SEGURANÇA DE REDES WIRELESS COM PROTOCOLO RADIUS: PADRÃO 802.1x

Thiago Luan Tenório da Silva
Graduando em Tecnologia em Redes de Computadores pela Fatec-Bauru
thiago.silva395@fatec.sp.gov.br

Wesley Gama Santos
Graduando em Tecnologia em Redes de Computadores pela Fatec-Bauru
wesley.santos73@fatec.sp.gov.br

Henrique Pachioni Martins
Docente na Fatec-Bauru
henrique.martins01@fatec.sp.gov.br

RESUMO

A busca por conexões à internet vem crescendo em uma escala elevada atualmente, essa busca se centraliza basicamente por conexões a redes sem fio (wireless), por apresentar uma maior flexibilidade, velocidade, custo baixo e conforto. Entretanto a rede wireless apresente muitas vulnerabilidades e que são exploradas por criminosos virtuais, e isso acaba requerendo mais atenção dos administradores de rede. Esse artigo tem como finalidade apresentar uma alternativa na segurança de rede sem fio utilizando o protocolo RADIUS com o padrão IEEE 802.1X, para garantir criptografia e autenticação de usuário.

Palavras-Chaves: Protocolo Radius; wireless; segurança; autenticação

1 INTRODUÇÃO

Com o avanço da tecnologia e com todos os recursos já disponíveis, com menos frequência nos deparamos com a conexões cabeadas. Na maior parte dos ambientes público ou privado atualmente é bem provável que tenha uma conexão Wi-Fi, e na maioria das vezes as pessoas não se perguntam como essa conexão se estabelece e muito menos se esse recurso tão desejado é seguro.

Sabe-se que na internet não existe segurança total. Fato este é comprovado quando nos deparamos com grandes empresas sofrendo ataques cibernéticos. Se é possível uma grande empresa com muitos recursos de segurança de rede, como firewall, antivírus e uma equipe especializada passar por tais problemas, imagine pequenas empresas ou até mesmo usuários comuns.

Quando realizamos uma conexão em uma rede sem fio, colocamos nossos aparelhos a serviço daquela conexão, e há uma troca de dados entre o aparelho de rede no qual estamos conectados e o nosso aparelho particular. Percebe-se nesse ponto a vulnerabilidade, uma porta para conexão é uma porta para um invasor mal-intencionado.

Verissimo (2002) aponta que a principal falha de segurança é o próprio ser humano, diferente de uma máquina que se pode controlar e agir de forma lógica, seres humanos agem por sentimentos e muitas das vezes por impulso, e sabendo desta

falha, os ataques ocorrem sem nem mesmo ligar um computador, mas somente analisando o cotidiano de uma pessoa, seus hábitos e suas informações.

A maioria dos ataques cibernéticos visam alvos com algum grau de importância e que, na maioria das vezes, se trata de grandes empresas, pois conseguem pagar resgate de dados com valores altíssimos. Entretanto, empresas grandes ou pequenas, multinacionais ou somente um pequeno comercio, precisam de segurança, pois todo seu trabalho está ligado à rede e a conexão, pensando nisso buscamos na literatura um meio coorporativo de defesa, algo que pudesse dificultar o acesso a uma rede sem fio, que conseguisse ser implementado de forma que todos fossem protegidos e ao mesmo tempo houvesse um controle dos aparelhos conectados.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Protocolo RADIUS

Identificamos o protocolo *Remote Authentication Dial In User Service* (RADIUS), usado para autenticar e autorizar usuários na tentativa de conexão a uma rede Wireless, seja por conexões de roteadores incorporados, modens etc.

Esse protocolo trata de uma segurança de acesso, ou seja, ele dificultará o acesso a uma determinada rede wireless, como afirma Rufino (2019). Eventualmente, caso uma pessoa consiga a senha e tente se conectar a uma rede Wi-Fi, esse usuário será automaticamente direcionado para um serviço de autenticação, o qual irá oferecer a este usuário um campo para preenchimento de dados, estes dados preenchidos serão enviados ao servidor do protocolo implementado na rede (RADIUS), que fará a varredura e identificará se ele tem acesso. Caso tenha acesso liberado, recolherá estes dados e registrará que o usuário se conectou, caso não tenha acesso será bloqueado (CARVALHO, 2008).

O protocolo RADIUS é um protocolo AAA de padrão aberto, que usa a porta UDP 1645 ou 1812 para realizar a autenticação e a porta UDP 1646 ou 1813 para contabilização (CARVALHO, 2008). AAA significa Autenticação, autorização e contabilidade. RADIUS irá verificar se um usuário pode ou não acessar a rede (autenticação) ele estabelece quais são os privilégios e permissões que a rede oferece (autorização) e deixa registrado a atividade do usuário conectado à rede (contabilidade) (CARVALHO, 2008).

RADIUS atua usando o modelo cliente-servidor, o qual segue três componentes principais:

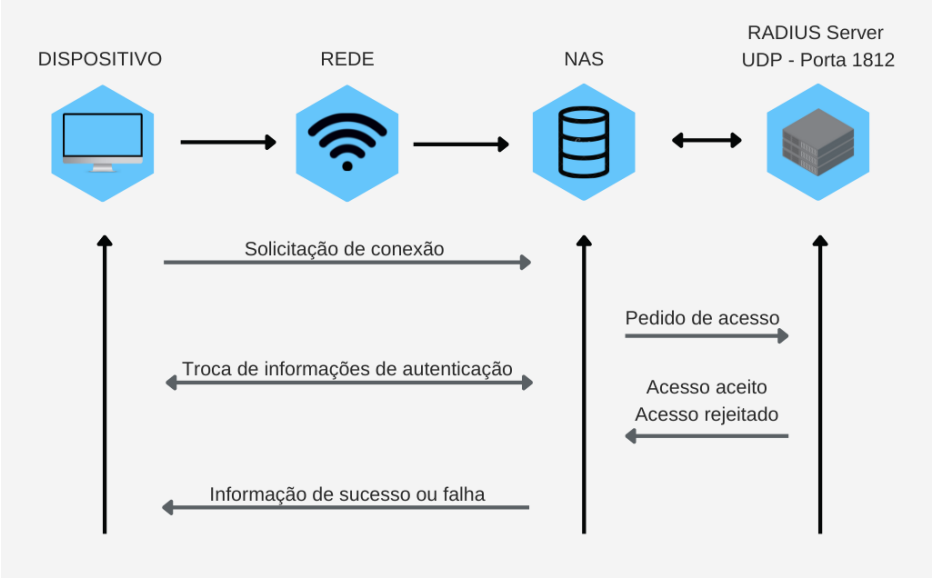
- Cliente/Suplicante: Dispositivo que busca o acesso à rede. Pode ser qualquer aparelho que consiga buscar conexão wireless.
- Servidor de acesso à rede, Network Access Server (NAS): atua como gateway entre o solicitante e a rede. Quando um usuário tenta obter acesso à rede o NAS passa as informações de autenticação (nome de usuário e senha por exemplo) entre o usuário e o servidor RADIUS, esse processo é o que chamados de sessão de autenticação. Ele fará a ligação entre o usuário e o servidor RADIUS.
- Servidor RADIUS: Servidor que autêntica o usuário para acessar a rede com os privilégios estabelecidos. O servidor RADIUS aguarda a solicitação do dispositivo NAS (CARVALHO, 2008).

Para que o protocolo RADIUS consiga realizar a autenticação, é necessário usar um protocolo que faça esse serviço. Existem vários protocolos que oferecem essa

função, porém o mais usual é o protocolo *Point-to-Point Protocol* (PPP). PPP é estruturado para estabelecer uma conexão entre dois nós.

De acordo com CARVALHO (2008), neste modelo cliente/servidor a troca de dados é feita através da camada de transporte do modelo *Open System Interconnection* (OSI). Esses pacotes trafegados pode ser a solicitação, nomes de usuários, senhas e muito mais. O transporte pode ocorrer através dos protocolos UDP e TCP, porém o RADIUS usa o protocolo de transporte UDP por padrão. Essa escolha pelo UDP está relacionada a sua sobrecarga de transmissão que é muito menor. O TCP tem por característica verificar se os dados foram recebidos, isso gera uma sobrecarga. No caso do RADIUS, é utilizado o protocolo UDP pois quem irá garantir uma transmissão bem-sucedida é o servidor RADIUS e não o protocolo de transmissão (Figura 1).

Figura 1 - Conexão entre dispositivo e servidor RADIUS por intermédio do NAS.



Fonte: Autoria própria

A utilização do RADIUS garante uma segurança considerável à rede, pois obtém um método mais segmentado de gerenciamento de acesso do usuário à infraestrutura de rede. Essa estratégia oferece controle geral sobre a infraestrutura, podendo gerenciar cada usuário conectado.

2.1.1 Protocolos de autenticação PAP e CHAP

Para receber os pacotes Access-Accept do servidor RADIUS é necessário inserir as informações corretas definidas pelo protocolo de autenticação que foi implementado.

Para PAIN (2009), essa autenticação pode ser realizada a partir de dois protocolos que são bastante utilizados para realizar essa tarefa, o *Password Authentication Protocol* (PAP) e o *Challenge Handshake Authentication Protocol* (CHAP).

PAP funciona de maneira simples, o usuário insere o nome de usuário e senha, que são enviadas diretamente para o NAS, esse envia posteriormente para o servidor RADIUS (PAIM, 2009).

Protocolo PAP é considerado inseguro pois o envio do nome de usuário e senha é enviado em texto simples, o que significa que qualquer invasor poderá

eventualmente interceptar esses pacotes entre o NAS e o servidor RADIUS, podendo desta formar roubar a mensagem (PAIM, 2009).

Conjuntamente temos o CHAP que é um método de autenticação mais seguro que o PAP. Diferentemente do PAP possuí criptografia para mascarar as informações que estão sendo transferidas.

De acordo com PAIM (2009), o funcionamento começa quando o usuário insere a sua senha, seu suplicante combina essa sequência aleatória de números que recebe do NAS, seguidamente ele executa essa combinação de senha e sequência aleatória por meio do hash MD5 (algoritmo de resumo de mensagem), com isso é criado um embaralhamento da sequência aleatória dos números com a senha inserida, tornando incompreensível.

O servidor RADIUS recebe tanto o nome de usuário como também a combinação e procura a senha que corresponde ao nome de usuário. Ele combina o desafio com a senha no seu banco de dados e faz a hash. Em seguida compara o resultado obtido e analisa a resposta recebida.

A senha precisa ser armazenada em texto sem formatação para realizar a hash, sendo isso o grande problema. Se eventualmente o servidor RADIUS seja comprometido, as senhas de todos os usuários estarão em texto simples. É por este motivo que formas de autenticação mais seguras foram desenvolvidas (PAIM, 2009).

2.1.2 Point-to-Point Protocol (PPP)

O protocolo *Point-to-Point Protocol* (PPP) ou protocolo ponto-a-ponto foi desenvolvido em 1993 com a finalidade de transferir todo tráfego entre dois dispositivos através da rede, sendo por cabo serial, linha telefônica, celulares, ligações de rádio especializadas ou ligação de fibras óticas. Com este protocolo, é possível conexões sobre Ethernet (PPPoE). O protocolo PPP é composto basicamente de três partes, sendo: encapsulamento de datagramas, *Link Control Protocol* (LCP) e *Network Control Protocol* (NCPs) (ABOBA, 1999).

O encapsulamento do PPP fornece multiplexação de diferentes protocolos da camada de rede, fazendo isso simultaneamente por intermédio do mesmo link. Ele foi projetado minuciosamente para garantir a compatibilidade com os suportes de hardwares mais utilizados (BLUNK, 2018).

São utilizados oito octetos adicionais para formar o encapsulamento do PPP. Somente em ocasiões em que a largura da banda é considerada crítica o encapsulamento e o frame podem ser encurtados para quatro ou até mesmo dois octetos.

Para que haja uma maior versatilidade e seja portável para mais ambientes, o PPP utiliza-se do protocolo de controle de link, o LCP, que é usado para lidar com variações nos limites de tamanho de pacotes, detectar repetições infinitas, detectar erros na configuração, iniciar e terminar a conexão além de concordar sobre opções de formato de encapsulamento. O LCP também pode prover facilidades de autenticação sobre o link, analisando assim se ele está apresentando falhas ou funcionando normalmente (BLUNK, 2018).

O NCP é o protocolo que gerencia e configura os protocolos da camada de rede que serão utilizados pelo PPP. Geralmente, links ponto-a-ponto geram problemas comuns em diferentes famílias de protocolos de rede, um exemplo é a atribuição e gerenciamento de endereço, esse e outros problemas são tratados pela família do NCPs.

O protocolo PPP é um protocolo da camada enlace do modelo OSI, que vem logo após a camada física. Isso significa que a utilização do PPP pode ser feita por diversas aplicações e pode transferir dados por vários protocolos, como TCP e UDP (BLUNK, 2018).

Alguns protocolos derivam do protocolo PPP, que são o *protocolo Point-toPoint Protocol over ATM* (PPPoA) e o *Point-to-Point Protocol over Ethernet* PPPoE.

O PPPoE utiliza a tecnologia Ethernet, e é muito utilizado pela facilidade em identificar o usuário que está conectado, isso depois de ele ser autenticado pelo menos uma vez (ABOBA, 1999).

O padrão PPPoE é suportado pelos sistemas operacionais como Windows ou Linux (e também derivados Linux), entretanto algumas versões mais antigas não contam com suporte nativo para o protocolo. No Windows o suporte ao protocolo PPPoE passa a ser nativo a partir do Windows XP. A sua finalidade é basicamente facilitar a transmissão de dados entre uma ligação ponto-a-ponto.

O protocolo PPPoA diferente do PPPoE só pode transportar os dados sobre o ATM, enquanto o PPPoE em Ethernet, com isso criou-se a nomenclatura PPPoA (ATM) e PPPoE (Ethernet) (ABOBA, 1999).

2.2 Protocolo IEEE 802.1X

O funcionamento do protocolo RADIUS foi desenvolvido inicialmente para redes dial-in, mas, atualmente, a maioria dos usuários está conectando seus sistemas a redes via cabos ethernet a uma rede local (LAN) ou Wireless Local Area Network/WiFi (WLAN). E essas conexões seguem os padrões prescritos pelos RFCs IEEE 802.1x (ABREHA, 2018).

O IEEE 802.1X segue uma lógica simples, o cliente precisa ser autenticado ao servidor RADIUS, e para isso é realizado uma autenticação por meio do *Extensible Authentication Protocol* (EAP) sobre rede LAN, o pacote é encapsulado em mensagens EAP sobre as redes locais. O processo dará início quando o usuário cliente envia uma solicitação de conexão a uma rede sem fio, através do *Acess Point* (AP). O autenticador ao receber a solicitação abre uma porta na sessão IEEE 802.1X (CROW, 2018).

De acordo com ABREHA (2018), para que haja a autenticação do protocolo 802.1x é necessária uma requisição à rede sem fio para o ponto de acesso (AP – *Access Point*), essa é enviada ao servidor de autenticação (RADIUS). A confirmação de acesso pelo servidor RADIUS pode ser efetuada tanto para o próprio usuário (usando a senhas e certificado) como pelo sistema (utilizando o endereço MAC – Media Access Control).

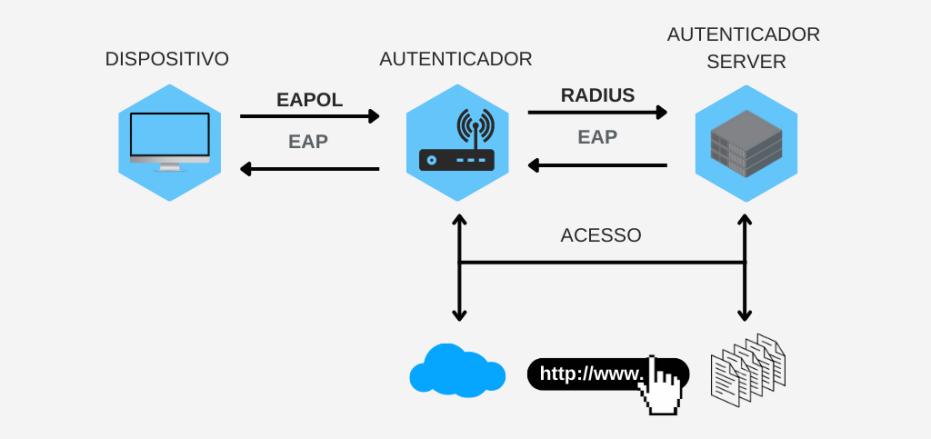
Semelhante aos parâmetros do protocolo RADIUS, a autenticação 802.1x segue esses três componentes distintos: Suplicante, o software em um dispositivo fornece as credenciais de usuário; Autenticador, dispositivo que permite o acesso do cliente ao recurso de rede, podendo ser um ponto de acesso sem fio ou switch ethernet; Servidor de autenticação, um servidor RADIUS que é o mais comum utilizado para autenticação 802.1x, embora isso não seja obrigatório (CROW, 2018).

A estrutura utilizada pelo protocolo 802.1x é a EAP como dito anteriormente, que tem a função de mover os pacotes de autenticação entre dois componentes. O EAP tem a capacidade de alavancar mais protocolos de autenticação do que PAP ou CHAP. Isso abrange os protocolos EAP-TLS, EAP-TTLS e EAP-PEAP, entre outros. O EAP não é um protocolo, mas sim uma estrutura para estabelecer um padrão de

solicitação/resposta. É muito flexível e por isso os acrônimos TTLS, TLS e PEAP anexados (CONCEIÇÃO, 2006).

Ao contrário do PPP que inicia uma conexão com um modem para discar para outro modem, o suplicante, neste caso, cria uma conexão que chamamos de *Extensible Authentication Protocol Over LAN* (EAPOL). A Figura 2 retrata a conexão por intermédio do protocolo 802.1x.

Figura 2: Conexão entre dispositivo e servidor RADIUS pelo 802.1x.



Fonte: Autoria própria

No lugar do NAS, utiliza-se um autenticador, que atua como um porteiro da internet ou dos recursos da rede LAN para conexões com fio. O autenticador pode ser um switch ou pode ser ponto de acesso sem fio, para conexões wireless. O servidor RADIUS continua na mesma posição, executando a mesma função, agora utilizando protocolos de autenticação mais robustos.

2.2.1 Autenticação EAP-TLS, EAP-TTLS e EAP-PEAP

Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) apresenta uma forma de segurança muito mais eficiente do que os autenticadores citados anteriormente. Podemos dar o exemplo do ataque *man-in-the-middle*, onde um invasor intercepta a mensagem no meio do caminho a fim de descobrir o conteúdo, isso era possível quando o autenticador enviava uma senha criptografada. Porém o EAP-TLS para evitar esses tipos de ataque, utiliza certificados digitais, chamados de certificados CA (autoridade certificada), que são utilizados para autenticar o usuário, não utilizando mais senhas trocadas. No caso do EAP-TLS, ambas as partes trocam um certificado para autenticar uma à outra (INTEL, 2018).

Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS) diferente da EAP-TLS esta forma de autenticação irá utilizar apenas um certificado para autenticar no servidor. O servidor não é autenticado no cliente mediante certificado CA, em vez disso, um túnel TLS é estabelecido entre o servidor e o cliente (INTEL, 2018).

O túnel TLS é criptografado, e todos os dados trafegados entre o cliente e o servidor também são criptografados, e a decriptação ocorre quando os dados chegam até o servidor RADIUS que verifica se a solicitação é permitida ou negada. O EAP-TTLS não tem a mesma robustez que o EAP-TLS, porém sua configuração é muito mais simplificada.

Extensible Authentication Protocol - Protected Extensible Authentication Protocol (EAP-PEAP) semelhante ao EAP-TTLS, também utiliza um túnel TLS criptografado

para enviar as informações entre o cliente e o servidor. O PEAP realiza a autenticação utilizando apenas um certificado do lado do servidor, simplificando assim a configuração (INTEL, 2018).

Uma comparação dos Protocolos de autenticação TLS, TTLS e PEAP é apresentada no Quadro 1

Quadro 1 - Descrição dos protocolos de autenticação

EAP 802.1X Recursos/Benefício	**TLS Segurança de Nível de transporte**	**TTLS Segurança de nível de transporte com túnel**	**PEAP Segurança de nível de transporte protegido**
Certificado lado do cliente necessário	Sim	Não	Não
Certificado do lado do servidor obrigatório	Sim	Sim	Sim
Gerenciamento de chaves WAP	Sim	Sim	Sim
Atributos de autenticação	Mútuo	Mútuo	Mútuo
Dificuldade de implantação	Difícil (por causa da implantação do certificado do cliente)	Moderada	Moderada
Segurança Wi-Fi	Muito Alta	Alta	Alta

Fonte: Intel, 2018

3 MATERIAIS E MÉTODOS

Com fundamentos em pesquisa bibliográficas, além de bases de dados cientificas, tais como Scielo e Google Acadêmico. Este artigo proporciona uma maior segurança nas organizações, no quesito acesso à rede sem fio provendo uma validação de usuário e senha.

Com a implementação do protocolo RADIUS é possível ver na prática o funcionamento de autenticação quando um usuário efetua tentativas de acesso a uma rede wireless.

Para o desenvolvimento e os testes foram utilizadas as seguintes ferramentas:

- Notebook Acer: Processador CORE I5 10 geração, SSD 500 GB, Memória: 8 GB, Windows 11 pro com uma máquina virtual (Virtual Box);
- Windows Server 2022: configurado com DHCP Serve, Active Directory e Certificado - NPS com RADIUS;
- Autenticação: Notebook Samsung core I5 com Windows 10, Celular Samsung, modelo A50 com Android 11;
- Router: Acess Point Air Live 802.11G Wireless AP.

3.1 Microsoft Windows Server 2022

O processo de implementação se inicia com a instalação do Windows Server versão de 2022 em uma máquina virtual. Começamos atualizando o Windows Server logo após a instalação. Com o Windows Server atualizado iniciou-se as configurações do Active Directory (AD), responsável por disponibilizar ao usuário o cadastro e as configurações necessárias para implementação do servidor RADIUS.

3.2 Router: Acess Point Air Live 802.11G Wireless AP

Este dispositivo atende os padrões 802.11G e 802.11B, e é compatível com a maioria dos dispositivos sem fio. Possuí 2 portas LAN para conexão ao roteador (Figura 3).

Figura 3 – Access Point AirLive Wireless AP.

Fonte: manualslib.com

O roteador possuí 54Mbps Wireless AP, 18dBm de potência, Antena removível, 2 portas LAN, 2MB de Flash e 16MB SDRAM. Conexão de rede Bridge, Client, Repeater, WDS e regulação de potência TX.

3.3 Metodologia

Para o desenvolvimento desta implementação seguimos a seguinte metodologia: levantamento bibliográfico sobre as tecnologias em torno do protocolo RADIUS, bem como o seu funcionamento e o funcionamento do protocolo 802.1X.

Com os estudos realizados sobre o protocolo RADIUS foi possível implementar e visualizar na prática o desempenho da autenticação por meio deste protocolo.

4 RESULTADOS E DISCUSSÃO

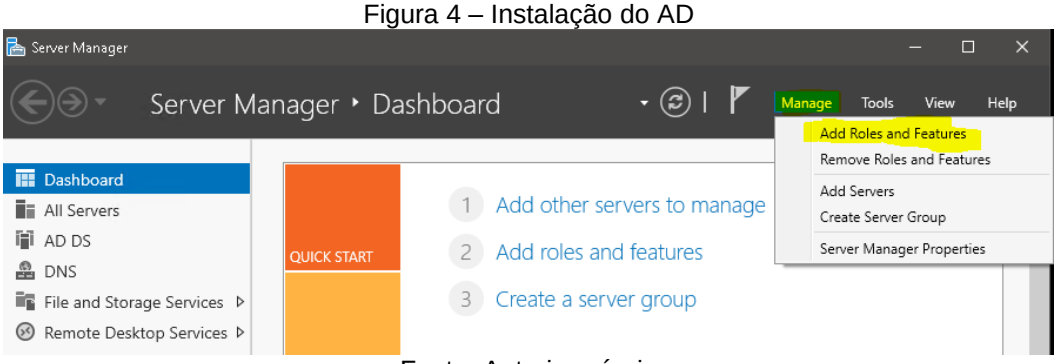
Esta seção apresenta os resultados do trabalho realizado. Inicialmente apresenta-se a instalação dos serviços de aceso e configuração das políticas de rede.

4.1 Instalação do AD e configuração do serviço

1. Inicia-se com a configuração do ambiente onde será adicionado as funções e recursos no Server Manager (Figura 4).
2. A seguir a instalação do *Active Directory Certificate Services* (AD CS) é iniciada, este serviço dentro do AD é um servidor designado para emitir os certificados

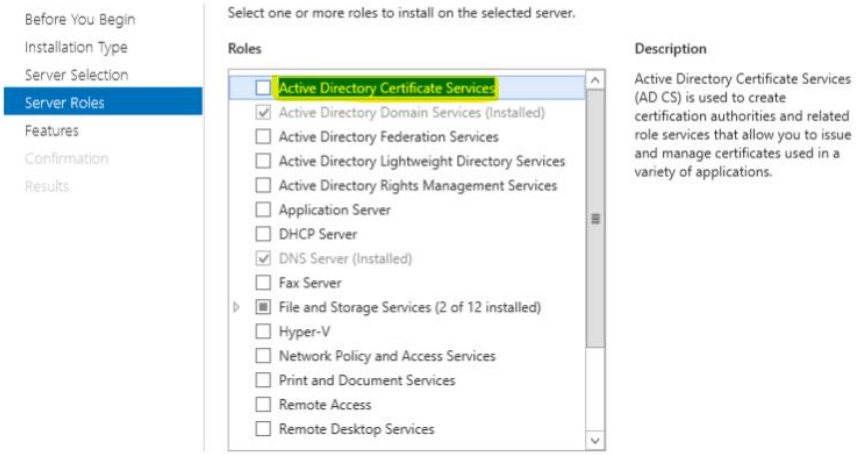
de infraestrutura de chaves públicas, *Public Key Infrastructure* (PKI), e gerenciar as listas de revogação de certificados (Figura 5).

Figura 4 – Instalação do AD



Fonte: Autoria própria

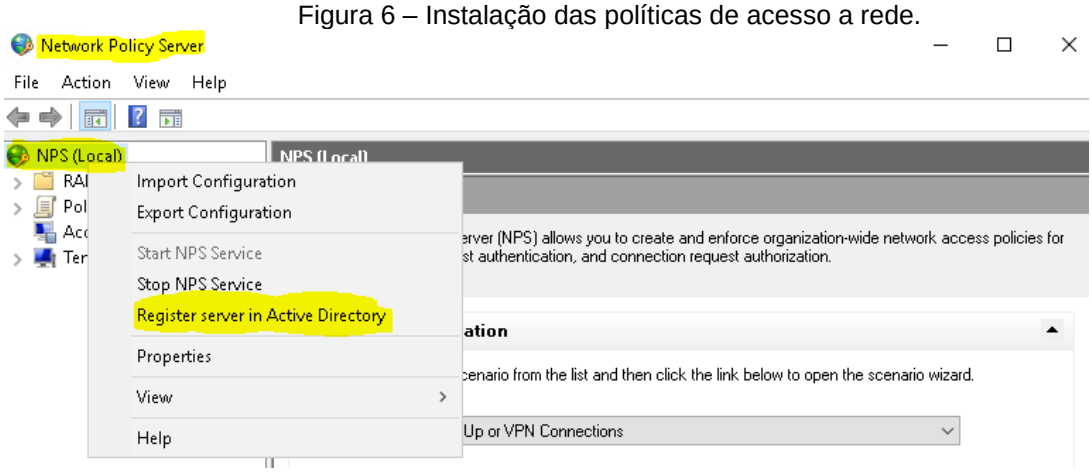
Figura 5 – Instalação Active Directory Certificate Services.



Fonte: Autoria própria

3. Após a instalação do AD CS inicia-se a instalação do Serviço de política de acesso à rede, *Network Policy and Access Services* (NPAS) (Figura 6). Esse serviço irá garantir a integridade e a segurança da rede. O NPAS inclui Network Policy Server (NPS), Health Registration Authority (HRA) e Host Credential Authorization Protocol (HCAP). Nesta implementação usaremos o NPS.

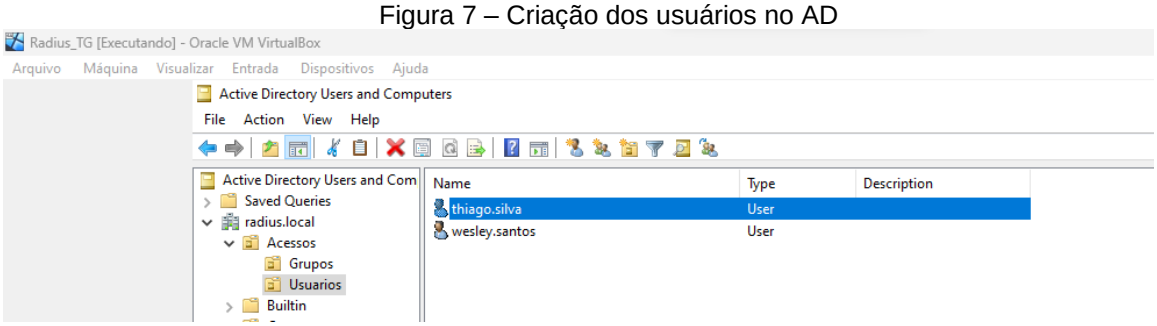
Figura 6 – Instalação das políticas de acesso a rede.



Fonte: Autoria própria

4. Configuração de usuário ao AD (Figura 7).

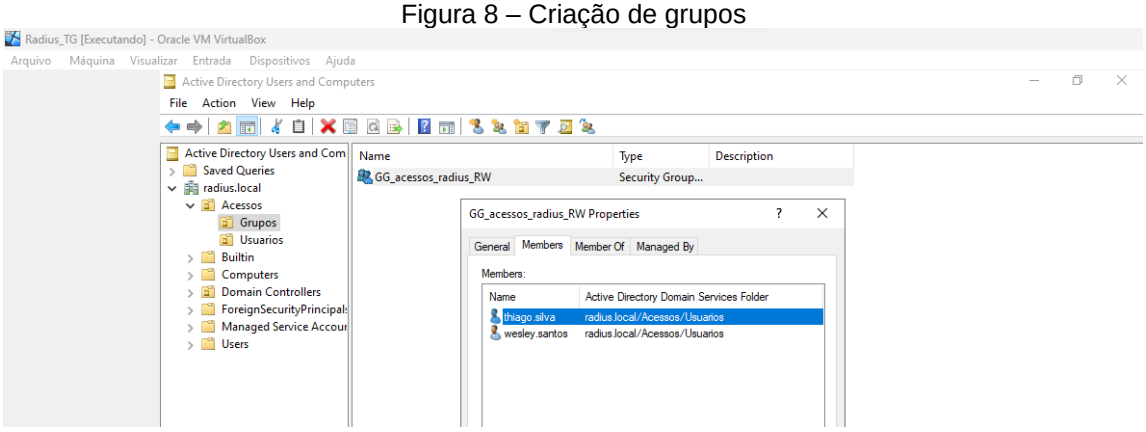
Figura 7 – Criação dos usuários no AD



Fonte: Autoria própria.

5. Criação do grupo para permissão dos usuários ao acesso à rede (Figura 8).

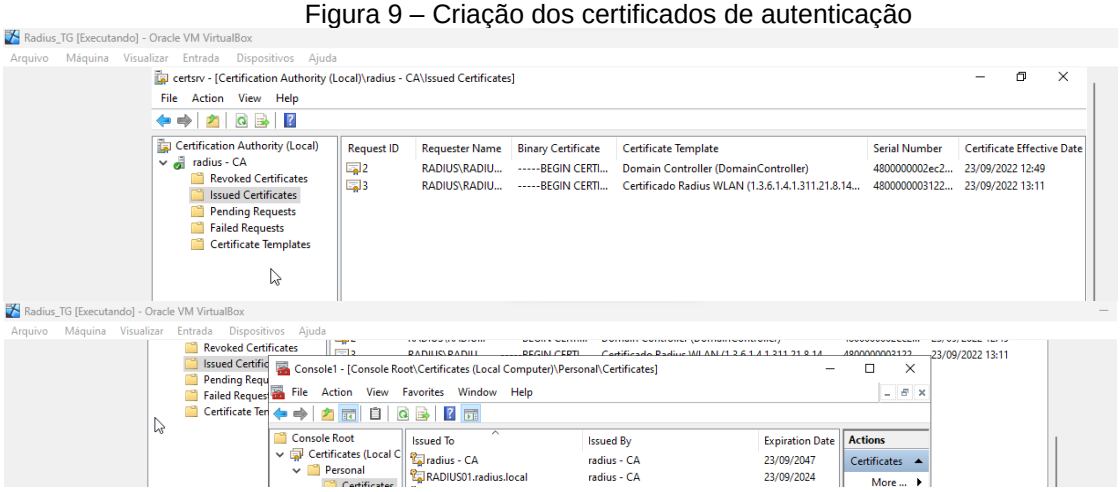
Figura 8 – Criação de grupos



Fonte: Autoria própria

6. Criação do certificado para autenticação de acesso (Figura 9).

Figura 9 – Criação dos certificados de autenticação



Fonte: Autoria própria

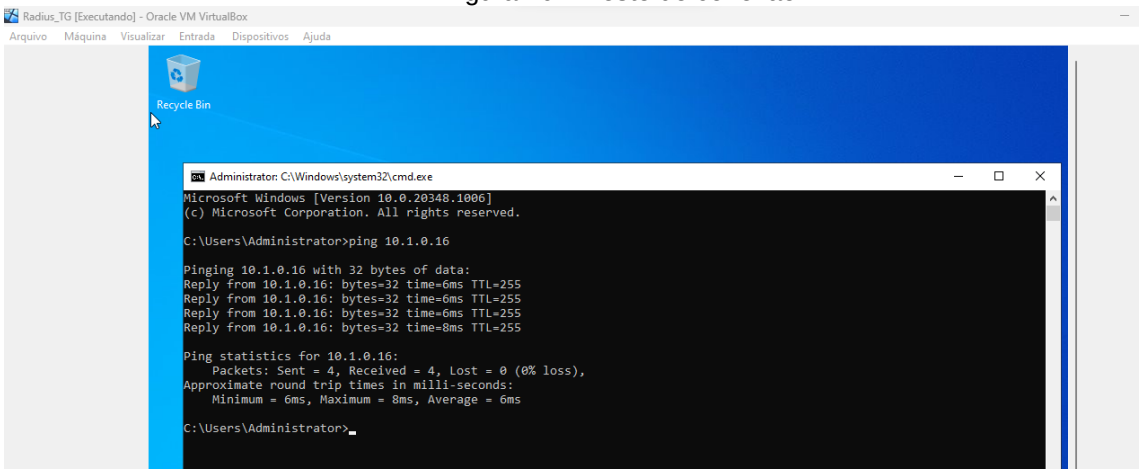
Neste ponto, o RADIUS foi configurado, ou seja, recebeu um nome e o endereço IP do servidor para o cliente, que realizará a conexão do protocolo RADIUS com o Active Directory.

Após a configuração do cliente RADIUS, configurou-se a política de segurança do servidor.

A seguir são apresentados os testes realizados.

7. Teste de ping ao roteador realizado (Figura 10).

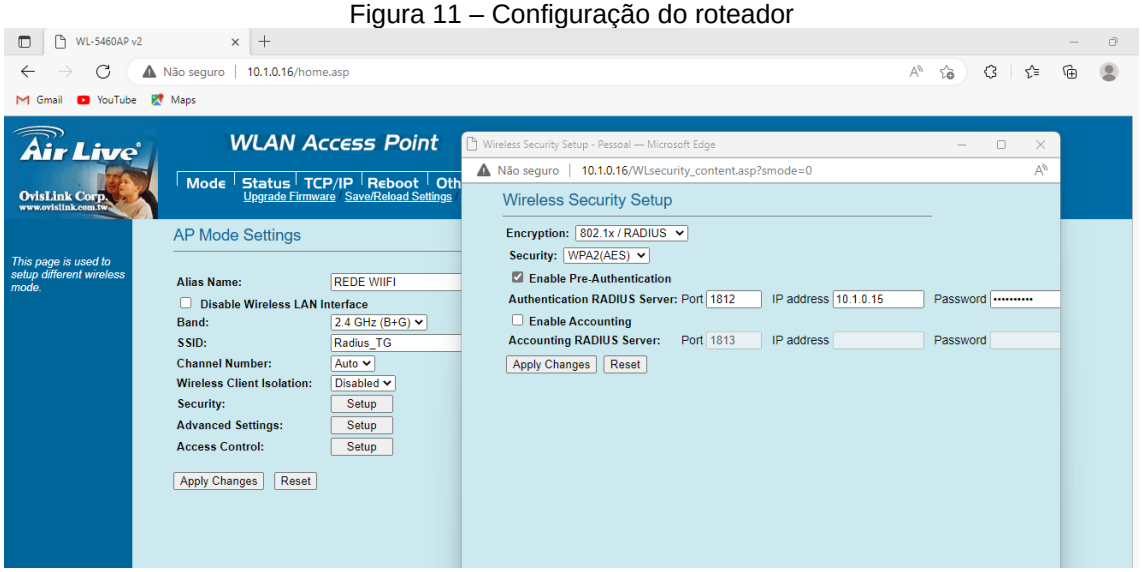
Figura 10 – Teste de conexão



Fonte: Autoria própria

8. Acessando o roteador para realizar as configurações (Figura 11).

Figura 11 – Configuração do roteador



Fonte: Autoria própria

9. Acesso à rede RADIUS pelo notebook (Windows 11) e pelo Smartphone (Android) (Figura 12).
10. Teste de conexão com a internet bem-sucedido (Figura 13).

As conexões realizadas foram autorizadas e autenticadas pelo servidor RADIUS que permitiu o acesso apenas aos usuários cadastrados dentro do AD.

A conexão acontece de forma rápida e estável, não houve problemas de lentidão e de perda de conexão. A autenticação do usuário acontece de forma simples, bastando colocar o ID e senha cadastrados do AD anteriormente.

Fizemos o teste inserindo duas credenciais dentro do servidor, ambas se conectaram com sucesso, provando que o RADIUS como uma alternativa segura e confiável.

Figura 12 – Conectando a rede RADIUS

Fonte: Autoria própria

Figura 13 – Teste de conexão com a internet.

Fonte: Autoria própria

5 CONCLUSÃO

A autenticação do protocolo RADIUS mostrou ser um recurso eficiente e capaz de fornecer uma proteção elevada ao usuário quando combinada com o padrão IEEE 802.1X. Por apresentar uma flexibilidade de autenticação e controle é competente em disponibilizar funcionalidades que o qualifica como um protocolo de autenticação eficiente nas mais adversas estruturas de rede, provendo segurança e confiabilidade. Com o protocolo RADIUS a administração de usuários autenticados é mais simplificada e transparente podendo apresentar ao administrador de rede um maior controle e um ponto central de autenticação.

6 REFERÊNCIAS

ABOBA, B.; SIMON D. RFC 2716 - **PPP EAP TLS Authentication Protocol**. 1999.

ABREHA, Meareg. **History and implementation of IEEE 802 security architecture. Department of Computer Science, Addis Ababa University**, Addis Ababa, Ethiopia. Disponível em: Acesso em: 20 set. 2018.

BLUNK, L,VOLLBRECHT, J. **RFC 2284 - PPP Extensible Authentication Protocol (EAP).** Disponível em < http://www.ietf.org/rfc/rfc2284.txt> Acesso em: 10 set. 2018.

CARVALHO, H. E. T. **Radius.** 2008. Disponível em: <https://www.gta.ufrj.br/grad/08_1/radius/Introduo.html>. Acesso em: 21 set. 2018.

CONCEIÇÃO, A.F; KON, F. Desenvolvimento de aplicações adaptativas para redes IEEE 802.11. In: **24th Brazilian Symposium on Computer Networks (SBRC)**, Curitiba-PR, Brazil. 2006. Disponível em: https://www.ime.usp.br/~kon/papers/sbrc06-ieee-adapt.pdf. Acesso em: 5. mar. 2022.

CROW B. et al. **IEEE 802.11 wireless local area networks**. 1997. Artigo Científico. In IEEE Communications Magazine, vol. 35, n9, pag. 116-126.

DUARTE, L. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. 2003. Monografia. Universidade Estadual Paulista Júlio de Mesquita Filho, São José do Rio Preto.

RUFINO, N.M.O. **Segurança em Redes sem Fio: Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**. 4. ed. São Paulo, Novatec, 2019.

VERISSIMO, F. **Segurança em Redes sem Fio**. Rio de Janeiro, V 1.0.1, Janeiro. 2002.

INTEL. **Visão geral e os tipos de EAP do 802.1**. 2018. Disponível em: . Acesso em: 20 set. 2018.

PAIM, Rodrigo R. WEP, WPA e EAP. 2011. Disponível em: Acesso em: 15 setembro 2018. RIGNEY, J. **RFC 2865 – Remote Authentication Dial In User Service (RADIUS)**. Disponível em < https://tools.ietf.org/html/rfc2865> Acesso em: 10 set. 2018.