

ARTICA v4

Firewall feature rev2

Version 4.26.012900



TABLE OF CONTENT

Firewall Feature.....	4
Install the Firewall service.....	4
Display modules information.....	5
Activate your firewall on Interfaces.....	6
Your Networks	6
Firewall rules.....	8
Services objects.....	9
Sources and destinations objects.....	11
Objects type	12
Create a rule	12
Affect objects to a rule.....	14
Positive or negative object.....	15
Object Deep Packet inspection	16
Object Time restriction	17
Object Geo-location	18
Manage items.....	20
Bulk importation.....	20
Find a rule based on an item.....	21
Cybercrime IP Feeds.....	22
Enable Cybercrime IP Feeds	22
Categories.....	23
Display blocked IP database.....	23
Whitelist.....	24
Monitoring rules and service	25
Firewall service	25
Status, size and packets	27
Log rule events	28
Display events	29
Remote log/syslog server	30
Interfaces connectors	31
Create an interface connector	32
Create rules for an interface connector.....	33
NAT (Network adress translation) rules	34
The N.A.T section.....	34
Create a destination NAT.....	34
Route packets to a node	36
Masquerade.....	38
Define the Network outgoing interface to masquerade.	38
Create firewall Masquerade rules.....	38
Outgoing rule for the Artica server itself.....	39
Traffic shaping.....	40
Install the Firewall addons module.....	40
Create a rule for traffic shaping.....	40

Mandatory, define traffic shaping elements.	41
--	----

Firewall Feature

Artica Firewall feature simplifies network security with a single, modular, software platform designed to fit the evolving needs of your organization.

Designed specifically for organizations with limited IT resources and budgets, Artica firewall provides a browser-based, responsive and intuitive interface enabling you to quickly gain visibility into the traffic on the network.

Artica Firewall feature delivers a comprehensive, enterprise-grade network security platform for organizations in any industry

INSTALL THE FIREWALL SERVICE

The firewall service can be installed using the “features” section.

On the search field, type **Firewall**

Click on **Install** button on the “Your Firewall” row

Install or uninstall features

This section allows you to install/uninstall available features on your server

select ▾

Expand

Wizards

firewall

✕ ▾

Status	Software	Action
Installed	Your Firewall	<div>✓ uninstall</div>
	Web Application Firewall (WAF)	<div>⚠ Not installed</div>
	GreenSQL Firewall	<div>⚠ Require installed MySQL database server</div>

DISPLAY MODULES INFORMATION.

Firewall features depends on installed/loaded modules.

The “Your Firewall / Parameters / Modules” displays current loaded/Unloaded/installed modules.

Artica loads automatically modules depends on your firewall rules.

Take care on uninstalled modules, this means you have to install **Firewall addons** if you need them.

The screenshot shows the 'Firewall parameters v1.8.2' interface. On the left is a dark sidebar with navigation links: Dashboard, Your system, Network, DNS, Your Firewall (expanded), Parameters (highlighted with a red box), Rules, Firewall objects, Firewall services, Interfaces connectors, NAT, Masquerade, Cybercrime IP Feeds, Configuration file, Events, Databases, and Logs center. The main panel is titled 'Firewall parameters v1.8.2' and has three tabs: Interfaces, Options, and Modules (highlighted with a red box). Below the tabs is a search bar and a table of modules. The table has columns: Status, Module, Description, Aliases, and [Depends]. The table lists various modules, some loaded (green status) and some unloaded (orange status). At the bottom, a group of modules is highlighted with a red box: 'Not installed' status for xt_fuzzy, xt_geoip, xt_iface, and xt_ip2p.

Status	Module	Description	Aliases	[Depends]
Loaded	nf_defrag_ipv4		—	—
Loaded	nf_defrag_ipv6		—	—
Unloaded	nf_dup_ipv4	nf_dup_ipv4: Duplicate IPv4 packet	—	—
Unloaded	nf_dup_ipv6	nf_dup_ipv6: IPv6 packet duplication	—	—
Unloaded	nf_dup_netdev		—	—
Loaded	nf_log_common		—	—
Unloaded	nf_reject_ipv4		—	—
Unloaded	nf_reject_ipv6		—	—
Unloaded	nf_socket_ipv4	Netfilter IPv4 socket lookup infrastructure	—	—
Unloaded	nf_socket_ipv6	Netfilter IPv6 socket lookup infrastructure	—	—
Unloaded	nf_tproxy_ipv4	Netfilter IPv4 transparent proxy support	—	—
Unloaded	nf_tproxy_ipv6	Netfilter IPv4 transparent proxy support	—	—
Loaded	nfnetlink		net-pf-16-proto-12	—
Loaded	x_tables	(ip,ip6,arp,eb)_tables backend module	—	—
Not installed	xt_fuzzy		—	—
Not installed	xt_geoip		—	—
Not installed	xt_iface		—	—
Not installed	xt_ip2p		—	—

ACTIVATE YOUR FIREWALL ON INTERFACES.

The “Your Firewall / Parameters” section defines which network interface will be protected by the Firewall

By default, no interface are enabled,

Firewall parameters v3.1.7

Interfaces Options

Search

Network Interface	Enabled	Firewall Default Policy	Firewall Behavior	Masquerading	Allow Artica Web Console
eth2 Interface eth2 192.168.1.242	—	—	—	—	—
eth1 Interface eth1 192.168.100.12	—	—	—	—	—
eth0 Interface eth0 172.16.5.22	—	—	—	—	—

This table show the global default behavior of the firewall on each active interface.

YOUR NETWORKS

Your networks is a dedicated section that should list all your Internal networks.

Networks used by the Firewall are “Trusted Network”, trusted networks, by default, are allowed to pass through the firewall

Your networks

Set your local networks in this area in order to drive network services such as the Network scanner, IDS, firewall, proxy...

+ New network Scan your network

Networks	Trusted network	% used	Ping	Scan	Scan report 0 Items	DEL
172.16.5.0/255.255.255.0	—	—	—	—	—	—
Network 172.16.5.0/255.255.255.0	—	—	—	—	—	—
192.168.100.0/255.255.255.0	—	—	—	—	—	—
Network 192.168.100.0/255.255.255.0	—	—	—	—	—	—
192.168.1.0/255.255.255.0	—	—	—	—	—	—
Network 192.168.1.0/255.255.255.0	—	—	—	—	—	—

To enable an Interface, click on the Interface name

eth1 Interface eth1 192.168.100.12

eth1 Interface eth1 192.168.100.12

Activate The FireWall On This Interface: ☒ ON

Firewall Default Policy: Finally deny all

Firewall Behavior: Act as WAN

Masquerading: ☒ ON

Allow Artica Web Console: ☒ ON

« Apply »

This example is typically a rule for a router, this Interface represents the WAN interface.

To turn the firewall on enable the “**Activate the Firewall on this interface**”

- **Firewall default policy** defines what is the last rule defined at the end values are finally deny all or allow all.
- **Firewall behavior** defines protection and the trusted networks behavior of the defined Interface:
 - **Act as Wan:**
network is trusted and specials features are enabled to protect the network:
 - **Bad-packets:** Drops all the bad packets
 - **Invalid:** Drops all incoming invalid packets, as detected INVALID by the connection tracker.
 - **Fragments:** Drops all packet fragments.
 - **New-tcp-w/o-syn:** Drops all TCP packets that initiate a socket but have not got the SYN flag set.
 - **Malformed-xmas:** Drops all TCP packets that have all TCP flags set.
 - **Malformed-null:** Drops all TCP packets that have all TCP flags unset.
 - **Malformed-bad:** Drops all TCP packets that have illegal combinations of TCP flags set.
 - **Act as LAN:**
Networks defined as trusted network in the Network configuration are allowed to access to any service of the server.
- **Masquerading:**
Masquerading is a special form of Source NAT (SNAT) that changes the source of requests when they go out and replaces their original source when they come in.
This way a Linux host can become an Internet router for a LAN of clients having unrouteable IP addresses.
Masquerading takes care to re-map IP addresses and ports as required.
Masquerading is expensive compare to SNAT because it checks the IP address of the outgoing interface every time for every packet.
If your host has a static IP address you should generally prefer SNAT.
- **Allow Artica Web Console:**
Open the local Artica Web console port in order to manage Artica outside the server in a closed environment.

The table will reflect main defined options.

If no interface is enabled in the Firewall, understand that the firewall did not protect your server.

Firewall parameters v3.1.7

Interfaces		Options				
		Search				
Network Interface	Enabled	Firewall Default Policy	Firewall Behavior	Masquerading	Allow Artica Web Console	
eth2 Interface eth2 192.168.1.242	✓	Deny all	WAN	✓	✓	
eth1 Interface eth1 192.168.100.12	—	—	—	—	—	
eth0 Interface eth0 172.16.5.22	—	—	—	—	—	

FIREWALL RULES.

A firewall rule is designed into 4 parts

1. **The rule itself** that defines the rule behavior (Deny access, Allow access, Mark TCP packets).
2. A **service object** that stores destination protocols and ports.
3. **Destination objects** that stores destinations IP addresses or MAC addresses.
4. **Source objects** that stores sources IP addresses or MAC addresses

Before creating any rule in the “rules” section, you should create your desired objects

Services objects

The section “Firewall services” list a objects that defines protocols and ports, by default, Artica provide a list of “standard” services that you can use directly on your rules.
You can create your own service by clicking on the “**New service**” button.

Firewall services

This section store all ports and protocols that can be used in your firewall rules.
You are free to create any service in this section in order to create a dedicated rule according a specific destination port

[+ New service](#) [Apply Firewall rules](#)

Search

Enabled	Type	Ports	
✓	AH	51/any	
✓	ESP	50/any	
✓	GRE	47/any	
✓	ICMP	icmp/any	
✓	ICMPV6	icmpv6/any	
✓	OSPF	89/any	
✓	amanda	udp/10080	
✓	apcupsd	tcp/6544	
✓	apcupsdnis	tcp/3551	
✓	aptproxy	tcp/9999	

A service can handle multiple ports and multiple protocols.

The following are required for all simple services:

service name: myservice

Ports: proto/sports

myservice is the name we will give our service.

Proto: is anything that firewall accepts as a protocol e.g. "tcp", "udp", "icmp" "all" and numeric protocol value.

Sports: is the ports the server is listening at. It is a space-separated list of port numbers, names and ranges (from:to).The keyword **any** will match any server port.

Service:

New service

Required entries

The following are required for all simple services:

- service name: myservice
- Ports: proto/sports
- Local ports: cports

myservice is the name we will give our service.

proto is anything that firewall accepts as a protocol e.g. "tcp", "udp", "icmp" and numeric protocol values.

sports is the ports the server is listening at. It is a space-separated list of port numbers, names and ranges (from:to).The keyword **any** will match any server port.

cports is the ports the client may use to initiate a connection. It is a space-separated list of port numbers, names and ranges (from:to). The keyword **any** will match any client port. The keyword **default** will match default client ports.

Service Name:

Enabled: ☒ ON

Ports:

1	tcp/80
2	tcp/443
3	tcp/9000
4	tcp/25
5	any/53
6	udp/61

[« Add »](#)

Ports examples:

Format	Explain
tcp/80	Matches port number 80 on TCP protocol
tcp/80:120	Matches ports number 80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,97,98...120 on TCP protocol
Any/9090	Matches port number 9090 on all protocols
tcp/any	Matches any port on TCP protocol
tcp/80 tcp/443 tcp/9000 tcp/25 any/53 udp/61	Matches port number 80 on TCP protocol Or matches port number 443 on TCP protocol Or matches port number 9000 on TCP protocol Or matches port number 25 on TCP protocol Or matches port number 53 on all protocols Or matches port number 61 on UDP protocol
tcp/80,443,9000,25	Matches port number 80 on TCP protocol Or matches port number 443 on TCP protocol Or matches port number 9000 on TCP protocol Or matches port number 25 on TCP protocol

The option “enabled” allow rules to use the service. If the service is disabled, the rule will matches any protocols and any ports.

Services can be found using the TOP search field, you can search by service name or a defined port.

The screenshot shows the Artica Manager web interface. On the left is a dark sidebar with navigation links: Manager (Administrator), Dashboard, Your system, Network, DNS, Your Firewall, Databases, and Logs center. The main content area has a top header with system status (Cpu: 7%, Mem: 30.3%/1.92 GB, 12:44:06) and user options (Members, Admin Guide, Log out). Below the header, a search bar contains the text 'tcp/80'. The search results are titled 'Search messages «tcp/80»'. A table of results is shown, with three items highlighted by a red box:

Items	Search Results	Category
(A) companyoutgoingports	tcp/80 tcp/443 tcp/9000 tcp/25 any/53 udp/61 tcp/1000:2000	Firewall services
(A) http	tcp/80	Firewall services
(A) httpalt	tcp/8080	Firewall services

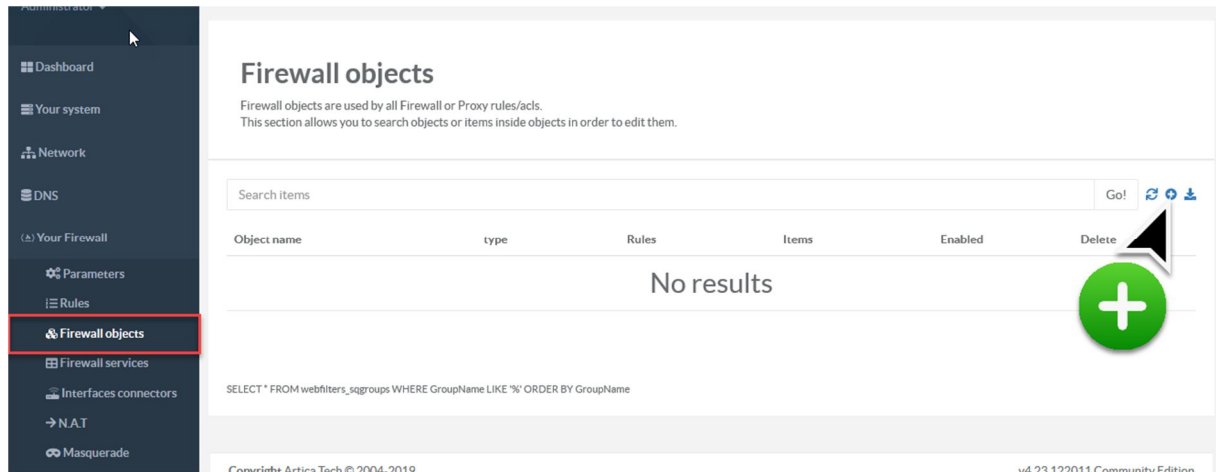
Below the table, there is a link to 'Artica and Cisco's Web Cache Coordination Protocol - Artica Proxy' and a search result from Google dated Jun 18, 2015, mentioning 'access-list wccp_redirect extended permit tcp workstations ... LAN clients proxy port 80 only access-list 120 permit tcp 10.254.253.0 0.0.0.255 ...'.

Sources and destinations objects.

Sources and destination objects are used in firewall rules, objects can store a list of IP addresses, networks using CIDR notation, MAC addresses.

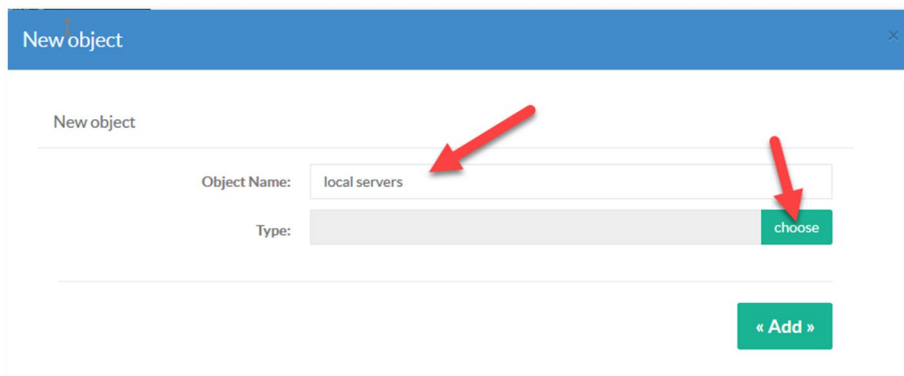
Objects can store many items, this is the reason Artica use these kind of groups in order to build firewall rules.

- Select “Firewall objects” on the left menu.
- Click on the cross on the left side of the search field.

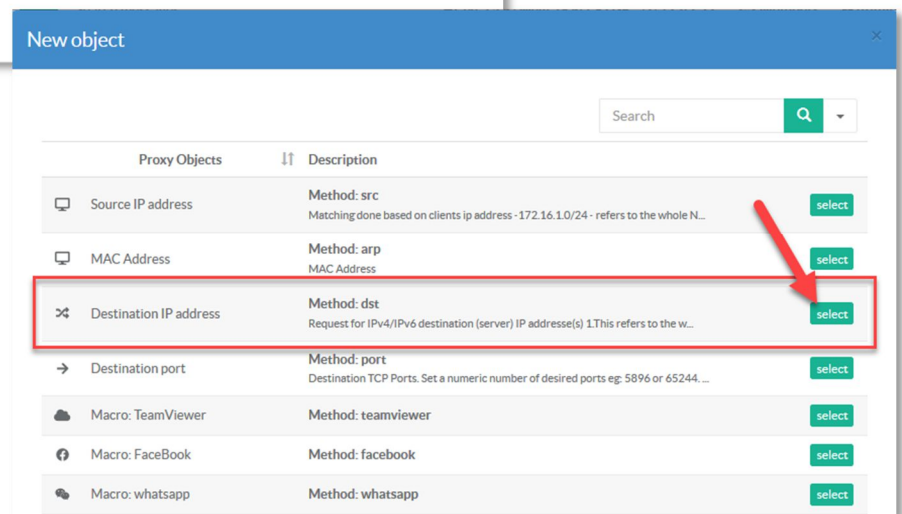


Set the name of your object.

Click on **Choose** button in order to define the object type.



Choose the method/type of your object



Objects type

Object type	Description
Source IP address	A set of source IPV4 or network mask in CDIR format such as 192.168.1.1 or 192.168.1.0/24
MAC Address	A list of MAC addresses in aa:bbb:ccc:fff:eee format
Destination IP address	A set of destination IPV4 or network mask in CDIR format such as 192.168.1.1 or 192.168.1.0/24
Destination port	A list of TCP destination ports
Macro: TeamViewer	TeamViewer networks
Macro: FaceBook	FaceBook networks
Macro: whatsapp	Whatsapp networks
Macro: Skype	Skype networks
Macro: Youtube	Youtube networks
Macro: Office 365	Office 365 networks
Macro: DropBox networks	DropBox networks
Countries	List of subnets stored in each country
Local Network	Networks defined in "Your network section"

Create a rule

To create rule, go to "Your Firewall / Rules"

The screenshot shows the 'Firewall Rules' management interface. The left sidebar contains a menu with 'Rules' highlighted. A red arrow points from the 'Rules' menu item to the '+ New Rule' button in the main content area. The main content area displays a table of existing firewall rules.

Order	Rule Name	Network Interface	Type	Enabled	Order	Delete
-	Allow Artica Web Console TCP/5000	Interface eth2 (eth2)	PASS	-	-	-
-	Internet access Allow this server to reach remote DNS, HTTP, HTTPS, FTP services and 217.182.193.199 Port 6000	Interface eth2 (eth2)	OUT PASS	-	-	-
-	Default Finally deny all	Interface eth2 (eth2)	IN/OUT DENY	-	-	-

SELECT * FROM iptables_main ORDER BY zOrder

Click on "New rule"

Rule: 0 New Rule

Rule

If you enable the outgoing rule option, then this rule is applied from the server itself to the destination network/service.

Outgoing Rule: ☐ OFF

Rule Name:

Enabled: ☒ ON

Order:

Network Interface:

Service:

☐ Drop

☒ Accept

☐ Mark packets

Log All Events: ☐ OFF

Section for MARK TCP packets

Outgoing rule: An Outgoing rule is a rule dedicated for the Artica itself, means connections came from Artica to outside using the defined interface.

- **Rule Name:** A short description of the rule.
- **Enabled:** Make the rule active or inactive.
- **Order:** Position of the rule.
- **Network Interface:** The Network interface defined by the rule (if none selected, the rule is applied for all interfaces and rules without interfaces are evaluated after rule linked with a Network Interface.)
- **Service:** If the rule is designed only for one service, select the service object in the drop-down list.
- **Rule behavior:** Select Drop (reject packets), Accept (allow connections), Mark packets (ADD a MARK entry and allow packets).
- **Log all events:** Write matched connections to firewall events file.

Affect objects to a rule

You can affect multiple objects types for a rule :

- **Firewall services:** Add more services objects in your rule.
- **Inbound objects:** Object that matches sources networks / Mac Addresses.
- **Outbound objects:** Objects that matches destinations networks
- **Deep Packets inspection:** Objects that matches applications in protocol.
- **Time restriction:** Object that enable/disable a rule during a period.

Firewall Rules

Search messages Go!

[+ New Rule](#) [Apply Firewall rules](#) All Interface eth2 (eth2)

Search Q

Order	Rule Name	Network Interface	Type	Enabled	Order	Delete
1	Allow SSH For all nodes and To everything and Service «ssh» then Accept All times	Interface eth2 (eth2)	PASS	<input checked="" type="checkbox"/>	↑ ↓	🗑️

When you create a rule no destinations or sources are defined, this means the rule matches from any to any.

To affect sources and destinations, click on the rule and select the “Inbound object” or “Outbound object”

Rule: 1 Allow SSH ACCEPT ×

[Rule](#) [Firewall services](#) **[Inbound object](#)** [Outbound object](#) [Deep Packet Inspection](#) [Time restriction](#)

[+ New object](#) [Link object](#)

Search Q

ID	Objects	Type	Items
No results			

You can use “**New object**” to create a new object and add items inside this object or “**Link object**” to affect an already created object for this rule.
 You can add unlimited objects and mixt multiples object types.

Rule: 1 Allow SSH ACCEPT

Rule Firewall services **Inbound object** Outbound object Deep Packet Inspection Time restriction

+ New object Link object

Search

ID	Objects	Type	Items			
1	My Net	Source IP address	2			
2	MacAddr	MAC Address	3			
3	mybnet2	Source IP address	2			

Positive or negative object

You can find in the table a “Is” column.
 This column can be switched between “is” or “is not”

Rule: deny SSH Firewall services **Inbound object** Outbound object Deep Packet Inspection

Time restriction

+ New object Link object

Search

ID	Is	Objects	Type	Items			
5	is not	Denied Countries	countries	250			

Artica merge all defined groups into a single container for the same type “IP addresses or MAC addresses”, when you sets “is not” it means all items inside this group will not matches the rule.

For example, you set a deny rule that stores the group with the source network “192.168.1.0/24” and you create a second group with “is not” with the item “192.168.1.1”. means the whole group 192.168.1.0/24 will matches except for the IP address 192.168.1.1.

Inside the generated container, the matches is selected by the most relevant IP to the largest network.
 The 192.168.1.1 will matches first, second the 192.168.1.0/24 and finally the 192.168.0.0/16.

If you set a deny rule that stores the group with the source network “192.168.1.0/24” and you create a second group with “is not” with the item “192.168.0.0/16” means the group 192.168.1.0/24 will still matches.
 Because it matches before the 192.168.0.0/16

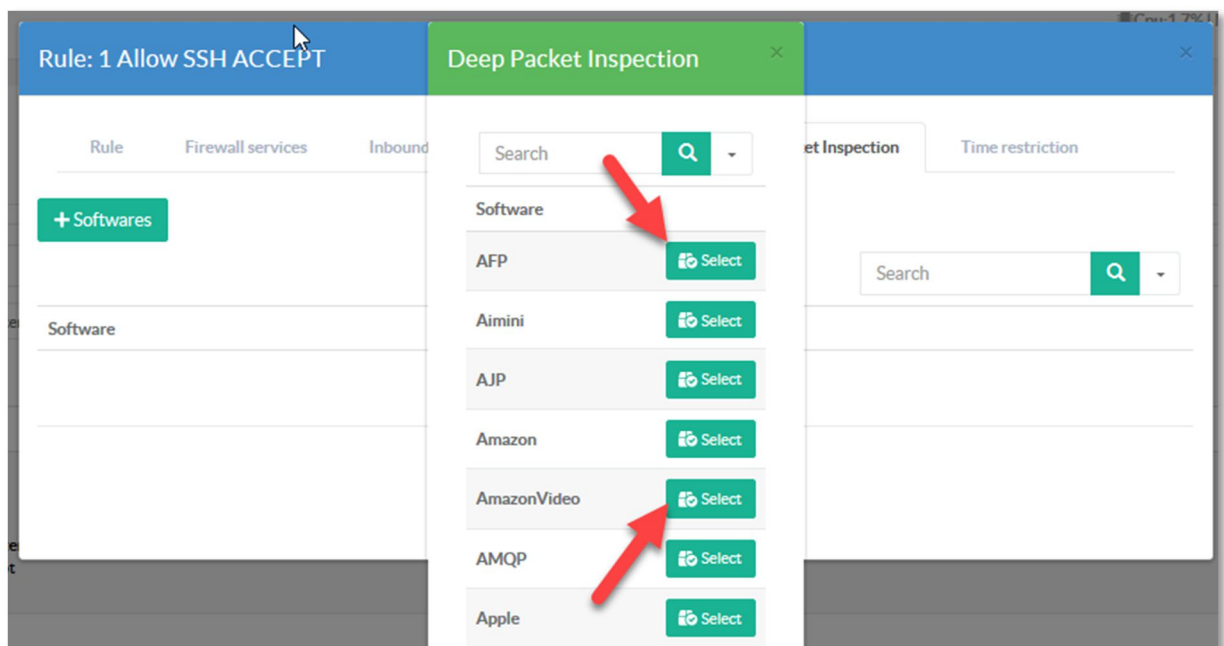
Object Deep Packet inspection

Deep packet inspection allow the firewall to detect 239 applications inside the protocol.

As the module detects data inside the protocol, there is no direction (inbound or outbound), it matches data in-transit.

Available applications are : afp, aimini, ajp, amazon, amazonvideo, amqp, apple, applecloud, appleitunes, applejuice, applepush, appstore, armagetron, ayiya, battlefield, bgp, bittorrent, bjnp, checkmk, ciscoskinny, ciscovpn, citrix, cloudflare, cnn, coap, collectd, corba, crossfire, csgo, dce_rpc, deezer, dhcp, dhcpv6, diameter, direct_download_link, directconnect, dns, dnscrypt, dofus, drda, dropbox, eq, ebay, edonkey, egg, facebook, facebookzero, fasttrack, fiesta, fix, florensia, free, free_49, ftp_control, ftp_data, genericprotocol, git, github, gmail, gnutella, google, googledocs, googledrive, googlehangout, googlemaps, googleplus, googleservices, gre, gtp, guildwars, h323, halflife2, hep, hotmail, hotspotshield, http, http_activesync, http_connect, http_download, http_proxy, iax, icecast, icmp, icmpv6, iflix, igmp, imap, imaps, instagram, ip_in_ip, ipp, ipsec, irc, kakaotalk, kakaotalk_voice, kerberos, kontiki, lastfm, ldap, linkedin, lisp, llmnr, lotusnotes, maplestory, mdns, megaco, memcached, messenger, mgcp, microsoft, mining, modbus, mpeg_ts, mqtt, ms_onedrive, msn, mssql-tds, mysql, nestlogsink, netbios, netflix, netflow, nfs, nintendo, noe, ntop, ntp, ocs, office365, ookla, opendns, openft, openvpn, oracle, oscar, ospf, pando_media_booster, pandora, pastebin, pcanalyzer, playstation, playstore, pop3, pops, postgresql, pplive, ppsstream, pptp, qq, qqlive, quic, radius, rdp, redis, remotescan, rsync, rtcp, rtsp, rtp, rtsp, rx, sap, sctp, sflow, shoutcast, signal, sina(weibo), sip, skype, skypecall, slack, smb1, smb2, smpp, smtp, smtps, snapchat, snmp, socks, someip, sopcast, soulseek, soundcloud, spotify, ssdp, ssh, ssl, ssl_no_cert, starcraft, stealthnet, steam, stun, syslog, teamspeak, teamviewer, telegram, telnet, teredo, tftp, thunder, tinc, tor, truphone, tuenti, tvants, tvplayer, twitch, twitter, ubuntu2, ubuntuone, unencrypted_jabber, unknown, upnp, usenet, vevo, vlua, viber, vmware, vnc, vrrp, warcraft3, waze, webex, wechat, whatsapp, whatsappfiles, whatsappvoice, whois-das, wikipedia, windowsupdate, worldofkungfu, worldofwarcraft, xbox, xdmcp, yahoo, youtube, youtubeupload, zattoo, zeromq

- Select the tab “**Deep packet Inspection**”
- Click on **Software** button.
- Choose applications you want to detects in your rule.



Object Time restriction

Object time restriction define the period when the rule is active, outside the defined period, the rule did not matches.

Rule: 1 Allow SSH ACCEPT

Rule Firewall services Inbound object Outbound object Deep Packet Inspection **Time restriction**

Allow SSH - Time restriction

The possible time range is 00:00:00 to 23:59:59, if you need to set a rule from 22:00:00 to 07:00:00, create 2 rules: one from 22:00:00 to 23:59:00 and second from 00:00:00 to 07:00:00

Enabled: ☒ ON

From Time: 01:00:00

To Time: 08:00:00

Monday: ☒ ON

Tuesday: ☒ ON

Wednesday: ☒ ON

Thursday: ☒ ON

Friday: ☒ ON

Saturday: ☒ ON

Sunday: ☒ ON

« Apply »

You can define a time range and set the day of the week the rule is enabled.

The possible time range is 00:00:00 to 23:59:59, if you need to set a rule from 22:00:00 to 07:00:00, create 2 rules: one from 22:00:00 to 23:59:00 and second from 00:00:00 to 07:00:00

Object Geo-location

Artica retrieve a list of subnets for each country, you need to allow the Artica server to retrieve patterns via HTTP from the www.ipdeny.com repository server.

- When creating a new object, select the “**Countries**” type and add your new object.

Rule: 6 deny SSH DROP

Rule: deny SSH Firewall services **Inbound object** Outbound object Deep Packet Inspection

Time restriction

+ New object [Link object](#)

New Object

Group Name: Denied Countries

Type: countries

« Cancel » **« Add »**

- Once the object is created, you can see that it have 0 item, click on the object link.

Rule: 6 deny SSH DROP

Rule: deny SSH Firewall services **Inbound object** Outbound object Deep Packet Inspection

Time restriction

+ New object [Link object](#)

ID	Objects	Type	Items	
5	Denied Countries	countries	0	

- Select “items”
- You can search by country and activate a country inside your rule.

Items - Group: Denied Countries countries

Denied Countries

Items

+ Select all

Disable all

Search

Q

Country	Selected
Andorra	<input checked="" type="checkbox"/>
United Arab Emirates	<input checked="" type="checkbox"/>
Afghanistan	<input checked="" type="checkbox"/>
Antigua and Barbuda	<input checked="" type="checkbox"/>
Anguilla	<input checked="" type="checkbox"/>
Albania	<input checked="" type="checkbox"/>
Armenia	<input checked="" type="checkbox"/>
Angola	<input checked="" type="checkbox"/>
Asia/Pacific Region	<input checked="" type="checkbox"/>
Antarctica	<input checked="" type="checkbox"/>
Argentina	<input checked="" type="checkbox"/>
American Samoa	<input checked="" type="checkbox"/>
Austria	<input checked="" type="checkbox"/>
Australia	<input checked="" type="checkbox"/>

MANAGE ITEMS

When create a group inside a rule, you can manage several items.

A search engine (the first search field) allows you to find the item.

The interface list is limited to 150 rows, if your item is not displayed in the first rows you have to use the search engine.

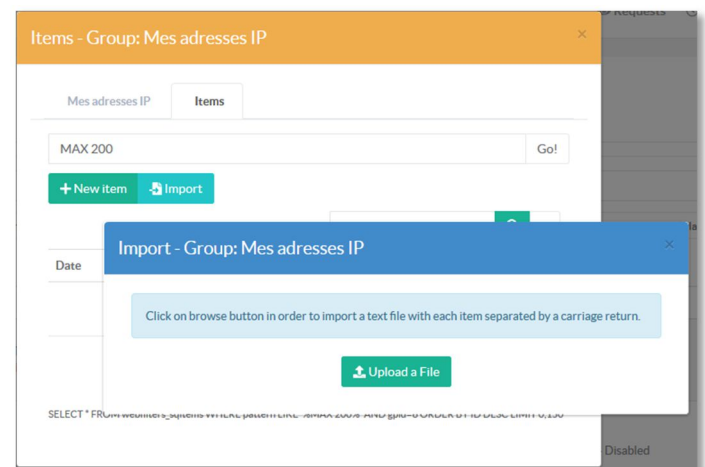
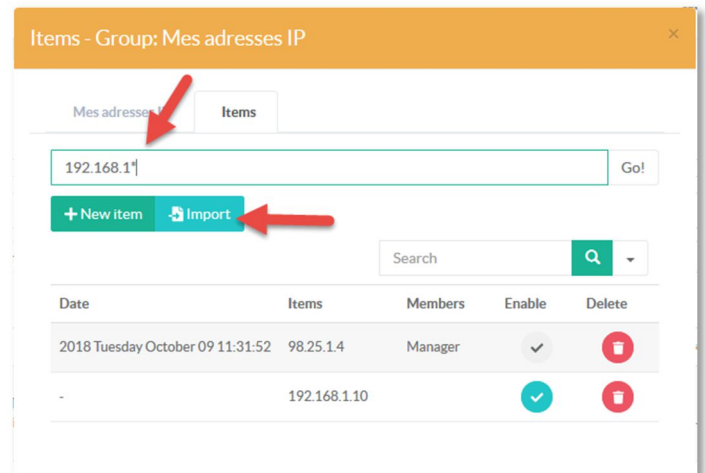
An item can be enabled or disabled, when the item is disabled, it will be not add into the FireWall rules but still available on the Web interface.

Bulk importation.

The Import button allows you to massively import items in the group.

Items must be stored in a text file separated by a carriage return.

A group has no item limits, you just have to think about memory used by the firewall according to 25,000 elements takes up about 350k of memory.



Find a rule based on an item

The global search engine on the firewall-rule list allows you to find a rule according to a defined item. The wildcard is supported, if you need to find a specific IP string or subnet, the table will display rules that stores the group with the desired item.

Firewall Rules

98.25.1.4

+ New Rule

Apply Firewall rules

All

Interface externe (eth1)

Interface Interne (eth0) → Interface externe (eth1)

Interface Interne (eth0) → Interface wlan0 (wlan0)

Interface

Order	Rule Name	Network Interface
1	<div>Test groupe</div> <div>For inbound objects <u>Mes adresses IP (2 Items)</u> and To everything and Service «ssh» then Deny access All times</div>	Interface wlan0 (wlan0) → Interface In
-	<div>Internet access</div> <div>Allow this server to reach remote DNS, HTTP, HTTPS, FTP services and 217.182.193.199 Port 6000</div>	Interface externe (eth1)
-	<div>Proxy service</div> <div>Allow all computers in trusted networks to be connected to proxy ports listed in Listen ports section</div>	Interface externe (eth1)
-	<div>default</div> <div>Finally deny all</div>	Interface externe (eth1)

CYBERCRIME IP FEEDS

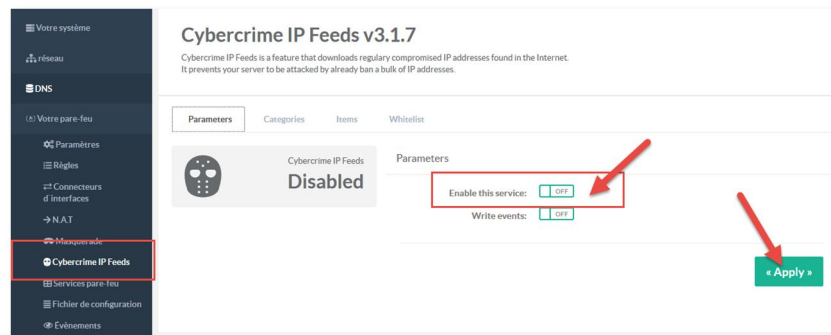
Cybercrime IP Feeds is a feature that downloads regularly compromised IP addresses found in the Internet. It prevents your server to be attacked by already ban a bulk of IP addresses. You have to enable this feature only if your Artica server is installed inside Internet in order to protect him.

Enable Cybercrime IP Feeds

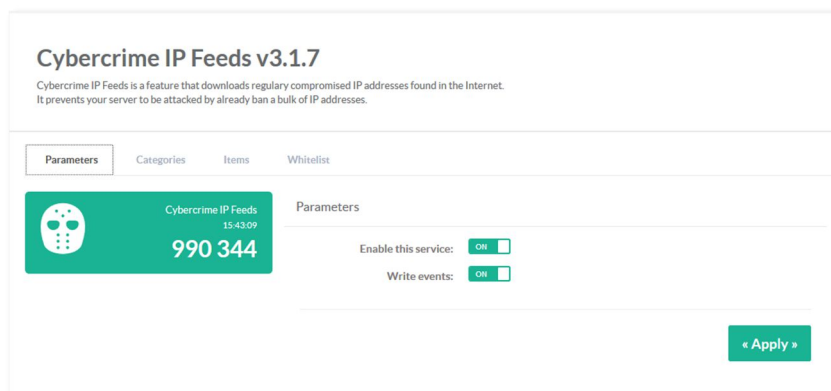
On “Your Firewall”, select **Cybercrime IP Feeds** menu.

On the Parameters section, click on “Enable this service”

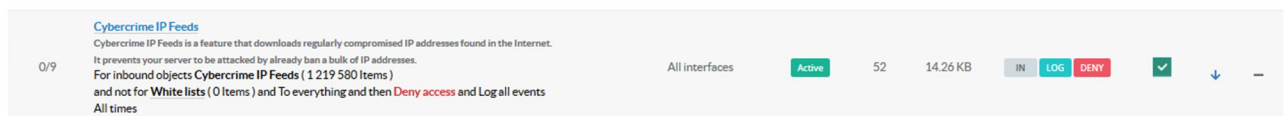
If you want to log all banned addresses from Cybercrime IP Feeds, turn on the “**Write events**” checkbox.



Wait a few minutes, you will see that the status is turned to green with the number of IP addresses saved in databases and that is automatically rejected by the firewall.



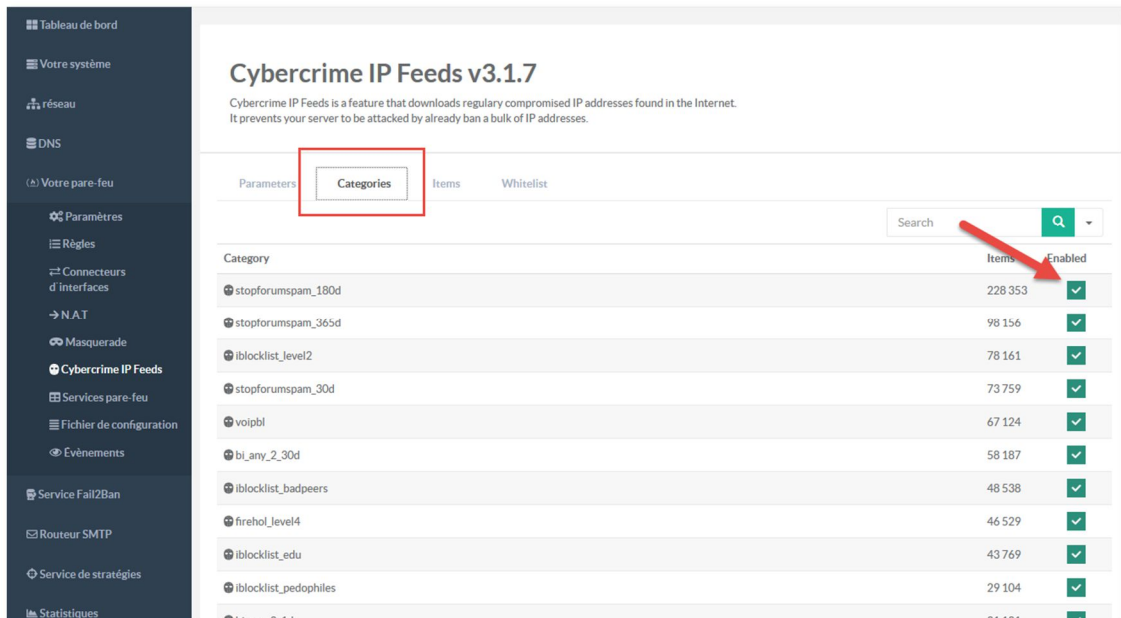
Go into your rules, you will find a new locked rule



Categories

Blocked IP addresses are generated from several community groups. These community groups (aka categories) can be displayed in the “**Categories**” section.

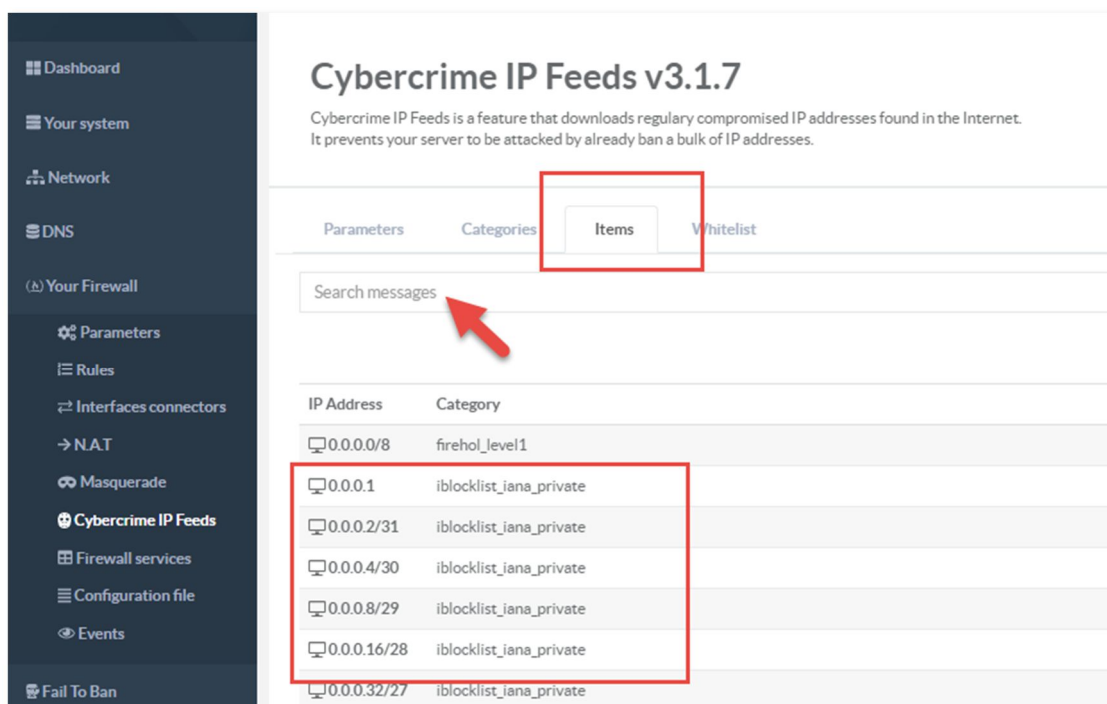
This section list groups and allows you to enable or disable the banned list.



Display blocked IP database.

The **items** tab allows you to search and display blocked remote addresses added in your firewall database. A search engine allows you to find some elements.

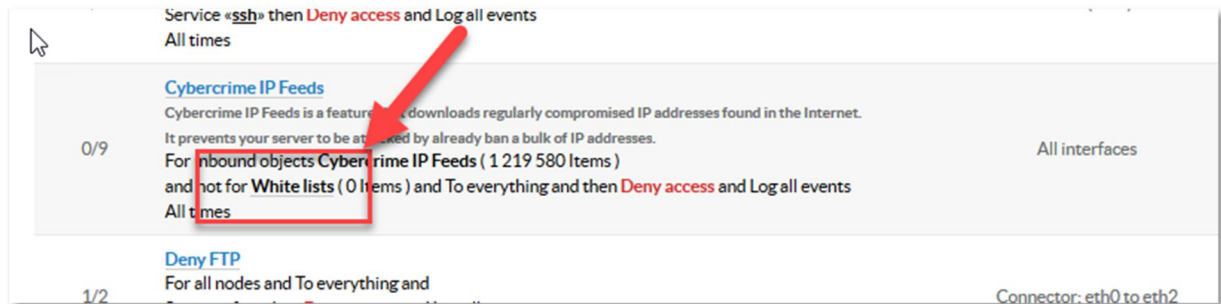
Search pattern can be 192.168.1.1 for an IP or 192.168.*.1 or 192.168.1.0/24 to see all IPs inside the CDIR network.



Whitelist

If you need to allow some blocked addresses (a single IP address or a network), use the whitelist tab. The whitelist section allows you to add/import IP addresses you need to bypass for the Cybercrime IP Feeds feature.

Search the CyberCrime rule



Click on the White lists link to add CDIR or ip addresses in the whitelist database.

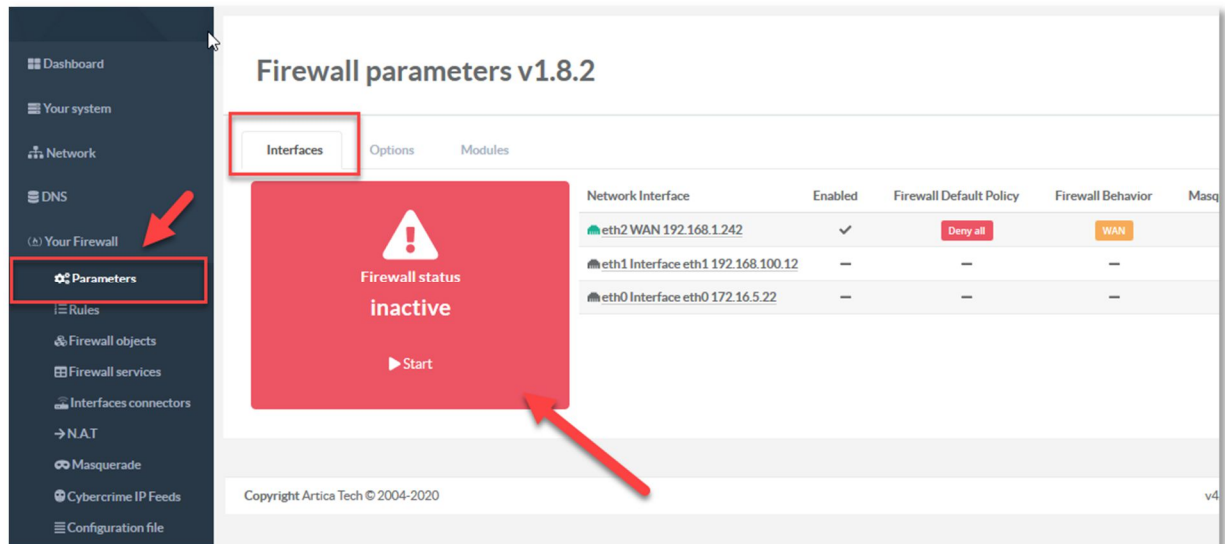
MONITORING RULES AND SERVICE

Firewall service

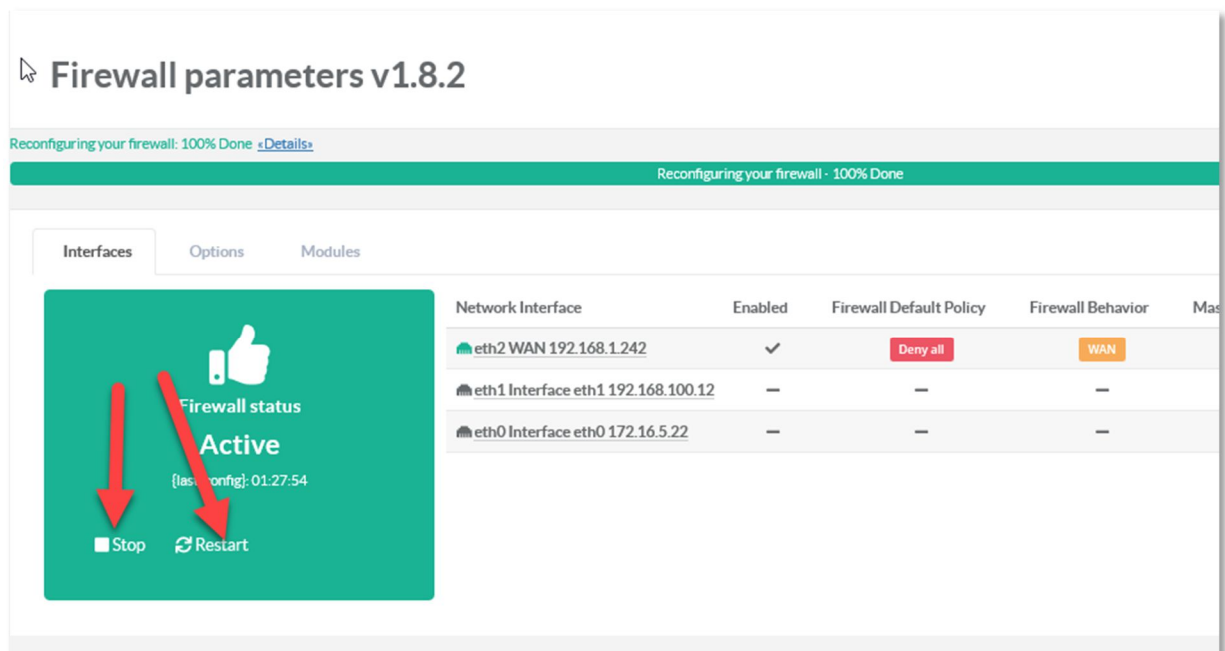
Start/stop via the Web console

On the Artica Web console, under “Your Firewall” and **parameters**, the “**interfaces**” section display the status of the firewall if it is active or not.

A button under the status allows you to start the firewall.

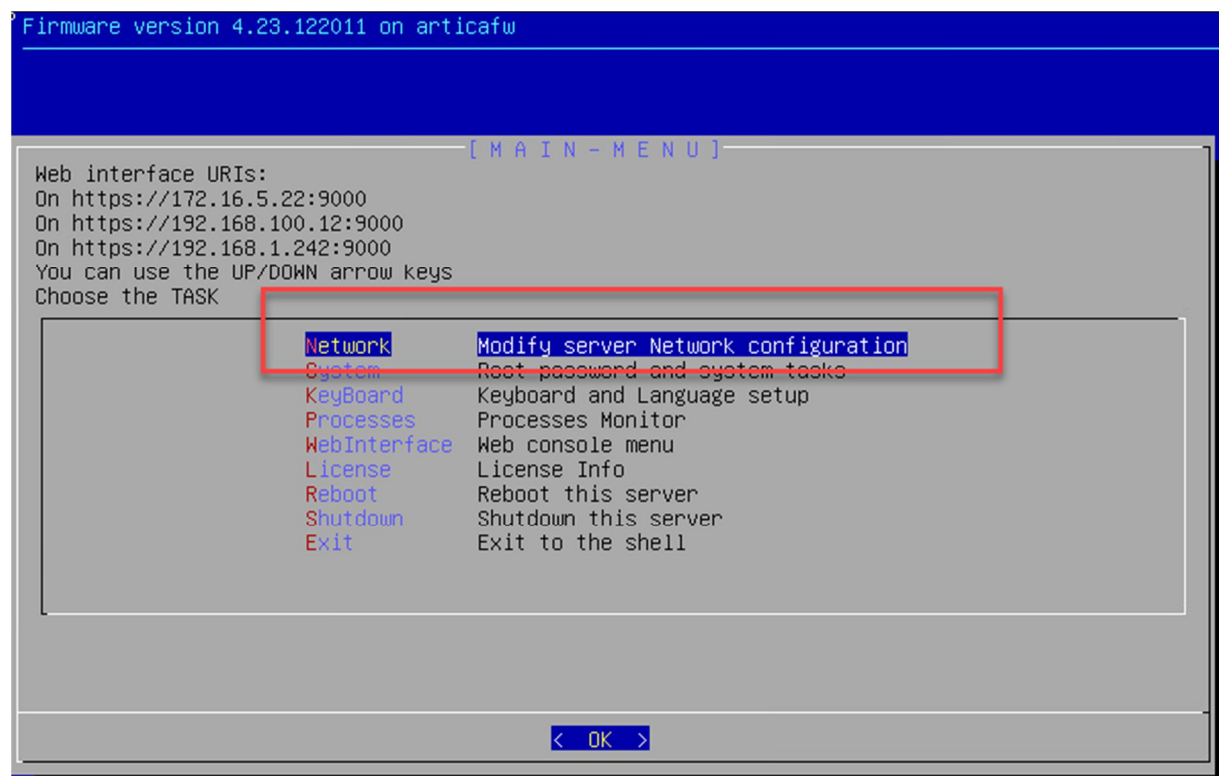


If the Firewall is active, you can use the button “**Stop**” to stop the firewall and “**Restart**” to reset and reconfigure the firewall.



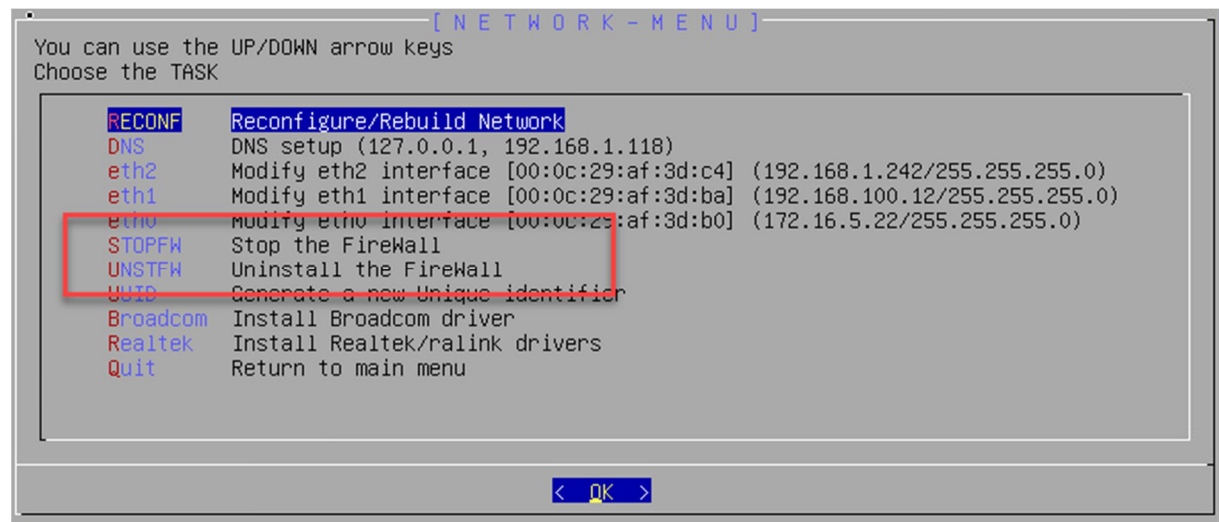
Start/stop via the system console

On the system console , select the “Network” menu



If the firewall is installed, you can stop the firewall or uninstall the firewall service.

If the firewall is not installed, you can install the firewall service.



Status, size and packets.

In the rules table, a rule can be inactive or active, inactive means the rule is not in production mode or as been refused for incompatibility issue.

If a rule is applied and matches any packets, you will see in the rules table the sum of packets and packets size passed through the rule.

Order/id	Rule Name	Network Interface	Status	Packets	Size	Type	Enabled	Order	Delete
1/1	Allow SSH For inbound objects My Net (3 Items) and To everything and Service «ssh» then Accept and Log all events All times	Interface eth2 (eth2)	Active	1 249	350 Bytes	IN LOG PASS	✓	↑ ↓	

Log rule events

If you need to trace a rule, on the rule setting, enable the **Log All Events** option

Rule: 1 Allow SSH ACCEPT

Rule Firewall services Inbound object Outbound object Deep Packet Inspection Time restriction

Rule 1) eth2::Allow SSH

If you enable the outgoing rule option, then this rule is applied from the server itself to the destination network/service.

Outgoing Rule: ☐ OFF

Rule Name: Allow SSH

Enabled: ☒ ON

Order: 1

Network Interface: Network Interface:eth2 - Interface eth2

Service: ssh tcp/22

☐ Drop ☒ Accept ☐ Mark TCP packets

Log All Events: ☒ ON

A stamp "LOG" will be displayed in the table. If the stamp is grey, this means the event rule is **not active**.

Order/id	Rule Name	Network Interface	Status	Packets	Size	Type	Enabled	Order	Delete
1/1	Allow SSH For inbound objects MyNet (3 Items) and To everything and Service «ssh» then Accept and Log all events All times	Interface eth2 (eth2)	Active	0	0 Bytes	IN LOG PASS	<input checked="" type="checkbox"/>	↑ ↓	

If the stamp is **turquoise blue**, then the LOG rule is **active**.

Order/id	Rule Name	Network Interface	Status	Packets	Size	Type	Enabled	Order	Delete
1/1	Allow SSH For inbound objects MyNet (3 Items) and To everything and Service «ssh» then Accept and Log all events All times	Interface eth2 (eth2)	Active	1 082	300 Bytes	IN LOG PASS	<input checked="" type="checkbox"/>	↑ ↓	

Display events

The events section allows you to display events (rules with events enabled) in order to see which node are allowed or denied.

If you want to find a specific rule, type in the search field **ACCEPT_[ruleid]** or **DROP_[ruleid]** as ruleid is the numeric ID of your firewall rule. Except defaults rules as:

- -999 The default rule according to policy
- -998: MALFORMED BAD
- -997: MALFORMED XMAS
- -996: SYN FLOOD
- -995: ICMP FLOOD
- -994: NEW TCP w/o SYN
- -993: DHCP Query
- -992: Artica Web console
- -991: MALFORMED NULL

Firewall events (syslog)

today this hour protocol tcp 50 events Go!

Date	Rule	OUT	Source IP address	source port	OUT	Destination IP(s)	Destination port
2019-12-09 09:51:14	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	54040	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:51:10	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	54040	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:51:14	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	54040	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:51:10	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	52110	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:51:10	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	52110	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:51:10	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	52110	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:51:10	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	52110	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:51:04	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	54040	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:51:04	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	54040	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:51:03	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	54040	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:51:02	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	54040	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:51:02	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	54040	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:50:47	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	54040	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:50:45	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	52110	-	192.168.1.242 00:0c:29:af:3d:c4	22
2019-12-09 09:50:45	PASS Allow SSH eth2 - Interface eth2	-	192.168.1.48 d4:3b:04:b6:87:35	52110	-	192.168.1.242 00:0c:29:af:3d:c4	22

Remote log/syslog server

You can send all firewall event to a log server using syslog (or to an Artica server act as syslog server)

To use this feature, you need a valid Enterprise license

- On the left menu, choose “Your Firewall” / “Parameters”
- Turn on the **Send Events by Syslog** option.
- Set the IP address of your **Syslog server** and the **remote udp or tcp port**.
- If your remote server use TCP protocol,

Firewall parameters v1.8.2

Interfaces Options Modules

Global rules

DNS Amplification DDOS Protection: ☐ OFF

Log All Events: ☐ OFF

Remote Syslog server

Send Events By Syslog: ☒ ON

Do Not Store Events Locally: ☐ OFF

Remote Syslog Server: 192.168.1.153

Listen Port: 514

Enable TCP/IP Sockets: ☐ OFF

Use SSL: ☐ OFF

Certificate: None

Logs storage

If your remote syslog server accept only SSL, turn on the “**Use SSL**” option and select a client certificate from the certificate center.

By default, events are stored locally on the Artica Firewall and are sent to the syslog server.

If you want to store events only on the syslog server, click on “**Do not store Events locally**”. In this case no event will be generated on the Firewall itself and display events feature will hidden on the Artica Interface.

If the target syslog server is an Artica, you will be able to see firewall events trough the Artica Web console on the Artica server that acts as the syslog server

Dashboard

Your system

Network

Active Directory

DNS

Databases

Logs center

Logs Viewer

Legal logs

Syslog Daemon service

DNS Queries

Firewall

Firewall events (syslog)

today this hour protocol tcp 50 eventsGo!

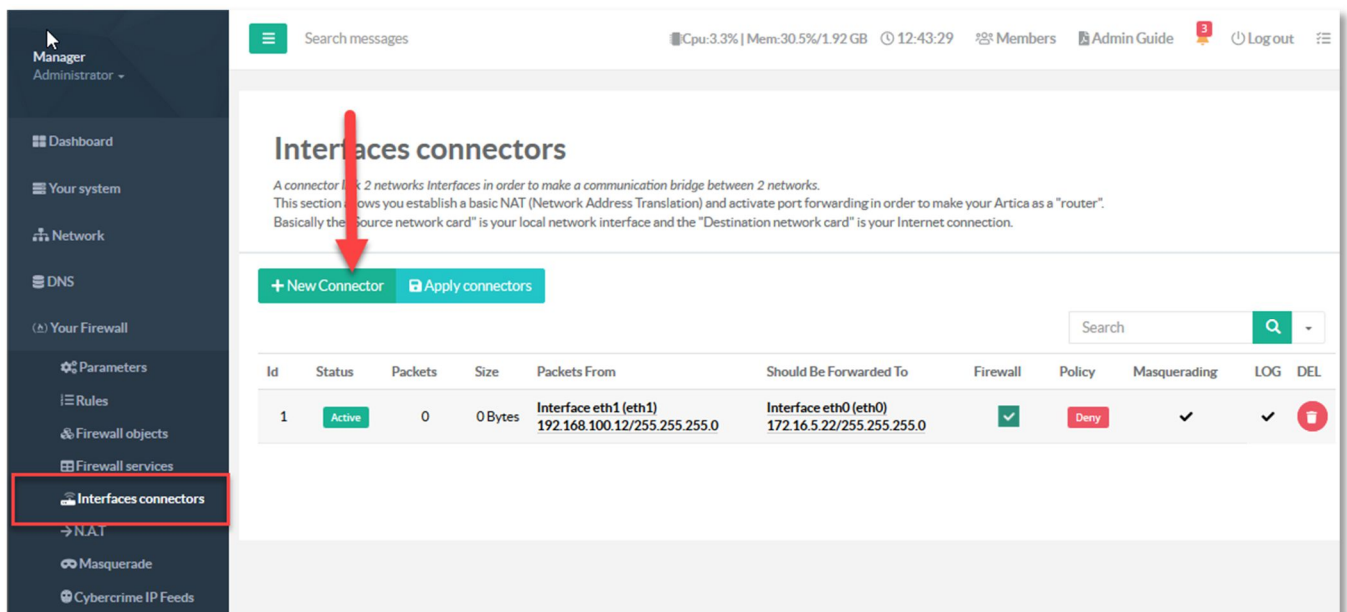
Date	Rule	IN	Source IP address	source port	OUT	Destination IP(s)	Destination port
2020-01-04 14:23:10	FORWARD	Unknown (1)	eth0 - Interface eth0172.16.5.20 00:0c:29:e1:74:b3	3693	eth2 - Interface eth2	192.168.1.46 00:0c:29:af:3d:b0	13000
2020-01-04 14:23:10	FORWARD	Unknown (1)	eth0 - Interface eth0172.16.5.20 00:0c:29:e1:74:b3	3693	eth2 - Interface eth2	192.168.1.46 00:0c:29:af:3d:b0	13000
2020-01-04 14:23:09	FORWARD	Unknown (1)	eth0 - Interface eth0172.16.5.20 00:0c:29:e1:74:b3	3693	eth2 - Interface eth2	192.168.1.46 00:0c:29:af:3d:b0	13000
2020-01-04 14:23:09	FORWARD	Unknown (1)	eth0 - Interface eth0172.16.5.20 00:0c:29:e1:74:b3	3693	eth2 - Interface eth2	192.168.1.46 00:0c:29:af:3d:b0	13000
2020-01-04 14:23:09	PASS	Unknown (1)	eth2 - Interface eth2192.168.1.20 d4:3b:04:b6:87:35	61923	-	192.168.1.242 00:0c:29:af:3d:c4	22
2020-01-04 14:23:09	PASS	Unknown (1)	eth2 - Interface eth2192.168.1.20 d4:3b:04:b6:87:35	61923	-	192.168.1.242 00:0c:29:af:3d:c4	22
2020-01-04 14:23:09	PASS	Unknown (1)	eth2 - Interface eth2192.168.1.20 d4:3b:04:b6:87:35	61923	-	192.168.1.242 00:0c:29:af:3d:c4	22
2020-01-04 14:23:09	PASS	Unknown (1)	eth2 - Interface eth2192.168.1.20 d4:3b:04:b6:87:35	61923	-	192.168.1.242 00:0c:29:af:3d:c4	22
2020-01-04 14:23:09	PASS	Unknown (1)	eth2 - Interface eth2192.168.1.20 d4:3b:04:b6:87:35	61923	-	192.168.1.242 00:0c:29:af:3d:c4	22

INTERFACES CONNECTORS

A connector link 2 networks Interfaces in order to make a communication bridge between 2 networks.
A connector definition consists of a set of rules for traffic passing through the host running the firewall

This section allows you establish a basic NAT (Network Address Translation) and activate port forwarding in order to make your Artica as a "router".

Basically the "Source network card" is your local network interface and the "Destination network card" is your Internet connection.



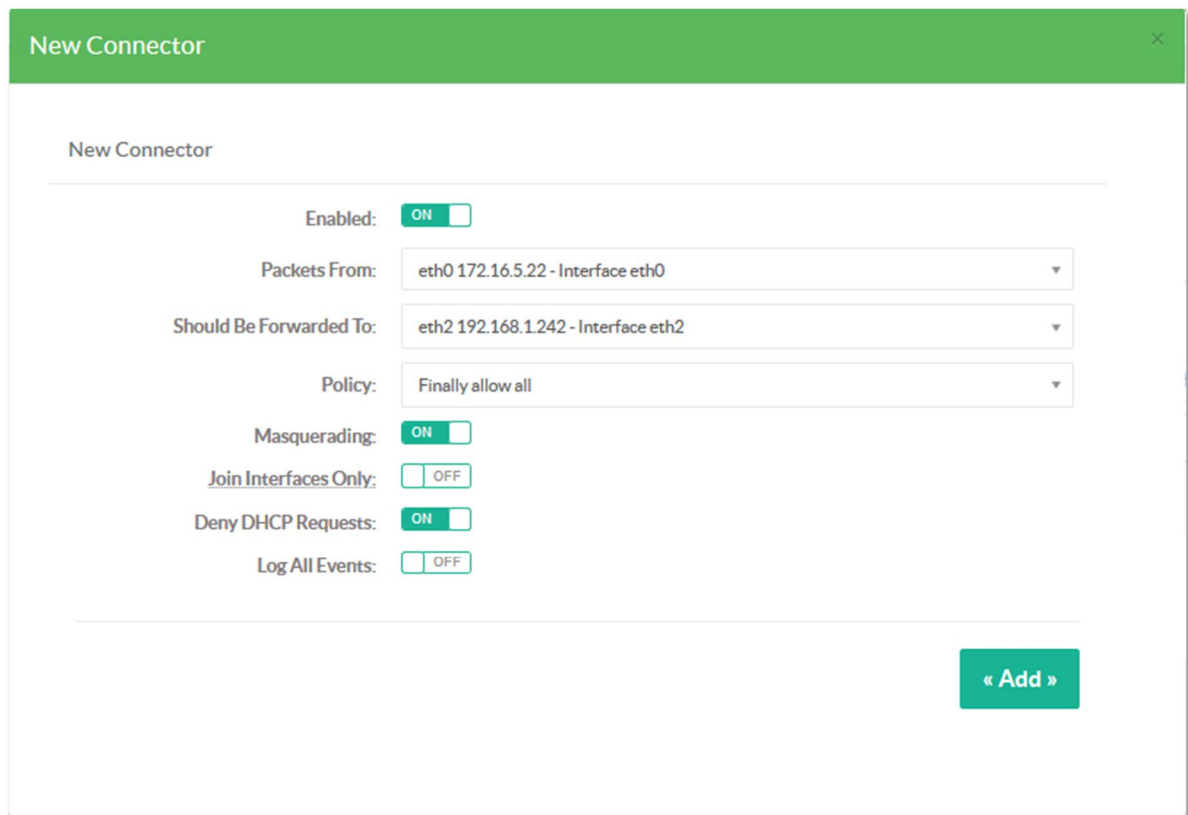
The screenshot displays the Mikrotik WinBox interface for managing firewall connectors. The left sidebar contains a menu with items like Dashboard, Your system, Network, DNS, Your Firewall, Parameters, Rules, Firewall objects, Firewall services, and Interfaces connectors (highlighted with a red box). The main content area is titled 'Interfaces connectors' and includes a description: 'A connector link 2 networks Interfaces in order to make a communication bridge between 2 networks. This section allows you establish a basic NAT (Network Address Translation) and activate port forwarding in order to make your Artica as a "router". Basically the "Source network card" is your local network interface and the "Destination network card" is your Internet connection.' Below the description are two buttons: '+ New Connector' and 'Apply connectors'. A red arrow points to the '+ New Connector' button. Below the buttons is a table with the following data:

Id	Status	Packets	Size	Packets From	Should Be Forwarded To	Firewall	Policy	Masquerading	LOG	DEL
1	Active	0	0 Bytes	Interface eth1 (eth1) 192.168.100.12/255.255.255.0	Interface eth0 (eth0) 172.16.5.22/255.255.255.0	✓	Deny	✓	✓	✖

A connector can be displayed in the Firewall rules section, with a connector, your are allowed to specify which packets are allowed or denied to be forwarded

Create an interface connector

When adding a new Interface connector you have to define the direction of the packets flow. Means from which interface and from which interface packets are forwarded.



The screenshot shows a 'New Connector' configuration window. It has a green header bar with the title 'New Connector' and a close button. The main area is white and contains several configuration options:

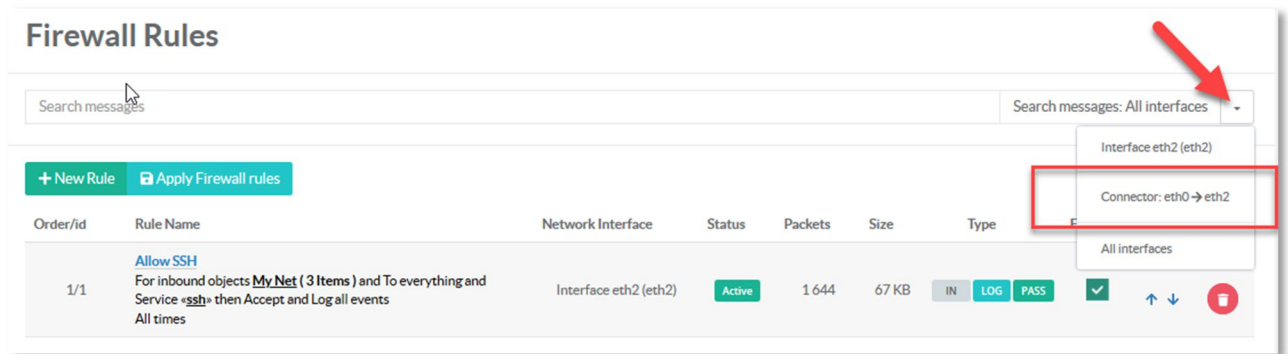
- Enabled:** A toggle switch set to 'ON'.
- Packets From:** A dropdown menu showing 'eth0 172.16.5.22 - Interface eth0'.
- Should Be Forwarded To:** A dropdown menu showing 'eth2 192.168.1.242 - Interface eth2'.
- Policy:** A dropdown menu showing 'Finally allow all'.
- Masquerading:** A toggle switch set to 'ON'.
- Join Interfaces Only:** A toggle switch set to 'OFF'.
- Deny DHCP Requests:** A toggle switch set to 'ON'.
- Log All Events:** A toggle switch set to 'OFF'.

At the bottom right, there is a green button labeled '« Add »'.

- **Enabled:** Activate or disable the connector.
- **Packets From:** Source Network interface.
- **Should be Forwarded to:** The destination interface.
- **Policy:** the default policy (everything are denied or allowed)
- **Masquerading:** Masquerade packets from the outgoing interface if you want to specify what to MASQUERADE, see Masquerade section.
- **Join interfaces only:** Disable Firewall rules based on this connector
- **Deny DHCP requests:** Deny any DHCP broadcast pass through this connector.
- **Log all events:** Add connector events in the global Log rule events.

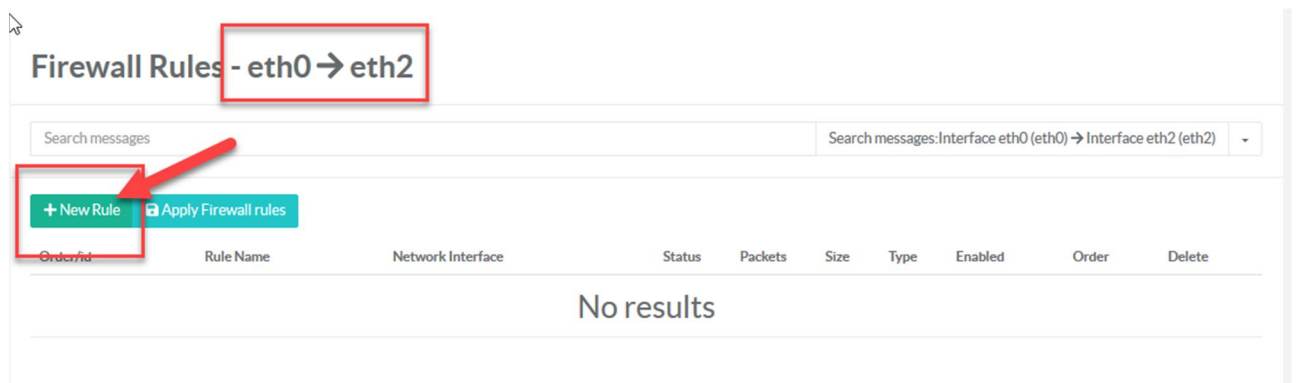
Create rules for an interface connector.

In the rules section, Click on the drop-down button in order to choose the connector.



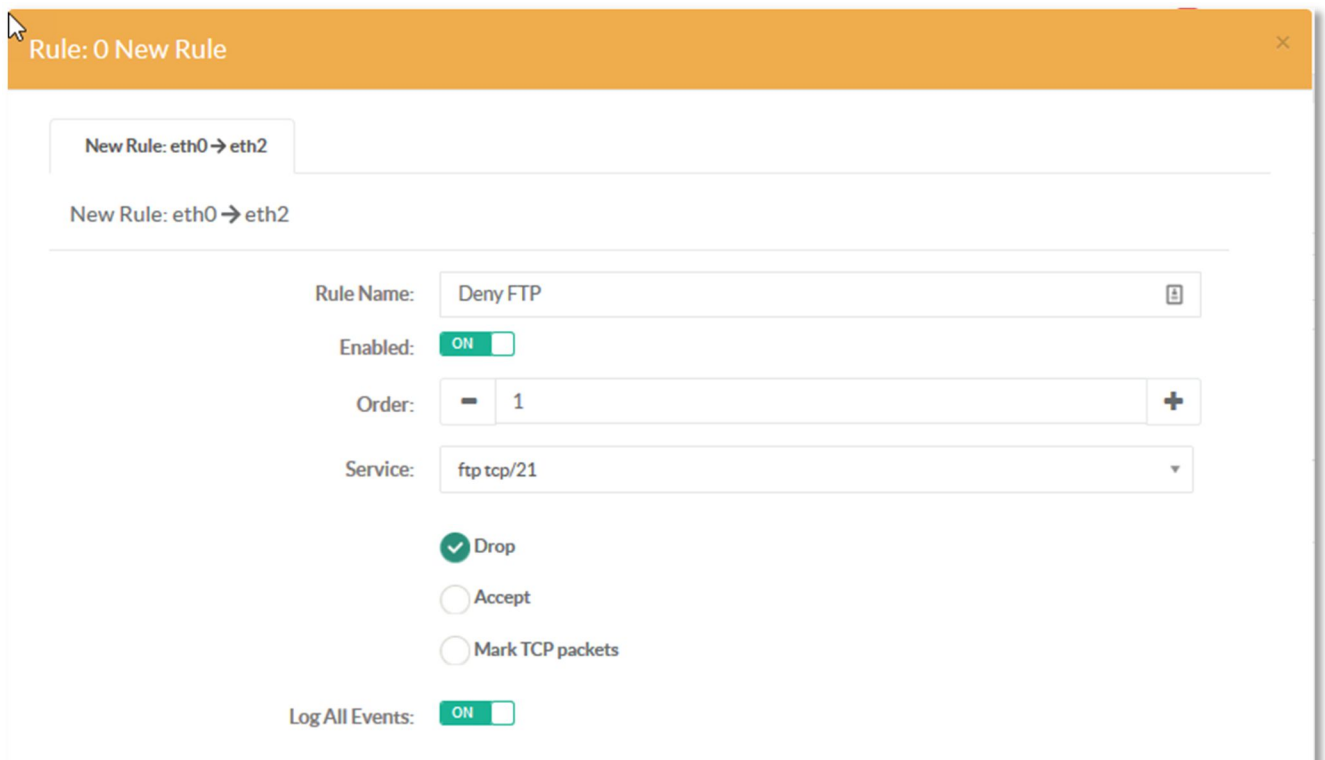
The screenshot shows the 'Firewall Rules' page. At the top, there is a search bar and a dropdown menu labeled 'Search messages: All interfaces'. A red arrow points to this dropdown, which is open, showing options: 'Interface eth2 (eth2)', 'Connector: eth0 → eth2' (highlighted with a red box), and 'All interfaces'. Below the dropdown, there is a table of firewall rules. The first rule is 'Allow SSH' with a status of 'Active' and a network interface of 'Interface eth2 (eth2)'.

The table will switch to selected rules for your connector.
Click on **New rule** button.



The screenshot shows the 'Firewall Rules - eth0 → eth2' page. The title 'Firewall Rules - eth0 → eth2' is highlighted with a red box. Below the title, there is a search bar and a dropdown menu labeled 'Search messages: Interface eth0 (eth0) → Interface eth2 (eth2)'. A red arrow points to the '+ New Rule' button, which is also highlighted with a red box. Below the button, there is a table with columns: Order/id, Rule Name, Network Interface, Status, Packets, Size, Type, Enabled, Order, and Delete. The table is currently empty, displaying 'No results'.

Create the rule according to the same behavior as a standard firewall rule.



The screenshot shows the 'Rule: 0 New Rule' configuration window. The title bar is orange and says 'Rule: 0 New Rule'. Below the title bar, there is a section for 'New Rule: eth0 → eth2'. The configuration fields are as follows:

- Rule Name: Deny FTP
- Enabled: ☒ ON
- Order: 1
- Service: ftp tcp/21
- Action: ☒ Drop, ☐ Accept, ☐ Mark TCP packets
- Log All Events: ☒ ON

NAT (NETWORK ADDRESS TRANSLATION) RULES

The N.A.T section

Nat rules allows you to forward packets to a specific destination. Destinations and forward behaviors are defined in NAT section.

This section is only used to define the main rule behavior, others details (sources addresses, destination addresses...) are defined in the rules section.

Create a destination NAT.

The first step is to create your NAT destination. On the left menu, click on NAT link. On the table, click on "New rule"

The screenshot displays the 'Network address translation' section of a firewall configuration tool. On the left, a sidebar menu shows 'NAT' selected under 'Interfaces > Connectors'. The main area features a table with one rule: 'Redirect to the node' on 'Interface eth0 (eth0)' pointing to '172.16.5.20:3389'. A 'New Rule' button is highlighted. Below, the 'New Rule' dialog is open, showing configuration options: 'Enabled' (ON), 'Type' (Redirect to the node), 'Network Interface' (Network Interface:eth0 - Interface eth0), 'Destination Address' (192.168.1.25), 'Destination Port' (3389), and 'Log All Events' (ON). An 'Add' button is at the bottom right.

Id	Type	Network Interface	Destination	LOG	DEL
1	Redirect to the node	Interface eth0 (eth0)	172.16.5.20:3389	✓	✗

Rule:

New Rule

Enabled: ☒ ON

Type: Redirect to the node

Network Interface: Network Interface:eth0 - Interface eth0

Destination Address: 192.168.1.25

Destination Port: 3389

Log All Events: ☒ ON

Add

Enabled: Activate/ disable the Main rule.

Network Interface:

The inbound interface that accept the rule.

Destination address: The IP address that Will receive packets.

Destination Port: The listen port of the targeted service.

Log All events: Add in the log section all events related to this NAT rule.

NAT behaviors

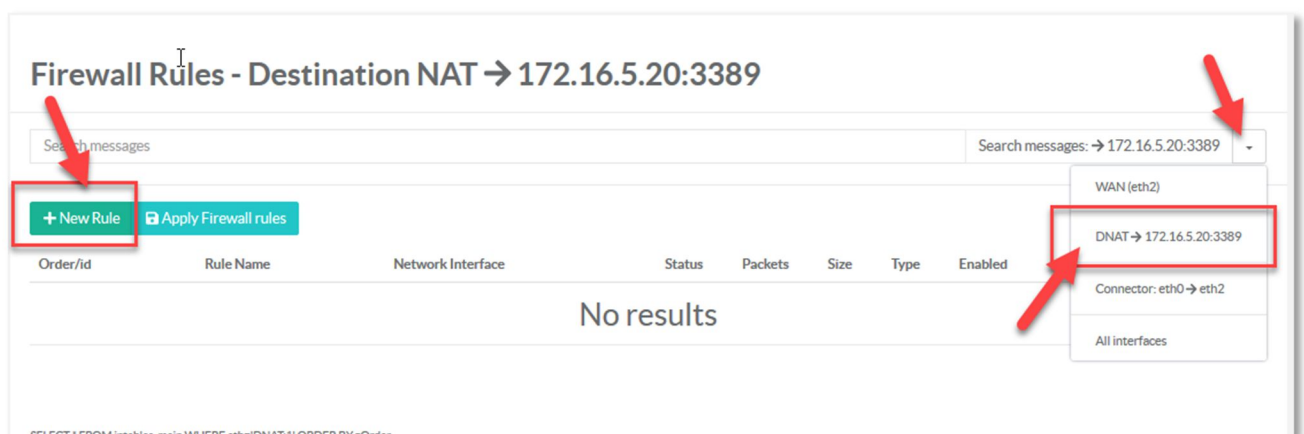
You have 3 main NAT behaviors:

- **Destination NAT:**
Defines a Destination NAT (DNAT). Commonly thought of as port-forwarding (where packets destined for the firewall with a given port and protocol are sent to a different IP address and possibly port), DNAT is much more flexible in that any number of parameters can be matched before the destination information is rewritten.
This is the most used NAT where you redirect a requested port to a destination and port.
- **Source NAT:**
Defines a Source NAT (SNAT). SNAT is similar to masquerading but is more efficient for static IP addresses.
You can use it to give a public IP address to a host which does not have one behind the firewall
- **Redirect to the node:**
Redirect matching traffic to the local machine.
This is typically useful if you want to intercept some traffic and process it on the local machine

Affect firewall rules to a destination NAT.

After adding your main NAT rule, click on **Rules** on the left menu.

In the rules section, Click on the drop-down button in order to choose the main NAT rule

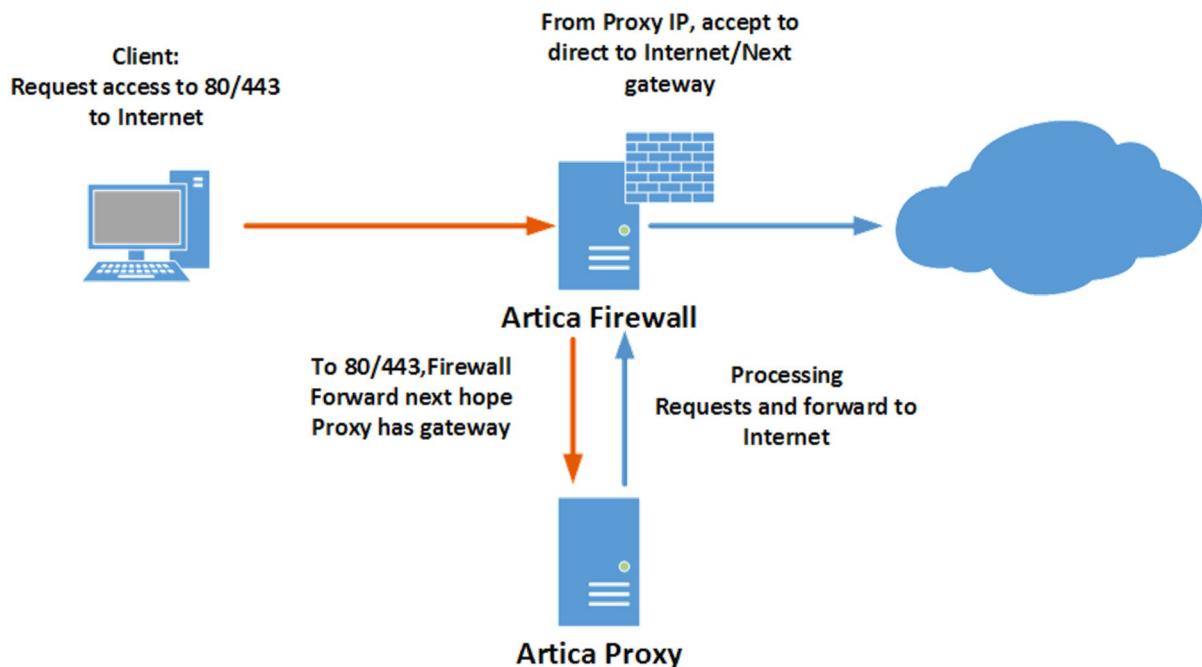


Click on **New rule** in order to define the context of your NAT rule.

Route packets to a node

Route packets to a node allows you to forward TCP packets to a specific remote gateway.

It is most commonly used when you want to route HTTP/HTTPS packets to a transparent proxy but it's working for any port.



- On the NAT section, create a rule and type to "Route packets" to a node.
- Choose the Interface that will receive packets.
- Set the IP address on the Destination Address.

Rule:

Rule 5) ::Route packets to a node

Enabled: ☒ ON

Type:

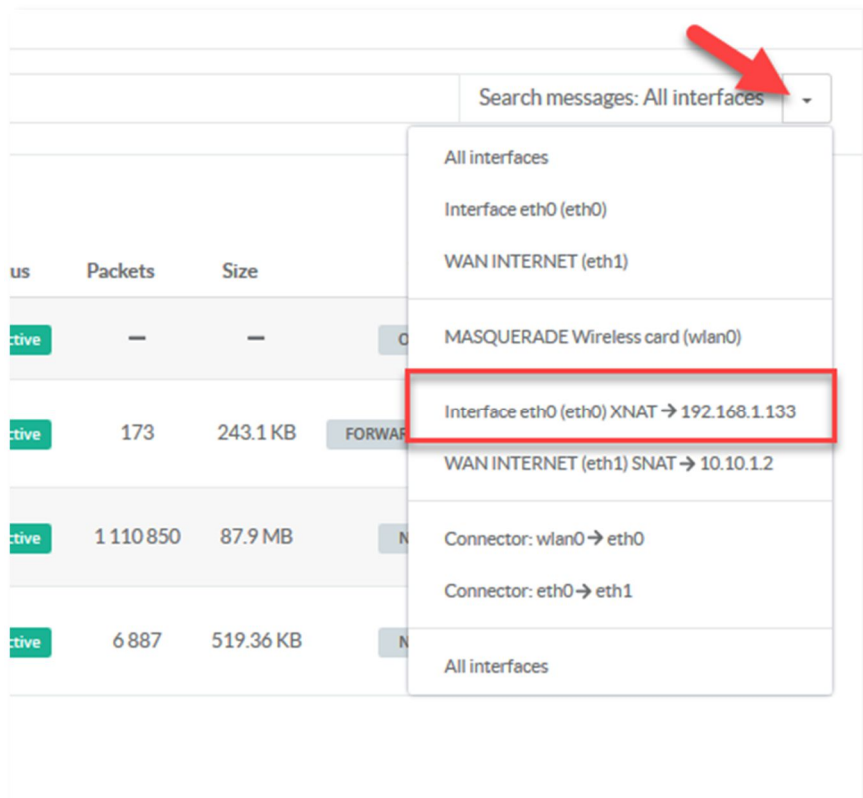
Network Interface:

Destination Address:

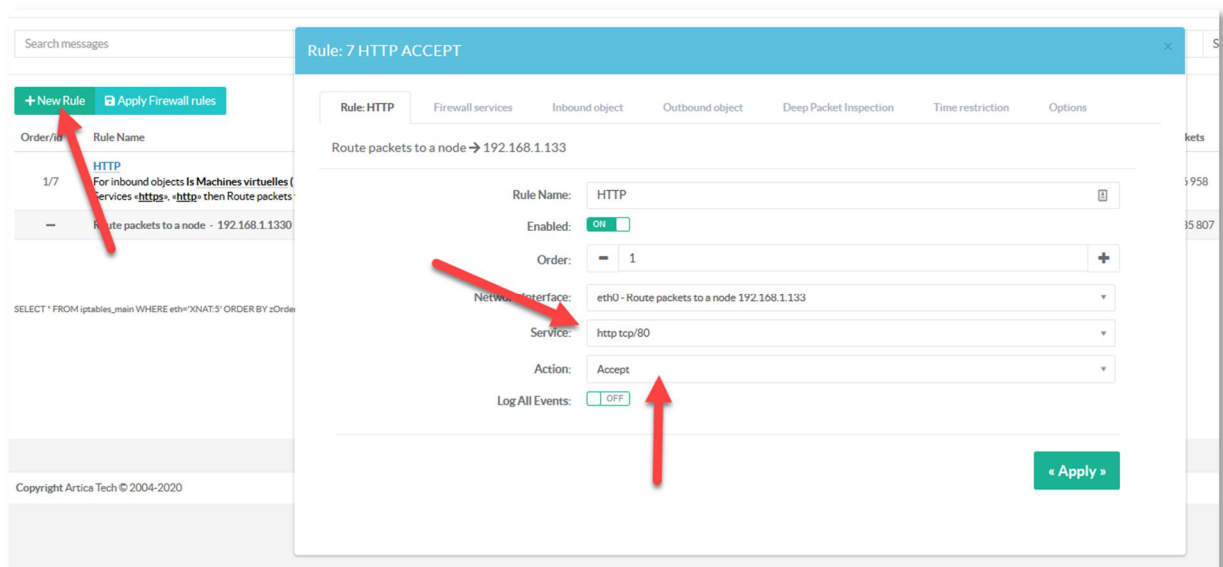
Destination Port:

Log All Events: ☐ OFF

Go to the Firewall rules section, in the drop-down list, near the search field, choose the “XNAT” rule



Create a rule that “Allow” for service HTTP/HTTPs and set the source IP addresses object.



In this way, this firewall rule force the firewall to route packets to the next gateway with transparent proxy.

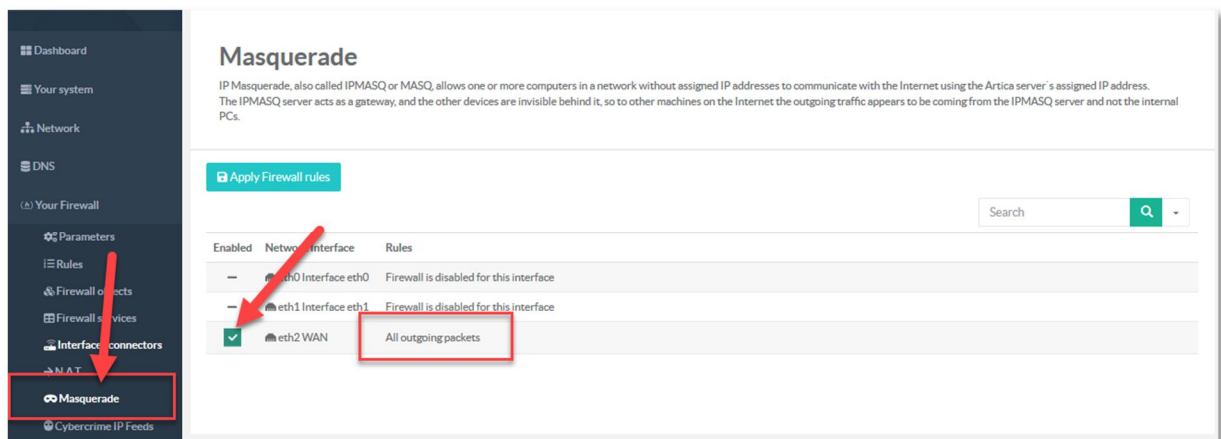
MASQUERADE

IP Masquerade, also called IPMASQ or MASQ, allows one or more computers in a network without assigned IP addresses to communicate with the Internet using the Linux server's assigned IP address.

The IPMASQ server acts as a gateway, and the other devices are invisible behind it, so to other machines on the Internet the outgoing traffic appears to be coming from the IPMASQ server and not the internal PCs

Define the Network outgoing interface to masquerade.

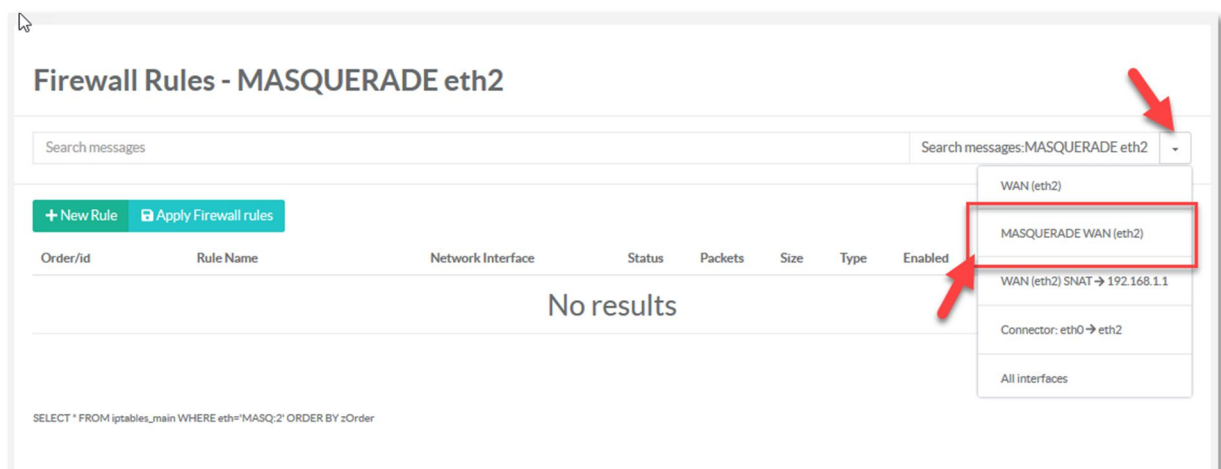
The masquerade feature allows you to enable the output interface for masquerading but also create specific firewall rules.



If no rule is specified, Artica will understand that all outgoing packets must be masqueraded

Create firewall Masquerade rules.

- Once the network interface as been defined, go into the **Rules** section
- On the drop-down icon, choose the “**MASQUERADE [interface]**” item.
- Click on **New rule** in order to create your rule.



OUTGOING RULE FOR THE ARTICA SERVER ITSELF

To ensure the Artica server can connect to some destination, a specific outgoing default rule is displayed

Order/id	Rule Name	Network Interface	Status	Packets	Size	Type	Enabled	Order	Delete
0/0	Default Allow this server to establish communications to 119 remote nodes. Autorise Ping OVH	All interfaces	Active	—	—	OUT PASS	✓	—	—

When clicking on this rule, only one object can be managed.
Some items cannot be removed because remote addresses are used by Artica to retrieve information/updates
To add a new entry, click on “New item”

Outgoing rule

[+ New item](#) [Compile rules](#)

[Go!](#)

Address	Delete
147.135.249.253:tcp:443 [2020-01-11 20:14:24] Default by Artica Tech on	—
147.135.249.253:tcp:21 [2020-01-11 20:14:24] Default by Artica Tech on	—
147.135.249.253:tcp:80 [2020-01-11 20:14:24] Default by Artica Tech on	—
35.231.145.0/24:tcp:443 [2020-01-11 20:14:24] Default by Artica Tech on	—
35.231.145.0/24:tcp:21 [2020-01-11 20:14:24] Default by Artica Tech on	—

Address field: can be a single IP address or a network using CIDR notation.

Listen port:

The [proto:]port part of the elements may be expressed in the following forms

portnumber[-portnumber]

TCP port or range of ports expressed in TCP port numbers (80 or 1024-1030 for 1024 to 1030 port

Proto can be any of tcp, sctp, udp, udplite

Outgoing rule:New item

New item

Address: 192.168.1.0/24

Listen Ports: tcp:80

Comment: LAN 3

[« Cancel »](#) [« Add »](#)

TRAFFIC SHAPING

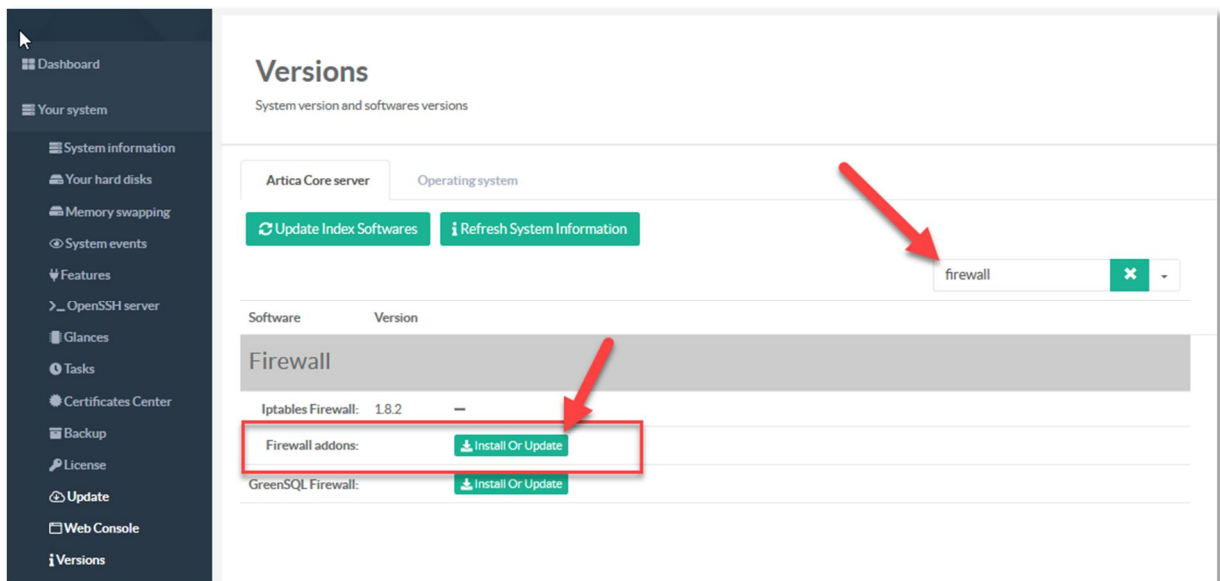
This module is An high-performance implementation of committed access rate, or simply rate limiting, or policing.

By default, this module is limited to 10 000 IP addresses.

If you plan to use for more, contact the support team.

Install the Firewall addons module.

- On “Your system”, select the menu “Versions”
- On the search field, type “firewall”
- If you did not have any version on the **Firewall addons** row, this means you have to install it.



- Click on **Install or Upgrade** button

Create a rule for traffic shaping

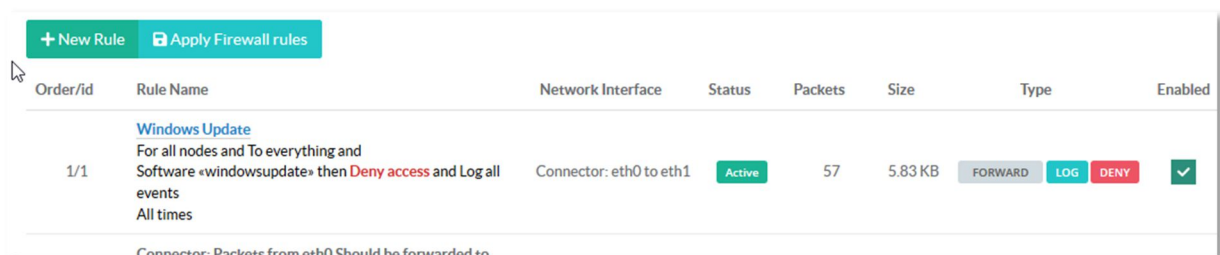
- Return back to your Firewall rules
- Create a “**deny**” rule or choose a **deny** rule you want to enable traffic shaping
- Select the rule in order to open the “**Options**” tab.

In most cases you want to shape “FORWARD” packets, means rules defined for Interfaces connectors.

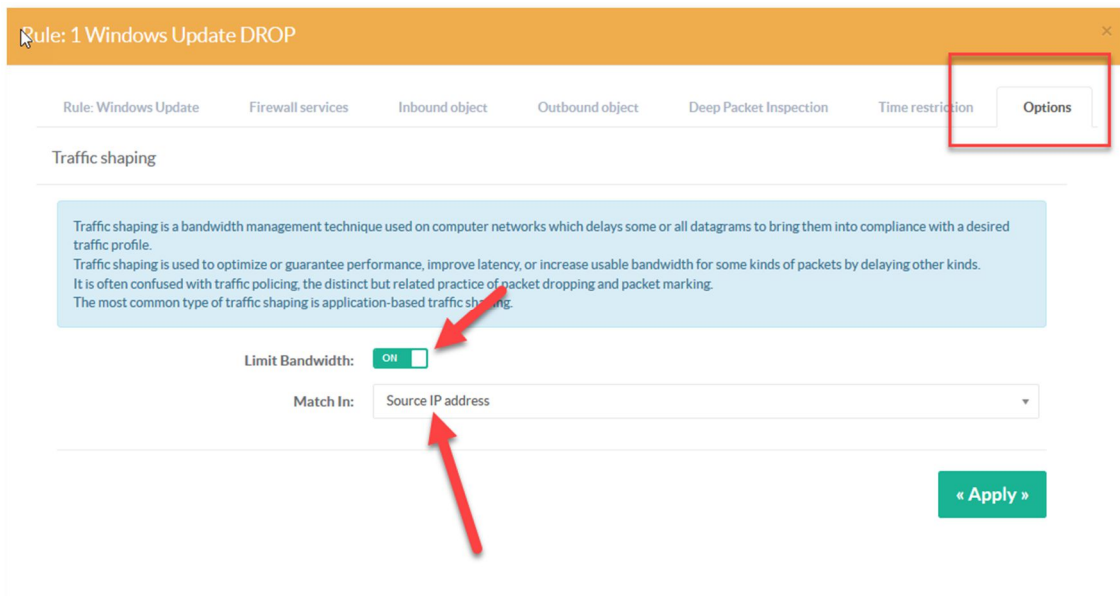
If you 2 network interfaces, this should be from the LAN interface to the WAN interface.

If you have only one interface and use Artica as single gateway, this should be FROM the Interface to the same interface.

In our example, we use a rule inside the connector LAN -> WAN that deny the application “Windowsupdate”



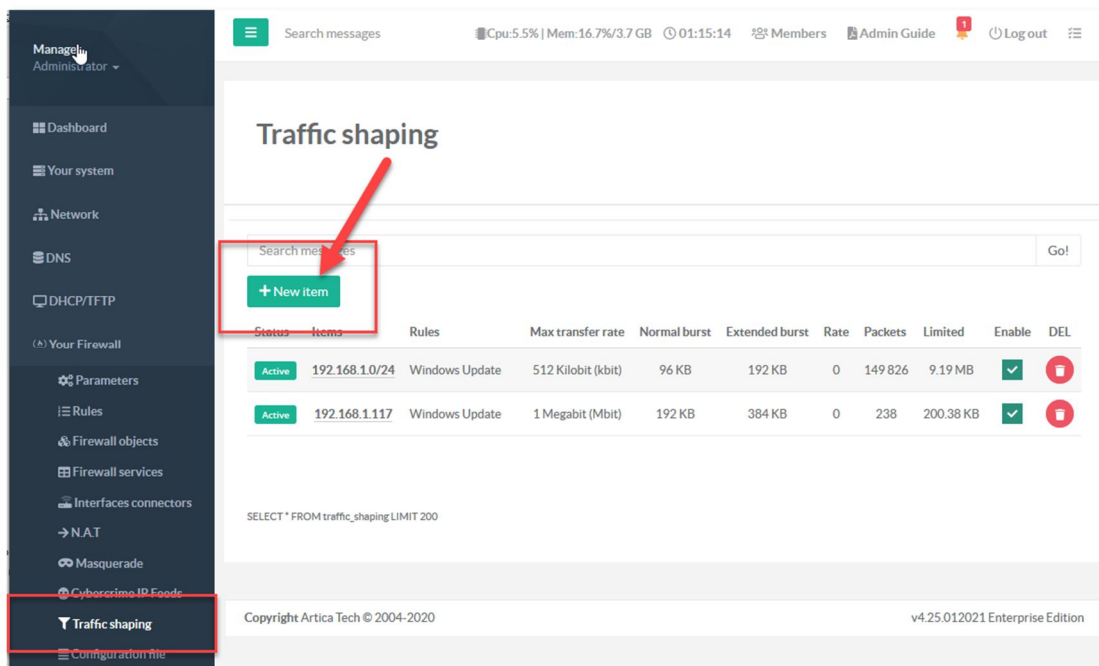
- Select the **Options** tab
- Under Traffic shaping section, turn on the “**Limit Bandwidth**” checkbox.
- Defines which element will matches the rule(Source IP address or destination IP address).



Mandatory, define traffic shaping elements.

You have 2 method to add items that will matches the main rule for reduce bandwidth.

- 1) The Global section “Traffic shaping” that allows you to add an item and choose which rule will matches this item.



- 2) By clicking on the explain inside the limit traffic rule that will display only elements for the defined rule.

The screenshot shows the 'Firewall Rules' management interface. A modal window titled 'Traffic shaping Items' is open, displaying a table of items. A red arrow points to the 'Status' column of the table, and another red arrow points to the 'Limit traffic' text in the rule description of the background interface.

Status	Items	Rules	Max transfer rate	Normal burst	Extended burst	Rate	Packets	Limited	Enable	DEL
Active	192.168.1.0/24	Windows Update	512 Kilobit (kbit)	96 KB	192 KB	538.25 KB/s	314 743	18.34 MB	✓	✗
Active	192.168.1.117	Windows Update	1 Megabit (Mbit)	192 KB	384 KB	0	238	200.38 KB	✓	✗

When adding a new element, define the **Address** that will matches the rule (in CIDR format or IP address) format.

Set the **Max Transfer rate** using the Unit drop-down field to define if the limit is in bit, kilobit, megabit.

When adding/editing/deleting an item, rules are automatically applied (it is not necessary to compile rules after)

The screenshot shows the 'New entry' form for adding a new item. The form includes a text input for the item name, a text input for the address, a numeric input for the max transfer rate, and a dropdown menu for the unit. A green 'Add' button is at the bottom right.

New item

Windows Update

Address: 192.168.1.0/24

Max Transfer Rate: 512

Unit: Kilobit (kbit)

« Add »