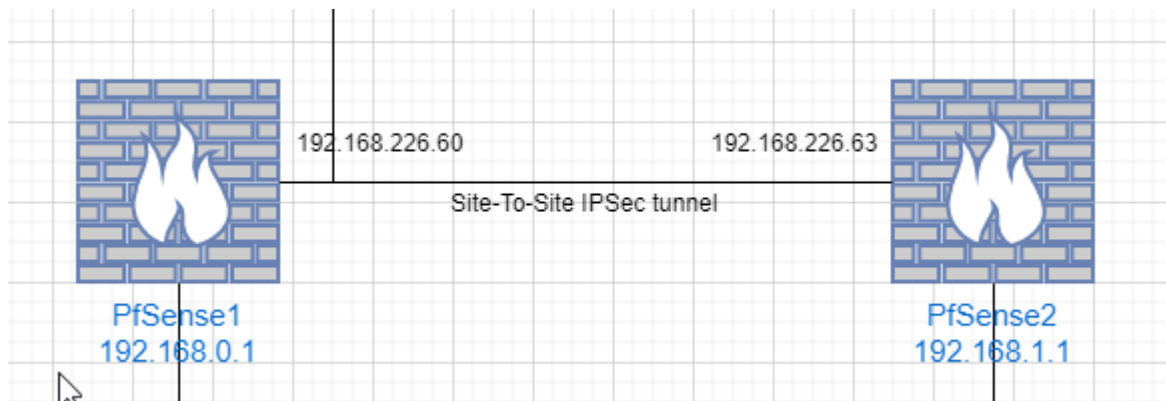


VPN IPsec tunnel PfSense



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

VPN / IPsec / Tunnels / Edit Phase 1

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Disabled ☐ Set this option to disable this phase1 without removing it from the list.

Key Exchange version IKEv1
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and ac

Internet Protocol IPv4
Select the Internet Protocol family.

Interface WAN
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway 192.168.226.63
Enter the public IP address or host name of the remote gateway.

Description IPSEC naar LAN LINUX
A description may be entered here for administrative reference (not parsed).

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

Algorithm

128 bits

Key length

SHA256

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

Step 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

General Information	
Disabled	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.
Mode	Tunnel IPv4
Local Network	Network 192.168.0.0 / 24
Type Address	
Local network component of this IPsec security association.	
NAT/BINAT translation	None / 0
Type Address	
If NAT/BINAT is required on this network specify the address to be translated	
Remote Network	Network 192.168.1.0 / 24
Type Address	
Remote network component of this IPsec security association.	
Description	
A description may be entered here for administrative reference (not parsed).	

Phase 2 Proposal (SA/Key Exchange)	
Protocol	ESP
Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.	
Encryption Algorithms	<input checked="" type="checkbox"/> AES 256 bits
	<input checked="" type="checkbox"/> AES128-GCM 128 bits
	<input type="checkbox"/> AES192-GCM Auto
	<input type="checkbox"/> AES256-GCM Auto
	<input type="checkbox"/> Blowfish Auto
	<input type="checkbox"/> 3DES
	<input type="checkbox"/> CAST128
Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.	
Hash Algorithms	<input type="checkbox"/> MD5 <input type="checkbox"/> SHA1 <input checked="" type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512 <input type="checkbox"/> AES-XCBC
Note: MD5 and SHA1 provide weak security and should be avoided.	
PFS key group	15 (3072 bit)
Note: Groups 1, 2, 22, 23, and 24 provide weak security and should be avoided.	
Lifetime	3600
Specifies how often the connection must be rekeyed, in seconds	

Advanced Configuration	
Automatically ping host	192.168.1.1
IP Address	

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

Edit Firewall Rule	
Action	<div>Pass</div> <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>IPsec</div> <div>Choose the interface from which packets must come to match this rule.</div>
Address Family	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div>
Protocol	<div>Any</div> <div>Choose which IP protocol this rule should match.</div>
Source	
Source	<div><input type="checkbox"/> Invert match.</div> <div>Network</div> <div>192.168.1.0 / 24</div>
Destination	
Destination	<div><input type="checkbox"/> Invert match.</div> <div>any</div> <div>Destination Address /</div>
Extra Options	

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

Status / IPsec / Overview

Overview Leases SADs SPDs

IPsec Status									
IPsec ID	Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
con1000: #1	IPSEC naar LAN LINUX	192.168.226.60	192.168.226.60	192.168.226.63	192.168.226.63	IKEv1 initiator	22343 seconds (06:12:23)	AES_CBC HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	ESTABLISHED 5801 seconds (01:36:41) ago Disconnect

[+ Show child SA entries](#)

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

C:\ 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>
```