ENGENHARIAS ELÉTRICA E DE COMPUTAÇÃO:

O TERCEIRO PILAR

LILIAN COELHO DE FREITAS
(ORGANIZADORA)

Atena Editora
Ano 2021

ENGENHARIAS ELÉTRICA E DE COMPUTAÇÃO:

O TERCEIRO PILAR

LILIAN COELHO DE FREITAS
(ORGANIZADORA)

Atena Editora
Ano 2021

Editora chefe
Profª Drª Antonella Carvalho de Oliveira
Editora executiva
Natalia Oliveira
Assistente editorial
Flávia Roberta Barão
Bibliotecária
Janaina Ramos
Projeto gráfico
Camila Alves de Cremo
Luiza Alves Batista
Maria Alice Pinheiro
Natália Sandrini de Azevedo
Imagens da capa
iStock
Edição de arte
Luiza Alves Batista

Atena Editora
Ano 2021

Atena Editora
Ano 2021

Ciências Exatas e da Terra e Engenharias

Engenharias elétrica e de computação: o terceiro pilar

Diagramação: Camila Alves de Cremo
Correção: Mariane Aparecida Freitas
Indexação: Gabriel Motomu Teshima
Revisão: Os autores
Organizadores: Lilian Coelho de Freitas

Dados Internacionais de Catalogação na Publicação (CIP)

E57 Engenharias elétrica e de computação: o terceiro pilar / Organizadora Lilian Coelho de Freitas. – Ponta Grossa - PR: Atena, 2021.

Formato: PDF
Requisitos de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia
ISBN 978-65-5983-543-0
DOI: https://doi.org/10.22533/at.ed.430213009

1. Engenharia elétrica. 2. Computação. I. Freitas, Lilian Coelho de (Organizadora). II. Título.

CDD 621.3

Elaborado por Bibliotecária Janaina Ramos – CRB-8/9166

Atena Editora
Ponta Grossa – Paraná – Brasil
Telefone: +55 (42) 3323-5493
www.atenaeditora.com.br
contato@atenaeditora.com.br

Atena Editora
Ano 2021

DECLARAÇÃO DOS AUTORES

Os autores desta obra: 1. Atestam não possuir qualquer interesse comercial que constitua um conflito de interesses em relação ao artigo científico publicado; 2. Declaram que participaram ativamente da construção dos respectivos manuscritos, preferencialmente na: a) Concepção do estudo, e/ou aquisição de dados, e/ou análise e interpretação de dados; b) Elaboração do artigo ou revisão com vistas a tornar o material intelectualmente relevante; c) Aprovação final do manuscrito para submissão.; 3. Certificam que os artigos científicos publicados estão completamente isentos de dados e/ou resultados fraudulentos; 4. Confirmam a citação e a referência correta de todos os dados e de interpretações de dados de outras pesquisas; 5. Reconhecem terem informado todas as fontes de financiamento recebidas para a consecução da pesquisa; 6. Autorizam a edição da obra, que incluem os registros de ficha catalográfica, ISBN, DOI e demais indexadores, projeto visual e criação de capa, diagramação de miolo, assim como lançamento e divulgação da mesma conforme critérios da Atena Editora.

Atena Editora
Ano 2021

DECLARAÇÃO DA EDITORA

A Atena Editora declara, para os devidos fins de direito, que: 1. A presente publicação constitui apenas transferência temporária dos direitos autorais, direito sobre a publicação, inclusive não constitui responsabilidade solidária na criação dos manuscritos publicados, nos termos previstos na Lei sobre direitos autorais (Lei 9610/98), no art. 184 do Código Penal e no art. 927 do Código Civil; 2. Autoriza e incentiva os autores a assinarem contratos com repositórios institucionais, com fins exclusivos de divulgação da obra, desde que com o devido reconhecimento de autoria e edição e sem qualquer finalidade comercial; 3. Todos os e-book são *open access, desta forma* não os comercializa em seu site, sites parceiros, plataformas de *e-commerce,* ou qualquer outro meio virtual ou físico, portanto, está isenta de repasses de direitos autorais aos autores; 4. Todos os membros do conselho editorial são doutores e vinculados a instituições de ensino superior públicas, conforme recomendação da CAPES para obtenção do Qualis livro; 5. Não cede, comercializa ou autoriza a utilização dos nomes e e-mails dos autores, bem como nenhum outro dado dos mesmos, para qualquer finalidade que não o escopo da divulgação desta obra.

Atena Editora
Ano 2021

APRESENTAÇÃO

Os avanços na pesquisa científica em Engenharias Elétrica e de Computação tem revolucionado nossa vida em sociedade. Conexões cada vez mais rápidas, processadores super velozes e a autonomia dos sistemas decorrentes do progresso em Inteligência Artificial são alguns exemplos de aplicações em nosso dia-a-dia.

Este e-book torna acessível os resultados da pesquisa científica realizada por diversos pesquisadores do país. Ao decorrer dos capítulos, apresenta-se aplicações práticas de inteligência artificial, gerência de redes e técnicas de otimização. Aproveite esse momento para aprimorar seus conhecimentos.

Desejo aos autores, meu mais sincero agradecimento pelas significativas contribuições, e aos nossos leitores, desejo uma proveitosa leitura, repleta de boas reflexões.

Lilian Coelho de Freitas

SUMÁRIO

CAPÍTULO 4

SERVIDOR DE GERÊNCIA DE REDE

Data de aceite: 01/09/2021

Roger Robson dos Santos
Pontifícia Universidade Católica do Paraná (PUCPR)

Jackson Mallmann
Instituto Federal Catarinense (IFC Brusque)

RESUMO: Este artigo conta com a descrição de ferramentas focadas na gerência de um servidor de rede em um ambiente corporativo, visando assim um melhor controle de toda a estrutura, gerando maior segurança e confiabilidade para a empresa. Com o passar dos anos, o ataque as redes vêm crescendo cada vez mais, e um bom gerenciamento da rede é primordial dentro de um ambiente corporativo. O objetivo é demonstrar a implementação de ferramentas de redes, que se aplicam para um melhor gerenciamento em grande parte de ambientes corporativos e assim poder demonstrar que o uso de softwares livres, podem trazer ótimos resultados para as empresas com um baixo custo.
PALAVRAS-CHAVE: Servidor, segurança, serviços.

ABSTRACT: This article has the description of tools focused on the management of a network server in a corporate environment, aiming at a better control of the entire structure, generating greater security and reliability for the company. Over the years, attacking networks have been growing more and more, and good network management is paramount within a corporate environment. The goal is to demonstrate the implementation of network tools, which apply to better management in large part of corporate environments and thus to demonstrate that the use of free software, can bring great results for companies with a low cost.
KEYWORDS: Server, security, services.

1 | INTRODUÇÃO

A informática é apresentada como uma ferramenta para auxiliar nos trabalhos diários das empresas e garantir a segurança. Além disso, é uma ferramenta capaz de prover uma conectividade entre as pessoas da própria empresa, tanto em um meio interno, quanto externo. Com isso, temos a segurança de redes para garantir uma melhor segurança de todo o ambiente. Para isso se deve traçar um planejamento de toda estrutura de rede e servidores para se ter uma melhor segurança do ambiente e procurar adequar ao máximo dentro dos orçamentos dispostos pela empresa. Neste planejamento temos como foco todos os equipamentos necessários e os *softwares* para ter o melhor aproveitamento do *hardware* de baixo custo garantindo a segurança da empresa com a utilização de ferramentas (*softwares*) livres. Em nosso meio, utilizamos como estudo de caso uma empresa leiloeira. Problemas na estrutura de rede que causavam problemas durante a transmissão ao vivo do leilão, ocorrendo diversas quedas do sistema. Os

serviços de rede sempre instáveis e sem confiança, paravam de funcionar inesperadamente, e para quem acompanha o leilão *online* isso causa quedas na conexão deixando o serviço do leilão inativo ou com grandes lentidões. Entretanto, para a empresa leiloeira, a maior necessidade é uma transmissão de áudio ao vivo para um melhor aproveitamento do leilão e por ter uma alta demanda de compradores (usuários) *online*. Com estes problemas, buscamos a implantação de uma nova estrutura de rede para solucionar estes problemas, onde possibilita um total gerenciamento do sistema durante os leilões, trazendo a confiança nos serviços hospedados localmente e implantando a transmissão de áudio ao vivo. Como a empresa já possui um parque de *hardware* com bom potencial, foi decidido pela estrutura local, pelo melhor gerenciamento e suporte. Com isso foi desenvolvido servidor de internet, arquivos e *streaming* de áudio ao vivo para o novo ambiente, utilizando máquinas virtuais, onde os servidores utilizam sistema Linux e para utilização, foi aplicado máquinas com ambiente Windows para os testes das funções. Implantamos serviço de Firewall, Squid, DHCP, DNS, Icecast2 e Samba com (AD) *Active Directory*. Ademais, com toda estrutura de gerenciamento da nova rede, esperamos ter como resultado, uma confiabilidade nos serviços oferecidos pela empresa leiloeira, maior agilidade nos processos e um melhor controle da rede. Além de todo gerenciamento, espera-se ter um bom aproveitamento da transmissão ao vivo dos leilões, onde é uma grande necessidade da empresa, devido à alta demanda de compradores *online*. Por fim, a motivação para a realização deste trabalho sobre a administração de rede de computadores é demonstrar com as boas práticas de utilização das ferramentas necessárias, pode-se tornar o ambiente da internet dentro das empresas mais confiáveis através da aplicação de *softwares* (ferramentas) públicas.

2 | ESTADO DA ARTE

2.1 Introdução a História da Internet

A internet é uma ferramenta que se tornou dependência na vida das pessoas, seja para o trabalho, lazer, e outras coisas. A internet surgiu durante a Guerra Fria nos Estados Unidos cobrindo a necessidade da comunicação entre as bases americanas em 1945. Quando se iniciou, se chamava ARPNET, nome derivado da empresa que a desenvolveu (*Advanced Research and Projects Agency*) [STALLING 2007]. Membros da MIT (*Masschusetss Instite of Technology*) tiveram uma ideia: converter toda a linguagem da ARPANET para uma linguagem mais humana. Com isso desencadeou os primeiros conhecedores de informática, conhecidos como *hackers*, que foram capazes de criarem e desenvolverem os primeiros compiladores da época até chegar os compiladores atuais [STALLING 2007]. Com o passar dos anos começaram a nascer problemas de invasões em redes de internet nas organizações, com isso em 1994 a IAB (*Internet Architecture Board*) começou a emitir relatórios de arquitetura de internet. Mostrando assim que havia

a necessidade de melhorar a segurança da internet. Para se ter uma ideia, na Figura 1 é apresentado gráfico com incidentes relatados durante os anos de 1999 até 2015.

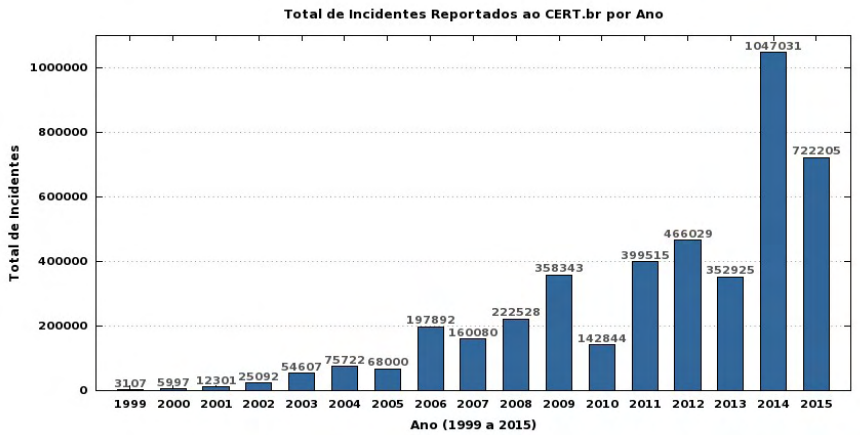

Figura1 - Gráfico de total de incidentes reportados ao CERT.br por ano.
Retirado em https://www.cert.br/stats/incidentes/ retirado 27/02/2017.

2.2 Invasores e Serviços de Segurança

Hackers são pessoas que constroem ferramentas que auxiliam e facilitam o trabalho dos usuários. Normalmente os *hackers* costumam ter uma ideia de que o acesso à rede da internet deve ser ilimitado com o objetivo do autoconhecimento. Em meio a isso, *hackers* cometem crimes de invasões a certos lugares, com o intuito de corrigir problemas que os técnicos das organizações desconhecem, ajudando os mesmos a evitar ataques por meio de crackers [FILHO 2010]. Por sua vez, *crackers* são opostos aos *hackers*. Eles têm apenas o entendimento utilizado para o mal, utilizam suas habilidades técnicas e ferramentas com intuito de destruir uma rede, piratear programas, jogos e entre outros, e ainda a construção de vírus capazes de destruir todas as informações de uma rede [FILHO 2010].

Entre alguns serviços de segurança podemos contar com o serviço de autenticação de dados, onde se faz com que a segurança de alguns serviços importantes realize a autenticação dos dados durante uma comunicação, seja ela uma entidade par onde é um serviço utilizado durante uma comunicação ou em fase de transferência de dados. Além desta autenticação utiliza-se também a autenticação de origem de dados ao qual provê a confirmação da origem dos dados. A autenticação nos assegura que a entidade ao qual estamos se comunicando, é realmente aquela que afirma ser [STALLING 2007]. Outro serviço importante é o controle de acesso. Ele impede que o uso não autorizado de algum recurso dentro da organização trabalhe com a instrução de confidencialidade, ou seja, assegura que não haja divulgação dos dados não autorizados e garantindo a proteção de

dados durante a conexão e mesmo em uma conexão de um arquivo local [STALLING 2007]. Além dos serviços citados, existe o serviço de integridade de dados. Ele garante que os dados recebidos durante uma conexão estejam exatamente como foram enviados de uma entidade, sem que haja modificação, inserção, exclusão ou repetição de dados [STALLING 2007]. Ademais, a irretratabilidade é um serviço que oferece uma proteção contra imposição ou negação das entidades envolvidas em uma comunicação. É assegurado que a origem da mensagem prove ao seu destino que sua mensagem foi recebida por quem enviou sem nenhuma ocorrência de desvio durante o caminho até quem vai receber [STALLING 2007]. Por fim, a realização do projeto será baseada na arquitetura apresentada na Figura 2.

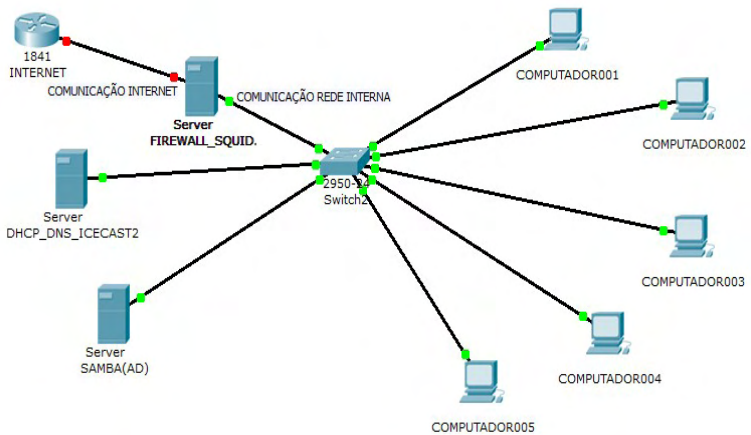

Figura2 - Fluxograma de computadores.

A rede irá possuir três servidores seguindo as seguintes regras: o principal servidor de internet contendo os serviços de Firewall com NetFilter IPTABLES para cuidar da segurança utilizando um conjunto de regras criadas pelo administrador da rede, e Squid com Proxy Transparente, um serviço para restringir acessos indevidos e armazenar em *cache* páginas já navegadas na rede agilizando a requisição destas páginas, um segundo servidor contendo o serviço de DHCP para que seja definido todas as máquinas no mesmo protocolo de comunicação TCP/IP usando Ipv4. Este servidor também contará com serviço de DNS para resolução de nomes dos *sites* de forma localmente. Também teremos o servidor Samba contendo o serviço de AD e *streaming* de áudio com Icecast. E para entendermos o funcionamento dos servidores, faz-se uma breve explicação de cada serviço.

2.3 Firewall

É uma ferramenta de segurança baseada em *hardware* e *software*, que junto de

um conjunto de regras e instruções, analisa o tráfico de rede durante a transmissão e recepção de dados. Neste trabalho, o firewall será construído com o pacote NetFilter Iptables, uma ferramenta que cria e administra através de regras filtrando pacotes na rede [NETO 2004]. O Iptables poderá funcionar baseado em endereços, portas de origem e destino dos pacotes e prioridade, além disso, ele funcionará a partir da comparação de regras para saber se um pacote possui ou não permissão para passar. No firewall será possível restringir e registrar tudo que estiver acontecendo na rede através de diversos *logs* gerados pelo Iptables. Entre os principais objetivos do Iptables: redirecionamentos de portas e serviços, a troca de protocolos (um exemplo ssl3 para tls1), criar regras com intuito de bloquear serviços, usuários da rede, acessos por determinado IP, liberações de navegação, entre muitos outros serviços [NETO 2004].

2.4 Squid

É uma ferramenta utilizada com diversos objetivos, principalmente impor regras de restrição de acesso baseadas no endereço IP da máquina, login, horário e bloqueio de conteúdos indevidos. Além disso, ele possui um *cache* de navegação onde é capaz de armazenar todas as páginas e arquivos já acessados em uma memória e quando alguém acessar uma página que já foi carregada. O Proxy envia os dados que armazenou no *cache*, sem a necessidade de baixar arquivos da mesma página repetidamente. Isso gera uma grande economia de banda e torna o acesso mais rápido sem a necessidade de um investimento com uma conexão rápida de internet [WESSELS 2004]. Hoje em dia, muitos *sites* costumam ter um conteúdo dinâmico em suas páginas onde mudam muitas coisas na página em cada visita do usuário.

Mesmo assim, o Proxy ainda é uma forte ferramenta, vendo que conteúdo de HTML e animações não mudam e acabam sendo reaproveitados pelo Proxy [MORIMOTO 2006]. Outra vantagem na utilização do Proxy é o fato do Squid armazenar todos os acessos dando possibilidade ao administrador da rede ver quem acessou, o que acessou e em quais horários acessou [MORIMOTO 2006]. Na configuração do Squid mais simples é necessário adicionar o Proxy máquina a máquina tornando pouco vantajoso todo esse trabalho, mas existe uma forma simples de resolver tudo isso: Proxy Transparente. Com isto não existe a necessidade de colocar o Proxy no navegador dos usuários. Uma conexão compartilhada via NAT, com a mesma configuração básica nos clientes. Para isso é criado uma regra no firewall que faz com que toda navegação na porta 80 seja redirecionada ao Squid passando automaticamente através do Proxy, sem que se precise fazer nenhuma configuração adicional aos seus clientes [MORIMOTO 2006].

2.5 *Dynamic Host Configuration Protocol* (DHCP)

É um recurso essencial para distribuir dinamicamente endereços IP e parâmetros de rede. Com este serviço as implementações de redes em Ipv4 e Ipv6 apresentam as

mesmas funcionalidades básicas, mas com significativas diferenças nas opções que podem ser enviadas [ALMEIDA 2000]. O DHCP possibilita uma maior segurança na configuração da rede, pois evita erros causados pela necessidade de digitação manual de valores em cada computador. Além disso, o DHCP ajuda a impedir conflitos de endereço IP na rede causados por um endereço atribuído anteriormente, ou que já esteja sendo utilizado por outro computador na rede, mantendo assim um melhor gerenciamento da rede. Usar servidores DHCP pode diminuir bastante o tempo gasto na configuração e reconfiguração de computadores da rede [TECHNET 2017]. Por exemplo, um cliente, termo utilizado para descrever um computador ligado à rede que obtém as configurações do protocolo TCP/IP a partir de um servidor DHCP, onde qualquer computador ou dispositivo de rede seja capaz de se comunicar com o servidor DHCP e obter as configurações do TCP/IP, é considerado um cliente DHCP. Segundo a RFC 2132, publicado pela Internet *Engineering Task Force* – IETF, cliente DHCP é considerado qualquer equipamento que ofereça suporte e seja compatível com o comportamento de cliente DHCP [BATTISTI 2013].

2.6 *Domain Name System* (DNS)

É um serviço de resolução de nomes e domínios em um banco de dados distribuído. Permite-se um controle total dos seguimentos que estejam disponíveis em toda a rede através de um sistema de cliente-servidor, ou seja, um computador pessoal que faz uma pergunta a outro computador que por sua vez se encarrega de encontrar a informação que você precisa [CAMPOS 2017].

> 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 distribuídos para implementar esse esquema de nomenclatura (TANEMBAUM 2003, p.617).

Com o serviço DNS é possível efetuar o acesso a *sites* sem a necessidade de saber o seu endereço IP, bastando apenas saber o nome deste *site*. Todo este trabalho de tradução do nome de domínio para o endereço IP é efetuado pelo protocolo DNS. Além da resolução de nomes externos, o DNS pode ser utilizado como ferramenta para poder definir nome a diversos dispositivos dentro da rede, facilitando que sejam encontrados esses aparelhos através dos nomes e não mais apenas pelos seus endereços de IP [CAMPOS 2017].

2.7 Samba

Segundo SILVA (2005), o Samba é um conjunto de ferramentas em um servidor, que permite a comunicação entre máquinas executando Linux e Windows, possibilitam o compartilhamento de arquivos, diretórios e impressão através do protocolo SMB (*Server Message Block*) e pode atuar como um PDC (*Primary Domain Controller*), autenticando assim usuários de redes locais [MORIMOTO 2006]. O Samba foi através deste protocolo para resolver os problemas de comunicação entre um sistema UNIX e um MS DOS, pois

para se ter esta comunicação, se fez necessário o uso da interface NetBIOS (*Network Basic Input Output Sustem*) [MORIMOTO 2006]. Toda a configuração do Samba é centralizada no arquivo smb.conf. O smb.conf pode ser visto como dividido em três partes: a configuração do servidor Samba (parâmetros na seção [*global*]), a configuração dos diretórios/pastas pessoais dos usuários (parâmetros na seção [*homes*]) e as demais seções que correspondem aos diretórios compartilhados [ZUCARINO 2001].

2.8 AD (*Active directory*)

O AD tem como principal função ser um único diretório, onde ao invés do usuário possuir várias senhas para cada tipo de serviço disponível na rede (e-mail, sistema da empresa, *logar* no computador), o usuário poderá ter apenas uma senha para acessar todos os recursos disponíveis na rede [SANTANA 2014]. Em um ambiente de TI corporativo, o serviço de AD é muito utilizado, sendo o centro para implementação de Serviços de Diretório. O AD gerencia os recursos da rede, armazenando informação sobre os recursos disponíveis. Com isso facilita a pesquisa e a autenticação [STANEK 2009]. O AD utiliza vários protocolos para seu funcionamento, mas segundo STANEK (2009), "o protocolo principal para acesso ao AD é o LDAP (*Lightweight Directory Access Protocol*), um protocolo padrão do setor para acesso a diretórios administrativos através do TCP/IP". Para o funcionamento do AD é necessário ter o serviço de DNS disponível na rede, pois o AD utiliza do DNS para nomeação dos recursos, e para resolução de nomes na rede [SANTANA 2014].

2.9 Icecast2

É um servidor de *streaming* de áudio e vídeo, que suporta as extensões Mp3, Opus, WebM e Ogg. Pode ser utilizado para criar estações de rádio na internet ou uma transmissão ao vivo de eventos e entre outros. Possibilita novos formatos a serem adicionados com relativa facilidade e suporta padrões abertos para comunicação e interação [PERMALINK 2015].

3 I DESENVOLVIMENTO

Neste trabalho aplica-se o Oracle VM Virtualbox 5.1.2, para implementação do projeto em cinco máquinas virtuais. Tem-se três máquinas virtuais com sistema operacional Debian e duas máquinas com sistema operacional Windows XP. Os arquivos de configurações estão disponíveis[1].

1 https://drive.google.com/drive/folders/1tRpo6Z7IDWjYJOW1x1NvaGorA0XmyELt?usp=sharing

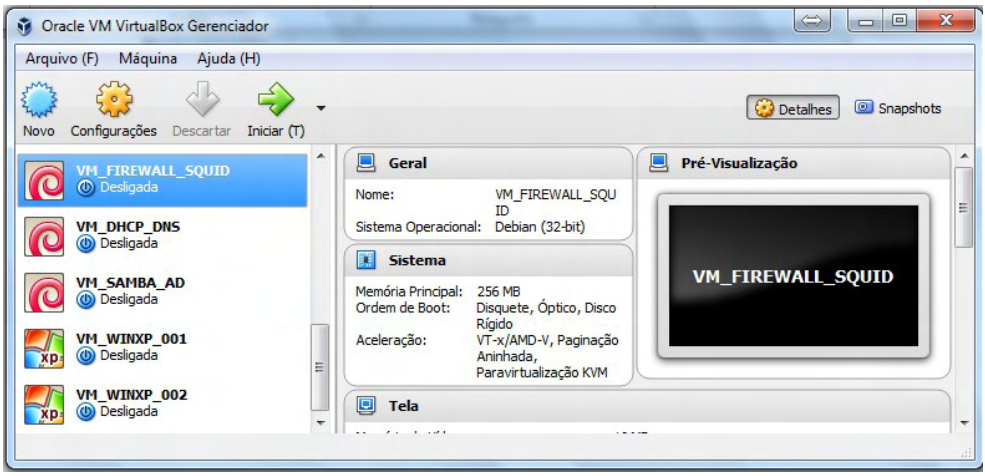

Figura3 – Interface web VirtualBox 5.1.2.

3.1 Configurações do Firewall

A configuração do firewall fica no arquivo /etc/init.d/firewall.sh, sendo que é descrito cada regra contida no firewall conforme a representação da rede. Por fim, para iniciar o serviço utilize o comando /etc/init.d/firewall.sh.

3.2 Configurações do Squid3

Configurando arquivo de configuração /etc/squid3/squid.conf. Para finalizar e iniciar o Proxy, utilize o comando /et c/init.d/squid3 start.

3.3 Configurações do DHCP

Configurando o arquivo de configuração /etc/dhcp/dhcpd.conf. Após, iniciar o serviço com o comando /etc/init.d/isc-dhcp-server start.

3.4 Configurações do DNS

Iniciando configuração dos arquivos de configuração do Bind9. Iniciar o serviço com o comando /etc/init.d/bind9 start.

3.5 Configuração do Icecast2

Para finalizar e iniciar o serviço, utilizar o comando /etc/init.d/icecast2 restart.

3.6 Configurações Samba - AD

Após, configuração da placa de rede em /etc/network/interfaces para iniciar a configuração do serviço.

4 | REALIZAÇÃO DOS TESTES

Para realizações de testes foi verificado se todas as configurações estavam corretas. Para tal, abra o CMD via o iniciar do Windows, e digite “ipconfig /all”. Desta forma, obtém-se todas as configurações de rede. Endereço do gateway deve ser o IP onde está o firewall 192.168.0.1, servidor DHCP deve ser 192.168.0.2 e os servidores DNS o endereço do servidor com o AD 192.168.0.3.

Sufixo DNS específico de conexão: redevirtual.local .int

Endereço de IP: 192.168.0.100

Máscara de Sub-rede: 255:255.255.0

Gateway padrão: 192.168.0.1

Servidores DHCP: 192.168.0.2

Servidor DNS: 192.168.0.3

Realizar testes de Ping (Figura 5) para verificar a comunicação com os servidores da rede, e observar se todos estão respondendo pelo próprio IP e respondendo pelos nomes definidos nas configurações do DNS.

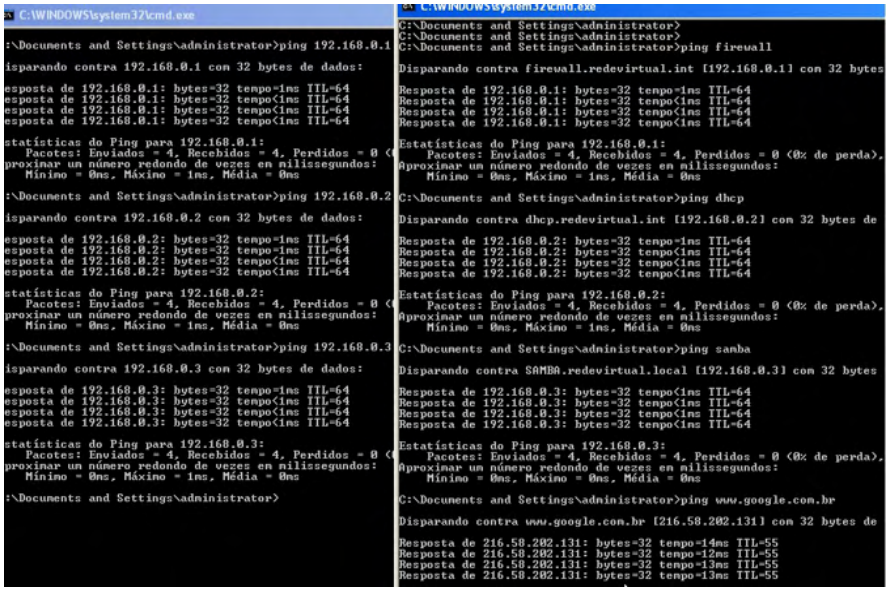

Figura5 – Testes de Ping.

Realizar alguns testes de navegação para verificar as funcionalidades do Proxy dentro da rede (Figura 6). Verificar se os bloqueios dentro da rede estão funcionando corretamente.

Figura6 – Testes de bloqueio do Proxy.

Testes de verificação da tela web do Icecast2 e verificações de acesso através do nome:porta(icecast:8000) configurados no servidor de DNS. Figura 7.

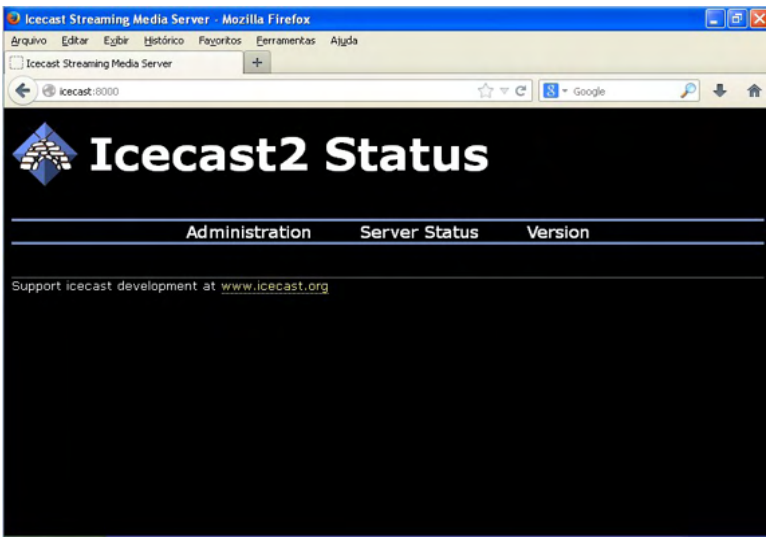

Figura7 – Interface Web do icecast.

Testes de criação de usuário no AD gerenciados pelo Windows (Figura 8).

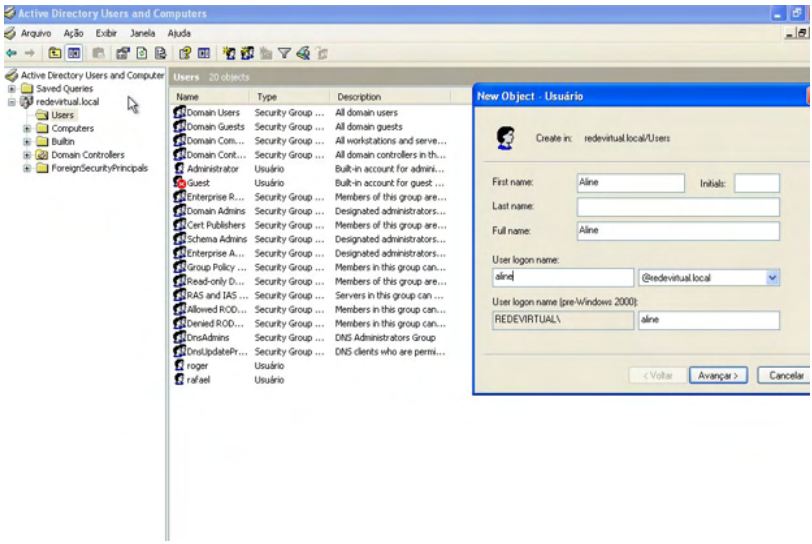

Figura8 – Interface de configuração de usuários do AD.

Realizando testes nas diretivas do AD (Figura 9).

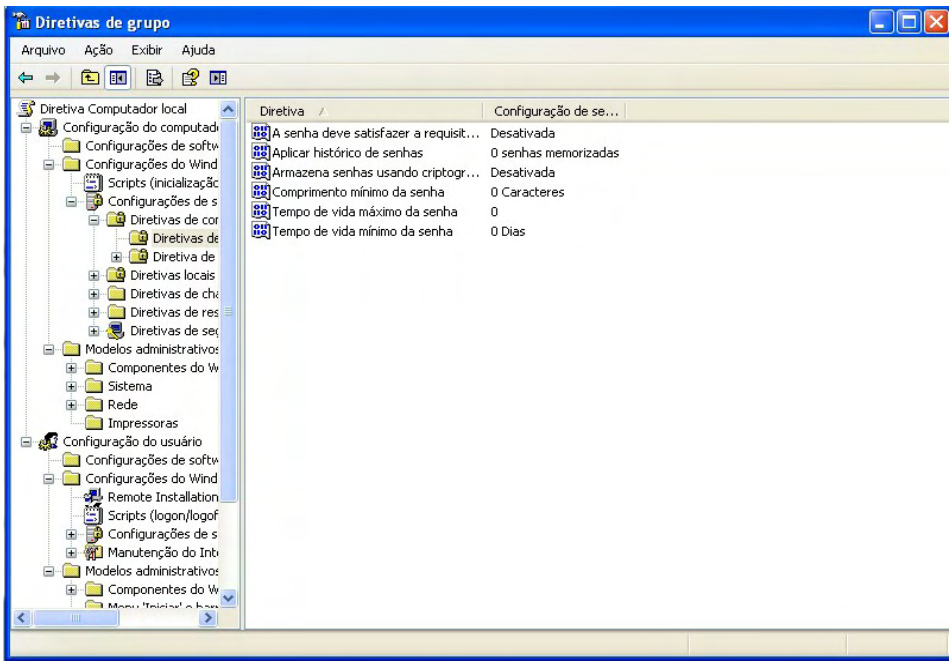

Figura9 – Interface configurações das Diretivas de grupo do AD.

5 | RESULTADOS OBTIDOS

Com a implementação destes servidores será obtido um enorme resultado em tudo que foi planejado e esperado para o ambiente de trabalho. Através das regras do Iptables será possível compartilhar internet com a rede, bloquear portas e evitar perigos da internet, liberar portas necessárias para o trabalho com segurança, ativar acessos externos para serviços específicos dentro da rede e entre outros. Por sua vez, aplicando o Squid será proporcionado uma grande economia de banda de internet na organização, já que os principais *sites* navegados terão suas sintaxes armazenadas no *cache* do Proxy, bloqueios de URL indevidas garantindo a segurança da organização e gerando logs necessários para o aprimoramento da rede. O DHCP proporciona a configuração da rede para que todas as máquinas sejam configuradas de forma automática e fácil, atribuindo o IP, máscaras de rede, gateway e DNS. Além do DHCP, o serviço do DNS irá proporcionar um trabalho de resolução de nomes da internet e da rede interna localmente muito interessante, pois com essa resolução é possível economizar banda de internet sem a busca de resoluções de nomes em algum DNS externo. Agora também poderemos contar com a transmissão ao vivo dos serviços da empresa no próprio *site*, ou em outros domínios com o Icecast. Com o serviço do AD, poderemos armazenar e acessar facilmente arquivos da empresa em qualquer máquina dentro da rede utilizando apenas uma conexão de rede com o servidor.

6 | CONCLUSÃO

É importante trabalhar com um risco reduzido e segurança dentro da organização, garantindo integridade de arquivos e dados, pois esta implementação é necessária devido ao crescimento e avanço da tecnologia e técnicas de segurança de rede. O objetivo deste trabalho foi demonstrar a implementação de serviços de segurança para toda a rede garantindo a eficácia em diversos ambientes corporativos com ferramentas livres, garantindo e convencendo as empresas que o *software* gratuito proporciona vantagens devido à alta qualidade e o baixo custo. Assim, este artigo envolveu o estudo da programação de redes de computadores, configurações de servidores Firewall, Proxy, DHCP, DNS, *Streamings* de Áudio, compartilhamento de arquivos de rede. O resultado disto proporciona um enorme aprendizado na área de Redes de Computadores.

7 | REFERÊNCIAS

ALMEIDA, Rubens Queiroz de. **Domain Name Service Configuração e Administração.** Disponível em < http://www.inf.ufes.br/~zegonc/material/Redes_de_Computadores/Apostila%20DNS%20Rubens%20Queiroz.pdf>. Acesso em 23 de julho de 2021.

BATTISTI, Julio. "**Introdução ao DHCP 2013"**. Disponível em: <http://juliobattisti.com.br/artigos/windows/tcpip_p9.asp>. Acessado em 05 de março 2017.

CAMPOS, David Robert Camargo de. **Introdução a DNS & DNSSEC.** 2017. Disponível em <https://ftp.registro.br/pub/doc/introducao-dns-dnssec.pdf>. Acesso em 23 de julho de 2021.

FILHO, Glenio Leitão Marques. "**Hackers e Crackers na internet: as duas faces da moeda 2010**". Disponível em: <www.insite.pro.br>. Acessado em 05 de março 2017.

MORIMOTO, Carlos E. **"Linux Redes e Servidores – Guia prático".** 2006.

NETO, Urubatan. **Dominando Linux Firewall Iptables.** Rio de Janeiro: Editora Ciência Moderna LTDA. 2004.

PERMALINK. "**Epirat**". Disponível em: <http://icecast.org/>. Acessado 05 março 2017.

SANTANA, Fabiano. "**AD – Active Directory 2014**". Disponível em: http://juliobattisti.com.br/fabiano/artigos/activedirectory.asp. Acessado em 05 de março 2017.

STALLING**,** Willian. **Criptografia e segurança de redes, Princípios e prática**, 4°Edição, 2007. Editora O'Reilly.

STANEK, Willian R. (2009). "**Windows Server 2008: guia completo**", Porto Alegre: Bookman.

TANEMBAU, Andrew S. "**Redes de Computadores"**. Tradução Vandenberg D. de Souza. 4. ed. Campus, 2003.

TECHNET. "**Microsoft. Visão geral do DHCP"**. Disponível em: https://technet.microsoft.com/pt-br/library/cc731166(v=ws.11).aspx. Acessado em 05 de março 2017.

ZUCARINO, Victor. "**Utilizando o SAMBA - Parte I"**. Disponível em: <http://www.ebah.com.br/content/ABAAABeIMAB/aula-08-servidor-samba>. Acessado em 05 de março 2017.

WESSELS, Duane. **Squid: The Definitive Guide**. 1st Edition. 2004. O'Reilly.

SOBRE A ORGANIZADORA

LILIAN COELHO DE FREITAS - Professora do Instituto Federal de Educação, Ciência e Tecnologia do Pará (IFPA). Possui graduação em Engenharia da Computação pela Universidade Federal do Pará (2007) e mestrado em Computação Aplicada pelo Programa de Pós-Graduação em Engenharia Elétrica (PPGEE) da UFPA, obtido em 2009. Em 2008, realizou estágio de mestrado no Instituto de Engenharia de Sistemas e Computadores (INESC/ Porto - Portugal). Atuou como pesquisadora membro do Laboratório de Eletromagnetismo Aplicado (LEA/UFPA) de 2004 a 2014 e do Laboratório de Sensores e Sistemas Embarcados (LASSE/UFPA) de 2008 a 2012. Atuou como Pesquisadora Visitante no *Georgia Institute of Technology* (Atlanta, Georgia, Estados Unidos), no período de Março/2012 a Fev/2013. Tem mais de 50 trabalhos publicados, envolvendo publicações em livros, revistas e eventos científicos. Seus interesses de pesquisa são: telecomunicações (comunicações sem fio, rádio cognitivo) e *machine learning*.

ÍNDICE REMISSIVO

ENGENHARIAS ELÉTRICA E DE COMPUTAÇÃO:

O TERCEIRO PILAR

www.atenaeditora.com.br
contato@atenaeditora.com.br
@atenaeditora
www.facebook.com/atenaeditora.com.br

Atena Editora
Ano 2021

ENGENHARIAS ELÉTRICA E DE COMPUTAÇÃO:

O TERCEIRO PILAR

www.atenaeditora.com.br
contato@atenaeditora.com.br
@atenaeditora
www.facebook.com/atenaeditora.com.br

Atena Editora
Ano 2021