Implementando autenticação de segurança com um servidor Freeradius em uma rede wi-fi com AP's Unifi gerenciados pelo sistema operacional RouterOS

Guilherme Levy[1], Cleber Caldana[1]

[1]Pós-Graduação em redes de computadores Academia CISCO - Faculdade Guairacá

ti@faculdadeguairaca.com.br, caldana.cleber@gmail.com

Abstract. *This article introduces the concept of security authentication for connection to a wi-fi network, as well as component and method information needed to configure a RADIUS server. Next, it will be demonstrated the installation and configuration of the Debian operating system with the Freeradius tool on a server that will search the authentication credentials in a SQL database, in order to manage and select the users that connect in the wi-fi network using the EAP protocol, improving security and data traffic effectively and blocking unauthorized users' access to the network.*

Resumo*. O presente artigo traz o conceito de autenticação de segurança para conexão em uma rede wi-fi, além de informações de componentes e métodos necessários para configuração de um servidor RADIUS. Em seguida será demonstrada a instalação e configuração do sistema operacional Debian com a ferramenta Freeradius em um servidor que fará a busca das credenciais de autenticação em um banco de dados SQL, com o objetivo de gerenciar e selecionar os usuários que se conectam na rede wi-fi utilizando o protocolo EAP, melhorando a segurança e o tráfego de dados de forma eficaz e bloqueando acessos de usuários não autorizados à rede.*

1. Introdução

Provavelmente a *Internet* pode ser considerada o maior sistema de engenharia já criado pelo homem, são bilhões de dispositivos e usuários que necessitam utilizar as centenas de milhões de rotas e enlaces para conectá-los ao redor do mundo, hoje a *Internet* é utilizada em quase todos os segmentos de um ambiente corporativo, seja ele de vendas ou prestação de serviços, sendo que seu uso torna-se quase indispensável para manter a empresa competitiva em meio às constantes mudanças, Kurose e Ross (2013).

O panorama das redes mudou muito desde os anos 90 e inicio dos anos 2000, nessa época podíamos encontrar grandes tipos de *LAN's* e *WAN's*, sem contar a numerosa quantidade de protocolos, hoje podemos afirmar que a rede *Ethernet* domina o cenário mundial, entretanto a tecnologia das redes sem fio obteve um grande salto na quantidade de utilizadores pela conveniência e praticidade na utilização dos dispositivos móveis, Tenenbaum (2003).

Com o crescimento exponencial das redes sem fio criaram-se novos riscos aos dispositivos e usuários e consequentemente novos desafios às empresas desenvolvedoras e aos administradores de redes, portanto foram necessários investimentos para o desenvolvimento de tecnologias que aliem mais segurança e qualidade na utilização dessas redes. Além dos riscos à segurança, que podem ser minimizados com regras de acesso à rede e utilização de ferramentas que utilizem protocolos de autenticação de usuários podemos enumerar outros dois quesitos importantes que devem ser observados para que os usuários tenham uma boa usabilidade dos dispositivos móveis na rede *wi-fi*; restrições na taxa de transferência de dados de um ponto a outro da rede (*throughput*) e especificações de capacidade de tráfego dos equipamentos que disponibilizam o acesso sem fio à rede (*Access Points*), Nakamura e DeGeus (2007).

Durante esse projeto foi identificada a necessidade de implementação de segurança no momento da conexão do usuário à rede *wi-fi* para um consequente aumento do *throughput* entre os usuários e os *Access Points*, desse modo poderá se garantir um serviço amplo, seguro e de qualidade em uma instituição que fornece aos seus quase 2500 usuários cadastrados um serviço *Hotspot* gratuito de conexão à *Internet*.

Os *Access Points* atuais possuem severas limitações quanto ao seu *throughput* se compararmos aos equipamentos da rede cabeada, portanto dispositivos conectados à rede *wi-fi* de usuários que não possuem credenciais para autenticação no *Hotspot* da instituição criam um tráfego de dados inútil e perigoso, prejudicando o desempenho dos *Access Points* e colocando em risco a segurança dos usuários já autorizados a trafegar nessa rede. A implementação dessa autenticação no servidor *Freeradius* tem como finalidade filtrar e bloquear os usuários que não possuem autorização para se conectar à rede *wi-fi*, fazendo com que nos *Access Points* somente trafegue dados de usuários autorizados.

Este projeto traz métodos e técnicas para a implementação de segurança por meio de um servidor de autenticação que fará a verificação das credenciais e a posterior liberação dos usuários ao tentarem se conectar na rede sem fio da instituição, fazendo com que o tráfego diminua nos *Access Points*, trazendo mais agilidade e segurança aos usuários autorizados e conectados.

2. Fundamentação teórica

Na sociedade contemporânea a utilização das redes de computadores e a *Internet* são imprescindíveis para quase todos os ramos que utilizam os sistemas de informação. A *Internet* pública é basicamente uma rede de computadores em escala mundial, ou seja, ela é responsável por conectar milhões de equipamentos, desde computadores pessoais, servidores e dispositivos móveis em todo o planeta, Kurose e Ross (2003). As redes de computadores foram criadas a partir da necessidade de compartilhar recursos da informação e computacionais, como impressoras e arquivos nas empresas, um dos primeiros sistemas utilizados com o auxílio das redes de computadores foi em 1964 para reservas de passagens aéreas, Pinheiro (2003). Hoje podemos afirmar que a Internet revolucionou a transmissão de informações e as comunicações, basta que o computador seja ligado para que estejamos conectados literalmente ao mundo, Kalinke (2003), ainda sobre a Internet pode-se afirmar que a quantidade de informações disponibilizadas em

milhares de sites é imensa e pode ter várias finalidades como acesso a sites de empresas com produtos e serviços e conteúdo informativo com assuntos diversificados como política, economia, estudo, empregos e esportes, Costa (2007).

Uma rede de computadores pode ser composta por uma grande variedade de equipamentos, como roteadores, *Access Points*, servidores, *switches*, *gateways*, cabos, outros equipamentos além dos *softwares*, a partir desses equipamentos a rede possui basicamente três meios de transmissão, cabos metálicos por onde são transmitidos sinais elétricos, fibra ótica na qual os dados são transmitidos por sinais luminosos e transmissão por irradiação de ondas de rádio, na atualidade, em todos esses três casos precisamos nos preocupar basicamente com dois importantes pontos, *throughput* e segurança, portando novas tecnologias são desenvolvidas para aprimorar a cada dia mais essas transmissões, Sousa (2010).

A *Internet* opera por meio da distância, tempo e línguas diferentes, por meio de um ambiente multi-conectado, permitindo que as pessoas compartilhem e acessem informações de forma mais dinâmica e com vários processos, Rainer e Cegielski (2011). O uso da *Internet* traz eficiência aos negócios das empresas, fazendo com que elas possam alcançar sucesso em um mundo globalizado, seja no ramo de produtos e serviços, atendimento ao cliente ou outro setor que sempre esteja em mudança devido às novas tecnologias, O'Brien (2006).

Uma rede de computadores associada à *Internet* tem várias funções para um segmento, como por exemplo, ser um meio de comunicação eficaz entre os funcionários de uma empresa, utilizando recursos como o correio eletrônico (*e-mail*), podendo ser um facilitador em negócios eletrônicos com outras empresas, fornecedores e clientes e tornando mais eficiente a realização da compra ou venda de suprimentos, Tanembaum (2003). Complementando, pode-se afirmar que a aliança entre equipamentos de informática e a *Internet*, melhorou a agilidade e praticidade ao acessar informações e no gerenciamento nos bens intangíveis de uma empresa, com o principal objetivo de dinamizar processos que antes eram burocráticos e que demandavam um maior tempo e pessoas envolvidas, Primak (2009).

Pequenas e médias empresas podem ter mais de uma filial, inclusive em outras localidades ou países, a *Internet* também possibilita uma comunicação imediata para resolução de problemas, facilitando o acesso a informações disponibilizadas em modo *on-line* como extratos financeiros, averiguação de impostos e estoques, entre outros, independente de sua disposição geográfica, Tanembaum (2003). A ligação entre os computadores é usada em cada área do negócio, seja na propaganda, na produção ou transporte de produtos até seu uso final como o faturamento e contabilidade, Comer (2009).

A inserção de novas tecnologias de informação e comunicação no ambiente institucional aumentam os processos de produção de redes pessoais e coletivas, dando oportunidade à criação de rotas alternativas e criativas entre os pontos conectados. Essa rede de usuários conectados proporciona a superação das barreiras disciplinares e das hierarquias de conteúdo, Magdalena e Costa (2003).

Com todo esse crescimento da utilização da *Internet*, veio a necessidade de segurança, pois enquanto aumenta a velocidade e a eficiência em todas as áreas dos negócios a falta de segurança nos meios onde a *Internet* trafega pode resultar em grandes prejuízos, Nakamura e DeGeus (2007). Os crimes virtuais são frequentes e

podem atingir desde o usuário residencial com seus dados pessoais ou sua conta bancaria como informações confidenciais de grandes empresas, Carvalho (2005). Complementando, podemos citar algumas situações que as empresas estão expostas como o acesso físico ou lógico de pessoas não autorizadas a lugares restritos, a obtenção de senhas de usuários e até mesmo o acesso aos locais onde equipamentos físicos estão alojados. Portanto é necessário utilizar sistemas de segurança eficazes como servidores de *Firewall*, *Web Proxy* e sistemas de autenticação de usuários para tentar minimizar esses problemas, Torres (2010).

Desse modo é necessária a implantação de políticas de segurança em uma rede, ou seja, regras e padrões sobre o que e como deve ser feito para assegurar que os acessos à rede e às informações que nela trafegam recebam a proteção devida. Uma política de segurança utilizada em redes e sistemas é a autenticação de usuários, ela tem a função de validar as credenciais informadas pelo usuário, autorizando ou não o acesso desse usuário à rede, sistema ou arquivo, Carvalho (2005). Ainda podemos afirmar que a autenticação e o controle de acesso de usuários tem como função limitar a utilização dos sistemas e aplicações baseados nos enlaces de comunicação da rede, Stallings (2008), portanto todo sistema computacional que tem a intenção de ser seguro deve determinar que o seu usuário faça a autenticação de suas credenciais ao conectar-se, Tanembaum (2009).

A autenticação das credenciais do usuário pode ser basicamente de quatro maneiras, com base no que o usuário sabe: senhas, chaves criptográficas e *PIN*, com base no que o usuário tem: *token* ou cartão, com base nas características do usuário: biometria, reconhecimento facial ou de íris, etc, ou então, com uma combinação desses modos anteriores: cartão bancário que ainda pede uma senha, Carvalho (2005).

Com esse aumento da utilização da *Internet* em ambientes empresariais e de acesso público necessita-se também de um modo de otimizar e garantir a disponibilização da conectividade com qualidade e segurança por meio de um processo de autenticação de usuários cadastrados, para um controle mais amplo da rede é possível utilizar o *RouterOS* como servidor de rede. Segundo a documentação oficial de sua desenvolvedora Mikrotik, site wiki.mikrotik.com (2018), o *RouterOS* é um sistema operacional *stand-alone* baseado no *Kernel Linux* v.3.3.5, instalado em um microcomputador ou rodando em seu próprio hardware proprietário (*Routerboard)* ele transforma-se em um poderoso servidor de rede com várias ferramentas, tais como servidor *DHCP*, cliente *DHCP*, *Hotspot*, limitador de banda, *Firewall*, *WebProxy*, *VPN*, entre outros. Um servidor de rede é um equipamento cuja função primária é servir e controlar a rede a partir de regras, que são os parâmetros de configuração que lhe são atribuídos, Primak (2015).

Hotspot é uma ferramenta de disponibilização de serviços de *Internet*, sejam eles pagos ou gratuitos, essa ferramenta normalmente é utilizada em redes sem fio em locais públicos. O *Hotspot Mikrotik* nos oferece vários métodos de autenticação de usuários para navegação. Além de utilizar um banco de dados local para as credenciais de autenticação para a navegação, a ferramenta *Hotspot Mikrotik* pode utilizar também um servidor externo de autenticação, Stato (2017), uma dessas ferramentas para autenticação externa chamada *Freeradius* roda sobre o *Linux*, um sistema operacional gratuito, robusto e completo que por sua estabilidade pode exercer a tarefa de um servidor, Anunciação (2007).

No mercado existem vários produtos que utilizam o protocolo *RADIUS*, entre os de código aberto podemos citar o *Freeradius* e o *GNU Radius*, atualmente o Freeradius possui mais recursos e aceita uma maior quantidade de métodos de autenticação que o seu rival, Rufino (2011). A ferramenta *Freeradius* utiliza o protocolo *RADIUS* [RFC 2865] para criar uma comunicação entre o *Access Point* e o servidor de autenticação, permitindo assim a centralização das decisões de autenticação e acesso de vários *Access Points* em um único servidor, mantendo os custos baixos e uma boa segurança nesses dispositivos, o protocolo IEEE 802.11i que define os aspectos de segurança da família 802.11 utiliza essa técnica. Na estrutura de funcionamento do IEEE 802.11i, além do *Access Point* e do cliente sem fio utiliza-se um servidor de autenticação, com o qual o *Access Point* se comunica solicitando a confirmação ou negação da conexão do dispositivo sem fio, Kurose e Ross (2013). Os *Access Points* são dispositivos que fornecem conectividade a microcomputadores e dispositivos móveis, não necessitando o uso de cabeamento, Nakamura e De Geus (2007).

O servidor *Freeradius* utiliza o protocolo fim a fim *EAP* (protocolo de autenticação extensível) para autenticação dos clientes sem fio, as mensagens *EAP* são encapsuladas utilizando o *EAPoL* (*EAP* on *LAN*) e encaminhadas através de um enlace sem fio 802.11 entre o *Access Point* e o cliente e utilizando o protocolo *RADIUS* por meio de *UDP*/*IP* entre o *Access Point* e o servidor de autenticação, Kurose e Ross (2013). O protocolo *EAP* possui variações de geração de chaves e autenticação mútua entre os clientes sem fio e os *Access Points*, segundo a documentação oficial do site microsoft.com (2018) um deles é o *PEAP* (*Protected EAP*), desenvolvido pela *CISCO* e *Microsoft*, ele cria um canal criptografado entre o cliente sem fio e o servidor de autenticação *RADIUS*.

De acordo com Rufino (2011), o *Freeradius* reconhece vários métodos de autenticação, entre ele o *MySQL DB*, que permite a utilização de um banco de dados externo *MySQL* com as credenciais dos usuários cadastrados.

O banco de dados é uma coleção de dados, eles são uma parte essencial para o dia a dia na sociedade, sua tecnologia tem um importante papel no crescimento do uso de microcomputadores, pois eles são registros dos fatos conhecidos e que possuem um significado implícito, como por exemplo, nomes de amigos e telefones guardados no disco rígido de um computador, Elmarsi e Navathe (2011), ou seja, o **dado** consiste um fato ou material bruto na produção da informação, Audy, Andrade e Cidral (2005). Um banco de dados pode ter qualquer tamanho e nível de complexidade, dependendo de seu uso, desde uma agenda telefônica guardada em uma planilha, credenciais de autenticação em um servidor ou um gigantesco banco de dados como o da Receita Federal que monitora os dados de entrega de declaração de imposto de renda dos últimos três anos dos brasileiros, Elmarsi e Navathe (2011).

Para criar e fazer a manutenção da estrutura desses bancos de dados utilizamos conjuntos de comandos de manipulação, o *SQL* (*Structured Query Language*) é um desses conjuntos. Para utilização desse conjunto de comandos em um servidor *Debian* podemos utilizar o *My-SQL Server*, o programa é executado como um servidor e possibilita aos usuários gerenciar diversos bancos de dados, assim como o utilizado pelo *Freeradius* no cadastro dos usuários do servidor de autenticação, Oliveira (2002). O *MySQL* é um dos sistemas de gestão de banco de dados que suportam o *SQL*, ele é um sistema de código aberto e é um dos mais utilizados sistemas de gerenciamento de

banco de dados relacionais no mundo, para facilitar as operações nas estruturas de dados dentro do *MySQL* podemos utilizar ferramentas auxiliares, tais como *PhpMyAdmin*, *MySQL Administrator*, *MySQL Query Browser*, etc, Neves e Ruas (2005).

3. Aplicação prática

O presente projeto baseou-se na ideia que uma conexão à *Internet* tornou-se indispensável à vida cotidiana de pessoas e empresas, seja para fins de lazer, trabalho ou estudo, tendo em vista essa necessidade de conexão contínua, deve-se então considerar a manutenção de um nível aceitável de qualidade e segurança para que as atividades executadas não sejam prejudicadas. Dessa maneira esse projeto identificou a necessidade de impor regras de conexão aos usuários de uma rede *wi-fi*, com a finalidade de melhorar o *throughput* da conexão e dar mais segurança aos seus usuários.

O projeto foi planejado e desenvolvido em uma instituição de ensino superior que disponibiliza aos seus quase 2500 clientes entre acadêmicos, professores e funcionários, uma conexão gratuita à *Internet* por meio de uma rede *wi-fi* sem chave de segurança, mas com um servidor *Hotspot* exigindo a autenticação dos usuários cadastrados. Os clientes que se autenticam no *Hotspot* e navegam nessa rede *wi-fi* utilizam basicamente *notebooks* e *smartphones* para fins de estudo e recebem uma limitação de banda de 5*Mbps*.

Anteriormente à implementação do projeto esse ambiente possuía um servidor *RouterOS*, que gerenciava através da ferramenta *Hotspot* a autenticação dos usuários já conectados à rede *wi-fi* que era propagada por *Access Points Ubiquiti Unifi* sem chave de segurança. A figura 1 a seguir mostra a representação da infraestrutura física da rede anterior à implementação do projeto.

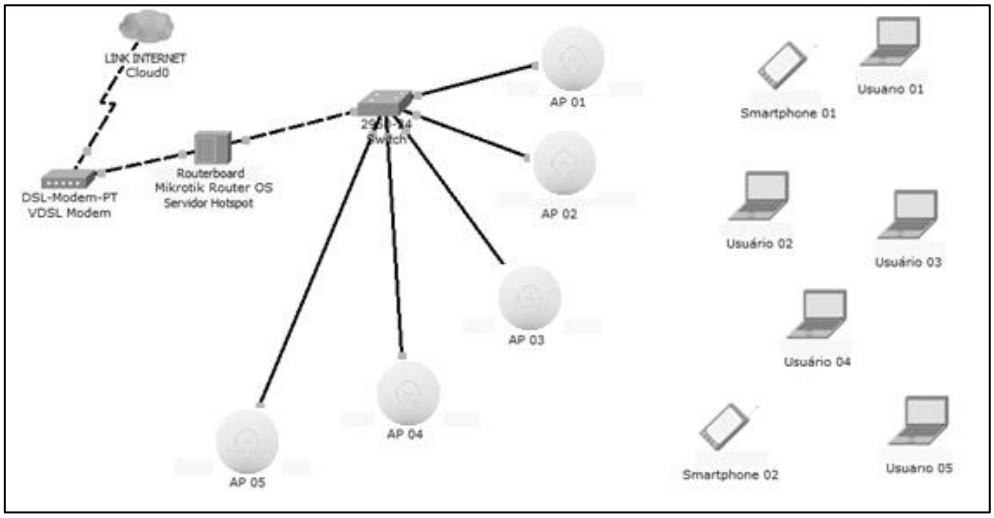

Figura 1: Representação da infraestrutura de rede do ambiente acadêmico anterior à implantação do servidor *Freeradius*.

O *link* de *Internet* de 100*Mbps* era autenticado em um modem *VDSL* e enviado diretamente ao servidor *RouterOS* que fazia o seu gerenciamento, e em seguida a

implementação de todas as suas regras de acesso, após isso distribuía o *link* já tratado aos *Access Points*. Dessa maneira, todos os usuários, mesmo sem credenciais para a autenticação no *Hotspot* e consequente navegação na *Internet* conseguiam se conectar à rede *wi-fi*, fazendo com que os *Access Points* tivessem um grande tráfego inútil de usuários conectados, mas não autorizados à navegação, muitos deles pessoas que simplesmente passavam por frente da instituição e conectavam-se por verificar que a rede não possuía chave de segurança para o acesso, diminuindo assim consideravelmente o desempenho e segurança desses pontos de acesso sem fio e dos usuários neles conectados, chegando ao ponto em horários de pico, de o cliente não conseguir abrir a tela de login no *Hotspot* pela quantidade muito grande de tráfego entre os *Access Points* e o cliente, no mesmo momento em que o *link* de Internet tinha no máximo vinte por cento de utilização. Isso mostrava que o problema na lentidão da rede *wi-fi* era devido ao congestionamento do tráfego entre os *Access Points* e usuários, e não no *link* de *Internet*.

Depois de verificados os erros existentes na infraestrutura utilizada, buscou-se então uma proposta de implementação de um servidor que fizesse a verificação e autenticação dos usuários já no momento da conexão à rede *wi-fi*, diminuindo assim o número de acessos dos usuários não autorizados à navegação conectados à rede *wi-fi* e consequentemente o tráfego de dados entre os *Access Points* e os clientes sem fio, melhorando o *throughput* dos usuários conectados e autorizados.

Após a proposta elaborada ser aprovada pela direção da instituição o primeiro passo foi escolher um sistema operacional robusto e confiável, capaz de suprir essas necessidades e que possuísse essa funcionalidade buscada, esse sistema operacional também deveria possuir uma ferramenta que criasse um servidor *Radius*, protocolo essencial para o desenvolvimento do projeto. Após testes com sistemas de variadas distribuições e versões o escolhido foi o sistema operacional *Linux Debian* 7.4 (Wheezy), que possui disponibilizado o pacote com a ferramenta gratuita *Freeradius*, esse sistema foi instalado em um microcomputador com uma configuração básica, processador *Intel Celeron E4300, 2Gb RAM DDR3, HD 160GB SATA2*.

Após a escolha do sistema operacional para a base da nossa implantação precisamos criar na controladora dos *Access Points* a rede *wi-fi* com o perfil e os parâmetros necessários para a autenticação em um servidor *Radius*. Utilizando a *Unifi Controller 5.0.7* criamos a rede wi-fi com a opção de segurança *WPA-Enterprise*, que nos dá a opção de autenticar os usuários que solicitam a conexão em um servidor *Radius*, com a utilização dessa chave é solicitado o endereço de *IP* do equipamento e a porta onde está rodando o servidor *Radius*, e o *Access Point* poderá assim confirmar as credenciais informadas pelo usuário que deseja se conectar à rede *wi-fi*.

Após criarmos a rede *wi-fi* efetuamos a instalação e configuração do servidor *Debian* para a posterior implantação de todos os pacotes e dependências necessárias para o funcionamento da ferramenta *Freeradius*. No equipamento que foi instalado o sistema operacional *Debian* foi especificado um endereço de *IP* fixo para que os *Access Points* acessem corretamente o endereço de *IP* do servidor ao solicitarem a confirmação das credenciais. Após o fim da instalação do *Debian* nós efetuamos uma atualização completa do sistema operacional para deixá-lo o mais completo possível em relação aos seus pacotes, fontes e dependências.

Logo em seguida instalamos o pacote da ferramenta *Freeradius,* versão gratuita da ferramenta que utiliza o protocolo *Radius* para autenticação, um servidor de autenticação permite autenticar utilizadores, equipamentos, serviços, etc. Quando efetuada a instalação desse pacote já foi instalado automaticamente a ferramenta *My-SQL Server*, que será necessária para manipulação dos bancos de dados dos usuários e *Access Points* cadastrados.

No momento da instalação do pacote *Freeradius* junto ao pacote do *My-SQL Server* foi necessário efetuar a criação de um usuário *ROOT* e senha do *My-SQL*, após a confirmação desse usuário o *Debian* finalizou o procedimento de instalação do *Freeradius*.

Depois de finalizada a instalação foi necessário efetuar as mudanças nos arquivos de configuração do *Freeradius* como mostra a tabela a seguir.

Tabela 1: Arquivos de configuração do *Freeradius*

Arquivo	Alteração
/etc/freeradius/radiusd.conf	Ativar as duas regras que se referem à conexão do *Freeradius* com o banco de dados *MySQL*
/etc/freeradius/sql.conf	Configurações dos parâmetros de conexão do *Freeradius* com o banco de dados no *MySQL-Server*, nesse arquivo iremos utilizar o usuário e senha que criamos na hora da instalação do *My-SQL Server* e especificaremos o nome do banco de dados do *Freeradius* no *My-SQL*
/etc/freeradius/clientes.conf	Incluir a rede e máscara dos *Access Points* que irão solicitar ao *Freeradius* a conexão e a chave que foi cadastrada quando criamos a rede dos *AP's* na *Unifi Controller*
/etc/freeradius/eap.conf	Escolha do tipo de protocolo *EAP* que iremos utilizar para a autenticação dos usuários no *Freeradius*
/etc/freeradius/sites-enabled/default	Definir a permissão de autenticação dos usuários que solicitarem a conexão ao *Freeradius* em um banco de dados *MySQL*
/etc/freeradius/sites-enabled/inner-tunnel	Definir a permissão de autenticação dos usuários que solicitarem a conexão ao *Freeradius* em um banco de dados *MySQL*

Após finalizar as alterações dos arquivos de configuração do *Freeradius* foi feito o teste e verificou-se que ele já se encontrava em funcionamento e já estava recebendo as solicitações dos *Access Points*, mas como o banco de dados ainda não tinha sido

criado ele retornava a mensagem de erro acusando que os parâmetros informados no arquivo */etc/freeradius/sql.conf* do banco de dados *My-SQL Server* eram desconhecidos.

Em seguida iniciamos a criação do banco de dados do *Freeradius* no *My-SQL Server* utilizando o mesmo nome informado no arquivo */etc/freeradius/sql.conf.* Após criado o banco de dados utilizamos o arquivo */etc/freeradius/sql/mysql/schema.sql*, fornecido pela própria ferramenta *Freeradius*, e que traz o modelo de tabelas a serem criadas em nosso banco de dados.

Finalizada a criação do banco de dados e tabelas instalamos o *phpMyAdmin* para facilitar a visualização e manipulação das informações em nosso banco de dados do *Freeradius*. Depois de instalado o *phpMyAdmin* inserimos na tabela *NAS* os parâmetros referentes aos *Access Points*.

Ainda no *phpMyAdmin* inserimos na tabela *RADCHECK* as credenciais dos usuários que estarão autorizados a autenticar-se no servidor *Freeradius*. No campo *username* iremos preencher com o login do usuário, no campo *attribute* vamos colocar *password*, pois vamos utilizar a autenticação via usuário/senha e no campo *value* vamos colocar a senha que escolhemos para nosso usuário.

Como especificado no arquivo */etc/freeradius/eap.conf* nós selecionamos *PEAP* como o tipo padrão de protocolo *EAP* para autenticação, portanto o dispositivo deve ter a opção de autenticação através desse protocolo ou através do protocolo *TTLS* que também foi configurado para conexão. Depois de configurado o equipamento foram efetuados os testes que obtiveram êxito na autenticação dos usuários cadastrados.

A infraestrutura da rede da instituição de ensino superior ficou do modo apresentado na figura 2 a seguir após as alterações:

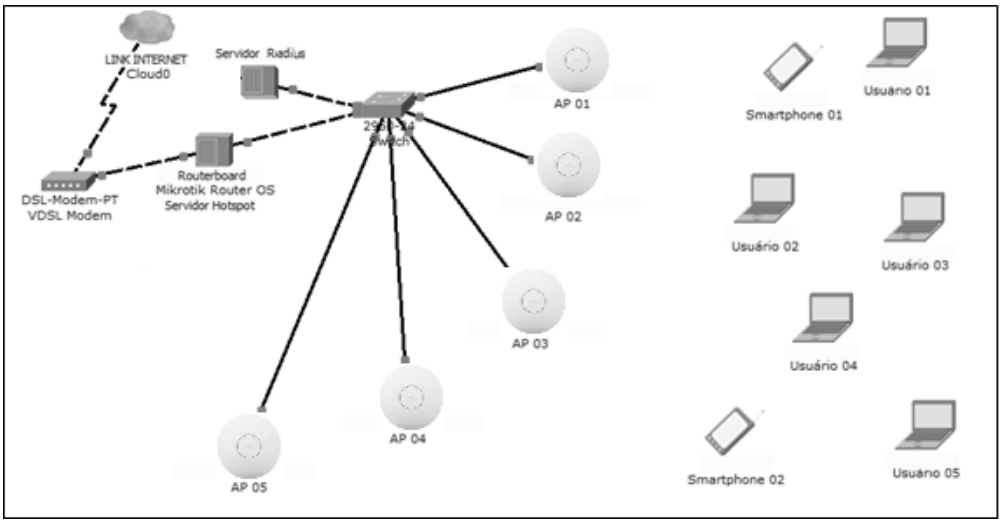

Figura 2: Representação da infraestrutura física de rede da instituição após a implantação do servidor *Debian* com a ferramenta *Freeradius*.

Devido às configurações feitas, todos os usuários que tentam se conectar à rede *wi-fi* disponibilizada na instituição tem sua requisição de conexão direcionada pelos

Access Points ao servidor *Freeradius* que processa o pedido e libera ou não a conexão de acordo o cadastro dos usuários no banco de dados *My-SQL*.

4. Resultados e conclusões

A implementação da autenticação de segurança em um servidor *Radius* instalado em um sistema operacional *Debian* trouxe resultados positivos aos usuários e ao administrador da rede *wi-fi* disponibilizada na instituição, pois o administrador pôde resolver questões de segurança mais rapidamente pela praticidade em bloquear os usuários não autorizados a se conectarem à rede *wi-fi*, outro benefício trazido aos usuários foi a diminuição do tráfego de dados inúteis nos *Access Points*, isto é, tráfego de dados dos usuários não autorizados a se autenticarem no *Hotspot*, aumentando assim o *throughput* dos usuários conectados e autenticados.

Diante disso, o projeto proporcionou um maior conhecimento profissional durante seu período de implementação, os resultados obtidos atenderam a proposta inicial enviada à diretoria da instituição, trazendo vantagem competitiva para a empresa e qualidade ao serviço prestado.

Com a necessidade de crescimento profissional constante e na oportunidade de satisfazer as metas estabelecidas em um estudo, a implementação de um servidor *Freeradius* proporcionou o aumento da concepção e entendimento sobre como, quando e de que modo formular as configurações necessárias para um bom funcionamento do sistema, colocando o administrador da rede a frente de questões técnicas aparentemente sem solução, mas que em uma segunda vista mais detalhada fizeram com que criasse modos e desvios lógicos, para chegar ao final do projeto obtendo êxito.

Outra oportunidade que foi conquistada com a realização desse projeto foi a criação de um ***manual para a implementação de segurança com um servidor Freeradius em uma rede wi-fi com ap's Unifi gerenciados pelo sistema operacional RouterOS***, que tem como principal finalidade o auxílio aos administradores de rede que possuírem dúvidas e encontra-se nesse artigo como Apêndice 01.

A melhoria constante do conhecimento continua, e os próximos passos são referentes à otimização e criação de novos processos e regras para a segurança da rede utilizada no projeto. Serão levantadas também questões de segurança quanto à diferença de perfis de usuário na hora da conexão, que forneça ao administrador a possibilidade de efetuar o bloqueio ou liberação de uma gama de equipamentos em determinada época, e após a implementação dessas novas funcionalidades a intenção é propiciar o aumento na qualidade dos serviços prestados pela instituição.

Referências bibliográficas

ANUNCIAÇÃO, Heverton. Linux Total e Software Livre. Rio de Janeiro RJ: Ciência Moderna 2007.

AUDY, Jorge L.N, ANDRADE, Gilberto K. e CIDRAL, Alexandre. Fundamentos de Sistemas de Informação. Porto Alegre RS: Bookman 2005.

CARVALHO, Luciano G. Segurança de redes. Rio de Janeiro RJ: Ciência Moderna 2005.

COMER, Douglas E. Redes de computadores e *Internet*. Porto Alegre RS: Bookman 2009.

COSTA, Gilberto C. G. Negócios Eletrônicos: uma abordagem estratégica e gerencial. Curitiba PR: Ibpex 2007.

ELMARSI, Ramez e NAVATHE, Shamkant B. Sistemas de bancos de dados. 6ª Ed. São Paulo SP: Pearson Addison 2011.

KALINKE, Marco A. *Internet* na Educação. Curitiba PR: Chain 2003:

KUROSE, James F. e ROSS, Keith W. Redes de computadores e a *Internet*: uma abordagem top-down. 6ª Ed. São Paulo SP: Pearson Education do Brasil 2013.

KUROSE, James F. e ROSS, Keith W. Redes de computadores e a *Internet*: uma nova abordagem. 1º Ed. São Paulo SP: Addison Wesley 2003.

LEVY, Guilherme. Manual para criação e configuração de um servidor Hotspot no sistema operacional RouterOS utilizando uma Routerboard Mikrotik. Trabalho de conclusão de curso de graduação em Tecnologia em Análise e Desenvolvimento de Sistemas, páginas 1 – 77, Faculdade Guairacá, Set 2015.

MAGDALENA, Beatriz C. e COSTA, Iris E. T. *Internet* em sala de aula. Porto Alegre RS: Artmed 2003.

MICROSOFT site Oficial. Disponível em:

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754179(v=ws.11). Acesso em 02/02/2018 às 16h 33min.

MIKROTIK site Oficial. Disponível em:

http://www.mikrotik.com/pdf/what_is_routeros.pdf. Acesso em 20/12/2017 às 19h 19min.

MIKROTIK Documentation. Disponível em:

http://wiki.mikrotik.com/wiki/Main_Page. Acesso em 04/02/2017 às 21h 01min.

NAKAMURA, Emilio T. e DE GEUS, Paulo L. Segurança de redes em ambientes cooperativos. São Paulo SP: Novatec 2007.

NEVES, Pedro M. C. e RUAS, Rui P. F. O guia prático do MySQL. 1ª Ed. Lisboa: Centro Atlântico 2005.

O'BRIEN, James A. Sistemas de informação e as decisões gerenciais na era da *Internet*. 2º Ed. São Paulo SP: Saraiva 2006.

OLIVEIRA, Celso H. Poderoso. SQL – Curso prático. 1º Ed. São Paulo SP: Novatec 2002.

PINHEIRO, José M. dos S. Guia completo de cabeamento de redes. 10º Ed. Rio de Janeiro RJ: Elsevier, 2003.

PRIMAK, Fábio V. Infortabilidade – A Contabilidade na era da informática. Rio de Janeiro RJ: Ciência Moderna 2009.

PRIMAK, Fábio V. Tecnologias da Informação Aplicadas ao Direito. Rio de Janeiro RJ: Ciência Moderna 2015.

RAINER, R. Kelly Jr. e CEGIELSKI, Casey G. Introdução a Sistemas de Informação - Apoiando e transformando negócios na era da mobilidade. 3ª Ed. Rio de Janeiro RJ: Elsevier 2011.

RUFINO, Nelson Murilo de Oliveira. Segurança em redes sem fio: aprenda a proteger suas informações em ambientes Wi-fi e Bluetooth. 3ª Ed. São Paulo SP: Novatec Editora 2011.

SOUSA, Lindeberg B. Redes de computadores - Guia Total. São Paulo SP: Érica 2010.

STATO, André Filho. Domine o Mikrotik RouterOS – Um guia prático de estudos para iniciantes. Juatuba MG: 1ª Ed. Instituto Alpha 2017.

STALLINGS, Willian. Criptografia e segurança de redes. São Paulo SP: 4ª Ed. Pearson Prentice Hall 2008.

TANEMBAUM, Andrew S. Redes de Computadores. 4ª Ed. Rio de Janeiro RJ: Elsevier 2003.

TANEMBAUM, Andrew S. Sistemas Operacionais Modernos. 3ª Ed. São Paulo SP: Pearson Prentice Hall, 2009.

TORRES, Gabriel. Redes de Computadores. Vila Isabel RJ: Novaterra 2010.