GAJSHIELD

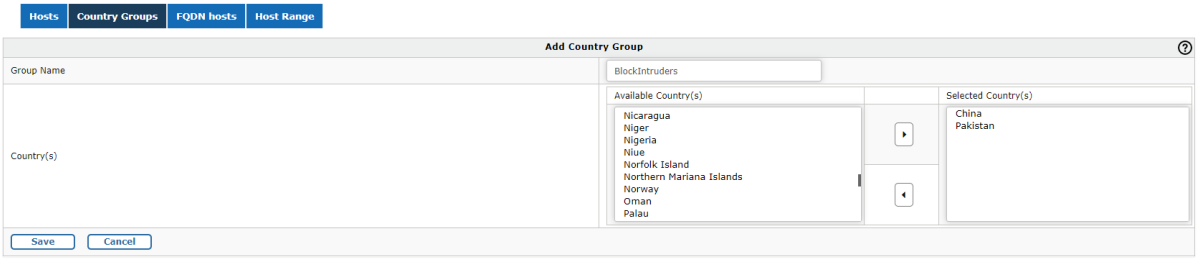
Data Security Firewall

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.

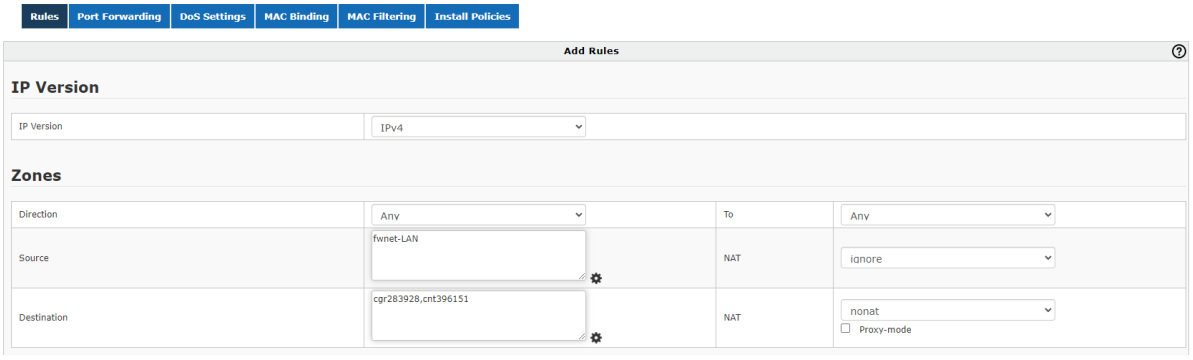
You can specify individual countries or create a group of countries by going to Definition -> Hosts -> Country Groups to add those group to the firewall policy as shown below:



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.

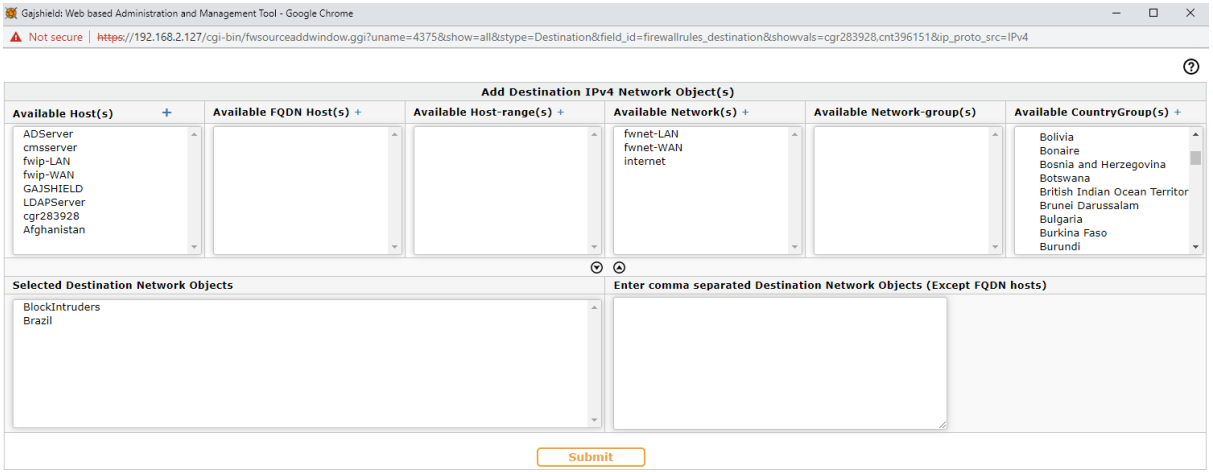
For Outgoing Traffic

Go to Firewall -> Policies -> Rules



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**.

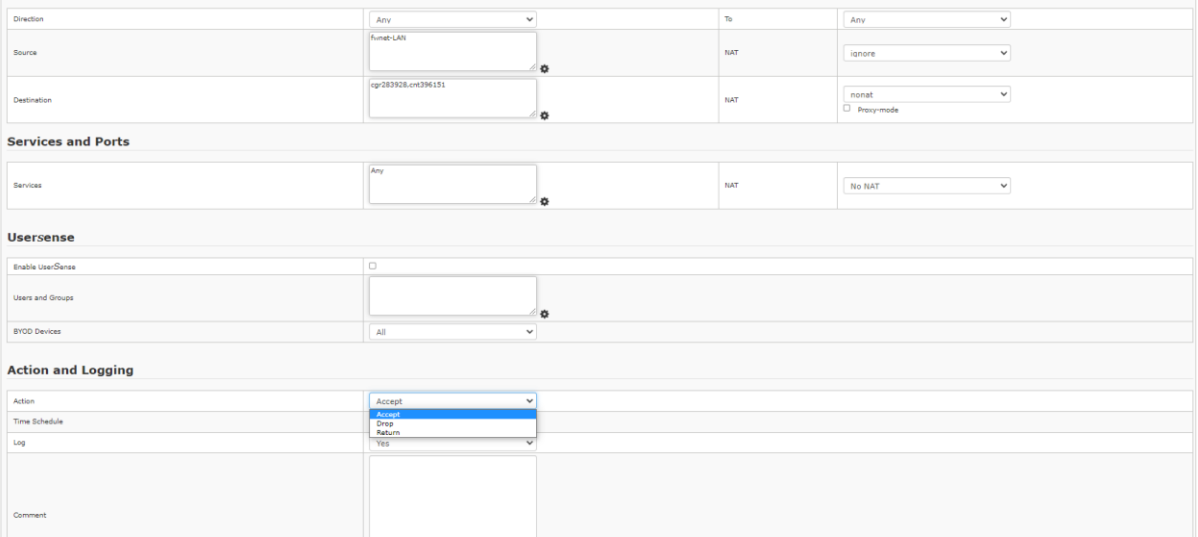
Add the specific countries or country groups from “**Available Country Groups**” tab.



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

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.

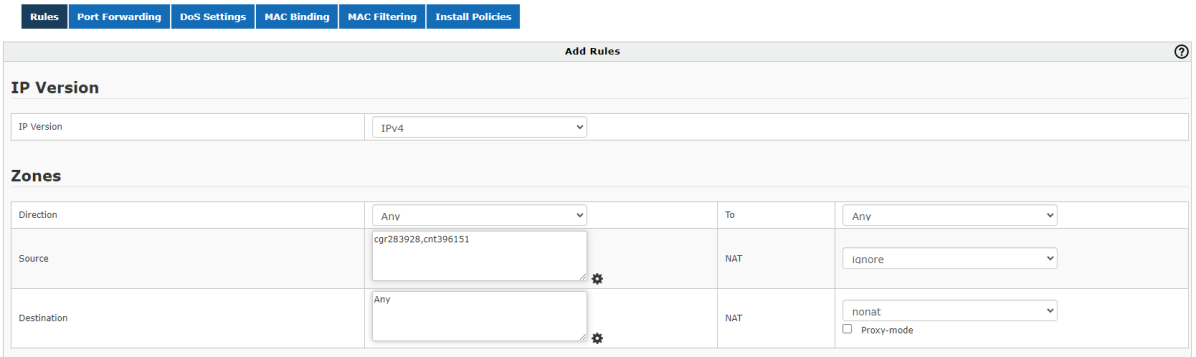


After adding the countries and country groups and specifying the action to be taken, you can create this firewall rule and add it into the policies as per your requirement to allow or block traffic from IPs from specified countries.

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

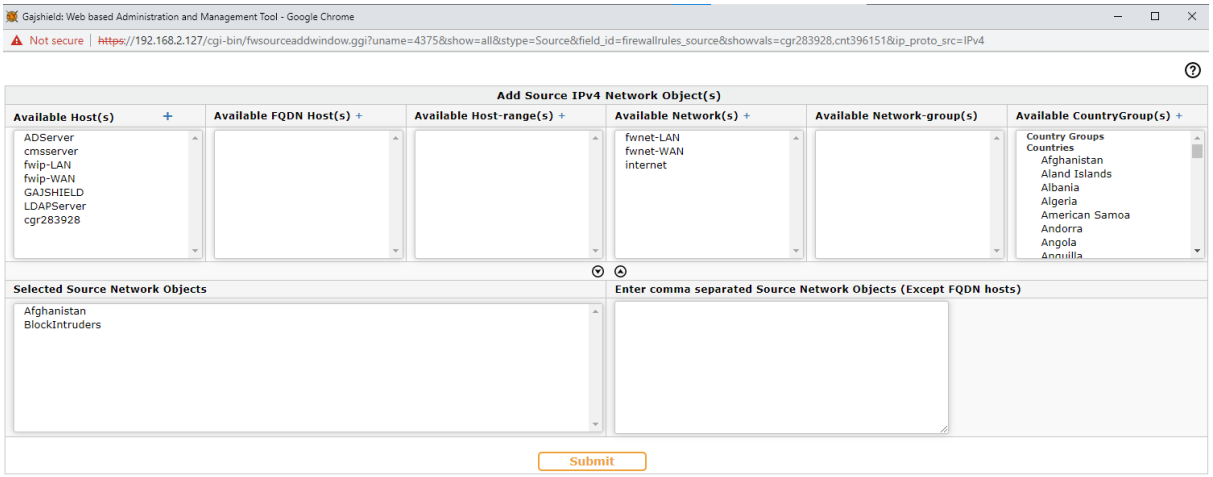
For Incoming Traffic

Go to Firewall -> Policies -> Rules



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**

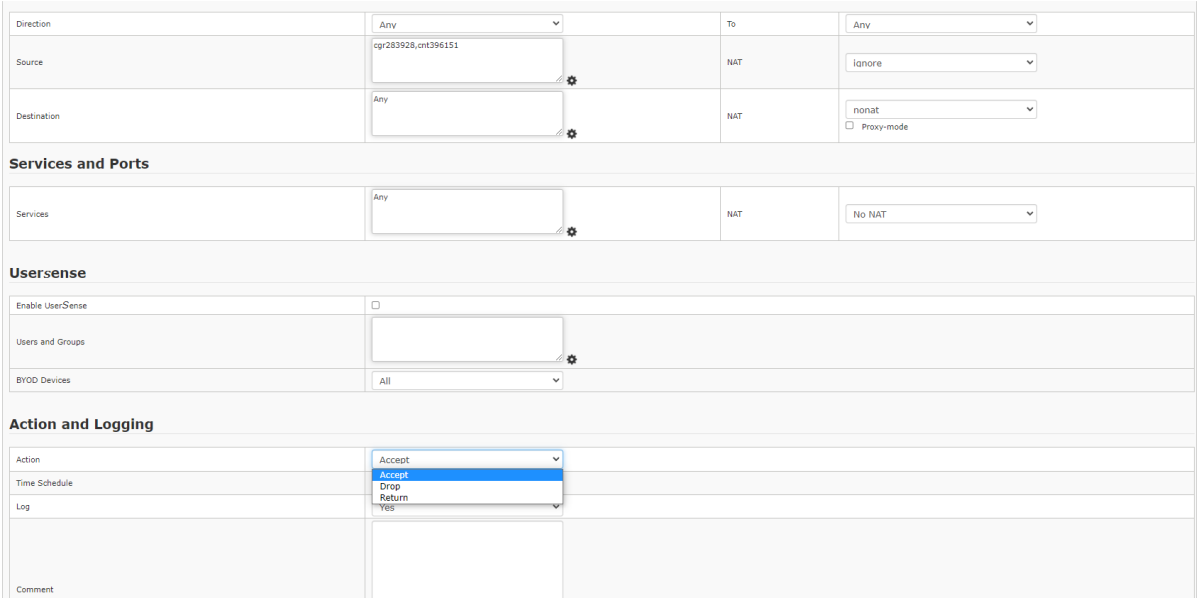
Add the specific countries or country groups from "**Available Country Groups**" tab.



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

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.



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.