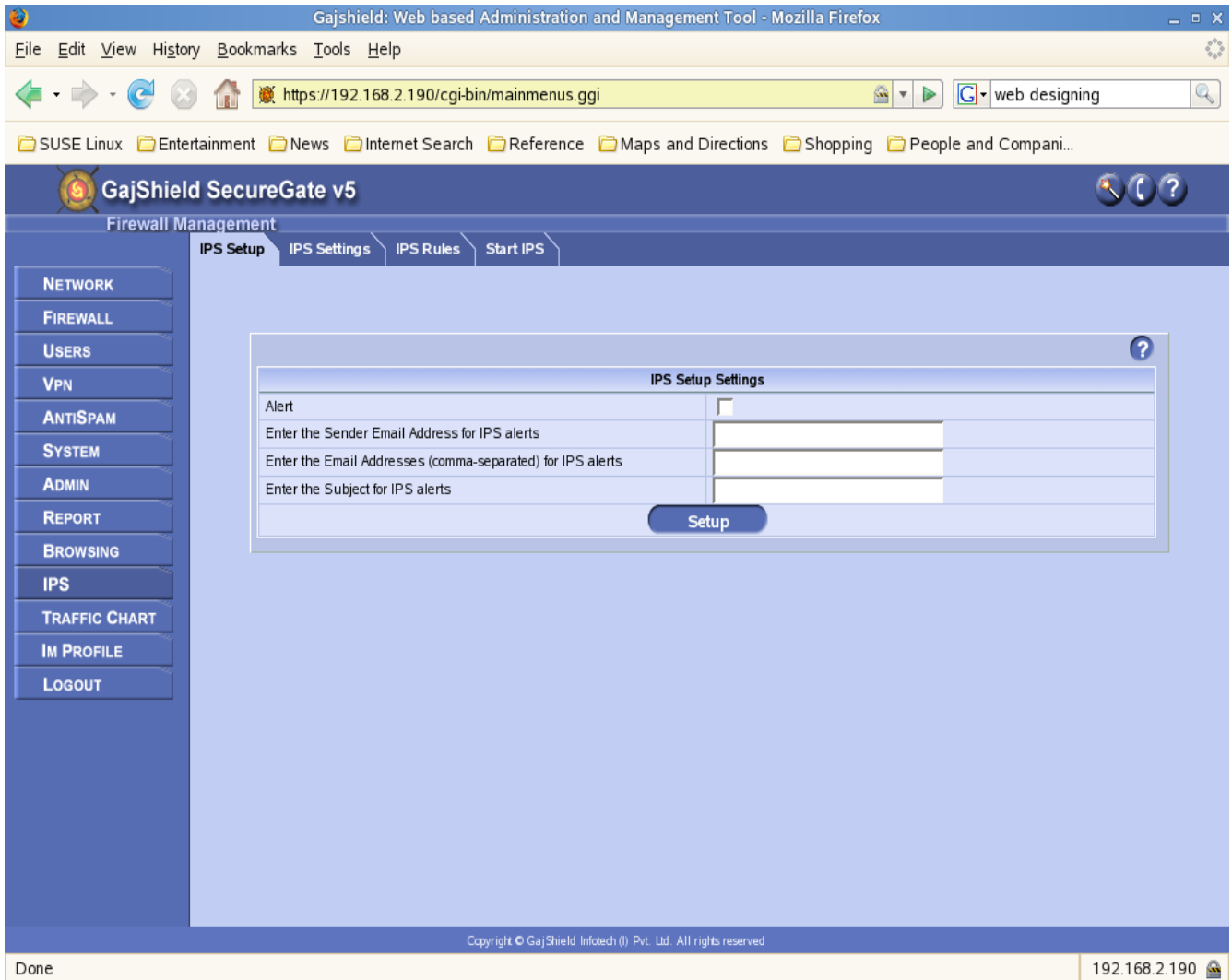


## IPS How-To

### Step 1 : IPS Setup

- Alert : Check the this checkbox if you wish to receive alerts for IPS.
- Enter the Sender Email Address for IPS alerts : you will receive emails from this id.
- Enter the Email Addresses (comma-separated) for IPS alerts : This is the email address where the alerts will be mailed. Multiple email id's can be entered by separating the id's with a comma.
- Enter the Subject for IPS alerts : The alert mail will have this subject.



The screenshot displays the GajShield SecureGate v5 web-based administration interface. The browser window title is "GajShield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.190/cgi-bin/mainmenu.cgi". The interface features a navigation menu on the left with options like NETWORK, FIREWALL, USERS, VPN, ANTISPAM, SYSTEM, ADMIN, REPORT, BROWSING, IPS, TRAFFIC CHART, IM PROFILE, and LOGOUT. The main content area is titled "Firewall Management" and includes tabs for "IPS Setup", "IPS Settings", "IPS Rules", and "Start IPS". The "IPS Setup" tab is active, showing a form titled "IPS Setup Settings" with the following fields:

IPS Setup Settings	
Alert	<input type="checkbox"/>
Enter the Sender Email Address for IPS alerts	<input type="text"/>
Enter the Email Addresses (comma-separated) for IPS alerts	<input type="text"/>
Enter the Subject for IPS alerts	<input type="text"/>

A "Setup" button is located below the form. The footer of the interface contains the text "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" and the IP address "192.168.2.190".

- To get the alerts you first need to configure the Admin > Settings > Email Settings Tab. Configure them as follows;
  - # Default Admin Email ID : A valid email id from which the mails would be sent
  - # SMTP Server IP : IP of the local mail server.
  - # Email ID For Service Alerts : The email id where the alerts would be sent.
  - # SMTP Server Login : The Login name of the admin email id.
  - # SMTP Server Password : Password of the admin email id.

The screenshot shows a web browser window displaying the GajShield SecureGate v5 administration interface. The browser's address bar shows the URL `https://192.168.2.190/cgi-bin/mainmenus.cgi`. The interface has a blue header with the title "GajShield SecureGate v5" and a "Firewall Management" section. Below the header, there are several tabs: "System Settings", "Email Settings" (which is selected), "Misc Options", "Default Settings", and "Date and Time". On the left side, there is a vertical navigation menu with categories like NETWORK, FIREWALL, USERS, VPN, ANTISPAM, SYSTEM, ADMIN, REPORT, BROWSING, IPS, TRAFFIC CHART, IM PROFILE, and LOGOUT. The "ADMIN" category is expanded, showing sub-items: Administration, Settings, Utility, and License. The main content area displays a "Configure Email Settings" form with the following fields:

Configure Email Settings	
Default Admin Email ID	<input type="text"/>
SMTP Server IP	<input type="text"/>
Email ID For Service Alerts	<input type="text"/>
SMTP Server Login	<input type="text"/>
SMTP Server Password	<input type="password"/>

Below the form is an "Update" button. At the bottom of the page, there is a footer with the text "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" and a status bar showing "Done" and the IP address "192.168.2.190".

## Step 2 : IPS Settings

- To begin click on the “Add” (+) button.

The screenshot shows the GajShield SecureGate v5 Firewall Management interface. The browser window title is "GajShield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows "https://192.168.2.190/cgi-bin/mainmenuus.ggi". The interface has a navigation menu on the left with options: NETWORK, FIREWALL, USERS, VPN, ANTI SPAM, SYSTEM, ADMIN, REPORT, BROWSING, IPS, TRAFFIC CHART, IM PROFILE, and LOGOUT. The main content area is titled "Firewall Management" and has tabs for "IPS Setup", "IPS Settings", "IPS Rules", and "Start IPS". The "IPS Settings" tab is active, showing a configuration table with columns: Protocol, Scan Type, Sense Level, Watch IP Group, Ignore Scanner IP, and Ignore Scanned IP. Below the table are two rows of configuration options: "Home Network", "External Network", "DNS", "SMTP", "HTTP", "SQL", "TELNET", "SNMP", and "HTTP Ports". Each row has a "+" and "?" icon. The status bar at the bottom shows "Done" and the IP address "192.168.2.190".

- Port Scan Settings :

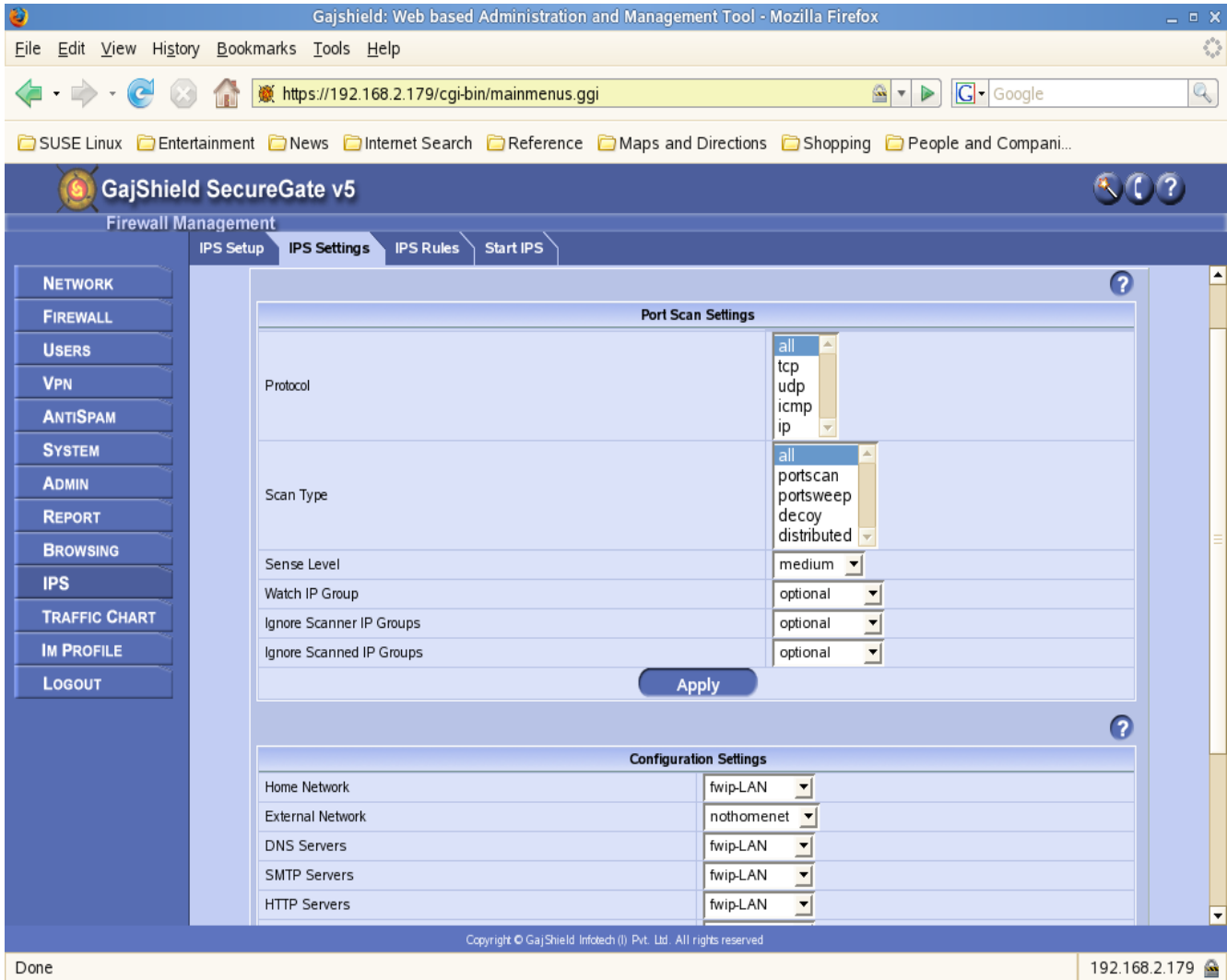
- # Protocol : Select among the different protocols to be scanned.
- # Scan Type : Select among the different Scan types.
- # Sense Level : Select between high, medium and low sense levels.
- # Watch IP Group : This option is optional. So you can leave it as it is.
- # Ignore Scanner IP Group : This option is optional. So you can leave it as it is.
- # Ignore Scanned IP Groups : This option is optional. So you can leave it as it is.

- When this is done, click on Apply and your Settings will be saved.

- Configuration Settings : ( for the below options you need to make a host if you have any of the following servers and then select them in the drop down menu)

- # Home Network : Select the host of the server present in you network
- # External Network : Select the host of the server present in you network
- # DNS Servers : Select the host of the server present in you network
- # SMTP Servers : Select the host of the server present in you network
- # HTTP Servers : Select the host of the server present in you network
- # SQL Servers : Select the host of the server present in you network
- # TELNET Server : Select the host of the server present in you network
- # SNMP Servers : Select the host of the server present in you network
- # HTTP Ports : Select the host of the server present in you network

- When this is done, click on Apply and your Settings will be saved.



***The recommended setting are as follows :***

Protocol	: All	.....	*** select atleast one option here
Scan Type	: All	.....	*** select atleast one option here
Sense Level	: Medium	.....	*** select atleast one option here

- After doing this click on apply.
- And then go again to the settings menu, to configure the Configuration Settings.

GajShield: Web based Administration and Management Tool - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://192.168.2.179/cgi-bin/mainmenus.ggi

SUSE Linux Entertainment News Internet Search Reference Maps and Directions Shopping People and Compani...

### GajShield SecureGate v5

Firewall Management

IPS Setup **IPS Settings** IPS Rules Start IPS

Scan type: portsweep, decoy, distributed

Sense Level: low

Watch IP Group: optional

Ignore Scanner IP Groups: optional

Ignore Scanned IP Groups: optional

Apply

**Configuration Settings**

Home Network	fwnet-LAN
External Network	nothomenet
DNS Servers	fwip-LAN
SMTP Servers	Mail-Server
HTTP Servers	HTTP-Server
SQL Servers	fwip-LAN
TELNET Servers	fwip-LAN
SNMP Servers	fwip-LAN
HTTP Ports	http

Apply

Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved

Done 192.168.2.179

- If you have any of the mentioned servers then make their respective Hosts and select them in the drop-down menu.
- After doing the configuration click on apply.

### Setup 3 : IPS Rules

- All the attacks are divided in different categories.
- These rules help monitor different categories
- The actions that can be performed are *Alert*(IDS), or *Drop*(IPS)
- It can also be kept as *Default* which will work as per the default behaviour set for that rule, ie. IPS or IDS.
- These rules can be further edited by clicking on the (+) sign, to edit the sub rules as per the requirements.

The screenshot shows the GajShield SecureGate v5 web interface. The browser address bar shows the URL <https://192.168.2.190/cgi-bin/mainmenus.cgi>. The interface has a navigation menu on the left with options like NETWORK, FIREWALL, USERS, VPN, ANTI SPAM, SYSTEM, ADMIN, REPORT, BROWSING, IPS, TRAFFIC CHART, IM PROFILE, and LOGOUT. The main content area is titled 'Firewall Management' and has tabs for 'IPS Setup', 'IPS Settings', 'IPS Rules', and 'Start IPS'. The 'IPS Rules' tab is active, displaying a table of rules.

Enable/Disable	Ids/IPS	+	Category	Description
<input checked="" type="checkbox"/>	Default	+	ATTACK RESPONSES	These signatures are those when they happen, its usually because a machine has been compromised. These should not false that often and almost always mean a compromise.
<input checked="" type="checkbox"/>	Default	+	BACKDOOR	Back Door Attack
<input checked="" type="checkbox"/>	Default	+	BAD TRAFFIC	These signatures are representative of traffic that should never be seen on any network. None of these signatures include datagram content checking and are extremely quick signatures
<input checked="" type="checkbox"/>	Default	+	CHAT	These signatures look for people using various types of chat programs (for example: AIM, ICQ, and IRC) which may be against corporate policy
<input checked="" type="checkbox"/>	Default	+	DDOS	Distributed Denial of Service attack
<input checked="" type="checkbox"/>	Default	+	DNS	Domain Name System
<input checked="" type="checkbox"/>	Default	+	DOS	Denial Of Service Attack
<input checked="" type="checkbox"/>	Default	+	EXPLOIT	Exploits
<input checked="" type="checkbox"/>	Default	+	FINGER	finger
<input checked="" type="checkbox"/>	Default	+	FTP	Ftp attacks
<input checked="" type="checkbox"/>	Default	+	ICMPINFO	These rules are standard ICMP traffic. They include OS pings, as well as normal routing done by ICMP. There are a number of "catch all" rules that will alert on unknown ICMP types.
<input checked="" type="checkbox"/>	Default	+	ICMP	These rules are potentially bad ICMP traffic. They include most of the ICMP scanning tools and other "BAD" ICMP traffic (Such as redirect host)
<input checked="" type="checkbox"/>	Default	+	IMAP	Imap Attack
<input checked="" type="checkbox"/>	Default	+	INF	Info
<input checked="" type="checkbox"/>	Default	+	MISC	Miscellaneous
<input checked="" type="checkbox"/>	Default	+	MULTIMEDIA	These signatures look for people using streaming multimedia technologies. Using streaming media may be a violation of corporate policies.
<input checked="" type="checkbox"/>	Default	+	MYSQL	These signatures detect unusual and potentially malicious mysql traffic.

Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved

Done 192.168.2.190

#### Step 4 : Start IPS

- When all the settings have been done you need to Start the IPS Service.
- To do that click on the green button.

The screenshot shows a web browser window titled "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar contains the URL "https://192.168.2.190/cgi-bin/mainmenus.ggi". The browser's search bar contains the text "web designing".

The main content area of the browser displays the "GajShield SecureGate v5" interface. The page title is "GajShield SecureGate v5". Below the title, there is a "Firewall Management" section with tabs for "IPS Setup", "IPS Settings", "IPS Rules", and "Start IPS". The "Start IPS" tab is currently selected.

On the left side of the interface, there is a vertical navigation menu with the following items: NETWORK, FIREWALL, USERS, VPN, ANTI SPAM, SYSTEM, ADMIN, REPORT, BROWSING, IPS, TRAFFIC CHART, IM PROFILE, and LOGOUT.

The main content area of the "Start IPS" tab features a "IPS Options" section. This section contains a single line with a green play button icon, indicating the start of the IPS service. A help icon (?) is visible in the top right corner of this section.

At the bottom of the interface, there is a footer with the text "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved".

The browser's status bar at the bottom shows "Done" on the left and "192.168.2.190" on the right.