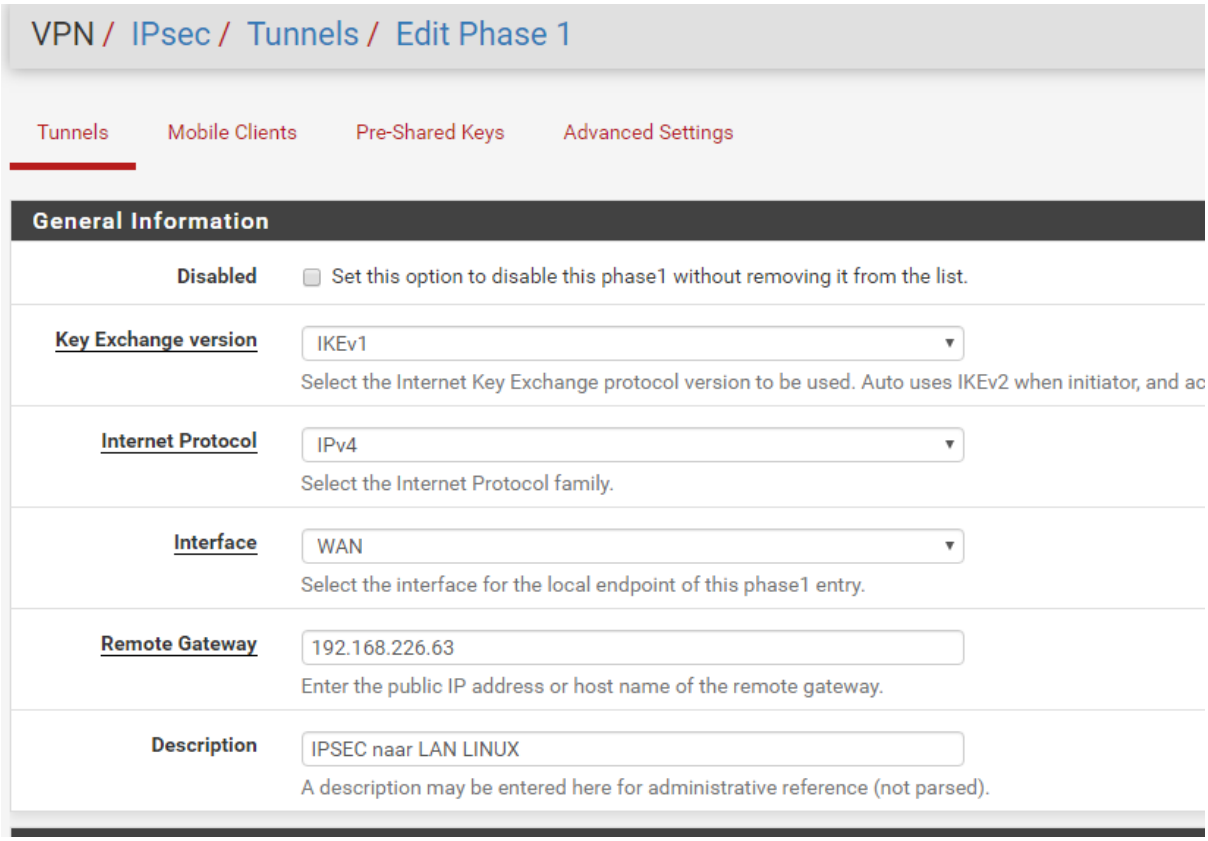
VPN IPsec tunnel PfSense



Op Pfsense 1:

Stap 1: Phase 1 maken op PFsense1

1. VPN -> IPsec -> Add P1
2. Remote Gateway: WAN IP van Pfsense 2 (192.168.226.63)
3. Description: VPN naar Pfsense 2
4. Klik op Generate new Shared Key, copy paste deze naar een txt bestandje
5. Save, Apply Changes



Phase 1 Proposal (Authentication)

Authentication Method: Mutual PSK

Must match the setting chosen on the remote side.

Negotiation mode: Main

Aggressive is more flexible, but less secure.

My identifier: My IP address

Peer identifier: Peer IP address

Pre-Shared Key: 2dfeab4b2c000ae60546e8217ff8c09882ba2422d1f08262f7b9e6c2

Enter the Pre-Shared Key string. This key must match on both peers.

This key should be long and random to protect the tunnel and its contents. A weak Pre-Shar

Generate new Pre-Shared Key

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm

AES	128 bits	SHA256
Algorithm	Key length	Hash

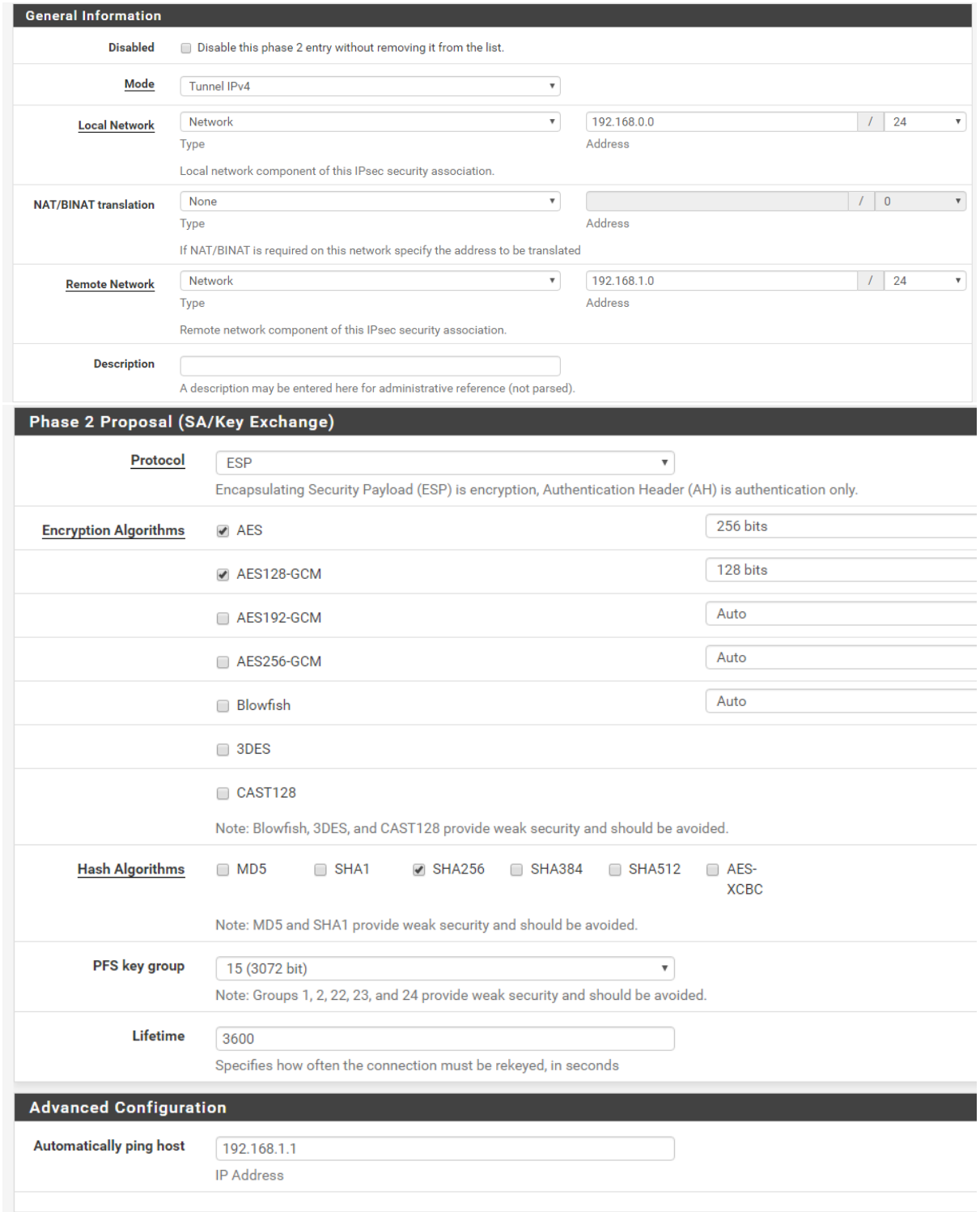
Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 22, 23, and 24 provide wea

Add Algorithm: Add Algorithm

Lifetime (Seconds): 28800

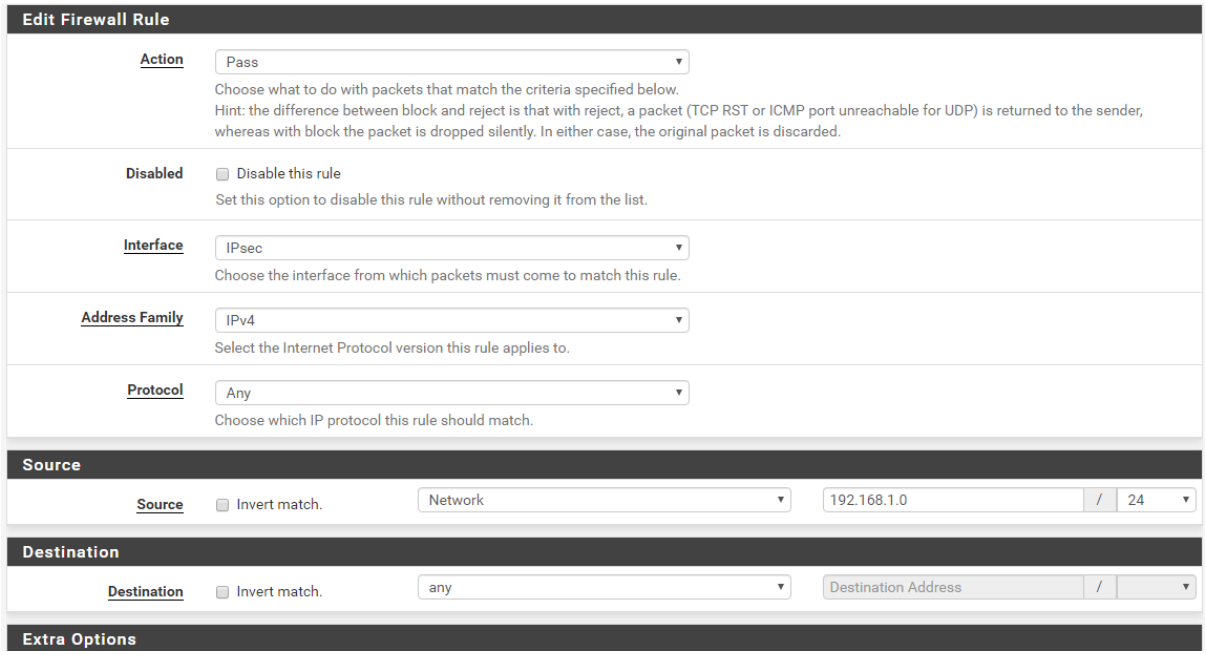
Stap 2: Phase 2 maken op PFsense 1

1. VPN – Ipsec – Show Phase 2 – Add phase 2
2. Local network: Network -> 192.168.0.0/24
3. Remote network: Network -> 192.168.1.0/24
4. AES : 256 bits
5. PFS Keygroup: 15
6. Auto ping: 192.168.1.1 (PFsense 2, Lan Adres)
7. Save, Apply changes



Stap 3: Firewall regel op PFsense 1

1. Firewall – Rules – Ipsec: Add rule
2. Protocol: any
3. Source: Network – 192.168.1.0/24 (PFsense 2 LAN)
4. Save, apply changes



Dan alles hetzelfde doen op pfsense2:

Stap 4: Phase 1 maken op PFsense2

1. VPN -> IPsec -> Add P1
2. Remote Gateway: WAN IP van Pfsense 1 (192.168.226.60)
3. Description: VPN naar Pfsense 1
4. Shared key: Copy paste vanop Pfsense1: 2dfeab4b2c000ae60546e8217ff8c09882ba2422d1f08262f7b9e6c2
5. Save, Apply Changes

Stap 5: Phase 2 maken op PFsense 2

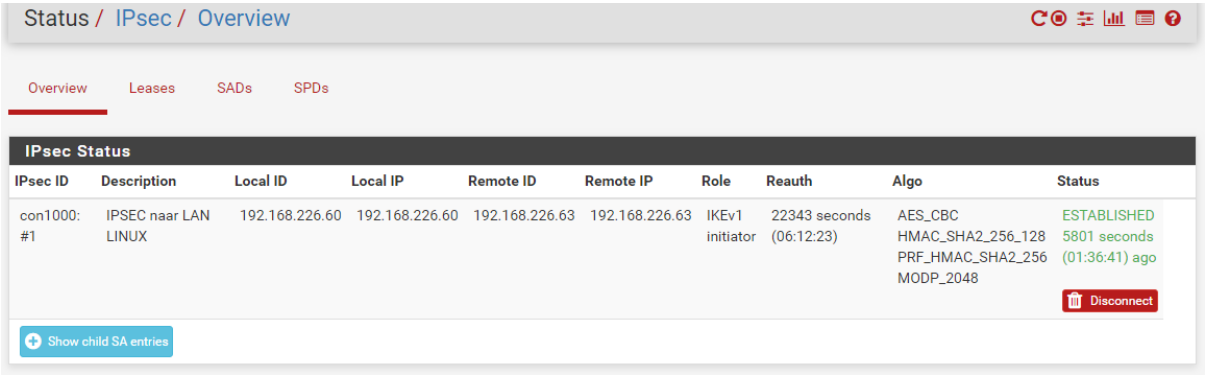
1. VPN – Ipsec – Show Phase 2 – Add phase 2
2. Local network: Network -> 192.168.1.0/24
3. Remote network: Network -> 192.168.0.0/24
4. AES : 256 bits
5. PFS Keygroup: 15
6. Auto ping: 192.168.0.1 (PFsense 2, Lan Adres)
7. Save, Apply changes

Stap 6: Firewall regel op PFsense 2

1. Firewall – Rules – Ipsec: Add rule
2. Protocol: any
3. Source: Network – 192.168.0.0/24 (PFsense 1 LAN)
4. Save, apply changes

Stap 7: Test

1. Status – Ipsec: kijk of tunnel ESTABLISHED is



2. Ping vanop een client in LAN1 naar Pfsense2 (192.168.1.1)

Opdrachtprompt

```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. Alle rechten voorbehouden.

C:\Users\gust>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\gust>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\gust>
```