UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
CURSO DE ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

SILAS MAIESKI

ESTUDO DE CASO: IMPLANTAÇÃO DE AUTENTICAÇÃO DE USUÁRIOS EM REDE SEM FIO EMPRESARIAL UTILIZANDO O PROTOCOLO 802.1X

MONOGRAFIA DE ESPECIALIZAÇÃO

PATO BRANCO
2018

SILAS MAIESKI

ESTUDO DE CASO: IMPLANTAÇÃO DE AUTENTICAÇÃO DE USUÁRIOS EM REDE SEM FIO EMPRESARIAL UTILIZANDO O PROTOCOLO 802.1X

Monografia de especialização apresentada ao III Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Departamento Acadêmico de Informática, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Fábio Favarim

PATO BRANCO
2018

TERMO DE APROVAÇÃO

ESTUDO DE CASO: IMPLANTAÇÃO DE AUTENTICAÇÃO DE USUÁRIOS EM REDE SEM FIO EMPRESARIAL UTILIZANDO O PROTOCOLO 802.1X.

por

Silas Maieski

Esta monografia foi apresentada às 19h30min do dia 21 de novembro de 2018, como requisito parcial para obtenção do título de ESPECIALISTA, no III Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho **aprovado**.

Prof. Dr. Fábio Favarim
Orientador / UTFPR-PB

Prof. Dr. Dalcimar Casanova
UTFPR-PB

Prof. Dr. Eden Ricardo Dosciatti
UTFPR-PB

Prof. Dr. Fábio Favarim
Coordenador do III Curso de Especialização
em Redes de Computadores

A Folha de Aprovação assinada encontra-se na Coordenação do Curso.

AGRADECIMENTOS

Primeiramente, dedico este trabalho a Deus, que me guia na jornada da minha vida, pois sem ele eu não teria conseguido a oportunidade de estudar o curso de especialização em redes de computadores e a força de concluí-lo.

A minha esposa Jenifer Luana Vanderlinde, por todo apoio, companheirismo e amor. Por sempre estar ao meu lado ao longo da especialização e não me deixar desistir nessa caminhada.

Aos meus pais e irmãs que me incentivaram a sempre buscar o conhecimento e aperfeiçoamento através dos estudos.

Ao meu orientador Prof. Dr. Fábio Favarim, por todas as ideias, incentivo e orientação nesta etapa.

E a todos os professores que passaram por minha formação, por toda dedicação, conhecimento e experiências repassadas.

RESUMO

MAIESKI, Silas. Estudo de caso: Implantação de autenticação de usuários em redes sem fio empresarial utilizado o protocolo 802.1X. 2018. 56 f. Monografia (Especialização em Redes de Computadores) – Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2018.

Este trabalho de conclusão de curso de especialização apresenta a implantação do protocolo 802.1X em ambiente empresarial, visando expor as melhorias apresentadas pelo mesmo na autenticação de usuários. A implantação foi feita utilizando o padrão IEEE 802.1X, protocolo RADIUS de autenticação, método de autenticação CHAP e base de dados *Active Directory*. Com o intuito de minimizar os riscos de acesso não autorizado, utilizou-se o método WPA2 e algoritmo AES. Após a conclusão da instalação, pode-se observar a facilidade da criação de novas redes sem fio, bem como uma melhor gestão e permissão de acesso da mesma. O controle de permissão de acesso agora se dá apenas pela equipe do TI da empresa. Também garantiu melhor desempenho no uso da rede sem fio, limitando o acesso apenas a pessoal autorizado. Este protocolo auxiliou no controle de acessos de usuários e monitoramento dos mesmos, beneficiando amplamente a empresa.

Palavras-chave: RADIUS. Autenticação. 802.1X. WPA2.

ABSTRACT

MAIESKI, Silas. Case study: Deployment of authentication of users on enterprise wireless networks using the 802.1X protocol. 2018. 56 f Monografia (Especialização em Redes de Computadores) – Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2018.

This work conclusion of specialization course presents the implementation of the 802.1X protocol in business environment, aiming to expose the improvements presented by it in the authentication of users. Deployment was done using the IEEE 802.1X standard, authentication RADIUS protocol, CHAP authentication method, and Active Directory database. In order to minimize the risks of unauthorized access, the WPA2 method and AES algorithm were used. Upon completion of the installation, it is possible to observe the ease of creating new wireless networks, as well as better management and access permission. Access permission control is now only performed by the company's IT staff. It also ensured better performance in using the wireless network, limiting access only to authorized personnel. This protocol assisted in the control of user access and monitoring of users, benefiting the company.

Keywords: RADIUS. Authentication. 802.1X. WPA2.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

AAA	Autenticação, Autorização e Auditoria/Contabilização
AD	*Active Directory*
AES	*Advanced Encryption Standard*
AES	*Advanced Encryption Standard*
AP	*Access Point*
BSS	*Basic Service Set*
CCMP	*Counter Cipher Mode*
CHAP	*Challenge-Handshake Authentication Protocol*
CNSA	Conjunto de Algoritmos de Segurança Nacional Comercial
DS	*Distribution System*
EAP	*Extensible Authentication Protocol*
EAP-LEAP	*Extensible Authentication Protocol - LightWeight*
EAP-TLS	*Extensible Authentication Protocol - Transport Layer Security*
ESS	*Extended Service Set*
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
IV	Vetor de Inicialização
NAC	*Network Access Control*
NPS	*Network Policy Server*
PAP	*Password Authentication Protocol*
PEAP	*Protected EAP*
PSK	*Pre-Shared Key*
RADIUS	*Remote Authentication Dail In User Service*
SAE	*Simultaneous Authentication of Equals*
STA	*Wireless LAN Stations*
TCP	Protocolos de Controle de Transmissão
TKIP	*Temporal Key Integrity Protocol*
WEP	*Wired Equivalent Privacy*
WLAN	*Wireless Local Area Network*
WMAN	*Wireless Metropolitan Area Network*
WPA	*WiFi Protected Access*
WPA2	*WiFi Protected Access II*
WPA3	*WiFi Protected Access III*WPAN *Wireless Personal Area Network*

WWAN *Wireless Wide Area Network*

SUMÁRIO

1. INTRODUÇÃO

O processo de evolução dos Sistemas de Informação caminhou junto com as tecnologias de informática e de telecomunicações. A evolução dessas tecnologias desencadeou o surgimento das redes de computadores e os novos sistemas que possibilitam maior integração das áreas empresariais. Toda essa tecnologia gera mobilidade, liberdade e agilidade em sua utilização (RUFINO, 2007).

Todo esse aperfeiçoamento possibilitou a integração de sistemas através de redes de computadores e a criação de servidores com grande capacidade de processamento de informações, o que se tornou popular e deixou o mercado concentrado na tendência tecnológica de comunicação por redes sem fio. O uso recorrente dessa tecnologia gera a necessidade de segurança às empresas. O objetivo de toda essa segurança é proteger informações de pessoas que não tem autorização a obtê-las, dificultando seu acesso a elas.

Um mecanismo de segurança que foi inicialmente utilizado, era o WEP (*Wired Equivalent Privacy*). Segundo Araujo Neto e Silva (2004), "o objetivo desse mecanismo era garantir em uma rede sem fio a segurança implícita obtida pela restrição de acesso ao barramento em uma rede cabeada". Ainda, segundo os autores, o WEP mostrou-se deficiente, pois suas chaves podem ser quebradas com facilidade.

Após isso, criou-se o WPA (*WiFi Protected Access*) pensando em uma solução definitiva para a segurança. Entretanto, foi produzido de forma a tornar os dispositivos WEP atualizáveis, o que acabou reaproveitando o antigo protocolo e trazendo problemas do antecessor. Para tratar desses problemas, uma nova versão do WPA foi desenvolvida, o WPA2. Trata-se de um padrão mais seguro, em que o risco de intrusões é praticamente zero, pois utiliza o padrão de segurança CCMP (*Counter Cipher Mode*) e AES (*Advanced Encryption Standard)* (DEMARTINI, 2013). No momento, a principal vulnerabilidade é quando um atacante já possui acesso a rede Wi-Fi e consegue obter certas chaves de acesso de segurança e executa um ataque.

O WPA3 foi lançado no final do primeiro semestre do ano de 2018 com a intenção de implementar novos recursos e fortalecer a segurança do protocolo WPA2. Este novo protocolo busca melhorar a autenticação e a criptografia, e ao mesmo tempo, facilitar a configuração de redes sem fio. O WPA3 busca impedir os ataques *Man in the Middle* (quando o atacante tem acesso ao meio físico, a rede) através do uso de uma criptografia de dados de forma individualizada. O protocolo não veio para substituir o WPA2 (que ainda receberá

atualizações), apenas melhorar a segurança do usuário. Para redes de nível empresarial, o problema está na chave (senha) de acesso, pelo fato de todos os usuários utilizam a mesma senha, e não há como identificar individualmente o usuário que esteja fazendo uso indevido da mesma. Uma das formas de controlar esse acesso indevido é através de um servidor de autenticação RADIUS (*Remote Authentication Dail In User Service*) que é um protocolo de autenticação utilizado pelo IEEE 802.1X, que pode se autenticar e gerenciar individualmente o acesso de usuários. Facilmente a organização poderá atribuir ou remover permissão de acesso, auditoria e outros itens de acordo com sua necessidade (ARAUJO NETO E SILVA, 2004).

Com esse estudo, pode se contribuir para a facilidade na gestão e controle de acesso, o que resulta em menor custo operacional, e principalmente, melhorar a segurança dos dados da organização, pois limitará os acessos apenas ao pessoal autorizado, evitando acessos indevidos aos dados empresarias. Neste contexto, este trabalho tem como objetivo apresentar métodos de melhorias no uso da rede sem fio empresarial.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Este trabalho tem por objetivo a implantação da autenticação individual de usuários em rede sem fio empresarial utilizando o protocolo 802.1x.

1.1.2 Objetivos Específicos

- Garantir confiabilidade do acesso à rede sem fio empresarial;
- Autenticar todos os usuários no momento da sua conexão de modo a autorizar esses usuários a acessar somente os recursos que tem autorização para acesso dentro da rede da empresa;
- Implantar políticas de acesso à rede, de acordo com o papel de cada usuário;
- Monitorar todos os acessos e uso de usuários.

1.2 JUSTIFICATIVA

Com o uso de uma rede estruturada em uma empresa, o acesso à rede interna pode ser através de pontos de rede sem fio existentes na empresa, o que permite que o usuário possa se locomover entre departamentos sem a necessidade de alteração na rede.

Em muitas organizações o cenário onde apenas um usuário e senha são utilizados é bastante comum, o que permite que qualquer um com a senha possa acessar a rede da empresa. Com isso, quando ocorre o desligamento de algum colaborador, faz-se necessário a alteração da senha de acesso. Ainda assim, caso algum colaborador ativo compartilhe dados com pessoas não-autorizadas, o mesmo terá acesso aos dados da rede se estiver conectado na rede sem fio da empresa e a empresa não terá como identificar qual usuário está acessando.

O uso de um servidor RADIUS vai resolver o problema de segurança. A autenticação em nível de usuário permite que apenas usuários devidamente registrados tenham acesso à rede. Dessa forma, o acesso de pessoal não autorizado é impossibilitado pela exigência de informações de autenticação.

O servidor RADIUS também permitirá a autorização dos usuários na rede, pois uma vez identificado o usuário, o mesmo dará permissão de acesso a determinados recursos na rede, assim como a empresa poderá ter acesso a um controle de navegação de cada usuário, podendo obter relatórios detalhados de utilização da rede.

1.3 ESTRUTURA DO TRABALHO

O Capítulo 2 apresenta alguns conceitos sobre redes sem fio, mecanismos de segurança de redes sem fio, protocolo IEEE 802.1x e servidor RADIUS.

No Capítulo 3 encontram-se as metodologias utilizadas para a realização deste trabalho, e os materiais utilizados para que a pesquisa fosse realizada.

E por fim, no Capítulo 4 apresentam-se as conclusões deste trabalho.

2 REFERENCIAL TEÓRICO

Neste capítulo são abordadas tecnologias de segurança para redes sem fio, cuja explicação é indispensável para a compreensão do projeto de implantação desenvolvido neste trabalho. Inicialmente são abordadas as classificações de redes sem fio quanto a sua área de cobertura. Em seguida são descritos mecanismos de segurança para redes sem fio. E por fim o protocolo utilizado na pesquisa.

2.1 REDES SEM FIO

A tecnologia das redes sem fio permite conexão sem a necessidade de uso de cabos, apenas por radiofrequência ou infravermelho. Esta tecnologia é mais utilizada em redes de computadores para navegação na Internet e possui classificação baseada na área de abrangência, sendo, segundo Da Silva (2008):

- WPAN (*Wireless Personal Area Network*): São redes pessoais de curta distância, normalmente até 10 metros.
- WLAN (*Wireless Local Area Network*): são redes locais que utilizam frequência de rádio para fazer a conexão com a Internet ou a rede. Alcançam distâncias de até 100 metros.
- WMAN (*Wireless Metropolitan Area Network*): São redes metropolitanas que possibilitam o uso até 10 quilômetros de distância.
- WWAN (*Wireless Wide Area Network*): utilizam operadoras de celulares para criar sua rede de transmissão, atingindo um raio de até 100 quilômetros.

Na Figura 1 ilustra-se a abrangência das redes sem fio.

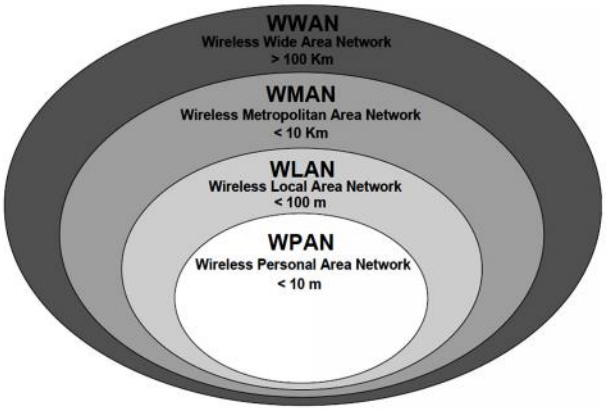

Figura 1 - Classificação das redes sem fio.
Fonte: Andrade (2013, p.8)

Segundo Da Silva (2008), a topologia das redes sem fio é composta de:

- BSS (*Basic Service Set*): Célula de comunicação da rede sem fio.
- STA (*Wireless LAN Stations*): Mais de um cliente na rede
- AP (*Access Point*): Coordenada a comunicação entre a rede sem fio e a rede convencional.
- DS (*Distribution System*): Permite a interconexão do ponto de acesso sem a utilização de cabos ou fios.
- ESS (*Extended Service Set*): São várias BSS com pontos de acesso conectados em uma mesma rede convencional, que faz com que uma STA possa se movimentar de uma BSS para outra sem desconectar da rede.

Inicialmente, as redes sem fio foram projetadas para estabelecer interatividade entre computadores, sem se pensar em segurança de dados. No decorrer do tempo, com o grande crescimento da demanda comercial, as empresas começaram a necessitar de sistemas viáveis e de longo prazo, o que tornou a segurança de informações necessária a fim de se evitar invasões de pessoas não autorizadas (COSTA, DA SILVA, & DA CRUZ, 2012).

A maioria das invasões pode ocorrer em três categorias, sendo elas: Ataque de vulnerabilidade (envio de mensagens a uma aplicação vulnerável e execução em um hospedeiro direcionado, que pode pifar o hospedeiro), inundação na largura de banda (envio de inúmeros pacotes ao hospedeiro, fazendo com que o mesmo fique entupido e não deixe os pacotes legítimos alcançarem o servidor) e inundação na conexão (o invasor estabelece um grande número de Protocolos de Controle de Transmissão – TCP no hospedeiro, e o hospedeiro para de aceitar conexões legítimas (KUROSE & ROSS, 2010).

Alguns mecanismos de segurança para redes sem fio foram criados a fim de se evitar esses tipos de ataque, os mesmos são relacionados a seguir.

2.2 MECANISMOS DE SEGURANÇA PARA REDES SEM FIO

O uso de mecanismos de segurança em redes sem fio se justifica em todas as aplicações, especialmente nas quais há informações pessoais e é necessário manter privacidade.

Segundo Kurose e Ross (2010), existem algumas propriedades desejáveis para a comunicação segura em redes sem fio, sendo elas:

- Confidencialidade: Apenas o remetente e o destinatário devem entender o conteúdo da mensagem transmitida, o que faz necessário que esta mensagem seja cifrada de alguma forma para impedir que invasores interceptem a mesma.
- Autenticação do ponto final: O remetente e o destinatário precisam confirmar a identidade um do outro, entretanto, esta autenticação não é tão simples assim.
- Integridade da mensagem: Se assegurar de que não foram feitas alterações nas mensagens originais enviadas. Algumas técnicas de soma de verificação e de enlaces confiáveis podem ser utilizadas neste caso.
- Segurança Operacional: Em redes de Internet pública, que é muito utilizada por empresas, universidades e outros, os invasores podem obter segredos corporativos, lançar ataques e mapear configurações da rede interna. Pode-se utilizar um *firewall* entre a rede organizacional e a rede pública para controlar os acessos de pacotes para a rede.

Segundo Paim (2011), existem diversos mecanismos para segurança em redes sem fio, entre eles WEP e WPA que são usados em pontos de acesso residenciais e em empresa de pequeno porte. Esses protocolos utilizam uma chave compartilhada por todos os usuários da rede. Nos tópicos a seguir, os mesmos são apresentados.

2.2.1 *Wired Equivalent Privacy* (WEP)

O WEP é um padrão de segurança disponibilizado em 1997 agregado a ao padrão 802.11, que é um protocolo que desenvolveu uma série de padrões para redes de transmissão de dados sem fio e que especifica as camadas física e de controle de acesso ao meio (VIEIRA, 2004).

Segundo Rufino (2007), no protocolo, o emissor e o receptor utilizam a mesma chave criptografada para a encriptação do texto puro e decriptação do texto cifrado.

> "A segurança WEP é composta de dois elementos básicos: uma chave estática, que deve ser a mesma em todos os equipamentos de rede, e um componente dinâmico, que, juntos, formarão a chave usada para cifrar o código. O protocolo não define de que forma essa chave deve ser distribuída, portanto a solução convencional é também a mais trabalhosa, em que a chave é cadastrada manualmente em todos os equipamentos" (RUFINO,2007).

Para Lehembre (2005), o padrão WEP é baseado no "algoritmo criptografado RC4, com uma chave de 40 bits ou 104 bits, sendo combinado com um Vetor de Inicialização (IV)". Paim (2011) comenta que as funções da criptografia RC4 são: gerar um código para encriptar e decriptar e realizar a criptografia propriamente dita da mensagem. O RC4 é um algoritmo de

chave simétrica de fluxo pois sua encriptação e decriptação são independentes do tamanho da mensagem. Para que haja uma segurança maior no processo, a permutação deve ser diferente a cada mensagem enviada, e para isso, o RC4 é combinado com um IV. O IV é recalculado a cada iteração do algoritmo e é acrescido à chave secreta. O IV deve ser incluído no texto cifrado que será enviado, pois quem recebe a mensagem não possui este valor.

O padrão WEP se encarrega de criptografar os dados transmitidos através da rede. Há dois tamanhos de padrões WEP, o de 64 *bits* que é suportado por qualquer ponto de acesso que siga o padrão Wi-Fi e o de 128 *bits* que não é suportado por qualquer produto pois é necessário que todos os componentes usados na sua rede suportem o padrão.

Devido ao uso do WEP ter se tornado tão popular, o mesmo passou a ser um algoritmo com inúmeras falhas de segurança. Essas falhas se deram devido ao aumento do poder de processamento dos computadores, deixando o WEP ineficaz pois possui uma chave de tamanho máximo de 128 *bits*. Sendo assim, se o invasor tiver um *software* de ataque-a senha da rede sem fio será descoberta (SILVA E FREITAS, 2013).

Para Paim (2011), entre os diversos ataques existentes, alguns se destacam pelo tempo de execução muito baixo, sendo eles:

- Força Bruta: Combinações de nomes de usuários e senhas que são comumente utilizados, até se encontrar um que funcione.
- Conexão: O suplicante conecta no ponto de acesso, o desafio passa em claro e após é encriptado. Então o atacante pode ter acesso ao mesmo conteúdo das duas formas, o que facilita o processo de obtenção da chave secreta.
- Escuta: Faz-se a escuta do tráfego por alguns minutos até que o valor do IV se repita.

2.2.2 Wi-Fi Protected Access (WPA)

O WPA é o protocolo WEP melhorado que teve seu lançamento no ano de 2003 e trouxe consigo a encriptação de 256 bits. O WPA utiliza o protocolo TKIP (*Temporal Key Integrity Protocol*) e, assim como o WEP, faz uso do algoritmo RC4, entretanto, não envia a chave secreta “em claro” e trabalha com vetores de inicialização mais inteligentes, a fim de evitar ataques (PAIM, 2011).

Segundo Kurose e Ross (2010), o WPA pode ser usado de dois modos, Empresarial ou Pessoal. No modo pessoal, a autenticação é feita através de uma chave previamente compartilhada. A chave compartilhada é armazenada no ponto de acesso e os dispositivos que querem ter acesso à rede sem fio, devem usar a mesma chave. Esse tipo é conhecido como

WPA-PSK, PSK vem de *Pre-Shared Key*. Já no modo empresarial, há um servidor que é responsável por fazer a autenticação dos usuários da rede, nesse caso cada usuário tem uma chave individual. Nesse modo, é usado o padrão 802.1x e o EAP (*Extensible Authentication Protocol)* (descritos posteriormente) para prover autenticação através de um servidor RADIUS. Neste tipo, toda solicitação de autenticação na rede sem fio é encaminhada pelos pontos de acesso ao servidor RADIUS.

> "802.1x e EAP para prover autenticação através de um servidor RADIUS, este fica encarregado de fazer a autenticação do usuário, todos os APs presentes na rede estarão associados a este servidor RADIUS, com isso a autenticação ficará centralizada em um único servidor para todos os APs" (STANGARLIN, 2012).

Sukhija e Gupta (2012), citam algumas falhas do WPA, entre elas: Uso do mesmo algoritmo de criptografia RC4, vulnerabilidade a ataques de força bruta e ataques de negação de serviço. Mas apesar de suas falhas, o mesmo não deixa de ser uma camada de proteção adicional.

2.2.3 *Wi-Fi Protected Access* 2 (WPA2)

O WPA2, também conhecido como 802.11i, foi desenvolvido em 2004 como um sucessor do WPA. O mesmo utiliza os mesmos parâmetros do antecessor e possui novos mecanismos melhorados de segurança de dados (OLIVEIRA & BEM, 2017). Entre esses mecanismos está o método criptográfico utilizado, no qual o protocolo utiliza o AES (*Advanced Encryption Standard*) com o TKIP. O TKIP com o AES, permite uma chave de criptografia ponto a ponto inicial exclusiva para cada autenticação, assim como a alteração sincronizada da chave de criptografia (AGUIAR, 2005).

A principal vulnerabilidade do WPA2 é através de ataques, onde invasores interceptam dados de sites sem https pela rede sem fio. Esta falha se encontrava no *handshake*, que é onde duas máquinas firmam um acordo antes de iniciar a troca de dados. Este erro pode ser corrigido via *software* (LEHEMBRE, 2005).

2.2.4 *Wi-Fi Protected Access* 3 (WPA3)

O lançamento oficial do novo protocolo de segurança WPA3 ocorreu em 25 de junho de 2018 pela *Wi-Fi Alliance* com a intenção de melhorar a segurança em conexões Wi-Fi domésticas e empresariais. Este protocolo oferece proteção robusta mesmo quando o usuário

opta por uma senha pouco complexa e simplifica o processo de configuração de segurança para dispositivos que tenham pouca interface de exibição. Outro recurso é o reforço na privacidade do usuário em redes abertas utilizando criptografia de dados individualizada e segurança de 192 bits, junto com o Conjunto de Algoritmos de Segurança Nacional Comercial (CNSA) (WI-FI ALLIANCE, 2018).

Segundo a Wi-Fi Alliance, o WPA3 utiliza dois níveis de segurança, o WPA3-*Personal* e o WPA3-*Enterprise*. O WPA3-*Personal* utiliza o SAE (*Simultaneous Authentication of Equals* ou em português Autenticação Simultânea de Iguais), um protocolo que estabelece uma chave pré-compartilhada (PSK) segura entre os dispositivos a fim de evitar tentativas de adivinhação de senhas por invasores. O WPA3-*Enterprise* possui criptografia de 192 bits, fornecendo proteção adicional a redes que transmitem dados confidenciais, como governo ou finanças. Este pacote de 192 bits garante uma combinação consistente de ferramentas criptográficas da rede WPA3.

O Quadro 1 compara e resume as características de cada protocolo (WEP, WPA, WPA2 e WPA3) discutidas nas subseções 2.2.1, 2.2.2, 2.2.3 e 2.2.4 do Capítulo 2.

Quadro 1 -Comparação entre os protocolos WEP, WPA, WPA2 e WPA3.

	WEP	**WPA**	**WPA2**	**WPA3**
Propósito	Aumentar a segurança as redes *ethernets*, equivalente a segurança inerente a um meio cabeado	Solucionar temporariamente falhas de segurança do WEP sem utilização de novo *hardware*	Utilizar o padrão 802.11i do IEE e substituir formalmente o WPA	Aumentar a segurança em conexões *Wi-Fi* doméstica e empresarial
Criptografia	RC4	TKIP	AES	CNSA
Autenticação	WEP-Open / WEP-Shared	WPA-PSK / WPA-Enterprise	WPA2-Personal / WPA2-Enterprise	SAE

Fonte: Autoria Própria (2018).

2.3 PROTOCOLO IEEE 802.1X

O padrão 802.1x foi desenvolvido pelo IEEE (Instituto de Engenheiros Eletricistas e Eletrônicos) na década de 1990 para padronizar o controle de acesso às redes e para ser uma solução de segurança padrão em redes cabeadas e sem fio (MORAIS, 2016). O protocolo realiza identificação e autenticação em redes sem fio ou cabeadas através de um servidor de autenticação (ABREHA, 2018).

O IEEE 802.1x é um padrão baseado na porta NAC (*Network Access Control*), originalmente desenvolvido para o IEEE 802.2, que fornece um mecanismo de autenticação para que um dispositivo se conecte a uma LAN sem fio ou cabeada. Esse controle de acesso utiliza as características físicas da LAN para autenticar dispositivos conectados na porta LAN. Este acesso pode ser negado se o processo de autenticação falhar (ABREHA, 2018).

A autenticação usando o protocolo 802.1x envolve três entidades: suplicantes (clientes que desejam acessar a rede), autenticadores (equipamentos responsáveis por regularizar o acesso do suplicante, por exemplo, um *switch*) e um servidor de autenticação (aplicação responsável por responder as requisições de acesso à rede). As funções do autenticador e do servidor podem ser executadas pelo mesmo dispositivo (IEEE, 2010). A Figura 2 apresenta a especificação IEEE 802.1x.

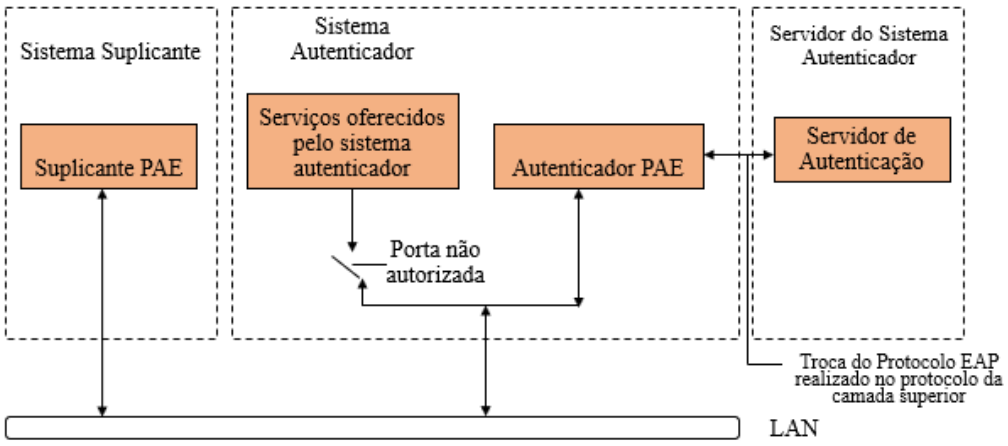

Figura 2 - Modelo IEEE 802.1x da especificação IEEE 802.1x
Fonte: IEEE (2018).

O IEEE 802.1X utiliza um modelo de arquitetura de controle integrada ao padrão de AAA (Autenticação, Autorização e Auditoria/Contabilização). A autenticação verifica a identidade digital do usuário de um sistema, a autorização garante que um usuário autenticado somente tenha acesso aos recursos autorizados e, por fim, a auditoria/contabilização refere-se a coleta de informações sobre o uso dos recursos de um sistema pelos seus usuários. Na autenticação é necessária reciprocidade. O usuário deve se identificar e se autenticar para o sistema, entretanto, o sistema não se autentica para o usuário. Um problema neste caso é o aumento de vulnerabilidade no pacote de protocolos TCP/IP, o qual pode gerar informações incorretas para um usuário que esteja tentando acessar um recurso da rede indevido. Para resolver isto, é necessário que haja autenticação mútua, que é quando o *host* autentica o cliente e o cliente autentica o *host* (BARROS & FOLTRAN JR., 2008).

O procedimento de autorização é baseado em restrições como hora e localização física. A autorização determina a natureza do serviço que será concedida ao usuário, como, por exemplo, filtragem de endereço IP e concessão de endereço IP e rotas (VOLLBRECHT, 2000).

Já a contabilização monitora o consumo de recursos da rede pelos usuários. A contabilização em tempo real refere-se à informação que é entregue com o consumo de recursos, simultaneamente. Já a contabilização em *batch* são as informações armazenadas até que seja utilizada no momento necessário (BARROS & FOLTRAN JR., 2008).

Todos estes procedimentos de AAA são necessários para oferecer autenticação segura a uma rede onde se faz necessário ter controle dos acessos dos usuários.

Para que seja possível implementar uma rede com o padrão IEEE 802.1X, é necessário que exista uma infraestrutura de suporte, na qual o cliente possua suporte a este padrão, *switches*, pontos de acesso sem fio, servidor RADIUS e banco de dados de usuários. A Figura 3 apresenta a infraestrutura mínima para operar com o 802.1X.

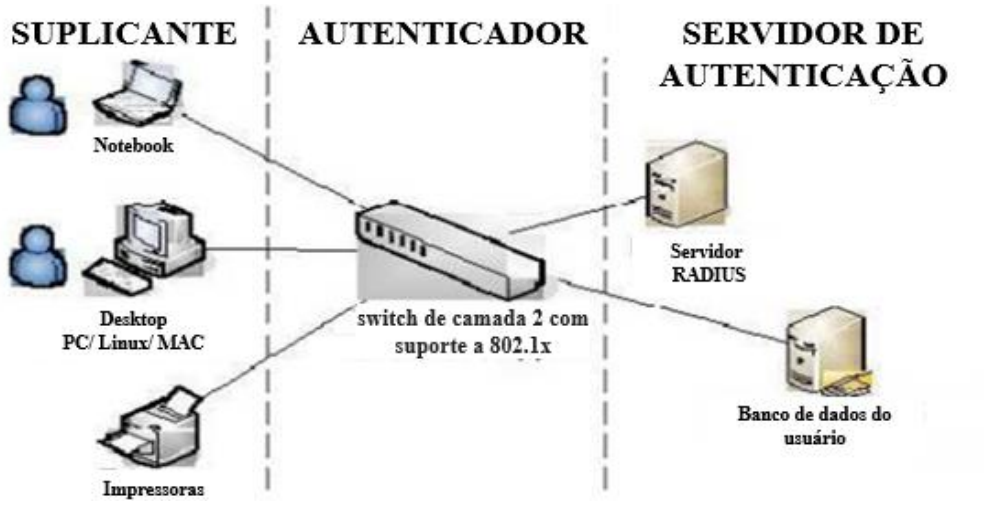

Figura 3 - Infraestrutura para operar com o protocolo IEEE 802.1X
Fonte: Blunk e Vollbrecht (2012)

2.4 REMOTE AUTHENTICATION DIAL IN USER SERVER (RADIUS)

O RADIUS (RIGNEY et al., 2000) pode ser utilizado para diversos serviços, tais como: um protocolo de autenticação utilizado pelo 802.1x a fim de melhorar a criptografia do padrão WEP ou com outros recursos de utilização como o EAP.

Segundo a RFC 2865 (RIGNEY et al., 2000) que especifica o RADIUS, os principais recursos providos são:

- Modelo cliente/servidor: O NAS opera como um cliente do RADIUS. Ele é o responsável por passar informações do usuário para os servidores RADIUS e, na sequência, atuar no retorno da resposta. O RADIUS é responsável por receber a solicitação do usuário, autenticar o mesmo e retornar as informações de configuração necessárias para que o cliente entregue ao usuário.
- Segurança de rede: as trocas de informações entre o cliente e o servidor RADIUS são autenticadas através do uso de uma criptografia compartilhada, a qual não é enviada pela rede. As senhas dos usuários também são enviadas de forma criptografada entre eles, a fim de se eliminar a possibilidade de algum invasor interferir na troca de senhas
- Mecanismos de autenticação flexíveis: O servidor RADIUS pode suportar vários métodos de autenticação de usuário, entre eles: Protocolo de autenticação de senha (PAP - *Password Authentication Protocol*), Protocolo de autenticação por Desafios de Identidade (CHAP - *Challenge-Handshake Authentication Protocol*) e Protocolo de Autenticação Extensível (EAP - *Extensible Authentication Protocol*).
- Protocolo extensível: Permite métodos de autenticação arbitrários usando trocas de informação e credenciais em tamanhos arbitrários.

O RADIUS possui três funções básicas, sendo elas: (i) autenticar usuários; (ii) autorizar serviços providos pela rede; e (iii) contabilizar todo novo pedido de entrada na rede. Em resumo, um suplicante faz uma requisição de acesso (utilizando *login* e senha) a um cliente RADIUS. O cliente requisita as credenciais de origem e envia para o servidor, em forma de mensagem RADIUS. O servidor chega e autentica os dados, e faz a autorização do cliente RADIUS. O acesso pode ser negado ou autorizado. Se for autorizado, o cliente libera o acesso à rede ao suplicante que fez a solicitação (BARROS & FOLTRAN JR., 2008). A Figura 4 representa esse processo de autenticação e autorização.

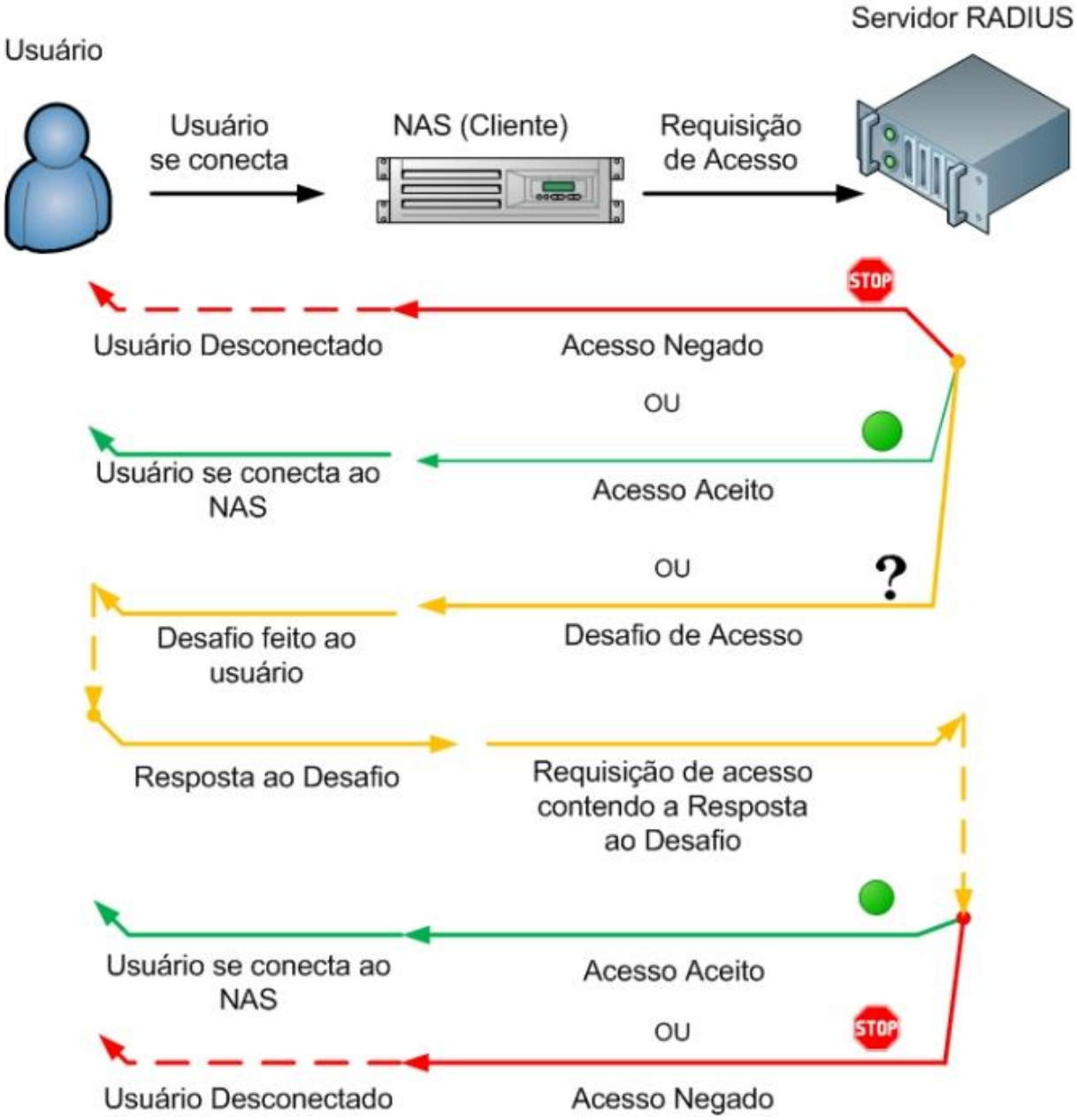

Figura 4 - Processo de autenticação RADIUS
Fonte: Carvalho (2008).

A utilização do RADIUS não é totalmente segura, pois quando se acessa este servidor, é necessário consultar uma base de dados a qual é responsável por associar as informações de autenticação com as identidades dos usuários. Então, recomenda-se que cada usuário esteja associado a somente uma forma de autenticação e que as senhas dos usuários e segredos compartilhados estejam armazenadas de forma segura (CARVALHO, 2008).

2.4.1 Atributos do protocolo RADIUS

Os atributos do protocolo RADIUS são subdivididos em número de identificação (ID), tamanho e valor. Os NAS, servidores de acesso à rede, fornecem dados complementares para uso nos critérios de concessão do acesso do servidor. O Quadro 2 apresenta uma lista de atributos utilizados para autenticação.

Quadro 2 - Lista de atributos RADIUS.

Nome	ID Tipo	Descrição
User-Password	2	Caso outra forma de autenticação não seja utilizada, este atributo contém a senha do usuário sendo autenticado. O seu valor é criptografado utilizando o algoritmo MD5 com a chave compartilhada entre o NAS e o servidor RADIUS.
NAS-IP-Address	4	Transmite o endereço IP do NAS.
NAS-Port	5	Identifica qual porta física do NAS que o usuário, que deseja se autenticar, está conectado.
Reply-Message	18	Transmite um texto do servidor RADIUS para ser apresentado ao usuário.
Vendor-Specific	26	Alocado para prover suporte a atributos específicos de fabricantes. O campo "valor" citado anteriormente, é dividido em dois, sendo que a primeira parte contém um outro número de identificação, e a segunda parte os dados relacionados.
Session-Timeout	27	Define o tempo máximo, em segundos, que a sessão da autenticação deverá ser mantida
Idle-Timeout	28	Determina o tempo máximo consecutivo, também em segundos, que a conexão pode permanecer ociosa antes que seja interrompida.
Calling-Station-Id	31	Identificação do NAS, por exemplo, o número físico da interface. No caso de redes LANs e WANs é o número do *Media Access Control*
NAS-Identifier	32	Transmite uma cadeira de caracteres contendo o nome atribuído ao NAS.
NAS-Port-Type	61	Indica o tipo de porta que o cliente está conectado ao NAS.
EAP-Message	79	Atributo que transporta um pacote do protocolo EAP. No uso do IEEE 802.1X a mensagem do suplicante é retransmitida ao servidor dentro deste atributo.

Fonte: Ulhôa (2010, p. 20)

2.4.2 Mecanismos de autenticação do RADIUS (PAP, CHAP e EAP)

Carvalho (2008), comenta cada um dos mecanismos de autenticação flexíveis, que é um dos recursos do RADIUS, sendo eles: PAP, CHAP e EAP (este utilizado no estudo). O PAP é um protocolo simples que transmite as senhas sem criptografia, o que o torna inseguro. Este protocolo é utilizado como uma última solução para a autenticação dos usuários. No PAP, o cliente envia o seu usuário e senha e o servidor envia uma permissão de acesso ou uma negação de acesso. O CHAP é mais seguro que o PAP, pois verifica periodicamente a identidade dos usuários em três etapas. A verificação dessa autenticidade é feita com segredo compartilhado entre o usuário e o servidor RADIUS. Após se estabelecer conexão, o RADIUS envia um desafio para o usuário e o usuário responde com um *hash* ao mesmo. O servidor verifica a resposta enviada e compara com o *hash* gerado por ele mesmo. Se estiver correto, o acesso é liberado, caso contrário, a conexão é finalizada.

O EAP foi criado pelo IETF (*Extensible Authentication Protocol*) para trabalhar com o protocolo PPP (Protocolo Ponto-a-Ponto) com o objetivo de enviar informações de identificação, evitando invasões não autorizadas em redes e conexões. O EAP permite que o usuário se identifique em um servidor específico (neste caso o servidor utilizaria o protocolo RADIUS) a fim de receber mensagens oriundas do ponto de acesso (PAIM, 2009).

O EAP utiliza quatro mensagens básicas durante a conexão: Requisição, Resposta, Sucesso e Falha. Paim (2009) explica que para iniciar uma conexão em uma rede sem fio que utiliza o EAP é necessário primeiramente enviar uma Requisição para o ponto de acesso. Este ponto de acesso retornará com um pedido de identidade do suplicante, o qual enviará uma resposta ao mesmo. Ao receber a resposta do suplicante, o ponto de acesso envia para o servidor RADIUS que cria então um desafio para o suplicante responder. Se o suplicante responder de maneira correta, terá acesso à rede sem fio, caso contrário, receberá uma mensagem de falha de conexão. No EAP, em nenhum momento o suplicante envia mensagens diretamente para o RADIUS, sempre há algum intermédio do ponto de acesso, o que garante maior segurança ao servidor. Este isolamento de contato permite também uma maior flexibilidade na hora da manutenção da rede. A Figura 5 apresenta de forma simplificada este processo.

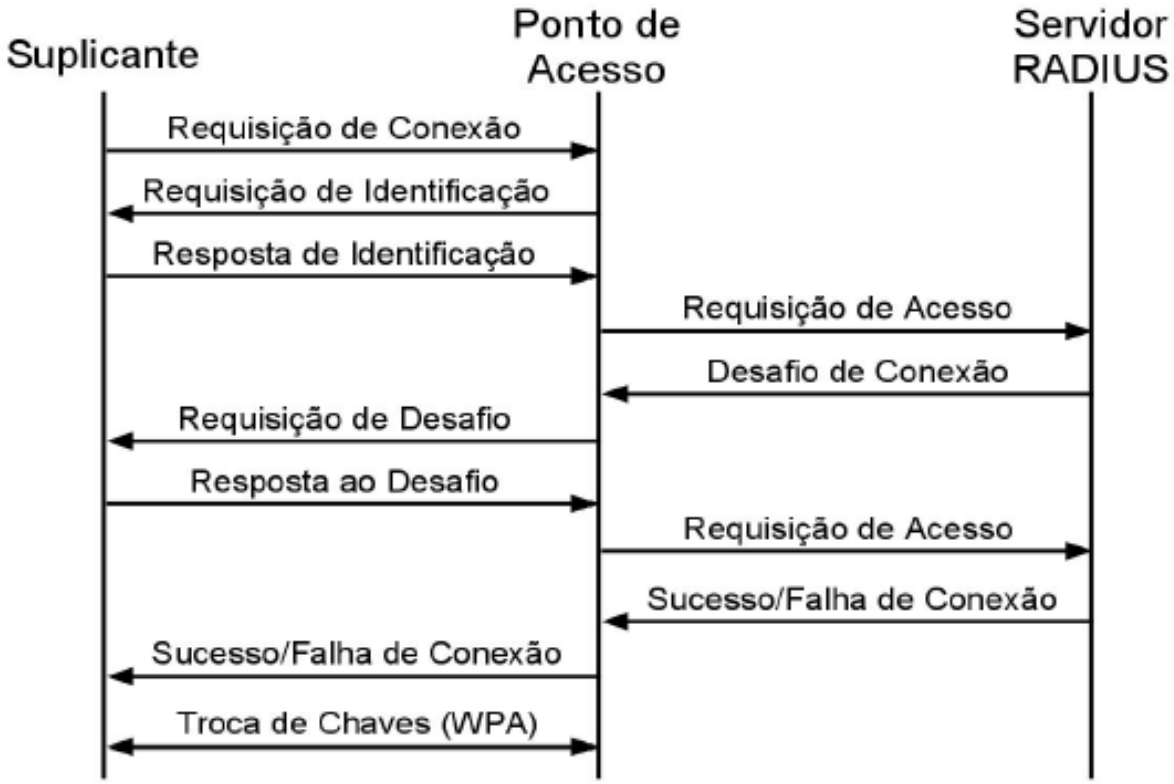

Figura 5 - Autenticação EAP com servidor RADIUS
Fonte: Paim (2009).

O 802.1x utiliza o protocolo EAP para gerenciar a autenticação na rede, pois ele possibilita a escolha de um método de autenticação para se utilizar (senha, certificado digital, *tokens* de identificação) (AGUIAR, 2005).

Intel (2018) cita alguns tipos de EAP que dão suporte a métodos de autenticação, sendo eles: EAP-LEAP (*LightWeight EAP*) que utiliza *login* e senha para transmitir a identidade do usuário, EAP-TLS (*Transport Layer Security*) que é especificado na RFC 2716 e PEAP (*Protected EAP*) que solicita certificado digital no servidor de autenticação, mas não exige este certificado nos clientes.

Neste contexto, percebe-se que a aplicação do protocolo RADIUS é de grande vantagem em ambientes empresariais, pois com ele é possível gerenciar individualmente o acesso de usuários, então, facilmente a empresa poderá atribuir ou remover a permissão dos mesmos. O protocolo também facilita a gestão, o que resulta em menor custo operacional e aumenta a segurança de dados, limitando o acesso apenas ao pessoal autorizado.

3 MATERIAIS E METODOLOGIA

Neste capítulo são descritos materiais utilizados, que são necessários para os objetivos de implantação da autenticação individual de usuários em redes sem fio. Além disso, também é apresentada a metodologia utilizada na realização deste trabalho.

3.1 MATERIAIS

O Quadro 3 apresenta as ferramentas utilizadas para o desenvolvimento do trabalho e as seções a seguir, descrevem brevemente cada uma delas.

Quadro 3 – Ferramentas utilizadas na implantação do protocolo RADIUS

Ferramentas	Versão	Aplicação
Active Directory	Microsoft Windows Server 2012 Standard	A base de dados de usuários foi utilizada em testes no ambiente restrito ao TI, onde foram criadas contas temporárias, e pós confirmação de funcionamento, a base real de dados dos usuários foi apontada nas configurações.
Controladora Ruckus sem fio	ZD1200 9.13.3.0 build 41	A controladora Ruckus sem fio foi utilizada na integração ao *Active Directory* e entregou de forma automática aos roteadores sem fio da rede as configurações RADIUS aplicadas.
Rede sem fio de ponto de acesso Ruckus	R600 9.13.3.0.41	As redes sem fio de ponto de acesso Ruckus receberam as configurações da controladora e passaram a entregar sua rede sem fio com a necessidade de autenticação com credencias do domínio.
Swicht HP	A5120EI-CMW520R2222P09	O *switch* HP foi utilizado como camada de transporte interligando as ferramentas.

Fonte: Autor (2018).

3.1.1 Microsoft Windows Server 2012 Standard

Para a implantação do protocolo RADIUS foram necessários serviços instalados no servidor Microsoft Windows Server 2012 *Standard*. Sendo um dos serviços o AD (*Active Directory)*, responsável por possibilitar ao usuário ter uma única senha para acessar o sistema principal da empresa, seus e-mails, seu computador, entre outros ativos de rede. Com a utilização do AD, serviço onde os usuários podem ter apenas uma senha para acessar todos os

recursos disponíveis na rede, é o responsável pela base de dados de usuários. O segundo foi o Serviço NPS (*Network Policy Server*) Servidor de Políticas de Rede, que permite que você configure e gerencie a autenticação de acesso à rede, a autorização e a contabilidade.

3.1.2 Controladora Ruckus sem fio

A controladora Ruckus sem fio apresenta uma interface de usuário Web altamente intuitiva para facilitar a configuração e administração de toda rede sem fio. Possui duas portas de 1.000 Mbps para redundância total. Cobertura com garantia vitalícia, suporte para 256 WLANs, servidor para entrega automática de endereços IP integrado, balanceamento de carga, controle de admissão de cliente em tempo real, estatísticas e monitoramento de desempenho. Seus recursos oferecem excelente funcionamento da rede sem fio, entregando segurança e possibilidades de otimização em tempo real, sua configuração inteira pode ser realizada em poucos minutos. Em seus recursos avançados podem ser detectados pontos de acesso invasores desconhecidos pela empresa, detecção de interferência e direcionamento de banda de Internet.

A controladora Ruckus centraliza a autenticação de autorização para todos os pontos de acesso, proporcionando um controle de admissão seguro em toda a WLAN. Tem capacidade de gerenciar até 75 pontos de acesso, e 2000 conexões simultâneas. Funciona com qualquer banco de dados de autenticação remota, como RADIUS e *Active Directory*. Na Figura 6 é apresentada uma imagem da controladora utilizada.

Figura 6 - Controladora Ruckus sem fio
Fonte: Ruckus (2014).

3.1.3 Ponto de Acesso Ruckus

O ponto de acesso Ruckus, modelo R600, oferece alto desempenho para as redes sem fio, com tecnologia patenteada de antena adaptável e redução de interferência automática para fornecer desempenho consistente e previsível em maior alcance. Seleciona automaticamente canais para obter o maior potencial de saída usando o gerenciamento de canal dinâmico. Comporta até 512 clientes simultâneos por ponto de acesso. Possui suporte a WPA-PSK (AES), 802.1x para RADIUS e *Active Directory*. A Figura 7 apresenta uma imagem do ponto de acesso utilizado.

Figura 7 - Rede sem fio de ponto de acesso Ruckus
Fonte: Ruckus (2017).

3.1.4 *Switch* HP 5120

O *switch* é um equipamento para extensão física dos pontos de rede, realiza as mesmas funções que um *hub*, mas com uma diferença importante: vários pacotes são transmitidos ao mesmo tempo, o que aumenta a velocidade da rede em comparação com a utilização de um *hub*. Se um pacote demora a ser transmitido, não interfere tanto na performance da rede, visto que muitos outros pacotes são transmitidos em paralelo. Em redes com grande tráfego de dados, a utilização de um *switch* em vez de um *hub* é altamente recomendável e desejável. A Série de *Switches* HP 5120 compreende *switches Gigabit Ethernet* inteligentes e totalmente gerenciados que oferecem alto desempenho, alta densidade de portas e instalação simplificada. O 5120 foi aprimorado para a camada de acesso em redes corporativas que exigem *Gigabit Ethernet*. Como parte de seu abrangente controle de segurança, o 5120 emprega IEEE 802.1X para identificar usuários que tentam acessar a rede. Esses interruptores são altamente confiáveis, fornecendo redundância e eliminando *loops* na rede. Eles também

oferecem uma gama de protocolos de gerenciamento para simplificar a administração da rede. Na Figura 8 apresenta–se imagem ilustrativa do *Switch* HP 5120.

Figura 8 - *Switch* HP 5120
Fonte: Hewlett Packard Enterprise (2015).

3.2 METODOLOGIA

A metodologia e os passos para o desenvolvimento desta implantação do protocolo 802.1x foram os seguintes: (i) validação das ferramentas e materiais disponíveis; (ii) estudo e levantamento bibliográfico referente as ferramentas utilizadas; e (iii) listagem junto a empresa quanto aos problemas e necessidades de correção no uso da rede sem fio.

Na sequência, com essas informações, realizou-se estudos junto aos fabricantes dos materiais, para entendimento das configurações e validação de compatibilidade ao protocolo 802.1x, tendo como objetivo conhecer as melhores práticas para as configurações.

Após a validação das ferramentas e compatibilidades, realizou-se configurações em um ambiente restrito ao TI, ambiente de homologação, com objetivo de atestar o entendimento quanto as configurações.

Com a confirmação de funcionamento, o procedimento foi documentado e a última etapa teve início. Foi realizada a configuração do ambiente de produção, e os *feedbacks* foram coletados junto a empresa.

4 RESULTADOS

Este capítulo apresenta o resultado da realização do trabalho. Inicialmente, apresenta-se a instalação dos serviços de acesso e políticas de rede. Na sequência tem-se as configurações das políticas de rede. E por fim, os *feedbacks* coletados junto a empresa.

4.1 INSTALAÇÃO DOS SERVIÇOS DE ACESSO E POLITICAS DE REDE

1) Iniciou-se a configuração do ambiente de produção adicionando funções e recursos no *Server Manager*, encontrada no painel inicial, conforme Figura 9.

Figura 9 - Adicionamento de funções e recursos
Fonte: CISS Software e Serviços (2018).

2) No menu “Tipo de Instalação”, deixou-se a opção “Instalação baseada em função ou recurso” selecionada, como apresenta a Figura 10.

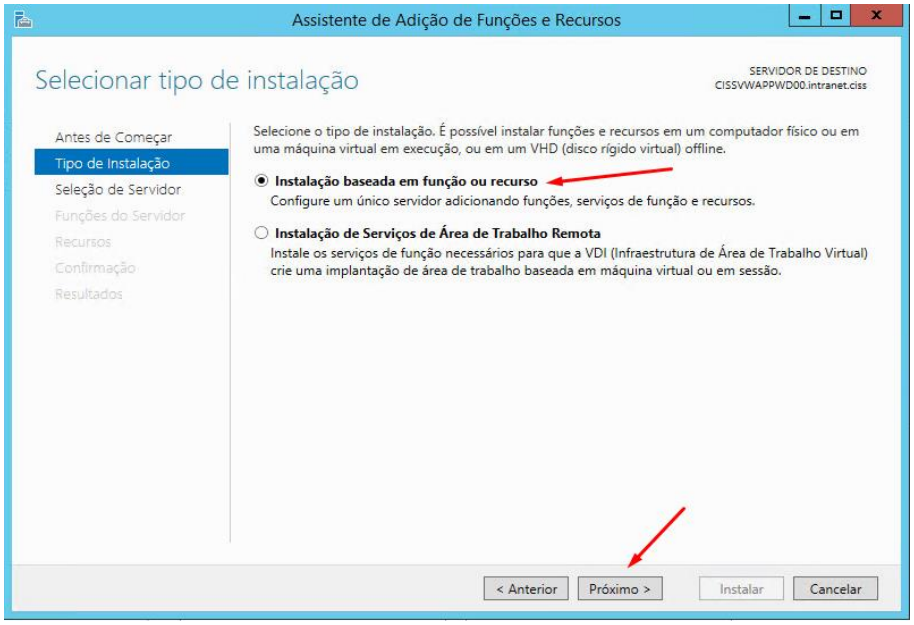

Figura 10 - Tipo de instalação a selecionar
Fonte: CISS Software e Serviços (2018).

3) Na sequência, no menu "Seleção de servidor", optou-se por "Selecionar um servidor em *pool* de servidor" e entre os servidores disponíveis, escolheu-se em qual servidor se instalaria o RADIUS, como mostrado na Figura 11.

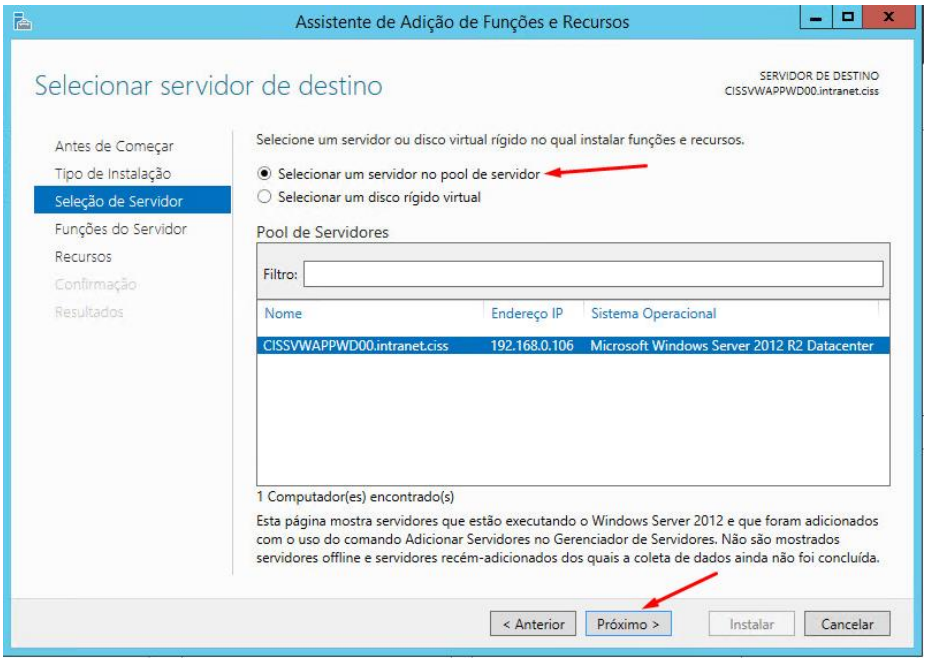

Figura 11 - Seleção do servidor que será instalado o RADIUS
Fonte: CISS Software e Serviços (2018).

4) Em “Funções do Servidor”, marcou-se a opção “Serviços de Acesso e Política de Rede”, como mostrado na Figura 12, e em “Recursos”, deixou-se o modo padrão, mostrado na Figura 13.

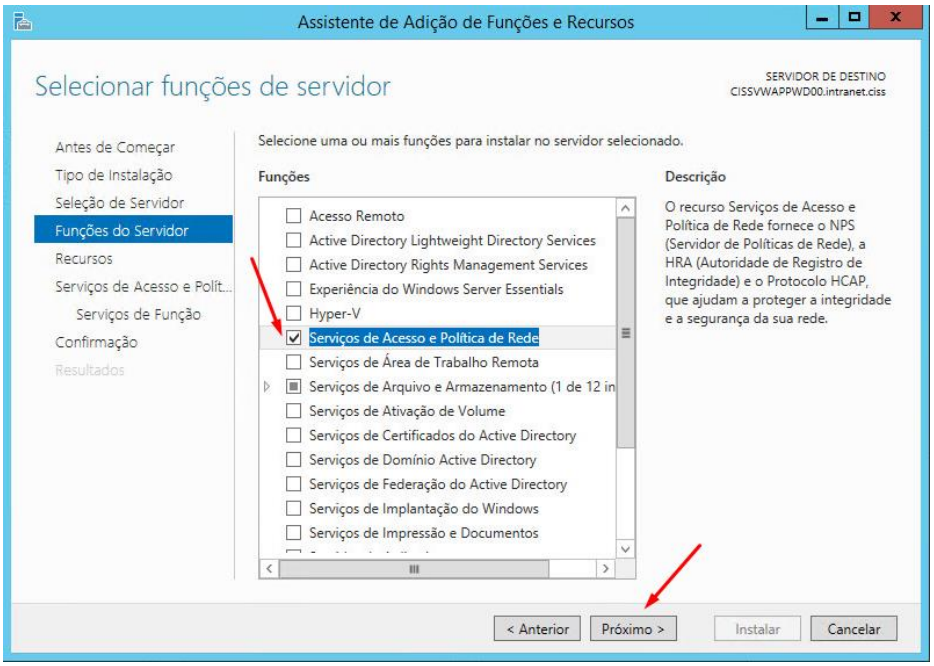

Figura 12 - Funções do servidor
Fonte: CISS Software e Serviços (2018).

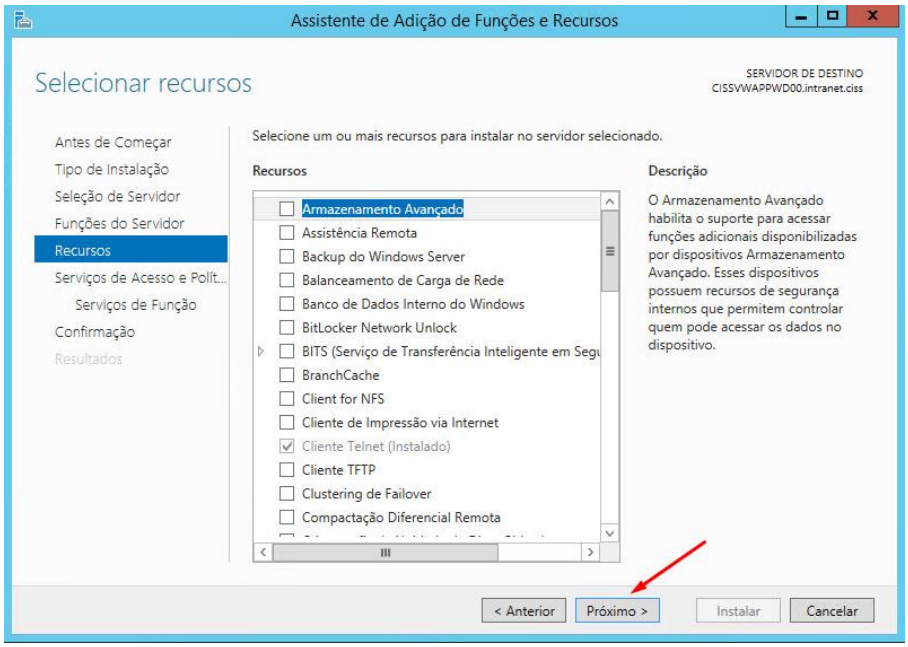

Figura 13 - Seleção de recurso modo padrão
Fonte: CISS Software e Serviços (2018).

5) Já em “Serviços de Função”, marcou-se a opção “Servidor de políticas de rede”, que se trata de um NPS que permite criar políticas de acesso, como apresentado na Figura 14.

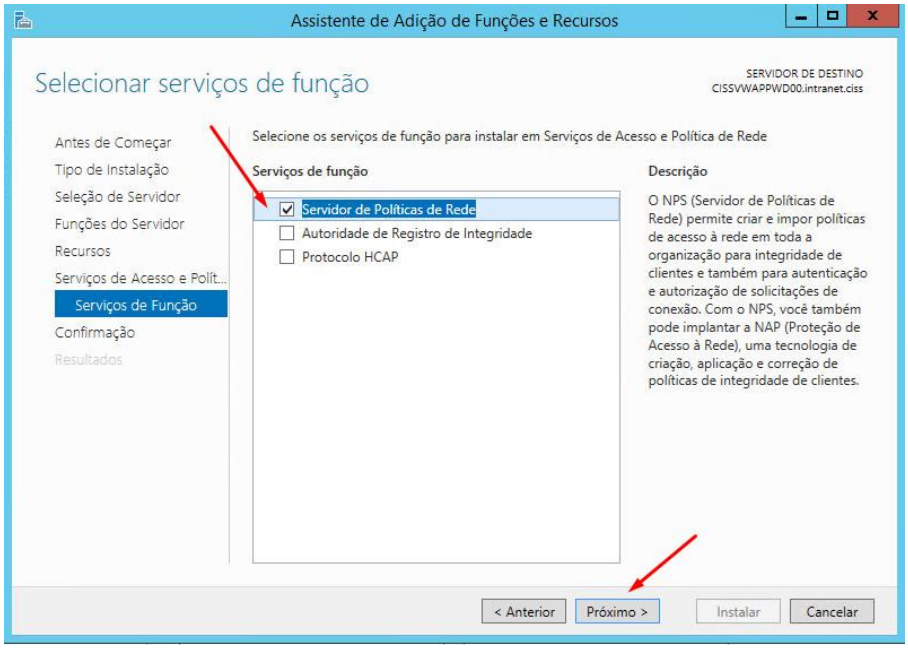

Figura 14 - Serviços de Função
Fonte: CISS Software e Serviços (2018).

6) No menu “Confirmação”, selecionou-se a opção “Reiniciar cada servidor de destino automaticamente”, e clicou-se em “sim” para o “Assistente de Adição de Funções e Recursos” e por fim instalou-se o RADIUS, mostrado na Figura 15.

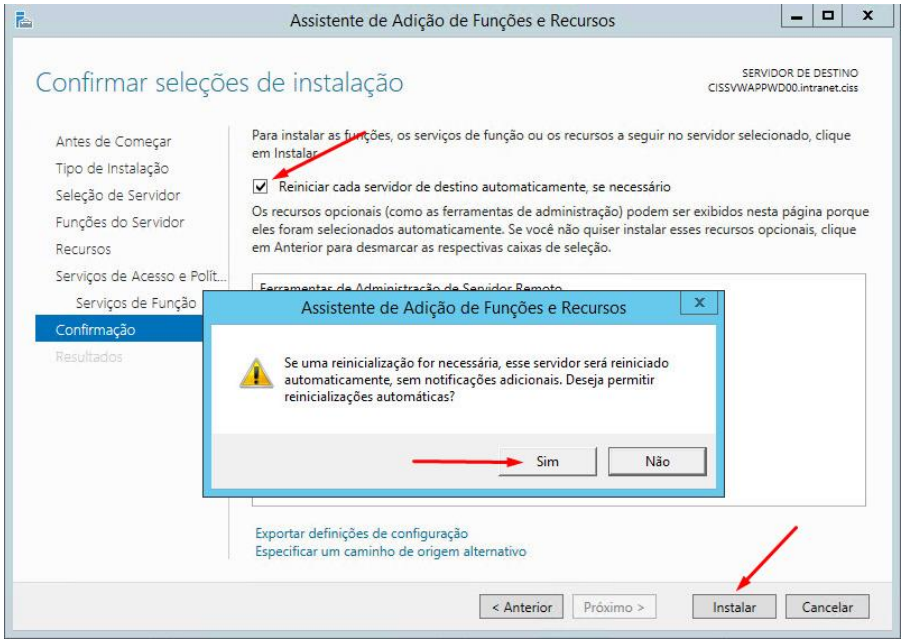

Figura 15 - Confirmação de seleções de instalação
Fonte: CISS Software e Serviços (2018).

7) Após o aguardo do fim da instalação, se reiniciou o servidor. As figuras 16 e 17 apresentam o andamento deste processo.

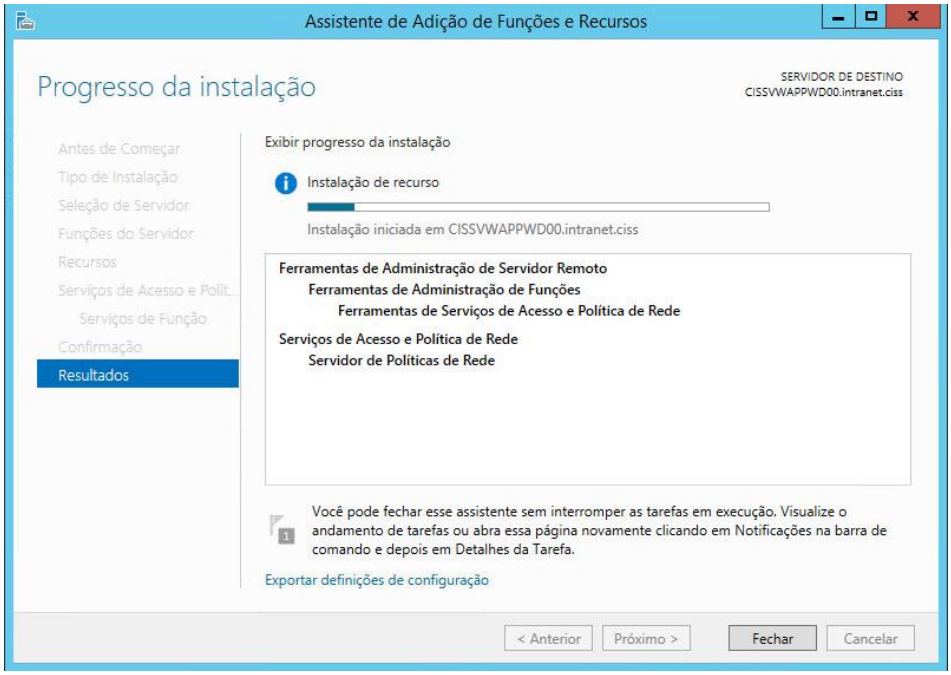

Figura 16 – Progresso de instalação dos Serviços de Acesso e Política de Rede
Fonte: CISS Software e Serviços (2018).

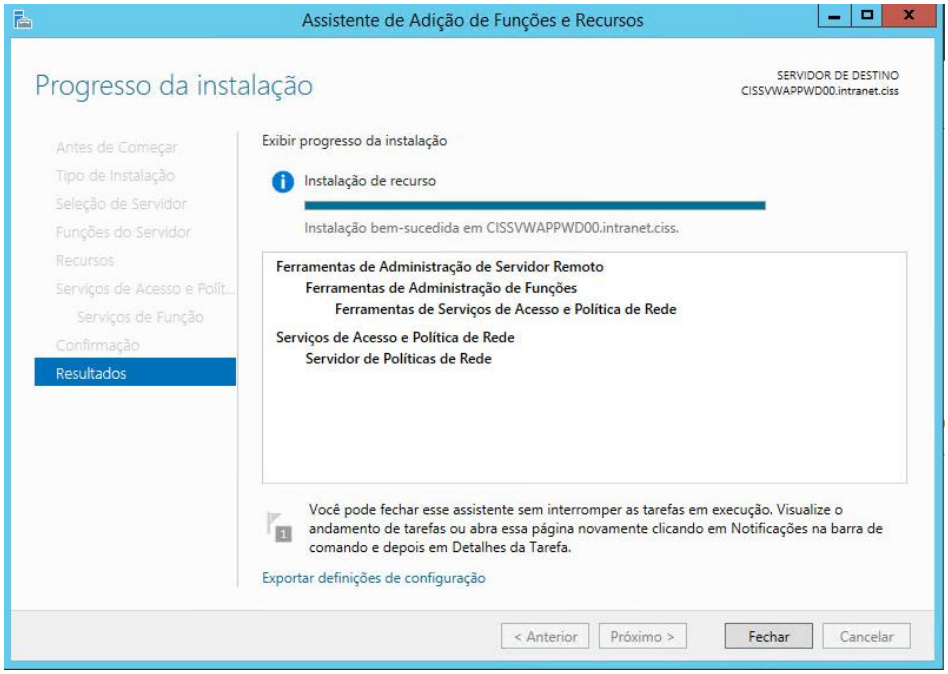

Figura 17 - Fim da instalação do serviço e reinicialização do servidor
Fonte: CISS Software e Serviços (2018).

8) Na sequência, na janela “Gerenciador do Servidor”, no menu “NAP”, tem-se uma opção de servidor. Com o botão direito do mouse sobre este servidor, selecionou-se os “Servidores de Políticas de Rede”, mostrado na Figura 18.

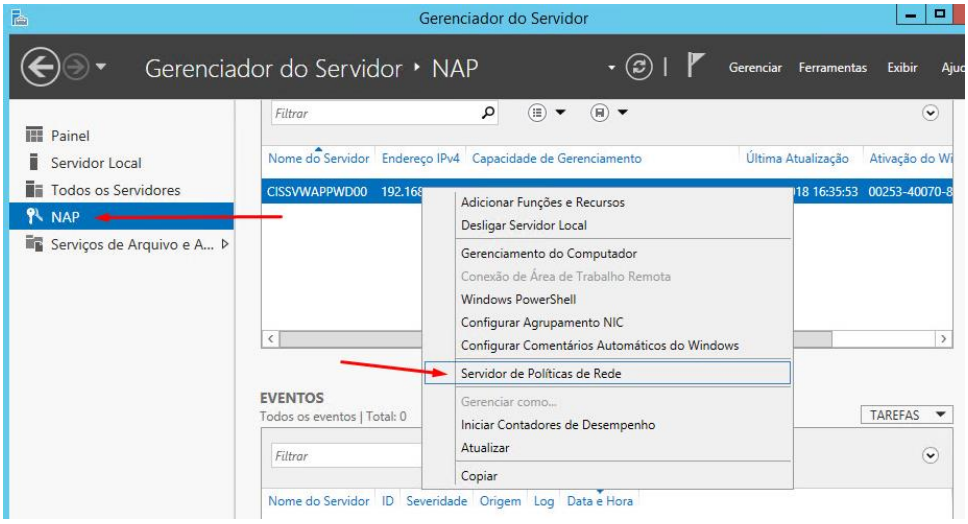

Figura 18 - Gerenciador de Servidor NAP
Fonte: CISS Software e Serviços (2018).

9) Na nova janela que se abriu, selecionou-se o separador “Clientes RADIUS” para criar um novo cliente, mostrado na Figura 19.

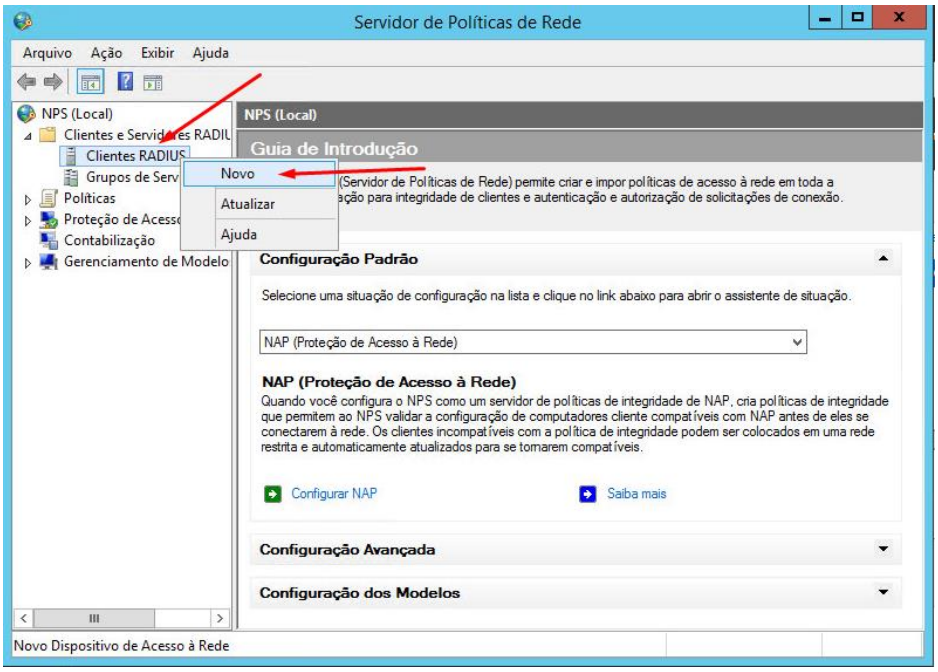

Figura 19 - Criação de novo cliente RADIUS
Fonte: CISS Software e Serviços (2018).

10) Em seguida, configurou-se com as seguintes informações: Nome amigável, endereço de IP do equipamento adicionado e palavra-chave que será compartilhada entre o servidor e seu equipamento de rede, neste caso, a própria controladora, mostrado na Figura 20.

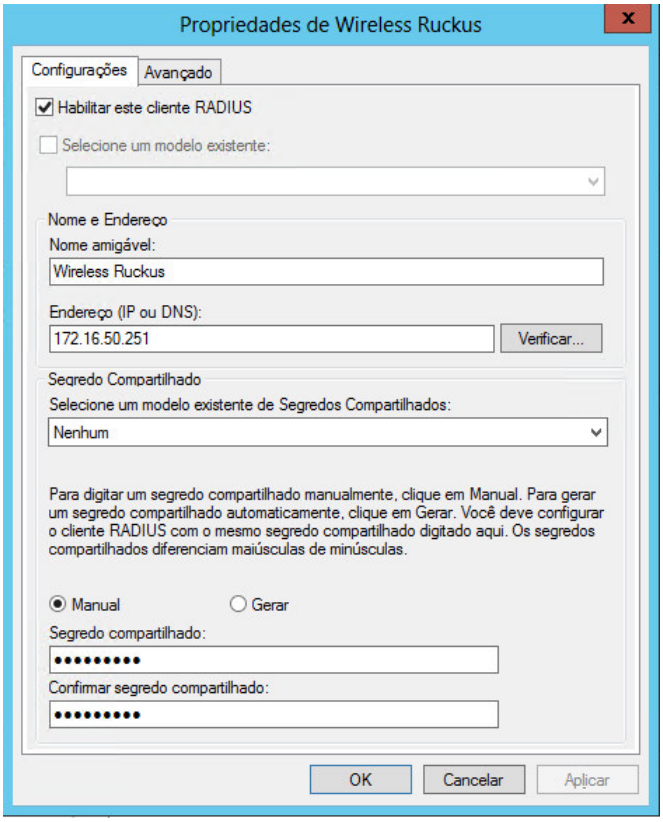

Figura 20 - Configuração de informação de cliente RADIUS
Fonte: CISS Software e Serviços (2018).

11) No NPS (Local), a opção selecionada foi “Servidor RADIUS para conexões 802.1x com/sem fio”, mostrado na Figura 21.

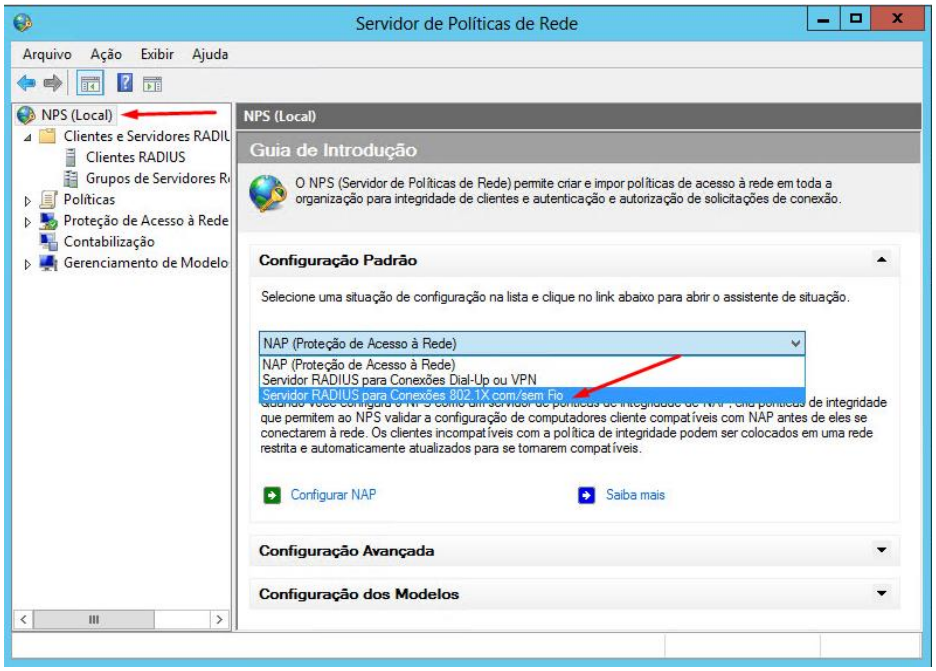

Figura 21 - Seleção do servidor RADIUS para conexões 802.1X
Fonte: CISS Software e Serviços (2018).

12) Após, iniciou-se a configuração do 802.1X. O tipo de conexão selecionada foi a conexão sem fio segura, conforme apresentado nas Figuras 22 e 23.

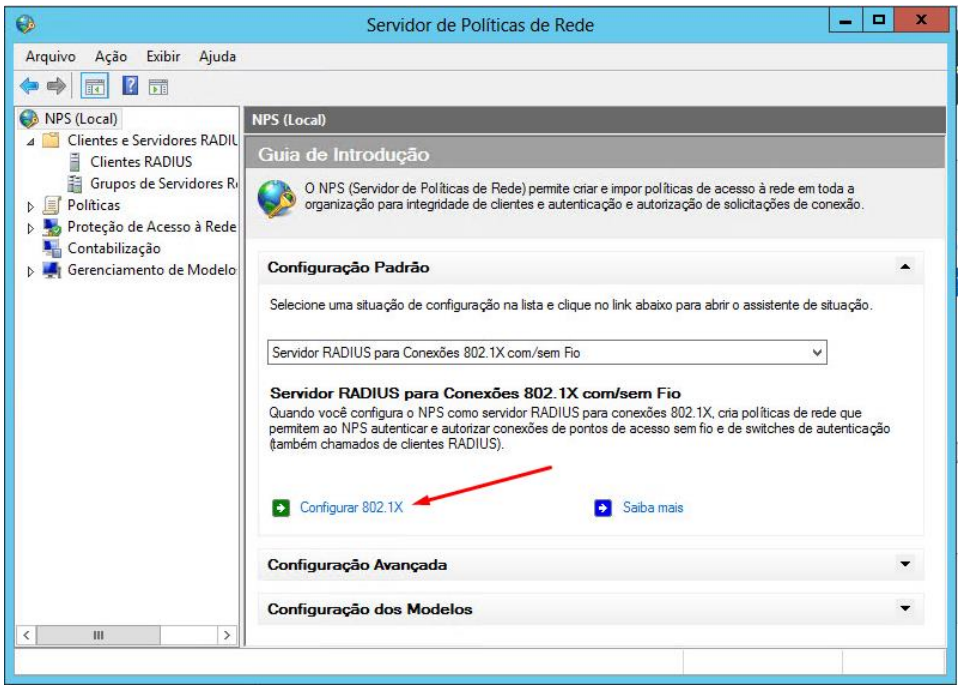

Figura 22 - Configuração do 802.1X
Fonte: CISS Software e Serviços (2018).

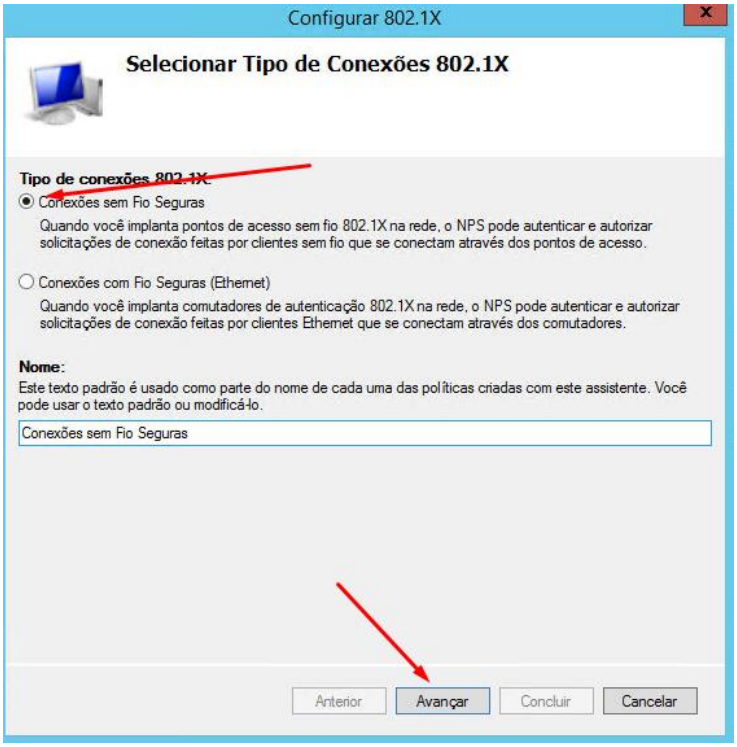

Figura 23 - Seleção do tipo de conexão 802.1X
Fonte: CISS Software e Serviços (2018).

13) Na nova janela que se abriu, selecionou-se o cliente RADIUS, já configurado anteriormente, como mostrado na Figura 24.

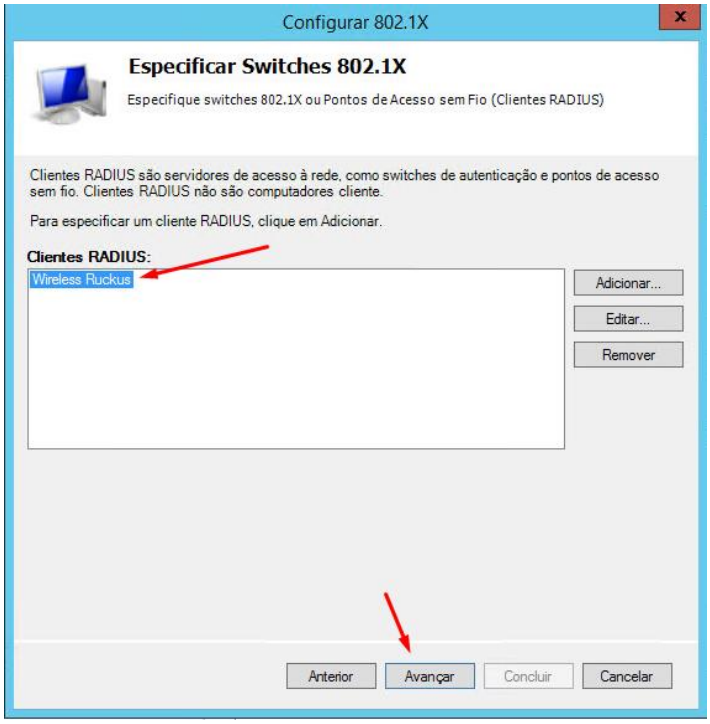

Figura 24 - Seleção do cliente RADIUS já configurado
Fonte: CISS Software e Serviços (2018).

14) Na sequência, a política de autenticação selecionada foi a “Microsoft: EAP protegido (PEAP)”, mostrado na Figura 25.

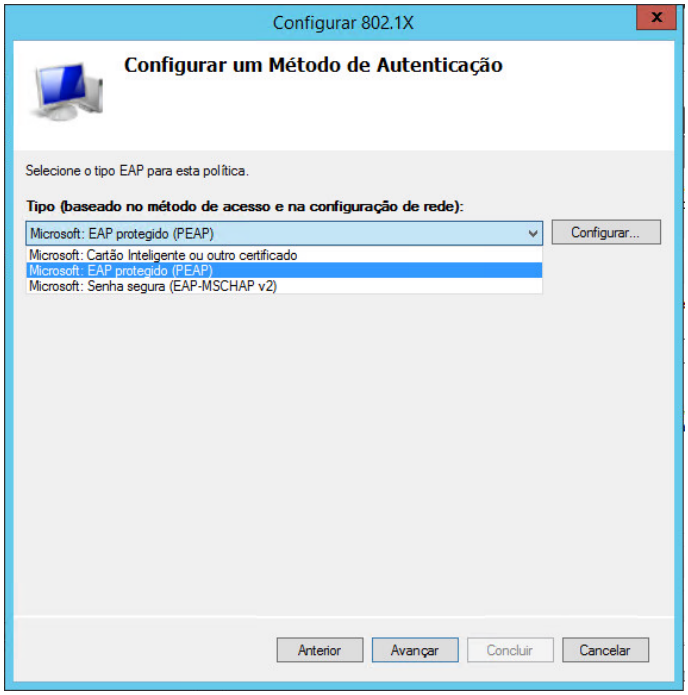

Figura 25 - Seleção do tipo de EAP para a política
Fonte: CISS Software e Serviços (2018).

15) Selecionou-se o grupo que teria acesso (grupo criado no *Active Directory*), como apresentado na Figura 26. Avançou-se para as próximas etapas e o mesmo estava configurado.

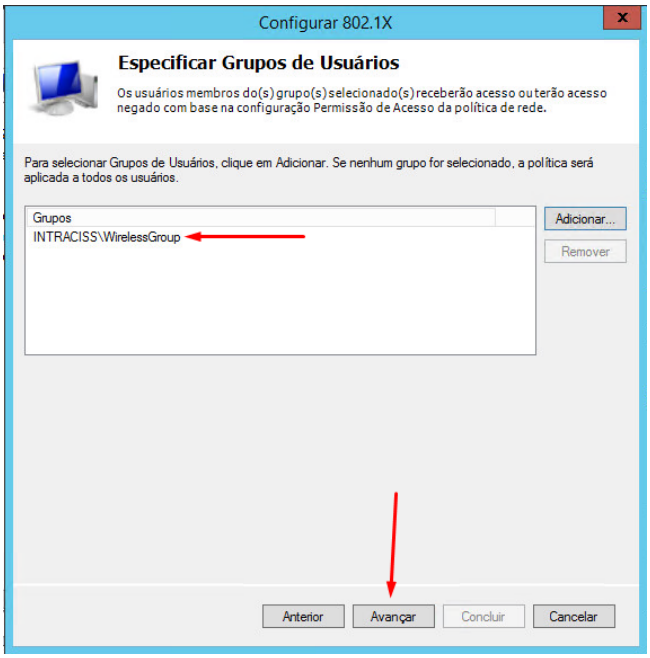

Figura 26 - Grupos de usuários com direito a acesso
Fonte: CISS Software e Serviços (2018).

4.2 CONFIGURAÇÃO DAS POLÍTICAS DE REDE

1) Com a instalação anterior completa, iniciou-se a configuração de Políticas de Solicitação de Conexão, criando-se uma nova política, como mostrado na Figura 27.

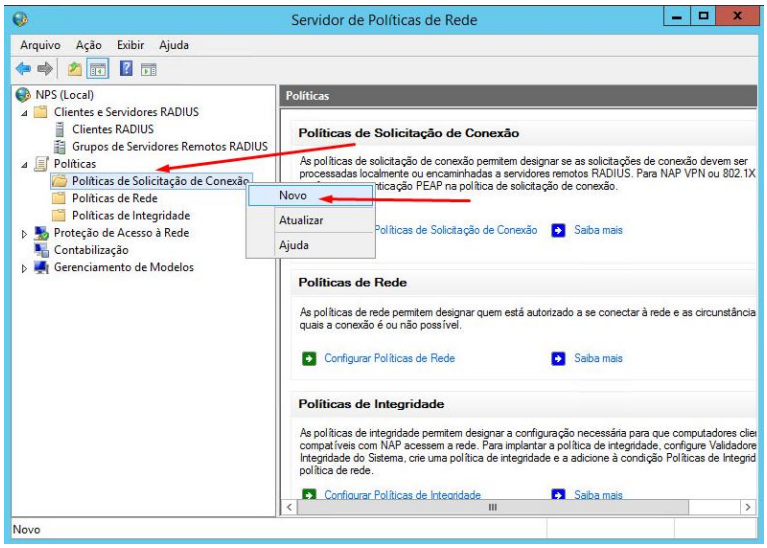

Figura 27 - Criação de uma nova Política de Solicitação de Conexão
Fonte: CISS Software e Serviços (2018).

Em outra janela, tem-se as guias visão geral, condições e configurações. As especificações utilizadas em cada uma estão a seguir nas Figuras 28, 29 e 30.

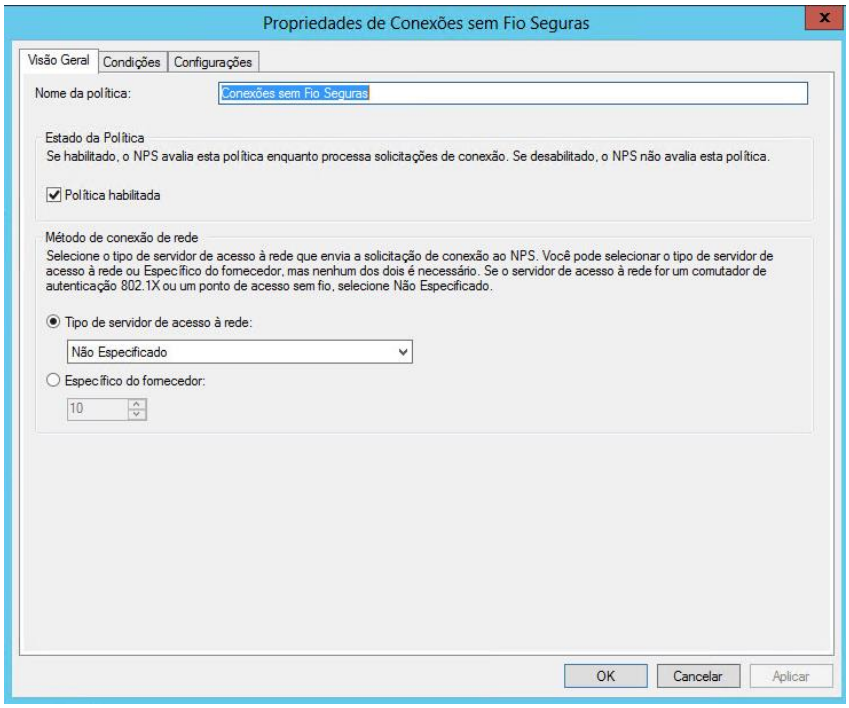

Figura 28 - Configurações na guia Visão Geral
Fonte: CISS Software e Serviços (2018).

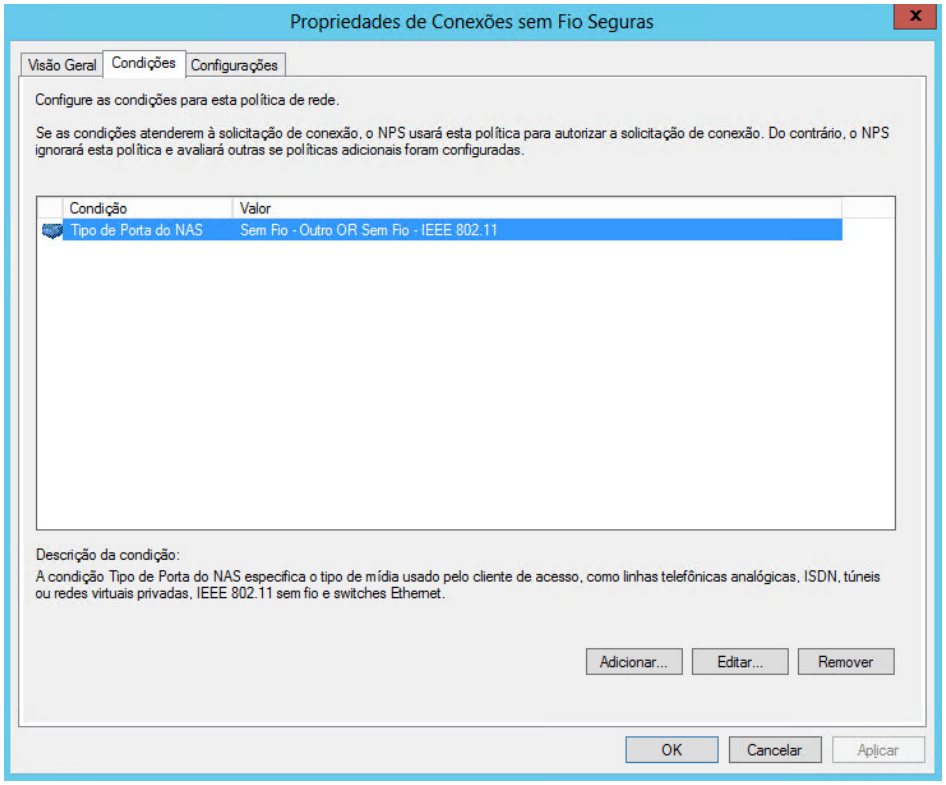

Figura 29 - Configurações na guia Condições
Fonte: CISS Software e Serviços (2018).

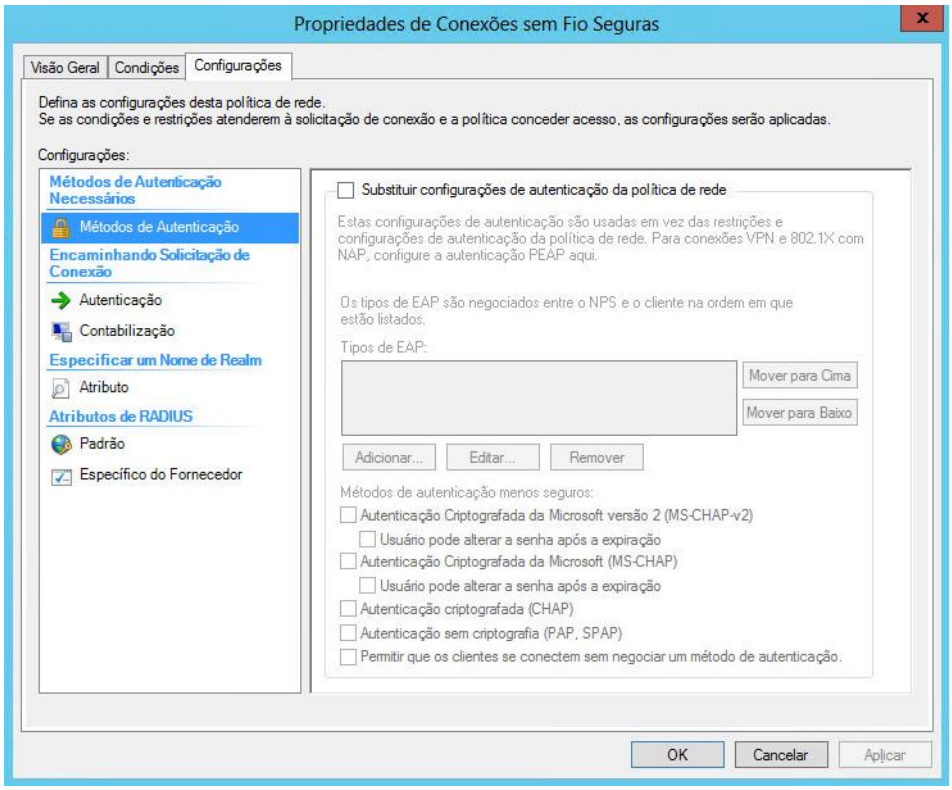

Figura 30 - Configurações na guia de Configurações
Fonte: CISS Software e Serviços (2018).

2) Na nova janela aberta, na guia da visão geral, a nova política foi criada, conforme apresentado na Figura 31.

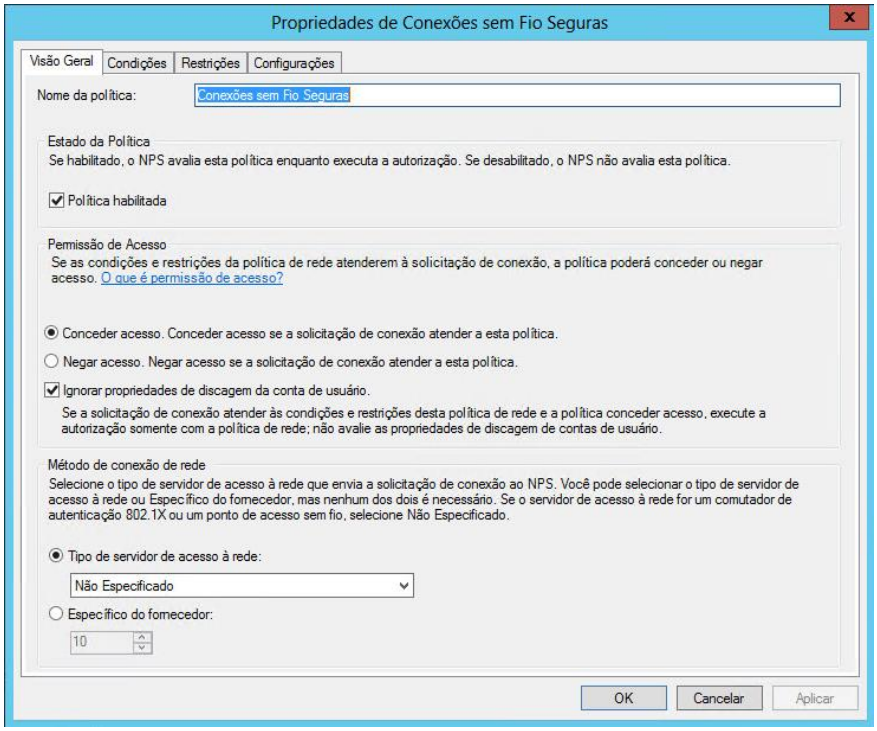

Figura 31 - Criação de nova política de conexões sem fio seguras
Fonte: CISS Software e Serviços (2018).

3) Adicionou-se o grupo do *Active Directory* que contém os usuários que se autenticarão e o configurou, conforme as Figuras 32, 33 e 34.

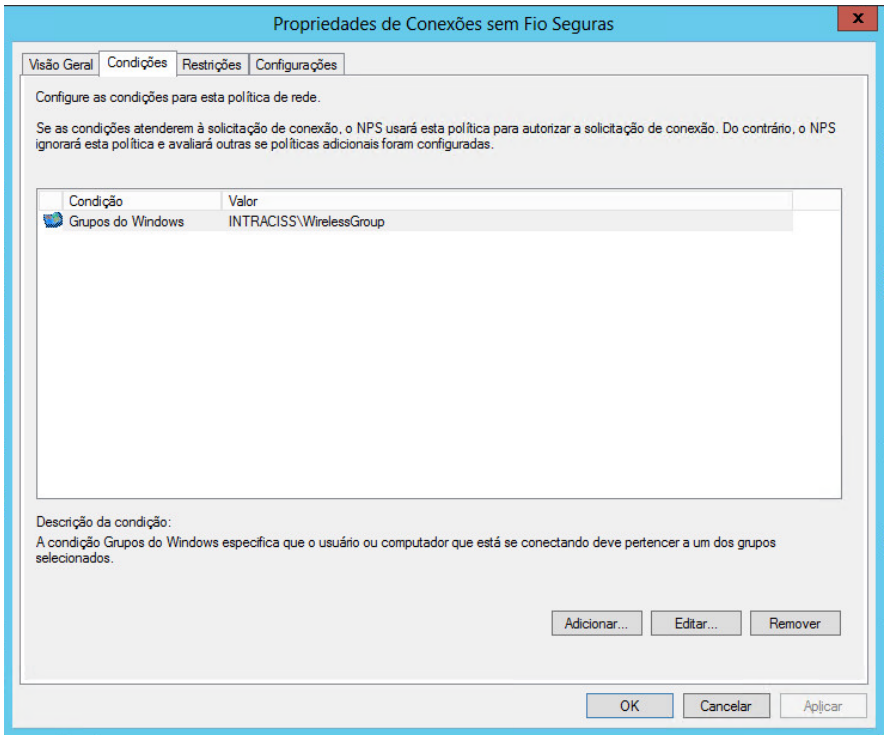

Figura 32 – Configuração das condições do *Active Directory*
Fonte: CISS Software e Serviços (2018).

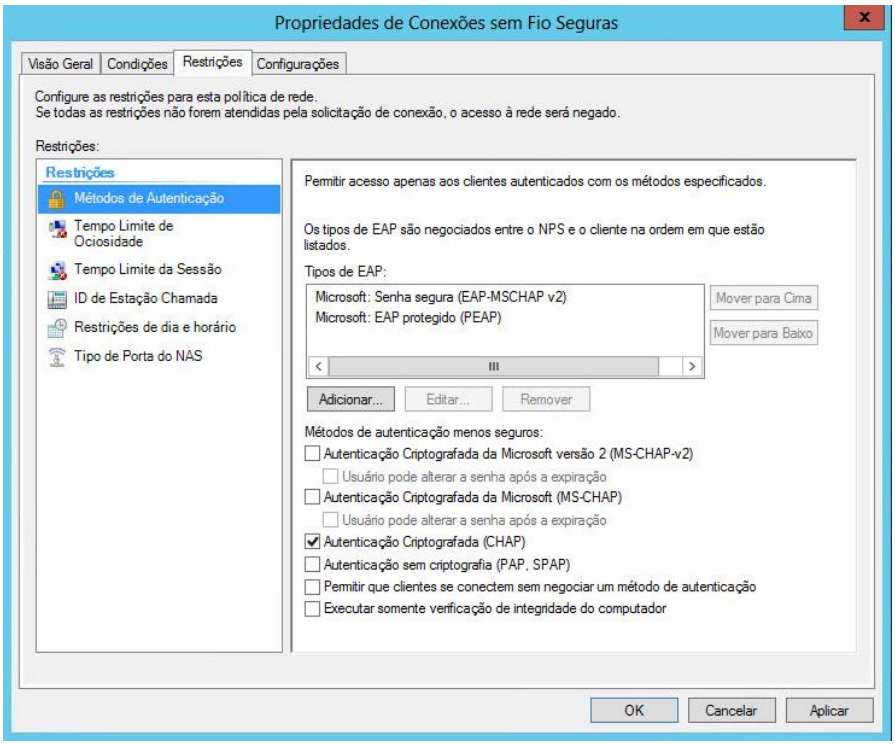

Figura 33 – Configuração das restrições do *Active Directory*
Fonte: CISS Software e Serviços (2018).

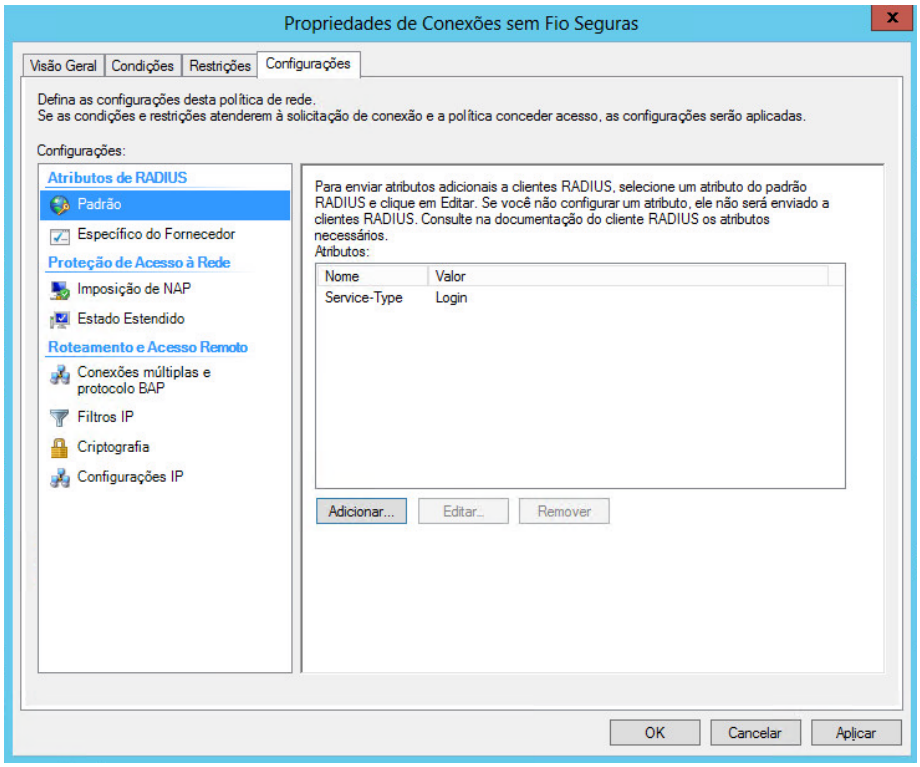

Figura 34 – Configuração do *Active Directory*
Fonte: CISS Software e Serviços (2018).

4) Para a configuração da Controladora Ruckus sem fio, acessou-se a mesma e criou-se um novo servidor de autenticação, conforme apresentado nas Figuras 35 e 36.

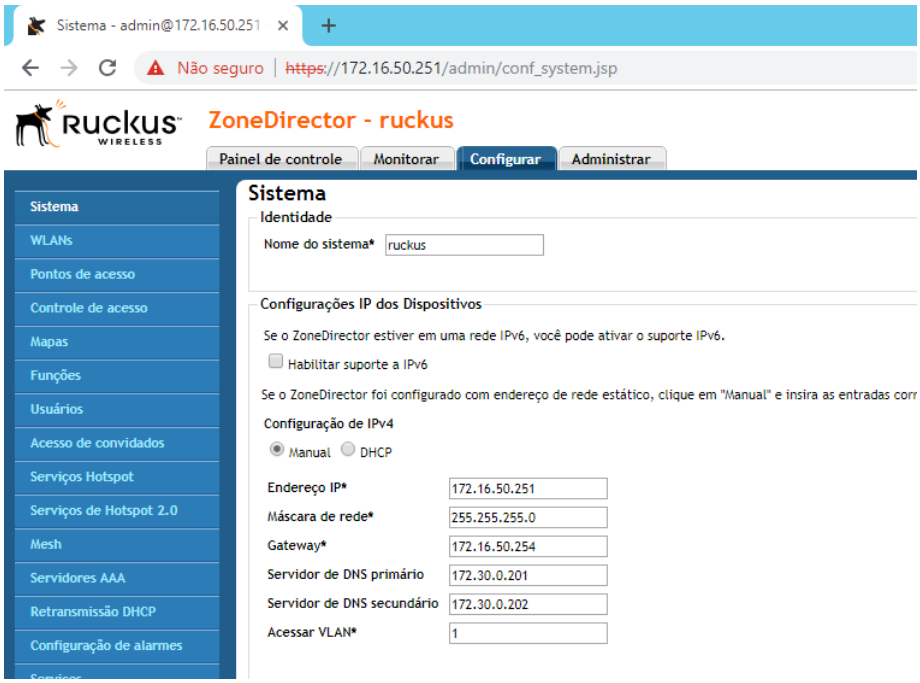

Figura 35 – Acesso a controladora Ruckus
Fonte: CISS Software e Serviços (2018).

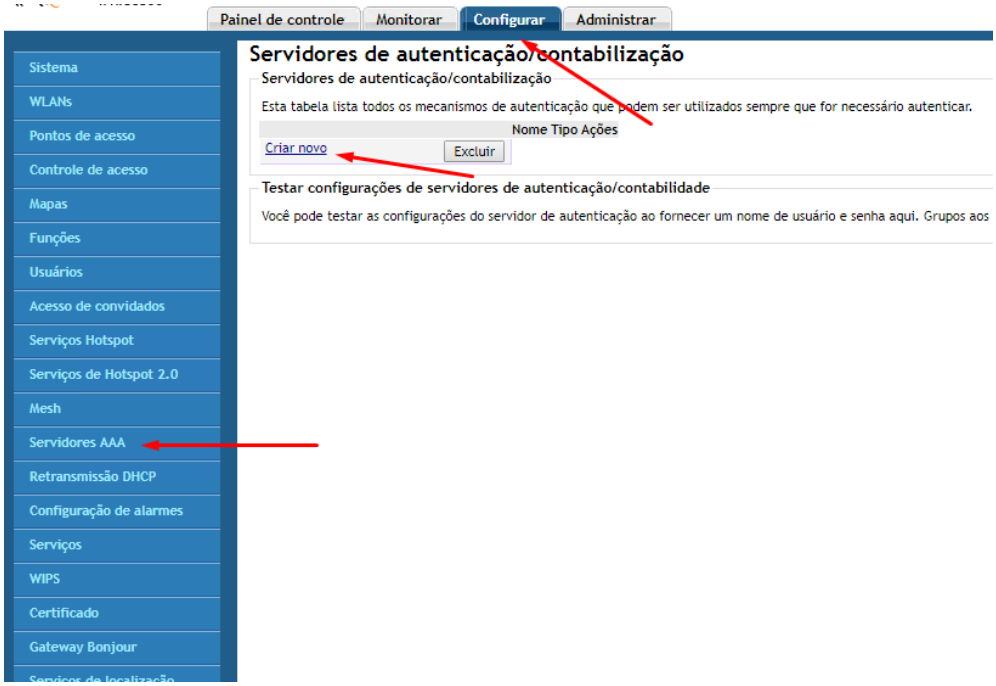

Figura 36 – Configuração da controladora Ruckus
Fonte: CISS Software e Serviços (2018).

5) Preencheu-se os campos de nome, tipo, método de autenticação, endereço de IP, porta, palavra-chave, tempo limite de solicitação e número máximo de tentativas, conforme mostrado na Figura 37.

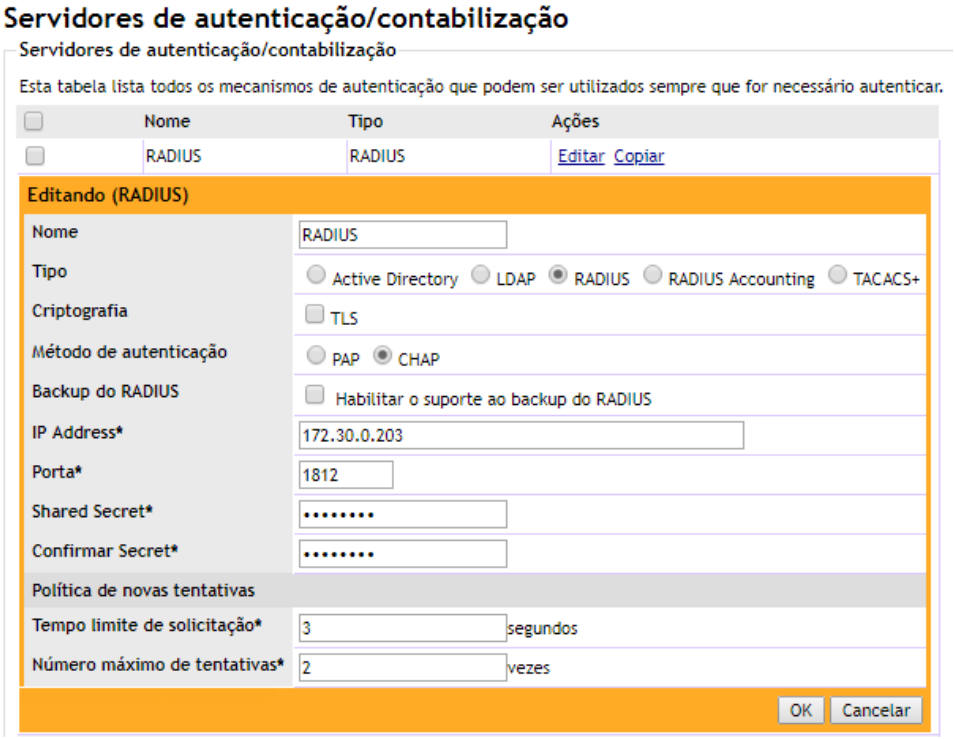

Figura 37 - Configuração dos servidores de autenticação AAA
Fonte: CISS Software e Serviços (2018).

6) Na sequência criou-se uma nova WLAN, mostrado na Figura 38 e a configurou.

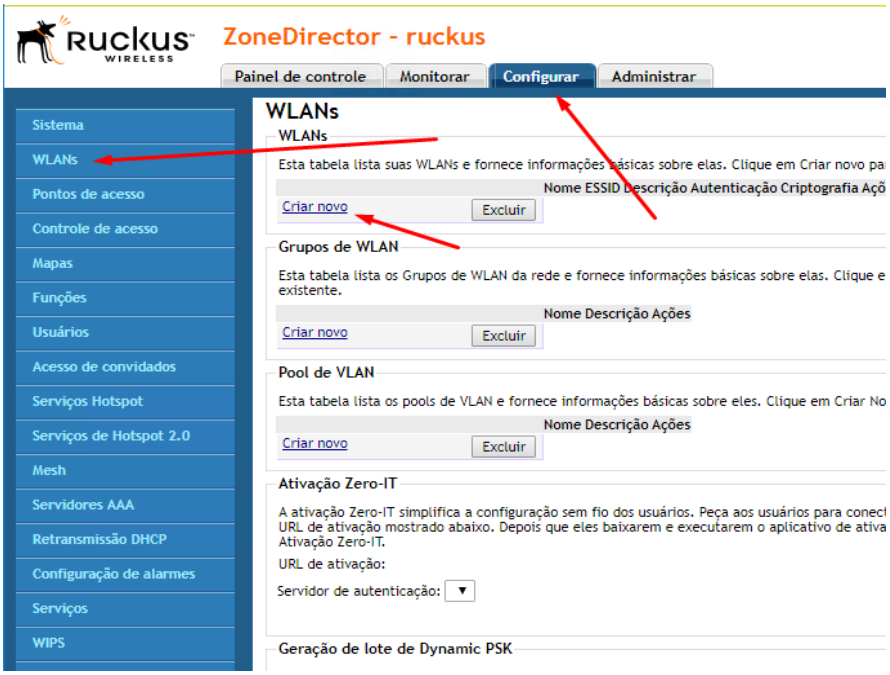

Figura 38 – Criação da nova WLAN
Fonte: CISS Software e Serviços (2018).

7) Para isso preencheu-se os campos: Nome/ESSID, descrição, utilização da WLAN, opções de autenticação, opções de criptografia, servidor e prioridade, conforme apresentado na Figura 39. O servidor selecionado foi o servidor de autenticação/contabilização criado anteriormente.

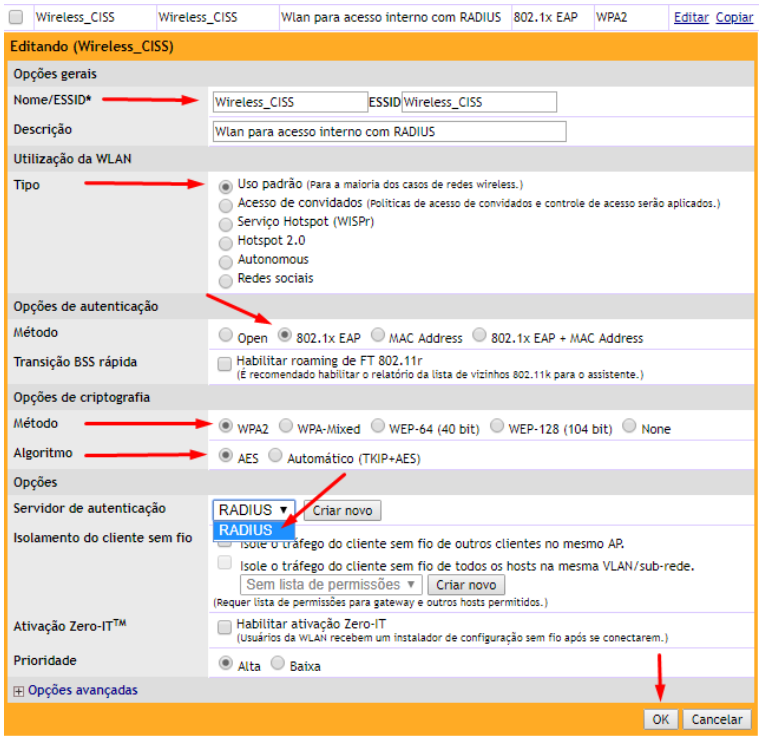

Figura 39 - Configurações da WLAN
Fonte: CISS Software e Serviços (2018).

8) Os pontos de acesso sem fio conectados a controladora receberam as configurações realizadas imediatamente, entregando a nova rede sem fio com autenticação RADIUS nos pontos de acesso.

Os resultados obtidos durante a realização deste estudo garantem que é possível implantar este tipo de autenticação baseada no padrão IEEE 802.1X, utilizando RADIUS como protocolo de autenticação CHAP, como método de autenticação, e uma base de usuários *Active Directory*.

Para diminuir os riscos de acessos não autorizados e reforçar a segurança da rede, o protocolo utilizado foi o 802.1X EAP com método WPA2 e algoritmo AES, como apresentado acima, na Figura 39.

Durante o experimento, se fez necessário validar os materiais utilizados e sua compatibilidade com o protocolo RADIUS. Como sua compatibilidade foi comprovada em laboratório, aplicou-se o mesmo no ambiente de produção e obteve-se êxito, conforme apresentado nas Figuras 40, 41 e 42.

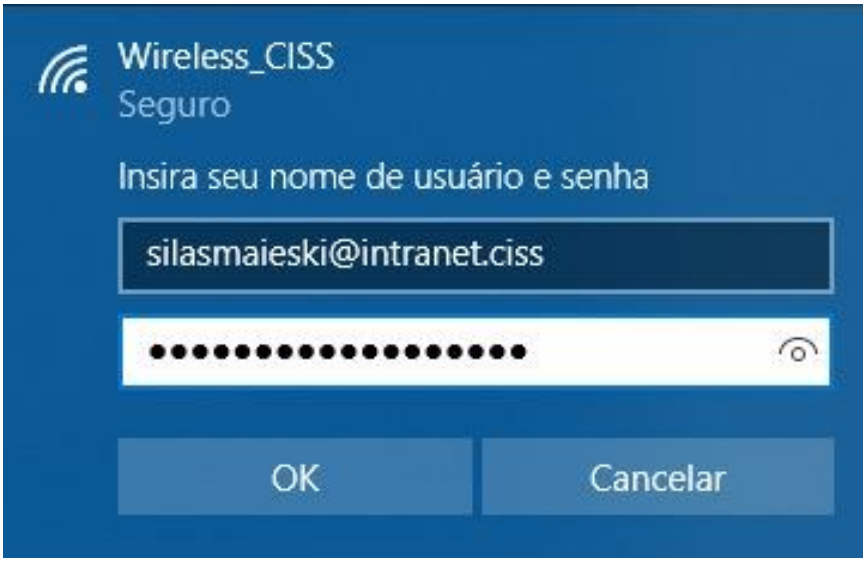

Figura 40 - Login de acesso na rede sem fio empresarial
Fonte: CISS Software e Serviços (2018).

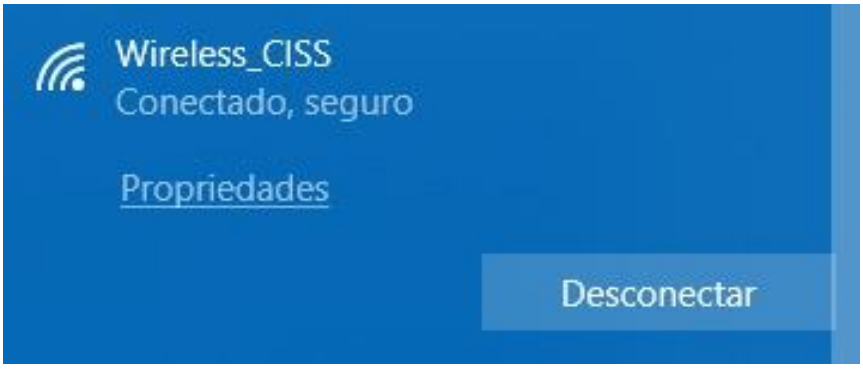

Figura 41 - Conexão na rede sem fio empresarial
Fonte: CISS Software e Serviços (2018).

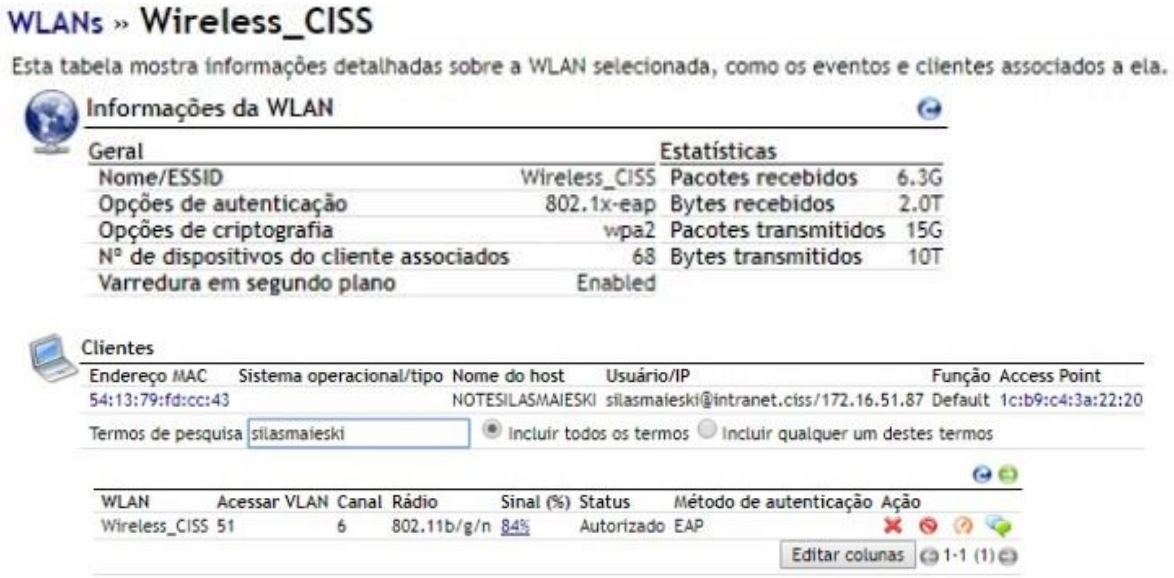

Figura 42 – Usuários conectados na WLAN empresarial
Fonte: CISS Software e Serviços (2018).

Uma vantagem observada é a possibilidade de criação de redes sem fio com maior facilidade, podendo implementá-las em áreas dinâmicas da empresa. Isto ocasiona melhor gestão de permissão e liberação de acesso. A liberação de acesso foi feita através do grupo *WirelessGroup* criado no *Active Directory* e atribuído nas configurações da política de rede. Os usuários que pertencem a esse grupo possuem permissão de acesso. Na empresa todos os colaboradores possuem usuário e senha individuais. Com essas credenciais, realizou-se a autenticação. Um exemplo disto foi um evento realizado por um número específico de colaboradores por um determinado período, onde criou-se uma nova e temporária rede *sem fio* para uso dos mesmos. Na conclusão do evento, esta rede foi removida.

Para usuários convidados, fornecedores ou clientes a empresa possui uma rede sem fio exclusiva. Essa rede tem apenas acesso à Internet e tem sua autenticação realizada via *voucher* disponibilizado pós cadastro de dados pessoais, não fazendo parte deste estudo.

Outra vantagem observada foi a facilidade de implementar controle de banda em redes temporárias, como a citada anteriormente, calculando-se o número de usuários que a utilizaram. Com a implantação do protocolo, conseguiu-se um melhor desempenho no uso da rede sem fio, que foi comprovada através do parecer dos usuários e do registro de *tickets* de problemas relacionados a rede sem fio a partir do mês de agosto, conforme Figura 43, pois apenas usuários com permissão conseguiram utilizá-la, diminuindo consequentemente a concorrência pelo *link*.

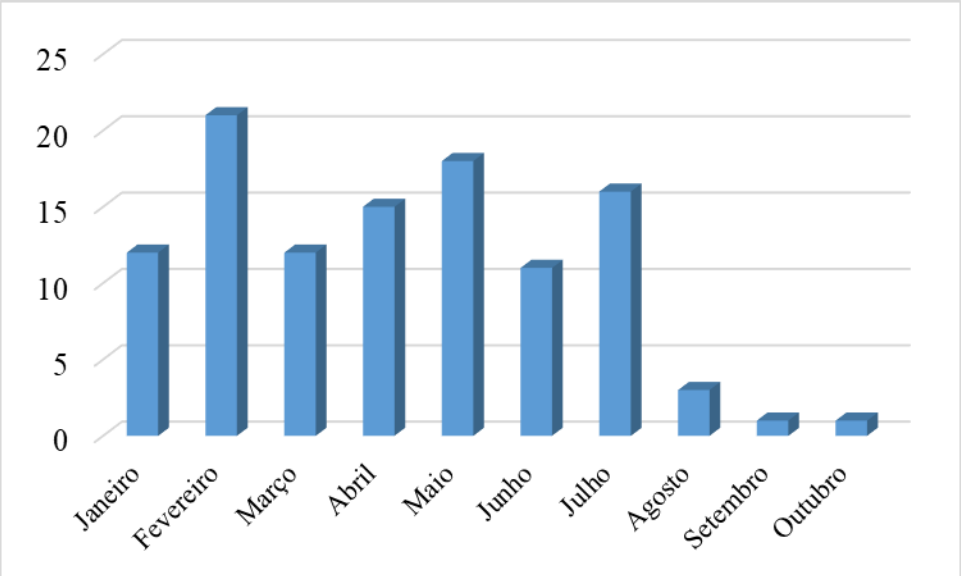

Figura 43 - Relatório de *Tickets* - Problemas de rede sem fio no ano de 2018
Fonte: CISS Software e Serviços (2018).

Em conexões onde o usuário foi autorizado, a autenticação RADIUS permitiu acesso apenas aos servidores e serviços onde seu usuário já era previamente autorizado, respeitando assim a autenticação do ambiente já controlado por controlador de domínio.

Um exemplo das políticas de acesso implantadas, são as configuradas no servidor de arquivos que está integrado ao mesmo domínio que o RADIUS. Nesse servidor, grupos ou usuários específicos foram liberados com permissão de acesso em diretórios de cada área, semelhante a liberação que é realizada no grupo *WirelessGroup* para uso da rede sem fio. As figuras 44 e 45 apresentam o diretório Fabrica, liberado para acesso aos grupos USR Fabrica e FabricaLeitura. Quando o usuário do grupo *WirelessGroup* conecta-se à rede sem fio, o mesmo estando liberado em um dos grupos citados anteriormente, automaticamente possui acesso ao diretório Fabrica.

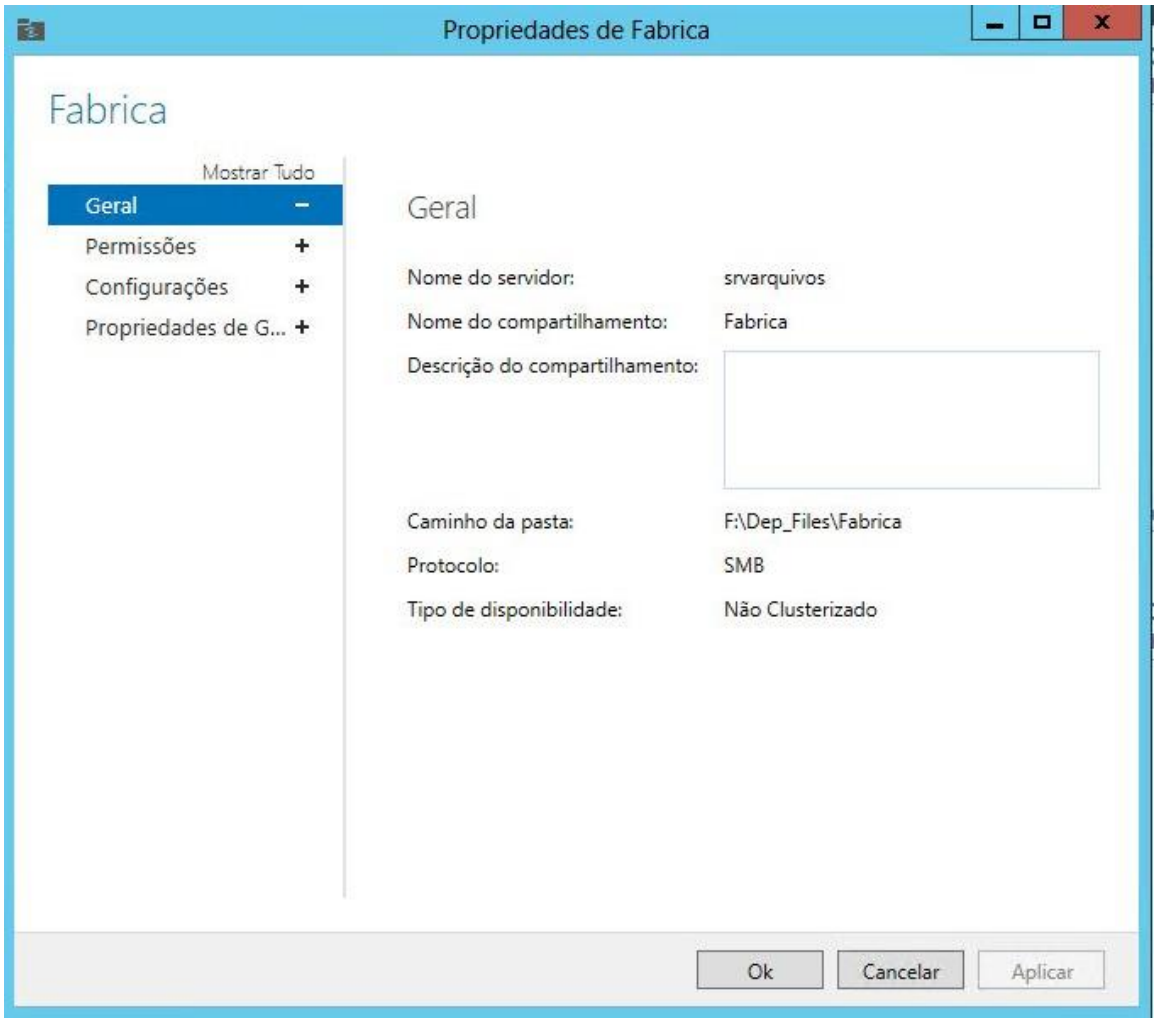

Figura 44 – Diretório Fábrica do servidor de arquivos
Fonte: CISS Software e Serviços (2018).

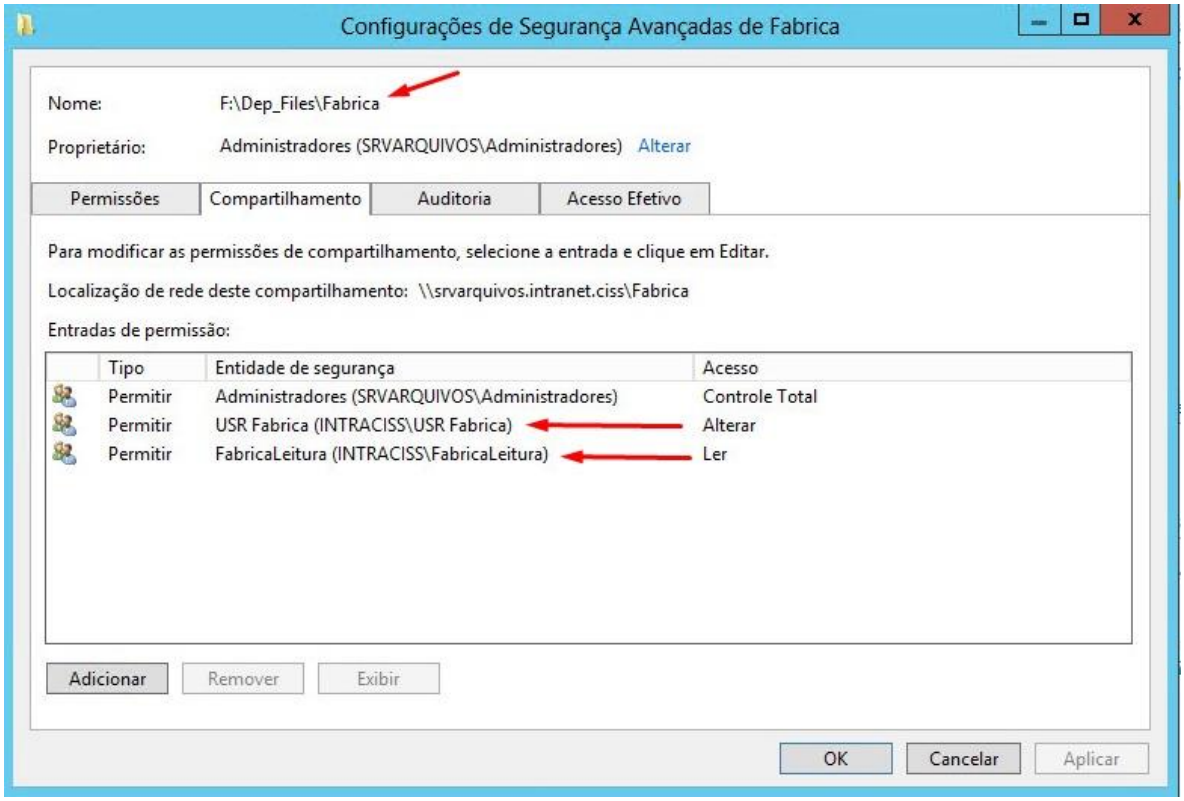

Figura 45 – Configurações de segurança do diretório Fábrica no servidor de arquivos
Fonte: CISS Software e Serviços (2018).

5 CONCLUSÕES

Este trabalho teve como objetivo propor uma solução para o problema de autenticação de usuários em redes sem fio, porém, a autenticação segura é apenas um dos controles de segurança que devem ser adotados.

Alguns pontos a serem testados no experimento foram: garantia de confiabilidade de acesso à rede sem fio empresarial, autenticação de usuários no momento da sua conexão, implantação de políticas de acesso à rede e monitoramento do acesso de cada um destes usuários autenticados. Estes procedimentos foram testados utilizando o protocolo 802.1X com servidor RADIUS.

Pode-se concluir, através do estudo de caso deste experimento, que o RADIUS se trata de um protocolo confiável, seguro e estável, auxiliando na gestão da TI, facilitando e assegurando um melhor uso da rede sem fio.

O RADIUS melhorou o desempenho no uso da rede sem fio, quando comparado a utilização antes de sua implantação, pois limitou o acesso somente aos usuários autorizados. Desta forma o consumo de *link* não concorreu com usuários não autorizados, o que, no antigo padrão utilizado, era um problema, pois as credenciais de acesso eram compartilhadas.

O RADIUS autenticou com o *Active Directory* e recebeu as políticas do domínio, sendo, desta forma, necessária a troca da senha periodicamente, respeitando complexidade estabelecida da mesma.

A confiabilidade foi garantida através de grupo específico *WirelessGroup*, atribuído nas configurações de política de rede, configurado para permissão de acesso, sendo este grupo de total controle e gestão da equipe de TI da empresa. Esta permissão de acesso respeitou as políticas do controlador de domínio, dessa forma, a política de acesso à rede ficou de acordo com o papel de cada usuário.

Antes da implantação do RADIUS, as senhas eram compartilhadas entre todos os usuários e não se permitia um monitoramento. Após a implantação, o monitoramento tornou-se possível pois na *dashboard* da controladora sem fio pôde-se identificar usuários e dispositivos conectados, conforme apresentado na **Figura 42**.

Para trabalhos futuros sugere-se a configuração de Listas de Controle de Acesso, com restrições por sistemas operacionais ou modelos de equipamentos. Também, sugere-se a integração da rede cabeada com a autenticação RADIUS.

REFERÊNCIAS

ABREHA, Meareg. **History and implementation of IEEE 802 security architecture. Department of Computer Science, Addis Ababa University**, Addis Ababa, Ethiopia. Disponível em: <http://www.standardsuniversity.org/wp-content/uploads/History-and-implementation-of-the-IEEE-802-security-architecture-Abreha.pdf> Acesso em: 20 set. 2018.

AGUIAR, P.A. F. **Segurança em Redes WI-FI.** Montes Claros, MG. Universidade Estadual de Montes Claros, 2005, 79p. Monografia defendida para obtenção do grau de Bacharel em Sistemas de Informação.

ANDRADE, Tiago Pedroso da Cruz. **Integração de Redes de Sensores sem Fio com tecnologia Rádio-sobre-Fibra**. 2013. 137 p. Dissertação (Mestrado em Ciência da Computação)- Instituto de Computação da Universidade Estadual de Campinas, Campinas, 2013.

ARAUJO NETO, A. C., & SILVA, B. C. **Os novos padrões de segurança em redes wireless**. Universidade Federal do Rio Grande do Sul. 2004.

BARROS,, L. G. and Foltran Junior, D. C. (2008). **Autenticac¸ao ieee 802.1 x em redes de computadores utilizando tls e eap**.

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

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

COSTA, J. d., DA SILVA, J., & DA CRUZ, M. A. (2012)**. Segurança de Redes de Computadores na Internet**. *Revista Inova Ação, 1*, 77-88.

DA SILVA, Renato Lopes. **Tecnologia Wireless**. [S.l.]: Network Technologies, 2008. 8 p.
DERMATINI, Felipe. **WEP, WPA, WPA2: o que as siglas significam para o seu WiFi?** 2013. Disponível em: <https://www.tecmundo.com.br/wi-fi/42024-wep-wpa-wpa2-o-que-as-siglas-significam-para-o-seu-wifi-.htm>. Acesso em: 08 set. 2018.

HPE FlexNetwork 5120 SI Switch Series. Disponível em: <https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5120_SI_Switch_Series.pdf>. Acesso em: 15 set. 2018.

IEEE. **IEEE 802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control.** Disponível em: <https://standards.ieee.org/standard/802_1X-2010.html#Standard>. Acesso em: 19 set. 2018.

INTEL. **Visão geral e os tipos de EAP do 802.1**. 2018. Disponível em: <https://www.intel.com.br/content/www/br/pt/support/articles/000006999/network-and-i-o/wireless-networking.html>. Acesso em: 20 set. 2018.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down**. 5. ed. São Paulo: Person Addison Wesley, Brasil, 2010.

LEHEMBRE, G. (2005). **Wi-Fi security – WEP, WPA and WPA2**. In Proceedings of the 7th Annual International Conference on Mobile Computing and Networking.

MORAIS, Giovane. **Segurança da Informação Através de Autenticação Centralizada por IEEE 802 1x Baseada em Protocolo RADIUS e Base de Dados LDAP Aplicada à Redes Sem Fio**. IN: SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA, 13. 2016, Resende – RJ.

OLIVEIRA, Lucas Vinícius; BEM, Ricardo Orige. **Análise e proposta de melhoria na estrutura de redes sem fio em escolas públicas na microrregião de Araranguá**. 2017. 81 p. Monografia (Bacharel em Tecnologias da Informação e Comunicação)- Universidade Federal de Santa Catarina, Araranguá, 2017.

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

RUCKUS R600**. Pontos de acesso Smart WiFi 802.11ac 3x3:3 dual-band.** Disponível em: <https://ruckus-www.s3.amazonaws.com/pdf/datasheets/ds-ruckus-r600-pt.pdf>. Acesso em: 15 set. 2018.

RUFINO, Nelson Murilo de Oliveira. **Seguranças em Redes sem Fio: Aprenda a proteger suas informações em ambientes wi-fi e bluetooth**. 2. ed. São Paulo: Novatec, 2007. 206 p.
SILVA, Alexandre C. FREITAS, Rogério N. (2013)**. Segurança em redes sem fio**. Faculdade Network. *Revista da Faculdade de Sistemas de Informação, 1*, 4-11.

STANGARLIN, Douglas Pegoraro. **Análise de desempenho de redes sem fio com diferentes protocolos de criptografia: um estudo de caso**. 2012. 77 p. Monografia (Técnologo em Redes de Computadores)- Universidade Federal de Santa Maria, Santa Maria, 2012.

SUKHIJA S.; GRUPTA S. 2012. **Wireless Network Security Protocols A Comparative Study.** International Journal of Emerging Technology and Advanced Engineering [Online]. Volume 2. Disponível: <http://www.ijetae.com/files/Volume2Issue1/IJETAE_0112_61.pdf>. Acesso em: 18 set. 2018.

ULHÔA, Rafael de Sales. **Implementação de 802.1X e RADIUS Integrado ao *Active Directory* e Network Access Protection no CAC/UFG**. 2010. 46 p. Monografia (Bacharelado em Ciência da Computação) - Universidade Federal de Goiás, Catalão - GO, 2010.

VIEIRA, Danielle L. F. G. **IEEE 802.11**. Artigo (B. Sc. em Engenharia de Telecomunicação)- Universidade do Estado do Rio de Janeiro, Rio de Janeiro - RJ, 2004.

VOLLBRECHT, J. et al. **RFC 2904 - AAA Authorization Framework**, 2000.

WI-FI ALLIANCE **Wi-Fi Alliance® introduces security enhancements**. Disponível em <https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements>. Acesso em: 19 set. 2018.

ZONEDIRECTOR™ 1200 Controlador Empresarial Smart Wireless Lan. Disponível em: <https://ruckus-www.s3.amazonaws.com/pdf/datasheets/ds-zonedirector-1200-pt.pdf>. Acesso em: 15 set. 2018.