José António Mulaze Júnior

Gestão do consumo de largura de banda de utilizadores, com recurso ao protocolo RADIUS - Caso de estudo Faculdade de Economia e Gestão UP-Maputo

Licenciatura em Informática com habilitação em Engenharia de Redes

Universidade Pedagógica

Maputo

2023

José António Mulaze Júnior

Gestão do consumo de largura de banda de utilizadores, com recurso ao protocolo RADIUS - Caso de estudo Faculdade de Economia e Gestão UP-Maputo

Monografia apresentada à Faculdade de Engenharias e Tecnologias da Universidade Pedagógica de Maputo, como requisito parcial para a obtenção do grau académico de Licenciatura em Informática

Supervisor

dr. Xavier Domingos Bila

Universidade Pedagógica

Maputo

2023

Indice

Lista de Figuras

Lista de Abreviaturas

MIT - Massachusetts Institute of Technology.

LDAP - Lightweight Directory Access Protocol.

RADIUS - Remote Authentication Dial-In User Service.

CCITT - Comitê Consultivo de Telefonia e Telegrafia Internacional.

FEG - Faculdade de Economia e Gestão.

UP - Universidade Pedagogica.

CTA - Corpo Técnico Administrativo.

IEEE - Instituto de Engenheiros Eletricistas e Eletrônicos.

LAN - Local Area Network.

WLAN - Wireless Local Area Network.

AP - Access Point.

WEP - Wired Equivalent Privacy.

TKIP - Temporal Key Integrity Protocol.

EAP - Extensible Authentication Protocol.

TGT - Ticket Granting Ticket.

KDC - Key Distribution Center.

TGS - Ticket Grantig Server.

OSI - Open Systems Interface.

DAP - Directory Access Protocol.

TCP/IP - Transmission Control Protocol/Internet Protocol.

OU - Unidade organizacional.

CN - Nome Comum.

TLS - Transport Layer Security.

LDIF - Lightweight Directory Interchange Format.

AAA - Authentication, Authorization and Accounting.

NAS - Network Access Server.

ADSL - Asymmetric Digital Subscriber Line.

DSLAM - Digital Subscriber Line Access Multiplexer.

FTP - File Transfer Protocol.

SQL - Structured Query Language.

IP - Internet Protocol.

IAS - Internet Authentication Service.

ACS - Access Control Server.

UPS - Uninterruptible Power Supply.

WPA - Personal - Wireless Protected Access - Personal

Declaração

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

Declaro ainda que este trabalho não foi apresentado em nenhuma outra Instituição para obtenção de qualquer Grau Académico.

Maputo,_____de_____de_____

_____

(*Jose Antonio Mulaze Junior*)

Dedicatória

Dedico este trabalho a Deus, a minha mãe Ana Luisa Tafula ao meu Pai José António Mulaze que infelizmente ja nao se encontra entre nós. Dedico também este trabalho as minhas Tias, irmãos, amigos e a todos que directa ou indirectamente partilharam momentos comigo até que pudesse chegar até aqui. E não menos importante, dedico este trabalho final a mim.

Agradecimentos

Agradeço a Deus pela iluminação nos momentos de dúvida.

Agradeço a minha mãe meus irmãos que sempre estiveram do meu lado até que pudesse chegar aqui. A minha família que direta ou indiretamente ajudaram em especial a Tia Mafalda e Tia Zinha pelo apoio prestado.

Agradeço à minha namorada Inês Kantinthe pelo apoio, compreensão e companheirismo.

Agradeço aos meus colegas do curso de informática pelo apoio, momentos experiências acadêmicas e sociais que tivemos em especial ao Jeronimo Sitefane, Alívio Manjate, Fernando Mate, Aquilio Sigauque e Edmilson Hapata.

Agradeço também a todos os meus amigos pelos momentos em especial ao Nélio da Conceição, Milton Weber, Gerson Stefane, Adriano Wate e Melo do Santos. E não menos importante agradecer a mim.

Resumo

O presente trabalho de monografia consiste em um caso de estudo de um projecto de implementação de gestão do consumo de largura de banda de utilizadores, com recurso ao protocolo RADIUS na Faculdade de Economia e Gestão da Universidade Pedagógica de Maputo. O trabalho tem como finalidade integrar os estudantes e CTA no uso da internet no recinto universitário utilizando a infraestrutura de rede já existente. O objectivo específico é de criar políticas de acesso onde os funcionários têm acesso ilimitado da rede de dados e os estudantes e CTA limitado onde será necessário integrar um router de mikrotik ou de outra marca com a função de segurança WPA/WPA2 Enterprise e um servidor RADIUS na sala de informática.

Dessa forma este projeto permite constatar como é o servidor RADIUS, a gestão e contabilização de utilizadores através de resultados obtidos com essa tecnologia.

Palavras-chaves: Servidor RADIUS, Internet, mikrotik, router, WPA/WPA2 Enterprise.

Abstract

This monograph consists of a case study of a project to implement the management of user bandwidth consumption, using the RADIUS protocol at the Faculty of Economics and Management of the Pedagogical University of Maputo. The purpose of the work is to integrate students and CTA in the use of the internet on the university campus using the existing network infrastructure. The specific objective is to create access policies where employees have unlimited access to the data network and students and limited CTA where it will be necessary to integrate a mikrotik router or another brand with the WPA/WPA2 Enterprise security function and a RADIUS server in the computer room.

In this way, this project allows us to verify how the RADIUS server works, the management and accounting of users through the results obtained with this technology.

Keywords: RADIUS Server, Internet, mikrotik, router, WPA/WPA2 Enterprise.

CAPÍTULO I - Introdução

Segundo (GOMES, Daniel Cardoso, 2005) em tempos em que a competitividade faz com que as organizações preocupem-se cada vez mais com a racionalização e o aproveitamento máximo de seus recursos, a fim de obter ganhos de eficiência, é imprescindível a procura constante de novas soluções. E com o aumento da complexidade das redes de computadores, surgiu a necessidade de realizar uma gestão das redes mais eficiente e abrangente, com vista a manter a disponibilidade e consistência dos serviços baseados em redes de computadores.

Segundo (FRANCISCATTO, Roberto; CRISTO, Fernando, Cristo; PERLIN, Tiago, 2014, p. 15) As redes de computadores constituem-se de um conjunto de dois ou mais computadores interligados com o objectivo de compartilhar recursos e trocar informações. Cada vez mais presentes no dia-a-dia das pessoas, as redes de computadores estão espalhadas em diversos locais: grandes e médias empresas, pequenos escritórios ou até mesmo em casa.

Nesta onde de ideias, há uma necessidade de se fazer uma gestão adequada de utilizadores e dispositivos que se conectam e utilizam um determinado serviço de rede em uma intranet.

De acordo com o dicionário Houaiss da língua portuguesa (HOUAISS, Villar. 2011), gestão é o acto ou efeito de gerir, ou seja, exercer gerência sobre alguma coisa, administrar, dirigir, cuidar, executar e/ou praticar[1]

Segundo (DE OLIVEIRA, L. Marlúcia, 2010 p. 20) a intranet proporciona uma maior comunicação entre empresa e seus funcionários, além de ajudar em suas atividades. O uso de intranets têm-se mostrado altamente eficazes na informatização dos mais diversos tipos de organizações. A intranet é caracterizada pela sigla B2E (business to employee) em oposição às siglas utilizadas para os sistemas web de comércio eletrônico com B2B (business consumer). Tradicionalmente, a comunicação B2E é unidireccional (da empresa para o funcionário).

Assim sendo, torna-se difícil ter o controle de todos utilizadores e/ou dispositivos que acessam a uma rede ou a determinados serviços da rede. Daí que foram criadas soluções para se fazer a gestão dos mesmos, e uma delas em estudo no presente trabalho é o protocolo RADIUS.

Segundo (HASSEL, Jonathan. 2002) RADIUS (Remote Authentication Dial-In User Service) é um protocolo amplamente implantado que permite às empresas autenticar, autorizar e contabilizar utilizadores remotos que desejem aceder a um sistema ou serviço de rede central servidor.

---

[1] Disponivel em <https://gestaodeseguranca privada.com.br/gestao-o-que-e-que-faz-conceitos/> acesso a 02.12.2021

Ao longo do desenvolvimento do tema, iremos debruçar mais acerca de conceitos importantes para o bom entendimento do tema e como será implementado.

1.1 Delimitação do tema

A importância da implementação do protocolo RADIUS para a gestão do consumo de largura de banda de utilizadores na Faculdade de Economia e Gestão da UP Maputo.

1.2 Problema

A Faculdade de Economia e Gestão (FEG), outrora Escola Superior de Contabilidade e Gestão (ESCOG) é uma unidade orgânica criada a 20 de Agosto de 2008, com vocação para pesquisa, ensino, extensão e inovação nas áreas das ciências económicas e empresariais.

A sua criação foi uma resposta da UP-Maputo às exigências e necessidades do mercado de trabalho, que se fazia e ainda se faz sentir por profissionais qualificados de nível superior, com competência para competir no mercado de trabalho nacional e internacional e também para gerar o auto-emprego.

Algum tempo depois, sentiu-se a necessidade de haver uma conexão de internet para o acesso aos e-mails pessoais, assim como o e-mail da instituição, a solução mais viável na altura, era o uso de modems de operadoras de telefonia móvel para o acesso à internet que este, por sua vez, não garantia que todos os funcionários tivessem o acesso à internet. Recentemente, a FEG contratou provedores de serviço de internet para que esta passasse a fazer o uso de seus serviços no recinto universitário, unicamente, para os seus funcionários. Por sua vez, os estudantes e CTA (Corpo Técnico Administrativo) ficam isentos dos mesmos serviços para o uso pessoal e/ou académico, tendo em conta que os mesmo pagam a inscrição e propinas, semestralmente e mensalmente com o intuito de também poder ter acesso aos mesmos serviços que agora estão destinados aos funcionários da instituição.

Uma vez que, não existe nenhum protocolo de controle e/ou gestão de utilizadores implementado na FEG, torna-se necessário a implementação do mesmo, de modo, a que todos os setores e gabinetes da faculdade tenham acesso a esses serviços, visto que, este protocolo tem como foco o controle de utilizadores e/ou dispositivos, podendo assim incluir todos setores e gabinetes no uso da internet.

De que forma a FEG pode abranger o uso moderado da internet a todos os setores do recinto universitário?

1.3 Justificativa

Com vista a solucionar o problema acima citado, o uso do protocolo RADIUS mostra-se eficaz, uma vez que, este se preocupa, essencialmente, em autenticar os utilizadores ou dispositivos para o acesso à rede, autorizar os utilizadores ou dispositivos na utilização de determinados serviços da rede e em contabilizar e rastrear o uso desses serviços pelos utilizadores ou dispositivos da rede.

1.4 Objectivos

O objectivo do presente trabalho é de propor uma solução para o uso do protocolo RADIUS de modo que a Faculdade de Economia e Gestão consiga fazer o uso racional de dados no recinto universitário.

1.4.1 Objetivo Geral

Propor a implementação do protocolo RADIUS para a autenticação de utilizadores para o uso da rede de dados.

1.4.2 Objetivos Específicos

- Pesquisar os principais conceitos para o servidor RADIUS;
- Analisar diferentes protocolos com a mesma funcionalidade; e,
- Traçar uma solução eficaz para a abrangência de toda a comunidade no recinto universitário.

1.5 Questões de pesquisa

1. Por que os serviços de internet não abrange a todos da faculdade?
2. Quais são as vantagens do uso do protocolo RADIUS?

1.6 Hipóteses de Pesquisa

H0: Não faz muito tempo em que a FEG adquiriu os serviços de internet na faculdade, adicionado com a falta de profissionais da área de informática, isso contribui para o acesso restrito da rede de dados devido ao uso abusivo da mesma.

H1: O protocolo RADIUS é um protocolo amplamente implantado que permite às empresas autenticar, autorizar e contabilizar utilizadores remotos que desejam aceder a um sistema ou serviço de rede central.

1.7 Metodologia

Segundo (SILVA & MENEZES, 2001) existem várias formas de classificar uma pesquisa, pode-se classificar quanto a natureza da pesquisa, quanto a forma de abordagem do problema que incluem Pesquisas Quantitativas e Pesquisas Qualitativas e quanto aos seus objetivos e aos procedimentos técnicos.

Quanto a natureza da pesquisa usou-se a metodologia aplicada ou tecnológica, a qual tem como finalidade gerar conhecimentos para aplicação prática dirigida à solução de problemas específicos e envolve verdades e interesses locais, usou-se também o ponto de vista: procedimentos técnicos, em que incluem:

1.7.1. Pesquisa Bibliográfica

Para concretização deste trabalho de pesquisa foi usada uma revisão bibliográfica de modo a colher experiências já escritas por pesquisadores em livros e na internet inerentes ao tema com a finalidade de resolver o problema acima supracitado.

1.7.2. Pesquisa Ação

Para a implementação deste tema em plataforma virtual é uma pesquisa aplicada, pois tem como premissa fundamental gerar conhecimentos para a aplicação prática imediata, e do ponto de vista de forma a este tipo de abordagem, é uma pesquisa qualitativa, tendo como ambiente institucional de ensino a Faculdade de Economia e Gestão da UP Maputo que foi feita a coleta de dados.

1.8 Organização da Pesquisa

O presente trabalho encontra-se organizado em quatro (4) capítulos onde:

O Capítulo I – Dá uma visão geral do trabalho, desde a problematização, justificativa, delimitação do tema, objetivos e metodologia.

O Capítulo II - Far-se-á um cruzamento de diferentes protocolos com a mesma funcionalidade para determinar o motivo da escolha do protocolo RADIUS.

Capítulo III - Versa sobre o desenvolvimento do trabalho, com tecnologia escolhida.

O Capítulo IV - Versa sobre a conclusão do trabalho e as recomendações.

CAPÍTULO II - Revisão Bibliográfica

2.1. Redes sem fio padrão 802.11

De acordo com (MORAIS, Giovane. 2015) citando (Goranson. 2003) uma rede sem fio é uma ramificação das redes locais (LAN - Local Area Network) com fio. A partir dessa definição nasce o conceito de rede local sem fio, Wireless Local Area Network (WLAN). Uma WLAN realiza a conversão de pacote de dados em ondas de rádio ou infravermelho e os envia para outros dispositivos sem fio ou para pontos de acesso (AP - Access Point) que servem como uma conexão para uma rede com fio.

Segundo (MORAIS, Giovane. 2015) o IEEE (Instituto de Engenheiros Eletricistas e Eletrônicos) definiu, em 1990, um padrão para o funcionamento da tecnologia wireless. Esse padrão ficou conhecido como IEEE 802.11 (IEEE, 1990). Porém, apenas em 1997 este padrão pôde ser usado em larga escala pois, até então, os dispositivos sem fios eram escassos e ineficientes.

2.1.1. Funcionamento

O padrão IEEE 802.11 abrange os níveis físico e de enlace. No nível físico são tratadas as formas de transmissão, podendo ser por frequência de rádio ou infravermelho. No nível de enlace, o protocolo IEEE exerce controle de acesso ao protocolo MAC do dispositivo wireless, bastante semelhante ao protocolo usado em redes locais Ethernet. Além disso, o protocolo define o métodos de transmissão, e outros aspectos de transferência de dados sem fio, permitindo que várias WLAN's consigam se comunicar entre si.

Segundo (MORAIS, Giovane. 2015) citando (CISCO SYSTEMS, 2008) relata que o protocolo 802.11 possui dois métodos de autenticação de rede: o sistema aberto e o sistema chave compartilhada.

Na autenticação aberta, conforme (MORAIS, Giovane. 2015) citando (Goranson. 2003), qualquer aparelho de acesso à rede sem fio pode solicitar autenticação para o servidor. O cliente envia uma solicitação de gestão de autenticação que possui a sua própria identidade. O receptor wireless (AP) aceita todos os requerimentos de autenticação. A autenticação aberta admite que qualquer aparelho acesse a rede se não houver nenhuma criptografia funcional nela.

Na autenticação de chave compartilhada, como descreve (MORAIS, Giovane. 2015) citando (Wrightson. 2014), cada receptor recebe uma chave compartilhada secreta através de um canal seguro (independente do canal de comunicação da rede sem fio). A autenticação por chave

compartilhada ocorre quando ele passa por uma autenticação baseada em desafios. Para ter acesso à rede, o cliente deve possuir uma chave para realizar a autenticação, podendo ser do tipo WEP, WPA-Personal (Wireless Protected Access - Personal) ou WPA2-Personal.

2.1.2. Wired Equivalent Privacy (WEP)

O protocolo WEP criptografa seus dados para impedir a recepção não autorizada de conexão sem fio. A WEP usa criptografia com chaves de 64 ou 128 bits antes de enviá-las à rede. Somente os dispositivos que possuírem a mesma chave de criptografia tem o direito de acessar a rede ou decodificar os dados transmitidos por outros computadores. Para se comunicarem com a chave WEP, todos os aparelhos Wi-fi precisarão ter as mesmas chaves de criptografia. A partir destas chaves, o servidor analisa se a chave do cliente confere com a dele. Caso sim, é aceito o acesso ao cliente à rede.

2.1.3. Wireless Protected Access - Personal

O WPA-Personal foi adotado formalmente em 2003. Possuindo uma encriptação de 256 bits dava uma maior segurança para as redes. O método disponibiliza, também, os algoritmos de criptografia de dados como o TKIP (Temporal Key Integrity Protocol) e o AES-CCMP (Advanced Encryption Standard). Mesmo com tantas melhorias, o WPA-Personal é passível de ataques tipo brute force (força bruta).

2.1.4. Wireless Protected Access 2 - Personal

O WPA2-Personal é um aprimoramento do WPA e implementa o padrão IEEE 802.11i completo. Ele funciona da mesma forma que o WPA-Personal e ambos são interoperáveis. O que diferencial do WPA2-Personal é que, além de possuir compatibilidade ascendente com o WPA, este método de encriptação pode lidar com senhas e algoritmos de uma forma mais otimizada, reconhecendo possíveis ataques de força bruta na rede e mitigando a possibilidade de um ofensiva desta forma ocorra. Este protocolo é, do gênero, o mais seguro da atualidade.

2.2. Protocolo IEEE 802.1X

De acordo com (MORAIS, Giovane. 2015) O padrão 802.1x foi desenvolvido pelo IEEE em junho de 2001 como uma solução de segurança, que realiza identificação e autenticação em redes cabeadas ou sem fio através de um servidor de autenticação. Além disso, o protocolo provê mecanismos de autenticação para aparelhos para que possam se anexar a uma LAN ou

WLAN. A IEEE 802.1x baseia-se no protocolo EAP (Extensible Authentication Protocol), definido pelo IETF, com função de transportar as informações de identificação de quem utiliza a rede.

Segundo (LATERZA, Leando Reis. 2012) O padrão 802.1X tem como ideia prover controle de acesso nas portas dos dispositivos de conexão, de modo a impedir que conexões clandestinas tenham acesso a rede. O padrão 802.1X define três atores durante o processo de autenticação:

1. **Suplicante:** É um cliente que deseja ser autenticado na rede, este representado por uma interface de rede sem fio no padrão 802.11, geralmente um notebook.
2. **Autenticador:** É o dispositivo intermediário entre o suplicante e o servidor,
3. **Servidor de Autenticação:** É um dispositivo responsável pelo controle de acesso.

2.3. Kerberos

2.3.1. Breve Historial

De acordo com (JUNIOR, A. Wagner, 2011), o nome Kerberos advém da mitologia grega de Cerberus, o guardião dos portões do submundo. Os gregos acreditavam que para lá eram enviadas as almas dos mortos e era trabalho de Cerberus garantir que apenas eles entrassem no reino e que nenhuma alma pudesse sair dele. Embora o nome Cerberus tenha sido popularizado, a grafia correta para o seu nome em grego é Kerberos. Não por acaso, o protocolo Kerberos nasceu de um projeto desenvolvido a partir de maio de 1983 pelo Massachusetts Institute of Technology (MIT) chamado Athena.

(JUNIOR, A. Wagner, 2011) acrescenta que com o advento das redes de comutação de pacotes mudou muito a maneira como os utilizadores interagem com computadores. Se antes eles constituíam um recurso caro e centralizado, acessado através de terminais leves em um sistema de compartilhamento de tempo, com a rede os utilizadores passaram a ter seus próprios computadores pessoais conectados a todos os outros computadores de determinada organização, por exemplo. No entanto, os sistemas pessoais chamados de desktops, não possuíam grande poder de processamento. Isso tornou necessário que alguns serviços fossem disponibilizados por computadores com maior poder de processamento, chamados de servidores. Esse modelo, conhecido como cliente/servidor, possibilitou diversas novas situações e o MIT percebeu que era necessária uma mudança dramática na arquitetura de software e na maneira de se usar o computador. A principal mudança em relação ao modelo antigo era que, se antes o computador central que todos os utilizadores utilizavam era

controlado pelo administrador, agora cada utilizador podia controlar o seu próprio sistema da maneira que desejasse, tornando-se assim não mais confiável. Em resposta a essa situação, foi desenvolvido o projeto Athena. O foco do projeto era desenvolver estratégias e software para a integração de computadores no MIT. Embora seu objetivo tenha sido inicialmente educacional, muito do que foi desenvolvido na época incluindo o protocolo Kerberos, ainda está em uso atualmente.

2.3.2. Funcionamento

De acordo com (JUNIOR, A. Wagner, 2011), o Kerberos é um serviço seguro, de autenticação única e mútua através de uma terceira parte confiável. O serviço é seguro uma vez que as senhas nunca são enviadas pela rede. A autenticação é única porque os utilizadores precisam logar-se apenas uma vez para acessar todos os serviços da rede e é mútua, pois garante a identidade não só do utilizador, mas também do servidor. O termo terceira parte confiável refere-se ao fato de que o Kerberos trabalha através de servidores centralizados nos quais todos os sistemas na rede confiam.

Ainda de acordo com (JUNIOR, A. Wagner, 2011), o objetivo do Kerberos é aumentar a segurança e a conveniência para os administradores de redes e utilizadores. Ele opera através de um ou mais servidores centralizados chamados Key Distribution Centers, ou KDCs. Cada KDC possui uma base de dados contendo todos os logins e senhas dos utilizadores da rede. A centralização é conveniente para o administrador à medida em que ele passa a ter que se preocupar em manter uma única base de dados. Além disso, se todas as informações estiverem centralizadas em uma máquina ou em um pequeno grupo delas, torna-se mais fácil manter a segurança e a confidencialidade. O Kerberos adiciona segurança a redes inseguras. Ao invés de enviar senhas através da rede ele faz uso de tickets encriptados para comprovar a identidade dos utilizadores.

2.3.3. Componentes do Kerberos

2.3.3.1. Reinos

De acordo com (JUNIOR, A. Wagner, 2011), cada implementação do Kerberos define um reino sobre o qual ela terá controle administrativo. O reino é um conjunto de sistemas conectados em rede que utiliza e confia no servidor Kerberos para se autenticar. Normalmente o reino Kerberos é definido dentro de um determinado domínio possui o mesmo nome do domínio

convertido para letras maiúsculas. Dessa forma, o domínio meudominio.org seria o reino MEUDOMINIO.ORG.

Esse tipo de definição, embora facilite a configuração, não é obrigatório, podendo haver um reino MEUREINO.COM ou MeuReino.COM dentro de um domínio meudominio.org, ressaltando que a nomenclatura dos reinos, ao contrário da dos nomes de domínio, é case sensitive (sensível ao caso), ou seja, faz distinção entre letras maiusculas e minusculas. Dessa forma, MEU-REINO.COM e Meu-Reino.COM são exemplos de reinos diferentes.

2.3.3.2. Principals

De acordo com (JUNIOR, A. Wagner, 2011) Principals são associações feitas a cada entidade que deverá ser autenticada pelo Kerberos, seja ela um utilizador, máquina ou serviço. Cada principal possui um nome único e uma chave, na forma de senha, que o identifica. Para garantir que um principal seja único, a sua nomenclatura é dividida de forma hierárquica.

Para utilizadores, a primeira parte do principal é o nome, seguido ou não de uma ou mais instâncias opcionais, seguido de @ e o nome do reino. O exemplo a seguir é a forma mais simples de definir um utilizador:

usuario@MEUDOMINIO.ORG

As instâncias opcionais são usadas em duas situações, para definir utilizadores com privilégios administrativos e especificar serviços ou máquinas. Um utilizador com permissões de administrador pode ser representado da seguinte forma:

usuario/admin@MEUDOMINIO.ORG

Principals associados a serviços e máquinas também são necessários em um reino Kerberos, uma vez que a autenticação deve ser mútua. No caso dos serviços, ao invés do nome de utilizador, é utilizado o nome do serviço seguido do nome completo de domínio Fully Qualified Domain Name (FQDN) da máquina no qual ele está instalado. Por exemplo:

ftp/ftp.meudominio.org@MEUDOMINIO.ORG

Máquinas são representadas pelo nome host seguido de seu FQDN:

host/pc1.meudominio.org@MEUDOMINIO.ORG

2.3.3.3. Tickets

De acordo com (JUNIOR, A. Wagner, 2011), o Kerberos trabalha com o conceito de tickets. Um ticket é um conjunto de informações encriptadas que confirma a identidade de um principal. Ele possui duas funções: a primeira é identificar os participantes de uma transação, e a segunda é estabelecer uma chave de sessão de curta duração que será usada pelas partes

para estabelecer uma comunicação segura. Isso dispensa o tráfego de senhas todas as vezes que uma autenticação é solicitada. Dentre as informações que formam um ticket, encontramos:

- O nome do principal solicitante;
- O nome do principal do serviço solicitado;
- A partir de quando o ticket é válido e quando ele expira;
- Uma lista de endereços IP a partir dos quais o ticket pode ser usado;
- Uma chave de sessão encriptada que é usada na comunicação entre o usuário e o serviço.

Os Tickets possuem tempo de validade limitada, geralmente variando entre 8 e 24 horas. Isso acontece para minimizar a ameaça que um ticket roubado possa causar, e simultaneamente, manter a autenticação única por um prazo de tempo razoável.

Um tipo especial de ticket, que é sempre o primeiro a ser emitido em um processo de autenticação, é o Ticket Granting Ticket (TGT). Quando um cliente deseja autenticar-se, ele recebe um TGT encriptado com a sua senha. Caso seja informada a senha correta, ele passa a ter permissão para solicitar novos tickets para serviços específicos. O TGT é o principal responsável pela autenticação única. Por padrão, tickets são armazenados em um arquivo temporário. Neste arquivo são armazenados o principal do utilizador e todos os tickets obtidos por ele.

2.3.3.4. Key Distribution Center (KDC)

De acordo com (JUNIOR, A. Wagner, 2011), o Key Distribution Center (KDC), é a parte central de um sistema Kerberos. É ele o responsável por armazenar os dados dos principals e autenticá-los. O KDC é composto por três partes lógicas, nomeadamente, base de dados, servidor de autenticação e ticket grantig server.

i) Base de dados

Cada KDC deve armazenar todos os principals contidos em um reino, bem como suas chaves e diversas outras informações opcionais. Para isso, deve haver um sistema de base de dados.

As principais implementações do Kerberos possuem uma base de dados leve e especializado, que é executado na mesma máquina do KDC.

ii) Servidor de Autenticação

É o responsável por emitir o TGT encriptado para os clientes que queiram autenticar-se no reino.

iii) Ticket Grantig Server (TGS)

Diferente do servidor de autenticação, o TGS emite tickets específicos de cada serviço aos clientes. Ele recebe do cliente um pedido de ticket que inclui o nome do principal representando o serviço requerido e o TGT emitido pelo Servidor de Autenticação. O TGS então emite para o cliente o ticket relativo ao serviço requisitado.

Ainda segundo (JUNIOR, A. Wagner, 2011) a figura 1 exemplifica a autenticação de um usuário em um servidor KDC. Inicialmente, o cliente se autentica e recebe o Ticket Granting Ticket do servidor de autenticação. O TGT é então enviado ao TGS que deve emitir o ticket específico para o serviço solicitado. O servidor recebe o ticket e deve descriptografá-lo com sua chave, obtendo dessa forma uma chave de sessão de duração limitada.

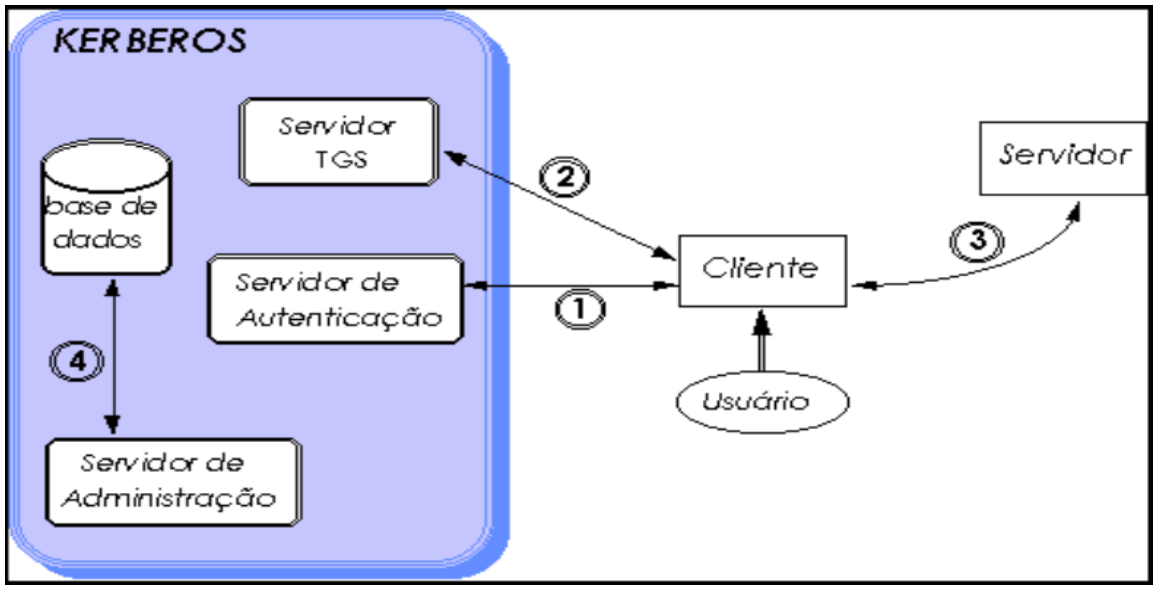

Figura 1: Exemplo de autenticação em um servidor Kerberos**. Fonte:** (JUNIOR, A. Wagner, 2011).

2.3.4. Vantagens

- Suporta vários sistemas operacionais.
- A chave de autenticação é compartilhada com muito mais eficiência do que o compartilhamento público.
- O Kerberos é um programa que possui uma boa aplicação quando nos referimos a uma rede de grande porte, comunicação e troca de serviços entre redes em diferentes domínios

2.3.5. Desvantagens

- Por se preocupar diretamente com a segurança, tanto de serviços como de utilizador, este programa exige uma troca muito intensa de tickets, o que inclui muitas comunicações com os servidores, além da criptografia, o que acaba gerando um tempo de atraso grande.
- Mostra vulnerabilidade a senhas fáceis ou fracas

2.4. Lightweight Directory Access Protocol (LDAP)

2.4.1. Breve Historial

De acordo com (CANEVER, Muriel. 2016) citando (MENEGUITE. 2009, p.14) em sua monografia, afirma que a utilização deste serviço surgiu da necessidade de se empregar um modelo de gestão de diretórios que não fosse baseado em bases de dados relacionais. O autor cita a necessidade de se desenvolver um protocolo que tivesse a capacidade de organizar entradas em um serviço de nomes de forma hierárquica, capaz de suportar grandes quantidades de dados e com uma enorme capacidade de procura de informações. Porém, o LDAP não foi desenvolvido sem uma base inicial, ele surgiu como uma alternativa “leve" para acesso ao serviço de diretório X.500.

Segundo (CANEVER, Muriel. 2016) citando (TUTTLE, et al, 2004, p.13), o X.500, definido pela RFC 1487, é um protocolo padrão de serviços de diretórios, que deu origem ao desenvolvimento do LDAP. O CCITT (Comitê Consultivo de Telefonia e Telegrafia Internacional) criou o padrão X.500 em 1988. X.500 organiza entradas de diretórios em um espaço de nome hierárquico capaz de suportar grandes quantidades de informação. Ele também define uma capacidade de pesquisa poderosa para fazer a recuperação de informações mais fácil.

Ainda segundo (JÚNIOR, A. Wagner, 2011), afirma que o serviço de diretórios X.500 era originalmente acessado através do DAP (Directory Access Protocol). Esse protocolo realizava a comunicação entre cliente e servidor utilizando a pilha de protocolo de sete camadas do modelo OSI (Open Systems Interface). O padrão OSI é extremamente didático e amplamente utilizado no meio académico para definir a base de desenvolvimento de protocolos de rede, no entanto na prática ele é muito complexo.

2.4.2. Funcionamento

Segundo (CANEVER, Muriel. 2016) o LDAP, é especificamente um serviço de diretórios baseado em X.500, executado sobre arquitetura TCP/IP, é baseado em um modelo cliente/servidor, como demonstra a Figura 2, podendo receber uma variedade de consultas e requisições das aplicações.

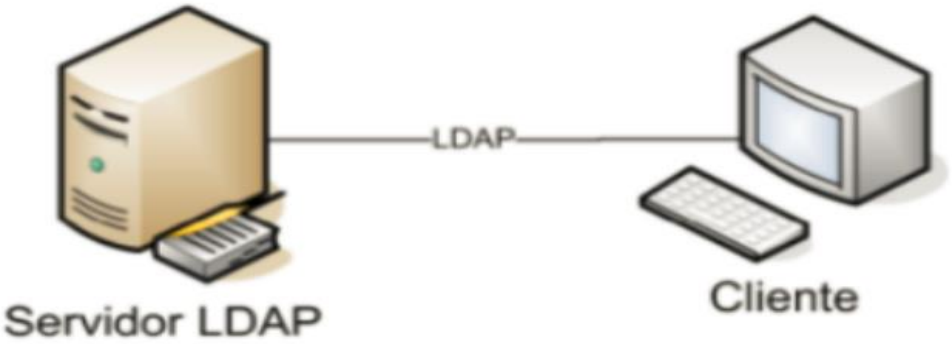

Figura 2: Modelo Cliente/Servidor. **Fonte:** (CANEVER, Muriel. 2016).

A estrutura de uma árvore de diretórios LDAP, segundo (CANEVER, Muriel. 2016) citando GIL (2012), busca organizar as informações em forma de diretórios, ou seja, em forma de árvore. As partes que permitem essa formação são as especificações do protocolo, onde, baseando-se em campos, chamado de atributos, e em seus conjuntos chamados de schemas, é possível armazenar qualquer tipo de informação de forma estruturada.

Cada entrada de informação, estará retida a uma hierarquia de armazenamento dos dados na base LDAP. É necessário que se crie uma estrutura organizada na árvore, ou seja, para se habilitar acessos a determinada aplicação, foi criado um tributo Common Name - CN (Nome comum) próprio para a aplicação, não utilizando atributos ou Organizational Unit - OU (Unidade organizacional) previamente configuradas no Zimbra.

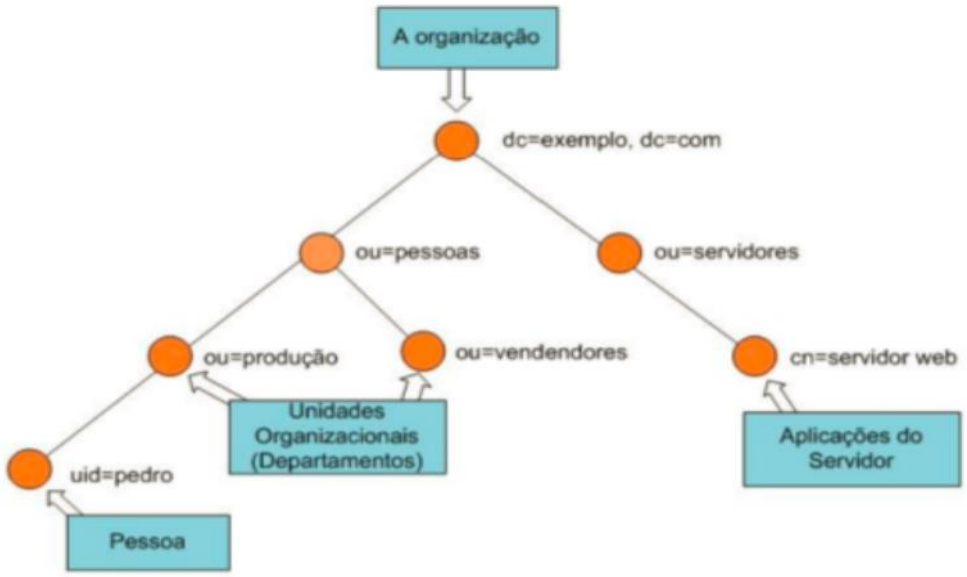

Figura 3: Sistema de diretórios**. Fonte:** (CANEVER, Muriel. 2016)

Segundo (CANEVER, Muriel. 2016) citando (DONLEY. 2003, pg 4), o LDAP é um padrão que computadores e dispositivos de rede podem usar para acessar informações sobre a internet. O protocolo LDAPv3 que é definido pela RFC 2251, se apresenta em muitas aplicações que são utilizadas por profissionais da área de tecnologia, embora integrado com a maioria delas, seu uso para a gestão não é muito difundido. A ideia por trás do LDAP, segundo (DONLEY. 2003, p.27), é que não importa onde os dados finais estão armazenados, desde que tanto o cliente e o servidor possam usar LDAP para trocar informações de uma maneira que possam se entender pelos dois lados. A arquitetura de uma requisição ao servidor LDAP segue exemplificada pela Figura 4, onde são apresentadas basicamente quatro operações: ldap open, ldap bind, ldap search e ldap unbind.

Ainda (CANEVER, Muriel. 2016) citando TUTTLE (2009), afirma que o LDAP é um padrão aberto capaz de facilitar, de forma flexível, o compartilhamento, a manutenção e a gestão de grandes volumes de informações, definindo um método-padrão de acesso e atualização de informações dentro de um diretório.

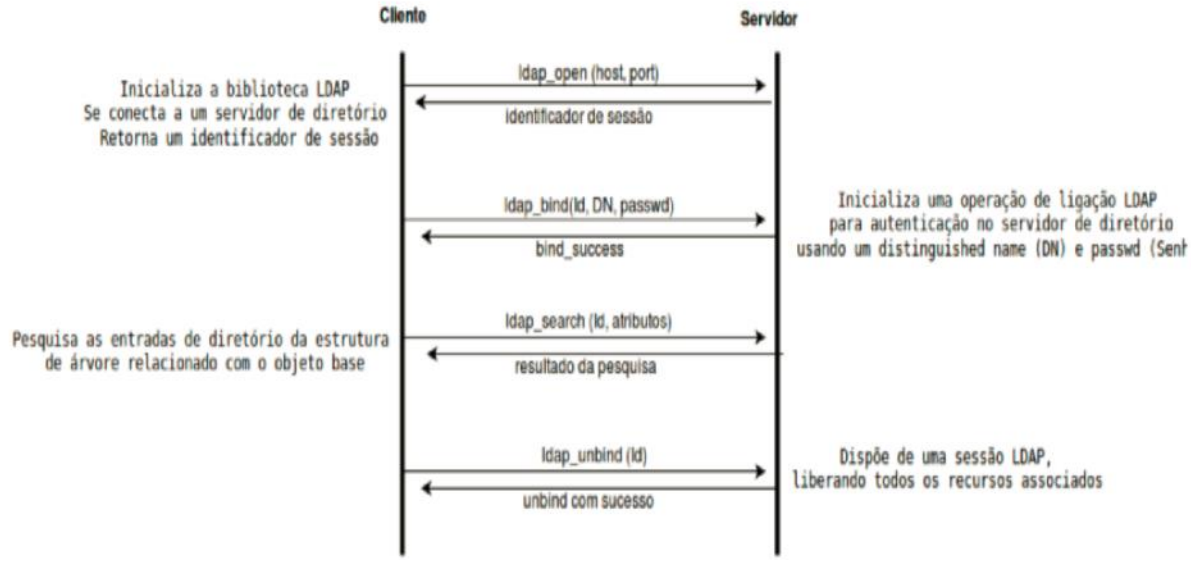

Figura 4: Funcionamento de uma pesquisa ao servidor LDAP. **Fonte:** (CANEVER, Muriel. 2016).

Segundo (CANEVER, Muriel. 2016) as seguintes operações são aceites pelo protocolo LDAP:

- ldap open - abre uma conexão com o serviço de diretório e retorna uma sessão para uso futuro;
- ldap bind - é responsável pela autenticação do cliente;
- Bind - permite o cliente se autenticar com o servidor de diretório através de um DN (distinguished name, ou nome distinto), e credenciais, como utilizador e senha. Quando a operação bind é completada com sucesso, o servidor de diretório salva esta informação antes que um novo bind seja realizado ou quando a sessão é terminada pela chamada de um ldap unbind. A identidade é usada pelo servidor para fazer decisões sobre qual tipo de mudanças podem ser feitas no diretório;
- ldap search - é a operação que se inicia a pesquisa LDAP através de um critério especificado que se combina com um filtro associado. Finalmente, a sessão LDAP é fechada utilizando o ldap unbind.

(JUNIOR, A. Wagner, 2011) acrescenta algumas operações realizadas pelo protocolo LDAP, tais como:

- start_TLS - utiliza o protocolo TLS (Transport Layer Security) para garantir uma conexão segura;
- compare – testa-se uma entrada possui determinado atributo;
- add - adiciona uma nova entrada;
- delete - remove uma entrada;

- modify - altera uma entrada;
- modify_DN - renomeia ou move uma entrada;
- abandon - aborta uma operação, mas não envia resposta;
- extended operations - é uma operação genérica que permite criar novas operações. Podemos citar como exemplo Password Modify para alteração de senha e Cancel que funciona de maneira semelhante à Abandon, mas retorna mensagem de erro ou sucesso.

2.4.3. Schemas

Segundo (JUNIOR, A. Wagner, 2011) schemas ou esquemas são os responsáveis por definir um conjunto de regras que determina quais tipos de dados poderão ser armazenados em um determinado diretório. Cada item adicionado ou alterado é comparado com um schema para validação. Caso um item não corresponda às regras definidas no schema ocorre uma schema violation (violação de esquema). Novos schemas podem ser adicionados e até mesmo criados pelo administrador do sistema.

2.4.4. Arquivos LDIF

Segundo (JUNIOR, A. Wagner, 2011) o LDAP Interchange Format, definido na RFC 28497, é um formato padrão de arquivo texto usado para armazenar configurações e itens do diretório. Arquivos LDIF são geralmente utilizados para inserir ou modificar informações no diretório. Os dados contidos em um arquivo LDIF devem estar de acordo com as regras definidas pelos schemas em uso. A Figura 5 exemplifica um arquivo LDIF que contém o topo da árvore que possui o DN dc=meudominio, dc=org.

```
# Arquivo LDIF para a entrada dn: dc=meudominio,dc=org
dn: dc=meudominio,dc=org
objectClass: domain
dc: meudominio
```

Figura 5: Arquivo LDIF. **Fonte:** (JUNIOR, A. Wagner, 2011)

2.4.5. Atributos

Segundo (JUNIOR, A. Wagner, 2011) atributos são, de várias maneiras, similares a variáveis usadas em programação. Ambos armazenam valores e possuem tipos bem definidos. Os atributos podem armazenar mais de uma informação. Quando um novo valor é inserido em um

atributo que já possui outro previamente alocado, ele é adicionado à lista de valores do atributo. Isso é útil, por exemplo, para armazenar números de telefone de utilizadores, já que atualmente é cada vez mais comum possuirmos dois ou mais números de contato. Embora seja possível haver atributos com mais de um valor, alguns deles são únicos e só podem armazenar um valor de cada vez. Um exemplo de atributo único é o uidNumber, que identifica o ID numérico de um utilizador UNIX.

Voltando à Figura 5, observamos que atributos são listados à esquerda do sinal ":"e seus valores ficam à direita do sinal, separados por um espaço.

2.4.6. Vantagens e desvantagens do LDAP

Segundo (CANEVER, Muriel. 2016) citando (CHAVES. 2010), as principais vantagens do LDAP são:

- É um padrão aberto;
- É otimizado para realizar pesquisas e leitura;
- Centraliza toda a informação proporcionando enormes benefícios tais como: um único ponto de administracao, menos informação duplicada, maior transparência das informações;
- Possui um mecanismo de replicação da base incluído;
- Muitas aplicações e serviços possuem suporte ao LDAP.

As principais desvantagens do LDAP são:

- Em alguns casos não substitui as bases de dados relacionais;
- Pouco eficiente para operações de escrita e atualização;
- Integração com outros serviços e aplicações torna a implantação complexa.

2.5. Remote Authentication Dial-In User Service (RADIUS)

De acordo com (HASSELL, Jonathan. 2002) RADIUS (Remote Authentication Dial-In User Service) é um protocolo amplamente implantado que permite às empresas autenticar, autorizar e contabilizar utilizadores remotos que desejam acesso a um sistema ou serviço a partir de um servidor de rede central.

2.5.1. Breve Historial

De acordo com (MORAIS, Giovane. 2015) o RADIUS foi instituído pela Livingston Enterprises, Inc. no início da década de 90. Sua função era permitir acesso dos utilizadores aos

servidores de autenticação por meio de protocolos. Logo depois, segundo (Aboba. 2003), foi incorporado como padrão IETF sendo muito usado por empresas que atuam no controle de acesso de utilizadores à internet ou intranet (rede local), também podendo ser integrado a serviços de e-mail.

2.5.2. Arquitetura AAA (Authentication, Authorization, Accounting)

Segundo (LATERZA, Leandro Reis. 2012) O protocolo RADIUS é desenvolvido com base em um processo denominado AAA, este constituído em autenticação, autorização e accounting (acompanhamento / monitoramento / contabilidade do uso de recursos de rede por utilizadores). As etapas que o RADIUS segue são.

1. **Autenticação do usuário:** é um processo para identificar se a identidade alegada é autêntica, por meio de comparação das credenciais apresentadas pelo cliente com outras já pré-definidas.
2. **Autorização de serviços:** A autorização ocorre logo após a autenticação e possui a função de distinguir e separar os privilégios atribuídos ao cliente que está tentando realizar a autenticação. Isto significa que ele apenas entregará os privilégios ao utilizador do grupo em que o mesmo pertencer.
3. **Contabilização:** O processo de accounting (contabilização) coleta informações sobre a atividade do cliente e as envia ao servidor de autenticação como um relatório de todos os acessos. Caso algum incidente de segurança ocorra, o administrador de redes pode utilizar o relatório de accounting para rastrear o problema.

2.5.3. Componentes do Sistema RADIUS

RADIUS é um protocolo de rede que implementa um sistema de regras e convenções para a comunicação entre dispositivos de rede. Seu modelo é do tipo cliente/servidor. O cliente RADIUS é chamado de NAS (Network Access Server) pois é ele que requisita os serviços AAA de RADIUS. O servidor RADIUS encaminha ou processa requisições e envia respostas ao NAS.

NAS é um ponto de acesso para uma rede sem fio. Em sistemas profissionais temos equipamentos que formam um pool de modems atendendo ligações que são chamados de concentradores NAS. A tabela a seguir lista os componentes de RADIUS e uma breve descrição.

RADIUS Components		
Component Name	**Functions**	**Examples**
User / Device	Requests access to the network.	Laptop Asymmetric Digital Subscriber Line (ADSL) Modem VOIP Phone
Network Access Server (NAS)	Provides access to the network for the user/device.	Switch Wireless Access Point DSLAM VPN Terminator
Authentication Server	Receives authentication requests from the NAS. Returns authentication results to the NAS. Optionally requests user and configuration information from the database or directory. May return configuration parameters to the NAS. Receives accounting information from the NAS.	FreeRADIUS Radiator IAS NPS ACS
Data Store	Optional database or directory with user authentication and authorisation information. RADIUS server communicates with the data store using DB API or LDAP.	SQL Database Kerberos Service Server LDAP Directory

Figura 6: Componentes do Sistema RADIUS. **Fonte:** https://www.vivaolinux.com.br/artigo/FreeRADIUS-Nocoes-basicas-Parte-I?pagina=2

2.5.3.1. Network Access Server (NAS)

É uma porta de acesso (gateway) entre o utilizador e uma rede mais ampla. Quando o utilizador tenta obter acesso a essa rede ampla, NAS age passando informações do utilizador para o servidor RADIUS. Esse processo é chamado de autenticação de sessão. Observe que o simples login dá início a uma conversação denominada autenticação de sessão. Esse é um conceito chave, pois no fim do processo de autenticação de sessão o servidor RADIUS define se o NAS deve aceitar ou rejeitar o acesso deste utilizador à rede. Uma vez que, este utilizador foi autorizado, a política de segurança deve ser forçada pelo NAS ao utilizador . Neste momento, o NAS age como um roteador ou firewall. O servidor RADIUS recebe do NAS um resumo das atividades do utilizador durante a sessão. Isso pode incluir informações sobre o tempo total de uso e a quantidade de tráfego trocado em cada sentido.

Existem diversos tipos de NAS. No ambiente empresarial podem ser switches ou pontos de acesso wireless bloqueando acessos não autorizados. Centrais de ADSL (Asymmetric Digital

Subscriber Line) ou DSLAM (Digital Subscriber Line Access Multiplexer) podem ser vistas como NAS, pois o utilizador se autentica e registra sua contabilidade nelas. Na prática, qualquer dispositivo que verifica nome e senha é potencialmente um cliente RADIUS. Por exemplo, servidores de FTP (File Transfer Protocol), de web e de login são potenciais clientes RADIUS. Neste contexto, NAS é sempre um cliente e RADIUS é sempre um servidor, pois toda a conversação da sessão de autenticação sempre se inicia do NAS para o RADIUS. Para o utilizador, NAS é um servidor; para RADIUS ele será sempre um cliente.

2.5.3.2. Servidor RADIUS

Usualmente é uma aplicação em software executada em um hardware computacional ou embarcado em um equipamento autocontido. Aparelhos (appliances) RADIUS podem simplificar a manutenção e a gestão. Em cada caso, esses equipamentos possuem uma função idêntica: Funcionam como um servidor que aguarda uma requisição de um NAS, processa ou encaminha essa requisição, e retorna uma resposta ao NAS. A resposta, em si, pode conter políticas de autorização ou uma confirmação de dados de contabilidade recebidos anteriormente. Um único servidor RADIUS pode atender diversos tipos de NAS e pode receber, encaminhar ou processar milhares de requisições ao mesmo tempo. Aparelhos de NAS como os concentradores ADSL, dial-up e VPN são clientes que se encontram em locais físicos variados.

Um servidor RADIUS pode interagir com diretórios LDAP, base de dados, outros servidores RADIUS ou simples arquivos de texto plano usados como base de dados. Para tomar a decisão final, o servidor RADIUS pode consultar diversas dessas fontes simultaneamente. Após enviar a decisão ao NAS, o servidor RADIUS não tem condição de saber se o NAS recebeu a resposta ou se o cliente final obedeceu as instruções enviadas. Servidores NAS costumam ter poucos registros (logs) de suas atividades por questões de segurança. Por isso, é tão difícil criar e depurar a política de segurança usando NAS e RADIUS.

2.5.3.3. Data Stores

São considerados armazéns de dados as bases de dados ou os diretórios (LDAP) que permitem o armazenamento e a recuperação de dados. Esses armazéns de dados tem capacidade de decisão limitada. A diferença chave entre servidores RADIUS e armazéns de dados é que eles suportam políticas e autenticação. A função de um armazém no processo de autenticação é fornecer dados para o servidor RADIUS. O servidor é quem usa um método para autenticar o utilizador. Sob vários aspectos, o protocolo RADIUS é similar a uma linguagem de consulta

como SQL (Structured Query Language). A base de dados nunca pode ser acessada diretamente pela NAS, cabendo ao RADIUS transformar essa requisição em consulta SQL.

2.5.4. Funcionamento do RADIUS

De acordo (MORAIS, Giovane. 2015) citando (Rigney et al. 2000) o servidor RADIUS tem três funções básicas: a de autenticar usuários, de autorizar a serviços providos pela rede e de contabilizar todo novo pedido de entrada na rede por parte do requisitante.

Segundo (LATERZA, Leandro Reis. 2012) o RADIUS tem como base em seu desenvolvimento o modelo cliente/servidor, sendo o cliente o NAS e o servidor RADIUS. É realizada a troca de mensagens entre o utilizador, o NAS e o servidor quando o utilizador solicita se autenticar para utilização de um servidor na rede. A mensagem do protocolo RADIUS é constituída de um pacote contendo cabeçalho RADIUS com o tipo de mensagem, também podendo conter atributos associados à mensagem. No RADIUS existem atributos para nome de utilizador, senha do mesmo, tipo de serviço solicitado pelo utilizador bem como para o IP (Internet Protocol) do servidor de acesso.

O NAS responsabiliza-se em receber todos os dados do utilizador, que em grande parte dos casos são o nome de utilizador e senha (a senha é cifrada no envio do NAS para o servidor evitando assim intrusões) e também enviá-los ao servidor RADIUS através do pedido de acesso este designado de Access-Request.

Após receber a solicitação de acesso o servidor realiza a tentativa de autenticação do utilizador, em seguida é enviada uma resposta para o NAS, resposta essa contendo um Access-Reject, em caso de acesso negado e um Access-Accept em caso de acesso aceito ou então Access-Challenge no caso de uma pedida de nova confirmação. Após o processo de autenticação, é realizada a comparação e verificação de alguns dados para que o servidor determine o nível de acesso a ser fornecido ao utilizador que foi autenticado. A figura 7 descreve o funcionamento do servidor RADIUS.

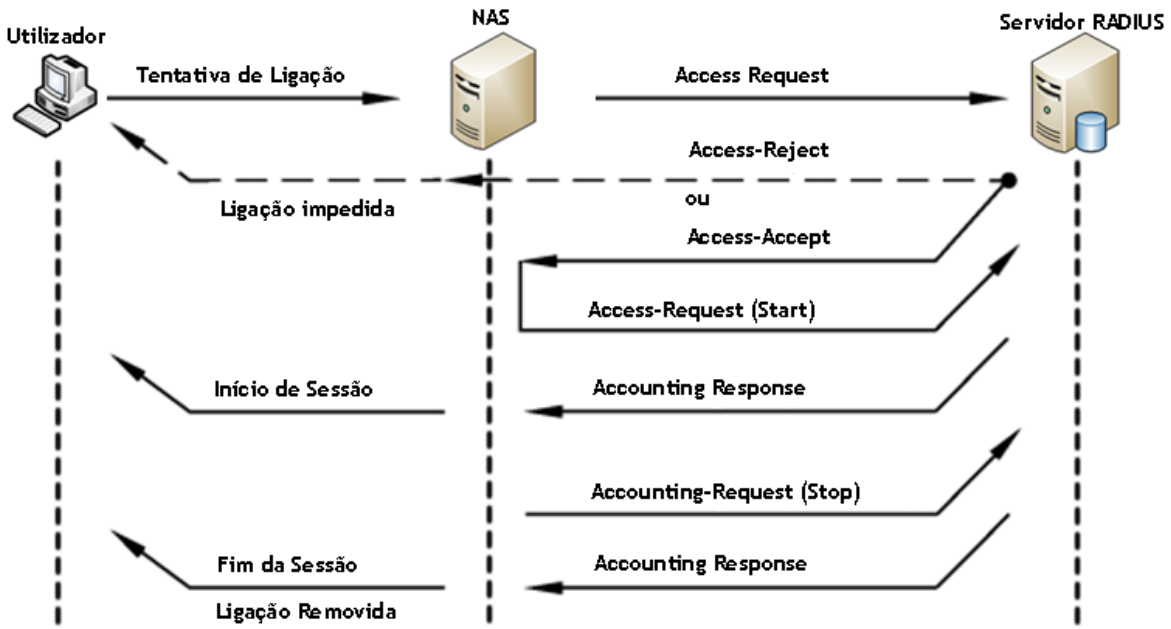

Figura 7: Funcionamento do servidor RADIUS. **Fonte:** (LATERZA, Leandro Reis. 2012).

2.5.5. Vantagens

- É um ótimo mecanismo para fornecer acesso múltiplo para administradores.
- Ele fornece uma identidade única para cada utilizador em uma sessão.

2.5.6. Desvantagens

- A implementação inicial desse mecanismo é difícil para o hardware.
- Possui uma variedade de modelos que podem requerer uma equipe especial que consome muito dinheiro.

2.5.7. Soluções de Servidores RADIUS Existentes

Existem no mercado muitas soluções para servidores RADIUS. O freeRADIUS é o servidor RADIUS mais utilizado para sistemas Linux. Este é responsável pela autenticação de pelo menos um terço dos utilizadores na Internet. Os restantes utilizadores encontram-se divididos entre os restantes servidores, destacando-se entre eles o Cisco Access Control Server (ACS) e o Microsoft Internet Authentication Service (IAS).

2.5.8. Software FreeRADIUS

Segundo (MORAIS, Giovane. 2015) citando (SLAVIN, 2003) o FreeRADIUS é um software livre, onde muitos servidores RADIUS comerciais no mundo estão sediados. O FreeRADIUS gera um servidor que acumula o maior número de formas de autenticação e, atualmente, é o único servidor RADIUS de código livre que suporta o método de autenticação EAP. Além disto, este software é o único que suporta virtualização, mantendo os custos de implantação e manutenção baixos. Apesar de não utilizar muitos recursos de processamento e memória RAM da máquina hospedeira (virtual ou física) um servidor RADIUS pode manipular de poucas até milhares de requisições por segundo com grande desenvoltura.

2.6. Principais diferenças entre Kerberos LDAP e RADIUS

Algumas das principais diferenças entre Kerberos, LDAP e RADIUS são:

1. Mecanismo de autenticação: o Kerberos usa um mecanismo de autenticação baseado em tíquete, enquanto o LDAP e o RADIUS usam um mecanismo de autenticação baseado em nome de utilizador e senha.

2. **Criptografia:** Kerberos fornece criptografia forte para autenticação e proteção de dados, enquanto LDAP e RADIUS não fornecem criptografia por padrão.

3. **Autorização:** Kerberos é usado principalmente para autenticação, enquanto LDAP e RADIUS fornecem autorização e gestão de contabilidade.

4. **Implantação:** Kerberos é normalmente usado em ambientes corporativos, LDAP é comumente usado para a gestão centralizada de contas e permissões de utilizadores, enquanto RADIUS é amplamente usado em ambientes ISP e VPN para a gestão AAA centralizada de dispositivos de rede.

CAPÍTULO III - Apresentação e Discussão dos Resultados

A autenticação de utilizadores é a primeira prioridade ao responder à solicitação feita para o acesso a uma rede de dados de uma organização/instituição. Para tal, dos protocolos existentes para a autenticação de utilizadores, destacamos alguns, tais como: Kerberos, LDAP e RADIUS.

- O Kerberos é mais focado na autenticação segura e na distribuição de chaves em ambientes corporativos;
- O LDAP é comumente usado para a gestão centralizada de contas e permissões de utilizadores; e,
- O RADIUS fornece a gestão AAA centralizada para dispositivos de rede em ambientes ISP e VPN.

Dentre os mesmos, o protocolo RADIUS mostrou-se o ideal para a implementação do caso de estudo na FEG, visto que, o acesso à internet para os funcionários é feito por via da rede sem fio e com fraca segurança, pois apenas é necessário obter a senha do roteador mais próximo para acessar a rede.

O RADIUS é um protocolo amplamente implantado que permite às empresas autenticar, autorizar e contabilizar utilizadores remotos que desejam acesso a um sistema ou serviço a partir de um servidor de rede central. Deste modo, cada utilizador terá acesso único, isto é, cada utilizador terá um nome de utilizador e senha única, assim o administrador da rede poderá fazer uma melhor gestão da rede e poderá expandir para toda a comunidade do recinto universitário.

3.1. Situação Actual da Rede de Dados na FEG

A FEG, outrora ESCOG é uma unidade orgânica criada a 20 de Agosto de 2008, com vocação para pesquisa, ensino, extensão e inovação nas áreas das ciências económicas e empresariais.
A sua criação foi uma resposta da UP-Maputo às exigências e necessidades do mercado de trabalho, que se fazia e ainda se faz sentir por profissionais qualificados de nível superior, com competência para competir no mercado de trabalho nacional e internacional e também para gerar o auto-emprego.

A FEG contém departamentos tais como,

- ❖ Departamento de Administração e Gestão de Recursos humanos;
- ❖ Departamento de Auto - Avaliação e Qualidade;

- Departamento de Extensão e Inovação; e,
- Departamento Pedagógico.

Neste capítulo são apresentadas técnicas e ferramentas utilizadas para a implementação e configuração do protocolo RADIUS para a gestão e controle de utilizadores na internet.

A internet da FEG é dependente de uma provedora de serviços de internet que atualmente suporta somente dados. É uma rede que começou a ser construída em meados de 2021 e contém uma rede de computadores que fornece alguns serviços básicos, destacando o mais importante, o acesso a internet para os seus funcionários, estes que na sua maioria são acessados via rede sem fio, com excepção da sala de informática onde contém uma rede de computadores cabeada. Porém, a rede da FEG contém fraca segurança na rede onde só é necessário a senha para o acesso da mesma, tomando como base a figura que será apresentada e o trabalho desenvolvido após um de levantamento de informação sobre a estrutura física e lógica da actual rede, é possível verificar a ausência de vários componentes que garantem a segurança da rede. Verifica-se também que a rede da FEG é desprovida de políticas de segurança, sendo esta acessível por qualquer utilizador que obtenha a senha da rede sem fio.

O acesso a internet é efectuado sem restrições localmente definidas, estando apenas à mercê do provedor de serviços.

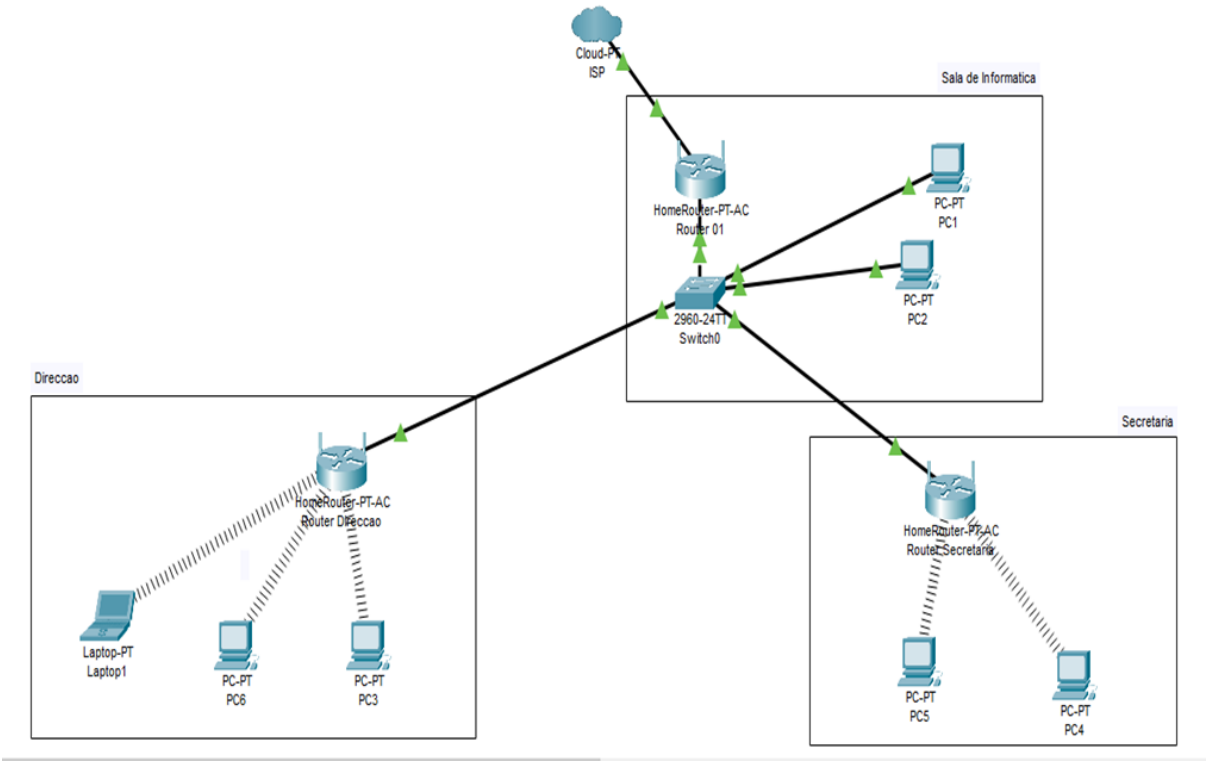

Figura 8: Rede atual da FEG**. Fonte:** Autor

A FEG, tem se empenhado na massificação do uso dos sistemas de informação como um recurso indispensável para alcançar seus objetivos que passam por oferecer serviços íntegros e confiáveis aos seus utilizadores, esta possui uma rede de computadores distribuída em todos os departamentos que a constituem, com acesso à internet por via da rede sem fio em todos os departamentos com excepção da sala de informática onde é comum encontrar pontos de rede inutilizados para a conexão de laptops dos seus funcionários, locais de trabalho com fraco alcance da rede sem fio.

Nesse contexto, é de maior importância que a rede local de dados da FEG se torne disponível e alcançável para os funcionários, CTA e os estudantes (para estudo individual ou em grupo) da faculdade. Por conseguinte, para garantir a operacionalização da rede, far-se-á necessário incorporar mecanismos de segurança e de gestão integrais para que esta não seja alvo de um dispêndio sem benefícios a longo prazo.

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

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

O protocolo RADIUS surgiu da necessidade de se estabelecer um limite no número de utilizadores que devem autenticar-se a rede de dados local da faculdade.

3.2. Apresentação e Discussão dos Resultados

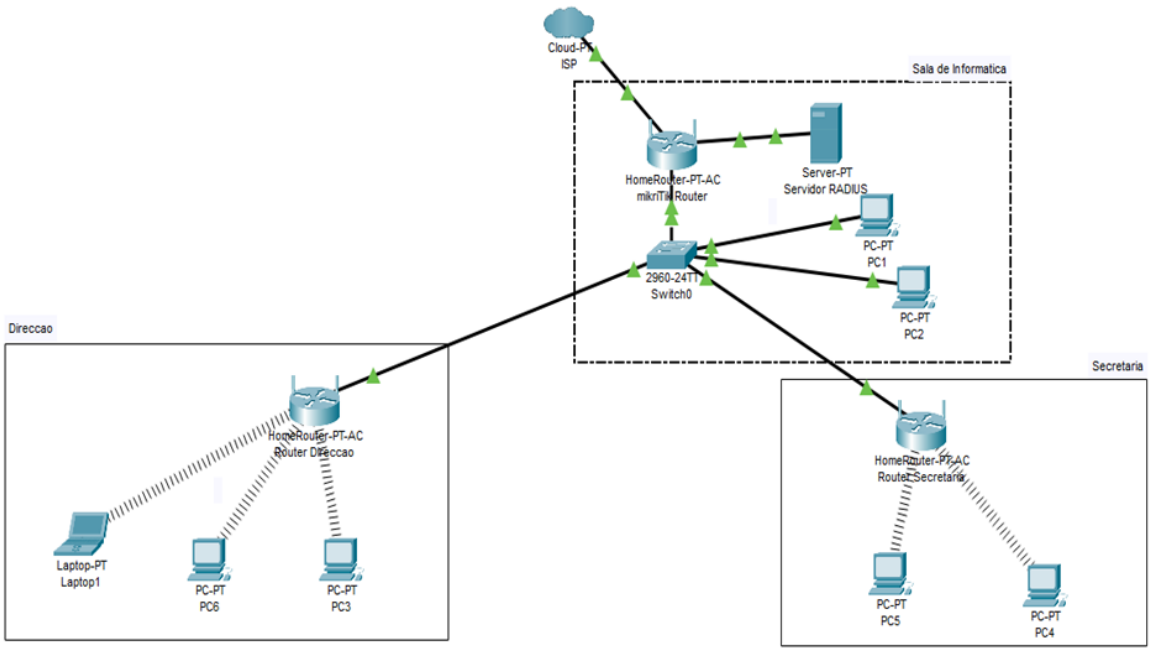

Figura 9: Implementação do Servidor RADIUS na FEG**. Fonte:** Autor.

Com vista na requalificação da rede informática da FEG como instituição de ensino, requalificação esta que visa no melhoramento da infraestrutura física da rede e diferentes níveis de acesso de forma a abranger toda a comunidade de utilizadores da faculdade, coube desenvolver uma proposta para a gestão do consumo de largura de banda de utilizadores, com recurso ao servidor RADIUS.

Hoje em dia é necessário assegurar a boa utilização da internet através de soluções que permitam fazer uma gestão com eficácia no seu uso em ambientes corporativos, impedindo o acesso a utilizadores não autorizados. Com o crescimento da tecnologia e a conectividade entre as instituições e a internet, cada vez mais um administrador de sistemas se preocupa com as informações que estão dentro da sua rede.

Dessa forma, entende-se que o acesso à internet pelos utilizadores é algo que necessita ser controlado, seja por questões de segurança ou de produtividade. Aos administradores, é designada a tarefa de implantar soluções com o objetivo de garantir a segurança da rede através de acções como:

- autenticar utilizadores ou dispositivos antes de permitir que acessem a rede;
- autorizar utilizadores ou dispositivos ao uso de determinados serviços da rede. e
- contabilizar e rastrear o uso desses serviços pelos utilizadores ou dispositivos.

3.3. Segurança

Trata-se de um aspecto muito importante do projeto de uma rede de computadores, especialmente com conexões à Internet dada a vulnerabilidade a qual se expõe. O objetivo básico desta precaução passa por garantir que problemas de segurança não afetem a instituição. Para tal, é preciso proceder com os seguintes requisitos:

1. Planificação;
2. Análise de riscos; e,
3. Levantamento de requisitos.

3.4. Planificação

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

3.4.1. Vertente física

A segurança física de uma rede inclui a proteção de todo um conjunto de componentes constituintes desta. É de extrema importância o estabelecimento de um perímetro devidamente protegido para todos os equipamentos de rede. A segurança física num ambiente de rede deve incluir: estabelecimento de uma sala especializada para incorporação dos diferentes servidores de rede, switches de camada de distribuição, e dispositivos de acesso WAN. Sendo que este é um aspecto patente na instituição e com condições apropriadas para o efeito desde o ponto de vista de acesso a climatização da mesma. É importante realçar que a segurança física dum ambiente de rede estende-se ainda a necessidade de incorporação de uma sala de UPS's (Uninterruptible Power Supply) capazes de garantir a alimentação dos componentes de rede prevenindo perdas de dados e danificação dos sistemas informáticos que possam ser causados por quedas de energia. Sob esse aspecto a rede não dispõe dessa capacidade dado que apenas a sala de informática possui um conjunto de UPS's que não são capazes de responder às necessidades.

3.4.2. Vertente lógica

A segurança lógica de uma rede de computadores constitui um aspecto crucial na administração da mesma, a falta de políticas claras de segurança pode comprometer a disponibilidade da rede e, até no nível mais crítico do negócio da instituição. Havendo necessidade de garantir o sigilo

de informações sensíveis e garantir a privacidade dos utilizadores da rede, prover parâmetros de conduta para utilizadores da rede. Contudo, a FEG até o exacto momento encontra-se desprovida de mecanismos de segurança para o acesso a internet para todos utilizadores. Aspectos como protecção de perímetro, protecção de acesso interno, são de grande relevância neste projecto.

3.5. Análise de riscos

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

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

3.6. Levantamento de requisitos

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

- Servidores;
- Dispositivos de interconexão (switches, roteadores, pontos de acesso);
- Dados de sistemas ou de aplicações;
- Imagem da instituição.

Convém ao administrador estabelecer políticas claras e demonstrar apoio e comprometimento com a segurança da informação através da emissão e manutenção de políticas de segurança da informação para toda a instituição. Os requisitos devem atingir objectivos, tais como:

- Identificar, autenticar e autorizar estudantes, CTA e funcionários da instituição a aceder à internet.
- Proteger hosts e dispositivos fisicamente;
- Proteger hosts e dispositivos logicamente através de senhas e direitos de uso;
- Proteger aplicações e dados contra vírus;

- Treinar utilizadores sobre políticas de segurança da instituição e sobre formas de evitar problemas de segurança.

As etapas que compõem o projecto de inclusão de estudantes e CTA são:

1. Identificação dos recursos de rede;
2. Análise de riscos (implicações) de segurança;
3. Elaboração de um plano de segurança;
4. Elaboração de políticas de segurança;
5. Elaboração de procedimentos para aplicação e implementação das políticas de segurança;
6. Manutenção da segurança através de auditorias periódicas.

3.7. Políticas de Segurança

1. Política de Acesso

a. Todos os estudantes, funcionários, técnicos de redes e dirigentes têm direito de acesso à rede mediante uma senha fornecida pelo administrador de rede.

b. Todos esses com excepção dos administradores de redes têm acesso a estes recursos de segunda a sexta no horário compreendido entre as 07h00 às 22h00 (52000s).

c. A conexão a dispositivos de rede é concedida apenas a equipe das TIC;

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

2. Política de Responsabilidade

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

b. O sistema deve gerar logs de auditoria para avaliar situações de risco.

3. Política de Autenticação

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

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

4. Políticas de Uso

a. Todos os funcionários podem fazer o uso ilimitado da rede de dados.

b. Todos os estudantes e CTA têm uso limitado de até 100 Kb/s da rede de dados.

CAPÍTULO IV - Conclusão e Recomendação

4.1. Conclusão

Em suma, Kerberos, LDAP e RADIUS são protocolos usados para autenticação e autorização em redes de computadores. Embora tenham algumas semelhanças, eles também têm algumas diferenças em termos de recursos e uso.

Kerberos é um protocolo de autenticação de rede que fornece autenticação mútua entre um cliente e um servidor. É usado principalmente em ambientes corporativos para autenticação segura de utilizadores e serviços. Ele usa um servidor de autenticação tercerizado confiável, conhecido como Key Distribution Center, para fornecer autenticação e distribuição de chaves seguras.

O LDAP, por outro lado, é um protocolo usado para acessar e manter serviços de informações de diretório distribuído em uma rede. É comumente usado para armazenar e recuperar dados de autenticação do utilizadores, como nomes de utilizador e senhas, e para a gestão centralizada de contas e permissões de utilizadores.

O RADIUS é um protocolo cliente/servidor que fornece a gestão centralizada de autenticação, autorização e contabilização para dispositivos de rede. É amplamente utilizado em ambientes de Provedor de Serviços de Internet e Rede Privada Virtual (VPN) para autenticar utilizadores remotos e fornecer acesso seguro a recursos de rede.

De uma forma geral, enquanto todos os três protocolos fornecem recursos de autenticação e autorização, o Kerberos é mais focado na autenticação segura e na distribuição de chaves em ambientes corporativos, o LDAP é comumente usado para a gestão centralizada de contas e permissões de utilizadores e o RADIUS fornece a gestão AAA centralizada para dispositivos de rede em Ambientes ISP e VPN.

Dentre as várias soluções do servidor RADIUS existentes e verificou-se que o FreeRADIUS é o mais utilizado para sistemas Linux, sendo responsável pela autenticação de pelo menos um terço dos utilizadores na Internet.

4.2. Recomendações

Recomenda-se a FEG para a implementação desta solução pois traz consigo uma vantagem no que se refere aquilo que virá a ser a gestão dos utilizadores no recinto universitário.

4.3. Referências Bibliográficas

GOMES, Daniel Cardoso. Proposta de Otimização do Tráfego da Rede da Universidade Federal de Lavras utilizando Spanning Tree Protocol. Lavras-Minas Gerais, 2005. 103 páginas.

FRANCISCATTO, Roberto; CRISTO, Fernando, Cristo; PERLIN, Tiago. Frederico Westphalen : Universidade Federal de Santa Maria, Colégio Agrícola de Frederico Westphalen, 2014.

HOUAISS, Villar. 2011. Disponivel em <https://gestaodesegurancaprivada.com.br/gestao-o-que-e-que-faz-conceitos/> acesso a 02.12.2021

SILVA, Edna Lúcia, MENEZES, Estera Muszkat. Metodologia da pesquisa e elaboração de dissertação 3. ed. rev. atual. – Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001.

DE OLIVEIRA, L. Marlúcia. Intranet; Uma Ferramenta Estratégica de Apoio à Gestão do Conhecimento nas Organizações. Belo Horizonte 2010.

LATERZA, Leandro Reis. Redes Sem Fio Padrão 802.1X Implementação de Uma Rede Segura Utilizando Protocolo de Autenticação EAP-TLS. Brasília. 2012.

MORAIS, Giovane. Segurança da Informação Através de Autenticação Centralizada por IEEE 802 1x Baseada em Protocolo RADIUS e Base de Dados LDAP Aplicada à Redes Sem Fio. 2015.

JÚNIOR, A. Wagner. Kerberos com Backend LDAP: Análise e Implantação. Lavras-Minas Gerais 2011.

CANEVER, Muriel. Implantação de um controle centralizado de usuários utilizando o protocolo LDAP. São José-SC. Dezembro/2016.

CHIRINDZA, A. Hilário. Proposta de implementação do servidor proxy para segurança de dados-caso de estudo Universidade Pedagógica - Campus Lhanguene. Maputo. 2018.

HASSELL, Jonathan. Radius, 1 ed, O'Reilly. 2002.

ANTUNES, Vitor H. L. Frontend Web 2.0 para gestão RADIUS. 2009

ANTUNES, Vitor. Dissertação-Frontend Web2.0 para Gestão de RADIUS. Disponível em <https://paginas.fe.up.pt/~ee04199/radius.html 2008/2009> acesso a 28.01.2023.

Disponível em <https://www.vivaolinux.com.br/artigo/FreeRADIUS-Nocoes-basicas-Parte-I?página=2> acesso a 07.02.2023.

Apêndices

Imagens da Rede de Dados da FEG

Figura 1: Antena que recebe dados para o acesso a Internet.

Figura 2: Roteador principal que recebe dados, adaptador PoE e switches para compartilhar dados pela faculdade.

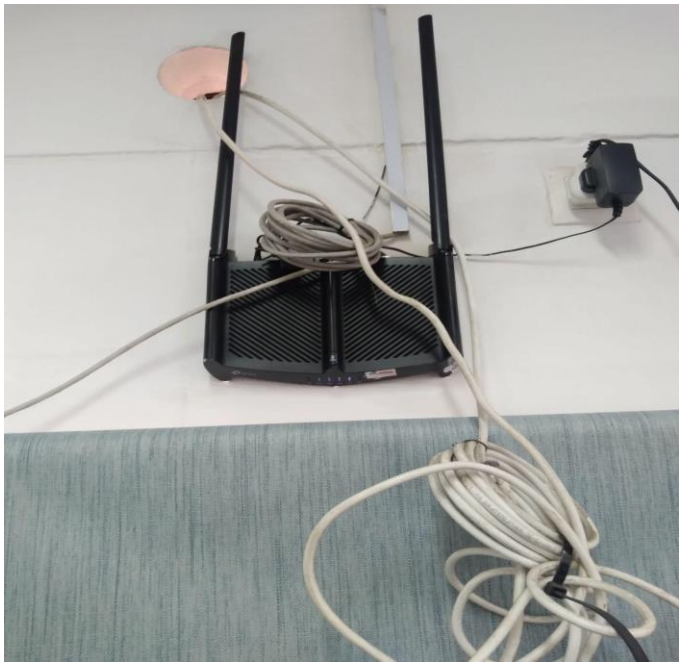

Figura 3: Roteador da Secretaria.

Figura 4: Roteador da Direcção.

Figura 5: Adaptador de rede sem fio.

Instalação e configuração do Servidor RADIUS

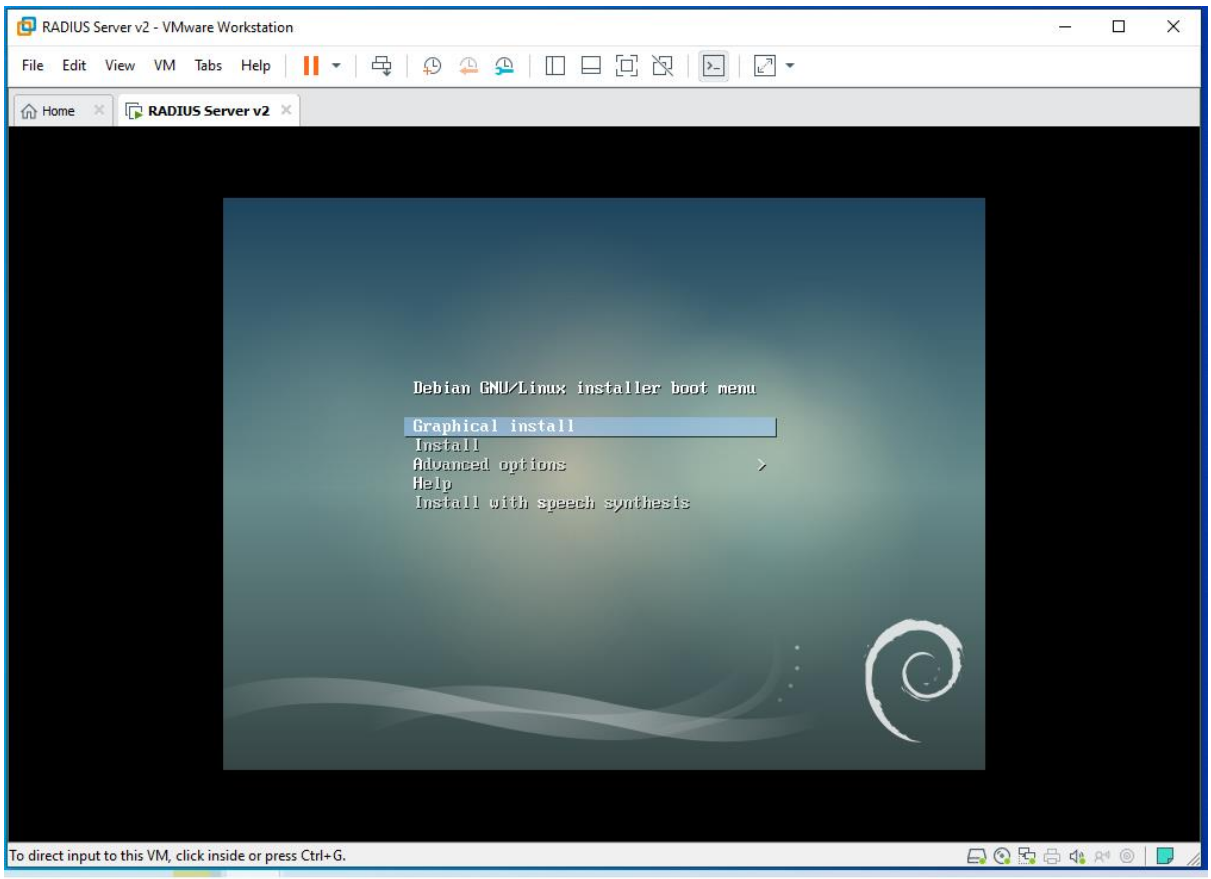

Figura 6: Tela inicial da instalação do sistema Debian.

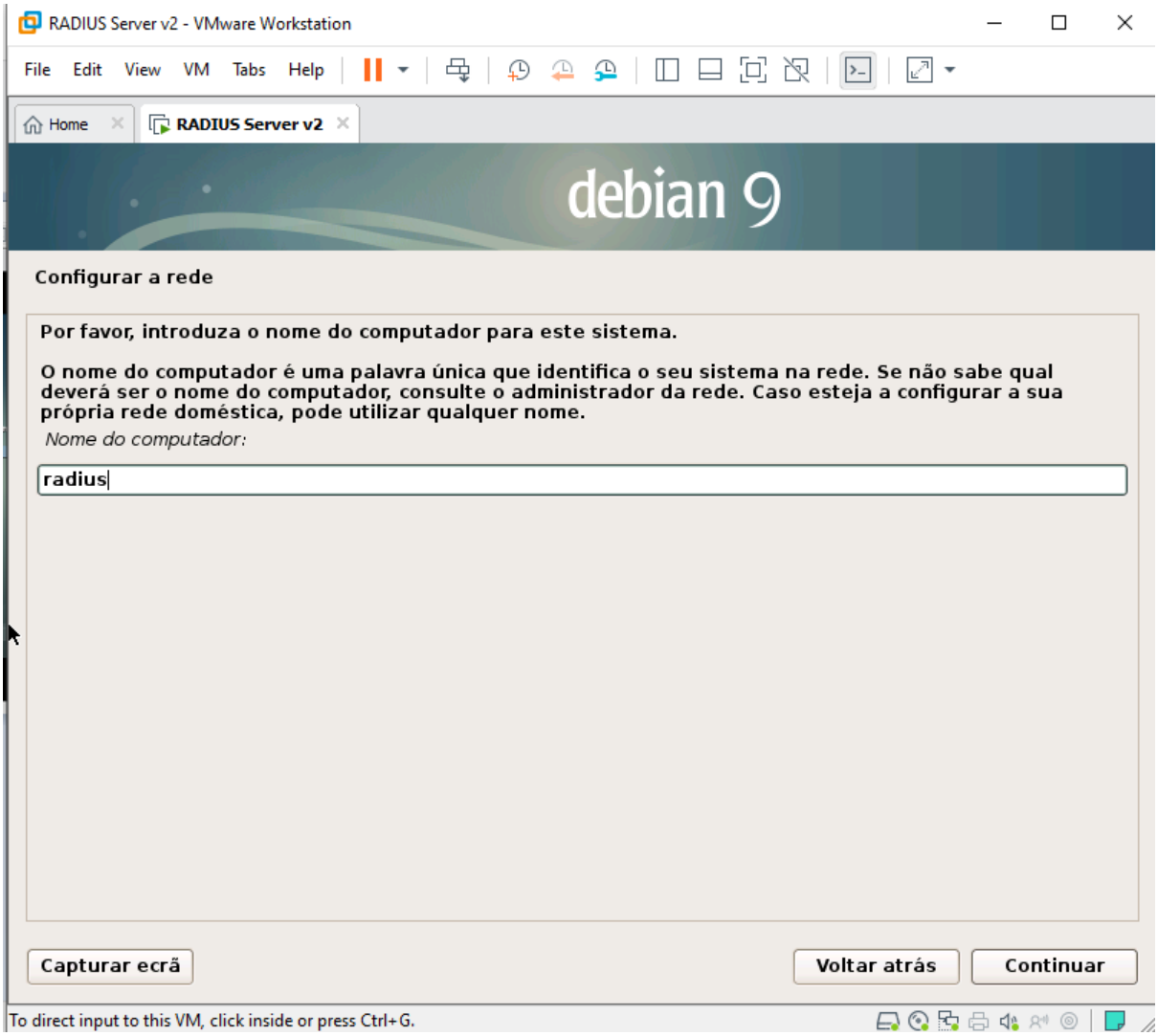

Figura 7: Definição do nome do computador.

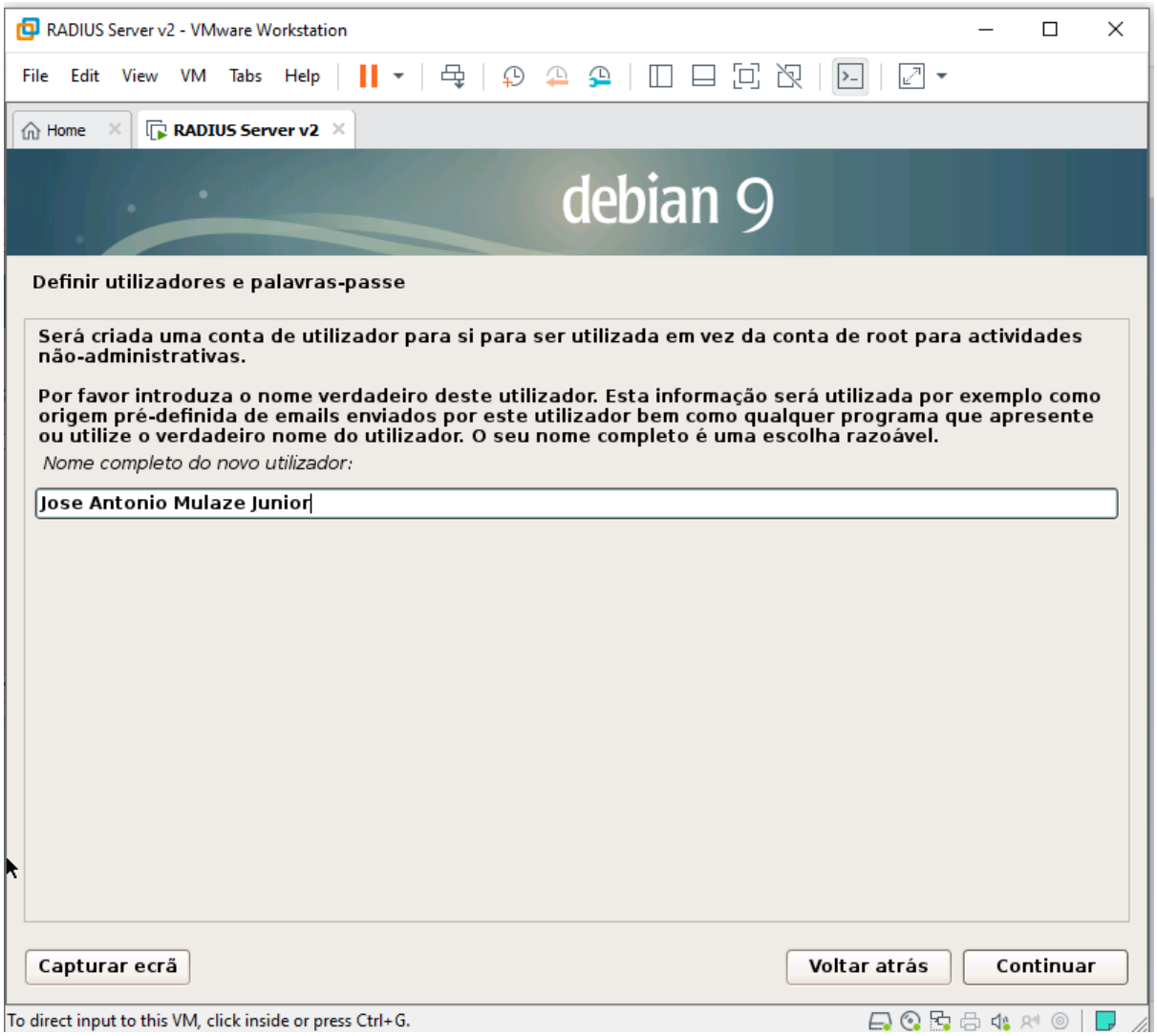

Figura 8: Definição do nome do utilizador.

Figura 9: Instalação do sistema concluído.

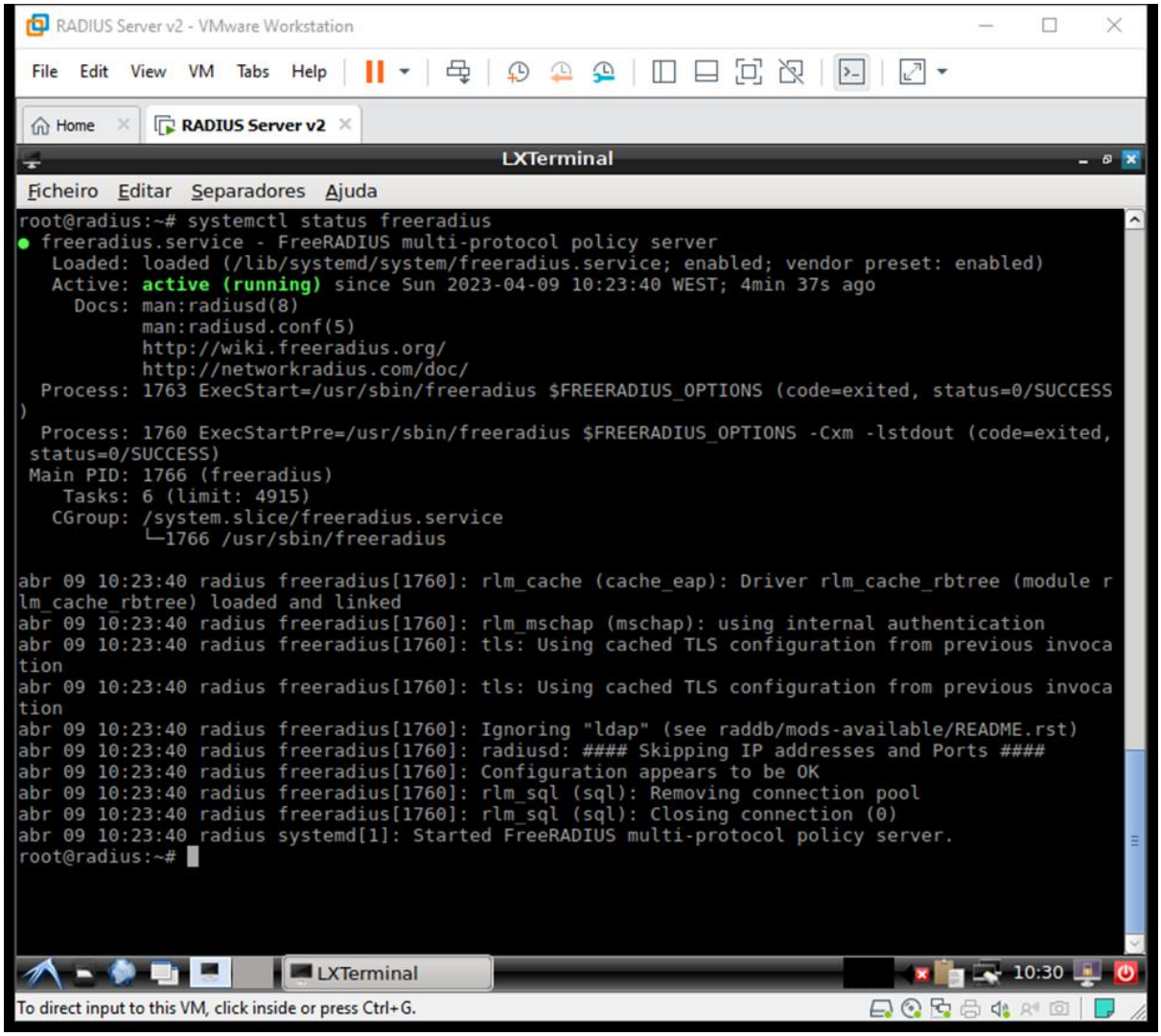

Figura 10: Estado do servidor FreeRADIUS.

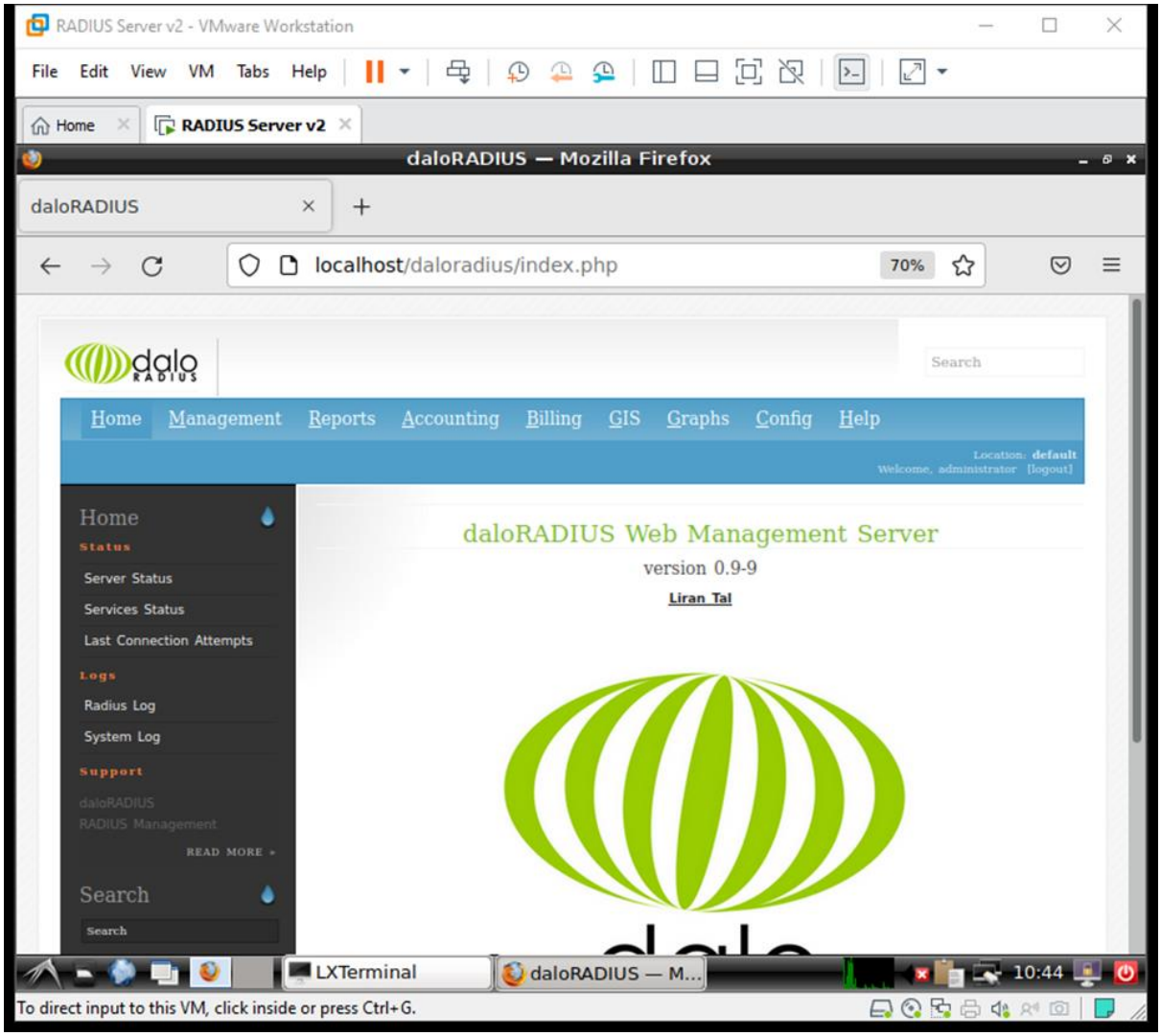

Figura 11: Tela inicial do daloRADIUS.

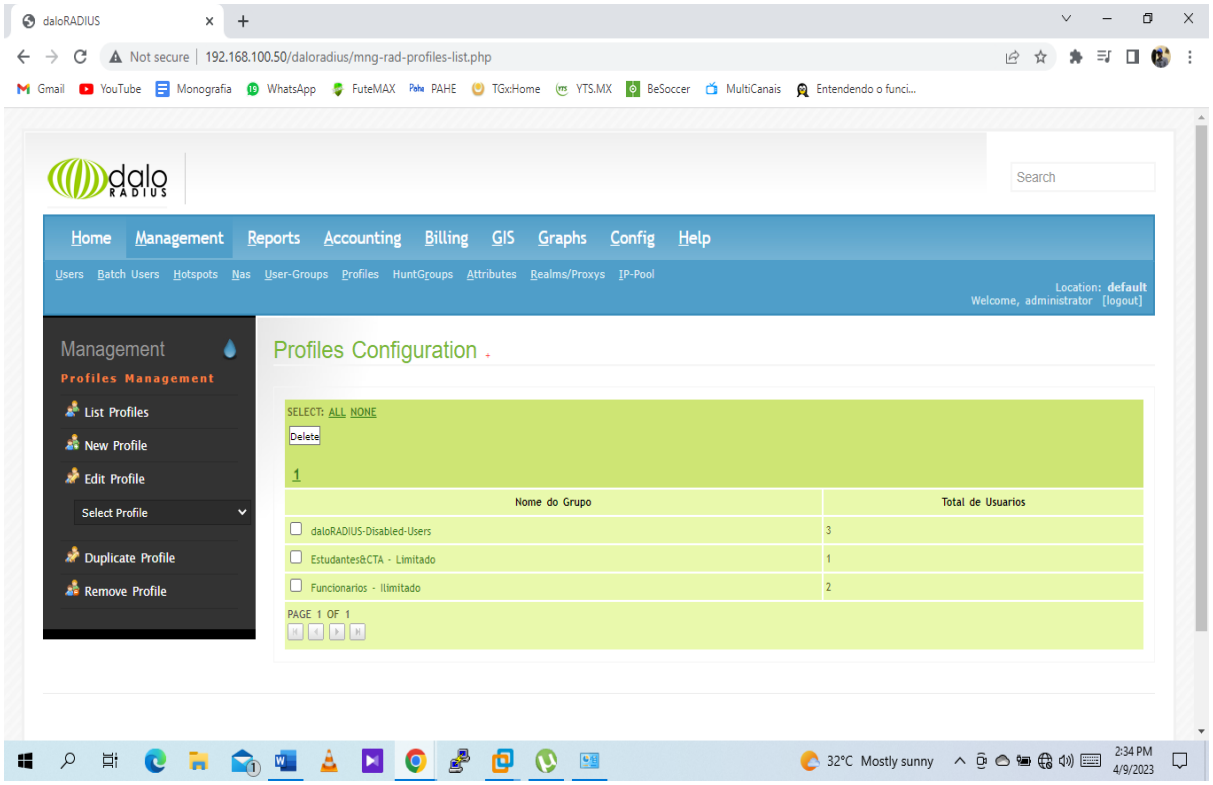

Figura 12: Lista dos perfis para os funcionários e estudantes.

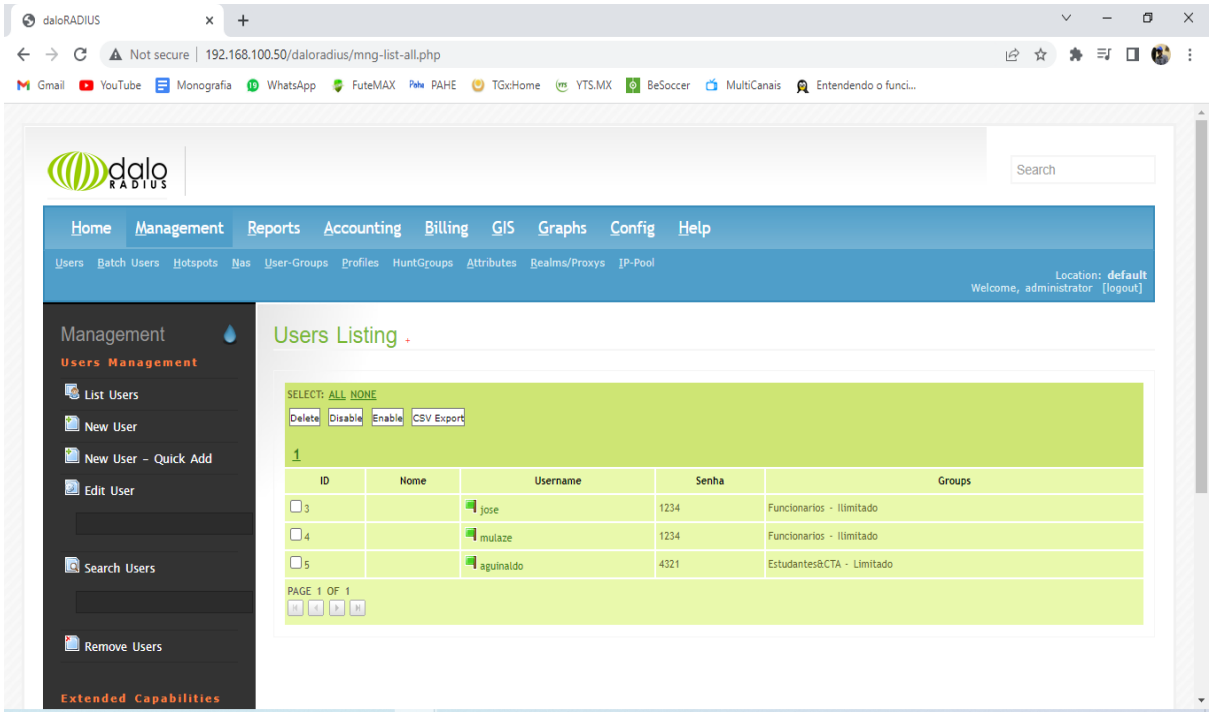

Figura 13: Lista dos utilizadores que podem se autenticar ao servidor freeRADIUS

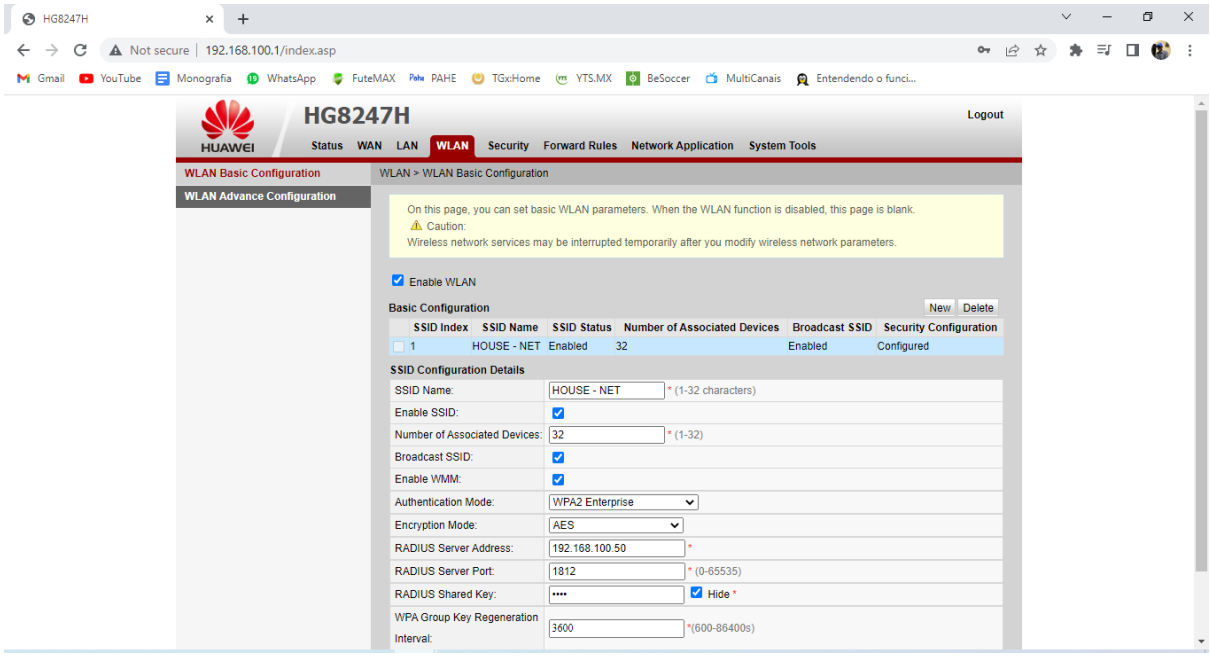

Figura 14: Ilustração da conexão do roteador e o servidor freeRADIUS para a autenticação dos utilizadores.