Einstein Technologies

Firewall

Thrive

One Security for the Entire Network

Just one firewall device solution to secure network infrastructure from burglary, data theft and network damage due to hacking.

Prepared by:

Thrive

More Data More Sales

thrive.co.id

About ET Firewall

Thrive

Secure Network with Reliable Firewall

ET Firewall is a hardware firewall that can protect IT network infrastructure, provides a reliable security system, and can be adjusted according to specific network security needs.

Why Choose ET Firewall?

Thrive

Ensuring the security of cyber infrastructure does not need to be a complex task. You just need the right tools.

The four advantages of ET Firewall make it the best choice for protecting your network infrastructure.

1. Easy to use
2. Complete security features
3. Tough and reliable
4. The best solution to secure the network

Target ET Firewall?

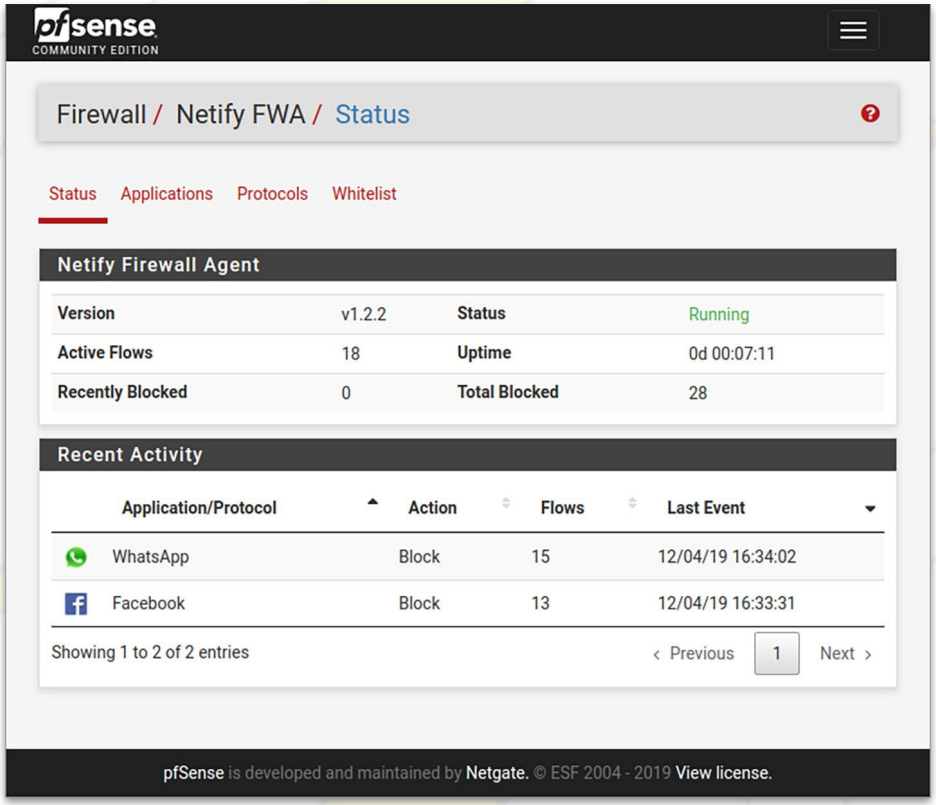
Thrive

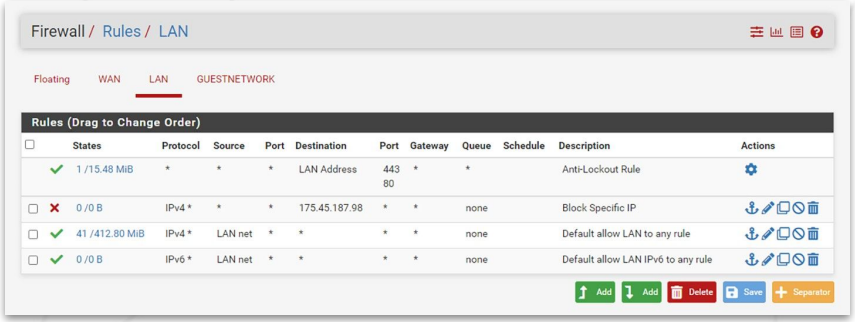
1. Ordinary users or home users who have several devices (computers, gaming consoles, CCTV cameras, alarms, etc.) connected to the internet.
2. Business owners, government organizations, and educational institutions that have large IT infrastructures and manage servers from specific locations.
3. IT service providers who serve customers and find solutions to maintain network security, public and private clouds.

Stateful Packet Inspection (PSI)

Complete Rules Configuration

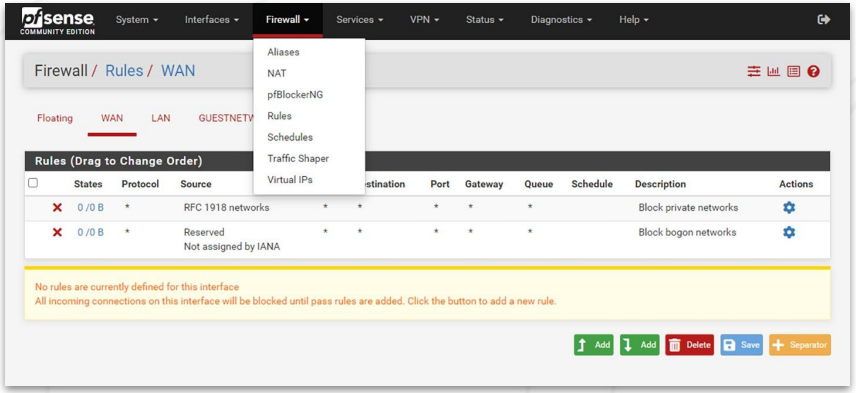
ET Firewall is very easy to configure, and you can start making settings to manage traffic on the network





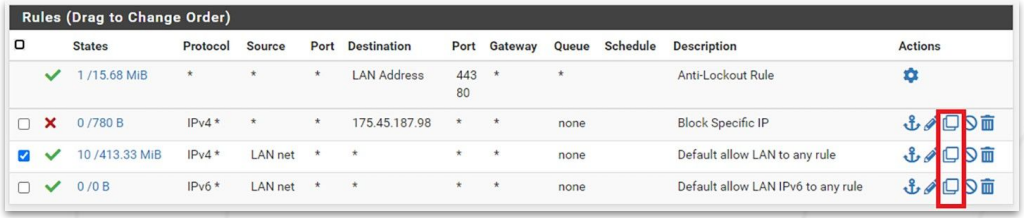
Open or Block Access from Certain Sources

Network administrators can open (pass), block (block), or reject (reject) traffic in the network, using the menu available in the ET Firewall software included in the sales package.



Easily Add and Change Firewall Rules

Administrators can add, modify, and edit rules using the easy-to-understand ET Firewall software interface.



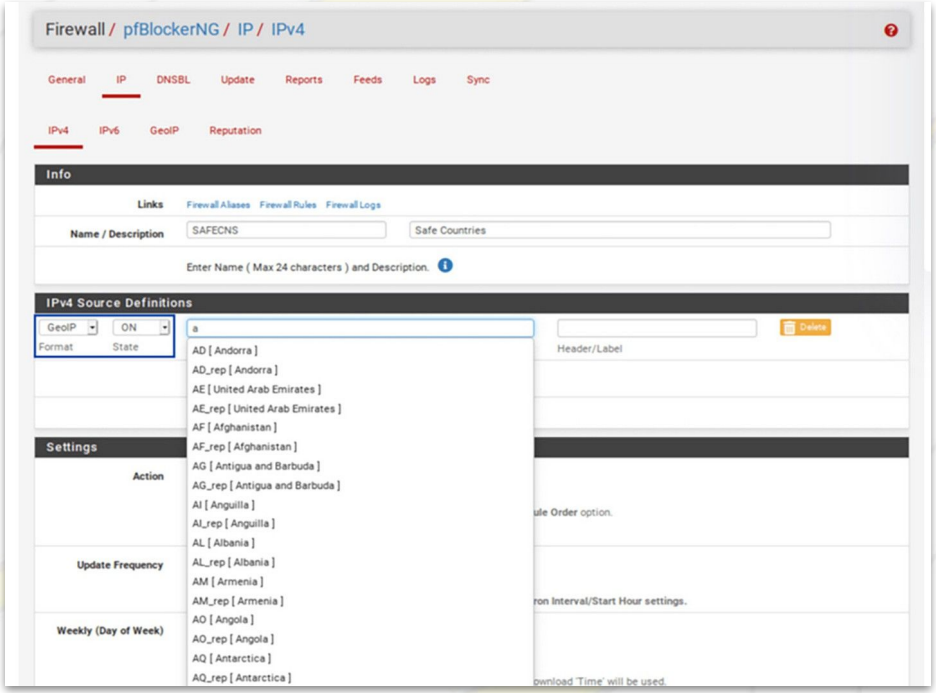
Duplicate Rules Through One Click

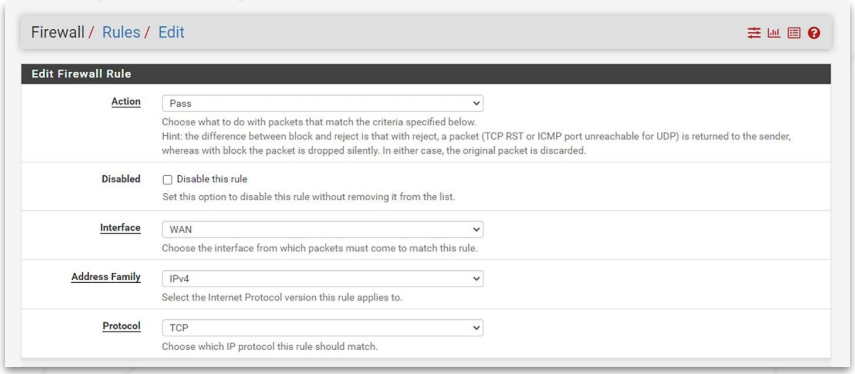
You can use the same rules for different kinds of traffic settings.

GeoIP Blocking

Block Traffic Based on Location and IP

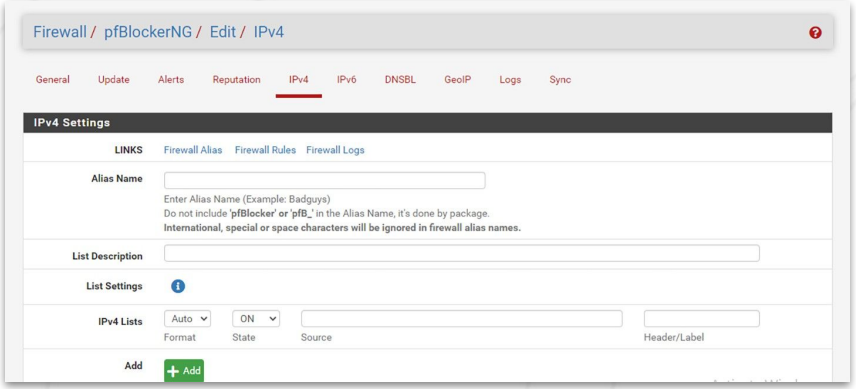
When enabled, administrators can prevent suspicious traffic from entering the network, using a set of blocking settings based on location and IP address.





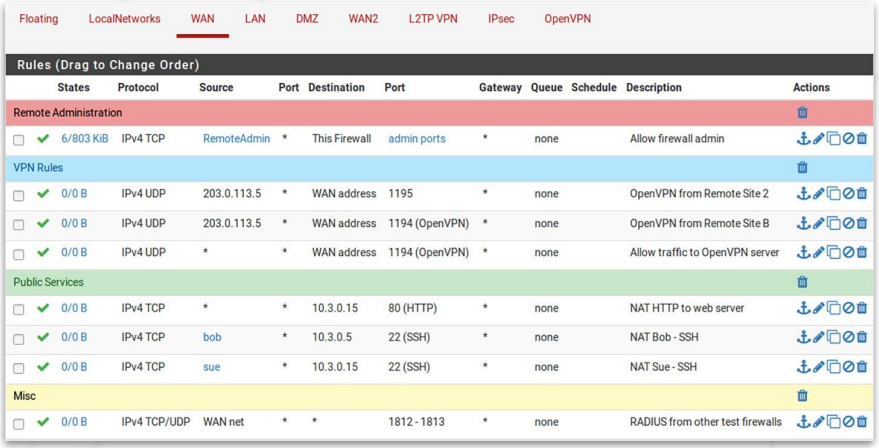
Add IP Address to One Blocking List

Assigns multiple URL lists of IP addresses in the blocking list to one alias and then selects a rule action.



One Package, Same Function

Replacement of Countryblock and IPblocklist by providing the same functionality in one package.



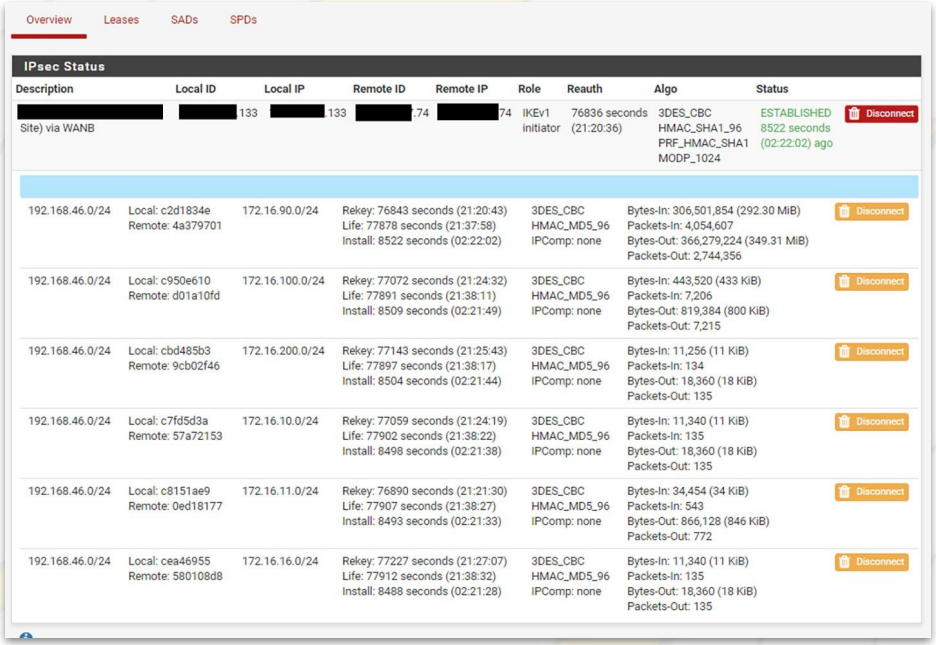
Just One Software

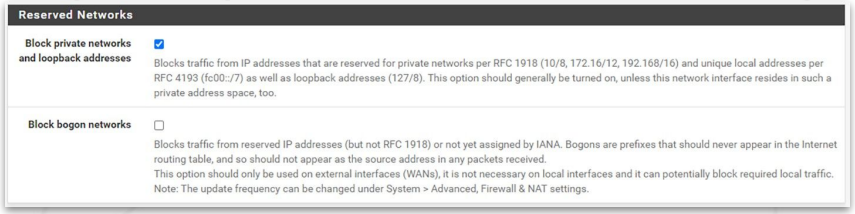
Administrators can manage blocking using one of the blocking functions available in the ET Firewall software.

Anti Spoofing

Avoid Fake Traffic

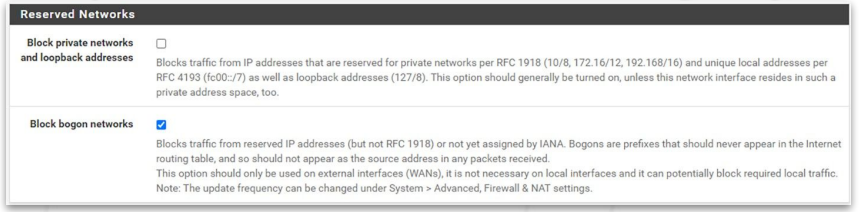
Suspicious traffic sent to your network can be prevented using an anti-spoofing feature that is easy for administrators to configure.





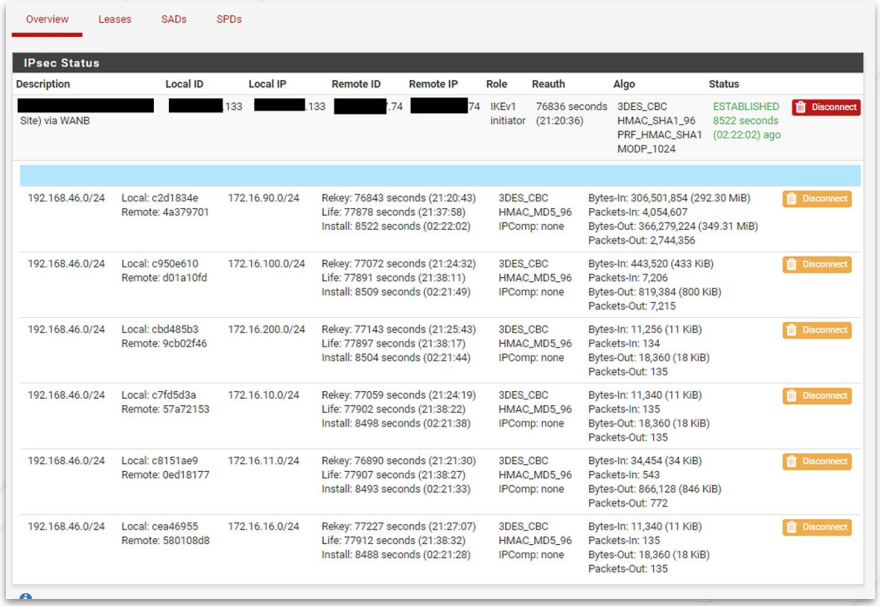
Prevent Private Networks

The firewall checks every traffic. If a spoofing attempt enters the network and originates from an IP address that is detected to be spoofed, traffic from that source will be prevented from entering.



Bogon Networks Block

Prevent traffic from bogon networks. ET Firewall can be set to show fake traffic or unused subnets that have been hijacked for malicious purposes.



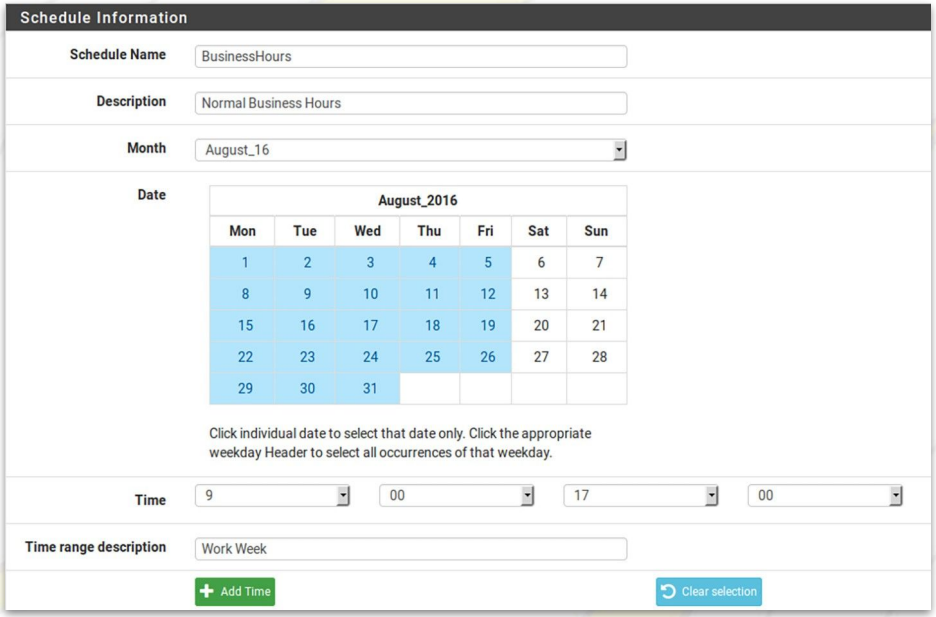
Easy IPsec Setup

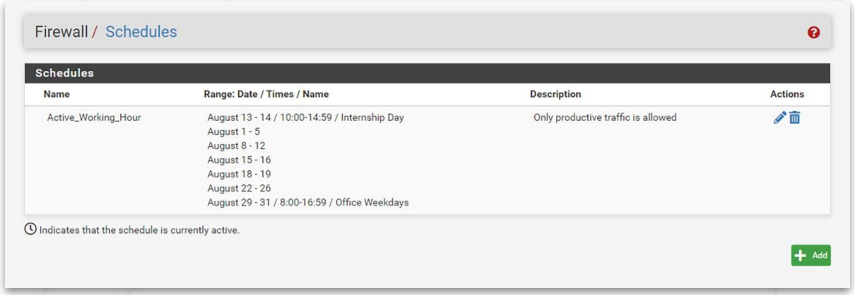
When an IPsec connection is enabled, the firewall automatically adds certain rules to make the connection work properly.

Time-Based Rules

Time Based Firewall Settings

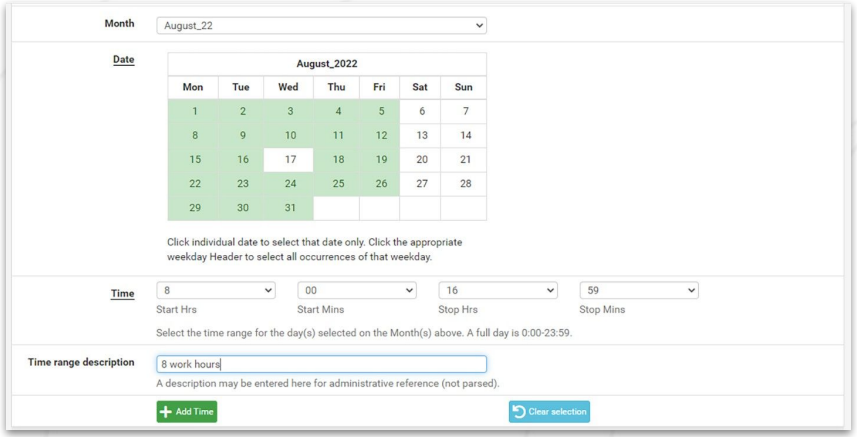
Time-based rules allow the ET Firewall to be activated during certain days and/or timescales.





Set Firewall Uptime

The schedule must be defined before it can be used on firewall rules. Schedules are defined in a special menu, and each schedule can contain multiple timeframes.



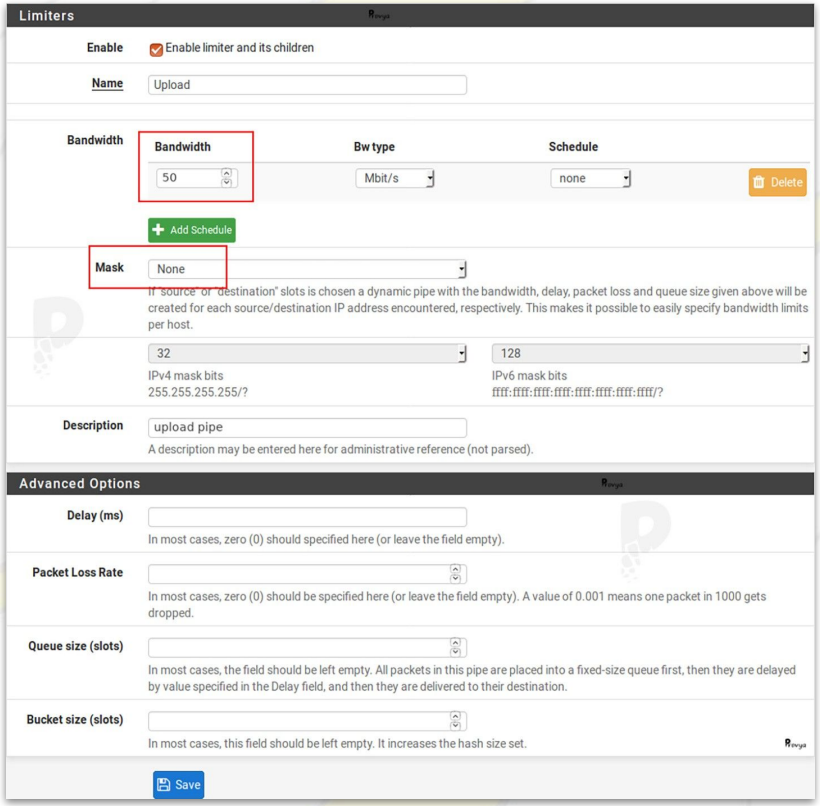
Use Schedule in Firewall Rules

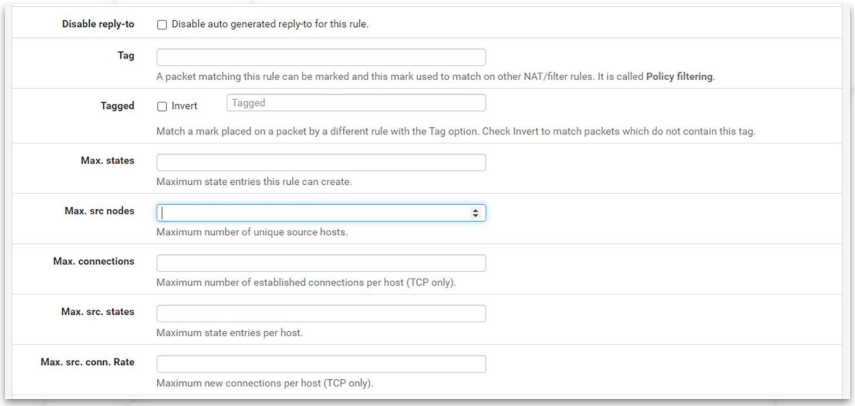
To create firewall rules using a specific schedule, create a new rule on the desired interface.

Connection Limits

Limit Connections Easily

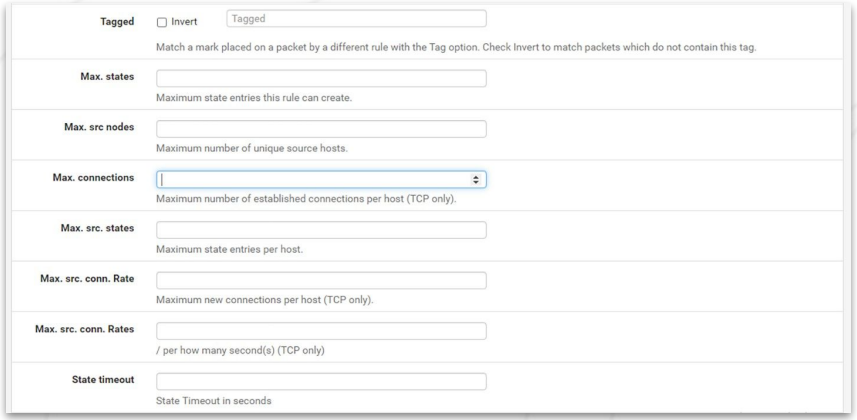
If needed, you can restrict your network connection based on certain rules.





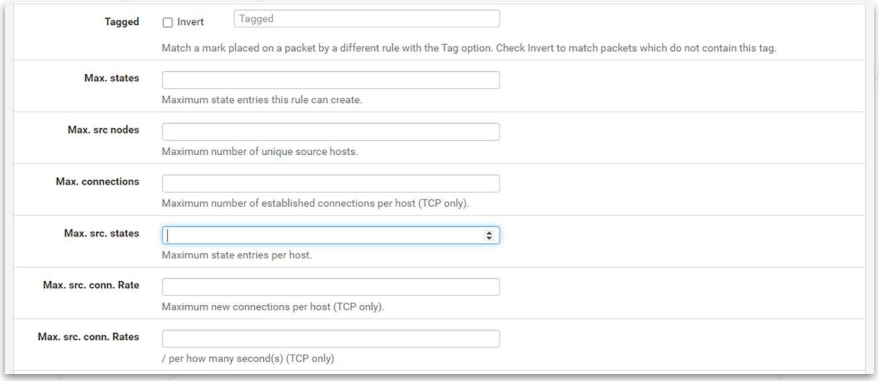
Specify Maximum Number of Source Hosts

This option determines how many total source IP addresses can be connected simultaneously for this rule.



Set Maximum Number of Connections Per Host

To restrict access on a per-host connection, use this setting. This value can limit the rule to a specific number of connections per source host, not the total connection as a whole.



Maximum Status Entry Per Host

This setting works similarly to setting the maximum number of connections per host, but checks only status entries rather than tracking if a connection was established successfully.

Thrive

One Firewall for Your Business

Secure your network with reliable ET Firewall software and tools

Thrive

Get Free Consultation

Discuss your IT requirements with our customer support at

+62 822 9998 8870

Thank You

Prepared by:

Thrive

More Data More Sales