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

Giovane de Morais
giovane.dmorais@gmail.com
UNASP

Resumo:O presente trabalho destina-se a realizar um estudo de caso sobre o processo de autenticação centralizada RADIUS de usuários de rede sem fio descrevendo quais são as vantagens deste tipo de implementação. Utilizando-se de protocolos adjacentes como o IEEE 802.1x e serviços de diretórios LDAP a solução RADIUS provê um controle rígido de acesso à rede sem fio realizando qualidade de serviço e garantindo segurança da informação de seus usuários. Este artigo tem como foco mostrar, através de um estudo de caso, indicar os problemas e tratar do aprimoramento necessário para que as redes sem fio possam garantir bons níveis de segurança aos seus usuários.

Palavras Chave: Autenticação - Informação - Protocolo - Redes - Segurança

1. INTRODUÇÃO

Atualmente, com o crescimento exponencial das redes de computadores e a grande produção de dispositivos móveis como *tablets* e *smatphones*, aumenta a necessidade de manter estes aparelhos conectados com segurança à Internet. Com isso, a necessidade de sistemas wireless seguros também se expande com rapidez.

Para garantir que usuários possam ter acesso aos serviços *Wi-fi* com qualidade, segurança e que o serviço possa ser de fácil implementação e manutenção por parte daqueles que provem o serviço, chegou-se ao consenso de que uma autenticação de usuários centralizada e homogênea seria a melhor solução para a resolução deste problema. O *Remote Authentication Dial In User Service* (RADIUS) é a solução mais viável para solucionarmos problemas de autenticação e prover segurança da informação a usuários de uma rede *Wi-fi*.

O objetivo deste trabalho é, através de uma metodologia de pesquisa teórico-descritiva e um estudo de caso de um experimento de virtualização, analisar se o protocolo RADIUS, juntamente com o a metodologia de transmissão wireless IEEE 802.1x (IEEE 2001), utilizando o serviço de diretórios LDAP como base de dados é capaz de realizar processo de autenticação de um usuário de uma rede sem fio garantindo estabilidade e segurança neste processo.

2. PROTOCOLO IEEE 802.1X

O padrão 802.1x foi desenvolvido pelo IEEE (Instituto de Engenheiros Eletricistas e Eletrônicos) em junho de 2001 como uma solução de segurança, que realiza identificação e autenticação em redes cabeadas ou sem fio (*wireless*) através de um servidor de autenticação. Além disso, o protocolo provê mecanismos de autenticação para aparelhos para que possam se anexar a uma LAN (*Local Area Network*) ou WLAN (*Wireless Local Area Network*). 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.

2.1. ESTRUTURA E COMPONENTES

Qualquer dispositivo que seja necessário se conectar a rede onde este protocolo está aplicado precisa, primeiramente, fornecer informações de autenticação antes de ser permitida a sua entrada. A seguir, será mostrado como o quais são os principais componentes do IEEE 802.1x e sua forma de funcionamento.

2.2. FUNCIONAMENTO DO IEEE 802.1X

Segundo FILIPPETTI (2008) a autenticação do protocolo 802.1x começa com uma solicitação de autorização vinda do ciente da rede sem fio para o ponto de acesso (AP – *Access Point*), que autentica o cliente à um servidor de autenticação (neste caso o RADIUS) que possua compatibilidade com o EAP (Extensible Authentication Protocol). O servidor RADIUS é capaz de realizar confirmação de acesso tanto para o usuário (por senhas ou certificados) como o sistema (por endereço MAC - *Media Access Control*). O cliente sem fio só pode adentrar à rede assim que a transação esteja completa.

2.2.1. SUPLICANTE

O cliente que quer ser autenticado na rede recebe o nome de “suplicante”.

2.2.2. AUTENTICADOR

Os dispositivos físicos que realizam o processo de recebimento do pedido até a autenticação propriamente dita, são chamados de “autenticadores”, os autenticadores são responsáveis pelo controle de acesso dos usuários.

2.2.3. SERVIDOR DE AUTENTICAÇÃO

O servidor de autenticação é aquele que realiza a identificação e autenticação, ou não, do usuário para a rede que está recebendo a requisição. Um exemplo seria um servidor RADIUS. A figura 1 mostra como é a estrutura de uma rede com autenticação cliente-servidor.

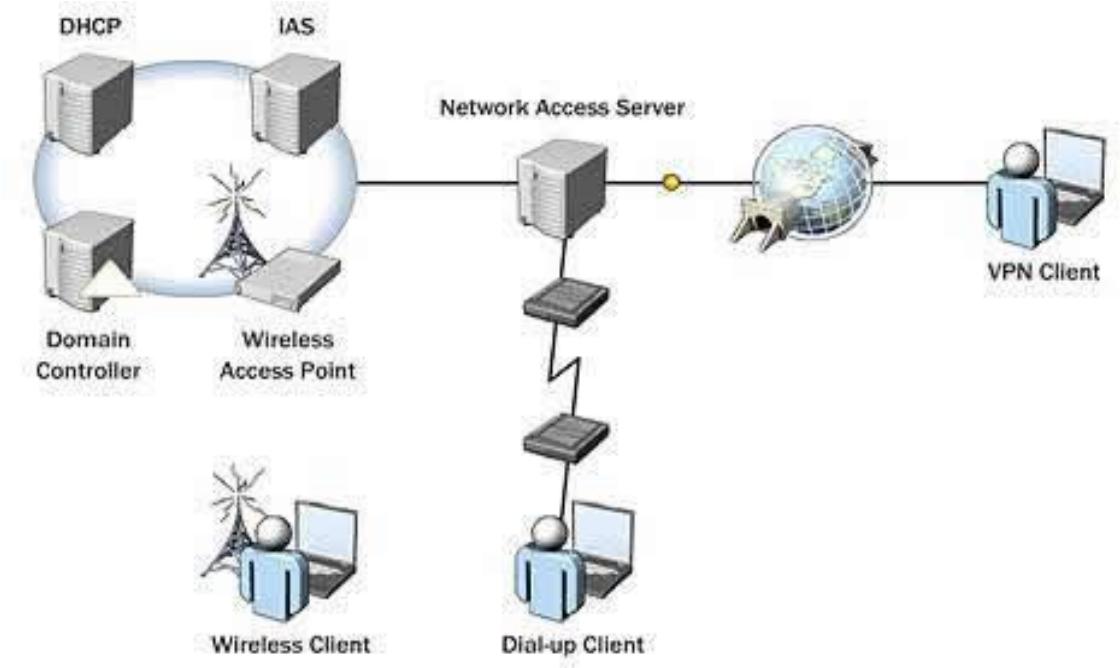

Figura 1: Tipos de Cliente em Uma Rede.

3. PRINCIPAIS METODOLOGIAS DE AUTENTICAÇÃO EXTERNAS

A seguir, serão explanadas as principais metodologias de autenticação externas (ou autenticação de primeira fase) utilizadas pelo IEEE 802.1X.

3.1. PROTOCOLO DE AUTENTICAÇÃO EXTENSIVA (EAP)

O protocolo EAP (*Extensible Authentication Protocol*), foi criado pelo IETF (*Internet Engineering Task Force*), com função de transportar informações de identificação dos clientes com o objetivo de ajudar a manter os intrusos afastados, evitando que os mesmos acessem determinadas redes e conexões.

O EAP é o mecanismo na internet que garante a segurança da rede. Ele assegura que os dispositivos se conectem a determinadas redes de forma legal e autentica, através da expedição de senhas de segurança.

Este protocolo funciona com base na utilização de um autenticador, encarregado de estabelecer, ou não, a entrada na rede para um cliente. No caso de uma rede sem fios, é o AP que desempenha o papel de controlador de acesso.

3.1.1. EAP-TLS

O EAP-TLS, definido na RFC 2716, é um IETF padrão aberto, e é bem suportado entre os fornecedores sem fio. É considerado um dos padrões mais seguros disponíveis EAP sendo suportado por todos os fabricantes de hardware LAN sem fio e software, abrangendo também a Microsoft. Este método de autenticação possui um canal criptografado entre um cliente (TLS).

Numa situação onde ocorra a exposição da senha de um usuário a alguém mal-intencionado, não é suficiente para o mesmo invadir sistemas habilitados com EAP-TLS, pois o invasor ainda precisa ter o certificado do lado do cliente. Atualmente, este método autenticador é usado pela Microsoft, Cisco, Apple, Linux, soluções *Open Source*, entre outras.

3.1.2. EAP-TTLS

EAP-TTLS é um tipo de metodologia EAP que possui uma série de ferramentas mais desenvolvidas que o TLS. No protocolo EAP-TLS, descrito anteriormente, ocorre uma troca de pacotes (*handshake*) através de um canal seguro de autenticação que é utilizada para autenticar tanto a máquina cliente quanto o próprio servidor. Já no EAP-TTLS esta negociação de autenticação se amplia, também, para transmissão de dados. O canal seguro, que antes era usado somente no momento da negociação cliente-servidor, agora é mantido ativo por toda conversa e é usado para fazer o trânsito de pacotes entre o cliente e o servidor.

Utilizando EAP-TTLS, o cliente e o servidor se comunicam sempre utilizando os atributos-valores encriptados sempre em pares. Isso permite segurança na transmissão e uma compatibilidade com a estrutura AAA (*authentication, authorization and accounting*).

Assim sendo, o EAP-TTLS é maleável o suficiente para se adequar aos protocolos de autenticação legados e baseados em senha que é normalmente transmitida em formato de texto claro, protegendo os mesmos contra-ataques de captura de senha ou de qualquer tipo de interceptação de pacotes.

3.2. PROTOCOLO DE AUTENTICAÇÃO EXTENSÍVEL PROTEGIDO (PEAP)

O PEAP pertence à família do EAP (sendo o mais jovem dos protocolos de autenticação aqui relatados). O PEAP cria um canal criptografado entre um cliente através de uma aplicação de segurança chamada de *Transport Level Security* (TLS) apontando para um servidor RADIUS.

O protocolo usa métodos de autenticação, mas pode ter uma segurança adicional para outros protocolos que possuem autenticação EAP, através de uma criptografia TLS.

Este protocolo permite que se estabeleça nova conexão rapidamente caso a primeira conexão caia. Ou seja, se o servidor de autenticação estiver sobrecarregado e não atender a requisição rapidamente e ela cair, o PEAP reconhece esta queda e reestabelece uma nova conexão com o servidor sem a necessidade do cliente se autenticar novamente.

Outra vantagem do PEAP para usuários de redes wireless é o fato de o cliente poder se locomover fisicamente, acessar outras antenas *Wi-fi* durante o trajeto e não necessitar realizar novas requisições de autenticação para o servidor.

4. PROTOCOLOS DE AUTENTICAÇÃO INTERNA

Segundo Wrightson (2014) grande parte das redes wireless usa algum tipo de configurações de segurança. Essas configurações de segurança definem como os dispositivos vão se autenticar na rede e como será realizada a criptografia dos dados à medida que os mesmos trafegam pela rede. Caso não ocorra uma especificação correta dessas opções a rede sem fio, pode se tornar vulnerável a invasões e até inacessível aos usuários. A seguir, segue os principais protocolos de autenticação interna disponíveis no mercado atualmente.

4.1. *PASSWORD AUTHENTICATION PROTOCOL* (PAP)

O PAP é um método de autenticação interna para EAP- TTLS. O protocolo PAP utiliza-se de chaves de acesso de texto sem criptografia sendo o protocolo de autenticação menos seguro.

Deve-se ressaltar que, uma vez desabilitado no servidor, os clientes que se autenticam com o protocolo PAP não poderão mais se conectar. E se a senha expirar, o PAP não poderá realizar alteração das senhas durante o processo de autenticação.

4.2. MSCHAPV2

O protocolo MSCHAP versão dois gera um processo de autenticação mútua, usando o modelo de usuário com uma senha criptografada unidimensional iniciando com o autenticador (geralmente um servidor RADIUS) que envia a requisição ao cliente, que consiste em um identificador de sessão e uma sequência arbitrária de desafio.

O cliente, por sua vez, envia uma resposta ao servidor que contém o nome do usuário com uma sequência arbitrária de desafio de mesmo nível e uma criptografia unidirecional contendo a sequência de desafio recebida, a sequência de desafio de mesmo nível, o identificador da sessão e a senha do usuário.

O autenticador verifica a resposta do cliente e envia de volta uma reposta indicando sucesso ou falha da tentativa de vinculação com o servidor juntamente com um retorno autenticado com base na sequência de desafio enviada, a sequência de desafio de mesmo nível, a resposta criptografada do cliente e a senha do usuário.

O cliente verifica a resposta de autenticação e, se estiver correta, ele entra na conexão. Se a resposta de autenticação não estiver correta, o cliente fechará a conexão.

5. PADRÃO IEEE 802.11 PARA REDES SEM FIO

Goranson (2003) relata que uma rede sem fio é uma ramificação das redes locais *(LAN)* com fio. A partir dessa definição nasce o conceito de rede local sem fio *Wireless Local Área Network* (WLAN). Uma WLAN converte pacotes de dados de pulsos elétricos ou óticos dos cabos ou fibras óticas em ondas de rádio ou de pulsos infravermelhos e os manda para outros dispositivos que possuam receptores de rede sem fio ou para um ponto de acesso (*AP*) que serve como uma conexão para uma LAN com fio.

5.1. HISTÓRICO

O IEEE definiu, em 1990, um padrão que para o funcionamento a tecnologia wireless. Esse padrão ficou conhecido como IEEE 802.11 (IEEE,1990). Porém, apenas em 1997 este padrão pode ser usado em larga escala pois, até então, os dispositivos sem fios eram escassos e ineficientes.

5.2. FUNCIONAMENTO

O padrão IEEE 802.11 abrange os níveis *físico* e de *enlace*. No nível físico são tratadas as formas de transmissões, 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 métodos de transmissão, e outros aspectos de transferência de dados sem fio, permitindo que várias WLAN's consigam comunicar entre si.

5.3. MÉTODOS DE AUTENTICAÇÃO PARA REDES SEM FIO

O protocolo 802.11 possui dois métodos de autenticação de rede: o sistema aberto e o sistema chave compartilhada (CISCO SYSTEMS, 2008).

Na autenticação aberta, conforme Goranson (2003), qualquer aparelho de acesso à rede sem fio pode solicitar autenticação para o servidor. O cliente envia uma solicitação de gerenciamento 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.

Já na autenticação de chave compartilhada, como descreve 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 passar 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 ou WPA2-Personal.

5.3.1. *WIRED EQUIVALENT PRIVACY* (WEP)

O protocolo WEP criptografa seus dados para impedir o recebimento não autorizado em alguma conexão sem fio. A WEP usa criptografia com chaves de 64 ou 128 bits antes de manda-los a 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 bate com a dele. Caso sim, é liberado acesso ao cliente à rede.

5.3.2. WPA-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. Mesmo com tantas melhorias, o WPA-Personal é passível de ataques tipo *brute force* (força bruta).

5.3.3. WPA2-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.

6. ARQUITETURA AAA (*AUTHENTICATION, AUTHORIZATION, ACCOUNTING*)

Conforme Congdon et al. (2003*)* *authentication* (autenticação), *authorization* (autorização) e *accounting* (contabilidade) são os três passos no processo de autenticação de um cliente à rede.

6.1. AUTENTICAÇÃO

Autenticação é um processo para identificar se a identidade alegada é autentica, por meio de comparação das credenciais apresentadas pelo cliente com outras já pré-definidas.

6.2. AUTORIZAÇÃO

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 usuário do grupo em que o mesmo pertencer.

6.3. *ACCOUNTING* (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.

7. *REMOTE AUTHENTICATION DIAL IN USER SERVER*

Segundo Aboba (2003) o *Remote Authentication Dial In User Service* (RADIUS) é um protocolo que providencia uma forma centralizada de gerência de usuários numa rede através do conceito de AAA (autenticação, autorização e contabilização). Ele é capaz de realizar uma triagem dos dispositivos que requerem acesso à rede utilizando padrões predefinidos pelo administrador de redes.

7.1. HISTÓRICO

O RADIUS foi instituído pela Livingston Enterprises, Inc. no início da década de 90. Sua função era permitir acesso dos usuários 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 usuários à internet ou intranet (rede local), também podendo ser integrado a serviços de e-mail.

7.2. FUNCIONAMENTO

De acordo com 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. Abaixo, na figura 2, é explanado melhor como é a infraestrutura de uma rede com um servidor RADIUS.

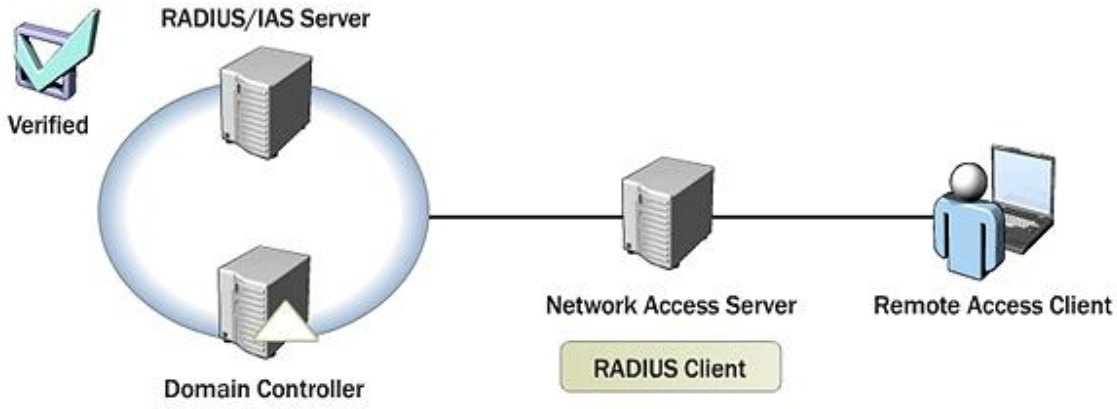

Figura 2: Autenticação de Um Cliente Pelo Servidor RADIUS.

O usuário ou aparelho envia um pedido para poder ter acesso a um recurso de uma determinada rede protegida a um *Network Access Server* (NAS. Para isso ele utiliza suas credenciais de acesso que, por sua vez, são passadas ao dispositivo NAS.

Esta solicitação leva consigo as credenciais de acesso, que geralmente estão sob a forma de *login* e senha ou um certificado de segurança ambos fornecidos pelo usuário. Estas credenciais serão comparadas em uma base de dados que, no caso do nosso experimento é um servidor LDAP. Após isso, o servidor RADIUS devolve uma das três respostas a seguir para o NAS:

Access Reject- É negado totalmente o acesso à rede solicitada.

Access Challenge – Devem-se adicionar mais informações do usuário para que seja liberado o acesso.

Acess Accept - O usuário tem acesso.

Este processo de autenticação ocorre todas as vezes que um usuário retorna à rede ou após um período que o administrador de redes define para que a autenticação seja refeita (*time out*).

7.3. SOFTWARE FREERADIUS

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 (SLAVIN, 2003).

8. CONCEITOS DE VIRTUALIZAÇÃO DE SERVIDORES E *PROXY*

Segundo Sardinha (2009) uma parte importante deste estudo é o conhecimento a respeito do conceito de virtualização de servidores e a utilização de servidores *proxys* já que o RADIUS ao realizar o processo de autenticação se comporta como um.

8.1. VIRTUALIZAÇÃO DE SERVIDORES

A ideia da virtualização surgiu na década de 1960, tomando força na década seguinte. Seu conceito se tratava em desenvolver soluções computacionais que permitissem que vários sistemas operacionais e seus respectivos softwares funcionassem em um único hardware físico. Conceitualmente seriam computadores distintos dentro de um só.

Cada máquina virtual tem um ambiente computacional amplo e completo onde todos os recursos podem ser utilizados como em uma máquina física comum. Em uma máquina virtual pode-se instalar programas, executar aplicações, ou realizar quaisquer tarefas que o sistema operacional permitir.

Com a virtualização pode-se tirar proveito de um computador já existente para executar dois ou mais sistemas distintos, desde que o hardware suporte a carga de consumo de memória e processamento de cada máquina virtual. A virtualização impede onerações com aquisição de novos equipamentos e aproveita todos recursos possíveis que estejam ociosos no computador (SARDINHA, 2009).

Neste estudo, com exceção dos equipamentos wireless, todos os demais servidores (RADIUS, LDAP e o banco de dados SQL) foram virtualizados por questão de custo-benefício.

8.2. SERVIDOR *PROXY*

Conforme Mclean (2004) o objetivo principal de um servidor *proxy* é permitir que aparelhos de uma rede privada (interna) possam ter acesso a uma rede externa, como a Internet, sem que para isto tenham uma ligação direta com esta. O termo *proxy* significa, a grosso modo, um procurador, ou seja, sistema que faz solicitações em nome de terceiros.

O *proxy* também pode armazenar informações sobre páginas de sites. Isso facilitara a procura do cliente, pois o mesmo não necessita sair à rede externa para encontrar o que procura. Este conceito é denominado de *caching*. Também é possível implementar uma funcionalidade que permita o controle do que os clientes podem acessar e em qual momento.

Nos momentos em que ocorrem a autenticação do usuário, dependendo na necessidade do administrador de redes, pode-se exigir que o requisitante acesse alguma página de *login* ou autenticação. Para preservar a segurança da rede e não permitir que um possível invasor acesse a rede, o RADIUS faz o papel de *proxy*; uma vez que ele guarda copias das páginas que o usuário as utilize ao invés de acessar as mesmas através da rede interna. Isso garante que não ocorram possíveis ataques através das páginas de *login* e/ou autenticação.

9. LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

Segundo Sungaila (2009) o protocolo de acesso aos diretórios ligeiro LDAP (Tradução livre de "*Lightweight Directory Access Protocol*") tem como modelo de referência mais atual o RFC 2251 e é utilizado em grandes empresas e corporações para gestão dos usuários de sua rede.

O protocolo permite usuários sejam organizados hierarquicamente, como uma árvore de diretórios, onde se há, primeiramente, o diretório origem (raiz), seguido pela rede da empresa, o departamento e, por fim, o computador do cliente da rede e os arquivos compartilhados por ele. A árvore de diretório é criada de acordo com a necessidade de cada administrador de rede.

A qualidade que se destaca na base de dados LDAP é a facilidade em encontrar dados e arquivos armazenados. Os usuários possuem uma conta no servidor LDAP para que tenham permissão acessar a rede e compartilhar arquivos. Além disso, o LDAP possui grande escalabilidade. Desta forma, torna-se possível a clonagem de servidores, tanto para recuperação quanto para equalização de carga, e auxiliar na adição de novos servidores de forma hierárquica, interligando-os em departamentos ou unidades distintas.

A disposição dos servidores se dá especificando um servidor raiz. A partir deste servidor é possível criar vários graus de servidores, além cópias do servidor principal. O LDAP pode ser empregado em qualquer tipo de rede TCP/IP e possui código aberto (STEWART, 2011).

9.1. AUTENTICAÇÃO DA REDE SEM FIO ATRAVES DO LDAP

O LDAP, segundo Sungaila (2009), nada mais é do que um banco de dados que armazena as credenciais dos usuários de uma determinada rede. Cada cliente (suplicante) necessita de um usuário e senha validos para adentrar a rede.

Quando um suplicante solicita entrada na rede, o ponto de acesso manda uma requisição ao servidor de autenticação centralizada (pode ser o RADIUS ou qualquer outro) este por sua vez, consulta no servidor LDAP se o usuário é valido, a senha é a correspondente e quais são as permissões daquele usuário dentro da rede.

9.2. SOFTWARE OPENLDAP

O software mais conhecido de aplicação LDAP é o OpenLDAP (GPL), cuja especificações podem ser encontradas no site oficial: http://www.openldap.org. Uma vez instalado, o OpenLDAP pode ser configurado através de linhas de comando no arquivo *sldap.conf*, localizado no diretório /etc, mas também pode ser criado e gerido através de interface gráfica.

O OpenLDAP pode ser aproveitado em conjunto com múltiplos clientes permitindo a criação de vários níveis de permissões e controle de acesso para os dados públicos. Além, disso, as informações trafegas por este software podem ter encriptação caso o administrador encontre necessidade.

10. ESTUDO DE CASO: AUTENTICAÇÃO IEEE 802.1X ATRAVES DO PROTOCOLO RADIUS E BASE DE DADOS LDAP

Para corroborar com a afirmativa que o protocolo RADIUS é uma solução eficiente e eficaz para realizar uma autenticação centralizada por IEEE 802.1X garantido segurança, estabilidade e rapidez.

Discentes do UNASP-HT criaram, em menor escala um *case* de um ambiente de autenticação de redes sem fio virtualizado utilizando o IEEE 802.1X como protocolo para conexão utilizando primeiramente EAP-TTLS e, posteriormente, o PEAP; RADIUS (utilizando o software FreeRADIUS) como protocolo de autenticação e o LDAP (utilizando o software OpenLDAP) como base de dados para este experimento.

Os equipamentos físicos utilizados nesta experimentação foram apenas uma access point da marca Ruckus ZoneFlex T710 e seu respectivo controlador. Após criar o ambiente e povoar o diretório LDAP com alguns registros de usuários para autenticação, iniciou-se o experimento.

O cliente que está com seu aparelho para realizar a conexão (suplicante), manda um pedido de conexão para o autenticador (no caso o controlador wireless) através de um método de autenticação interno. O método pode ser aberto (não possuir senha para se acessar ao controlador) ou com um sistema de chaves compartilhadas (WEP, WPA-Personal ou WPA2-Personal). Os testes principais do experimento, nesta fase, giraram em torno dos protocolos WPA-Personal ou WPA2-Personal, pois, segundo Dulaney (2011), são chaves de autenticação mais difíceis de serem "quebradas". A figura 3 retrata como é a infraestrutura física do processo de autenticação experimentado neste estudo de caso.

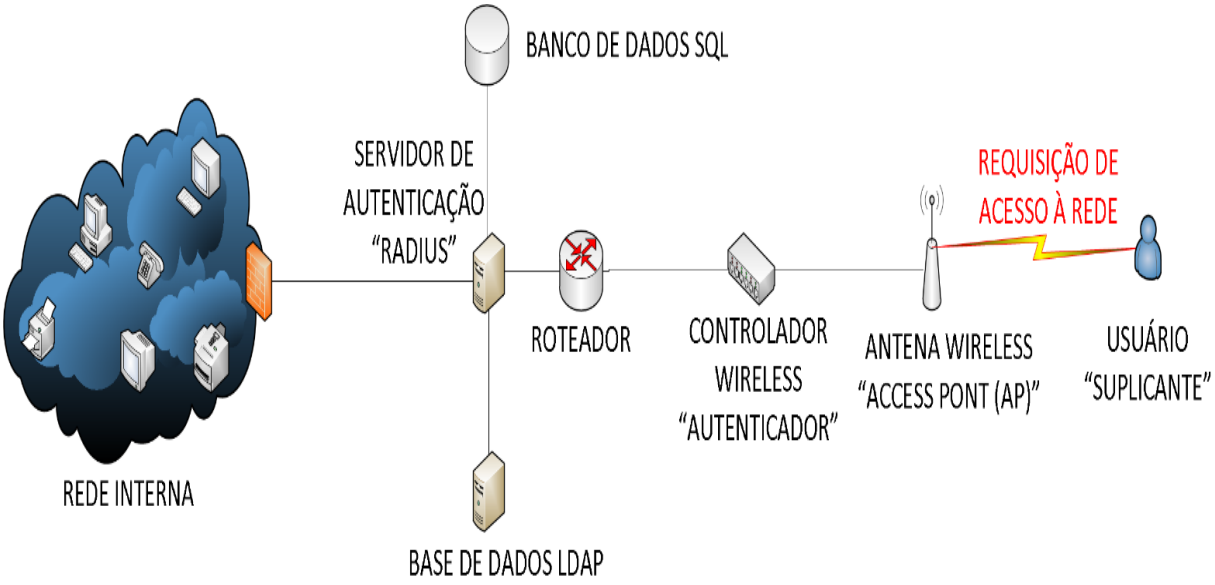

Figura 3: Infraestrutura do processo de autenticação por RADIUS.

Quando a conexão for estabelecida é criada uma conexão com o servidor de autenticação RADIUS que, neste estudo de caso foi virtualizado em uma máquina FreeBSD utilizando o software FreeRADIUS.

Para garantir a segurança dos dados que trafegam por esta conexão, é possível implementar métodos de criptografia como o PAP ou o MSCHARPV2. O RADIUS realiza o processo de autorização do suplicante para a conexão. No presente experimento, o protocolo utilizado foi o EAP-TTLS (único suportado pelo FreeRADIUS) com o uso de um certificado

digital cliente-servidor e o método de criptografia PAP pois é o que se comunica melhor com a base de dados LDAP.

Quando o servidor RADIUS recebe uma requisição do suplicante, o protocolo consulta uma base de dados segura para verificar a veracidade dos dados fornecidos pelo usuário e se o mesmo possui autorização para adentrar à rede, neste caso, um servidor LDAP que realiza o processo de autenticação. Neste estudo de caso criou-se um serviço de diretórios LDAP através do software OpenLDAP para consulta do RADIUS.

Caso a requisição seja aprovada, um registro é mandando a um banco de dados para realizar o *Accounting* (contabilização) do momento que o usuário foi autenticado. A requisição volta ao usuário e ele entra na rede. Caso o pedido seja rejeitado, também ocorre a contabilização do usuário e o motivo da rejeição. Logo depois, a conexão com o suplicante é fechada. A figura 4 esquematiza a atuação de cada protocolo e as etapas do processo AAA na autenticação de um usuário por RADIUS.

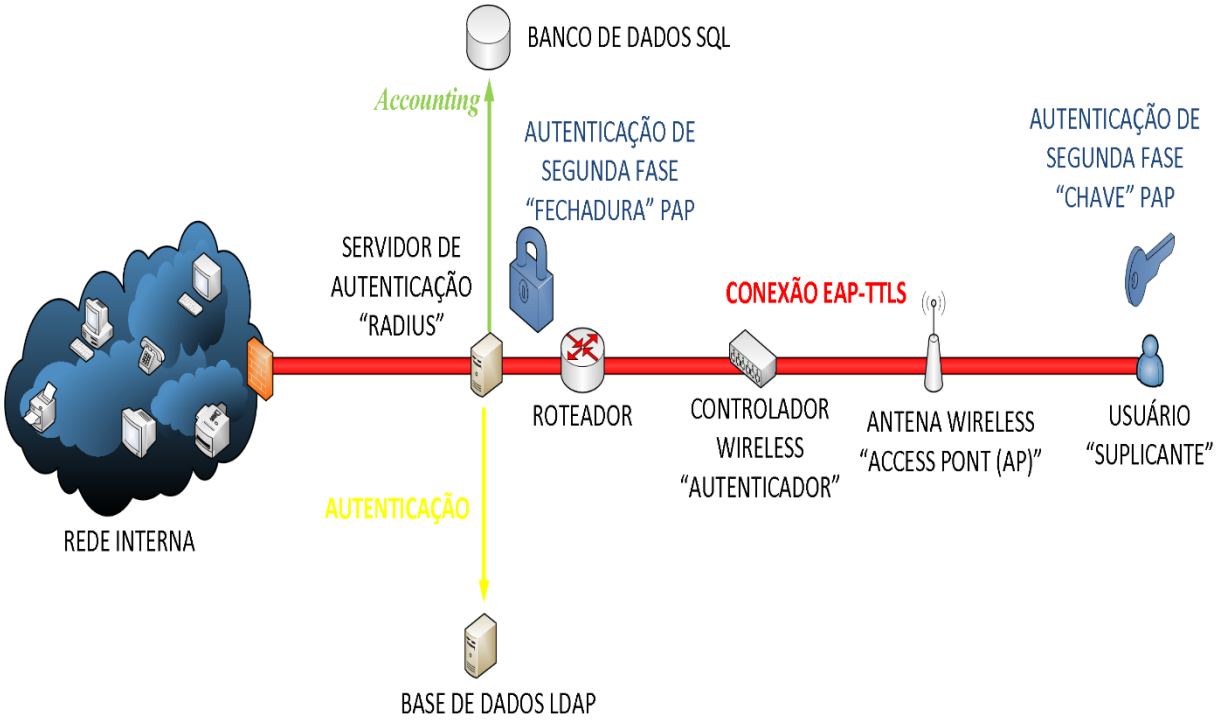

Figura 4: Protocolos utilizados no processo de autenticação por RADIUS.

11. RESULTADOS

Os resultados apresentados durante a realização deste estudo garantem é possível implantar este tipo de autenticação baseada no padrão IEEE 802.1X, utilizando RADIUS como protocolo de autenticação, e uma base de dados LDAP como local de registros.

Durante o experimento alguns entraves foram encontrados: o software FreeRadius se limita a aceitar apenas a metodologia EAP-TTLS (que é o mais seguro na atualidade). Outro problema observado no estudo de caso foi o fato de que o LDAP, devido à natureza dos dados armazenados, não consegue se comunicar com o método de autenticação de segunda fase MSCHARPV2 ficando, portanto, de uso restrito ao método PAP.

Apesar destas limitantes, se implementado da maneira correta e mantendo as plataformas RADIUS e LDAP constantemente atualizadas, é possível criar uma maneira completamente virtualizada de autenticação de um usuário em uma rede sem-fio. O método de autenticação através do protocolo IEEE 802.11 fornece grande segurança para os usuários

que se autenticam neste tipo de rede; com isso, dificilmente dados serão interceptados de forma maliciosa.

Além disso, outras vantagens podem ser observadas através do estudo destes protocolos, entre elas pode-se citar: a possibilidade de criação de redes wireless com maior facilidade podendo implementar *Virtual Local Área Network* (VLAN) dinâmica. Além de permitir com que cada usuário tenha acessos e restrições distintas na rede, aumentando a segurança. Além de realizar uma melhor utilização das faixas de IP disponíveis na rede.

12. CONSIDERAÇÕES FINAIS

Conclui-se, através do levantamento de dados combinado com o estudo de caso do presente experimento, que a hipótese que o RADIUS poderia trabalhar bem com quaisquer protocolos de segurança do IEEE 802.1X é verdadeira. O método de conexão EAP-TTLS e a autenticação de segunda fase PAP reforçam a segurança da rede e acrescentam um maior controle de acesso, garantindo o desempenho da rede e controle no acesso dos usuários.

A base de dados LDAP é simples de ser implementada graças à sua interface amigável do OpenLDAP e possui bom desempenho de leitura, porém nem tanto em escrita dos dados, além de apresentar alguns problemas de compatibilidade com os métodos de autenticação de segunda fase, porém nada que o impedisse de ser utilizado.

O RADIUS é um protocolo confiável que, segundo citações de Aboba (2003), é extremamente seguro e estável. E, por ser um padrão IETF, o mesmo pode ser implementado em diferentes ambientes e sistemas. O RADIUS também é uma boa solução quando se trata de redes sem fio uma vez que as mesmas, quando foram estabelecidas, nãos possuíam grandes políticas de segurança como sugere Filippetti (2008). O RADIUS, então, surge como uma solução que garanta a segurança dos sistemas wireless, sem que existam grandes mudanças na infraestrutura dos mesmos.

13. BIBLIOGRAFIA

ABOBA, B.; CALHOUN, P. RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP). 2003

CISCO SYSTEMS. Disponível em: <http://www.cisco.com/web/BR/index.html> .Acesso em: 18 de maio de 2016.

CONGDON, P., ABOBA, B., SMITH, A., ZORN, G., ROESE, J. IEEE 802.1X Remote Authentication Dial In User Service (RADIUS). Usage Guidelines, 2003.

DULANEY, E. CompTIA Security+: Study Guide, 5. ed., 186-187 USA: Sybex Wiley, 2011.

FILIPPETTI, M. CCNA 4.1 - Guia Completo de Estudo. Florianopolis: Visual Books, 2008.

GORANSON, P. 802.11. A Standard for the Present and Future. White Paper, 2003.

MCLEAN, J. C. Windows Server 2003 Network Infrastruture. In: Implementing, Managing, and Maintaining a Microsoft, 2004.

RIGNEY, C., WILLENS, S., RUBENS, A., SIMPSON, W. Remote Authentication Dial In User Service (RADIUS), 2000.

SARDINHA, G. Virtualização de Servidores. Voolivrelinux, 30 set. 2009. Disponível em: <http://voolivrelinux.blogspot.com/2009/09/virtualizacao-de-servidores.html>. Acesso em: 05 de outubro. 2015.

SLAVIN, W. (2003). "FreeRADIUS Server Project". : http://www.freeradius.org . Acesso em: Maio de 2015.

STEWART, J. M. CompTIA Security+: Review Guide, 2. ed., 212-213 USA: Sybex Wiley, 2011.

SUNGAILA, M. Autenticação Centralizada com OpenLDAP: Integrando Serviços de Forma Simples e Rápida. Novatec, 2009.

WRIGHTSON, T. Segurança de Redes Sem Fio: Guia do Iniciante. Bookman, 2014.