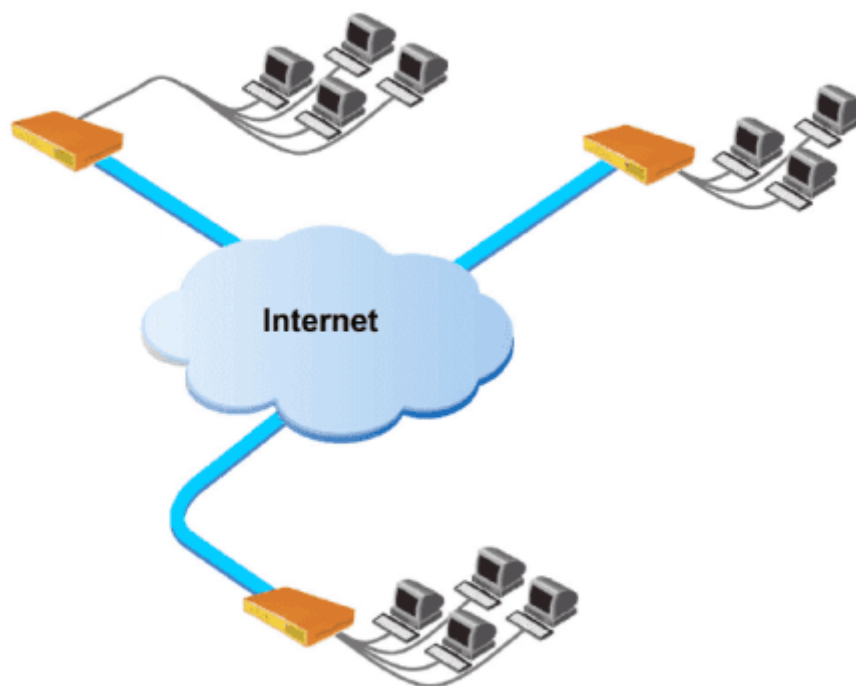


Pfsense и MikroTik, настройка VPN туннеля

Инструкция по настройке VPN туннеля типа IpSec между облачным роутером Pfsense и MikroTik. В результате настройки должно получиться объединение двух сетей, за MikroTik и за Pfsense.



Что такое Pfsense

PfSense — дистрибутив для создания межсетевого экрана/маршрутизатора, основанный на FreeBSD. PfSense предназначен для установки на персональный компьютер, известен своей надежностью и предлагает функции, которые часто можно найти только в дорогих коммерческих межсетевых экранах. Настройки можно проводить через web-интерфейс, что позволяет использовать его без знаний базовой системы FreeBSD. Сетевые устройства с pfSense обычно применяются в качестве периметровых брандмауэров, маршрутизаторов, серверов DHCP/DNS, и в технологии VPN в качестве узла топологии hub/spoke.

Настройка VPN в MikroTik для подключения к Pfsense

Со стороны роутера MikroTik будет настроен стандартный VPN туннель типа IpSec. Больше сведений по настройке VPN типа IpSec представлено в статье:

VPN туннель IpSec состоит из двух фаз:

- PHASE-1 – идентификация устройств между собой, по заранее определенному IP адресу и ключу.
- PHASE-2 – определение политики для трафика между туннелей: шифрование, маршрутизация, время жизни туннеля.

Создание профиля для MikroTik IpSec phase-1

Настройка находится в IP→IPsec→Profile

The screenshot shows the configuration window for an IPsec Profile in MikroTik WinBox. The profile name is 'Pfsense'. The hash algorithm is 'md5'. The encryption algorithm is '3des'. The DH group is 'modp1024'. The proposal check is 'obey', the lifetime is '08:00:00', and the lifebytes field is empty. The 'NAT Traversal' checkbox is checked. The DPD interval is '120' seconds and the DPD maximum failures is '5'. The window includes standard buttons for 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove'.

Pfsense и MikroTik, создание профиля для IpSec phase-1

Создание Peer для MikroTik IpSec phase-1

Настройка находится в IP→IPsec→Peers

IPsec Peer <Pfsense>

Name: Pfsense

Address: 10.10.10.10

Port:

Local Address:

Profile: Pfsense

Exchange Mode: main

Passive

Send INITIAL_CONTACT

enabled responder

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Pfsense и MikroTik, создание Peer для IpSec phase-1

Определение ключа MikroTik IpSec phase-1

Настройка находится в IP→IPsec→Identities

IPsec Identity <Pfsense>

Peer: Pfsense

Auth. Method: pre shared key

Secret: Pt36ENepT3t3

Policy Template Group: default

Notrack Chain:

My ID Type: auto

Remote ID Type: auto

Match By: remote id

Mode Configuration:

Generate Policy: no

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Pfsense и MikroTik, определение ключа IpSec phase-1

Настройка параметров MikroTik Proposal IpSec phase-2

Настройка находится в IP→IPsec→Proposals

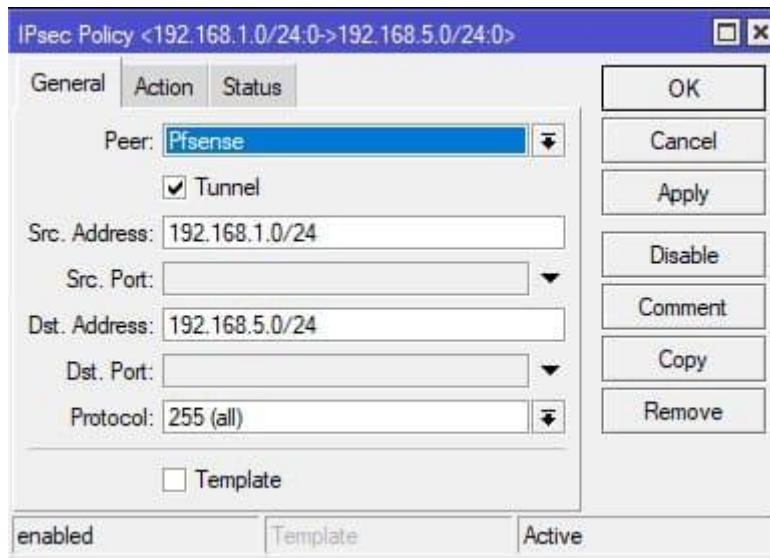
The screenshot shows the 'IPsec Proposal <Pfsense>' configuration window. The 'Name' field is set to 'Pfsense'. Under 'Auth. Algorithms', 'md5' is selected. Under 'Encr. Algorithms', '3des' is selected. The 'Lifetime' is set to '08:00:00' and the 'PFS Group' is set to 'modp1024'. The status at the bottom is 'enabled'. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Copy', and 'Remove'.

Category	Algorithm	Selected
Auth. Algorithms	md5	Yes
	sha1	No
	null	No
	sha256	No
Encr. Algorithms	sha512	No
	null	No
	des	No
	3des	Yes
	aes-128 cbc	No
	aes-192 cbc	No
	aes-256 cbc	No
	blowfish	No
	twofish	No
	camellia-128	No
	camellia-192	No
	camellia-256	No
aes-128 ctr	No	
aes-192 ctr	No	
aes-256 ctr	No	
aes-128 gcm	No	
aes-192 gcm	No	
aes-256 gcm	No	

Pfsense и MikroTik, настройка параметров Proposal IpSec phase-2

Создание политики(Policies) MikroTik IpSec phase-2

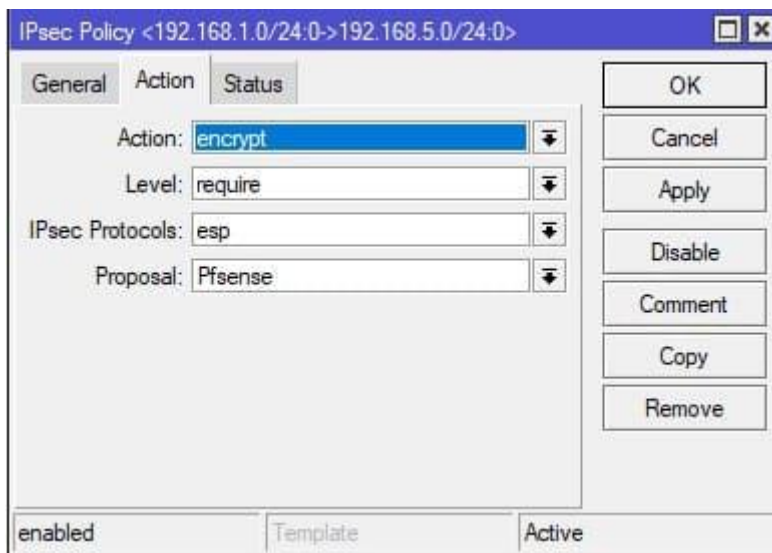
Настройка находится в IP→IPsec→Policies



Pfsense и MikroTik, создание политики(Policies) IpSec phase-2

Настройка политики(Policies) MikroTik IpSec phase-2

Настройка находится в IP→IPsec→Policies→Action



Pfsense и MikroTik, настройка политики(Policies) IpSec phase-2

```

/ip ipsec profile
add dh-group=modp1024 enc-algorithm=3des hash-algorithm=md5 lifetime=8h
name=Pfsense
/ip ipsec peer

```

```
add address=10.10.10.10/32 name=Pfsense profile=Pfsense
/ip ipsec proposal
add auth-algorithms=md5 enc-algorithms=3des lifetime=8h name=Pfsense
/ip ipsec policy
add dst-address=192.168.5.0/24 peer=Pfsense proposal=Pfsense \
sa-dst-address=10.10.10.10 sa-src-address=0.0.0.0 src-address=\
192.168.1.0/24 tunnel=yes
/ip ipsec identity
add peer=Pfsense secret=Pt36ENepT3t3
```

Настройка VPN в Pfsense для подключения к MikroTik

Pfsense имеет удобный web интерфейс, с помощью которого и будет производиться настройка VPN туннеля типа IpSec для связи с роутером MikroTik.

Настройка phase-1 для Pfsense IpSec

The screenshot displays the 'Edit Phase 1' configuration page in the Pfsense web interface. The page is divided into two main sections: 'General Information' and 'Phase 1 Proposal (Authentication)'. The 'General Information' section includes fields for 'Disabled' (checked), 'Key Exchange version' (Auto), 'Internet Protocol' (IPv4), 'Interface' (WAN), 'Remote Gateway' (11.11.11.11), and 'Description'. The 'Phase 1 Proposal (Authentication)' section includes fields for 'Authentication Method' (Mutual PSK), 'Negotiation mode' (Main), 'My identifier' (My IP address), 'Peer identifier' (Peer IP address), and 'Pre-Shared Key' (Pt36ENepT3t3). A 'Generate new Pre-Shared Key' button is located at the bottom of the Pre-Shared Key field.

General Information	
Disabled	<input checked="" type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
Key Exchange version	Auto <small>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</small>
Internet Protocol	IPv4 <small>Select the Internet Protocol family.</small>
Interface	WAN <small>Select the interface for the local endpoint of this phase1 entry.</small>
Remote Gateway	11.11.11.11 <small>Enter the public IP address or host name of the remote gateway.</small>
Description	<input type="text"/> <small>A description may be entered here for administrative reference (not parsed).</small>

Phase 1 Proposal (Authentication)	
Authentication Method	Mutual PSK <small>Must match the setting chosen on the remote side.</small>
Negotiation mode	Main <small>Aggressive is more flexible, but less secure.</small>
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	Pt36ENepT3t3 <small>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-Shared Key can lead to a tunnel compromise.</small> Generate new Pre-Shared Key

Создание phase-1 для Pfsense IpSec

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm 3DES 2 (1024 bit)

Algorithm Key length Hash DH Group

Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm

Lifetime (Seconds)

Advanced Options

Disable rekey Disables renegotiation when a connection is about to expire.

Margintime (Seconds)

How long before connection expiry or keying-channel expiry should attempt to negotiate a replacement begin.

Responder Only Enable this option to never initiate this connection from this side, only respond to incoming requests.

NAT Traversal

Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.

Dead Peer Detection Enable DPD

Delay

Delay between requesting peer acknowledgement.

Max failures

Number of consecutive failures allowed before disconnect.

Настройка phase-2 для Pfsense IpSec

VPN / IPsec / Tunnels 🔍 📄 📌 📧

[Tunnels](#) [Mobile Clients](#) [Pre-Shared Keys](#) [Advanced Settings](#)

IPsec Tunnels

	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> <input type="button" value="Disable"/>	Auto	WAN 11.11.11.11	main	3DES	MD5	2 (1024 bit)		<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="button" value="+ Add P2"/>								

Настройка phase-2 для Pfsense IpSec

Phase 2 Proposal (SA/Key Exchange)	
Protocol	ESP <small>Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.</small>
Encryption Algorithms	<input type="checkbox"/> AES Auto <input type="checkbox"/> AES128-GCM Auto <input type="checkbox"/> AES192-GCM Auto <input type="checkbox"/> AES256-GCM Auto <input type="checkbox"/> Blowfish Auto <input checked="" type="checkbox"/> 3DES <input type="checkbox"/> CAST128 <small>Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.</small>
Hash Algorithms	<input checked="" type="checkbox"/> MD5 <input type="checkbox"/> SHA1 <input type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512 <input type="checkbox"/> AES-XCBC <small>Note: MD5 and SHA1 provide weak security and should be avoided.</small>
PFS key group	2 (1024 bit) <small>Note: Groups 1, 2, 22, 23, and 24 provide weak security and should be avoided.</small>
Lifetime	28800 <small>Specifies how often the connection must be rekeyed, in seconds</small>

Настройка phase-2 для Pfsense IpSec, шифрование

VPN / IPsec / Tunnels / Edit Phase 2

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information	
Disabled	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.
Mode	Tunnel IPv4
Local Network	Network: 192.168.5.0 / 24 <small>Type Address</small> <small>Local network component of this IPsec security association.</small>
NAT/BINAT translation	None / 0 <small>Type Address</small> <small>If NAT/BINAT is required on this network specify the address to be translated</small>
Remote Network	Network: 192.168.1.0 / 24 <small>Type Address</small> <small>Remote network component of this IPsec security association.</small>
Description	 <small>A description may be entered here for administrative reference (not parsed).</small>

Настройка phase-2 для Pfsense IpSec, общие параметры

Настройка Pfsense Firewall

The screenshot shows the 'Edit Firewall Rule' configuration page in Pfsense. The 'Action' is set to 'Pass'. The 'Interface' is 'IPsec'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'Any'. The 'Source' is set to 'any' and the 'Destination' is set to 'WAN address'. The 'Source' and 'Destination' fields are currently empty, indicating that the rule applies to all traffic from any source to any destination on the WAN interface.

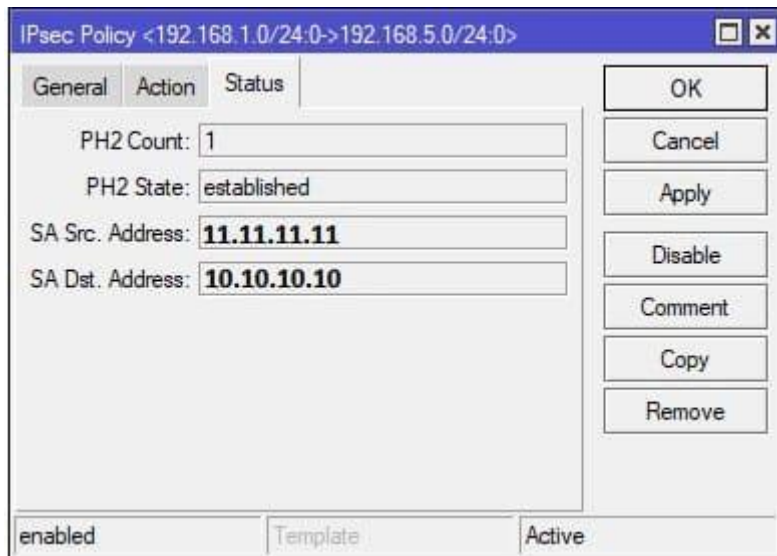
Настройка Pfsense Firewall, разрешение внешнего подключения IpSec

The screenshot shows the 'Edit Firewall Rule' configuration page in Pfsense. The 'Action' is set to 'Pass'. The 'Interface' is 'IPsec'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'Any'. The 'Source' is set to 'Network' with the address '192.168.1.0' and subnet '24'. The 'Destination' is set to 'Network' with the address '192.168.5.0' and subnet '24'. This configuration allows traffic between the two internal networks through the IPsec tunnel.

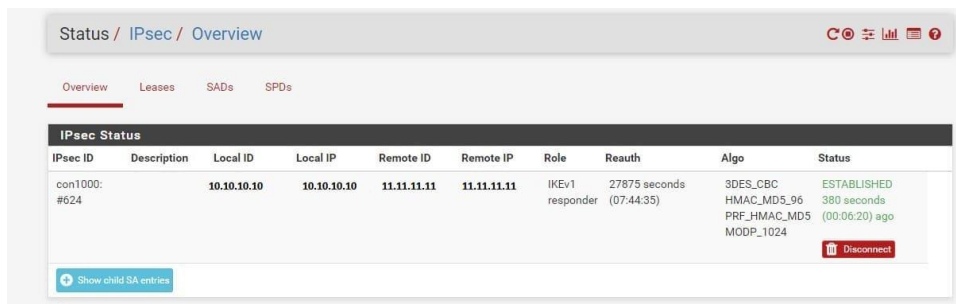
Настройка Pfsense Firewall, обмен трафиком внутри VPN

Результат настройки VPN IpSec между Pfsense и MikroTik

После успешно принятых настроек, проверить соединение VPN типа IpSec между Pfsense и MikroTik можно так:



Pfsense и MikroTik, статус VPN туннеля IpSec



MikroTik и Pfsense, статус VPN IpSec туннеля

[ИСТОЧНИК](#)