

For IPsec pfsense to Mikrotik.

1. Create peers....

IPsec Peer configuration dialog:

- Address: 500 (Remote WAN IP)
- Port: 500
- Auth. Method: pre shared key
- Secret: [Redacted] (Set Secret Key.. Ex. Abc@123)
- Exchange Mode: main
- Send Initial Contact:
- NAT Traversal:
- My ID User FQDN: [Empty]
- Proposal Check: obey
- Hash Algorithm: md5
- Encryption Algorithm: aes-256
- DH Group: modp1024
- Generate Policy:
- Lifetime: 1d 00:00:00
- Lifebytes: [Empty]
- DPD Interval: 120 s
- DPD Maximum Failures: 5
- Status: enabled

2. Set proposal....

IPsec Proposal configuration dialog:

- Name: default
- Auth. Algorithms:
 - md5
 - sha1
 - null
- Encr. Algorithms:
 - null
 - 3des
 - aes-192
 - blowfish
 - camellia-128
 - camellia-256
 - des
 - aes-128
 - aes-256
 - twofish
 - camellia-192
- Lifetime: 00:30:00
- PFS Group: modp1024
- Status: enabled

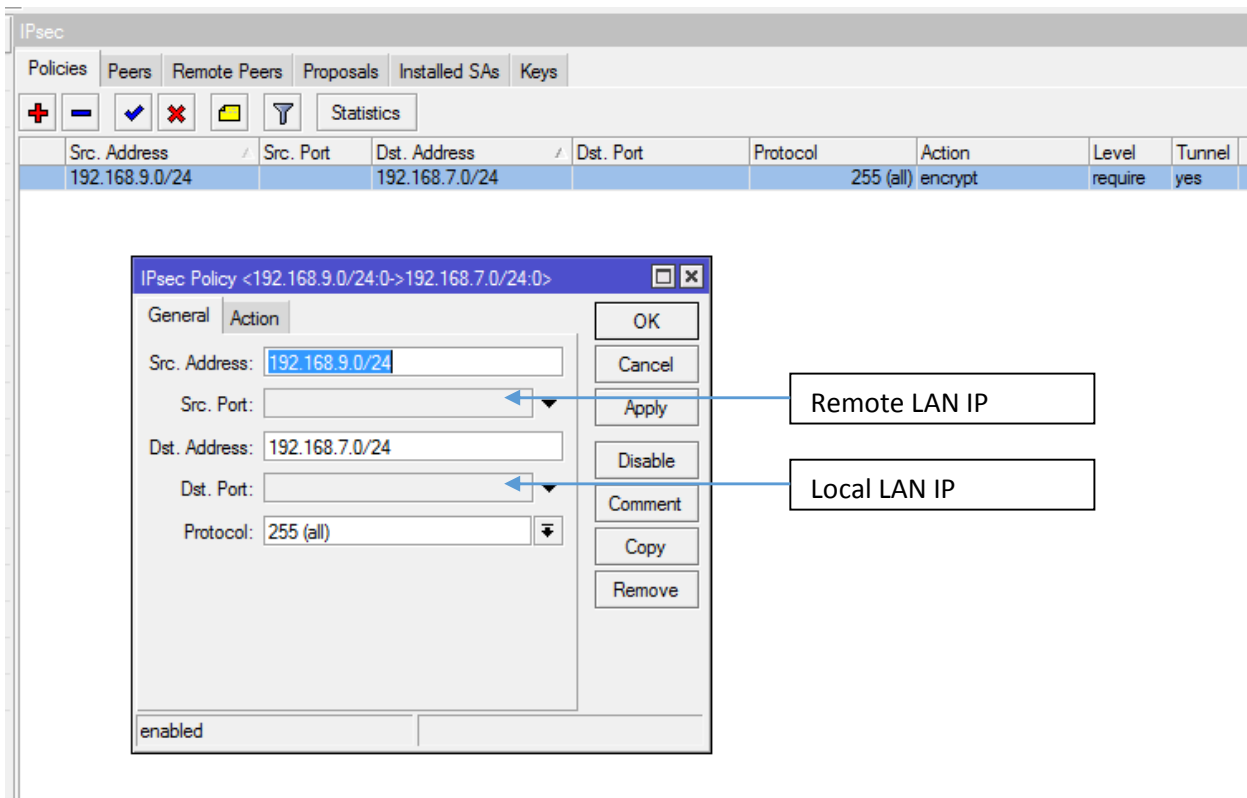
3. Set Policies...

IPsec Policy configuration dialog:

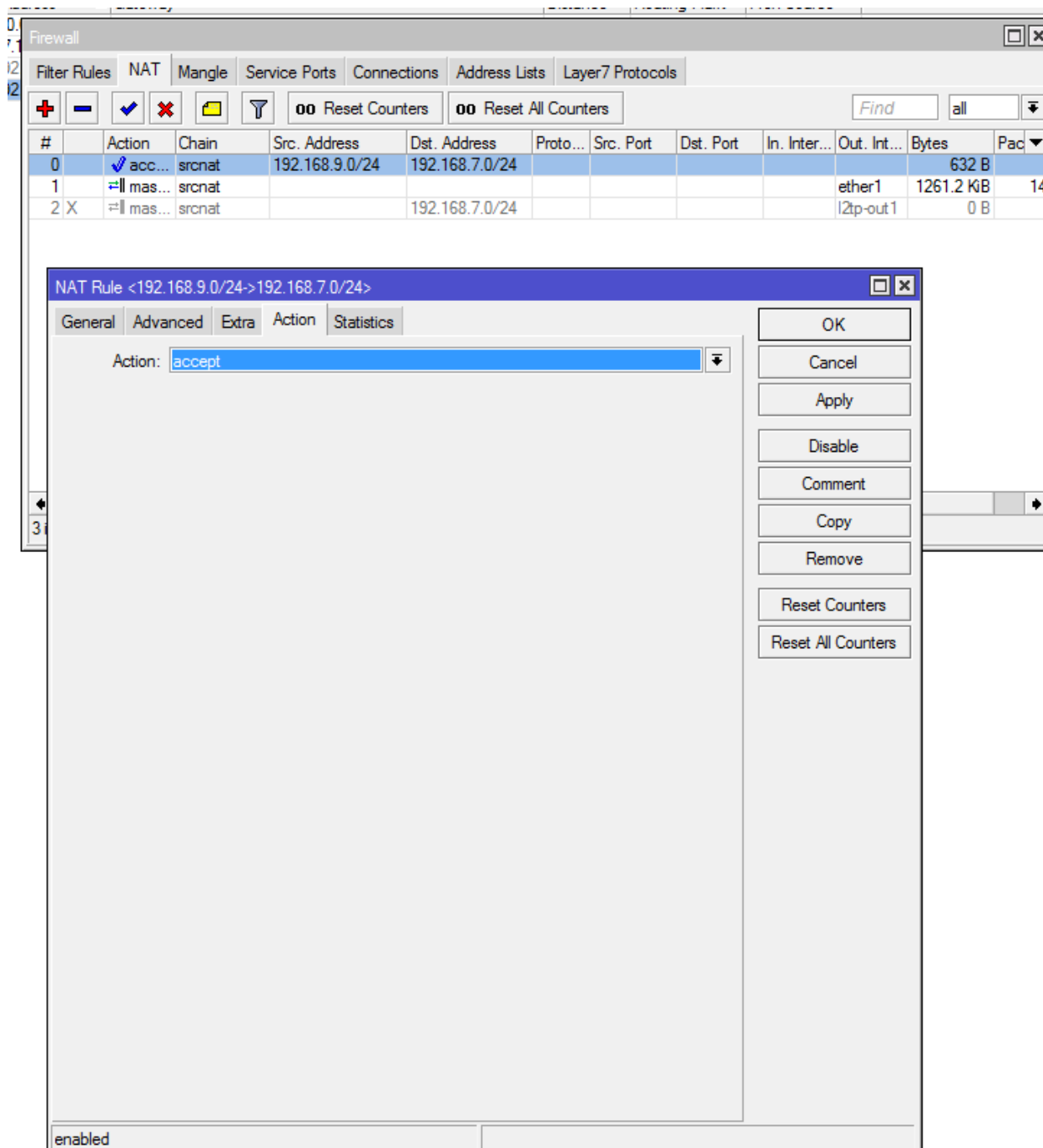
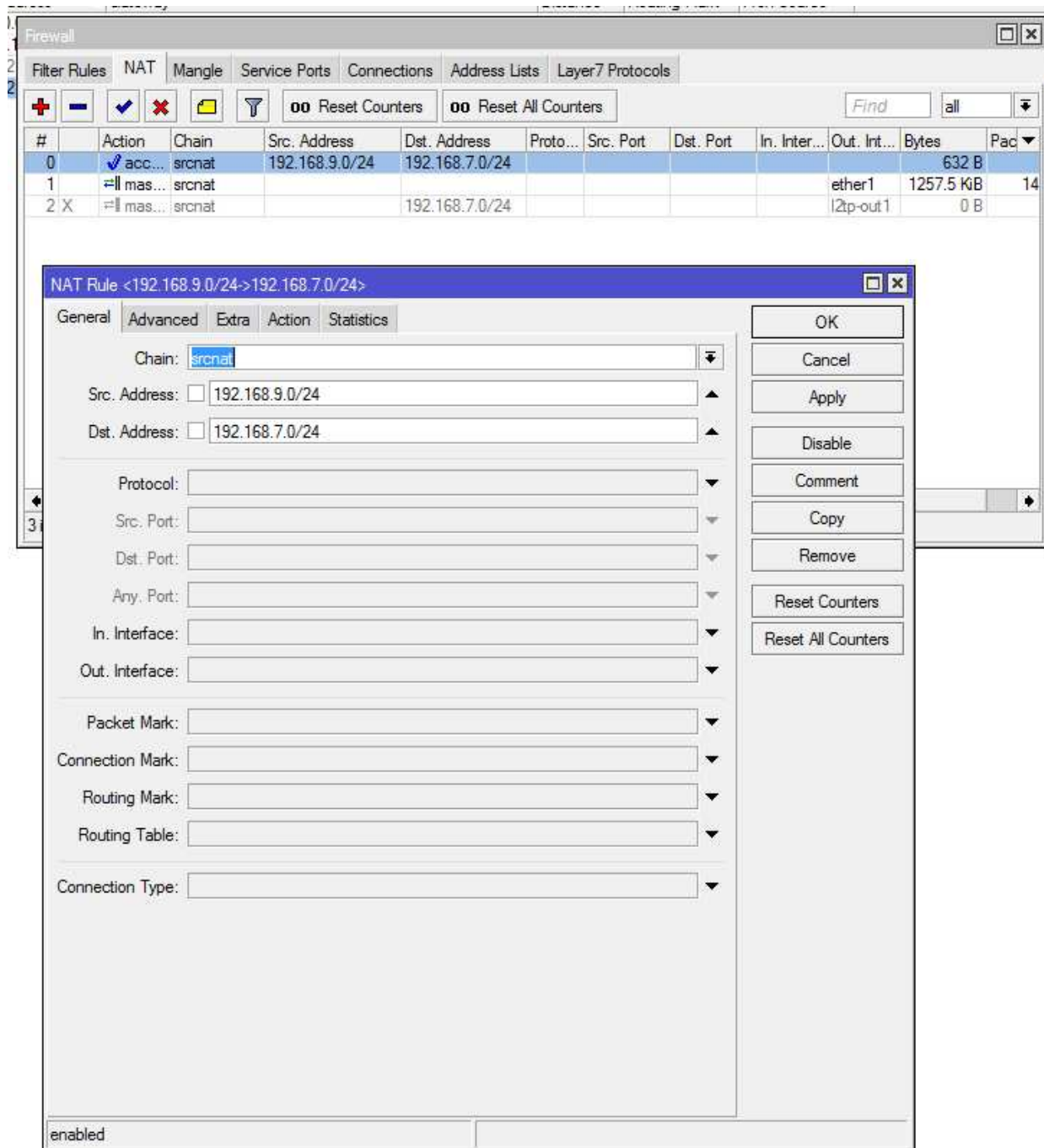
Src. Address	Src. Port	Dst. Address	Dst. Port	Protocol	Action	Level	Tunnel
192.168.9.0/24		192.168.7.0/24		255 (all)	encrypt	require	yes

IPsec Policy configuration details:

- SA Src. Address: [Redacted] (Local WAN IP)
- SA Dst. Address: [Redacted] (Remote WAN IP)
- Proposal: default
- Priority: 0
- Action: encrypt
- Level: require
- IPsec Protocols: esp
- Tunnel:
- Status: enabled



4. Create NAT Rule in Firewall.



Pfsense Configuration stapes

1. Create phase1

The screenshot shows the 'VPN: IPsec: Edit Phase 1' configuration page in pfSense. The 'General information' section is expanded, showing the following settings:

- Disabled:** **Disable this phase1 entry**. Set this option to disable this phase1 without removing it from the list.
- Key Exchange version:** V1. Select the Internet Key Exchange protocol version to be used, IKEv1 or IKEv2.
- Internet Protocol:** IPv4. Select the Internet Protocol family from this dropdown.
- Interface:** WAN. Select the interface for the local endpoint of this phase1 entry.
- Remote gateway:** [Empty field]. Enter the public IP address or host name of the remote gateway. A callout box labeled 'Remote wan IP' points to this field.
- Description:** OZTFS. You may enter a description here for your reference (not parsed).

The 'Phase 1 proposal (Authentication)' section is also visible, showing:

- 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:** abcd1234. Input your Pre-Shared Key string.

The 'Phase 1 proposal (Algorithms)' section shows:

- Encryption algorithm:** AES, 256 bits.
- Hash algorithm:** MD5. Must match the setting chosen on the remote side.
- DH key group:** 2 (1024 bit). Must match the setting chosen on the remote side.
- Lifetime:** 86400 seconds.

The 'Advanced Options' section includes:

- Disable Rekey:** Whether a connection should be renegotiated when it is about to expire.
- Responder Only:** Enable this option to never initiate this connection from this side, only respond to incoming requests.
- NAT Traversal:** Auto. 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 between requesting peer acknowledgement: 10 seconds. Number of consecutive failures allowed before disconnect: 5.

A 'Save' button is located at the bottom of the page.

2. Create phase 2

The screenshot shows the 'VPN: IPsec: Edit Phase 2' configuration page in pfSense. The 'General information' section is expanded, showing the following settings:

- Disabled:** **Disable this phase2 entry**. Set this option to disable this phase2 entry without removing it from the list.
- Mode:** Tunnel IPv4.
- Local Network:** Type: LAN subnet. Address: [Empty field] / 128. In case you need NAT/BINAT on this network specify the address to be translated: Type: None. Address: [Empty field] / 0.
- Remote Network:** Type: Network. Address: 192.168.9.0 / 24. A callout box labeled 'Remote Lan IP' points to this field.
- Description:** office. You may enter a description here for your reference (not parsed).

The 'Phase 2 proposal (SA/Key Exchange)' section is also visible, showing:

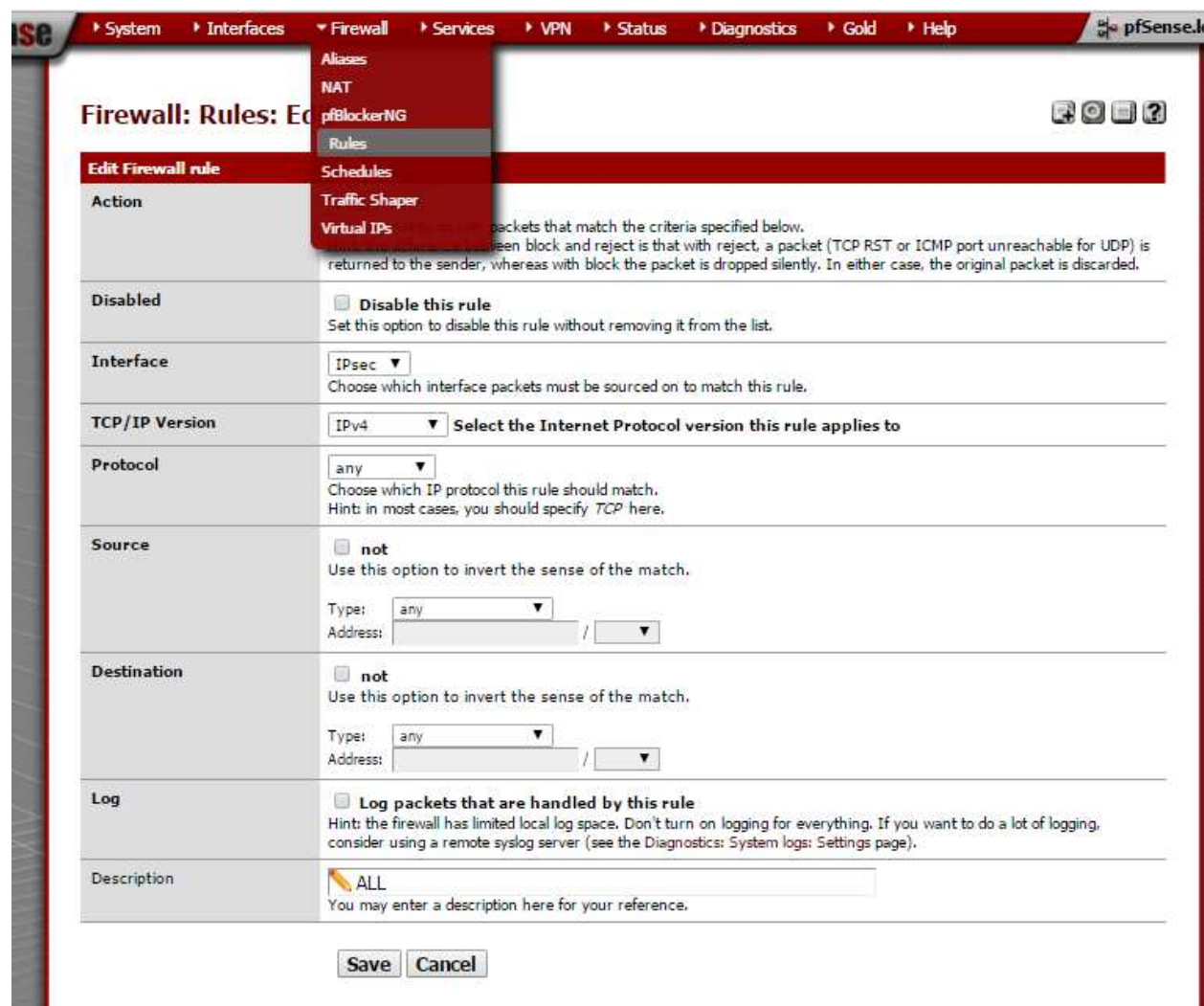
- Protocol:** ESP. ESP is encryption, AH is authentication only.
- Encryption algorithms:** AES, 256 bits. AES128-GCM, auto. AES192-GCM, auto. AES256-GCM, auto. Blowfish, auto. 3DES. CAST128. DES. Hint: use 3DES for best compatibility or if you have a hardware crypto accelerator card. Blowfish is usually the fastest in software encryption.
- Hash algorithms:** MD5. SHA1. SHA256. SHA384. SHA512. AES-XCBC.
- PFS key group:** 2 (1024 bit).
- Lifetime:** 1800 seconds.

The 'Advanced Options' section includes:

- Automatically ping host:** [Empty field] IP address.

A 'Save' button is located at the bottom of the page.

3. Create IPsec firewall rules, if not create auto..



The screenshot shows the pfSense web interface for editing a firewall rule. The breadcrumb navigation at the top reads: System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Gold > Help. The page title is "Firewall: Rules: Edit". A dropdown menu is open over the "Rules" link, showing options: Aliases, NAT, pfBlockerNG, Rules (highlighted), Schedules, Traffic Shaper, and Virtual IPs. The main form contains the following fields:

- Action:** A text area with a placeholder: "packets that match the criteria specified below. When 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."
- Disabled:** **Disable this rule**
Set this option to disable this rule without removing it from the list.
- Interface:**
Choose which interface packets must be sourced on to match this rule.
- TCP/IP Version:** **Select the Internet Protocol version this rule applies to**
- Protocol:**
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify *TCP* here.
- Source:** **not**
Use this option to invert the sense of the match.
Type:
Address: /
- Destination:** **not**
Use this option to invert the sense of the match.
Type:
Address: /
- Log:** **Log packets that are handled by this rule**
Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
- Description:**
You may enter a description here for your reference.

At the bottom of the form are "Save" and "Cancel" buttons.