FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE

NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO – NPGE

PÓS GRADUAÇÃO MBA EM

GERÊNCIA DE REDES E SEGURANÇA DA INFORMAÇÃO IV

RODRIGO BUSTAMANTE BORGES

PROJETO DE IMPLANTAÇÃO DE REDE SEM FIO COM AUTENTICAÇÃO FREE RADIUS E ZENTYAL SERVER

Aracaju/SE

2016

RODRIGO BUSTAMANTE BORGES

PROJETO DE IMPLANTAÇÃO DE REDE SEM FIO COM AUTENTICAÇÃO

FREE RADIUS E ZENTYAL SERVER

Projeto de Pesquisa Científica apresentado à instituição de Ensino Superior, FANESE, com o intuito de adquirir titulação em Especialista em Gestão de Redes e Segurança da Informação.

Msc. Adriano Lima

Aracaju/SE

2016

PROJETO DE IMPLANTAÇÃO DE REDE SEM FIO COM AUTENTICAÇÃO FREE RADIUS E ZENTYAL SERVER

Rodrigo Bustamante Borges

Msc. Adriano Lima

RESUMO

Este artigo tem como objetivo mostrar como podemos implementar em um ambiente empresarial ou pequeno comércio, um sistema de autenticação segura através de uma rede sem fio para acesso à internet. Para propor a solução utilizaremos um laboratório virtual para esta análise, onde configuramos um servidor com software livre, neste caso utilizamos o Zentyal Server 3.0, e nele adicionamos o pacote para autenticação de usuários o RADIUS, para que através deste, os clientes/usuários solicitem e autentiquem o acesso à rede, via pontos de acesso (AP), de maneira prática e segura. Como resultado do implemento deste cenário, conseguimos melhor controle e segurança no acesso de usuários a redes sem fio no local.

PALAVRAS CHAVE:

Redes sem Fio, Zentyal Server, FreeRADIUS

1 INTRODUÇÃO

Este artigo demonstra através do uso de softwares e ferramentas de uso livre, como uma organização pode implementar melhorias na gestão dos acessos a suas redes sem fio, e que são disponibilizadas comumente em seus ambientes para seus clientes e/ou colaboradores.

Muito se fala no uso de softwares livres, e não é para menos, geralmente as licenças de softwares proprietários são caras, e a questão financeira para pequenas e médias empresas é um fator de crucial. Com o uso de equipamentos mais baratos, sem que possuam uma configuração mais atualizada (hardware) e atual, podemos implementar todo o gerenciamento com o uso do Linux mais especificamente a distribuição chamada de Zentyal 3.0, que é um software de fácil operação e implementação.

A proposta é que através do uso de políticas de autenticação e segurança (RADIUS) para acesso a estas redes, as empresas possam minimizar os impactos causados por acessos indevidos e maliciosos que causem danos a estrutura lógica do seu ambiente de rede, bem como, por exemplo tenham acesso a informações sigilosas. Com o uso destas ferramentas podemos centralizar toda e qualquer informações referentes a autenticação, criar um banco estatístico que tenha dados sobre horário de pico nos acessos, o que pode ou não ser acessado, assim como planejar melhor a expansões futuras na estrutura física da empresa.

O intuito desta sugestão de implementação é oferecer uma solução barata e acessível a pequenas empresas, que queiram oferecer o serviço de internet aos seus clientes quando estiverem em suas dependências, já que o acesso a web se tornou algo indispensável.

2 DESENVOLVIMENTO

2.1 AS TRANSMISSÕES VIA RÁDIO

Com base em uma série de descobertas sobre as transmissões via rádio que datam do século passado nos anos de 1900, e que são atribuídas, por exemplo, a Nikola Tesla que descobriu as transmissões via rádio, a Guglielmo Marconi que desenvolveu o código Morse baseado em patentes de Tesla, ou até mesmo a Faraday por seus experimentos sobre indução eletromagnética, podemos dizer que estes são os primórdios da tecnologia Wireless que conhecemos hoje.

Segundo a Wikipédia, (https://pt.wikipedia.org/wiki/R%C3%A1dio_(telecomunica%C3%A7%C3%B5es, acesso em 24/02/2016) a tecnologia de transmissão de som por ondas de rádio foi desenvolvida pelo italiano Guglielmo Marconi, no fim do século XIX, mas a Suprema Corte Americana concedeu a Nikola Tesla o mérito da criação do rádio, tendo em vista que Marconi usara 19 patentes de Tesla no seu projeto.

Apesar das transmissões a rádio, como dito, terem um bom tempo desde sua descoberta, as das redes sem fio, é algo relativamente novo, pois somente com o barateamento dos dispositivos que são usados para transmissão é que a implementação desta solução se popularizou.

> Segundo Kurose (2010, p.385) Presentes no local de trabalho, em casa, em instituições educacionais, em cafés, aeroportos e esquinas, as LANs sem fio agora são uma das mais importantes tecnologias de rede de acesoo na Internet de hoje. Embora muitas tecnologias e padrões para LANs sem fio tenham desenvolvidos na década de 1990, uma classe particular de padrões surgiu claramente como vencedora: LAN sem fio IEEE 802.11, também conhecida como Wi-Fi.

Com a popularização e massificação dos dispositivos móveis, assim como a facilidade na implementação das redes sem fio (onde grande parte da infra-estrutura dispensa uso de cabeamento), as organizações o comércio, assim como o usuário doméstico, nos mostram de forma prática que as redes sem fio tornaram-se parte de nosso dia a dia como uma necessidade básica.

> Segundo NAKAMURA, Emílio Tissato (2007, p. 138) As redes sem fio devem ser consideradas seriamente, pois cada vez mais elas passam a fazer parte da vida das pessoas. As mudanças advindas da WLAN, por exemplo, são evidentes em uma empresa. Funcionários passa a ter mais flexibilidade com relação a necessidade de cabos de rede, e o mais importante, passam a usufruir da mobilidade. Para as empresas o ganho de produtividade pode ser grande pois as informações passam a estar disponíveis de uma forma mais fácil, dentro do limite da distância coberta pela tecnologia.

Segundo Starllings, Willian (2005, p. 241), existe algumas razões para usar uma LAN sem fio: mobilidade, redução no custo de instalação, rede provisória e conexão de nós geograficamente remotos.

O implemento deste tipo de rede vem motivando as organizações a utilizar deste recurso devido as suas facilidades.

> De acordo com Olifer, Natália (2008, p.185), a possibilidade de transmitir informações sem fios, libertando assim os assinantes de ficarem limitados a uma determinada localização, sempre foi uma perspectiva atraente. Uma vez que estejam disponíveis tecnologias suficientes para possibilitar que um novo serviço sem fio incorpore dois componentes de sucesso necessário – conveniência de uso e baixo custo - seu sucesso está praticamente garantido.

Apesar de todos os fatos favoráveis, uma preocupação suje diante deste cenário: a segurança da informação no acesso a estas redes sem fio seja de uso particular ou corporativo.

> De acordo com Starllings, Willian (2005, p. 241) muitas organizações têm de enfrentar o problema de decidir se devem ou não usar uma LAN sem fio, ou WLAN. Esse problema se agrava por vários motivos relacionados à WLAN, como segurança, gerenciamento de dispositivos utilizados e uma confusa matriz de padrões. Finalmente, a utilização de uma WLAN aumenta a responsabilidade da equipe de suporte sem que necessariamente ela receba treinamento ou experiência para manuseá-la.

Ainda segundo Starllings, Willian (2005, p. 241), a confiança das empresas no uso de sistemas de processamento de dados e o uso cada vez maior de redes e

recursos de comunicação para construir sistemas distribuídos têm resultado em uma forte necessidade de segurança de computador e de rede.

2.2 TIPOS DE REDES SEM FIO

Ao realizarmos uma pequena pesquisa e análise com relação aos tipos de redes sem fio existentes nos deparamos com alguns padrões que são mais populares e conhecidos, estes vários tipos são especificados pelo Institute of Electrical and Electronics Engineers (Instituto de Engenheiros Eletricistas e Eletrônicos ou IEEE), que é uma organização profissional sem fins lucrativos formada por engenheiros, cientistas, pesquisadores e outros profissionais em vários países. Este instituto é responsável em estabelecer padrões para os equipamentos e que são desenvolvidos pelos fabricantes, dentre eles podemos citar:

- IEEE 802.11a;
- IEEE 802.11b;
- IEEE 802.11g;
- IEEE 802.11n;

Geralmente estes padrões são chamados apenas por: padrão A, B, G e N. O número 802.11 faz referência às redes sem fio e a letra que o acompanha é a forma como a rede sem fio opera, em que freqüência e velocidade funcionam.

> Torres, (2010, p. 86) existem várias tecnologias para se montar uma rede sem fio, sendo o padrão IEEE802,11 o mais popular. Este padrão é também conhecido como Wi-Fi, mas é importante saber que Wi-Fi e IEEE 802.11 não são as mesmas coisas. Wi-Fi é uma marca registrada Aliança Wi-Fi, um grupo formado por diversos fabricantes. Para um equipamento ter o direito de ser chamado Wi-Fi ele tem de ter passado pelo processo de certificação deste grupo. Sendo assim, todo equipamento Wi-Fi é IEEE 802.11, mas nem todo equipamento IEEE 802.11 é Wi-Fi.

Na transmissão por redes sem fio o mais utilizado é o padrão IEEE 802.11, que utiliza transmissão por ondas de rádio freqüência. O que vai determinar justamente a taxa de transferência e o alcance, e o padrão descrito através destas nomenclaturas ex.: IEEE 802.11b, IEEE 802.11g, do ambiente e do tipo de antena usado.

Abaixo faremos um breve descritivo do funcionamento de cada um desses padrões.

2.2.1 PADRÃO IEEE 802.11a

Devido à velocidade de transmissão deste padrão e a pouca interferência incidente, o IEEE 802.11a geralmente é utilizado em empresas que necessitam de grande tráfego de dados e informações. Esse padrão Wi-Fi é para freqüência 5 GHz com capacidade teórica de 54 Mbps. O único problema encontrado nesse tipo de padrão é o seu alcance, que não costuma ser muito grande.

2.2.2 PADRÃO IEEE 802.11b

No meio doméstico este é o padrão de rede mais usado, e é uma evolução do padrão IEEE 802.11a também é encontrado em pequenas empresas. A sua principal vantagem realmente é o seu alcance, permite um alcance de 100 metros em ambiente fechado e 180 metros em uma área aberta. Trabalha usando a freqüência de 2,4 GHz, mas a sua desvantagem, é a sua velocidade, que costuma ser inferior se comparada às outras.

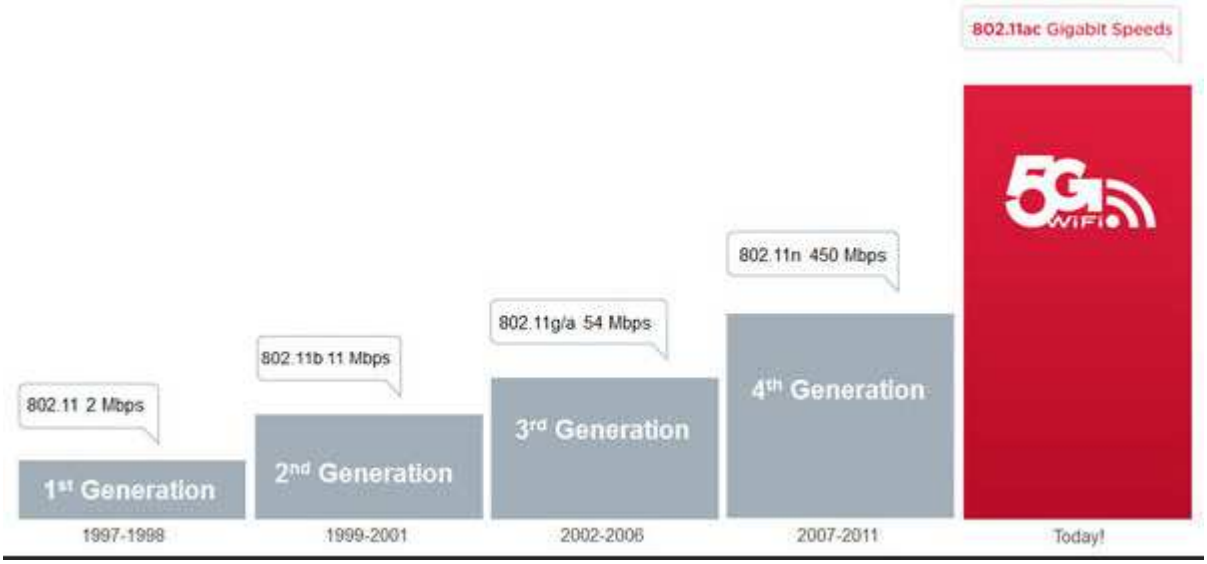
2.2.3 PADRÃO IEEE 802.11g

Muitas vezes este padrão é comparado ao padrão IEEE 802.11b, sendo que neste a questão velocidade é superior. Como o padrão “b”, é bastante utilizado em residências e empresas de porte pequeno. O padrão Wi-Fi para frequência 2,4 GHz com capacidade teórica de 54 Mbps. O ponto negativo deste padrão é que o seu alcance costuma ser menor que o padrão “b”.

2.2.4 PADRÃO IEEE 802.11n

Este é o mais recente padrão, ele mantém a compatibilidade com seus antecessores na sua transmissão funciona na freqüência de 2,4 GHz e/ou 5 GHz, com capacidade teórica de 65 à 600 Mbps. Elas também suportam velocidades superiores a 100 Mbps e têm um alcance muito superior aos padrões anteriores.

Atualmente tem se falado em um novo padrão chamado de IEEE 802.11ac que não iremos nos aprofundar, mas a título de análise visual de como acorreu a evolução das redes sem fio segue abaixo figura que demonstra este evolutivo.



Fonte: http://lifehacker.com/5988340/what-is-80211ac-and-will-it-make-my-wi-fi-faster

2.3 SEGURANÇA PARA REDES SEM FIO, MÉTODO WEP E WPA2 DE AUTENTICAÇÃO

Uma das maiores preocupações ao se implementar uma rede sem fio corporativa, que esteja disponível desde seus funcionários e/ou seus clientes, é com a segurança. Devido à facilidade de acesso aos meios sem fio cabe a empresa tentar proteger ao máximo as suas informações, para que não tenha estas acessadas por hackers.

> Segundo CARRANO, Ricardo Campana e PASSOS, Diego (2016, p. 92) Quando a conexão entre computadores em um rede é feita através de cabos, a sua invasão só é possível através do acesso direto a infra-estrutura cabeada. Por se tratar de um meio de transmissão guiado, o cabo provê o beneficio adicional de isolar a comunicação de agentes externos. Em redes sem fio, no entanto, como o sinal se propaga de maneira não guiada, não existe segurança física provida pelo cabeamento. Com isso, um atacante

> pode facilmente interferir na comunicação, tornando o problema da segurança mais importante e complicado.

Foi diante destes fatores que foram criados alguns protocolos que buscam suprir estas brechas na segurança das redes sem fio, podemos citar o protocolo WEP (Wired Equivalent Privacy ou “Privacidade Equivalente à de Redes com Fios”) e o protocolo e o WPA (Wi-Fi Protected Access ou Acesso sem fio protegido).

Em 1997 o WEP foi lançado diante da preocupação com a segurança, e veio a tornar-se, digamos, o primeiro protocolo para segurança de redes sem fio. Dentre suas funcionalidades ele usa como pré-requisito que seja configurada no ponto de acesso uma chave pré configurada no ponto de acesso (AP) e distribuída para todos os usuários como também trouxe um sistema de detecção de erros que verifica se a mensagem recebida foi corrompida ou “burlada” durante o processo de transmissão.

O padrão WEP deixou de ser seguro, com o desenvolvimento tecnológico dos computadores que foram sendo lançados e de seu alto poder de processamento, o sistema de 128 bits do protocolo WEP (no caso o máximo de combinações de senhas possíveis a serem configuradas em um AP), descobriu-se algumas vulnerabilidades e falhas que fizeram com que o WEP perdesse quase toda a sua credibilidade. O próprio algoritmo de criptografia RC4 foi apontado como o principal problema do protocolo, e mesmo sendo indicadas outras opções para substituí-lo, o WEP caiu em descrédito e deixou de ser usado em aplicações sérias.

Apesar do descrédito do protocolo WEP com o passar dos anos, o protocolo ainda é muito usado ainda hoje em instalações residenciais. Isso ocorre em parte por pura falta de informação dos usuários de redes sem fio e também pela insistência de fabricantes de pontos de acesso em permitir que esses equipamentos ainda suportem este padrão de segurança.
Em termos oficiais a Wi-Fi Alliance — associação que certifica produtos sem fio e promove a tecnologia, não considera o WEP um protocolo seguro desde o ano de 2004, quando encerrou o suporte a ele.

> CARRANO, Ricardo Campana e PASSOS, Diego (2016, p. 92) O uso de chaves pré-compartilhadas é um procedimento intrinsecamente

> inseguro. Afinal, as chaves têm de ser escolhidas pelo administrador da rede, configurada no ponto de acesso e distribuída para todos os usuários. A experiência mostra que essas chaves dificilmente são trocadas com a periodicidade recomendada. Além disso, como a chave é compartilhada, é difícil evitar que a mesma se espalhe e seja conhecida por usuários não autorizados seja porque um usuário previamente autorizado a ter a chave perdeu esse status, mas a chave não foi alterada ou porque pessoas que conhecem a chave a compartilham informalmente com outros usuários não autorizados.

O padrão WAP é considerado uma evolução do WEP, foi desenvolvido pela Aliança Wi-Fi e do IEEE para combater algumas das vulnerabilidades do WEP e aumentar o nível de segurança das redes sem fio. Lançado em 2002, esse protocolo utilizava criptografia TKIP e era chamado de WEP2 por algumas pessoas, por ele ser uma medida intermediária da Wi-Fi Aliance para substituir o WEP. Logo em 2004 ele recebeu uma atualização, quando passou a ser chamado de WPA2 e a utilizar uma criptografia mais forte chamada AES. Ele também ficou conhecido como IEEE 802.11i-2004.

Abaixo o quadro mostra um breve evolutivo dos dois padrões:

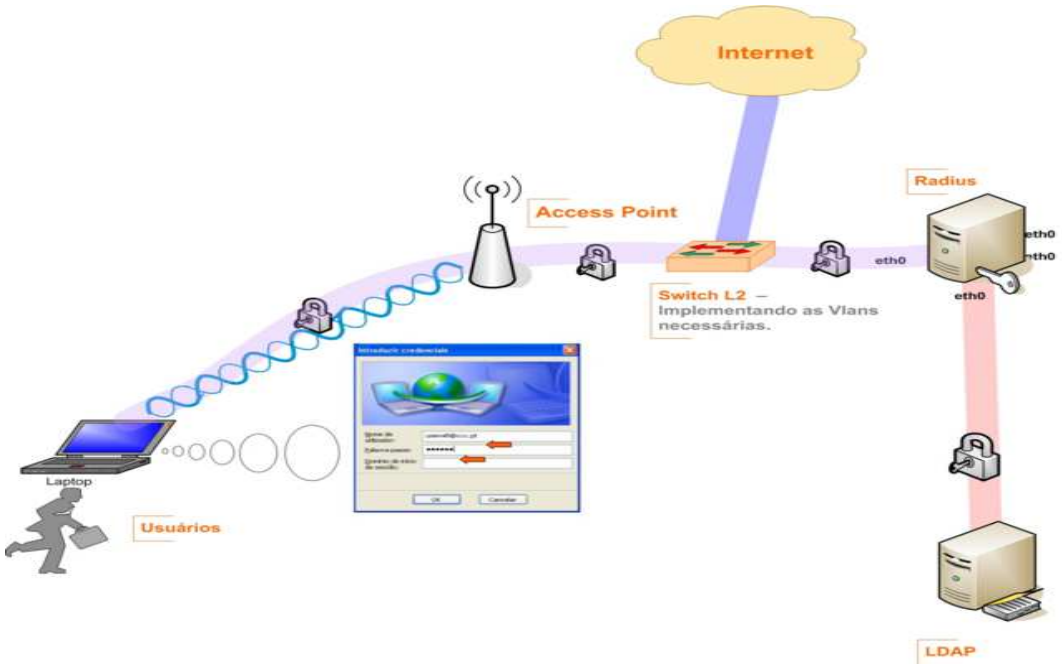
Fonte: http://pt.scribd.com/doc/206659698/Tecnologias-de-Redes-sem-Fio

Ainda que o WAP seja um protocolo melhorado em relação ao WEP ele preserva o esquema de chaves pré-compartilhadas, se formos levar em conta o quesito segurança este fato volta a ser um problema. Mas uma alternativa foi oferecida para o padrão WAP, a possibilidade de utilizarmos servidores de autenticação.

Então na tentativa de resolver essa questão temos 2 soluções para o WAP: o “WAP Personal” e o WAP Enterprise.

O WAP Personal, é conhecido como modo WPA-PSK (chave pré-compartilhada), cada dispositivo de rede Wireless autentica com o ponto de acesso utilizando a mesma chave de 256 bits gerada a partir de uma senha ou frase secreta. Esse método foi projetado o uso em redes pequenas e não requer um servidor de autenticação.

Já no WAP Enterprise, através de um ponto de acesso (AP), os usuários solicitam autenticação a um servidor que centraliza as credenciais (servidor RADIUS), e decide se deve ou não aceitar a solicitação. Neste caso os usuários possuem senhas individuais e chave de rede para a liberação de acesso. Este método de acesso também é conhecido como modo WPA-802.1x. Neste tipo de arquitetura o ponto de acesso, age como autenticador, que intermedia a conexão do usuário com o servidor assim como bloqueia todo tráfego caso a requisição não preencha os requisitos de usuário e senha. Caso o servidor de autenticação libere o acesso, o usuário tem acesso liberado aos serviços de rede (ex.: acesso a internet, compartilhamento de arquivos, impressão). Abaixo segue esquema simplificado do acesso via WAP2-Enterprise.



Fonte: https://static.vivaolinux.com.br/imagens/artigos/comunidade/diagrama-001.jpg

Abaixo temos um quadro comparativo das principais características inerentes a cada um dos métodos de autenticação citados anteriormente.

Fonte: Próprio Autor

2.4 EXPANÇÃO DE REDES SEM FIO COM A UTILIZAÇÃO DO SERVIÇO WDS EM PONTOS DE ACESSO

Não poderíamos deixar de citar a utilização do serviço para replicação de sinal de Wi-Fi chamado WDS – Wireless Distribution System (em português: Sistema de Distribuição sem Fio).

A depender do local instalado um AP (Ponto de Acesso Wi-Fi) pode não fornecer sinal de boa qualidade ou podemos ter problemas de acesso através de dispositivos móveis, devido a barreiras, tais como: paredes, espelhos e portas, ou até mesmo a necessidade de mudança e/ou ampliação física de um ambiente (residencial ou corporativo) podem comprometer a potência do sinal de rede sem fio.

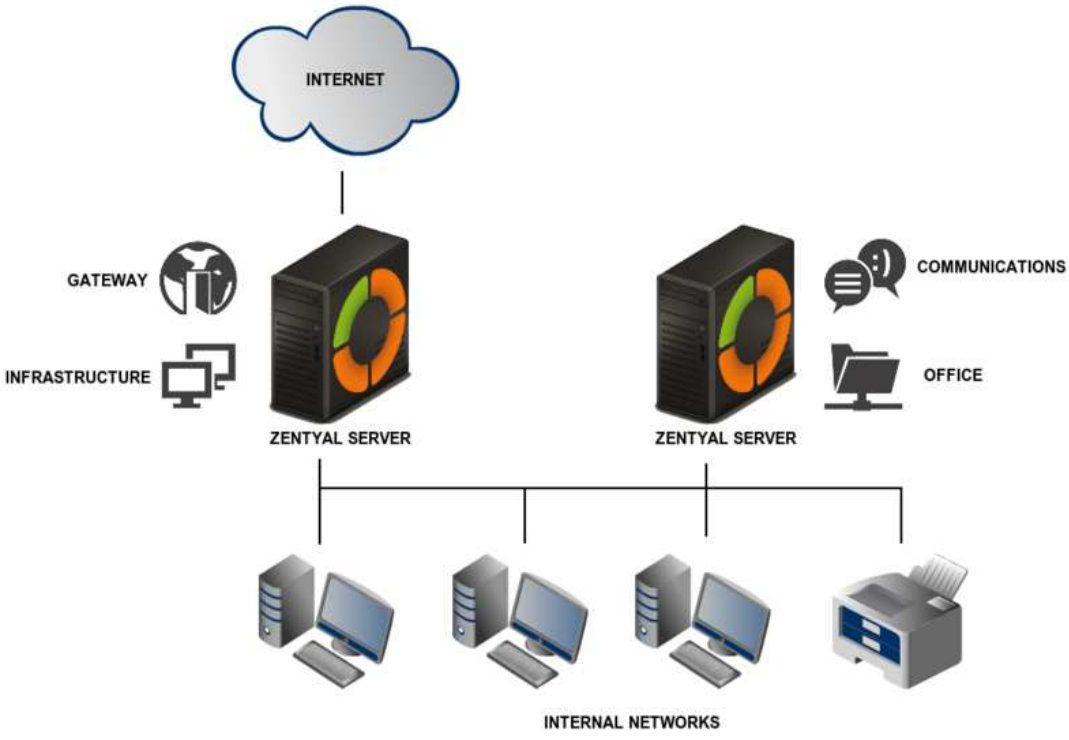
O serviço WDS está disponível na maioria dos equipamentos para rede sem fio, e serve para replicar sinal Wi-Fi, dispensando o uso de cabeamento físico para interligar roteadores ou AP´s de uma rede. Com o WDS ativo utilizamos a própria rede sem fio para expandir e/ou melhorar o sinal da Wi-Fi de um local, economizando com material e ganhando tempo. A maioria dos fabricantes recomenda que seja utilizado equipamentos da mesma marca para que possam garantir o perfeito funcionamento da função WDS. Podemos verificar abaixo a ilustração do funcionamento do serviço WDS.

Fonte: http://www.tp-link.com.br/resources/uploadfiles/file/Q3.Conex_o_WDS_v2.pdf

2.4 DISTRIBUIÇÃO LINUX ZENTYAL

O Zentyal é uma distribuição Linux concebida em 2004, e com sede em Zaragoza, Espanha e é segundo o próprio site oficial, a primeira companhia a oferecer interoperabilidade nativa com o protocolo do Exchange (Serviço e plataforma de correio eletrônico nativo do pacote Office) e com o Active Directory ambos de propriedade da Microsoft, com o Linux. O Zentyal oferece uma série de ferramentas que podem ser adicionadas em seu pacote de instalação, tais como serviço de DHCP (Protocolo de configuração dinâmica para endereços de IP em estações clientes), Serviço de Serviço de DNS (Sistema de Nomes de Domínio), Firewall, Proxy, Gerenciamento de impressoras, serviço de correio e uma série de outros recursos. Para este trabalho utilizaremos o Zentyal como servidor de autenticação de usuários via RADIUS, que é um pacote disponível em sua distribuição 3.0.

Abaixo temos uma figura que ilustra alguns de seus serviços.



Fonte: http://www.linuxdescomplicado.com.br/2013/09/zentyal-32-uma-solucao-completa-para.html

3 MATERIAL E MÉTODOS

Neste ponto demonstraremos como utilizamos os recursos disponíveis bem como fizemos as configurações dos sistemas utilizados para solução proposta.
Utilizamos uma CPU genérica com processador Intel I3, com 4 Gb de memória e 500Gb de disco rígido, e instalamos fisicamente duas placas de rede Ethernet 10/100Mbps.

Conseguimos facilmente a distribuição Zentyal 3.0 na internet através do link: http://iso.linuxquestions.org/zentyal/zentyal-3.0/, vale ressaltar que foi feita a instalação da versão mais recente do Zentyal a 4.2, mais o pacote do serviço RADIUS não era incluso para configuração. Devido a isso resolvemos utilizar a versão 3.0. Abaixo segue o passo a passo utilizado para configuração dos serviços necessários.

Para funcionamento de todo o processo, são pré-requisitos a instalação dos seguintes pacotes:

- Serviços de Rede
- Certificador de Autoridade
- Configuração de Rede
- Firewall
- Serviço de DHCP
- Serviço de DNS
- Pacote para gerenciamento de usuários e grupos
- RADIUS

Figura 1 – Pacotes selecionados para instalação no servidor.

Com o Linux Zentyal versão 3.0 instalada e com os seus pacotes, configuramos a placa de rede Eth0 com padrão “DHCP externo” conectada fisicamente ao modem ADSL que provê acesso à internet, e a segunda placa de rede, a Eth1 (192.168.100.1) foi utilizada para interligar o servidor Zentyal com o AP (ponto de acesso sem fio) com IP de rede na mesma faixa do AP (IP: 192.168.100.2).

Figura 2 – Configuração de placas de rede do servidor.

Criamos um range DHCP para IP´s da conexão RADIUS. Configuramos o range DHCP de: 192.168.100.10 até 192.168.100.100.

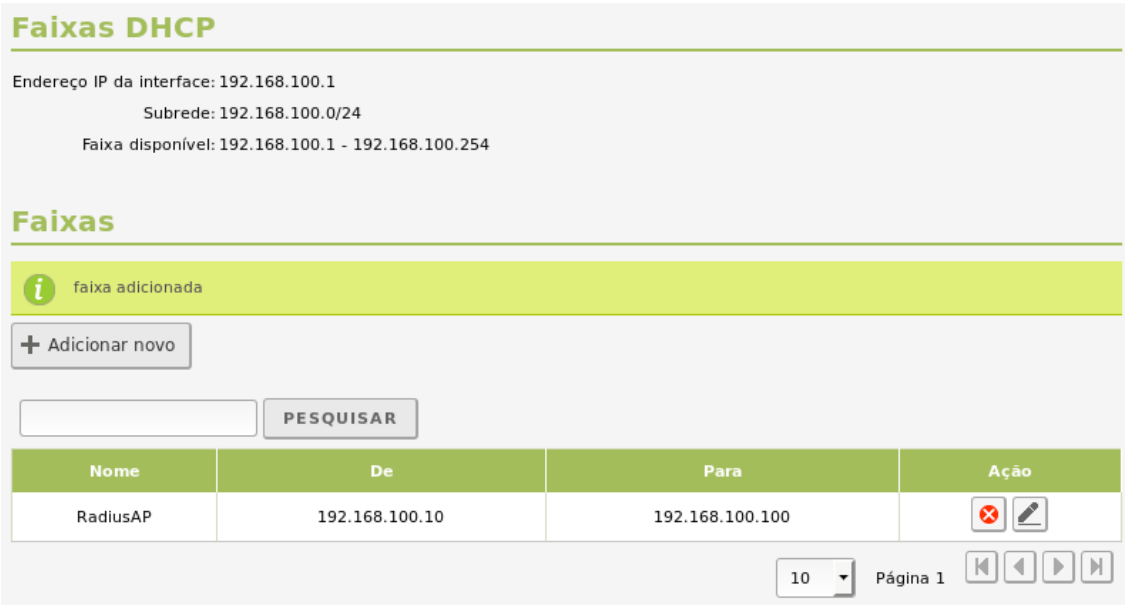


Figura 3 – Faixa de IP´s para RADIUS.

Para que as estações cliente consigam navegar através da rede RADIUS criamos um grupo DHCP para o acesso.

Figura 4 – Grupo de usuários RADIUS.

Criando usuários para autenticação via estação cliente.

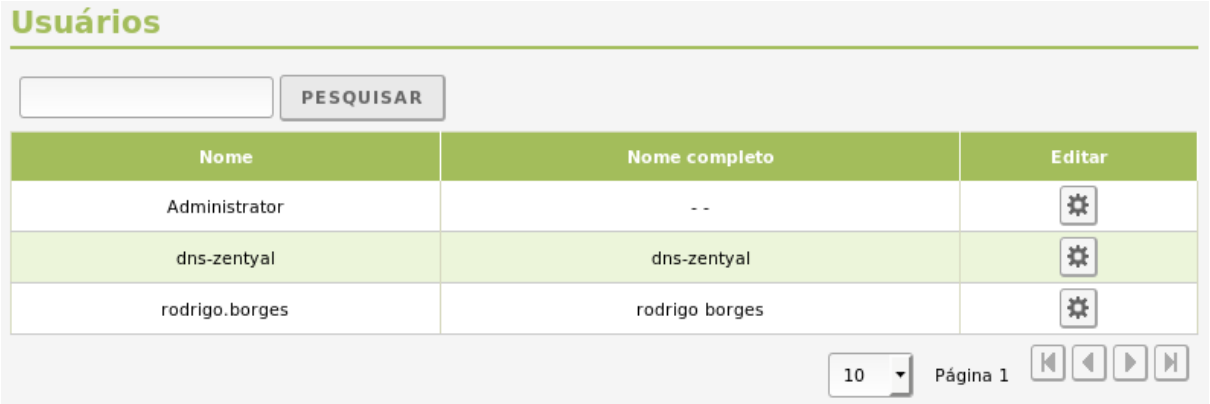


Figura 5 – Criando conta de usuário para acesso.

Configuramos o roteador TP-LINK sem fio para servir de ponto de acesso para autenticação junto ao servidor, desabilitamos o serviço DHCP do AP para fornecimento de IP´s, visto que esta será uma função atribuída ao servidor RADIUS.

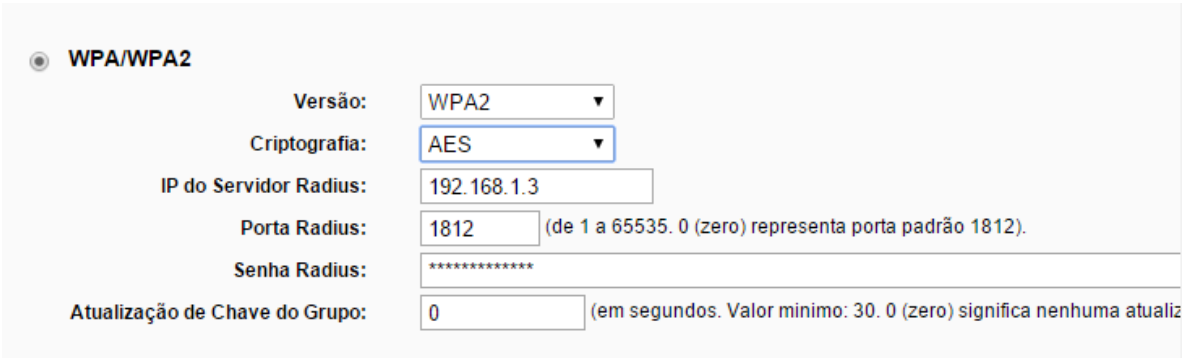


Figura 6 – Configuração do AP com Protocolo WAP-Enterprise

Como estação de acesso utilizamos um notebook CCE, Modelo win com processador Celeron de 1Gb, com 1Gb de memória e HD de 320Gb com o sistema operacional Windows 7.

Mostraremos abaixo o processo de configuração da placa de rede sem fio do notebook para autenticação no AP.

Adicionamos uma nova conexão sem fio manualmente.

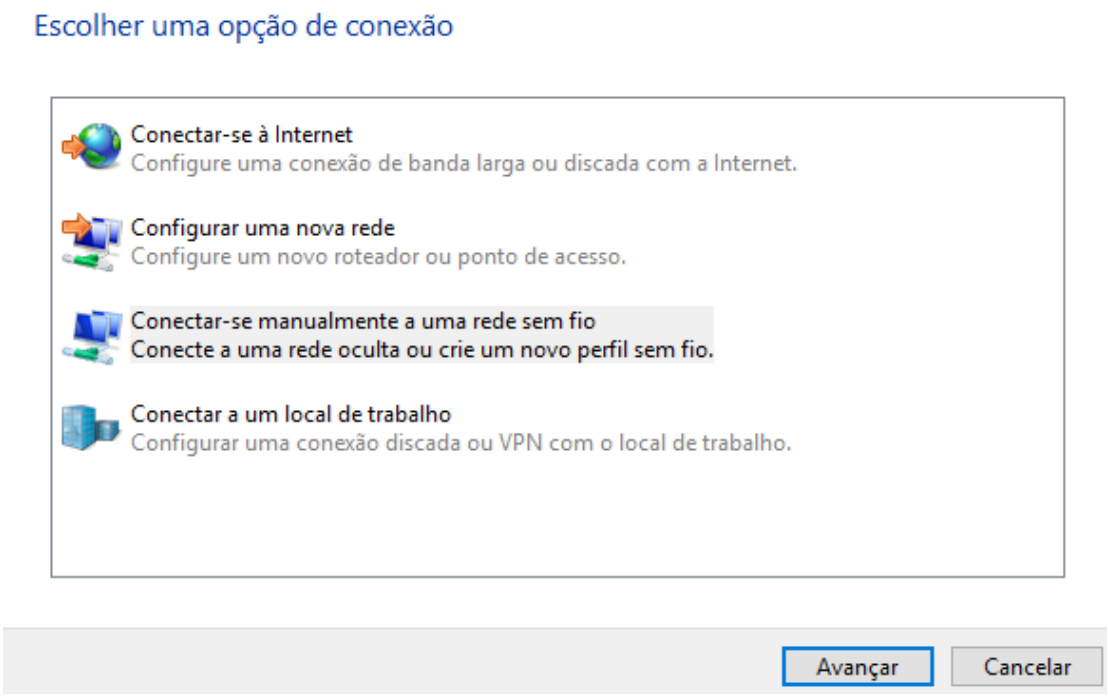


Figura 7 – Adição manual de configurações de rede para acesso ao AP

Adicionamos manualmente o nome da rede sem fio e o método de autenticação.

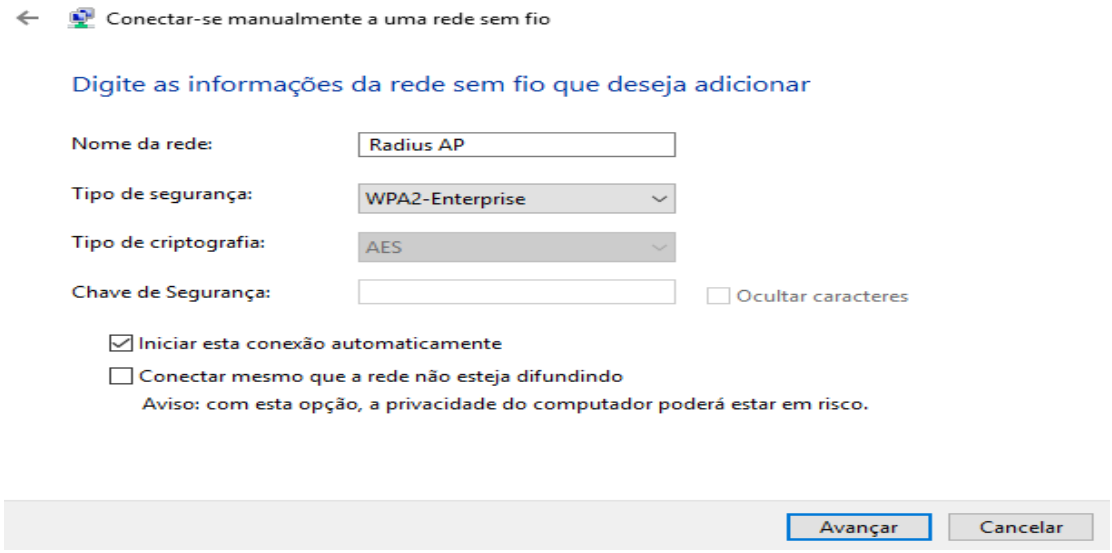


Figura 8 – Configuração do tip o de protocolo de segurança

Alteram-se as propriedades da nova conexão:

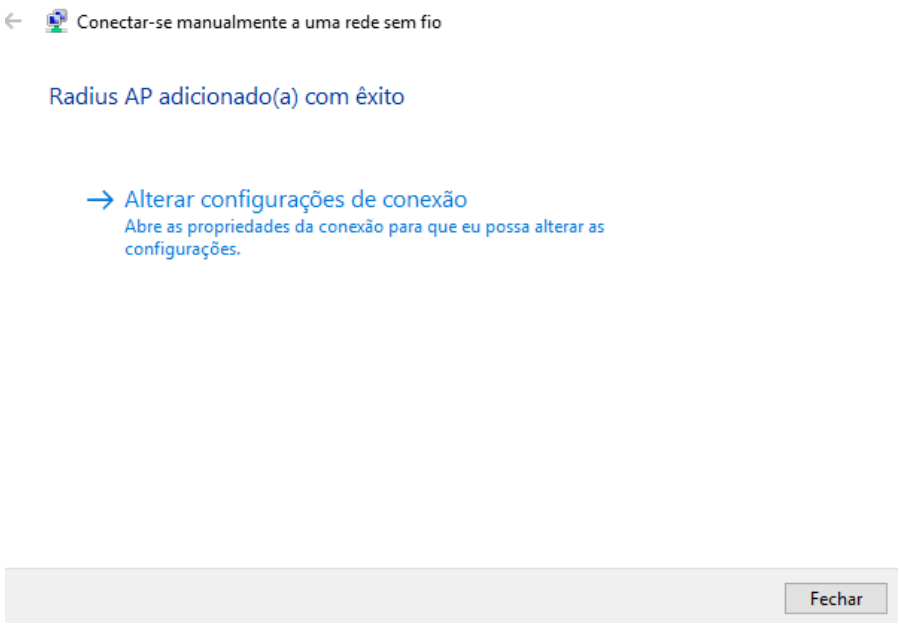


Figura 9 – Necessidade de alteração de propriedades de conexão.

Como neste trabalho não tratamos sobre certificados de autenticação, devemos desmarcar a opção em configurações das propriedades.

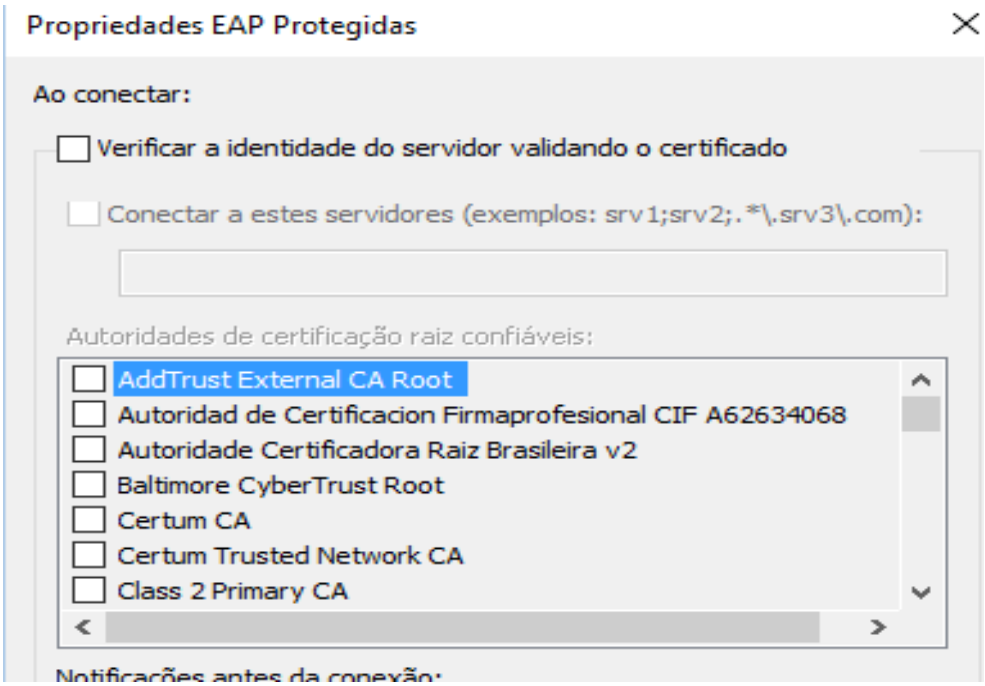


Figura 10 – Configurações das propriedades.

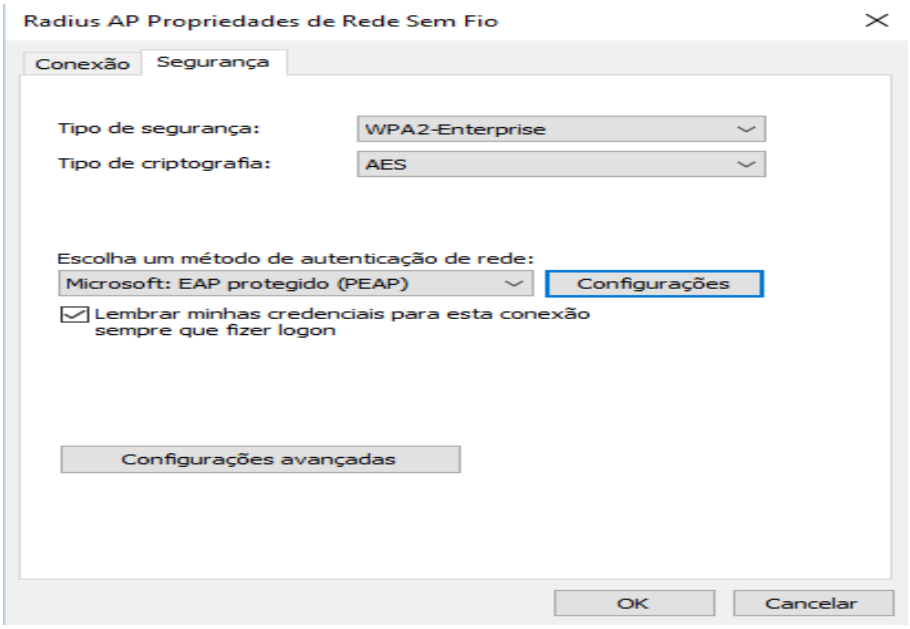


Figura 11 - Desmarcando opção de certificado digital

Em configurações avançadas deve-se marcar o modo; especificar modo de autenticação e neste momento é quando devemos colocar o usuário e senha adicionada no RADIUS do servidor Zentyal.

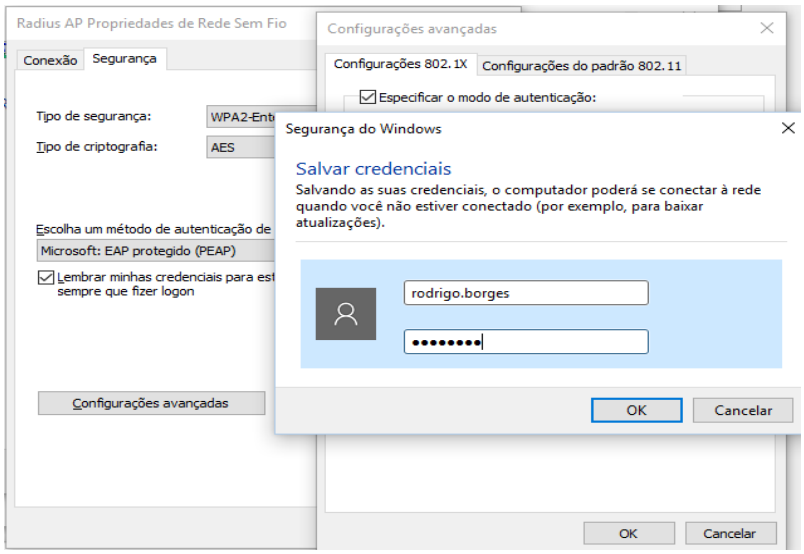


Figura 12 – Inclusão de usuário de rede

4 SITE SURVEY PARA IMPLEMENTAÇÃO DE PONTOS DE ACESSO EM ESCRITÓRIO FICTÍCIO.

Para melhor entendimento, instalação e aplicação da solução com rede Wi-Fi, com o uso de pontos de acesso, podemos utilizar softwares que simulam a instalação física dos AP´s e o quando eles serão funcionais quando instalados em um cenário real. Para isso utilizamos o software Xirrus Wi-Fi Design, e simulamos a configuração e instalação de pontos de acesso em um escritório fictício.

A planta do escritório que utilizamos para simular a instalação possui aproximadamente 1000m2 (mil metros quadrados), e utilizamos 5 pontos de acesso que trabalham com duas frequências de transmissão distintas (Freq. 2,4Ghz e 5Ghz) distribuídos pelo ambiente.

Figura 13: Planta de escritório para instalação de rede sem fio.

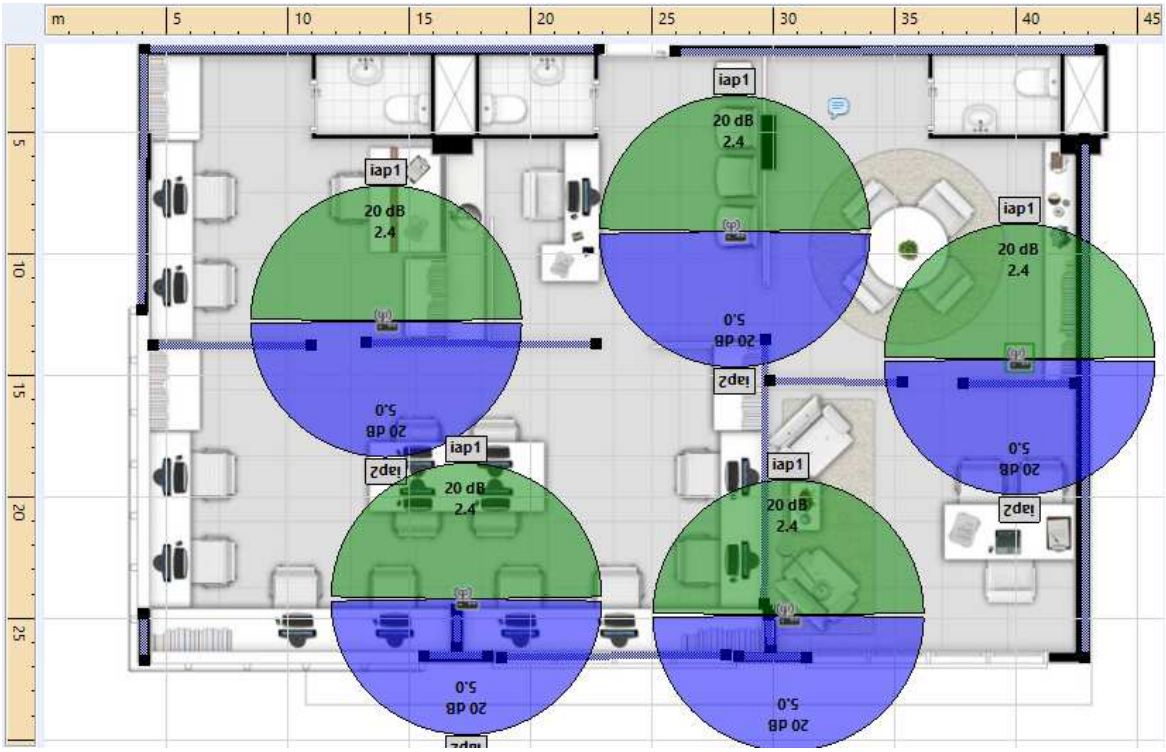


Figura 14: Visão dos AP´s e freqüências utilizadas

O próprio programa Xirrus Design nos oferece vários tipos de AP´s com diferentes funcionalidades e que podemos configurá-los individualmente, assim como nos permite inserir na planta as diferentes texturas e obstáculos, tais como: tipos de parede, divisórias, janelas de vidros o que nos proporciona ao ligarmos o “mapa de calor” (o alcance do sinal de rádio dos AP´s) a melhor posição que o equipamento deve ser instalado.

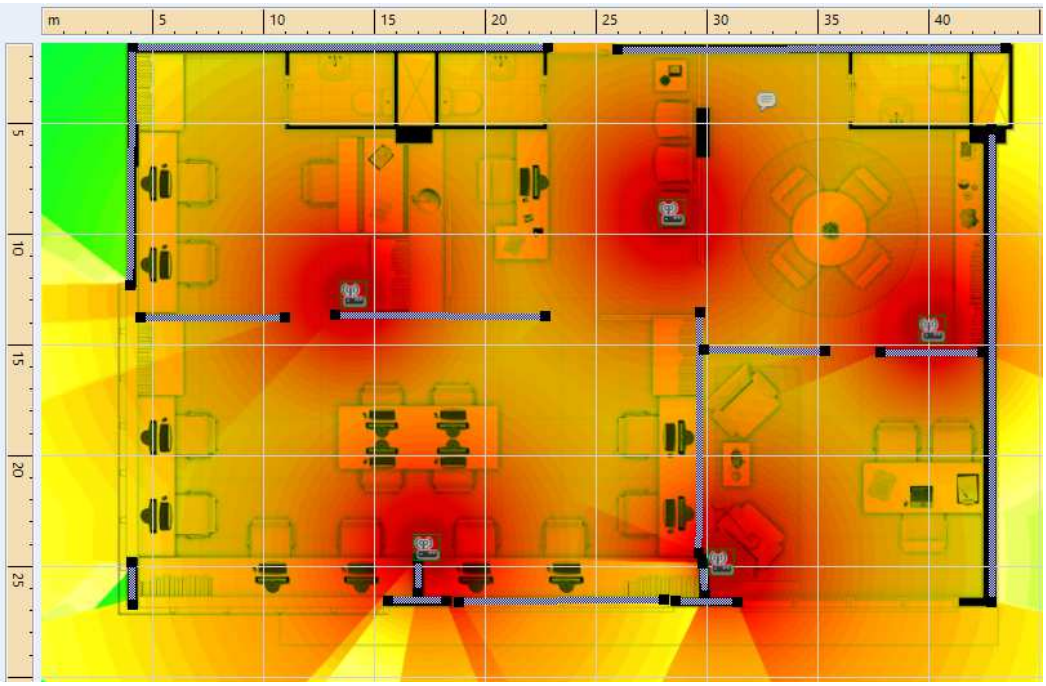


Figura 15: Mapa de calor dos pontos de acesso (Alcance o sinal Wi-Fi)

Umas das questões que devem ser levadas em consideração e que muitas vezes é ignorada, é o vazamento do sinal da rede sem fio para o ambiente externo, o que compromete a segurança da rede local, pois usuários mal intencionados podem facilmente “enxergar” a rede instalada internamente. Na figura acima podemos visualizar o vazamento do sinal pois a planta do imóvel contempla grandes janelas de vidro em sua infra-estrutura.

No projeto em questão levando em consideração os dados apresentados neste artigo, sugerimos o cronograma abaixo para execução de todos os passos, desde a análise do ambiente, até a sua entrega com o cenário em pleno funcionamento.

CRONOGRAMA DE IMPLANTAÇÃO DO PROJETO						
DIA 1	DIA 2	DIA 3	DIA 4	DIA 5	DIA 6	DIA 7
Analisar o Ambiente	Adequar Estrutura do Ambiente/Comprar material	Definir local de instalação do Servidor e dos AP's	Instalar e configurar o Servidor e os AP's	Testar equipamentos instalados	Corrigir falhas e readequar equipamentos	Validar projeto
Analisar o Ambiente	Adequar Estrutura do Ambiente/Comprar material	Reunião com Diretores	Instalar e configurar o Servidor e os AP's	Testar equipamentos instalados	Corrigir falhas e readequar equipamentos	Entrega de Projeto aos Diretores

Figura 16: Cronograma de execução e implantação do projeto.

4 CONCLUSÃO

Podemos concluir que boa parte das pequenas e médias empresas que já utilizem ou venha utilizar a solução de redes sem fio, podem se beneficiar com o implemento do cenário proposto neste artigo, visto que além de ser uma solução não requer um investimento financeiro alto com infra-estrutura e principalmente cabeamento estruturado, também não necessita de equipamentos muito sofisticados e potentes para que tudo funcione de maneira satisfatória. A solução com software livre mostra ser um implemento estável e confiável que possui uma série de pacotes que podem se que instalados e configurados facilmente através de interface gráfica. Além de possuir fóruns e canais de discussões na internet que provêem suporte para qualquer tipo de dúvida ou problema que venha a ocorrer no sistema operacional. Já o processo de autenticação para acesso à rede sem fio, apesar de apresentar um a certa complexidade para que um usuário final configure em sua estação de trabalho, pode ser suprido com um manual básico e simples de configuração. Embora este trabalho não apresente uma solução via “captive portal” (método de autenticação por browser de acesso à internet), que traria várias outras vantagens e facilidades, fica a oportunidade de aproveitar este trabalho como introdução a estas e outras melhorias.

5 ABSTRACT

This article aims to show how we can implement in a business environment or small business, a secure authentication system via a wireless network for internet access. To propose the solution we will use a virtual laboratory for this analysis, where we set up a server with free software, in this case we use the Zentyal Server 3.0, and in it added the package to user authentication RADIUS, so through this, customers / users to request and to authenticate network access via access points (AP) in a practical and safe way. As a result of the implement of this scenario, we obtain a better control and safety in the users access to wireless networks in place.

KEYWORDS:

Wireless Networks, Zentyal Server, FreeRADIUS

REFERÊNCIAS

ALECRIM, Emerson, **O que é WI-FI (IEEE 802.11)?.** Disponível em: http://www.infowester.com/wifi.php . Acesso em: 25 fev. 2016.

BRANDÃO, Patrick, **Freeradius – Servidor radius eficiente e completo.** Disponível em: https://www.vivaolinux.com.br/artigo/Freeradius-servidor-radius-eficiente-e-completo . Acesso em: 04 mar. 2016.

BRITO, Edivaldo, **Qual a Diferença entre os Padrões B, G e N?.** Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/10/qual-diferenca-entre-os-padroes-de-rede-wireless-b-g-e-n.html . Acesso em: 05 mar. 2016.

CABIANCA, Luis Antonio, **Redes LAN/MAN Wireless III: Site Survey.** Disponível em: http://www.teleco.com.br/tutoriais/tutorialrwlanman3/pagina_2.asp. Acesso em: 06 mai. 2016.

CARRANO, Ricardo Campana e PASSOS, Diego **Tecnologia de Redes Sem Fio** Rio de Janeiro: Ed. Rede Nacional de Ensino e Pesquisa – Escola Superior de Redes, 2016

DUQUE, Luciano Henrique, **Banda Larga: Extração de Parâmetros de Qualidade do Serviço a Partir do CDR (Call Detail Record).** Disponível em: http://www.teleco.com.br/tutoriais/tutorialblcdr/pagina_2.asp Acesso em: 27 fev. 2016.

FERREIRA, Fernando Nicolau Freitas e ARAÚJO, Márcio Tadeu de, **Política de Segurança da Informação – Guia Prático para Elaboração e Implementação.** 2. Ed. Revisada. Rio de Janeiro: Editora Ciência Moderna LTDA, 2008

FERREIRA, Ricardo, **Zentyal 3.2 – Uma Solução Completa para Administrar sua Rede.** Disponível em: http://www.linuxdescomplicado.com.br/2013/09/zentyal-32-uma-solucao-completa-para.html. Acesso em: 05 mar. 2016.

FLORENZANO, Cláudio, **40 Livros Gratuitos da Área de TI da Escola Superior de Redes.** Disponível em: http://www.cbsi.net.br/2015/05/40-livros-gratuitos-da-area-de-ti-da-RNP.html . Acesso em: 05 mar. 2016.

HENRY, Alan, **What is 802.11ac and Will It Make My WiFi Faster?.** Disponível em: http://lifehacker.com/5988340/what-is-80211ac-and-will-it-make-my-wi-fi-faster. Acesso em: 05 mar. 2016.

HRUSKA, Thomas, **Using a Radius Server on Ubuntu 14.04 For Wifi Authentication,** Disponível em: http://www.ossramblings.com/using-freeradius-ubuntu-server-wifi Acesso em: 02 mar. 2016.

JÚNIOR, Marcos Antonio Costa Corrêa, **Evolução da Segurança Em Redes Sem Fio.** Disponível em: http://www.cin.ufpe.br/~tg/2008-1/maccj.pdf. Acesso em 05 mai. 2016.

KUROSE, James F. e ROSS Keith W, **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. 5 Ed. São Paulo: Editora Addison Wesley, 2010

LINHARES, André Guedes e GONÇALVES, Paulo André da Silva, **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w.** Disponível em: http://www.cin.ufpe.br/~pasg/gpublications/LiGo06.pdf . Acesso em: 23 fev. 2016.

LUIZ, Marcelo, **A História da Rede sem Fio.** Disponível em: http://www.lifestyles.com.br/index.htm/2013/02/a-historia-da-rede-sem-fio/ . Acesso em: 25 fev. 2016.

MAGUETAS, David Lucas e GUARDIA, Hélio Crestana, **Implementando Segurança Através da Autenticação RADIUS em um Cenário Corporativo.** Disponível em: http://revistatis.dc.ufscar.br/index.php/revista/article/view/48 . Acesso em: 04 mar. 2016.

MENESES, Emerson Barros de, **Rede Wireless: Uma Solução Sem Fios.** Disponível em: http://semanaacademica.org.br/system/files/artigos/redewireless.pdf Acesso em: 27 fev. 2016.

MIRALDO, Alexandre, O **que é Site survey para Rede Wireless.** Disponível em: https://www.sodalitait.com.br/SITE%20SURVEY.PDF. Acesso em: 06 mai. 2016.

MUCHACUAR, Jorge, **Protocolos de Segurança em Redes Wireless.** Disponível em: http://globotecnologias.com/protocolos-de-seguranca-em-redes-wireless/ . Acesso em: 22 fev. 2016.

NAKAMURA, Emílio Tissato e GEUS, Paulo Lício de, **Segurança de Redes em Ambientes Cooperativos.** 1 Ed. São Paulo: Novatec Editora, 2007

OLIFER, Victor e Natalia Olifer, **Redes de Computadores: Princípios, Tecnologias e Protocolos para o Projeto de Redes.** 1 Ed. Rio de Janeiro: Editora LTC, 2008

PASSOS, Diego e CARRANO, Ricardo Campanha, **Tecnologias de Redes sem Fio.** Disponível em: http://pt.scribd.com/doc/206659698/Tecnologias-de-Redes-sem-Fio . Acesso em: 05 mar. 2016.

PINHEIRO, José Maurício Santos, Site **Survey, O Segredo de um bom Projeto**. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_site_survey.php . Acesso em: 06 mai. 2016.

PINTO, Pedro, **Aprenda a Instalar e Configurar o FreeRadius (Parte II).** Disponível em: http://pplware.sapo.pt/linux/aprenda-a-instalar-e-configurar-o-freeradius-parte-ii/ . Acesso em: 04 mar. 2016.

PINTO, Pedro, **dalo Radius: Um Servidor de Autenticação pronto a Funcionar.** Disponível em: http://pplware.sapo.pt/linux/dalo-radius-um-servidor-de-autenticao-pronto-a-funcionar/ . Acesso em: 02 mar. 2016.

PEREIRA, Hélio Brilhante, **Segurança em Redes Wireless 802.11 Infraestruturadas.** Disponível em: http://repositorio.ufla.br/bitstream/1/9644/1/ARTIGO_Seguranca_em_redes_wireless_802.11_infraestruturadas.pdf . Acesso em: 23 fev. 2016.

PEREIRA, Marcelo Veiga, **Implementando segurança no Nível de Acesso Utilizando Servidor Radius.** Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/419/1/CT_GESER_1_2011_17.pdf . Acesso em: 04 mar. 2016.

RAMIRÉZ, José Manuel, **FreeRadius: WiFi Más Seguro.** Disponível em: http://www.masqueteclas.com/tutorial/wifi-mas-seguro-con-freeradius/ . Acesso em: 05 mar. 2016.

RODRIGUES, Carlos, **Radius,** Disponível em: http://www.projetoderedes.com.br/artigos/artigo_radius.php Acesso em: 27 fev. 2016.

SANTOS, Luis Antonio, Redes **LAN/MAN Wireless III: Site Survey.** Disponível em: http://www.teleco.com.br/tutoriais/tutorialrwlanman3/pagina_2.asp. Acesso em: 05 mai. 2016.

STALLINGS, William, **Redes e Sistemas de Comunicação de Dados – Teoria e Aplicações Corporativas**. Tradução 5 Ed. Rio de Janeiro: Editora Elsevier, 2005

VIT'ANGELO, Eduardo, **Hotspot com Ubuntu Sever 11.04 32-Bits.** Disponível em: https://www.vivaolinux.com.br/artigo/Hotspot-com-Ubuntu-Server-11.04-32Bits. Acesso em: 06 mar. 2016.

WILLIAN, Fonseca, **Wireless: Diferenças entre as Gerações b, g e n.** Disponível em: http://www.tecmundo.com.br/internet/2764-wireless-diferencas-entre-as-geracoes-b-g-e-n.htm . Acesso em: 05 mar. 2016.