DOI: 10.5748/20CONTECSI/PSE/SEC/7256

eLocator: e207256

A METHODOLOGY FOR IMPLEMENTING SECURE WIRELESS NETWORKS IN HYBRID CORPORATE ENVIRONMENTS UMA METODOLOGIA PARA IMPLANTAÇÃO DE REDES SEM FIO SEGURAS EM AMBIENTE CORPORATIVO HÍBRIDO

Robson Do Nascimento – https://orcid.org/0009-0005-2107-9058
Ipt

Matheus Jacon Pereira – https://orcid.org/0000-0002-0668-1033
Ipt

A Methodology for ImplementingSecure Wireless Networks in Hybrid Corporate Environments

Abstract In recentyears, therehasbeen a significantincrease in the use of radio frequency-accessibledevices. Thesedevices range fromthoseenabling internet access, such as computers, smartphones, smartwatches, andtablets, tosensorsandactuators in home andcorporateIoT networks, as well as devices in industrial networks. Thiseaseofconnectivitybrings new possibilities for attackson data security, exploitingvulnerabilities in thevariousmentioneddevices for data theftandmanipulation. In certaincorporateenvironments, it isnecessarytoprovideaccesstobothcorporateequipmentandexternalpublicdevices. In thiscontext, the network must havedifferentlevelsofprotectionandmonitoringtoensureadequatesecurityand performance. Thisworkaimstopresent a methodology for implementing a corporate wireless network in a mixedenvironment, with a focuson IEEE 802.11ac technology, andtointroducethemostappropriatemitigationtechniques.

Keywords: wi-fi 5, wi-fi 6, wireless, security.

Uma metodologia para implantação de redes sem fio seguras em ambiente corporativohúbrido

Resumo

Nos últimos anos houve um grande aumento do uso de dispositivos acessíveis por rádio frequências. Desde dispositivos que permitem o acesso ao conteúdo da internet tais como computadores, smartphones, smartwatchese tablets, passando por sensores e atuadores das redes IoT domésticas e corporativas e ainda dispositivos em redes industriais. Tal facilidade de conexão traz consigo novas possibilidades de ataques contra a segurança de dados, explorando as vulnerabilidades dos diversos dispositivos mencionados acima para roubo e manipulação de dados. Em certos ambientes corporativos é necessário o fornecimento de acesso aos equipamentos da própria corporação bem como a equipamentos de público externo. Neste contexto, a rede deve possuir diferentes níveis de proteção e monitoramento de modo a garantia a segurança e desempenho adequados. Este trabalho tem como objetivo apresentaruma metodologia de implementação de rede sem fio corporativa com ambiente misto e foco na tecnologia IEEE 802.11ac, apresentando as técnicas de mitigação mais adequadas.

Palavras-Chave: wi-fi 5, wi-fi 6, redes sem fio, segurança.

1. INTRODUÇÃO

As comunicações sem fio, nas quais as informações são transmitidas por ondas eletromagnéticas no espaço livre, são imprescindíveis no contexto das comunicações modernas. Seu principal apelo é a mobilidade. Por exemplo, o fato de poder trocar informações pela internet, mesmo em trânsito, é o que faz dos smartphones verdadeiros "escritórios ambulantes" no ambiente corporativo.

Atualmente há grande variedade de dispositivos que podem participar de redes sem fio, tais como computadores, tablets, impressoras, smartphones, etiquetas de identificação por rádio frequência, dispositivos para pagamento por aproximação, dispositivos *bluetooth*, sensores, atuadores, controles de iluminação e dispositivos IoT. Estes dispositivos são conectados por diferentes padrões de sinais padronizados pelo IEEE (*InstituteofElectricalandElectronicsEngineers* – Instituto de Engenheiros Eletricistas e Eletrônicos) de modo que equipamentos de fabricantes diferentes sejam totalmente compatíveis no processo de comunicação.

Essa ampla gama de utilizações oferece para um potencial atacante também grande variedade de formas de ataques de segurança.

As comunicações sem fio apresentam as seguintes vantagens e desvantagens, conforme poder ser visto no Quadro 1:

Vantagens	Desvantagens
Custo: sem a utilização de cabos e interfaces de rede físicas, o custo da infraestrutura é menor do que uma rede cabeada.	**Interferência:** ondas eletromagnéticas causam e sofrem interferência de outras ondas eletromagnéticas que estejam no mesmo espaço, isso pode alterar a informação que está sendo transmitida.
Mobilidade: principal vantagem das redes sem fio, permitindo uso em qualquer local em que haja sinais disponíveis.	**Atenuação:** a intensidade de uma onda eletromagnética diminui à medida que ela se afasta da fonte ediminui ainda mais sehouver obstáculos pelo caminho.
Facilidade de instalação: por não necessitar de cabos, o ingresso em uma rede sem fio é muito mais simples e rápido do que uma rede cabeada.	**Segurança:** por não possuir uma barreira física que há em uma rede cabeada, os dados transmitidos por redes sem fio são mais suscetíveis às recepções não autorizadas e/ou alterações indevidas.

Quadro 1– Vantagens e desvantagens das comunicações sem fio
(Adaptado de SILVA, 2021)

A principal causa de vulnerabilidades das redes sem fio é a inexistência de uma barreira física entre um atacante e as ondas eletromagnéticas que transmitem os dados entre os equipamentos. No nível puramente físico, para poder receber estas ondas basta estar em umaregião coberta por elas. Claro que, no nível lógico, há técnicas de transmissão que restringem a interpretação das informações somente a certos dispositivos autorizados.

Mas, nem sempre eles oferecem a segurança adequada e podem apresentar vulnerabilidades. Nesse contexto, vários tipos de ataques podem ocorrer (CHOI, 2008):

- Captura passiva de pacotes de informação e a subsequente interpretação de seu conteúdo (ataque contra a confidencialidade dos dados);
- Alteração dos dados em trânsito entre os dispositivos (ataque contra a integridade da informação);
- Sequestro da comunicação, na qual o atacante se passa por um dos dispositivos válidos (ataque contra a autenticidade);
- Indisponibilidade da rede pelo comprometimento dos dispositivos que controlam as conexões nos chamados ataques de negação de serviço (*Denialof Services* – DoS) (ataque contra a disponibilidade dos serviços);
- Invasão e comprometimento de equipamentos da rede cabeada a partir de uma rede sem fio.

O objetivo principal deste trabalho é fornecer uma metodologia adequada para o fornecimento de uma rede sem fio segura em umambiente corporativo de modo a providenciar acesso, tanto a um público externo, quanto aos dispositivos da própria corporação considerando os ataquesmais comuns à segurança de redes sem fio e os métodos para mitigar suas vulnerabilidades,contribuindo para projetos de redes sem fio mais seguras.

Este trabalho tem foco no padrão IEEE 802.11ac (Wi-Fi 5) adotado na maioria das redes sem fio atuais, mas também abordará aspectos do padrão IEEE 802.11ax (Wi-Fi 6) eestá dividido em cinco seções. A seção 2descrevea fundamentação teórica do funcionamento das redes sem fio Wi-Fi 5 e 6. A seção 3 descreve as vulnerabilidades encontradas nas redes Wi-Fi 5 e as técnicas de mitigação mais comuns. A seção 4 apresenta as melhorias de segurança do Wi-Fi 6 e a quinta seção contém as conclusões, limitações e sugestões para futuros trabalhos de pesquisa e aplicação prática em projetos de redes.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 Padrão IEEE 802.11ac (Wi-Fi 5)

Em 1997, o IEEE lançou o padrão 802.11 definindo para os fabricantes de dispositivos as especificações para as redes sem fio em áreas locais (*Wireless Local Area Networks* – WLAN), operando na faixa de 2,4 GHz e oferendo uma taxa de transmissão de 2 Mbit/s. Este padrão ficou conhecido,mais tarde, como Wi-Fi, uma abreviação de "*wireless fidelity*" (fidelidade sem fio), um nome comercial registrado pela associação de fabricantes Wi-Fi *Alliance.*

À medida que novas melhorias de desempenho e segurança são criadas, o IEEE segue lançando novos padrões. Em2013, foi lançado o padrão 802.11ac, também conhecido como Wi-Fi 5. Este é o padrão de redes Wi-Fi adotado pelas operadoras no Brasil atualmente.

O Wi-Fi 5 oferece taxas de transmissão de até 7Gbits/s operando na frequência de 5GHz. Esta faixa de 5GHz é dividida em canais de 20 Mhz até 160Mhz por dispositivo. Por questão de compatibilidade, os pontos de acesso e roteadores sem fio desenvolvidos para este padrão também oferecem suporte para o padrão anterior (802.11n, Wi-fi 4), operando na faixa de 2,4 GHz.

2.2 Padrão IEEE 802.11ax (Wi-Fi 6)

Lançado em 2019, o padrão 802.11.ax contém um novo protocolo de camada física que proporciona taxas de transmissão de até 9,6Gbp/s. Utiliza as faixas de frequência de 2,4 GHz e 5 Ghz, para compatibilidade com os padrões anteriores e uma nova faixa de 6 Ghz para permitir uma maior densidade de equipamentos.

O ponto chave deste novo padrão é a adoção da técnica de modulação OFDMA (*OrthogonalFrequency-DivisionMultiple Access*, acesso múltiplo por divisão de frequência ortogonal) em contraste com a técnica OFDM (*OrthogonalFrequencyDivisionMultiplexing*, multiplexação por divisão de frequências ortogonais) utilizada pelo Wi-Fi 5. O OFDMA permite que cada canal de transmissão com o access point seja utilizado por mais de uma estação cliente ao mesmo tempo, conforme mostra a figura 1.

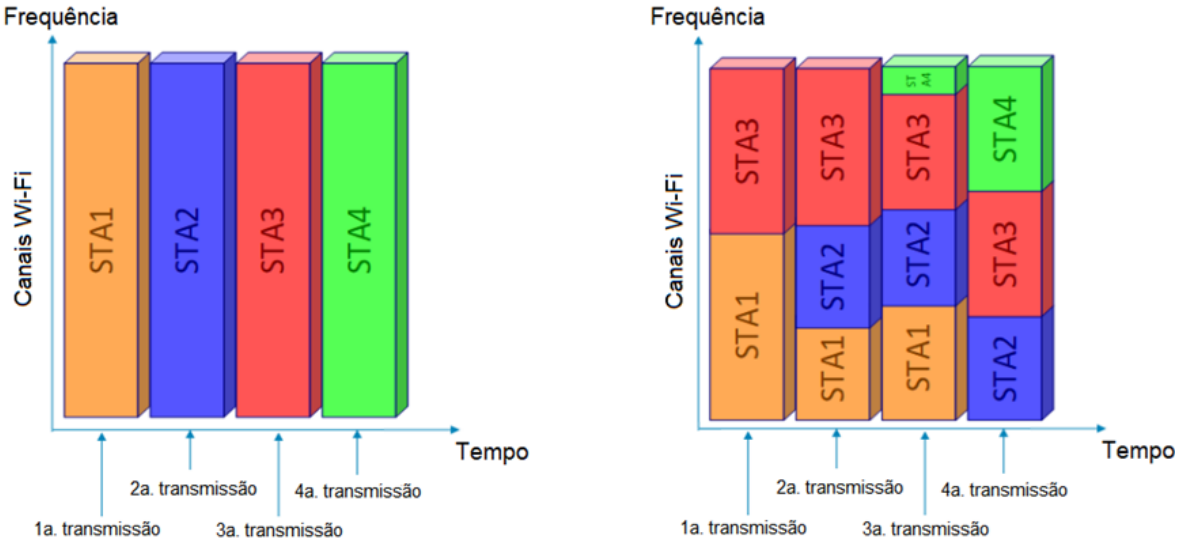

Figura 1. Representação da utilização dos canais no OFDM (esquerda) e OFDMA (direita) (STOILOV, 2020)

O IEEE 802.11ax modifica tanto as camadas física e MAC (*Media Access Control*). Ele atinge as expectativas atuais graças a canais mais amplos, MU-OFDMA para acesso ao canal, uplink (UL) MU-MIMO para melhorar a capacidade, SR para eficiência espectral, *Target Wake Time* (TWT) para gerenciar o consumo de energia e Modulação em Amplitude em Quadratura (QAM) de 1024 para aumentar o *throughput*. Juntas, essas características resultam em taxas de dados elevadas de até 9,6 Gb/s.

2.3Ameaças e vulnerabilidades das redes Wi-Fi atuais

As ameaças às redes Wi-Fi são listadas abaixo:

- **Associação acidental**: Redes locais sem fio (WLANs) da empresa ou pontos de acesso em proximidade podem criar faixas de transmissão sobrepostas. Um usuário que pretende se conectar a uma LAN pode, inadvertidamente, se conectar a um ponto de acesso da rede vizinha, expondo recursos de forma não intencional. Risco: Exposição acidental dos recursos de uma LAN a um usuário não pretendido.
- **Associação maliciosa**:Um dispositivo sem fio é configurado para parecer um ponto de acesso legítimo, permitindo que o atacante roube senhas de usuários legítimos e penetre em uma rede com fio por meio de um ponto de acesso sem fio genuíno. Risco: Acesso não autorizado e possíveis violações de dados.
- **Redes *ad hoc***:Redes ponto a ponto entre computadores sem fio sem um ponto de acesso, sem um ponto central de controle. Risco: Ameaças de segurança devido à ausência de um ponto de controle central.
- **Roubo de identidade** (*spoofing* de MAC):Atacantes interceptam o tráfego de rede para identificar o endereço MAC de um computador com privilégios de rede. Risco: Acesso não autorizado e possível uso indevido de privilégios de rede.
- **Ataques de intermediário** (man-in-the-middle):Convencer um usuário e um ponto de acesso de que estão se comunicando diretamente quando, na realidade, a comunicação é interceptada por um dispositivo intermediário de ataque. Risco: Redes sem fio são particularmente vulneráveis a esses ataques, levando a potenciais interceptações e manipulações de dados.
- **Negação de Serviço (***Denialof Service* - DoS):Ocorre quando um atacante continua a bombardear um ponto de acesso sem fio ou alguma outra porta sem fio acessível com várias mensagens de protocolo projetadas para consumir recursos do sistema. O ambiente sem fio é propício a esse tipo de ataque, pois é fácil para o atacante direcionar várias mensagens sem fio ao alvo.
- **Injeção de rede**: Esse ataque visa pontos de acesso sem fio que estão expostos ao tráfego de rede não filtrado, como mensagens de protocolo de roteamento ou mensagens de gerenciamento de rede. Um exemplo desse tipo de ataque ocorre com comandos de reconfiguração falsos enviados para afetar roteadores e switches, degradando o desempenho da rede.

As redes sem fio são compostas por três componentes que podem ser explorados por atacantes:

- **Meio de transmissão:** Redes sem fio geralmente envolvem comunicações por difusão (*broadcast*), o que as torna mais suscetíveis que redes cabeadas para escuta e/ou alteração das mensagens por atacantes e interferências. Redes sem fio também são mais vulneráveis a ataques ativos que exploram vulnerabilidades em protocolos de comunicação.

- **Ponto de acesso:** A principal ameaça envolvendo pontos de acesso sem fio é o acesso não autorizado à rede.
- **Dispositivo móvel:** alguns dispositivos sem fio, como *smartphones* e *tablets*, possuem sistemas operacionais sofisticados, mas recursos limitados de memória e processamento para enfrentar ameaças, incluindo negação de serviço e *malware*. Estes dispositivos, muitas vezes de uso pessoal, acessam redes domésticas e/ou públicas inseguras e executam aplicativos de terceiros que podem conter software malicioso. Já outros dispositivos sem fio, como sensores e robôs, podem ser deixados em locais remotos e/ou hostis ficando expostos a ataques físicos.

2.4 Fortalecimento de redes Wi-Fi

Considerando as vulnerabilidades dos componentes das redes sem fio podemos agrupas as contramedidas para mitigar as vulnerabilidades destas redes em três grupos: fortalecimento das transmissões, fortalecimento dos pontos de acesso e fortalecimento dos dispositivos. Todas estas medidas devem ser descritas na Política de Segurança da organização a

2.4.1 Fortalecimento das transmissões

Para minimizar ataques de escuta e alteração de dados em trânsito, duas contramedidas podem ser efetuadas:

- **Técnicas de ocultação de sinal:** Consiste em desativar a transmissão do identificador de conjunto de serviços (SSID) pelos pontos de acesso sem fio.Reduzir a potência do sinal para o nível mais baixo que ainda fornece cobertura necessária; e posicionar os pontos de acesso sem fio no interior do edifício, longe de janelas e paredes externas. Maior segurança pode ser alcançada ainda pelo uso de antenas direcionais e técnicas de blindagem de sinal.
- **Criptografia:** O uso de protocolos de criptografia e autenticação é o método padrão para combater tentativas de alterar ou inserir transmissões. A criptografia de todas as transmissões sem fio é eficaz contra a escuta, na medida em que as chaves de criptografia são seguras.

Adicionalmente, varreduras no ambiente (*Site survey*) podem detectar a existência de outros dispositivos usando a mesma faixa de frequência, ajudando a determinar onde posicionar os pontos de acesso sem fio. As intensidades de sinal podem ser ajustadas e técnicas de blindagem podem ser utilizadas na tentativa de isolar um ambiente sem fio de transmissões concorrentes próximas.

2.4.2 Fortalecimento dos pontos de acesso

A abordagem principal para prevenir acesso não autorizado é o padrão IEEE 802.1X para controle de acesso à rede baseado em porta.

O IEEE 802.1X utiliza os termos *suplicante*, *autenticador* e *servidor de autenticação* (AS). No contexto de uma WLAN 802.11, os dois primeiros termos correspondem à estação sem fio e ao ponto de acesso. O AS é geralmente um dispositivo separado no lado com fio da rede, mas também pode residir diretamente no autenticador.

Antes que um suplicante seja autenticado pelo AS usando um protocolo de autenticação, o autenticador apenas repassa mensagens de controle ou autenticação entre o suplicante e o AS; o canal de controle 802.1X é desbloqueado, mas o canal de dados 802.11 é bloqueado. Uma vez que um suplicante é autenticado e as chaves são fornecidas, o autenticador pode encaminhar dados do suplicante, sujeitos a limitações predefinidas de controle de acesso para a rede. Nessas circunstâncias, o canal de dados é desbloqueado.

O padrãoIEEE 802.1X oferece um mecanismo de autenticação para dispositivos que desejam se conectar a uma LAN ou rede sem fio. O uso do 802.1X pode evitar que pontos de acesso não autorizados e outros dispositivos não autorizados se tornem portas de entrada inseguras.

Adicionalmente, para evitar acesso não autorizado aos pontos de acesso, recomenda-se trocar as senhas e nomes de usuário administrativos destes equipamentos.

Para a autenticação de usuários podem ser utilizados os protocolos WPA2 (Wi-Fi Protected Access 2) ou WPA3. Este último introduz um algoritmo de criptografia mais robusto, o *SimultaneousAuthenticationofEquals* (SAE), que oferece uma segurança aprimorada em comparação com o algoritmo de chave pré-compartilhada (*PreShared Key*, PSK) usado no WPA2. Mesmo em redes abertas, sem o uso de senhas de autenticação, o WPA3 utiliza o algoritmo de criptografia *Opportunistic Wireless Encryption* (OWE) para proteger a confidencialidade das comunicações, proporcionando uma camada extra de privacidade.

2.4.3 Fortalecimento dos dispositivos móveis

A política de segurança para dispositivos móveis deve ser baseada na suposição de que qualquer dispositivo móvel pode ser roubado ou, pelo menos, acessado por uma parte maliciosa. A ameaça é dupla: uma atacante pode tentar recuperar dados sensíveis do próprio dispositivo ou pode usar o dispositivo para obter acesso aos recursos da organização.

Muitas organizações acham conveniente ou até mesmo necessário adotar uma política de traga-seu-próprio-dispositivo (*BYOD*) que permite que os dispositivos móveis pessoais dos funcionários tenham acesso aos recursos corporativos. Cada dispositivo deve ser inspecionado antes de acessar à rede. Dispositivos com segurança alterada como "*rooted*" ou "*jail-broken*" não devem são permitidos na rede, e dispositivos móveis não podem armazenar contatos corporativos no armazenamento local. Seja um dispositivo de propriedade da organização ou BYOD, a organização deve configurar o dispositivo com controles de segurança, incluindo o seguinte:

- Habilitar o bloqueio automático, que faz com que o dispositivo seja bloqueado se não for usado por um determinado período de tempo, exigindo que o usuário

insira novamente um PIN de quatro dígitos ou uma senha para reativar o dispositivo.

- Habilitar proteção por senha ou PIN. O PIN ou senha é necessário para desbloquear o dispositivo. Além disso, pode ser configurado para que e-mails e outros dados no dispositivo sejam criptografados usando o PIN ou senha e só possam ser recuperados com o PIN ou senha.
- Evitar o uso de recursos de auto-completar que lembram nomes de usuário ou senhas.
- Habilitar a remoção remota.
- Garantir que a proteção SSL esteja ativada, se disponível.
- Certificar-se de que o software, incluindo sistemas operacionais e aplicativos, esteja atualizado.
- Instalar software antivírus conforme disponibilidade.
- Proibir o armazenamento de dados sensíveis no dispositivo ou criptografá-los.

A equipe de TI também deve ter a capacidade de acessar dispositivos remotamente, apagar todos os dados do dispositivo e, em seguida, desativar o dispositivo em caso de perda ou roubo.

A organização pode proibir toda a instalação de aplicativos de terceiros, implementar lista de permissões para proibir a instalação de todos os aplicativos não aprovados, ou implementar um ambiente seguro que isole os dados e aplicativos da organização de todos os outros dados e aplicativos no dispositivo móvel. Qualquer aplicativo na lista aprovada deve ser acompanhado por uma assinatura digital e um certificado de chave pública de uma autoridade aprovada.

A organização pode implementar e impor restrições sobre quais dispositivos podem ser sincronizados e sobre o uso de armazenamento em nuvem.

Para lidar com a ameaça de conteúdo não confiável, as respostas de segurança podem incluir o treinamento de pessoal sobre os riscos inerentes a conteúdos não confiáveis e a desativação do uso da câmera em dispositivos móveis corporativos.

Para combater a ameaça do uso malicioso de serviços de localização global (GPS), a política de segurança pode ditar que esse serviço seja desativado em todos os dispositivos móveis.

Deve ser utilizado um protocolo de autenticação robusto para limitar o acesso do dispositivo aos recursos da organização. Frequentemente, um dispositivo móvel possui um autenticador específico do dispositivo, pois se assume que o dispositivo tem apenas um usuário. Uma estratégia preferível é ter um mecanismo de autenticação de duas camadas, que envolve autenticar o dispositivo e, em seguida, autenticar o usuário do dispositivo.

A organização deve ter mecanismos de segurança para proteger a rede contra acesso não autorizado. A estratégia de segurança também pode incluir políticas de firewall específicas para o tráfego de dispositivos móveis. As políticas de firewall podem limitar o escopo de acesso a dados e aplicativos para todos os dispositivos móveis. Da mesma forma, sistemas de detecção e prevenção de intrusões (IDS/IPS) podem ser configurados com regras mais rígidas para o tráfego de dispositivos móveis.

3. METODOLOGIA PARA IMPLANTAÇÃO DE REDE WI-FI HIBRIDA SEGURA

3.1 Contexto e Diretrizes

Em certos ambientes corporativos há a necessidade de fornecimento de acesso à internet tanto para o público interno, constituído de colaboradores e funcionários terceirizados, como para o público externo, tal como clientes e visitantes por meio de dispositivos móveis.

Constitui um desafio implementar uma rede Wi-Fi com políticas de segurança extremamente diferentes compartilhando a mesma infraestrutura de equipamentos. Neste contexto, os tráfegos dos clientes internos e externos deve ser separado e monitorado com abordagens diferentes. Os clientes internos devem ter acesso aos recursos essenciais para seu trabalho oriundos de servidores da empresa com acesso restrito. Já os visitantes terão acesso aos recursos da internet, entretanto não poderão ter acesso à rede interna da empresa.

3.2 Implementação da solução

As diretrizes e técnicas que devem ser utilizadas para implementação a rede Wi-Fi híbrida são descritos a seguir.

3.2.1 Segmentação de rede

Para que sejam aplicadas políticas de segurança diferentes para os públicos interno e externo, na mesma infraestrutura física, a melhor solução é a criação de redes LAN virtuais (VLANs).

As VLANs permitem que portas de um mesmo switch de camada 2 não tenham conectividade, separando totalmente seu tráfego. Cada VLAN em uma rede é um domínio de *broadcast* diferente, constituindo uma rede IP distinta. Para que dois *hosts*, conectados em portas de switch que estejam em VLANs diferentes possam se comunicar, seu tráfego deve passar por um elemento de camada 3, seja um roteador ou switch de camada 3 que fará o roteamento de tráfego entre as VLANs. As VLANs podem ser propagadas por outros switches da mesma rede permitindo que *hosts* que estejam distantes fisicamente possam ter conectividade.

Uma vez que a VLAN permite separar o tráfego de hosts dentro de uma mesma rede física, ela proporciona um importante mecanismo de segurança isolando redes críticas. O uso de VLANs aumenta o desempenho da rede como um todo uma vez que ela isola o tráfego de broadcast dentro de sua VLAN de origem. Além disso, em redes cujos dispositivos intermediários, ou seja, roteadores, switches e pontos de acesso suportem qualidade de serviço (QoS), asVLANs podem ser usadas para priorizar o tráfego com base em requisitos de desempenho, por exemplo, configurando os dispositivos de rede para que o tráfego de voz seja encaminhado prioritariamente, estando numa VLAN específica, diminuindo sua latência na transmissão.

No caso de uma rede Wi-Fi híbrida deve ser criada ao menos uma VLAN para tráfego do público interno e outra para o público externo. Estas VLANs devem ser propagadas para os switches e pontos de acesso onde se deseja conectividade para estes públicos. O acesso aos clientes deve ser feito por identificadores de rede sem fio (SSIDs) diferentes, sendo cada um associado a uma VLAN.

3.2.2 Métodos de autenticação

Devem ser implementados métodos diferentes de autenticação para os clientes.

Para o público interno deve ser usado o protocolo WPA3 ou, em caso de incompatibilidade com os dispositivos de rede, o WPA2 com uma senha forte e trocada com frequência. Adicionalmente, pode ser usada a filtragem de endereços MAC permitindo o acesso à SSID do público interno somente aos equipamentos cadastrados previamente. Se for possível, ative a autenticação baseada em portas (IEEE 802.1X) para restringir o acesso a dispositivos autorizados apenas.

Para o público externo deve ser configurado um portal de autenticação (*captive portal*) para visitantes que desejam acessar a internet. Esse portal pode exigir um login simples, mediante aceitação de termos e condições, indicando claramente as diretrizes de uso, limitações e penalidades por violações. Se for conveniente, pode ser concedido um código de acesso temporário. Os visitantes devem estar cientes das práticas de segurança recomendadas pela organização e as informações pessoais dos visitantes devem ser armazenadas para futura auditoria em conformidade com a Lei Geral de Proteção de Dados (LGPD).

Garanta que o acesso seja limitado na VLAN de visitantes e que não haja conectividade direta com a rede corporativa efetuando bloqueios na camada 3 isolando o tráfego desta VLAN. Também é interessante ativar o isolamento de cliente na rede de visitantes para evitar que os dispositivos conectados se comuniquem entre si. Isso adiciona uma camada extra de segurança.

3.2.3 Confinamento e monitoramento do tráfego

Na camada 3 deve ser implementada uma configuração que restrinja o tráfego da rede de visitantes e que impeça o acesso de seus usuários aos ativos da rede interna da organização. Isso pode ser feito por meio de listas de controle de acesso (ACLs) em roteadores ou por meio de regras baseadas em endereços IP em firewalls do tipo filtro de pacotes.

É interessante ativar um controle de largura de banda para a VLAN do público externo. Com isso o desempenho da rede interna não é comprometido se houver um aumento dos clientes externos ou haja um ataque oriundo da VLAN externa que aumente o tráfego.

Deve haver um monitoramento constante da rede verificando o estado dos *links* principais e o comprometimento dos recursos dos dispositivos de rede fazendo uso, por

exemplo, de alguma ferramenta baseada no protocolo SNMP (*Simple Network Management Protocol*).

O backbone da rede deve ser monitorado por um IDS/IPS de modo a detectar atividades suspeitas e garantir conformidade com as políticas de segurança estabelecidas.

Todos os *firmwares* e sistemas operacionais dos dispositivos de rede devem ser atualizados.

Para evitar que haja ataques de DHCP (*Dynamic Host ConfigurationProtocol*) *spoofing* nos quais um dispositivo mal-intencionado tenta distribuir informações de configuração DHCP falsas para outros dispositivos na rede deve-se habilitar a técnica de segurança DHCP *Snooping. O* DHCP *Snooping* opera em switches de rede e monitora o tráfego entre os clientes e o servidor DHCP não permitindo que servidores DHCP falsos respondam às solicitações DHCP.

4. CONCLUSÃO

A implementação de uma rede Wi-Fi híbrida, que atenda tanto aos requisitos dos clientes internos de uma organização quanto aos visitantes externos, requer uma abordagem cuidadosa e abrangente em termos de segurança. Ao combinar tecnologias e estratégias, é possível criar um ambiente que ofereça acessibilidade e funcionalidade, ao mesmo tempo em que mantém a integridade e a confidencialidade dos dados. Algumas das técnicas essenciais discutidas incluem a segmentação da rede por meio de VLANs, a utilização de autenticação forte, como o IEEE 802.1X, para controle de acesso, a implementação de criptografia robusta para proteger a comunicação sem fio e a aplicação de políticas de segurança adaptadas a diferentes perfis de usuários.

Além disso, a monitorização contínua, a atualização de dispositivos de rede bem configurados e a pronta detecção de anomalias são cruciais para manter a segurança ao longo do tempo. A integração de ferramentas de detecção de intrusões e a realização de auditorias regulares podem fortalecer ainda mais a postura de segurança da rede sem fio híbrida. Em última análise, ao adotar uma abordagem multicamadas e proativa, as organizações podem garantir um ambiente sem fio que promova a colaboração e a produtividade, sem comprometer a segurança dos dados sensíveis.

REFERÊNCIAS BIBLIOGRÁFICAS

AHADI, Said Abdul Ahad; RAKESH, Nitin; VARSHNEY, Sudeep. **Overview On Public Wi-Fi Security Threat Evil Twin Attack Detection**. 2020 Ieee International Conference On Advent Trends In Multidisciplinary Research And Innovation (Icatmri), Buldhana, India,, 30 dez. 2020. IEEE. http://dx.doi.org/10.1109/icatmri51801.2020.9398377. Disponívelem: https://ieeexplore.ieee.org/abstract/document/9398377. Acessoem: 24 jan. 2023.

BRENZA, Sebastian; PAWLOWSKI, Andre; PÖPPER, Christina. **A practical investigation of identity theft vulnerabilities in Eduroam**. Proceedings Of The 8Th Acm Conference On Security & Privacy In Wireless And Mobile Networks, p. 1-11, 22 jun. 2015. ACM. http://dx.doi.org/10.1145/2766498.2766512. Disponívelem: https://dl.acm.org/doi/10.1145/2766498.2766512. Acessoem: 18 fev. 2023.

CHOI, M., et al. **Wireless Network Security: Vulnerabilities, ThreatsandCountermeasures**. InternationalJournalofMultimediaandUbiquitousEngineering, July 2008. Disponível em: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1b0de694f8ac13396df9fc8a821164d95dcd04f5. Acesso em 10 set. 2023.

EFE, Ahmet; KAPLAN, MesrureBetül. **Wi-Fi Security Analysis For E&M-Government Applications**. International Journal Of Multidisciplinary Studies And Innovative Technologies. Ancara, Turquia, vol. 3, no. 2, pp. 86–98, 2019. Disponívelem: https://dergipark.org.tr/en/download/article-file/859231. Acessoem: 02 abr. 2023.

IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN, in IEEE Std 802.11ax-2021 (Amendment to IEEE Std 802.11-2020) , vol., no., pp.1-767, 19 Mai 2021, doi: 10.1109/IEEESTD.2021.9442429. Disponível em: https://ieeexplore.ieee.org/document/9442429. Acesso em: 20 jul. 2022.

IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,em *IEEEStd 802.11-1997* , p.1-445, 18 Nov. 1997, doi: 10.1109/IEEESTD.1997.85951. Disponível em: https://ieeexplore.ieee.org/document/654749. Acesso em: 20 dez. 2022.

IEEE Standard for Information technology--Telecommunications and information exchange between systems—Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications--Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz., em *IEEE Std 802.11ac(TM)-2013*, p.1-425, 18 Dec. 2013, doi: 10.1109/IEEESTD.2013.7797535. Disponível em: https://ieeexplore.ieee.org/document/9363693. Acesso em: 17 ago. 2023.

KWON, Songhui; CHOI, Hyoung-Kee. **Evolution of Wi-Fi Protected Access: security challenges**. Ieee Consumer Electronics Magazine, v. 10, n. 1, p. 74-81, 01 jan. 2021.

Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mce.2020.3010778. Disponívelem: https://ieeexplore.ieee.org/document/9146348. Acessoem: 5 jan. 2023.

MA, D., andTSUDIK, G. **Security andPrivacy in Emerging Wireless Networks**. IEEE Wireless Communications, October 2010.

MEDEIROS, Henrique. **Operadoras do Brasil migrarão para o Wi-Fi 6 em 2023**. 2022. Disponível em: https://www.mobiletime.com.br/noticias/27/10/2022/operadoras-do-brasil-migrarao-para-o-wi-fi-6-em-2023/. Acesso em: 27 dez. 2022.

MOURA, Matheus José de. **Uso do sistemapfSense para a coleta de dados de redessem-fio**. 2019. 41 f. TCC (Graduação) - Curso de Sistemas de Informação, Faculdade de Computação (Facom), Universidade Federal de Uberlândia, Uberlândia, 2019. Disponívelem: https://repositorio.ufu.br/handle/123456789/27473. Acessoem: 21 jan. 2023.

MOZAFFARIAHRAR, E.; THEOLEYRE, F.; MENTH, M. **A Surveyof Wi-Fi 6: Technologies, Advances, andChallenges**. *Future Internet* **2022**, *14*, 293. https://doi.org/10.3390/fi14100293.

REDDY, Dr. B. Indira, SRIKANTH, V., **Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3)**, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Vol. 5 Issue 4, pp. 28-35, Julho-Agosto 2019. Disponívelem https://doi.org/10.32628/CSEIT1953127 Journal URL : http://ijsrcseit.com/CSEIT1953127. Acessoem 10 out. 2023.

RIECKERS, Jan-Frederik. **Passive security analysis of current TLS implementations and configurations in the eduroam EAP-TLS environment**. 2021. 76 f. TCC (Graduação) - Curso de BacharelemCiências, Staats- Und Universitätsbibliothek (Suub), Bremen, 2021. https://doi.org/10.26092/elib/1577. Disponívelem: https://media.suub.uni-bremen.de/bitstream/elib/5972/3/Bachelor_EAP-TLS.pdf. Acessoem: 10 dez. 2022.

SCHEPERS, Domien; RANGANATHAN, Aanjhan; VANHOEF, Mathy. **Let numbers tell the tale: measuring security trends in wi-fi networks and best practices**. Proceedings Of The 14Th Acm Conference On Security And Privacy In Wireless And Mobile Networks, p. 100-105, 28 jun. 2021. ACM. http://dx.doi.org/10.1145/3448300.3468286. Disponívelem: https://dl.acm.org/doi/pdf/10.1145/3448300.3468286. Acessoem: 20 mar. 2023.

SILVA, Fernanda Rosa; SOARES, Juliane A.; SILVA, Lídia P C.; et al. **Redes sem fio**. Grupo A, 2021. ISBN 9786556901374. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556901374/. Acessoem: 24 jul. 2022.

STALLINGS, William. **Cryptography and Network Security Principles and Practice**. Pearson Education, 8 ed., 2023. ISBN 978-0-13-670722-6.

STOILOV, Petar. **An overview of the recent standards and security technologies for wireless local area networks**. Proceedings Of University Of Ruse, Ruse, v. 59, n. 32, p.

142-150, 13 nov. 2020. Disponível em: https://conf.uni-ruse.bg/bg/docs/cp20/3.2/3.2-22.pdf. Acesso em: 16 dez. 2022.