Inácio Francisco Nhamahango

Implementação do Servidor Proxy para Segurança de Dados na Rede UP-NET
Estudo do Caso: Universidade Pedagógica de Maputo – Campus de Lhanguene

Licenciatura em Informática

Universidade Pedagógica de Maputo
Maputo
2023

Inácio Francisco Nhamahango

Implementação do Servidor Proxy para Segurança de Dados na Rede UP-NET

Estudo do Caso: Universidade Pedagógica de Maputo – Campus de Lhanguene

Licenciatura em Informática

Monografia científica apresentada ao curso de informática, Faculdade de Engenharias e Tecnologias da Universidade Pedagógica de Maputo para obtenção do grau académico de Licenciatura em Engenharia Informática.

Supervisor:

dr. Xavier Domingos Bila

Universidade Pedagógica de Maputo

Maputo

2023

ÍNDICE

Lista de Tabelas

Lista de Figuras

Lista de Abreviaturas

ACL – *Access Control List*

AD – *Active Directory*

CGI – *Common Gateway Interface*

CIUP – Centro de Informática da Universidade Pedagógica

DAC – *Discretionary Access Control*

FTP – *File Transfer Protocol*

HTTPS – *Hypertext Transfer Protocol Secure*

IMS – *If-Modified-Since*

IP – *Internet Protocol*

ISP – *Internet Service Provider*

LAN – *Local Area Network*

LDAP – *Lightweight Directory Access Protocol*

LFU – *Least Frequently Used*

LM – *Last Modified*

LRU – *Least Recent Used*

MAC – *Mandatory Access Control*

MD5 – *Message Digest 5*

MSNT – *Microsoft New Technology*

NCSA – *National Center for Supercomputing Applications*

NT – *New Technology*

NTLM – *NT Lan Manager*

PAM – *Pluggable Authentication Modules*

RF – *Requisito Funcional*

RFC – *Request For Comments*

RNF – Requisito Não Funcional

SARG – *Squid Analysis Report Generator*

SMB – *Server Message Block*

SMTP – *Server Message Transfer Protocol*

TCC – Trabalho de Conclusão de Curso

TCP/IP – *Transmition Control Protocol/Internet Protocol*

UC – *Use Case*

UML – *Unifield Modeling Language*

UPM – Universidade Pedagógica de Maputo

Declaração

Declaro que esta Monografia é resultado da minha investigação pessoal e das orientações do meu supervisor, o seu conteúdo é original e todas as fontes consultadas estão devidamente mencionadas no texto, nas notas e na bibliografia final.

Declaro ainda que este trabalho não foi apresentado em nenhuma outra instituição para obtenção de qualquer grau académico.

Maputo, 02 de Fevereiro de 2023

_____

Dedicatória

Dedico este trabalho aos meus pais Francisco João Nhamahango e Elisa Micas Boque, minhas avós Carolina e Catarina Mutambe, minha irmã Hortência pelos sacrifícios em prol da minha educação, apesar de várias dificuldades, fizeram tudo que estava ao seu alcance para proporcionar-me uma melhor educação, a minha esposa Rita da Lídia e aos meus filhos Sheila, Franklésio e Layerson vai o meu muito obrigado pelo apoio em todos os momentos e por serem minha fonte de inspiração.

Dedico ainda este trabalho a toda família Nhamahango, Mutambe e Boque que directa ou indirectamente incentivaram-me e nos momentos difíceis, deram o apoio necessário.

Vai ainda, uma dedicatória especial as turmas de informática de 2014 e de 2018 que durante anos partilhamos várias experiências acadêmicas e sociais.

Agradecimentos

Em primeiro lugar agradeço à Deus, pelo seu amor incondicional, graça e pelo dom da vida que me foi concedido.

Em Segundo lugar, agradecimentos especiais a minha família, amigos e todos que directa ou indirectamente, moral e financeiramente apoiaram a minha caminhada académica até alcançar este nível.

Ainda nesta íntegra, agradecimentos especiais ao meu supervisor, pela orientação, dicas e auxílio prestado no desenvolvimento deste trabalho e a todos os docentes da Universidade Pedagógica de Maputo em particular os da Faculdade de Engenharias e Tecnologias, pela forma mais sábia e inteligente como transmitem seus conhecimentos.

Aos colegas da Faculdade que trilhamos juntos esta caminhada longa e difícil, pois foram vários obstáculos e desafios que graças ao apoio e suporte um do outro, foi possível superar.

Resumo

Este trabalho de monografia com o tema "Implementação do servidor proxy para segurança de dados na rede UP-NET, estudo do caso: Universidade Pedagógica de Maputo – Campus de Lhanguene" consiste em um estudo teórico-prático sobre a implementação de um servidor *proxy (proxy server)* para segurança de informação em uma rede de computadores, apresentando-se as características e vantagens da mesma.
Pretende-se ainda demonstrar os mecanismos e políticas na solução de problemas de segurança da informação em uma rede de computadores, bem como alertar para aderência a esta tecnologia não só instituições de ensino mas também todas as instituições.
O trabalho tem como finalidade demonstrar a importância da segurança da informação e para a verificação dos resultados esperados, foi usada a ferramenta *virtual machine*, *ubuntu server* e *microssoft service pack 2* na sua virtualização.
O objectivo específico deste trabalho é demonstrar os mecanismos, as políticas de segurança de informação, acesso a internet e como funciona usando o *proxy server.*
Dessa forma, através da análise dos resultados obtidos com a virtualização do *proxy server*, é possível constatar o seu funcionamento e como é garantida a segurança de informação e largura de banda.

Palavras- Chave: *Proxy, Firewal, Internet.*

Abstract

This monograph work with the theme "Implementation of the proxy server for data security in the UP-NET network, study case of Universidade Pedagógica de Maputo – Campus de Lhanguene" consists on a theoretical-practical study of information security in a computers network, presenting the characteristics and advantages of the same. It also intends to demonstrate the mechanisms and policies in the solution of network information security, as well as to warn to adhere to this technology not only educational institutions but also institutions.

The work aims to demonstrate information security and to reach the results was used the virtual machine tool, ubuntu server and microsoft service pack 2 in virtualization.

The specific objective of the work is to demonstrate the mechanisms, information security policies, access to the internet and how it works using the proxy server.

In this way this project allows to verify how is the proxy server, the security of information, the bandwidth through results obtained.

Keywords: *Proxy, Firewall, Internet.*

CAPITULO I – INTRODUÇÃO

Com o advento da Internet, a grande rede está sendo utilizado cada vez mais facilmente como ferramenta de trabalho e para fins diversos. No caso de instituições, cabe ao administrador da rede fazer o controlo dos acessos à internet, visando a segurança da rede local, fazendo o bloqueio de *sites* indesejados, de downloads que são ou não permitidos, entre outros.

Cada vez mais os administradores têm que controlar e monitorar o acesso aos recursos das redes de computadores. Com isto, surgiram ferramentas que implementam diversas funções, entre elas, o filtro de pacotes, que trabalha na camada de rede, e os servidores proxy, que trabalham na camada de aplicação. Estas camadas baseiam-se no modelo de referência *Transfer Control Protocol / Internet Protocol* (TCP/IP).

A segurança da informação (SI) está directamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade.

A SI não está restrita somente a sistemas informáticos, informações electrônicas ou sistemas de armazenamento. O conceito aplica-se a todos os aspectos de proteção de informações e dados. O conceito de Segurança Informática ou Segurança de Computadores está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

A maioria das definições do conceito Segurança da Informação (SI) (Brostoff, 2004; Morris e Thompson, 1979; Sieberg, 2005; Smith, 2002) pode ser sumarizada como a proteção contra o uso ou acesso não-autorizado à informação, bem como a proteção contra a negação do serviço a utilizadores autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas. A SI não está confinada a sistemas de computação, nem à informação em formato electrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio da mesma. É importante lembrar que a SI também cobre toda a

infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias, e outros.

Nos dias actuais não existe outra fonte de informação tão extensa, dinâmica e de fácil acesso quanto à Internet. Através dela, é possível se ter acesso a todo e qualquer tipo de conteúdo, necessário no cotidiano da empresa. Porém, nem todo o conteúdo é benéfico aos interesses da empresa, podendo muitas das vezes, prejudicar o bom funcionamento e danificar equipamentos utilizados pela instituição.

Existe ainda, a possibilidade de acessos indevidos à rede interna da instituição, oriundos de equipamentos situados fora das dependências da mesma, podendo até serem considerados como ataques de *hackers* ou algo do tipo.

Mediante este cenário e a crescente busca pela optimização e segurança das redes, surgem a partir daí, diversos desafios, a fim de solucionar problemas de segurança e ao mesmo tempo optimizar os devidos acessos aos conteúdos que realmente se fazem necessários na instituição.

A finalidade deste trabalho é demonstrar alguns dos controlos que podem ser aplicados, utilizando os recursos da ferramenta proposta a fim de garantir a segurança em uma rede de computadores.

1.1. Problema

A Universidade Pedagógica de Maputo tem como ferramentas *open source,* o *zabbix e log-analise* e o seu *firewall* encontra-se nos seus roteadores, ou seja, não tem um *firewall* físico (*firewall* em *hardware*), assim sendo para segurança da sua informação, os roteadores não tem a capacidade de impor regras na rede para garantir a segurança da informação com maior rigor.

Invasões nos sistemas internos de empresas têm preocupado os profissionais da área de segurança de redes. Ataques que antes visavam apenas reafirmar a ousadia dos *hackers,* hoje se mostram com objectivos mais claros, tais como, roubo de informações confidenciais, desvio electrônico de recursos e congestionamento de serviços.

Perante o exposto, será apresentada a proposta de implementação de uma ferramenta de segurança de informação, assim como a importância de se implementar essa ferramenta no âmbito corporativo. Porém é importante salientar que não é o único dispositivo de segurança de rede, contudo um dos mais importantes.

Até que ponto o *firewall* implementado pela Universidade Pedagógica de Maputo - Campus de Lhanguene garante a segurança da informação na organização?

1.2. Objectivos

1.2.1. Objectivo geral

- Propor a implementação do servidor proxy na rede UP-Net para segurança de dados na Universidade Pedagógica de Maputo.

1.2.2. Objectivos específicos

- Analisar as fragilidades na rede UP-Net
- Identificar ferramentas para a segurança de dados;
- Implementar um servidor proxy para segurança de dados; e
- Avaliar vantagens de uso do servidor proxy na segurança de dados.

1.3. Justificativa

Contexto pessoal - O que levou-me a escolher o tema deve-se ao facto de ter paixão com as tecnologias de informação e comunicação, sendo que é a área em que me encontro na informática que abrange muitas áreas de informação e comunicação e pelo facto de estar a fazer Redes de Computadores.

O que me motivou mais para a pesquisa do tema proposto é o facto de querer progredir nesta área pesquisando mais e expandir os meus horizontes na pesquisa de redes informáticas explorando as formas de funcionamento, sendo que este ramo da informática está cada dia a crescer e a se implementar novas formas da sua constituição assim como os novos termos de protocolos, e este assunto porque tem a ver com a área na qual estou a me formar.

Outra razão da escolha do tema, é o desejo de dar o meu contributo na melhoria de condições de segurança na rede não só da instituição que formou-me mas também a todas instituições públicas ou privadas e alertar a todos sobre a importância de se investir em segurança no uso da internet.

1.4. Questões de pesquisa

- Quais são as características e as funcionalidades do *proxy server*?
- Quais são os benefícios de usar o *proxy server* na rede UP- Net**?**
- Será que a ferramenta de segurança de dados implementado pela Universidade Pedagógica de Maputo é eficiente?

1.5. Hipóteses

H0: A adopção de um servidor *proxy* a nível interno irá contribuir para a redução da possibilidade de invasão, roubo de informação e na minimização de riscos de segurança dos dados da Universidade Pedagógica de Maputo.

H1: A não implementação de um servidor *proxy* na rede, aumenta a probabilidade de invasão, roubo e riscos de segurança da informação na empresa Universidade Pedagógica Maputo.

H2: Se implementar o *servidor proxy* na rede da instituição, o nível de segurança da informação vai ser garantido.

1.6. Metodologia do trabalho

Para materialização deste trabalho de pesquisa, foram aplicados vários métodos, que podem ser classificados quanto a, natureza, abordagem, procedimentos e técnicas de coleta de dados.

1.6.1. Quanto a natureza

- **Metodologia aplicada**, que consiste em gerar um conhecimento a ser aplicado na resolução de um determinado problema;
- **Pesquiza acção ou aplicada,** consiste na implementação da solução em uma plataforma virtual, com a premissa fundamental de gerar conhecimentos para a aplicação prática num ambiente institucional de ensino, a Universidade Pedagógica de Maputo onde foi feita a colecta dos dados.

1.6.2. Quanto a abordagem

- **Metodologia qualitativa,** consiste na análise dos resultados esperados através de experiência.

1.6.3. Quanto aos procedimentos

- **Revisão bibliográfica,** consiste na consulta de manuais e outros documentos escritos que abordam o tema em estudo, de modo a colher experiências descritivas de vários autores.

1.7. Técnicas de recolha de dados

Para obtenção de dados, foram aplicadas seguintes técnicas:

- **A entrevista:** Consistiu em um questionário feito aos funcionários, estudantes e técnicos do CIUP. O questionário feito consta no anexo 1.

- **A Observação directa e participante**: Na qualidade de estudante e consequentemente utilizador da rede, pode verificar o desempenho da rede UP-Net.

1.8. Estrutura do trabalho

Este trabalho está dividido em quatro capítulos, que serão explanados a seguir:

- **Capítulo I:** É apresentada a introdução, a problematização, os objectivos almejados, questões de pesquiza, hipóteses e uma breve explicação sobre o que se pretende alcançar com este trabalho.

- **Capítulo II**: Neste capítulo, é apresentada a fundamentação teórica do trabalho, abordando os tópicos de gestão de redes e alguns dos seus conceitos: Gestão de redes de computadores; Servidor *proxy*, *Cache* e seus tipos: *Browse cache*, *proxy cache* e *transparent proxy cache.* Os filtros do *proxy*. Vantagens e desvantagens de um *proxy*, *Squid.* Autenticação com os módulos compatíveis com o *Squid*. Configuração do *Squid e* controlos de acesso, seus mecanismos e ACL.

- **Capítulo III:** Aqui, é a apresentação e discussão dos resultados alcançados com a pesquisa.

Por fim, é apresentada a conclusão, recomendações, referências bibliográficas e apêndices.

CAPITULO II - REVISÃO BIBLIOGRÁFICA

2.1. Gestão em redes

A gestão de rede pode ser definida como a coordenação (controlo de actividades e monitoramento de uso) de recursos materiais (moderms, roteadores, etc.) ou lógicos (protocolos), fisicamente distribuídos na rede, assegurando na medida do possível, a confiabilidade, tempos de resposta aceitáveis e segurança das informações.

Segundo Lima (1997), com o aumento da presença das redes de computadores nas instituições e como consequência o aumento da sua importância, faz-se necessária a gestão das redes de computadores para garantir e prevenir que alguns problemas mais graves interrompam ou prejudiquem seu desempenho e funcionalidade.

2.2. Gestão de redes de computadores

Segundo Sauvé (2002), a gestão de redes de computadores é divida em cinco partes nomeadamente:

- **Gestão de configuração** – Tem por objectivo analisar, monitorar mudanças referentes a infraestrutura física e lógica e fazer a manutenção da rede. Faz a colecta de informações de configuração de equipamentos e elementos de uma rede. Gera eventos quando recursos são agregados ou eliminados da rede, permitindo manter um inventário da rede, pois faz o registo de informações de todos os elementos que possam ser geridos na rede;

- **Gestão de falhas** – É responsável pela deteção, isolamento e resolução de falhas da rede. Através da deteção de falhas é notado algum problema nos elementos, por meio de monitoramento do estado de cada um. Com o isolamento de falhas, pode-se, depois de identificada, verificar-se a sua causa e pode-se também fazer a antecipação das falhas, ou seja, solicitar a manutenção do elemento através de alarmes, para não prejudicar o funcionamento da rede;

- **Gestão de desempenho** – É responsável pelo monitoramento do desempenho, sua análise e pelo planeamento da capacidade. O monitoramento e análise de desempenho baseiam-se em indicadores, como tempo de resposta, latência da rede, disponibilidade, taxa de erros, entre outros. A planificação da capacidade vai basicamente demonstrar dados que sugerem a alteração no modo de operação das redes;

- **Gestão de segurança** – Protege elementos da rede, monitorando e detetando violações das políticas de segurança. Preocupa-se com a proteção dos elementos da rede, sempre com base nas políticas de segurança pré-determinadas e faz toda a manutenção dos *logs* de segurança para detectar violações das políticas de segurança;

- **Gestão de contabilidade** – É responsável pela contabilização e verificação de limites da utilização dos elementos da rede. Monitora quais e quantos recursos da rede estão sendo utilizados, classificando por quem e quando são utilizados e também estabelece uma escala de tarifação.

2.3. Segurança de Informação

Segundo a norma ISO/IEC 17799, é a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos.
O conceito não está restrito somente a sistemas informáticos, informações electrônicas ou sistemas de armazenamento, se aplica a todos os aspectos de proteção de informações.
Esta definição leva a concluir que segurança de informação é o conjunto de diversas acções que visam garantir segurança de dados da instituição contra ameaças de diversa natureza através de implementação de diversos mecanismos desde lógicos até aos físicos.
Para uma proteção eficaz de informação, cada empresa ou instituição precisa definir suas políticas de segurança de informação.
Segundo a definição da norma ISSO 27001, entende-se por **Políticas de Segurança de Informação**, que é o conjunto de regras estabelecidas pela instituição com vista a proteger os dados da empresa contra qualquer tipo de ameaça e riscos, entre os quais, espionagem, sabotagem, ataques por piratas informáticos, vírus ou códigos maliciosos e até acidentes com incêndios ou inundações.
Segundo a norma ISO/IEC 17799, são princípios básicos de SI a tríade CIA (*Confidentiality, Integrity and Availability*) - Confidencialidade, Integridade e Disponibilidade – Que representam os principais atributos que, actualmente orientam a análise, a planificação e implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos a destacar são a irretratabilidade e a autenticidade.

- **Confidencialidade** – Também conhecido por princípio de privacidade, é propriedade que limita o acesso a informação somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da mesma.

- **Integridade** - Propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controlo de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

- **Disponibilidade** - Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles utilizadores autorizados pelo proprietário da informação.

- **Autenticidade -** É a propriedade que visa garantir a identidade inequívoca do autor ou remetente da informação.

- **Irretratabilidade -** É o princípio que visa garantir a impossibilidade do autor negar a autoria de determinada informação.

A proteção de uma rede de computadores é feito tendo em conta as duas partes que compõem a rede (Lógica e física). Sendo que **Proteção física** é a proteção de toda a infraestrutura física da rede contra qualquer tipo de ameaça (utilizadores não autorizados e desastres naturais), esta proteção pode ser garantida através de recursos humanos, sistemas de controlo de acessos e ou de identificação.

Por sua vez, **Proteção Lógica** é a proteção da parte lógica da rede (Sistema Oprativo, dados, programas) contra qualquer tipo de ameaça (acessos indevidos, ataques por *hackers*) e esta proteção é feito com recurso a *softwares* de controlo de acessos, senhas, firewalles, criptografia e antivírus.

2.4. Proxy

Em sua grande maioria, os navegadores de páginas web, fazem conexões directas com a internet. Mas há outra forma bem mais interessante de conexão: Eles podem ser configurados para se conectarem através de um servidor *proxy*.

O *Proxy* é um serviço que está disponível em um ambiente servidor, que recebe requisições das estações de trabalho para conexões à internet, onde seu papel fundamental é buscar a informação primeiramente no seu *cache* local e caso não encontre o documento requisitado, faz a busca no *site* solicitado pela estação de trabalho.

Na segunda situação, o endereço internet que fica registrado no servidor da página solicitada, é o do servidor *proxy*, pois o mesmo é o dispositivo que está entre a rede local e a internet.

O servidor *Proxy* surgiu da necessidade de intermediação do tráfego entre a rede local e a grande rede de computadores, a internet, através de um computador que provesse a partilha de internet com os demais computadores. Pode-se fazer a seguinte analogia: Rede local é uma rede interna e a internet é uma rede externa, sendo assim, o *proxy* é o dispositivo que permite as máquinas da rede interna se conectarem ao mundo externo. Como na maioria dos casos as máquinas da rede local não têm um endereço válido para a internet, elas fazem a solicitação de um endereço externo para o servidor *proxy*, que encaminha a requisição à internet. Caso não ache o documento solicitado em sua *cache* de internet, o servidor está habilitado a fazer essa consulta, pois o mesmo tem um endereço válido na internet. Sendo assim, pode-se dizer que é normal ter um servidor *proxy* directamente ligado à internet e com um endereço válido.

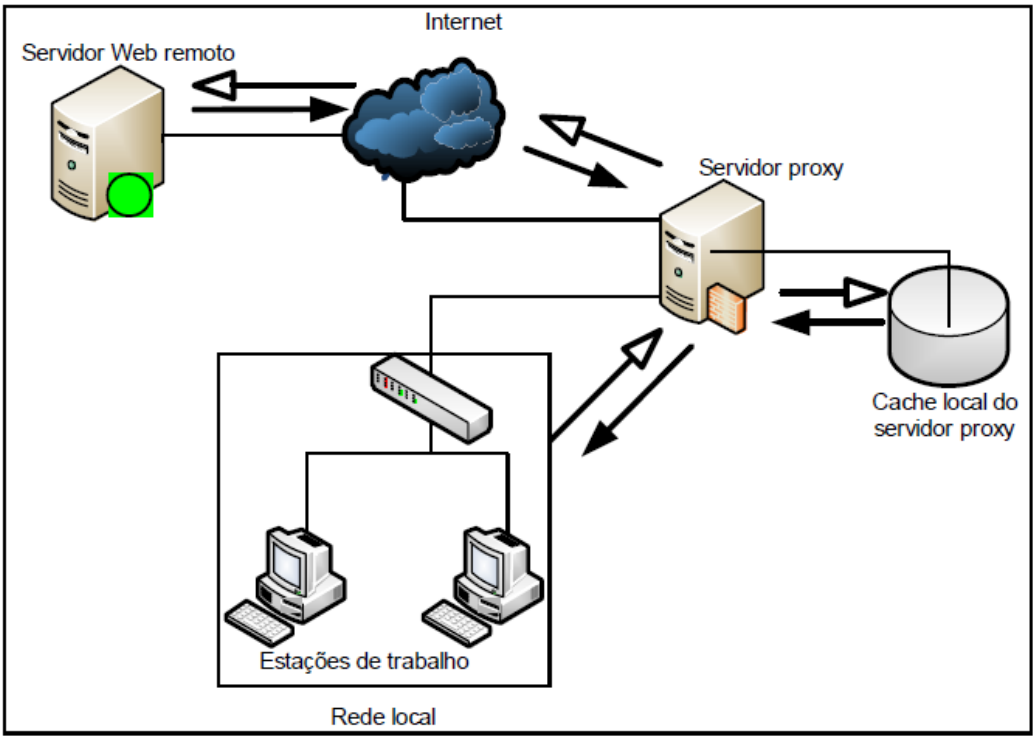

Figura 1: Exemplo de funcionamento de um servidor proxy.

Fonte: FOROUZAN, (2010.)

Um dos elementos mais importante de um servidor *proxy* é a sua cache, e claro os seus filtros de bloqueio ou liberação de sites, as *Access Control Lists (ACLs).*

2.5. Cache

Conforme Watanabe (2000), cache é onde os arquivos requisitados pelo servidor *proxy* são armazenados e repassados posteriormente para os clientes, que são as estações de trabalho da rede interna. Esse é um espaço que deve ser monitorado sempre, pois pode deixar um servidor inoperante, já que são arquivos armazenados em disco e caso falte espaço em disco, o servidor para de funcionar. Para que isso não aconteça é necessário determinar quando os objectos serão actualizados ou removidos da cache, sendo que alguns desses podem permanecer sem alteração por um tempo indeterminado e outros podem sofrer alterações frequentemente.

Visando o controlo da cache, os servidores *proxy* utilizam algoritmos de substituição que monitoram os objectos conforme seu cabeçalho, que contém a informação de período, tamanho e histórico de acessos. Dois deles são o *Least Recent Used (LRU),* que remove objectos existentes a muito tempo e o *Least Frequently Used (LFU),* que remove os objectos menos utilizados. A utilização do espaço em disco pela cache do *proxy* é controlada através desses algoritmos, juntamente com regras pré-determinadas pelo administrador.

Segundo Watanabe (2000), no caso de um objecto expirado, o servidor web original será consultado para revalidar o objecto. Quando o objecto tem em seu cabeçalho o campo *Last-Modified (LM),* indicando qual foi sua última alteração, o *proxy* pode usá-lo para fazer a requisição *If-Modified-Since (IMS)* ao servidor *web* remoto, fazendo a comparação da data da alteração, identificando se o objecto foi alterado ou não e poderá actualizá-lo, caso necessário, na sua cache.

Existem três tipos de cache, nomeadamente:

a) *Browse cache* – Conforme Watanabe (2000), a maioria dos navegadores de internet possuem uma cache próprio, pois é muito provável que os utilizadores acessem os mesmos objectos frequentemente e neste caso, a cache não é compartilhado;

b) *Proxy cache* – Conforme *Proxy* (2007), são as implementações mais utilizadas de *proxy*, e são conhecidos também como *caching web proxy*. Este disponibiliza em cache páginas e arquivos de servidores remotos da internet, permitindo que os

clientes da rede local acessem de forma rápida esses arquivos, considerando que a velocidade do *link* da LAN é muito maior do que da internet. Quando o *proxy cache* recebe uma solicitação de acesso a um recurso externo, como uma página da internet, este procura primeiramente na sua cache local e caso não encontre o recurso solicitado, ele imediatamente faz a requisição à internet armazenando na sua cache e responde a solicitação do cliente; e

c) *Transparent proxy cache* – Segundo Watanabe (2000), é utilizado especialmente por empresas provedoras de acesso à internet, conhecidas como internet *Service Provider* (ISP), porque permite o melhor aproveitamento de banda da internet e não necessita fazer nenhuma configuração nas estações clientes. É uma forma de obrigarem os clientes a utilizarem o *proxy*, ou seja, além das características do *proxy* cache, ele implementa de forma transparente as políticas de utilização e permite a colecta de dados estatísticos, entre outros.

2.6. Filtros do *proxy*

Segundo Marcelo (2005), além da cache, outra característica muito importante de um servidor *proxy* são os filtros que podem ser aplicados através de regras pré-determinadas pelo administrador. Dentre elas estão as restrições a *sites*, configuração ou não de autenticação dos utilizadores e controlos de acesso por horário e data. Os filtros, são conhecidos em geral como ACLs.

Os administradores podem criar os filtros dos mais simples aos mais complexos, contendo regras baseadas em diversos critérios, Watanabe (2000) destaca, os seguintes:

Endereço da estação de trabalho, domínio requisitado, rede de origem ou destino, localização do objecto requisitado, período de acesso á páginas da internet, habilitar ou não a autenticação.

Os filtros destacados acima podem ser implementados em conjunto ou sozinhos, porém as ACLs são analisados de forma sequencial. Por exemplo, se existir uma ACL com duas regras, a primeira bloqueando uma determinada página da internet e a segunda dando permissão para todas as páginas da internet, então a primeira regra não tem função alguma, pois a última regra invalidou a primeira.

2.7. *Access Control List* (ACL)

Em segurança informática (ACL), ou seja, Lista de Controlo de Acesso é uma lista sequencial de privilégios e permissões dos utilizadores sobre um determinado objecto ou recurso, ou seja, estabelece que utilizadores podem acessar os objectos, bem como quais as operações são permitidos.

Por exemplo, pode se ter uma ACL que contém Objecto 1 (Sujeito 1: leitura, escrita; Sujeito 2: leitura), isso significa que o sujeito 1 tem permissão de leitura e escrita enquanto que o sujeito 2 tem apenas permissão de leitura em relação ao objecto.

2.8. Tipos de *Proxy*

O *proxy* funciona em três modos: Convencional, Autenticado e em modo Transparente.

2.8.1. *Proxy* Convencional

Com o uso do *proxy* em modo convencional, é necessário configurar em cada máquina o navegador e todos os outros programas, que forem acessar a internet. Esta é uma tarefa que acaba gerando bastante trabalho, pois toda vez que um micro novo for colocado na rede ou for preciso reinstalar o sistema, será preciso fazer a configuração novamente. (MORIMOTO,2008). Em contrapartida, é nesse modelo que ele funciona em modo autenticado podendo ser uma alternativa a mais para segurança da instituição.

2.8.2. *Proxy* em Modo Autenticado

O modo autenticado fornece a rede de computadores uma camada a mais de segurança. A Figura 18, ilustra a sequência dos processos executados durante a tentativa de acesso a internet através de um *proxy* configurado para autenticar seus utilizadores. Primeiro, uma estação de trabalho cujo navegador *Web* tenha sido configurado para utilizar *web proxy* como meio de acesso a internet, terá que apresentar suas credenciais de acesso para obter o acesso desejado. O questionamento é feito geralmente através de um formulário no qual deve ser digitado o nome do utilizador e a respectiva senha. Vesperman (2001).

2.8.3. *Proxy* em Modo Transparente

É possível configurar o *Squid* e o *firewall* de forma que o servidor *proxy* fique escutando todas as conexões na porta 80. Mesmo que alguém tente desabilitá-lo manualmente nas configurações do navegador, ele continuará sendo usado (MORIMOTO, 2008). Nesse

modelo o utilizador muitas vezes nem sabe que ele está passando por um *proxy*. Todavia não será necessário visitar localmente as estações de trabalho para configurar seus navegadores *Web*, o que facilita bastante o trabalho do administrador da Rede. Todo acesso à internet será forçosamente obtido através do serviço de *proxy*. Para activar o suporte ao modo transparente é preciso incluir no início do arquivo *squid.conf*, para as versões 2.6 em diante, a linha http_port3128 transparent.
A configuração do *Squid* é feita através da edição do arquivo *squid.conf* e sua localização pode ser determinado no momento da instalação.

Com estas definições, ficou claro que o *proxy* tem em todos os modos o mesmo principio de funcionamento, sendo que a diferença está no facto de: No modo convencional, é preciso configurar manualmente o navegador e todos os programas que forem acessar a internet em cada dispositivo da rede, enquanto que no modo autenticado, será necessário autenticar- se sempre que for a internet (normalmente com nome do utilizador e senha), porém o navegador guarda as senhas para não ter que solicitar novamente sempre que for a acessar mesmos conteúdos e no modo transparente, as configurações são implementadas automaticamente.

2.9. Principais vantagens do uso de servidores *proxy*

Existem enumeras vantagens que incentivam o uso de servidores *proxy*, Watanabe (2000) destaca seguintes vantagens:

- ✓ **Redução do tráfego de rede** – São utilizadas menos requisições e respostas, sendo que o objecto da cache é recuperado, actualizado ou buscado do servidor uma única vez, o que reduz consideravelmente a utilização de banda por parte do cliente;

- ✓ **Redução da carga dos servidores** – São feitas menos requisições para os servidores web responderem. Por exemplo, diminui consideravelmente o congestionamento a esses servidores, quando há o lançamento de um novo produto;

- ✓ **Redução da latência** – Possibilita maior velocidade de resposta a requisições feitas ao objecto que está na cache do *proxy* e não directamente ao servidor remoto;

- ✓ **Possibilidade de acesso** – considerando que a página de internet solicitada está inacessível, se a página estiver como um objecto da cache, será possível responder a requisição, apenas não possibilitando a actualização da página solicitada.

2.10. Algumas desvantagens na utilização de servidores *proxy*

Como é sabido tudo tem algum ponto fraco, assim é também com servidores *proxy,* Marcelo (2005) destaca três principais desvantagens na implementação de servidores *proxy*:

- ✓ **Alguns serviços não suportados** – Nem todos os serviços têm suporte com os *proxies* actuais, sendo assim, a relação entre o cliente e o servidor *proxy* deve ser muito bem analisada;

- ✓ **Actualização de configurações em clientes** – Carga muito grande de modificações e/ou actualizações em clientes, principalmente em redes locais com grande número de equipamentos. Em ambientes mistos o problema pode ser maior;

- ✓ **Segurança em protocolos e aplicações** – O *proxy* não garante a segurança de um cliente para possíveis falhas de segurança em protocolos ou aplicações, sendo assim é necessário que o *proxy* seja implementado junto a um *firewall*.

2.11. Autenticação

Conforme Marcelo (2005), a autenticação do *Squid* só pode ser habilitada se o mesmo for configurado em modo *Proxy cache*. Caso seja configurado no modo *transparent Proxy cache,* a autenticação não é permitida com seus módulos padrão.
Vesperman (2001), afirma que existem vários módulos de autenticação padrão do *Squid,* a saber:

a) *Lightweigght Diretctory Access Protocol (LDAP)* – Módulo que permite a autenticação baseada na base de dados LDAP;

b) *Microsoft New Technology (MSNT)* – Módulo que permite a autenticação baseada em um controlador de domínio Windows NT;

c) *National Center for Supercomputing Applications (NCSA)* – Módulo que permite a autenticação baseada no tipo de arquivo *password* de muitos servidores *web* NCSA e segundo Marcelo (2005, p. 23) esse é o mais utilizado;

d) *Pluggable Authentication Modules (PAM)* – É um módulo de autenticação plugável e pode ser configurado para utilizar vários sistemas de autenticação;

e) *Server Message Block (SMB)* – Módulo que permite a autenticação baseado em um servidor SMB tipo *Microsoft* NT ou Samba;

f) *New Technology Lan Manager (NTLM)* – Módulo baseado em um protocolo de desafio / resposta, muito utilizado em ambientes *Microsoft*;

g) *Getpwnam* – Módulo baseado nos arquivos de senhas do GNU/Linux: o *password* e o *shadow*.

2.12. Controlo de acesso

Segundo Resende (2015), Controlo de acesso em segurança, especificamente em segurança física de ambientes, é a permissão do acesso a recursos, salas, prédios, entre outros, a somente pessoas autorizadas. O controlo físico de ambientes é feito por pessoas, meios tecnológicos, cartão de acesso, abertura de porta por meio de tranca electrônica e/ou liberado por senha, ou mecanismos de segurança como: Catracas, fechaduras, chaves, entre outros.

Campos (2006) refere que o controlo de acesso na segurança da informação é baseado em três processos, nomeadamente: Autenticação, autorização e contabilidade.

a) **Autenticação -** É o processo de identificação de quem pode acessar um determinado recurso, consiste em dois passos, que verificam a identidade de quem pretende acessar determinado sistema normalmente através do nome do utilizador e senha;

b) **Autorização** – Define o que o utilizador pode fazer, ou seja, estabelece os direitos e permissões. Este processo é executado após a autenticação do utilizador;

c) **Contabilidade** – Apresenta dados estatísticos de utilização dos recursos da rede e informa o que o utilizador fez. Siewert (2007), afirma que existem dois tipos de

contabilidade: A feita em tempo real e a em *batch*, sendo que, em tempo real, as informações são apresentadas no momento da utilização do recurso. Em *batch*, os dados são gravados e enviadas após o uso, normalmente num pré-determinado intervalo de tempo. As principais informações apresentadas na contabilidade são a identidade do utilizador, o recurso acessado e o tempo de utilização do referido recurso.

2.13. Mecanismos de controlo de acesso

Os mecanismos de controlo de acesso mais conhecidos são os baseados em identidade ou discricionários, os baseados em regras ou obrigatórios, e os baseados em papéis.

2.14. Discretionary Acces Control

Conforme Silva (2004), o *Discretionary Access Control (DAC)* é uma política de controlo de acesso baseada na permissão determinada pelo proprietário do recurso, por exemplo, um arquivo, o proprietário define quem tem acesso, qual a permissão e qual privilégio tem referente ao recurso. O Quadro 1 demonstra como são atribuídos os privilégios e as permissões dos sujeitos aos objectos.

	Objecto 1	**Objecto 2**
Sujeito 1	(read)	(read, write, Executive)
Sujeito 2	-	(read, write)
Sujeito 3	(write)	-

Tabela 1: Permissões e privilégios
Fonte: Autor

Os controlos discricionários podem ser utilizados através de duas técnicas:

a) Lista de controlo de acesso (ACL) – Que estabelece os privilégios e permissões dos utilizadores sobre um determinado objecto ou recurso;

b) Controlo de acesso baseado em papéis – Determina as permissões e privilégios com base no papel de determinado utilizador na organização. Esse método visa a simplificação da gestão de permissões e privilégios dados aos utilizadores.

Segundo Siewert (2007), as permissões de acesso e direitos sobre determinados objectos são dados para qualquer grupo ou indivíduo. Um indivíduo pode pertencer a um ou mais grupos e podem adquirir permissões cumulativas ou serem eliminadas algumas permissões, dos grupos que ele não pertence.

2.15. Mandatory Access Control

Mandatory Access Control (MAC) é um método que limita o acesso a informação em função da sensibilidade da mesma e identidade de quem pretende acessar. Segundo Silva (2004), afirma que, MAC implementa uma política obrigatória, ou seja, as regras de controlo de acesso são impostas por uma autoridade central, normalmente o administrador do sistema, que especifica regras de controlo de acesso para recursos e informações, garantindo que as mesmas sejam incontornáveis. Sendo assim esse mecanismo é bem mais complexo para implementar, pois utiliza política multinível e devido a sua rigidez com as regras de controlo e também com relação as limitações dos seus modelos.

2.16. Acess Control List

Conforme Marcelo (2005), a web *proxy* permite ou não a autenticação, o que vai possibilitar a implementação de perfis de acesso à i*nternet*, com bloqueio ou liberação de serviços. Já o *proxy* transparente, não permite que seja configurada a autenticação, somente com algum módulo ou sistema a mais que possibilite a autenticação. Para poder implementar esse tipo de controlo por utilizadores, é necessário a implementação de políticas de acesso, que são as populares ACLs.

Segundo Silva (2004), se for considerado uma coluna do Quadro 1, veremos que a relação de todos os sujeitos com seus respectivos direitos de acesso sobre um determinado objecto, correspondem a coluna, formando uma lista de controlo de acesso, ou uma ACL, do objecto considerado. As ACLs são uma forma de representação da matriz de acesso.

Objectos	**Lista de Controlo de Acesso**
Objecto 1	Sujeito 1 (read), Sujeito 2 (write, read), Sujeito 3 (write, read, execute)
Objecto 2	Sujeito 2 (read, execute), Sujeito 3 (write)
Objecto 3	Sujeito 3 (read, write, execute), Sujeito 1 (execute)

Tabela 2: Lista de controlo de acesso.
Fonte: Autor

CAPITULO III- APRESENTAÇÃO E DISCUSSÃO DE RESULTADOS

3.1. Situação actual da rede UP-NET

A Universidade Pedagógica de Maputo é uma instituição de ensino vocacional cuja missão estatutária é a formação superior de professores para todos níveis de ensino e de outros profissionais para área de educação e afins, a investigação e a extensão. Neste contexto, a UPM pugna pela universalização e regionalização, para além da sua função instrumental na produção e disseminação de conhecimento para a transformação da sociedade moçambicana rumo ao desenvolvimento social, cultural e tecnológico.

Neste capítulo são apresentadas técnicas e ferramentas utilizadas para a implementação e configuração do *firewall proxy* para a segurança de dados.

A UP-Net é uma rede não independente que suporta dados e voz, ou seja, esta plataforma tem um nó de dados e de voz.

Esta rede começou a ser construída em 2008, sendo que numa primeira fase tomou-se como prioridade a componente de dados, porque na altura o Centro de Informática da UPM não tinha equipamento de voz.

Segundo um dos administradores da rede UP-Net actualmente a UPM Campus de Lhanguene possui uma rede de computadores oferecendo diversos serviços como o acesso a internet e base de dados, contendo diversas informações de funcionários, estudantes e várias estações de trabalho que disponibilizam um conjunto de aplicações aos utentes.

Porém do estudo feito, verificou-se que, a rede UP-Net encontra-se desprovida de políticas de segurança tomando como base a figura que será apresentada e o trabalho desenvolvido após um levantamento de informações sobre a estrutura física e lógica da actual rede, é possível verificar a ausência de vários componentes que garantiriam a segurança da rede UP-Net.

Verifica-se que a rede UP-Net é desprovida de políticas de segurança sendo esta acessível para qualquer utilizador (Funcionários e estudantes).

O acesso a internet é efectuado sem restrições localmente definidas, estando apenas a mercê do provedor de serviços. Assim sendo, a UPM Campus de Lhanguene anos depois foram se criando melhorias na rede com o equipamento de voz e outros mas não se implementou mecanismos ou ferramentas para a segurança da informação.

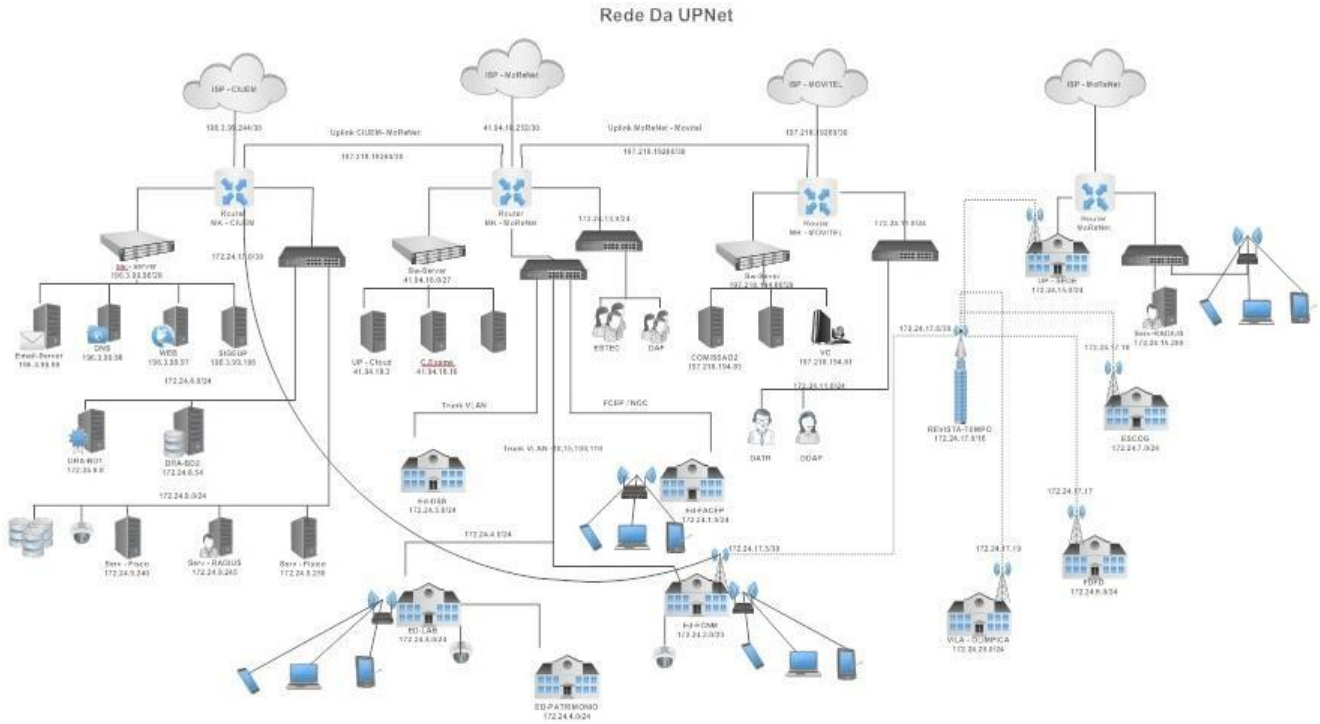

Figura 2: Rede UP-Net

Fonte: Bila, Xavier (2015)

A UPM, sendo uma instituição de ensino superior, tem-se empenhado na massificação do uso dos sistemas de informação como um recurso indispensável para alcançar seus objectivos que passam por oferecer serviços íntegros e confiáveis aos seus utentes, esta possui uma rede de computadores distribuída em todos os departamentos que a constituem, porém, o acesso à mesma encontra-se por hora limitada devido à degradação da infraestrutura de rede local. Sendo comum encontrar pontos de rede inutilizados, locais de trabalho sem acesso a rede, com a estrutura de cabos desfeita em vários departamentos inclusive nas salas e laboratórios de informática, tornando a disponibilidade da rede um requisito por hora insatisfeito.

Nesse contexto, existe a necessidade de uma revisão abrangente da infraestrutura da rede local da UPM Campus de Lhanguene de modo que a disponibilidade desta se torne um desejo alcançável. É de maior importância que todos os gabinetes de trabalho, salas de aulas, laboratórios, bibliotecas e outros locais de estudo individual ou em grupo beneficiem-se de acesso à rede de dados, seja pela rede cabeada ou pela rede sem fio de modo a garantir um acesso mais abrangente e eficiente aos recursos disponibilizados por esta. Por conseguinte, para garantir a operacionalização da rede, far-se-á necessário

incorporar mecanismos de segurança e de gestão integrais para que esta não seja alvo de um dispêndio sem benefícios a longo prazo.

Uma rede pode ser protegido do ponto de vista lógico (com a implementação de politicas de seguranças) ou físico (em termos de manutenção eléctrica, por exemplo). Além do mais, as ameaças podem vir de programas maliciosos que se instalam no computador do utilizador (como um vírus) ou chegar por via remota.

A segurança dos sistemas informáticos limita-se a garantir os direitos de acesso aos dados e recursos de um sistema implementando mecanismos de autenticação e controlo, que garantem que os utilizadores dos ditos recursos possuem unicamente os direitos que lhes foram concedidos. No entanto, os mecanismos de segurança implementados podem provocar embaraço a nível dos utilizadores e as instruções e regras tornarem-se cada vez mais complicadas à medida que a rede se estender. Assim, a segurança informática deve ser estudada de maneira a não impedir os utilizadores de desenvolver os usos necessários e fazer com que possam utilizar o sistema de informação com total confiança.

Esta é a razão pela qual é preciso definir, em primeiro lugar, uma política de segurança cuja implementação seja feita de acordo com as quatro seguintes etapas:

- Identificar as necessidades em termos de segurança, os riscos informáticos que pesam sobre a instituição e as suas eventuais consequências;
- Elaborar regras e procedimentos a serem implementados nos diferentes serviços da organização para os riscos identificados;
- Supervisionar e detectar as vulnerabilidades do sistema de informação e manter-se informado sobre as falhas nas aplicações e *hardwares* utilizados;
- Definir as acções a serem empreendidas e as pessoas a serem contactadas em caso de deteção de uma ameaça.

O servidor *proxy* surgiu da necessidade de intermediação da conexão entre a rede local (LAN) com a internet, garante navegação de uma forma anónima na internet através de um computador da rede que compartilha a sua conexão com as demais máquinas, Ou seja, considerando que a rede local é uma rede "interna" e a internet é uma rede "externa", pode-se dizer que o *proxy* permite que outras máquinas tenham acesso externo.

3.2. Situação final proposta

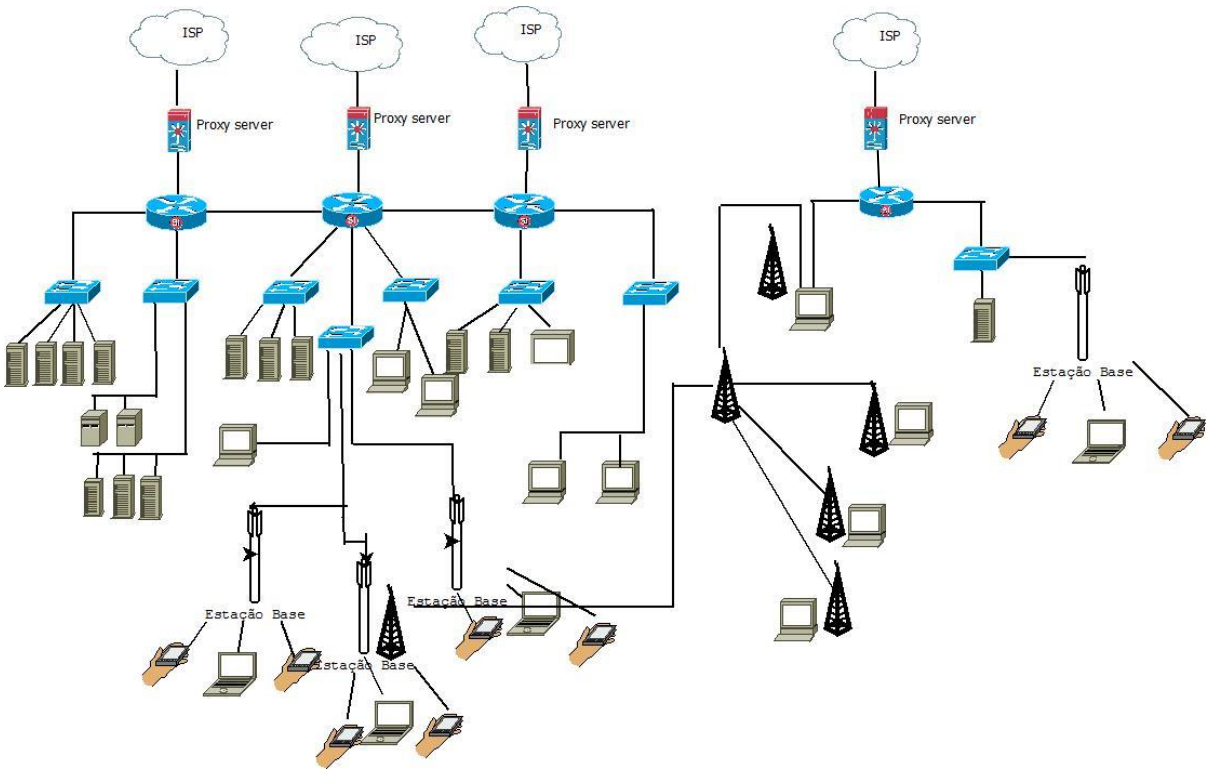

Figura 3: Implementação de um servidor *proxy* na rede UP-Net.

Fonte: Autor

A UPM Campus de Lhanguene como instituição de ensino debate se com uma necessidade de requalificação da sua rede informática, necessidade esta que passa pelo melhoramento da sua infraestrutura física nos diferentes níveis de acesso e distribuição de forma a garantir um acesso mais abrangente à sua comunidade de utilizadores que por sinal encontra-se em franco crescimento devido ao aumento de utilizadores móveis. Sob essa perspectiva, coube desenvolver uma proposta de segurança da rede UP-Net.

A UPM Campus de Lhanguene é uma instituição pública de ensino superior, sendo o seu maior negócio ministrar cursos de formação de professores e cursos técnicos a cidadãos moçambicanos e estrangeiros sendo o seu maior fornecedor o Governo de Moçambique dada a sua natureza pública.

Hoje em dia é necessário assegurar a boa utilização da internet através de soluções que permitam gerir com eficácia o seu uso em ambientes corporativos, impedindo o acesso por utilizadores, *sites* e serviços considerados inapropriados ou potencialmente perigosos para a instituição. Com o crescimento da tecnologia e a conectividade entre as instituições

através da internet, cada vez mais um administrador de sistemas deve se preocupar com as informações que estão dentro da sua rede.

A internet traz facilidades para comunicação e transmissão de informações entre empresas ou mesmo para uso pessoal, porém, existe a preocupação com vírus, roubo de informações, má utilização de recursos e outros tipos de incidentes de segurança.

Dessa forma, entende-se que o acesso à web é algo que necessita ser controlado, seja por questões de segurança ou de produtividade. Aos administradores, é designada a tarefa de implantar soluções com o objectivo de garantir a segurança da rede através de acções como: Bloqueio de acesso a *sites* inadequados, controlo de navegação dos utilizadores, cache (armazenamento) de páginas mais acessadas para optimizar o uso de recursos, bem como emitir relatórios de navegação para análise posterior. A função básica de um *proxy server* na rede é servir como um ponto intermediário entre a rede local e a internet, atuando na optimização da velocidade de acesso a conteúdos *web* através da cache, filtro de *sites* indesejados e controlo de acessos.

3.3. Segurança

Trata-se de um aspecto muito importante do projecto de uma rede de computadores, especialmente com conexões à i*nternet* e e*xtranet* dada a vulnerabilidade a qual se expõe. O objectivo básico desta precaução passa por garantir que problemas de segurança não afectem os negócios da instituição. Para tal, é preciso proceder com as seguintes questões:

- Planificação;
- Análise de riscos;
- Levantamento de requisitos.

3.3.1. Planificação

A planificação de aspectos de segurança é crucial para garantir a operacionalidade de uma rede a longo prazo, levando em conta que este processo inclui duas vertentes, a física e a lógica.

a) Vertente física

A segurança física de uma rede inclui a proteção de todo um conjunto de componentes constituintes desta. É de extrema importância o estabelecimento de um perímetro devidamente protegido para todos os equipamentos de rede. A segurança física num

ambiente de rede deve incluir: Estabelecimento de uma sala especializada (*Server farm)* para incorporação dos diferentes servidores de rede, *switches* de camada de distribuição, e dispositivos de acesso *WAN*. Sendo que este é um aspecto patente na instituição e com condições apropriadas para o efeito desde o ponto de vista de acesso a climatização da mesma. É importante realçar que a segurança física dum ambiente de rede estende se ainda a necessidade de incorporação de uma sala de *UPS's* capazes de garantir à alimentação dos componentes de rede prevenindo perdas de dados e danificação dos sistemas informáticos que possa ser causado por quedas de energia. Sob esse aspecto a rede não dispõe dessa capacidade na sua totalidade dado que apenas a sala de servidores e sala de *TIC's* possuem um conjunto de *UPS's* capazes de responder as necessidades dessas divisões.

b) Vertente lógica

A segurança lógica de uma rede de computadores constitui um aspecto crucial na administração da mesma, a falta de políticas claras de segurança pode comprometer a disponibilidade da rede e, até no nível mais crítico do negócio da instituição. Havendo necessidade de garantir o sigilo de informações sensíveis e garantir a privacidade dos utentes da rede, prover parâmetros de conduta para utilizadores da rede. Contudo, a UPM Campus de Lhanguene até o exacto momento encontra se desprovida de mecanismos de segurança próprios. Aspectos como proteção de perímetro, proteção de acesso interno e externo, são de grande relevância neste projecto.

3.3.2. Análise de riscos

Para implementar a segurança de um *site* ou grupo de utilizadores, deve-se investigar os riscos de não implementar a segurança fazendo a seguinte análise: Qual é a sensibilidade dos dados disponibilizados pela instituição e quais são os efeitos de roubo ou alteração dos mesmos na medida em que as empresas se preocupam principalmente com os seguintes três aspectos da segurança:

- Vírus;
- Problemas causados por erros de utilizadores;
- Problemas causados pelos utilizadores internos maliciosos.

3.3.3. Requisitos de segurança

Os requisitos de segurança são identificados através de uma avaliação sistemática dos riscos de segurança. Os recursos que devem ser protegidos são:

- Hospedeiros, incluindo servidores;
- Dispositivos de interconexão (*switches*, roteadores, pontos de acesso);
- Dados de sistemas ou de aplicações;
- A imagem da instituição.

Convém que o administrador estabeleça uma política clara e demonstre apoio e comprometimento com a segurança da informação através da emissão e manutenção de uma política de segurança da informação para toda a instituição. Os requisitos devem atingir os seguintes objectivos:

- Permitir que pessoas externas tenham acesso apenas a dados públicos (via *http*, *https* e *ftp*), e nunca a dados internos;
- Identificar, autenticar e autorizar utilizadores da organização, utilizadores móveis e funcionários que eventualmente trabalhem remotamente;
- Detectar intrusos e identificar os danos causados por estes;
- Proteger *hosts* e dispositivos fisicamente;
- Proteger *hosts* e dispositivos logicamente através de senhas e direitos de uso;
- Proteger aplicações e dados contra vírus;
- Prover cópias de segurança;
- Treinar utilizadores sobre as políticas de segurança da instituição e sobre formas de evitar problemas de segurança.

A segurança num ambiente compartilhado, no caso a rede da UPM Campus de Lhanguene é cada vez mais importante devido a:

- Conexão para *internet;*
- A formação de uma intranet;
- Uso da rede corporativa por utilizadores móveis e funcionários que trabalham remotamente.

3.3.4. As etapas que compõem um projecto da segurança são:

a) Identificação dos recursos da rede;
b) Análise de riscos (implicações) de segurança;
c) Elaboração de um plano de segurança;
d) Elaboração de políticas de segurança;
e) Elaboração de procedimentos para aplicação e implementação das políticas de segurança;
f) Manutenção da segurança através de auditorias periódicas.

3.3.5. Identificação de recursos de rede e análise de riscos

Para implementar a segurança de um *site* ou grupo de utilizadores, deve-se investigar os riscos de não implementar a segurança. Feita essa análise, verificou-se que:
A UPM Campus de Lhanguene possui um servidor de base de dados contendo um conjunto de informações referentes aos funcionários da instituição e dos estudantes da mesma, sendo que estas requerem um nível de proteção maior, dado que sua alteração, ou roubo pode resultar na anulação de nível de certo estudante, por exemplo.
Entretanto, são recursos a proteger: As bases de dados da instituição, os dispositivos de interconexão, os sistemas operativos e máquinas hospedeiras.

3.3.6. Análise de implicações de segurança

O custo da proteção contra uma ameaça deve ser menor do que recuperar-se da concretização desta, portanto, a segurança como qualquer outro requisito possui implicações que devem ser tomadas em conta:

- **Custo** - Maior complexidade pode exigir custos de manutenção maiores;
- **Usabilidade** - Mecanismos complexos dificultam o utilizador final;
- **Disponibilidade** - Pode originar um ponto único de falha no *firewall*;
- **Gerenciabilidade** - Existe a necessidade de manter o histórico de *logins*, senhas, e nomes de utilizadores e posteriormente fazer uma auditoria de segurança. Portanto a perda ou aquisição ilegal destas pode abrir maiores brechas de segurança.

3.4. Desenvolvimento de um plano de segurança

Um plano de segurança é um conjunto de especificações a serem feitas de modo a cumprir requisitos de segurança, especificando o tempo, as pessoas e outros recursos necessários para desenvolver e implementar as políticas de segurança.
O plano faz referência à topologia da rede e determina quais serviços serão providos, especificando os provedores de serviços, pessoas com direitos de acesso, forma de acesso e os administradores da rede.
Como resposta a estas especificações, importa referir que a UPM Campus de Lhanguene oferece serviços de acesso *web*, a princípio para todos os estudantes e funcionários da instituição, sendo que com a implementação deste projecto, o acesso a este recurso será mediante uma conta de acesso assim como para outros serviços disponibilizados pela rede.
É importante que todos os envolvidos se sintam comprometidos com o plano de segurança.

3.5. Desenvolvimento de políticas de segurança

Uma política de segurança específica, formalmente são as regras que devem ser seguidas pelas pessoas que irão aceder os recursos da UPM Campus de Lhanguene, as obrigações das pessoas (utilizadores, e equipa técnica) para manter a segurança passam pelo cumprimento das componentes que abaixo se descrevem.

- **Uma política de acesso**

a) Todos os estudantes, funcionários, técnicos de redes e dirigentes têm direito de acesso a rede mediante uma senha provida pelo administrador de rede;

b) Todos com acesso a rede excepto os administradores de redes devem ter acesso aos recursos da rede de segunda a sexta no horário compreendido entre as 7:00h e 22:00h, e aos sábados das 7:00h as 18:00h;

c) O acesso à sala de servidores, concedido apenas aos técnicos de redes, da manutenção e de outros trabalhos de rotina mediante a presença de um agente do departamento de TIC;

d) Só os técnicos de redes é que podem efectuar uma sessão de acesso remoto;

e) Todos utentes a excepção dos agentes do departamento de TIC possuem uma conta de *login* de domínio e não local, tal conta é válida para utilização conjunta das redes *Ethernet* e *wireless;*

f) A conexão a dispositivos de rede é concedida apenas a equipa das TIC;

g) A incorporação de um novo *software* nas estações de trabalho é concedida apenas ao pessoal de TIC sendo que para as salas públicas como as de informática, o processo será encarregue ao responsável pela sala em questão;

h) Restringir o acesso à páginas por conteúdo;

- **Uma política de responsabilidade**

a) Os utilizadores são responsáveis pela gestão dos seus próprios conteúdos, sendo estes de acesso exclusivo;

b) Todos os utilizadores de rede são responsáveis pela alteração das suas chaves de acesso e nunca de conta de acesso;

c) O sistema deve gerar *logs* de auditoria para avaliar situações de risco.

- **Uma política de autenticação**

a) A política de autenticação estabelece a existência de uma única sessão para cada conta criada;

b) Os utilizadores da rede sem fio poderão aceder qualquer ponto de acesso ligado à rede bastando prover as mesmas credenciais designadas a este para a rede fixa.

3.6. Mecanismos de segurança

Os mecanismos de segurança levados em conta neste projecto dependem do nível de segurança exigido pela UPM Campus de Lhanguene de acordo com o nível de sensibilidade de informações disponibilizadas por esta, caso de informações mantidas no registo académico, é de grande importância que estas sejam íntegras e seguras.

i. Autenticação

Mecanismo normal: Nome de *login* e senha, usadas durante a sessão de *login*, sendo que todas as estações de trabalho poderão pedir a emissão da senha em casos de mais de 10 minutos de inactividade; (Figura 18)

ii. Autorização

Baseada em permissões de acesso usando ACL's para conexões a *internet*. (Figura 19 e 20);

Baseada em políticas de grupos para acesso local, usando grupos de utilizadores do AD;

A escolha da solução de segurança passa por identificar meios que permitam usar os mecanismos acima numa solução de segurança, havendo necessidade de definir mecanismos de segurança para diferentes tipos de acções, tais como: Conexão com a *internet*, acesso sem fio, serviço de rede e serviços do utilizador.

A inclusão de um servidor *proxy* permite controlar o acesso dos utentes ao exterior, criando um conjunto de ACL's que estabelecem a conduta de navegação pela *web*. Trata-se de um sistema (*Squid*) que roda em plataformas *Unix*, apesar disso, este pode interagir com o AD permitindo autenticações baseadas nas contas de utilizador do AD.

Proxies são soluções que permitem ganho de desempenho e economia da largura de banda implementando um sistema de cache no acesso a sites, armazenando localmente o conteúdo requisitado de forma que, em uma segunda requisição, não precise buscar novamente na internet. Além disso, também é possível trabalhar com alguns filtros de origem e destino, permitindo um controlo na navegação *web*, bem como bloqueio de conteúdos indesejados.

3.7. Controlo de Acesso ou Bloqueio

Assim como no caso dos servidores SMTP, *softwares* que fazem *proxy* de *Web* (tais como *Squid, Wingate e Microsoft Proxy Server*) também podem ser abusados se não forem tomadas as devidas precauções. Um *proxy* mal configurado pode ser usado por utilizadores externos como um "trampolim" para acessar recursos de forma anônima. Esta anonimidade pode ser usada para cometer crimes, tais como envio de mensagens caluniosas, difamatórias ou ameaçadoras e divulgação de pornografia envolvendo estudantes. A configuração correcta para um *proxy Web* é aquela que libera o acesso somente aos endereços IP de utilizadores autorizados (pertencentes à sua rede).

3.8. Logs

Logs são muito importantes para a administração segura de sistemas, pois registam informações sobre o seu funcionamento e sobre eventos por eles detectados. Muitas vezes, os *logs* são o único recurso que um administrador possui para descobrir as causas de um problema ou comportamento anómalo.

3.8.1. Gestão de Logs

Para que os *logs* de um sistema sejam úteis para um administrador, eles devem estar com o horário sincronizado via NTP, ser tão detalhados quanto possível, sem no entanto gerar dados em excesso. Informações especialmente úteis são aquelas relacionadas a eventos de rede, tais como conexões externas e registos de utilização de serviços (arquivos transferidos via FTP, acessos a páginas Web, tentativas de *login* sem sucesso, avisos de disco cheio, etc.), para registar estas informações, é necessário configurar o sistema da maneira apropriada. A forma de fazer isto geralmente varia para cada componente específico.

3.8.2. Armazenamento de *Logs*

3.8.2.1. Armazenamento *online*

Os *logs* são tradicionalmente armazenados em disco, no próprio sistema onde são gerados. Essa é a opção mais óbvia, mas ela possui alguns riscos inerentes que devem ser compreendidos.

O primeiro deles diz respeito à possibilidade dos *logs* serem destruídos durante uma invasão do sistema (uma ocorrência bastante comum). Em alguns sistemas, isso pode ser contornado através da instalação de um *loghost* centralizado.

Um segundo risco é a possibilidade de um atacante usar o *logging* para executar um ataque de negação de serviço contra um determinado sistema, gerando eventos em excesso até que o disco onde são armazenados os *logs* fique cheio e o sistema trave em consequência disto. O uso de uma partição separada para armazenar os *logs* pode minimizar o impacto deste problema.

Outro ponto que merece atenção é a rotação automática de *logs*. Quando este recurso é utilizado, deve-se garantir que os *logs* sejam movidos para o armazenamento *offline* antes que eles sejam removidos do sistema pela rotação, evitando assim a perda de registros. Alguns sistemas trazem a rotação automática habilitada na sua configuração padrão. Ao instalar um destes sistemas, verifique se esta configuração é compatível com os seus procedimentos de *backup* e armazenamento *offline* de *logs*.

3.8.2.2. Armazenamento offline

Evidentemente, os *logs* não podem ser mantidos *online* por tempo indeterminado, pois acabam por consumir muito espaço em disco. A melhor estratégia para resolver esta questão é transferir periodicamente os *logs* do disco para dispositivos de armazenamento *offline*, tais como fita, CD-R ou DVD-R.
Os *logs* armazenados *offline* devem ser mantidos por um certo período de tempo, pois podem vir a ser necessários para ajudar na investigação de incidentes de segurança descobertos posteriormente.

3.8.3. Monitoramento de Logs

Os *logs* possibilitam o acompanhamento do que acontece com a rede e seus sistemas. Portanto, é importante que eles sejam monitorados com frequência para permitir que eventuais problemas sejam rapidamente identificados.
Existem algumas práticas recomendáveis no que diz respeito ao monitoramento de *logs*:

- Incorporar o hábito de inspecionar os *logs* à sua rotina de trabalho, pelo menos uma vez por dia, tendo em mente que sistemas muito importantes ou que geram muita informação podem precisar ter seus *logs* analisados com maior frequência;
- Investigar as causas de qualquer registo que lhe pareça incorrecto ou anômalo, por mais insignificante que ele aparente ser;
- Identificar o padrão de comportamento normal do sistema, para poder encontrar eventuais anomalias com maior rapidez.

Ao analisar *logs*, deve certificar-se do *timezone* usado para registar o horário dos eventos, por exemplo, alguns *softwares* (como o *Microsoft* IIS, dependendo da configuração adoptada) registam eventos com a hora de Greenwich (GMT), e não com a hora local. O desconhecimento do *timezone* em que estão os *logs* pode facilmente invalidar uma análise e levar a conclusões equivocadas.

À medida que se adquiri prática com a análise dos *logs*, poderá escrever *scripts* ou pequenos programas para auxiliar nesta tarefa, automatizando assim parte do processo. Estes *scripts* são úteis, por exemplo, para pré-processar os *logs* em busca de determinados conteúdos, para eliminar conteúdo repetitivo e para elaborar um resumo que pode ser enviado por correio electrónico para o administrador do sistema. A eliminação de padrões relacionados a eventos considerados normais pelo administrador é especialmente importante porque, além de reduzir o volume de *logs* a serem analisados, pode evidenciar alguma actividade incomum.

Uma outra opção é utilizar ferramentas que permitam monitorar *logs* em tempo real, como por exemplo o *swatch*. O *swatch* requer que seja especificado um conjunto de padrões a serem monitorados e as acções a serem tomadas quando um destes padrões é registado nos *logs*. As acções podem ser de diversos tipos, como exibir a informação registada, notificar um determinado utilizador por correio electrónico e invocar um programa do sistema. A capacidade de execução de comandos arbitrários do *swatch* torna-o muito atraente, pois permite, por exemplo, que sejam tomadas medidas como filtragem de um endereço IP que gere determinado log e envio de uma mensagem de alerta para um telefone celular.

3.9. Filtragem de pacotes

Existem basicamente dois critérios de filtragem que podem ser empregues em *firewalls*. O primeiro é o de *default deny*, ou seja, todo o tráfego que não for explicitamente permitido é bloqueado. O segundo, *default allow*, é o contrário, ou seja, todo o tráfego que não for explicitamente proibido é liberado.

A configuração dos *firewalls* deve seguir a política de segurança da rede. Se a política permitir, é recomendável adoptar uma postura de *default deny*. Esta abordagem é, geralmente, mais segura, pois requer uma intervenção explícita do administrador para liberar o tráfego desejado, o que minimiza o impacto de eventuais erros de configuração na segurança da rede. Além disso, ela tende a simplificar a configuração dos *firewalls*.

No perímetro da rede, pelo menos as seguintes categorias de tráfego devem ser filtradas:

- Tráfego de entrada (*ingress filtering*): Pacotes com endereço de origem pertencente a uma rede reservada ou a um dos blocos de endereços da sua rede interna;
- Tráfego de saída (*egress filtering*): Pacotes com endereços de origem pertencente a uma rede reservada ou que não faça parte de um dos blocos de endereços da rede interna.

Diversas arquiteturas podem ser empregues para a implantação de *firewalls* em uma rede. A opção por uma delas obedece a uma série de factores, incluindo a estrutura lógica da rede a ser protegida, custo, funcionalidades pretendidas e requisitos tecnológicos dos *firewalls*.

Esta secção apresenta duas destas arquiteturas. A intenção não é cobrir todas as possibilidades de uso de *firewalls* mas fornecer exemplos de arquiteturas que funcionam e que podem eventualmente ser adoptados (na sua forma original ou após passarem por adaptações) em situações reais.

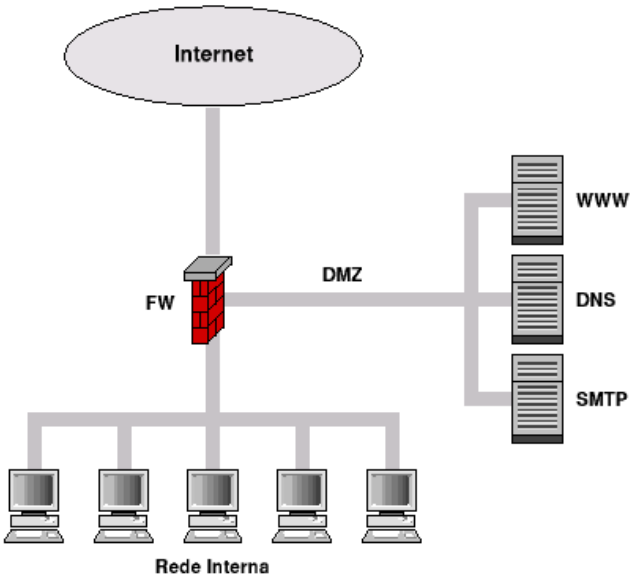

Figura 4: Exemplo de Rede em default deny.
Fonte: BEHROUZ A. FOROUZAN, (2010).

A figura ilustra um exemplo simples de uso de *firewall*. Neste exemplo, o *firewall* possui três interfaces de rede: uma para a rede externa, uma para a rede interna e outra para a DMZ. Por default, este *firewall* bloqueia tudo o que não for explicitamente permitido

(*default deny*). Além disso, o *firewall* usado é do tipo *stateful*, que gera dinamicamente regras que permitam a entrada de respostas das conexões iniciadas na rede interna; portanto, não é preciso incluir na configuração do *firewall* regras de entrada para estas respostas.

O tráfego liberado no exemplo da figura é o seguinte:

- Interface externa:
  - Saída: Tudo com exceção de:
    - Pacotes com endereços de origem pertencentes a redes reservadas;
    - Pacotes com endereços de origem não pertencentes a blocos da rede interna.
  - Entrada: Apenas os pacotes que obedecem às seguintes combinações de protocolo, endereço e porta de destino:
    - 25/TCP para o servidor SMTP;
    - 53/TCP e 53/UDP para o servidor DNS;
- Interface interna:
  - Saída: tudo;
  - Entrada: nada;
- Interface da DMZ:
  - Saída: Portas 25/TCP (SMTP), 53/UDP e 53/TCP (DNS) e 113 (IDENT);
  - Entrada: Além das mesmas regras de entrada da interface externa, também é permitido o tráfego para todos os servidores com porta de destino 22/TCP (SSH) e endereço de origem na rede interna.

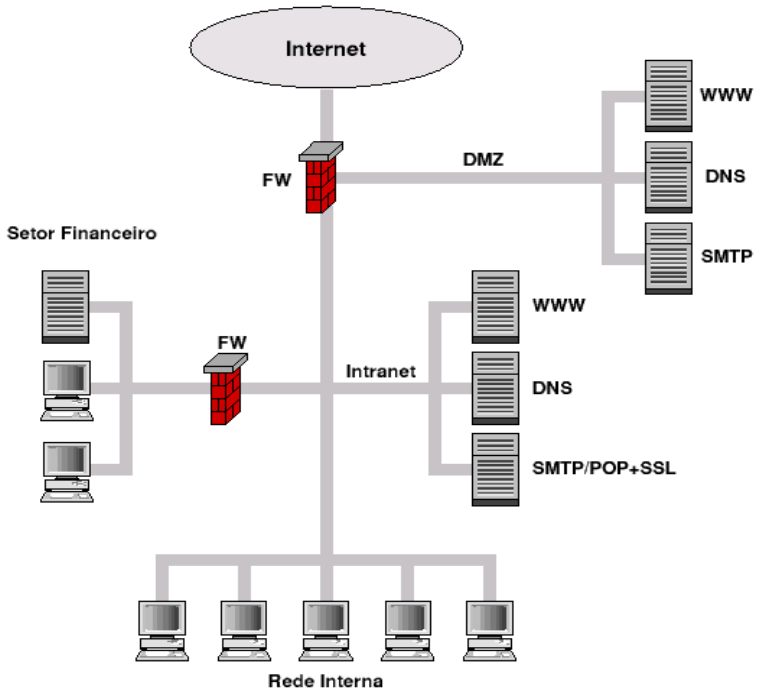

Figura 5: Exemplo de Rede em default allow

Fonte: BEHROUZ A. FOROUZAN, (2010).

A figura ilustra o uso de *firewalls* em uma situação mais complexa do que a anterior. Neste segundo exemplo, além dos servidores externos na DMZ, há também servidores na intranet e no sector financeiro da organização. Devido à importância das informações mantidas neste sector, a sua rede conta com a proteção adicional de um *firewall* interno, cujo objectivo principal é evitar que utilizadores com acesso à rede interna da organização (mas não à rede do sector financeiro) possam comprometer a integridade e/ou o sigilo dessas informações.

A configuração do *firewall* externo neste segundo exemplo é quase idêntica ao primeiro. Entretanto, no presente caso supõe-se que o servidor SMTP visível externamente (o da DMZ) repassa as mensagens recebidas para o servidor SMTP da intranet. Para que isso seja possível, é necessário mudar a regra de filtragem para a interface interna, liberando o tráfego do servidor SMTP da DMZ para a porta 25/TCP do servidor SMTP da intranet.

A configuração do *firewall* interno, por sua vez, é bastante simples. O servidor da rede do sector financeiro permite apenas acesso via HTTPS para que os funcionários da organização possam consultar seus contra cheques. Outros tipos de acesso não são permitidos. O tráfego liberado por este *firewall* é o seguinte:

- Interface externa (rede interna):
    - Saída: Tudo;
    - Entrada: Apenas pacotes para o servidor do setor financeiro com porta de destino 443/TCP (HTTPS) e endereço de origem na rede interna;

- Interface interna (rede do setor financeiro):
    - saída: Tudo;
    - entrada: Tudo (a filtragem é feita na interface externa).

3.10. Vantagens de Implementação de um Servidor proxy

A implementação de um Servidor Proxy na rede UP-Net (Rede da Universidade Pedagógica de Maputo – Campos de Lhanguene) trará inúmeros benefícios, para além das vantagens de servidores *proxy* descritas no ponto 2.9, pode se destacar:

- ✓ Redução de riscos de ataques e invasão por piratas informáticos;
- ✓ Maior privacidade, pois não há conexão directa entre o computador da rede interna e o servidor web;
- ✓ Optimização do acesso a conteúdos da *web*;
- ✓ Filtragem de *sites* com conteúdos indesejados, controlo e proteção de acessos interno e externo;
- ✓ Acesso a rede mediante autenticação;
- ✓ Redução da sobrecarga da rede;
- ✓ Aumento da velocidade de conexão;
- ✓ Diminuição da quantidade de *downloads*.

CONCLUSÃO E RECOMENDAÇÕES

4.1. Conclusão

Durante a execução do presente trabalho foi possível concluir que a segurança da informação é indispensável para qualquer instituição que possui uma rede de computadores, nesse contexto baseando-se nos testes efctuados verificou-se que a implementação do servidor *proxy* poderá resolver de forma satisfatória o problema de segurança da informação na rede da UPM Campus de Lhanguene.

Com a implementação do servidor *proxy* pode se tornar possível o controlo de acesso a internet e minimizar o consumo da largura de banda, possibilidade de geração de relatórios periódicos. Melhoramento considerável da velocidade da internet para utilizadores devido ao armazenamento interno das páginas *web* consultados com frequência.

O aumento da demanda do uso da internet, impulsionado pelos mais diversos usos, como utilizadores finais, instituições de ensino e de pesquisa, órgãos públicos e governamentais entre outros, tem deixado o acesso à internet insatisfatório e lento, devido as altas latências e tempos de resposta. Em vista deste cenário, a utilização de servidores *proxy* e cache, é uma das soluções e melhor alternativa para minimizar o problema.

À partir do desenvolvimento deste trabalho, com a proposta de implementação de servidor *proxy*, na rede UP-Net da UPM Campus de Lhanguene, observou-se que o recurso que realiza cache de conteúdos da Web, conhecido como cache *web*, disponibilizado pelo *proxy* é realmente muito útil, obteve-se resultados positivos no estudo prático realizado neste trabalho, pois reduz a utilização da largura de banda da internet, o tempo necessário para realizar *download* de arquivos, além de permitir, com recursos adicionais, o controlo de acesso a determinadas páginas e conteúdos considerados inapropriados para certos horários de expedientes e no ambiente acadêmico para o período de aulas, e outras em ocasiões para negar o acesso a sites com conteúdos impróprios.

Concluindo, como proposta de trabalhos futuros, sugere-se implementação do *Proxy* em um ambiente real, com a utilização de computadores físicos, pois os valores obtidos, o desempenho e a performance em âmbito geral seriam melhor mensurados e aproveitados.

4.2. Recomendações

Dito tudo isso, é muito importante lembrar que o comportamento dos utilizadores é um dos grandes responsáveis pela segurança ou pela insegurança dos dados corporativos, Ou seja, além de ter um bom *firewall* para registar e controlar o uso da internet pelos colaboradores, é importante prepará-los para detectar quando há ameaças (tentativas de *publishing* no *e-mail*, por exemplo). Não acessar sites ou baixar conteúdos de proveniência duvidosa, etc. A política de segurança na rede UP-Net deve ser clara e os utilizadores devem ser engajados na luta diária contra a vulnerabilidade dos dados.

Recomenda-se a UPM Campus de Lhanguene para implementar esta solução pois traz consigo uma vantagem no que se refere aquilo que virá a ser no processo da segurança da informação na rede UP-Net.

5. REFERÊNCIAS BIBLIOGRÁFICAS

- ALECRIM, Emerson. *Firewall:* Conceitos e Tipos. 2004. Disponível em: <http://www.infowester.com/firewall.php>. Acesso em: 12 nov. 2021;
- AWICHY, Elizabeth; CHAPMAN, D. Brent. *Building Internet Firewalls*. *O'Relly & Associates*, Inc. 1995;
- BEHROUZ A. FOROUZAN, Comunicação de dados em Redes de Computadores. 2010;
- BILA, Xavier. Trabalho de conclusão de curso, Universidade Pedagógica. Maputo. 2015;
- BROSTOFF, S. *Improving password system security efectiveness*. Tese de Doutorado. *University College London*. 2004;
- CHESWICK, William R.; BELLOVIN, S (EspaçoReservado1)teven M.; RUBIN, Aviel D. *Firewalls and Internet Security; Repelling the Wily Hacker.* Addison-Wesley, Reading, MA, 2ª ed., 2003;
- Comissão de Revisão Curricular Central. Normas para Produção e Publicação de Trabalhos Científicos na Universidade Pedagógica. Maputo. 2009
- LAKATOS, Eva Maria e MARCONI, Maria de Andrade. Metodologia do Trabalho Científico. Editora Atlas, São Paulo, 1999;
- MARCELO, Rocha Oliveira. Direito de trabalho e internet. São Paulo. 2005;
- MARIMOTO, Carlos Eduardo. [*Hardware:* Manual completo]. Cabo Coaxial. 2008
- MORRIS, R & THOMPSON, K. *Password security: a case of history. Communications of the ACM.* 1979;
- PÉRICAS, F. A. Redes de computadores*:* conceitos e a arquitetura Internet. Blumenau: Edifurb, 2003.
- RESENDE, Hendrikus Francisco e STELLA, Wagner Correa de Oliveira, Proxy Transparente Aplicado em um Ambiente Institucional – Trabalho de Conclusão do Curso, Ponta Grassa, 2015.

- RICHARDSON, Roberto Jarry. Pesquisa Social: Métodos e Técnicas. 2ed. Atlas, São Paulo.1999;
- SAUVÉ, J. P. Gerência de redes de computadores. [Campina Grande]: Departamento de Sistemas e computação da Universidade Federal de Campina Grande – Paraíba, 2002;
- SIEWERT, Vanderson Clayton, Ferramenta web para Administração do Srervidor Proxy Squid, Blumenau, 2007;
- SIEBERG, D. *Hackers shift focus to financial gain*. 2005;
- SILVA, Edna, MUSZKAT, Estera. Metodologia da Pesquisa e Elaboração de Dissertação - Programa de Pós-Graduação em Engenharia de Produção. 4ed. ver e act. Florianópolis, Brazil, UFSC Editora, 2004.
- SMITH, R. E. *The strong password dilema. Authentication: From Passwords to public keys;*
- TRIPP, David. Pesquisa-acção: uma introdução metodológica*. Disponível em: <http://www.scielo.br/pdf/ep/v31n3/a09v31n3>. Acesso mm: 16 de Agosto 2021.)
- UNIVERSIDADE PEDAGOGICA. *Regulamento Académico para os cursos de Graduação e Pós-graduação*. Maputo, 2016;
- WATANABE, R. et all. *Journal Article Reseach Support,* USA, 2000;

Websites

- http://www.netacad.com - Cisco Networking Academy.
- http://www.dsc.ufcg.edu.br/~jacques/cursos/2002.1/gr/>. Acesso em: 16 Nov.2021.

Apêndices

Figuras ilustrativas das configurações e testes na Rede

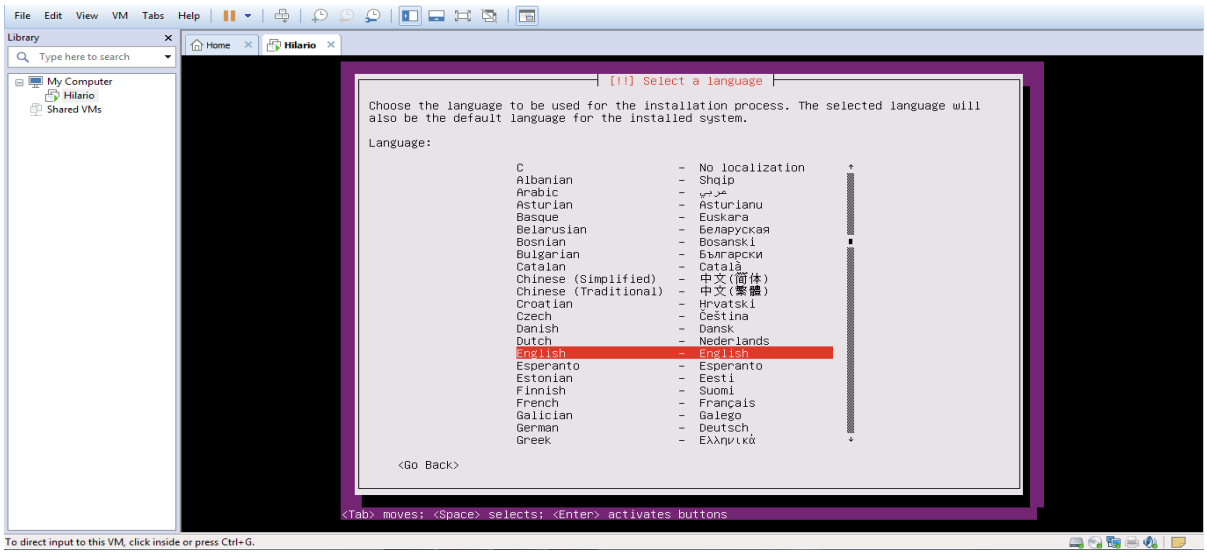

Figura 6: Escolha do idioma que permanecerá no sistema.
Fonte: Autor

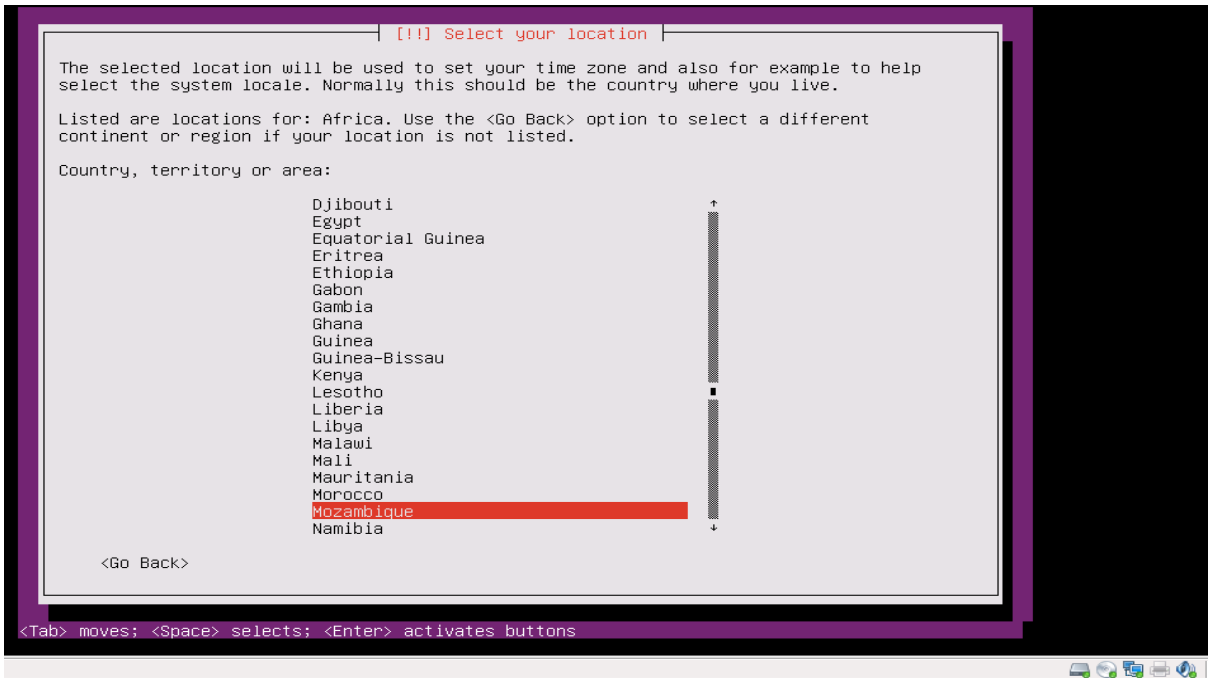

Figura 7: Escolha da área geográfica / país.
Fonte: Autor

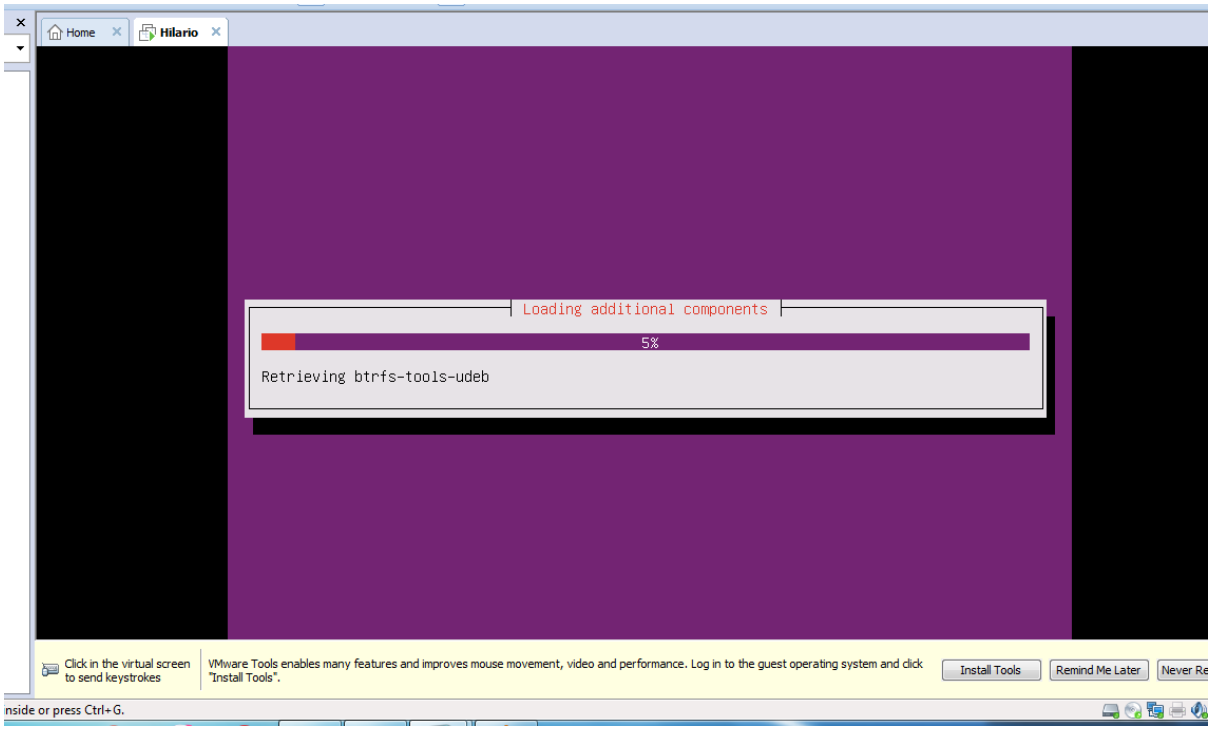

Figura 8: Detectando componentes adicionais
Fonte: Autor

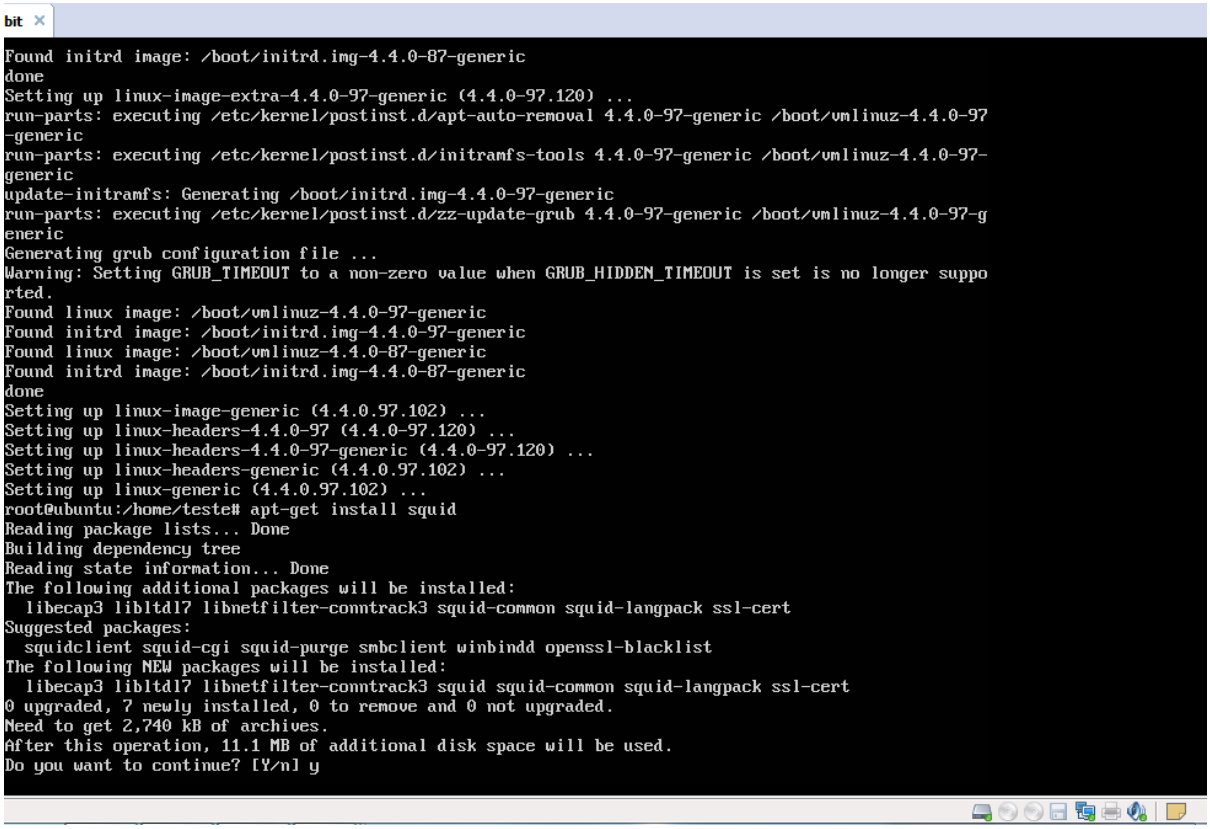

Figura 9: Instalação do pacote squid3.
Fonte: Autor

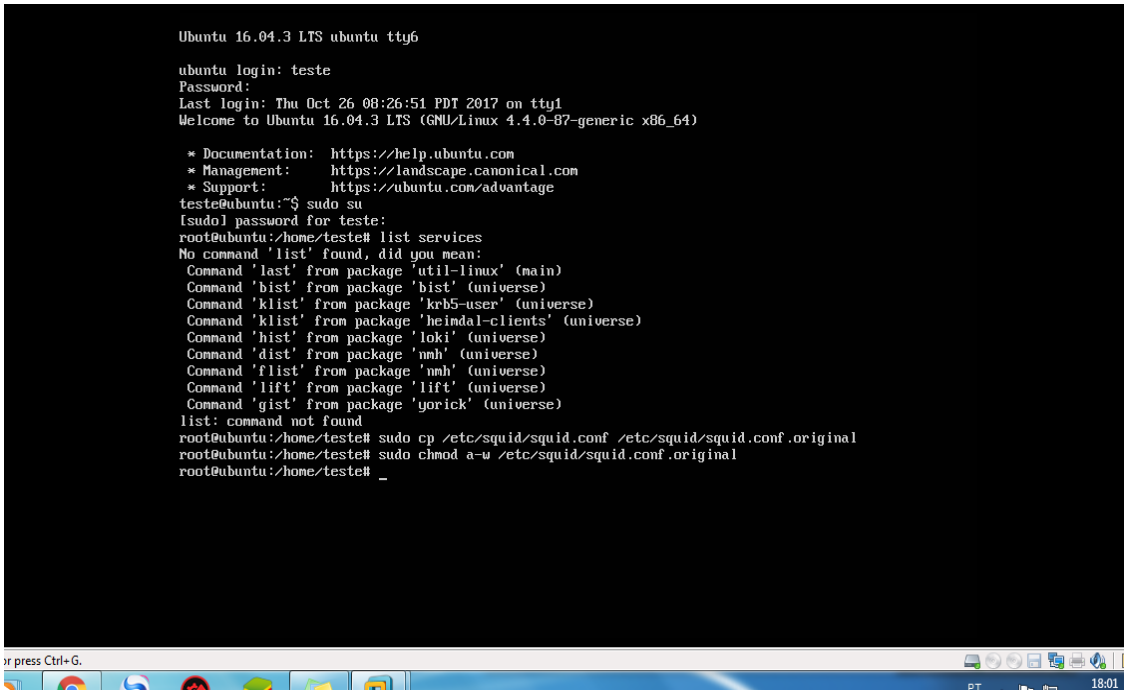

Figura 10: Descrição do sistema.
Fonte: Autor

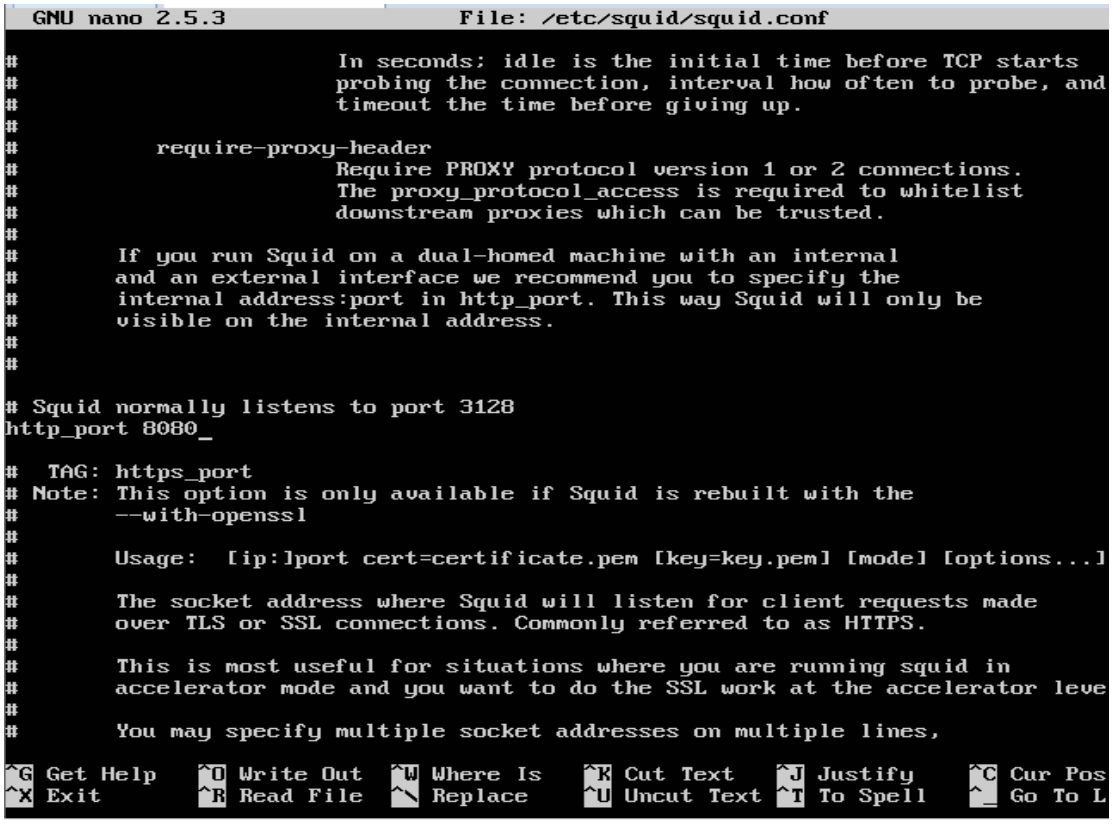

Figura 11: Arquivo de configuração do squid.
Fonte: Autor

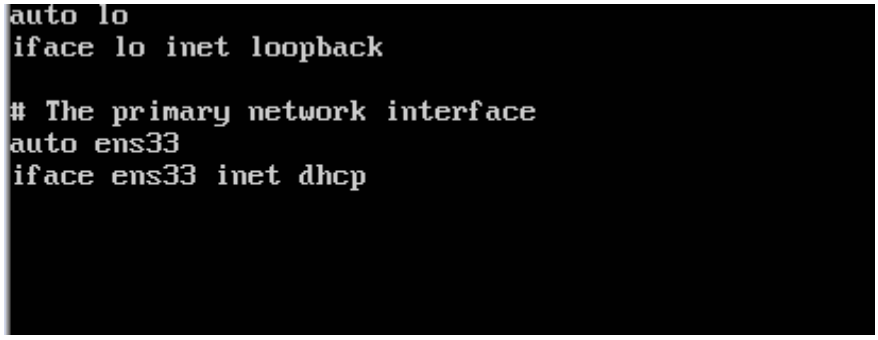

Figura 12: Interfaces padrão.
Fonte: Autor

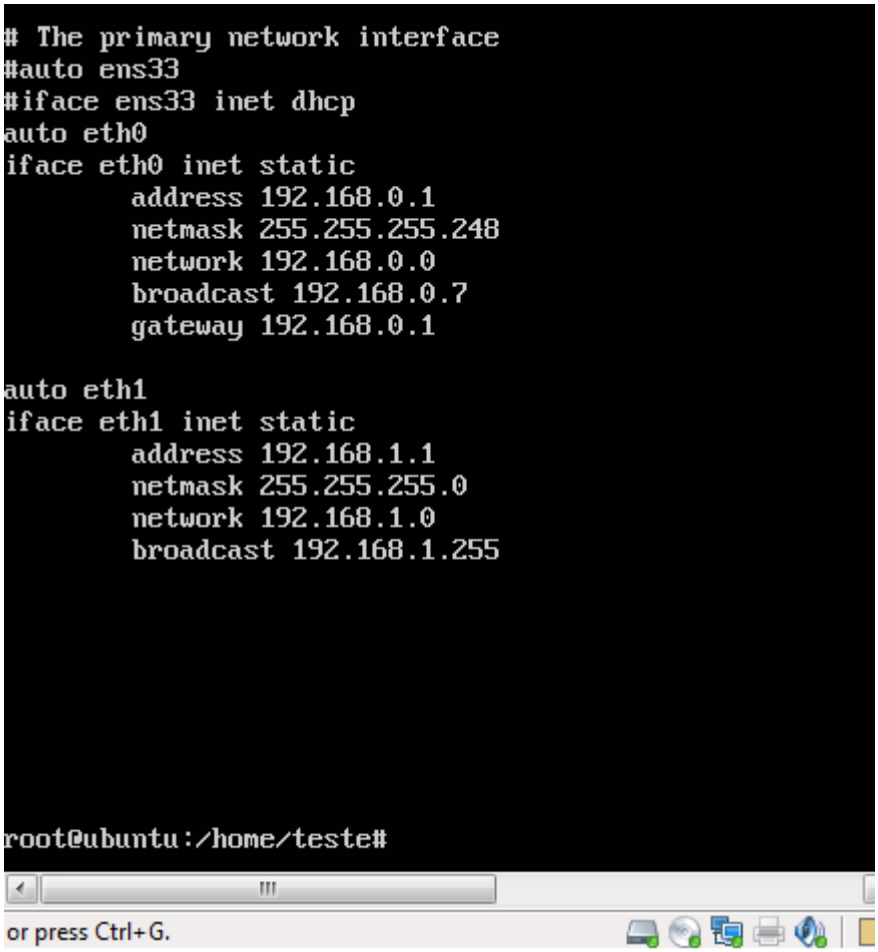

Figura 13: Interfaces da rede.
Fonte: Autor

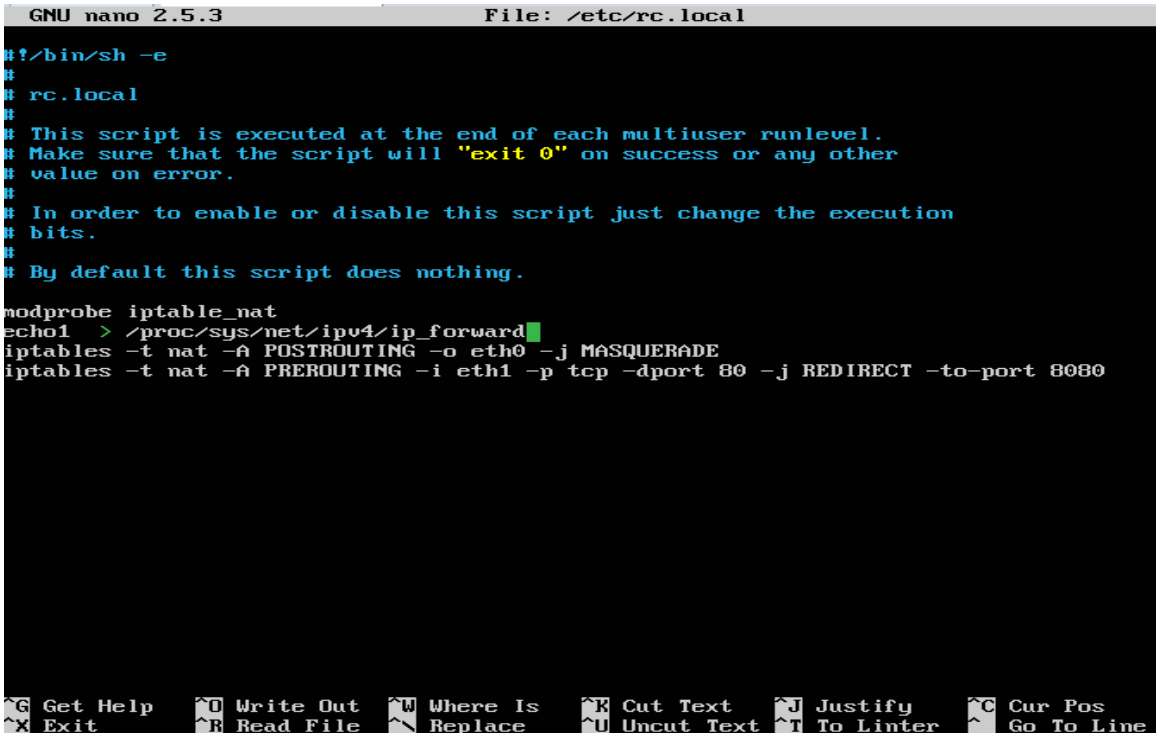

Figura 14: Arquivo local, definição de tudo que deve ser executado após o *boot.*
Fonte: Autor

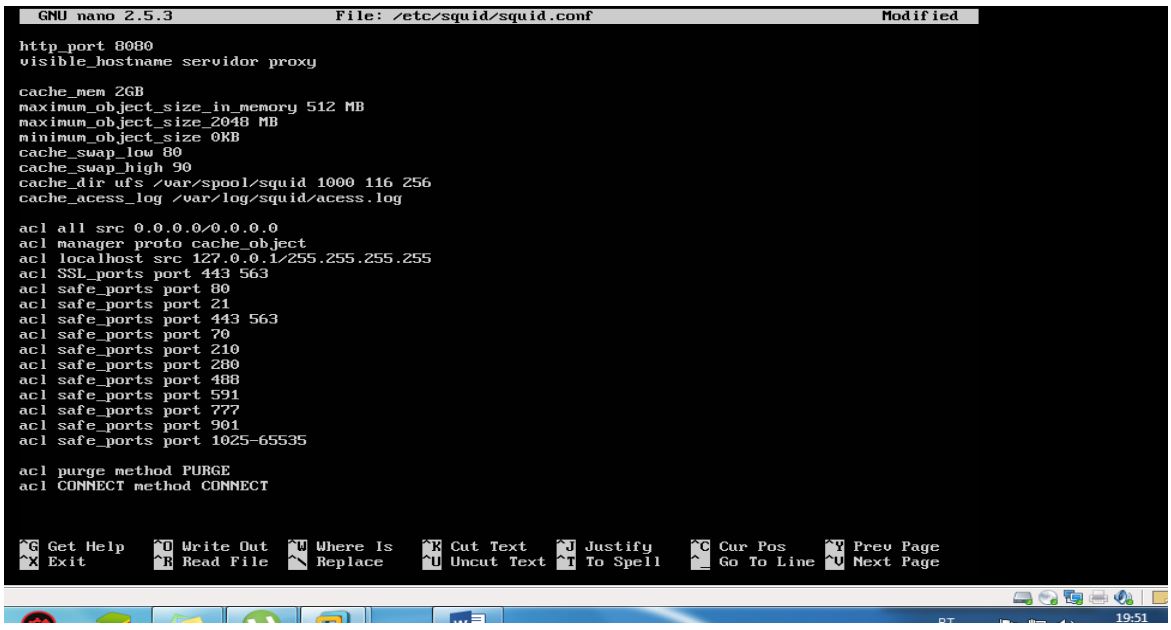

Figura 15: Arquivo de configuração do Squid (parte 1).
Fonte: Autor

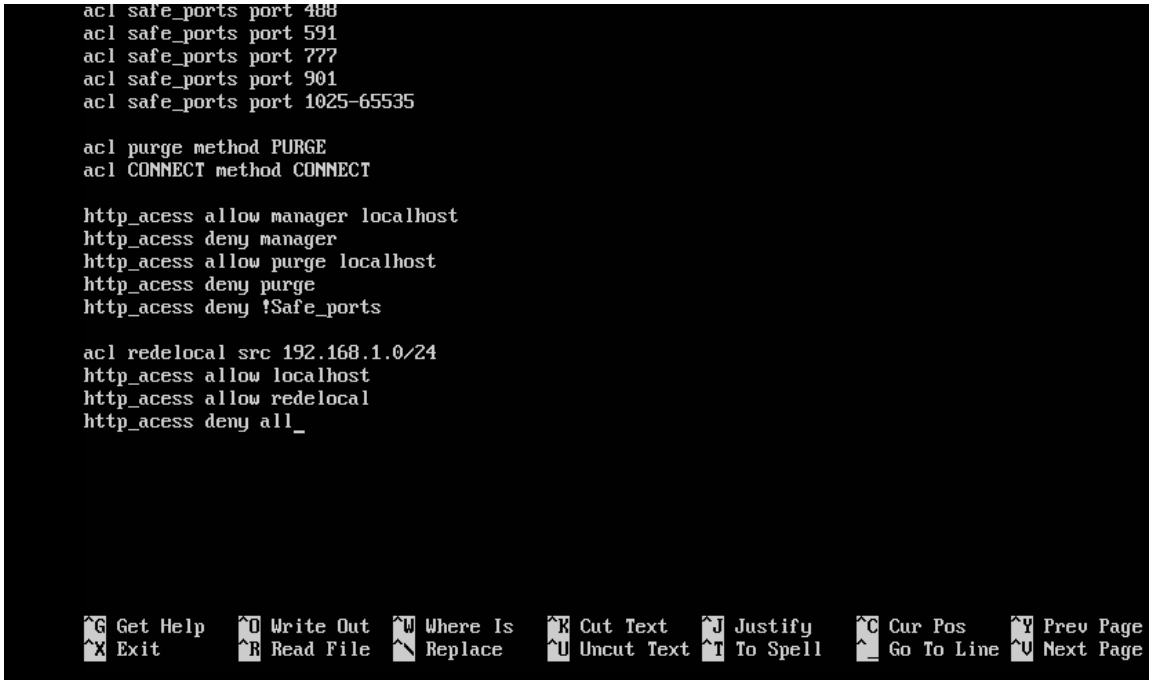

Figura 16: Arquivo de configuração do Squid (parte 2).
Fonte: Autor

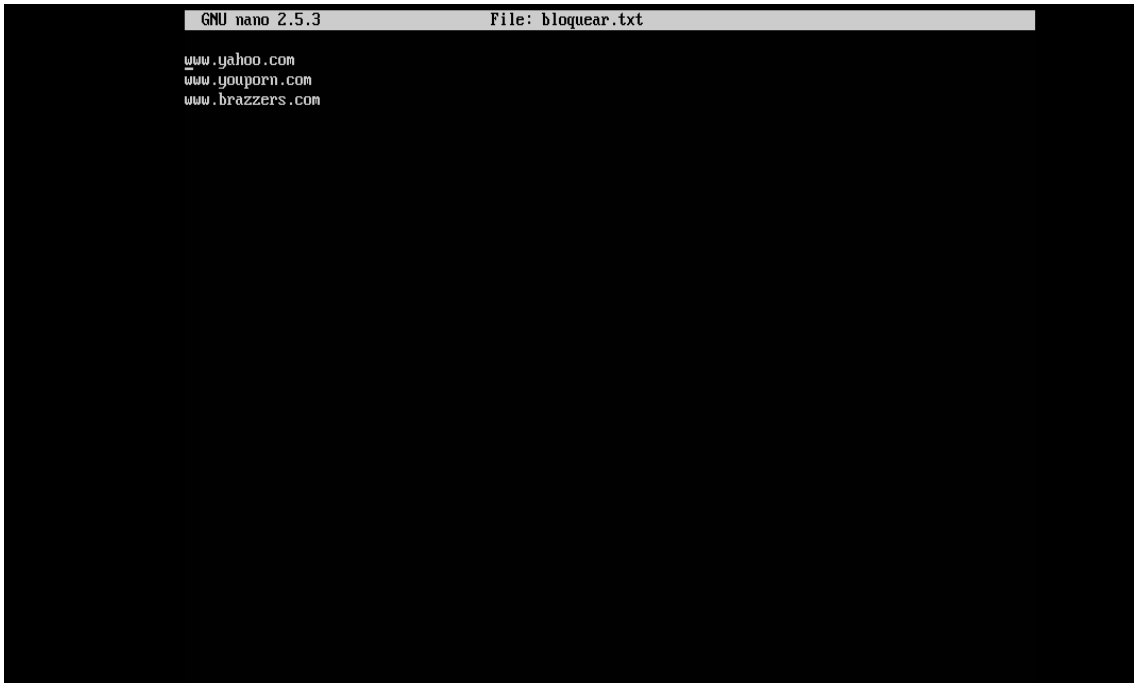

Figura 17: Arquivo final de bloqueio
Fonte: Autor

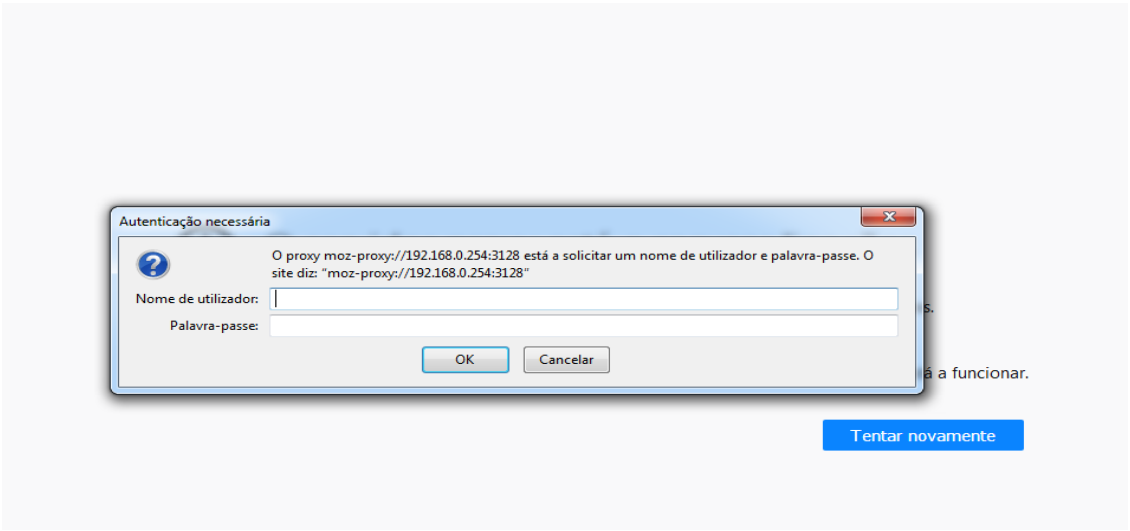

Figura 18: Autenticação.
Fonte: Autor

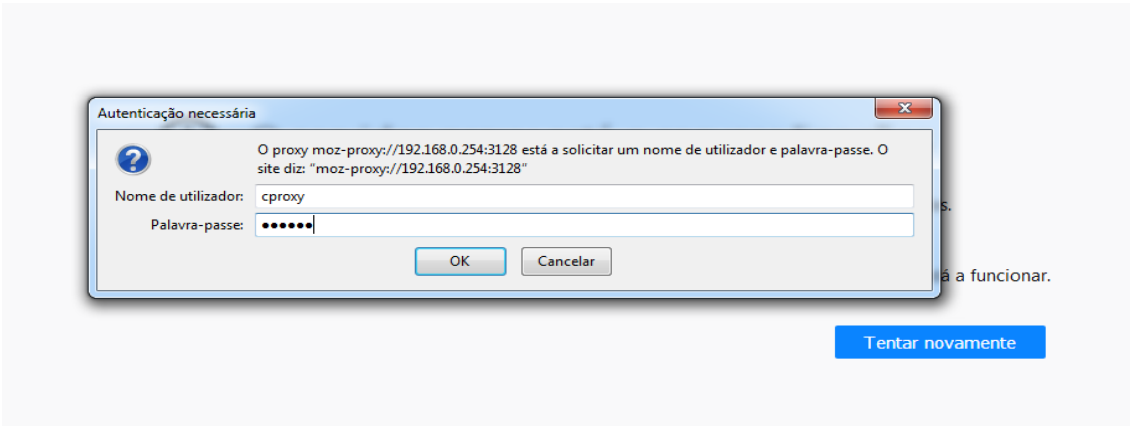

Figura 19: Informar o nome do utilizador e a senha.
Fonte: Autor

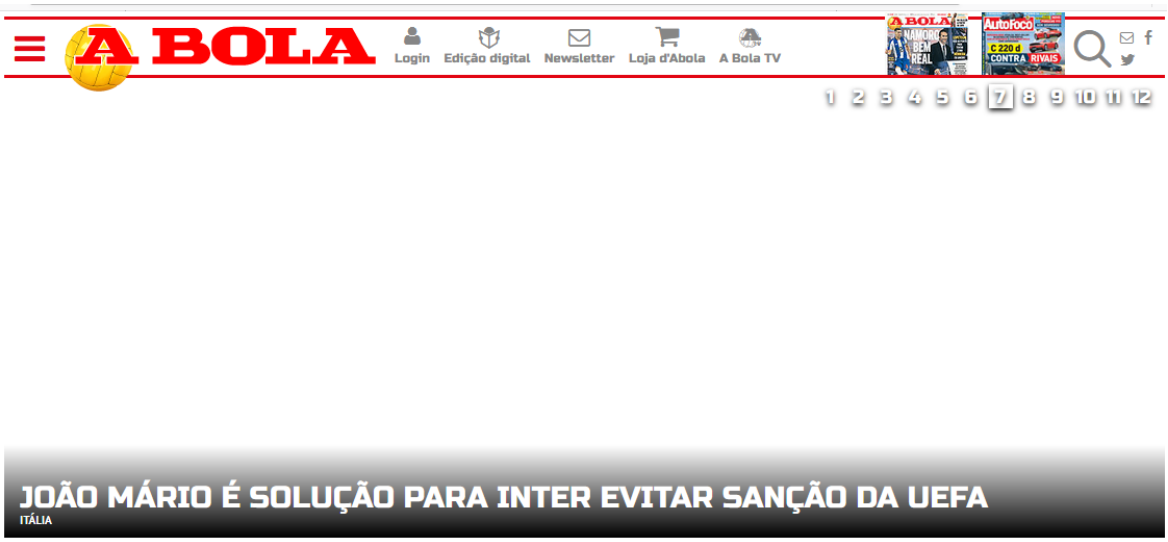

Figura 20: Pagina solicitada.
Fonte: Autor

Anexos

Anexo 1. Questionário

Grupo 1: Técnicos da CIUP e outros funcionários da UPM.

1. A quanto tempo trabalha na CIUP?

   _____

2. Qual ou quais as ferramentas de segurança implementada na rede UP-NET?

   _____

   _____

3. Até que ponto as ferramentas implementadas garantem segurança?

   _____

   _____

4. A CIUP tem programas de conscientização do pessoal sobre a importância da segurança de dados na rede?

   _____

   _____

5. A CIUP restringe o acesso a rede a pessoas não autorizadas?

   _____

6. Tem algum registo de perca, roubo de dados ou invasão da rede UP_NET?

   _____

   _____

7. Tem algum conhecimento sobre servidores *proxies* e sua importância?

   _____

   _____

a) Se sim, concorda com a sua implementação na rede UP_NET?

   _____

   _____

b) Porquê?

_____

_____

Grupo 2: Utilizadores da rede (Estudantes)

1. Qual é o curso que frequenta, ano e regime?

   _____

2. Tem conhecimento da existência da rede UP_NET?

   _____

3. Se sim, é utilizador com que frequência?

   _____

4. Existe alguma restrição de acesso a rede?

   _____

5. Tem partilhado seus dados com outros utilizadores da rede?

   _____

6. O que pode ser melhorado na rede UP_NET?

   _____

   _____