

How to block/allow IPs country wise on your firewall

How to block/allow IPs country wise on your firewall

In this document, we'll configure firewall rules to block incoming and outgoing IP requests from specific countries or country groups.

You can specify individual countries or create a group of countries by going to Definition -> Hosts -> Country Groups to add those group to the firewall policy as shown below:

The screenshot shows the 'Add Country Group' configuration window. The 'Country(s)' field is empty. The 'Available Country(s)' list includes Nicaragua, Niger, Nigeria, Niue, Norfolk Island, Northern Mariana Islands, Norway, Oman, and Palau. The 'Selected Country(s)' list contains China and Pakistan. There are 'Save' and 'Cancel' buttons at the bottom.

Group Name	Country(s)	Status	Tasks
Blockintruders	China, Pakistan	inactive	

Click on to move countries from Available Country(s) to Selected Country(s) and click on to move countries from Selected Country(s) field into Available Country(s) field.

For Outgoing Traffic

Go to Firewall -> Policies -> Rules

Direction	Source	Destination	NAT	Proxy-mode
Any	fwnet-LAN	cgr283928;cnt396151	NAT	<input type="checkbox"/> Proxy-mode

Select the countries or country groups you want to block or allow in the **Destination** from a popup window displayed below. Source can be selected as **FWNET LAN**.

Add the specific countries or country groups from “**Available Country Groups**” tab.

The country code will be displayed in the destination field as shown below.

Direction	Source	Destination	To
Any	fwnet-LAN	cgr283928,cnt396151	NAT

You can also specify the action to be taken in the “Action and logging” tab in the Action field by choosing to Allow, Drop or return the traffic coming from the specified countries or country groups.

Clicking on Accept will Allow all the traffic from the specified countries or country groups and clicking on Drop will block all the traffic from the specified countries or country groups.

Direction	Any	To	Any
Source	funet-LAN	NAT	ignore
Destination	cpr283928.cnt396151	NAT	nonat <input type="checkbox"/> Proxy-mode
Services and Ports			
Services	Any	NAT	No NAT
Usersense			
Enable UserSense	<input type="checkbox"/>		
Users and Groups			
BYOD Devices	All		
Action and Logging			
Action	Accept		
Time Schedule	Drop		
Log	Yes		
Comment			

After adding the countries and country groups and specifying the action to be taken, you can create this firewall rule and add it into the policies as per your requirement to allow or block traffic from IPs from specified countries.

You will have to install policies by going to Firewall -> Policies -> Install policies for the changes to be applicable.

For Incoming Traffic

Go to Firewall -> Policies -> Rules

Rules Port Forwarding DoS Settings MAC Binding MAC Filtering Install Policies			
Add Rules ⊞			
IP Version			
IP Version	IPv4		
Zones			
Direction	Any	To	Any
Source	cpr283928.cnt396151	NAT	ignore
Destination	Any	NAT	nonat <input type="checkbox"/> Proxy-mode

Select the countries or country groups you want to block or allow in the Source from a popup window displayed below. **Destination** can be selected as **ANY**

Add the specific countries or country groups from “**Available Country Groups**” tab.

Gajshield: Web based Administration and Management Tool - Google Chrome
 Not secure | https://192.168.2.127/cgi-bin/fwsouceaddwindow.cgi?uname=4375&show=all&stype=Source&field_id=firewallrules_source&showvals=cgr283928.cnt396151&ip_proto_src=IPv4

Add Source IPv4 Network Object(s)

Available Host(s) +	Available FQDN Host(s) +	Available Host-range(s) +	Available Network(s) +	Available Network-group(s)	Available CountryGroup(s) +
ADServer cmsserver fwip-LAN fwip-WAN GAJSHIELD LDAPServer cgr283928			fwnet-LAN fwnet-WAN internet		Country Groups Countries Afghanistan Aland Islands Albania Algeria American Samoa Andorra Angola Annunilla

Selected Source Network Objects

Afghanistan
BlockIntruders

Enter comma separated Source Network Objects (Except FQDN hosts)

The country code will be displayed in the source field as shown below.

Zones

Direction	Any	To	Any
Source	cgr283928.cnt396151	NAT	ignore
Destination	Any	NAT	nonat <input type="checkbox"/> Proxy-mode

You can also specify the action to be taken in the “Action and logging” tab in the Action field by choosing to Allow, Drop or return the traffic coming from the specified countries or country groups.

Clicking on Accept will Allow all the traffic from the specified countries or country groups and clicking on Drop will block all the traffic from the specified countries or country groups.

Direction	Any	To	Any
Source	cgr283928.cnt396151	NAT	ignore
Destination	Any	NAT	nonat <input type="checkbox"/> Proxy-mode

Services and Ports

Services	Any	NAT	No NAT
----------	-----	-----	--------

Usersense

Enable UserSense	<input type="checkbox"/>
Users and Groups	
BYOD Devices	All

Action and Logging

Action	Accept
Time Schedule	
Log	Yes
Comment	

After adding the countries and country groups and specifying the action to be taken, you can create this firewall rule and add it into the policies as per your requirement to allow or block traffic from IPs from specified countries.

NOTE: You will have to install policies by going to Firewall -> Policies -> Install policies for the changes to be applicable.

Thus, you have learnt how to allow/block incoming and outgoing traffic from specific country IPs in your firewall.