RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

OPENVPN E SUA APLICAÇÃO EM AMBIENTE EMPRESARIAL

OPENVPN AND ITS APPLICATION IN A BUSINESS ENVIRONMENT

OPENVPN Y SU APLICACIÓN EN UN ENTORNO EMPRESARIAL

Paulo Marcelo Gervasio Fernandes[1], Edimar Soares de Oliveira[1]

e5125992
https://doi.org/10.47820/recima21.v5i12.5992

PUBLICADO: 12/2024

RESUMO

As Redes Privadas Virtuais são essenciais para garantir a comunicação segura em redes públicas. Este estudo apresenta explicações dos protocolos de segurança empregados em VPNs e sua aplicação em ambientes de rede. Inicialmente, o documento define as VPNs e sua relevância na proteção da transmissão de dados em redes vulneráveis. A seguir, explora-se a evolução dessa tecnologia, com foco na evolução dos tradicionais protocolos IPSec e SSL/TLS para versões mais atuais. São avaliados os protocolos de segurança das VPNs, analisando IPSec, SSL/TLS, SHA-256 considerando suas características de segurança, desempenho e adequação para diferentes cenários. Além disso, são discutidas as aplicações das VPNs em contextos atuais, incluindo o acesso remoto, a conectividade entre filiais. O estudo aborda ainda os desafios e as considerações no processo de implantação e gerenciamento de VPNs em redes complexas. Por fim, destaca-se a importância das VPNs para assegurar comunicações seguras nas infraestruturas atuais.

PALAVRAS-CHAVE: VPN. Protocolo. Comunicação segura.

ABSTRACT

Virtual Private Networks are essential to ensure secure communication on public networks. This study presents explanations of the security protocols used in VPNs and their application in network environments. Initially, the document defines VPNs and their relevance in protecting data transmission on vulnerable networks. Next, the evolution of this technology is explored, focusing on the evolution of traditional IPSec and SSL/TLS protocols to more current versions. VPN security protocols are evaluated, analyzing IPSec, SSL/TLS, SHA-256 considering their security characteristics, performance and suitability for different scenarios. Furthermore, the applications of VPNs in current contexts are discussed, including remote access and connectivity between branches. The study also addresses the challenges and considerations in the process of deploying and managing VPNs in complex networks. Finally, the importance of VPNs is highlighted to ensure secure communications in current infrastructures.

KEYWORDS*: VPN. Protocol. Secure communication.*

RESUMEN

Las Redes Privadas Virtuales son esenciales para garantizar una comunicación segura en las redes públicas. Este estudio presenta explicaciones de los protocolos de seguridad utilizados en las VPN y su aplicación en entornos de red. Inicialmente, el documento define las VPN y su relevancia para proteger la transmisión de datos en redes vulnerables. A continuación, se explora la evolución de esta tecnología, centrándose en la evolución de los protocolos tradicionales IPSec y SSL/TLS hacia versiones más actuales. Se evalúan los protocolos de seguridad VPN, analizando IPSec, SSL/TLS, SHA-256 considerando sus características de seguridad, rendimiento e idoneidad para diferentes escenarios. Además, se discuten las aplicaciones de las VPN en los contextos actuales, incluido el acceso remoto y la conectividad entre sucursales. El estudio también aborda los desafíos y consideraciones en el proceso de implementación y gestión de VPN en redes complejas. Finalmente, se destaca la importancia de las VPN para garantizar comunicaciones seguras en las infraestructuras actuales.

PALABRAS CLAVE*: VPN. Protocolo. Comunicación segura.*

[1] Universidade do Estado de Mato Grosso - UNEMAT.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

INTRODUÇÃO

As VPNs são fundamentais no cenário atual de segurança da informação, garantindo que dados sensíveis possam ser transmitidos de forma segura por redes públicas, especialmente com o aumento do trabalho remoto e da computação em nuvem. (Henrique Santos 2020):

A utilização de VPNs em ambientes corporativos permite que organizações descentralizadas mantenham uma comunicação segura entre suas diferentes unidades, mesmo que estejam geograficamente distantes, assegurando a confidencialidade e integridade das informações trocadas." (Gonçalves, 2019).

Este artigo conceitual tem como objetivo oferecer uma revisão detalhada da tecnologia VPN, com ênfase nos protocolos de segurança que a sustentam e sua aplicação em redes modernas. Ele mostra a evolução dos softwares que fornecem aplicações de VPNs , destacando os avanços nos protocolos de segurança e os desafios enfrentados pelas organizações na implementação e gerenciamento dessas redes.

Com a crescente necessidade de proteção de dados e o aumento das ameaças digitais, as VPNs tornaram-se uma ferramenta crucial para empresas brasileiras que operam em múltiplas localidades, permitindo uma comunicação segura e eficiente (Moreira, 2021).

Além disso, abordaremos a aplicação das VPNs em redes empresariais, destacando sua importância no suporte ao acesso remoto de funcionários, na conexão entre filiais e na proteção de dados em serviços baseados em estruturas físicas. Também discutiremos os desafios e considerações relacionados à implementação e ao gerenciamento de softwares de VPNs.

No Brasil, as VPNs têm sido amplamente adotadas para garantir que a privacidade e a segurança das informações sejam mantidas, especialmente em setores sensíveis, como o financeiro e o governamental, onde o sigilo dos dados é de extrema importância (Almeida, 2018).

Utilizam-se certificados digitais para validação de informações e criptografias, que são transmitidas de um servidor para outro ou entre operações de comunicação de dados. Atualmente, temos diferentes tipos de certificados, mas este artigo se manterá apenas nos que serão utilizados para alcançar o resultado de uma comunicação entre empresas e suas filiais e entre usuários que acessam essas informações remotamente.

Um certificado SSL/TLS é um objeto digital que permite aos sistemas verificar a identidade e posteriormente estabelecer uma conexão de rede criptografada com outro sistema usando o protocolo Secure Sockets Layer / Transport Layer Security (SSL/TLS). Os certificados são emitidos usando um sistema criptográfico conhecido como infraestrutura de chave pública (PKI). A PKI permite que uma parte estabeleça a identidade de outra parte através do uso de certificados se ambas as partes confiarem em um terceiro, conhecido como autoridade de certificação. Portanto, os certificados SSL/TLS funcionam como cartões de identidade digitais que protegem as comunicações em rede e estabelecem a identidade de sites na Internet, bem como de recursos em redes privadas (Amazon Web Services, 2024).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Transport Layer Security, ou TLS, é um protocolo de segurança amplamente adotado, projetado para facilitar a privacidade e a segurança dos dados nas comunicações pela Internet. Um caso de uso principal do TLS é a criptografia de comunicações entre aplicativos web e servidores, como navegadores que carregam um site. O TLS também pode ser usado para criptografar outras comunicações, como e-mail, mensagens e voz sobre IP (VoIP) . O TLS foi proposto pela Internet Engineering Task Force (IETF), uma organização internacional de padrões. A primeira versão do protocolo foi publicada em 1999. A versão mais recente é o TLS 1.3, publicada em 2018 (Amazon Web Services, 2024).

Uma Rede Virtual Privada (VPN – Virtual Private Network) é uma tecnologia que vem ganhando popularidade em grandes organizações que usam a Internet global para a comunicação intra e interorganizacional, mas que exigem privacidade na comunicação interorganizacional. Uma VPN é uma rede privada, porém virtual. Ela é privada, pois garante privacidade dentro da organização. É virtual porque não usa WANs privadas reais; a rede é fisicamente pública, porém virtualmente privada. (Forouzan, 2013).

O intuito principal de uma VPN é a transmissão e recepção de dados com o máximo de segurança possível. Essa transmissão deve garantir que, mesmo que os dados sejam interceptados, não haverá acesso às informações e nem alterações ou inserções de informações.

Para que essa comunicação aconteça de forma correta, é utilizado o sistema de criptografia para garantia dessa proteção. Mas, para uma assertividade maior, precisamos entender o que é uma criptografia e como ela realiza a proteção dos dados, e quais são os tipos que podemos utilizar.

Criptografia é uma forma de embaralhar os dados para que somente as partes autorizadas possam entender as informações. Em termos técnicos, é o processo de converter um texto legível por seres humanos em texto incompreensível, também conhecido como texto cifrado ou criptografado. Em termos mais simples, a criptografia altera dados legíveis e faz com que pareçam aleatórios. A criptografia requer o uso de uma chave criptográfica: um conjunto de valores matemáticos com o qual tanto o remetente quanto o destinatário de uma mensagem criptografada concordam (Cloudflare, 2024).

1. METODOLOGIA

A prática desse projeto foi desenvolvida para interligar uma matriz e três filiais. O projeto tem o intuito de elevar o nível de segurança, atualizando as políticas de segurança dos túneis, identificando cada rede e gerando uma criptografia ponto a ponto com os padrões de segurança especificados anteriormente.

Foi utilizada a ferramenta PFSense em cada ambiente, junto com o *software* OpenVPN, muito utilizado para criação de túnel e gerenciamento de rede.

O *software* pfSense ® é uma distribuição gratuita, de código aberto e personalizada do FreeBSD, especialmente adaptada para uso como firewall e roteador, que é totalmente gerenciada via interface web. Além de ser uma plataforma de firewall e roteamento poderosa e flexível, ele inclui uma

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

longa lista de recursos relacionados e um sistema de pacotes que permite maior expansibilidade sem adicionar inchaço e potenciais vulnerabilidades de segurança à distribuição base. O projeto pfSense é hospedado e desenvolvido pela Rubicon Communications, LLC (Netgate, 2024).

O desenvolvimento desse projeto trouxe práticas atuais de configuração de rede, como a interligação de redes remotas, com o intuito de aumentar os padrões de segurança e unificar o ambiente utilizando um software do PFSense. Gerou-se a estruturação do ambiente, com a utilização de um firewall de segurança e a ferramenta OpenVPN disponível gratuitamente em seus recursos adicionais.

Foi possível realizar a configuração das VPNs**,** com os protocolos de segurança atualizados, seguindo um padrão elevado de segurança devido à criptografia atual.

2. DESENVOLVIMENTO DAS ATIVIDADES

O cenário que iremos abordar o desenvolvimento do projeto, consiste em quatro ambientes distintos, que precisam se comunicar em tempo real, realizando a unificação de uma rede para compartilhamento seguro de informações, impressoras, pastas compartilhadas, bancos de dados de sistemas ERP locais.

Foi utilizada a configuração do serviço de OpenVPN dentro do software firewall PFSense e entre filiais distintas utilizando também o *software* de firewall PFSense. Após a instalação do software e da ferramenta OpenVPN, que é disponibilizada gratuitamente dentro do aplicativo PFsense, começamos os processos de configuração do túnel que interligou com segurança e estabilidade a matriz com as três filiais.

Para realização desse projeto houve alguns pré-requisitos para sua execução.

- Os quatro estabelecimentos precisariam adquirir um equipamento de firewall com o PFsense instalado e atualizado.
- Os quatro estabelecimentos precisara de um link de internet com endereço de IP fixo.

Após os requisitos serem atendidos começamos a configuração do OpenVPN pela matriz para que as demais filiais se comuniquem com ela.

2.1 Configuração autoridade certificadora interna

Realizamos a criação do certificado digital, com o método de autoridade certificadora interna, que tem a função de emitir certificados digitais dentro de uma organização, como um selo de confiança para documentos e comunicações. Esse método permite que a empresa controle quem tem acesso a certos dados e garante que todas as interações digitais sejam seguras e legítimas, mantendo tudo sob controle próprio, em vez de depender de terceiros.

O nome do certificado foi Servidor-CA.

O tipo de chave utilizada foi a RSA, um dos algoritmos de criptografia mais conhecidos e seguros, que usa duas chaves: uma pública, que pode ser compartilhada com todos, e uma privada, que deve ser mantida em segredo. Juntas, elas permitem que se envie e receba informações de forma segura.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Com essas informações foi criado o CA como podemos ver nas figuras 1 e 2.

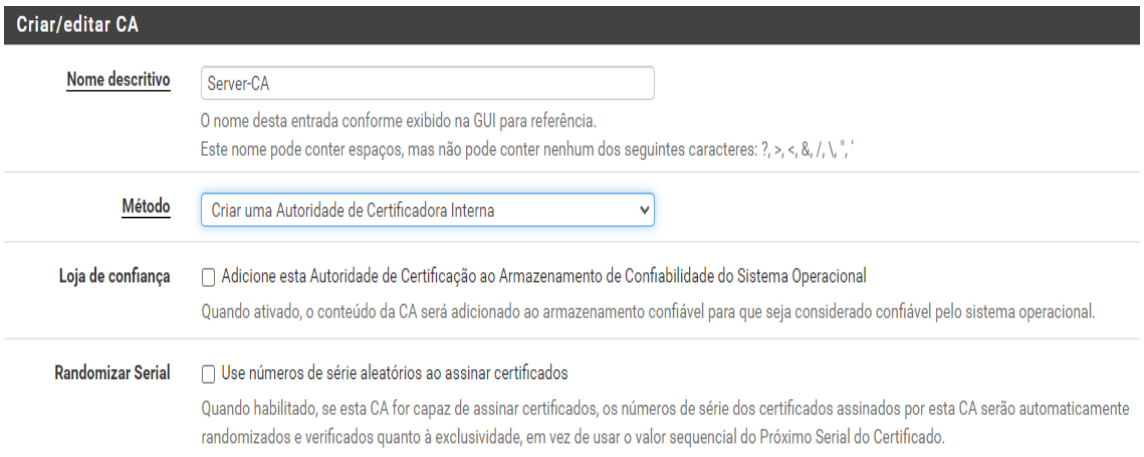


Figura 1.

Figura 2.

a. Configuração de CA interno

Na segunda etapa, foi realizada a configuração de um certificado interno, com vínculo com a autoridade certificadora interna criada anteriormente, para identificação do *firewall* da matriz onde as demais filiais vão se comunicar.

Como é exemplificado na figura número 3, fui utilizado o método de criação de um certificado interno. No campo de autoridade certificadora é feito o apontamento ao certificado criado anteriormente.

No tipo de chave manteremos as mesmas especificações do primeiro certificado criado, para manter o mesmo padrão de segurança utilizado.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

O tempo de vida útil delimita a validade do certificado, foi optado 10 anos, mas obrigatoriamente 1 ano é o limite mínimo estipulado pelo *software.*

Finalizando o processo de criação, relacionamos o tipo de certificado, como certificado servidor, pois o mesmo sera responsável por gerenciar os usuários que conectaram ao servidor. Como podemos ver nas figuras 3 e 4.

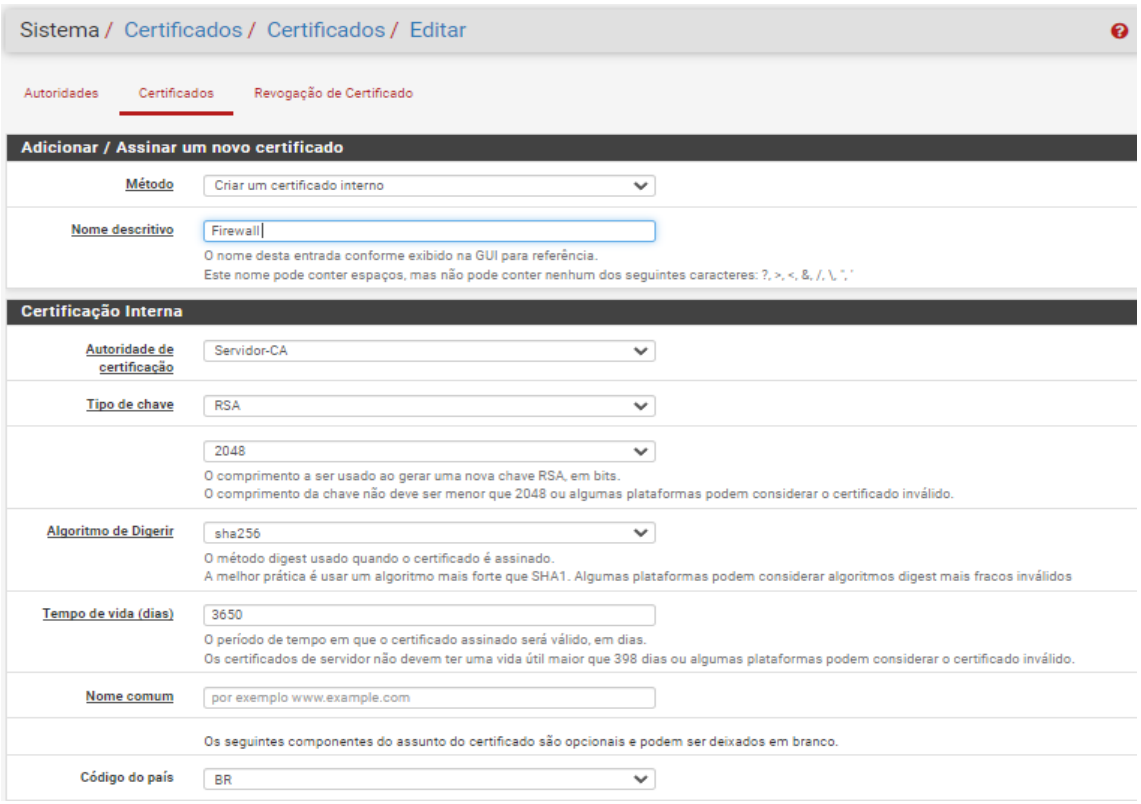


Figura 3.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

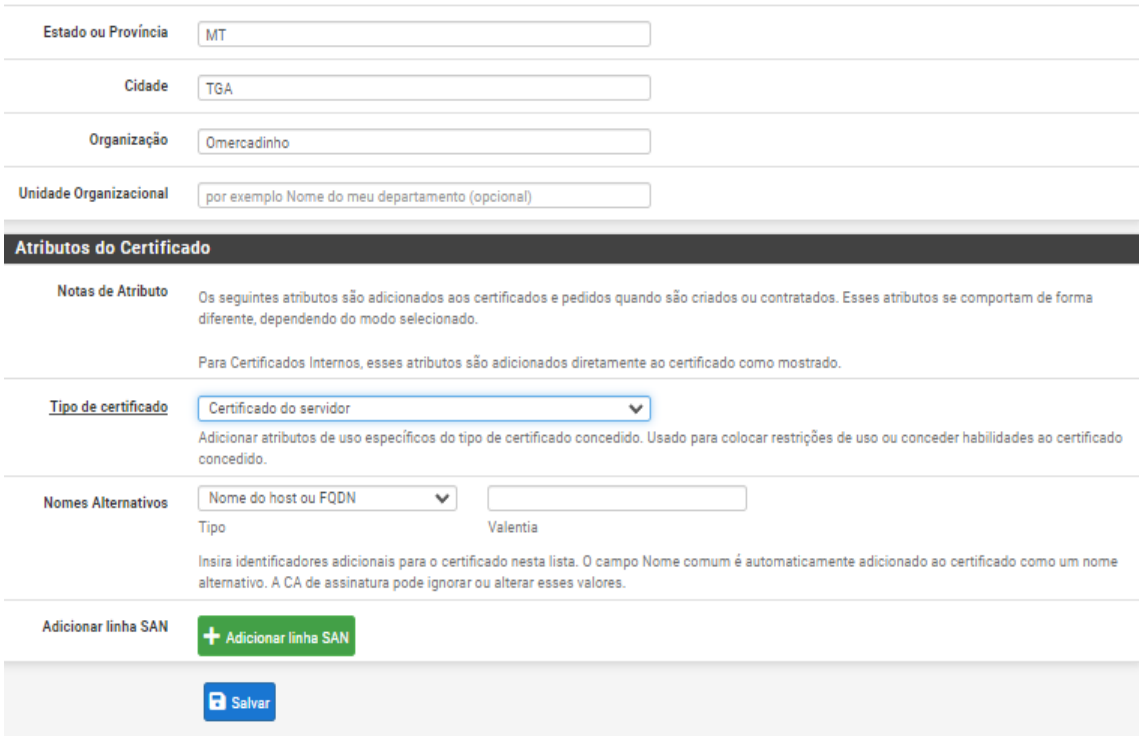


Figura 4.

b. Criação dos usuario dentro do *firewall* matriz

Nessa etapa será realizada a criação de usuários dentro do firewall matriz, com a finalidade de gerar um certificado digital com vínculo ao certificado de autoridade criado nos passos anteriores, no projeto desenvolvido, foi realizado a criação de três usuários, como podemos ver na figura 5.

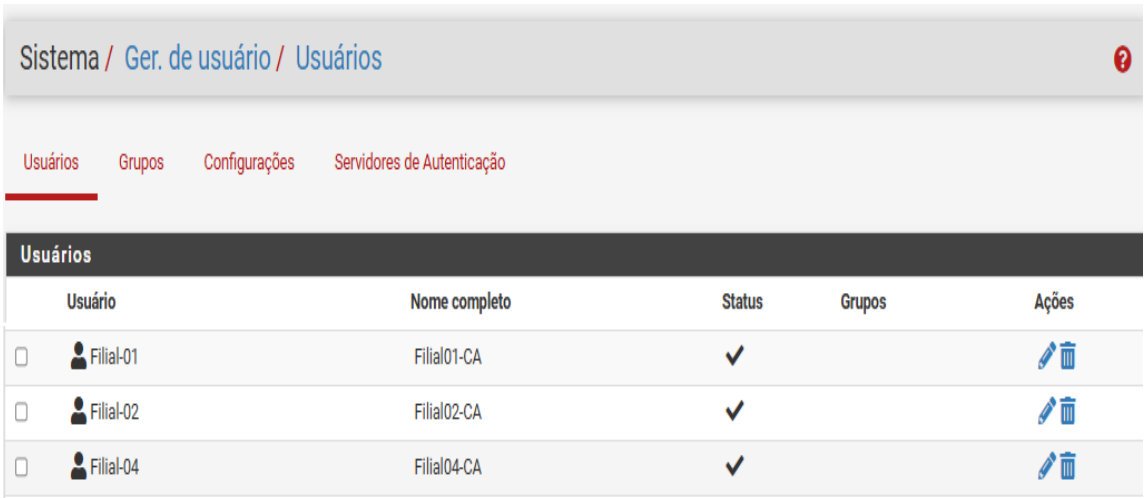


Figura 5.

Ao adicionar um novo usuário deve ser realizado as configurações seguindo a figura 6.

Especificando nome, senha, nome completo. Movendo o usuario para membros de admins, para que o mesmo possua direito de administrador dentro do *firewall* matriz.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

No campo certificado, flegar a opção clique para criar um certificado, para aparecer a opção de criação do certificado como exemplificado na figura 7.

Todos os certificados das filiais precisam estar relacionados a fonte autorizadora Servidor-CA, criado nos passos anteriores.

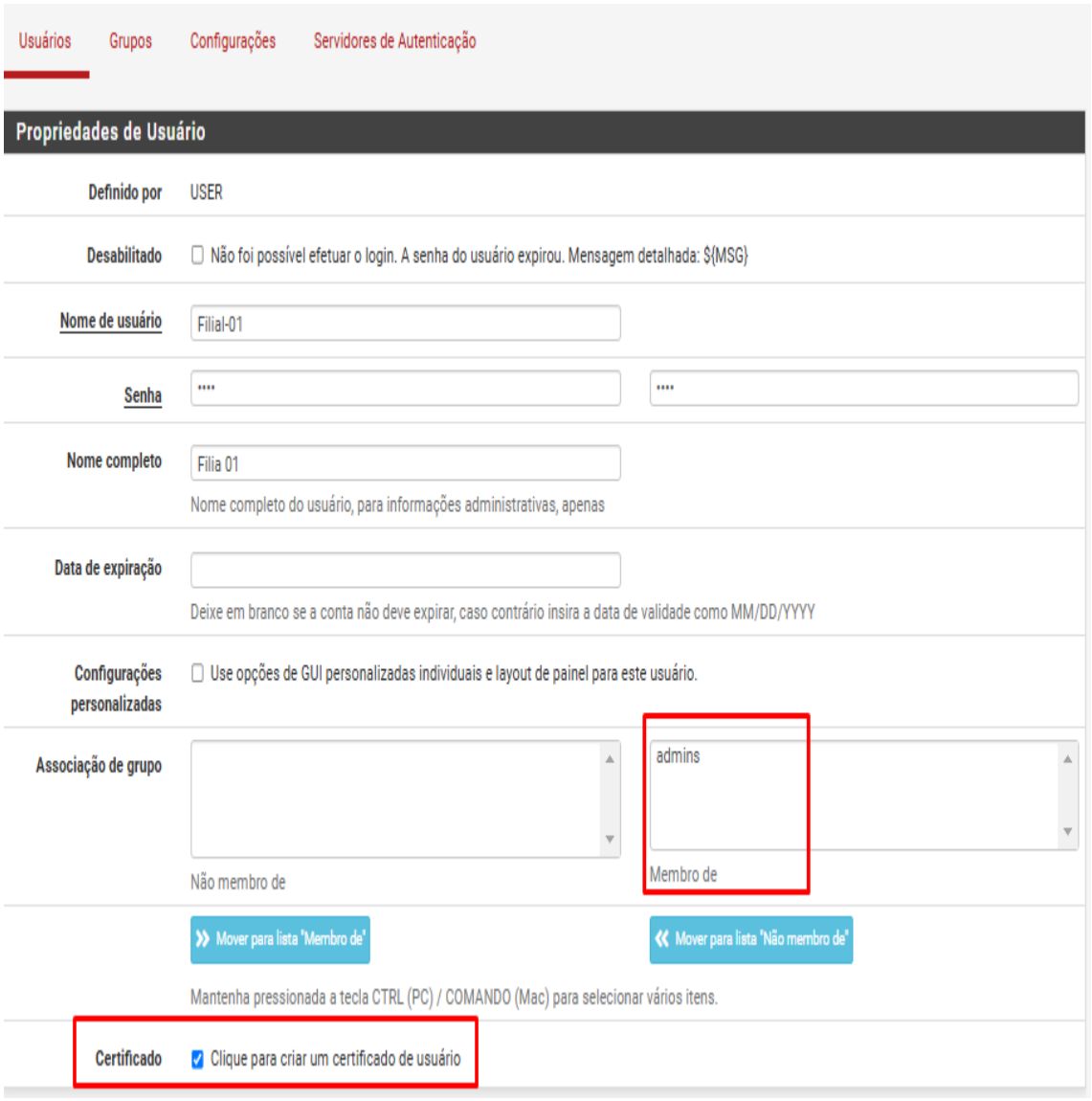


Figura 6.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

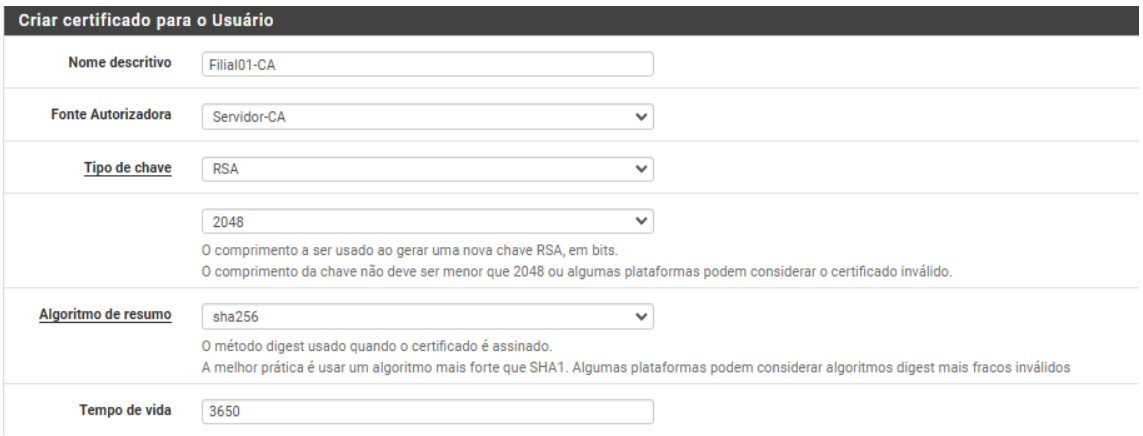


Figura 7.

c. **Criação do túnel da VPN**

Após realização das configurações de certificados e usuários, o software do firewall PFSense disponibiliza um *software* de fonte livre, gratuito que se integra ao sistema chamado OpenVPN, com a finalidade de criar redes privadas virtuais do tipo ponto-a-ponto ou *server-to-multiclient* através de túneis criptografados.

Dentro de VPN; OpenVPN ele trará a opção de adicionar servidores, esse servidor sera responsável pela criação do túnel e validação da criptografia, gerando a interligação das demais *firewalls*.

Ao iniciar a configuração utilizamos o modo de servidor ponto a ponto (SSL/TSL) que proporciona segurança e qualidade na comunicação de dados.

No modo dispositivo deixaremos o padrão tun-Layer 3, pois o mesmo comunica tanto em IPV4 e IPV6.

Em seguida definiremos a porta que o *software* utilizará para receber suas conexões, como podemos ver na figura 8.

Figura 8.

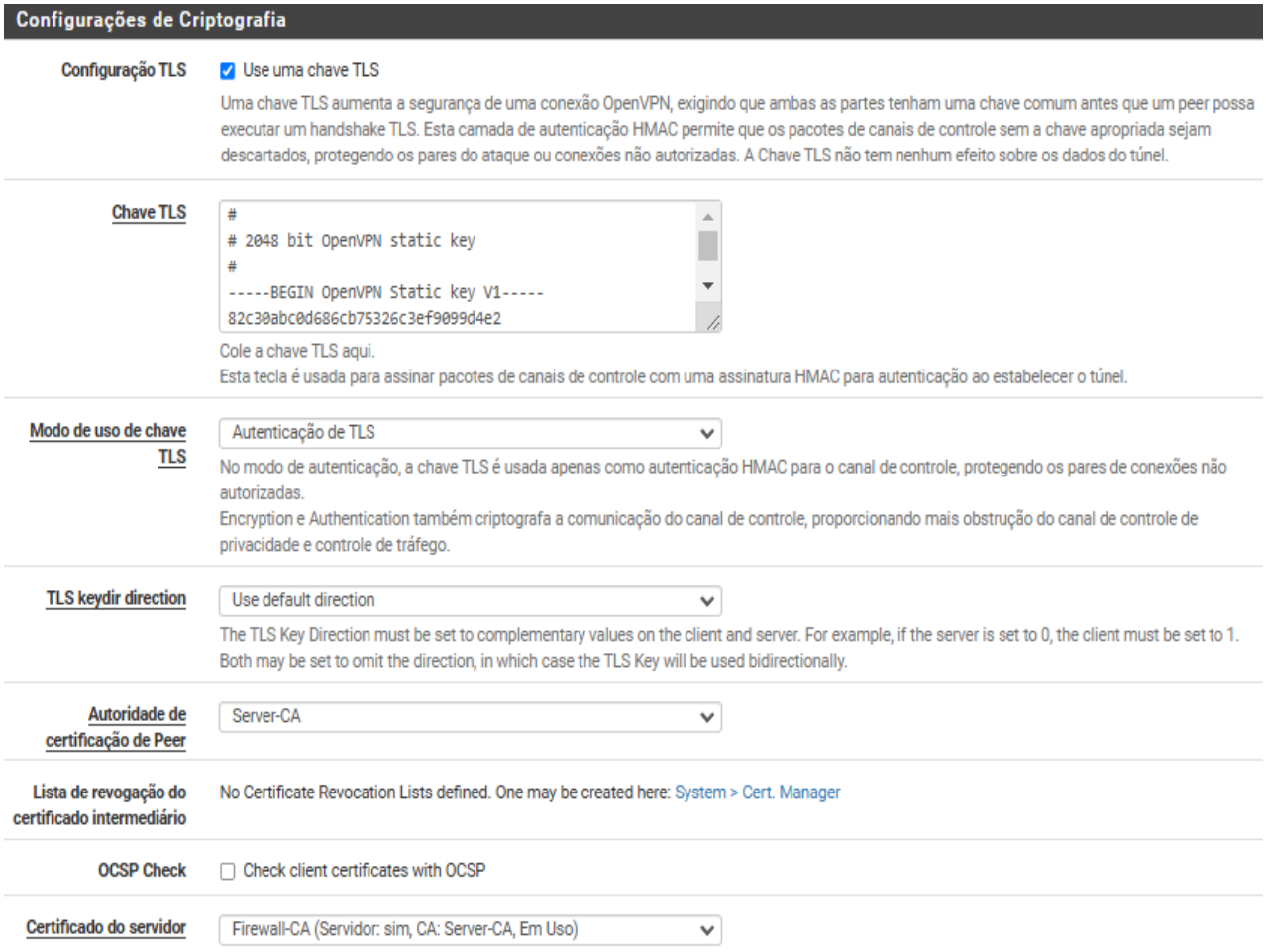
Na configuração de criptografia usamos uma chave TSL e solicitamos para que essa chave seja gerada automaticamente devido à complexidade.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Indicaremos a autoridade certificado Servidor-CA e o certificado do servidor criado Firewall-CA.

Adicionaremos o algoritmo de criptografia AES-256-GCM esse algoritmo criptografa cada bloco usando a mesma chave de criptografia e que, ao mesmo tempo, resulta em textos codificados diferentes, mesmo quando o texto simples em 2 ou mais blocos for idêntico. E utilizaremos o algoritmo de autenticação SHA3-512 devido a seu alto nível de segurança e complexidade na geração de códigos *hashes.*

A propriedade do certificado cliente mais servidor e a validação do uso de chave, tem o objetivo de aceitar somente a conexão dos clientes que possuam um certificado dentro firewall matriz onde o túnel está sendo criado, essa configuração foi feito em passos anteriores, quando criamos os usuario e seus certificados exemplificado na figura 9.



RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Figura 9.

Após finalizado a configuração de segurança do túnel, iniciamos o parâmetro geral do túnel, especificando o endereço da rede do túnel IPv4, esse endereço virtual tem a funcionalidade de entrada única de comunicação entre servidor e cliente.

No campo IPV4 as redes locais devem ser informadas e o *gateway* de cada rede que irá se comunicar.

Em redes remotas IPV4 é informado as mesmas redes que serão roteadas no túnel para que a VPN seja estabelecida sem alterar os endereços. Podemos visualizar na figura 10.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

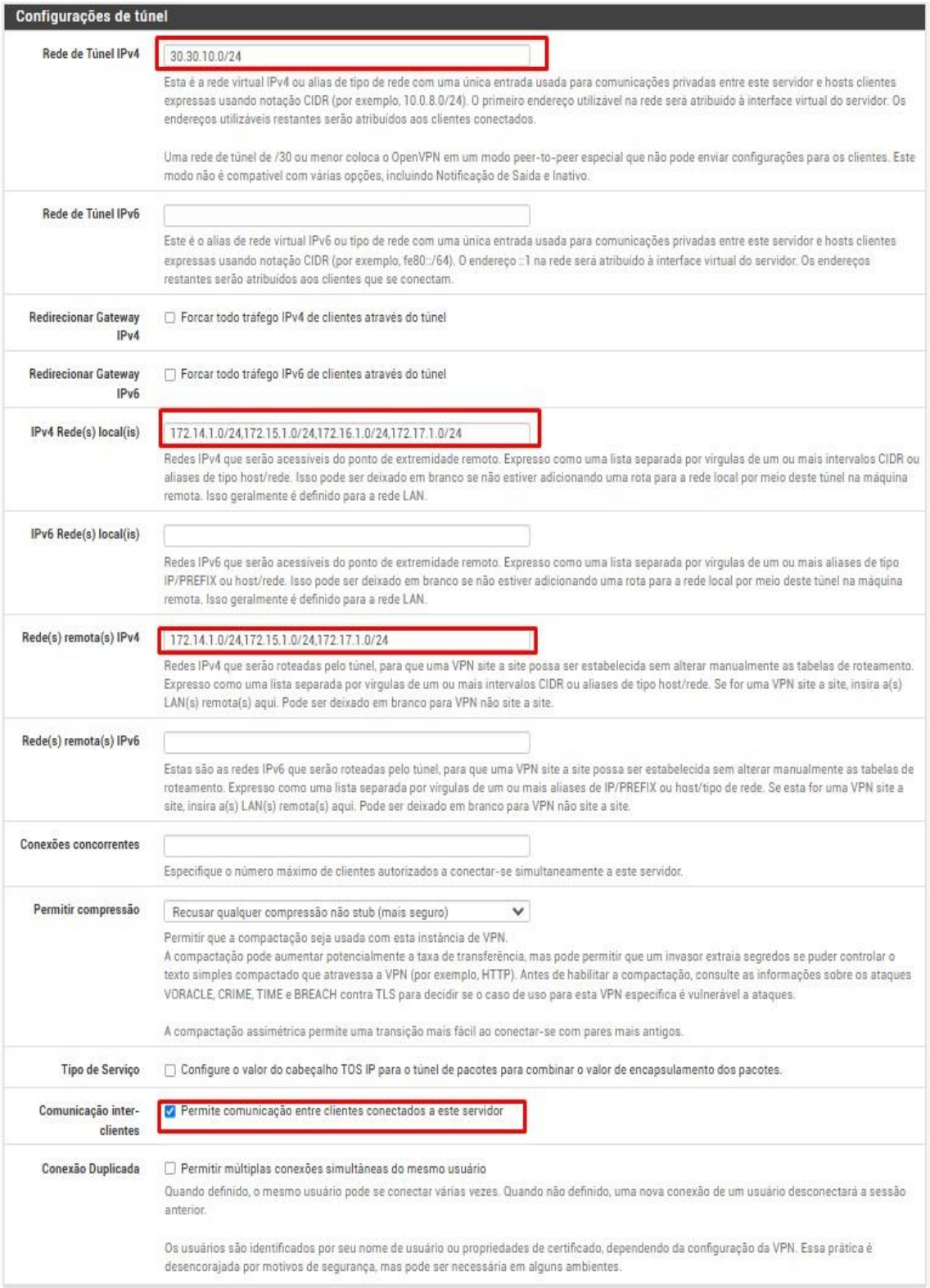


Figura 10.

Finalizando essa configuração, o túnel estará montado e configurado com um padrão de segurança elevado.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

d. Especificar cliente dentro do servidor OpenVPN

Tem a funcionalidade de especificar quem serão os clientes que acessarão os túneis, utilizaremos as mesmas nomenclaturas dos usuários criados. A descrição é opcional, o nome comum deverá ser o nome do usuário criado dentro do usuário nos passos anteriores. Em lista de servidores, selecionaremos o servidor criado, esse servidor é o túnel criado nos passos anteriores. Na rede remota, devemos especificar o endereço interno da rede do cliente para que o túnel reconheça a conexão. Podemos validar essa configuração na figura 11 e, na figura 12, o processo finalizado.

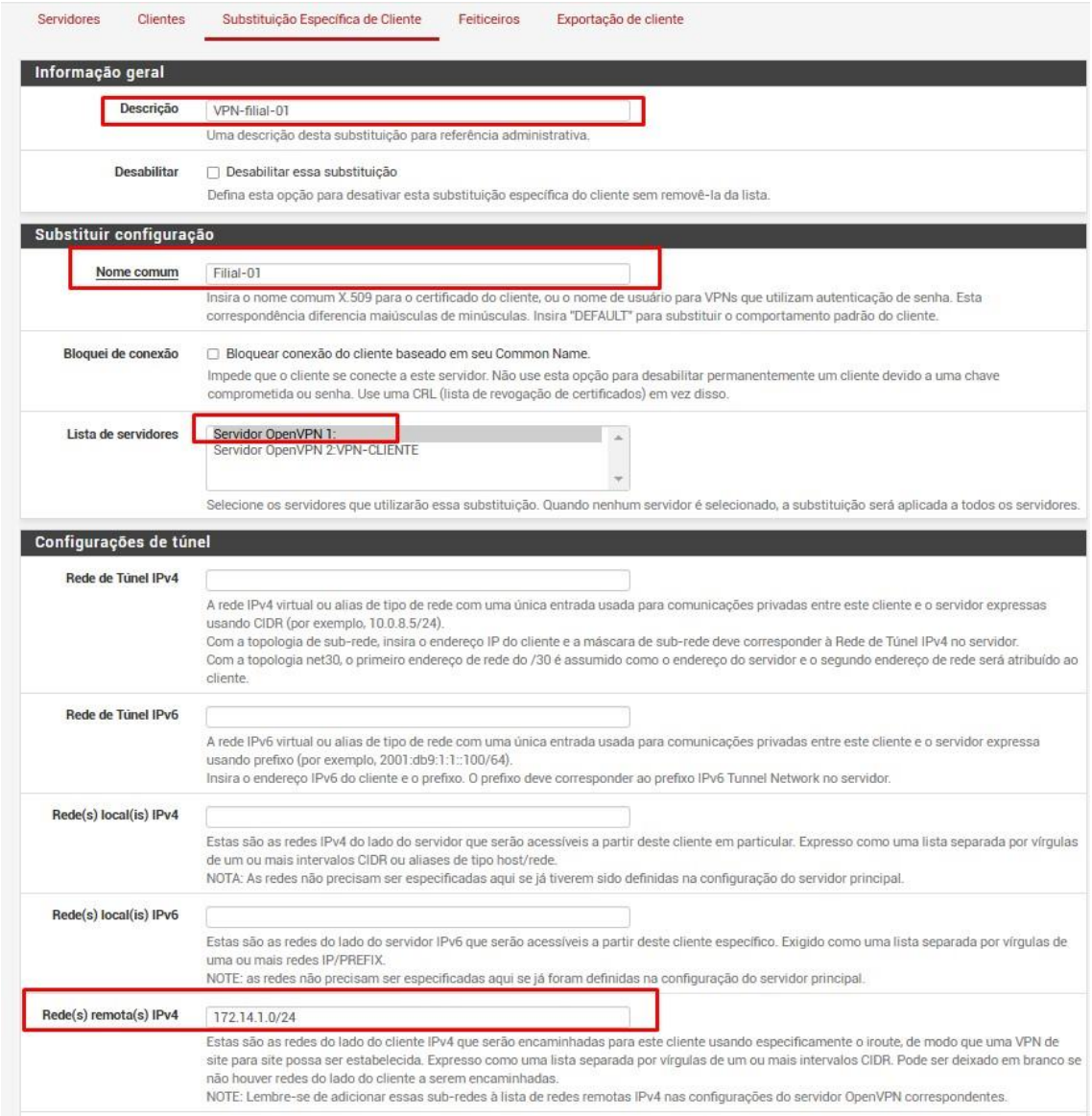


Figura 11.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

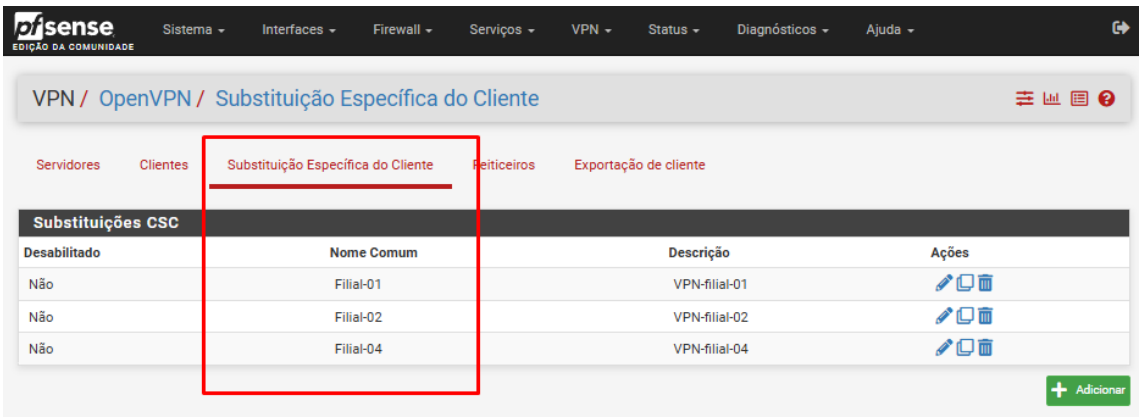


Figura 12.

e. Configuração do túnel e importação de certificado e chaves nas filiais

Dentro do *firewall* Servidor copiaremos os dados do certificado e chave primaria do certificado, informaremos essas informações nos *firewalls* das filiais, para que ambas possuam as mesmas informações do certificado Servidor-CA, como vemos na figura 13.

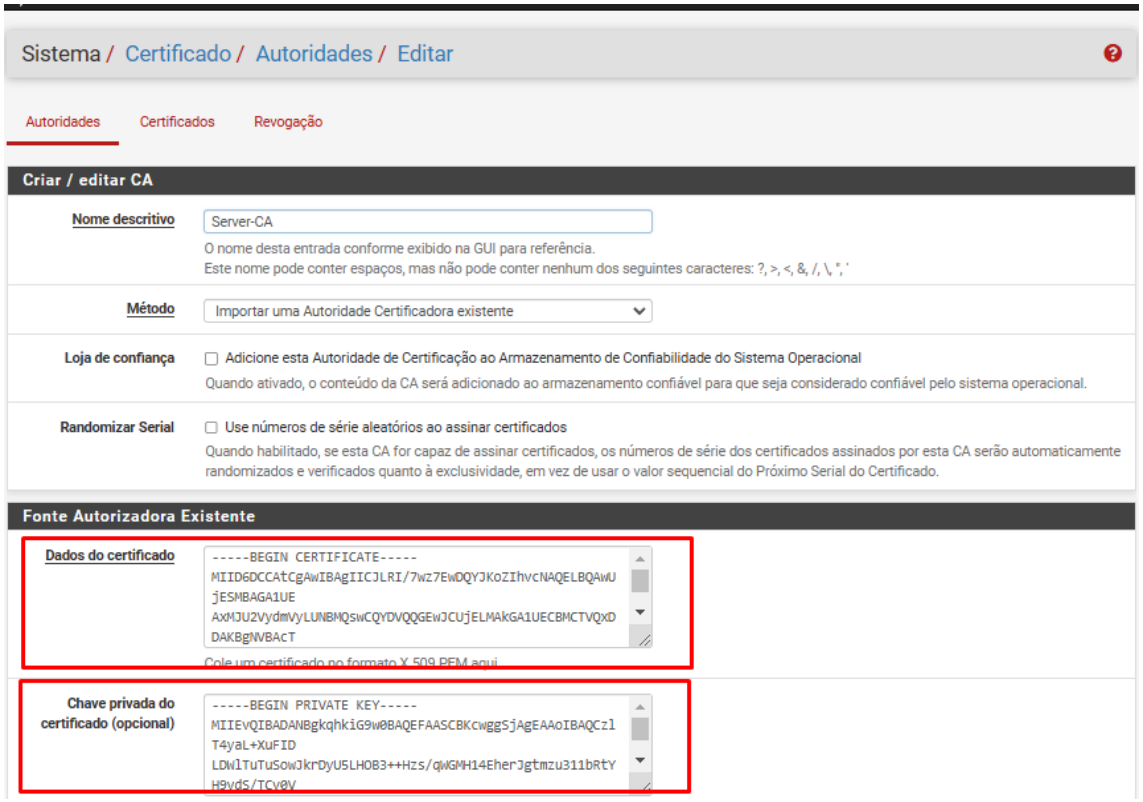


Figura 13.

Acessando *firewall* Filial-01, que será a primeira a ser configura.

Adicione um certificado de autoridade e utilize o método importar uma autoridade certificadora existente, cole os dados do certificado e a chave privada do certificado que foram copiados do *firewall*

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Servidor, como pode ser observado na figura 13, essas configurações serão repetidas nas demais *firewalls* Filial-02 e Filial-4.

Com o certificado adicionado, sera realizado a configuração do túnel semelhante aos passos anteriores com a diferença que as filiais serão clientes e não servidores como feito no início, como pode ser observado na figura 14.

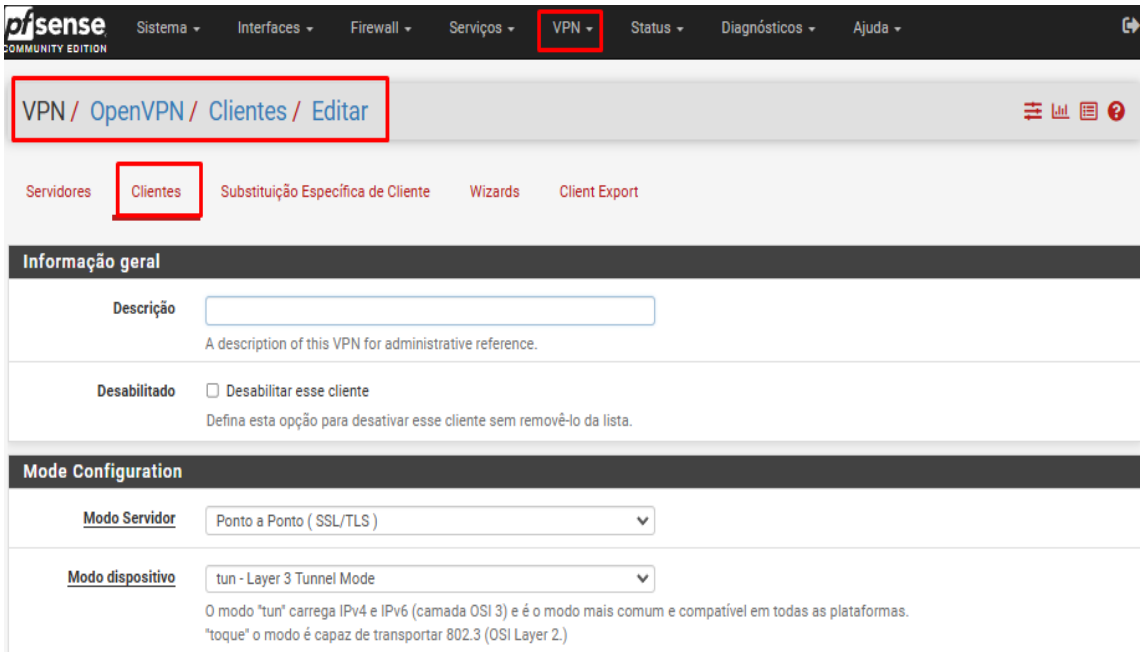


Figura 14.

No campo de configuração utilizaremos o mesmo protocolo UDP. A comunicação sera pela saída WAM, e deverá ser definida uma porta local, sua numeração é indiferente.

Em servidor *host* informaremos o número de IP do endereço público do nosso link, o IP deve ser fixo, pois através dele que faremos a interligação dos túneis.

Devera ser informada a porta do túnel do servidor, como podemos ver na figura 15.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

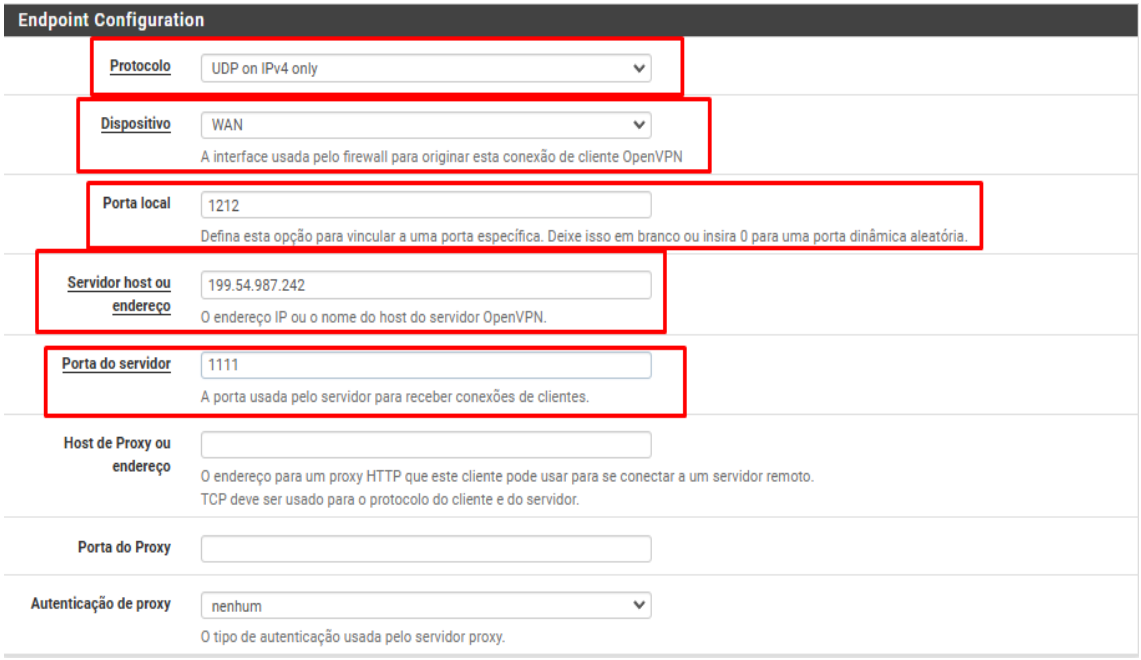


Figura 15.

Em configurações de criptografia deverá ser marcado o flag use uma chave TSL, utilizaremos a chave do Servidor-CA que foi gerada no firewall Servidor onde foi criado o túnel. Ao informar esses dados, a *firewall* Filial-01 possuirá a mesma chave TSL criada pelo Servidor-CA, ambos estarão com a mesma criptografia, servidor e cliente.

Esse processo se repete com a Filial-02 e Filial-04 igualando as mesmas configurações e as mesmas criptografias do servidor.

Identificaremos a autoridade certificadora Servidor-CA e o certificado do cliente Filial-01, na Filial-02 identifica a autoridade certificadora Servidor-CA e o certificado do cliente Filial-02 e na Filial-04 identifica a autoridade certificadora Servidor-CA e o certificado do cliente Filial-04.

A configuração das filiais é replica da configuração de segurança do Servidor.

Podemos observar a configuração na figura 16, o processo de configuração da Filial-01.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

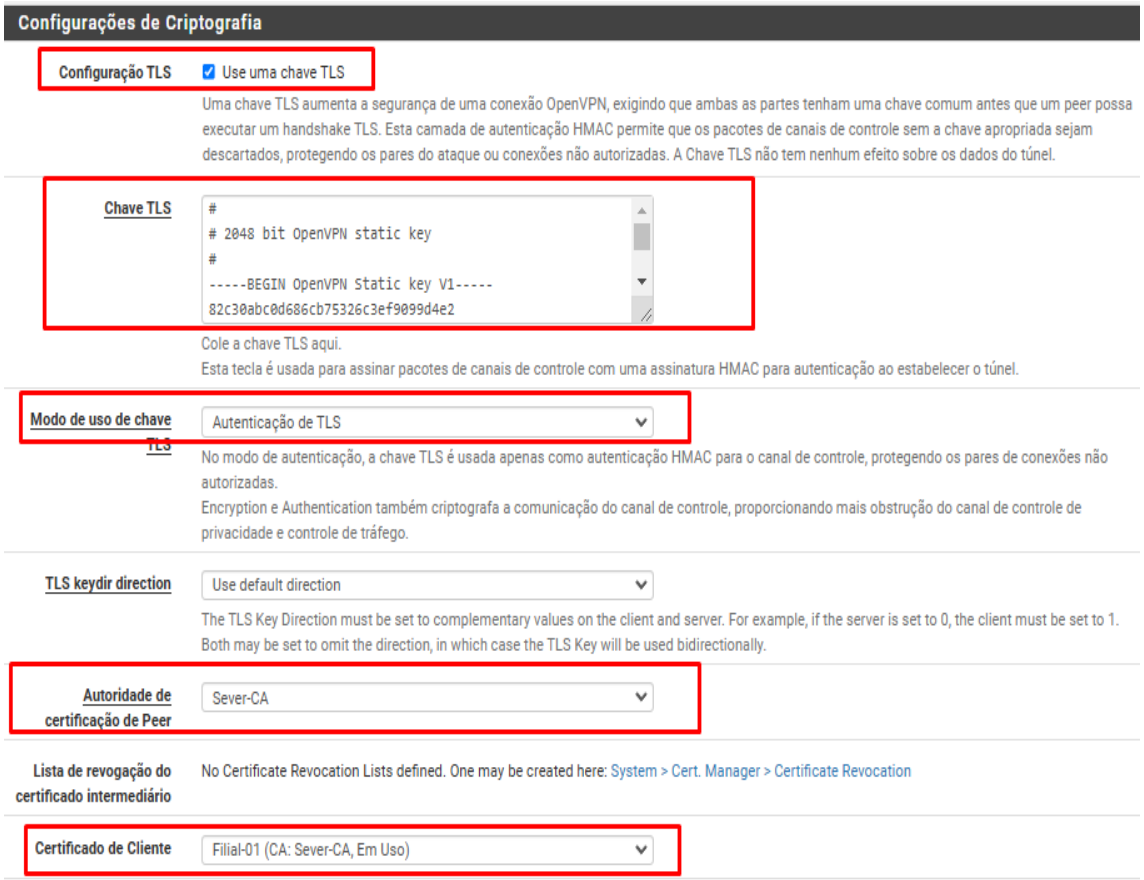


Figura 16.

Finalizado esse processo, o túnel esta funcional e comunicando *Firewall* servidor com os três *firewalls* filiais.

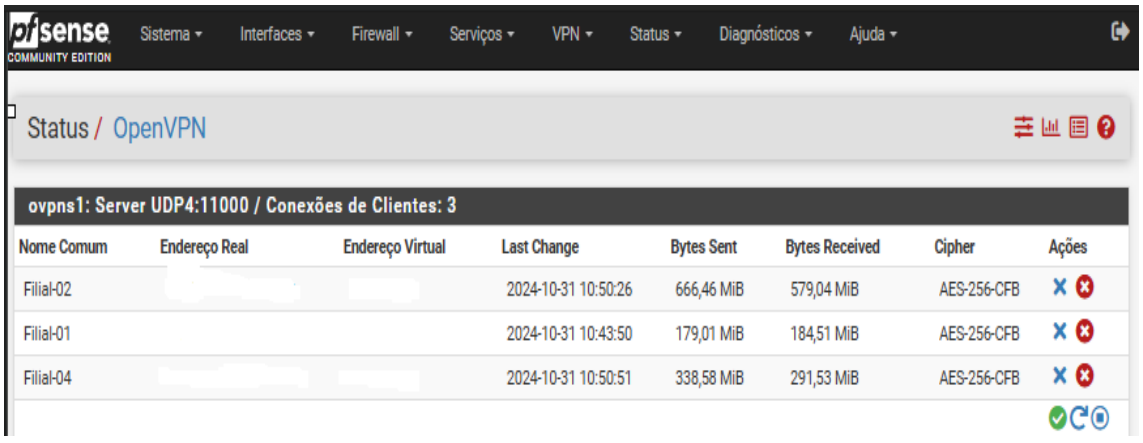


Figura 17.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

3. RESULTADOS

Através do projeto realizado**,** chegamos à estruturação de uma rede virtual privada, que unificou uma matriz e três filiais em locais distintos**,** seguindo os mais altos padrões de segurança da informação.

As redes virtuais possuem comunicação constante, com baixa latência e sem perda de pacotes. Todos os dados que trafegam pelo túnel estão criptografados e divididos em pacotes. Mesmo havendo uma eventual captura**,** as informações estariam divididas e criptografadas.

Utilizamos parâmetros de segurança atuais, com o intuito de manter um alto nível de segurança. Dentro do *software* existem diversas opções de criptografia. Após uma análise da demanda do ambiente**,** optou-se pelo sistema descrito.

Através desse processo**,** foi possível montar um ambiente seguro**,** com compartilhamento de pastas, dispositivos periféricos, servidores locais e bancos de dados locais.

REFERÊNCIAS

ALMEIDA, R. Adoção de VPNs no Brasil: Impactos e Benefícios em Setores Estratégicos. **Tecnologias de Informação e Comunicação no Brasil**, v. 5, n. 3, p. 120-136, 2018.

AMAZON WEB SERVICES**. ¿Qué es un certificado SSL/TLS?.** [S. l.]: AWS, 7 dez. 2024. Disponível em: https://aws.amazon.com/es/what-is/ssl-certificate/

CLOUDFLARE. **O que é criptografia?.** S. l.]: Cloudflare, 7 dez. 2024. Disponível em: https://www.cloudflare.com/pt-br/learning/ssl/what-is-encryption/

FOROUZAN, Behrouz A.; MOSHARRAF, Firouz. **Redes de Computadores**. Porto Alegre: Grupo A, 2013. E-book. ISBN 9788580551693. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788580551693/. Acesso em: 24 out. 2022.

GONÇALVES, C. A VPNs e a Segurança da Informação em Ambientes Corporativos Descentralizados. **Cadernos de Ciência da Computação**, v. 22, n. 1, p. 89-105, 2019.

MOREIRA, L. Proteção de Dados e Redes Privadas Virtuais: Um Estudo de Caso em Empresas Brasileiras. **Revista de Segurança Cibernética**, v. 10, n. 4, p. 75-90, 2019.

PFSENSE WEB SERVICES. **Faça um tour pelo pfSense**. [S. l.]: PFSense Web Services, 20 dez. 2024. Disponível em: https://pfsense.org/about-pfsense/

SANTOS, H. Segurança da Informação em Redes Corporativas: O Papel das VPNs no Ambiente de Trabalho Remoto. **Revista Brasileira de Tecnologia da Informação**, v. 15, n. 2, p. 45-60, 2020.