Intelligent Unified Threat Management (IUTM)

Manas Pratim Sarma

(B.Tech(IT), FPGDIS, CEHv8, CHFI)

CDAC Bangalore

What is IUTM

- Intelligent : Knowledge Based Anlysis.
- Unified : Multiple Component to Single One.
- Threat : Virus, Worms, BackDoor etc.
- Management : manage it.

UTM

- **Provide Multiple Security Functions within one single Appliance.**
- Network Firewalling
- Network Intrusion Prevention
- Network Intrusion Detection
- Gateway Antivirus (AV)
- Gateway Anti-spam
- VPN
- Content Filtering
- Load Balancing

Why Planning for IUTM

- A Large Organitation No Issue for Buying multiple UTM.
- A Startup IT Company : High Cost of UTM.
- So IUTM is Completly Open Source.
- Based on Integration of Open Source Software.

IUTM Function

- **IUTM Provide The Following Functions within one single Appliance.**

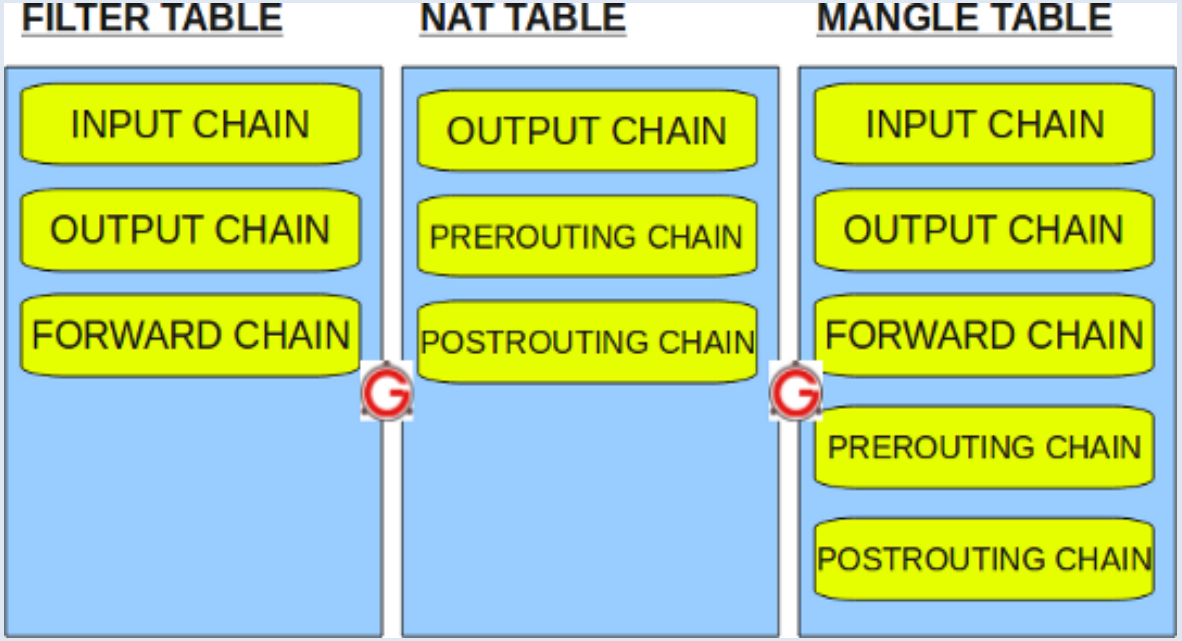
- Network Firewalling
- Network Intrusion Detection
- Gateway Antivirus (AV)
- Gateway Anti-spam
- Network Configuration
- Log Analysis

UTM Open Source Components

- IPTABLES
- SNORT
- CLAM-AV
- Linux Networking File
- Linux System Log

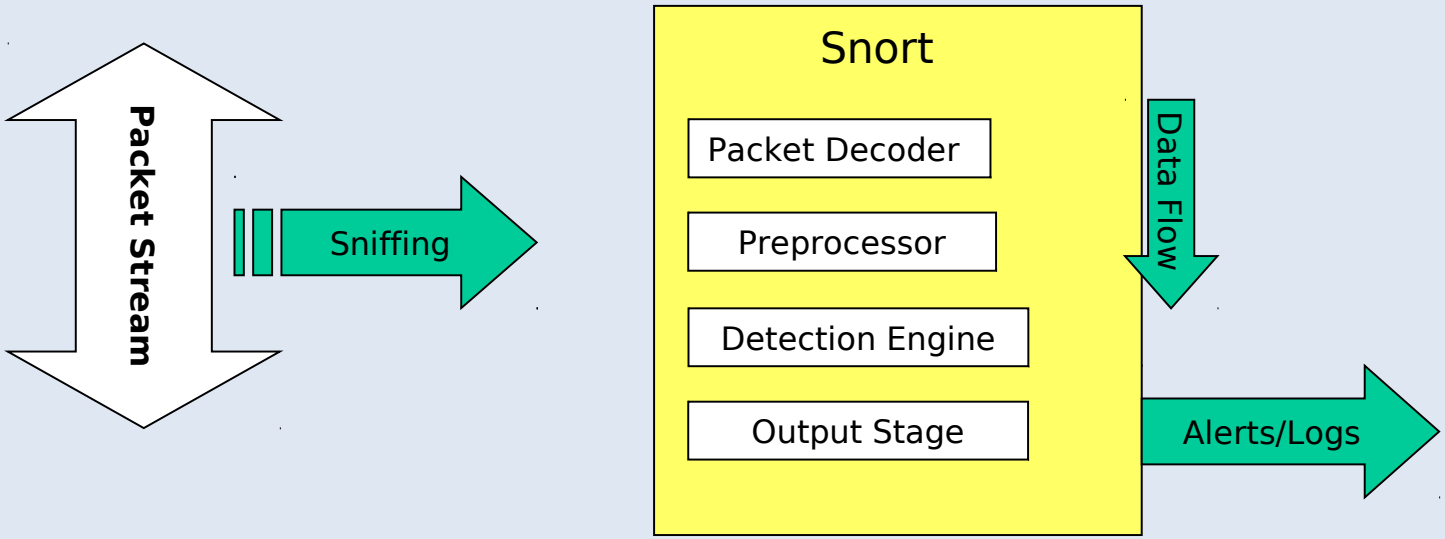
IPtables

- **IPtables are the tables provided by the Linux kernel firewall.**
- **Based on Netfilter modules.**
- **Tables >>> Chain >>> Rules.**



SNORT

- Snort is a free and open source network intrusion detection system (NIDS).
- Signature Based Packet Analysis.
- Three main modes : Sniffer, Packet Logger and Network Intrusion Detection.
- Snort Default Rule is Availabe in Snort Rule.

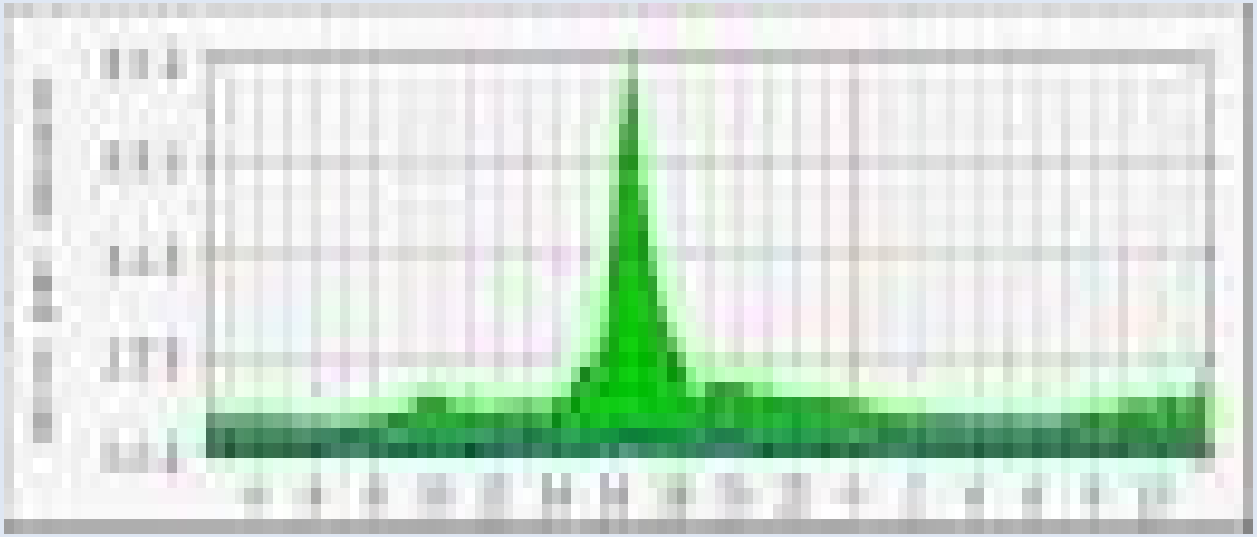


- **CLAM AV**
  - ClamAV is available for Linux and BSD-based operating systems.
  - Clam AntiVirus (ClamAV) is a free, cross-platform antivirus software tool-kit able to detect many types of malicious software, including viruses.
  - One of its main uses is on mail servers as a server-side email virus scanner.
  - We can developed our own Signature.

- **Networking and System log based on Linux File System.**

Why Intelligent UTM

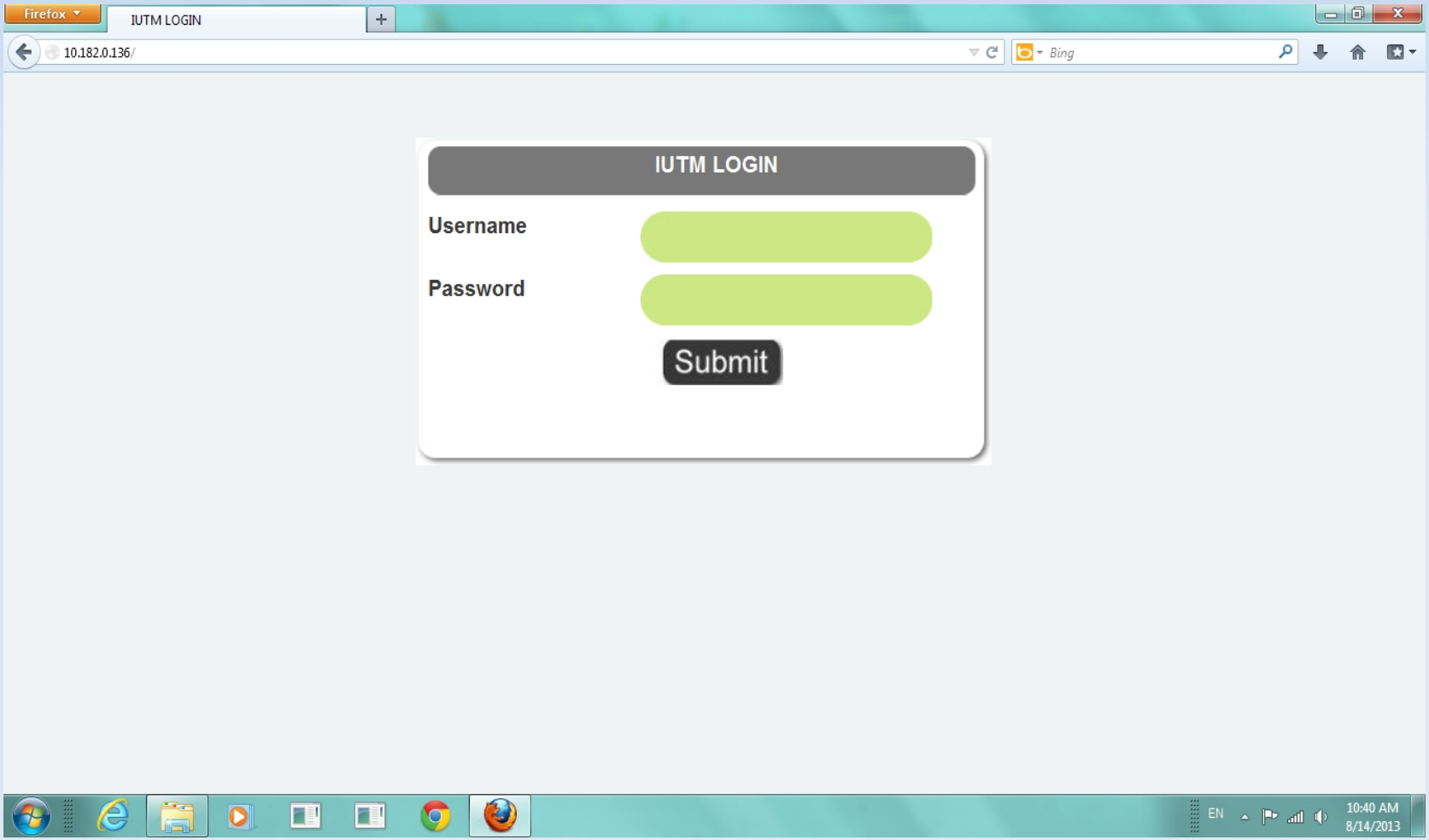
- **Able to Provide Block Traffic based on the current status of Network Behaviour.**
- Dynamically Addition of rule in Firewall.
- Interaction Between IDS(Snort) and Firewall(IPtables).
- Determine Threshold value of Alert.



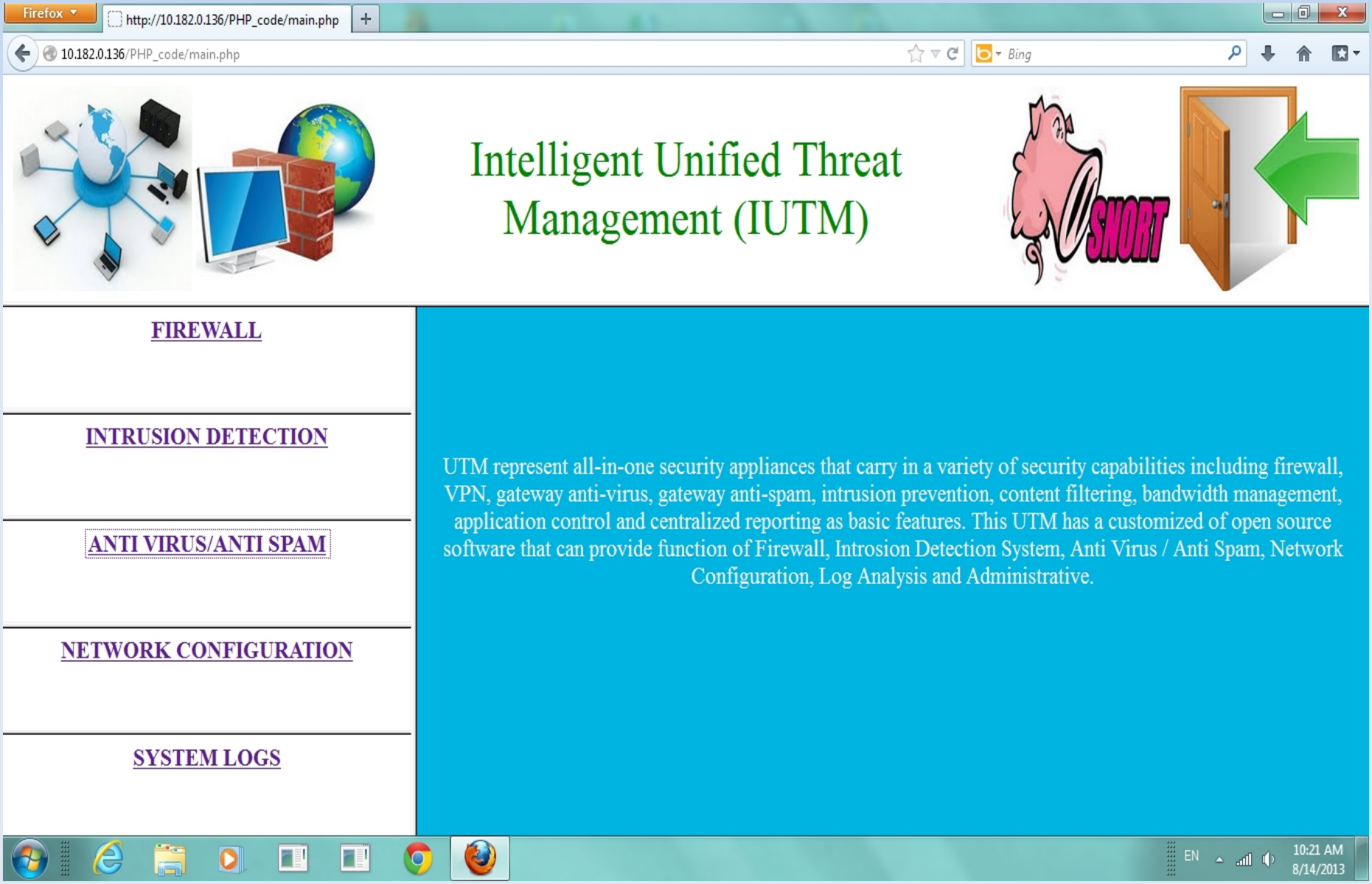
IUTM

- **Requirement Analysis:**
  - **Atleast 2 NIC System.**
  - **4 GB RAM.**
  - **1 TB HD.**
- **Language Used:**
  - **Front End: Php, HTML.**
  - **Back End: Java, Shell, C.**

Login Page


Firefox
IUTM LOGIN
10.182.0.136/
Bing
IUTM LOGIN
Username
Password
Submit
EN
10:40 AM
8/14/2013

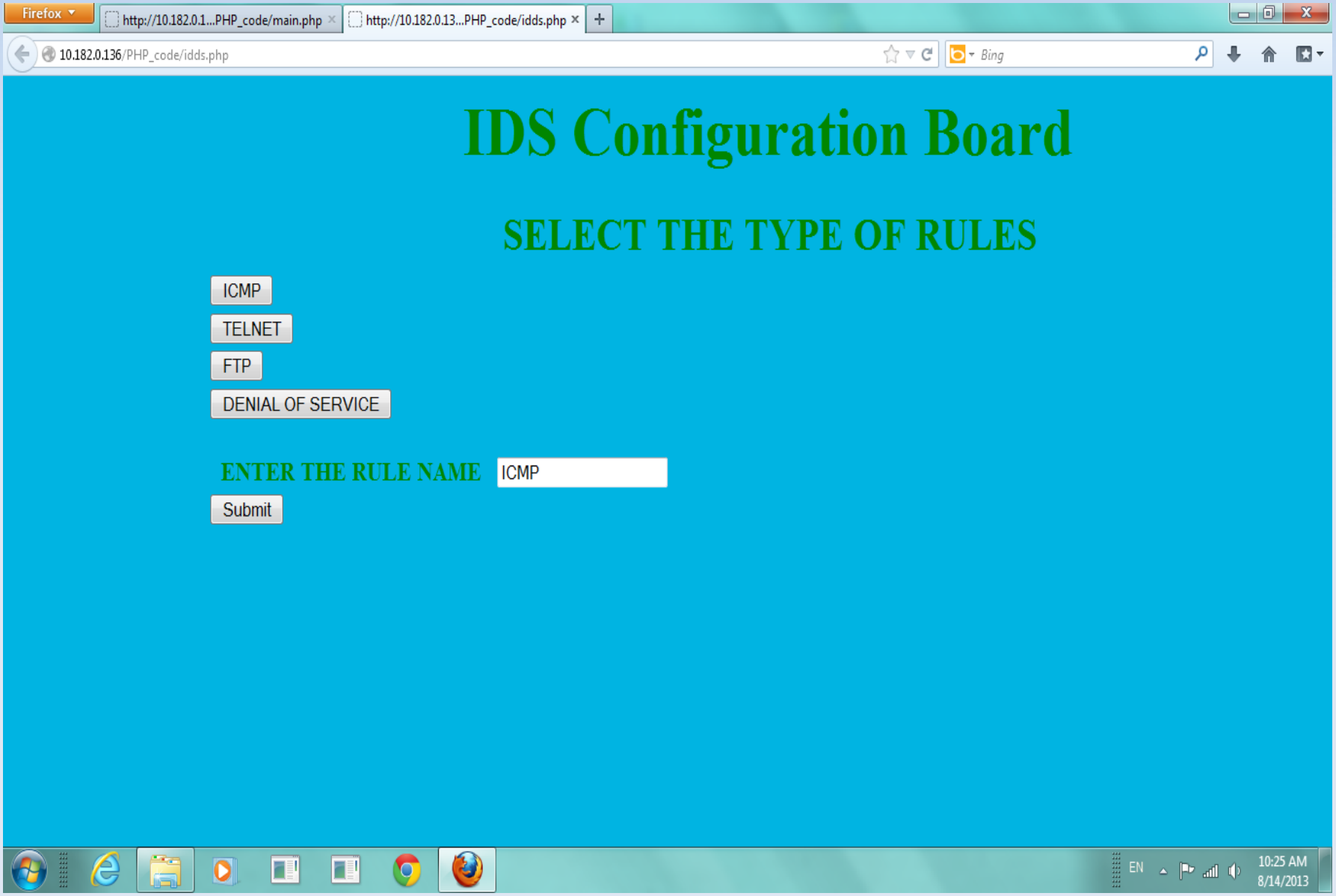
Home Page


Firefox
http://10.182.0.136/PHP_code/main.php
10.182.0.136/PHP_code/main.php
Bing
Intelligent Unified Threat Management (IUTM)
SNORT
FIREWALL
INTRUSION DETECTION
ANTI VIRUS/ANTI SPAM
NETWORK CONFIGURATION
SYSTEM LOGS
UTM represent all-in-one security appliances that carry in a variety of security capabilities including firewall, VPN, gateway anti-virus, gateway anti-spam, intrusion prevention, content filtering, bandwidth management, application control and centralized reporting as basic features. This UTM has a customized of open source software that can provide function of Firewall, Introsion Detection System, Anti Virus / Anti Spam, Network Configuration, Log Analysis and Administrative.
EN
10:21 AM
8/14/2013

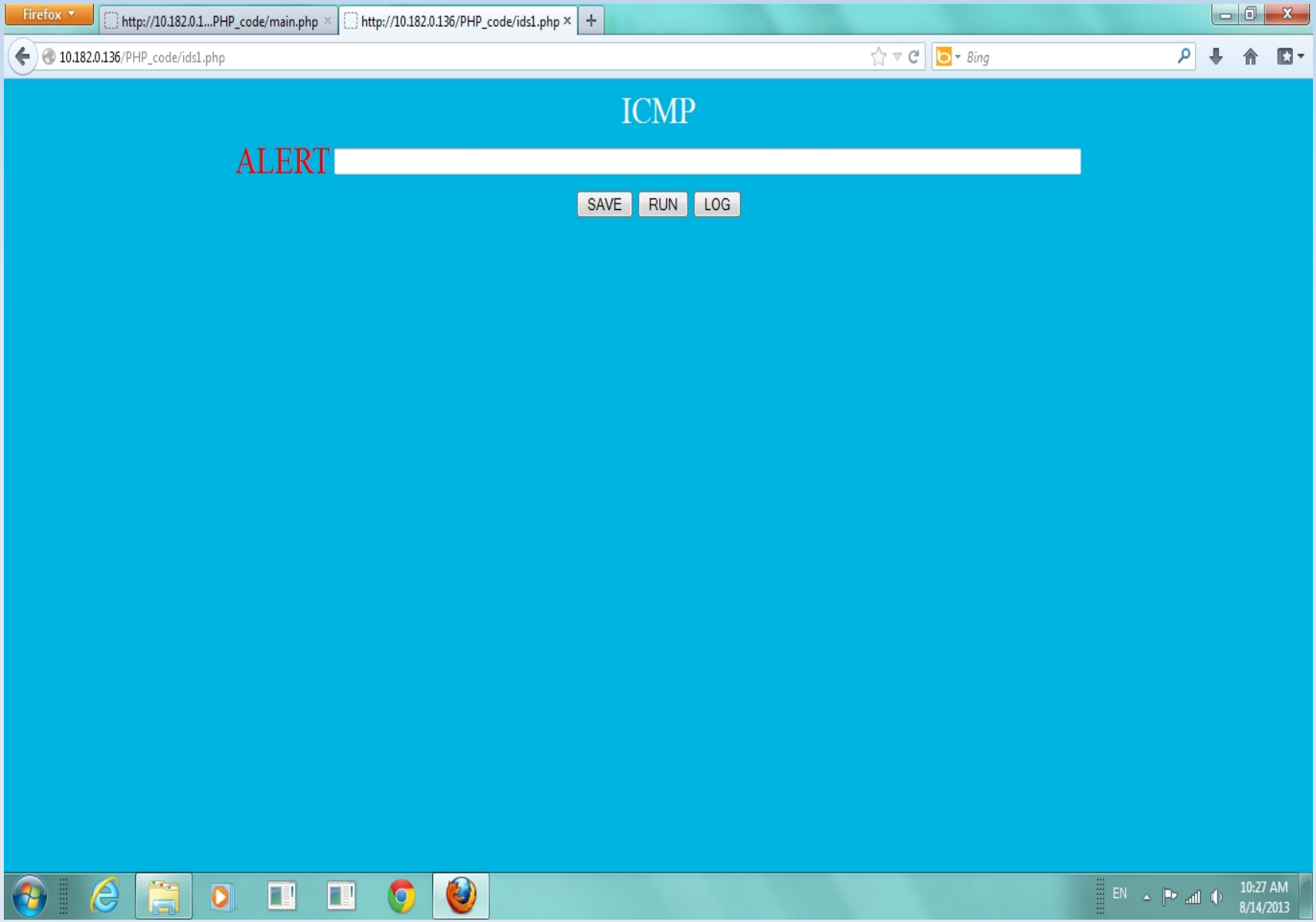
Firewall


Firefox
http://10.182.0.1...PHP_code/main.php
Index
10.182.0.136/PHP_code/ip.php
Bing
FIREWALL CONFIGURATION BOARD
select
select
select
select
select
select
select
select
select
select
select
select
save
flush
run
SHOW
EN
10:23 AM
8/14/2013

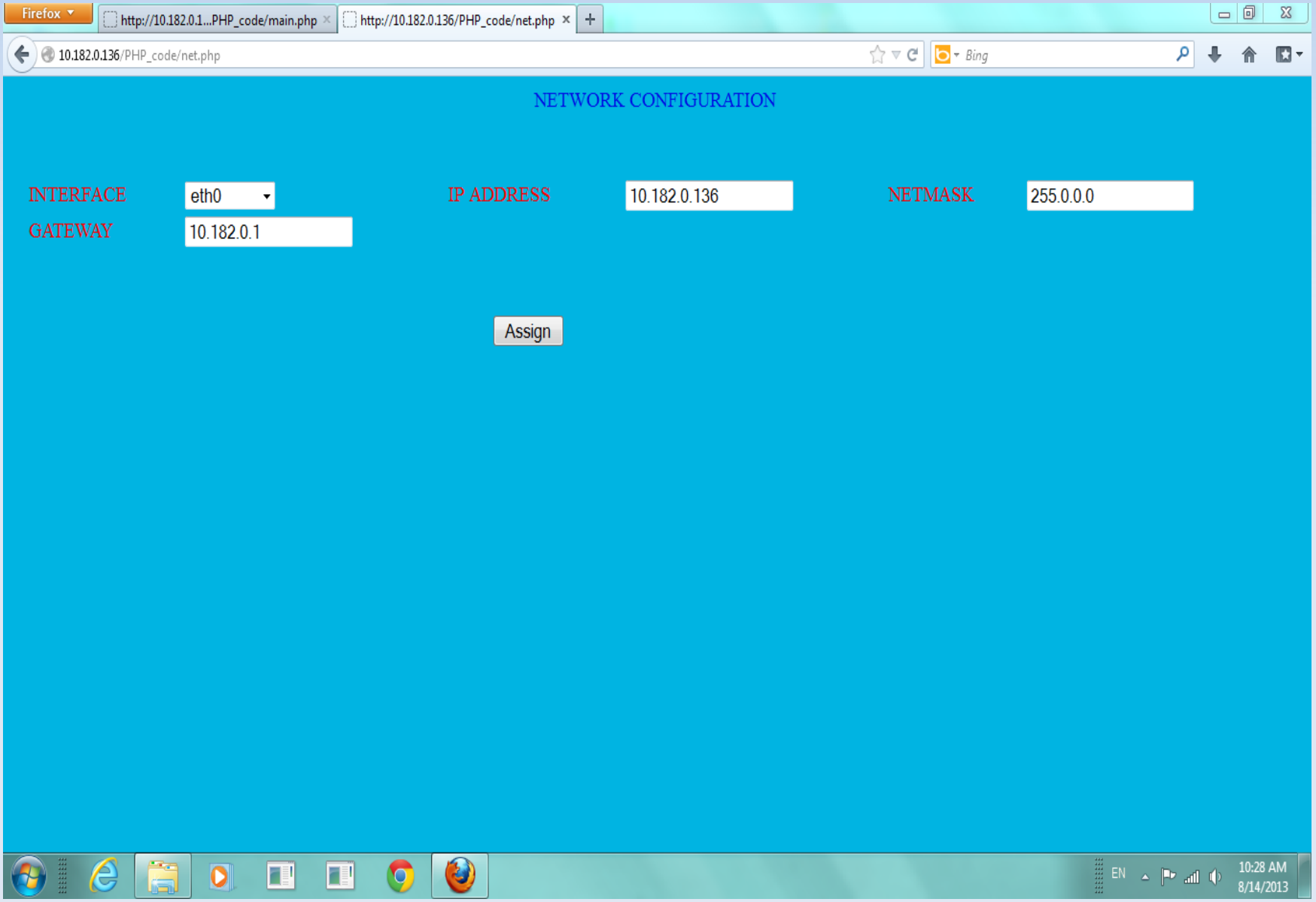
IDS


Firefox
http://10.182.0.1...PHP_code/main.php
http://10.182.0.13...PHP_code/idds.php
10.182.0.136/PHP_code/idds.php
Bing
IDS Configuration Board
SELECT THE TYPE OF RULES
ICMP
TELNET
FTP
DENIAL OF SERVICE
ENTER THE RULE NAME
ICMP
Submit
EN
10:25 AM
8/14/2013

Add Alert


Firefox
http://10.182.0.1...PHP_code/main.php
http://10.182.0.136/PHP_code/ids1.php
10.182.0.136/PHP_code/ids1.php
Bing
ICMP
ALERT
SAVE
RUN
LOG
EN
10:27 AM
8/14/2013

Networking


Firefox
http://10.182.0.1...PHP_code/main.php
http://10.182.0.136/PHP_code/net.php
10.182.0.136/PHP_code/net.php
Bing
NETWORK CONFIGURATION
INTERFACE
eth0
IP ADDRESS
10.182.0.136
NETMASK
255.0.0.0
GATEWAY
10.182.0.1
Assign
EN
10:28 AM
8/14/2013

Question ??
Feedback ??

Thank You