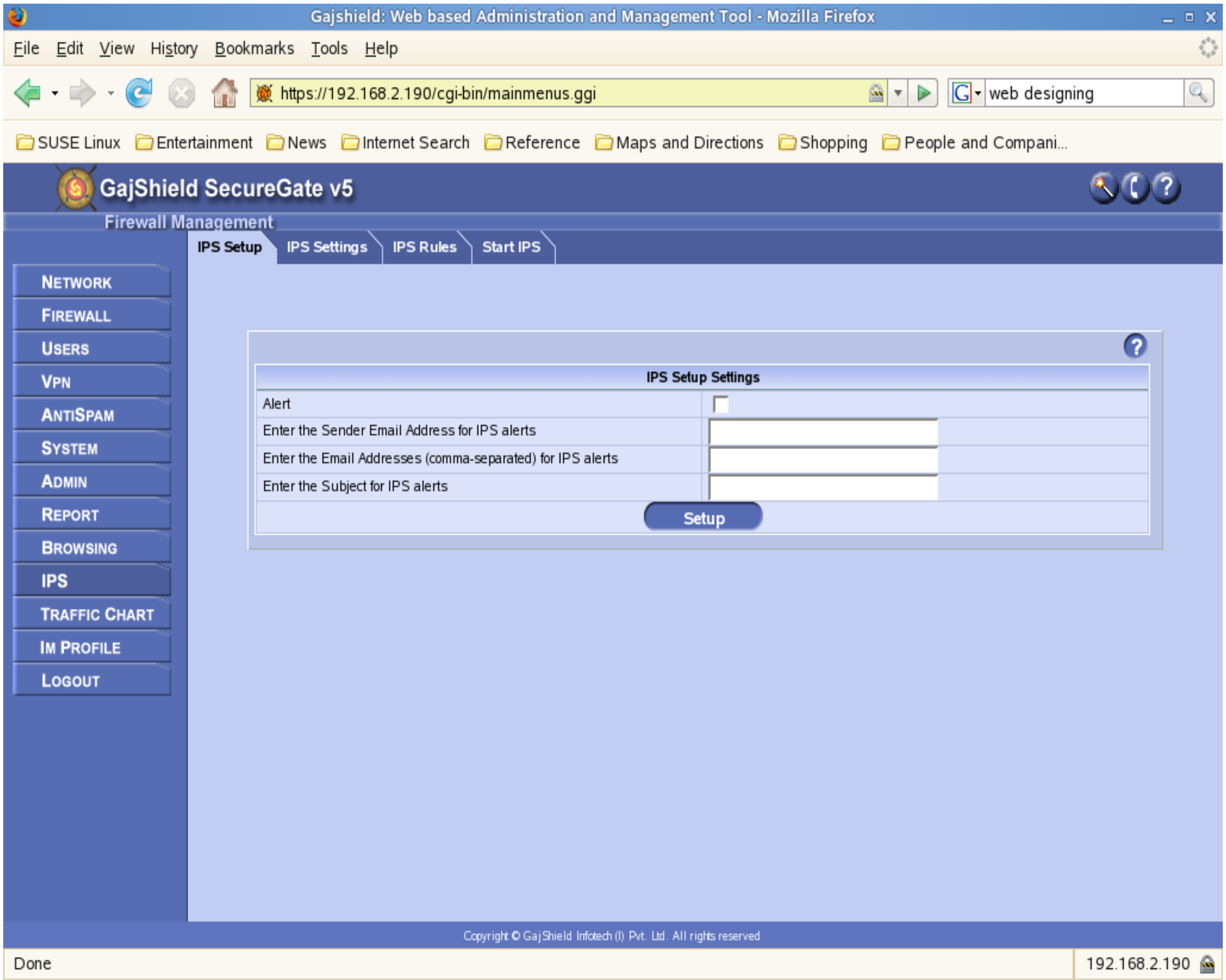
IPS How-To

Step 1 : IPS Setup

- Alert : Check the this checkbox if you wish to receive alearts for ISP.
- 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 alearts will be mailed.
  Multiple email id's can be entered by seperating the id's with a comma.
- Enter the Subject for IPS alerts : The aleart mail will have this subject.

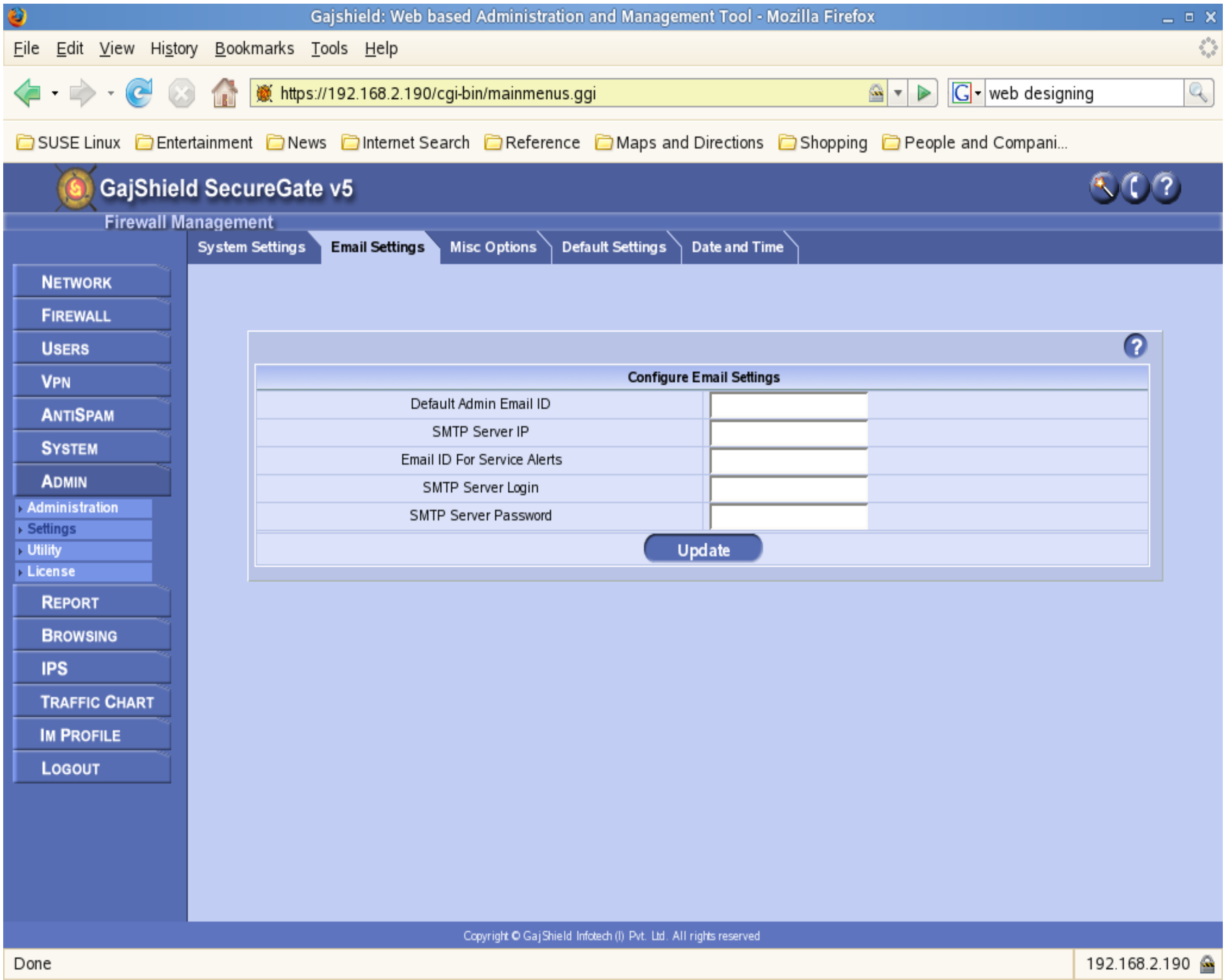


IPS Setup Settings

Alert	□
Enter the Sender Email Address for IPS alerts	
Enter the Email Addresses (comma-separated) for IPS alerts	
Enter the Subject for IPS alerts	

- To get the alearts 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 alearts would be sent.
  # SMTP Server Login : The Login name of the admin email id.
  # SMTP Server Password : Password of the admin email id.



Gajshield: Web based Administration and Management Tool - Mozilla Firefox

https://192.168.2.190/cgi-bin/mainmenus.ggi

Configure Email Settings

Default Admin Email ID	
SMTP Server IP	
Email ID For Service Alerts	
SMTP Server Login	
SMTP Server Password	

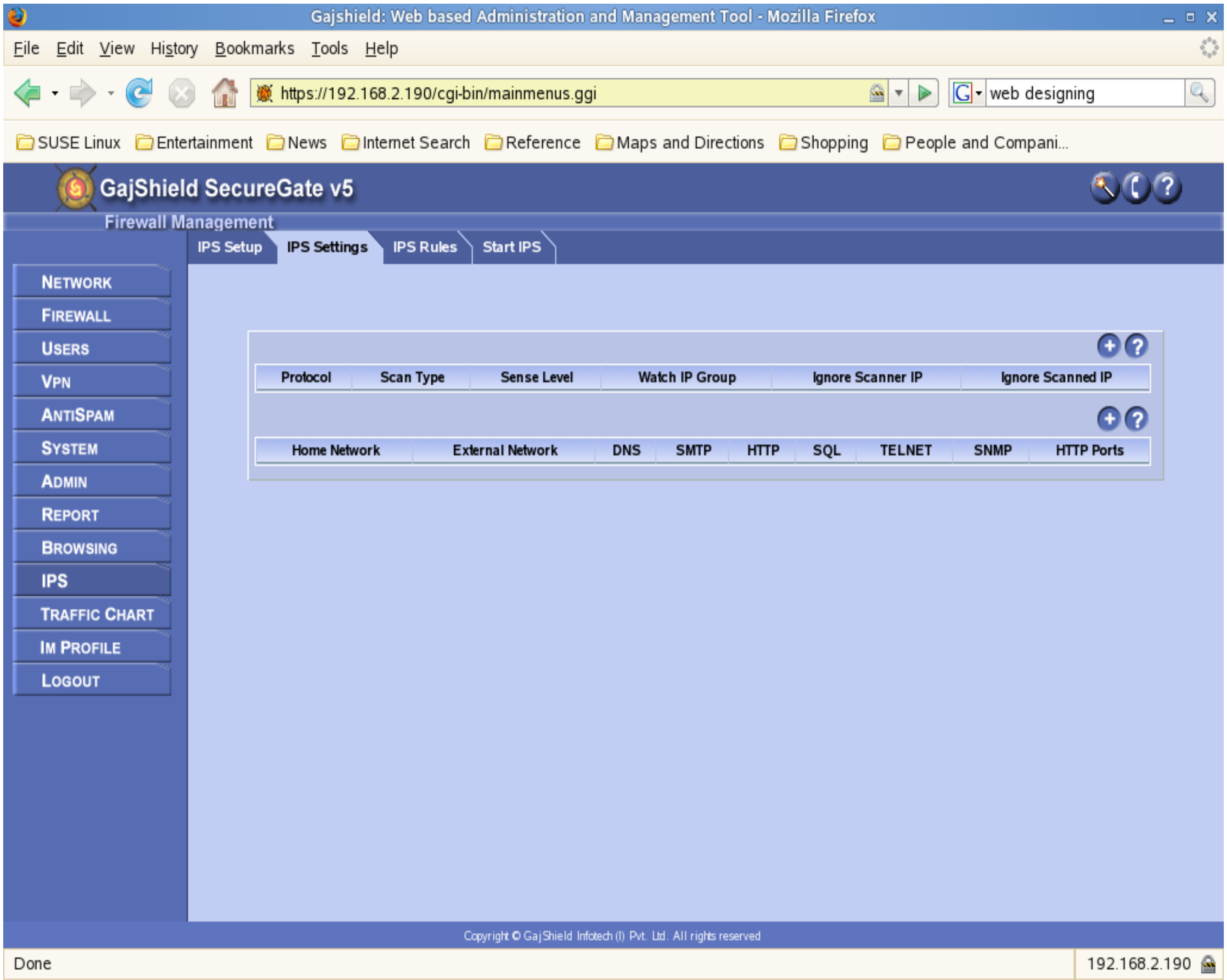
Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved

Done

192.168.2.190

Step 2 : IPS Settings

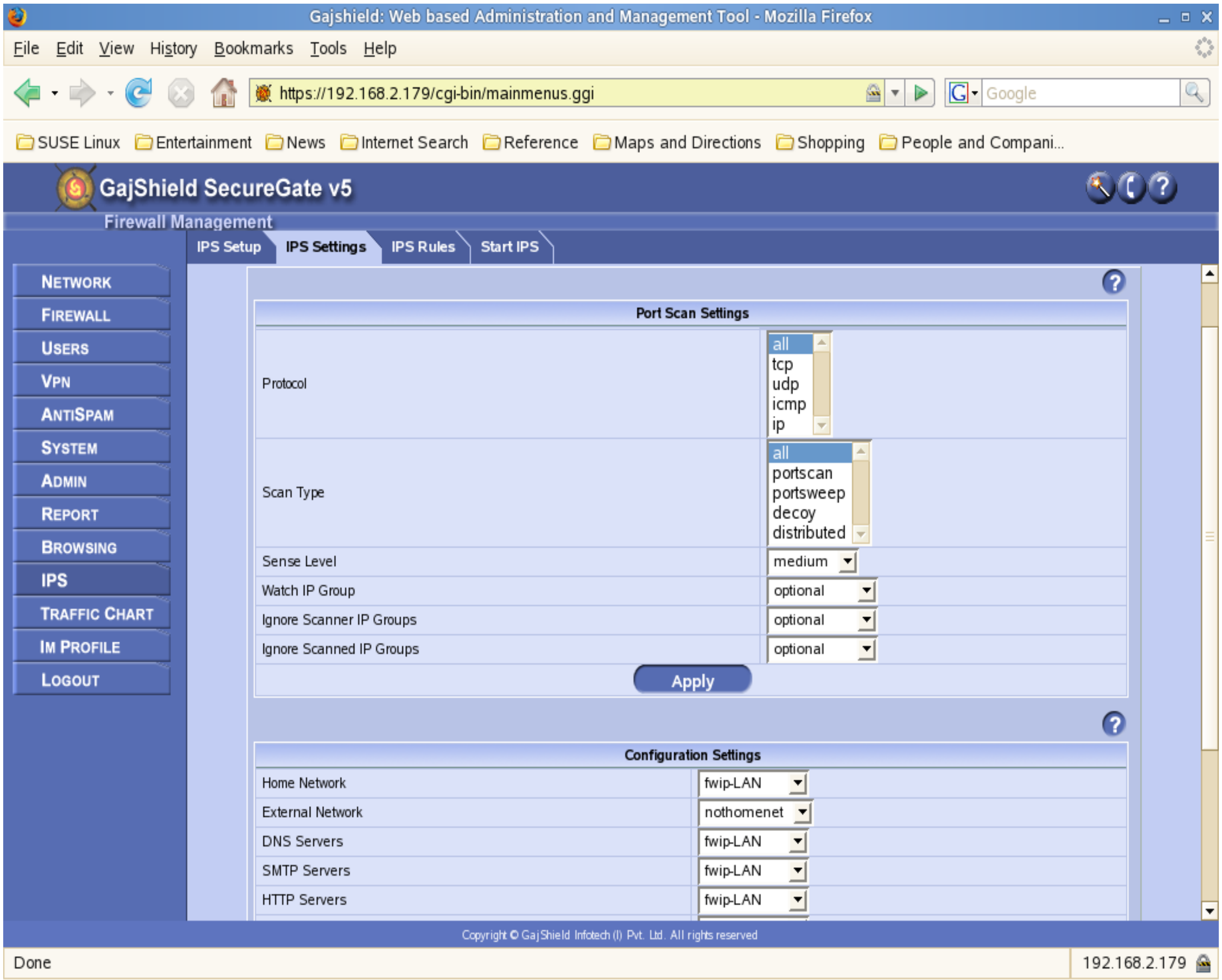
- To begin click on the “Add” (+) button.



Protocol	Scan Type	Sense Level	Watch IP Group	Ignore Scanner IP	Ignore Scanned IP

Home Network	External Network	DNS	SMTP	HTTP	SQL	TELNET	SNMP	HTTP Ports

- 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, mediunm 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.



Port Scan Settings

Protocol	all tcp udp icmp ip
Scan Type	all portscan portsweep decoy distributed
Sense Level	medium
Watch IP Group	optional
Ignore Scanner IP Groups	optional
Ignore Scanned IP Groups	optional

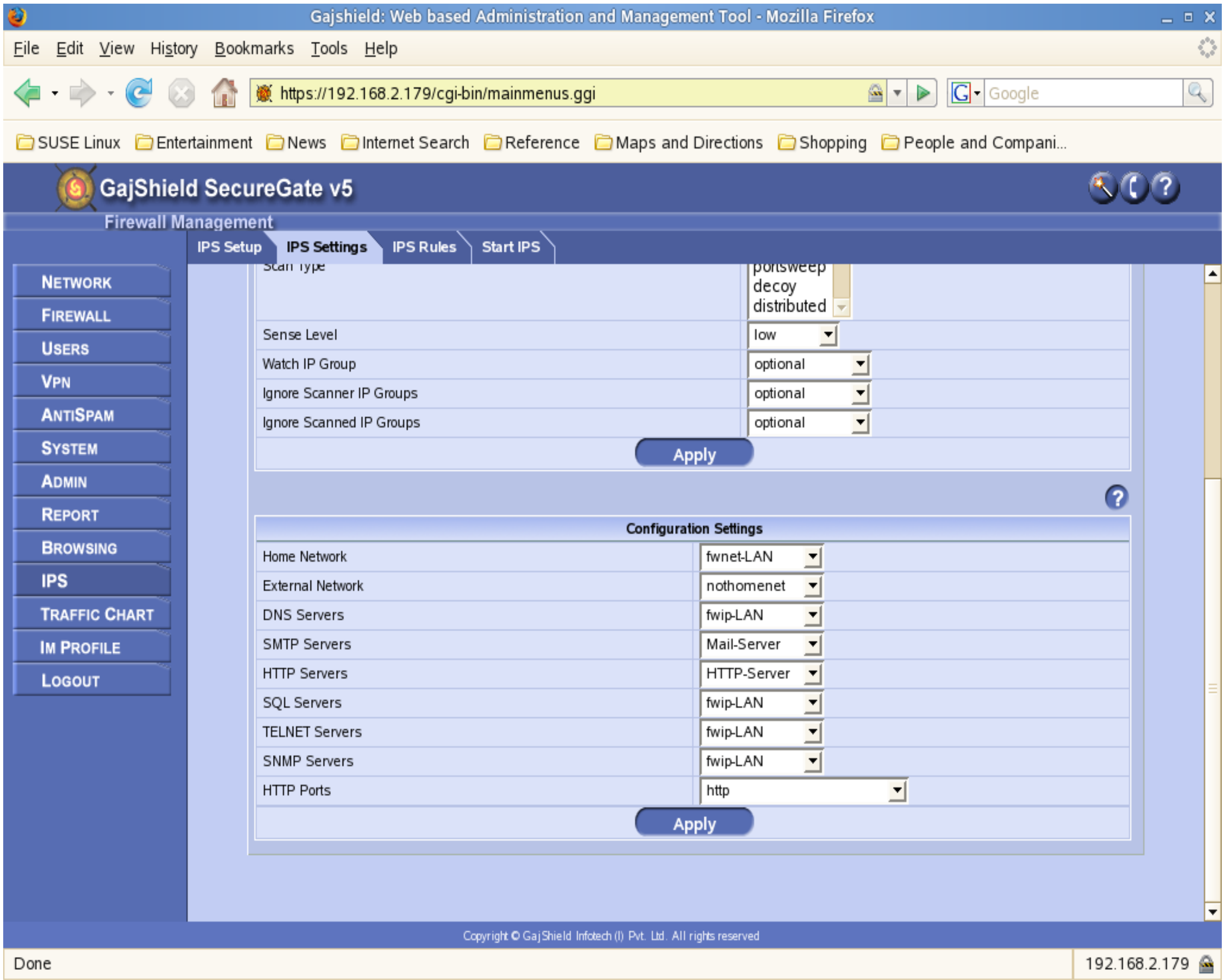
Configuration Settings

Home Network	fwip-LAN
External Network	nothomenet
DNS Servers	fwip-LAN
SMTP Servers	fwip-LAN
HTTP Servers	fwip-LAN

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.



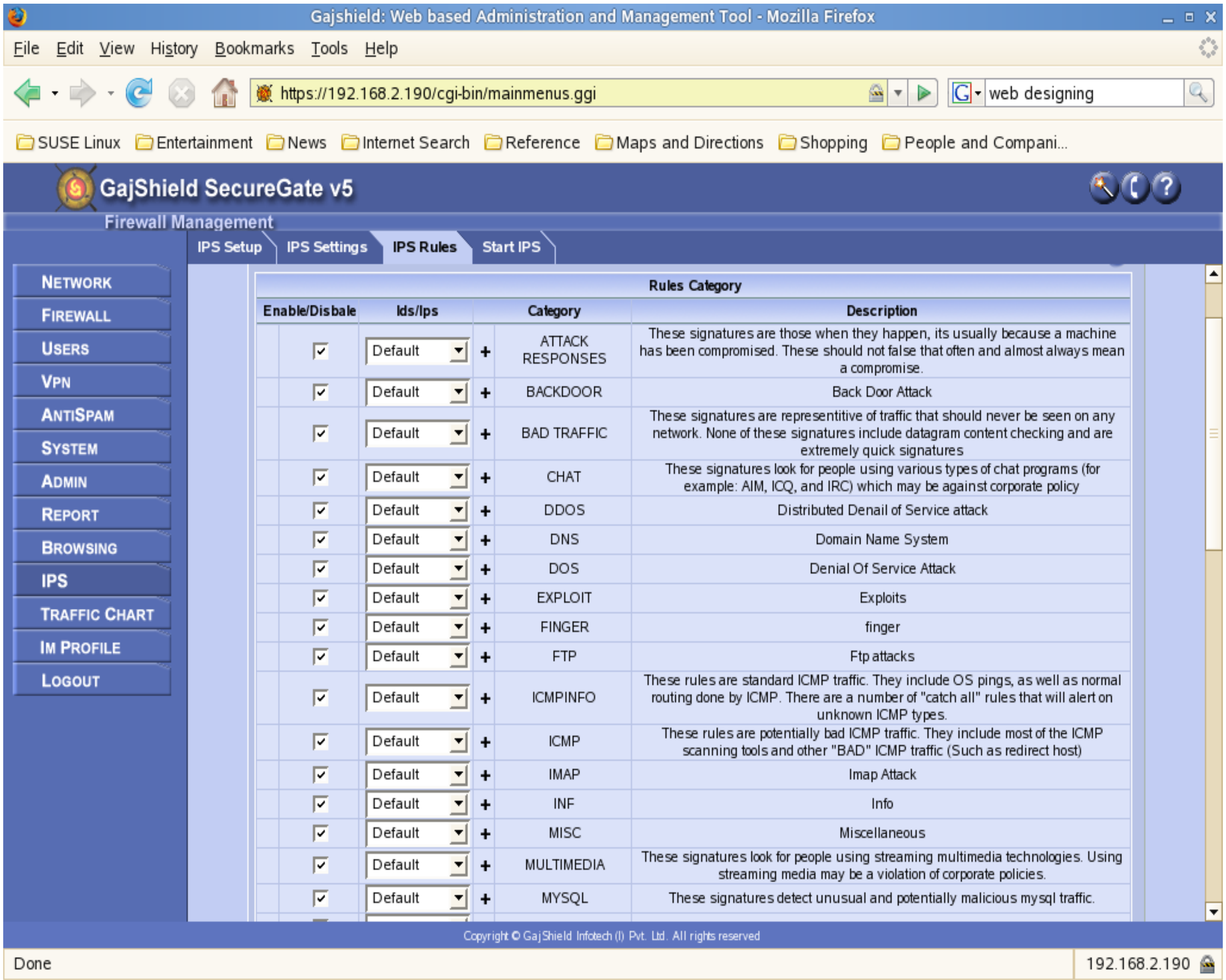
Scan Type	portsweep decoy distributed
Sense Level	low
Watch IP Group	optional
Ignore Scanner IP Groups	optional
Ignore Scanned IP Groups	optional

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

- 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 editted by clicking on the (+) sign, to edit the sub rules as per the requirements.



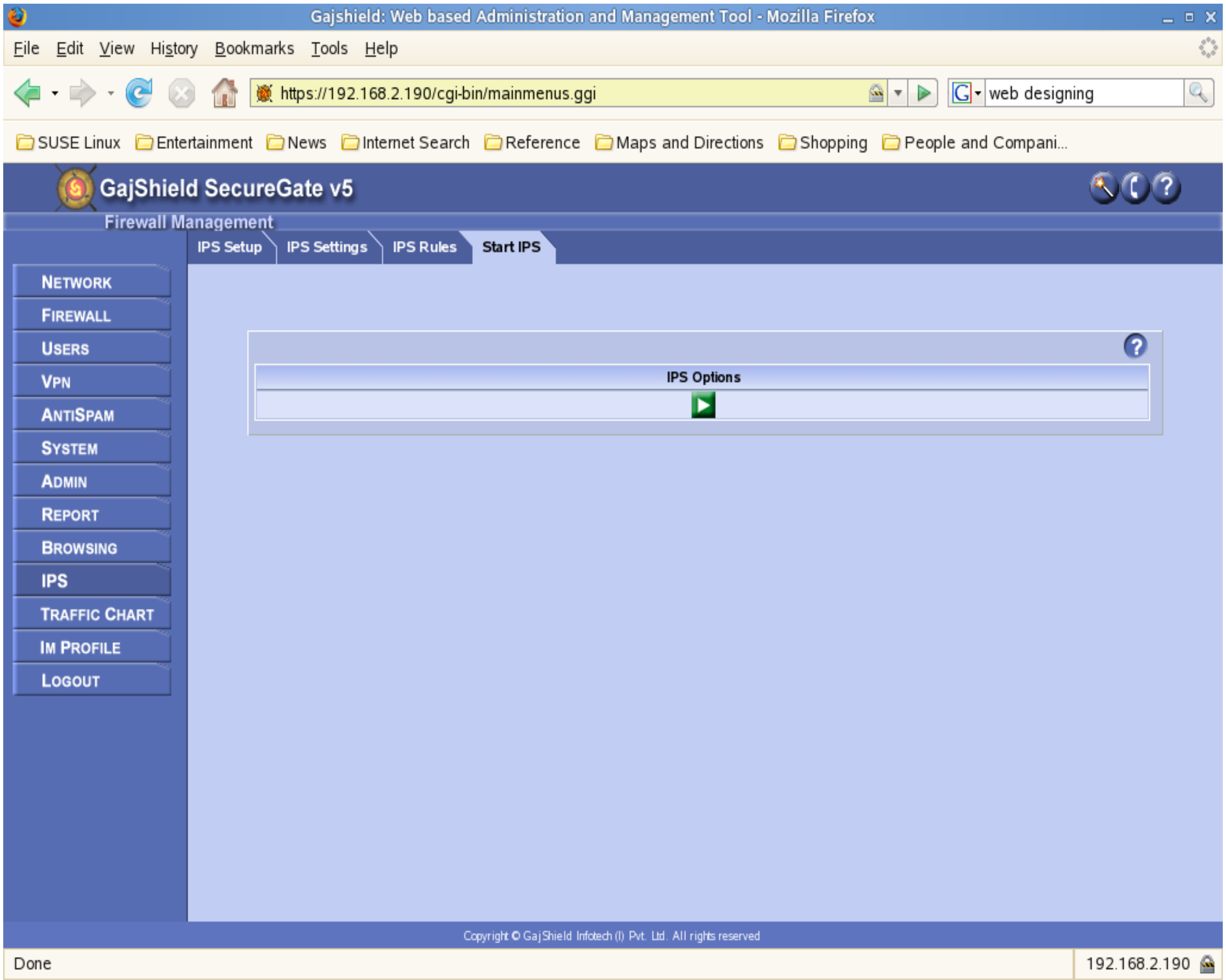
Rules Category

Enable/Disbale	Ids/Ips		Category	Description
☑	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.
☑	Default	+	BACKDOOR	Back Door Attack
☑	Default	+	BAD TRAFFIC	These signatures are representitive of traffic that should never be seen on any network. None of these signatures include datagram content checking and are extremely quick signatures
☑	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
☑	Default	+	DDOS	Distributed Denail of Service attack
☑	Default	+	DNS	Domain Name System
☑	Default	+	DOS	Denial Of Service Attack
☑	Default	+	EXPLOIT	Exploits
☑	Default	+	FINGER	finger
☑	Default	+	FTP	Ftp attacks
☑	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.
☑	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)
☑	Default	+	IMAP	Imap Attack
☑	Default	+	INF	Info
☑	Default	+	MISC	Miscellaneous
☑	Default	+	MULTIMEDIA	These signatures look for people using streaming multimedia technologies. Using streaming media may be a violation of corporate policies.
☑	Default	+	MYSQL	These signatures detect unusual and potentially malicious mysql traffic.

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

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.



Gajshield: Web based Administration and Management Tool - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://192.168.2.190/cgi-bin/mainmenus.ggi
web designing
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
NETWORK
FIREWALL
USERS
VPN
ANTISPAM
SYSTEM
ADMIN
REPORT
BROWSING
IPS
TRAFFIC CHART
IM PROFILE
LOGOUT
IPS Options
Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved
Done
192.168.2.190