

Intelligent Unified Threat Management (IUTM)

Manas Pratim Sarma

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

CDAC Bangalore



What is IUTM

- Intelligent : Knowledge Based Analysis.
- 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

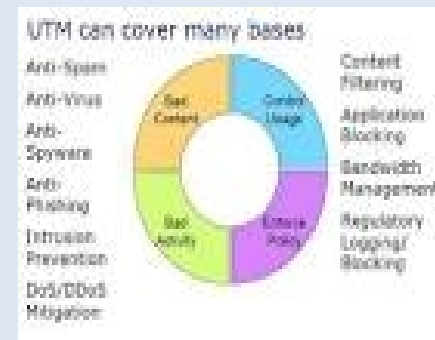
- A Large Organisation No Issue for Buying multiple UTM.
- A Startup IT Company : High Cost of UTM.
- So IUTM is Completely Open Source.
- Based on Integration of Open Source Software.

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

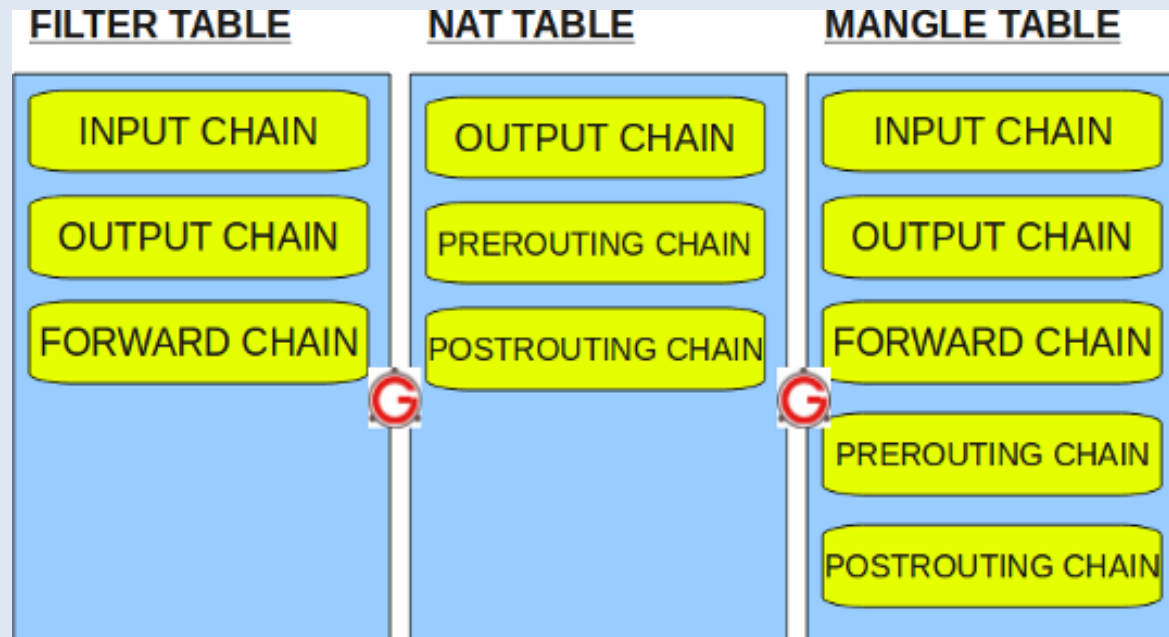
UTM Open Source Components

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



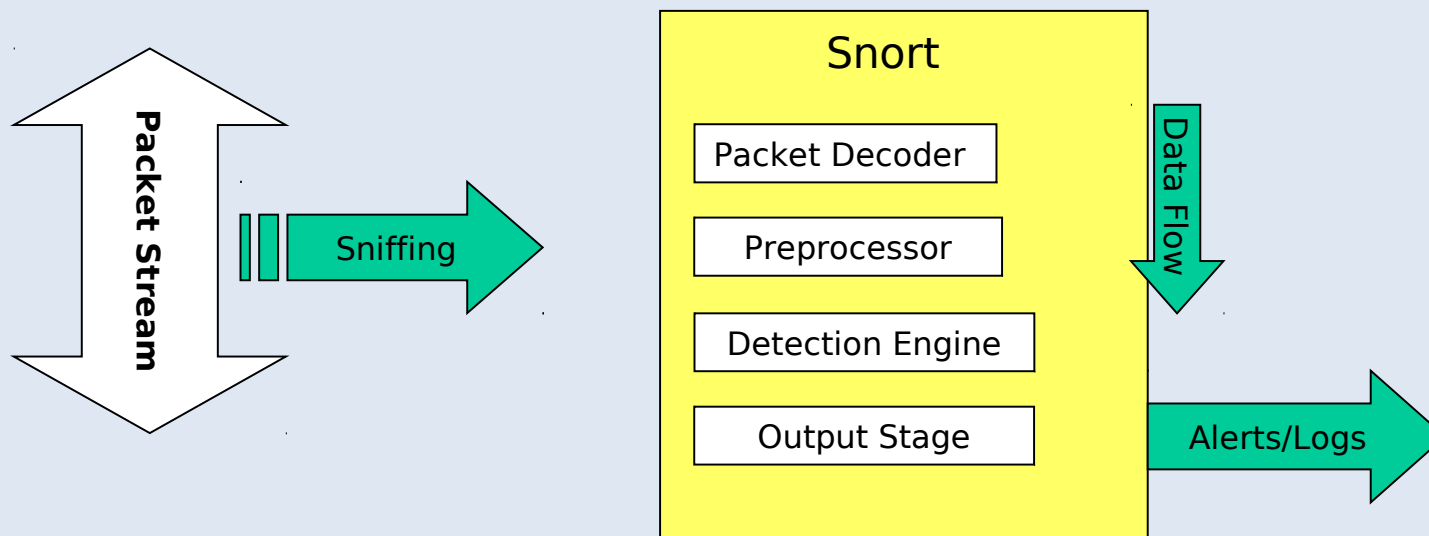
IPtables

- 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 Available in Snort Rule.



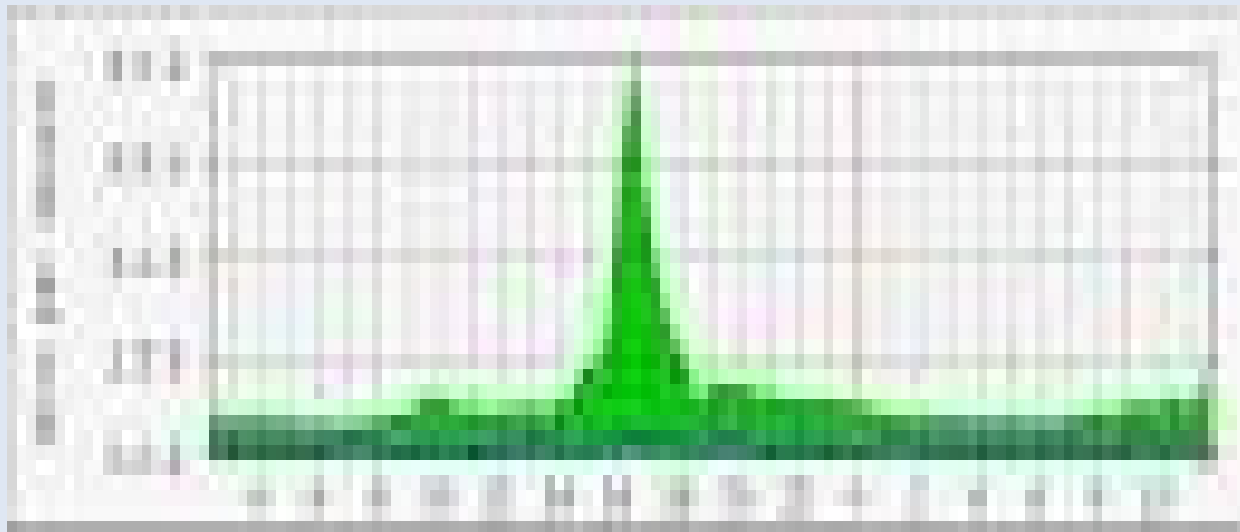
- **CLAM AV**

- 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.

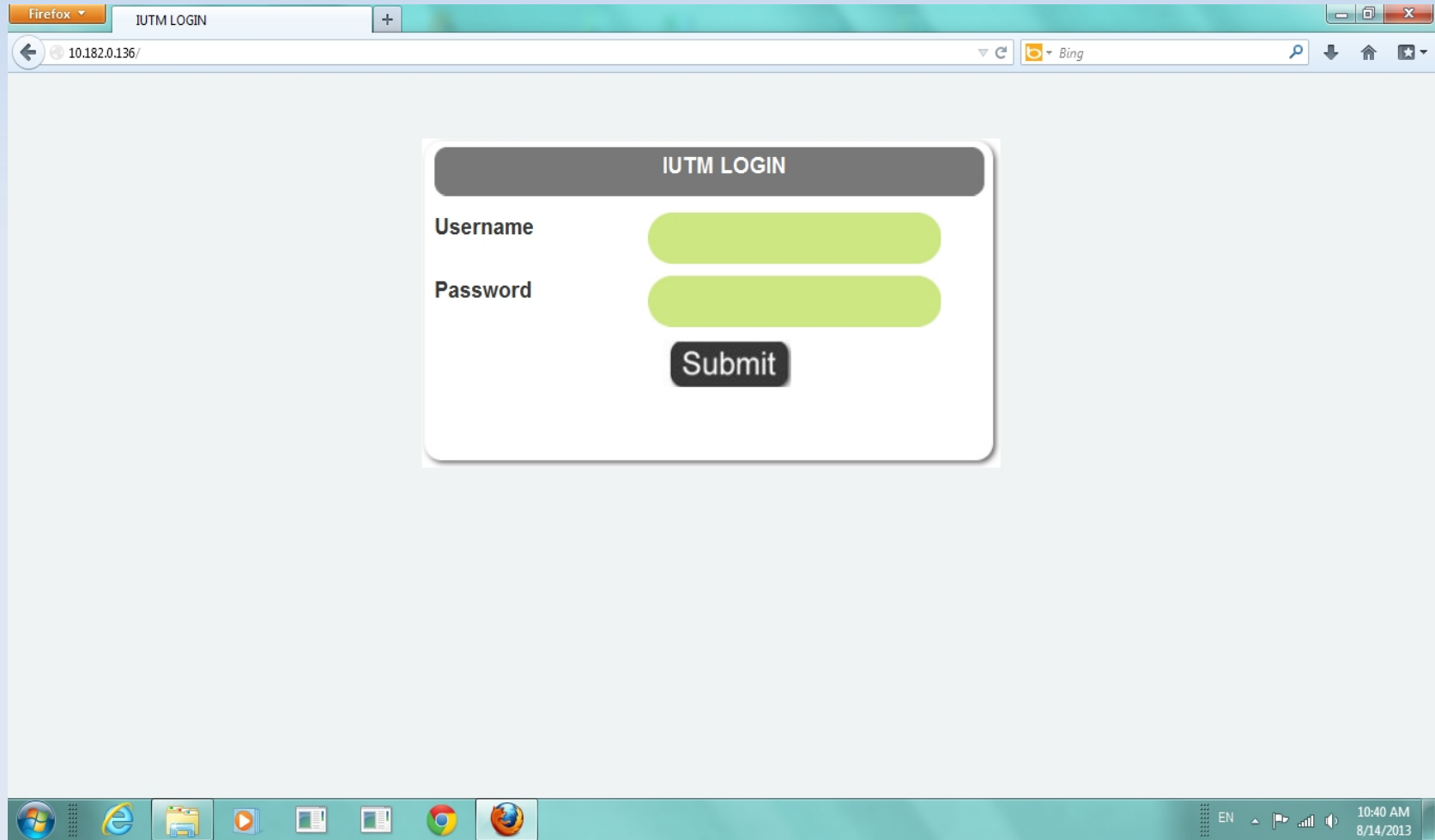


IUTM

- **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




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)



- [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 x 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

The screenshot shows a Firefox browser window with two tabs. The active tab is titled "http://10.182.0.136/PHP_code/idds.php". The address bar shows the URL "10.182.0.136/PHP_code/idds.php". The browser's search engine is set to Bing. The main content area has a blue background and displays the following text and elements:

IDS Configuration Board

SELECT THE TYPE OF RULES

ICMP

TELNET

FTP

DENIAL OF SERVICE

ENTER THE RULE NAME

Submit

The Windows taskbar at the bottom shows the Start button, several application icons (including Internet Explorer, a folder, a media player, and a document), and the system tray with the date and time "10:25 AM 8/14/2013".

Add Alert

The screenshot shows a web browser window with two tabs. The active tab is titled 'http://10.182.0.136/PHP_code/ids1.php'. The address bar contains the URL '10.182.0.136/PHP_code/ids1.php'. The browser's search engine is set to Bing. The main content area has a light blue background and features the text 'ICMP' centered at the top. Below this, the word 'ALERT' is written in red, followed by a long white text input field. Underneath the input field are three buttons: 'SAVE', 'RUN', and 'LOG'. The Windows taskbar is visible at the bottom, showing icons for Internet Explorer, File Explorer, a media player, two document icons, Google Chrome, and Firefox. The system tray on the right shows the language set to 'EN', signal strength, volume, and the date and time: '10:27 AM 8/14/2013'.

Networking

The screenshot shows a Firefox browser window with two tabs. The active tab is titled "http://10.182.0.136/PHP_code/net.php". The address bar shows the URL "10.182.0.136/PHP_code/net.php". The page content is titled "NETWORK CONFIGURATION" and features a form with the following fields:

INTERFACE	<input type="text" value="eth0"/>	IP ADDRESS	<input type="text" value="10.182.0.136"/>	NETMASK	<input type="text" value="255.0.0.0"/>
GATEWAY	<input type="text" value="10.182.0.1"/>				

Below the form is an "Assign" button. The Windows taskbar at the bottom shows the system tray with the date and time "10:28 AM 8/14/2013".

Question ??
Feedback ??

Thank You