Fundação Educacional do Município de Assis
IMESA - Instituto Municipal de Ensino Superior de Assis

MICHEL GARGEL NUNES

REESTRUTURAÇÃO DE REDES DE COMPUTADORES EM UMA INSTITUIÇÃO PÚBLICA: UM ESTUDO DE CASO

Assis/SP

2019

Fundação Educacional do Município de Assis
IMESA - Instituto Municipal de Ensino Superior de Assis

MICHEL GARGEL NUNES

REESTRUTURAÇÃO DE REDES DE COMPUTADORES EM UMA INSTITUIÇÃO PÚBLICA: UM ESTUDO DE CASO

Projeto de pesquisa apresentado ao Curso de Bacharelado em Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Linha de pesquisa: Ciências Exatas e da Terra

Orientando: Michel Gargel Nunes

Orientador: Fábio Eder Cardoso

Assis/ SP
2019

FICHA CATALOGRÁFICA

FICHA CATALOGRÁFICA

N972r NUNES, Michel Gargel
Reestruturação de redes de computadores em uma instituição pública: um estudo de caso / Michel Gargel Nunes. – Assis, 2019.

47p.

Trabalho de conclusão do curso (Ciência da Computação). –Fundação Educacional do Município de Assis-FEMA

Orientador: Me. Fábio Eder Cardoso

1.Redes 2.Servidor 3.Proxy

CDD 004.65

REESTRUTURAÇÃO DE REDES DE COMPUTADORES EM UMA INSTITUIÇÃO PÚBLICA: UM ESTUDO DE CASO

MICHEL GARGEL NUNES

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador:_____
Fábio Eder Cardoso

Examinador: _____
Luiz Carlos Begosso

Assis/SP

2019

DEDICATÓRIA

Dedico este trabalho aos meus pais, Mauricio de Almeida Nunes e Valeria Gargel Gonzales e ao meu irmão Willian Gargel Nunes que sempre estiveram ao meu lado, educando, repreendendo e consolando. Dedico isto a eles, pois sempre se esforçaram em me dar o melhor e jamais desistiram de lutar por minha educação.

AGRADECIMENTOS

Primeiramente eu agradeço a **Deus**, pois sem ele eu não teria alcançado o que alcancei e por imensa misericórdia, graça e consolo durante todo o tempo.

Agradeço a Deus por eu ter a minha única e especial amiga de coração **Bruna Moreira** pelo todo apoio conselhos incentivo estando comigo nos piores momentos da minha vida e nos melhores sempre me ajudando nas orações e dando apoio e por todo carinho que ela tem por mim, sem ela eu não estaria presente.

Agradeço a minha ex-namorada **Jheniffer Cruz** por ter me ajudado muito nos estudos e me apoiando sempre nas decisões uma pessoa maravilhosa e pelos pais dela **Luciano** e **Angelita** por sempre me ajudar.

Aos meus amigos de coração **Gabriel Alan, Geovanna, Lucas Cesar, Cristiano e Israel** umas amizades verdadeiras que sempre mostrou presente em me aconselhar, incentivar e me ajudar.

Aos meus colegas **Vitor, Kimberly, Marcos Antônio, Gaby** e **Renato Virto Moreira** pelas ajudas, conselhos e fazendo cada dia sendo diferente de outros dias.

Aos meus professores, **Alex Poletto, Almir, Fernando Brito, Luiz Carlos Begosso, Luiz Ricardo Begosso, Marisa, Osmar** e outros. Por serem excelentes profissionais, por todo auxílio, umas das melhores amizade que tenho.

Agradeço em especial o Professor **Douglas Sanches da cunha,** que me aconselhou, ajudou e das ótimas aulas de Arquitetura de Computadores e Sistemas Operacionais, pelos jeitos de ministrar que levarei de lembrança para sempre**.**

E ao meu orientador **Fábio Eder** pela orientação e apoiou com seus grandes conhecimentos neste trabalho. Aos delegados e todos funcionários da Central de Polícia Judiciaria que me auxiliaram.

“Um pássaro descansando num galho
Nunca tem medo que o galho se quebre
Porque a sua confiança não está no galho,
Mas na força de suas próprias asas.
Sempre confie em você.”
Confúcio

“Tudo posso naquele que me fortalece.”
(BÍBLIA, Filipenses, 4, 13)

RESUMO

Diante dos diversos impactos e discussões sociais que os problemas referentes às negligências políticas para com os órgãos públicos, neste projeto de pesquisa, o principal objetivo foi otimizar o desenvolvimento dos trabalhos cotidianos desenvolvidos na Central de Polícia Judiciária, situada na cidade de Assis. Isto se deu através de uma proposta de intervenção baseada na reestruturação dos cabos de rede, tanto em seu estado físico quanto em seu sistema e servidor. Para tal trabalho foi necessário respaldo teórico que sustentassem a importância da boa estruturação das redes, como FINK e NEUMANN (2007), bem como outros escritores que articulam teorias e meios que proporcionem entendimento profícuo de como alcançar tais propósitos. Em suma, este trabalho resultou de uma proposta de conclusão de curso, exigida de Fundação Educacional do Município de Assis do curso de Bacharel em Ciências da Computação.

Palavra-Chave: Redes; Servidor; *Switch*; *Proxy*; STP; UTP.

ABSTRACT:

In view of the various social impacts and discussions that the problems related to political negligence towards public bodies, in this research project, the main objective is to optimize the development of the daily work developed at the Judicial Police Center, located in the city of Assis. This will be done through an intervention proposal based on the restructuring of the network cables, both in their physical state and in their system and server. For this work, theoretical support was needed to support the importance of good network structuring, such as FINK and NEUMANN (2007), as well as other writers who articulate theories and some ways that provide a useful understanding of how to achieve those goals. In short, this work results from a proposal for a of completion of course, required from the Educational Foundation of the Municipality of Assis of the Bachelor's Degree in Computer Science.

Keywords: NETWORK, SERVER, *SWITCH*, *PROXY*, STP, UTP

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

Vlan (Virtual Local área network)

CPJ (Central de Polícia Judiciaria)

ANSI (American National Standards Institute)

ISO (International Organization for Standardization)

EIA (Eletronic Industries Association)

TIA (Telecomunication Industries Association)

UTP (Unshielded Twisted Pair)

STP (Shielded Twisted-Pair)

LAN (Local áreal network)

SNMP (Simple Network Management Protocol)

WAN (Wide Area Network)

TAN (Tiny Area Network)

MAN (Metropolitan Area Network)

IP (Internet Protocol)

FTP (File Transfer Protocol)

ACLs (Access Control List).

WPAD (Web Proxy Auto Detection).

HTTP (Hypertext Transfer Protocol).

DNS (Domain Name System)

DHCP (Dynamic Host Configuration Protocol).

IRTF-RD (Internet Research Task Force Group on Resource Discovery)

IRCache (Information Resource Cache)

SARG (Squid Analysis Report Generator)

Sumário

1. INTRODUÇÃO

O presente trabalho visa aplicar e estruturar a rede de computadores, sua infraestrutura física, bem como, implementar servidores com sistemas de segurança, gerenciamento de usuários, distribuição de internet aos *hots* da rede, servidor de arquivos e *backup*, dentre outros serviços necessários em um órgão público de atendimento cívico situado na cidade de Assis-SP, conhecido como Central de Polícia Judiciária.

O órgão público, objeto deste trabalho, trata-se uma central de polícia judiciária, sendo assim, por questões de segurança o presente trabalho não apresentará detalhes específicos quanto a segurança de dado órgão, ou seja, focalizaremos este estudo apenas no tocante à estruturação e maior segurança da rede. O fato
é que a infraestrutura de rede se encontra devastada, vulnerável e não oferece um serviço adequado, o que debilita o devido funcionamento dos serviços prestados pelo órgão.

As pesquisas de FINK e NEUMANN (2007) afirmam que a principal diferença entre os conceitos de agilidade e flexibilidade estão centrados no fato de que, a agilidade depende da dimensão da velocidade. Esta por sua vez depende de como a organização de TI é feita. Seria dizer que, um sistema para ser rápido e eficaz depende de sua estrutura. Por essa razão, agir em prol da reestruturação de rede dos computadores da central de polícia judiciária significa contribuir para a agilidade na prestação de serviços.

1.1 OBJETIVOS

Dadas as necessidades encontradas no sistema de redes da Central de Polícia Judiciária, o principal objetivo deste projeto visa a reestruturação de todo o cabeamento de rede com o intuito de qualificar positivamente o desenvolvimento das atividades.

Outro objetivo fundamental é instalar e configurar servidores de rede, bem como, implementar serviços de rede e controlar o acesso a sites /sistemas,

visto que eles garantem a melhoria na qualidade da segurança e dificultam a invasão do sistema utilizado pela Central de Polícia Judiciária

Para tal, a implementação de uma política de segurança de rede, viria como uma ferramenta responsável pela não vulnerabilidade dos sistemas, otimizando os gastos com investimentos feitos e ainda necessários para a devida proteção dos seus referentes dados.

Por fim, implementado um sistema de relatório para a diretoria, com o intuito de informá-la sobre os acessos, bem como melhorar as análises relevantes a identificação de possíveis problemas ou falhas no funcionamento do sistema.

1.2 JUSTIFICATIVA

Este trabalho pretende ser desenvolvido em sua totalidade no CPJ (Central de Polícia Judiciária) de Assis porque neste local há uma grande defasagem quanto a estrutura de rede, onde notamos que seria de extrema importância a reconstrução de dados equipamentos.

Este órgão situa-se em um prédio alugado, onde antigamente abrigava uma unidade médica e dada as necessidades civis por um centro de polícia, o prédio teve que passar por uma adaptação de seu espaço para que as atividades que dizem respeito a esse órgão policial pudessem ser realizadas.

Devido à falta e indisponibilidade de recursos para a manutenção dos equipamentos utilizados, principalmente os referentes ao TI, na rotina dos colaboradores deste órgão policial, os funcionários tiveram que amenizar os problemas ocasionados pela falta de revisão de maneira amadora, o que foi debilitando gradativamente o funcionamento da rede.

Por essa razão buscou-se fazer um estudo aprofundado e crítico sobre a infraestrutura de rede, partindo do conceito classificatório tipológico de redes como tecnologia de transmissão e tecnologia de escala, fortemente discutido por Tanenbaum (2010) que define a rede de computadores como "[…] um conjunto de computadores autônomos interconectados por uma única tecnologia. Dois computadores estão interconectados quando podem trocar informações. A conexão não precisa ser feita por um fio de cobre; também podem ser usadas fibras ópticas, *microondas*, ondas de infravermelho e satélite de comunicações. […]"

Após análises e consideração sobre os pressupostos teóricos oferecidos por Tanenbaum é que fazer-se a uma reflexão e assim uma prática concisa dos resultados possibilitados por esse estudo teórico na prática. Ou seja, após uma pesquisa e observação dos conceitos teóricos projetados por Andrews (2010) é que será possível a busca por uma reestruturação dos cabos de rede de computadores da central de polícia judiciária de Assis – SP.

1.3 MOTIVAÇÃO

Com o intuito de aperfeiçoar a segurança, bem como, o funcionamento do sistema utilizado pela Central de Polícia Judiciária situada na cidade de Assis – SP, este projeto teve a finalidade de reconstruir a estrutura externa e interna dos cabeamentos referentes a determinada rede.

Essa proposta surgiu de uma necessidade interna notada e sofrida pelos funcionários desse órgão público, porque sem a rede fica impossibilitada a realização das atividades da central de polícia judiciária. Como a queda da rede era frequentemente ocasionada devido à má infraestrutura, e como a dispensabilidade deste órgão público para a sociedade é indispensável acredita-se que as reflexões e práticas elucidadas por este estudo torna-se imprescindível.

Enfim, após notarmos essa dificuldade e carência em determinado órgão, e após analisar todo o cenário, considerou-se que a gravidade do problema é agravante,

pois, uma infraestrutura debilitada expõe de modo negativo o desenvolvimento das atividades que dependem de TI.

1.4 CONTRIBUIÇÃO

Espera-se que com este trabalho o problema referente a infraestrutura e funcionamento do sistema seja solucionado, com isso o processo de atendimento ao usuário será otimizado. Tal resultado seria de fundamental importância dada a responsabilidade social que central de polícia judiciária possui diante da população Assisense.

Sendo assim, o devido desenvolvimento deste projeto também traria benefícios à população, porque, com a disponibilidade de um serviço melhor a capacidade do funcionamento seria aumentada e assim a maior eficiência ao acesso e uso de dados em diferentes níveis de informação.

1.5 METODOLOGIA

Para a realização deste trabalho foram utilizados materiais como, livros, cursos, artigos e consultas eletrônicas com a intenção de agregar conhecimento que serão de extrema importância para o seu desenvolvimento. Essa priorização do saber teórico como ponto de partida para a resolução do projeto vem em defesa do que diz Kahlmeyer-Mertens et. al. (2007):

> "Por construir um saber público, o conhecimento científico produzido no espaço acadêmico deve possuir padrões que uniformizem os métodos e as técnicas de sua elaboração, experimentação e publicação" (KAHLMEYER-MERTENS et. al. p.27)

Enfim, este trabalho seguiu em comum acordo com o cronograma e com o método, assim tivemos a instalação, estruturação e implementação de técnicas em prol da melhoria do funcionamento da rede de computadores da Central de Polícia Judiciária com intuito de fundamentar a metodologia.

Isso foi atingido por meio do aprimoramento de tarefas distintas, entre elas a configuração dos *switchs* com o uso de Vlan (*Virtual Local área network*) que é

um aparelho responsável pela recepção e transmissão física de pontos de acesso à rede, o que significa que este equipamento possibilita que outros aparelhos se conectem a ele; e também a implementação do servidor *Squid*.

O *Squid* referido proxy, é um serviço que permite o compartilhamento da conexão de Internet com outras variadas máquinas de rede.

De acordo com Paulinho (2009), a utilização do *Squid* instalado em um servidor que esteja conectado à internet, possibilita que outras máquinas executem sistemas operacionais distintos, páginas web e FTP (File Transfer Protocol) por meio do servidor. Para ele, o Squid é um software especializado em realizar operações de proxy web e FTP, totalmente livre e com excelente suporte para operações em servidores Linux.

Segundo Rick (2012) este servidor proxy funciona como uma saída principal da rede. Logo, pode-se centralizar o foco em segurança criando políticas de acesso, autenticação de usuários, registros e controle centralizado

2. INFRAESTRUTURA DE REDES DE COMPUTADORES

2.1 SISTEMA ESTRUTURADO

Até aqui, tomamos como sistema estruturado, determinado grupo de produtos condutores que são definidos por meio de regras específicas da área das engenharias. Sendo assim, determinado sistema é responsável por agregar distintas formas de transmissão que suportem aplicações, como por exemplo, vídeo, voz, sinalização etc. Este grupo de regras garantem que a conectividade entre os dispositivos responsáveis por preparar a infraestrutura das tecnologias que emergem bem como, sua tipologia, o que possibilita e otimiza os diagnósticos necessários para sua efetiva manutenção.

De acordo com Pinheiro (2003), um dos pontos principais do sistema estruturado de redes advém do fato de que ele nunca será melhor do que o cabeamento que utiliza, além disso, a maioria dos edifícios precisam de um sistema que seja projetado segundo diretrizes e especificações para estes fins.

2.2 REDE ESTRUTURADA

O que chamamos de rede estruturada, emergiu com o intuito de padronizar a infraestrutura até então instalada em edifícios públicos e privados, como por exemplo, comércios e residenciais, dando aos seus usuários a possibilidade de utilizar um aparelho tecnológico, fosse ele um computador ou celular, de modo dinâmico e bem estruturado.

2.3 PADRÕES

Levando em consideração a frequente necessidade de aplicar-se padrões que utilizem as características de rede com intuito de favorecer escalabilidade, interoperabilidade, segurança e portabilidade pautada em parâmetro na

programação visual de uma rede. Vale ressaltar que a programação visual tem seu fator primordial quanto á garantia de qualidade que uma rede pode oferecer, visto que, ele viabiliza a estabilidade, a modularidade, a conectividade, a disponibilidade além de facilitar a manutenção.

Atualmente, as redes individuais que fazem parte da internet, utilizam uma abordagem de desenvolvimento que varia de acordo com o nível da qualidade operacional, logo, se ela foi construída de forma não estruturada, pode enfrentar dificuldades ao tentar cooperar com outras redes.

De acordo com Ross (2007) experiências mostram que 2% dos custos de investimento equivalem aos cabos e conectores. Os outros 98% restante se destinam aos servidores, estações, hubs, switches, roteadores e softwares de rede e aplicativos. Em relação as falhas das redes 50% dos problemas estão relacionados a cabos e conectores, normalmente em função de má instalação, aquisição de produtos inferiores, precariedade ou manuseio incorreto por parte do usuário. No que pode acarretar prejuízos relevantes com a inatividade da rede.

Caso haja erros no procedimento do desenvolvimento, acabam acontecendo interrupções frequentes e essas interrupções negativam a navegação dos usuários de internet, por isso é importante ter-se um processo de engenharia de rede bem definido.

Sabendo que a importância da padronização de uma infraestrutura provem da necessidade de garantir a implementação de conceitos é que se desenvolveram as normas, tanto para os usuários como para os profissionais e fabricantes, que optaram por orientar-se a partir de organizações, tais como, ANSI, ISO, EIA, TIA etc.

Segundo Pinheiro (2003), a norma EIA/TIA é um padrão de auxílio da arquitetura de cabeamento, dos meios físicos, componentes e interfaces, tratando o cabeamento de um edifício como parte da infraestrutura. Desta forma, é possível o pré-cabeamento de um edifício, sem saber ao certo quais serão as telecomunicações que serão utilizadas

Abaixo apresentamos uma descrição sucinta de três das mais utilizadas e reconhecidas normas estruturais, de acordo com a *Eletronic Industries Association* (EIA) e *Telecomunication Industries Association* (TIA):

- ANSI/EIA/TIA 568 – Padrão de Cabeamento. Ele é reconhecido como o responsável por oferecer as normas de planejamento de instalação dos cabos de telecomunicação, bem como, os seus respectivos produtos a serem instalados.

As ordens de ligações especificam os fios do par trançado (UTP, STP) nos conectores RJ-45. Esta norma está diretamente ligada ao sucesso da expansão das redes de computadores, ela regulariza todos as conexões dos cabos, como por exemplo, as categorias de cabos aceitas, comprimentos, distâncias entre os mais variados níveis de distribuição. Posteriormente, os padrões estabelecidos foram gradativamente substituídos pelo 568-b1, b2, b3 são. São elas:

-Norma ANSI/EIA/TIA 568-b.1, responsável pelo cabeamento dos requerimentos mínimos das telecomunicações a serem instaladas tanto no interior como nas instalações externas dos edifícios.

-Norma ANSI/EIA/TIA 568-B.2, que especifica os padrões mínimos dos componentes de cabeamento metálico, procedimento de validação, levando em consideração a performance de transição do sistema de cabeamento. Ela dependente das características dos seus equipamentos de teste para a medição em campo.

-NORMA ANSI/EIA/TIA 568-B.3, que designa os padrões mínimos dos componentes de cabeamento óptico utilizado no sistema de cabeamento, como conectores, cabos ópticos, hardware de conexão patch e equipamentos de teste medição em campo.

Segundo Pinheiros (2003), este conjunto de regras que compõem esta norma, visa padronizar todos os elementos que irão constituir a estrutura de cabeamento horizontal/vertical com o intuito de alcançar seguintes objetivos:

“[..] 1- Implementar um padrão genérico de cabeamento de telecomunicações a ser seguido por fornecedores diferentes; 2- Estruturar um sistema de cabeamento intra e inter predial, com produtos de fornecedores distintos; 3- Estabelecer critérios técnicos de desempenho para sistemas distintos de cabeamento.”

Como esta norma está presente em todos os níveis de subsistema de cabeamento estruturado, devemos analisar passo a passo, pois, existem

algumas particularidades entre os níveis, como por exemplo o complemento, a categoria e os tipos de cabos, etc.

ANSI/EIA/TIA – 569 **–** Caracteriza a Infraestrutura de Cabeamento Estruturado bem como, define uma estrutura de dutos e espações para telecomunicações dedicada ao uso de um sistema que suporte uma grande variedade de serviços de telecomunicação e não apenas voz e dados. Estes requerimentos são específicos e apresentados para suster um ambiente de telecomunicação de multiproduto e multi-fabricante.

ANSI/EIA/TIA – 570 – Este padrão serve para que seja profícuo o cabeamento da telecomunicação, aplicando ao sistema de cabeamento os respectivos estações e caminhos para prédios residenciais multiusuário, bem como casas individuais. Ela especifica os sistemas de cabeamento na intenção de suportar uma larga faixa de aplicação e telecomunicações em ambiente residenciais

2.4 REQUISITOS

De acordo com as diretrizes internacionais, a estruturação de um sistema, tem como principal objetivo gerenciais e manter em bom funcionamento as comunicações, sejam elas de imagem, dados ou voz.

De acordo com Pinheiro (2015), por meio da documentação da rede, pode-se identificar alguns pontos com problemas, e assim sendo possível solucionar com mais facilidade. Documentar uma rede, além de necessário, é muito importante por garantia de seu desempenho no futuro.

Para tal, um sistema para ser estruturado adequadamente, precisa cumprir com alguns requisitos importantes tanto para de fato ser instalado quanto para documentar seu projeto físico, como por exemplo:

Memória Descritiva, que se trata de um documento responsável pela devida descrição dos serviços que uma empresa ou órgão propõe. No tocante a este projeto, ela serviu para melhorar a qualidade da internet do central de polícia judiciária de Assis, que precisa refazer toda a sua infraestrutura lógica de rede. Antes ela estava situada na parte externa superior do prédio, com desgastes físicos causados pela chuva e calor. Isto interferia muito na qualidade do serviço de *Network*, visto que estava exposta a frequentes interrupções.

Com isso, propõe-se a estruturação de toda a parte interior do prédio, protegendo do calor, humidades e garantindo maior proteção dos cabos, o que além de diminuir mais os custos, evita comprar novos cabos STP. Vale ressaltar que, atualmente o prédio tem 63 computadores e todos são cascateados em hubs, o que prejudica ainda mais a qualidade da rede.

Recomeçando pelas compras de conectores RJ45, cabo de rede par trançado CAT5E com padrões 568a, canaletas metálicas para fazer caminhamentos de pontos estratégicos, e aquisições de 4 *switch*, sendo uma delas gerenciáveis e 3 não gerenciáveis, bem como canaletas simples para serem ligadas no interno das salas. Por fim, será implementando um Servidor Linux com proxy com o intuito de filtrar os conteúdos indesejáveis à política do órgão da polícia.

Enfim, as atividades desenvolvidas pelo responsável do projeto de rede, relaciona tanto o ato de estabelecer padrões como a sua devida utilização técnica em prol de equipamentos que beneficiem a estrutura física, os documentos, a atualização da infraestrutura que já existem por meio de requisitos importantes tanto para a abrangência quanto para a requalificação da infraestrutura aqui referenciada.

2.5 INFRAESTRUTURA INTERNA

De acordo com Pinheiro (2017) O projeto da infraestrutura da edificação conterá os locas para instalação de dutos, leitos de cabo, execução de furos de parede, passagens de cabo de energia e aterramento para a alimentação do distribuidor interno. Os tipos de matérias serão indicados, tais como PVC, aço galvanizado e também os tipos de fixação como parafusos, abraçadeiras e outros itens que serão necessários para a instalação do sistema.

Infraestrutura interna, nada mais é do que um grupo de equipamentos, ou seja, um *hardware*, como por exemplo meios físicos de transmissão em geral, *hubs, switches,* roteadores, importantes para o suporte, bem como para os sistemas que gerenciam as redes. Assim, entende-se como um composto de quadro de distribuição, bloco terminal, ferragem e por fim material, todos úteis para a comunicação da rede externa responsável por prover serviços.

Estas ações, quando desenvolvidas de modo efetivo, cooperam para a diminuição dos curtos tanto da produção quanto da instalação dos equipamentos, das políticas gerenciais, entre outras, que proporcionam o desenvolvimento de técnicas para o devido cabeamento de redes que completem e alterem o padrão básico inicial de sua estrutura.

Por fim, seguindo esta linha de visão, as novas atividades tendem a privilegiar as redes locais, visto que, elas concentram os componentes ativos e/ou estruturais dos cabeamentos flexíveis, e servem como suporte para a reconfiguração dos conjuntos de trabalhos bem como, na mudança de layout. Assim, para implementar as alternativas aqui referenciadas em prol da obtenção de bons resultados, faz-se necessário o respeito aos critérios técnicos tanto do projeto quanto de sua rigorosa instalação, caso contrário, sem dúvida o desempenho do sistema será negativado e resultará em prejuízo financeiro.

A infraestrutura interna está composta pelos seguintes equipamentos:

O primeiro deles é o *Switch*, que se trata de um dispositivo de rede cuja responsabilidade está em de associar e garantir a comunicação entre distintos dispositivos de uma rede local (LAN). Fabricantes como, por exemplo, Cisco, produzem variados *switch*es com o intuito de atender as atividades mais simples (no caso de residências ou escritórios) ou até mesmo as industriais, que exigem maior nível de desempenho.

O que diferencia o *Switch* de outros equipamentos é o seu funcionamento bastante dinâmico. Ele recebe uma mensagem de qualquer dispositivo conectado à rede e envia esta mensagem apenas para o destinatário da mensagem. Isso significa que ele “conhece a maneira” mais eficiente de manipular e transmitir dados entre diferentes dispositivos dentro de uma LAN.

Existem duas categorias de *switch*, são elas, o *switch* gerenciável e o não gerenciável. A principal diferença entre eles está no fato de que o primeiro possui uma configuração que prioriza o tráfego da LAN garantindo que as informações sejam transmitidas primordialmente. Entretanto, um *switch* não gerenciável atua como dispositivo de “*plug and play*”, logo, ele não se configura

de modo simples, antes, permite que os dispositivos se comuniquem uns com os outros.

Assim como já foi relatado, o *Switch* gerenciável permite que o controle do tráfego da LAN possua recursos mais avançados de configuração que garantem o bom funcionamento do tráfego. De modo geral, ele se difere do não gerenciável pelo fato de conter recursos que controlam, gerenciam e monitoram uma LAN. O que faz com que a rede tenha o poder que saber e controlar que é o que tem trafegado na LAN.

Paralelo a isto, nota-se que não é possível que um *switch* seja configurado afinal ele suportaria nenhuma interface de configuração que priorize de tráfego. Ele semelhante aos dispositivos de *plug-and-play*, aqueles que permitem ao usuário conectar o seu aparelho tecnológico em uma rede, o que viabiliza a conexão entre eles. Por essa razão o *switch* não gerenciado pode ser considerado uma das melhores opções caso não haja a necessidade de aplicações avançadas em uma rede, afinal, bastaria conectá-lo.

Quanto ao *switch* gerenciável, é possível defender que ele viabiliza vários outros ganhos, pois, utiliza o protocolo SNMP ou *Simple Network Management Protocol,* responsável por monitorar os dispositivos na rede, enquanto que o SNMP ajuda na comutação de dados de gerenciamento entre dispositivos de redes, e, além disso, estas consultas SNMP também determinam a integridade e o status de dispositivos em uma rede. Assim, um administrador de TI pode interpretar os dados SNMP, acompanhar o desempenho da rede partindo de um ambiente remoto, detectando e reparando assim alguns problemas de rede de um local, sem necessitar inspecionar fisicamente os computadores e dispositivos. Enfim, o *switch* gerenciável garante as funções mais avançadas, o que leva a um aumento do nível de segurança.

Outro equipamento importante e muito utilizado é o *Hub*, também conhecido como concentrador por se tratar de um equipamento utilizado na área da informática para a realização da conexão de computadores de uma rede garantindo a transmissão de informações entre esses aparelhos.

O hub foi tido como o aparelho precursor utilizado por empresas que queriam mudar os dados de determinada rede para outra, além disso, o Hub está ligado

em LAN, WAN, TAN e MAN, possuindo um endereço de IP que permite que os dados trafeguem através destas conexões.

Logo que o aparelho é conectado à uma rede, ele transmite informações para o Hub, por isso é importante que ele esteja desocupado, afinal, se não ocorrer dessa maneira as informações voltam para o aparelho requisitante com um pedido de espera até que os dados que estão sendo feitos pelo Hub terminem.

> "O Hub é um dispositivo básico e de funcionamento interno simples, não possui nenhum gerenciamento especial dos dados que chegam até ele. Internamente, possui um único barramento, sendo assim, redes que usam *hub* classificadas como topologia em barra (no sentido lógico). Por isso, somente dois dispositivos podem trocar informações por vez. Se algum micro tentar enviar algum dado para outro, quando esses dados passarem pelo *hub*, ele será replicado em todas as suas portas. Todos os micros ligados ao *hub* receberão esses dados, mas somente o micro de destino é que irá aceita-lo." (Equipe Digerati Books, p.21, 2009)

Este é um dos pontos negativos do hub, porque além dele não conseguir repassar os pacotes ele os envia para outras máquinas que estão interligadas, o que acaba causando transtornos á segurança de seu usuário.

O *Router* é conhecido por ser um equipamento que oferece internet, encaminha informação da rede *Wifi* para os seus aparelhos pessoais, como por exemplo celulares, computadores, tablets, desde que estejam conectados à referente rede de internet de sua casa.

Assim, chegamos ao rack de rede, também conhecido como bastidor de rede, responsável por abrigar de modo padronizado as normas técnicas de todo o material ligado a rede local do edifício. Sendo assim, este rack guarda de modo seguro os aparelhos que garantem a comunicações com o exterior.

Por fim, as canaletas são uma categoria onde passam os fios que ficam abrigados, evitando a exposição excessiva do cabeamento que precisa ser fixado na parede, nos rodapés ou até mesmo no teto. Ela também é útil para a elaboração de novos pontos de acesso à tomada de rede.

2.6 CABEAMENTO METÁLICO

Segundo Siqueira (2010), o cabeamento se trata de um grupo de fios de cobre semelhantes aos do telefone, que tem por objetivo reduzir as interferências eletromagnéticas. Cabeamento metálico trata-se de um cabo de rede e para melhor exemplificar a sua importância, trataremos de ressaltar as suas categorias, todas possuem um padrão específico, taxa de transparência de informações e frequência, são elas:

Categoria 1: Que já não é reconhecida pela TIA (Associação da indústria de telecomunicação). Por conta de suas instalações telefônicas e redes antigas.

Categoria 2: Atualmente também não é mais reconhecida pela TIA, pois, foi projetada para às antigas redes *token-ring.*

Categoria 3: Que se trata do padrão inicial de desenvolvido, principalmente quanto às redes, além de possuir certificado para sinalização de até 16 MHz.

Categoria 4: Assim como as três anteriores, esta quarta categoria já não é reconhecida pela TIA, porque utiliza dados de frequência de até 20 MHz e dados a 20 Mbps para transmitir suas informações e por essa razão foi substituída pela categoria 5.

Categoria 5: Esta é comumente utilizada, porque consegue agregar qualquer placa de rede. Ela é pela TIA e é tida como CAT5e, podendo ser utilizada em uma frequência de até 125 MHz.

Categoria 6: Ela atua com uma frequência de 250 MHz, entretanto o seu alcance é se mantém apenas em até 55 metros (a CAT6a permite até 100m), suportando frequências de até 500 MHz além da possibilidade de reduzir interferências e perda de sinais.

Categoria 7: Mesmo estando em fase planejamento e desenvolvimento, esta categoria pretende garantir a criação de redes de 100Gbps em cabos de 15m usando fio de cobre.

2.7 MEIOS GUIADOS E NÃO GUIADOS

De maneira sucinta, o dever principal de todo e qualquer modo de transmissão

é o de levar o fluxo de informação por meio de determinada rede, fazendo desta competência em transmitir mais limitada pelo fato de possuir peculiaridades especificas para cada meio no qual está sendo aplicada.

Segundo Pinheiro (2015), o meio de transmissão chama-se “guiado” quando está contido na sua estrutura física, ou seja, a sua transmissão se restringe ao interior do cabo. Contudo, o meio de transmissão não guiado se caracteriza por utilizar o ar como meio de transmissão de sinal de informação, como por exemplo, sinais de micro-ondas, radiofrequência e infravermelho.

Tais meios de transmissão dividem-se em meios que são guiados, ou seja, que se dão através de cabeamentos de cobre ou fibra óptica, e meios que não são guiados, ou seja, que se dão através de ondas de rádio e raios laser.

Os modos de transmissão guiados possuem uma camada física responsável por transmitir um fluxo de bits entre os aparelhos. Muitas maneiras físicas são passíveis de serem utilizadas para esta ação, a transmissão. As maneiras físicas são juntas em modos guiados, como por exemplo os fios feitos de cobre e as fibras óticas, assim como os meios não guiados, como por exemplo as ondas de rádio e raio laser transmitido pelo ar.

Também existem os cabos não blindados, conhecidos como UTP, ao passo que os blindados são chamados de STP, responsáveis por protegerem contra os ruídos mais do que o cabeamento UTP. Porém, o STP quando comparado com o UTP é consideravelmente mais complicado e caro de ser instalado.

O STP agrega normas e formas de blindagem para livrar-se do fardo que as interferências eletromagnéticas e de frequência causando diafonia. Para aproveitar o máximo possível a blindagem, esses cabos STP terminam com conectores de dados STP especiais. Caso este cabo seja instalado de modo

equivocado, sua blindagem pode acabar detectando sinais que não são necessários, causando transtorno aos seus usuários.

Vale ressaltar que existem diferentes tipos de cabos STP, com diversas propriedades disponíveis.

A de que o cabo STP assegura todo os fios com uma camada metálica que elimina quase que totalmente qualquer interferência. E a de que o cabo STP preserva os fios, assim como, os pares de fios individuais com uma camada metálica que aniquila as interferências.

O cabo STP apresentado, utiliza quatro pares de fios, cada um deles está envolto em uma blindagem de camada metálica, estas por sua vez estão envolvidas em uma trança ou chapa metálica.

2.8 CABEAMENTO ESTRUTURADO

O Cabeamento estruturado nada mais é do que um grupo de distintos tipos de cabos instalados de modo padronizado privilegiando as normas de segurança, além disso, ele é utilizado como facilitador da distribuição de dados, sejam ele de telefone ou vídeo.

Por essa razão, ele garante o direcionamento dos sinais de comunicação por caminhos dos mais variados, além de visar e proporcionar o aproveitamento tanto dos equipamentos como dos recursos, servindo como uma possibilidade financeira mais econômica.

Anteriormente o cabeamento, fosse ele estruturado ou não, era tido como uma forma primitiva, pouco analisada, e por isso a sua instalação exigia melhorias em seu planejamento com o intuito de melhorar a sua demanda.

Porém, faziam-se necessárias redes que contassem com uma estrutura e estabilidade mais bem arquitetada estáveis e bem estruturados, e por isso, passou-se a fixar e a defender com ênfase e propósito um sistema baseado na padronização dos conectores bem como dos meios que transmitem, e isto deveria acontecer independente da aplicação e do layout do sistema, claro, seguindo o cabeamento estruturado.

O cabeamento estruturado está pautado em normas internacionais, e de acordo com o material editado pela Equipe Digerati Books (p. 24, 2009) estas normas são uteis para a orientação da montagem das redes organizadas, padronizadas e flexíveis, onde as infraestruturas suportam as diversas categorias de aplicação, assim, quando faz uso de padrões como de cabos e conectores facilita a conexão equipamentos distintos sejam quais forem os pontos da rede bem como das normas responsáveis pela distribuição dos cabos e da garantia de estrutura e identificação de seus gerenciadores.

Sendo assim, o corpo deste sistema permite a organização e expansão, uma vez que no caminho da transmissão de qualquer ponto de rede, os cabeamentos estruturados agregam todos os princípios, são eles, o planejamento, a estação de trabalho, a categoria do cabo, o trajeto e a rede de servidores.

Os mesmos pautam sua resolução nas seguintes etapas, na boa infraestrutura de estrada, onde é definida a entrada do edifício que a partir daí tende a programar a interface de cabeamento a estrutura do prédio, o que exige uma divisão que abrigue os aparatos dos servidores como um armário por exemplo.

Finalmente teremos o cabeamento vertical, ou *backbone*, que relaciona as salas de aparatos ao local onde se encontra o *Switch*, isso significa que, cabeamento é o principal equipamento que permite às salas a telecomunicação, enquanto, o cabeamento horizontal parte do *Switch* e se liga às estações de trabalho. Enfim, a administração, responsáveis por identificar os espaços e categorias de cabeamento.

2.9 PROJETO: ANTES E DEPOIS

Devido as condições instáveis nas quais se encontra a central de polícia judiciária de Assis, neste tópico mostraremos o atual estado do sistema de rede que garantem, ou melhor, deveriam garantir o bom funcionamento de

determinada instituição. A figura 1 ilustra situação:

Figura 1: Protótipo Rede CPJ Antes, Fonte próprio Ator

Esta imagem foi feita por meio de um programa que serve para fazer simular a construção de uma rede de aparelhos tecnológicos, como computadores. Este programa se chama *Cisco Packet Tracer* e muito tem contribuído para a formação de uma estrutura de redes melhor arquitetada, o que otimiza a sua análise e estudo de suas produções.

Como podemos ver na imagem, a CPJ possui apenas um *switch* central, onde é distribuída uma rede pautada em uma conectividade cascateada apenas entre *hub's*. Devido o fator negativo que o *hub* apresenta, que está em sua falta de direcionamento específico, os dados são compartilhados de modo inseguro, logo, as informações que deveriam ser transmitidas para um ponto específico acabam indo para todos os demais.

Posteriormente A figura 2 que apresenta a proposta já elucidada por este projeto, que é a de remanejar recursos e atividades que melhorem a qualidade da prestação de serviços de determinado órgão.

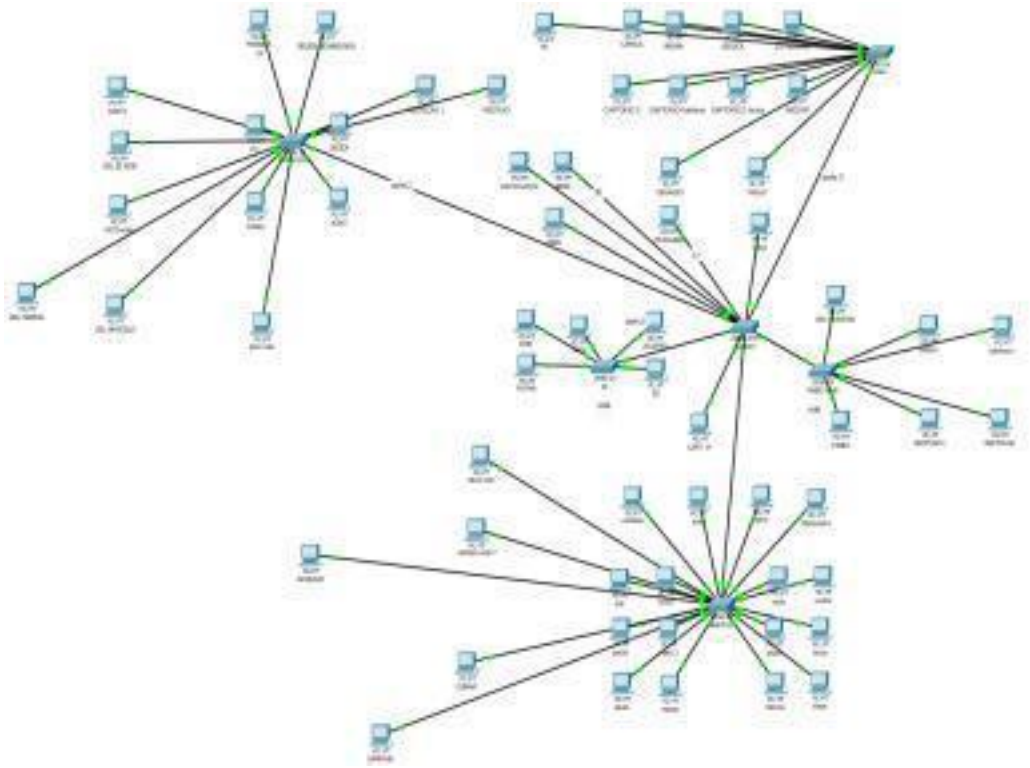

Figura 2: Protótipo Rede CPJ Depois Fonte próprio Ator

Aqui vemos que a proposta está pautada na substituição de 98% dos *hub's* por *Switchs* em pontos estratégicos, para que o cascateamento de *hub's* não seja necessário, como visto anteriormente, e também prevenindo contra a perda de pacote, visto que o fator principal do *Switch* é fazer com que o pacote chegue até o seu destinatário.

2.10 MAPA

Neste tópico apresentamos um mapa da planta baixa, que nada mais é do que a estruturação da Central de Polícia Judiciária, órgão ode será desenvolvido este projeto.

Figura 3: Planta Baixa CPJ

Como vemos, o órgão possui diferentes pavilhões, sendo eles mais de 30 salas, por volta de 63 computadores, 15 *hub's*, e uma *Switch*. Toda esta quantidade de equipamentos é necessária, porém, mal organizadas e mal estruturadas, logo, inadequadas. Por essa razão, cabe a este projeto a sua readequação em prol da melhoria efetiva da qualidade da rede.

3. PROXY SQUID

3.1 DEFINIÇÃO DE PROXY

De acordo com Zanoni (2007), o servidor proxy proporciona uma grande facilidade e controle, por se tratar de uma peça extremamente fundamental em uma rede local que tenha contato com uma rede pública (internet).

Para Morimoto (2011), o *proxy* é um servidor utilizado como um intermediário entre uma rede e a internet. Este servidor poderá desempenhar três funções em uma rede, tais como:

- Bloqueio ao acesso e utilização de algumas páginas. Por meio de um proxy, pode-se definir os bloqueios utilizando-se de políticas de acessos ACLs (*Access Control List*). A conexão passa pelo servidor *proxy* que adicionará uma lista de palavras e endereços que são bloqueadas, evitando como por exemplo o acesso indevido de funcionários em determinadas páginas durante seu expediente.
- Compartilhar a Internet com a rede interna através de um único IP (*Internet Protocol*) público disponível. Apenas o servidor está conectado à internet, e as outras máquinas da rede se conectam por meio dele.
- Melhorar a velocidade de acessos às páginas web através de um cache de páginas. O servidor *proxy* armazena as páginas e informações acessadas por seus usuários, possibilitando que quando este a solicitar, a página já armazenada, será recuperada automaticamente, sem que haja a necessidade de baixá-la novamente.

Segundo Tibet (2001) o proxy atua como um servidor com o intuito de melhorar a velocidade de acesso à determinado conteúdo. De modo eficiente, tal aceleração proporciona o acesso mais rápido de página que já foi acessada, isto porque o servidor *proxy* realiza a criação de um cache local onde é salvo todo o conteúdo acessado.

3.2 TIPOS DE PROXY

Utilizado para controle de rede local, o *proxy* possui muitos recursos que podem ser implantados e configurados de acordo com a necessidade de seus usuários e o tipo de rede.

3.2.1 PROXY TRANSPARENTE

É recomentado quando há a dificuldade de configurar o *proxy* em diferentes máquinas, pois ele intercepta todo o tráfego da porta oitenta e redireciona para o *proxy*, sendo assim todos os sites acessados são registrados para futuros relatórios e acesso ao monitoramento da rede local

De acordo com o Morimoto (2011), com o uso de um *proxy* transparente, tem-se basicamente o compartilhamento da conexão via NAT, com a mesma configuração básica dos usuários.

Uma regra de firewall faz o envio das requisições recebidas na porta oitenta do servidor para o *proxy*, e ele se encarrega de responder aos usuários. A partir de então, com a adoção deste meio, toda navegação será feita automaticamente por meio do *proxy*, sem que seja feita qualquer configuração adicional

3.2.2 PROXY TRADICIONAL

Configuração mais básica de um servidor *proxy* como o Squid. Para Alecrim (2013), o *proxy* tradicional exige constantemente que algumas configurações sejam feitas nas aplicações que utilizam a rede para que não ocorram erros na comunicação. Entretanto, de acordo com esta aplicação, a configuração pode ser de alto custo.

3.2.3 PROXY COM AUTENTICAÇÃO

Neste caso pode-se adicionar uma camada adicional de segurança, onde exige-se do usuário uma autenticação no *proxy* por meio de *login* e senha. Logo, este recurso é interessante pois viabiliza o controle de quem tem acesso à internet e auditar os acessos em caso de necessidade. Segundo Morimoto (2011), quase todos navegadores oferecem a opções de salvar a senha, onde o usuário precisa digitá-la apenas uma vez a cada sessão.

Ainda segundo o autor, a forma mais simples de se implementar autenticação utilizando o *Squid* é utilizando o módulo “ncsa_auth” que já faz parte do pacote principal do *Squid*. Além deste, o *Squid* também pode trabalhar com outros, como o “squid_ldap_auth”, que permite que o servidor autentique os usuários em servidor LDAP e o “ntlm_auth”, que permite o servidor *Squid* ao *Active Directory*.

3.2.4 PROTOCOLO WPAD

De Acordo com Ribeiro (2016), para a navegação na internet através de um servidor proxy, os usuários deverão ser configurados de forma manual. Contudo, é possível automatizar essas configurações por meio do protocolo WPAD (*Web Proxy Auto Detection*).

Este protocolo permite a detecção automática das configurações de proxy nos usuários. Os navegadores como Google Chrome, Mozilla Firefox, Internet Explorer, e entre outros; são configurados automaticamente por meio de um script wpad.dat anexado em um servidor HTTP (*Hypertext Transfer Protocol*).

Os navegadores podem localizar os arquivos de forma automática por meio de protocolos. DNS (*Domain Name System*) ou DHCP (*Dynamic Host Configuration Protocol*).

3.3 FERRAMENTAS DE PROXY

A seguir serão analisadas algumas ferramentas de proxy onde uma delas está exposta no presente trabalho.

3.3.1 TINYPROXY

De acordo com os desenvolvedores, o *TinyProxy* é um proxy HTTP/HTTPS de sistemas operacionais *posix*, considerado uma ótima solução para os casos com necessidade de um *proxy* HTTP com vários recursos, mas que os recursos deste sistema não suportam um servidor *proxy* maior. Tratando-se de um *software* pequeno, ele consome poucos recursos do sistema, podendo ser instalado em máquinas com menos recursos de *hardware* ou até mesmo roteadores baseados em Linux. Instalado com configuração mínima, mas, podem ser adicionadas bibliotecas de acordo com a necessidade.

3.3.2 PRIVOXY

É um *proxy* web não cache que possui opções avançadas possibilitando uma alta privacidade. Ele pode ser utilizado para alterar dados de páginas da web e cabeçalhos HTTP, também pode ser usado no controle de acesso e remoção de anúncios indesejáveis em páginas da internet, além de possibilitar alterações atendendo de acordo com as necessidades.

3.3.3 SQUID

O *Squid* referido *proxy* que é objeto de estudo deste trabalho, é um serviço que permite o compartilhamento da conexão de internet com outras variadas máquinas da rede. De acordo com Paulino (2009), a utilização do *Squid* instalado em um servidor que esteja conectado à internet, possibilita que outras máquinas executem sistemas operacionais distintos, páginas web e FTP por meio do servidor. Para ele, o *Squid* é um software especializado em realizar operações

de *proxy* web e FTP, totalmente livre e com excelente suporte para operações em servidores Linux.

Segundo Rick (2012) este servidor *proxy* funciona como uma saída principal da rede. Logo, pode-se centralizar o foco em segurança criando políticas de acesso, autenticação de usuários, registros e controle centralizado.

3.4 HISTORICIDADE DO SQUID

De acordo com Nordstrom (2013 apud Oliveira; Santos 2013), o *Squid* surgiu com a necessidade de controlar e qualificar o acesso à Internet. Em 1994 surgiu o HTTP CERN, primeiro servidor que desempenhava a função de cache e proxy. Ainda neste ano o *Internet Research Task Force Group on Resource Discovery* (IRTF-RD), iniciou o desenvolvimento de um projeto de ferramentas com a finalidade de coletar, extrair, localizar, organizar e fazer cache de informações da internet, onde se nomeou de *Harvest*. Quanto ao *cache* do *CERN*, o *Harvest* trouxe consideráveis melhorias, em relação a hierarquia de cache através da internet, o design de processo único e a velocidade no uso de sistema de arquivo

Em 1995 alguns membros do *Harvest* abandonaram o projeto. Os autores originais do código cache, o tornaram em produto comercial. No ano seguinte o projeto *Harvest* uniu-se ao projeto *Information Resource Cache* (IRCache), financiado pela *Nacional Science Fundation*. Posteriormente, houve alteração do código, de cache *Harvest* para o nome *Squid* e sua licença liberada. Em julho 2000, o financiamento do projeto foi encerrado e deste então seu desenvolvimento tem sito feito por voluntários.

3.5 SARG

Conforme Cisneiros (2003), o *Squid Analysis Report Generator* (Sarg), é uma ferramenta desenvolvida pelo brasileiro Pedro Orso e com ela é possível analisar os arquivos de log do *Squid*, como o acess.log possibilitando a extração de gráficos estatístico e relatórios. Destas formas pode-se analisar todos os acessos e movimentações WEB, como relatórios de sites mais acessados, horários e

usuários do acesso, quantidade de conexões e *bytes* baixados, sites negados, falhas na autenticação, entre outros. Esta ferramenta possibilita que os administradores de rede tenham controle de todo o conteúdo acessado pelos usuários na internet

3.6 BENEFÍCIOS DO USO DO PROXY

Como já dito, o uso do servidor *proxy* é de suma importância e gera um considerável benefício, principalmente, empresas e universidades que possuem um alto índice de usuários com acesso à internet. Com o uso do servidor *proxy*, este acesso torna-se limitado e controlado facilitando o controle de gerenciamento. Imagina-se que que em uma determinada empresa há pelo menos 20 pessoas com acesso diário à internet, com o programa é possível configurar bloqueios de sites, páginas, e evitar a sobrecarga na utilização, permitindo somente o download de arquivos necessários.

Existem fatores significativos para o uso do servidor *proxy*, dentre eles estão:

- Controle centralizado: com apenas um único ponto de acesso à internet o gerenciamento torna-se mais fácil, uma vez que se pode controlar todo o acesso à rede.
- Segurança: como há apenas um *proxy* conectado à internet, é possível concentrar todos os esforços para melhorar a segurança somente desta, que realmente é a única que está desprotegida ou potencialmente vulnerável.
- Autenticação: com este sistema, somente usuários autorizados terão acesso à internet, desta forma melhorando a segurança
- Registros de acessos: podendo ser utilizado para diversas finalidades, que irão deste a análise do servidor até a geração de relatórios detalhados do acesso à internet. Estes acessos são registrados em logs do *Squid*.

Dentre estas e outras vantagens, o servidor proxy tem sido utilizado cada vez mais dentro de empresas e outros estabelecimentos, para controle de acesso, tornando o *Squid* um servidor de credibilidade e confiança.

3.7 DESVANTAGENS NO USO DE PROXY

O ponto conflitante que há neste servidor é que sempre será exigido a autenticação do usuário, sendo obrigatório digitar as credenciais cadastradas toda vez que necessitar do acesso à internet. O que pode levar certo desconforto aos usuários a adequação desta mudança.

Outro ponto a ser considerado, é quanto a sua instalação que necessita de uma mão de obra qualificada para a configuração do *Squid*, o que pode gerar um custo extra para a empresa.

4 PROJETO

Por questão de inviabilidade financeira de se implementar a reorganização da estrutura cabeada, além disso, seria necessário a abertura de licitação para a instalação do projeto. Entretanto como medida preventiva de segurança foi implementado o servidor *proxy Squid*, com controle de acesso, *cache* de páginas e relatórios, como já descrito no trabalho, este servidor está sendo executado como um programa de controle de acesso, navegação e melhoria quanto a velocidade da rede.

4.1 INSTALAÇÂO DO SQUID

A figura 4 demonstra o comando para instalação do *proxy Squid* que é composto de um único pacote, por isso a instalação é simples, a instalação foi realizada no terminal Linux Debian 9.

Figura 4 Instalação Proxy Squid Fonte próprio ator

4.2 CONFIGURAÇÃO DO SQUID

A figura 5 ilustra a configuração do *proxy Squid*

Figura 5 Configuração do Proxy Squid, fonte próprio autor

Toda a configuração do *Squid* é realizada no único arquivo, que se encontra por padrão no diretório “/etc/squid/squid.conf”. O arquivo original que já vem instalado junto com o pacote vem com a documentação e comentários com exemplos para quase todas as opções disponíveis.

A figura 6 demonstra alguns comandos suficientes para que o *Squid* “Funcione”.

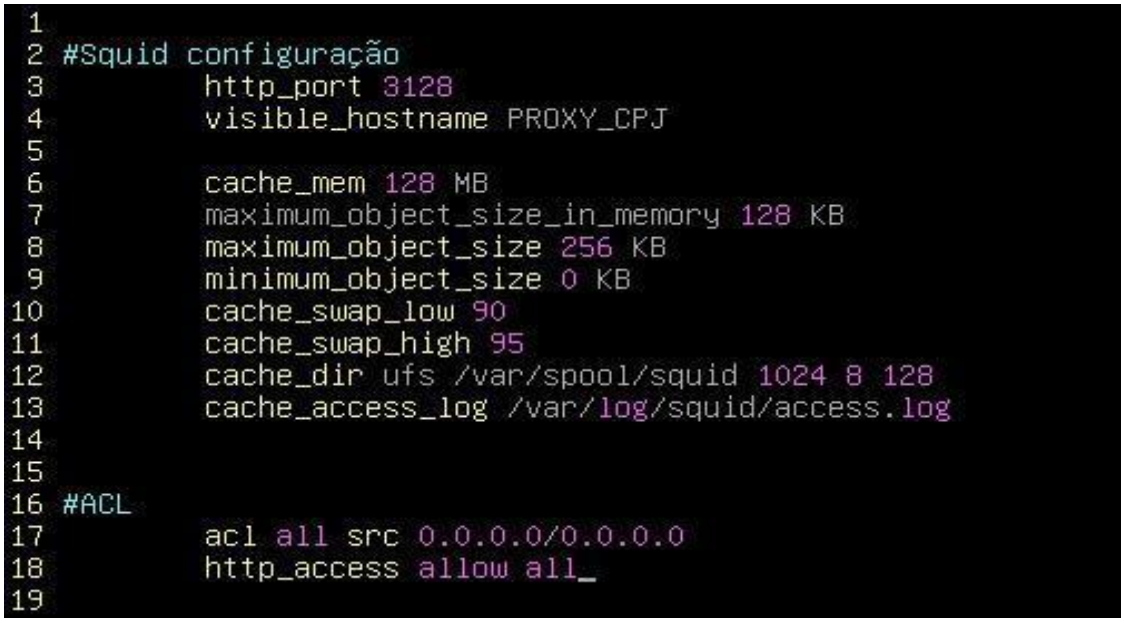

Figura 6 Configurando Proxy Squid, fonte próprio ator

- **http_port 3128:** A porta onde o servidor *Squid* vai ficar disponível. Sendo a porta default 3128, porem podendo ser utilizados pelos outros administradores a porta 8080.
- **visible_hostname PROXY_CPJ:** O nome do servidor, que ficara visível na hora da navegação no acesso negado no caso ficara com o nome do proxy_cpj.
- **cache_mem 128 MB:** É a configuração da quantidade de memória RAM que será reservada para o cache de memória, por padrão para cache utilizado em um servidor não dedicado são reservados 32 ou 64MB.
- **maximum_object_size_in_memory 128 KB:** é a configuração do cache que será feita no disco, que armazenará o grosso dos arquivos.

- **maximum_object_size 256 KB:** Por default, o máximo são downloads de até 16mb, na figura 6 foi reservado 256kb máximo para cada objeto que ficará salvo no cache do disco.
- **minimum_object_size 0 KB:** Por default fica reservado 0 KB, que seria o mínimo arquivo que pode ser salvo.
- **cache_swap_low 90:** É o mínimo porcentagem de uso do cache que fará o Squid começar a descartar os arquivos antigos para não encher o cache.
- **cache_swap_high 95:** É o máximo de porcentagem do uso do cache, sempre que o cache atingir 95% de uso, serão eliminados os arquivos antigos até que a percentagem volte para um número abaixo do cache_swap_low.
- **cache_dir:** é composta por quatro valores. O primeiro (**/var/spool/squid**) mostra a pasta aonde o *Squid* armazena os arquivos do cache, o segundo (**1024**) indica a quantidade de espaço no HD (MB) que sera utilizada para o cache, o terceiro (**8**) e o quarto (**128**) indicam a quantidade de subpasta que serão criadas dentro do diretório, Por padrão, temo 8 pasta com 128 subpastas cada uma.
- **cache_access_log /var/log/squid/access.log**: é o diretório que serão guardados os logs de acesso do *squid*. Este arquivo é usado pelo SARG para realizar relatórios de acessos.
- **Acl all src 0.0.0.0/0.0.0.0** e **http_access allow all**: estar duas linhas criam regra de politica de acesso ACL, se chamando de “*all*” que ficará disponível todos os endereços IP possíveis liberando os acesso a todos “*allow all*” e para negar é utilizada “*http_access deny all*”

A figura 7 demonstra como reiniciar o *Squid*

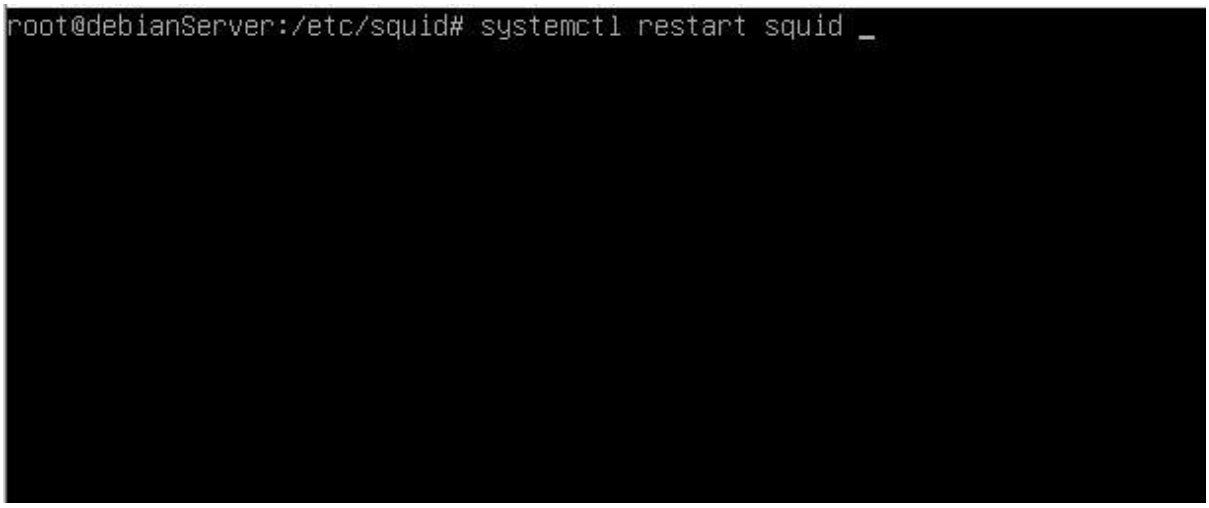

Figura 7 Reiniciando proxy Squid, fonte próprio ator

Para aplicar as configurações é necessário que reinicia o servidor *Squid*. Para testar o proxy é necessário configurar a máquina do cliente para apontar para o endereço do servidor proxy na porta 3128.

5. CONCLUSÃO

Foi implementado o servidor *Proxy Squid*, no Central de Polícia Judiciária do município de Assis (CPJ), com as regras ACL específica para cada departamento/usuário, melhorando consideravelmente a rede, fornecendo relatórios ao responsável, melhorando o ritmo do órgão, impedindo acessos indevidos ou desnecessários para função e melhorando a segurança e agilidade.

A restruturação da rede começará a ser executada após a licitação e liberação da verba para o projeto.

6. REFERÊNCIAS

ALECRIM, E. **O que é firewall? – Conceitos, tipos e arquiteturas.** 2013. Disponivel em: http://www.infowester.com/firewall.php Acesso em 09 junho 2019

CERVO, Amado Luiz; BERVIAN, Pedro Alcino; SILVA, Roberto da. **Metodologia Cientifica**. 6 ed. São Paulo: Pearson Prentice Hall, 2007.

CISNEIROS, H. **Sarg.** 2003. Disponível em: http://www.devin.com.br/sarg/ Acesso em 5 junho de 2019.

DESENVOLVEDORES PRIVOX. **Privoxy – Home Page.** Disponível em: https://www.privoxy.org/. Acesso em 3 junho 2019.

DESENVOLVEDORES TINYPROXY. **Tiniproxy.** Disponível em: https://tinyproxy.github.io/>. Acesso em 04 junho 2019.

Equipe Digerati Books. **Guia Técnico de Redes Windows**. Digerati Books, São Paulo, 2009.

FINK, Lior. NEUMANN, Seev. ***Journalof the Association for Information Systems*.** 2007. Disponível em: <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1421&context=jais>. Acesso em 17 nov. 2018.

KUROSE, James; ROSS, Keith. **Redes de computadores e a Internet: uma abordagem top-down**. 5ª ed. Tradução Opportunity translations. São Paulo: Editora Addison Wesley, 2010.

Kahlmeyer-Mertens, Roberto S.; [et. al.] . **Como elaborar projetos de pesquisa:**

Linguagem e método. Editora FGV. 1º Edição. Rio de Janeiro, 2007.

KELLER, Alexandre. **Asterisk na Prática**. Novatec Editora, 2ª Ed. 2011.

MARCONDES, José Sérgio. **Conceito de Cronograma: Que é? Definição, Aplicações, Exemplos.** Disponível em: <https://www.gestaodesegurancaprivada.com.br/conceito-de-cronograma-que-e-definicao/>. Acesso em 26 out. 2018.

MORIMOTO, C. E. **Servidores Linux – Guia Prático.** Porto Alegre: Sul Editores, 2011, 735 p.

MORIMOTO, C. E. **Configurando o proxy transparente nas novas versões do Squid.** 2006. Disponível em: http://www.hardware.com.br/dicas/configurando-proxy-transparente-nas-novas-versoes-squid.html. Acesso em 15 junho 2019

OLIVEIRA, I, L; SANTOS, L, M. **Análise de Desempenho de cache de Dados no Squid e Haarp**. 2013. Disponível em: http://lab.fateclins.edu.br/site/trabalhoGraduacao/P7gvHtXTkCjkCh8Hd2Z5iy2lJERsOQZ.pdf. Acesso em 14 junho 2019

PAULINO, D. **Squid o que é?**. 2009. Disponível em: https://www.oficinadanet.com.br/artigo/1998/squid_o_que_e. Acesso em 15 maio 2019

PINHEIRO, J, M, d, S, **Guia Completo de cabeamento de Redes**. Ed 2.- Rio de Janeiro Elsevier Brasil 2015.

PINHEIRO, J, M, d, S, **Redes ópticas de acesso em telecomunicações.** Ed 1 - Rio de Janeiro. Elsevier Brasil 2017

RIBEIRO, FERNANDO. **Configuração automática do proxy.** 2016. Disponivel em https://servidordebian.org/pt/jessie/intranet/proxy/wpad. Acesso em 1 junho 2019

RICK, G. **Servidor proxy com Squid instalação e configuração.** Viva o Linux. Jul. 2012. Disponível em: http://www.vivaolinux.com.br/artigo/Servidor-proxy-com-Squid-Instalacao-e-configuracao?pagina=1. Acesso em 3 Maio 2019

ROSS, Julio. **Cabeamento estruturado.** 1. Ed. Rio de Janeiro, Antenna, 2007

SIQUEIRA, Luciano Antônio. **Infraestrutura de Redes**. Linux New Media do Brasil Editora Ltda, São Paulo, 2010

TANENBAUM, Andrews S. **ComputerNetworks.** Editora Campus. *Trad. Vandenberg D. de Souza.* Amsterdam, Holanda, 2010.

TIBET, C. V. **Linux Administração e Suporte.** São Paulo: Novatec, 2001. 379p.
PINHEIRO, José Maurício dos S. **Guia Completo de Cabeamento de Redes**. Elsevier, Rio de Janeiro, 2003

ZANONI, G. **Servidor Proxy (Squid).** 2007 Disponível em: http://imasters.com.br/artigo/6220/linux/servidor-proxy-squid. Acesso em 2 Maio 2019