BANDWIDTH MANAGEMENT IN SMALL ORGANIZATIONS USING PFSENSE

FRIDAH MUTHIO KAVISA

VICTOR KIMUTAI

THIS PROJECT REPORT SUBMITTED TO THE SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS AT JARAMOGI OGINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY.

DECEMBER 2016

DECLERATION

We, Kimutai Victor and Fridah Muthio**,** hereby declare that this project is our original work and it has not been presented for an award of a diploma or conferment of a degree in any other university or institution.

Signature: …….

VICTOR KIMUTAI

I132/0885/2013

Date……/……/ 2016

Signature: …….

FRIDAH MUTHIO KAVISA

I132/0501/2013

Date……/……/ 2016

This project has been submitted with our approval as university supervisors

Supervisor Name:…….....Signature…….Date……/……./2016

DEDICATION

We dedicate this project to our families and friends

ACKNOWLEDGEMENTS

We thank God for giving us good health and strength during this project time, a lot of efforts have gone to developing this project till completion. However it would not have been possible without the kind support and help of many individuals. We would like to extend our sincere thanks to them all.

We are highly indebted to Jaramogi Oginga Odinga University of Science and Technology fraternity especially the school of informatics and innovative systems for their guidance and constant supervision as well as providing necessary resources regarding the project and also for the support in completing the project.

We would like to express our gratitude towards our parents for their kind co-operation and constant encouragement which helped in completion of this project

We would also like to express our special gratitude and thanks to our supervisor Mr. Paul Abuonji for giving us his undivided attention and time during the lifetime of this project.

Our thanks and appreciation also goes to our colleagues who shared with us ideas and gave us moral support and all who have willingly helped us out with their abilities.

Special thanks also go to our friend Charles Mapelu for lending us his laptop for use in the completion of this project.

God bless you.

ABSTRACT

Small organizations are growing rapidly with the current economy with each of them wanting to achieve high profits and minimize of their cost of expenditure. The growing digital error has seen each small organization having to adopt the use of technology in order to perform their operations efficiently. Every small organization faces the challenge of bandwidth management since most of them are focus mostly on the operations that seem to give quick returns. Most of the small organizations spend a lot of funds on purchasing bandwidth not knowing that bandwidth however much they purchase bandwidth it can never be enough until it is managed. Bandwidth management reduces the cost incurred by small organizations in purchasing bandwidth.

In this project, we address the problem of bandwidth management in small organizations and propose efficient economic-based solution in order to deal with these issues at different bandwidth management levels, and hence enhance the QoS support the small organizations' network. Specifically, we propose pfsense firewall to be used for bandwidth management in a small organization environment. The firewall is configured to support multiple classes of traffic with different users having different QoS requirements, maximize speed of traffic of some services with reserved bandwidth in some queues, support inter- and intra-class fairness, prevent network congestion and maximize the network operator's revenues. The framework consists of three related components, namely packet scheduling, bandwidth allocation and limiting. On implementing this project, CBQ scheduling method was able to be used, limiting of bandwidth to specific queues, blocking of some services from some queues like Facebook in the transport and customer care department. Captive portal was configured and we were able to authenticate users in the network and reject the ones that didn't have an account in the Radius server. Ntopng packet was installed and it helped in accounting for bandwidth usage by different departments of the organization with details of why and what is using the bandwidth. By efficiently managing the network's bandwidth prior to users' admission (i.e., pre-admission bandwidth management) and during the users' connections (i.e., post-admission bandwidth management), these schemes are shown to achieve the design goals of our project.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

SMEs	-Small and Medium enterprises
QOS	-Quality of service
HTTP	-Hyper Text Transfer Protocol
HTTPS	–Secure Hyper Text Transfer Protocol
FTP	-File Transfer Protocol
CEO	-Chief Executive Officer
ISP	-Internet Service Provider
DNS	-Domain Name Server
GPS	-Global Positioning System
WAN	-Wide Area Network
LAN	-Local Area Network
RSVP	-Resource Reservation Protocol
SMTP	-Simple Mail Transfer Protocol
TCP	-Transport control Protocol
FIFO	-First In First Out
CBQ	-Class Based Queuing

ATM	-Asynchronous Transfer Mode
SNMP	-Simple Network Management Protocol
HTML	-Hyper Text Markup Language
CPU	-Central Processing Unit
SQL	- Structured Query Language
DPI	-Deep packet inspection
IP	-Internet Protocol
ACL	-Access Control List
MAC	-Media Access Control
NAT	-Network Address Translation
RSVP	-Reservation Protocol
RAM	-Random Access Memory
KBPS	-Kilobytes per Second
URL	-Universal Resource Locator
IPV4	- Internet Protocol Version4
ICMP	- Internet Control Message Protocol
RRD	- Round-Robin Database

CHAPTER 1

INTRODUCTION

1.1 Background Information

According to World Bank standards small organizations are defined as those organizations with at least 10 number of employees and at most 50 employees. (Ayyagari, M. et al. 2015)

The concept of SMEs varies from one country to another depending on the indicators used (Visser, 1997).The first criteria, based on the number of employees, defines SMEs as those enterprises below a certain number of workers (i.e. can range from more than 10 to l less than 50 employees).The second criterion defines the SMEs as the degree of legal formality, and has been used to distinguish between the formal and informal sectors. The third criterion defines SMEs as based on the limited amounts of capital and skills per worker, (Ong'olo & Awino**,** 2013).

The Internet has revolutionized the way the world does business on both a local and global level. From recruiting employees to gathering data on the competition, the ways businesses utilize the Internet are numerous, as are the benefits of the Internet to the business community. While computers have been blamed for decreased activity and interaction in the local community, the Internet has been credited with providing a window into the global world. It allows anyone with a computer to think globally and has allowed the business world to forge international relationships with new vendors (to lower costs) and new customers (to increase sales) (Bryant, 2016).

100 years ago it might have taken over a month to get a letter to a friend in another country. Today, communication is as easy as a mouse click, and much cheaper too. Anyone in the world can communicate with another person through text messages, emails, and even live video. For business, this means higher efficiency and quicker processing of sales. Perhaps the most obvious benefit of the Internet is cost savings. Information at faster speeds saves time, which either saves or makes money. Many functions in the business process, i.e. bookkeeper, have been automated, which has helped to streamline processes and reduce the cost of labor, (Bryant, 2016).

A great small business high speed internet solution provides the perfect platform for your company's telecommunications. Businesses of all sizes are increasingly turning to hosted VoIP phone systems to take advantage of their many features and low costs. With dependable high

upload and download speeds, call quality matches or exceeds that of traditional copper wire phone systems, plus you can make use of great features like audio conferencing, automated call routing, and seamless mobile integration. You'll wonder how you ever got along without the benefits of a great hosted phone system. (Lahrssen, 2014)

Small organizations are under pressure to provide their staff with reliable Internet access. As Internet connectivity is increasingly becoming a strategic resource for organizations, a robust small organizations' network with good connectivity to the Internet is no longer a luxury to a small organization in actual fact, it is now a basic necessity. Internet connectivity is critical for any small organization achieve the core objectives of the business. Internet connectivity provides a gateway to vast amounts of information from the information highway and thus provides support and enhances good association between an organization and their clients as well as organization with other organizations. Under a normal circumstance an organization sets aside a significant fraction of its budgets towards increasing its bandwidth and upgrading its network. Despite considerable investment in bandwidth, an organization will still find itself not having a reliable, usable Internet access for their staff. (Chitanana, 2012)

The demand for bandwidth within organizations is constantly rising and the overall bandwidth usage continues its upward trend. This demand is caused by, among other things, communication which has rose to be very depended on the internet, the increased use of electronic resources for business deals including video conferencing, and the spread of desktop applications that can use practically any amount of bandwidth given to them. (Chitanana, 2012)

Organization's internet is supposed to be available during all the working hours of the day. To maximize the usage of the network connection services its use must be managed and monitored. There are a vast number of network monitoring, capturing and analysis tools available but before using any of them it is a good idea to pause and decide when and how to apply them.

Since bandwidth is a strategic resource, the efficient usage and management of such a resource should always be a priority. Without bandwidth management, mission critical applications would be starved of bandwidth, disrupting services that impact the operational activities of organizations. As such, this project is meant to illuminate the bandwidth management strategy that organizations should employ. (Chitanana, 2012)

Internet usage is now ubiquitous in every modern business. When employed properly it can be an extremely efficient and highly effective productivity enhancer. With the Internet, employees can keep tabs on critical changes, perform research and any number of business tasks. Email, another aspect of the Internet, allows for near instantaneous communication of business data. If either is unavailable, even for short periods of time, you can almost hear the grinding of gears as the entire enterprise comes to a halt. System failure is not the only potential problem however, unscrupulous or apathetic employees who choose to forget what the Internet and email are there for, can be just as damaging. (GFI Software, 2011).

Whether your business is a hotel, restaurant, sports arena, transportation hub or the like, operators are facing unprecedented demand on bandwidth. With many users carrying multiple Wi-Fi-enabled devices and expecting Internet access for each one, it becomes crucial to manage bandwidth properly. Bandwidth management allows you to control the amount of bandwidth available to your patrons. Used correctly, bandwidth management ensures that each user receives a fair share of bandwidth. (Nomadix, Inc. 2016)

Bandwidth management is the process of measuring and controlling the communications (traffic, packets) on a network link, to avoid filling the link to capacity or overfilling the link, which would result in network congestion and poor performance of the network. Among other techniques like quality of service (QoS) bandwidth management is used to prioritize network traffic. (Kithinji, 2016)

Bandwidth Management relies on user-defined bandwidth classes and policy rules to manage the available bandwidth coming into or out of the ProxySG appliance. There are four characteristics of bandwidth classes - minimum bandwidth, maximum bandwidth, priority, and parent designation (used to configure class hierarchies). Minimum bandwidth works by guaranteeing a predefined amount of bandwidth (if available on the network) to the class. Similarly, maximum bandwidth limits the amount of bandwidth that a particular class may use. Classes can also be prioritized so that certain traffic receives bandwidth before others. To implement minimums or prioritization, a class hierarchy must be created with a maximum bandwidth allocation. This allows the appliance to determine how much bandwidth is “too much” for a low or medium priority bandwidth class. Creating class hierarchies provides the most flexibility for Bandwidth Management. Class hierarchies allow administrators to apply classes at a granular level, taking

various criteria into consideration to determine the final bandwidth allocation allowed. To determine which class to assign to a particular connection, the ProxySG appliance evaluates the configured policy to determine if any of the connection attributes match the policy rules assigned to bandwidth classes. (Blue Coat, Inc. 2007)

For instance an administrator managing a branch office wants to ensure that no more than half of the total bandwidth available is used for HTTP or FTP traffic to guarantee that other business critical applications continue to function. However, when the CEO visits this branch office, she should have priority over other employees when using this allocated bandwidth. To accomplish this, the administrator creates a bandwidth class Branch Office and configures the maximum bandwidth to an amount equal to half of the total available bandwidth. Creates a policy rule for the Branch Office class, assigning all HTTP and FTP traffic to this bandwidth class. Creates two additional bandwidth classes Employees and CEO and sets the appropriate priorities. Creates policy rules identifying the CEO and "everyone else"; these rules assign such traffic to either the Employees or CEO bandwidth class. Makes the Branch Office class the parent class of both the Employees and CEO classes. The administrator now has a bandwidth hierarchy. Bandwidth is limited by the configuration of the parent class, and the two child classes are prioritized to determine how they share any unused bandwidth. Because no minimums have been set, the highest priority class has the first opportunity to use all of the available bandwidth; whatever is left then goes to the next priority class. The following figure gives a simple view of the classification of bandwidth in a branch of an organization. (Blue Coat, Inc. 2007)

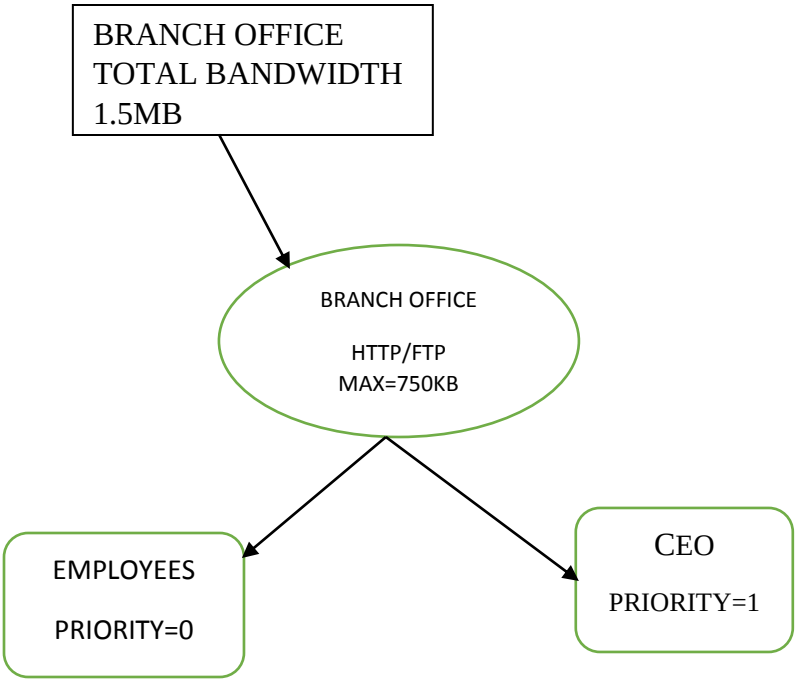


Figure 1: Sample classification of bandwidth in a branch of an organization.

Source: author's conception

1.2 Problem Statement

Employees in small organizations in most cases experience slow internet connection while performing their duties at work and a limited access to the wireless network while roaming around the organization's premises. This annoys the staff since they cannot rely on internet (as a resource) provided by the organization to perform their duties and other work related research. This is caused by uncontrolled access to the network and poorly managed bandwidth.

Providing a big pipe or larger bandwidth to the internet does not solve the issue of traffic and network performance on users or application used in the network. Nowadays, internet misuse in the workplace is increasing at a high risk. It has become one of the major problems in an organization.

The largely unrestricted access exposes the organization's Internet connectivity to bandwidth-hogging applications such as Internet gaming, peer-to-peer (P2P) file sharing and media streaming. Audio and video streaming applications embedded in Web sites like YouTube have grown in popularity among members of staff. Although organizations may increase their Internet

capacity by purchasing additional bandwidth from one or more Internet Service Providers (ISPs), it is very expensive to do so because the price of bandwidth in Kenya is still exorbitantly high. No matter how much more bandwidth is bought, a point will be reached when one can no longer buy more bandwidth and therefore the need to look to bandwidth management is necessary. Furthermore, increasing Internet capacity cannot be done affordably considering the rate at which unmanaged applications consume it.

It is due to these problems that we propose that the small organizations implement the use of pfsense firewall to manage their bandwidth and control network activities

1.3 Objectives

The main objective of this project is to implement a system that would help in managing bandwidth in small organizations.

1.3.1 Specific objectives

i. To prevent unauthorized access to the organizations' network or bandwidth
ii. To prevent unauthorized use of organization's bandwidth by authorized users
iii. To account for bandwidth usage in the organization.

1.4 Research questions

i. How do small organizations prevent unauthorized access to the organizations' network or bandwidth?
ii. What do small organizations do to prevent unauthorized use of organization's bandwidth by authorized users?
iii. Do small organizations account for their bandwidth usage?

1.5 Justification of the project

The need for this project is driven by various challenges faced by small organizations due to unauthorized access to the network, inappropriate use of existing bandwidth and absence of

bandwidth management strategies. That has promoted bandwidth wastage on unwanted traffic such as music and movie download by some users.

This project is designed to make sure that the available Internet facility is effectively and optimally used to support the core business of an organization that is, maximizing profit while minimizing expenditure.

1.6 Assumptions of the project

The subject organization has more than 10 employees and less than 50 employees

The organization is running on 10Mbps

The subject organization is running the following services DNS server, web server and mail server.

The subject organization exercise bring your own device policy.

1.7 Limitations of the project

Time: The time allocated for the project to be undertaken was not sufficient to cover exhaustively all aspects related to the project. However we were able to overcome this by doing intensive research and using the help of our able supervisor.

Funds: The research was basically financed through personal resources which were scarce. This was overcome by utilizing the easily available resources like computer labs and the university library.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Bandwidth management is a process helps an administrator in an organization to allocate bandwidth resources to critical applications on a network. By doing this helps in preventing some applications or users from taking control of all available bandwidth and prevent other applications or users from using the network. Network traffics that comprises in the network applications layer is impossible to differentiate its type among all network traffic. Thus it is also impossible to control which users or applications have priority on the network. Applications can also require a specific quantity and Quality of service (QoS) that cannot be predicted in real time available bandwidth on a network. This can make some applications run poorly if bandwidth is not properly allocated to them when necessary (Kassim, et al 2012).

Bandwidth management is about ensuring the best possible user experience end-to-end for all voice and video endpoints, clients, and applications in the Collaboration solution. (Cisco Systems, Inc. 2015)

There is an increasingly larger number of businesses that monitor what their employees do on the Internet in the workplace, with studies revealing that about half of all corporations routinely use various methods from email monitoring and website blocking to phone tapping and GPS tracking, combined with policy to manage productivity and minimize litigation, security, and other risks. Whether or not employers should engage in this practice or not often leads to a serious and spirited debate that puts an individual's right to privacy vs. the organization's right to security at the center of the controversy (GFI Software, 2011).

Bandwidth management is a general term given to a collection of tools and techniques that an organization can use to reduce demand on critical segments of networks. Often bandwidth management may be applied on the WAN segment that connects the organization to the greater internet. It may be applied on critical internal segments.

Most routers provide only best effort services and packets are treated in first in first out manner. Traditionally routers treat all the packets without any guarantees in a best effort model. In this model the router delivers packets without nay performance guarantees. On a shared network link,

this model allows users to transmit packets through the network without any limitations. This means that the performance of a network relies not only on the capacity of the link, but also on the amount of traffic each user puts into the network link. This means a single user running bandwidth intensive applications can consume a large portion of bandwidth, thus starving other users (Snehalatha, Julia & Rodrigues, 2013).

2.2 Methods of Bandwidth Management

The bandwidth is always finite and is an important system resource. Cheap and abundant bandwidth may be available in the future**,** but at present, we have to manage the bandwidth to use it efficiency. According to (Li, 1999) the following are some of the methods of bandwidth management that can be adopted.

2.2.1 Bandwidth allocation and dynamic bandwidth allocation

A system made up of the users as well as the network, has various resources that can be used to meet service demands. However, in ail realistic systems these resources are limited and some methods of allocating them is needed when told demand is greater than the resource limit. Bandwidth allocation is about efficiently allocating the network bandwidth among the sources. Dynamic bandwidth allocation refers to techniques that allocate bandwidth according to instantaneous demand. For example, a typical TDM (Time Division Multiplexing) network would require separate allocation of bandwidth for the voice and data. Dynamic bandwidth techniques allow data ta burst into the unused voice bandwidth, as it becomes available and force data to back off as voice connections are activated.

2.2.2 Bandwidth Sharing and Dynamic Bandwidth Sharing

The bandwidth sharing method relies on sharing the link bandwidth among a number of connections using one of the following methods:

1. Fair bandwidth sharing is based on sharing the link bandwidth among the different connections.
2. Bandwidth scheduling assigns a limited amount of bandwidth to a number of connections according to specific scheduling time dots.

Dynamic bandwidth sharing methods which rely on increased sharing of resources would yield better utilization of the network bandwidth. The burst nature of data traffic could be exploited by

allowing some users to consume the bandwidth during other users' ide
periods.

2.2.3 Bandwidth borrowing

If the whole bandwidth is assigned to all class of packets, each class is allocated a percentage of the bandwidth. When that limit is reached, normally no more traffic from that class can be forwarded. However, if the network link is not being fully used, a class can borrow bandwidth temporarily from its neighbor class, and send traffic at a percentage that exceeds its allocation. The configuration of a class defines the maximum percentage of bandwidth, including that borrowed, that can be used by a class at any time. Spare bandwidth is allocated temporarily to classes having the highest priority. The proportion of the spare bandwidth given to a class depends on the percentage of bandwidth configured for the class.

2.2.4 Bandwidth Reservation

Bandwidth reservation means that a request is made to the network to allocate a specific amount of bandwidth for data flow. It allows applications to reserve bandwidth and QoS along the data path. Many new content-rich applications, such as video conferencing, interactive multimedia video games or training programs, need stable, predictable QoS in terms of bandwidth and delay in order to function well. Bandwidth reservation protocol is based on the standard network control protocol RSVP (Reservation Protocol) which allows internet/intranet applications to reserve special QoS for their data. RSVP was proposed by the Internet Engineering Task Force (IETF), and is emerging as a standard protocol for bandwidth management. It is a component of the future Integrated Services (IntServ) in the Internet. When an RSVP-enabled multimedia application receives data for which it needs a certain QoS, it sends an RSVP request back along the data path, to the sending application. At each stage along the route, the QoS is negotiated with the routers or other network components. Non-RSVP network equipment simply ignores RSVP traffic and takes no part in the negotiation.

2.2.5 Preventing Bandwidth Starvation

Bandwidth can be controlled by simple mechanisms such as guarantees and limits. However, priorities provide the most powerful and flexible method to dynamically allocate limited bandwidth. The objective of priorities is to grant preferential privileges to one class of traffic over another. For example, a network manager could grant a higher bandwidth priority for Web traffic than SMTP traffic.
There are two types of bandwidth priorities: absolute and weighted. Absolute priority means to assign a priority level to each class of traffic. For example, if there are seven priority level available for Internet traffic, Web traffic may be given a priority of 7, and SMTP traffic assigned a priority of 6.AbsoIute priority is inefficient because it operates on an all or-nothing basis. When the tine is oversubscribed, al1 higher priority traffic gets through before any lower priority traffic receives bandwidth. As a result, heavy Web usage may deny bandwidth to all SMTP connections. This situation is defined as bandwidth starvation. In order to avoid bandwidth starvation, we have to use weighted priority. Weighted priority allocates available bandwidth based on relative merit or importance. When using weighted priorities, each class of traffic is given a weight that is relative to al1 other weights defined in the management policy. The weights define the basis upon which traffic competes for available bandwidth. For example, Web traffic can be assigned a weighted priority of 60, and SMTP traffic can be given a weight of 20. When bandwidth resources are oversubscribed, the ratio of Web traffic to SMTP traffic is accurately maintained at a 60:20 ratio. Weighted priority provides the only mean to prioritize traffic and prevent starvation.

2.2.6 Bandwidth pricing and Dynamic Bandwidth pricing

The bandwidth allocated to a user is considered to be a commodity, which is sold by the network to the user. We view the users as placing a benefit, or willingness-to-pay, on the bandwidth they are allocated. Given a price per unit of bandwidth, a user's benefit function completely determines that user's traffic input. Users are assumed to act in their own best interests and to be capable of responding to changes in the price for bandwidth. Assigning dynamic priority is difficult. If the real-time applications such as voice and

video are given priority to ensure timely delivery, then data traffic may suffer higher loss though it may not be able to tolerate ceil loss as well as voice. On the other hand, if priority is given to data and a lot of buffering is employed, then real-time applications may suffer large variable delays. Hence we need a dynamic adaptive inter temporal priority scheme. The priorities should change to track changes in the network state or in the application requirements over multiple time periods. Rather than having a complicated priority scheme, a pricing scheme could be used. The operator would set the benefit functions for the different applications, and could also set different benefit functions for applications of the same type. Each application would then input traffic according to its assigned benefit function and the current state of the network, as reflected in the prices.

2.3 Bandwidth Management Mechanisms and Techniques

Techniques brought to bear on bandwidth management include: Data compression ,to reduce the size of the data that must be transmitted ,local caching ,to store frequently used data locally instead of transmitting it multiple items, bandwidth prioritization ,to allocate bandwidth based on the importance of the application, distributed content, to move content from a single location to multiple locations nearer the end users, blocking unauthorized traffic, internet accounting packages, to track bandwidth usage and charge it back to customers and user education , to educate users about the consequences of their actions and convince them to be good citizens on the network(Daneen, 2002).

2.3.1 Queuing and Scheduling Techniques

Scheduling mechanisms employ different actions on data packets in order to provide different levels of service. These mechanisms are meant to control the transmission of packets and therefore considered to have a great impact on the quality of service since it determines the sequence in which packets from different flows are processed. These mechanisms are also used to ensure that all packets are handled in a fair manner to prevent one user from utilizing more than his or her share of resources (Snehalatha &Rodrigues, 2013).

2.3.1.1 First in First Out (FIFO) Queuing

In this mechanism the first packet in a queue is the first packet to be served. In a FIFO queue packets are treated the same and if a queue becomes congested incoming packets are dropped.

The main advantage of FIFO queue is that it is simple and considered a good solution for software based routers. In case there is no congestion in a FIFO queue, resource allocation in a network is done fast due to the simplicity of the technique. On the other hand FIFO does not provide a means of handling packets which are in different categories. In addition queuing delay increases as congestion increases which affects queued packets .Moreover during network congestion FIFO benefits non connection oriented flows such as UDP over connection oriented flows such as TCP. This is because if a TCP packet is lost, TCP understands that the queue is full and therefore reduces the amount of packets being sent. On the other hand if an UDP packet is lost, UDP continues to send packets normally. This leads to unfair allocation of network resources between UDP and TCP flows. FIFO is effective in situations where the number of packets is less than the capacity of the queue this is because in a case where there are excess packets these packets are discarded (Dhaini & Assi, 2007)

2.3.1.2 Priority Queuing

In priority queuing, packets are the first assigned to a priority class. Each priority class has its own queue. The packets in the highest-priority queue are processed first. Packets in the lowest-priority queue are processed last. None that the system does not stop serving a queue until it is empty. A priority queue can provide better QoS than the FIFO queue because higher-priority traffic, such a multimedia, can reach the destination with less delay. However, there is a potential drawback. If there is a continuous flow in a high priority queue, the packers in the lower-priority queues will never have a chance to be processed. This is a condition called starvation (Snehalatha, Angeline & Rodrigues, 2013).

To avoid starvation, (Dhaini & Assi, 2007) propose that the amount of traffic to the high priority queues should be limited using proper admission control policies. Also priority queuing can be combined with a rate meter such as leaky bucket to ensure that higher priority queues do not monopolize the link.

2.3.1.3 Weighted Fair Queuing

In weighted fair queuing, incoming packets are grouped into classes and admitted to different queues. Then these queues are assigned priority based on their weights, with high weights corresponding to high priority. Packets are then processed in a round robin manner with the number of packets selected from each queue based on the corresponding weight.

Weighted fair queuing is mostly suitable in environments where it is desirable to provide a constant response time for the demanding users or applications without adding an excessive bandwidth. Weighted fair queuing implements bitwise fairness, which allows a queue to be served based on the number of bytes. Weighted fair queuing ensures no traffic is starved off bandwidth. In this way low-level traffic can smoothly travel through the network. This increases service efficiency since an equal number of low-level and high level packets are transmitted. Weighted fair queuing can also automatically adapt to the changing network conditions. The weights are calculated from IP priority bits where values 0 to 5 are used (6 and 7 are reserved) and the weighted fair queuing algorithm calculates how many additional services must be provided for every queue. Weighted fair queuing reduces the round trip delay which makes it perform better than TCP and in the process reducing congestion and speeding up slow connections. Weighted fair queuing results in predictable behavior over the entire route while the response time for each active flow can be reduced by a multiple factor (Kithinji, 2016).

2.3.1.4 Class Based Queuing

CBQ is queuing algorithm that divides a networks connections bandwidth among multiple queens or classes. A queue may optionally be configured to borrow bandwidth from its parent queue it the parent is being under-utilized. CBQ arranged in hierarchical manner. A top of hierarchical is the root queue which defines the total amount of bandwidth available. Child queues are created under the root queue, each of which can be assigned some portion of the root queues bandwidth (Snehalatha, Angeline & Rodrigues, 2013).

Class Based Queuing is a scheduling mechanism that can provide link sharing between agencies, protocol families or service classes. This improves the utilization of dedicated pipes for each agency because link sharing guarantees that any excess bandwidth resulting from an agency that is not fully utilizing its share is redistributed to the other agencies (according to a set of predetermined rule set). With the CBQ's hierarchical link sharing capabilities, each agency can further share its bandwidth among different kinds of traffic allocating the right share to each one. This allows unused bandwidth of an agency's class to be distributed first to its sibling classes and later among other agencies. Classifying a packet is very similar to the problem of determining the route matching a specific address in a packet. In both cases, fields in the header are used to look up information in a table/firewall or by looking at a specific mark byte in a packet at the

firewall level. However, the classification problem is more complex because the patterns upon which the packet may match a class must be more general and can match any part of the header. For instance packets may be from one of multiple agencies, requiring the examination of destination and source addresses, classified on transport or other protocols such as TCP, UDP or ICMP, or applications such as ftp or telnet, requiring the examination of the port numbers. For Audio streams we may look even further within the packet to determine the level and "drop ability" of a packet within a hierarchically encoded stream of voice data. In few cases this packet matching technique can be external and the CBQ implementation may only schedule packets (Chereddi, 2009).

2.3.2 Traffic Shaping Techniques

Realistically, spacing between incoming packets has an irregular pattern, which in many cases causes congestion. The goal of traffic shaping in a communication network is to control access to available bandwidth to regulate incoming data to avoid congestion, and to control the delay incurred by packets Turbulent packets at rate λ and with irregular arrival patterns are regulated in a traffic shaper over equal-sized 1/g intervals (SJBIT, 2013).

Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network. Two techniques can shape traffic: leaky bucket and token bucket (Snehalatha, Angeline & Rodrigues, 2013).

Kashihara & Tsurusawa (2010) observed that traffic shaping can be done at the end systems or in the network by the switch hardware. At the end of systems can be implemented by the servers using a leaky bucket (single or dual shaper) consisting of a buffer and rate control mechanism, shaper delay and delay variation and the shaper buffer size at the server. The rate controller determines the outgoing data rate which should be consistent with the bandwidth available in the network. Close loop feedback rate control utilizes feedback obtained from the network to control traffic rate. The traffic shaper requires a large buffer to accumulate the incoming busty stream. Traffic shaping controls the data transfer rate. Data transfer rate can be limited to a specific configured rate or derived rate based on the level of congestion. The rate of transfer depends on burst size, mean rate and measurement interval. The mean rate is equivalent to burst size divided by the interval. When traffic shaping is enabled the bit rate of the interface will not exceed the mean rate at any time. This implies that during every interval a maximum burst size can be

transmitted. Traffic shaping smooth's traffic by storing traffic above the configured rate in a queue. In a shaping scheme when packets arrives the interface for transmission the following happens; if the queue is empty the arriving packet is processed by the traffic shaper. If possible the traffic shaper sends the packet. Otherwise the packet is placed in the queue. If the queue is not empty, the packet is placed in the queue. When there are packets in the queue, the traffic shaper removes the numbers of packets it can transmit from the queues every time ***t*** interval.

2.3.2.1 Leaky-Bucket Traffic Shaping

This algorithm converts any turbulent incoming traffic into a smooth, regular stream of packets. A leaky-bucket interface is connected between a packet transmitter and the network. No matter at what rate packets enter the traffic shaper, the outflow is regulated at a constant rate, much like the flow of water from a leaky bucket. The implementation of a leaky-bucket algorithm is not difficult. At the heart of this scheme is a finite queue. When a packet arrives, the interface decides whether that packet should be queued or discarded, depending on the capacity of the buffer. The number of packets that leave the interface depends on the protocol. The packet departure rate expresses the specified behavior of traffic and makes the incoming bursts conform to this behavior. Incoming packets are discarded once the bucket becomes full. This method directly restricts the maximum size of a burst coming into the system. Packets are transmitted as either fixed-size packets or variable-size packets. In the fixed-size packet environment, a packet is transmitted at each clock tick. In the variable-size packet environment, a fixed-sized block of a packet is transmitted. Thus, this algorithm is used for networks with variable length packets and also equal-sized packet protocols, such as ATM (SJBIT, 2013).

2.3.2.2 Token Bucket

This technique controls the traffic by the use of tokens. A token is generated at a rate of one toke every **T** time units, and then these tokens are stored in token pool of finite size **S**. In case the token pool is full, any additional token is discarded. For a packet to be transmitted it must make use of a token from the token pool. If a packet finds the token pool empty the token can either wait for anew token to be generated or it is discarded. The token bucket algorithm saves up tokens during idle times which are used later when there are no tokens in the bucket. This optimizes the speed of the network if N packets meet N tokens. But it can also cause congestion if the traffic gets too busty (Traver & Tarin, Cardona, 2009).

In their survey (Snehalatha, et al, 2013) argued that he leaky bucket is very restrictive. It does not credit an idle host. For example, if a host is not sending for a while, its bucket becomes empty. Now if the host has burst data, the leaky bucket allows only an average rate. The time when the host was idle is not taken into account. On the other hand, the token bucket algorithm allows idle host to `accumulate credit for the future in the form of tokens. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) 0f data sent. For example, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens Now the host can consume all these tokens in one tick with 10,000 cells, or the host takes 1000 ticks with 10 cells per tick. In other words, the host can send burst data as long as the bucket is not empty. The token bucket can easily be implemented with a counter.

The token is initialized to zero. Each time a token is added, the counter is incremented by 1.
Each time a unit of data is send, the counter is decremented by 1. When the counter is zero, the host cannot send data.

2.4 Bandwidth Management Implementation Tools

2.4.1 Networx

NetWorx icon NetWorx is a simple and free, yet powerful tool that helps you objectively evaluate your bandwidth consumption situation. You can use it to collect bandwidth usage data and measure the speed of your Internet or any other network connections. NetWorx can help you identify possible sources of network problems, ensure that you do not exceed the bandwidth limits specified by your ISP, or track down suspicious network activity characteristic of Trojan horses and hacker attacks.

The program allows you to monitor all your network connections or just a specific network connection, such as Wireless or Mobile Broadband. The software also features an array of highly customizable visual and sound alerts. You can set it up to alert you when the network connection is down or when some suspicious activity — such as unusually heavy data flow — occurs. It can also automatically disconnect all dial-up connections and shut the system down.

The incoming and outgoing traffic is represented on a line chart and logged into a file, so that you can always view statistics about your daily, weekly and monthly bandwidth usage and dial-

up duration. The reports can be exported to a variety of formats, such as HTML, MS Word and Excel, for further analysis (Paessler AG, 2016)

2.4.2 PRTG Network Monitor

PRTG Network Monitor is a comprehensive monitoring solution that checks bandwidth and monitors network usage, performance and availability. The network monitoring tool monitors bandwidth utilization via SNMP, packet sniffing and NetFlow, checks the availability of network components, and checks parameters such as CPU load, memory load, free disk space, etc. It can also be used for server room monitoring as PRTG can even check of the temperature or humidity in your server room and trigger an alert if a certain threshold is being passed.

In order to make server performance monitoring easier, PRTG comes with a range of built in server monitoring sensors:

- Email sensors check the availability of your email services
- Monitoring SQL server sensors: MySQL, Microsoft SQL, and Oracle SQL sensors. These sensors check whether your SQL server accepts connections, processes requests, and returns an expected result.
- File server sensors check free disk space, existence of files, changes to a file, etc.
- Virtual server sensors (e.g. ESX monitor, hyper-v monitor) make monitoring virtualized environments easier (Paessler AG, 2016).

2.4.3 Squid Linux

For traffic management squid utilizes proxing and caching features. In addition squid to support bandwidth management squid uses delay pools for bandwidth management by limiting the bandwidth for a particular user or group of users. Squid delay pools use the token bucket algorithm to allocate bandwidth to users connected to the internet. Each configured pool has a max value and a restore value. The max value indicates the maximum size of the token bucket while the restore value is the rate at which tokens are replaced into the bucket. Squid keeps log files of all sites visited which can be used by network administrators to determine bandwidth requirements for a particular user or group of users (Devajit, et al, 2013).

2.5 Bandwidth Management State of Practice

2.5.1 Kenya National Education Network

Kenya national education network (KENET) was established in 1999 with an aim of connecting education institutions and research center's with a goal of sharing knowledge throughout the country. Members are connected via the main node in Nairobi or via Kenya's telecom backbone. Members can connect to the main node at speeds of 3Mbps for the uplink via a leased line and 3Mbps downlink via VSAT. Member's networks speeds range from 64 Kbps to 960 Kbps of bandwidth capacity. This shows that members are limited in terms of available bandwidth .This combined with improperly set up networks due to lack of trained staff has made the available bandwidth unusable for most institutions. To solve the problem, as of 2004, KENET has embarked on a training program on network management, security and monitoring for system administrators from member institutions (Chege & Ford, 2009).

To address the problem of bandwidth wastage, KENET established custom servers for each member institutions to address problems at that institution. Access control lists are also established on routes to restrict access to only approved services. The networks in all the member institutions were standardized to one uniform platform of firewalled FreeBSD. KENET has employed technical measures to manage and optimize bandwidth for its members (Carr & Verner, 2013).

In future the organization targets at an integrated approach consisting of strict policy measures and technical solutions. Also in conjunction with Aidworld, KENET is developing an open source toolkit to provide affordable and reliable bandwidth management regardless of size of the network or network administrator's experience.

KENET and the member institutions want the flexibility to be able to push back on certain bandwidth-intensive applications at certain times of day, for example, when the network is under simultaneously high demand from researchers and staff trying to do their research at the educational institutions. From this perspective, the sort of solution that the LEDBAT WG is working on should benefit KENET. The LEDBAT WG charter identifies a common scenario wherein applications experience large delays in the presence of P2P applications uploading over thin home uplinks; for KENET its entire WAN is peppered with thin uplinks. The potential benefits of a deployable solution in this space are therefore much greater than just the well-

known use-case of an ADSL user simultaneously trying to run a P2P application and place a VoIP call (Chege & Ford, 2009).

2.5.2 Ipoque's Proven Application Classification Engine

Network operators' business models are evolving with the increase in smartphone penetration and application usage. The R&SCMW500 has been a market-leading product amongst network operators over the past decade, but with traffic shifting to become more mobile and application focused, it needs to add IP awareness to solve the new challenges network operators face. Operators need to know how applications impact the quality of their network, e.g. bandwidth consumption, security issues and, ultimately, their users' quality of experience (QoE). In areas such as voice over IP, messaging and video on demand in particular, the diversity of the applications and protocols is no longer manageable without a high-class application detection based on deep packet inspection (DPI).

In an all IP world, operators doing LTE deployment need to identify all influencers of network traffic and data connections to efficiently manage network resources. The R&SCMW500 needed to simply and easily integrate trustworthy IP analysis software and market-leading application awareness and bring a new feature to market that would increase the quality experienced by mobile customers in record time to stay ahead of competition. Furthermore, to ensure the quality experienced by the mobile customer, IP-aware application testing, previously unavailable on the market, was required.

Application-based IP analysis in real-time, integrated in a few days, set Rohde & Schwarz apart from the competition and represents a totally new product feature for the operator market. Ipoque's Protocol and Application Classification Engine (PACE) provides deep packet inspection solutions with support for thousands of network protocols and applications in real-time. The proven Layer 7 IP traffic detection combines different high quality DPI technologies to ensure a detection rate of nearly 100%. R&SPACE is fully flexible for integration and independent of any operating system. It helps network equipment vendors enhance their products with powerful network management and analysis capabilities without spending resource on trying to keep up with ever-changing network protocols. By integrating R&SPACE, a supplier can save significant costs and development resources, helping them to focus on core competencies and create stand out network products from the competition (Rohde &Schwarz, 2015).

2.5.3 Bandwidth Management and Optimization in the U.K Case of Blackburn College

The joint academic network (JANET) is the UK's education and research network that connects UK's universities to each other and to the internet. It is managed by the United Kingdom Education and Research Networking Association (UKERNA). Having a large network with high bandwidth demand and limited funding, in the past JANET has not been able to meet the bandwidth demand for its members which led to poor performance and frequent outages. These made JANET embark on a bandwidth management and optimization strategy. To manage and optimize bandwidth, JANET uses an acceptable use policy, user bandwidth limiting and network monitoring. They also provide services to their members in the areas of monitoring, control and reduction of bandwidth usage (JANET, 2014). Blackburn College is a research institute and a JANET member. Blackburn College connects to JANET for access to the internet and to other universities. To conserve bandwidth, the college implements disciplinary procedures to encourage users to 0use bandwidth wisely and in moderation. The college also performs constant monitoring and keeps records of network usage. The monitoring is meant to track down a user responsible for any network abuse. The college employs a proxy server which denies access to specific websites and also includes a proxy cache that reduces bandwidth usage. Inbound and outbound traffic is filtered by the boarder router by use of ACLS on the basis of protocols and port numbers. In Future Blackburn College is looking at improving their filtering both at the gateway router and on the proxy server (Kotti, Hamza & Bouleimen, 2009).

2.6 Proposed System

PfSense Bandwidth Manager

Effective bandwidth management is critical to the performance of any network. In most networks many users share a single internet connection. The biggest problem on a shared network is that one user could potentially consume all of the available internet bandwidth and slow down the connections for all of the other users as a result. High-bandwidth users can create an even bigger problem if your network has critical traffic such as VOIP that depends on having enough bandwidth to function. PfSense Bandwidth Manager solves this problem by implementing traffic shaping which prioritizes important or time critical network traffic to guarantee performance and a the same time throttle less important traffic.

How to Find High Bandwidth Users In order to properly manage bandwidth usage, you need to determine who is using the most bandwidth and why. PfSense offers a package called Darkstat that can quickly give you a view of what is taking place on your network. Darkstat creates a list of hosts sorted by total upload and download traffic usage. You can also drill down on this report to see which TCP or UDP ports make up that usage. This information can be used to determine whether a traffic shaper will help your network, and if so which ports you should be shaping.

In the case of VOIP phones, you will probably want to prioritize the traffic sent by the phones to improve the communication in the organization, pfsense will help in prioritizing the traffic.

Pfsense provide a feature called a “penalty box” where if you have one or more hosts on your network that are using most of the bandwidth, you can place them in a "penalty box" to limit their usage to a certain percentage of available bandwidth, you can specify whether to de-prioritize peer-to-peer networking traffic, since P2P traffic is often the largest user of internet bandwidth on a network.

Pfsense also provide you with option to raise or lower the priority assigned to different applications (HTTP, DNS, and ICMP) on an individual basis. Most of the options depend on the applications in use on your network.

Pfsense provide us also with an interesting feature called Captive portal which allows you to force authentication, or redirection to a click through page for network access. The following are the features of captive portal that will help in controlling unauthorized access to the organizations network:

- Logon pop up window - Option to pop up a window with a log off button.
- URL Redirection - after authenticating or clicking through the captive portal, users can be forcefully redirected to the defined URL.
- MAC filtering - by default, pfSense filters using MAC addresses. If you have a subnet behind a router on a captive portal enabled interface, every machine behind the router will be authorized after one user is authorized.
- Authentication options - There are three authentication options available.
    - No authentication - This means the user just clicks through your portal page without entering credentials.

  - Local user manager - A local user database can be configured and used for authentication.
  - RADIUS authentication - This is the preferred authentication method for corporate environments and ISPs. It can be used to authenticate from Microsoft Active Directory and numerous other RADIUS servers
- HTTP or HTTPS - The portal page can be configured to use either HTTP or HTTPS.
- Pass-through MAC and IP addresses - MAC and IP addresses can be white listed to bypass the portal. Any machines with NAT port forwards will need to be bypassed so the reply traffic does not hit the portal. You may wish to exclude some machines for other reasons.

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter explains the design used to execute the project. In particular this chapter discusses the approach used to achieve the objectives of the project. It also highlights the system requirements that is the hardware requirements, software requirements and network requirements.

3.2 Research Design

The study is to adopt simulation approach. A virtual LAN was developed with three computers. Of the three computers one was dedicated as a firewall that is the pfsense firewall, the second computer was used as network administrator's machine and at the same time it was used to test one of the simulated departments that is the management department and finally the last machine was set to test the Transport and customer care departments network. Bandwidth of 10 mbps was supplied. The LAN simulation was achieved by use of one laptop which was used to install VMware workstation version 12. In the VMware hypervisor is where the three guest computers were created for the sake of simulation.

The pfsense firewall was installed in the virtual environment with two Network interface Cards. The configurations were done so that the external interface of the pfSense virtual machine (Network Adapter 1) Bridged with the external interface of our pfsense em0. Secondly the internal interface of the pfSense virtual machine (Network Adapter 2) was set to a specific virtual network with the internal interface of our pfsense em1, and so is the only network interface of our client Virtual Machine. The pfsense acted as a router to the virtualized environment. The host computers were to be connect to the internet through the pfsense firewall and they are set to have static IP addresses.

TP-Link router was used to act as our source of internet. The router was supplied bandwidth by a modem with Airtel SIM card loaded with Airtel data bundles. The connection of the laptop with VMware workstation to the TP-Link was done using Ethernet Cable cat 6 twisted pair.

Figure 2 below shows the simulated model of our network.

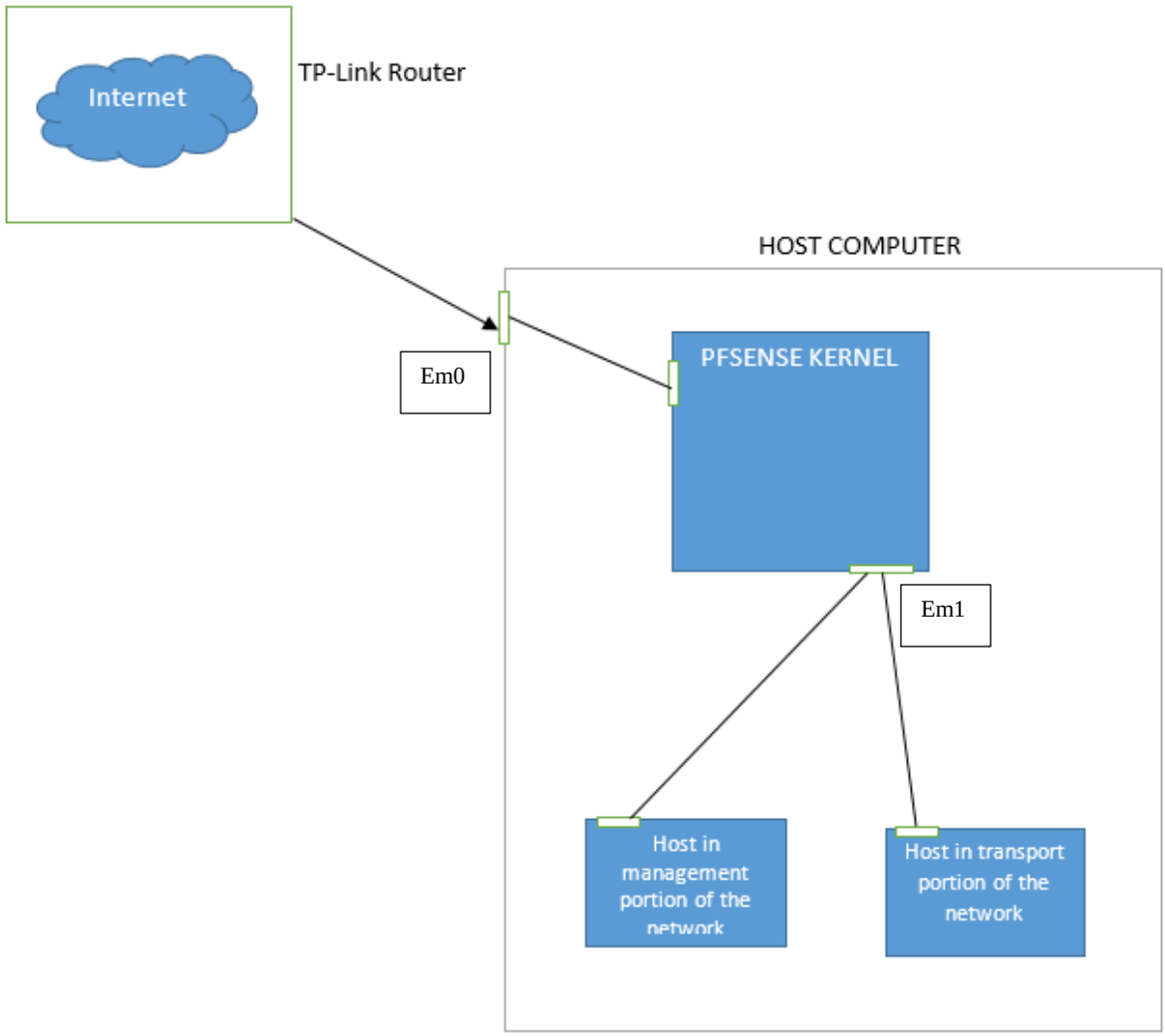


Figure 2: simulation Design

Source: author's conception

3.3 Sub netting

Due to the department setup we are to subnet the IP address 192.168.1.0 to give the several hosts in the departments (classes) IP addresses. Table 1. Below shows the range of IP addresses hosts occupy in different class or department.

Class/department	Range of host IP addresses
Management	192.168.1.2 – 192.168.1.31
ICT	192.168.1.32 – 192.168.1.63
Finance and procurement	192.168.1.64 – 192.168.1. 95
Human resource	192.168.1.96 – 192.168.1.127
Transport and customer care	192.168.1.128 – 192.168.1.159
Reserved IP addresses	192.168.1.160 – 192.168.1.255

Table 1: Table showing classes and their corresponding host IP addresses

3.4 System Requirements

3.4.1 Hardware System Requirements

For the implementation of this project one computer(laptop) was required, the computer was having a capacity of 500 GB hard disk, 4GB Random Access Memory (RAM) and processing speed of 2.67 GHz.

3.4.2 Software System Requirements

One of the most fundamental software in this project is PFSense, we used version 2.3.2. PfSense software is a free, open source customized distribution of FreeBSD tailored for use as a firewall and router. In addition to being a powerful, flexible firewalling and routing platform, it includes a long list of related features and a package system allowing further expandability without adding bloat and potential security vulnerabilities to the base distribution. Basically pfSense software is an engine that makes a firewall go, but not the actual hardware and it is customizable. This allows the engineer to meet the needs of the project with a device with the right I/O and specifications, and then customize the pfSense software settings to their needs. PfSense is suitable for all sizes of organizations from small offices to large organizations with thousands of network devices.

To access the pfsense web interface we use Mozilla Firefox browser version 47.1, the browser will help us to do the configurations on our firewall and to test the presence of internet on our network.

To enable us to simulate the use of firewall we use VMware workstation version 12 to help we work in a virtualized environment and to maximize on the resources we have.

3.4.3 Network Requirements

In this project a TP-Link wireless router which is compatible with a USB modem to provide us with internet was used. The network will not be complete without the presence of 1 twisted category 6 internet Cables with a standard length of 3 meters. In this project a 10MBps bandwidth was used to assume the working environment of a small organization

The services that were be running in the network include the DNS server, web server and mail server. DNS server is a server that is used to interact with the domain name system which is the global directory domain names and corresponding IP addresses. Web server is a program that uses HTTP protocol to serve the files that form web pages to users, in response to their requests which are forwarded by their computers HTTP clients. Mail server is a computer/application within your network that works as your virtual post office. A mail server usually consists of a storage area where e-mail is stored for local users, a set of user definable rules which determine how the mail server should react to the destination of a specific message, a database of user accounts that the mail server recognizes and will deal with locally, and communications modules which are the components that actually handle the transfer of messages to and from other mail servers and email clients

3.5 Conclusion

In this chapter the design of project is explained. A clear design of the network was discussed here. The chapter has also highlighted the requirements of the project that is hardware, software and network requirements

CHAPTER 4
IMPLEMENTATION AND TESTING

4.1 Simulation

By using this design our goal is to generate statistical results that represent the behavior of a small organization's elements and their functions. In this case we are able to observe link utilizations, response times and other events as they happen over time, and collect performance measures to draw conclusions on the performance of a small organization's the network.

4.1.1 Simulation Model

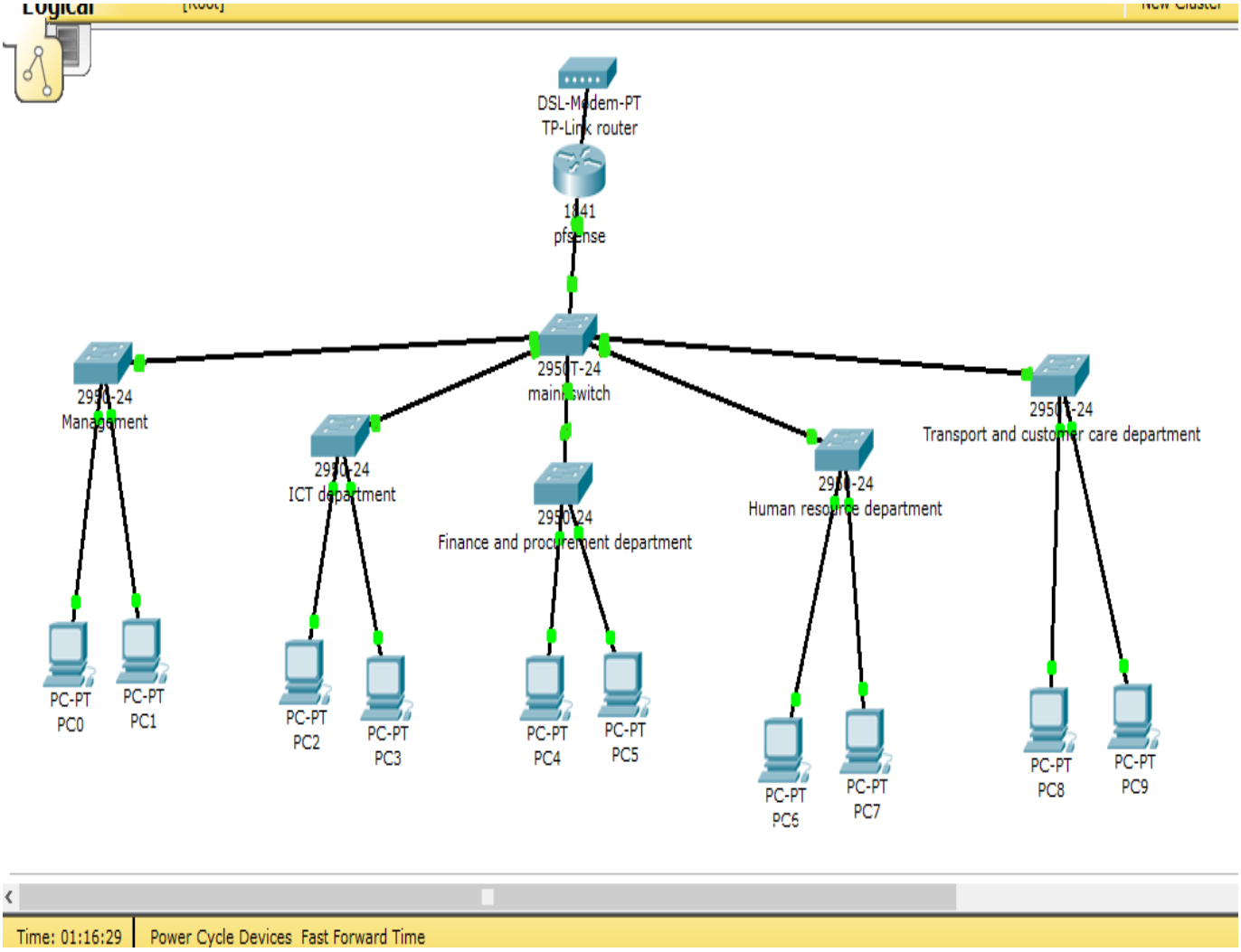


Figure 3: Simulated model of a small organization

4.2 Bandwidth Allocation Model

4.3 Classification of a Small Organization in Terms of Classes and Priority

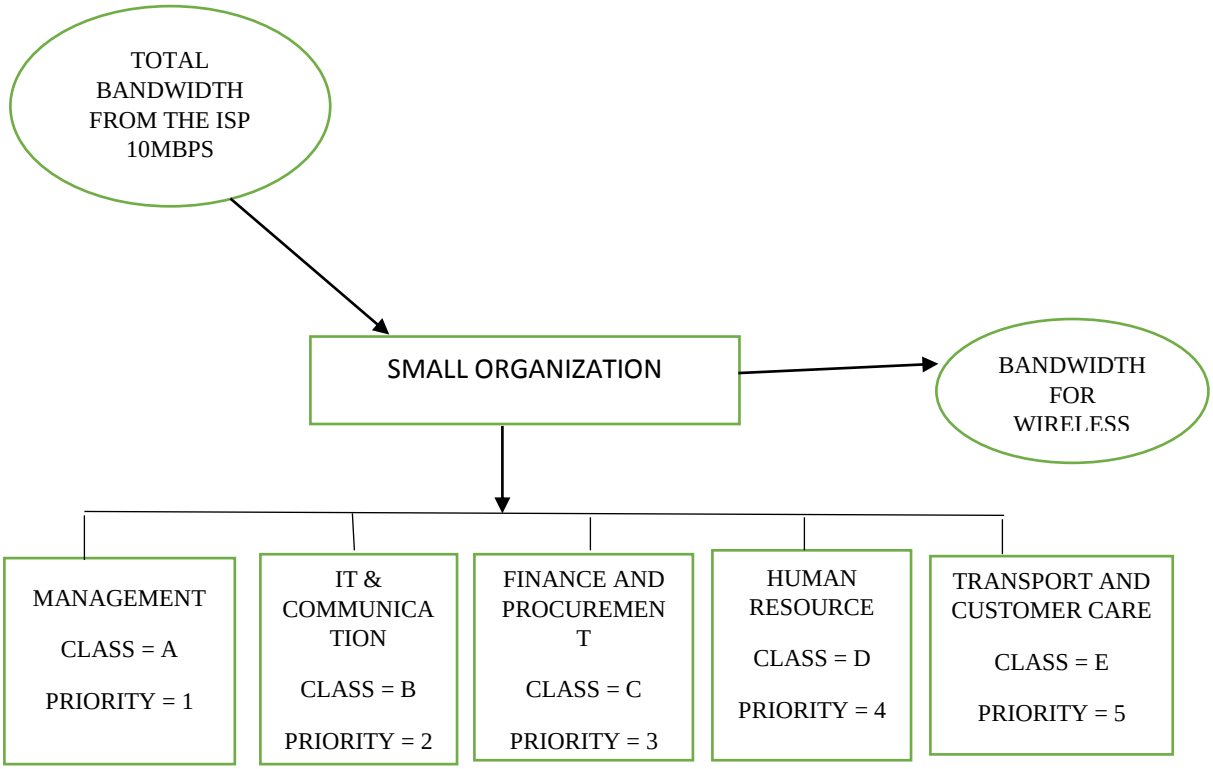


Figure 4 : Classification of a Small Organization in Terms of Classes and Priority

In the figure above a network of a small organization is categorized into a group of classes. There are five classes namely class A, class B, class C, class D and class E. Class A is assigned to management this means the C.E.O of the small organization and managers are in this class, Class B is assigned to the Information Technology and communication department, class C Finance and procurement departments, class D is assigned to Human Resource department and the last one is class E which is assigned to transport and customer care departments. As per the order the classes are given priority in bandwidth allocation starting with class A which has the highest priority meaning it is allocated high bandwidth compared to the rest going down to the transport and customer care departments having low priority that is priority 5 having the least bandwidth allocated to them.

It is assumed that this small organization use both wired and wireless networks. The small organization is also assumed to be receiving 10MbPs from the internet service provider. The bandwidth is shared between the wired and wireless networks.

	CLASS A	CLASS B	CLASS C	CLASS D	CLASS E
BANDWIDTH ALLOCATED(Kbps)	3500	2500	1600	1000	900
SERVICE(S) WITH RESERVED BANDWIDTH	Video conferencing	Social networking sites	Null	Null	Null

Table 2 Table showing bandwidth allocated and service(s) with reserved bandwidth in respect to class

The table above gives an outlay of the bandwidth allocation in the wired network. The table indicates bandwidth allocated to each class in kbps as well as the services which have bandwidth reserved for them in each class.

4.4 Configuring pfSense as a router

To configure pfsense as a router first we configured the external interface of the pfSense virtual machine (Network Adapter 1) Bridged with the external interface of our pfsense em0. Secondly the internal interface of the pfSense virtual machine (Network Adapter 2) was set to a specific virtual network with the internal interface of our pfsense em1, and so is the only network interface of our client Virtual Machine. This allowed us to connect client Virtual Machine/s to em1 and use them to test our connections, as well as the configurations.

4.4.1 Configure the Interfaces

To set class based queuing the total bandwidth and the scheduler on each interface were set: Open the pfSense web Configurator and log in, from the menu choose Firewall/Traffic Shaper, Click on the WAN interface, Check the box Enable/disable discipline and its children, Ensure that the scheduler type is set to CBQ, Set the Bandwidth to 10000 Kbit/s and finally Click on the

Save button. The queue interface were added by clicking on the Add new queue button, Check the box Enable/Disable queue and its children, For the Queue Name enter Other, Check the box Default queue, for the Description enter All other traffic, for the Bandwidth enter 200 and choose Kbit/s*, this is the WAN interface, so we are configuring the upstream bandwidth then click on the Save button. Apply the changes to the traffic shaper configuration by clicking on the Apply button.

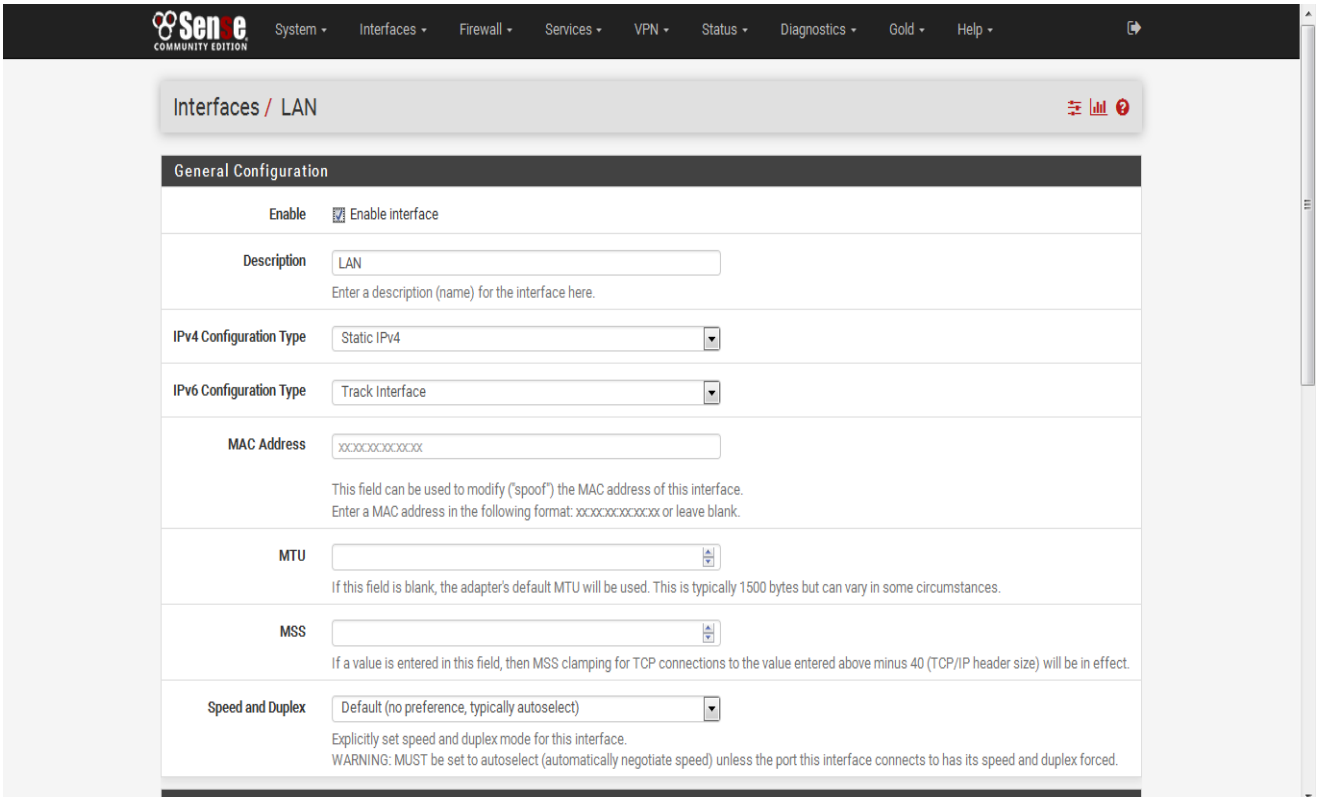


Figure 5: LAN interface configuration.

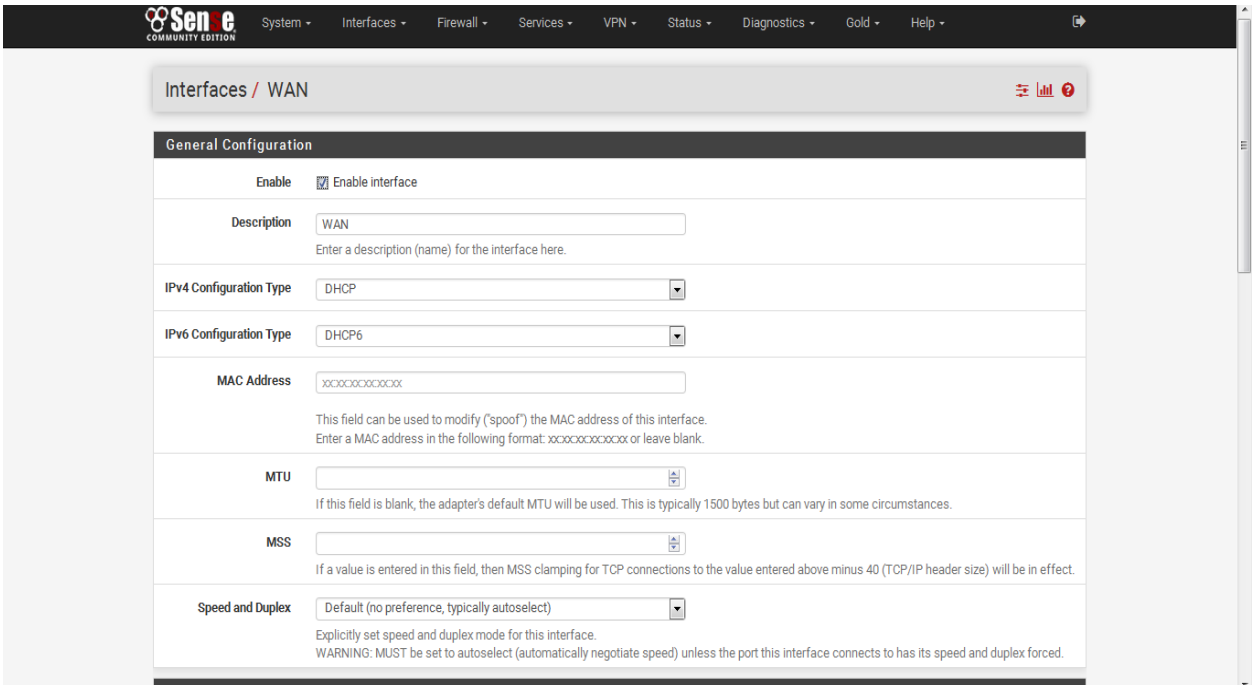


Figure 6: WAN interface configuration.

4.4.2 Traffic and Ping times

Pinging the pfSense firewall which has the IP address 192.168.1.1 what happens to ping times with and without a download in progress? Why the difference? Without a download in progress, you should see very short ping times, around 1 Ms:

PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.

64 bytes from 192.168.1.1: icmp_req=1 ttl=64 time=0.480 ms

64 bytes from 192.168.1.1: icmp_req=2 ttl=64 time=0.385 ms

64 bytes from 192.168.1.1: icmp_req=3 ttl=64 time=0.537 ms

64 bytes from 192.168.1.1: icmp_req=4 ttl=64 time=0.350 ms

64 bytes from 192.168.1.1: icmp_req=5 ttl=64 time=0.454 ms

With a download in progress, you should see much longer ping times, around 150 Ms:

PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.

64 bytes from 192.168.1.1: icmp_req=1 ttl=64 time=147 ms

64 bytes from 192.168.1.1: icmp_req=2 ttl=64 time=136 ms

64 bytes from 192.168.1.1: icmp_req=3 ttl=64 time=154 ms

64 bytes from 192.168.1.1: icmp_req=4 ttl=64 time=163 ms
64 bytes from 192.168.1.1: icmp_req=5 ttl=64 time=132 ms

This is because the ping packets must wait in the queue behind the download packets, when a download is in progress. We can reduce this, at the cost of some dropped packets, by reducing the Queue limit on the WAN interface, other class, to 5 or 10 packets. If a ping arrives when the output queue on the interface is full, then the reply packet will be dropped instead of placed in the queue.

4.5 Use of Captive Portal for Authentication

To set up authentication is to use radius authentication because it allows doesn't limit the number of users and it is much more flexible. A small organization's objectives in most cases unless exceptional case is to grow in terms of profits they and increase in services they offer and this means increase in number of employees and customers/clients as well. This made us choose radius authentication database in pfsense. Installation of the FreeRadius package is done directly on pfSense.
For the installation of FreeRadius package the following steps were followed:

1.) Go to System>> Packages>> Available Packages>>
2.) Click on the plus (+) sign button to install the application, and wait until the application installation is done.

Create Freeradius User

1.) Go to Services>> FreeRADIUS>>

2.) With "Users" tab selected, click on plus (+) sign button.

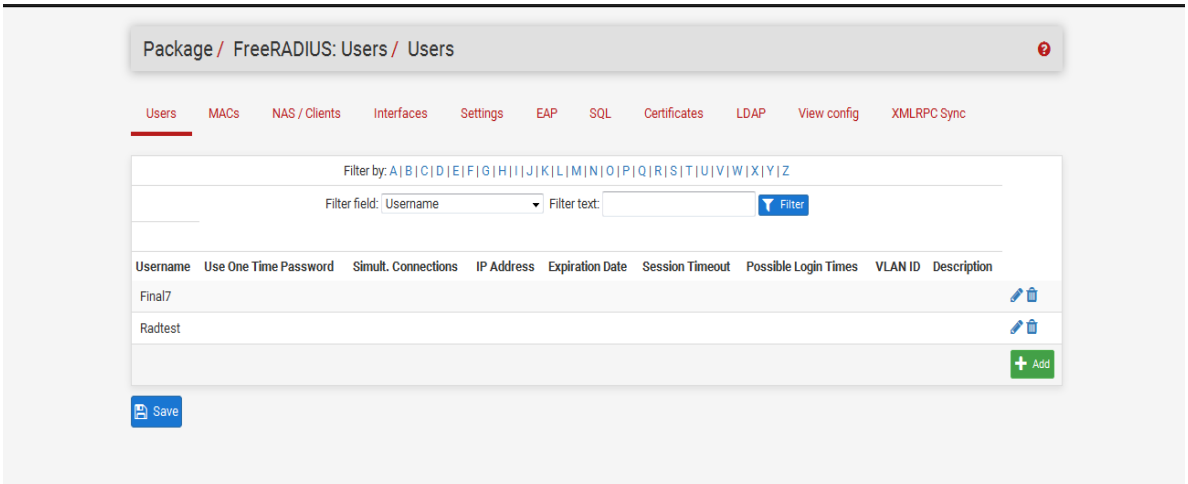


Figure 7: FreeRADIUS users

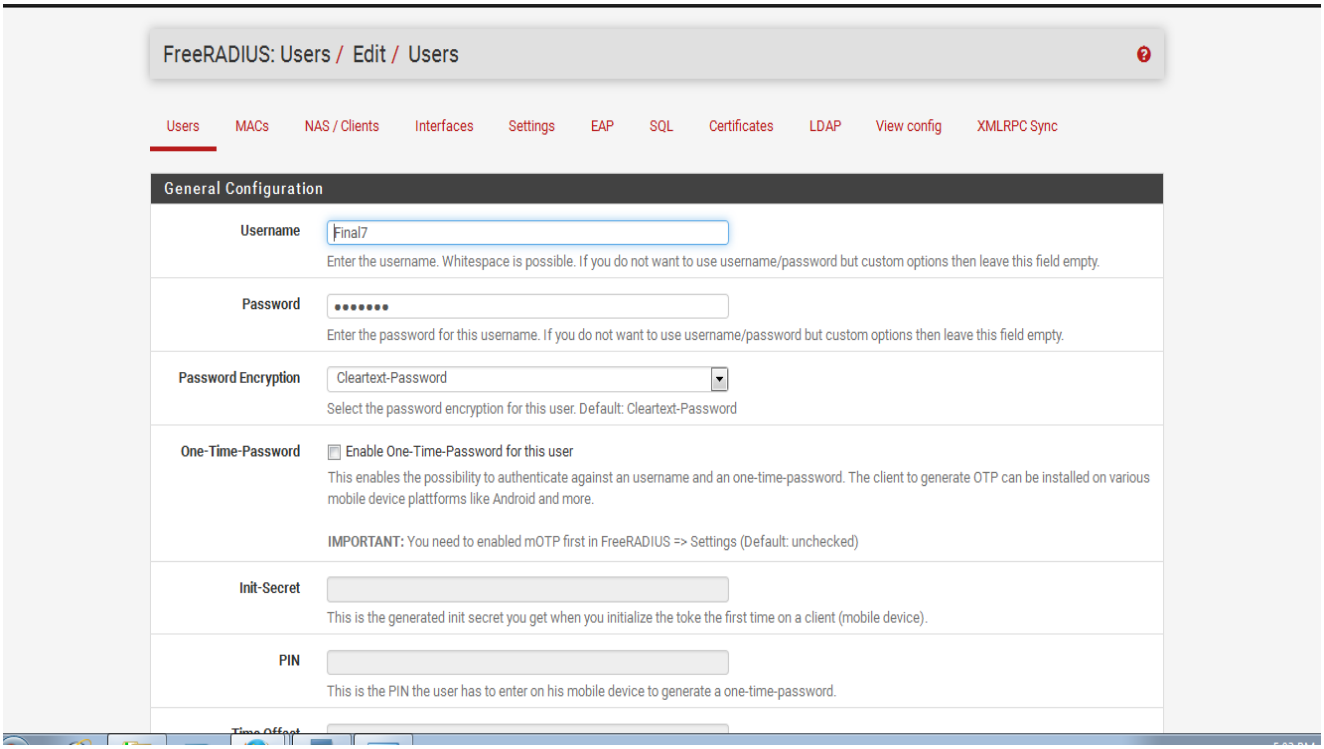


Figure 8: Adding and editing FreeRADIUS users

Create Radius Client

1.) Go to Services>> FreeRADIUS>>

2.) With "Nas/Clients" tab selected, click on plus (+) sign button.

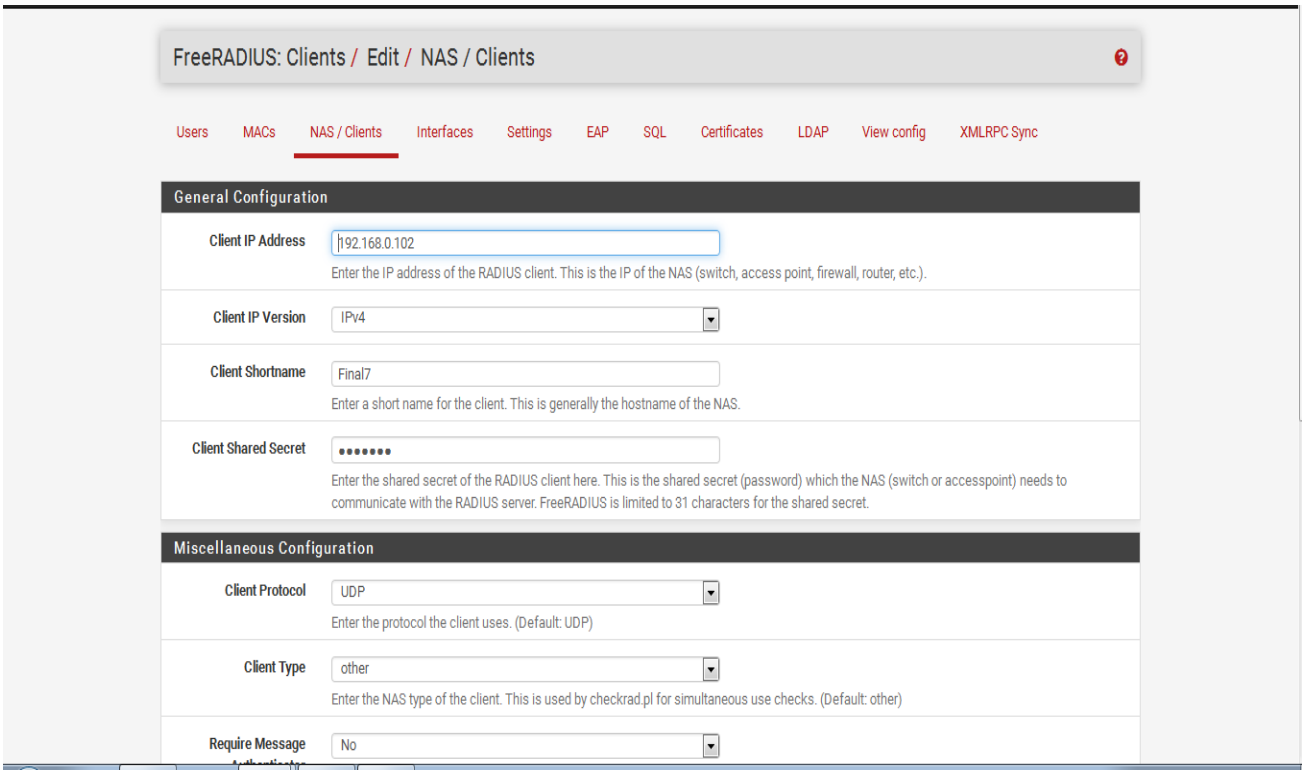


Figure 9: Creating RADIUS NAS/clients

4.5.1 Enable FreeRADIUS on Captive Portal

1.) Go to Services>> Captive Portal>>

2.) On Authentication section, select RADIUS Authentication and enter the IP address and shared secret we just created.

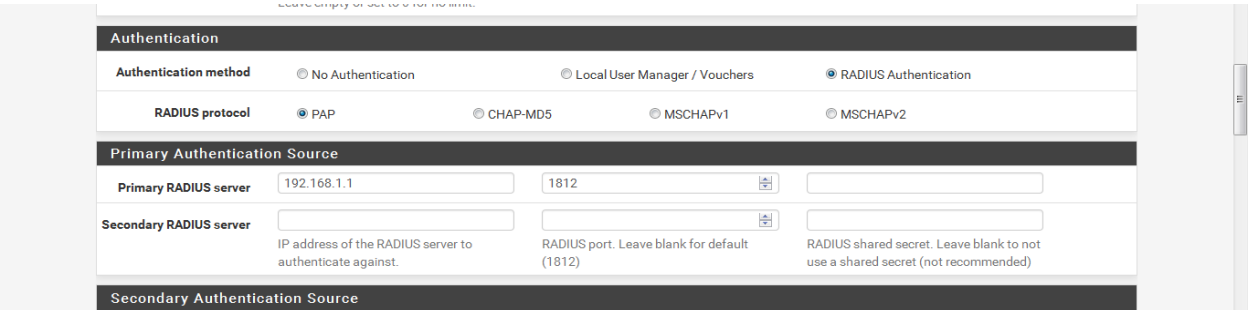


Figure 10: Enable FreeRADIUS on Captive Portal

Modifying the HTML

In order for this to work we used a HTML landing page that has username and password fields. To upload an image click on the file manager tab in the captive portal settings. In order for files to be used by the portal they must have a prefix of "captiveportal-" in the filename.

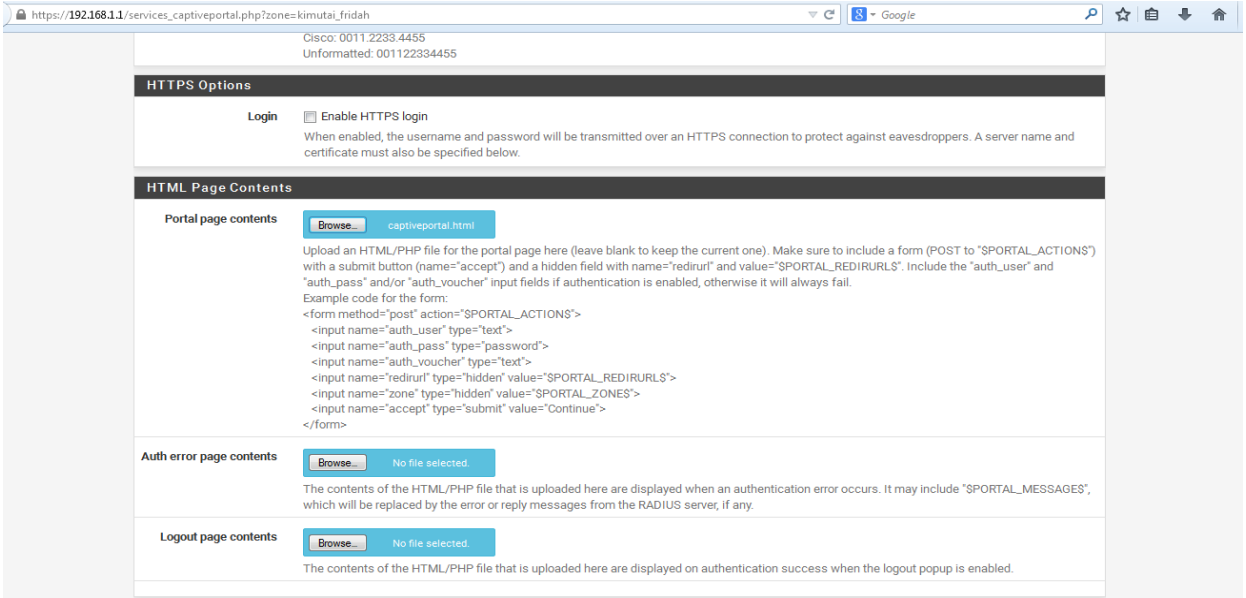


Figure 11: Modifying the HTML captive portal page

To create a simple user you only need to enter a username and password. Other configurations that were made include the following:

i. **Expiration Date** - This option allows to define a date that the account will automatically expire. So if you know the account is temporary this will save you the trouble of having to manually disable the account.
ii. **Idle timeout** - If a user is idle for a certain number of minutes they will be automatically disconnected. The timeout is set to be considerable so that it is not too low which frustrate users by making them to keep on logging after few minutes , and at the same time don't set it so long since the results that the captive portal won't be efficient. Therefore even setting it to something like 8 hours will help.
iii. **Redirection URL** - By default users will continue to the web page they originally requested after passing through the portal. This setting allows you to force clients to be directed to a page of your choice after connecting. Users can then enter a new URL and browse the web normally.
iv. **Concurrent user logins** - Enabling this setting will allow only one connection to the portal per user. This will prevent users from making multiple connections using the same username and password.

4.5.2 Securing the Captive Portal Login Page

The common problem of captive portal is ARP Spoofing that may allow an attacker to intercept data frames on a LAN, modify the traffic, stop the traffic altogether, or even sniff the username and password / voucher code in a captive portal login page.

To solve this problem HTTPs should be set since it provides encrypted authentication of captive portal server, and protects against man-in-the-middle attacks or ARP Spoofing.

Creating a HTTPs Certificate on the pfsense graphical user interface **Go to System > Cert Manager**, Click on CAs tab then click the (+) sign button.

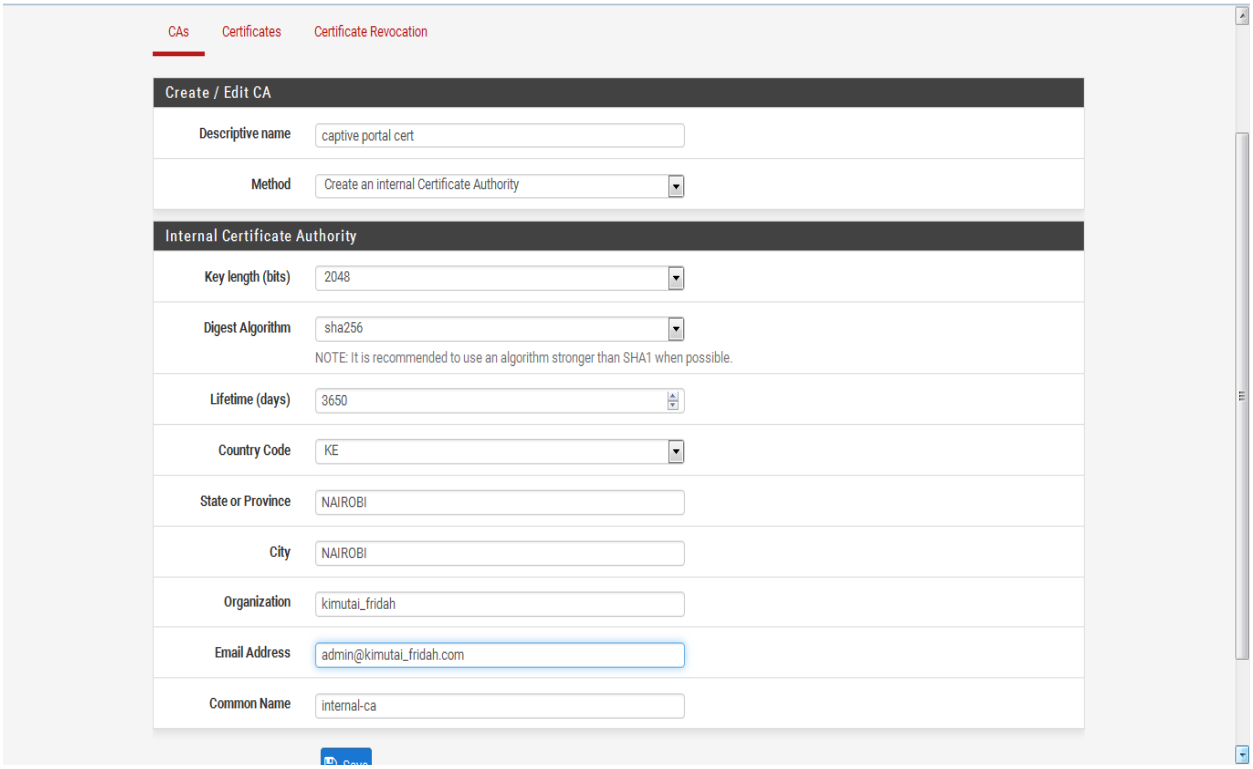


Figure 12: Creating a HTTPs Certificate

Save the settings and next click on the edit sign button

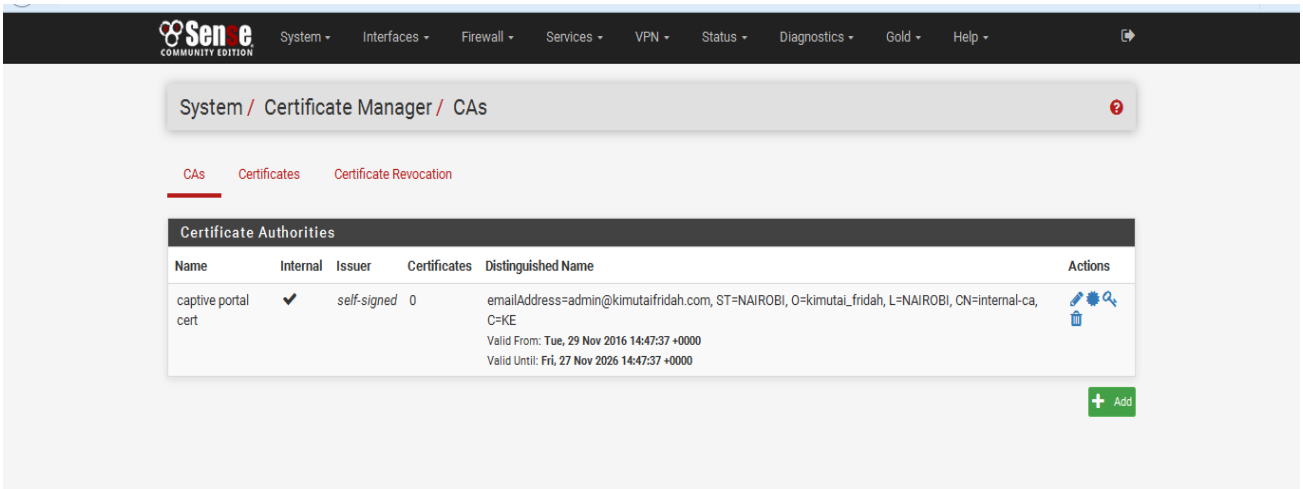


Figure 13: Created HTTPs certificate

Now the certificate is created. Click on the saved button.

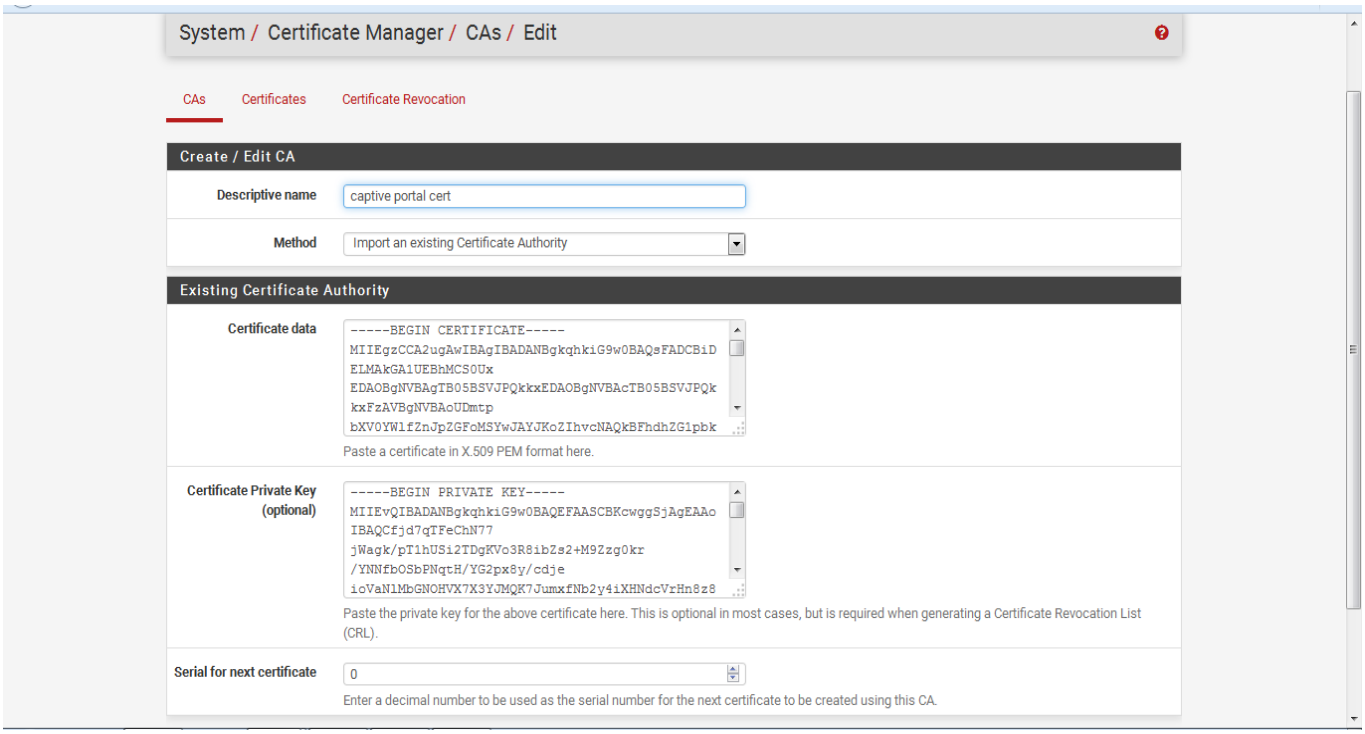


Figure 14: Editing HTTPs created certificate

4.5.3 Enabling HTTPs on Captive Portal Page

First **Go to Services > Captive Portal** Check "Enable HTTPs Login" and set HTTPs server name to your Pfsense Server Name. Select the certificate you created earlier from the dropdown arrow then press save to save your configuration.

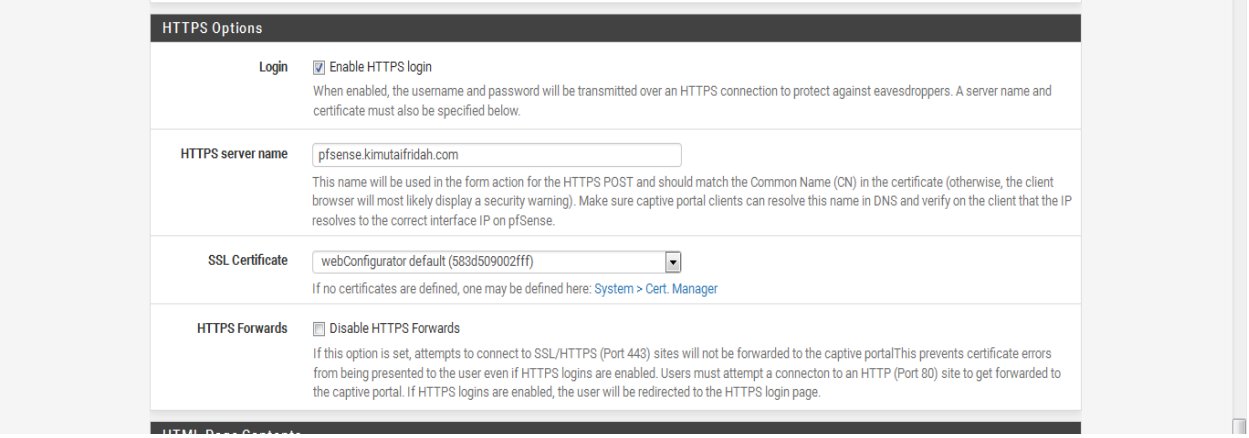


Figure 15: Enabling HTTPs on Captive Portal Page

4.5.4 Testing Captive Portal

To test the captive portal a browser of one of the host machine is opened and any IP address is typed for connection to be established. Before the connection is established the captive portal window pops up requesting for authentication that is user name and the password of the user. For a user who is registered they are able to input their credentials. However the user whose credentials are not registered an error message is returned when they enter their credentials.

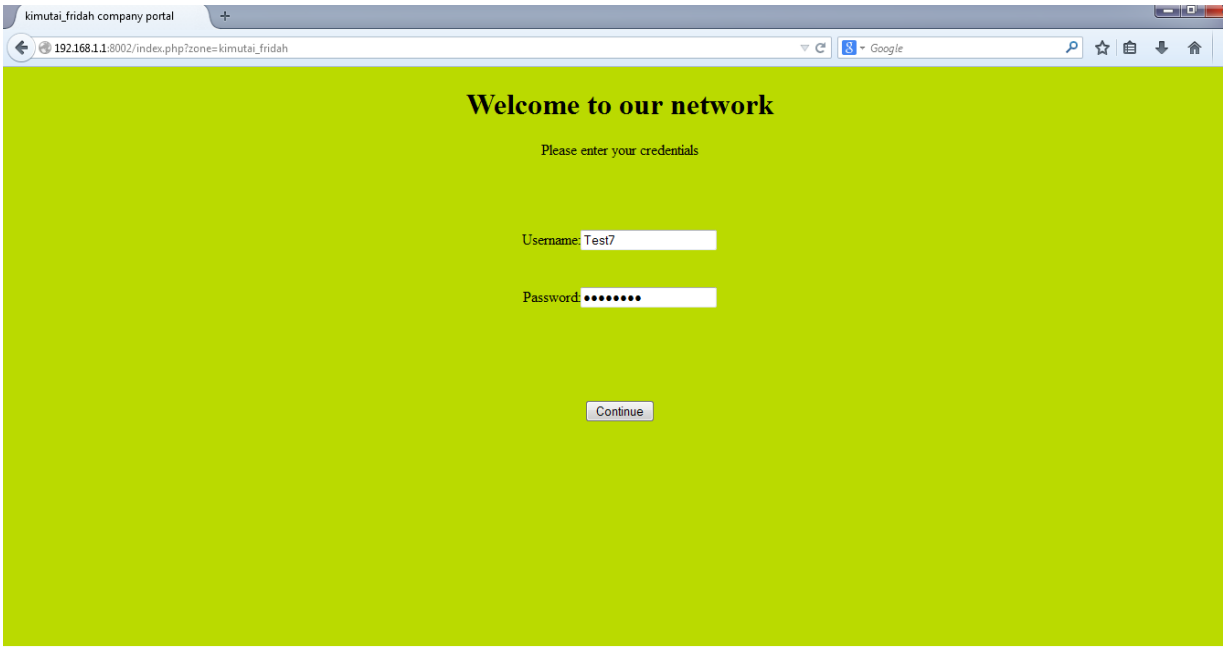


Figure 16: captive portal page where a user is prompted to enter credentials

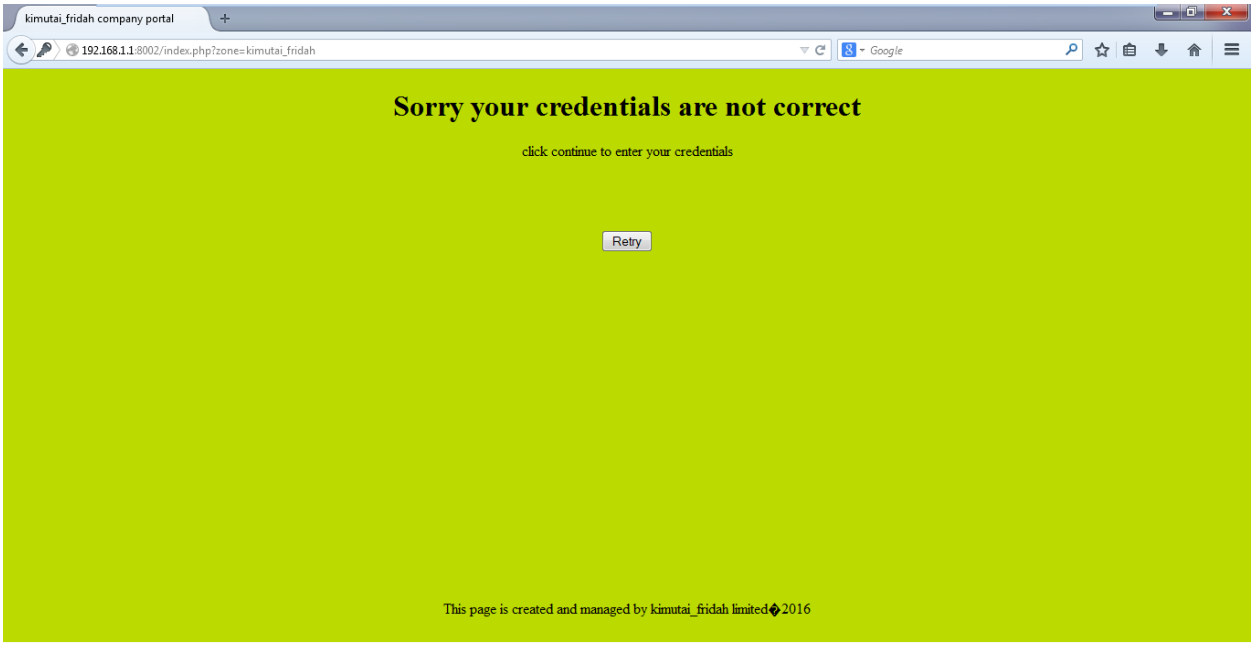


Figure 17: when a user entered wrong details

Setting and configuring captive portal in pfsense helps us to achieve our first objective since every user that will connect the small organization will have to be registered and therefore any other user with no account will not be able to connect to the organization's network. This helps in preventing unauthorized access to the organizations' network or bandwidth.

4.6 Creating Aliases

Aliases act as placeholders for real hosts in the departments of a small organization. By adding all of the hosts in a small organizations' departments to an alias, only one firewall rule is necessary. In a case of a small organization we have five departments that will be added as Aliases.

In the pfsense menu click the firewall tab where you will see Aliases tab in the drop box. Click the Aliases and click on the (+) add sign for creating the Aliases. The requirement here is the properties for the Aliases, the first Aliases name in this case is our first class of which is management, the description for the Aliases is "this is management portion of the network", the type is hosts, the prompt that requires has to enter the IP address of the Alias the IP address of the management department subnet that is 192.168.1.1/27 is set, click on the save button and apply the changes as prompted. The same procedure is used to add all our five Aliases that is management, ICT, finance and procurement, human resource and transport and customer care departments.

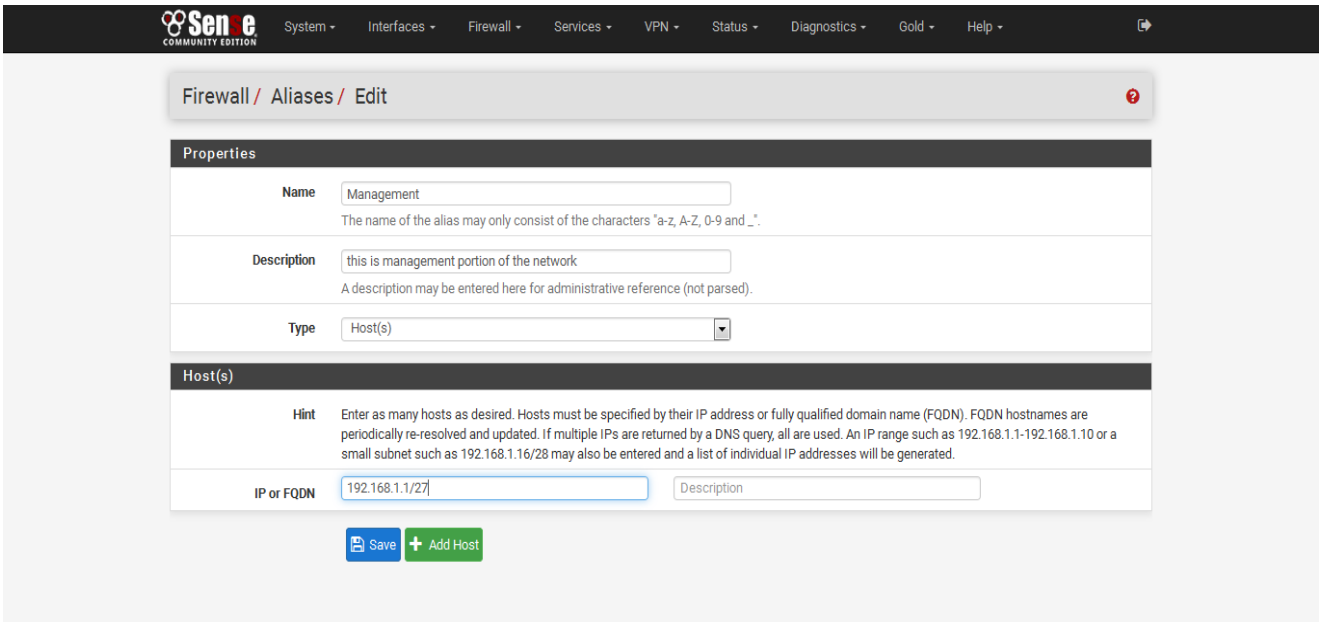


Figure 18: Creating Aliases

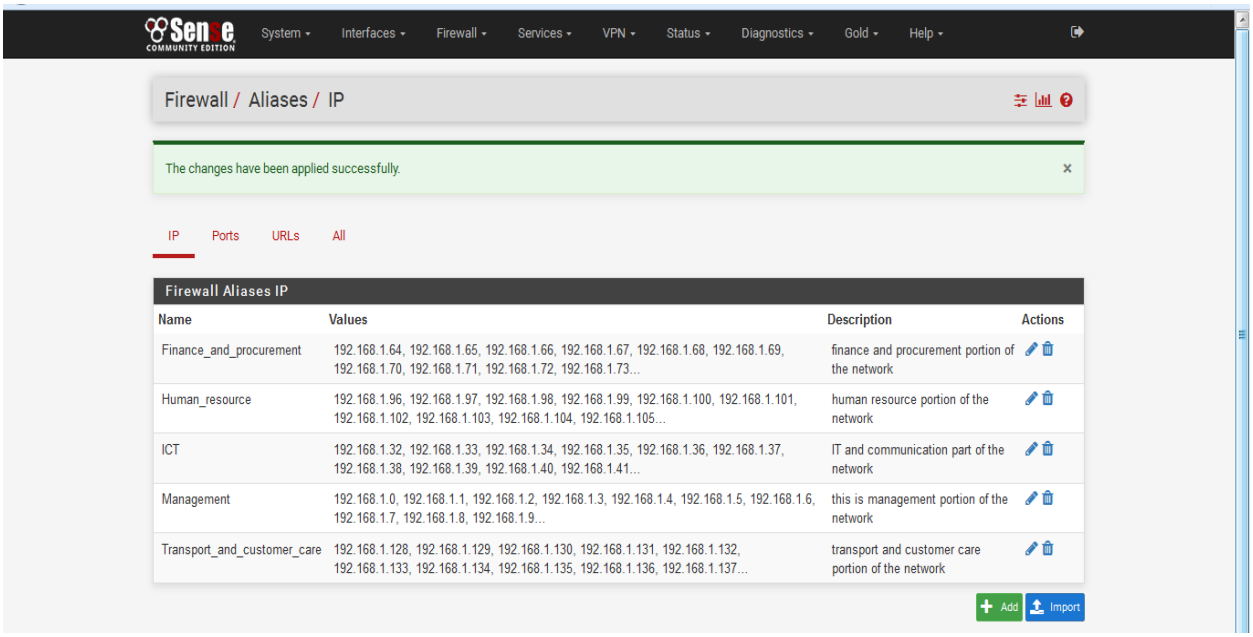


Figure 19: Created with their host IP addresses

4.7 Adding Queues

The first step is to use the Traffic Shaper. Click firewall, then traffic shaper and finally click the by interface and choose LAN interface. Select CBQ for the scheduler type, Check the

Enable/disable discipline and its children, enter the name of the queue which in our case is management, select the priority for the queue in this case management will have the highest priority that is 6, enter the bandwidth for the queue in this case the bandwidth for the management is 3500 Kbits as highlighted in previously in the table1. Click on the save button and apply the changes in the pfsense. The same procedure is applied to create queues for all other departments of a small organization but with each department allocated its share of bandwidth indicated in table1.

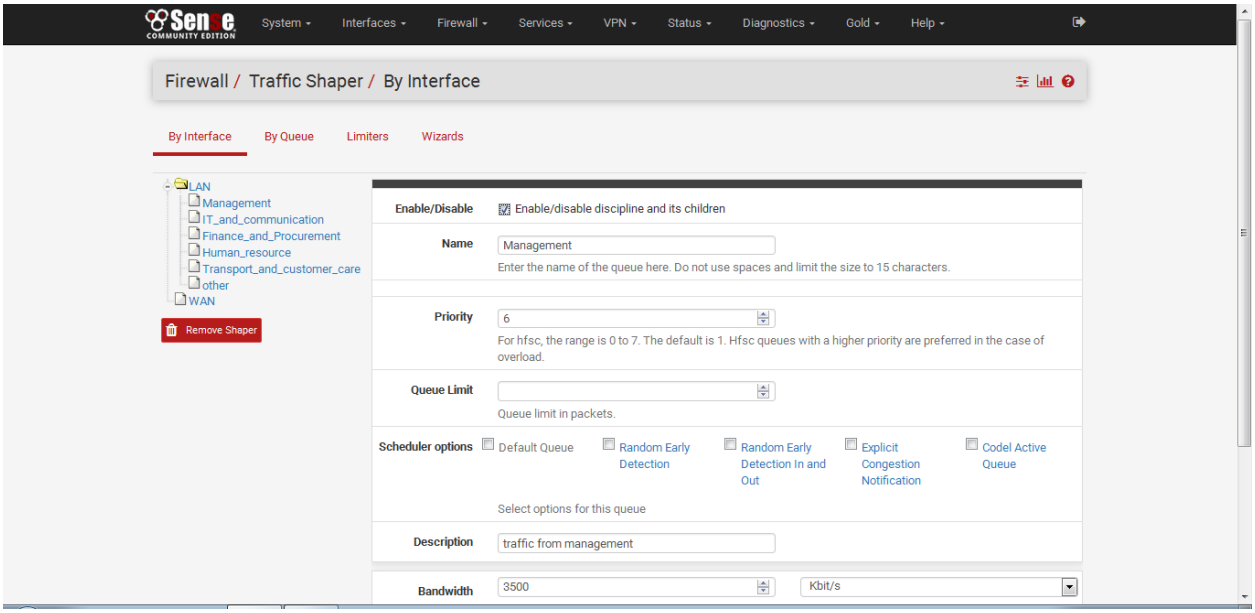


Figure 20: Creating queues

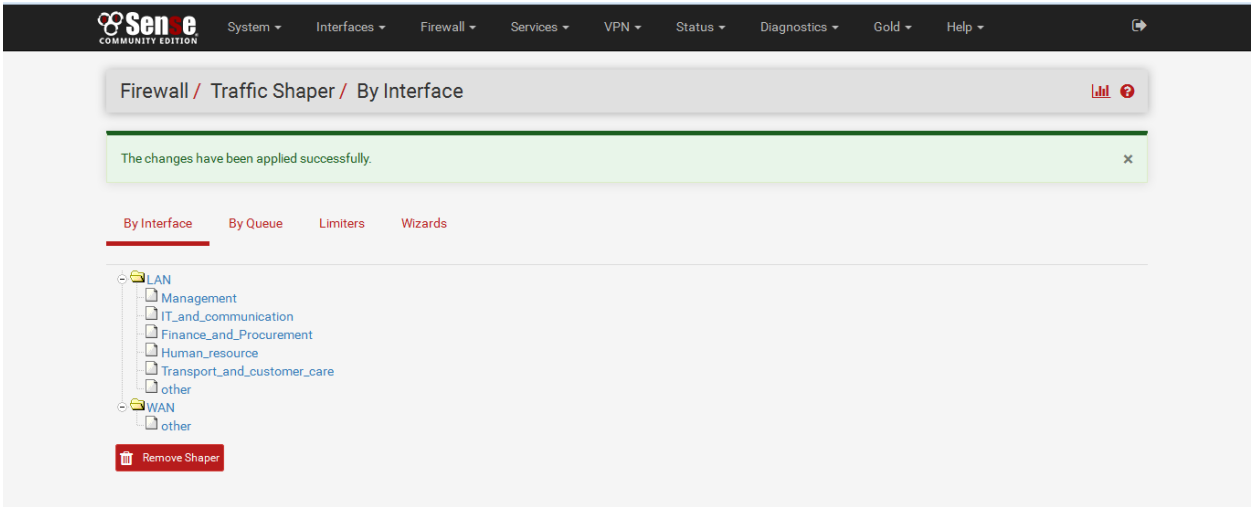


Figure 21: Created Queues for all the departments in the LAN interface

4.7.1 Limiting Bandwidth for Specific Queues

The purpose of using limiters is that it helps us to limit the amount of bandwidth a group of hosts have access to. That is to mean the management which we allocated 3500kbits is only limited to access 3500kbits and cannot exceed that.

To set the limiters the following configurations are done; on the pfsense select firewall, and on the firewall select traffic shaper, on the traffic shaper interface select limiters after which the limiters are added to every queue, that is every queue here is configured to have access to the bandwidth allocated to it. On the limiters click on the add sign (+) to add the limiters on the each of the queues that were previously configured. To set the limiter for the queue management as shown in the picture below. First check enable the limiter and its children, for the name its management since we are setting the limiter for management, bandwidth for management is 3500kbits, for mask select source address ,click on the save button and apply the changes on the pfsense. All the other queues in the small organization are added using the same procedure used in creating a limiter for management queue.

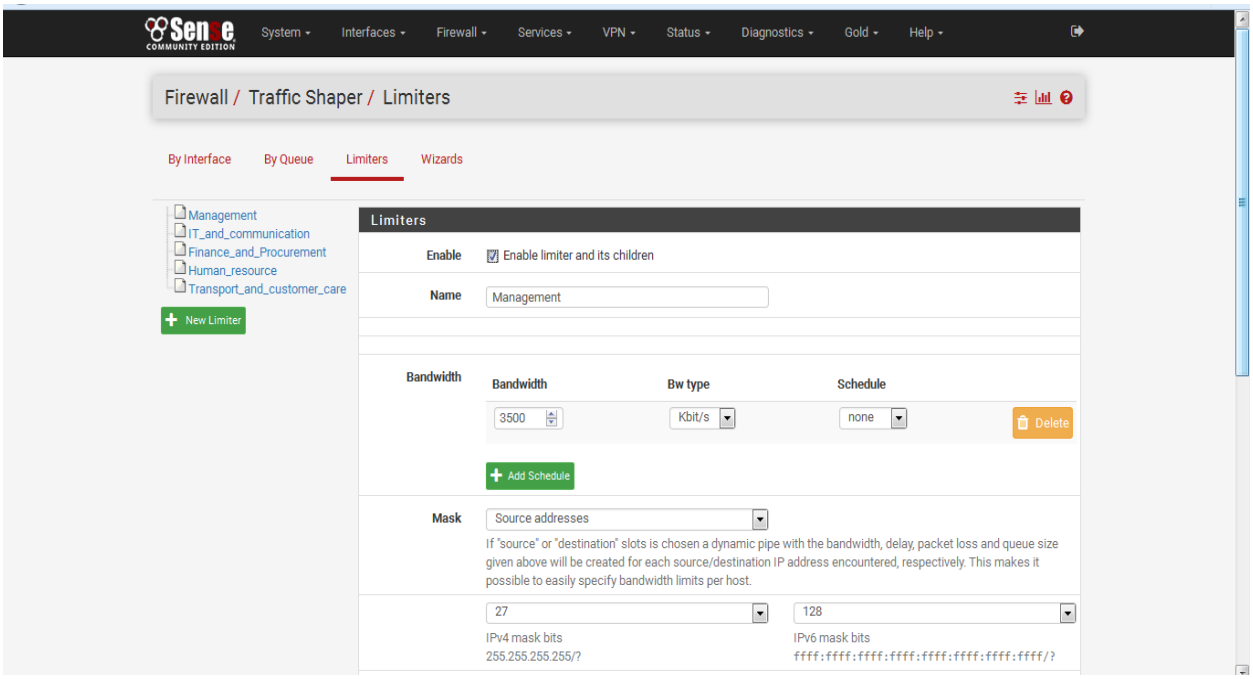


Figure 22: Creating limiters for queues

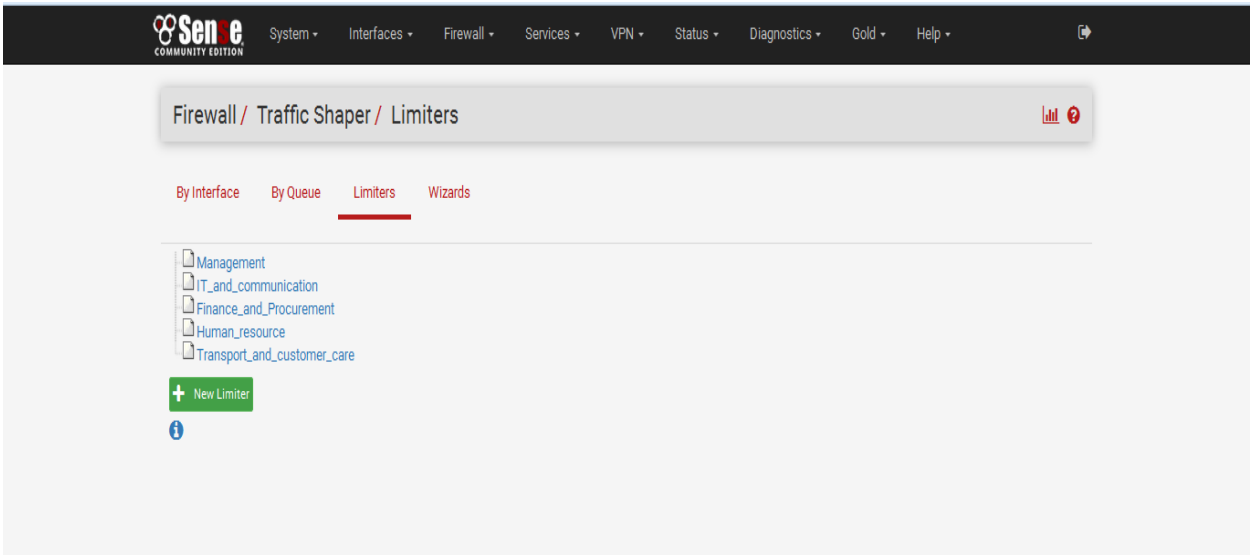


Figure 23: Limiters created to all the queues

Limiting Internet Access for Some Applications in Some Queues

Limiting some queues not to access some applications/services to reduce bandwidth consumption in unnecessary services in the internet that doesn't benefit the organization was necessary**.** This will ensure that those queues/classes with high priority that is management and

ICT have some bandwidth allocated for specific applications/services which require high speed internet. It will also help in making sure that bandwidth wastage is reduced as well as to make sure that authorized users can only use the bandwidth with which they are authorized to use thereby avoid unauthorized use of bandwidth by authorized users.

To do this we created Aliases for those applications that we would like them to have high priority in the bandwidth for the case of high priority classes. In the case of the low priority classes that is the transport and customer care departments we as well created Aliases for those services/applications that we would like to limit their access in the class.

We limited hours of access to Facebook in the transport and customer care department so that they will only be able to access Facebook from 12noon to 2pm in the working days that is from Monday to Friday.

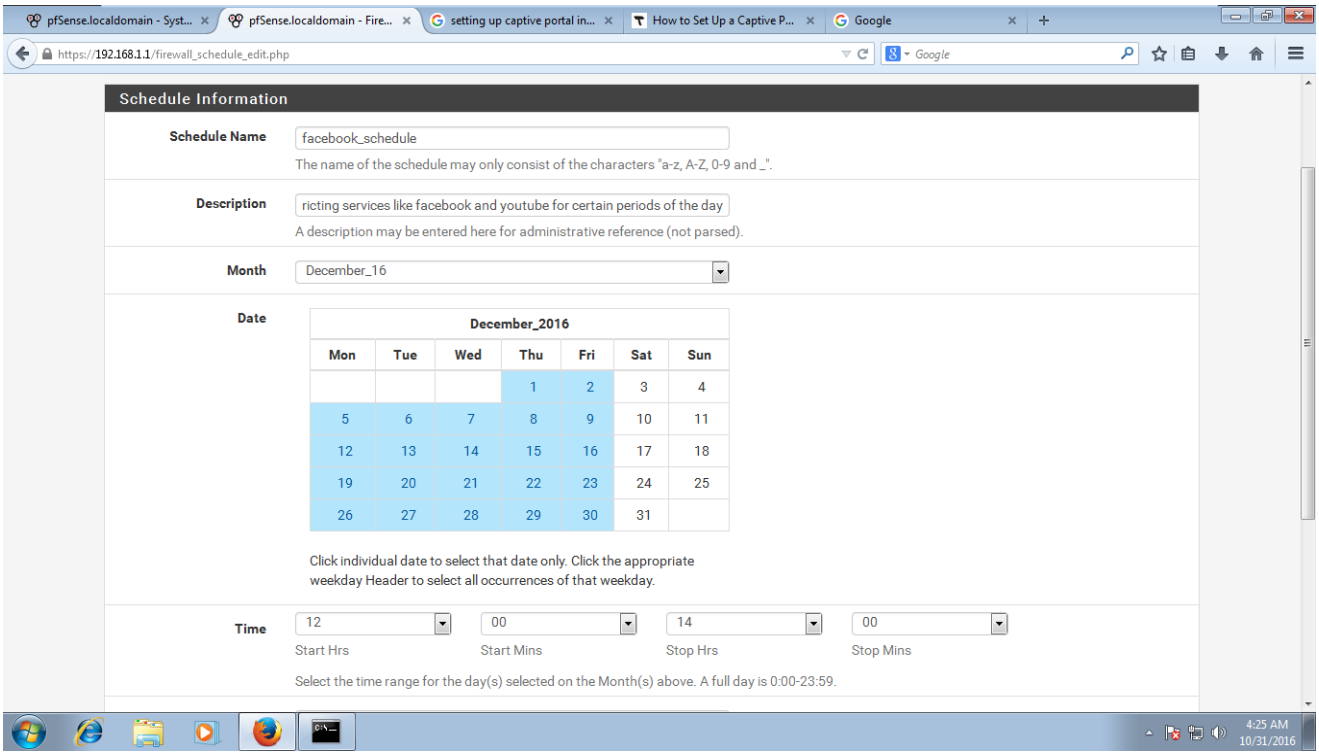


Figure 24: Facebook access limit in the transport and customer care departments

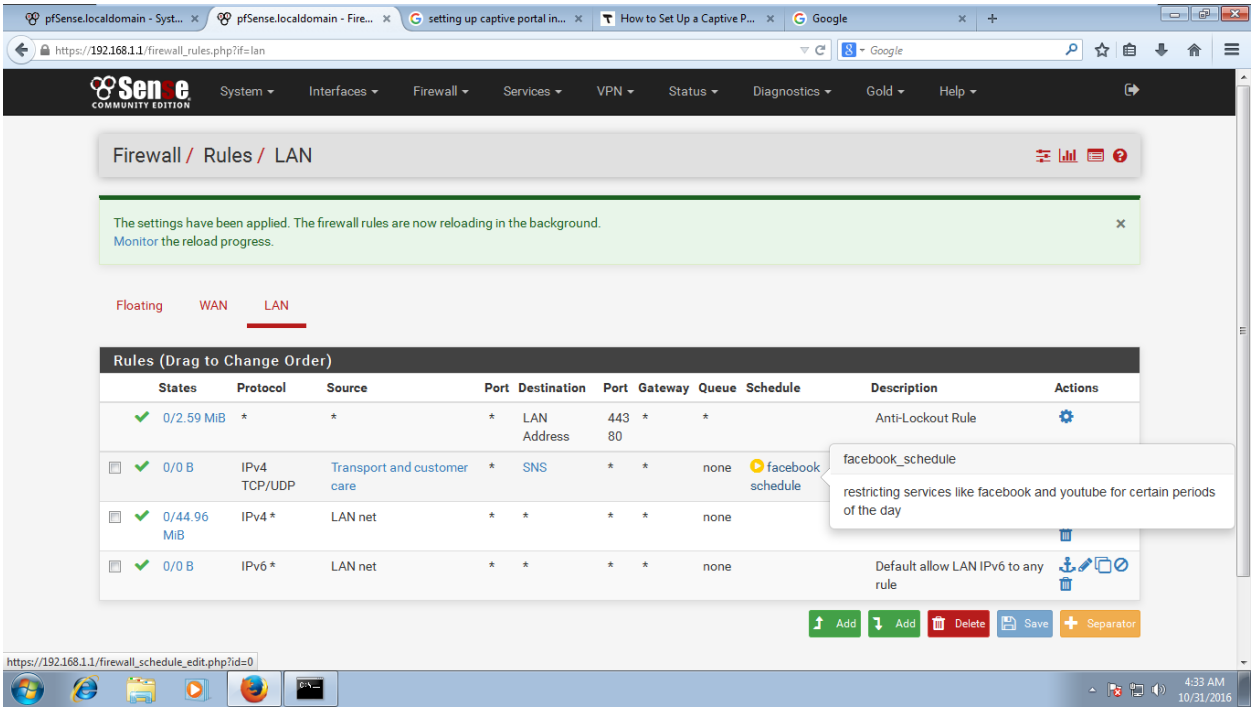


Figure 25: Firewall rule created for Facebook limit hours

Figure 25 above shows the firewall rules created to restrict access to Facebook by transport and customer care departments users in the hours that they are not supposed to access.

4.7.2 Filtering Traffic in the Queues

We use firewall rules to assign traffic to a queue. The rule allows the outbound traffic, and at the same time assigns the returning packets into a queue. To do this we add filtering rules in the pfsense firewall. From the pfSense menu choose Firewall/Traffic Shaper, Click on the LAN tab. When adding filtering rules click on the Add Rule button, For Action choose Pass, For Interface choose LAN, for address family choose IPV4, for protocol choose chose any. For source choose single host or Alias, For Destination choose Management, click on the Save button and apply the changes. The screenshot below illustrates the rule being created for each single Alias. We have five Aliases in our case that is management, ICT, Human Resource, Finance and procurement and finally Transport and Communication. All these Aliases are created the firewall rules by their own as single Aliases independently. The procedure done for the management queue is done to all our five queues.

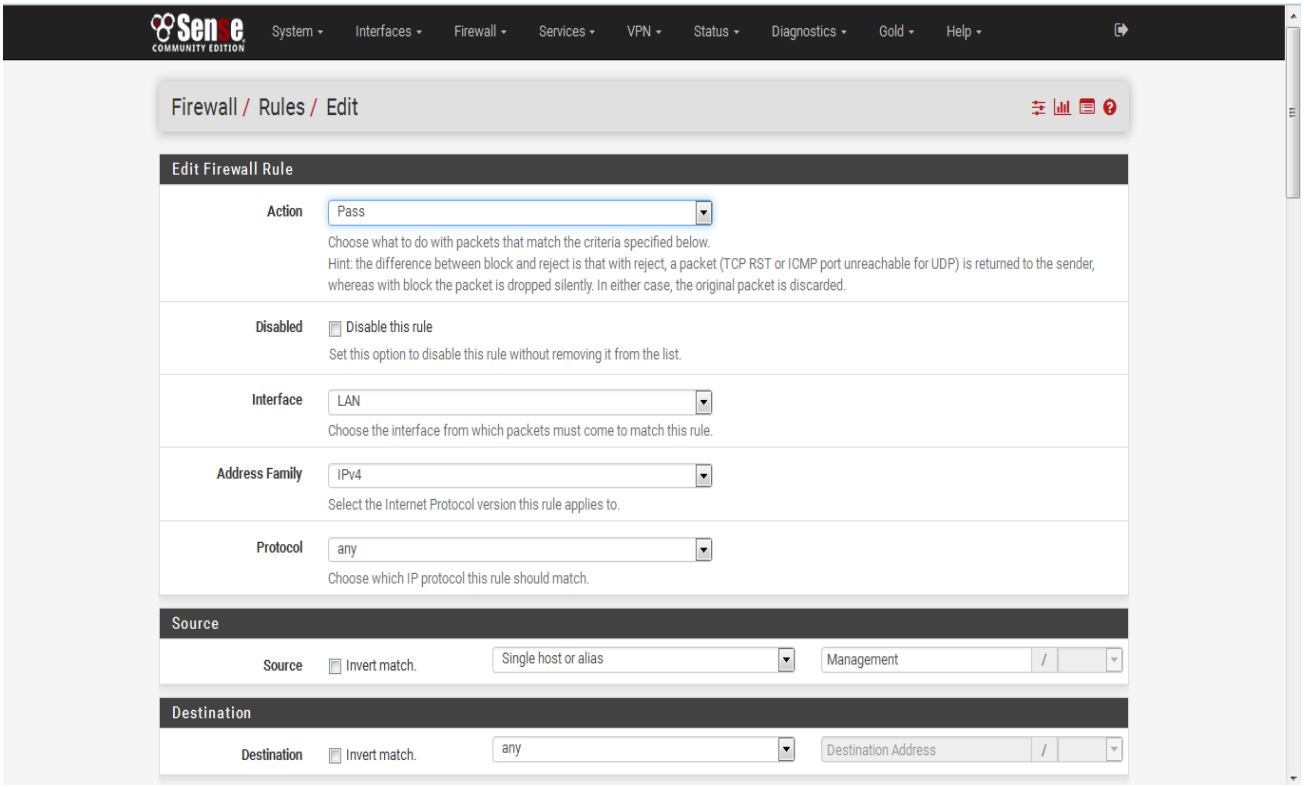


Figure 26: Adding and editing filtering rules

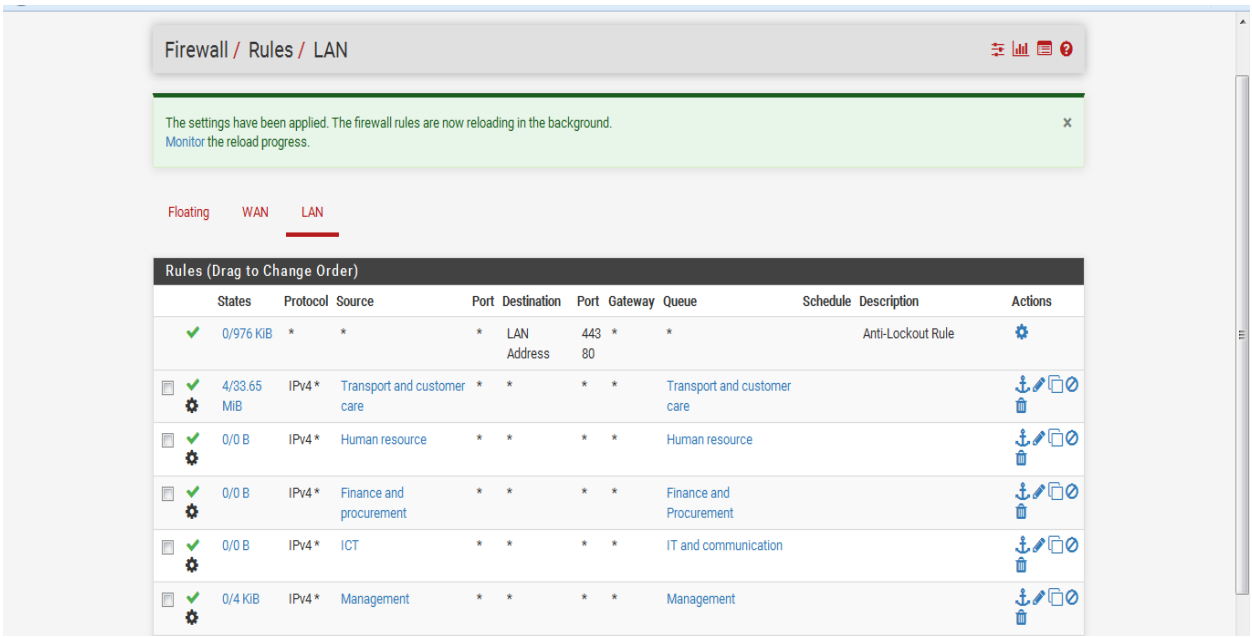


***Figure 27: Filtering rules set for all the queues*.**

4.7.3 Penalty box

For those hosts who are notorious in the network by misusing the internet we put them in a category called the penalty box we create an alias for those hosts and call it penalty box and go to rules and limit their internet usage in the network

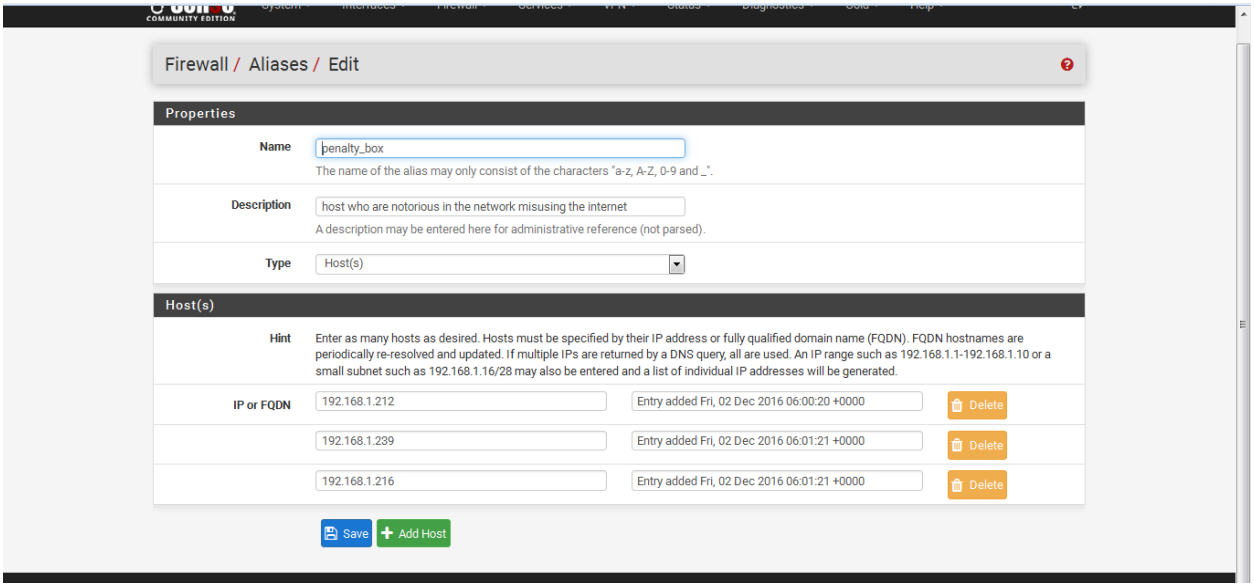


Figure 28 Creating alias for penalty box

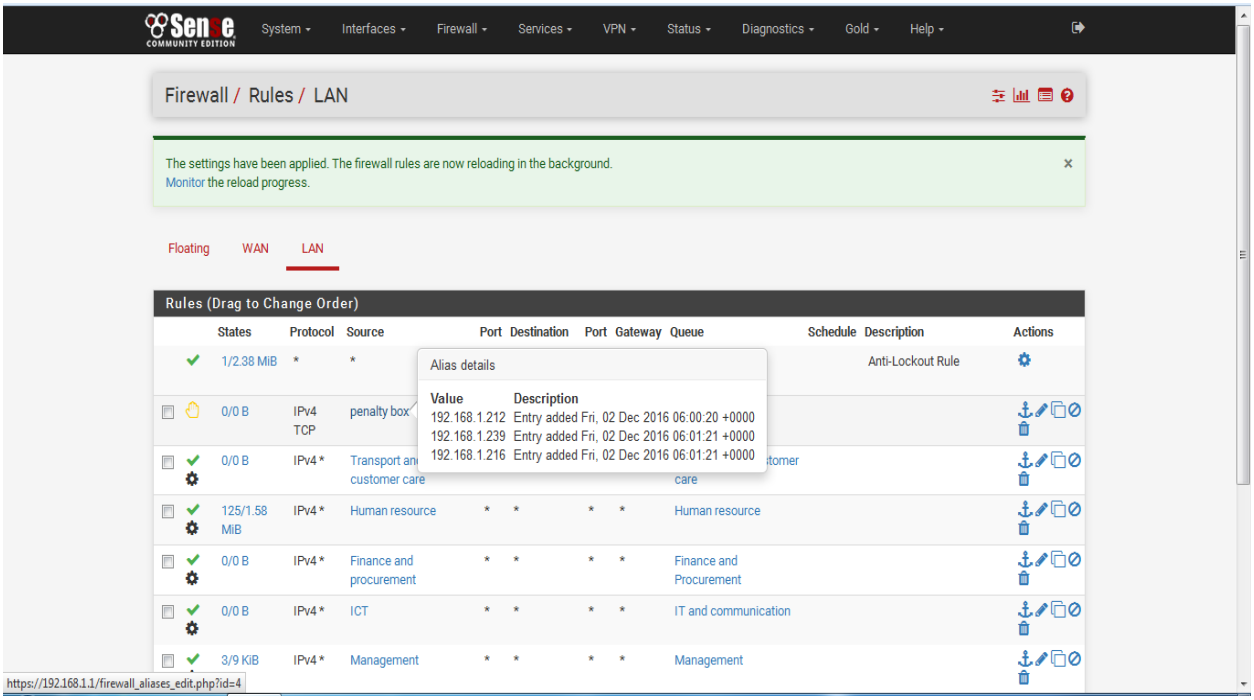


Figure 29: Limiting bandwidth for users in the penalty box

4.7.3 Classifying Inbound Connections

Put a large file on the internal web server .Add a port forwarding rule in pfSense, classifying traffic as HTTP by choosing Firewall/NAT from the pfSense menu, on the Port Forwarding tab, add a new rule, for Destination port range choose HTTP, for Redirect target IP enter 192.168.1.1, for Redirect target port choose HTTP, for Description enter Forward HTTP to internal web server, click on the Save button.

Now click on the Edit button next to the rule to edit it again, scroll down to Filter rule association and click on View the filter rule. Scroll down to Ackqueue/Queue, click on the Advanced button and choose none/none. Then click on the Save button. We also want to ping the pfSense external interface from outside, to measure the queue responsiveness. To do that, add a rule that Passes protocol ICMP, ICMP type echo-request, destination that is WAN address and Description that is allow pings to pfSense external. You should see a prompt to apply changes to the firewall rules, Click on the Apply changes button.

By creating rules using CBQ scheduler creates a tree hierarchy of classes; each with an assigned priority and bandwidth limit. Priority in CBQ only process enough packets until the bandwidth limit is reached. This helps us in prioritizing each class or queue by choosing each queue's priority as well as allocating bandwidth for each class. This means inbound and outbound traffic will be given priority to the queues /classes with highest priorities first. This means traffic in the management queue will be given the first priority as compared to a traffic in the transport and customer care queue.

Adding limiters to every queue as highlighted previously helps us to limit the amount of bandwidth a group of hosts have access to. Without adding the limiter the queues created could access bandwidth more than what is allocated to them. To prevent queues from accessing bandwidth which they have not been allocated we use the limiters to each queue to make sure they are limited to the bandwidth that is allocated to them. This helps in making sure that authorized users/hosts don't use bandwidth which they have not been allocated to use.

All the above procedures lead to one and most vital procedure which we cannot avoid or ignore and that is creating firewall filtering rules. Firewall rules control what traffic is allowed to enter an interface on the firewall. Rules can be created for either inbound traffic or outbound traffic.

The rule can be configured to specify the computers or users, program, service, or port and protocol. You can specify which type of network adapter the rule will be applied to: local area network (LAN), wireless, remote access, such as a virtual private network (VPN) connection, or all types. You can also configure the rule to be applied when any profile is being used or only when a specified profile is being used.

As soon as a network packet matches a rule, that rule is applied, and processing stops. For example, an arriving network packet is first compared to the authenticated pass rules. If it matches one, that rule is applied and processing stops. The packet is not compared to the block, allow, or default profile rules. If the packet does not match an authenticated pass rule, then it is compared to the block rules. If it matches one, the packet is blocked, and processing stops, and so on. Inbound rules explicitly allow, or explicitly block, inbound network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly allow traffic secured by IPsec for Remote Desktop through the firewall, but block the same traffic if it is not secured by IPsec. To allow a certain type of unsolicited inbound traffic, you must create an inbound rule that describes that traffic. For example, if you want to run a Web server, then you must create a rule that allows unsolicited inbound network traffic on TCP port 80.

Outbound rules explicitly allow, or explicitly block, network traffic originating from the computer that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to a computer (by IP address) through the firewall, but allow the same traffic for other computers. Because outbound traffic is allowed by default, you typically use outbound rules to block network traffic that you do not want.

Adding aliases, creating queues and creating filtering rules combined enable us to achieve the objective of preventing unauthorized use of organization's bandwidth by authorized users.

4.8 Accounting for Bandwidth Usage

Accounting for bandwidth usage means being able to ascertain that the bandwidth being used by every department in a small organization is the one that they are allowed to. In order to make

sure that users and departments in a small organization are using bandwidth as they should, we make use of ntopng package in the pfsense which is a network probe that shows network usage.

In order to make use of ntopng package the package is first installed in the pfsense. After installation using the pfsense graphical user interface: Navigate to Diagnosis tab and select the **ntopng settings**. In the settings enter user name and password.

To ensure that users are using only bandwidth they are assigned using ntopng navigate to diagnosis and click on the **ntopng**. Ntopng gives interfaces that will enable view the following:

i. Sort network traffic according to many criteria including IP address, port, protocols, and throughput.
ii. Show network traffic and IPv4/v6 active hosts.
iii. Produce long-term reports about various network metrics such as throughput, application protocols
iv. Top number of talkers/listeners, top ASs, top L7 applications.
v. For each communication flow report network/application latency/RTT, TCP stats (retransmissions, packets OOO, packet lost), bytes/packets
vi. Store on disk persistent traffic statistics in RRD format.
vii. Geo-locate hosts and display reports according to host location.

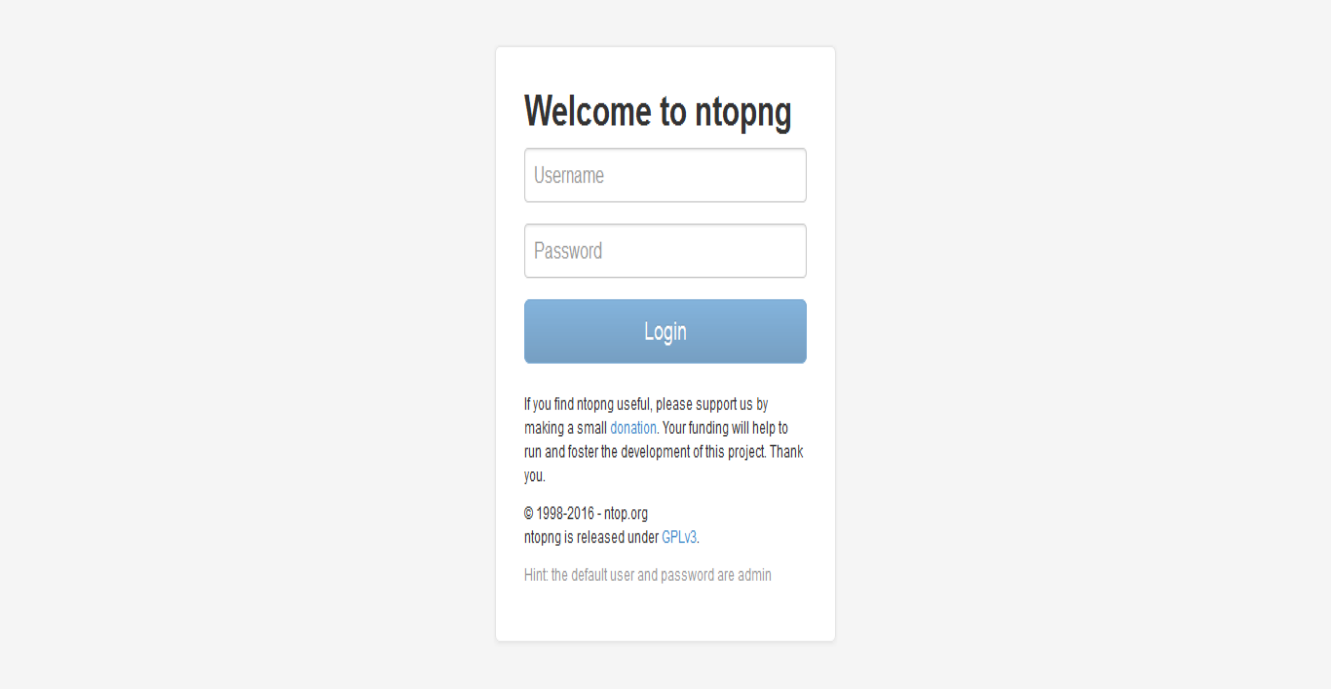


Figure 30: Logging in to ntopng

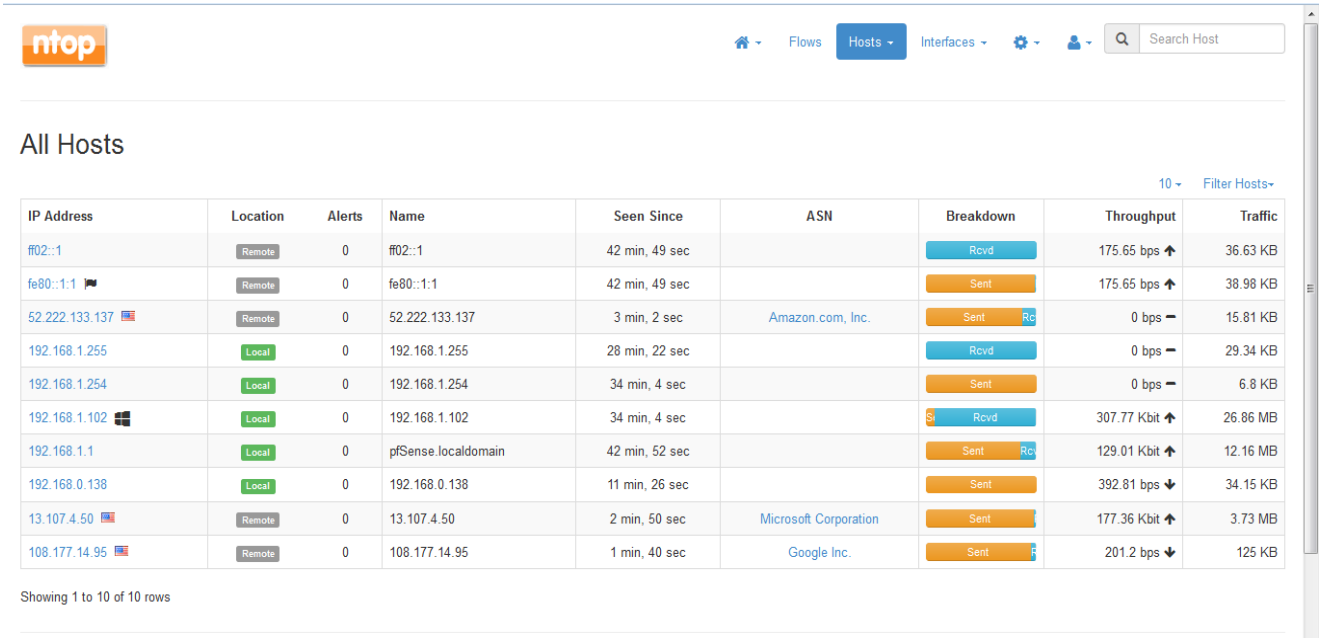
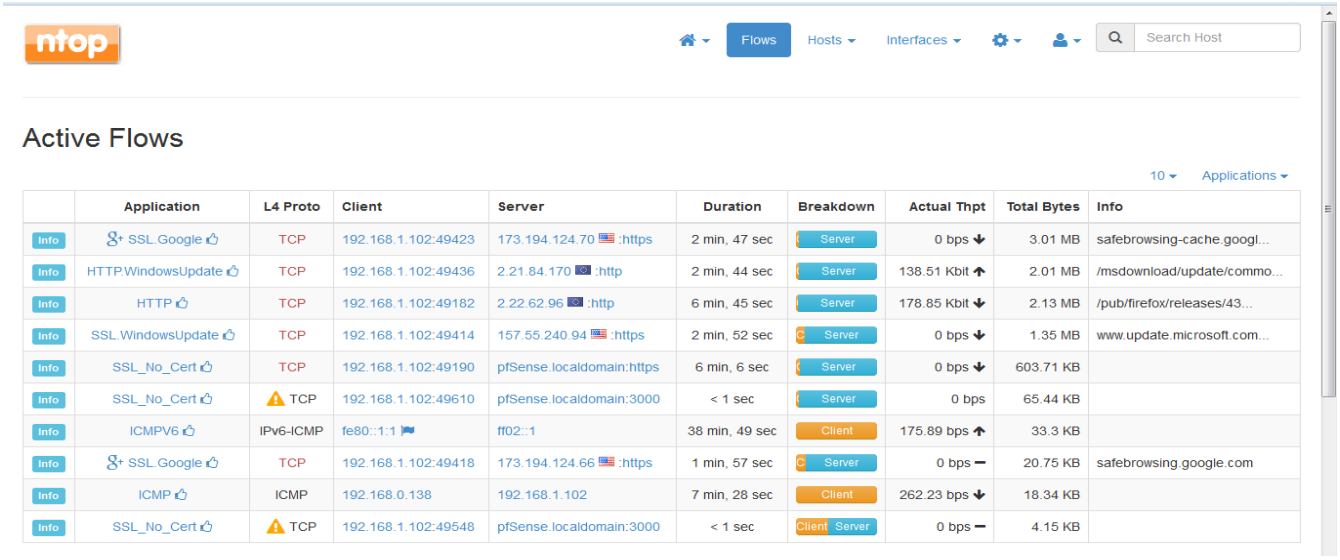


Figure 31: List of all hosts in the network



	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	SSL.Google	TCP	192.168.1.102:49423	173.194.124.70 :https	2 min, 47 sec	Server	0 bps	3.01 MB	safebrowsing-cache.googl...
Info	HTTP.WindowsUpdate	TCP	192.168.1.102:49436	2.21.84.170 :http	2 min, 44 sec	Server	138.51 Kbit	2.01 MB	/msdownload/update/commo...
Info	HTTP	TCP	192.168.1.102:49182	2.22.62.96 :http	6 min, 45 sec	Server	178.85 Kbit	2.13 MB	/pub/firefox/releases/43...
Info	SSL.WindowsUpdate	TCP	192.168.1.102:49414	157.55.240.94 :https	2 min, 52 sec	Server	0 bps	1.35 MB	www.update.microsoft.com...
Info	SSL_No_Cert	TCP	192.168.1.102:49190	pfSense.localdomain:https	6 min, 6 sec	Server	0 bps	603.71 KB	
Info	SSL_No_Cert	TCP	192.168.1.102:49610	pfSense.localdomain:3000	< 1 sec	Server	0 bps	65.44 KB	
Info	ICMPV6	IPv6-ICMP	fe80::1:1	ff02::1	38 min, 49 sec	Client	175.89 bps	33.3 KB	
Info	SSL.Google	TCP	192.168.1.102:49418	173.194.124.66 :https	1 min, 57 sec	Server	0 bps	20.75 KB	safebrowsing.google.com
Info	ICMP	ICMP	192.168.0.138	192.168.1.102	7 min, 28 sec	Client	262.23 bps	18.34 KB	
Info	SSL_No_Cert	TCP	192.168.1.102:49548	pfSense.localdomain:3000	< 1 sec	Client Server	0 bps	4.15 KB	

Figure 32: Active flows

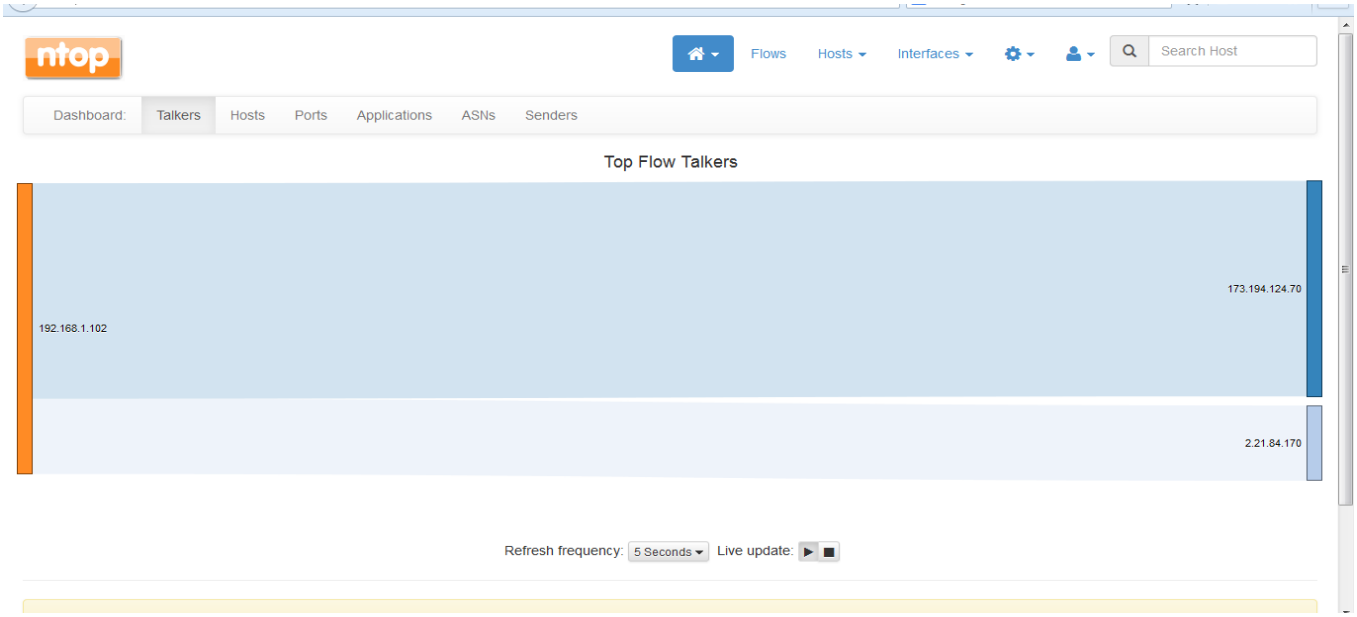


Figure 33: Top flow talkers

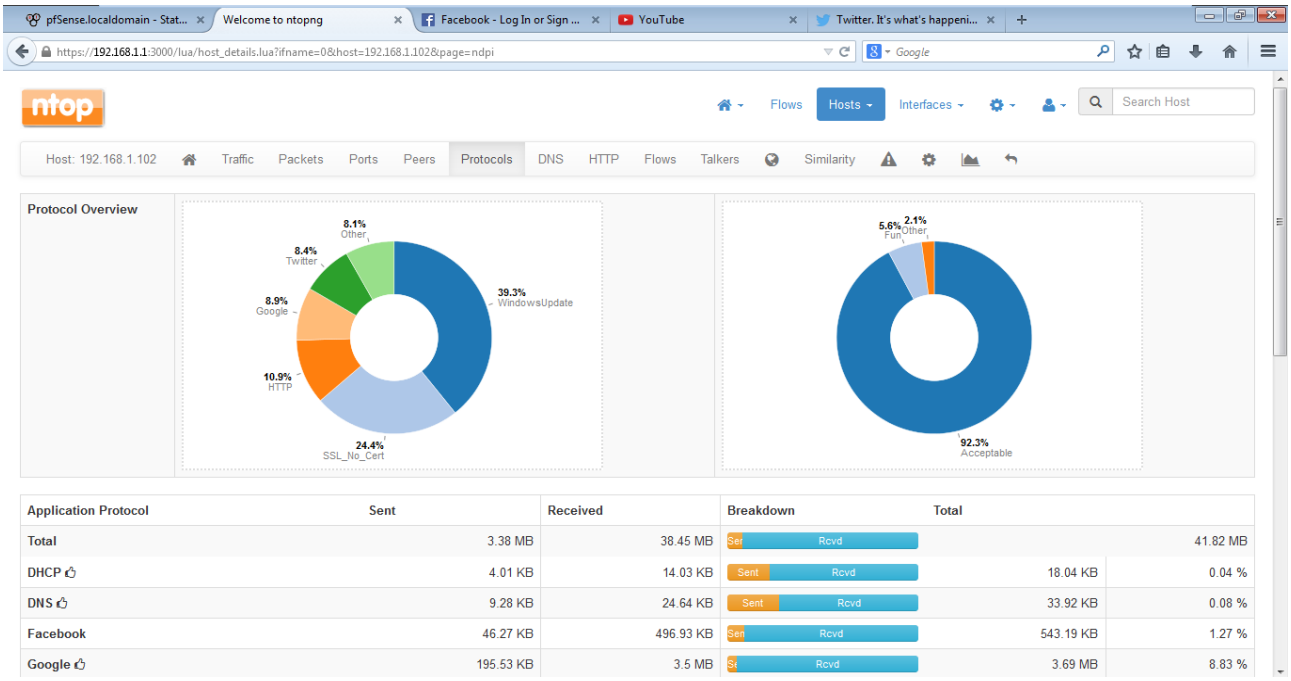


Figure 34: Protocols overview used by a single host

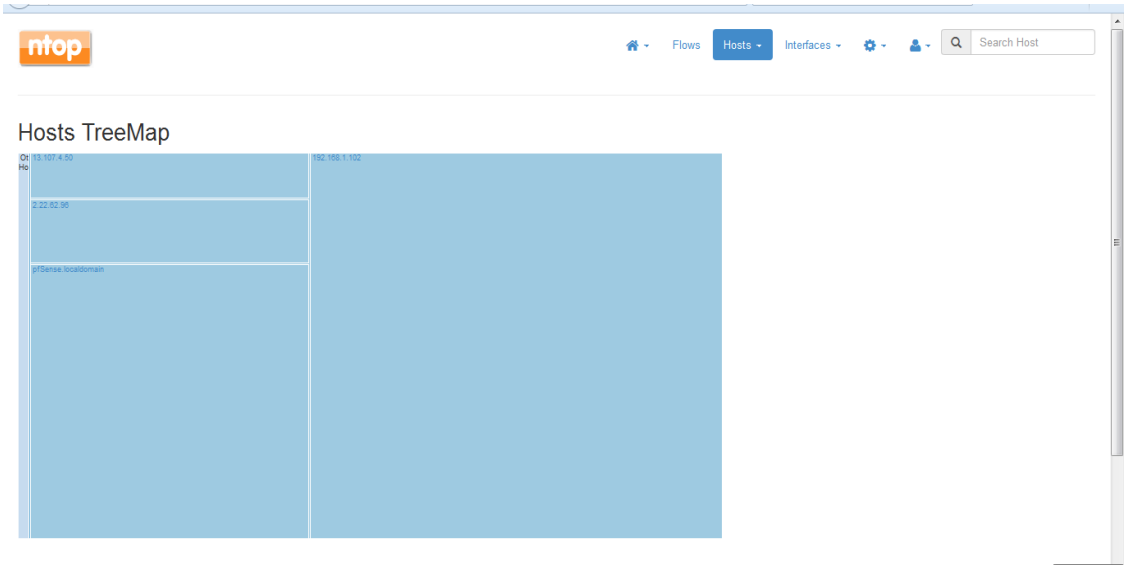


Figure 35: Hosts treemap

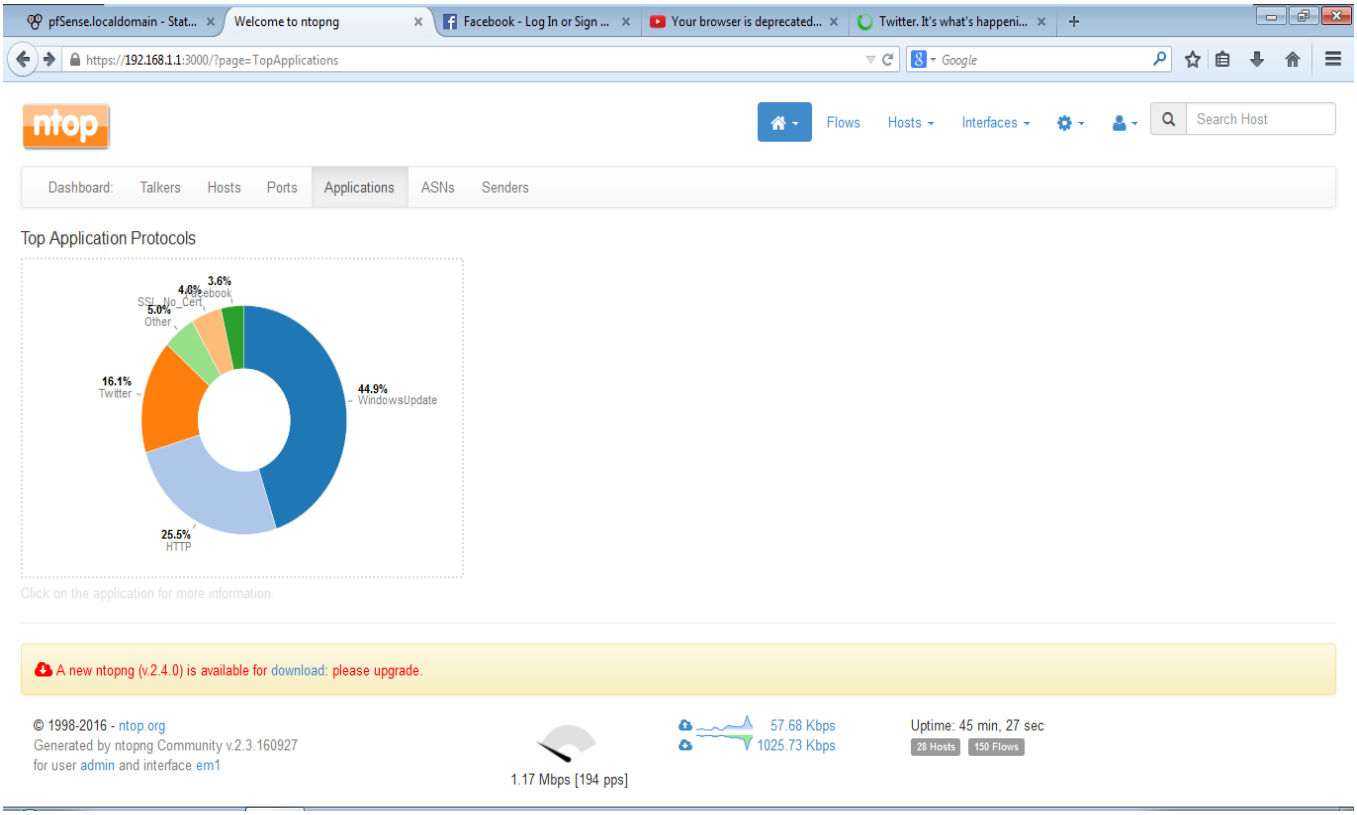


Figure 36: Top application protocols

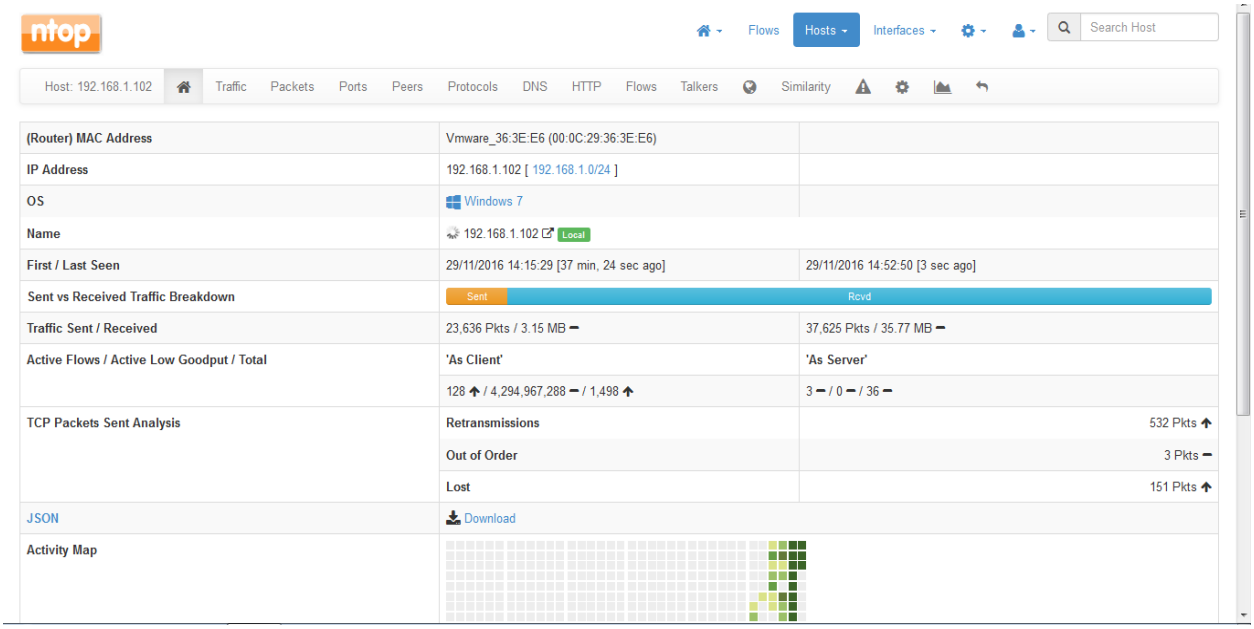


Figure 37: Host details

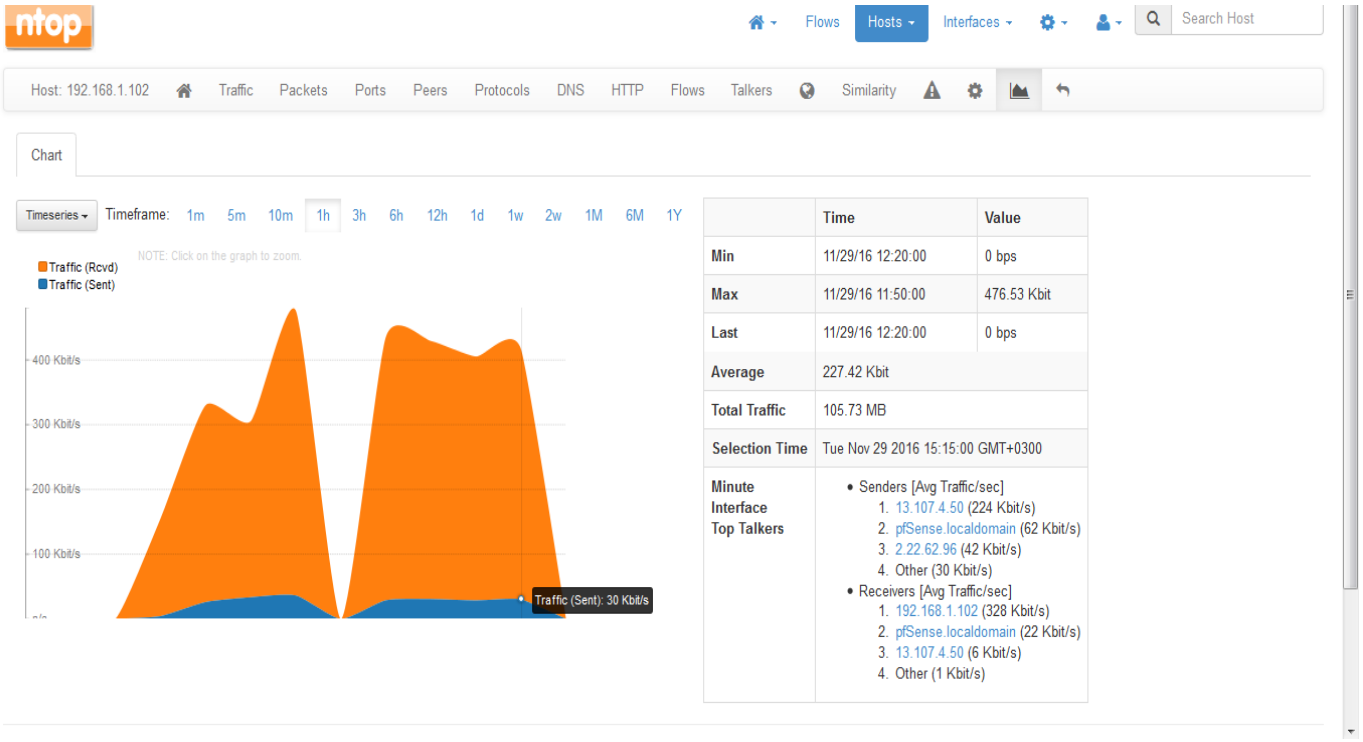


Figure 38: Average usage by a single host

By use of ntopng packet the objective of accounting for bandwidth used is attained since any abnormal traffic/unusual can be identified and traced down to single user by use of their IP address, services they are accessing and protocols used. By tracing each user or department we are able to know who is using what and whether they are using the services they are allowed to access.

CHAPTER 5

DISCUSSIONS, CONLUSION AND RECOMMENDATION.

5.0 Discussion

From the results obtained from the configuration and testing of captive portal authentication we find that Captive Portal may be used to prevent unauthorized access to the organizations' network or bandwidth by authenticating users by username and password entered on a portal page before they can use the network. The captive portal has two ways to set up authentication that is the use of local database or use of a radius server. The simplest way to set up captive portal authentication is to use a local database but this is limited to a fewer number of users and since this project is designed for small organizations which the number of users to be managed may vary RADIUS authentication was preferable and also it much more flexible. FreeRADIUS server and PfSense works perfectly since the service doesn't require much system resources. The service can easily handle authentication for several hundred clients without impacting performance. Captive portal authentication can suffer from man-in-the-middle attack and ARP poisoning that may allow an attacker to intercept data frames on a LAN or even sniff the username and password in a captive portal login page, the solution to this is to use HTTPs which provides encrypted authentication of captive portal server, and protects against man-in-the-middle attacks or ARP Spoofing. Captive portal is the best way to restrict the unauthorized users from accessing the internet using your bandwidth.

After users have been authenticated to the network and they have access to the internet what they do in the internet is a concern for the organization since most users are prone to wasting bandwidth. This project explained the use of queues, limiters and rules in a network to manage bandwidth provided by the ISP. To shape traffic in an organization we must identify different classes of users in the organization where their traffic will be queued basing on their priority so that users with high priority will get attended to first and those with lower priority will follow. Limiters on the other hand limit users in a certain department or class to a certain amount of bandwidth they are supposed to uses and are restricted from over using the bandwidth in the network starving other hosts, limiters also allow us to set specific limit of bandwidth at which a class is allocated. Rules help us to direct traffic in the network to specific queues like the management queues and human resource queue where we set a rule stating that traffic coming

from a certain portion of the network should be directed through a specific queue. Also the rules help us to uphold the limits from the limiters where by a rule states that a certain portion of the network should have a specific amount of bandwidth. By use of queues, limiters and rules proves to be the best way to restrict unauthorized of bandwidth by the authorized users in the network.

For the organization to account for its bandwidth usage it must monitor the status of its network. Ntopng is a package in pfsense that allows us to monitor the status of the network from the host level to application protocols level. Ntopng will even track where connections were made by local PCs, and how much bandwidth was used on individual connections. Thus enabling the accounting of bandwidth easy.

5.1 Conclusion

After implementing bandwidth management using pfsense in a simulated environment of a small organization, we have come to believe that it is possible to manage bandwidth. Pfsense firewall allows us to allocate appropriate bandwidth different departments using Class Based Queuing as our scheduler. On the other hand it makes it possible to give different queues (departments) priorities as per the urgency and how important the traffic from the department is to the organization. For instance we were able to assign highest priority to the management department with higher number of bandwidth since the management's network traffic is very fundamental to a small organization. Management ensures that all the operations of the business are in line with achieving objectives of the small organization that is by either having to connect with other small organizations and other activities which may require video conferencing. Other departments like transport and customer care department whose operations may not rely much on internet were able to be allocated less bandwidth with the least bandwidth. We are able to limit each class/queue (department) with its allocated bandwidth so that no class will exceed bandwidth which they are allocated. By limiting we are able to reserve bandwidth for some specific services in each department which their operations may require high speed traffic. The management network was able to be configured so that video conferencing is reserved bandwidth so that the management will have an easier time when having online meetings with top advisors and any other dignitaries. We were able to enable bandwidth borrowing in interclass bases .All the above enabled has to achieve the objective of making sure that there is no unauthorized use of bandwidth by authorized users.

We were able to ensure unauthorized access to a small organizations' network (bandwidth) by using the interesting package of sense that is captive portal. This enabled us to make sure that the small organization's bandwidth is used only by those users that have their accounts in the captive portal.

The objective of accounting for small organization's bandwidth is achieved by use of top package which gives all the every detail of the users that's by showing their IP addresses, operating system and the queue they belong, services they are accessing, protocols, time taken by the user in the internet and many more details that will enable evaluate whether the bandwidth is being used in s proper manner.

It is therefore clear that with use of pfsense firewall in a small organization environment Internet is more than adequate to meet the needs of a small organization, although without bandwidth management it would be completely overloaded. Bandwidth management will save us money on bandwidth while allowing small organizations to provide better and more appropriate network access.

5.2 Recommendation

We would recommend small organizations to adopt the use of pfsense firewall for bandwidth management by using the methods and techniques used in this project. Using pfsense will enable them to save funds used on bandwidth which is wasted when this firewall is not used. Pfsense is an open source firewall and this also will help them to save the funds that could have been used to purchase commercial firewalls. Pfsense is user friendly meaning it's easy to use by system administrators.

Every s small organization is trying to maximize profits while minimizing the cost of their business operation and hence adopting pfsense firewall in bandwidth management will play a very big role in making this achieved.

REFERENCES

Ayyagari, M. Beck, T. & Demirgüç-Kunt, A. (2015). Small and Medium Enterprises across the Globe retrieved from http://siteresources.worldbank.org/DEC/Resources/84797-1114437274304/SME_globe.pdf

Blue Coat Systems, Inc. (2016). QoS and Bandwidth Management retrieved on 30th October, 2016 from https://www.bluecoat.com/sites/default/files/documents/files/QoS_and_bandwidth_management.7.pdf

Bryant, B.J (2016). What Are the Benefits of the Internet to Business? Retrieved on 21st October 2016 from http://smallbusiness.chron.com/benefits-internet-business-316.html

Carr, M & Verner, J. (2013).Prototyping and software development approaches. Retrieved on 30/10/2016 from Http://www.cb.cityu.edu.hk/is/getFile.cfm?id=55

Cisco Systems, Inc. (2015). Cisco Preferred Architecture for Enterprise Collaboration 11.0. Retrieved on 30/10/2016 from http://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/11x/collbcvd/bwmgmt.pdf

Chege, K. and Ford, M. (2009) KENET: A Bandwidth Management Case Study IETF Journal retrieved on 30 Oct, 2016 from http://www.internetsociety.org/articles/kenet-bandwidth-management-case-study

Chereddi, K. C , (2009).Class Based Queuing (CBQ) for Link Sharing and Resource Management (The Linux Implementation) retrieved on 30th Oct, 2016 from http://www.hserus.net/~cck/pubs/ieee.pdf

Chitanana. L (2012). Bandwidth management in universities in Zimbabwe: Towards a responsible user base through effective policy implementation. International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2012, Vol. 8, Issue 2. Retrieved on 21/10/2016 from http://files.eric.ed.gov/fulltext/EJ1084130.pdf

Daneen, L. (2002). Bandwidth management tools, strategies and issues. Retrieved on 30 Oct, 2016 from https://net.educause.edu/ir/library/pdf/DEC0202.pdf

Dept. of CSE, SJBIT. (2013). Computer Networks-II retrieved on 30 Oct, 2016 from http://www.elearningatria.files.wordpress.com/2013/10/cse-vi-computer-networks-ii-10cs64-notes.pdf

Devajit, M, Majidul, A & Utpal, J.B. (2013)A study of Bandwidth Management in Computer Networks, International Journal of Innovative Technology and Exploring Engineering (IJITEE) .Vol.2, no.2 retrieved on 30th Oct, 2016 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.674.9846&rep=rep1&type=pdf

Dhaini, R.A, Assi, M.C. (2007). Dynamic bandwidth allocation schemes in hybrid TDM/WDM EPON Networks retrieved on 30th Oct, 2016 from http://www.eng.uwo.ca/electrical/faculty/shami_a/docs/Publications/EPON-JLT-Jan-2007.pdf

GFI Software. (2011). GFI White Paper: Internet monitoring: not 'Big Brother' but 'Wise Management'. Retrieved on 30th Oct, 2016 from http://www.gfi.com/whitepapers/Internet_Monitoring.pdf

Kashihara, S & Tsurusawa, M.(2010)Dynamic Bandwidth Management System Using IP Flow Analysis for the QoS-Assured Network,IEEE Global Telecommunications Conference, vol.5, no.2 retrieved on 30th Oct, 2016 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.308.7766&rep=rep1&type=pdf

Kassim, M, Ismail, M, Jumari, K. & Yusof, M.I. (2012), Bandwidth Management in an IP Based Network retrieved on 21/10/2016 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.308.7766&rep=rep1&type=pdf

Kithinji, J. (2016) A Survey of Packets Scheduling Congestion Control Algorithms in Internet Protocol Storage Area Networks. Retrieved on 30th Oct, 2016 from http://www.ijcat.com/archives/volume5/issue4/ijcatr05041008.pdf

Kotti, A, Hamza, R, & Bouleimen, K. (2009) New Bandwidth Management Framework for Supporting Differentiated Services in MPLS Networks, ICCSN International Conference .Vol.5 retrieved on 30th Oct, 2016 from http://ieeexplore.ieee.org/document/5076958/

Lahrssen, C. (2014). Top benefits of high speed internet for business accessed on October 2016. http://www.nexogy.com/blog/top-benefits-of-high-speed-internet-for-business

Li, S. (1999). Network Traffic Control and Bandwidth Management in Internet: A Differentiated Services Case Study retrieved on 30th Oct, 2016 from http://www.collectionscanada.gc.ca/obj/s4/f2/dsk1/tape3/PQDD_0029/MQ64392.pdf

Nomadix, Inc. (2016). Introduction to bandwidth management retrieved on 30th October, 2016 from http://www.nomadix.com/bandwidth-management

Ong'olo, D. & Awino, S. (2013). Small and Medium Enterprises and Devolved Government System: an Assessment of the Regulatory and Institutional Challenges Affecting the SMEs Development in Kenya retrieved on 21/10/2016 from http://www.trustafrica.org/en/publications-trust/icbe-research-reports?download=342:small-and-medium-enterprises-and-devolved-government-system-an-assessment-of-the-regulatory-and-institutional-challenges-affecting-the-smes-development-in-kenya

Paessler AG, (2016).All-In-One Bandwidth Monitoring: PRTG Network Monitor retrieved on 30th Oct 2016 from https://www.paessler.com/bandwidth_monitoring

Peter, M.O, and Babatunde, P.J. (2012) Software Prototyping: A Strategy to Use When User Lacks Data Processing Experience, ARPN Journal of Systems and Software.Vol.2,No.6. Retrieved on 1st Nov, 2016 from http://scientific-journals.org/journalofsystemsandsoftware/archive/vol2no6/vol2no6_4.pdf

Rohde &Schwarz. (2015). Case study R&S CMW500 retrieved on 30th Oct 2016 from www.ipoque.com/news-media/resources/casestudies

Snehalatha, N, Angeline, J. S. & Paul Rodrigues. (2013)Survey of Bandwidth Management Techniques retrieved on 30th Oct, 2016 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.676.4968&rep=rep1&type=pdf

Taecheol,O, Kiyeon,L & Sangyeun,C.(2011)An Analytical Performance Model for Management of Last-Level Cache and Bandwidth Sharing Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS),IEEE 19th International Symposium.Vol.12, retrieved on 1st Nov, 2016 from http://toc.proceedings.com/12663webtoc.pdf

Traver, L, Tarin, C, Cardona, N. (2009) Bandwidth Resource Management for Neural Signal Telemetry, Information Technology in Biomedicine, IEEE, Vol.13, and no.6 retrieved on 30th Oct, 2016 from

https://www.researchgate.net/publication/224586169_Bandwidth_Resource_Management_for_Neural_Signal_Telemetry

Visser, K. (1997). Enterprise education in South Africa". Papers in education, training and enterprise. Centre for African Studies, University of Edinburgh. www.http://napck.org / www.thedti.gov.za