SITE TO SITE VPN CONFIGURATION

## Between pfSense and MikroTik Router

**Document by:**

**Sujal Lamichhane**

# Introduction

In today’s enterprise and organizational environments, secure and reliable communication between geographically separated networks is critical. Whether it's for branch offices, remote teams, or multi-location infrastructure, maintaining a seamless and encrypted connection is essential for productivity and data protection. A Site-to-Site VPN (Virtual Private Network) allows two or more physically distant networks to connect securely over the internet as if they were on the same local area network (LAN). This document outlines the comprehensive configuration and implementation of a Site-to-Site VPN tunnel between two widely used networking platforms: pfSense, an open-source firewall/router based on FreeBSD, and MikroTik RouterOS, a versatile operating system used for network routing, firewall, and VPN services. Both devices are configured to create an IPsec VPN tunnel that ensures encrypted communication between two different LANs across the internet. The purpose of this setup is to provide secure, private communication between internal resources located at both sites. After successful implementation, users and devices on either side of the VPN tunnel will be able to communicate with each other without requiring any additional routing or NAT configuration beyond the VPN endpoints. This document is intended for system administrators, network engineers, or IT professionals who are familiar with basic networking principles and seek to integrate pfSense and MikroTik in a site-to-site IPsec VPN topology. It covers all the necessary prerequisites, configuration steps, and testing procedures needed to achieve a stable and secure tunnel between the two devices.

# Network Overview

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Site** | **Device** | **LAN Network** | **WAN IP (Public)** | **VPN Type** |
| Site A | pfSense | 192.168.20.0/24 | 192.168.110.155 | IPsec / IKEv2 |
| Site B | MikroTik | 192.168.30.0/24 | 192.168.110.10 | IPsec / IKEv2 |

# Network Diagram

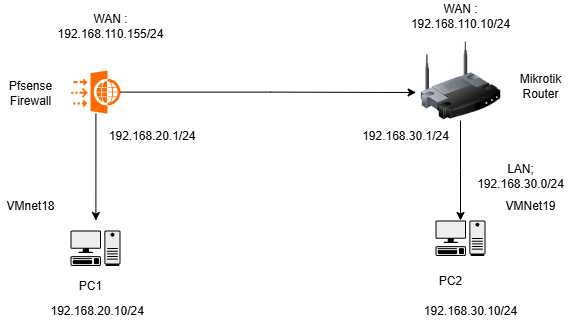


Figure Network Architecture

# **Configuration on pfSense**

### Configure the IPsec VPN on Pfsense firewall:

Let’s start the configuration IPsec site to site VPN configuration at the pfsense side and then we will proceed with the MikroTik router side. Once we’ve got everything set up, we’ll test the connectivity.

### Pfsense Phase1 configuration

We are going to start IPsec tunnel configuration with phase1 and then we’ll go ahead with phase2.

To configure the IPsec Phase1, navigate to VPN -> IPsec. Under the ‘Tunnels‘ tab, click on ‘Add ‘to create a new tunnel.

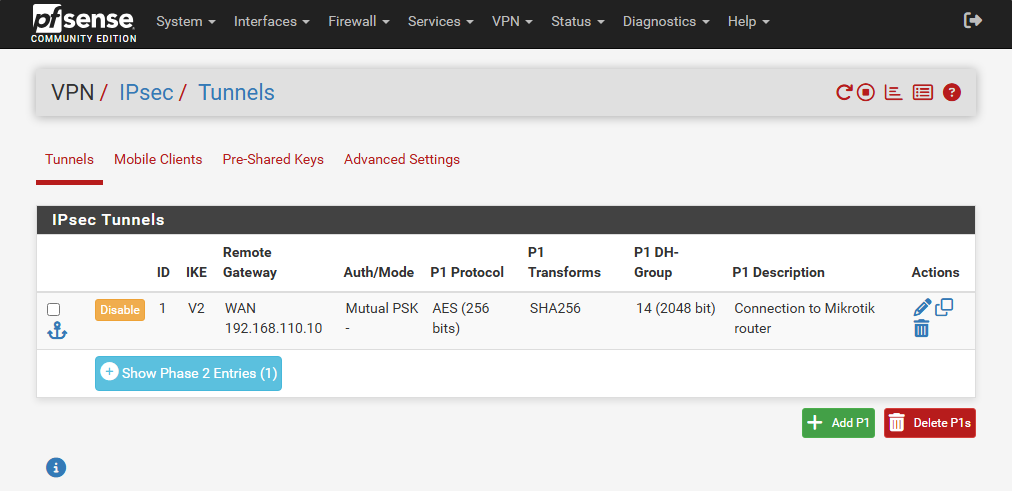


Figure Tunneling

### General Information.

For the ‘Description ‘, enter a distinct name that you can use to identify the tunnel we’re about to create.

A screenshot of a computer

AI-generated content may be incorrect.

Figure General Information

### IKE Endpoint Configuration

A screenshot of a computer

AI-generated content may be incorrect.

Figure IKE Endpoint Configuration

### Phase1 Proposal (Authentication)

A screenshot of a computer

AI-generated content may be incorrect.

Figure Phase 1 Proposal

### Phase1 proposal (Encryption Algorithm)

A screenshot of a computer

AI-generated content may be incorrect.

Figure Phase 1 Proposal (Encryption)

Leave everything default in the expiration and Replacement and click on Ok. And apply configuration.

### Configure the pfsense phase2 of the tunnel.

A screenshot of a computer

AI-generated content may be incorrect.

Figure Phase 2 Configuration

### Click on Add P2 to add the phase 2 parameters.

### General Information.

Description: Enter the description for phase2 of the tunnel.

Mode: Choose Tunnel IPv4.

### A screenshot of a computer AI-generated content may be incorrect.

Figure Phase 2 General Information

### Networks

### Local Network: LAN Subnet – This will take care of the whole 192.168.20.0/24 network which is configured on the pfsense Lan side.

### Remote Network: Choose Network from the drop down and specify the remote address which is 192.168.30.0/24

### A screenshot of a computer AI-generated content may be incorrect.

Figure Network Configuration

### Phase2 Proposal

### A screenshot of a computer AI-generated content may be incorrect.

Figure Phase 2 SA/Key Configuration

### Leave **expiration and replacement default** and click on Finish.

### You will see the phase2 of the tunnel is now created, you may **apply the changes.**

### You can check the status of the IPsec tunnel by going into**Status-> IPsec**

### As you can see, we have not configured anything remotely and the tunnel is down now.

### Configure the IPsec policy

We have configured the transport, but in order to allow the traffic through the IPsec transport that we created, we must configure policies.

We are going to allow the traffic that comes from the remote branch network which is 192.168.30./24 network.

Goto -> Firewall-> Rules.

Click on the IPsec tab, and click on Add to add new policy.

A screenshot of a computer

AI-generated content may be incorrect.

Figure IPSec Rule Creation

**Action: Pass**

Protocol: Any – I am not restricting any traffic now, if you would like to specify specific protocol, you can do that here as well.

A screenshot of a computer

AI-generated content may be incorrect.

Figure Firewall rule action , interface , address, protocol

A screenshot of a computer

AI-generated content may be incorrect.  
**Source:**Choose network from the drop down – And mention the MikroTik LAN address –192.168.30.0/24  
**Destination:** Choose LAN net that will cover the entire pfsense LAN network.  
**Check the log box and click on Save.**

Setup the IPsec tunnel at the MikroTik branch side

Let’s now proceed with the MikroTik branch side IPsec site to site vpn configuration. So, the configuration is almost identical to the pfsense firewall, we will configure phase1 first and then we will proceed with phase

### Open Winbox and access Microtik Router

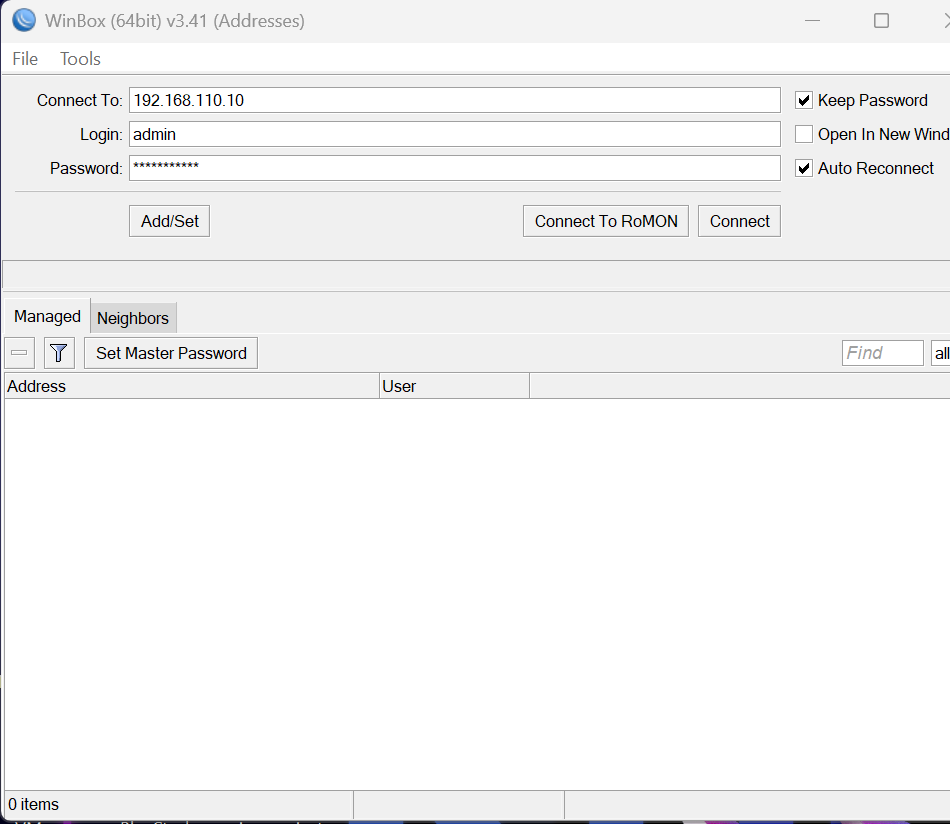


Figure Winbox

### Go to IP – > IPsec > Click on the **profiles**tab > click on the plus icon to add a new profile

A screenshot of a computer

AI-generated content may be incorrect.

Figure ipsec profile

### Configure the Peer

We are now going to define the pfsense as the IPsec peer here.

Click on the peer > plus icon to add new peer

A screenshot of a computer

AI-generated content may be incorrect.

Figure ipsec peer

### Configure the Identity – Pre-shared key

A screenshot of a computer

AI-generated content may be incorrect.

### MikroTik IPsec Phase2 configuration

### We are done with phase1 of the configuration, let’s now proceed with phase2.

IPsec Proposal >Click on the proposals tab, and click on the plus icon>

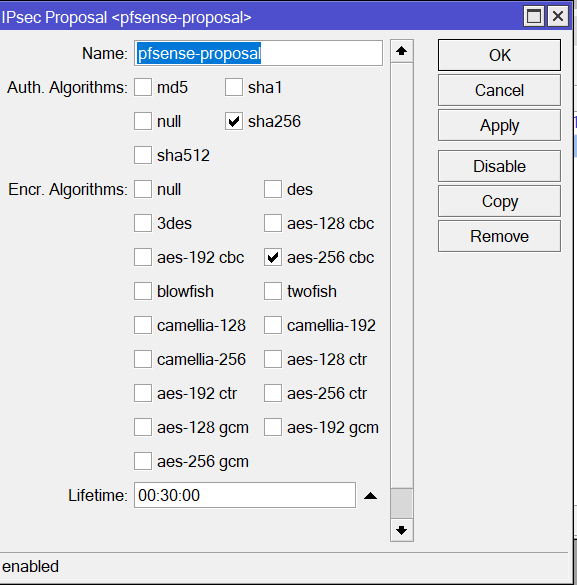


Figure ipsec proposal

### Configure the MikroTik Phase2 policies.

Click on the policies tab, and press the plus icon to add new phase2 policies > In the new policy window configure as follows.

A screenshot of a computer

AI-generated content may be incorrect.

Figure Ipsec policy

In the action tab, under Action drop down choose to encrypt. Proposal: Select the phase 2 proposal that we defined and click on Ok.

A screenshot of a computer

AI-generated content may be incorrect.

### MikroTik NAT configuration.

We have completed the whole MikroTik pfsense phase1 and phase2 tunnel configuration. However, the traffic will not pass now. As we configured the security policies in pfsense, we got to do the same thing on the MikroTik side as well.

Click on IP-> firewall-> NAT >General:

A screenshot of a computer

AI-generated content may be incorrect.

Figure NAT rule

Click on the **Action**tab:

A screenshot of a computer

AI-generated content may be incorrect.

You will see the newly created NAT policy at the bottom, move the rule all the way to the top

A screenshot of a computer

AI-generated content may be incorrect.

## Verify the IPsec VPN tunnel connectivity between pfsense and MikroTik

### Pfsense IPsec status

To check the pfsense IPsec status go to -> Status-> IPsec

As you can see, both the phase1 and phase2 of the IPsec tunnel is now showing up.

A screenshot of a computer

AI-generated content may be incorrect.

Figure IPsec connection

### MikroTik IPsec status

A screenshot of a computer

AI-generated content may be incorrect.

You can see the phase2 also now established.

# Test connectivity from both the pfsense and Mikrotik LAN hosts

### Test the connectivity from the pfSense LAN.

I logged into the machine at the pfsense LAN side, and I tried to ping the PC at MikroTik side, as you can see the ping was successful.

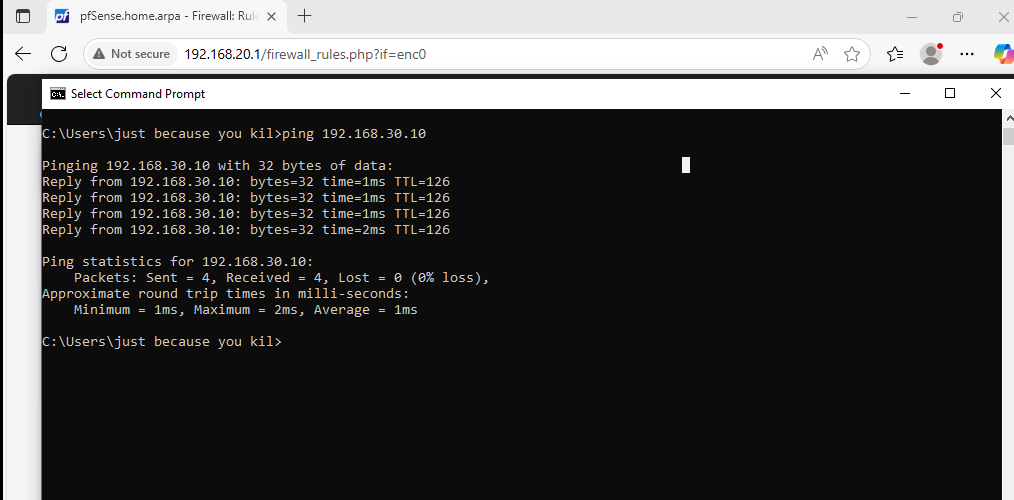


Figure Connectivity of pfsense LAN Client

### Test the connectivity from the MikroTik LAN side.

The same way I am going to initiate the ping from the MikroTik side, as you can see, the first ping was before we initiated the IPsec tunnel and the second ping afterwards, as you can see, we are getting response to the ICMP traffic.

A computer screen with white text

AI-generated content may be incorrect.

Figure Connectivity of Mikrotik LAN Client

Conclusion

The successful configuration of a Site-to-Site VPN between pfSense and MikroTik demonstrates the interoperability and flexibility of modern networking solutions. By leveraging IPsec tunneling, this setup enables secure, encrypted communication between two physically separated networks, effectively bridging them as if they were part of the same local infrastructure. This configuration not only enhances data security by protecting traffic over the internet but also allows seamless access to services, applications, and resources across both locations. It eliminates the need for complex NAT configurations or third-party tunneling services, giving full control over the VPN infrastructure. Maintaining such a setup also provides scalability—additional subnets or sites can be integrated in the future using similar configurations. However, regular monitoring, key rotation, and updates to both pfSense and MikroTik firmware are recommended to ensure long-term reliability and security. With proper configuration, a Site-to-Site VPN can become a cornerstone of any distributed network architecture, supporting secure communication, resource sharing, and efficient IT operations.