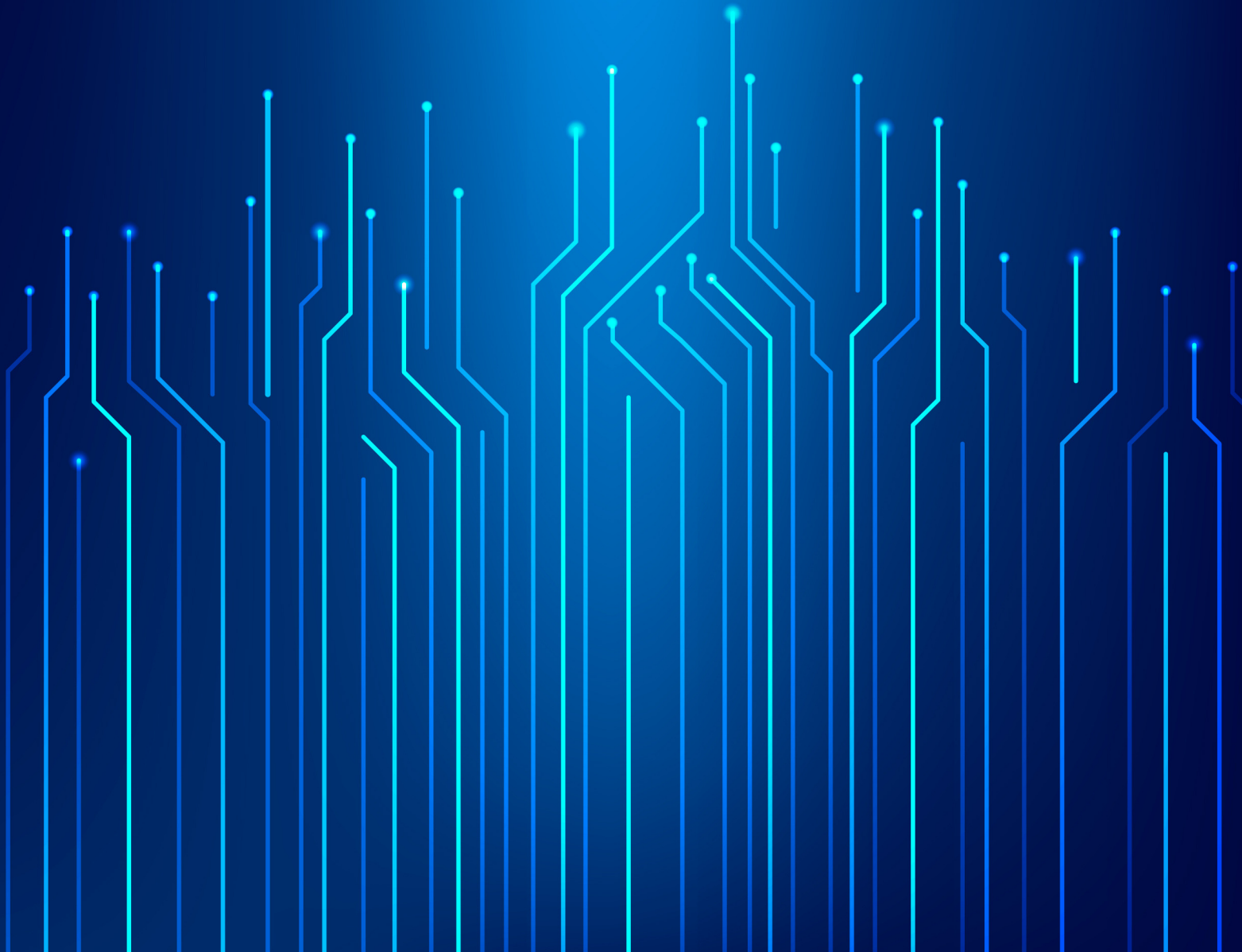


How to configure IPS in firewall




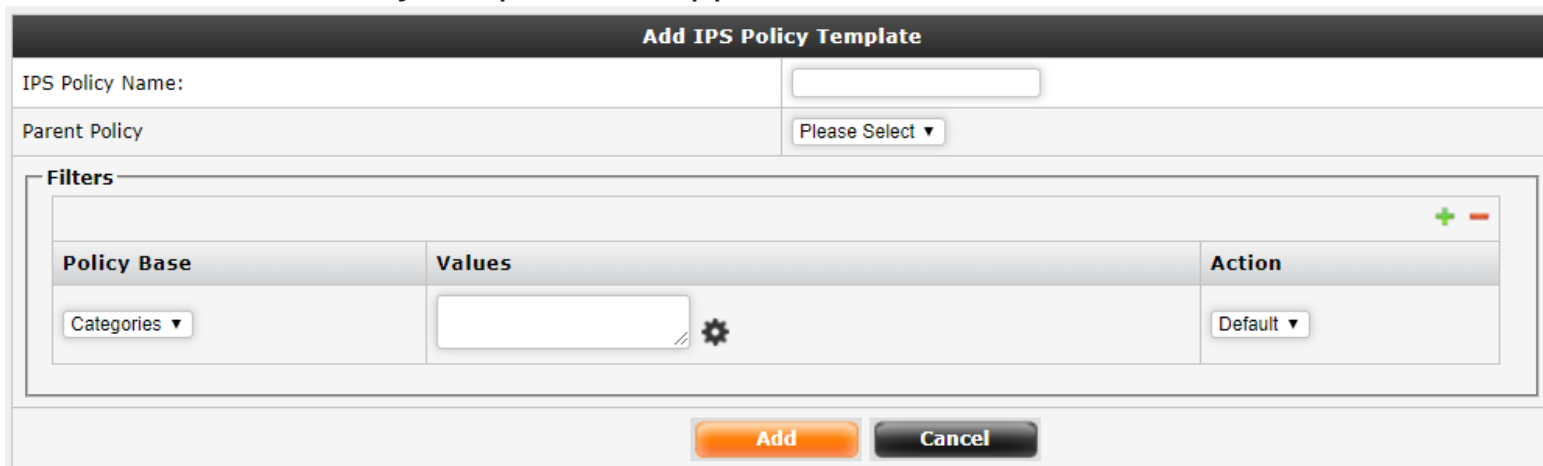
How to configure IPS in firewall

In this document, we will guide you through IPS Configuration.

IPS Policies are generally used for natting

To configure IPS in your firewall, follow these steps:

1. To begin with the configuration, go to IPS-> IPS Policy and click on  icon
2. Add IPS Policy template will appear as shown below:



Add IPS Policy Template

IPS Policy Name:

Parent Policy: Please Select ▼

Filters

| Policy Base | Values | Action |
|---------------------------|--|------------------------|
| Categories ▼ | <input type="text"/>  | Default ▼ |

Add Cancel

3. You will need to add the following information to successfully add an IPS Template.

IPS policy name: You can set the name of the IPS Policy in this field.

Parent Policy: This field is optional. It is used to specify the parent policy of the policy you are adding.

Filters: This allows us to create multiple IPS categories with different actions.


To add new IPS filter, click on  button.

Doing this will create an additional row which can be used to specify different policies based on different actions.


To remove the last row of filters, click on  button.


Doing this will delete the last row of the IPS policy filter added.

Policy Base: This field is used to select the options. Currently we have only one option - "Category". Policy base is based on IPS categories.

Values: Based on the selected IPS categories, these values will be applied. To edit IPS Categories' values, click on  button and the following screen appears from which you can select from the available IPS Categories.

| Available IPS Categories | | Selected IPS Categories |
|---|---------------------------------|-------------------------|
| ATTACK RESPONSES BACKDOOR BAD TRAFFIC CHAT DDOS DNS DOS EXPLOIT FINGER ETD | <div>></div> <div><</div> | |
| <div>Submit</div> | | |

To add from the available IPS Categories, select the category and click on  button. This will move selected signatures from Available IPS Categories into Selected IPS Categories.

To remove the selected IPS category, select on the IPS category and click on  button. This will remove selected signatures from Selected IPS Categories into Available IPS Categories.

To save the selected IPS Categories, click on submit button.

Action: This field specifies the action options on IPS settings of all the groups. The options can be Default, Alert or Drop.

Default: By default, the all the signature in the category is enabled with it's default actions.

Alert: If you select Alert in the action then all the signatures in that category would be in "Alert Mode"




Drop: If you select Drop in the category then all the signatures in that category would be in "Drop Mode"

If you select alert action, you will have to first do Email configuration by Going to Management -> Settings -> Email Settings





| Configure Email Settings | |
|---|-----------------------------------|
| To Email-ID (Admin Email-ID) | <input type="text"/> |
| SMTP Server IP/Domain name | <input type="text"/> |
| SMTP Server Port | <input type="text" value="25"/> |
| Connection security | <input type="text" value="None"/> |
| From Email-ID | <input type="text"/> |
| SMTP Server Login | <input type="text"/> |
| SMTP Server Password | <input type="password"/> |
| Send Alert-Email for Admin-logs | <input type="checkbox"/> |
| <input type="button" value="Test Config"/> <input type="button" value="Update"/> <input type="button" value="Reset"/> | |

and configure email on IPS by going to IPS -> IPS Alert Settings.

| IPS Alert Settings | |
|--|--------------------------|
| Alert | <input type="checkbox"/> |
| Sender Email-ID | <input type="text"/> |
| Recipient Email-ID(s) | <input type="text"/> |
| Subject for IPS alerts | <input type="text"/> |
| <input type="button" value="Update"/> <input type="button" value="Reset"/> | |

| Policy Name | Parent Policy | Home Network |
|-------------|---------------|---|
| test | |    |

After adding new IPS policy, you need to make sure those policies are added in the firewall rule by going into Firewall -> policies -> Rules and add those rules there to be able to successfully install the policies.

| Rules | | | | | | | | | | | |
|-------|------------|------------|--------|-----------------------|-------------|------------|------------------|--------|----------|-----|---|
| No. | IP Version | Direction | Source | Destination | Service | User Sense | Policies | Action | Schedule | QoS | Tasks |
| 1 | IPv4 | WAN To LAN | Any | fwip-WAN Webserver | http, https | - | IPS Policy: test | accept | AllTime | - |     |

By following these steps you can successfully configure IPS policies in the firewall.