

**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**

BRUNO SANTOLIN DORNELLES FRANCO

GERENCIAMENTO DE UMA REDE SEM FIO COM PFSense

TRABALHO DE CONCLUSÃO DE CURSO

PONTA GROSSA

2015

BRUNO SANTOLIN DORNELLES FRANCO

GERENCIAMENTO DE UMA REDE SEM FIO COM PFSense

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas, do Departamento Acadêmico de Informática, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Msc. Rogério Ranthum

PONTA GROSSA

2015



TERMO DE APROVAÇÃO

GERENCIAMENTO DE UMA REDE SEM FIO COM PFSENSE

por

BRUNO SANTOLIN DORNELLES FRANCO

Este Trabalho de Conclusão de Curso foi apresentado em preencher o dia de preencher o mês de preencher o ano como requisito parcial para a obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

Prof. Msc. Rogério Ranthum
Prof. Orientador

Prof. Msc. Geraldo Ranthum
Membro titular

Prof. Dr. Richard Duarte Ribeiro
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho à minha família, que
me incentivou em todos os momentos.

AGRADECIMENTOS

Primeiramente agradeço minha família, que esteve presente em todos os momentos, sempre me incentivando a evoluir, através do estudo.

Ao meu orientador, Prof. Msc. Rogério Ranthum, pela ajuda, instrução, muita paciência, incentivo e confiança.

A Adriana Volaco, que esteve presente no final dessa jornada, clareando minha mente e me incentivando a não desistir.

Ao Leonardo Alves da Silva, que esteve presente nos momentos finais desta jornada, dando grande suporte pessoal.

Ao Lucas Vallim e sua esposa Andriele Vallim, devido a grande bagagem e experiência de vida, sempre me aconselharam nas situações mais inusitadas e, também, ao auxílio prestado no entendimento da língua inglesa americana.

RESUMO

FRANCO, Bruno Santolin Dornelles. **Gerenciamento de uma rede sem fio com pfSense**. 2015. 47. Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas) - Universidade Tecnológica Federal do Paraná. Ponta Grossa, 2015.

Este trabalho apresenta um estudo de caso de implantação do *software pfSense*, utilizado como principal solução para gerenciamento da rede sem fio de uma instituição de ensino superior. Em um primeiro momento, são apresentados os problemas da rede de computadores da instituição. São abordados conceitos de segurança de redes de computadores e serviços de rede necessários para a solução dos problemas apresentados. Este trabalho demonstra como a infraestrutura da instituição estava organizada antes e depois das modificações. O estudo principal se dá em torno do *software pfSense*, onde são evidenciados recursos desta ferramenta e como estes recursos resolveram os problemas na rede sem fio da instituição.

Palavras-chave: *Firewall. Pfsense. Segurança. Wi-Fi. Captive Portal.*

ABSTRACT

FRANCO, Bruno Santolin Dornelles. ***Wireless network management with pfSense***. 2015. 47. Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas) - *Federal Technology University* - Parana. Ponta Grossa, 2015.

This work present a study case that shows the pfSense deployment, used as a main solution on a higher education institution's wireless network management. At first, the Institution's Computer Network issues are presented. The concepts of network security are discussed and network services are required to solve the presented issues. This work demonstrates on how the infrastructure of the institution was organized before and after the changes. The main study revolves around the pfSense software where the features of this tool are highlighted and how these problems in the institution's wireless network are solved.

Keywords: Firewall. Pfsense. Security. Wi-Fi. Captive Portal.

LISTA DE ILUSTRAÇÕES

Figura 1 - Camadas modelo <i>OSI</i>	20
Figura 2 - Camadas do modelo <i>TCP/IP</i>	20
Figura 3 - <i>WLAN</i>	22
Figura 4 - <i>Firewall</i> entre uma rede interna e a Internet	25
Figura 5 – Exemplo de <i>captive portal</i>	27
Figura 6 - Rede anterior da Famper	29
Figura 7 - Nova estrutura da rede da Famper	31
Figura 8 - <i>AP Engenius EAP350</i>	32
Figura 9 - Tela de configuração das redes sem fio do <i>AP Engenius EAP350</i>	33
Figura 10 - <i>Switch HP 2530-24-PoE+ (J9779A)</i>	34
Figura 11 - Configuração da <i>VLAN</i> “FAMPERALUNO”, no <i>Switch HP 2530-24-PoE+ (J9779A)</i>	35
Figura 12 - Tela de <i>boot</i> para instalação do <i>pfSense</i>	36
Figura 13 - Tela final da Instalação do <i>pfSense</i>	36
Figura 14 - Assistente para configurações iniciais do <i>pfSense</i>	37
Figura 15 - <i>Dashboard pfSense</i>	37
Figura 16 - Tela de configuração de <i>VLAN</i>	38
Figura 17 - Regras de <i>firewall</i>	39
Figura 18 - Regra de <i>firewall</i> liberando comunicação entre redes distintas	39
Figura 19 - Configurações do <i>captive portal</i>	40
Figura 20 - Tela personalizada de autenticação do <i>captive portal</i>	40
Figura 21 - Configuração do <i>DHCP Server</i>	41
Figura 22 - Configuração da lista de bloqueios do servidor <i>proxy</i>	41
Figura 23 - <i>Captive portal</i> da rede “FAMPERALUNO”	42
Figura 24 - Teste de velocidade	42
Figura 25 - Teste de acesso em outra rede	43
Figura 26 - Mensagem do bloqueio de site pelo <i>proxy</i>	43
Figura 27 - <i>Proxy</i> transparente em site <i>HTTPS</i>	44
Quadro 1 - Resumo de padrões <i>WiFi</i> 802.11	23
Quadro 2 - <i>VLANs</i> da nova estrutura	31
Quadro 3 - Mapeamento das portas do switch gerenciável	32
Quadro 4 - Configurações dos <i>APs</i>	34

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

AES	<i>Advanced Encryption Standard</i>
AP	<i>Access Point</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
DMZ	<i>Demilitarized Zone</i>
DNS	<i>Domain Name System</i>
FTP	<i>File Transfer Protocol</i>
GB	<i>Gigabyte</i>
HP	<i>Hewlett-Packard</i>
HTTP	<i>Hypertext Transfer Protocol</i>
HTTPS	<i>Hyper Text Transfer Protocol Secure</i>
IBM	<i>International Business Machines</i>
ICMP	<i>Internet Control Message Protocol</i>
ID	<i>Identification</i>
IP	<i>Internet Protocol</i>
ISO	<i>International Organization for Standardization</i>
KVM	<i>Kernel-based Virtual Machine</i>
LAN	<i>Local Area Network</i>
MAN	<i>Metropolitan Area network</i>
OSI	<i>Open Systems Interconnection</i>
PDA	<i>Personal Digital Assistant</i>
PING	<i>Packet Internet Network Grouper</i>
PSK	<i>Pre-Shared Key</i>
RADIUS	<i>Remote Authentication Dial In User Service</i>
RAM	<i>Random Access Memory</i>
SNA	<i>System Network Architecture</i>
SSID	<i>Service Set Identifier</i>
SSL	<i>Secure Socket Layer</i>
TCP	<i>Transmission Control Protocol</i>
UDP	<i>User Datagram Protocol</i>
VLAN	<i>Virtual Local Area Network</i>
VPN	<i>Virtual Private Network</i>
WAN	<i>Wide Area Network</i>
WEB	<i>World Wide Web</i>
WLAN	<i>Wireless Local Area Network</i>
WPA2	<i>Wi-Fi Protected Acces II</i>

SUMÁRIO

1 INTRODUÇÃO	13
1.1 O PROBLEMA	13
1.2 OBJETIVOS.....	15
1.3 JUSTIFICATIVA.....	15
2 FUNDAMENTAÇÃO TEÓRICA	17
2.1 REDES DE COMPUTADORES E A INTERNET NAS EMPRESAS E NO ENSINO.....	17
2.2 REDES DE COMPUTADORES	18
2.2.1 Classificação das Redes.....	18
2.2.2 Topologia de Redes.....	18
2.2.3 Modelos de Referência	19
2.2.4 Domain Name System (DNS)	20
2.2.5 Dynamic Host Configuration Protocol (DHCP).....	21
2.2.6 Redes Locais Sem Fio (WLAN)	22
2.2.7 LANs Virtuais (VLANs).....	23
2.2.8 Remote Authentication Dial In User Service (RADIUS)	24
2.3 SEGURANÇA EM REDES DE COMPUTADORES	24
2.3.1 Firewall	24
2.3.1.1 Tipos de firewall	25
2.3.1.2 Arquiteturas de firewall.....	26
2.3.2 Secure Sockets Layer (SSL).....	26
2.3.3 Captive Portal	27
2.4 PFSENSE	27
3 ESTUDO DE CASO.....	29
3.1 ESTRUTURA ANTERIOR.....	29
3.2 A NOVA ESTRUTURA.....	30
3.2.1 Pontos De Acesso Sem Fio	32
3.2.2 Switch Gerenciável	34
3.2.3 Pfsense	35
3.2.3.1 Instalação.....	35
3.2.3.2 Configurações iniciais	37
3.2.3.3 VLANs.....	38
3.2.3.4 Firewall.....	38
3.2.3.5 Captive portal	39
3.2.3.6 DHCP server	41
3.2.3.7 Proxy.....	41
4 RESULTADOS OBTIDOS.....	42
5 CONCLUSÃO E TRABALHOS FUTUROS.....	45

REFERÊNCIAS.....	46
------------------	----

1 INTRODUÇÃO

Imaginar a vida das pessoas sem redes de computadores e a Internet nos dias atuais, não somente para usuários domésticos, mas também é difícil imaginar empresas que não estão conectadas em rede.

A Internet de hoje é provavelmente o maior sistema de engenharia já criado pela humanidade, com centenas de computadores conectados, links de comunicação e comutadores; centenas de milhares de usuários que se conectam esporadicamente por meio de telefones celulares e PDAs; e dispositivos como sensores, webcams, console para jogos, quadros de imagens, e até mesmo máquinas de lavar sendo conectadas à Internet (KUROSE; ROSS, 2010, p. 1).

A necessidade de compartilhamento de recursos e informações fez com que surgissem as redes de computadores. “[...] O objetivo é deixar todos os programas, equipamentos e, especialmente, dados ao alcance de todas as pessoas na rede, independentemente da localização física do recurso ou do usuário. [...]” (TANENBAUM; WETHERALL, 2011, p.2).

1.1 O PROBLEMA

A Famper, Faculdade de Ampére, iniciou suas atividades em meados de 2005, com três cursos de graduação. De 2005 até os dias atuais a instituição cresceu e, atualmente conta com sete cursos de graduação, descontando-se as demais atividades realizadas pela instituição, como pós-graduação e extensão. (FAMPER, 2015).

No início a instituição não possuía rede sem fio. Todo equipamento que necessitava de conexão de rede e Internet precisava ser plugado em um cabo de rede. Com o passar dos anos e a popularização da Internet e do uso das tecnologias como métodos auxiliares de ensino (projetores interativos, *notebooks*, *tablets* e *smartphones*), surgiu a necessidade de permitir o acesso a rede utilizando tecnologia sem fio. Como a quantidade de equipamentos que seriam conectados a

rede sem fio ainda era baixa e, os equipamentos ficariam em uma área específica, foi adquirido um *AP* (*Access Point* – Ponto de Acesso), com capacidade para poucos clientes. Conforme aumentava o número de equipamentos e a necessidade de ampliar a cobertura do sinal sem fio, eram adicionados mais *APs* à rede. Os *APs* que foram adicionados à rede, eram equipamentos de uso residencial, suportavam poucos clientes e a qualidade do sinal era baixa.

O usuário que se conectava a rede sem fio, necessitava configurar o servidor *proxy* manualmente, para que fosse possível o acesso a Internet. A segurança da rede era baixa, já que qualquer pessoa que possuísse um equipamento (*notebook*, *smartphone*, etc.) que estivesse ao alcance do sinal da rede sem fio e soubesse configurar o *proxy*, conseguia acessar a Internet da instituição sem se identificar.

Ao mesmo tempo em que, a segurança da rede era baixa, a navegação à Internet era de difícil acesso, devido à necessidade de que o servidor *proxy* fosse configurado manualmente. Os usuários de *smartphones* e *tablets* sofriam ainda mais, pois a configuração do *proxy* nestes equipamentos é difícil para usuários leigos, chegando a ser impossível para determinados modelos destes equipamentos.

Outra dificuldade encontrada é que todos estavam conectados na mesma rede. Dessa maneira, por exemplo, quando um acadêmico conectava seu *notebook* na rede sem fio, os computadores dos setores administrativos, dos laboratórios de informática e, até mesmo dos outros alunos, eram visíveis para ele. Conforme Kurose e Ross (2010, p. 355), este é um problema de segurança e privacidade, devido à falta de isolamento do tráfego. Por isso os computadores da instituição estavam vulneráveis a execução de analisadores de pacotes, o que poderia, por exemplo, gerar acesso indevido à informações confidenciais.

Por fim, outro problema enfrentado pela instituição de ensino era o fato de a rede não possuir controle no uso da velocidade da Internet, sendo assim, um usuário que, por exemplo, utilizava a Internet para baixar filmes e músicas, assistir vídeos no *Youtube*, entre outras atividades que consomem bastante largura de banda, deixavam a utilização da Internet lenta para toda a instituição.

Este trabalho está organizado da seguinte maneira:

- No capítulo 2 são abordados os conceitos necessários para a resolução dos problemas apresentados, como: conceitos de redes de computadores e do *software pfSense*.
- O capítulo 3 demonstra como estava a organização da rede da instituição, e como ficou a nova organização, além de como os problemas foram resolvidos com a implementação do servidor *pfSense*.

1.2 OBJETIVOS

Objetivo geral:

- Implantar um servidor *pfSense*, para gerenciamento da rede sem fio na Famper, Faculdade de Ampère.

Objetivos específicos:

- Ampliar e facilitar o acesso à rede sem fio;
- Realizar três segmentações de redes sem fio com *VLAN*, divididas em: rede sem fio para administrativo, rede sem fio para alunos e rede sem fio para professores;
- Implantar o *Captive Portal* do *pfSense* para prover acesso à rede sem fio somente para usuários autenticados;
- Alimentar a base de credenciais de um servidor *FreeRADIUS*;
- Estabelecer um limite de *download* e *upload* para cada cliente conectado a rede sem fio.
- Configurar um servidor *Proxy* transparente.

1.3 JUSTIFICATIVA

Com a popularização dos *notebooks*, *tablets* e *smartphones*, o uso desses equipamentos em instituições de ensino está cada vez maior. Professores estão deixando de lado a ultrapassada caderneta de chamada e realizando o controle de presença através de sistemas acadêmicos na *Web*. Alunos utilizam seus *notebooks*,

tablets e/ou *smartphones* para anotações, pesquisas e apresentações de trabalhos acadêmicos.

Por isso surgiu a necessidade de ampliar e, ao mesmo tempo facilitar o acesso a rede sem fio da instituição, bem como estabelecer parâmetros para uma navegação segura, controle de acesso e seu gerenciamento.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo abordará conceitos de redes de computadores e Internet, necessários para a realização deste trabalho.

2.1 REDES DE COMPUTADORES E A INTERNET NAS EMPRESAS E NO ENSINO

Toda empresa necessita de redes até para uma tarefa simples como compartilhar o uso de uma impressora. Além disso, as empresas precisam compartilhar as informações, como por exemplo, registros de clientes e produtos, dados financeiros e muitas outras informações. Outra facilidade fornecida pelas redes é a *VPN* (*Virtual Private Network* – Rede Privada Virtual), que possibilitam, por exemplo, que um vendedor que está fora do escritório possa acessar o banco de dados de estoque de produtos (TANENBAUM; WETHERALL, 2011).

Nos dias de hoje é fato que as empresas, independente do seu tamanho, não sobreviveriam sem estarem conectadas em redes de computadores e à Internet.

As empresas também utilizam *e-mail* (correio eletrônico), um meio de comunicação muito importante para a troca de mensagens. Outra importante facilidade é o *e-commerce* (comércio eletrônico), a qual permite que muitas empresas possibilitem aos seus clientes acesso a pedidos de produtos pela Internet (TANENBAUM; WETHERALL, 2011).

Nas instituições de ensino não pode ser diferente, a “[...] Internet é uma tecnologia que facilita a motivação dos alunos pela novidade e pelas possibilidades inesgotáveis de pesquisa que oferece.[...]” (MORAN, 1999, p.20).

A Internet está trazendo inúmeras possibilidades de pesquisa para professores e alunos, dentro e fora da sala de aula. Digitando-se duas ou três palavras nos serviços de busca, encontram-se múltiplas respostas para qualquer tema. [...] (MORAN, 1999, p.20).

2.2 REDES DE COMPUTADORES

Nas próximas seções serão estudados conceitos de rede de computadores. Segundo Ferreira (2008, p. 350), “rede de computadores é um conjunto de computadores autônomos, interconectados, capazes de trocar informações e compartilhar recursos.”

2.2.1 Classificação das Redes

As redes de computadores podem ser classificadas em:

- *LAN (Local Area Network – Rede de Área Local)*, “[...] é uma rede de computadores concentrada em uma área geográfica, tal como prédio ou um campus universitário.” (KUROSE; ROSS, 2010, p. 337).
- *MAN (Metropolitan Area Network – Rede de Área Metropolitana)*, “[...] abrange uma cidade. O exemplo mais conhecido de *MANs* é a rede de televisão a cabo disponível em muitas cidades. [...]” (TANENBAUM; WETHERALL, 2011, p. 14).
- *WAN (Wide Area Network – Rede de Longa Distância)*, “[...] abrange uma grande área geográfica, com frequência um país ou continente. [...]” (TANENBAUM; WETHERALL, 2011, p. 15).

2.2.2 Topologia de Redes

Para Ferreira (2008, p. 351), “[...] as duas topologias principais de redes são redes canais ponto a ponto e redes canais multiponto.”

As redes na topologia redes canais ponto a ponto conectam individualmente um nó a outro. Elas são classificadas em:

- Estrela ponto a ponto: “Nesta topologia, todo nó tem uma conexão com o nó central. O nó central é o único roteador nesse tipo de rede. [...]” (FERREIRA, 2008, p. 351).
- Árvore: “É a arquitetura *SNA (System Network Architecture)* criada pela IBM em 1974. É uma topologia hierarquizada, sendo muito utilizada em

grandes sistemas de rede baseados em mainframe.” (FERREIRA, 2008, p. 352).

- Anel: “Nesta topologia de rede, cada nó é conectado a outros dois nós adjacentes ao anel.” (FERREIRA, 2008, p. 352).
- Completa: “Neste caso, cada nó tem uma conexão direta com todos os outros nós da rede. [...]” (FERREIRA, 2008, p. 353).

As redes em topologia para canais multiponto realizam a conexão direta de um nó para vários outros simultaneamente. São classificadas em:

- Barramento: “É muito usada em redes locais. Tem a forma de um varal. Nesta topologia, não há, normalmente, hierarquia de acesso.” (FERREIRA, 2008, p. 353).
- Estrela Multiponto: “Neste caso, o nó central sempre realiza o *broadcast* (envio dos quadros recebidos para todos os nós). [...]” (FERREIRA, 2008, p. 354).

2.2.3 Modelos de Referência

As duas principais arquiteturas de rede são: os modelos de referência *OSI* e *TCP/IP*. Os protocolos associados ao modelo *OSI* raramente são utilizados, mas as características descritas em cada camada são muito importantes. O modelo *TCP/IP* é pouco utilizado, mas os protocolos são muito utilizados (TANENBAUM; WETHERALL, 2011, p.25).

Para Ferreira (2008, p. 358):

O modelo OSI (Open System Interconnection) foi criado em 1977 pela ISO (International Standardization Organization) com o objetivo de criar padrões de conectividade para interligação de sistemas de computadores locais ou remotos. Os aspectos gerais da rede estão divididos em sete camadas funcionais, facilitando a compreensão de questões fundamentais sobre a rede. As regras que orientam a conversação entre as camadas são chamadas de protocolos da camada. Essa conversação é processada entre as respectivas camadas de cada sistema comunicante, porém para que essa comunicação seja efetivada, tem de descer até a camada mais baixa (física) onde efetivamente as informações são transmitidas. [...]

Podem-se ver as sete camadas do modelo *OSI*, representadas na Figura 1.



Figura 1 - Camadas modelo OSI
Fonte: Autoria própria

O modelo *TCP/IP* une dois protocolos de comunicação: o *IP* (*Internet Protocol* – Protocolo de Internet), que transmite os dados em forma de *datagramas* e o *TCP* (*Transmission Control Protocol* – Protocolo de Controle de Transmissão), o qual remonta os *datagramas* na ordem correta e assegura a entrega ao destino final (FERREIRA, 2008, p.361).

Enquanto o modelo *OSI* possui sete camadas, o modelo *TCP/IP* é composto de quatro camadas, representadas na Figura 2.

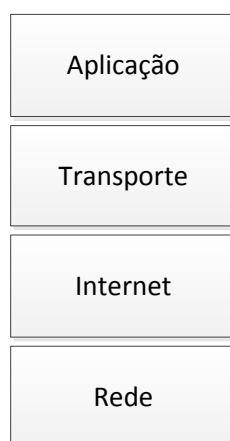


Figura 2 - Camadas do modelo TCP/IP
Fonte: Autoria própria

2.2.4 Domain Name System (DNS)

Tanenbaum e Wetherall (2011), explicam a essência do *DNS*:

A essência do DNS é a criação de um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuído para implementar esse esquema de nomenclatura. Ele é mais usado para mapear nomes de hosts em endereços IP, mas também pode servir para outros objetivos.[...]

Em suma, se não existisse o *DNS (Domain Name System* – sistema de nomes de domínio), para, por exemplo, acessar uma página na *Web*, seria necessário memorizar o endereço *IP* do servidor onde está hospedada a página em questão.

Para este estudo de caso é importante abordar sobre o *cache DNS*, que, segundo Kurose e Ross (2010, p. 101) “[...] em uma cadeia de consultas, quando um servidor de nomes recebe uma resposta *DNS* (contendo, por exemplo, o mapeamento de um nome de hospedeiro para um endereço *IP*), ele pode fazer cache das informações da resposta em sua memória local. [...]”

Em uma *LAN* com muitos computadores é aconselhável, possuir no mínimo um servidor *cache DNS*, evitando assim, para sites frequentemente acessados, consultas desnecessárias aos servidores *DNS* externos a *LAN*.

2.2.5 Dynamic Host Configuration Protocol (DHCP)

De acordo com Tanenbaum e Wetherall (2011), o *DHCP* funciona da seguinte maneira:

[...] O computador envia uma solicitação de broadcast por endereço IP em sua rede. Ele faz isso usando um pacote DHCP DISCOVER. Esse pacote precisa alcançar o servidor DHCP. [...]

Quando o servidor recebe a solicitação, ele aloca um endereço IP livre e o envia ao host em um pacote DHCP OFFER [...]. Para poder fazer isso funcionar até mesmo quando os hosts não têm endereços IP, o servidor identifica um host usando seu endereço Ethernet (que é transportado no pacote DHCP DISCOVER).

O *DHCP (Dynamic Host Configuration Protocol* – Protocolo de Configuração Dinâmica de Host) é responsável por fornecer as configurações de rede (endereço

IP, máscara de sub-rede, endereço do *gateway*, endereço dos servidores *DNS*, dentre outras configurações) para os equipamentos que se conectarem a rede.

As configurações de rede podem ser realizadas manualmente em cada equipamento conectado a rede. “[...] Em pequenas redes, isso é fácil de ser feito, mas em grandes redes se torna uma tarefa muito trabalhosa e bastante sujeita a falhas. [...]” (FERREIRA, 2008, p. 459).

2.2.6 Redes Locais Sem Fio (WLAN)

As *WLANs* estão cada vez mais populares em residências e prédios de escritórios. Geralmente cada computador possui um rádio modem e uma antena, que se comunica com um *AP*, conforme demonstra a Figura 3. O padrão de *LAN* sem fio é denominado 802.11, popularmente conhecido como *WiFi* (TANENBAUM; WETHERALL, 2011).

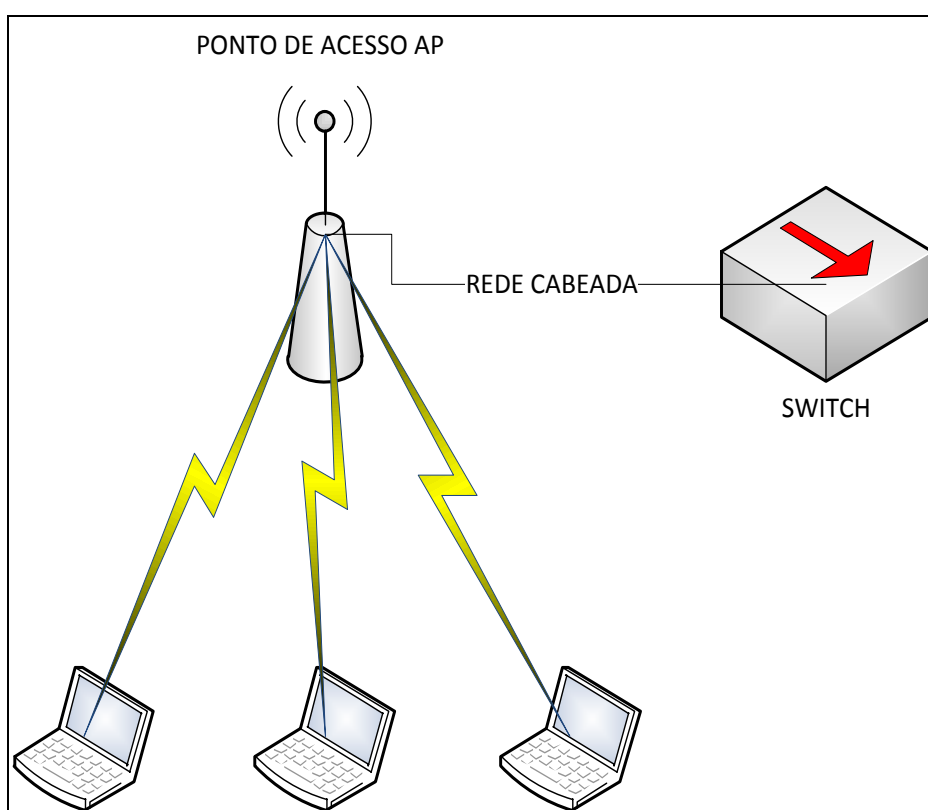


Figura 3 - WLAN
Fonte: Autoria própria

Os padrões 802.11 mais utilizados nos equipamentos sem fio são: 802.11b, 802.11a, 802.11g e 802.11n. As diferenças entre eles são basicamente a faixa de

frequência e a velocidade máxima. No Quadro 1 pode-se visualizar a frequência e a velocidade máxima que cada padrão pode atingir.

Padrão	Faixa de frequência	Taxa de dados
802.11b	2,4 GHz	até 11 Mbps
802.11a	5 GHz	até 54 Mbps
802.11g	2,4 GHz	até 54 Mbps
802.11n	2,4 GHz e/ou 5 GHz	até 600 Mbps

Quadro 1 - Resumo de padrões WiFi 802.11
Fonte: SOARES DE OLIVEIRA (2014)

2.2.7 LANs Virtuais (VLANs)

As *VLANs* (*LANs* virtuais) permitem que a rede local física possa ser segmentada em redes locais virtuais dentro de um mesmo *switch*.

De acordo com Kurose e Ross (2010, p. 355), as *VLANs* surgiram com o objetivo de resolver algumas dificuldades:

- Falta de isolamento do tráfego: com a utilização de *VLANs*, torna-se possível limitar o tráfego de *broadcast* (por exemplo, quadros carregando mensagens *DHCP*) na rede, dessa maneira, além de melhorar o desempenho da *LAN*, aprimoraria questões de privacidade e segurança. Por exemplo, em uma universidade, alunos poderiam utilizar um *software* analisador de pacotes para capturar informações trafegadas nos departamentos administrativos da instituição.
- Uso ineficiente de *switches*: por exemplo, para dividir em três grupos uma *LAN* com 20 computadores, conectados a um *switch* sem suporte a *VLANs*, seriam necessários três *switches*.
- Gerenciamento de usuários: por exemplo, em uma *LAN*, dividida em grupos que utilizando *switches* sem suporte a *VLANs*, caso um funcionário mude de grupo, seria necessário alterar o cabo de rede de *switch*. Problema que não existiria em *switches* com *VLANs*, pois seria necessário somente alterar as configurações nos *softwares* de gerenciamento das *VLANs*.

As principais implementações de *VLAN* são: *VLAN* baseada em porta, a qual opera em *switches* da camada 2 do modelo *OSI* e *VLAN* baseada em *IP*, utilizando a camada 3 do modelo *OSI* (FERREIRA, 2008, p.656).

2.2.8 Remote Authentication Dial In User Service (RADIUS)

O *RADIUS* (*Remote Authentication Dial In User Service*) é um protocolo para autenticação, comumente utilizado em provedores de Internet e redes sem fio.

[...] é um protocolo tratado na [RFC2865], definido nela como sendo desenvolvido para a realização de autenticação, autorização e encaminhamento de informações de configuração entre uma rede de acesso compartilhada, que deseja autenticar as suas ligações, e um servidor de autenticação (SILVA 2010, p. 49-50).

2.3 SEGURANÇA EM REDES DE COMPUTADORES

Os conceitos sobre segurança em redes de computadores são muito amplos e extensos, por isso abordaremos somente os conceitos necessários para o nosso estudo de caso.

2.3.1 Firewall

Um *firewall*, ilustrado na Figura 4, atua como uma barreira entre a rede interna e a Internet, filtrando tudo que entra e sai da rede. Pode ser uma solução combinada de *hardware* e *software* ou somente uma solução de *software* (STATO FILHO, 2009, p. 33).

Segundo Kurose e Ross (2010, p. 536) um *firewall* eficiente deve atender a três requisitos:

- Todo o tráfego, sem exceção, de fora para dentro e vice-versa, deve ser filtrado pelo *firewall*.
- Somente o tráfego definido nas políticas do *firewall* como permitido poderá atravessar.

- O próprio *firewall* deve ser imune a invasões.

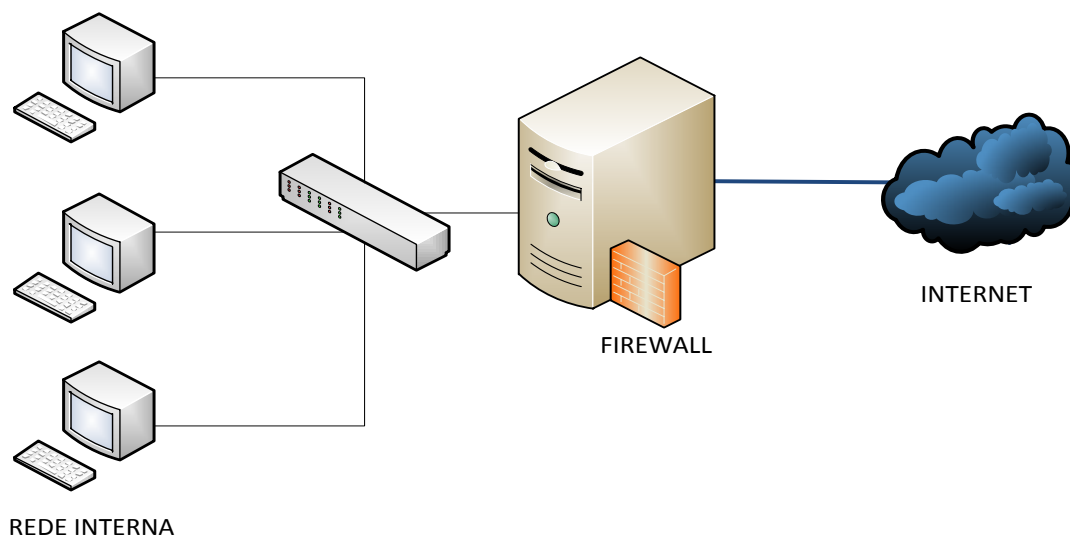


Figura 4 - Firewall entre uma rede interna e a Internet
 Fonte: Autoria própria

2.3.1.1 Tipos de firewall

Dentre os vários tipos de *firewall* existentes, os três tipos mais comuns são:

- *Packet Filtering* (filtragem de pacotes): trabalha filtrando a troca de pacotes entre a rede interna e a Internet. Os filtros podem ser feitos baseados em endereço *IP* e protocolo (*HTTP*, *FTP*, etc.). Este modelo de *firewall* é muito eficiente para defender a rede interna de invasões oriundas da Internet, bem como filtrar o tráfego da rede interna para Internet, e dessa forma, impedindo, que usuários da rede interna acessem serviços desnecessários. Por exemplo, no caso de um funcionário que utiliza a Internet da empresa para *download* de arquivos *torrent* (STATO FILHO, 2009).
- *Proxy Services*: um servidor *proxy*, captura as requisições oriundas da rede interna, verifica se o que o usuário está requisitando é permitido e caso positivo, repassa a requisição adiante. Normalmente o servidor *proxy* é transparente, ou seja, o usuário não sabe que existe um *proxy* entre ele e a Internet (STATO FILHO, 2009).
- *Circuit-Level Gateways*: este tipo de *firewall* “[...] cria um circuito entre o cliente e o servidor e não interpreta o protocolo de aplicação. Atua

monitorando o *handshaking* entre pacotes, objetivando determinar se a sessão é legítima.” (STATO FILHO, 2009, p. 37).

2.3.1.2 Arquiteturas de firewall

As três arquiteturas de *firewall* mais utilizadas no mercado são:

- *Dual-Homed Host*: nesta arquitetura o *firewall* opera em um computador com duas interfaces físicas de rede, uma das interfaces está conectada a rede interna e a outra a Internet. Esta arquitetura é recomendada para redes de pequeno porte (STATO FILHO, 2009).
- *Screened Host*: esta arquitetura é mais segura que a *Dual-Homed*, pelo fato de possuir duas camadas de segurança. Em uma camada está o *Screened Router*, conectado a Internet e na outra camada está o *Bastion Host*, conectado a rede interna. O *Bastion Host*, por sua vez não está conectado diretamente a Internet, ele recebe as requisições da rede interna e as repassa para o *Screened Router* (STATO FILHO, 2009).
- *Screened Subnet Firewall*: também conhecida como *DMZ (DeMilitarized Zone – Zona Desmilitarizada)*, é a mais segura entre as arquiteturas estudadas, pois provê três camadas de segurança. Esta arquitetura possui dois *firewalls* do tipo *Screened*, onde um deles está conectado a Internet e o outro a rede interna, entre esses dois *firewalls* existe um *Bastion Host* (STATO FILHO, 2009).

2.3.2 Secure Sockets Layer (SSL)

O *SSL (Secure Sockets Layer – Camada Segura de Sockets)* surgiu da necessidade de fornecer conexões seguras na *Web* para transações, como a compra de mercadorias por cartões de crédito, transações bancárias, etc (TANENBAUM; WETHERALL, 2011, p.534).

Segundo Tanenbaum e Wetherall (2011, p. 354), “[...] a principal tarefa do *SSL* é manipular a compactação e a criptografia. Quando o *HTTP* é usado sobre *SSL*, ele se denomina *HTTPS (Secure HTTP)*, embora seja o protocolo *HTTP* padrão. [...] Ele está disponível em uma nova porta (443) [...]”

2.3.3 Captive Portal

Um *captive portal* é comumente utilizado como uma camada adicional de segurança nas redes sem fio corporativas para acesso a Internet. O *captive portal* permite forçar a autenticação, ou seja, quando um usuário se conecta a rede sem fio e tenta abrir uma página *Web*, o *captive portal* intercepta a tentativa de acesso e, direciona o usuário para uma tela de autenticação, o acesso à Internet só será liberado se o usuário possuir *login* e senha válidos.

Na Figura 5 vemos um exemplo de *captive portal* solicitando as credenciais do usuário.

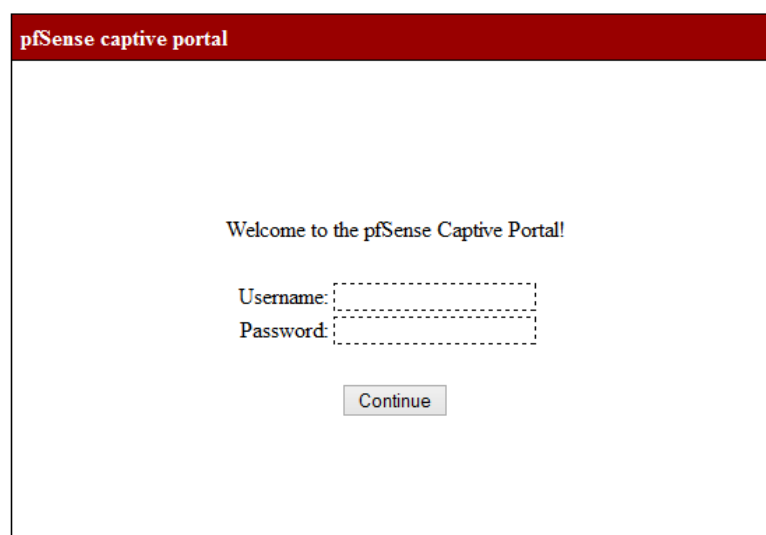
The image shows a web browser window displaying the pfSense captive portal. At the top, there is a dark red header with the text "pfSense captive portal" in white. Below the header, the main content area is white and contains the following elements: a welcome message "Welcome to the pfSense Captive Portal!", a "Username:" label followed by a dashed-line input field, a "Password:" label followed by a dashed-line input field, and a "Continue" button centered below the input fields.

Figura 5 – Exemplo de *captive portal*
Fonte: *pfSense*

2.4 PFSENSE

O *pfSense* é uma distribuição customizada do *FreeBSD*. Ele é um *software* gratuito e *open source* adaptado especialmente para ser utilizado como *firewall* e roteador. É totalmente gerenciável por uma interface *Web* e possui um sistema de pacotes que permite agregar recursos (pfSense, 2015).

O *pfSense* possui muitos recursos úteis para o gerenciamento de redes de computadores. Neste estudo são utilizados os seguintes recursos:

- *VLANs*;

- *Firewall;*
- *Captive Portal;*
- *DHCP Server;*
- *Cache DNS;*
- *Proxy server;*

3 ESTUDO DE CASO

Este capítulo demonstra como estava a rede da Famper antes das modificações e como ficou a nova estrutura. Também são demonstrados os procedimentos efetuados na instalação e configuração dos equipamentos físicos e do *pfSense*.

3.1 ESTRUTURA ANTERIOR

Anteriormente a estrutura da Famper possuía um servidor *firewall*, um servidor *proxy* e um servidor controlador de domínio *Active Directory*, os quais atendiam toda a rede, conforme ilustrado na Figura 6.

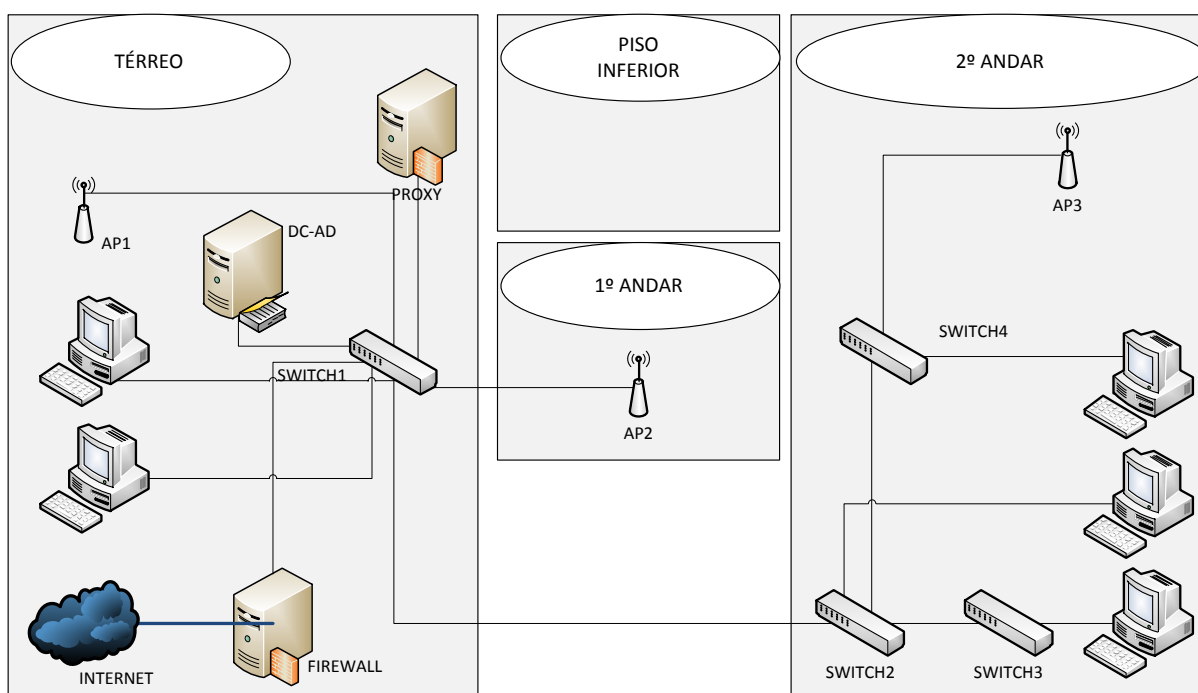


Figura 6 - Rede anterior da Famper
Fonte: Autoria própria

No total, a instituição possui quatro pisos:

- No térreo estão: os servidores, computadores do setor administrativo e um ponto de acesso sem fio, todos estavam conectados ao *switch1* (Figura 6).
- O piso inferior possui salas de aula e não possuía equipamentos de rede.

- O primeiro andar possui salas de aula e possuía somente um *AP*.
- O segundo andar possui salas de aula, dois laboratórios de informática, biblioteca e possuía um ponto de acesso sem fio. O *switch2* (Figura 6), ficava no laboratório de informática 1, este *switch* estava conectado ao *switch1*. O *switch3* (Figura 6) estava no laboratório de informática 2 e era conectado ao *switch2*. O *switch4* (Figura 6) estava na biblioteca e possuía um ponto de acesso conectado a ele, este *switch* estava conectado ao *switch2*.

Toda estrutura operava na rede 172.16.0.0/16. O servidor *proxy* não era transparente, ou seja, as configurações de *proxy* deveriam ser efetuadas manualmente no navegador *Web*, para que o usuário conseguisse acessar a Internet.

Como a rede possui um servidor controlador de domínio *Active Directory* (DC-AD, Figura 6), as configurações de *proxy* nas máquinas da instituição são efetuadas automaticamente, no momento do *login*, através das políticas de grupo do *Active Directory*. De fato, quem enfrentava dificuldade eram os acadêmicos e docentes que desejavam utilizar a rede sem fio, pois para utilizarem a Internet, deveriam configurar o *proxy*. Os demais problemas desta estrutura são abordados no capítulo 1.1.

3.2 A NOVA ESTRUTURA

Na nova estrutura foi adicionado um *switch* gerenciável da camada 2 do modelo *OSI*, para que seja possível separar a rede sem fio da rede cabeada, através da utilização de *VLANs*.

As *VLANs* resolveram o problema de segurança, em que os computadores dos setores administrativos e dos laboratórios de informática eram visíveis para qualquer usuário que se conectava na rede sem fio. De acordo com o Quadro 2, foram configuradas três *VLANs*, a primeira para funcionários do setor administrativo, a segunda para acadêmicos e a terceira para professores.

VLAN ID	Rede	Descrição	Modo de segurança	Nome da rede	Limite download/upload
10	192.168.3.0/24	VLAN para o setor administrativo	WPA2-PSK AES	FAMPERADM	Não possuirá
20	10.1.0.0/23	VLAN para acadêmicos	Captive Portal	FAMPERALUNO	1 Mega/1 Mega
30	192.168.4.0/24	VLAN para professores	Captive Portal	FAMPERPROFESSOR	1,5 Mega / 1,5 Mega

Quadro 2 - VLANs da nova estrutura
Fonte: Autoria própria

Foram adicionados três novos pontos de acesso sem fio e, os APs anteriores foram substituídos por novos equipamentos. Atualmente a estrutura possui seis APs, conforme demonstra a Figura 7.

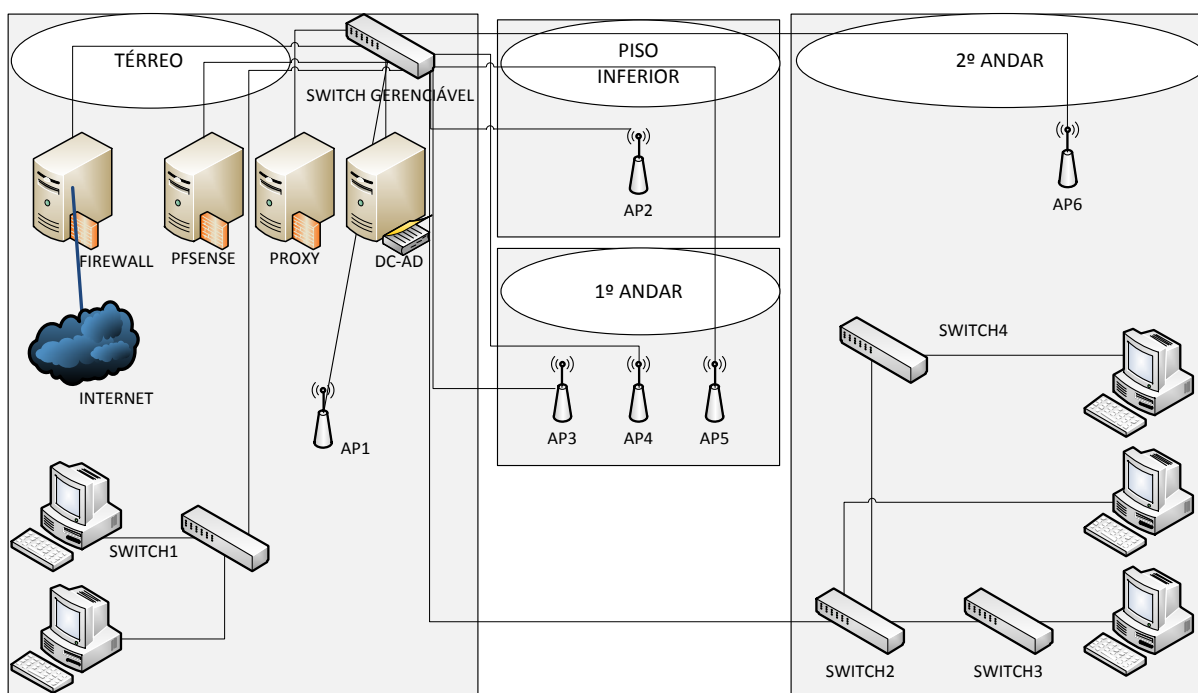


Figura 7 - Nova estrutura da rede da Famper
Fonte: Autoria própria

Os novos APs ampliaram o sinal de rede sem fio na instituição. O térreo continua com um ponto de acesso sem fio. O piso inferior, que antes não possui cobertura do sinal sem fio, agora conta com um AP. O primeiro andar está com três APs, pois este piso é maior que os demais, portanto necessita de três pontos de acesso para que tenha cobertura de sinal em toda área. O segundo andar possui um AP.

Neste novo cenário, de acordo com a Figura 7, foi adicionado o servidor *pfSense*, para controlar a rede sem fio. O *switch1*, que antes era conectado aos

servidores e levava a rede para os demais pisos, agora é utilizado somente para conectar os computadores do setor administrativo a rede. Os servidores e todos os APs agora estão conectados ao *switch gerenciável*. O *switch1* e o *switch2* também estão conectados ao novo *switch*.

Para realização das configurações das *VLANs* no *switch gerenciável*, as portas devem ser mapeadas, pois a configuração das *VLANs* é realizada em cada porta específica. No Quadro 3 pode-se visualizar o mapeamento das portas do *switch*.

Porta	Equipamento
1	SWITCH1
2	SWITCH2
3	PFSENSE
19	AP6
20	AP5
21	AP3
22	AP4
23	AP1
24	AP2
25	FIREWALL/PROXY/DC-AD
26	SERVIDOR DE ARQUIVOS

Quadro 3 - Mapeamento das portas do switch gerenciável
Fonte: Autoria própria

3.2.1 Pontos De Acesso Sem Fio

A nova estrutura possui seis APs do fabricante *Engenius*, modelo EAP350, conforme Figura 8.



Figura 8 - AP Engenius EAP350
Fonte: Engenius (2015)

Conforme especificações do fabricante Engenius (2015), o equipamento possui suporte para *VLANs*, capacidade para até cinquenta clientes simultâneos e opera nos padrões *WiFi* 802.11 b/g/n.

O equipamento pode ser configurado por um navegador *Web*. Após acessar a página de configuração, em “*Wireless Network*” é possível efetuar a configurações das redes sem fio, conforme Figura 9.

Este equipamento suporta até oito redes sem fio, e em nosso caso são três redes, mencionadas no Quadro 2. Clicando no botão “*edit*” (Figura 9), é possível configurar o nome da rede sem fio e a *ID* da *VLAN* de cada rede.

The screenshot shows the 'Wireless Network' configuration page. The sidebar on the left lists various settings categories: Status (Save/Reload:0, Main, Wireless Client List, System Log), System (Operation Mode, IP Settings, Spanning Tree Settings), Wireless (Wireless Network, Wireless MAC Filter, Wireless Advanced Settings, WPS), and Management (Administration, Management VLAN). The main configuration area includes fields for Wireless Mode (802.11 B/G/N Mixed), Channel HT Mode (20MHz), Extension Channel (Lower Channel), Channel / Frequency (Ch7-2.442GHz), and AP Detection (Scan). Below these fields is a table titled 'Current Profiles' with the following data:

SSID	Security	Isolation	VID	Enable	Edit
FAMPERADM	WPA2-PSK AES	<input checked="" type="checkbox"/>	10	<input checked="" type="checkbox"/>	Edit
FAMPERALUNO	None	<input checked="" type="checkbox"/>	20	<input checked="" type="checkbox"/>	Edit
FAMPERPROFESSOR	None	<input checked="" type="checkbox"/>	30	<input checked="" type="checkbox"/>	Edit
FAMPER	None	<input type="checkbox"/>	4	<input type="checkbox"/>	Edit
EnGenius274D4E_5	None	<input type="checkbox"/>	5	<input type="checkbox"/>	Edit
EnGenius274D4E_6	None	<input type="checkbox"/>	6	<input type="checkbox"/>	Edit
EnGenius274D4E_7	None	<input type="checkbox"/>	7	<input type="checkbox"/>	Edit
EnGenius274D4E_8	None	<input type="checkbox"/>	8	<input type="checkbox"/>	Edit

Figura 9 - Tela de configuração das redes sem fio do AP Engenius EAP350
 Fonte: Interface *Web* de configuração do AP Engenius EAP350

Em uma topologia de rede sem fio que possui vários *APs* é possível criar uma única rede sem fio, para isso, com exceção do endereço *IP* e do canal, as demais configurações (nome da rede sem fio (*SSID*), modo de operação, etc.) devem ser iguais em todos os *APs* (MORIMOTO, 2011).

Por motivos de compatibilidade com clientes mais antigos, o parâmetro “*Wireless Mode*” de todos os *APs* foi configurado como “802.11 B/G/N *Mixed*”, o canal e o endereço *IP* de cada equipamento ficou de acordo com o Quadro 4.

Equipamento	Canal	Endereço IP
AP1	1	172.16.0.10
AP2	7	172.16.0.11
AP3	4	172.16.0.12
AP4	6	172.16.0.13
AP5	11	172.16.0.14
AP6	2	172.16.0.15

Quadro 4 - Configurações dos APs
Fonte: Autoria Própria

3.2.2 Switch Gerenciável

Para gerenciamento das *VLANs* foi adquirido o *switch* da *HP*, Figura 10, modelo 2530-24-PoE+ (J9779A), gerenciável da camada 2 do modelo OSI.



Figura 10 - Switch HP 2530-24-PoE+ (J9779A)
Fonte: HPE (2015)

Este *switch* não possui *IP* padrão de fábrica para acessar a interface de configuração *Web*. Quando ele é conectado a rede, recebe um endereço *IP* através do servidor *DHCP* da rede. Logo para saber o *IP* é necessário visualizar os registros de eventos do servidor *DHCP* da rede.

Para criar uma *VLAN* no *switch* é necessário especificar *ID* e nome da *VLAN* e, as portas que farão parte da *VLAN* que está sendo configurada. A Figura 11 demonstra o exemplo de configuração da *VLAN* “FAMPERALUNO”, a *ID* e o nome desta *VLAN* estão especificados no Quadro 2 e, as portas podem ser visualizadas no Quadro 3, neste caso são: a porta 3, o qual está conectado o servidor *pfSense* e, as portas 19 até a 24, onde estão conectados os *APs*.

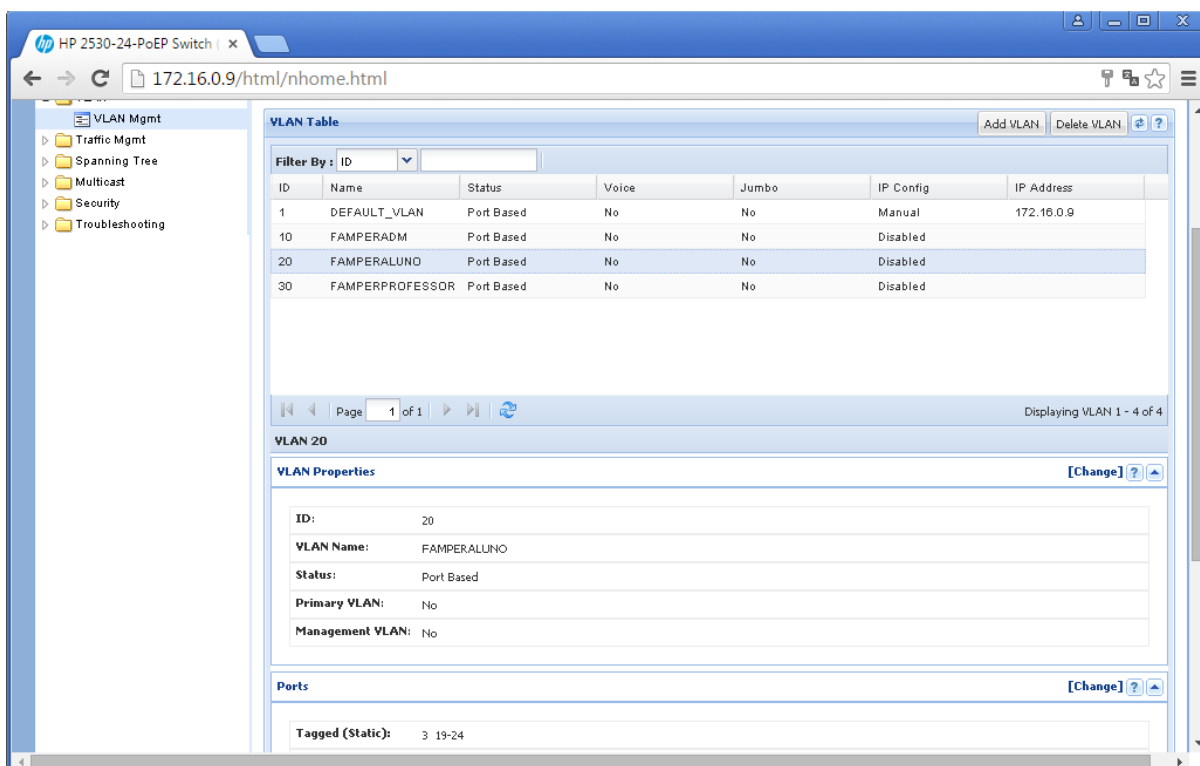


Figura 11 - Configuração da VLAN “FAMPERALUNO”, no Switch HP 2530-24-PoE+ (J9779A)
 Fonte: Interface Web de configuração do Switch HP 2530-24-PoE+ (J9779A)

3.2.3 PfSense

Diferente dos *APs*, onde são criadas as redes sem fio e, do *switch* gerenciável, onde são criadas as *VLANs*, o *pfSense*, além das *VLANs*, controla diversos recursos importantes, como: *firewall*, *proxy*, *DHCP* e o *captive portal*. Esta seção aborda resumidamente a instalação do *pfSense* e, em seguida as configurações dos recursos necessários.

3.2.3.1 Instalação

O servidor *pfSense* foi instalado em uma infraestrutura de servidores virtualizada, utilizando o *software* de virtualização *KVM (qemu)*, com as seguintes configurações:

- 2 GB de memória *RAM*.
- 4 processadores.
- 20 GB de disco.

- 2 interfaces de rede.

Foi utilizada a versão 2.2.4, última versão disponível na data da instalação. O processo de instalação é simples e guiado pelo assistente de instalação. Primeiramente a máquina virtual foi iniciada com a imagem de instalação do *pfSense*, o processo de *boot* ocorreu automaticamente, para iniciar a instalação foi pressionada a tecla “I”, conforme Figura 12.

```
Welcome to pfSense 2.2.4-RELEASE ...
Mounting unionfs directories...done.
Creating symlinks.....ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/local/lib
32-bit compatibility ldconfig path: /usr/lib32
done.
Launching the init system... done.
Initializing..... done.
Starting device manager (devd)...done.

[ Press R to enter recovery mode or ]
[ press I to launch the installer ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

(I)nstaller may be invoked now if you do
not wish to boot into the liveCD environment at this time.

(C)ontinues the LiveCD bootup without further pause.

Timeout before auto boot continues (seconds): 5
```

Figura 12 - Tela de *boot* para instalação do *pfSense*
Fonte: Instalação *pfSense* 2.2.4

O assistente de instalação copia os arquivos do *pfSense* para o disco e assim que concluir a instalação solicita permissão para reiniciar a máquina, conforme demonstrado na Figura 13. Depois que a máquina for reiniciada, já é possível iniciar as configurações do servidor.

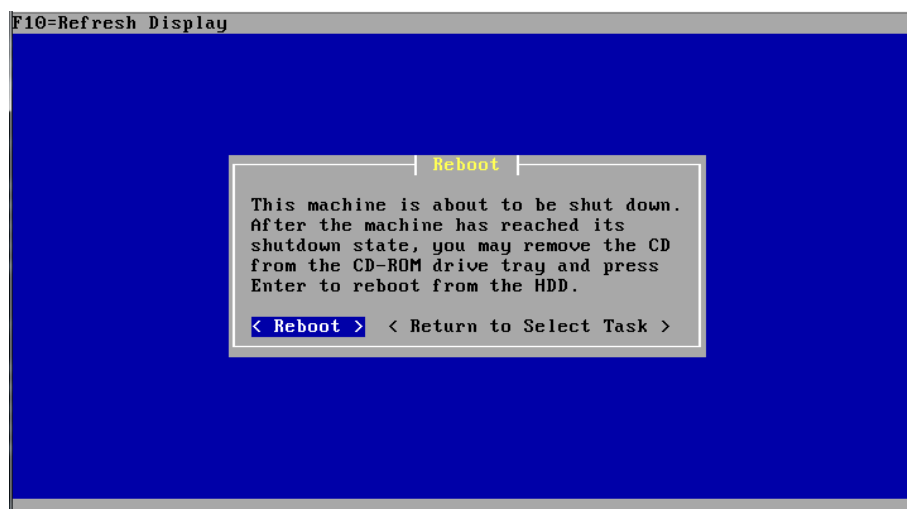


Figura 13 - Tela final da Instalação do *pfSense*
Fonte: Instalação *pfSense* 2.2.4

3.2.3.2 Configurações iniciais

No primeiro acesso da interface de *Web* do *pfSense*, conforme Figura 14, surge um assistente para auxiliar nas configurações básicas, como: nome do servidor, domínio, servidores *DNS*, configurações da interfaces *LAN* e *WAN*, etc.

The screenshot shows the 'General Information' configuration screen in the pfSense web interface. It includes the following fields and options:

- Hostname:** pfSense (EXAMPLE: myservser)
- Domain:** famper.local (EXAMPLE: mydomain.com)
- Primary DNS Server:** 8.8.8.8
- Secondary DNS Server:** 8.8.4.4
- Override DNS:** Allow DNS servers to be overridden by DHCP/PPP on WAN

A 'Next' button is located at the bottom right of the form.

Figura 14 - Assistente para configurações iniciais do pfSense
Fonte: Interface Web de configuração do pfSense 2.2.4

Na tela inicial do *pfSense* está o *dashboard*, visto na Figura 15. O *dashboard*, além de apresentar um resumo das configurações mais importantes, como endereço *IP* das interfaces, configuração do processador, *DNS*, dentre outros, fornece informações sobre utilização dos recursos do servidor e alerta sobre atualizações.

The screenshot shows the 'Status: Dashboard' page in the pfSense web interface. It displays various system and interface information:

- System Information:**
 - Name: pfSense.famper.local
 - Version: 2.2.4-RELEASE (amd64) built on Sat Jul 25 19:57:37 CDT 2015; FreeBSD 10.1-RELEASE-p15
 - Platform: pfSense
 - CPU Type: QEMU Virtual CPU version 1.5.3; 2 CPU(s); 2 package(s) x 1 core(s)
 - Uptime: 00 Hour 02 Minutes 07 Seconds
 - Current date/time: Thu Oct 29 6:59:09 BRST 2015
 - DNS server(s): 127.0.0.1, 8.8.8.8, 8.8.4.4
 - Last config change: Thu Oct 29 5:24:42 BRST 2015
 - State table size: 0% (203/98000); Show states
 - MBUF Usage: 4% (1020/26584)
 - Load average: 2.29, 1.23, 0.51
 - CPU usage: 0%
 - Memory usage: 13% of 389 MB
 - SWAP usage: 0% of 2047 MB
 - Disk usage: / (ufs): 4% of 9.7G; /var/run (ufs in RAM): 3% of 3.4M
- Interfaces:**
 - WAN: 1000baseT <-full-duplex> 172.16.0.16
 - LAN: 1000baseT <-full-duplex> 192.168.1.1

Figura 15 - Dashboard pfSense
Fonte: Interface Web de configuração do pfSense 2.2.4

3.2.3.3 VLANs

Assim como as VLANs foram adicionadas nos APs e no switch, deve-se criar também, no pfSense. Além de fornecer o nome e a ID para criar cada VLAN, agora é necessário configurar o endereço IP do servidor para cada VLAN. A Figura 16 demonstra o exemplo da VLAN “FAMPERALUNO”, o endereço IP foi baseado nas informações contidas no Quadro 2.

Interfaces: VLAN20

The screenshot displays the configuration page for a new interface named 'VLAN20'. It is divided into two main sections: 'General configuration' and 'Static IPv4 configuration'.

General configuration:

- Enable:** A checked checkbox labeled 'Enable Interface'.
- Description:** A text input field containing 'VLAN20'.
- IPv4 Configuration Type:** A dropdown menu set to 'Static IPv4'.
- IPv6 Configuration Type:** A dropdown menu set to 'None'.
- MAC address:** An empty text input field.
- MTU:** An empty text input field.
- MSS:** An empty text input field.
- Speed and duplex:** A dropdown menu set to 'Advanced'.

Static IPv4 configuration:

- IPv4 address:** A text input field containing '10.1.0.1' and a dropdown menu set to '23'.
- IPv4 Upstream Gateway:** A dropdown menu set to 'None'.

Figura 16 - Tela de configuração de VLAN
Fonte: Interface Web de configuração do pfSense 2.2.4

3.2.3.4 Firewall

São necessárias algumas liberações no firewall do pfSense para que seja possível a navegação Web e, acesso ao sistema acadêmico (Jacad). Na Figura 17 é possível visualizar as seguintes regras para a VLAN “FAMPERALUNO”:

- Permitir consultas ao DNS local, TCP/UDP 53 (DNS).
- Permitir navegação Web, porta TCP 80 (HTTP).

- Permitir navegação *Web* segura, porta TCP 443 (HTTPS).
- Permitir *ping* (ICMP) da rede local para o servidor *pfSense*.
- Permitir acesso ao destino sistema acadêmico da instituição (Jacad).

Firewall: Rules

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	▶	IPv4 TCP/UDP	VLAN20 net	*	jacad	*	none		jacad
<input type="checkbox"/>	▶	IPv4 TCP	VLAN20 net	*	*	80 (HTTP)	none		http
<input type="checkbox"/>	▶	IPv4 TCP	VLAN20 net	*	*	443 (HTTPS)	none		https
<input type="checkbox"/>	▶	IPv4 TCP/UDP	VLAN20 net	*	VLAN20 address	53 (DNS)	none		dns
<input type="checkbox"/>	▶	IPv4 ICMP	VLAN20 net	*	VLAN20 address	*	none		ping

Figura 17 - Regras de *firewall*
Fonte: Interface *Web* de configuração do *pfSense* 2.2.4

A rede “FAMPERADMINISTRATIVO” possui uma regra liberando a comunicação com a rede cabeada, conforme Figura 18, para que os funcionários que se conectarem nesta rede possam acessar recursos como impressoras e servidor de arquivos.

Firewall: Rules

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	▶	IPv4 *	VLAN10 net	*	172.16.0.0/16	*	none		liberando comunicação

Figura 18 - Regra de *firewall* liberando comunicação entre redes distintas
Fonte: Interface *Web* de configuração do *pfSense* 2.2.4

3.2.3.5 Captive portal

O *captive portal* realiza a autenticação e segurança das redes “FAMPERALUNO” e “FAMPERPROFESSOR”. O limite de velocidade de *download* e *upload* por usuário, também foi configurado no *captive portal*. O *captive portal* consulta as informações para autenticação em um servidor *RADIUS*, o qual possui os *logins* e senhas do sistema acadêmico, para acadêmicos e professores. A Figura 19 demonstra a configuração do *captive portal* para a rede “FAMPERALUNO”.

Per-user bandwidth restriction **Enable per-user bandwidth restriction**

Default download Kbit/s

Default upload Kbit/s

If this option is set, the captive portal will restrict each user who logs in to the specified default bandwidth. RADIUS can override the default settings. Leave empty or set to 0 for no limit.

Authentication

No Authentication

Local User Manager / Vouchers

Allow only users/groups with 'Captive portal login' privilege set

RADIUS Authentication

RADIUS Protocol

PAP

CHAP_MD5

MSCHAPv1

MSCHAPv2

Primary Authentication Source

Primary RADIUS server

IP address

Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.

Figura 19 - Configurações do *captive portal*
Fonte: Interface Web de configuração do pfSense 2.2.4

Ainda nas configurações do *captive portal*, é possível personalizar a tela que solicita autenticação ao usuário. Para a rede “FAMPERALUNO”, foi feito uma tela personalizada com o logotipo da Faculdade, conforme a Figura 20.



Rede sem fio para alunos da FAMPER
Internet disponibilizada para fins acadêmicos
Seu acesso poderá ser monitorado
Você deverá logar com o R.A. e senha do Jacad (Portal do Aluno)

Login (R.A.)

Senha

Figura 20 - Tela personalizada de autenticação do *captive portal*
Fonte: Autoria Própria

3.2.3.6 DHCP server

Para cada *VLAN* deverá ser habilitado um servidor *DHCP*, a fim de facilitar o acesso as redes *WiFi*, fornecendo as configurações da rede (endereço *IP*, *gateway*, *DNS*, etc.) automaticamente para quem se conectar. A Figura 21 demonstra a configuração do *DHCP* para a rede “FAMPERALUNO”

Services: DHCP server



WAN LAN VLAN10 **VLAN20** VLAN30

Enable DHCP server on VLAN20 interface

Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet 10.1.0.0

Subnet mask 255.255.254.0

Available range 10.1.0.1 - 10.1.1.254

Range to

Additional Pools If you need additional pools of addresses inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description

Figura 21 - Configuração do *DHCP* Server
Fonte: Interface *Web* de configuração do *pfSense* 2.2.4

3.2.3.7 Proxy

A rede “FAMPERALUNO” possui outra camada de segurança, um servidor *proxy* transparente. Este modelo de *proxy* não necessita ser configurado no navegador *Web*, pois ele intercepta as conexões, sem o usuário saber e, neste caso verifica se libera ou proíbe o acesso que está sendo solicitado. Na Figura 22, o *proxy* está configurado para proibir acesso aos sites: “www.uol.com.br” e “facebook.com”.

Blacklist

www.uol.com.br
www.facebook.com

Enter each destination domain on a new line that will be blocked to the users that are allowed to use the proxy. You also can use regular expressions.

Figura 22 - Configuração da lista de bloqueios do servidor *proxy*
Fonte: Interface *Web* de configuração do *pfSense* 2.2.4

4 RESULTADOS OBTIDOS

Agora quando um aluno se conecta a rede “FAMPERALUNO” e tenta acessar a Internet, surge a tela do *captive portal*, conforme demonstrado na Figura 23, solicitando para que o acadêmico faça autenticação para poder utilizar a Internet. O acesso só será liberado com *login* e senha válidos.



Figura 23 - Captive portal da rede “FAMPERALUNO”
Fonte: Autoria Própria

No teste de velocidade, visualizado na Figura 24, pode-se verificar que a velocidade está sendo limitada de acordo com as configurações para esta rede. Limite de 1 *Mega* para *download* e 1 *Mega* *upload*.

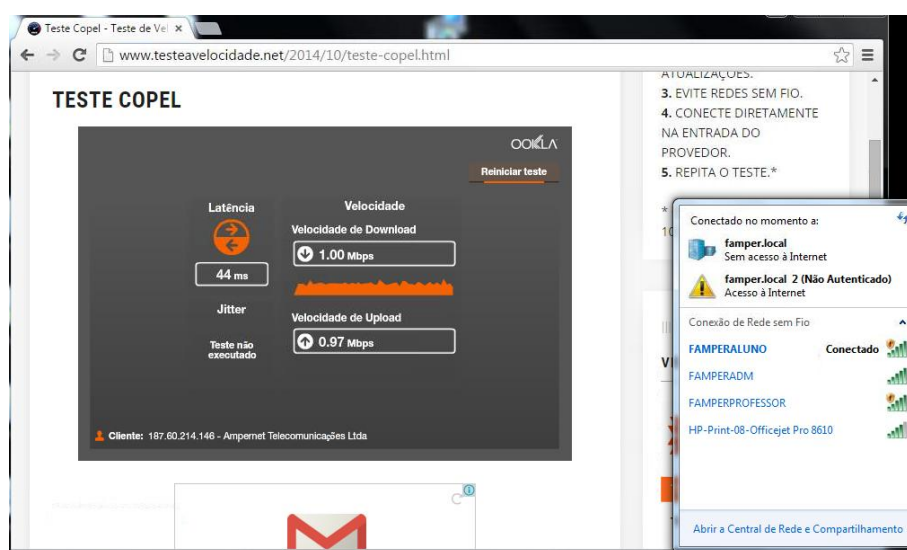


Figura 24 - Teste de velocidade
Fonte: www.testeavelocidade.net

A Figura 25 demonstra a tentativa de acesso ao servidor de arquivos do setor administrativo, verifica-se que a rede “FAMPERALUNO” não consegue enxergar a rede cabeada. Para a eficiência deste teste, o endereço *IP* da interface de rede sem fio, foi modificado para *IP* da rede cabeada.

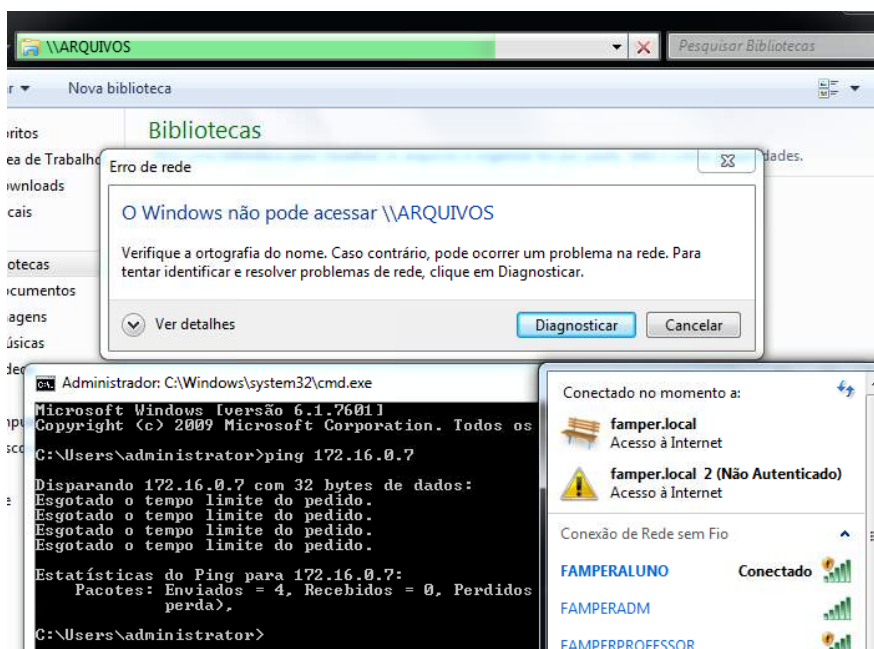


Figura 25 - Teste de acesso em outra rede
Fonte: Microsoft Windows 7

Outro teste efetuado foi para verificar a eficiência do *proxy* transparente. Conforme Figura 26, o usuário recebe uma mensagem dizendo que o site está bloqueado, quando tenta acessar o site “www.uol.com.br”.

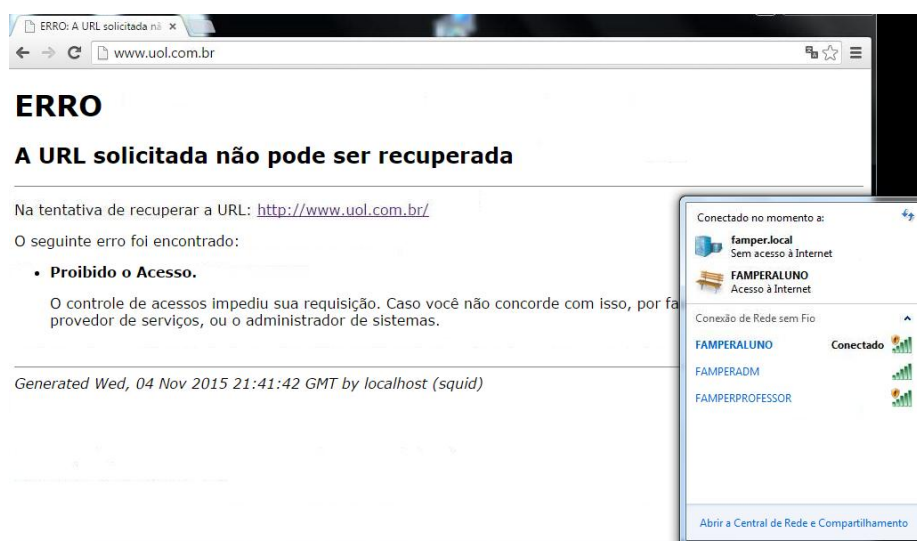


Figura 26 - Mensagem do bloqueio de site pelo *proxy*
Fonte: Proxy pfSense 2.2.4

Neste teste da eficiência do *proxy* transparente foi identificado um problema, pois, conforme a Figura 27, quando o usuário digitou no navegador Web "www.facebook.com", o site foi carregado.

O *Facebook* não foi bloqueado pelo *proxy*, pois ele utiliza o protocolo *HTTPS* e, o *proxy* transparente só atua no protocolo *HTTP*.



Figura 27 - Proxy transparente em site *HTTPS*
Fonte: www.facebook.com

5 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho foi motivado pela necessidade de solucionar problemas na rede de computadores de uma instituição de ensino superior. No decorrer deste trabalho foram apresentados problemas relacionados à segurança de redes e dificuldades que a Famper estava enfrentando para fornecer Internet, através da rede sem fio, aos acadêmicos e professores.

Foram vistos conceitos de redes de computadores, os quais auxiliaram na resolução dos problemas. Pode-se destacar o estudo de *VLANs*, o qual trouxe a solução para o problema de segurança relacionado a visibilidade dos computadores da instituição para todos que se conectavam a *WiFi*.

O *Captive Portal* em conjunto com o *proxy* transparente, outra solução importante estudada, resolveu dois problemas, a questão de segurança onde qualquer pessoa, mesmo não fazendo parte da instituição, mas que estivesse ao alcance do sinal da rede sem fio conseguia se conectar. Agora somente pessoas que fazem parte da instituição (acadêmicos devidamente matriculados, professores e colaboradores) conseguem utilizar a rede sem fio da Famper.

Outro problema resolvido é que, para utilizar a Internet, não existe mais a necessidade de configurar o *proxy* manualmente, agora o acesso ficou fácil, quando o usuário conectar na rede sem fio e, tentar acessar uma página na *Web*, surgirá o *Captive Portal*, solicitando a autenticação, o usuário deverá fornecer *login* e senha e, pronto, o acesso a Internet estará liberado.

Foi apresentado o *software pfSense*, escolhido para o gerenciamento dos serviços necessários para a nova estrutura de rede sim fio da instituição, pois além de ser uma ferramenta gratuita, ele possui recursos integrados, como: *Captive Portal*, *VLANs*, *firewall*, *proxy*, *DNS cache*, *servidor DHCP*, recursos estes, necessários para a solução dos problemas apresentados.

Atualmente a Famper possui mais segurança em sua rede, além de que ampliou e facilitou o acesso à rede sem fio para seus alunos e professores.

Para trabalhos futuros, sugere-se estudo em *proxy HTTPS* transparente, pois muitas páginas da *Web*, como por exemplo, páginas de bancos, páginas de *e-mail*, entre outras páginas, estão utilizando o protocolo *HTTPS* e, por isso não é possível bloquear todo tráfego neste protocolo. O *proxy HTTPS* é uma possível solução para o controle das páginas *Web* que utilizam este protocolo.

REFERÊNCIAS

ENGENIUS. Engenius. Disponível em: <<http://pt.engeniustech.com>>. Acesso em: 20 out. 2015.

FAMPER. Famper. Disponível em: <<http://www.famper.com.br>>. Acesso em: 25 out. 2015.

FERREIRA, R. E. **Linux: guia do administrador do sistema**. 2ª ed. São Paulo: Novatec Editora, 2008.

HPE. Hewlett Packard Enterprise. Disponível em: <<https://www.hpe.com/br/pt/home.html>>. Acesso em: 18 out. 2015.

KUROSE, J. F; ROSS, K. W. **Redes de computadores e a Internet: uma abordagem top-down**. 5ª ed. São Paulo: Addison Wesley, 2010.

MORAN, J. M. Internet no ensino. **Comunicação & Educação**, São Paulo, v. 5, n. 14, p. 17-26, jan./abr. 1999.

MORIMOTO, C. E. Expandindo a rede Wi-Fi com pontos de acesso adicionais. **Guia do Hardware**, jul.2011. Disponível em: <<http://www.hardware.com.br/tutoriais/expandindo-wifi/topologia.html>>. Acesso em: 19 out. 2015.

PFSENSE. pfSense. Disponível em: <<https://www.pfsense.org>>. Acesso em: 22 out. 2015.

SILVA, D. J. R. da. **Uso dos Dados de Contabilização do RADIUS para Faturamento e para Geração de Informações Gerenciais e Operacionais de Serviços em Banda Larga**. 2010. 156 f. Dissertação (Mestrado) – Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica. Brasília, 2010.

SOARES DE OLIVEIRA, S. **Procedimento para escolha de pontos de acesso de redes sem fio Wi-Fi indoor**. 2014. 156 f. Monografia (Graduação) – Escola de Engenharia de São Carlos da Universidade de São Paulo. São Paulo 2014.

STATO FILHO, A. **Linux - controle de redes**. 1ª ed. Florianópolis: Visual Books, 2009.

TANENBAUM, A. S; WETHERALL, D. **Redes de computadores**. 5ª ed. São Paulo: Pearson Prentice Hall, 2011.