



**Linux User Group Meeting June 26<sup>th</sup> 2009**  
**Network Management and Security**

Kyle Spencer – International Medical Group

Simon Vass – E-Tech Uganda Ltd

Reinier Battenberg – Mountbatten Ltd

# What are we going to do today?

- Why and how you waste your bandwidth.
- Cover the basics terms and concepts used for and around Network management
- Demonstrate how to install pfSense Firewall
- Discuss some of the advanced features of pfSense and how they help you management your bandwidth.

# What are we not doing?

- Giving you all the possible options in terms of network management.
- Giving you the equivalent of a Science Degree in Networks.

# Basic Concepts - Terminology

- Firewall – What is it?
- Interfaces – Types?
- Ports & Protocols – Types? SMTP, HTTP, ICMP
- Zones – WAN, LAN, DMZ
- Network Address Translation - Natting
- Rules - Examples
- IP Address + Subnets
- Bandwidth

# Basic Concepts - Firewall

- What is a Firewall?

“A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications.” Wikipedia



- Why have a Firewall?

# Basic Concepts - Interfaces

- Device your computer uses to connect to a network.
- Common Types: - Ethernet, Wireless, Modem

# Basic Concepts – Ports & Protocols

- “In computing, a protocol is a set of rules which is used by computers to communicate with each other across a network. “ Wikipedia
- Common Types: - TCP, UDP, ICMP, DHCP, HTTP, SSH, FTP

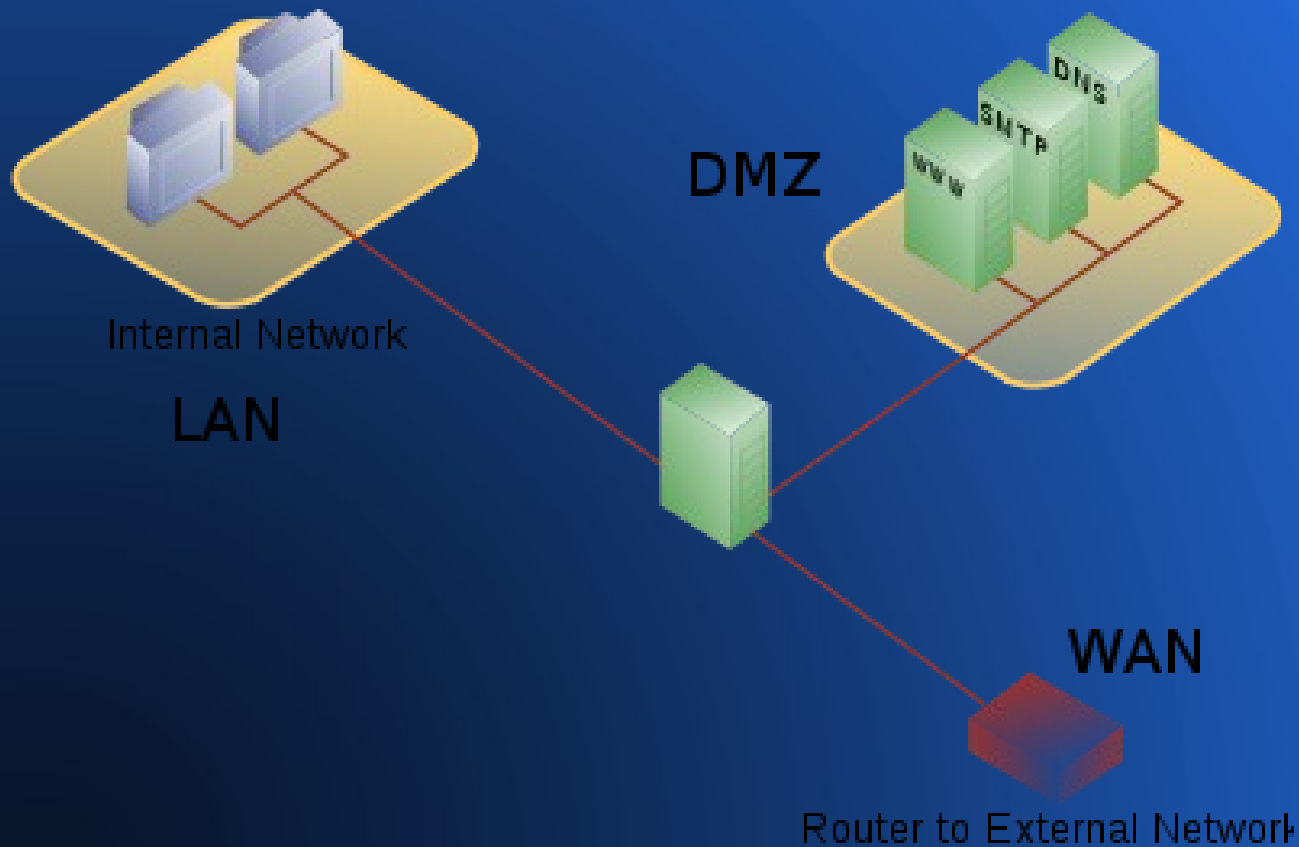
# Basic Concepts – Ports & Protocols

- Ports allow computers to differentiate multiple applications when communicating between machines
- Examples :- Well Known Ports, 25 = SMTP, 80 = HTTP
- Ports are numbered 1 through 65535.

# Basic Concepts - Zones

- WAN – Wide Area Network – usually the Internet
- LAN – Local Area Network – Usually where you users reside
- DMZ – De-Militerized Zone – Wall off area to place Internet facing servers

# Basic Concepts - Zones



# Basic Concepts - Cache

- “Local copy of remote data.”
- Common Type:- Web Cache, Apt-Cache, DNS Cache, Database Cache

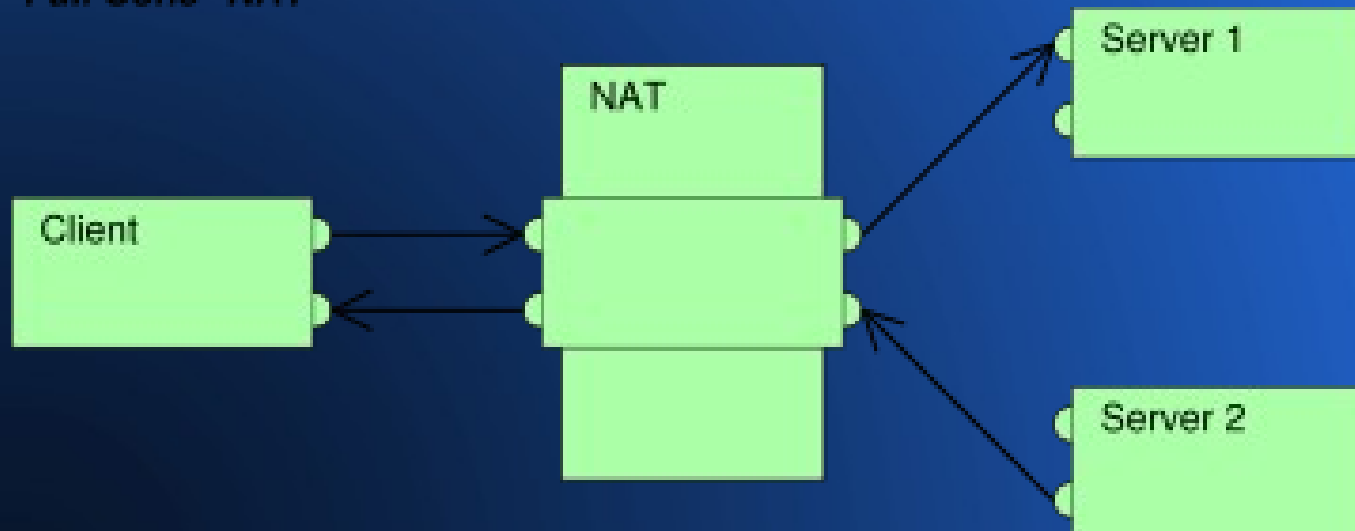
# Basic Concepts - Proxy

- “a computer network service that allows clients to make indirect network connections to other network services” - Wikipedia
- Common Types:- HTTP, FTP

# Basic Concepts – NAT

“...remapping a given address space into another.” Wikipedia

*"Full Cone" NAT*



# Basic Concepts – IP Address and Subnets

- An Internet Protocol (IP) address is a numerical identification and logical address that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes.
- Common Types:- 41.222.5.5,
- Private and public

# Basic Concepts – IP Address and Subnets

- A subnetwork, or subnet, describes networked computers and devices that have a common, designated IP address routing prefix.
- Example:- 192.168.0.x i.e. 192.168.0.2, 192.168.0.3, 192.168.0.4
- Example:- 10.0.x.x i.e. 10.0.10.1, 10.0.10.2 or 10.0.11.1, 10.0.11.2

# Basic Concepts - Rules

- Rules – Security system that uses rules to block or allow connections and data transmission between a computer and the Internet
- Examples:-

Direction	Protocol	Source	Address	Source	Port	Destination	Address	Destination	Port	Action
In/Out	Tcp	Any	Any	Any	10.10.10.0	25				Allow

Direction	Protocol	Source	Address	Source	Port	Destination	Address	Destination	Port	Action
Out	Tcp/Udp	10.10.10.0	Any	Any	Any	Any				Allow

# Basic Concept - Bandwidth

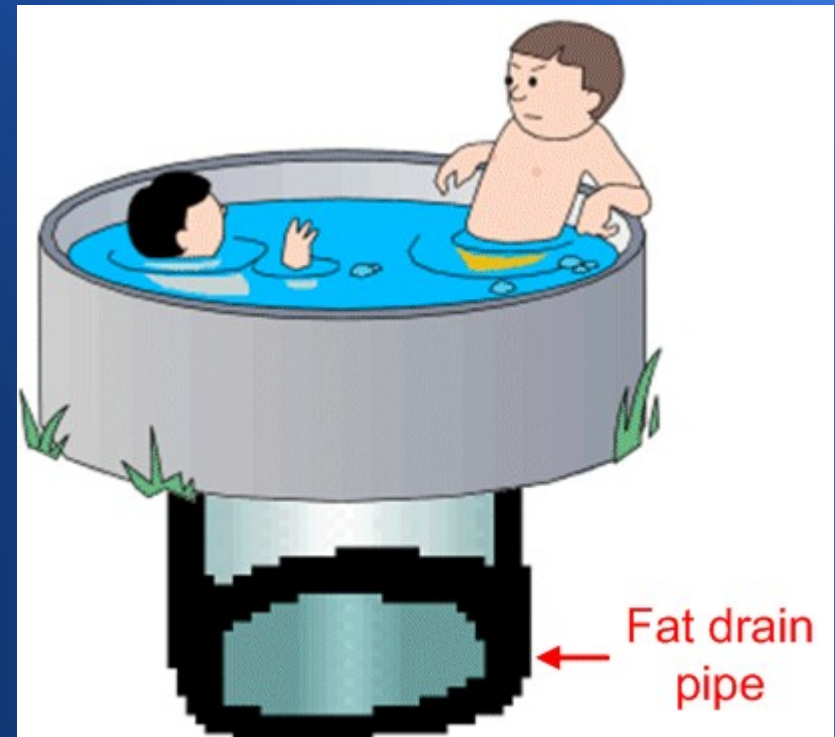
- “In computer networking and computer science, digital bandwidth, network bandwidth or just bandwidth is a measure of available or consumed data communication resources”  
Wikipedia
- Imagine the network wires as pipes - the larger the pipes, the more data can pass through.

# Basic Concept - Bandwidth

- Currently

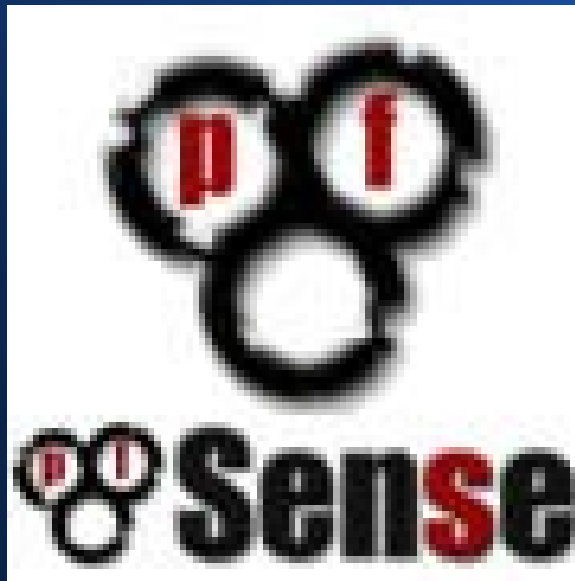


- Post 2009 (Hopefully)



# Demonstration

Installing a Firewall



# Cool Features to manage your bandwidth and security

This by no means is the only way to do it!

- Captive Portal
- Quality of Service
- Intrusion Detect System (Snort)
- Squid Web Cache
- LightSquid Reporting
- URL Blocking & Throttling
- HAVP – Antivirus Scanning

# Captive Portal

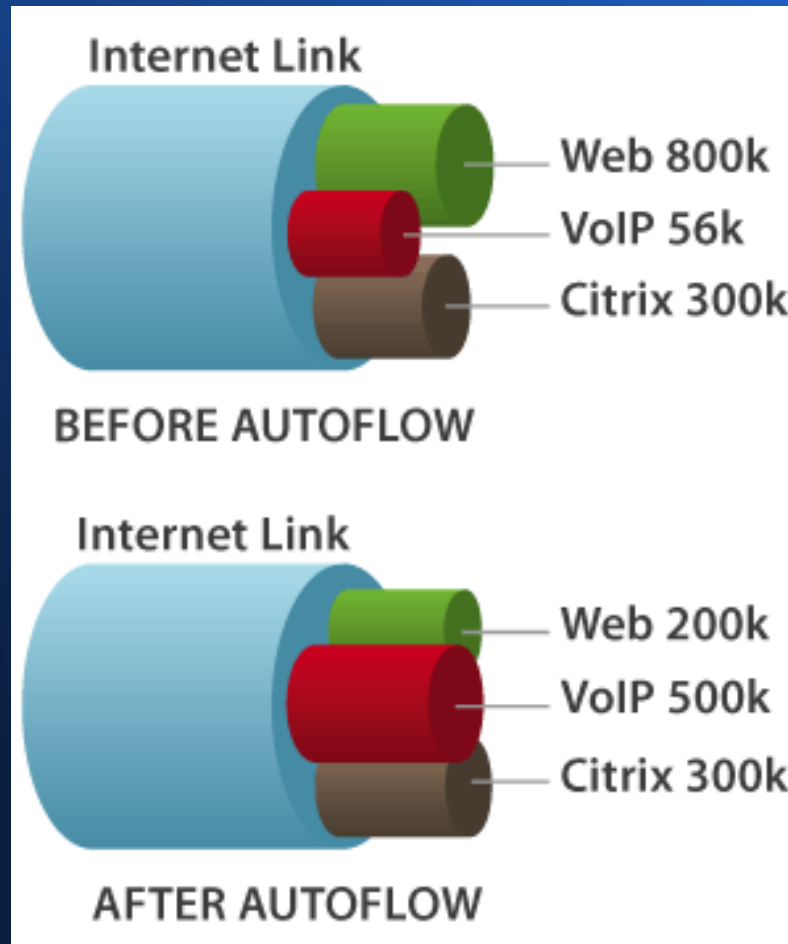
- Restricts access to the Internet on all ports
- User password based authentication
- MAC or IP Address Authentication bypass
- RADIUS Aware

# Quality of Service

- Rule based network traffic prioritization

“Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.” Wikipedia

# Quality of Service



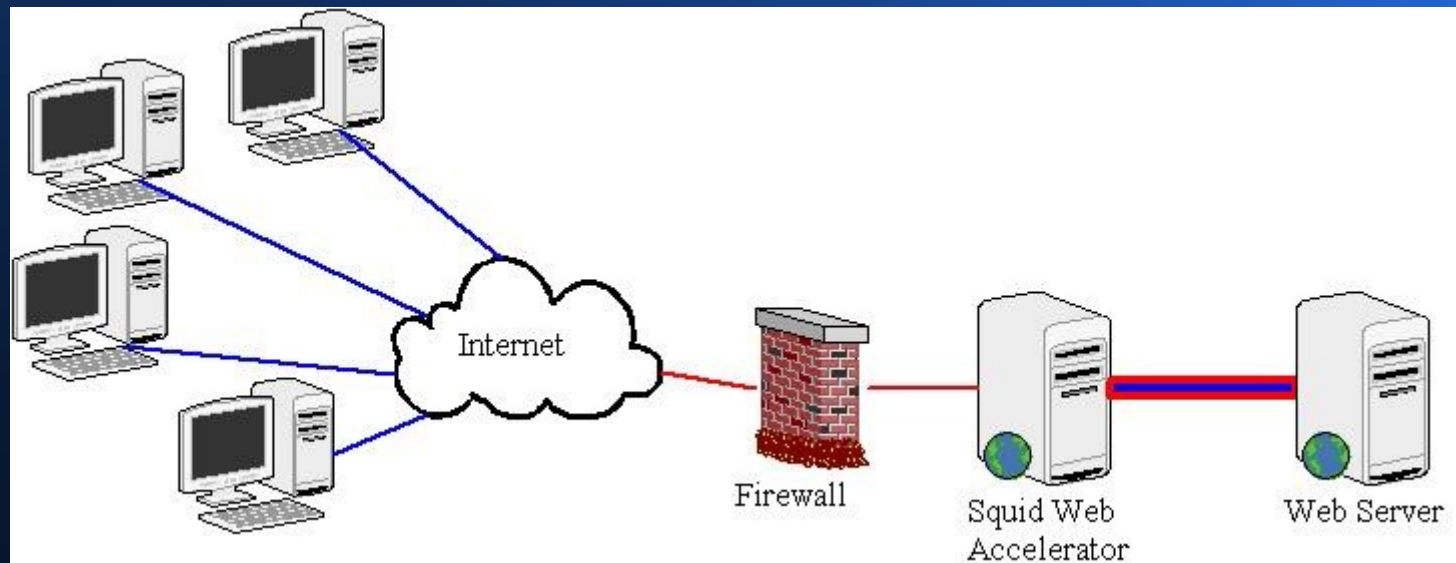
# Intrusion Detect System (Snort)

- Helps stops people from hacking your....network.



# Squid Web Cache

- Keeps a local copy of commonly accessed web content.



# LightSquid Reporting

- Generates reports on Proxy Usage by User and time

**Squid user access report**  
User: **user010 (?)**  
Group: ?  
Date: **27 Apr 2005**

**Total** **16.9 M**

#	Accessed site	Connect	Bytes	Cumulative	%
1	<a href="http://fishki.net">fishki.net</a>	262	5.7 M	5.7 M	33.4%
2	<a href="http://www.fishki.net">www.fishki.net</a>	38	3.5 M	9.1 M	20.3%
3	<a href="http://www.singles.ru">www.singles.ru</a>	78	2.1 M	11.2 M	12.3%
4	<a href="http://my.singles.ru">my.singles.ru</a>	129	1.4 M	12.6 M	8.0%
5	<a href="http://kreis.trl.ru">kreis.trl.ru</a>	34	974 454	13.5 M	5.4%
6	<a href="http://photo.singles.ru">photo.singles.ru</a>	36	698 137	14.2 M	3.9%
7	<a href="http://www.mail.ru">www.mail.ru</a>	123	657 743	14.8 M	3.7%
8	<a href="http://194.67.27.122">194.67.27.122</a>	80	338 379	15.1 M	1.9%
9	<a href="http://194.67.27.124">194.67.27.124</a>	65	318 596	15.4 M	1.7%
10	<a href="http://194.67.27.123">194.67.27.123</a>	55	247 488	15.6 M	1.3%
11	<a href="http://gunpurchase.com:443">gunpurchase.com:443</a>	39	146 254	15.8 M	0.8%
12	<a href="http://counter.rambler.ru">counter.rambler.ru</a>	131	142 469	15.9 M	0.8%
13	<a href="http://213.59.0.100">213.59.0.100</a>	11	117 469	16.0 M	0.6%
14	<a href="http://www.icq.com">www.icq.com</a>	19	88 596	16.1 M	0.4%
15	<a href="http://warlog.info">warlog.info</a>	33	74 090	16.2 M	0.4%
16	<a href="http://www.obozrevatel.com">www.obozrevatel.com</a>	12	72 344	16.3 M	0.4%
17	<a href="http://www.qunpurchase.com">www.qunpurchase.com</a>	51	68 667	16.3 M	0.3%
18	<a href="http://tips.singles.ru">tips.singles.ru</a>	6	64 714	16.4 M	0.3%
19	<a href="http://counter.yadro.ru">counter.yadro.ru</a>	38	64 526	16.4 M	0.3%
20	<a href="http://win.singles.ru">win.singles.ru</a>	3	61 237	16.5 M	0.3%
21	<a href="http://singles.ru">singles.ru</a>	3	61 154	16.6 M	0.3%
22	<a href="http://194.67.27.119">194.67.27.119</a>	107	55 772	16.6 M	0.3%
23	<a href="http://singles.bride.ru">singles.bride.ru</a>	121	42 602	16.7 M	0.2%
24	<a href="http://engine.awaps.net">engine.awaps.net</a>	2	36 614	16.7 M	0.2%

# SquidGuard - URL Blocking & Throttling

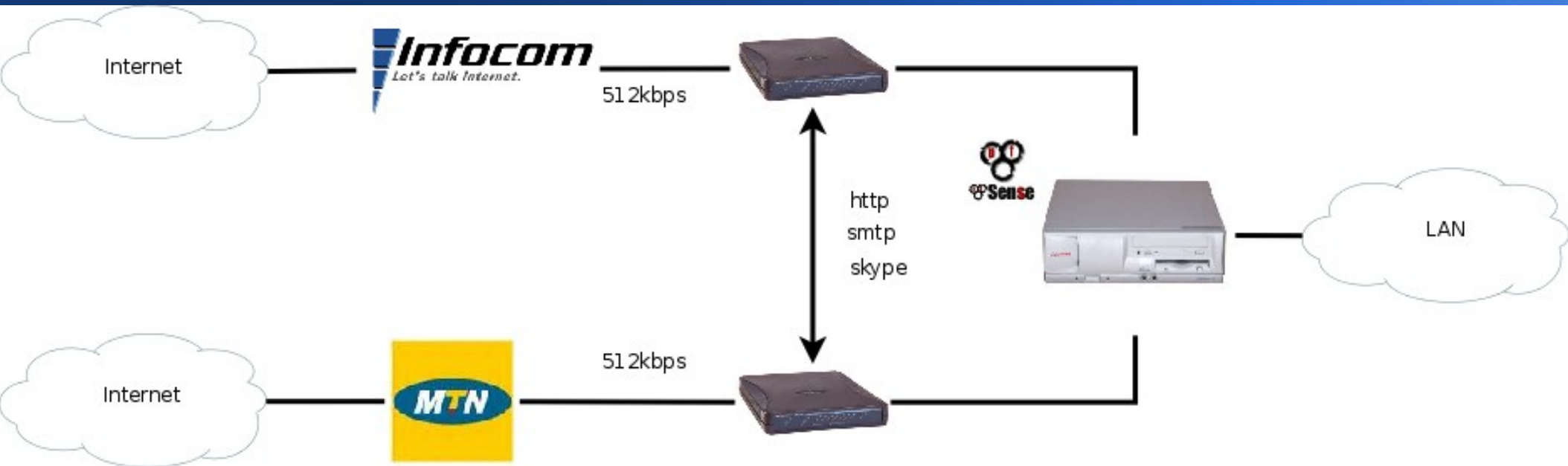
- Ability to Block unwanted websites



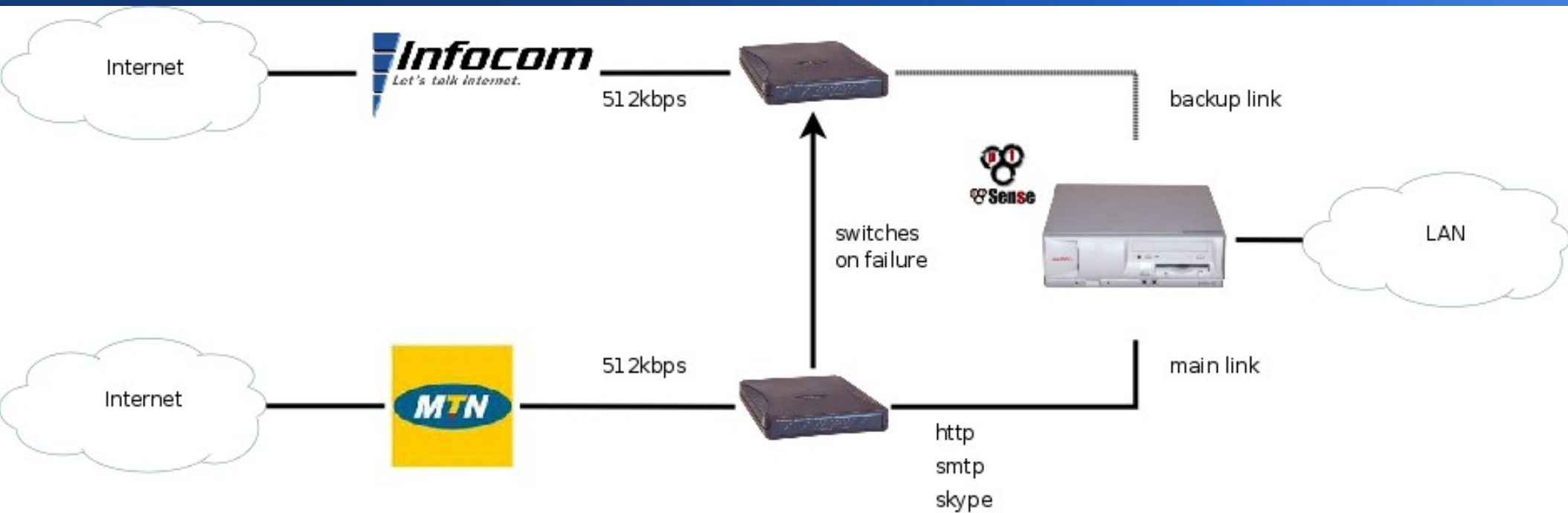
# HTTP Antivirus Proxy - HAVP – Antivirus Scanning

- Scans your incoming traffic for viruses in realtime.

# Load Balancing and Failover



# Load Balancing and Failover





# Q & A

- Any Questions?