



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 Fernandes¹, Edimar Soares de Oliveira¹

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.



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).



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



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

OPENVPN E SUA APLICAÇÃO EM AMBIENTE EMPRESARIAL
Paulo Marcelo Gervasio Fernandes, Edimar Soares de Oliveira

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

Criar/editar CA	
Nome descritivo	Server-CA <small>O nome desta entrada conforme exibido na GUI para referência. Este nome pode conter espaços, mas não pode conter nenhum dos seguintes caracteres: ?, >, <, &, /, \, ' , "</small>
Método	Criar uma Autoridade de Certificadora Interna
Loja de confiança	<input type="checkbox"/> Adicione esta Autoridade de Certificação ao Armazenamento de Confiabilidade do Sistema Operacional <small>Quando ativado, o conteúdo da CA será adicionado ao armazenamento confiável para que seja considerado confiável pelo sistema operacional.</small>
Randomizar Serial	<input type="checkbox"/> Use números de série aleatórios ao assinar certificados <small>Quando habilitado, se esta CA for capaz de assinar certificados, os números de série dos certificados assinados por esta CA serão automaticamente randomizados e verificados quanto à exclusividade, em vez de usar o valor sequencial do Próximo Serial do Certificado.</small>

Figura 1.

Fonte Autorizadora de Certificado Interno	
Tipo de chave	RSA
	2048 <small>O comprimento a ser usado ao gerar uma nova chave RSA, em bits. O comprimento da chave não deve ser menor que 2048 ou algumas plataformas podem considerar o certificado inválido.</small>
Algoritmo de Digerir	sha256 <small>O método digest usado quando o CA é assinado. A melhor prática é usar um algoritmo mais forte que SHA1. Algumas plataformas podem considerar algoritmos digest mais fracos inválidos</small>
Tempo de vida (dias)	3650
Nome comum	internal-ca <small>Os seguintes componentes da unidade são informativos e podem ser deixados em branco.</small>
Código do país	Nenhum
Estado ou Província	por exemplo Texas
Cidade	por exemplo Austin
Organização	por exemplo Minha Empresa Inc.
Unidade Organizacional	por exemplo Nome do meu departamento (opcional)

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, foi 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

OPENVPN E SUA APLICAÇÃO EM AMBIENTE EMPRESARIAL
Paulo Marcelo Gervasio Fernandes, Edimar Soares de Oliveira

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 será responsável por gerenciar os usuários que conectaram ao servidor. Como podemos ver nas figuras 3 e 4.

Sistema / Certificados / Certificados / Editar

Autoridades Certificados Revogação de Certificado

Adicionar / Assinar um novo certificado

Método Criar um certificado interno

Nome descritivo Firewall
O nome desta entrada conforme exibido na GUI para referência.
Este nome pode conter espaços, mas não pode conter nenhum dos seguintes caracteres: ?, >, <, &, /, \, '.

Certificação Interna

Autoridade de certificação Servidor-CA

Tipo de chave RSA

2048
O comprimento a ser usado ao gerar uma nova chave RSA, em bits.
O comprimento da chave não deve ser menor que 2048 ou algumas plataformas podem considerar o certificado inválido.

Algoritmo de Digerir sha256
O método digest usado quando o certificado é assinado.
A melhor prática é usar um algoritmo mais forte que SHA1. Algumas plataformas podem considerar algoritmos digest mais fracos inválidos

Tempo de vida (dias) 3650
O período de tempo em que o certificado assinado será válido, em dias.
Os certificados de servidor não devem ter uma vida útil maior que 398 dias ou algumas plataformas podem considerar o certificado inválido.

Nome comum por exemplo www.example.com

Os seguintes componentes do assunto do certificado são opcionais e podem ser deixados em branco.

Código do país BR

Figura 3.



RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR ISSN 2675-6218

OPENVPN E SUA APLICAÇÃO EM AMBIENTE EMPRESARIAL
Paulo Marcelo Gervasio Fernandes, Edimar Soares de Oliveira

Estado ou Província

Cidade

Organização

Unidade Organizacional

Atributos do Certificado

Notas de Atributo Os seguintes atributos são adicionados aos certificados e pedidos quando são criados ou contratados. Esses atributos se comportam de forma diferente, dependendo do modo selecionado.
Para Certificados Internos, esses atributos são adicionados diretamente ao certificado como mostrado.

Tipo de certificado
Adicionar atributos de uso específicos do tipo de certificado concedido. Usado para colocar restrições de uso ou conceder habilidades ao certificado concedido.

Nomes Alternativos
Tipo
Insira identificadores adicionais para o certificado nesta lista. O campo Nome comum é automaticamente adicionado ao certificado como um nome alternativo. A CA de assinatura pode ignorar ou alterar esses valores.

Adicionar linha SAN

Figura 4.

b. Criação dos usuário 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.

Sistema / Ger. de usuário / Usuários ?

Usuários Grupos Configurações Servidores de Autenticação

Usuários				
Usuário	Nome completo	Status	Grupos	Ações
<input type="checkbox"/> Filial-01	Filial01-CA	✓		
<input type="checkbox"/> Filial-02	Filial02-CA	✓		
<input type="checkbox"/> Filial-04	Filial04-CA	✓		

Figura 5.

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

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



RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR ISSN 2675-6218

OPENVPN E SUA APLICAÇÃO EM AMBIENTE EMPRESARIAL
Paulo Marcelo Gervasio Fernandes, Edimar Soares de Oliveira

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.

Usuários Grupos Configurações Servidores de Autenticação

Propriedades de Usuário

Definido por USER

Desabilitado Não foi possível efetuar o login. A senha do usuário expirou. Mensagem detalhada: \${MSG}

Nome de usuário

Senha

Nome completo
Nome completo do usuário, para informações administrativas, apenas

Data de expiração
Deixe em branco se a conta não deve expirar, caso contrário insira a data de validade como MM/DD/YYYY

Configurações personalizadas Use opções de GUI personalizadas individuais e layout de painel para este usuário.

Associação de grupo

Não membro de

Membro de

>> Mover para lista "Membro de" << Mover para lista "Não membro de"

Mantenha pressionada a tecla CTRL (PC) / COMANDO (Mac) para selecionar vários itens.

Certificado Clique para criar um certificado de usuário

Figura 6.



Criar certificado para o Usuário	
Nome descritivo	<input type="text" value="Filial01-CA"/>
Fonte Autorizadora	<input type="text" value="Servidor-CA"/>
Tipo de chave	<input type="text" value="RSA"/>
	<input type="text" value="2048"/>
	<small>O comprimento a ser usado ao gerar uma nova chave RSA, em bits. O comprimento da chave não deve ser menor que 2048 ou algumas plataformas podem considerar o certificado inválido.</small>
Algoritmo de resumo	<input type="text" value="sha256"/>
	<small>O método digest usado quando o certificado é assinado. A melhor prática é usar um algoritmo mais forte que SHA1. Algumas plataformas podem considerar algoritmos digest mais fracos inválidos</small>
Tempo de vida	<input type="text" value="3650"/>

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/TLS) 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.

Mode Configuration	
Modo Servidor	<input type="text" value="Ponto a Ponto (SSL/TLS)"/>
Modo dispositivo	<input type="text" value="tun - Layer 3 Tunnel Mode"/>
	<small>O modo "tun" carrega IPV4 e IPV6 (camada OSI 3) e é o modo mais comum e compatível em todas as plataformas. "toque" o modo é capaz de transportar 802.3 (OSI Layer 2)</small>
Endpoint Configuration	
Protocolo	<input type="text" value="UDP IPV4 and IPV6 on all interfaces (multihome)"/>
Porta local	<input type="text" value="1111"/>
	<small>A porta utilizada pelo OpenVPN para receber conexões de clientes.</small>

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

OPENVPN E SUA APLICAÇÃO EM AMBIENTE EMPRESARIAL
Paulo Marcelo Gervasio Fernandes, Edimar Soares de Oliveira

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.

Configurações de Criptografia

Configuração TLS Use uma chave TLS

Uma chave TLS aumenta a segurança de uma conexão OpenVPN, exigindo que ambas as partes tenham uma chave comum antes que um peer possa executar um handshake TLS. Esta camada de autenticação HMAC permite que os pacotes de canais de controle sem a chave apropriada sejam descartados, protegendo os pares do ataque ou conexões não autorizadas. A Chave TLS não tem nenhum efeito sobre os dados do túnel.

Chave TLS

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
82c30abc0d686cb75326c3ef9099d4e2
```

Cole a chave TLS aqui.
Esta tecla é usada para assinar pacotes de canais de controle com uma assinatura HMAC para autenticação ao estabelecer o túnel.

Modo de uso de chave TLS Autenticação de TLS

No modo de autenticação, a chave TLS é usada apenas como autenticação HMAC para o canal de controle, protegendo os pares de conexões não autorizadas.
Encryption e Authentication também criptografa a comunicação do canal de controle, proporcionando mais obstrução do canal de controle de privacidade e controle de tráfego.

TLS keydir direction Use default direction

The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Autoridade de certificação de Peer Server-CA

Lista de revogação do certificado intermediário No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSF Check Check client certificates with OCSF

Certificado do servidor Firewall-CA (Servidor: sim, CA: Server-CA, Em Uso)



Algoritmos de criptografia de dados

Algoritmos de criptografia de dados disponíveis
Clique para adicionar ou remover um algoritmo da lista

- AES-192-CFB1 (chave de 192 bits, bloco de 128 bits)
- AES-192-CFB8 (chave de 192 bits, bloco de 128 bits)
- AES-192-GCM (chave de 192 bits, bloco de 128 bits)
- AES-192-OFB (chave de 192 bits, bloco de 128 bits)
- AES-256-CBC (chave de 256 bits, bloco de 128 bits)
- AES-256-CFB (chave de 256 bits, bloco de 128 bits)
- AES-256-CFB1 (chave de 256 bits, bloco de 128 bits)
- AES-256-CFB8 (chave de 256 bits, bloco de 128 bits)
- AES-256-GCM (chave de 256 bits, bloco de 128 bits)
- AES-256-OFB (chave de 256 bits, bloco de 128 bits)

Algoritmos de criptografia de dados permitidos. Clique no nome de um algoritmo para removê-lo da lista

- AES-256-CFB

A ordem dos Data Encryption Algorithms selecionados é respeitada pelo OpenVPN. Esta lista é ignorada no modo Shared Key. ⓘ

Algoritmo de criptografia de dados de fallback

AES-256-CFB (chave de 256 bits, bloco de 128 bits) ▼

O Fallback Data Encryption Algorithm usado para pacotes de canal de dados ao se comunicar com clientes que não suportam negociação de algoritmo de criptografia de dados (por exemplo, Shared Key). Este algoritmo é automaticamente incluído na lista Data Encryption Algorithms.

Algoritmo de autenticação

SHA3-512 (512 bits) ▼

O algoritmo usado para autenticar pacotes de canal de dados e pacotes de canal de controle se uma chave TLS estiver presente. Quando um modo de algoritmo de criptografia AEAD é usado, como AES-GCM, este resumo é usado apenas para o canal de controle, não para o canal de dados. O servidor e todos os clientes devem ter a mesma configuração. Embora SHA1 seja o padrão para OpenVPN, este algoritmo é inseguro.

Criptografia de hardware

Sem aceleração criptográfica de hardware. ▼

Profundidade do certificado

Um (Cliente+Servidor) ▼

Quando um cliente faz login com base em certificados, não aceitar certificados com profundidade abaixo desta. Útil para negar certificados emitidos por CAs intermediários gerados a partir do mesmo CA que o servidor.

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

OPENVPN E SUA APLICAÇÃO EM AMBIENTE EMPRESARIAL
Paulo Marcelo Gervasio Fernandes, Edimar Soares de Oliveira

Configurações de túnel	
Rede de Túnel IPv4	<input type="text" value="30.30.10.0/24"/> <p>Esta é a rede virtual IPv4 ou alias de tipo de rede com uma única entrada usada para comunicações privadas entre este servidor e hosts clientes expressas usando notação CIDR (por exemplo, 10.0.8.0/24). O primeiro endereço utilizável na rede será atribuído à interface virtual do servidor. Os endereços utilizáveis restantes serão atribuídos aos clientes conectados.</p> <p>Uma rede de túnel de /30 ou menor coloca o OpenVPN em um modo peer-to-peer especial que não pode enviar configurações para os clientes. Este modo não é compatível com várias opções, incluindo Notificação de Saída e Inativo.</p>
Rede de Túnel IPv6	<input type="text"/> <p>Este é o alias de rede virtual IPv6 ou tipo de rede com uma única entrada usada para comunicações privadas entre este servidor e hosts clientes expressas usando notação CIDR (por exemplo, fe80::/64). O endereço ::1 na rede será atribuído à interface virtual do servidor. Os endereços restantes serão atribuídos aos clientes que se conectam.</p>
Redirecionar Gateway IPv4	<input type="checkbox"/> Forçar todo tráfego IPv4 de clientes através do túnel
Redirecionar Gateway IPv6	<input type="checkbox"/> Forçar todo tráfego IPv6 de clientes através do túnel
IPv4 Rede(s) local(is)	<input type="text" value="172.14.1.0/24,172.15.1.0/24,172.16.1.0/24,172.17.1.0/24"/> <p>Redes IPv4 que serão acessíveis do ponto de extremidade remoto. Expresso como uma lista separada por vírgulas de um ou mais intervalos CIDR ou aliases de tipo host/rede. Isso pode ser deixado em branco se não estiver adicionando uma rota para a rede local por meio deste túnel na máquina remota. Isso geralmente é definido para a rede LAN.</p>
IPv6 Rede(s) local(is)	<input type="text"/> <p>Redes IPv6 que serão acessíveis do ponto de extremidade remoto. Expresso como uma lista separada por vírgulas de um ou mais aliases de tipo IP/PREFIX ou host/rede. Isso pode ser deixado em branco se não estiver adicionando uma rota para a rede local por meio deste túnel na máquina remota. Isso geralmente é definido para a rede LAN.</p>
Rede(s) remota(s) IPv4	<input type="text" value="172.14.1.0/24,172.15.1.0/24,172.17.1.0/24"/> <p>Redes IPv4 que serão roteadas pelo túnel, para que uma VPN site a site possa ser estabelecida sem alterar manualmente as tabelas de roteamento. Expresso como uma lista separada por vírgulas de um ou mais intervalos CIDR ou aliases de tipo host/rede. Se for uma VPN site a site, insira a(s) LAN(s) remota(s) aqui. Pode ser deixado em branco para VPN não site a site.</p>
Rede(s) remota(s) IPv6	<input type="text"/> <p>Estas são as redes IPv6 que serão roteadas pelo túnel, para que uma VPN site a site possa ser estabelecida sem alterar manualmente as tabelas de roteamento. Expresso como uma lista separada por vírgulas de um ou mais aliases de IP/PREFIX ou host/tipo de rede. Se esta for uma VPN site a site, insira a(s) LAN(s) remota(s) aqui. Pode ser deixado em branco para VPN não site a site.</p>
Conexões concorrentes	<input type="text"/> <p>Especifique o número máximo de clientes autorizados a conectar-se simultaneamente a este servidor.</p>
Permitir compressão	<input type="text" value="Recusar qualquer compressão não stub (mais seguro)"/> <p>Permitir que a compactação seja usada com esta instância de VPN. A compactação pode aumentar potencialmente a taxa de transferência, mas pode permitir que um invasor extraia segredos se puder controlar o texto simples compactado que atravessa a VPN (por exemplo, HTTP). Antes de habilitar a compactação, consulte as informações sobre os ataques VORACLE, CRIME, TIME e BREACH contra TLS para decidir se o caso de uso para esta VPN específica é vulnerável a ataques. A compactação assimétrica permite uma transição mais fácil ao conectar-se com pares mais antigos.</p>
Tipo de Serviço	<input type="checkbox"/> Configure o valor do cabeçalho TOS IP para o túnel de pacotes para combinar o valor de encapsulamento dos pacotes.
Comunicação inter-clientes	<input checked="" type="checkbox"/> Permite comunicação entre clientes conectados a este servidor
Conexão Duplicada	<input type="checkbox"/> Permitir múltiplas conexões simultâneas do mesmo usuário <p>Quando definido, o mesmo usuário pode se conectar várias vezes. Quando não definido, uma nova conexão de um usuário desconectará a sessão anterior.</p> <p>Os usuários são identificados por seu nome de usuário ou propriedades de certificado, dependendo da configuração da VPN. Essa prática é desencorajada por motivos de segurança, mas pode ser necessária em alguns ambientes.</p>

Figura 10.

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



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.

The screenshot shows the configuration interface for OpenVPN, specifically the 'Substituição Específica de Cliente' tab. The interface is organized into several sections:

- Informação geral:**
 - Descrição:** VPN-filial-01 (highlighted with a red box). Below it, a note states: 'Uma descrição desta substituição para referência administrativa.'
 - Desabilitar:** A checkbox labeled 'Desabilitar essa substituição' is unchecked. Below it, a note states: 'Defina esta opção para desativar esta substituição específica do cliente sem removê-la da lista.'
- Substituir configuração:**
 - Nome comum:** Filial-01 (highlighted with a red box). Below it, a note states: 'Insira o nome comum X.509 para o certificado do cliente, ou o nome de usuário para VPNs que utilizam autenticação de senha. Esta correspondência diferencia maiúsculas de minúsculas. Insira "DEFAULT" para substituir o comportamento padrão do cliente.'
 - Bloqueio de conexão:** A checkbox labeled 'Bloquear conexão do cliente baseado em seu Common Name' is unchecked. Below it, a note states: 'Impede que o cliente se conecte a este servidor. Não use esta opção para desabilitar permanentemente um cliente devido a uma chave comprometida ou senha. Use uma CRL (lista de revogação de certificados) em vez disso.'
 - Lista de servidores:** A dropdown menu is open, showing 'Servidor OpenVPN 1' (highlighted with a red box) and 'Servidor OpenVPN 2:VPN-CLIENTE'. Below it, a note states: 'Selecione os servidores que utilizarão essa substituição. Quando nenhum servidor é selecionado, a substituição será aplicada a todos os servidores.'
- Configurações de túnel:**
 - Rede de Túnel IPv4:** An empty text input field. Below it, a note states: 'A rede IPv4 virtual ou alias de tipo de rede com uma única entrada usada para comunicações privadas entre este cliente e o servidor expressas usando CIDR (por exemplo, 10.0.8.5/24). Com a topologia de sub-rede, insira o endereço IP do cliente e a máscara de sub-rede deve corresponder à Rede de Túnel IPv4 no servidor. Com a topologia net30, o primeiro endereço de rede do /30 é assumido como o endereço do servidor e o segundo endereço de rede será atribuído ao cliente.'
 - Rede de Túnel IPv6:** An empty text input field. Below it, a note states: 'A rede IPv6 virtual ou alias de tipo de rede com uma única entrada usada para comunicações privadas entre este cliente e o servidor expressa usando prefixo (por exemplo, 2001:db9:1:1::100/64). Insira o endereço IPv6 do cliente e o prefixo. O prefixo deve corresponder ao prefixo IPv6 Tunnel Network no servidor.'
 - Rede(s) local(is) IPv4:** An empty text input field. Below it, a note states: 'Estas são as redes IPv4 do lado do servidor que serão acessíveis a partir deste cliente em particular. Expresso como uma lista separada por vírgulas de um ou mais intervalos CIDR ou aliases de tipo host/rede. NOTA: As redes não precisam ser especificadas aqui se já tiverem sido definidas na configuração do servidor principal.'
 - Rede(s) local(is) IPv6:** An empty text input field. Below it, a note states: 'Estas são as redes do lado do servidor IPv6 que serão acessíveis a partir deste cliente específico. Exigido como uma lista separada por vírgulas de uma ou mais redes IP/PREFIX. NOTA: as redes não precisam ser especificadas aqui se já foram definidas na configuração do servidor principal.'
 - Rede(s) remota(s) IPv4:** 172.14.1.0/24 (highlighted with a red box). Below it, a note states: 'Estas são as redes do lado do cliente IPv4 que serão encaminhadas para este cliente usando especificamente o iroute, de modo que uma VPN de site para site possa ser estabelecida. Expresso como uma lista separada por vírgulas de um ou mais intervalos CIDR. Pode ser deixado em branco se não houver redes do lado do cliente a serem encaminhadas. NOTA: Lembre-se de adicionar essas sub-redes à lista de redes remotas IPv4 nas configurações do servidor OpenVPN correspondentes.'

Figura 11.

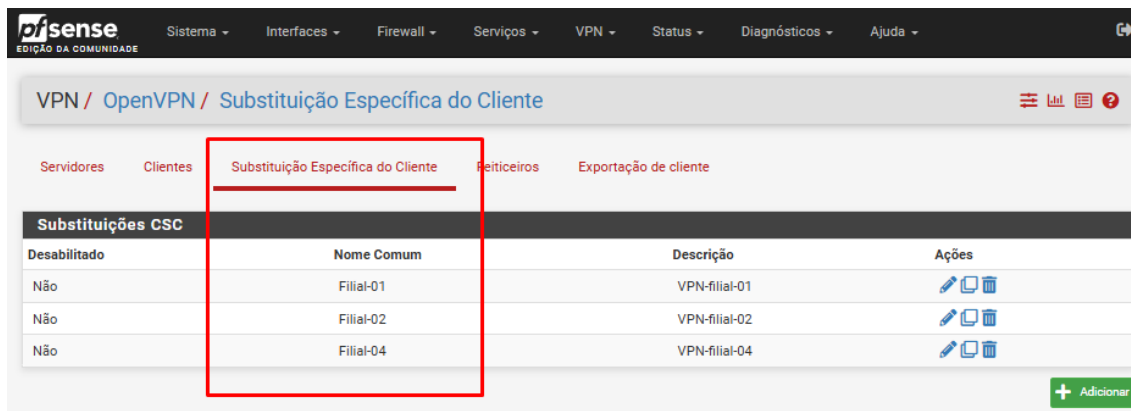


Figura 12.

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

Dentro do *firewall* Servidor copiaremos os dados do certificado e chave primária 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.

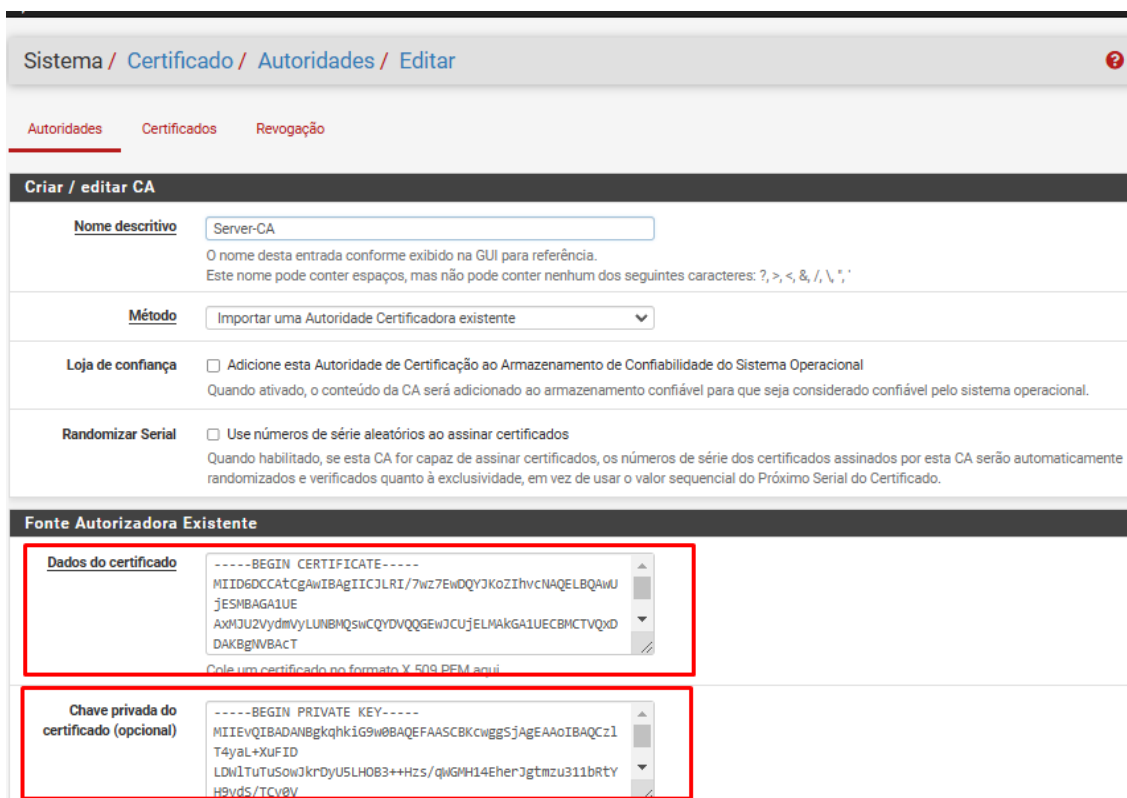


Figura 13.

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

OPENVPN E SUA APLICAÇÃO EM AMBIENTE EMPRESARIAL
Paulo Marcelo Gervasio Fernandes, Edimar Soares de Oliveira

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

Com o certificado adicionado, será 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.

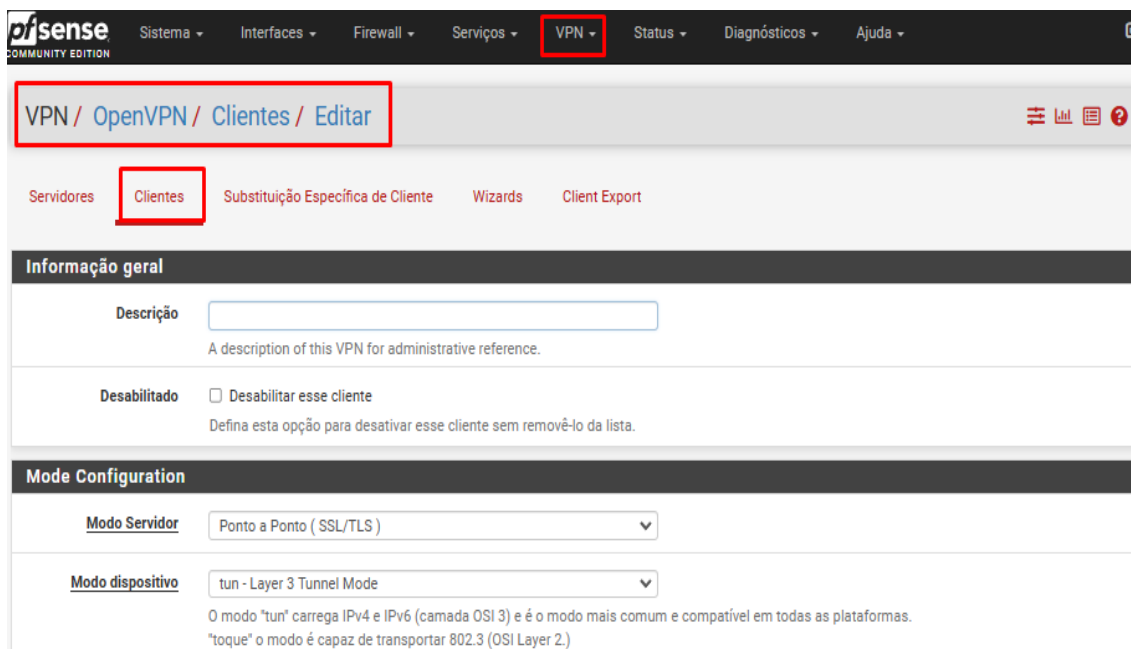


Figura 14.

No campo de configuração utilizaremos o mesmo protocolo UDP. A comunicação será 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.

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



Endpoint Configuration	
Protocolo	UDP on IPv4 only
Dispositivo	WAN <small>A interface usada pelo firewall para originar esta conexão de cliente OpenVPN</small>
Porta local	1212 <small>Defina esta opção para vincular a uma porta específica. Deixe isso em branco ou insira 0 para uma porta dinâmica aleatória.</small>
Servidor host ou endereço	199.54.987.242 <small>O endereço IP ou o nome do host do servidor OpenVPN.</small>
Porta do servidor	1111 <small>A porta usada pelo servidor para receber conexões de clientes.</small>
Host de Proxy ou endereço	<input type="text"/> <small>O endereço para um proxy HTTP que este cliente pode usar para se conectar a um servidor remoto. TCP deve ser usado para o protocolo do cliente e do servidor.</small>
Porta do Proxy	<input type="text"/>
Autenticação de proxy	nenhum <small>O tipo de autenticação usada pelo servidor proxy.</small>

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

OPENVPN E SUA APLICAÇÃO EM AMBIENTE EMPRESARIAL
Paulo Marcelo Gervasio Fernandes, Edimar Soares de Oliveira

Configurações de Criptografia

Configuração TLS Use uma chave TLS

Uma chave TLS aumenta a segurança de uma conexão OpenVPN, exigindo que ambas as partes tenham uma chave comum antes que um peer possa executar um handshake TLS. Esta camada de autenticação HMAC permite que os pacotes de canais de controle sem a chave apropriada sejam descartados, protegendo os pares do ataque ou conexões não autorizadas. A Chave TLS não tem nenhum efeito sobre os dados do túnel.

Chave TLS

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
82c30abc0d686cb75326c3ef9099d4e2
```

Cole a chave TLS aqui.
Esta tecla é usada para assinar pacotes de canais de controle com uma assinatura HMAC para autenticação ao estabelecer o túnel.

Modo de uso de chave Autenticação de TLS

TLS
No modo de autenticação, a chave TLS é usada apenas como autenticação HMAC para o canal de controle, protegendo os pares de conexões não autorizadas.
Encryption e Authentication também criptografa a comunicação do canal de controle, proporcionando mais obstrução do canal de controle de privacidade e controle de tráfego.

TLS keydir direction Use default direction

The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Autoridade de certificação de Peer Sever-CA

Lista de revogação do certificado intermediário No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager > Certificate Revocation](#)

Certificado de Cliente Filial-01 (CA: Sever-CA, Em Uso)

Figura 16.

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

Status / OpenVPN

ovpns1: Server UDP4:11000 / Conexões de Clientes: 3

Nome Comum	Endereço Real	Endereço Virtual	Last Change	Bytes Sent	Bytes Received	Cipher	Ações
Filial-02	[Redacted]	[Redacted]	2024-10-31 10:50:26	666,46 MiB	579,04 MiB	AES-256-CFB	X X
Filial-01	[Redacted]	[Redacted]	2024-10-31 10:43:50	179,01 MiB	184,51 MiB	AES-256-CFB	X X
Filial-04	[Redacted]	[Redacted]	2024-10-31 10:50:51	338,58 MiB	291,53 MiB	AES-256-CFB	X X

Figura 17.



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.