



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](http://thrive.co.id)

# About ET Firewall



## 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?

**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?

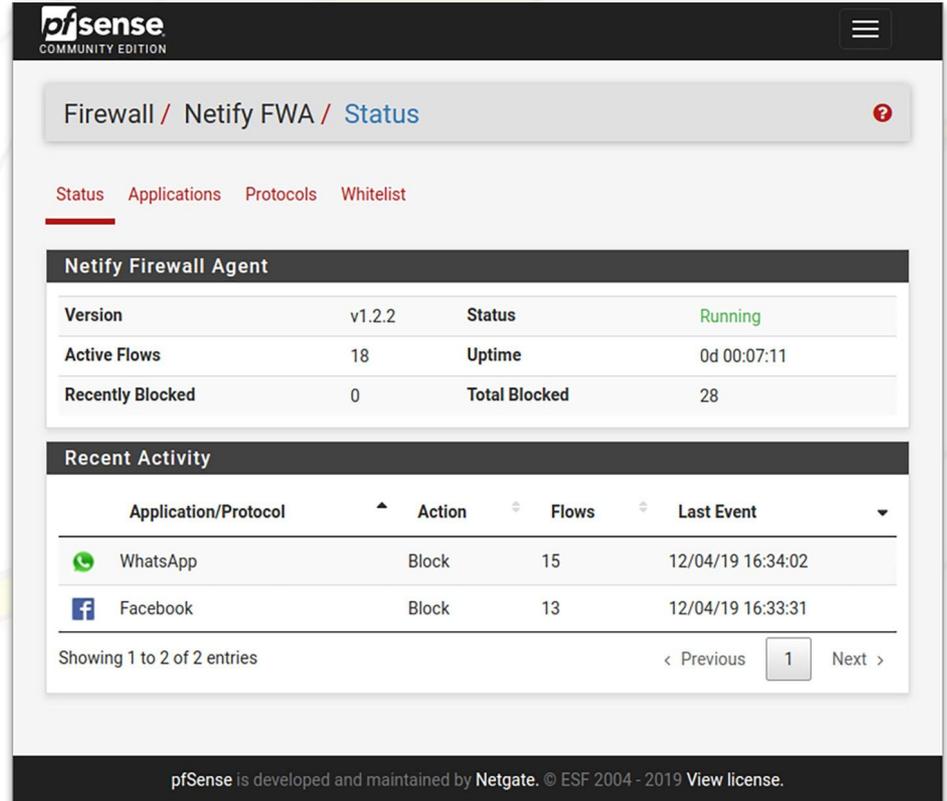


1. Ordinary users or home users who have several devices (computers, gaming consoles, CCTV cameras, alarms, etc.) connected to the internet.
2. Business owners, government organizations, and educational institutions that have large IT infrastructures and manage servers from specific locations.
3. IT 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



The screenshot shows the pfSense Community Edition interface for the Netify Firewall Agent status. The breadcrumb trail is Firewall / Netify FWA / Status. There are tabs for Status, Applications, Protocols, and Whitelist. The Status tab is active.

**Netify Firewall Agent**

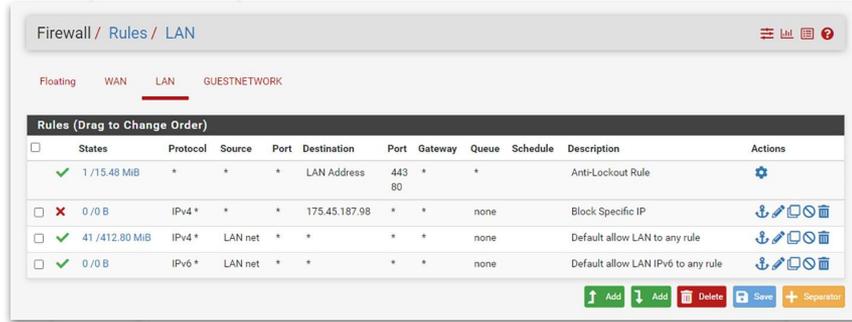
Version	v1.2.2	Status	Running
Active Flows	18	Uptime	0d 00:07:11
Recently Blocked	0	Total Blocked	28

**Recent Activity**

Application/Protocol	Action	Flows	Last Event
 WhatsApp	Block	15	12/04/19 16:34:02
 Facebook	Block	13	12/04/19 16:33:31

Showing 1 to 2 of 2 entries < Previous 1 Next >

pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.



Firewall / Rules / LAN

Floating WAN LAN GUESTNETWORK

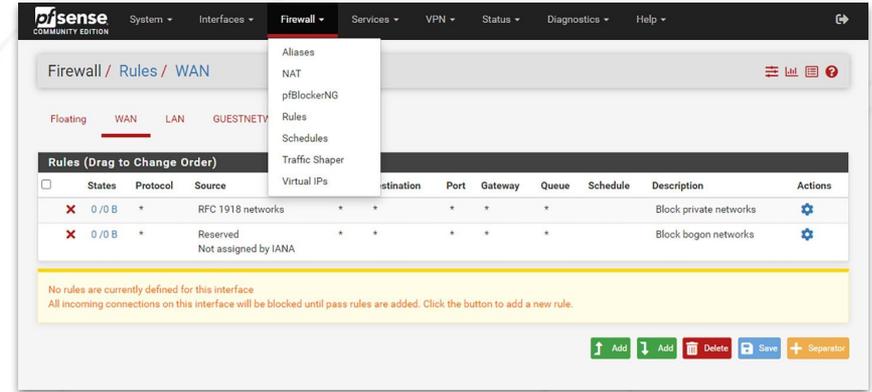
Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	1 / 15.48 MIB	*	*	LAN Address	443	80	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4*	*	175.45.187.98	*	*	none		Block Specific IP	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 41 / 412.80 MIB	IPv4*	LAN net	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv6*	LAN net	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

## 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.



Firewall / Rules / WAN

Floating WAN LAN GUESTNETWORK

Rules (Drag to Change Order)

States	Protocol	Source	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 0 B	*	RFC 1918 networks	*	*	*	*	Block private networks	
<input checked="" type="checkbox"/>	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	Block bogon networks	

No rules are currently defined for this interface  
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Add Add Delete Save Separator

## Easily Add and Change Firewall Rules

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

Rules (Drag to Change Order)												
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	1 /15.68 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule		
<input type="checkbox"/>	 0 /780 B	IPv4 *	*	*	175.45.187.98	*	*	none		Block Specific IP	  	
<input checked="" type="checkbox"/>	 10 /413.33 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	  	
<input type="checkbox"/>	 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	  	

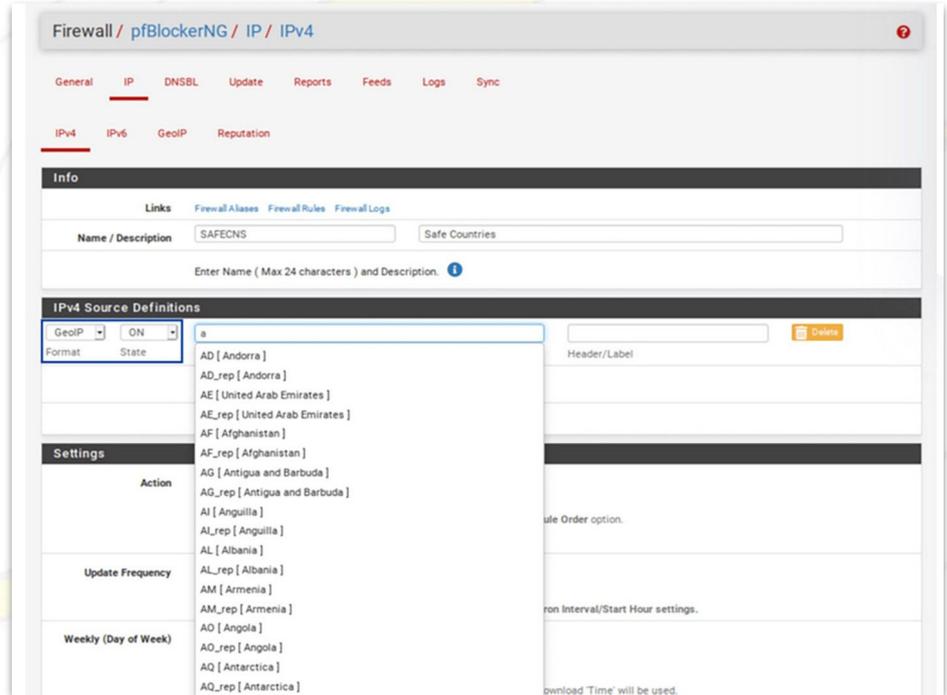
## Duplicate Rules Through One Click

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

# GeoIP Blocking

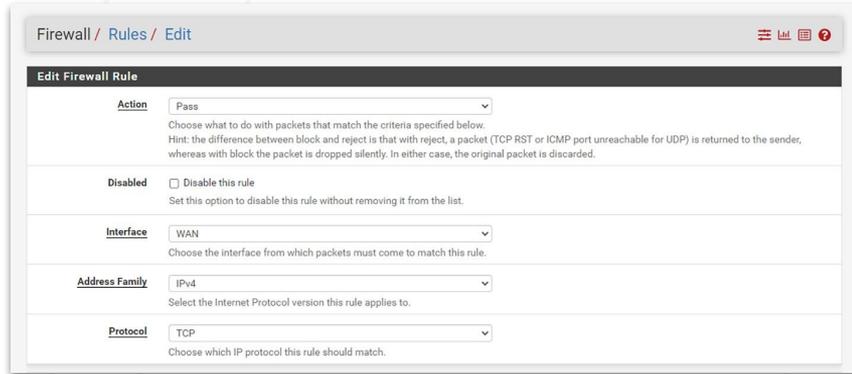
## Block Traffic Based on Location and IP

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



The screenshot shows the configuration page for IPv4 GeoIP blocking in pfBlockerNG. The breadcrumb trail is Firewall / pfBlockerNG / IP / IPv4. The 'GeoIP' tab is selected under the 'IP' section. The 'Info' section shows the rule name 'SAFECNS' and a description 'Safe Countries'. Below this, the 'IPv4 Source Definitions' section is active, displaying a list of countries and their corresponding rule names. The 'GeoIP' dropdown is set to 'ON' and the 'Format' is set to 'State'. The list of definitions includes:

Country	Rule Name
AD [Andorra]	AD_rep [Andorra]
AE [United Arab Emirates]	AE_rep [United Arab Emirates]
AF [Afghanistan]	AF_rep [Afghanistan]
AG [Antigua and Barbuda]	AG_rep [Antigua and Barbuda]
AI [Anguilla]	AI_rep [Anguilla]
AL [Albania]	AL_rep [Albania]
AM [Armenia]	AM_rep [Armenia]
AO [Angola]	AO_rep [Angola]
AQ [Antarctica]	AQ_rep [Antarctica]



Firewall / Rules / Edit

### Edit Firewall Rule

**Action**   
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.

**Disabled**  Disable this rule  
Set this option to disable this rule without removing it from the list.

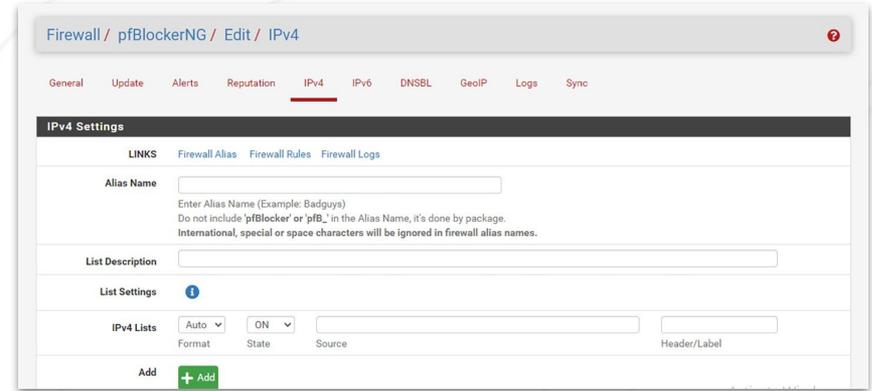
**Interface**   
Choose the interface from which packets must come to match this rule.

**Address Family**   
Select the Internet Protocol version this rule applies to.

**Protocol**   
Choose which IP protocol this rule should match.

## 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.



Firewall / pfBlockerNG / Edit / IPv4

General Update Alerts Reputation IPv4 IPv6 DNSBL GeoIP Logs Sync

### IPv4 Settings

**LINKS** [Firewall Alias](#) [Firewall Rules](#) [Firewall Logs](#)

**Alias Name**   
Enter Alias Name (Example: Badguys)  
Do not include 'pfBlocker' or 'pfb.' in the Alias Name, it's done by package.  
International, special or space characters will be ignored in firewall alias names.

**List Description**

**List Settings** ⓘ

IPv4 Lists     
Format State Source Header/Label

Add

## One Package, Same Function

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

Rules (Drag to Change Order)											
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
Remote Administration											
<input type="checkbox"/>	✓	6/803 KiB	IPv4 TCP	RemoteAdmin	*	This Firewall	admin ports	*	none	Allow firewall admin	
VPN Rules											
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	203.0.113.5	*	WAN address	1195	*	none	OpenVPN from Remote Site 2	
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	203.0.113.5	*	WAN address	1194 (OpenVPN)	*	none	OpenVPN from Remote Site B	
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none	Allow traffic to OpenVPN server	
Public Services											
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	10.3.0.15	80 (HTTP)	*	none	NAT HTTP to web server	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	bob	*	10.3.0.5	22 (SSH)	*	none	NAT Bob - SSH	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	sue	*	10.3.0.15	22 (SSH)	*	none	NAT Sue - SSH	
Misc											
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP/UDP	WAN net	*	*	1812 - 1813	*	none	RADIUS from other test firewalls	

## 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.

IPsec Status									
Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status	
Site) via WANB	133	133	74	74	IKEv1 initiator	76836 seconds (21:20:36)	3DES_CBC HMAC_SHA1_96 PRF_HMAC_SHA1 MODP_1024	ESTABLISHED 8522 seconds (02:22:02) ago	<a href="#">Disconnect</a>
192.168.46.0/24	Local: c2d1834e Remote: 4a379701	172.16.90.0/24	Rekey: 76843 seconds (21:20:43) Life: 77878 seconds (21:37:58) Install: 8522 seconds (02:22:02)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 306,501,854 (292.30 MiB) Packets-In: 4,054,607 Bytes-Out: 366,279,224 (349.31 MiB) Packets-Out: 2,744,356	<a href="#">Disconnect</a>			
192.168.46.0/24	Local: c950e610 Remote: d01a10fd	172.16.100.0/24	Rekey: 77072 seconds (21:24:32) Life: 77891 seconds (21:38:11) Install: 8509 seconds (02:21:49)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 443,520 (433 KiB) Packets-In: 7,206 Bytes-Out: 819,384 (800 KiB) Packets-Out: 7,215	<a href="#">Disconnect</a>			
192.168.46.0/24	Local: cbd485b3 Remote: 9cb02f46	172.16.200.0/24	Rekey: 77143 seconds (21:25:43) Life: 77897 seconds (21:38:17) Install: 8504 seconds (02:21:44)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 11,256 (11 KiB) Packets-In: 134 Bytes-Out: 18,360 (18 KiB) Packets-Out: 135	<a href="#">Disconnect</a>			
192.168.46.0/24	Local: c7fd5d3a Remote: 57a72153	172.16.10.0/24	Rekey: 77059 seconds (21:24:19) Life: 77902 seconds (21:38:22) Install: 8498 seconds (02:21:38)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 11,340 (11 KiB) Packets-In: 135 Bytes-Out: 18,360 (18 KiB) Packets-Out: 135	<a href="#">Disconnect</a>			
192.168.46.0/24	Local: c8151ae9 Remote: 0ed18177	172.16.11.0/24	Rekey: 76890 seconds (21:21:30) Life: 77907 seconds (21:38:27) Install: 8493 seconds (02:21:33)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 34,454 (34 KiB) Packets-In: 543 Bytes-Out: 866,128 (846 KiB) Packets-Out: 772	<a href="#">Disconnect</a>			
192.168.46.0/24	Local: cea46955 Remote: 580108d8	172.16.16.0/24	Rekey: 77227 seconds (21:27:07) Life: 77912 seconds (21:38:32) Install: 8488 seconds (02:21:28)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 11,340 (11 KiB) Packets-In: 135 Bytes-Out: 18,360 (18 KiB) Packets-Out: 135	<a href="#">Disconnect</a>			

**Reserved Networks**

**Block private networks and loopback addresses**

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

**Block bogon networks**

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

## 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.

**Reserved Networks**

**Block private networks and loopback addresses**

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

**Block bogon networks**

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

## 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.

Overview Leases SADs SPDs

### IPsec Status

Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status	
Site) via WAN	133	133	74	74	IKv1 Initiator	76836 seconds (21:20:36)	3DES_CBC HMAC_SHA1_96 PRF_HMAC_SHA1 MODP_1024	ESTABLISHED 8522 seconds (02:22:02) ago	<a href="#">Disconnect</a>
192.168.46.0/24	Local: c2d1834e Remote: 4a379701	172.16.90.0/24	Rekey: 76843 seconds (21:20:43) Life: 77878 seconds (21:37:58) Install: 8522 seconds (02:22:02)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 306,501,854 (292.30 MiB) Packets-In: 4,054,607 Bytes-Out: 366,279,224 (349.31 MiB) Packets-Out: 2,744,356	<a href="#">Disconnect</a>			
192.168.46.0/24	Local: c950e610 Remote: d01a10fd	172.16.100.0/24	Rekey: 77072 seconds (21:24:32) Life: 77891 seconds (21:38:11) Install: 8509 seconds (02:21:49)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 443,520 (433 KiB) Packets-In: 7,206 Bytes-Out: 819,384 (800 KiB) Packets-Out: 7,215	<a href="#">Disconnect</a>			
192.168.46.0/24	Local: cbd485b3 Remote: 9cb02f46	172.16.200.0/24	Rekey: 77143 seconds (21:25:43) Life: 77897 seconds (21:38:17) Install: 8504 seconds (02:21:44)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 11,256 (11 KiB) Packets-In: 134 Bytes-Out: 18,360 (18 KiB) Packets-Out: 135	<a href="#">Disconnect</a>			
192.168.46.0/24	Local: c7fd5d3a Remote: 57a72153	172.16.10.0/24	Rekey: 77059 seconds (21:24:19) Life: 77902 seconds (21:38:22) Install: 8498 seconds (02:21:38)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 11,340 (11 KiB) Packets-In: 135 Bytes-Out: 18,360 (18 KiB) Packets-Out: 135	<a href="#">Disconnect</a>			
192.168.46.0/24	Local: c8151ae9 Remote: 0ed18177	172.16.11.0/24	Rekey: 76890 seconds (21:21:30) Life: 77907 seconds (21:38:27) Install: 8493 seconds (02:21:33)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 34,454 (34 KiB) Packets-In: 543 Bytes-Out: 866,128 (846 KiB) Packets-Out: 772	<a href="#">Disconnect</a>			
192.168.46.0/24	Local: cea46955 Remote: 580108d8	172.16.16.0/24	Rekey: 77227 seconds (21:27:07) Life: 77912 seconds (21:38:32) Install: 8488 seconds (02:21:28)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 11,340 (11 KiB) Packets-In: 135 Bytes-Out: 18,360 (18 KiB) Packets-Out: 135	<a href="#">Disconnect</a>			

## 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.

### Schedule Information

**Schedule Name**

**Description**

**Month**

**Date**

August_2016						
Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

**Time**

**Time range description**

Firewall / Schedules

Name	Range: Date / Times / Name	Description	Actions
Active_Working_Hour	August 13 -14 / 10:00-14:59 / Internship Day August 1 - 5 August 8 - 12 August 15 - 16 August 18 - 19 August 22 - 26 August 29 - 31 / 8:00-16:59 / Office Weekdays	Only productive traffic is allowed	 

 Indicates that the schedule is currently active.

[+ Add](#)

## 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.

Month: August\_22

Date: August\_2022

Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

Time: Start Hrs: 8, Start Mins: 00, Stop Hrs: 16, Stop Mins: 59

Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.

Time range description: 8 work hours

A description may be entered here for administrative reference (not parsed).

[+ Add Time](#) [Clear selection](#)

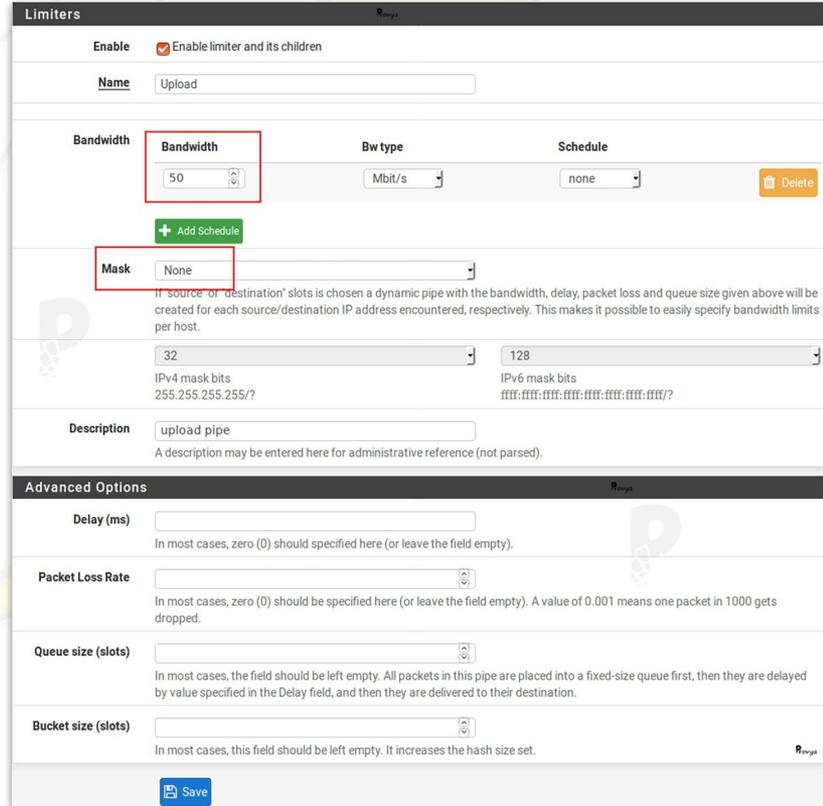
## Use Schedule in Firewall Rules

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.



The screenshot displays the 'Limiters' configuration page for a rule named 'Upload'. The interface includes the following sections and fields:

- Enable:** A checked checkbox labeled 'Enable limiter and its children'.
- Name:** A text input field containing 'Upload'.
- Bandwidth:** A section with three sub-fields: 'Bandwidth' (input: 50), 'Bw type' (dropdown: Mbit/s), and 'Schedule' (dropdown: none). A 'Delete' button is located to the right.
- Mask:** A dropdown menu set to 'None'.
- IP Masking:** Two dropdown menus for 'IPv4 mask bits' (set to 32) and 'IPv6 mask bits' (set to 128). Below them are the corresponding mask patterns: '255.255.255.255/?' and 'ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/?'.
- Description:** A text input field containing 'upload pipe' and a note: 'A description may be entered here for administrative reference (not parsed)'.
- Advanced Options:** A section with four fields: 'Delay (ms)', 'Packet Loss Rate', 'Queue size (slots)', and 'Bucket size (slots)'. Each field has a text input and a descriptive note below it.
- Save:** A blue button at the bottom left.

Disable reply-to	<input type="checkbox"/> Disable auto generated reply-to for this rule.
Tag	<input type="text"/>
	A packet matching this rule can be marked and this mark used to match on other NAT/filter rules. It is called Policy filtering.
Tagged	<input type="checkbox"/> Invert <input type="text" value="Tagged"/>
	Match a mark placed on a packet by a different rule with the Tag option. Check Invert to match packets which do not contain this tag.
Max. states	<input type="text"/>
	Maximum state entries this rule can create.
Max. src nodes	<input type="text" value="1"/>
	Maximum number of unique source hosts.
Max. connections	<input type="text"/>
	Maximum number of established connections per host (TCP only).
Max. src. states	<input type="text"/>
	Maximum state entries per host.
Max. src. conn. Rate	<input type="text"/>
	Maximum new connections per host (TCP only).

## Specify Maximum Number of Source Hosts

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

Tagged	<input type="checkbox"/> Invert <input type="text" value="Tagged"/>
	Match a mark placed on a packet by a different rule with the Tag option. Check Invert to match packets which do not contain this tag.
Max. states	<input type="text"/>
	Maximum state entries this rule can create.
Max. src nodes	<input type="text"/>
	Maximum number of unique source hosts.
Max. connections	<input type="text" value="1"/>
	Maximum number of established connections per host (TCP only).
Max. src. states	<input type="text"/>
	Maximum state entries per host.
Max. src. conn. Rate	<input type="text"/>
	Maximum new connections per host (TCP only).
Max. src. conn. Rates	<input type="text"/>
	/ per how many second(s) (TCP only)
State timeout	<input type="text"/>
	State Timeout in seconds

## 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.

Tagged	<input type="checkbox"/> Invert	<input type="text" value="Tagged"/>
Match a mark placed on a packet by a different rule with the Tag option. Check Invert to match packets which do not contain this tag.		
Max. states	<input type="text"/>	Maximum state entries this rule can create.
Max. src nodes	<input type="text"/>	Maximum number of unique source hosts.
Max. connections	<input type="text"/>	Maximum number of established connections per host (TCP only).
Max. src. states	<input type="text" value="1"/>	Maximum state entries per host.
Max. src. conn. Rate	<input type="text"/>	Maximum new connections per host (TCP only).
Max. src. conn. Rates	<input type="text"/>	/ per how many second(s) (TCP only)

## 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.

# One Firewall for Your Business

Secure your network with reliable ET Firewall software and tools



## **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

