Thrive

Einstein Technologies

Firewall

Satu Pengaman untuk Seluruh Jaringan

Cukup satu solusi perangkat firewall untuk mengamankan infrastruktur jaringan dari pembobolan, pencurian data dan kerusakan jaringan akibat peretasan.

Prepared by:

Thrive

More Data More Sales

thrive.co.id

Tentang ET Firewall

Amankan Jaringan dengan Firewall Handal

ET Firewall merupakan perangkat keras firewall yang sanggup melindungi infrastruktur jaringan IT, menyediakan sistem keamanan yang handal, dan bisa diatur sesuai kebutuhan pengamanan jaringan yang spesifik

Kenapa Pilih ET Firewall?

Memastikan keamanan infrastruktur *cyber* tidak perlu jadi tugas yang rumit. Anda hanya membutuhkan perangkat yang tepat.

Empat keunggulan ET Firewall menjadikan perangkat ini jadi pilihan terbaik untuk melindungi infrastruktur jaringan Anda.

1. Mudah digunakan
2. Fitur keamanan lengkap
3. Tangguh dan bisa diandalkan
4. Solusi terbaik untuk mengamankan jaringan

Untuk Siapa ET Firewall?

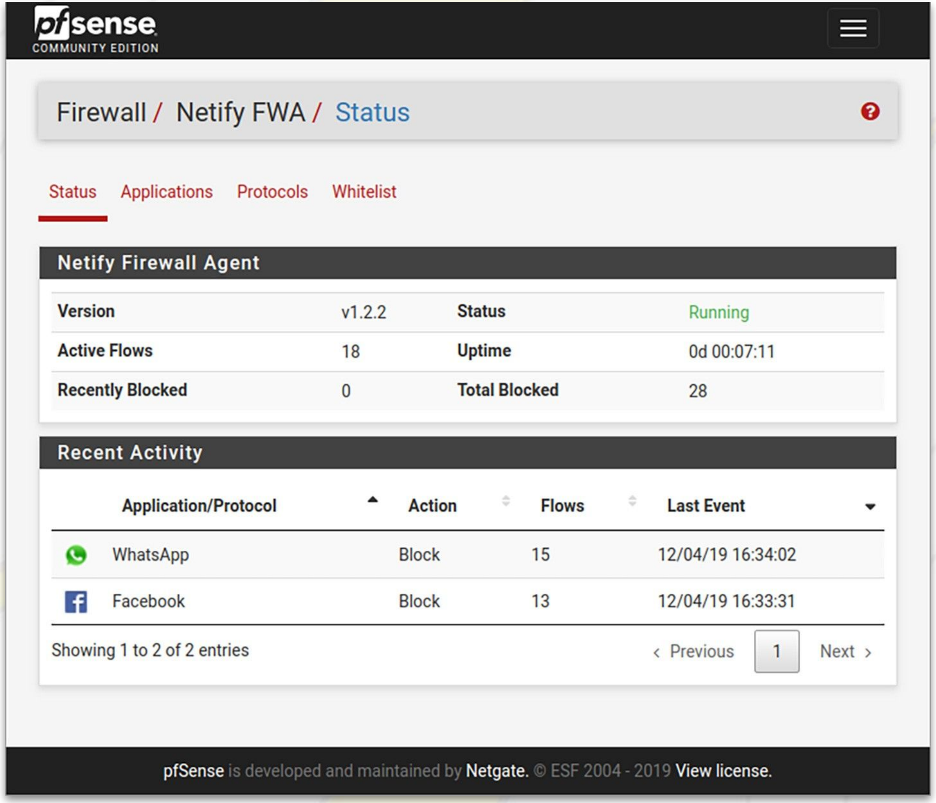
Thrive

1. User biasa atau pengguna rumahan yang memiliki beberapa perangkat (komputer, konsol gaming, kamera CCTV, alarm, dan lain sebagainya) yang terkoneksi dengan internet.
2. Pemilik bisnis, organisasi pemerintah, dan institusi pendidikan yang memiliki infrastruktur IT yang besar dan mengelola server dari lokasi spesifik.
3. Penyedia layanan IT yang melayani pelanggan dan mencari solusi untuk menjaga keamanan jaringan, *public cloud* maupun *private cloud*.

Stateful Packet Inspection (PSI)

Konfigurasi Rules Lengkap

ET Firewall sangat mudah dikonfigurasi, dan Anda bisa mulai melakukan pengaturan untuk mengatur traffic di dalam jaringan.



Firewall / Netify FWA / Status

Netify Firewall Agent

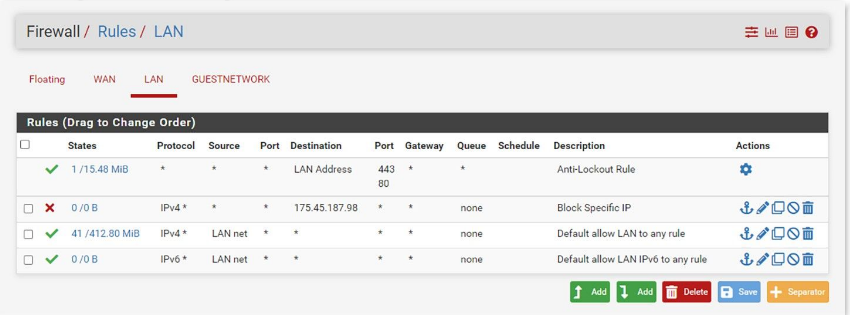
Version	v1.2.2	Status	Running
Active Flows	18	Uptime	0d 00:07:11
Recently Blocked	0	Total Blocked	28

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

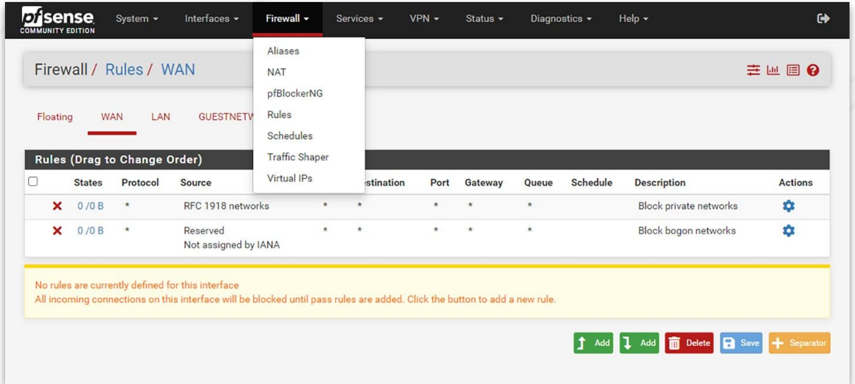
Showing 1 to 2 of 2 entries

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



Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1 /15.48 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
☐	✗	0 /0 B	IPv4 *	*	*	175.45.187.98	*	*	none		Block Specific IP	⚓✎❐⊘🗑
☐	✓	41 /412.80 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	⚓✎❐⊘🗑
☐	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓✎❐⊘🗑



Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	stination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0 /0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
	✗	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

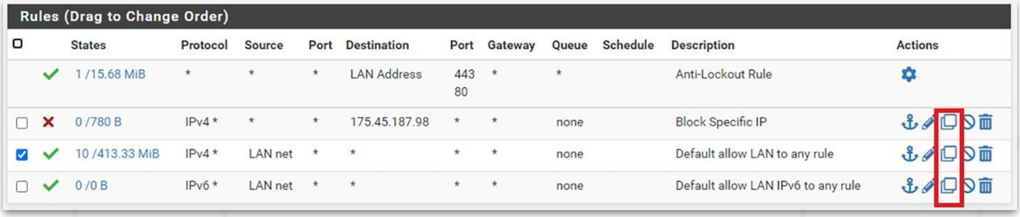
No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Buka atau Blok Akses dari Sumber Tertentu

Administrator jaringan bisa membuka (*pass*), mengeblok (*block*), atau menolak (*reject*) *traffic* dalam jaringan, memanfaatkan menu yang tersedia di dalam *software* ET Firewall yang disertakan dalam paket penjualan.

Tambahkan dan Ubah Firewall Rules dengan Mudah

Administrator bisa menambah, mengubah, dan menyunting *rules* memanfaatkan lewat *interface* software ET Firewall yang mudah dipahami.



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1 /15.68 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
□	✗	0 /780 B	IPv4 *	*	*	175.45.187.98	*	*	none		Block Specific IP	
☑	✓	10 /413.33 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

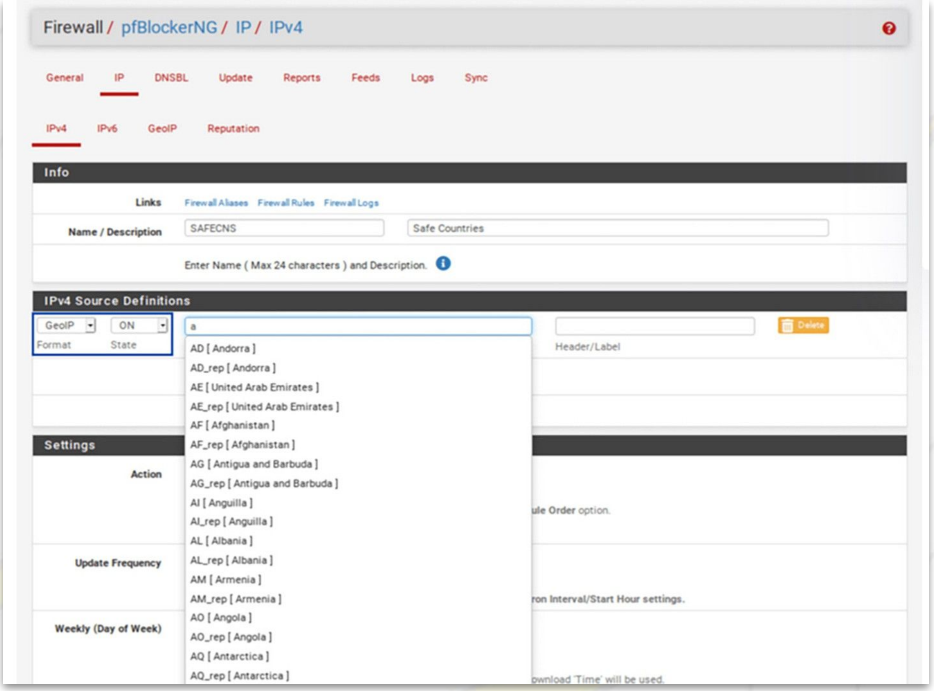
Gandakan Rules Lewat Satu Klik

Anda bisa memakai rules yang sama untuk beberapa macam pengaturan *traffic* yang berbeda.

GeoIP Blocking

Blok Traffic Berdasarkan Lokasi dan IP

Ketika diaktifkan, administrator bisa mencegah traffic mencurigakan masuk ke dalam jaringan, menggunakan seperangkat pengaturan blocking berdasarkan lokasi maupun IP Address.



Firewall / pfBlockerNG / IP / IPv4

Info

Links: Firewall Aliases Firewall Rules Firewall Logs

Name / Description: SAFECNS | Safe Countries

Enter Name (Max 24 characters) and Description.

IPv4 Source Definitions

Format: GeoIP
State: ON
a
Header/Label

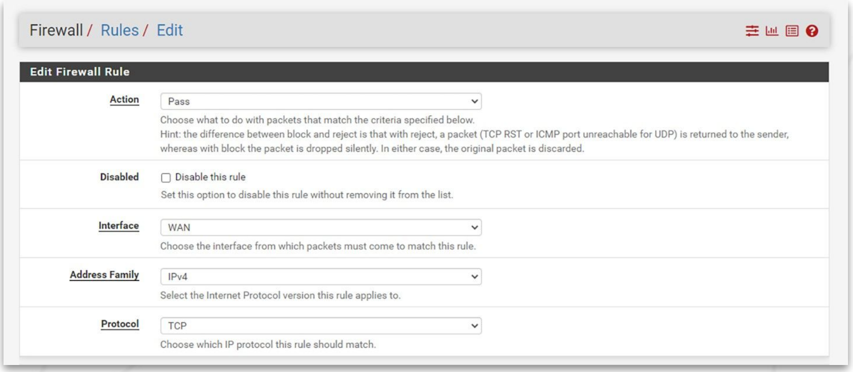
AD [Andorra]
AD_rep [Andorra]
AE [United Arab Emirates]
AE_rep [United Arab Emirates]
AF [Afghanistan]
AF_rep [Afghanistan]
AG [Antigua and Barbuda]
AG_rep [Antigua and Barbuda]
AI [Anguilla]
AI_rep [Anguilla]
AL [Albania]
AL_rep [Albania]
AM [Armenia]
AM_rep [Armenia]
AO [Angola]
AO_rep [Angola]
AQ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

Settings

Action
ule Order option.

Update Frequency
ron Interval/Start Hour settings.

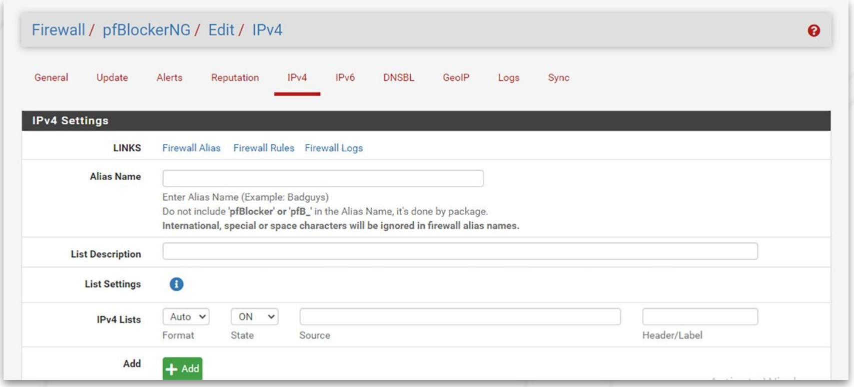
Weekly (Day of Week)
ownload 'Time' will be used.



Firewall / Rules / Edit

Edit Firewall Rule

Action	Pass 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	WAN Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	TCP Choose which IP protocol this rule should match.



Firewall / pfBlockerNG / Edit / IPv4

IPv4 Settings

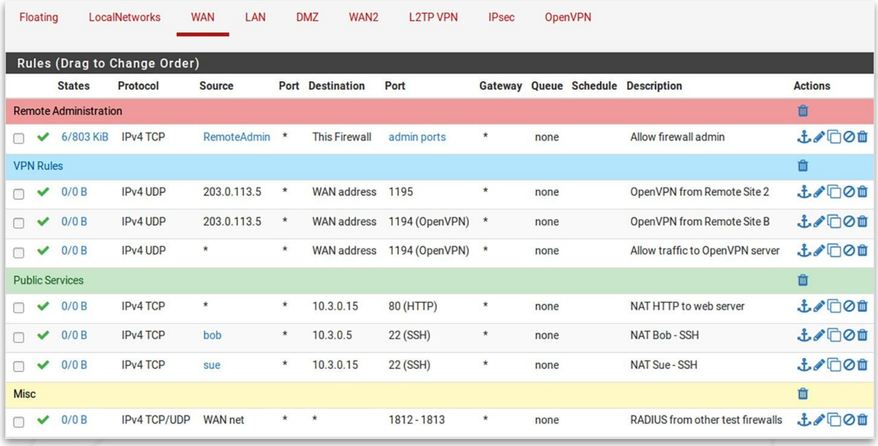
LINKS	Firewall Alias Firewall Rules Firewall Logs
Alias Name	Enter Alias Name (Example: Badguys) Do not include 'pfBlocker' or 'pfB_' in the Alias Name, it's done by package. International, special or space characters will be ignored in firewall alias names.
List Description	
List Settings	
IPv4 Lists	Auto (Format) ON (State) Source Header/Label
Add	+ Add

Tambahkan Alamat IP ke dalam Satu Daftar Blocking

Menetapkan banyak daftar URL alamat IP dalam daftar *blocking* ke satu alias dan kemudian memilih tindakan aturan.

Satu Package, Fungsi Yang Sama

Penggantian Countryblock dan IPblocklist dengan menyediakan fungsionalitas yang sama dalam satu paket.



Floating LocalNetworks WAN LAN DMZ WAN2 L2TP VPN IPsec OpenVPN

Rules (Drag to Change Order)

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

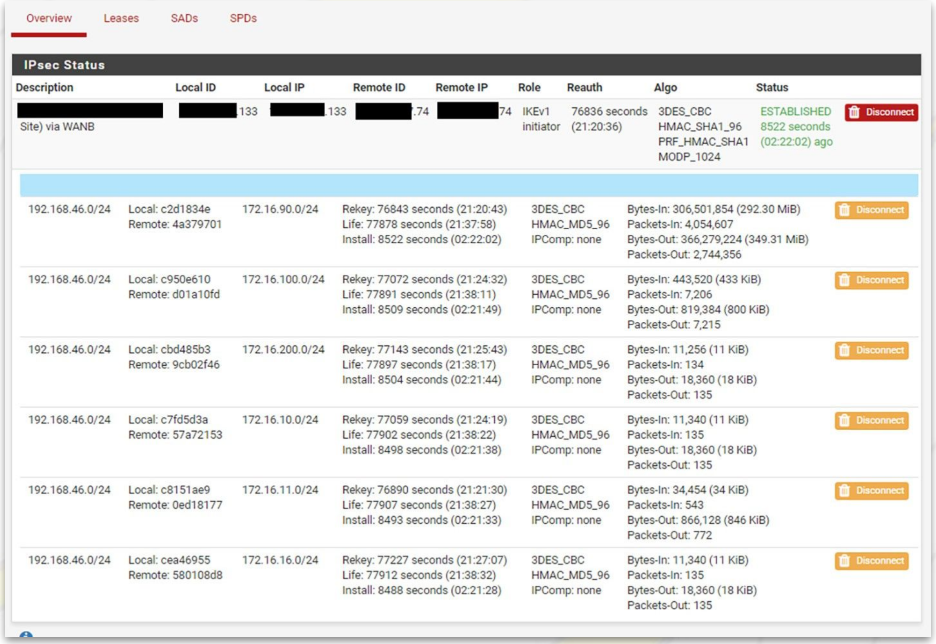
Cukup Satu Software

Administrator bisa mengatur *blocking* menggunakan satu fungsi *blocking* yang tersedia dalam *software* ET Firewall.

Anti Spoofing

Hindari Traffic Palsu

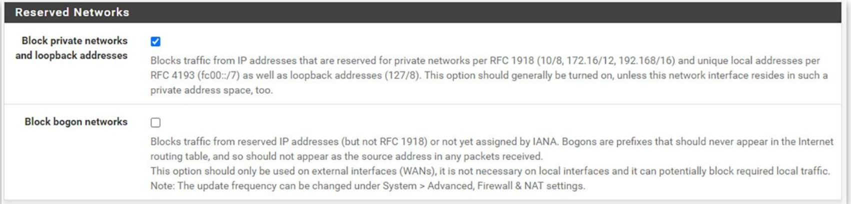
Traffic mencurigakan yang dikirimkan ke jaringan Anda bisa dicegah menggunakan fitur anti-spoofing yang mudah dikonfigurasi oleh administrator.



IPsec Status

Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status	
[redacted] Site) via WANB	[redacted].133	[redacted].133	[redacted].74	[redacted]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	Disconnect

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	Disconnect
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	Disconnect
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	Disconnect
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	Disconnect
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	Disconnect
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	Disconnect



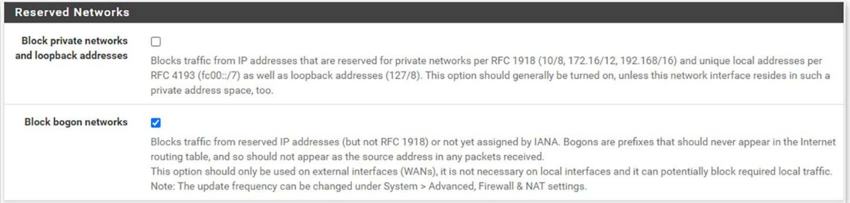
Reserved Networks

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.

Cegah Private Networks

Firewall memeriksa setiap *traffic*. Jika upaya *spoofing* masuk ke jaringan dan berasal dari alamat IP yang terdeteksi palsu, *traffic* dari sumber tersebut akan dicegah masuk.



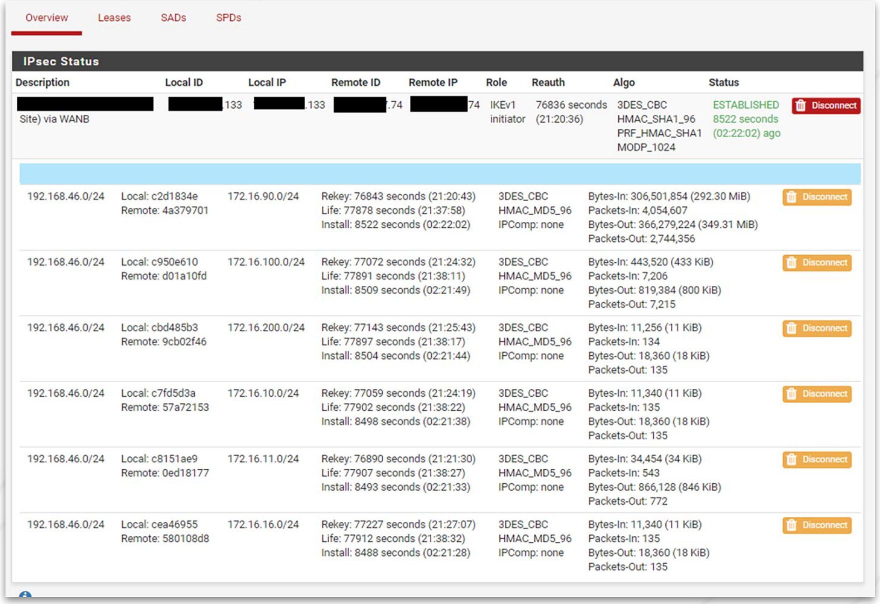
Reserved Networks

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.

Blok Bogon Networks

Cegah *traffic* dari bogon networks. ET Firewall bisa diatur untuk menunjukkan *traffic* palsu atau subnet yang tidak digunakan, yang telah dibajak untuk keperluan jahat.



IPsec Status

Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status	
[redacted] Site) via WANB	[redacted].133	[redacted].133	[redacted].74	[redacted]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	Disconnect

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	Disconnect
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	Disconnect
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	Disconnect
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	Disconnect
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	Disconnect
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	Disconnect

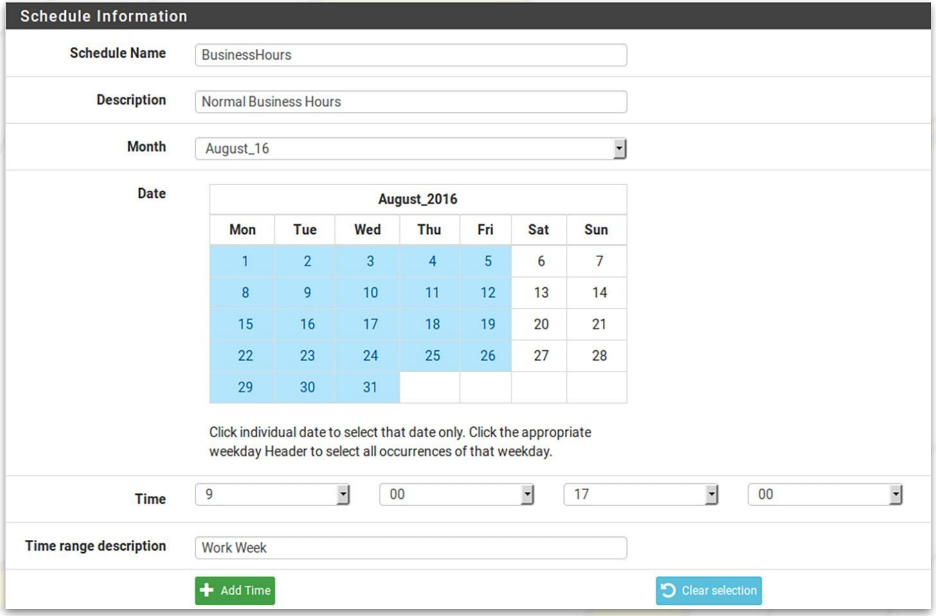
Pengaturan IPsec yang Mudah

Ketika koneksi IPsec diaktifkan, *firewall* secara otomatis menambahkan aturan tertentu agar koneksi bisa berjalan sebagaimana mestinya.

Time-Based Rules

Pengaturan Firewall Berbasis Waktu

Aturan berbasis waktu memungkinkan ET Firewall diaktifkan selama hari dan/atau rentang waktu tertentu.



Schedule Information

Schedule Name: BusinessHours

Description: Normal Business Hours

Month: August_16

Date:

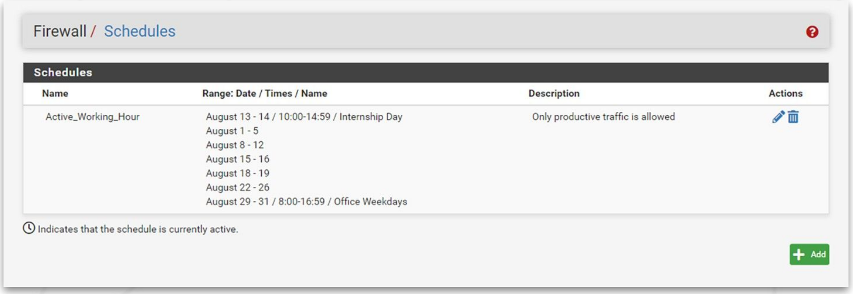
August_2016

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: 9 : 00 — 17 : 00

Time range description: Work Week

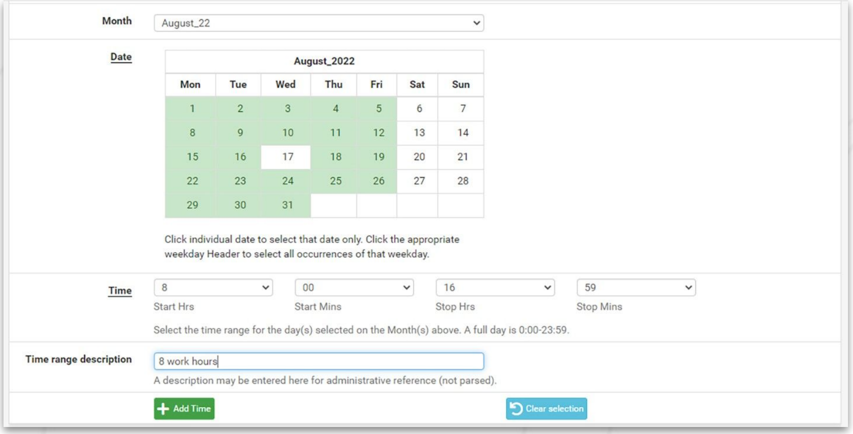


Firewall / Schedules

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.



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).

Tentukan Waktu Aktif Firewall

Jadwal harus ditentukan sebelum dapat digunakan pada aturan firewall. Jadwal ditentukan di menu khusus, dan setiap jadwal dapat berisi beberapa rentang waktu.

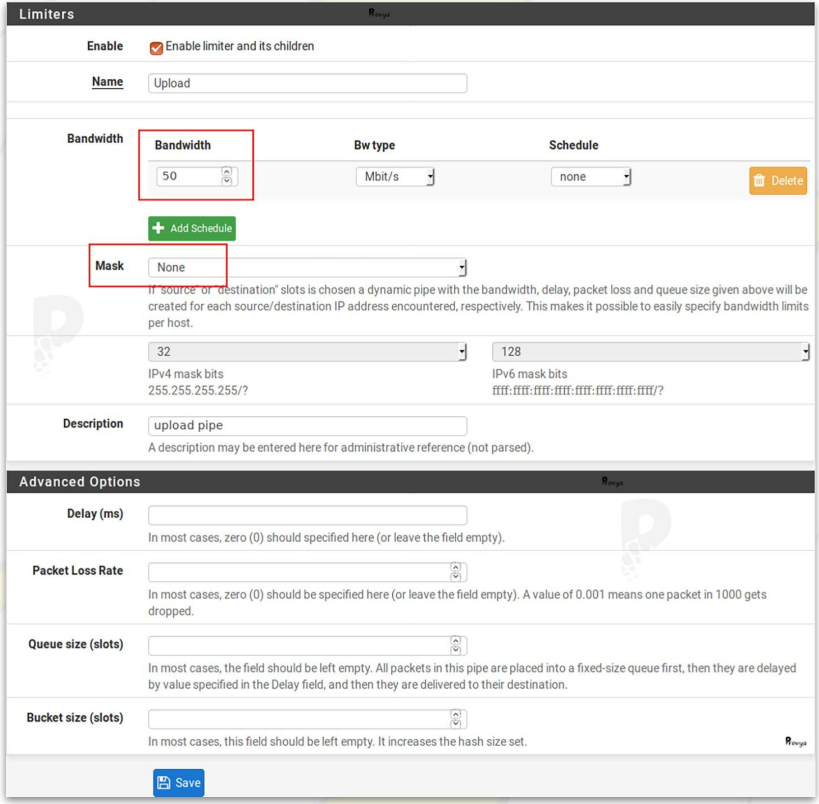
Gunakan Jadwal dalam Aturan Firewall

Untuk membuat aturan firewall menggunakan jadwal tertentu, buat aturan baru pada antarmuka yang diinginkan.

Connection Limits

Batasi Koneksi dengan Mudah

Bila dibutuhkan, Anda bisa membatasi koneksi jaringan Anda berdasarkan aturan tertentu.



Limiters

Enable	☑ Enable limiter and its children
Name	Upload

Bandwidth

Bandwidth	Bw type	Schedule	
50	Mbit/s	none	Delete

Add Schedule

Mask: None

If "source" or "destination" slots is chosen a dynamic pipe with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host.

32
IPv4 mask bits
255.255.255.255/?

128
IPv6 mask bits
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/?

Description: upload pipe
A description may be entered here for administrative reference (not parsed).

Advanced Options

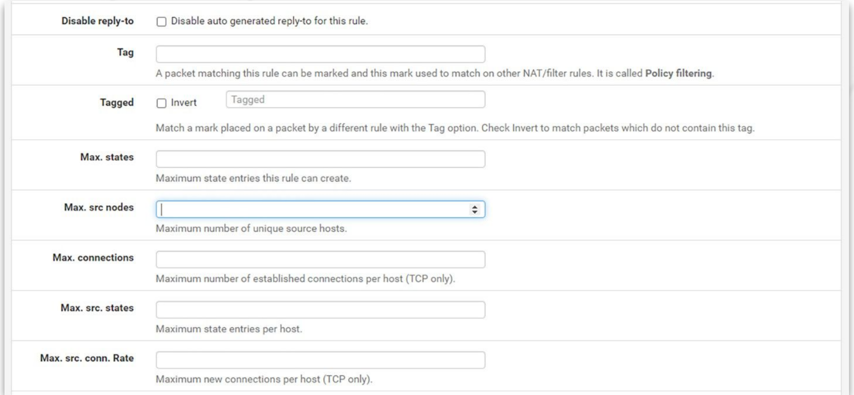
Delay (ms):
In most cases, zero (0) should specified here (or leave the field empty).

Packet Loss Rate:
In most cases, zero (0) should be specified here (or leave the field empty). A value of 0.001 means one packet in 1000 gets dropped.

Queue size (slots):
In most cases, the field should be left empty. All packets in this pipe are placed into a fixed-size queue first, then they are delayed by value specified in the Delay field, and then they are delivered to their destination.

Bucket size (slots):
In most cases, this field should be left empty. It increases the hash size set.

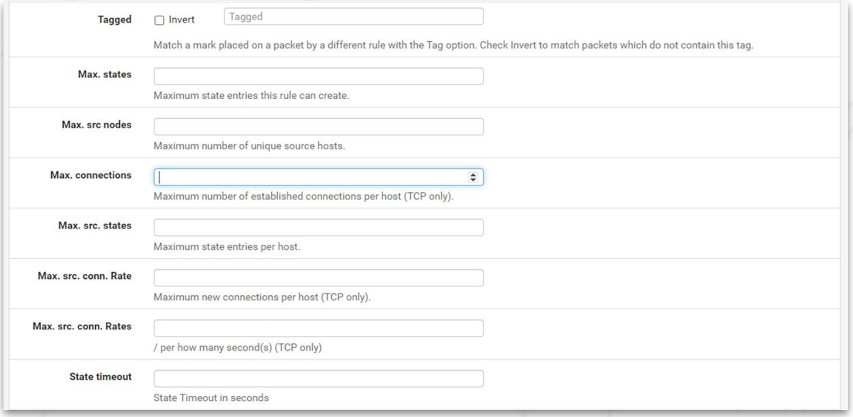
Save



Disable reply-to	□ Disable auto generated reply-to for this rule.
Tag	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	□ Invert 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	Maximum state entries this rule can create.
Max. src nodes	Maximum number of unique source hosts.
Max. connections	Maximum number of established connections per host (TCP only).
Max. src. states	Maximum state entries per host.
Max. src. conn. Rate	Maximum new connections per host (TCP only).

Tentukan Jumlah maksimum Host Sumber

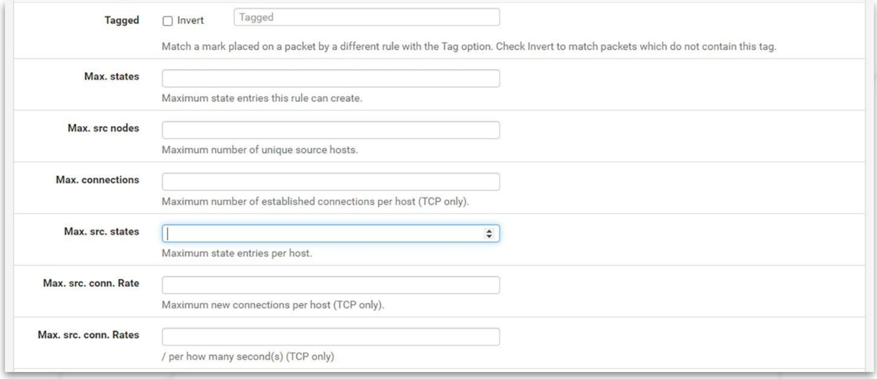
Opsi ini menentukan berapa banyak alamat IP sumber total yang dapat terhubung secara bersamaan untuk aturan ini.



Tagged	□ Invert 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	Maximum state entries this rule can create.
Max. src nodes	Maximum number of unique source hosts.
Max. connections	Maximum number of established connections per host (TCP only).
Max. src. states	Maximum state entries per host.
Max. src. conn. Rate	Maximum new connections per host (TCP only).
Max. src. conn. Rates	/ per how many second(s) (TCP only)
State timeout	State Timeout in seconds

Atur Jumlah Maksimum Koneksi Per Host

Untuk membatasi akses berdasarkan koneksi per host, gunakan pengaturan ini. Nilai ini dapat membatasi aturan untuk jumlah koneksi tertentu per host sumber, bukan total koneksi secara keseluruhan.



Tagged	□ Invert 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	Maximum state entries this rule can create.
Max. src nodes	Maximum number of unique source hosts.
Max. connections	Maximum number of established connections per host (TCP only).
Max. src. states	Maximum state entries per host.
Max. src. conn. Rate	Maximum new connections per host (TCP only).
Max. src. conn. Rates	/ per how many second(s) (TCP only)

Entri Status Maksimum Per Host

Pengaturan ini bekerja mirip dengan pengaturan jumlah maksimum koneksi per host, tetapi memeriksa entri status saja daripada melacak jika koneksi berhasil dibuat.

Thrive

Satu Firewall untuk Bisnis Anda

Amankan jaringan Anda dengan software dan perangkat ET Firewall yang handal

Dapatkan Konsultasi Gratis

Diskusikan sekarang juga kebutuhan IT perusahaan Anda dengan customer support kami di:

+62 822 9998 8870

Thank You

Prepared by:

Thrive

More Data More Sales

thrive.co.id