Fatec
Americana
Ministro Ralph Biasi

Configuração de VPN site-to-site e client-to-site com OpenVPN e routerboard MikroTik.

Elaborador:	Eduardo Mosna | Matheus Pissaia de Moraes
Orientador:	Marcus Vinícius Lahr Giraldi

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

M87c MOSNA, Eduardo

Configuração de VPN site-to-site e client-to-site com OpenVPN e routerboard MikroTik. / Eduardo Mosna; Matheus Pissaia de Moraes. – Americana, 2020.

134f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Marcus Vinícius Lahr Giraldi

1 Rede de computadores 2. VPN – rede de computadores I. MORAES, Matheus Pissaia de II. GIRALDI, Marcus Vinícius Lahr III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.519

EDUARDO MOSNA
MATHEUS PISSAIA DE MORAES

CONFIGURAÇÃO DE VPN SITE-TO-SITE E SITE-TO-CLIENT COM OPENVPN E ROUTERBOARD MIKROTIK

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança da Informação

Americana, 30 de junho de 2020.

Banca Examinadora:

Marcus Vinícius Lahr Giraldi (Presidente)
Especialista
Fatec Americana

Henri Alves de Godoy (Membro 1)
Mestre
Fatec Americana

Diógenes de Oliveira (Membro 2)
Mestre
Fatec Americana

SUMÁRIO

Lista de figuras

Lista de tabelas

1 Introdução

Todos os dias, milhares de empresas passam por processo de expansão em sua infraestrutura interna, podendo este ser definitivo ou até mesmo provisório. Esse processo pode incluir remanejamento interno do layout dos departamentos, criação de novos espaços, ampliação física do prédio local ou até mesmo extensão de sua estrutura para outro local, ou seja, um novo ponto físico, em diferente endereço, podendo este ser na mesma cidade de atuação ou até em outra cidade, estado ou país. Para que tal processo alcance o êxito, um projeto deve ser bem elaborado, aprovado, acompanhado e devidamente executado.

Sendo assim, toda a infraestrutura de tecnologia da informação (T.I.), física e lógica, deve ser planejada, para que, independentemente do local onde o funcionário estiver alocado, ele consiga acessar as informações necessárias para que possa entregar suas atividades diárias, sem nenhum impacto ou outro tipo de preocupação. E para que isso aconteça de maneira transparente ao funcionário, é comum as empresas recorrerem à tecnologia para encurtar tais distâncias, visto que na maioria dos casos não é possível ou tão simples de resolver apenas com a instalação de um cabo de comunicação, sendo este um cabo ethernet ou uma fibra ótica, para conectar as duas pontas em questão.

Tal solução pode não ser adotada devido há vários outros fatores, tais como: a distância entre os locais ser muito longa; o custo com essa interconexão ser alto demais; o tempo de execução e instalação não atender ao prazo de início das atividades; ou até mesmo, se a necessidade for para um período provisório, o investimento tornar-se um desperdício de recursos em poucos dias.

A devida solução deve ser projetada levando em consideração todos os aspectos do cenário atual do cliente, inclusive o valor do investimento que será disponibilizado para atender a situação e a disposição geográfica dos locais, facilitando assim a decisão pelo melhor projeto. Este, por sua vez, deve descrever qual é a infraestrutura física e logica que será utilizado para prover a solução e atender a expectativa do cliente.

Conforme o contexto descrito, a empresa que trabalhamos, a E&M Soluções e Consultoria em Tecnologia da Informação, foi contratada pela Quatro Cambalhotas, empresa de papelaria criativa e personalizados para eventos, festas e buffets, com sede em Santa Bárbara d’Oeste (SBO) e com expansão em Americana (AMR), para elaborar um projeto que interligue, com tecnologia da informação, seu ateliê de

criação, situado em SBO (na Rua do Césio, número 1270, bairro Vila Mollon IV) com seu salão de festas, recém locado, em AMR (na Av. Armando Sales de Oliveira, número 485 e no bairro Jardim Ipiranga), cidades vizinhas e ambas no estado de São Paulo.

O projeto decidido pelo cliente foi relatado, tecnicamente, neste documento e algumas das informações (endereços IP, usuários e senhas), por caráter de segurança, foram substituídas ou ocultadas, quando citadas nos menus e itens de configuração dos equipamentos que foram utilizados.

2 Sobre o cliente

Nosso cliente, a Quatro Cambalhotas, uma empresa relativamente jovem, fundada em 2018, iniciou atividade com uma infraestrutura de T.I. do tipo doméstica, instalada em um cômodo, na residência de um dos sócios, em Americana/SP. A partir de um notebook, uma impressora *laserjet* colorida, uma impressora *plotter* de recorte, muita criatividade e disposição por parte dos sócios, a empresa conquistou clientes, ganhou espaço no mercado e cresceu. Esse último fator – crescimento – fez com que os sócios procurassem um novo local para instalar a sede da empresa e foi em Santa Bárbara d'Oeste/SP, numa simples casa de bairro, que o ateliê de criação da Quatro Cambalhotas nasceu.

A Figura 1 ilustra o logotipo da empresa Quatro Cambalhotas.

Figura 1. Logotipo da empresa Quatro Cambalhotas

Fonte: Os autores

Ainda com uma infraestrutura de T.I. muito simples, mas com a preocupação de tornar o ambiente mais profissional, confiável e seguro, os empresários investiram em tecnologia para melhorar a rede de dados do local. Dentre as aquisições, contrataram um provedor ISP[1], instalaram um servidor de arquivos e mais uma ilha de criação, composta por um desktop e duas impressoras plotters de recorte.

Com pouco tempo no mercado, a empresa firmou-se e os empresários, Junior e Vinícius, tiveram a ideia de explorar um novo segmento, dentro do contexto do ramo de atuação, e em um imóvel em Americana/SP, o salão de festas e *buffet* infantil surgiu.

Acompanhado ao novo negócio, a necessidade de criar uma rede de dados, para que o atendimento ao cliente pudesse ocorrer, foi providenciada no local. Contrataram um provedor ISP e o instalaram no escritório do salão, proporcionando assim a utilização da internet para o notebook do sócio Vinícius, diretor comercial da Quatro Cambalhotas.

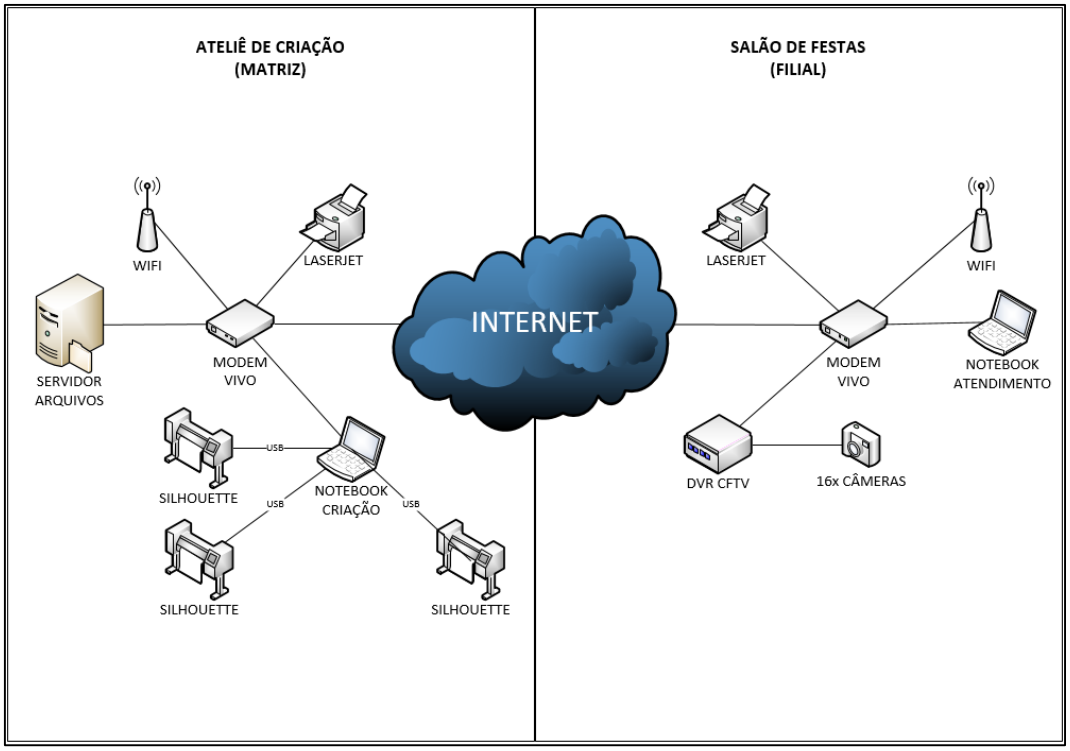
Com o passar dos dias, o empresário percebeu o tempo desperdiçado copiando, do servidor para um *pendrive*, minutos antes da reunião, os arquivos que seriam apresentados ao seu cliente, no salão de festas. Quando não por esse processo, solicitava que algum funcionário do ateliê de criação enviasse os arquivos para seu e-mail, também uma tarefa difícil e demorada, pois dependia sempre da disponibilidade do fator humano para tal ação e, sendo este, o principal motivo que levou os sócios a procurarem pela E&M Soluções e Consultoria em Tecnologia da Informação, de Americana/SP.

Em resumo, o pedido dos empresários consistia na possibilidade de unir as duas redes de dados e também proporcionar uma alternativa de acesso remoto ao ambiente Quatro Cambalhotas, para acessarem os arquivos hospedados no servidor, quando não estivessem em nenhum dos locais, e tais recursos a partir de tecnologia segura, confiável e de baixo custo. E tudo isso à um curto prazo de implantação, pois estavam prontos a inaugurar o salão de festas.

A Figura 2 ilustra qual era o cenário atual do cliente antes da implantação do projeto.

[1] Sigla do termo em inglês *Internet Service Provider* ou provedor de serviço internet, e que se refere as empresas ou corporações que fornecem às pessoas acesso à internet por um valor contratual.

Figura 2. Infraestrutura de T.I. Quatro Cambalhotas



Fonte: Próprio autor

3 Objetivo

Mediante inúmeras possibilidades e opções disponíveis atualmente no mercado de equipamentos e produtos para T.I., planejar uma solução que contempla as necessidades e expectativas do cliente é sempre um desafio, ainda mais quando temos que considerar diversas vertentes, tais como a tecnologia adotada, sua eficiência, seu custo, o tempo de implantação, a garantia e acima de tudo, a segurança.

Dentre os equipamentos, *softwares*, protocolos e serviços dispostos, foi utilizado, para a criação do projeto, produtos que são facilmente encontrados e comercializados em lojas *online* em *sites* na internet e em lojas físicas e especializadas em suprimentos para T.I., também conhecidos como produtos de prateleira à pronta entrega e com valores, na média, mais acessíveis.

Após a definição dos produtos, foi possível projetar uma solução de implantação simples, rápida, segura e de baixo custo, que foi o fator decisivo por sua escolha, visto que o salão de festas ainda é uma aposta para os empresários e por este motivo foram tão cautelosos quanto ao investimento.

Com isso, nosso objetivo neste documento é apresentar o projeto físico e lógico que foi desenvolvido e contratado para atender à necessidade informada, considerando alguns pontos solicitados pelo cliente (relacionados ao prazo de entrega e o valor do investimento destinado para a implantar a solução).

4 Revisão de conceitos

De modo a facilitar a elaboração deste documento, abordamos neste capítulo, as tecnologias que foram utilizadas para a realização deste projeto. Essas tecnologias serão citadas de maneira conceitual e resumida, no entanto, as configurações realizadas para cada uma delas serão descritas no decorrer dos próximos capítulos, conforme foram empregadas nas etapas de configuração dos equipamentos.

São tecnologias muito conhecidas no universo de redes de computadores e comum na grande maioria dos dispositivos, cuja finalidade é prover a conexão entre ambientes, interligando equipamentos e formando redes ainda maiores, rompendo limites estruturais e geográficos.

A partir desses novos caminhos de rede, conhecidos também como rotas, qualquer dispositivo pode alcançar e acessar outro, de qualquer lugar, mesmo este estando em uma rede diferente e distante, através de uma conexão direta, estável e segura, formada pelo tunelamento *VPN*, que foi o motivo por desenvolvermos esse relatório técnico. A seguir, iniciamos a abordagem e descrição conceitual dessas tecnologias.

4.1 WAN

WAN significa *Wide Area Network* ou rede de ampla abrangência, as *WANs* possibilitam a transferência de imagens, dados, áudio e vídeo por maiores distâncias geográficas, que podem compreender países ou continentes.

Temos dois tipos mais comuns de *WANs*, sendo:

- *WAN* Comutada: É geralmente formada por um roteador que se interliga a uma LAN ou outra WAN;
- *WAN* ponto a ponto: Para esse tipo de conexão é utilizado uma linha de provedora ou operadora que conecta uma *LAN* a um provedor de internet (ISP).

A Internet é basicamente formada por *LANs*, *MANs* e *WANs*, todas se interligando para entregar os dados enviados, por exemplo, pensando em um âmbito doméstico, temos os hosts que são basicamente os aparelhos de uso pessoal e as sub-redes de comunicação que pertencem a operadora ou provadora de internet. A sub-rede se encarrega de transportar os dados enviados da rede A a rede B (através de *LANs*, *MANs* e *WANs*).

A sub-rede é constituída por duas partes: elementos de comutação e linhas de transmissão. As linhas de transmissão é o meio em que o dado trafega (o cabo físico), podendo ser fio de cobre, enlace de rádio, ou fibra óptica.

E os elementos de comutação são os dispositivos especializados que conectam as linhas de transmissão.

Uma rede geograficamente distribuída, ou *WAN* (*wide area network*), abrange uma grande área geográfica, com frequência um país ou continente. Ela contém um conjunto de máquinas cuja finalidade é executar os programas (ou seja, as aplicações) do usuário. (TANENBAUM, 2003, p. 30).

4.2 LAN

A sigla *LAN* significa *Local Area Network* ou rede local, é uma rede privada que interliga dispositivos em uma área, sendo local ou corporativo, uma *LAN* pode ser uma rede simples ou uma rede complexa, contendo um computador e uma impressora, ou múltiplos computadores, *switches* ou dispositivos conectados à mesma rede.

O tamanho de uma *LAN* é limitado a alguns quilômetros, que é uma das características que distinguem ela de outra rede, outra característica é a tecnologia de transmissão que é meio físico em que os pacotes trafegam dentro da rede e a última característica é a topologia, as mais comuns são: estrela, barramento e anel.

Uma rede local (*LAN*) é privada e interliga dispositivos em um escritório, prédio ou campus. (KUROSE; ROSS, 2014, p. 13).

4.3 Bridge

É um dispositivo de redes que serve para encaminhamento de pacotes entre dispositivos em uma *LAN*.

Há quatros tipos de *bridges*, sendo: *Bridge* Simples, *Bridge* Multiporta, *Bridge* Transparente e *Bridge* de rota de origem.

Em redes *LAN* a *bridge* tem efeitos positivos, sendo:

- Aumento na largura de banda;
- Diminui a probabilidade de colisões, pois sem a *bridge* e em uma rede regular, as máquinas ficariam disputando o acesso ao meio de transmissão, e com a *bridge* ocorre uma redução nesta probabilidade.

Ela é capaz de verificar o endereço de destino de um *frame* e decidir se este deve ser encaminhado ou descartado. Se o *frame* tiver de ser encaminhado, a decisão deve especificar a porta. Uma *bridge* tem uma tabela que associa endereços a portas (FOROUZAN, 2010, p. 448).

4.4 Protocolos e portas

Os protocolos são utilizados para comunicação entre as máquinas, quando você solicita alguma informação ou envia alguma informação, as máquinas utilizam protocolos para enviar essa mensagem.

Um protocolo define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou no recebimento de uma mensagem ou outro evento. (KUROSE; ROSS, 2014, p. 7).

As portas são utilizadas por diferentes tipos de aplicações, as portas são utilizadas juntamente ao protocolo e o endereço IP da máquina para diferenciar um computador e a aplicação em que solicitou ou enviou dados, através desta rede.

4.5 Endereço IP

O endereço IP, que significa *Internet Protocol*, é utilizado para identificar (no meio lógico) um dispositivo conectado a certa rede que utiliza o protocolo de Internet para comunicação.

Pensando no conceito de uma rede *LAN*, o *switch* (caso seja de camada 3) ou roteador, pode utilizar o IP para direcionar o pacote a uma máquina, equipamento ou rede específica, lembrando que o IP não identifica um dispositivo, mas sim o seu endereço de conexão naquele momento.

O IPV4 é definido por um número de 32 *bits*, e o IPv6 é composto 128 *bits*, o IPv6 está sendo implantado desde os anos 2000, para atender uma crescente demanda de dispositivos conectados à internet.

Um endereço IPv4 é um endereço de 32 *bits* que define de forma única e universal a conexão de um dispositivo (por exemplo, um computador ou um roteador) à Internet. (KUROSE; ROSS, 2014, p. 256).

4.6 DHCP

É um serviço/protocolo instalado e configurado em um servidor ou no próprio roteador, onde atribui as configurações *TCP/IP* a serem utilizados para as máquinas cliente, esse servidor é solicitado pelas máquinas (quando configuradas) assim que entram na rede, para conseguir suas configurações para fechar a conexão.

Esse serviço é muito prático, pois quando se instala diversos dispositivos em uma empresa ou residência não precisará configurar os endereços *TCP/IP* manualmente, e ele adicionará o endereço de forma dinâmica e configurável, utilizando tempo de requisição e empréstimo de endereços *TCP/IP*, baseado em um *pool* de endereços configurados no servidor ou roteador.

A primeira tarefa de um hospedeiro recém-chegado é encontrar um servidor *DHCP* com quem interagir. Isso é feito utilizando uma mensagem de descoberta *DHCP*, a qual o cliente envia dentro de um pacote *UDP* para a porta 67 (KUROSE; ROSS, 2014, p. 256).

4.7 DNS

DNS significa *Domain Name System*, é um sistema cliente/servidor que fornece os serviços de resolução de nome de domínio ou *site* em IP, por exemplo, enviando uma requisição para o endereço **www.google.com.br** e o serviço de *DNS* traduziu esse nome em IP, sendo **172.217.162.99(no dia 20/06/2020 estava com este endereço)**, que é o que faz sentido para a linguagem de máquina (para localizar na rede este endereço). Esse recurso é ótimo pois facilita o dia-a-dia e a experiência, utilizando a Internet todos os dias.

Em DNS há o servidor primário e o servidor secundário, sendo:

- Servidor Primário: É responsável pela manutenção e atualização dos endereços, ele armazena todas as informações em seu disco, a máquina cliente busca a máquina servidor para resolução dos nomes (tradução do nome em *ASCII* em endereço lógico e vice-versa);

- Servidor Secundário: O servidor secundário replica todas as informações do servidor primário.

O *DNS* foi projetado como uma aplicação cliente/servidor. Um *host* que precisa mapear um endereço a um nome ou um nome a um endereço chama um cliente *DNS* denominado resolvedor. O resolvedor acessa o servidor *DNS* mais próximo com uma solicitação de mapeamento. Se o servidor tiver a informação, ele atende à solicitação do resolvedor; caso contrário, faz que o resolvedor consulte outros servidores ou então solicita que outros servidores forneçam a informação (FOROUZAN, 2010, p. 806).

4.8 DDNS

DDNS ou *DNS* Dinâmico é um método para atualização dinâmica de uma base de dados de nome no *DNS* em tempo real, mas essa base deve ter a configuração ativa de *DDNS* dos nomes de *host* configurado e suas demais informações.

Ele é muito utilizado para aplicações ou *sites* que alteram o seu IP com frequência, para que não tenha que atualizar manualmente, pois ele fica constantemente rastreando, vinculando e atualizando o IP para o atual.

4.9 FIREWALL

O *firewall* é um dispositivo de segurança de rede que monitora o tráfego (entrada/saída) de dados e permite ou nega o acesso a computadores ou redes, baseado em regras.

O *firewall* pode ser um *software*, *hardware* ou os dois, e existem diversos tipos de *firewalls*, sendo os mais comuns:

- *Firewall* com inspeção de estado: Atualmente é o *firewall* conhecido como tradicional, é um *firewall* que inspeciona a porta, estado e protocolo do pacote. Este tipo de *firewall* monitora desde a abertura da conexão até o seu fechamento. Nesse tipo de *firewall*, o administrador configura as regras de filtragem e analisa os pacotes enviados anteriormente pela mesma conexão;
- *Firewall* de próxima geração (*NGFW*): É uma evolução dos *firewalls*, neste modelo eles fazem mais que apenas uma filtragem de pacotes e inspeção *stateful*, neste modelo o *firewall* é capaz de bloquear ameaças de *malware* e ataques na camada da aplicação;

- *Firewall UTM* (gerenciamento unificado de ameaças): Por padrão este dispositivo combina as funções do *firewall* com inspeção de estado e prevenção contra intrusos e antivírus;
- *Firewall* de *proxy:* Serviço oferecido pelo próprio servidor de *proxy*, mas pode ser algo negativo, pois pode afetar a aplicação e a taxa de transferência que passam por ele.

O *firewall* permite a um administrador de rede controlar o acesso entre o mundo externo e os recursos da rede que ele administra, gerenciando o fluxo de tráfego de e para esses recursos (KUROSE; ROSS, 2014, p. 538).

4.10 NAT

O protocolo *NAT*, que significa *Network Address Translation*, ou Tradução de Endereço de Rede, é o processo em que traduz um endereço público, para um endereço privado, através da alteração das informações de rede e informações de endereço encontradas no cabeçalho IP dos pacotes de dados.

Basicamente, trata-se de que quando um pacote é enviado para uma *LAN*, ele é enviado para o endereço do seu roteador e, assim que chega no roteador, é traduzido para o endereço que a máquina tem internamente (dentro de sua *LAN*), o processo ocorre no inverso também, quando um pacote é enviado de uma máquina interna, ele é traduzido utilizando *NAT* para um endereço que o mundo externo entenda sua origem/destino.

4.11 DMZ

A *DMZ*, conhecida como zona desmilitarizada (*demilitarized zone*), é uma área separada da rede interna da companhia, e nela contém os serviços que devem ter acesso direto e externo, como essa área tem um maior risco de ataque, os administradores de rede preferem deixar essa área apartada da rede para caso ocorra um ataque, será possível mitigar o dano causado e deixar a rede local segura contra o mesmo.

Muito utilizado para servidores *HTTP*, correio eletrônico e *FTP*, que geralmente tem grande acesso externo.

4.12 VPN

A rede privada virtual, conhecida como *VPN*, é uma tecnologia amplamente utilizada por organizações, pois ela possibilita uma máquina conectada à internet a conectar-se em uma rede específica de forma segura, pois ela utiliza a tecnologia *IPsec* no modo túnel para autenticar-se, garantindo assim integridade e privacidade.

Utilizando a mesma tecnologia citada no final do parágrafo anterior no modo túnel, cada datagrama IP destinado ao uso para a organização é encapsulado em outro datagrama, encriptando no envio e decrepitando no recebimento.

Essa tecnologia é amplamente utilizada no ambiente corporativo, pois as vezes o colaborador está fora do ambiente físico da empresa, mas precisa conectar-se para na rede da mesma, e pode utilizar desta forma está tecnologia.

Virtual Private Network (*VPN*) – Rede privativa virtual, tecnologia que cria uma rede privada virtual sob uma rede física pública (FOROUZAN, 2010, p. 1102).

4.13 OpenVPN

OpenVPN é um software livre utilizado para criar redes privadas virtuais (*VPN*), tipo *server-to-multiclient* ou *point-to-point*, utilizando a tecnologia de túnel criptografado.

Quando configurado de forma correta, é um pacote repleto de funcionalidades para criar uma *VPN* de forma segura e o funcionamento desta comunicação requer duas instâncias, sendo servidor e cliente, que se comunicam entre si.

Este *software* utiliza a biblioteca *OpenSSL* para promover a criptografia entre os canais de controle de dados, que ocorre nos protocolos *UDP* ou *TCP*, sendo que as camadas de segurança podem ser reforçadas por um sistema de antivírus ou *firewall* corporativo.

4.14 PPP

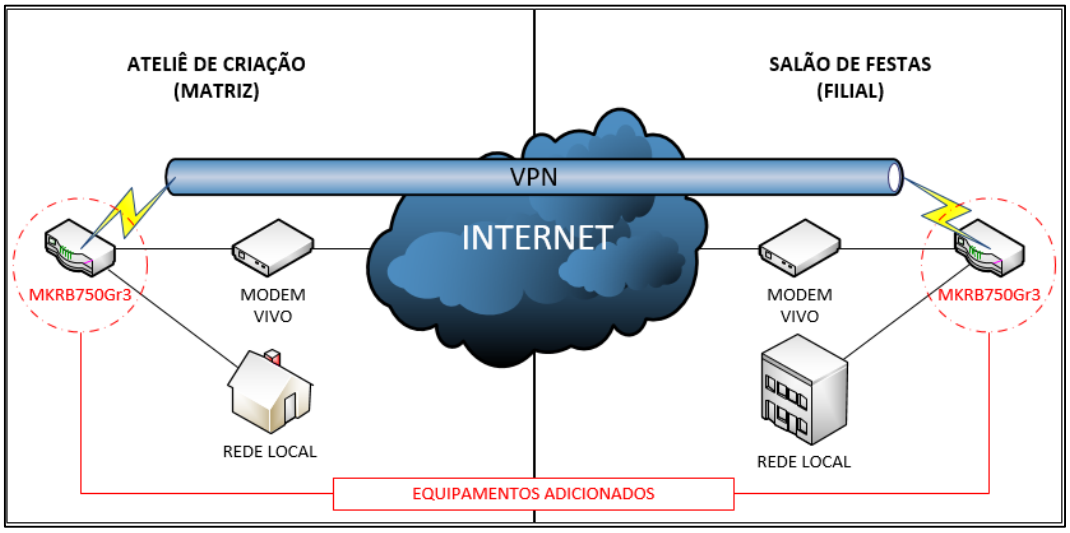
Sigla do termo em inglês *Point-to-Point Protocol* ou protocolo ponto-a-ponto, no português, é um protocolo da camada de enlace de dados, do modelo OSI, ele é utilizado para estabelecer conexão entre dois nós. Ele pode fornecer autenticação de conexão, criptografia de transmissão e compressão.

5 Desenvolvimento

Conforme aprovado pelo cliente, o projeto com o *routerboard* MikroTik RB750GR3 hEX foi utilizado em ambos os endereços da Quatro Cambalhotas, no ateliê e no salão de festas. Com a implantação dos equipamentos, foi possível realizar a criação da *VPN site-to-site* e *client-to-site*.

A Figura 3 ilustra a adição dos *routerboards* na rede local de cada endereço.

Figura 3. Adição dos *routerboards* nas redes locais



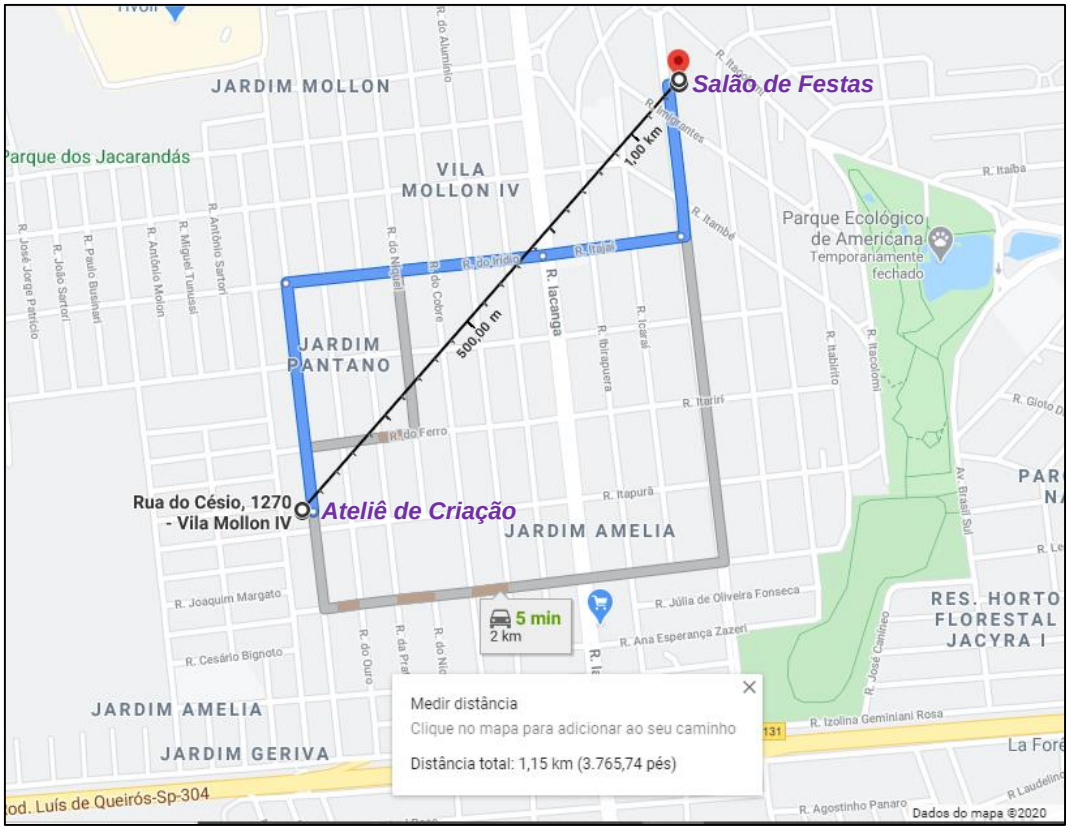
Fonte: Os autores

No decorrer deste documento, as configurações realizadas nos equipamentos serão descritas e ilustradas, de acordo com cada menu e item configurados, de forma breve e superficial. Estas configurações foram realizadas, em sua grande maioria, igualmente nos dois equipamentos, respeitando a rede lógica projetada para cada cenário.

5.1 Localização das empresas

As empresas estão distantes, em uma linha reta, em **1,15km**, conforme ilustrado na Figura 4. O ateliê de criação será abordado, neste documento, como a matriz e, o salão, consequentemente, como filial. Essas denominações facilitarão o entendimento das configurações que foram realizadas nos equipamentos.

Figura 4. Distância entre as empresas

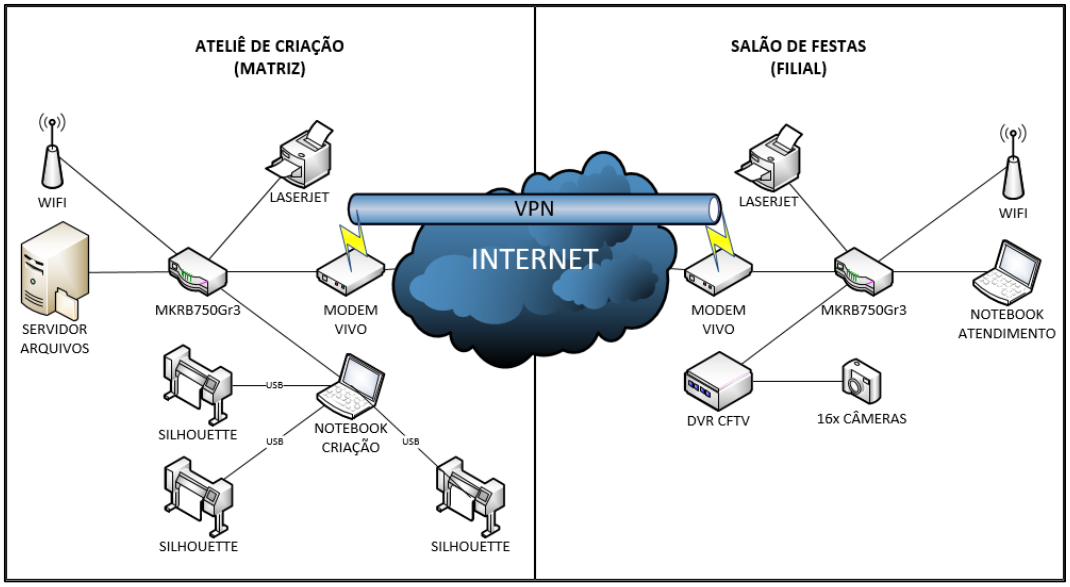


Fonte: Os autores

5.2 Projeto físico e lógico

Durante as etapas do projeto, algumas visitas foram realizadas nos locais da empresa Quatro Cambalhotas, onde foram coletadas as informações da infraestrutura de T.I. disponível nos endereços. Com as informações, foi criada a topologia ilustrada na Figura 5, que foi a base para a distribuição física dos equipamentos e a distribuição lógica dos endereços IP (*Internet Protocol address*) organizados no projeto.

Figura 5. Topologia da rede do cliente



Fonte: Os autores

5.2.1 Endereços de IP

Baseado nas informações já existentes e seguindo o que foi projetado, a distribuição de endereços IP configuradas nos equipamentos foram relacionadas em uma tabela, separando e organizando as informações entre a matriz e a filial, conforme são exibidas na Tabela 1.

Tabela 1. Lista de endereços IP – Matriz e Filial

ENDEREÇOS IP - ATELIÊ DE CRIAÇÃO & SALÃO DE FESTAS			
QUATRO CAMBALHOTAS		MATRIZ	FILIAL
MODEM VIVO	Dynamic address VIVO	201.1.127.10	201.1.127.130
	WAN mode (Router | Bridge)	Router	Router
	DDNS (NoIP)	quatrocambalhotas-mz.ddns.net	quatrocambalhotas-mz.ddns.net
	DHCP	192.168.15.10-192.168.15.129	192.168.15.130-192.168.15.249
	Wireless band	2.4 GHz | 5.0 GHz	2.4 GHz | 5.0 GHz
MIKROTIK RB750 Gr3	Interface WAN	182.168.15.11	192.168.15.131
	Local address	192.168.1.0/24	192.168.2.0/24
	Bridge LAN (Eth2|Eth3|Eth4|Eth5)	192.168.1.10	192.168.2.10
	Gateway	192.168.1.10	192.168.2.10
	DNS	192.168.1.10	192.168.2.10
	DHCP LAN	192.168.1.11-192.168.1.250	192.168.2.11-192.168.2.250
	Local address VPN	10.0.1.10	10.0.2.10
	DHCP VPN	10.0.1.11-10.0.1.25	10.0.2.11-10.0.2.25

Fonte: Os autores

Um endereço de protocolo da internet, vulgo endereço IP, do inglês *Internet Protocol address (IP address)*, é uma identificação numérica que é atribuída a cada

dispositivo (servidor, computador, impressora, smartphone, etc.) conectado a uma rede de computadores, que utiliza o protocolo de internet para comunicação e compartilhamento de recursos. Um endereço IP proporciona duas principais funções: identificação de interface de hospedeiro (ou de rede) e ao endereçamento de localização.

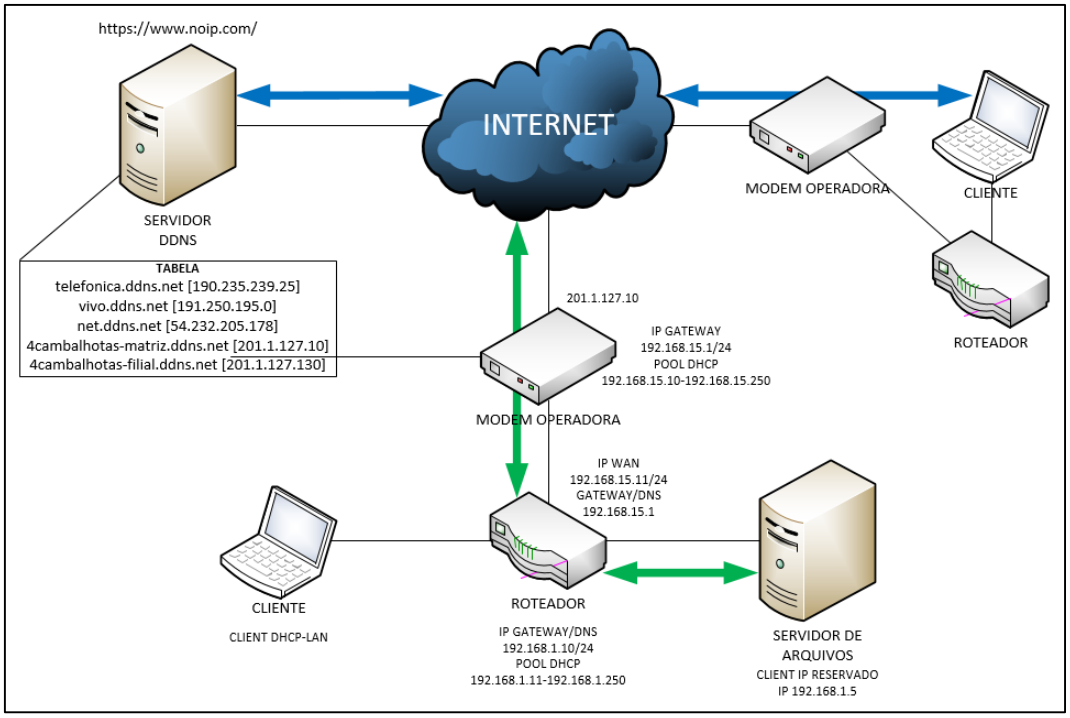
5.2.2 Registro no provedor No-IP

Foi criado uma conta e registrados os dois endereços *DDNS* no site do provedor No-IP[2], para publicar os *hostnames* **4cambalhotas-matriz.ddns.net** e **4cambalhotas-filial.ddns.net**, que foram utilizados na configuração dos equipamentos. Estes *hostnames* foram facilitadores na configuração da *VPN* entre os locais.

O site No-IP, que é administrado pela Vitalwerks LLC, é um provedor dinâmico de *DNS* (*DDNS*) para serviços pagos e gratuitos. O No-IP oferece serviços *DNS*, e-mail, monitoramento de rede e certificados *SSL* (*Secure Sockets Layer*). A Figura 6 ilustra um exemplo de consulta ao serviço *DDNS* feito pelo notebook cliente. Quando solicitado contato ao *DDNS* **4cambalhotas-matriz.ddns.net**, a requisição chega até os servidores *DNS,* local e externo, que se atualizam da informação do *host* hospedado no serviço *DDNS* do provedor No-IP. A resposta dessa requisição é retornada ao notebook cliente, já direcionando a conexão para o modem da operadora da matriz, cujo endereço IP está publicado na conta do usuário no provedor *DDNS*.

[2] Página disponível na URL <https://www.noip.com/remote-access>.

Figura 6. Exemplo de consulta ao serviço *DDNS*

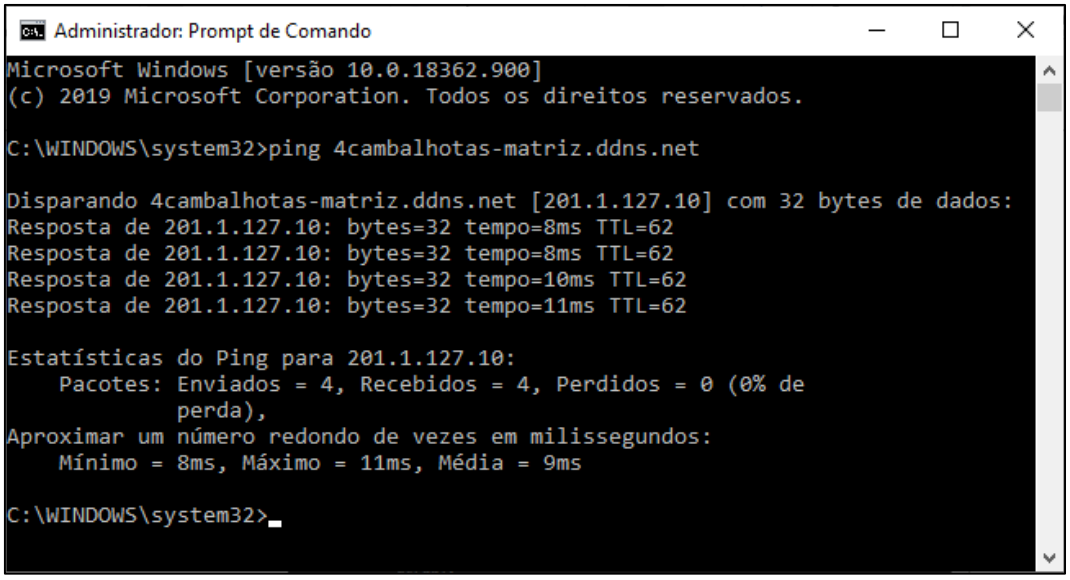


Fonte: Os autores

Escolhido o registro no provedor No-IP por disponibilizarem uma opção do serviço *DDNS* de forma gratuita. No entanto, foi comunicado ao cliente que sempre que seu endereço dinâmico da operadora VIVO for renovado em seus modems, eles terão que atualizar esses endereços no site No-IP manualmente, pois com a opção gratuita isso não ocorre automaticamente e deverá ser feito mensalmente (a cada 30 dias) para manter a configuração funcionando, visto que o cliente não contratou o serviço de link dedicado ou endereço de IP estático (IP fixo), junto a operadora VIVO, para os dois endereços da empresa.

Após registrados, foram testados via *prompt* de comando (*CMD*), no MS Windows 10, os *hostnames*. Primeiro foi testado o *DDNS* da matriz, teste este evidenciado na Figura 7.

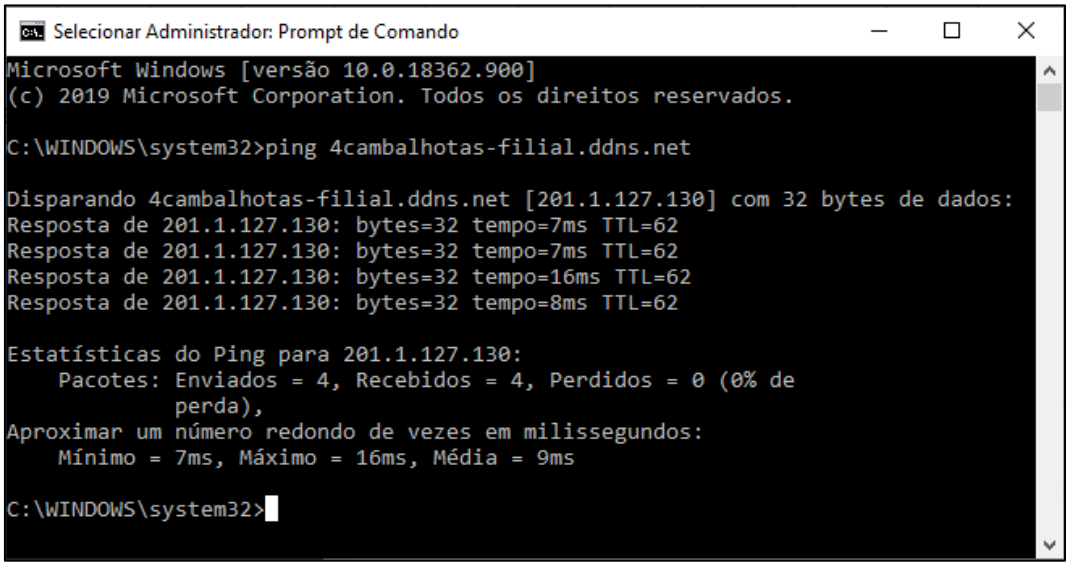
Figura 7. Teste *ping* para o *DDNS* da matriz



Fonte: Os autores

Em seguida, foi testado o *DDNS* da filial. A Figura 8 ilustra o resultado do teste, onde a resposta ao comando retornou êxito, pois a quantidade de pacotes enviados foi a mesma dos pacotes recebidos, sem nenhuma pacote perdido.

Figura 8. Teste *ping* para o *DDNS* da filial



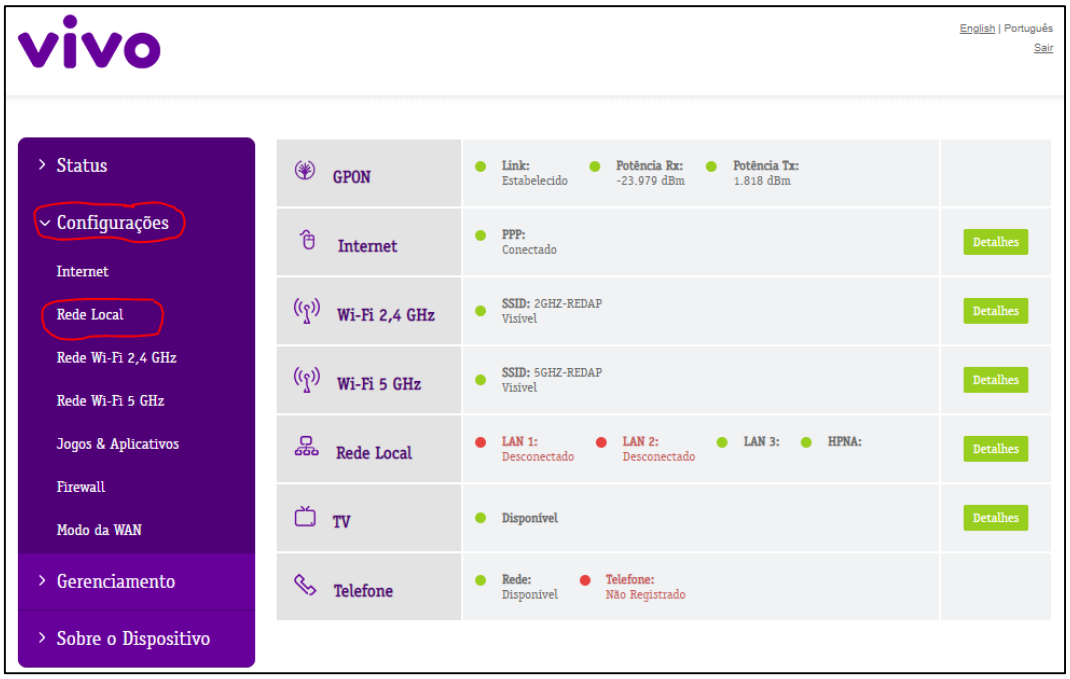
Fonte: Os autores

5.2.2.1 Liberação no modem da operadora de internet

Foi necessário realizar algumas liberações no modem da operadora, para que os serviços que utilizamos pudessem funcionar devidamente. Para isso, foi acessada

a interface *web* do modem da operadora, através do endereço IP **192.168.15.1,** estampado na etiqueta fixada na parte traseira do equipamento. A Figura 9 ilustra a interface inicial, onde foram realizadas, na zona da rede local, as configurações do *DDNS*, *DMZ* e Redirecionador de Portas. Navegado em Configurações > Rede Local para o acesso aos parâmetros mencionados.

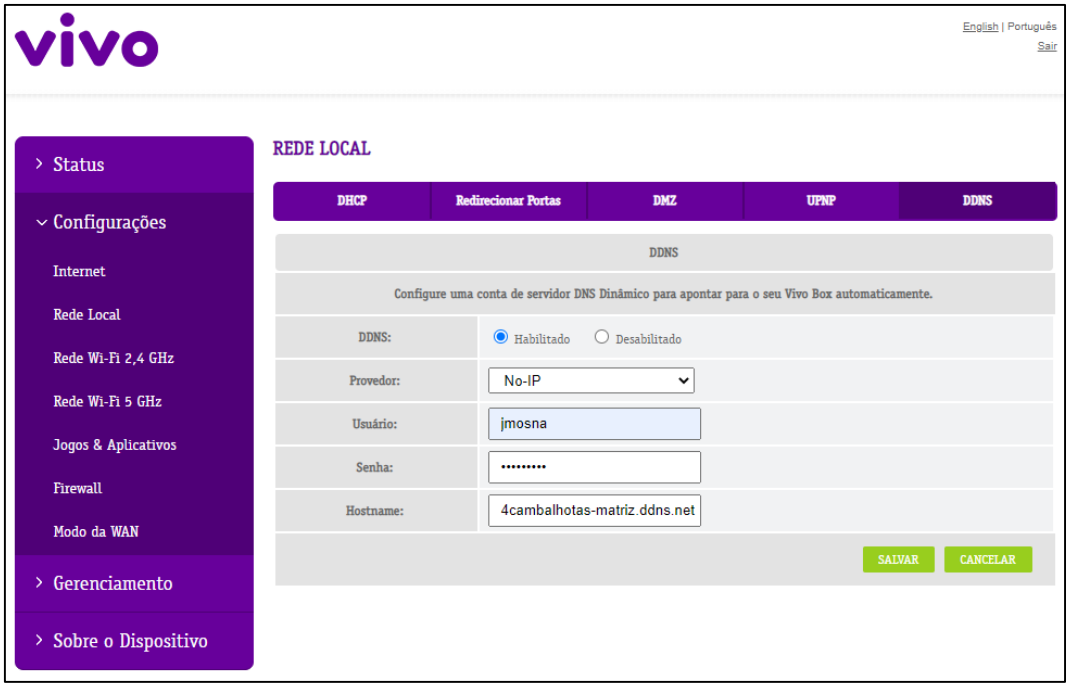
Figura 9. Interface *web* do modem da operadora



Fonte: Os autores

Acessado o menu *DDNS*, o recurso foi habilitado. Em seguida, na lista suspensa no campo Provedor, o item **No-IP** foi selecionado. Informado também, em seus respectivos campos, o **usuário**, a **senha** e o ***hostname***. São os mesmos que foram criados e utilizados no site do No-IP. Com um clique no botão Salvar, as alterações foram confirmadas. A Figura 10 ilustra essa configuração do *DDNS*.

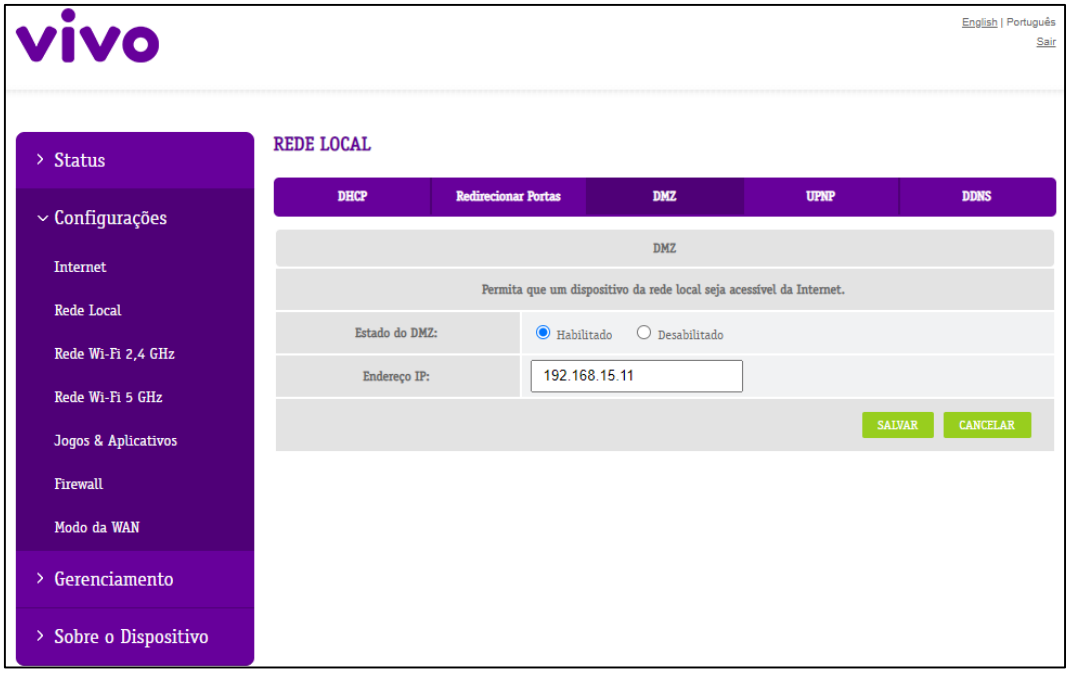
Figura 10. Configuração do *DDNS* no modem da operadora



Fonte: Os autores

Em seguida, o serviço *DMZ* foi **habilitado**. Também foi informado o endereço IP **192.168.15.11** da interface *WAN* do *routerboard* da matriz, endereço este que foi fornecido pelo serviço *DHCP* configurado no próprio modem da operadora. A Figura 11 ilustra os campos que foram preenchidos. As mesmas configurações foram realizadas no *routerboard* da filial, respeitando sempre o projeto logico de cada local.

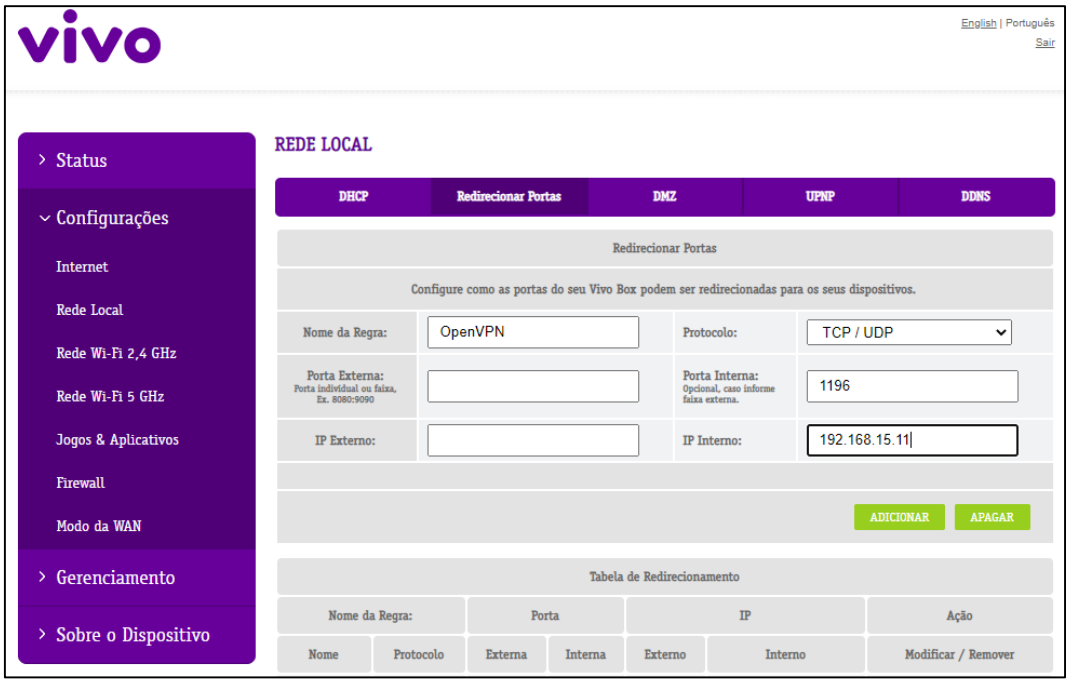
Figura 11. Configuração da *DMZ* no modem da operadora



Fonte: Os autores

De modo a evitar qualquer tipo de bloqueio relacionado à *VPN*, foi criada uma regra para o ***OpenVPN***. Foi escolhido o protocolo ***TCP/UDP***, a porta **1196** e informado o IP **192.168.15.11**, pertencente ao *routerboard* da matriz. Para aplicar as alterações, um clique no botão Adicionar. A Figura 12 exibe as configurações realizadas no item.

Figura 12. Configuração do Redirecionar Portas no modem operadora



Fonte: Os autores

Finalizadas as configurações, foi realizado o *logout* da interface *web* do modem da operadora e encerrada a janela do navegador.

5.2.3 Equipamentos utilizados

De modo a oferecer um projeto simples, rápido, eficiente e econômico, o equipamento escolhido para interligar as empresas do cliente através de um túnel *VPN* foi o *routerboard* da MikroTik, de modelo **RB750Gr3 hEX**. Esse roteador proporciona um excelente custo x benefício, pois possui recursos que geralmente são encontrados em roteadores mais robustos, de marcas renomadas no mercado de T.I., e que possuem valores mais elevados.

Para criar esse túnel, foi instalado um roteador em cada endereço, logo após o modem da operadora de internet e, interligado junto a este. O cliente já possui instalado em cada local um contrato VIVO Fibra 100Mbps convencional, para pessoa física (CPF). Vale lembrar que não foi contratado link dedicado ou o serviço de IP estático para nenhum dos locais, devido os valores serem maiores e o cliente não querer investir tanto, inicialmente, para este propósito.

5.3 MikroTik

MikroTik é uma empresa fabricante de equipamentos para redes de computadores com sede na Letônia. Comercializa roteadores e produtos com tecnologia *wireless*. Fundada em 1995 e com a intenção de comercializar no mercado emergente de tecnologias *wireless*, seus equipamentos foram bem aceitos por micros, pequenas e médias empresas e são muito utilizados por provedores de internet por banda larga e outras dos mais variados segmentos, tais como comércios, hotéis, universidades, residências, entre outros, e ficando mundialmente conhecida, devido aos equipamentos serem versáteis, estáveis e com valores mais acessíveis.

5.3.1 RouterOS

O *RouterOS*, um sistema operacional baseado em Linux, é o carro-chefe dos produtos da MikroTik, um dos principais comercializados. Ele permite que qualquer dispositivo com arquitetura *x86* (que se refere a uma família de processadores que tem como base o processador 8086 da Intel, originado em 1978) transforme-se num

robusto roteador, oferecendo funções como *VPN*, *Proxy*, *Hotspots*, Controle de Banda, Qualidade de serviço na banda (*QoS band*), *Firewall*, dentre outras, que podem variar de acordo com o nível de licença do sistema adquirido.

Utilizando o *RouterOS*, é possivel criar uma rede segura, com um *firewall* integrado eficiente e na concatenação de *links* (*link aggregation*). Além disso, a plataforma operacional conta com o suporte de protocolos de roteamento, entre eles *BGP*, *RIP*, *OSPF*, *MPLS*, entre outros. Um ótimo investimento, se comparado a outros que ofertam os mesmos recursos.

5.3.1.1 Administração do RouterOS

Para a administração do *RouterOS*, os métodos a seguir estão disponíveis:

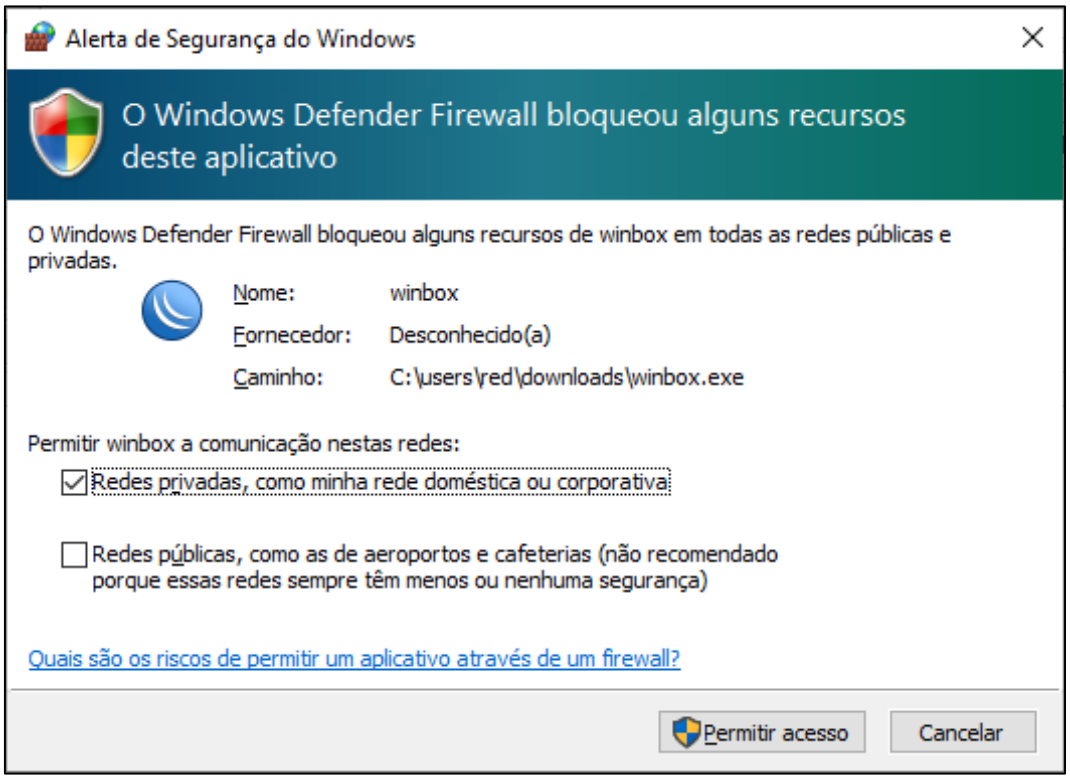
- *Command Line Interface (CLI)* — todas as funções podem ser configuradas por linha de comando via console (teclado e monitor e/ou remoto);
- *WinBox* — software de configuração com *Graphical User Interface (GUI)*, que roda em plataforma Windows, Linux ou MacOS. Oferece uma sofisticada *GUI* para o sistema, permitindo também conexões *FTP* (*File Transfer Protocol*) e *Telnet*, além de acesso via *SSH* (*Secure*.*Shell*). Disponível também o *RoMON* com *SafeMode* (protocolo proprietário *MikroTik*);
- *WEB (HTTP/HTTPS - remoto)* — configuração em ambiente *web*, porém com limitação para algumas versões (a partir da versão 5, o *Webfig* já tem acesso a configuração completa do *RouterOS*, sendo uma ferramenta muito boa para a sua configuração);
- *Dude* — *software* que permite a criação e manutenção de toda a rede. Permite o mapeamento da rede e também monitora em tempo real a banda dos *links* e funciona como ferramenta de monitoramento, indicando quando *hosts* estão ativos ou alarmando quando estão caídos.

Todas as configurações nos equipamentos foram realizadas através do aplicativo *WinBox*, que foi descarregado diretamente do site Mikrotik.com[3] e executado nos nossos notebooks corporativos. Ele dispensou instalação, pois é um aplicativo *portable* (portátil) e está disponível para as arquiteturas de 32 e 64 bits. Ao executá-lo, um alerta de segurança do Windows 10 foi exibido e optamos por liberar

[3] Download disponível na URL <https://MikroTik.com/download>.

a conexão ao *WinBox* apenas dentro de **redes privadas, doméstica ou corporativa**. Esse alerta foi evidenciado na Figura 13.

Figura 13. Alerta de segurança do *firewall* do Windows



Fonte: Os autores

5.3.1.2 Firewall

Uma outra função exercida pelos produtos MikroTik é a de *firewall*, um dispositivo de segurança de rede responsável por controlar e monitorar todo o tráfego de entrada e saída da rede, bem como todo o tráfego interno. Ele é uma espécie de filtro que libera ou bloqueia tráfegos específicos, de acordo com a definição de regras internas de segurança, configuradas pelo administrador ou responsável pela rede corporativa.

Um *firewall* pode ser baseado em *hardware* ou *software*:

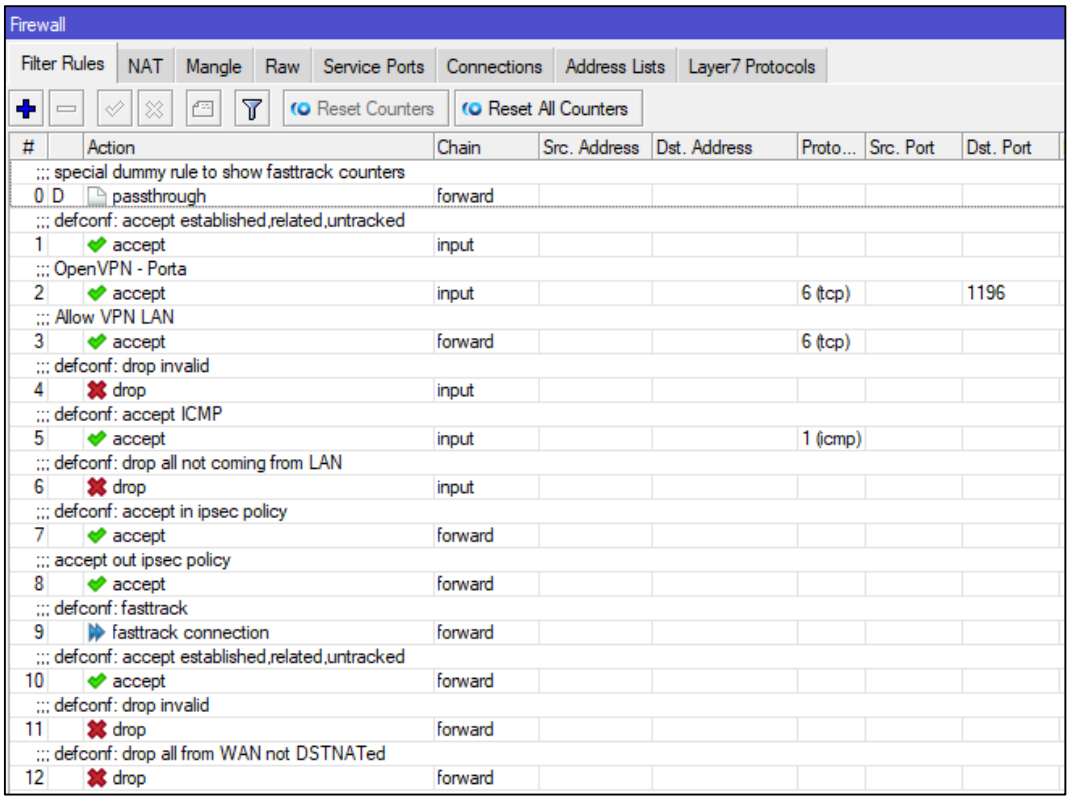
- O *firewall* baseado em *hardware* é um equipamento específico para o monitoramento e controle do tráfego dos pacotes de dados. Por isso, é o modelo mais utilizado no ambiente corporativo, por ser dedicado e por não haver necessidade de compartilhar recursos com outros programas e sistemas. Isso faz com que ele consiga suportar uma maior demanda e aplique filtros de maneira rápida e eficaz.

- O *firewall* baseado em *software* é um programa instalado nos servidores ou nos equipamentos designados para esta função. Ele pode vir nativo com o sistema operacional instalado ou pode ser instalado separadamente, após aquisição a do produto. É possível encontrar soluções de *firewall* gratuitas, geralmente as que são baseadas em código-aberto. O firewall é uma solução indispensável para a segurança do ambiente.

Vale ressaltar que a MikroTik vem ganhando espaço no mercado de T.I. por possuir funcionalidades inovadoras e simplificadas, estáveis e de fácil uso, especialmente pela interface de configuração que permite a implantação de complexas regras de *firewall* em questão de minutos.

Foi utilizado nas configurações dos roteadores as regras de firewall padrões embarcados no *RouterOS*, em sua versão estável atual, a **6.47**[4]. Essas regras foram revisadas e atualizadas após o término do projeto. Algumas dessas regras foram ilustradas na Figura 14.

Figura 14. Regras de *firewall* padrão na versão 6.47



Fonte: Os autores

[4] Versões disponíveis na URL <https://mikrotik.com/download/changelogs>.

Essas regras foram exportadas para um arquivo *backup* e as informações extraídas para montar a Tabela 2, de modo a manter um histórico das regras aplicadas nos equipamentos.

Tabela 2. Regras de *firewall* padrão na versão 6.47

REGRAS DE FIREWALL
/ip firewall filter
add action=accept chain=input comment="defconf: accept established,related,untracked" connection-state=established,related,untracked
add action=accept chain=input comment="OpenVPN - Porta" dst-port=1196 protocol=tcp
add action=accept chain=forward comment="Allow VPN LAN" disabled=yes dst-address=192.168.1.0/24 protocol=tcp src-address=10.0.1.0/24
add action=drop chain=input comment="defconf: drop invalid" connection-state=invalid
add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
add action=drop chain=input comment="defconf: drop all not coming from LAN" in-interface-list=!LAN
add action=accept chain=forward comment="defconf: accept in ipsec policy" ipsec-policy=in,ipsec
add action=accept chain=forward comment="defconf: accept out ipsec policy" ipsec-policy=out,ipsec
add action=fasttrack-connection chain=forward comment="defconf: fasttrack" connection-state=established,related
add action=accept chain=forward comment="defconf: accept established,related, untracked" connection-state=established,related,untracked
add action=drop chain=forward comment="defconf: drop invalid" connection-state=invalid
add action=drop chain=forward comment="defconf: drop all from WAN not DSTNATed" connection-nat-state=!dstnat connection-state=new in-interface-list=WAN
/ip firewall nat
add action=masquerade chain=srcnat comment="defconf: masquerade" ipsec-policy=out,none out-interface-list=WAN protocol=tcp
add action=dst-nat chain=dstnat comment="Allow DVR Seguran\E7a - Prime Guard" dst-port=3778 in-interface=pppoe-out1 protocol=tcp to-addresses=192.168.1.254 to-ports=3778
/ip firewall service-port
set ftp disabled=yes
set tftp disabled=yes
set irc disabled=yes
set h323 disabled=yes
set sip disabled=yes
set pptp disabled=yes
set udplite disabled=yes
set dccp disabled=yes
set sctp disabled=yes

Fonte: Os autores

5.3.2 RouterBOARD

Em 2002, a MikroTik decidiu fazer o seu próprio *hardware* e este foi batizado como *RouterBOARD*. *RouterBOARD* é o nome dado ao produto MikroTik que concilia o versátil e estável *RouterOS* (sistema operacional) com uma linha de *hardware* próprio, desenvolvido pelo laboratório letônio. Foi pensado e projetado para atender os provedores de pequeno e médios porte, oferecendo acesso à internet em banda larga via rede com ou sem fios. São equipamentos com transmissão por rádio ou

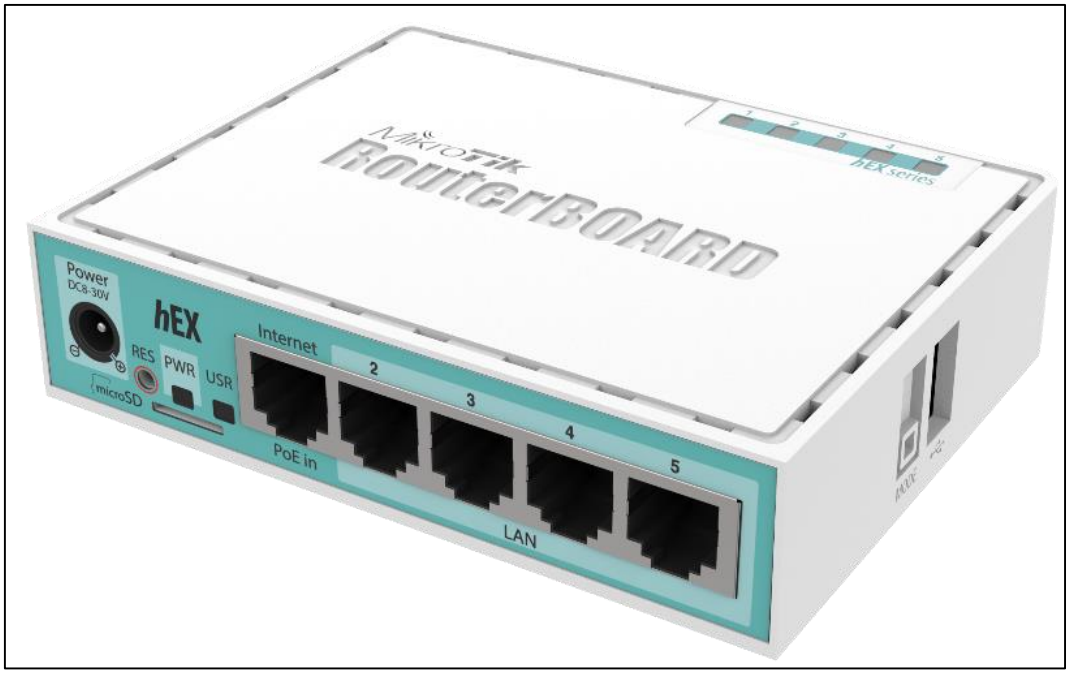
também roteadores compactos, que tem a capacidade de montar links *wireless* com alta capacidade de tráfego, inclusive utilizando duas antenas e uma configuração especial chamada *Nstreme*[5]. Além disso, conta com inúmeras ferramentas, funções e modos de operação, dais quais destacam-se:

- Roteador dedicado;
- *Bridge* com filtros em *layer2*;
- *Firewall* com *layer7* e diversos filtros;
- Controle de velocidade, garantia de banda, *burst*, hierarquia e disciplinas de filas;
- Ponto de Acesso *Wireless* modo 802.11 e proprietário, cliente *wireless*;
- *WDS*, *NSTREME*, *NSTREME Dual*;
- Concentrador *PPPoE*, *PPTP*, *IPsec*, *L2TP*, etc.
- Roteador de borda;
- Servidor *Dial-in* e *Dial-out*;
- *Hotspot* e gerenciador de usuários;
- *WEB Proxy* (*cache* de páginas e arquivos);
- Recursos de *Bonding*, *VRRP*, etc.;
- Virtualização com *Xen* e *MetaRouter*;
- Linguagem avançada de *scripts* e execução automática agendada;
- Roteamento com *OSPF*, *MPLS*, *BGP*, etc.;
- Ferramentas: *watchdog*, *bandwidth test*, *torch*, etc..

Conforme mencionado anteriormente, o modelo escolhido foi o **RB750Gr3** e a Figura 15 ilustra uma visão tridimensional do equipamento e seus componentes.

[5] *Nstreme* é um protocolo proprietário da MikroTik, que oferece baixa latência e serve para otimizar a rede, possibilitando um aumento considerável no *troughput* dos enlaces criados na rede.

Figura 15. *RouterBOARD* MikroTik hEX RB750Gr3



Fonte: Mikrotik.com[6]

Também foi criada a Tabela 3, onde as especificações técnicas do *hardware* podem ser visualizadas, de maneira ordenada, de acordo com suas categorias. As informações foram traduzidas do inglês, o idioma original, para o português, o nosso.

[6] Imagem disponível na URL <https://mikrotik.com/product/RB750Gr3>.

Tabela 3. Especificações técnicas do *routerboard*

Especificações da Routerboard RB750Gr3 hEX	
Descrição	**Informação**
Código do produto	RB750Gr3
Arquitetura	MMIPS
Processador (CPU)	MT7621A
Quantidade de núcleos (CPU)	2
Frequencia nominal (CPU)	880 MHz
Contagem de Threads (CPU)	4
Dimensões	113x89x28mm
Nível da licença	4
Sistema operacional	RouterOS
Capacidade da memória RAM	256 MB
Capacidade de armazenamento	16 MB
Tipo de armazenamento	FLASH
Temperatura ambiente testada	-40°C to 60°C
Preço sugerido	R$299,99 (US$59.99)
Energia	
Tipo de PoE in	Passive PoE
Voltagem da entrada PoE in	8-30 V
Número de entradas DC	2 (DC jack, PoE-IN)
Voltagem do plug de entrada DC	8-30 V
Consumo máximo de energia	10 W
Consumo máximo de energia sem acessórios	5 W
Interfaces Ethernet	
10/100/1000 Ethernet ports	5
Periféricos	
Tipo de cartão de memória	microSD
Quantidade de slots de cartão de memória	1
Número de portas USB	1
USB Power Reset	Sim
Tipo de slot USB	USB type A
Corrente (em A) máxima suportada na USB	1
Outros	
Temperatura do monitor PCB	Sim
Voltagem do monitor	Sim
Botão "Mode"	Sim
Certificação e Aprovações	
Certificação	CE/RED, EAC, ROHS

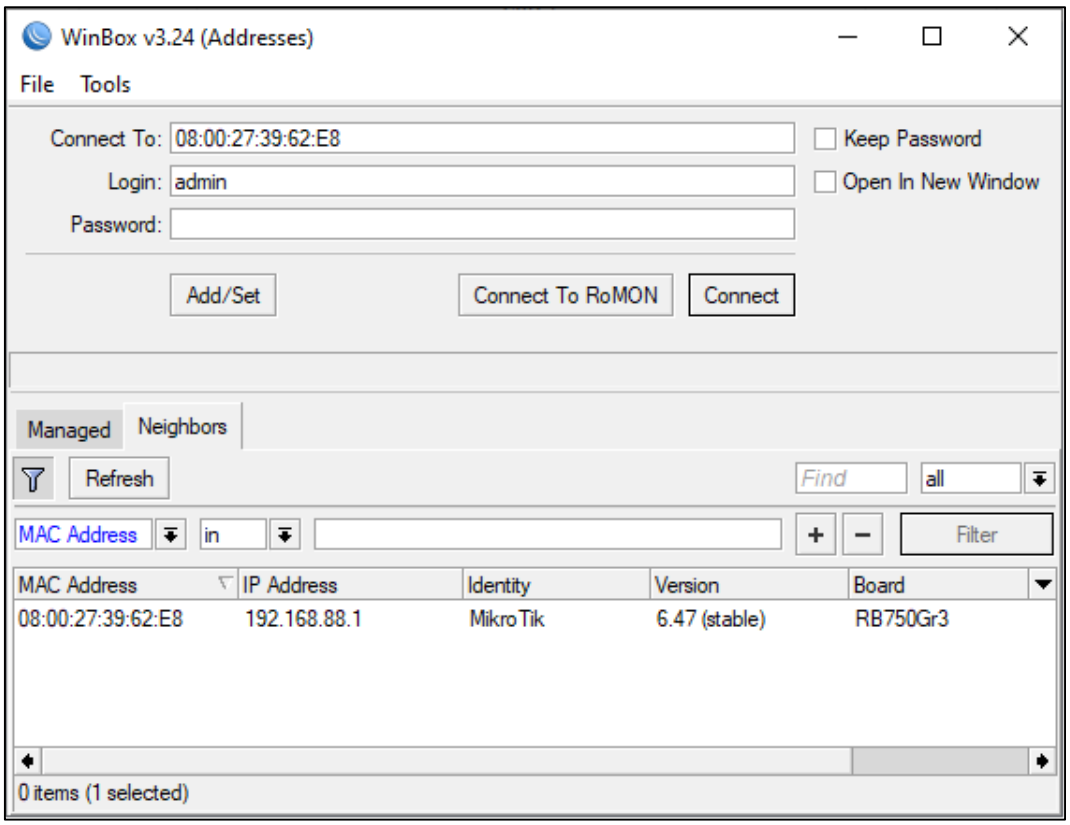
Fonte: Mikrotik.com[7]/

[7] Informações disponíveis na URL <https://mikrotik.com/product/RB750Gr3#fndtn-specifications>.

5.3.3 WinBox

O *WinBox* v3.24 foi executado e sua interface gráfica foi exibida. Por padrão de fábrica, o *routerboard* vem com o endereço IP **192.168.88.1**. No entanto, como a placa de rede *ethernet* do nosso notebook não estava setada com um IP de mesmo intervalo de rede, foi optado o acesso via *MAC address*[8], inicialmente. Confira na Figura 16.

Figura 16. Janela de conexão do *WinBox*



Fonte: Os autores

A credencial para *logon* na interface de configuração que o *RouterOS* carrega inicialmente é o usuário **admin** e a senha **em branco** (sem senha). Essas informações foram utilizadas para acessar a interface, digitadas nos campos *login* e *password*, respectivamente. Em seguida, um clique no botão *Connect*.

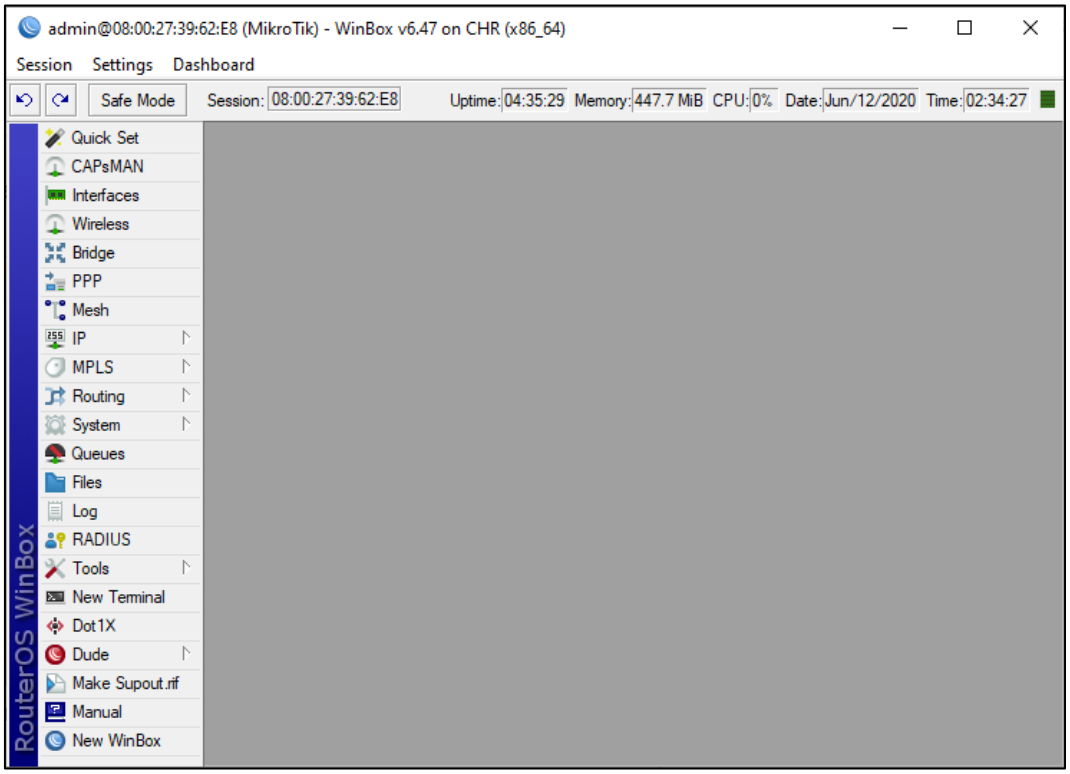
[8] Termo em inglês para *Media Access Control Address* (*MAC address*). É o endereço de controle de acesso à mídia de um dispositivo. É um identificador único e exclusivo, atribuído a uma interface de rede (ou do inglês *Network Interface Controller - NIC*).

Realizado a autenticação, a tela inicial do *WinBox* foi exibida. Ela é formada por uma barra horizontal e uma outra barra vertical, de menus e itens de parametrização, itens estes utilizados para a configuração dos equipamentos.

Por tratar-se de um projeto simplista e com necessidade de configuração apenas em funções básicas para funcionar, nem todos os menus e itens foram visitados e configurados, portanto não serão descritos ou ilustrados.

A Figura 17 exibe a disposição dos menus na tela inicial. Sua navegação é simples e bem intuitiva e alguns itens estão anexos nos menus principais. Não tivemos dificuldades em encontrar os itens que foram necessários para a configuração dos equipamentos.

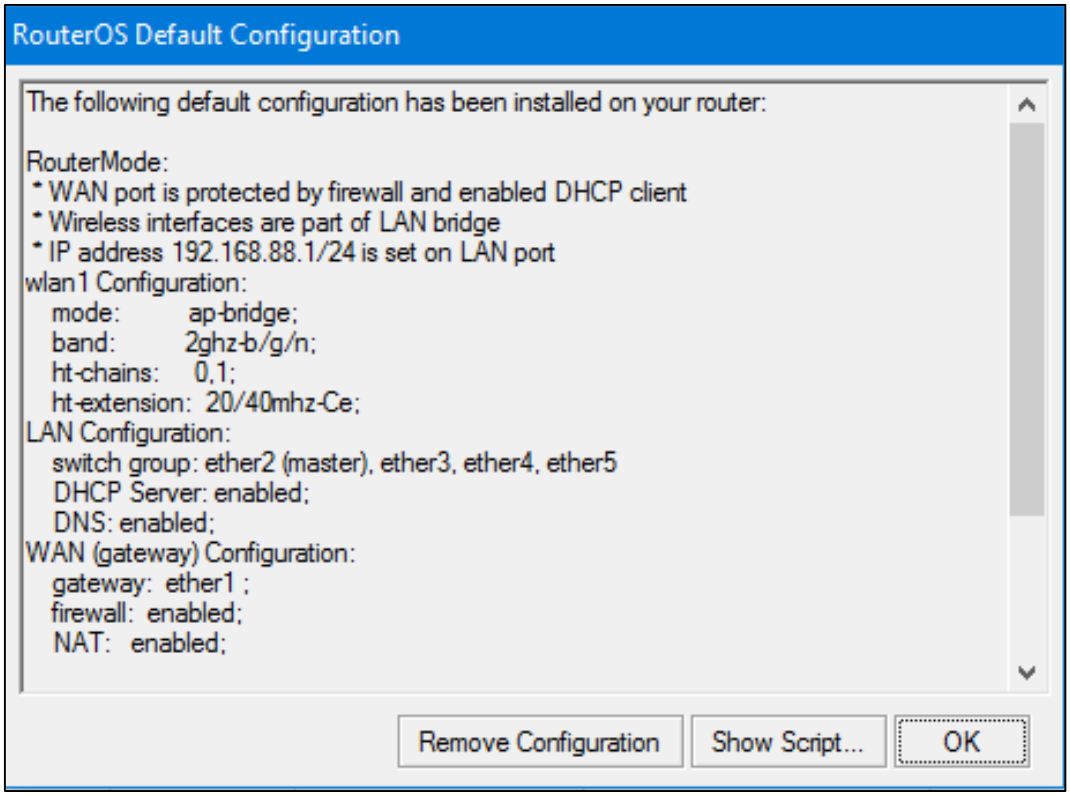
Figura 17. Sessão de usuário no *WinBox*



Fonte: Os autores

Importante mencionar que instantes após o acesso à interface de configuração, um aviso foi exibido, informando que o foi carregado pelo *RouterOS* a configuração padrão, de fábrica. A Figura 18 ilustra esse aviso. Para prosseguir, foi optado por assumir essa configuração com um clique no botão *OK*.

Figura 18. Aviso de configuração padrão do *RouterOS*



Fonte: Os autores

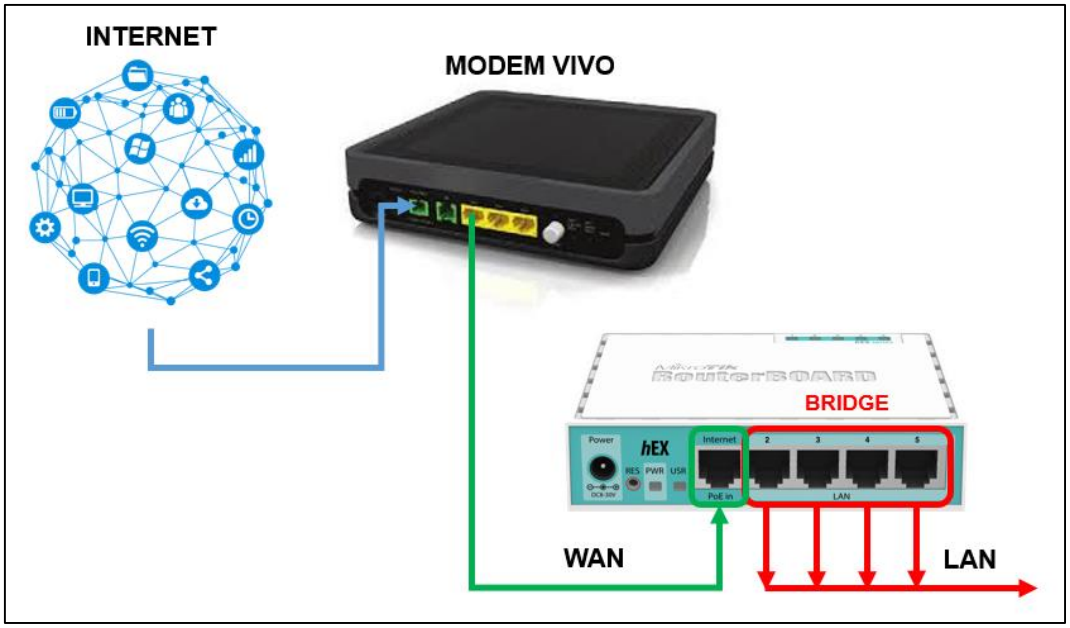
A partir deste ponto no documento, foram registradas as etapas de configuração dos equipamentos. As configurações foram semelhantes entre eles, alterado apenas o que foi necessário, de acordo com as informações disponibilizadas na Tabela 1.

5.4 Redes WAN e LAN

O *routerboard* possui cinco interfaces *gigabit ethernet*, das quais foram separadas, para utilização da rede *WAN*[9], a interface 1 e, para a rede *LAN*[10], as interfaces 2, 3, 4 e 5 (que juntas compõe a *bridge*[11] entre as interfaces *LAN*). A Figura 19 ilustra essa divisão das interfaces do *routerboard*.

[9] Sigla do termo em inglês *Wide Area Network – WAN*, que significa uma rede de longa distância ou rede de área alargada.
[10] Sigla do termo em inglês *Local Area Network – LAN*, e são denominadas como redes locais por cobrirem uma área geográfica mais limitada.
[11] Componente utilizado em redes de computadores que facilita a união entre dois equipamentos ou interfaces de acesso, criando uma ponte entre eles.

Figura 19. Designação das interfaces em *WAN* e *LAN* do *routerboard*



Fonte: Os autores

Na porta *WAN* do *routerboard* foi conectado um cabo *STP*[12], de categoria 6, que vem diretamente conectado da interface *ETH1* (nome de identificação) do modem da operadora. Não foi utilizado o cabo *UDP*[13], de mesma categoria, pois este cabo compartilha um eletroduto com outros cabos, inclusive alguns de energia elétrica. Essa mesma situação ocorreu nos dois endereços onde os equipamentos foram instalados, pois eles estão organizados e armazenados dentro de um móvel suspenso, fixado na parede, em cada local respectivo.

5.4.1 Configuração básica

Para que o equipamento possa prover as funções desejadas, algumas configurações mínimas foram realizadas, visto que o *routerboard* vem literalmente limpo de fábrica, sem nenhuma parametrização relevante para a continuidade do projeto.

As configurações realizadas nos dois *routerboards* são **semelhantes (~)** e as diferenças estão apenas nos endereços IP planejados para cada local. Sendo assim,

[12] Sigla do termo em inglês *Shielded Twisted Pair – STP*, que é um cabo de par trançado com blindagem, uma malha metálica que envolve os quatro pares. Utilizado em situações com grande exposição ou interferência eletromagnética.
[13] Sigla do termo em inglês *Unshieded Twisted Pair – UTP*, que é um cabo de par trançado sem blindagem. É o mais comum utilizado nos projetos de redes que não sofrerão com interferências eletromagnéticas relevantes ou moderadas.

as figuras ilustradas nesse documento foram tiradas das parametrizações feitas no *routerboard* da matriz, porém, as mesmas figuras foram utilizadas como roteiro para a configuração do *routerboard* da filial, substituindo devidamente as informações em seus respectivos campos.

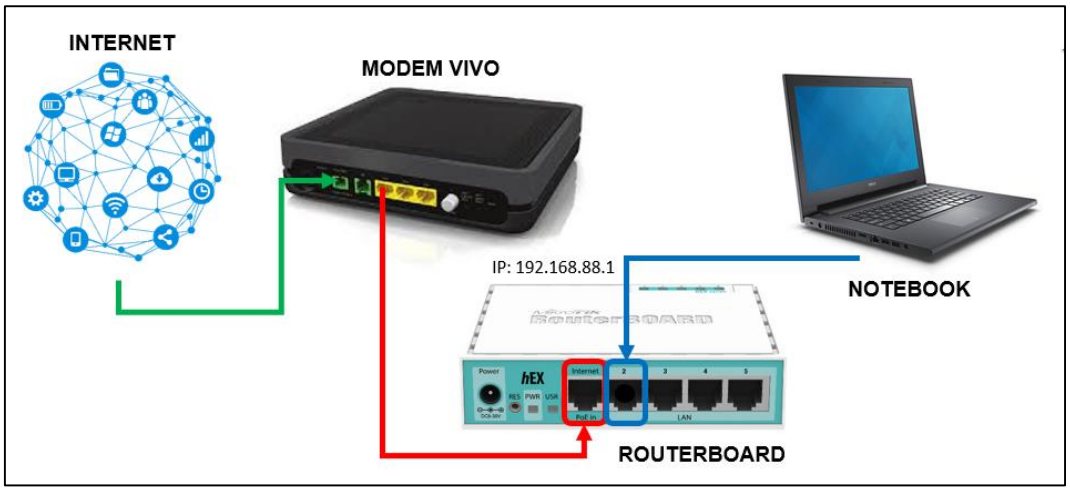
***Routerboard* matriz ~ *Routerboard* filial**

É importante dizer que para reduzir o tamanho deste documento, apenas as figuras relevantes do *routerboad* da filial foram evidenciadas e destacadas.

5.4.1.1 Método de configuração

Para facilitar a configuração, foi criada uma rede local entre nosso notebook e o *routerboard*. Para tal, foi conectado um cabo de rede entre a interface *ethernet* do notebook e a interface ***eth1*** do *routerboard*. A Figura 20 ilustra essa montagem local.

Figura 20. Conexão local entre notebook e *routerboard*



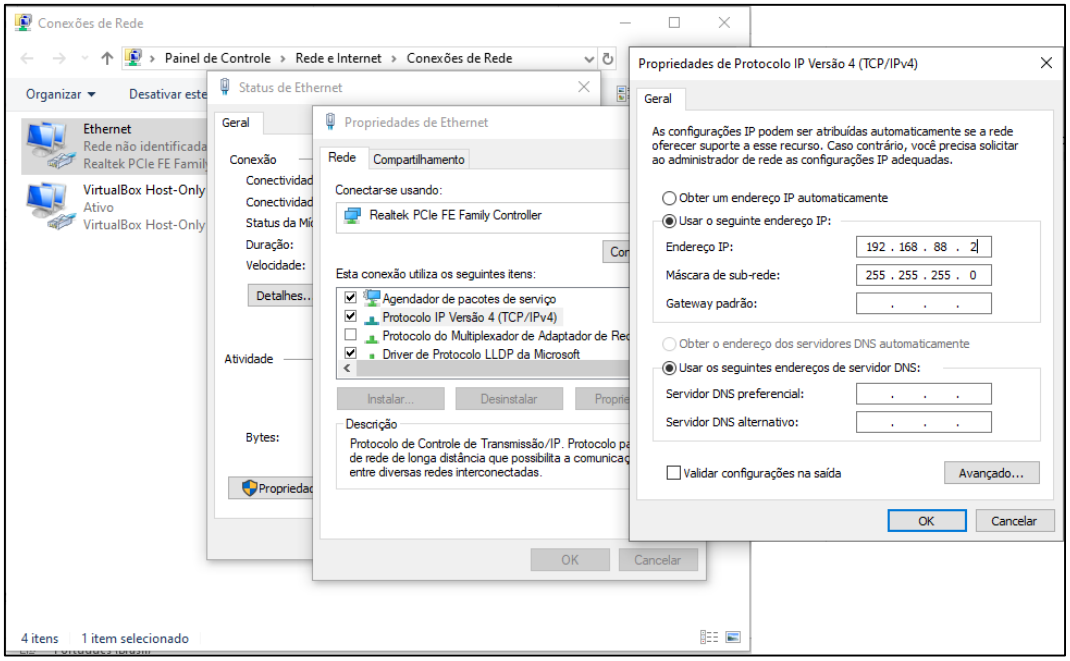
Fonte: Os autores

Foi escolhido um IP do mesmo intervalo de endereços da rede **192.168.88.0/24** do *routerboard* para a placa de rede *ethernet* do notebook, que viabilizou a conexão entre os equipamentos. Isso facilitou trabalharmos a configuração à nível de rede, a camada 3 do modelo OSI[14].

[14] O Modelo OSI, acrônimo do inglês *Open System Interconnection*, é um modelo de rede de computadores, com referência da ISO e dividido em camadas de funções, totalizado em sete. Foi criado em 1971 e formalizado em 1983, com objetivo de ser um padrão, para protocolos de comunicação entre os mais diversos sistemas em uma rede local do tipo *ethernet*, garantindo a comunicação entre dois sistemas computacionais (end-to-end).

Para isso, no Windows 10, foi acessado o Painel de Controle > Rede e Internet > Conexões de Rede > Adaptador Ethernet > Propriedades > Protocolo IP Versão 4 > Geral, e setado o IP **192.168.88.2/24**. Um clique no botão *OK* confirmou a configuração. O passo-a-passo desta configuração pode ser visualizado na Figura 21.

Figura 21. Configuração manual do endereço IP no adaptador de rede



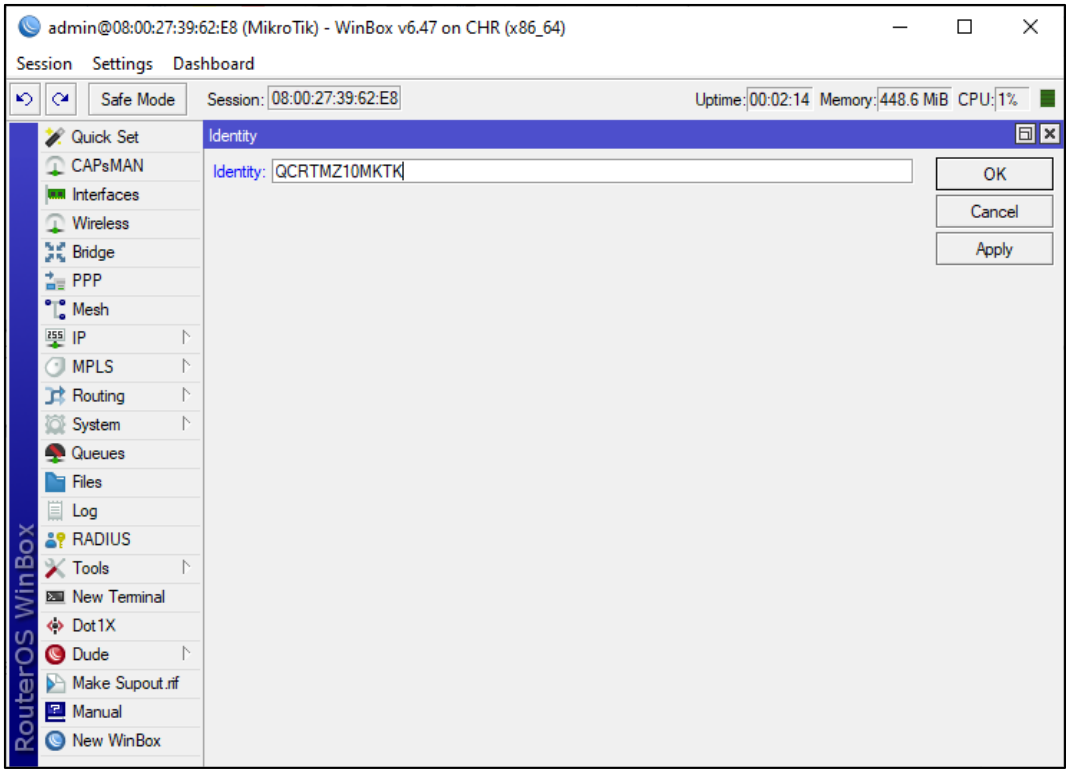
Fonte: Os autores

Foi executado o *WinBox* para dar continuidade na programação. O processo de conexão do *WinBox* com o *routerboard* pode ser revisitado na seção 5.3.3.

5.4.1.2 Identificação

O *hostname* do *routerboard* foi alterado, de acordo com o padrão que o cliente já aplica em seus equipamentos. Para alterar o nome, o menu *System* > *Identity* foi acessado e no campo *Identity*, o nome **QCRTMZ10MKTK** foi digitado. Um clique em *Apply* e depois em *OK* confirmaram essa alteração.

Figura 22. Identificação do *routerboard*



Fonte: Os autores

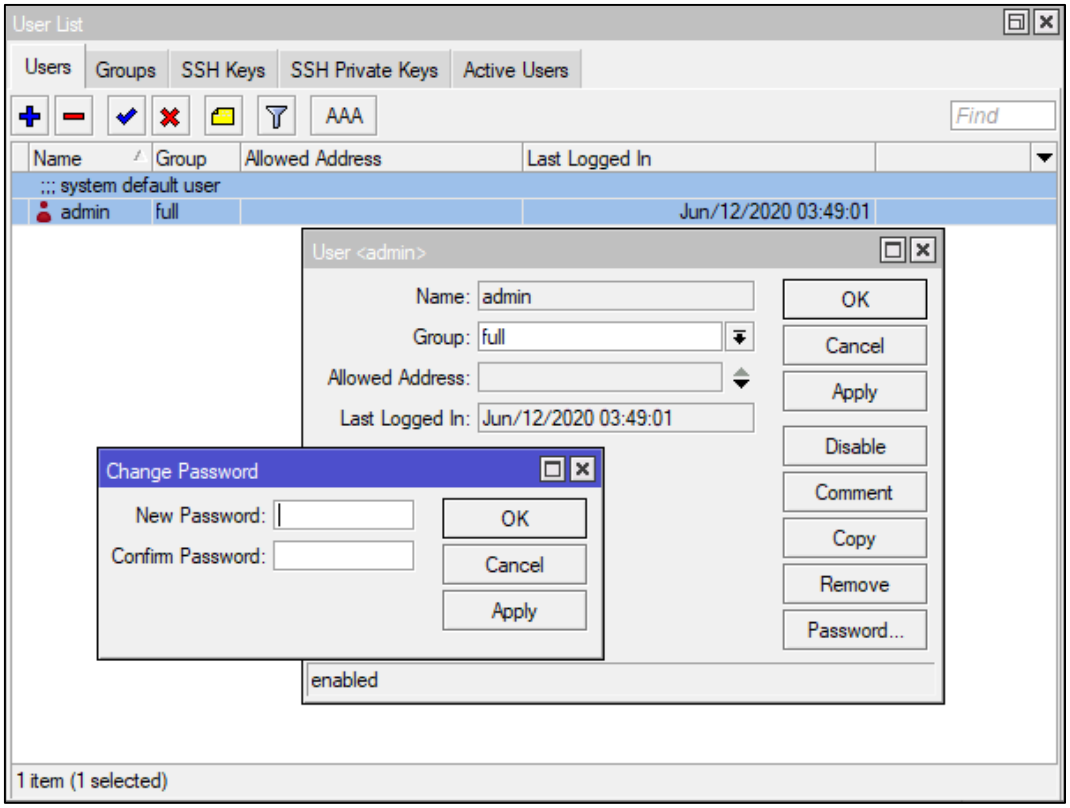
Conforme recomendação do fabricante, é boa-pratica em configurações no *RouterOS* utilizar o botão ***Apply*** ao finalizar uma alteração de item e logo depois o botão ***OK***. Isso garante que as informações são aplicadas. Por esse motivo, foi adotado esse método em todas as alterações realizadas nos itens necessários para preparo do equipamento.

5.4.1.3 Usuário administrador

Um dos pontos mais importantes do processo de configuração do *RouterOS* é a substituição da senha do usuário administrador. Por padrão, o usuário **admin** não possui uma senha inicial e essa é uma questão primária de segurança. Foi criada uma senha para o usuário **admin** através do menu *System* > *Users*.

O usuário **admin** é exibido em *User List*. Com um duplo-clique sobre o usuário e um clique no botão *Password* esse recurso foi acessado. Em *Change Password*, foi digitada e confirmada, em seus respectivos campos, uma nova senha (sem pré-requisitos). Um clique nos botões *Apply* e *OK* confirmaram essa alteração. A Figura 23 ilustra os campos que foram preenchidos.

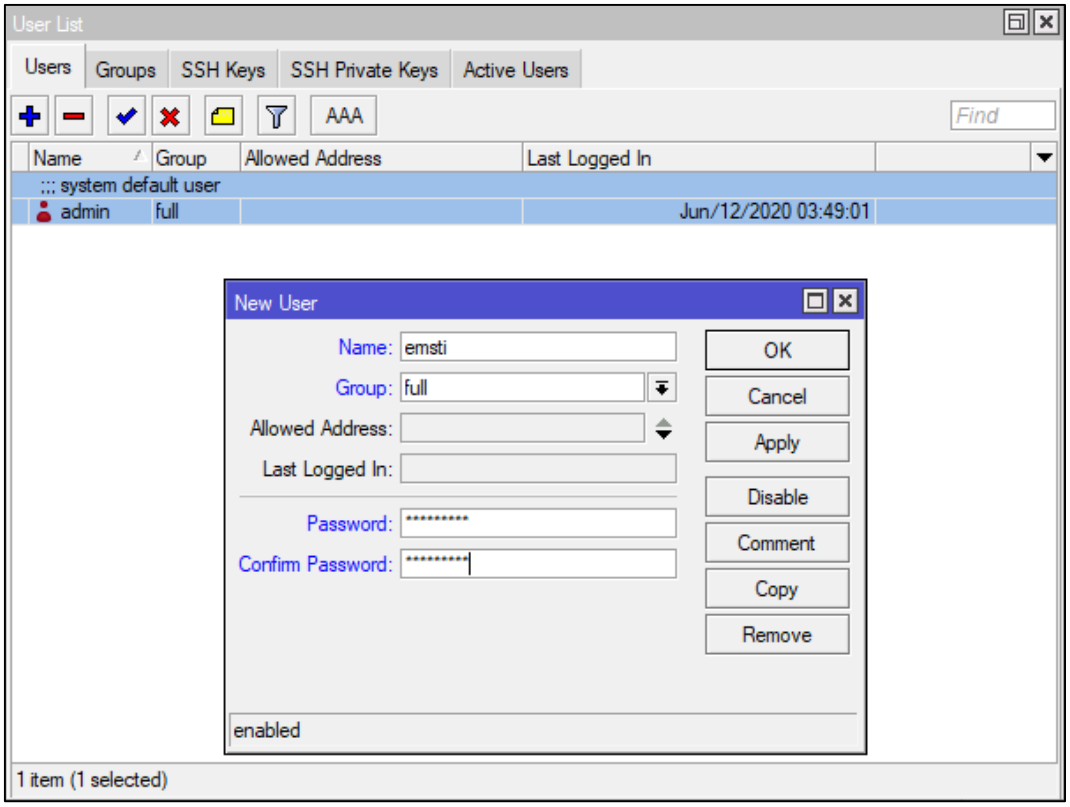
Figura 23. Gestão de usuários – Alteração de senha



Fonte: Os autores

Como boa-prática, foi criado um novo usuário, com perfil e privilegio administrador, que foi utilizado nas demais configurações. Em *User List*, foi clicado no botão *Add (+)*. Utilizado o nome **emsti** e uma **senha** padrão da nossa empresa (E&M Soluções em Tecnologia da Informação) para este usuário. Este usuário foi adicionado ao grupo ***full***. Logo após, um clique nos botões *Apply* e *OK* confirmaram essa configuração. Os campos preenchidos estão ilustrados na Figura 24.

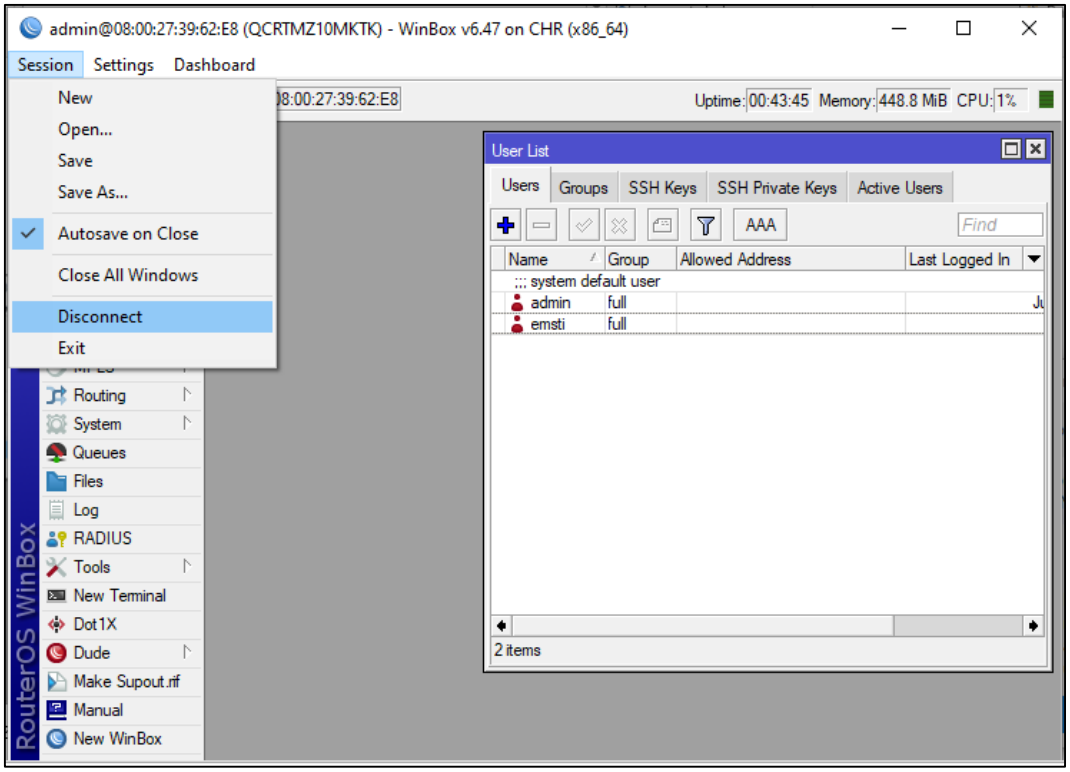
Figura 24. Adição de novo usuário



Fonte: Os autores

Após criado o novo usuário, o *WinBox* foi desconectado, pois a sessão anterior pertencia ao usuário **admin**. Foi iniciada uma nova sessão com o usuário **emsti**. Para desconectar, o menu *Session* > *Disconnect* foi acessado. Este caminho pode ser observado na Figura 25.

Figura 25. Menu de desconexão de sessão



Fonte: Os autores

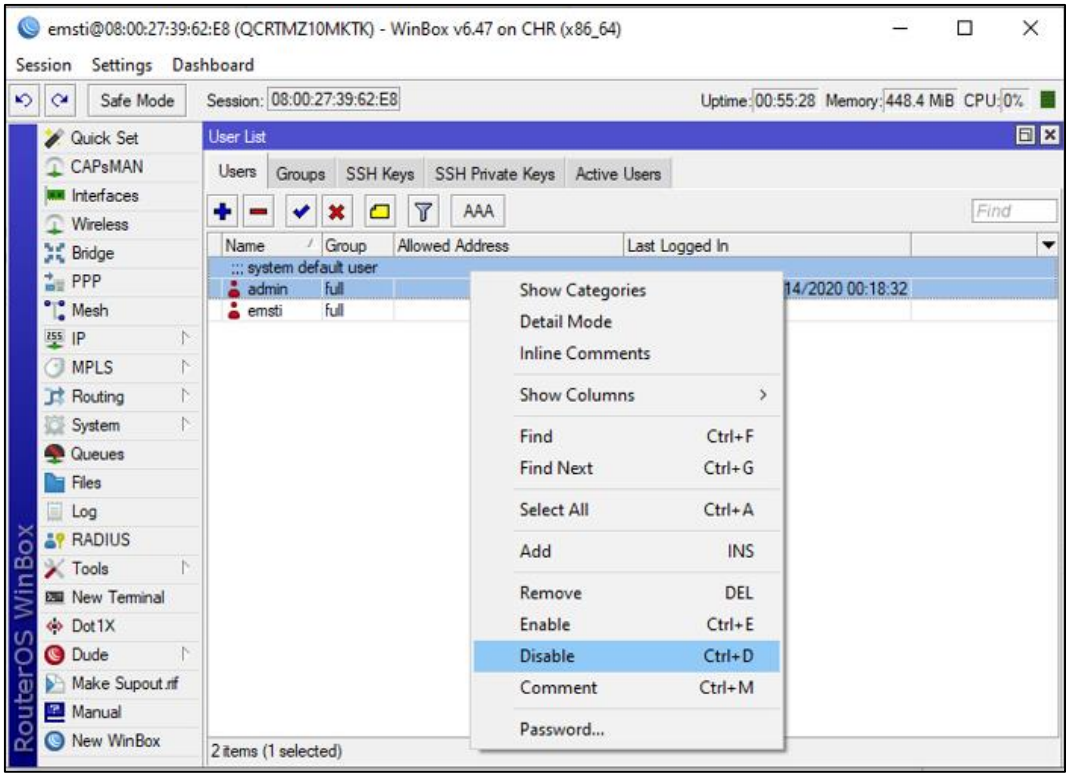
O *WinBox* encerrou a sessão do usuário **admin**. Inicializada uma nova sessão com o usuário **emsti**, o usuário **admin** foi desabilitado. Essa ação contribui para que possíveis ataques de força-bruta não obtenham sucesso, pois o usuário **admin** é um nome de usuário comum entre equipamentos de rede, geralmente possui acesso privilegiado e nem sempre possuem senhas fortes, pois essa questão é um pouco desprezada por leigos que configuram equipamentos sem um conhecimento básico em segurança da informação.

Existem três maneiras de desabilitar um usuário na tela *User List*. São elas:

1. Selecionar o usuário e clicar no botão ***Disable (X)***;
2. Selecionar o usuário e pressionar as teclas **CTRL + D**;
3. Clicar com o botão direito do mouse sobre o nome do usuário e escolher ***Disable***.

Na Figura 26 é possível visualizar os três métodos. Por praticidade, utilizamos o primeiro.

Figura 26. Gestão de usuários – Processo de desabilitação



Fonte: Os autores

5.4.1.4 Atualização do sistema

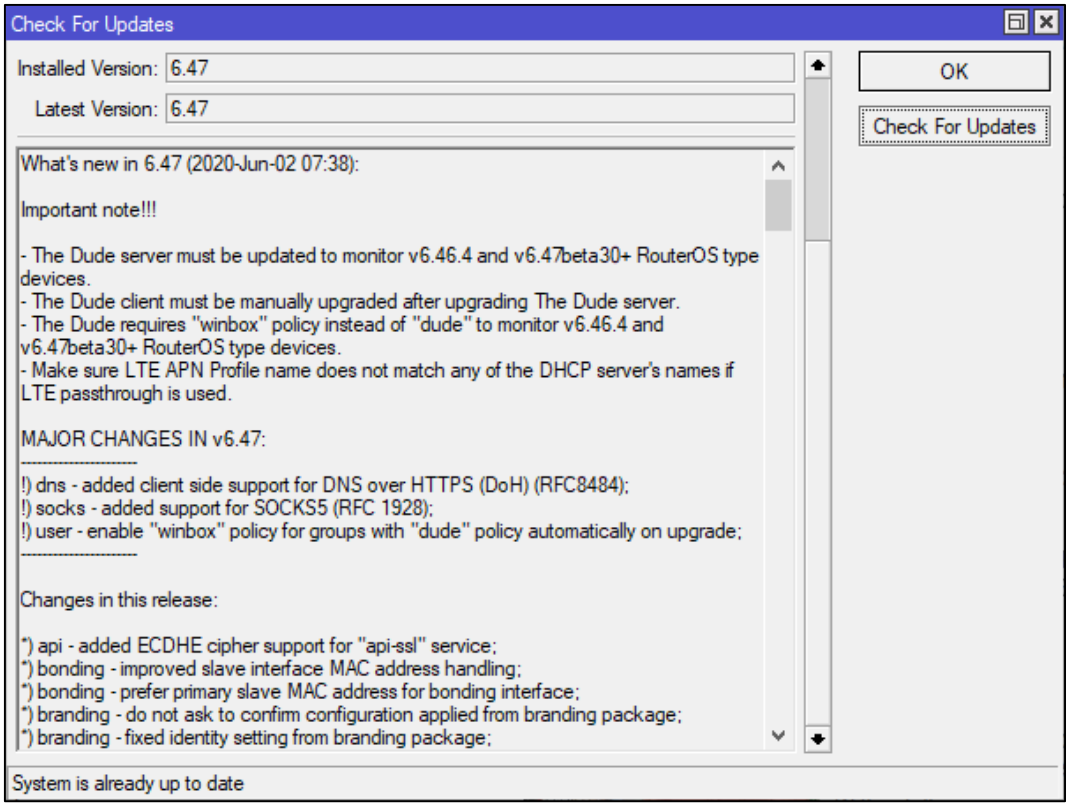
Por tratar-se de uma plataforma operacional em plena atividade e comercialização, o *RouterOS* é frequentemente atualizado. É um item de segurança procurar por atualizações e, se disponíveis, atualizar o sistema.

É bem simples fazer isso no *RouterOS*. Foi acessado o menu *System* > *Packages*. Em *Package List*, o botão ***Check for Updates*** foi clicado. O sistema iniciou uma busca por atualizações e não encontrou nenhuma, pois o *RouterOS* já estava instalado no *routerboard* em sua versão mais recente.

Caso o sistema encontre uma nova versão de *firmware*, os botões ***Download*** e ***Download & Install*** são exibidos, oferecendo a possibilidade de baixar a versão e instalar em outro momento ou baixar e instalar a versão ao mesmo tempo.

A Figura 27 evidencia que a versão do *RouterOS* instalada é a mais recente, como pode ser observado nos campos *Installed Version* e *Latest Version*. A versão **6.47** é exibida em ambos os campos.

Figura 27. Checagem de atualizações para o *RouterOS*



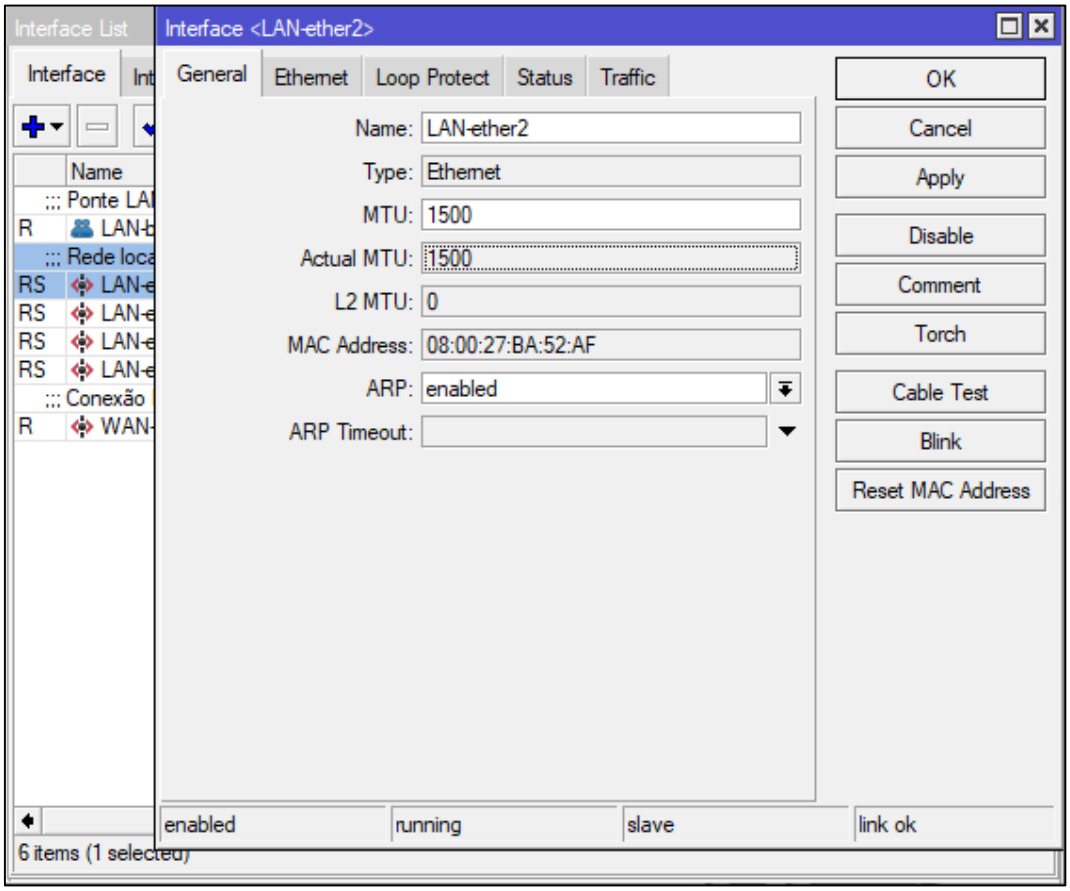
Fonte: Os autores

5.4.1.5 Interfaces ethernet

Originalmente as interfaces estão nomeadas como *ether1*, *ether2*, *ether3*, *ether4* e *ether5*. Visto que foi projetado utilizar a *ether1* como *WAN* e as demais como *LAN*, os nomes das interfaces foram alterados para facilitar a identificação. Para isso, o menu *Interfaces* > *Interface List* > *Interface* foi acessado. Em cada interface, com um duplo-clique, o **nome** no campo *Name* foi substituído e, em seguida, clicado nos botões *Apply* e *OK*. Esse processo foi repetido em todas as interfaces, obedecendo o nome designado para cada uma. A Figura 29 ilustra o processo de renomeação.

| *Ether1: WAN* | *Ether2: LAN* | *Ether3: LAN* | *Ether4: LAN* | *Ether5: LAN* |

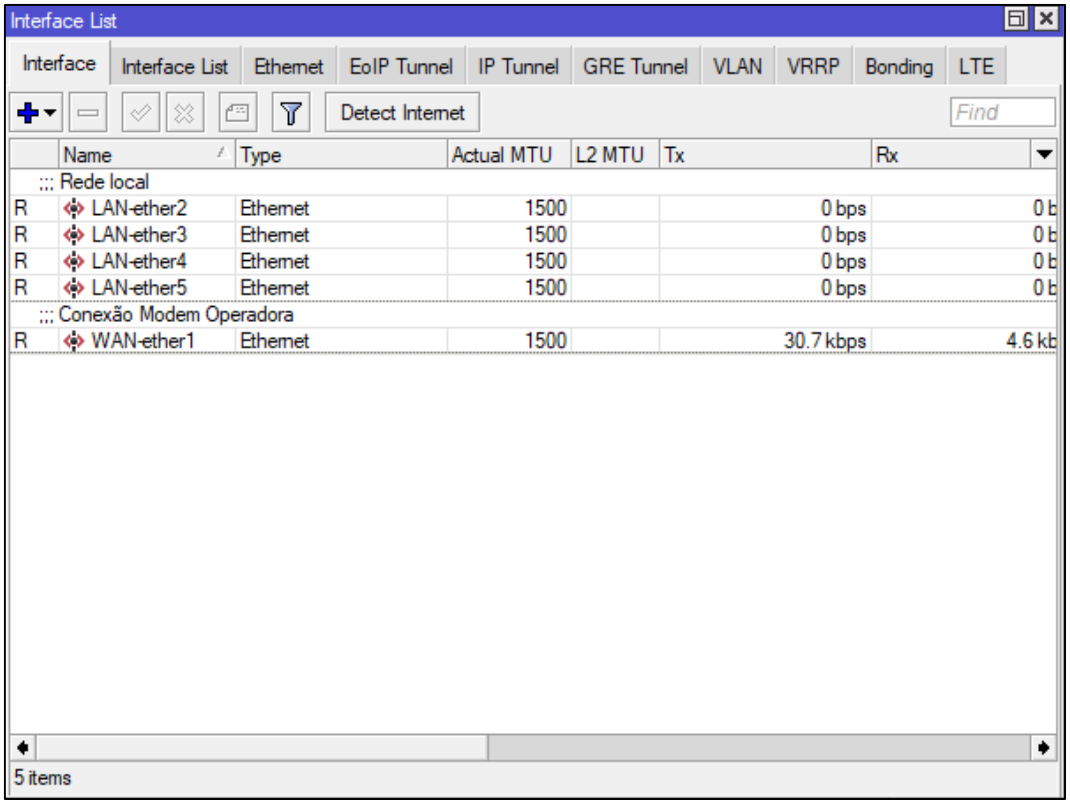
Figura 28. Nomeação de interface ethernet



Fonte: Os autores

A Figura 29 exibe a nova organização. Inserimos um comentário para separar em blocos e identificar a função de cada um deles.

Figura 29. Gestão da lista de interfaces

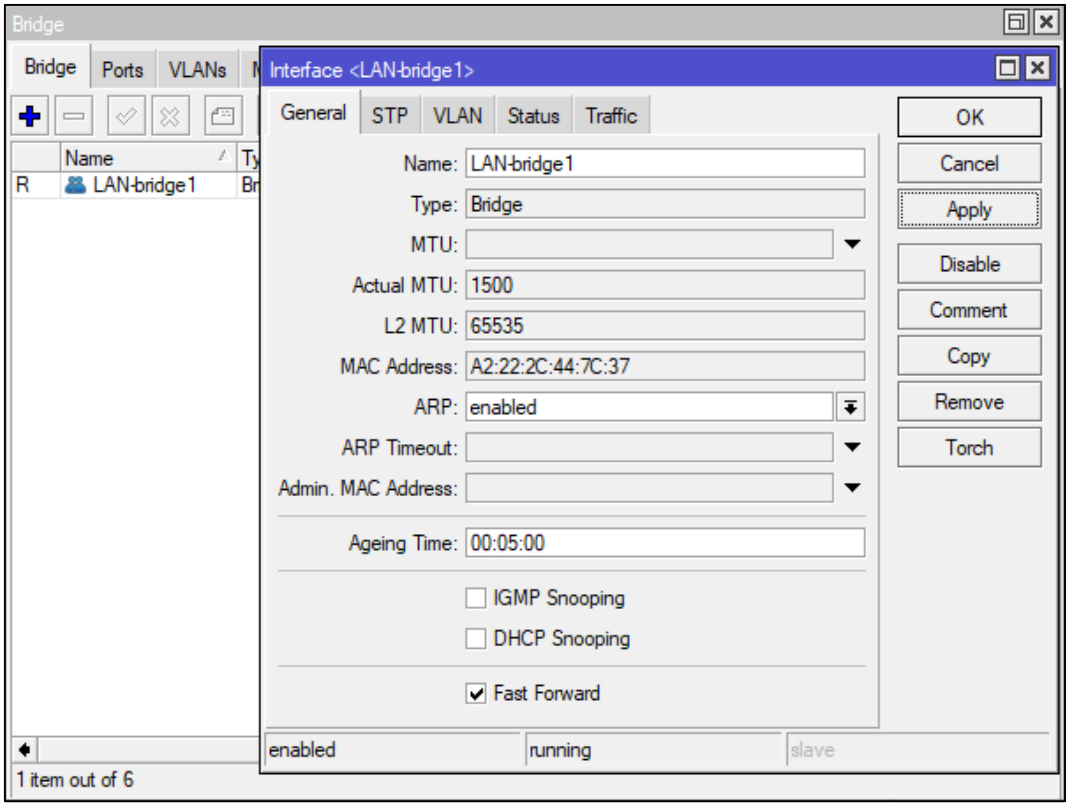


Fonte: Os autores

5.4.1.6 Bridge

Foi optado por criar uma *bridge*. Ela será responsável por interligar as quatro interfaces *LAN*, fazendo com que elas participem das mesmas regras de gerenciamento e roteamento na rede local. O menu *Bridge > Bridge > Add (+)* foi acessado e um nova *bridge* foi adicionada. A Figura 30 exibe a adição dessa interface.

Figura 30. Adição de interface bridge



Fonte: Os autores

5.4.1.7 Interfaces da bridge

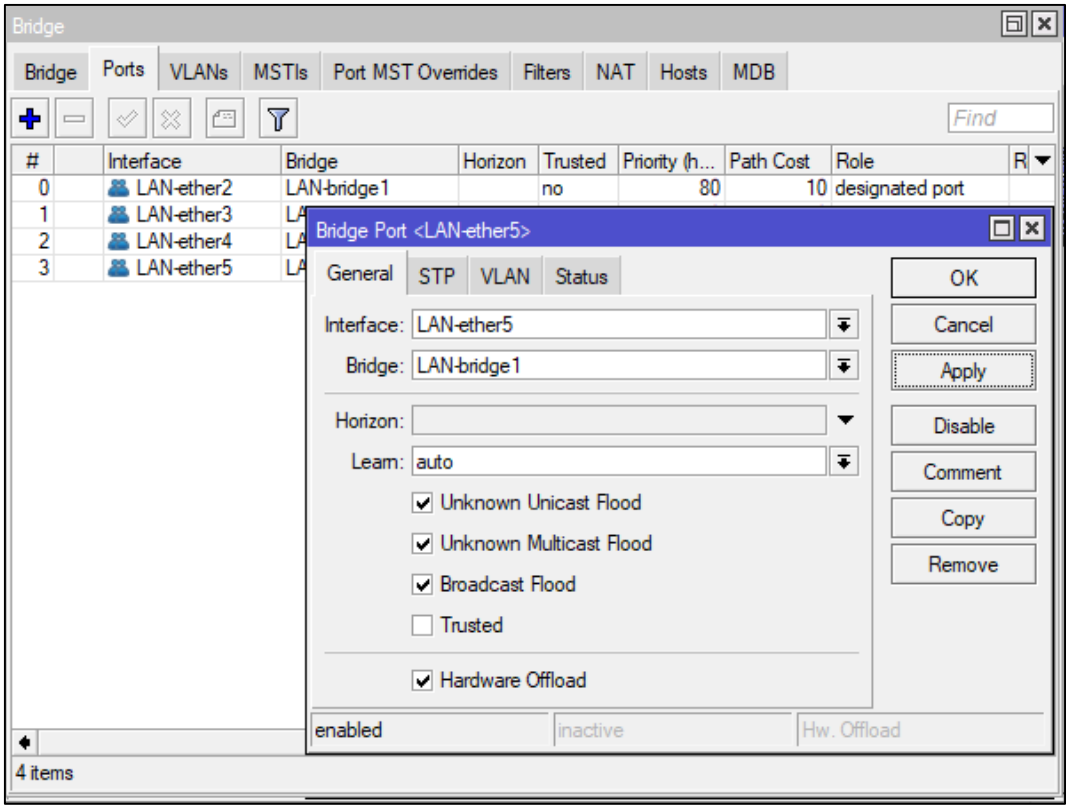
No menu *Bridge*, na aba *Ports*, foram adicionadas as quatro interfaces denominadas como *LAN* para fazer parte da ***LAN-bridge1***, criada recentemente. Para tal, foi clicado no botão *Add (+)* e navegado pelos itens *Bridge Port* > *General* e adicionada a interface ***LAN-ether2*** para atuar junto a ***LAN-bridge1***, informações estas inseridas nos campos *Interface* e *Bridge*, respectivamente. Para confirmar, os botões *Apply* e *OK* foram utilizados. O mesmo processo foi repetido para as demais interfaces identificadas como *LAN*.

Agora, a *LAN-bridge1* é formada pelas interfaces:

- *LAN-ether2;*
- *LAN-ether3;*
- *LAN-ether4;*
- *LAN-ether5.*

Na Figura 31, esta configuração na *LAN-bridge1* pode ser observada.

Figura 31. Administração de portas na bridge

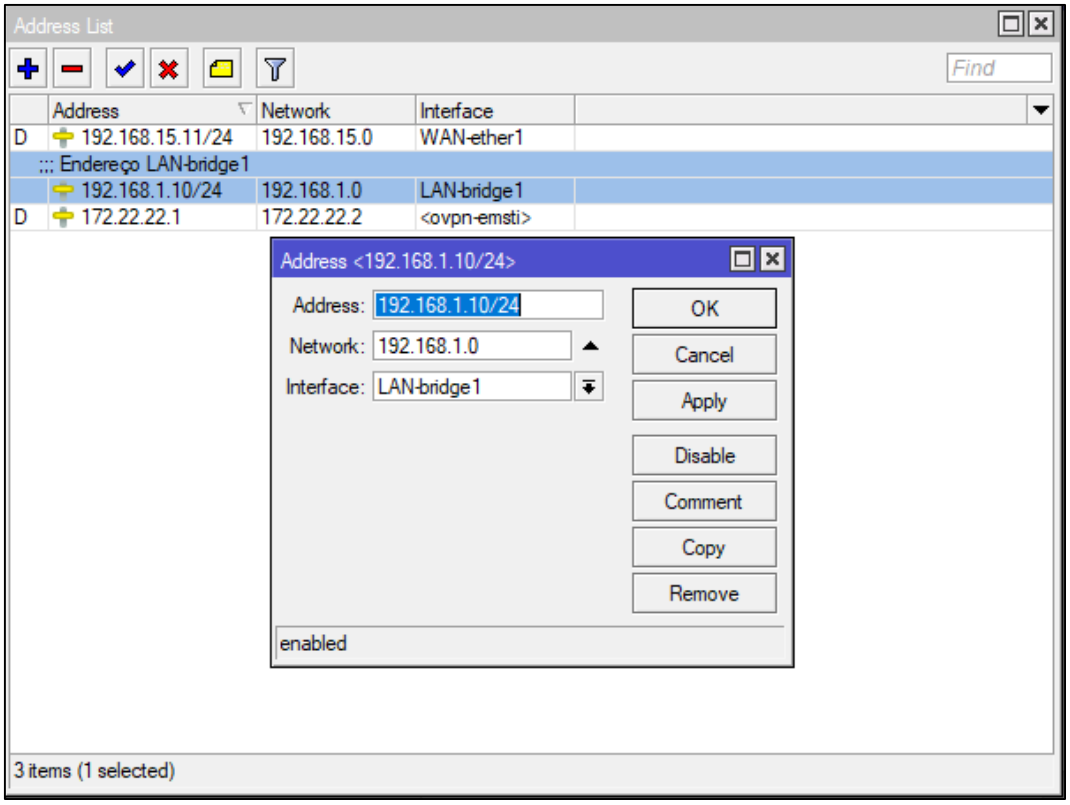


Fonte: Os autores

5.4.1.8 Lista de endereços WAN e Bridge

No menu *IP* > *Address List* o endereço IP **192.168.1.10/24** para a interface ***LAN-bridge1*** foi adicionado. Para isso, foi clicado no botão *Add (+)* e preenchidos os campos com suas informações respectivas. Os botões *Apply* e *OK* foram utilizados para salvar a configuração. O preenchimento desses campos pode ser visualizado na Figura 32. O endereço IP **192.168.15.11/24** da interface *WAN-ether1* é preenchido automaticamente pelo serviço *DHCP Client*, configurado no modem da operadora.

Figura 32. Lista de endereços de rede



Fonte: Os autores

5.4.1.9 Intervalo de endereços DHCP (Pool)

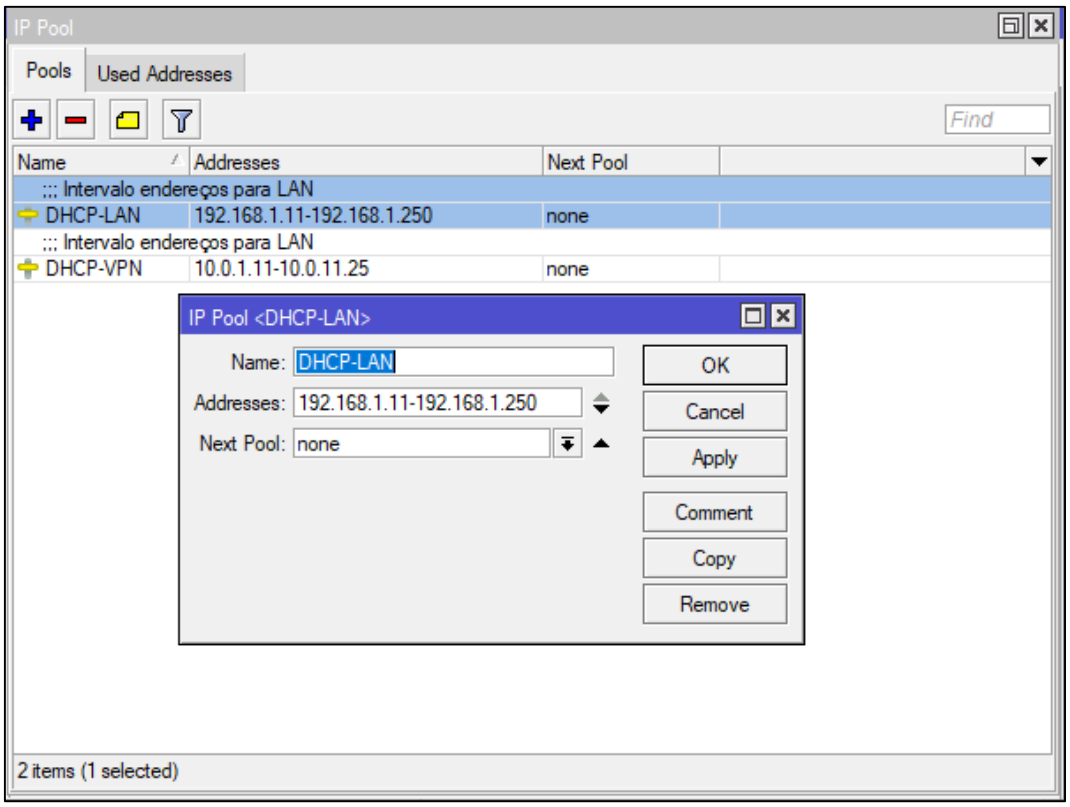
Após definido em projeto um escopo para o serviço *DHCP*, aplicado devidamente o intervalo de exclusão, os endereços remanescentes formaram o *pool* de endereços disponíveis dentro do escopo. Esses endereços em *pool* foram qualificados para a atribuição dinâmica para clientes *DHCP* na rede *LAN* da Quatro Cambalhotas.

Pool de endereços é o nome dado para o conjunto de endereços IP disponíveis, já descontados os endereços das faixas de exclusão. Ao definir uma exclusão desses endereços, você especifica que esses endereços não serão oferecidos a clientes *DHCP* quando eles solicitam a configuração ao servidor *DHCP*. Também é comum ouvir o termo **faixa de reserva de IP**, onde será utilizado para o cliente um IP que faz parte desse intervalo excluído do *pool*, cujo este não sofrerá nenhuma interferência ou ação do serviço *DHCP*, ou seja, não será renovado (substituído).

Um intervalo (*pool*) foi criado através do menu *IP* > *Pool* e com um clique no botão *Add (+)*. Após inseridas nos devidos campos, um clique nos botões *Apply* e *OK* salvaram as informações. A Figura 33 ilustra os campos parametrizados.

O nome ***DHCP-LAN*** foi utilizado para este *pool* e o intervalo que inicia no IP **192.168.1.11** e vai até o IP **192.168.1.250** foi setado em *Addresses*. Esse intervalo deve ser preenchido usando o **hífen (-)** entre o endereço inicial e o endereço final. As faixas exclusas serão utilizadas para a faixa de reserva de IP.

Figura 33. IP *Pool* - Intervalo de endereços IP para o *DHCP*

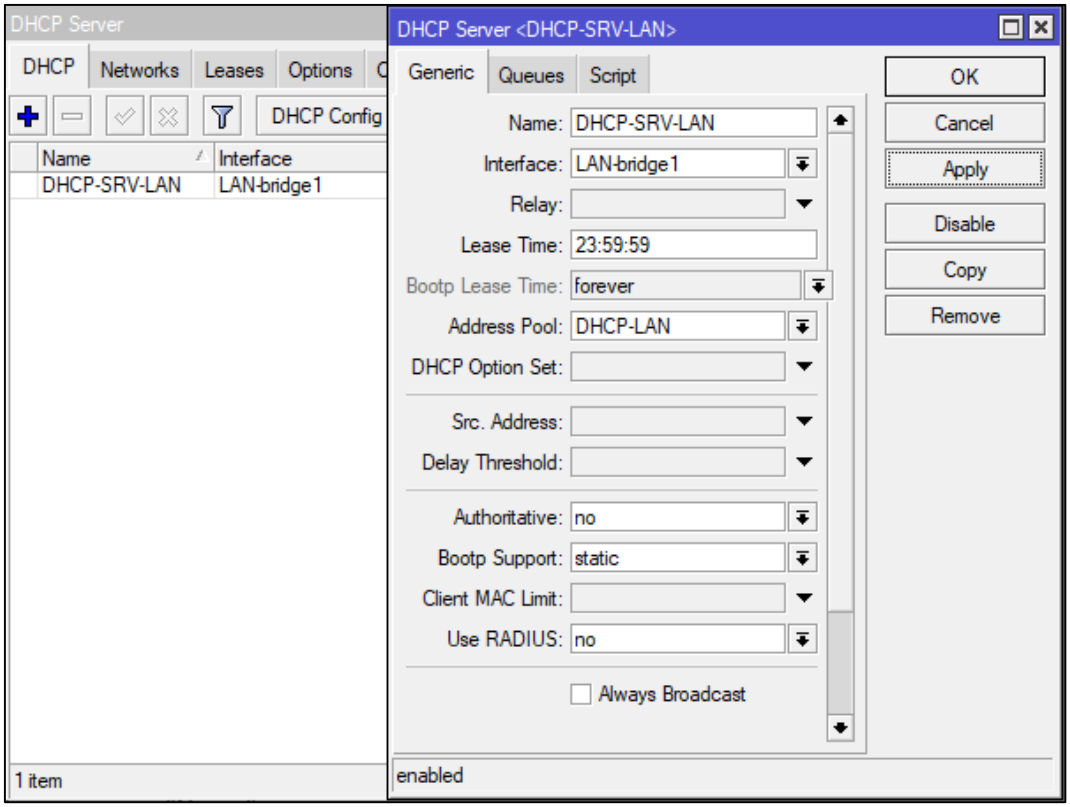


Fonte: Os autores

5.4.1.10 Servidor DHCP

Um servidor *DHCP* foi ativado para atuar na rede local através do menu *IP* > *DHCP Server* > *DHCP*. Em *DHCP* > *Add (+)* apenas os parâmetros *Name, Interface, Lease Time, Address Pool* e *Authoritative* foram alterados para os valores ***DHCP-SRV-LAN***, ***LAN-bridge1***, ***23:59:59***, ***DHCP-LAN*** e ***No***, em seus respectivos locais. Para os demais, o valor padrão foi mantido. As configurações foram salvas através dos botões *Apply* e *OK*. A Figura 34 ilustra a adição do serviço *DHCP*.

Figura 34. Adição do servidor DHCP



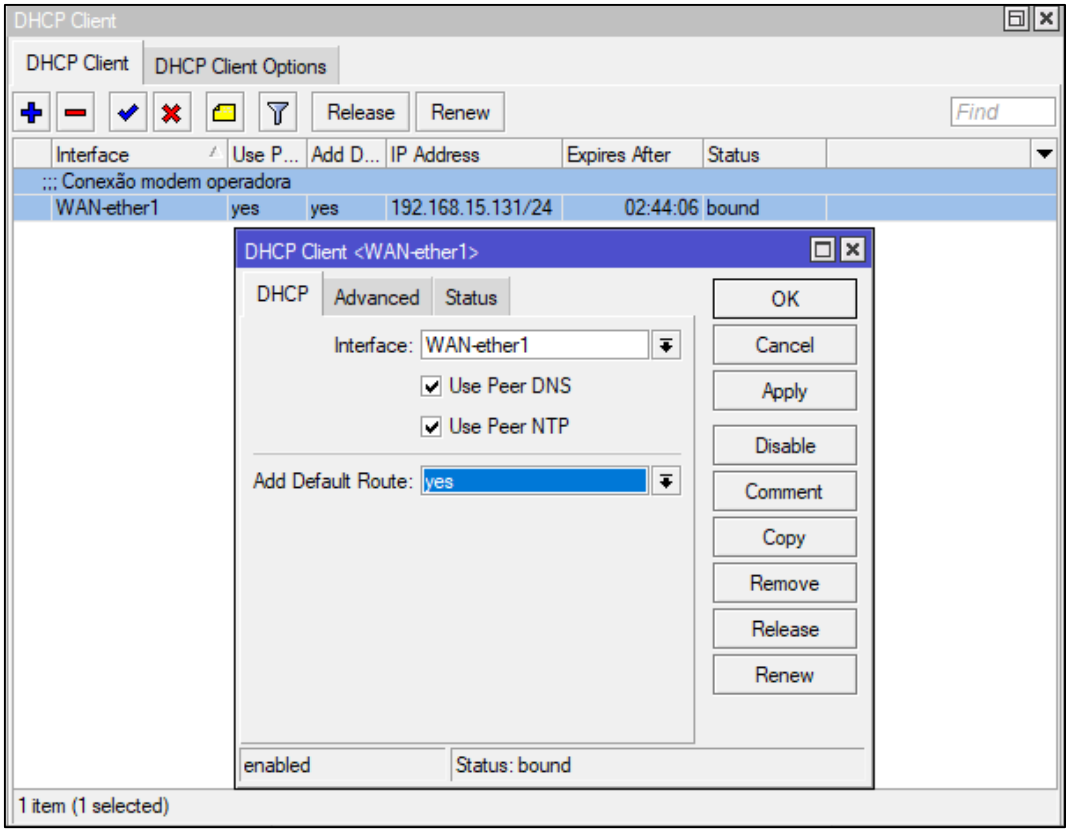
Fonte: Os autores

5.4.1.11 Cliente DHCP

Devido ao fato do *routerboard* estar conectado em uma das interfaces ethernet do modem da operadora e este estar com o serviço *DHCP* ativado, um endereço IP foi atribuído à interface *WAN-ether1*. Isso faz do *routerboard* um cliente *DHCP* do modem da operadora. Por isso, quando clicado no menu *IP > DHCP Client > DHCP Client*, o endereço IP pôde ser visualizado.

Caso não estivesse, para adicionar um novo cliente *DHCP*, bastava clicar no botão *Add (+)* e alterar apenas os parâmetros *Interface* e *Add Default Route* para ***WAN-ether1*** e ***Yes***, respectivamente e confirmando com um clique nos botões *Apply* e *OK*. Essa alteração pode ser observada na Figura 35.

Figura 35. Endereço do cliente DHCP

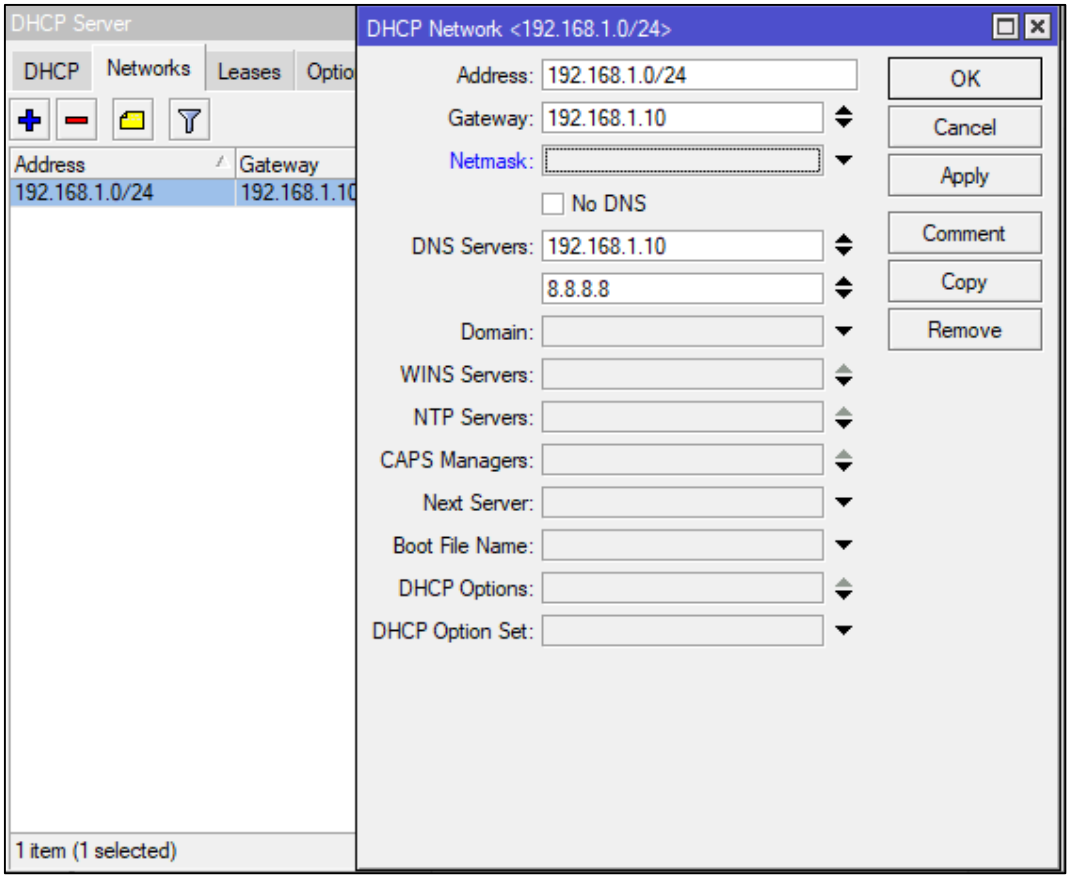


Fonte: Os autores

5.4.1.12 Endereços de rede

Este foi o momento de informar os endereços da *LAN* que serão entregues para o cliente *DHCP,* na rede local, quando forem solicitados no momento em que um dispositivo for conectado. Para configurá-los, foi acessado o menu *IP > DHCP Server* até a aba *Networks*. Nesta aba, os campos *Address*, *Gateway* e *DNS Server* foram preenchidos com os valores respectivos **192.168.1.0/24**, **192.168.1.10** e **192.168.1.10** e salvos através dos botões *Apply* e *OK*. A Figura 36 exibe esta tela de configuração.

Figura 36. Adição dos endereços de rede para DHCP



Fonte: Os autores

Ao informar o endereço IP em formato *CIDR* (*Classless Inter-Domain Routing*), o campo *Netmask* não precisou ser preenchido. Nesse campo, podemos inserir o endereço IP equivalente da máscara de sub-rede **255.255.255.0**, que é representado pelo ***/24***, já informado no campo *Address*.

É possível configurar mais um servidor *DNS*, se necessário, como por exemplo o servidor *DNS* do **Google**, representado pelo endereço IP **8.8.8.8** ou o **8.8.4.4**. Em alguns casos, isso pode facilitar e agilizar as consultas *DNS* da rede local.

O *routerboard* será o *gateway* e o servidor *DNS* da rede local e por este motivo atribuímos o mesmo endereço IP para estas funções.

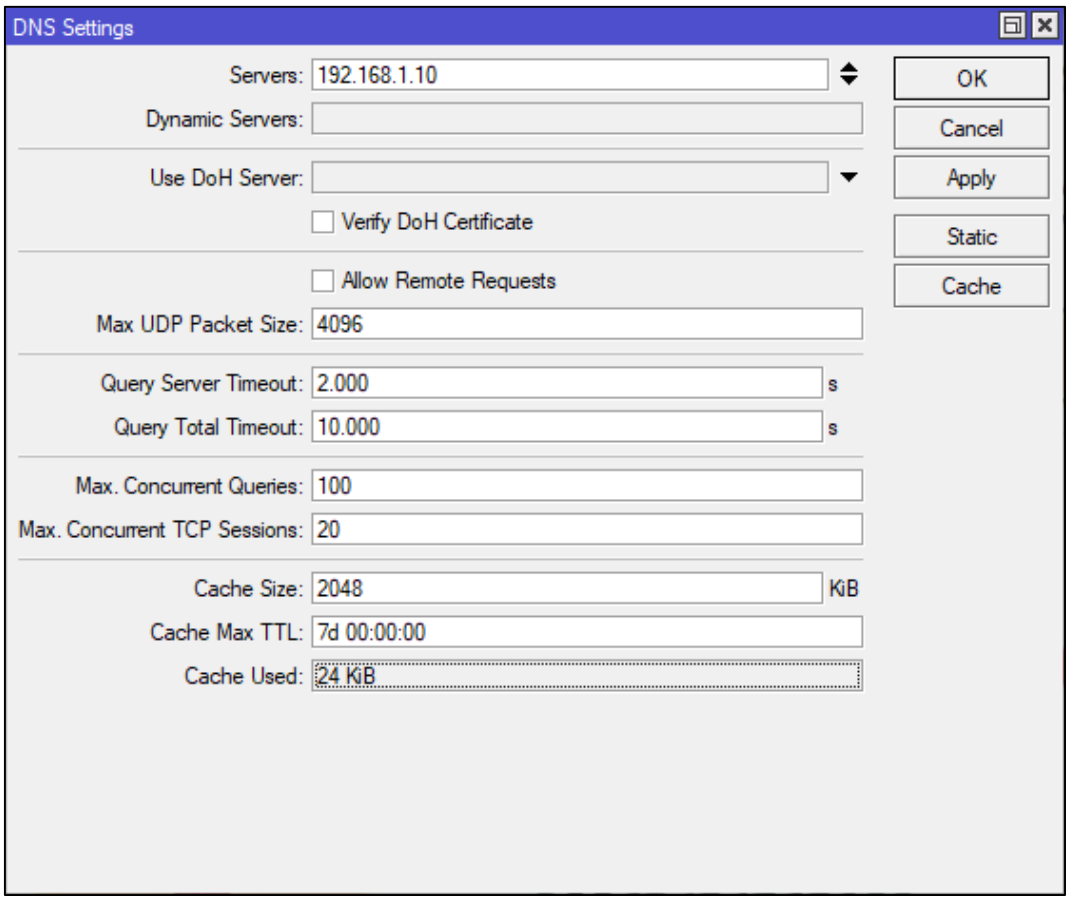
5.4.1.13 DNS

O *routerboard* foi promovido para servidor *DNS* da rede local. Ele será responsável pelas requisições geradas pelos dispositivos internos para o meio externo. Para isso, foi acessado o menu *IP* > *DNS* e, em *DNS Settings*, informado o endereço IP **192.168.1.10** no campo *Server***.** As alterações foram salvas com um

clique nos botões *Apply* e *OK*. É possível informar mais de um servidor *DNS*, caso necessário, mas não o fizemos. Para isso, bastava clicar na seta (▾) no final do campo *Server* que um segundo servidor *DNS* seria exibido para preenchimento.

A Figura 37 mostra a tela de configuração do servidor DNS.

Figura 37. Configurações em DNS



Fonte: Os autores

5.4.1.14 Rota padrão

Foi necessário criar rotas de comunicação entre as redes externa (*WAN*) e interna (*LAN*). Algumas foram criadas automaticamente, quando deixado o parâmetro *Add Default Route* com valor ***Yes***. Outras foram criadas manualmente, através do menu *IP* > *Routes*. Em *Route List*, as rotas informadas na Tabela 4 foram adicionadas.

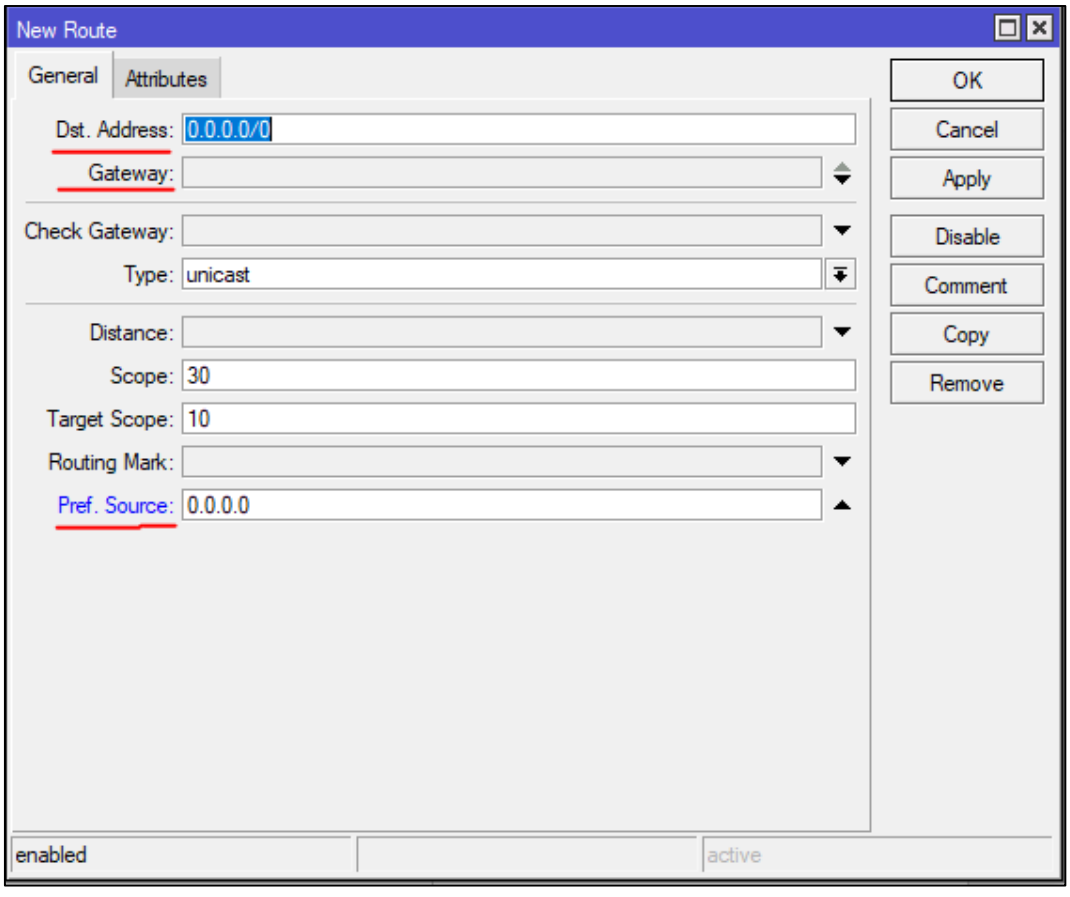
Tabela 4. Lista de rotas padrão

Endereço de destino	Gateway	Endereço origem preferencial	Descrição
0.0.0.0/24	192.168.15.1 reachable WAN-ether1		Saída pelo gateway do modem para qualquer endereço de rede na internet
192.168.1.0/24	LAN-bridge1	192.168.1.10	Tráfego interno entre as interfaces LAN
192.168.15.0/24	WAN-ether1	192.168.15.11	Tráfego externo entre a internet no modem e o routerboard

Fonte: Os autores

Para adicionar, o botão *Add (+)* foi clicado e os campos pertinentes para cada situação foram preenchidos. Para as três regras, os campos *Dst. Address*, *Gateway* e *Pref. Source* foram utilizados e preenchidos com os valores da Tabela 4. As configurações foram salvas através dos botões *Apply* e *OK*. A Figura 38 exibe a tela *New Route*, utilizada para adição de rotas.

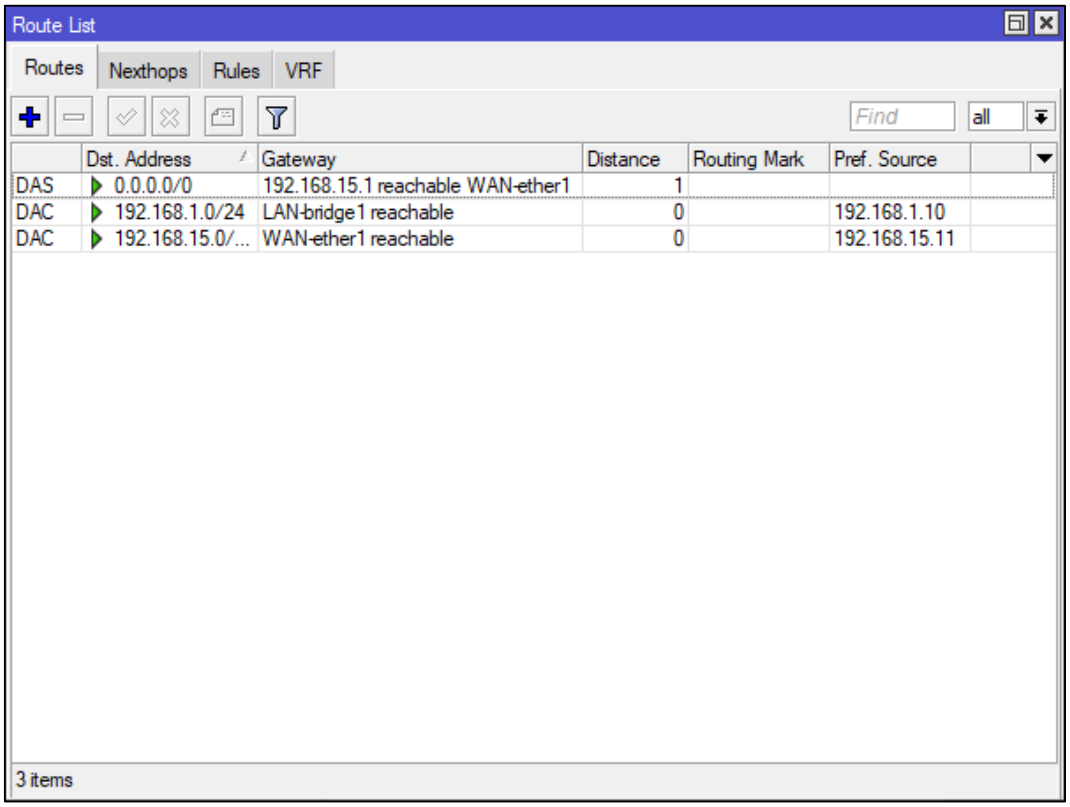
Figura 38. Adição de nova rota padrão



Fonte: Os autores

Finalizado a configuração das rotas, a informação alcançável (*reachable*) foi exibida na barra se *status*, indicando que o tráfego de dados entre as redes foi estabelecido. A Figura 39 ilustra a lista de rotas criadas no *routerboard*.

Figura 39. Gerenciamento da lista de rotas

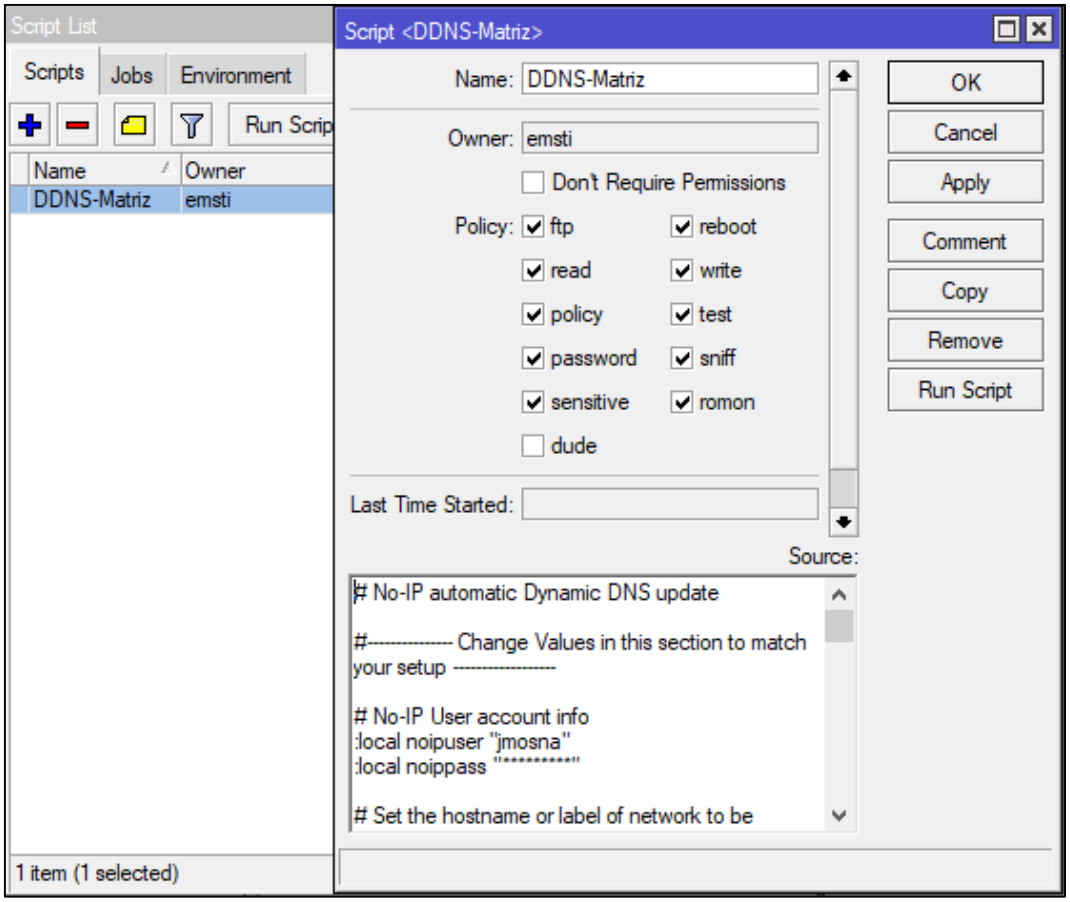


Fonte: Os autores

5.4.1.15 Script DDNS

Um *script* pronto, disponível na *wiki* da Mikrotik, foi revisado, copiado, adicionado e devidamente alterado no *routerboard*. Este script é utilizado para sincronizar os registros *DDNS* realizados no provedor No-IP. Através do menu *System* > *Scripts* e navegado até o item *Script List* > *Script*, o botão *Add (+)* foi cliado. O script foi nomeado para ***DDNS*-Matriz**. Em seguida, o *script*, já alterado, foi colado no campo *Source*. A Figura 40 exibe onde o script *DDNS* foi preparado.

Figura 40. Adição de novo script



Fonte: Os autores

As linhas que precisaram ser alteradas estavam separadas no primeiro bloco do código e foram destacadas na Figura 41. Inseridas as informações de **usuário** e **senha** para acesso à conta do servidor *DDNS* no provedor No-IP, o *hostname* **4cambalhotas-matriz.ddns.net** e o nome da interface ***WAN-ether1***, que é a interface de entrada do *routerboard*, o script estava preparado.

Figura 41. Parte do código do script DDNS

```
# No-IP automatic Dynamic DNS update

#--------------- Change Values in this section to match your setup ------------------

# No-IP User account info
:local noipuser "your_no-ip_user"
:local noippass "your_no-ip_pass"

# Set the hostname or label of network to be updated.
# Hostnames with spaces are unsupported. Replace the value in the quotations below with your host names.
# To specify multiple hosts, separate them with commas.
:local noiphost "hostname.no-ip.net"

# Change to the name of interface that gets the dynamic IP address
:local inetinterface "your_external_interface"

#-------------------------------------------------------------------------------
# No more changes need
```

Fonte: Os autores

Realizadas essas alterações, nenhuma outra mais foi necessária. Para salvar as alterações, os botões *Apply* e *OK* foram utilizados. A Figura 42 exibe a estrutura do código utilizado no *script DDNS* para o provedor *No-IP*.

Figura 42. Código do script para *DDNS* via No-IP

Script_Mikrotik_NOIP - Site MK - Bloco de Notas

Arquivo Editar Formatar Exibir Ajuda

```
# No-IP automatic Dynamic DNS update

#--------------- Change Values in this section to match your setup ------------------

# No-IP User account info
:local noipuser "your_no-ip_user"
:local noippass "your_no-ip_pass"

# Set the hostname or label of network to be updated.
# Hostnames with spaces are unsupported. Replace the value in the quotations below with your
host names.
# To specify multiple hosts, separate them with commas.
:local noiphost "hostname.no-ip.net"

# Change to the name of interface that gets the dynamic IP address
:local inetinterface "your_external_interface"

#-------------------------------------------------------------------------------
# No more changes need

:global previousIP

:if ([/interface get $inetinterface value-name=running]) do={
# Get the current IP on the interface
   :local currentIP [/ip address get [find interface="$inetinterface" disabled=no] address]

# Strip the net mask off the IP address
   :for i from=( [:len $currentIP] - 1) to=0 do={
       :if ( [:pick $currentIP $i] = "/") do={
           :set currentIP [:pick $currentIP 0 $i]
       }
   }

   :if ($currentIP != $previousIP) do={
       :log info "No-IP: Current IP $currentIP is not equal to previous IP, update needed"
       :set previousIP $currentIP

# The update URL. Note the "\3F" is hex for question mark (?). Required since ? is a special
character in commands.
       :local url "http://dynupdate.no-ip.com/nic/update\3Fmyip=$currentIP"
       :local noiphostarray
       :set noiphostarray [:toarray $noiphost]
       :foreach host in=$noiphostarray do={
           :log info "No-IP: Sending update for $host"
           /tool fetch url=($url . "&hostname=$host") user=$noipuser password=$noippass
mode=http dst-path=("no-ip_ddns_update-" . $host . ".txt")
           :log info "No-IP: Host $host updated on No-IP with IP $currentIP"
       }
   }  else={
       :log info "No-IP: Previous IP $previousIP is equal to current IP, no update needed"
   }
} else={
   :log info "No-IP: $inetinterface is not currently running, so therefore will not update."
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

Fonte: Wiki.mikrotik.com[15]

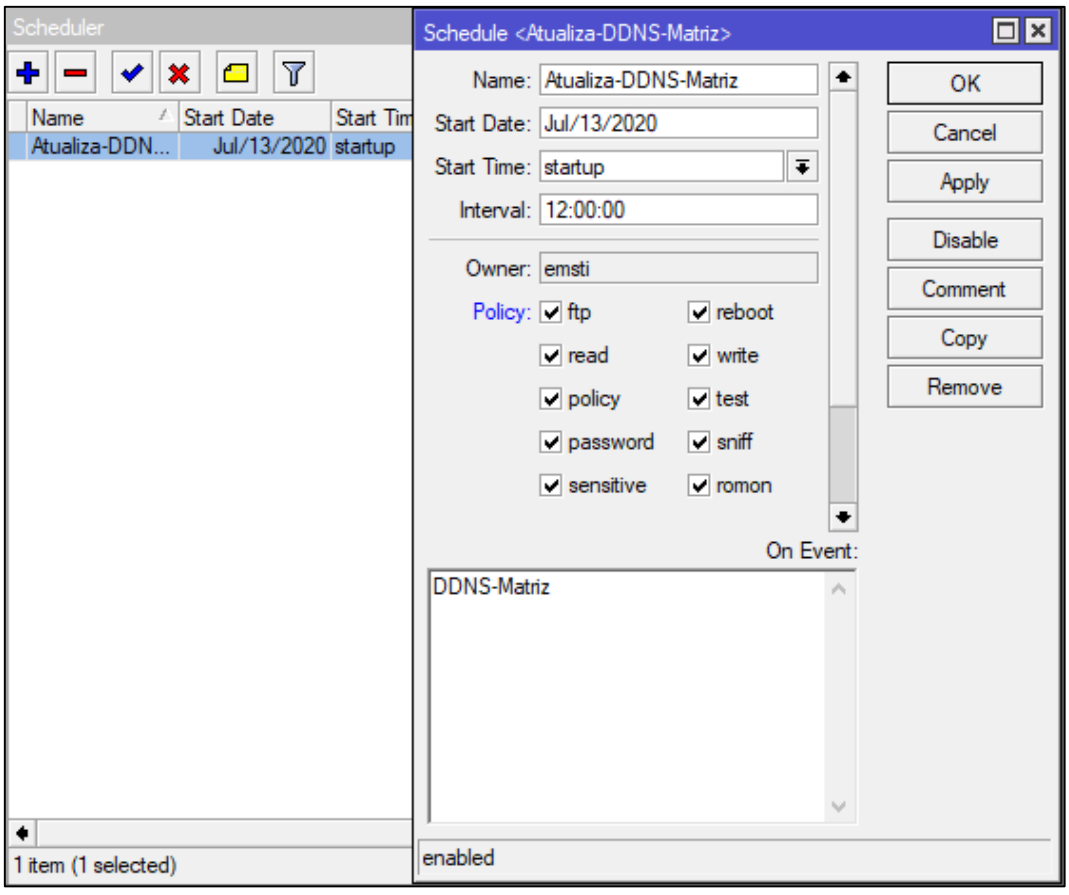
[15] Script disponível na URL <https://wiki.mikrotik.com/wiki/Dynamic_DNS_Update_Script_for_No-IP_DNS>.

5.4.1.16 Agendador de tarefas

O *script DDNS* precisa ser atualizado periodicamente, posto isto, foi automatizada essa ação através da ferramenta *Scheduler*. Pelo *Scheduler* foi possível agendar uma tarefa que executa o script todas as vezes durante o *startup* do *routerboard* e com um intervalo de atualização de 12 horas. Em resumo, após iniciado, a cada 12 horas o *script* é executado novamente e as informações no provedor *DDNS* são atualizadas. Isso garante que as informações nunca fiquem desatualizadas, comprometendo a conexão *VPN* e prejudicando o acesso remoto.

O menu *System* > *Scheluder* foi acessado e uma tarefa em *Schedule* foi criada, através do botão *Add (+).* Foi nomeada como **Atualiza-*DDNS*-Matriz**, com execução do ***startup*** do equipamento e com um intervalo de **12 horas**. No campo *On Event*, o nome do script **DDNS-Matriz** foi informado, criado anteriormente na seção 5.4.1.15. Essas informações foram preenchidas, respectivamente, nos campos *Name*, *Start Time*, *Interval* e *On Event*. A Figura 43 ilustra a adição da tarefa em *Schedule*.

Figura 43. Adição de nova tarefa no agendador

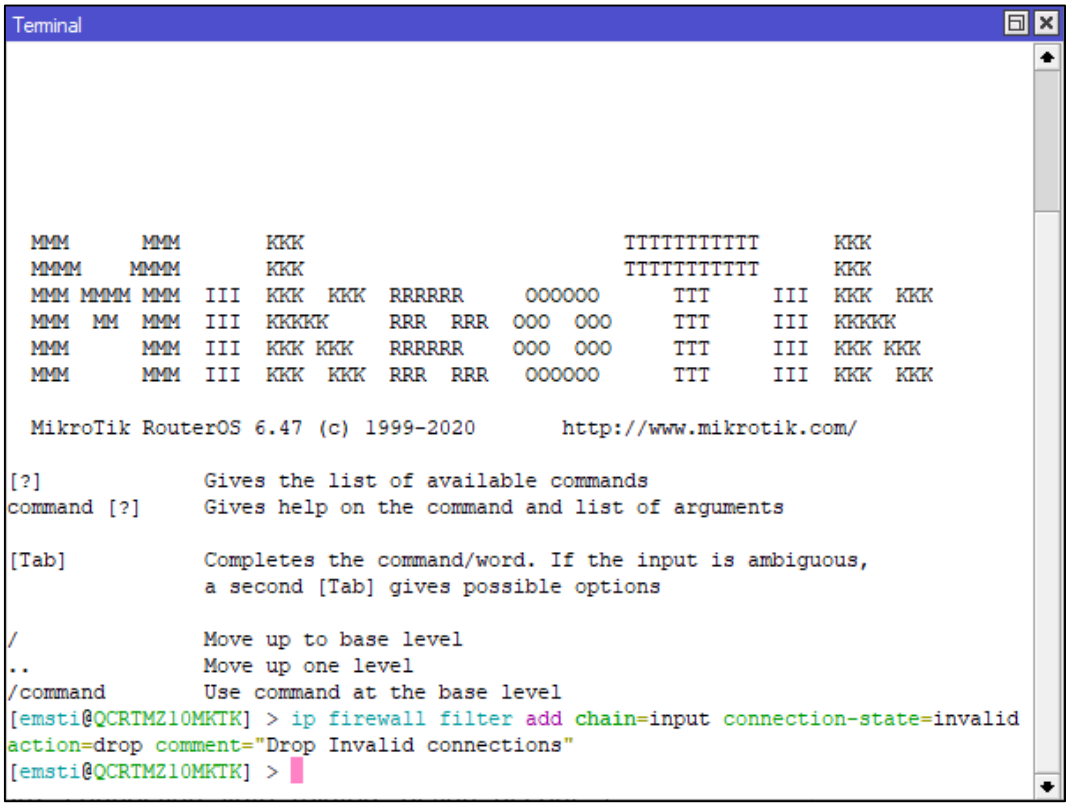


Fonte: Os autores

5.4.1.17 Regras de firewall

De modo a otimizar a proteção do *routerboard*, foram personalizadas algumas regras de *firewall* e aplicadas no *RouterOS*. Foram separadas por blocos, para facilitar a identificação e gerenciamento das regras. Essas regras foram parametrizadas via ferramenta *New Terminal*, localizada na barra vertical de menus. Esse terminal possibilita a utilização do **copiar** e **colar**, facilitando a configuração. A Figura 44 exibe a inserção de regra via ferramenta *New Terminal*.

Figura 44. Inserção de regra de *Firewall* via ferramenta *New Terminal*



Fonte: Os autores

A Figura 45 exibe algumas das regras que foram adicionadas ao *firewall* do *routerboard*. Essa customização, entre outras realizadas, melhora a proteção do *routerboard*, porém ressaltamos que as regras de *firewall* carregadas de fábrica já atenderiam para a realização do projeto, com uma proteção básica e satisfatória.

Figura 45. Regras de *Firewall* para tratamento de conexões

Tratamento das conexões:

```
# Deletar conexões inválidas
/ip firewall filter add chain=forward protocol=tcp connection-state=invalid
action=drop comment="drop invalid connections"

# Permitir conexões já estabelecidas
/ip firewall filter add chain=forward connection-state=established action=accept
comment="allow already established connections"

# Permitir conexões relacionadas
/ip firewall filter add chain=forward connection-state=related action=accept
comment="allow related connections"
```

Fonte: Os autores

A Figura 46 exibe as regras de tratamento de conexões que foram adicionadas ao *firewall* via *New Terminal*. Após digitar a regra, obedecendo sua estrutura, basta apertar a tecla *Enter* para confirmar e liberar o terminal para o próximo comando.

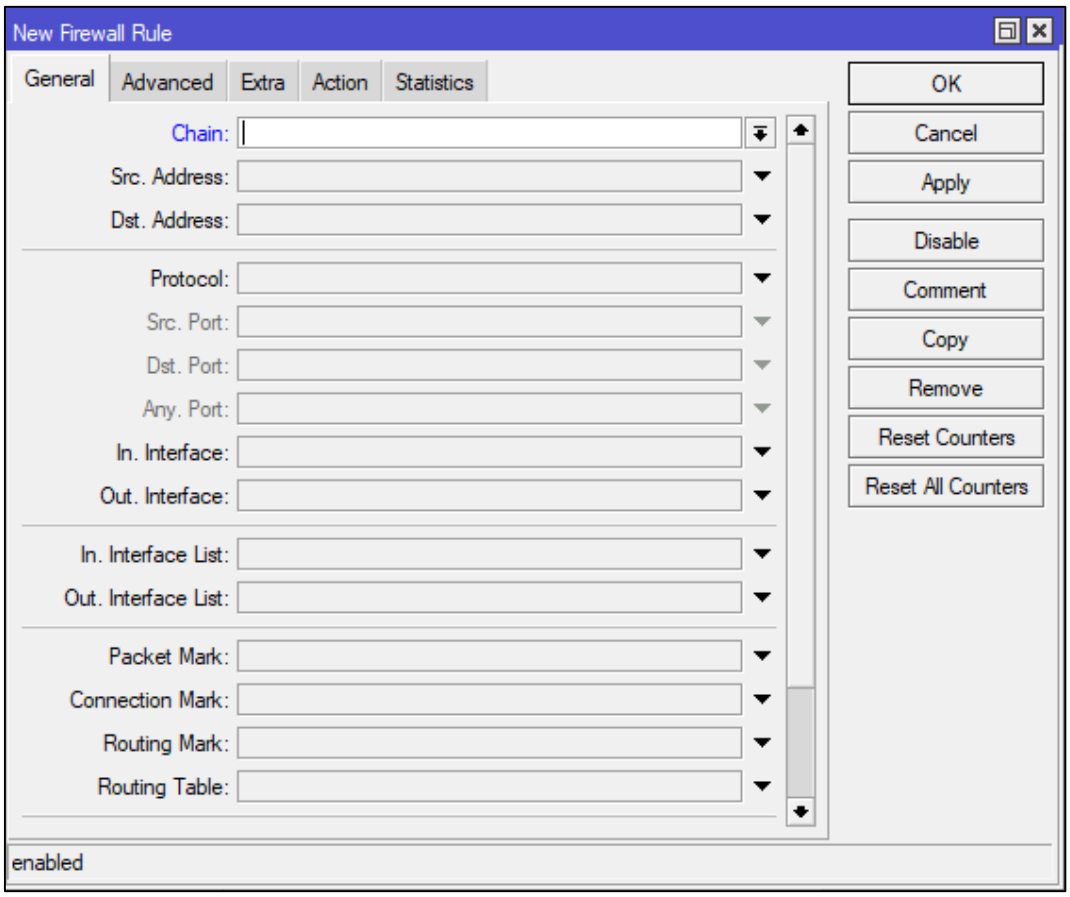
Figura 46. Inserção de regras de *Firewall* via ferramenta *New Terminal*

```
Terminal

  MMM      MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.47 (c) 1999-2020       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level
[emsti@QCRTMZ10MKTK] > /ip firewall filter add chain=forward protocol=tcp con
nection-state=invalid action=drop comment="drop invalid connections"
[emsti@QCRTMZ10MKTK] >
[emsti@QCRTMZ10MKTK] > /ip firewall filter add chain=forward connection-state
=established action=accept comment="allow already established connections"
[emsti@QCRTMZ10MKTK] >
[emsti@QCRTMZ10MKTK] > /ip firewall filter add chain=forward connection-state
=related action=accept comment="allow related connections"
[emsti@QCRTMZ10MKTK] >
```

Fonte: Os autores

Como dica, também é possível criar essas regras acessando o menu *IP* > *Firewall* > *Filter Rules* > *Add (+)* e parametrizando os campos disponíveis nas abas *General*, *Advanced*, *Extra* e *Action*, conforme ilustra a Figura 47.

Figura 47. Adição de regra de *Firewall*



Fonte: Os autores

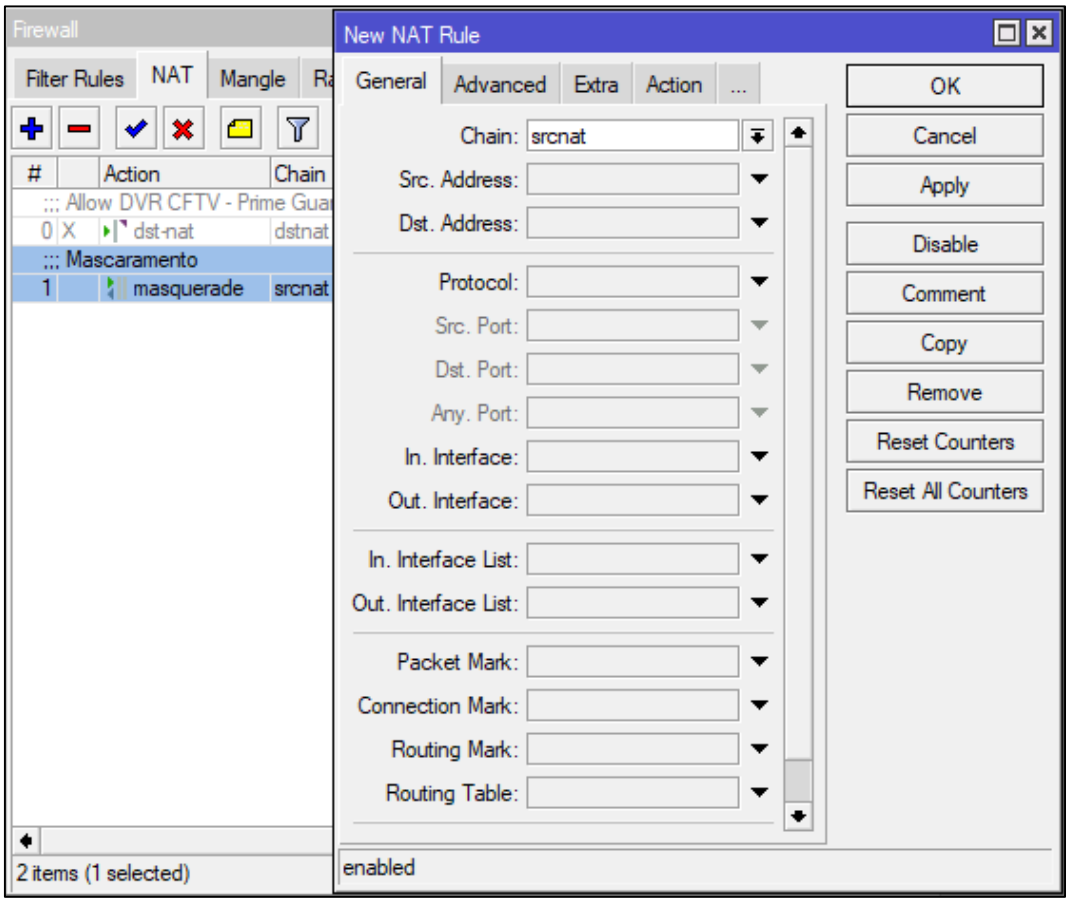
5.4.1.18 NAT

Um *NAT* com ação de mascaramento foi configurado no *firewall* do *routerboard*, através do menu *IP* > *Firewall* > *NAT* > *Add (+)*. Em *New Rule*, na aba *General*, foi alterado o *Chain* para ***srcnat*** e na aba *Action***,** a ação ***masquerade*** foi escolhida no campo *Action*. As alterações foram aplicadas através dos botões *Apply* e *OK*.

Essa regra converte os endereços internos e privados em um endereço externo e público, quando as solicitações saem dos endereços locais para a internet. O mesmo acontece no caminho reverso, onde o *NAT* traduz para qual endereço privado o pacote

de dados deve ser direcionado. Isso protege a identificação de cada *host* no meio externo. A Figura 48 ilustra a adição de nova regra de *NAT*.

Figura 48. Adição de regra de NAT

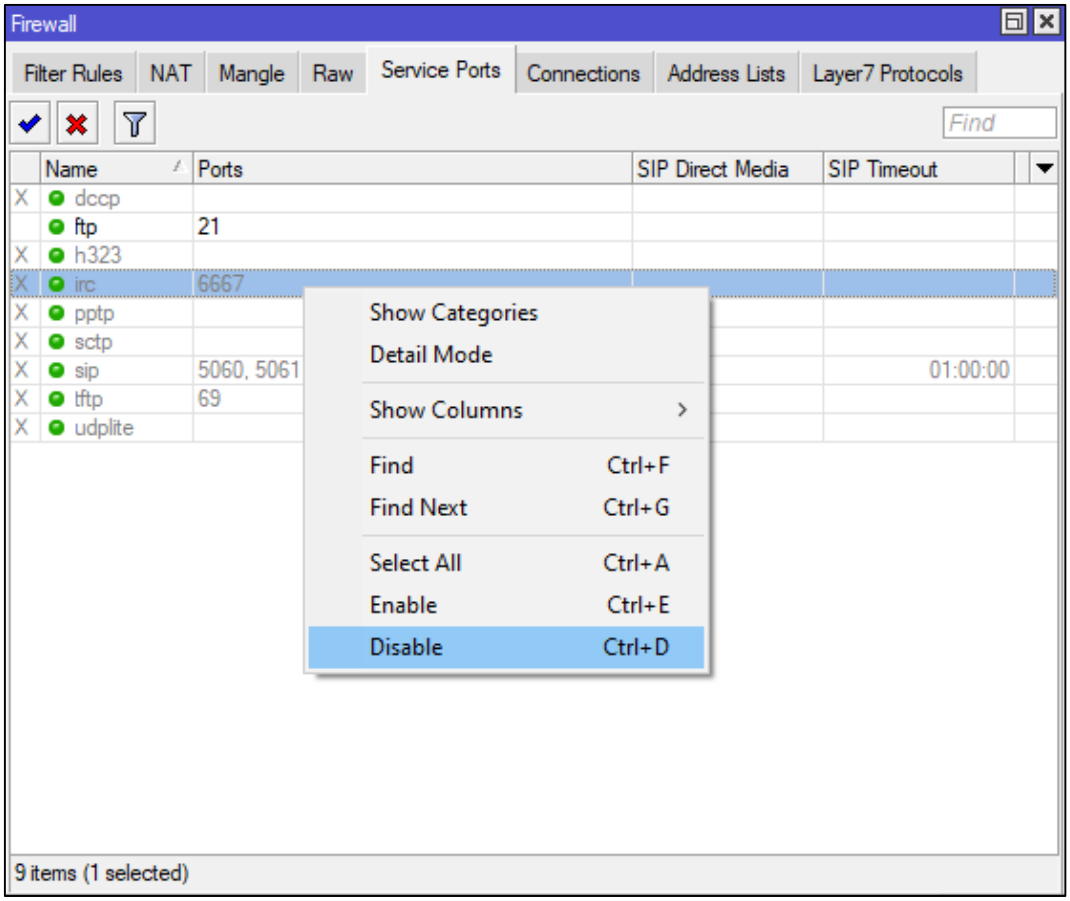


Fonte: Os autores

5.4.1.19 Portas de serviço

Foram desabilitadas portas de serviços que nãos seriam utilizadas pelo cliente, pois o mesmo não possui aplicações que exigem tais liberações. Para isso, o menu *IP > Firewall > NAT* foi utilizado. Cada porta de serviço foi selecionada e desabilitada, através do botão *Disable (X)*. A Figura 49 exibe a guia *Service Ports*, no menu *Firewall*.

Figura 49. Portas de serviço – Processo de desabilitação



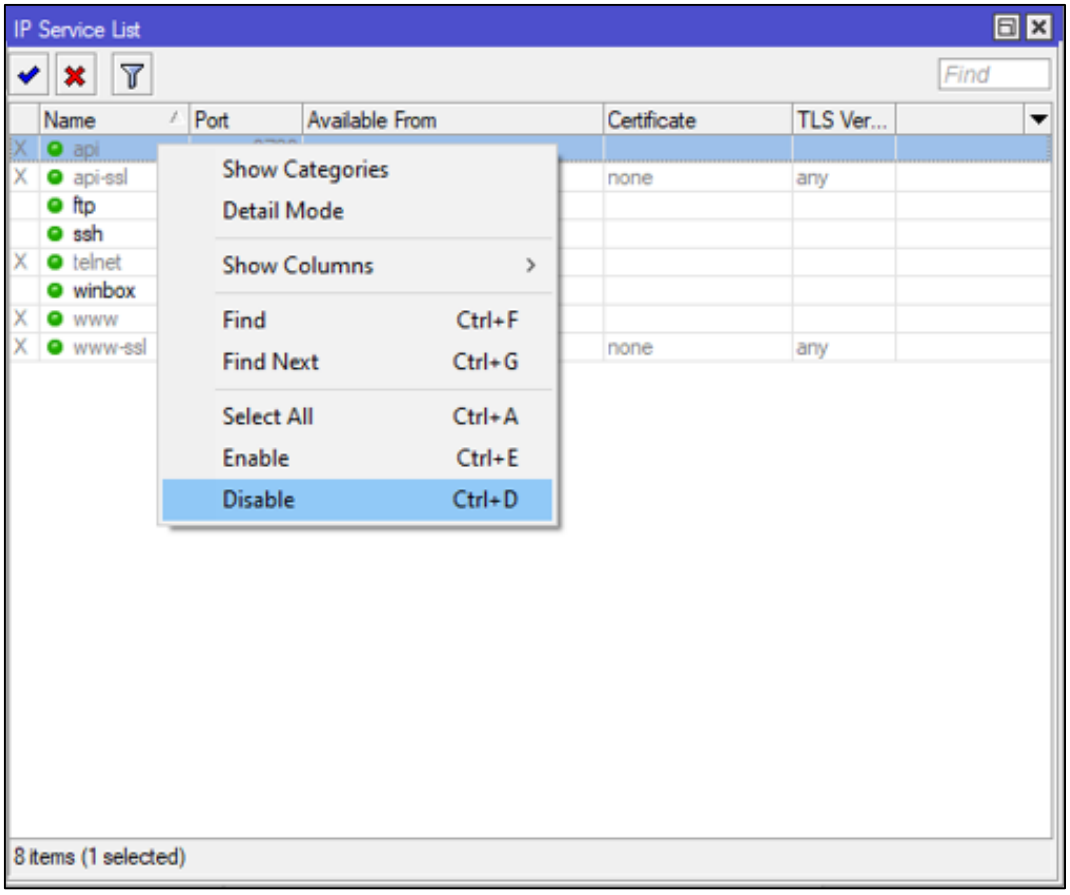
Fonte: Os autores

Existe uma prática realizada em *firewall* que determina o fechamento de portas de serviço caso não sejam utilizadas. Isso contribui na segurança do equipamento. Essa pratica foi adotada na configuração dos *routerboards* da Quatro Cambalhotas.

5.4.1.20 Lista de serviços IP

Semelhante a ação realizada na seção 5.4.1.19, foram desabilitados os serviços que não seriam utilizados através do menu *IP > Services > IP Service List*. Para tal, cada serviço deste foi selecionado e clicado no botão *Disable (X)***,** conforme ilustrado na Figura 50. Foram mantidos habilitados apenas os serviços ***SSH*** e ***Winbox***, que são utilizados para acesso ao *routerboard* com propósitos de suporte e manutenção.

Figura 50. Lista de serviços IP – Processo de desabilitação

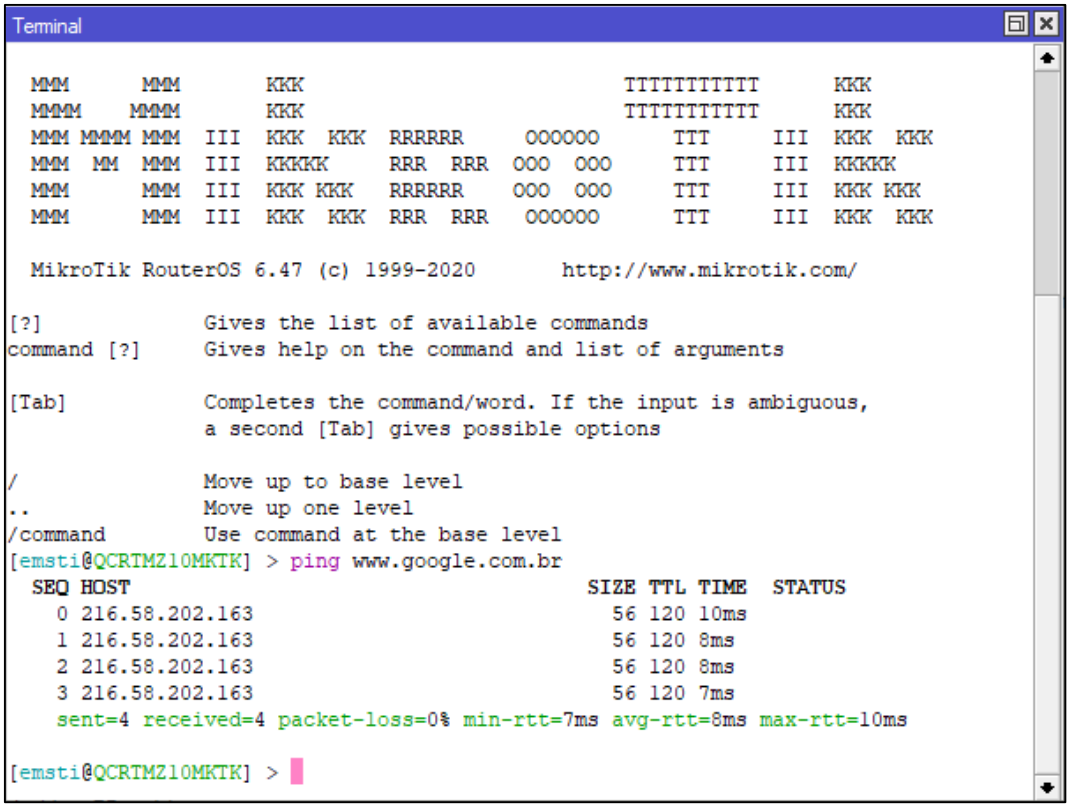


Fonte: Os autores

5.4.1.21 Testes via terminal

Ao término das configurações iniciais, foi realizado um teste de navegação do *routerboard* para o ambiente externo. Esse teste foi executado através do *New Terminal*, a partir de um teste *ping* para o *hostname* do Google. O comando ***ping*** **www.google.com.br** retornou êxito, conforme exibe a Figura 51, indicando que os pacotes enviados foram recebidos pelo *host* de destino.

Figura 51. Ferramenta *New Terminal*

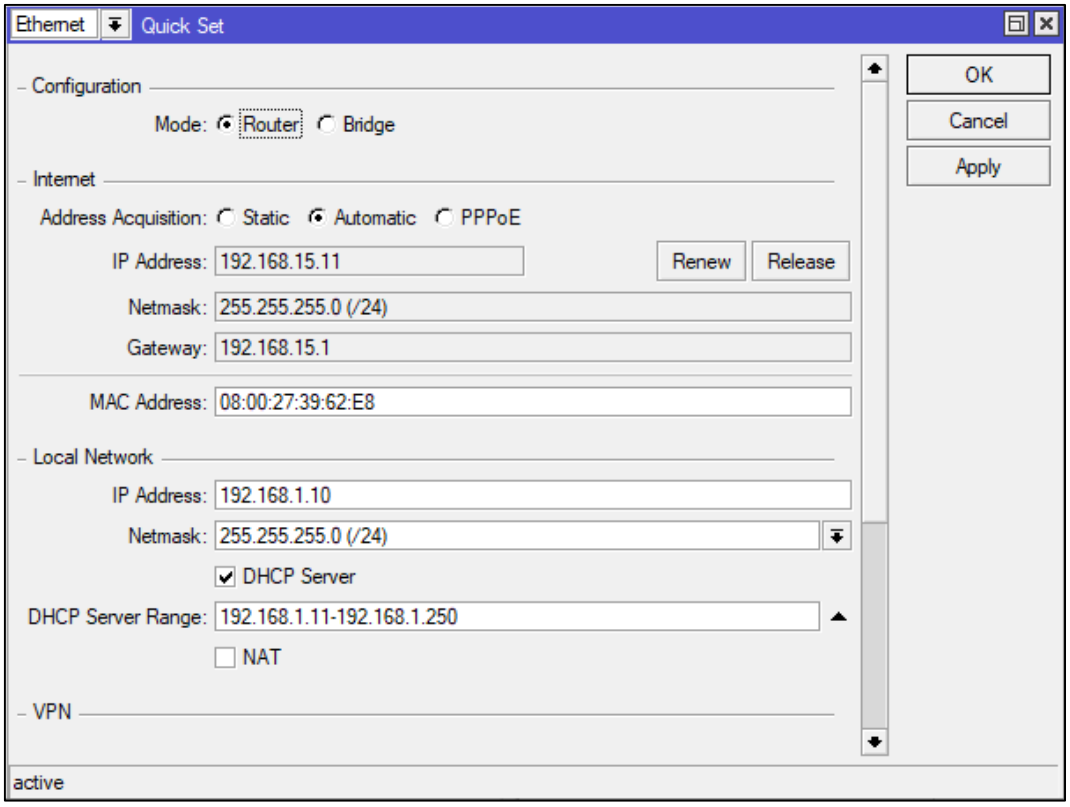


Fonte: Os autores

5.4.1.22 Quick Settings (Quick Set)

Existe um assistente rápido que pode ser utilizado para a configuração do equipamento, porém não utilizado, no caso. No entanto, é relevante indicarmos sua existência para os casos que apenas uma configuração mínima seja necessária para o funcionamento do *routerboard*. Ele pode ser acessado através do menu *Quick Set*, na barra vertical, localizada à esquerda no *Winbox*. A Figura 52 ilustra a tela desse assistente de configuração rápida.

Figura 52. Assistente de configuração rápido



Fonte: Os autores

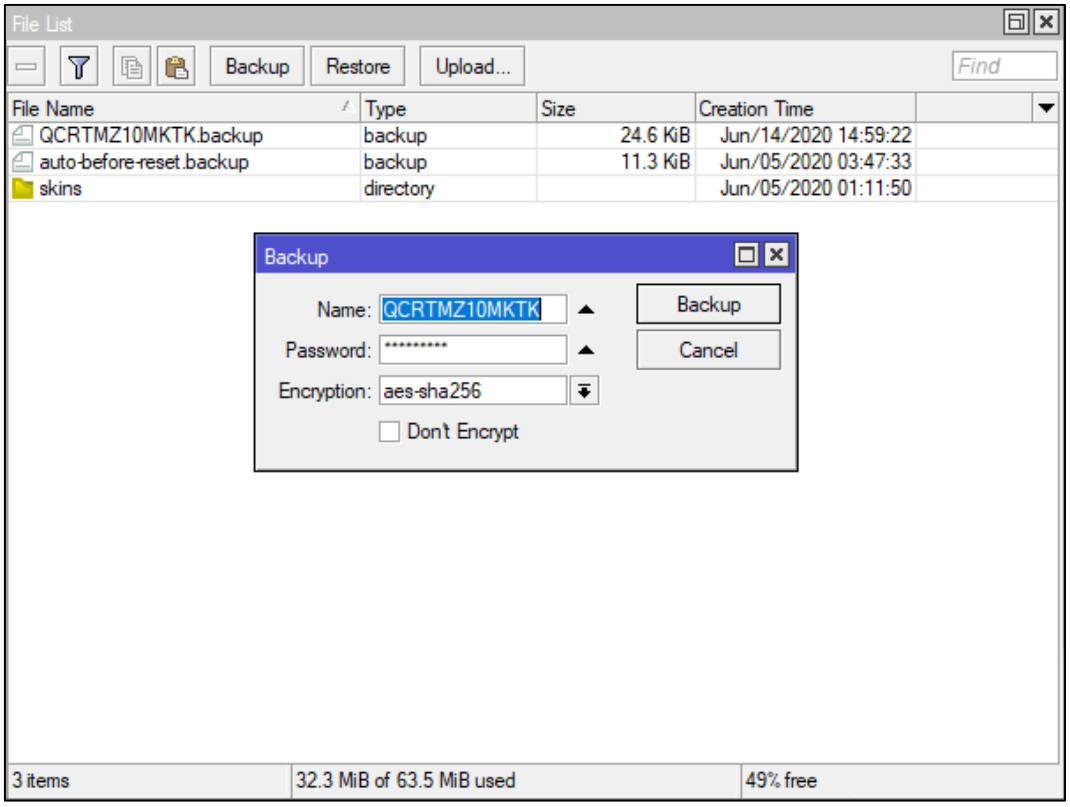
Todos os itens configurados podem ser facilmente identificados nesse assistente. Ele proporciona uma espécie de resumo que contempla todos os itens básicos de configuração.

5.4.1.23 Backup das configurações

Foi criado um *backup* das configurações, de modo a garantir um processo de *restore* caso necessário. Esse arquivo gerado foi encaminhado via *e-mail* aos cuidados dos proprietários e uma cópia também foi salva no servidor de arquivos. Esse arquivo possui uma senha e encriptação, que protege seu conteúdo contra manipulação indevida e mal-intencionada.

Através do menu *Files* > *File List*, o botão *Backup* foi clicado. Em seguida, o nome **QCRTMZ10MKTK** foi atribuído ao arquivo, juntamente com uma senha, no campo em *Password* e o método de encriptação **AES-SHA256,** em *Encryption*. O arquivo foi gerado após o clique no botão *Backup*, o arquivo e armazenado em *File List.* O processo do backup foi ilustrado na Figura 53.

Figura 53. *Backup* das configurações no *RouterOS*



Fonte: Os autores

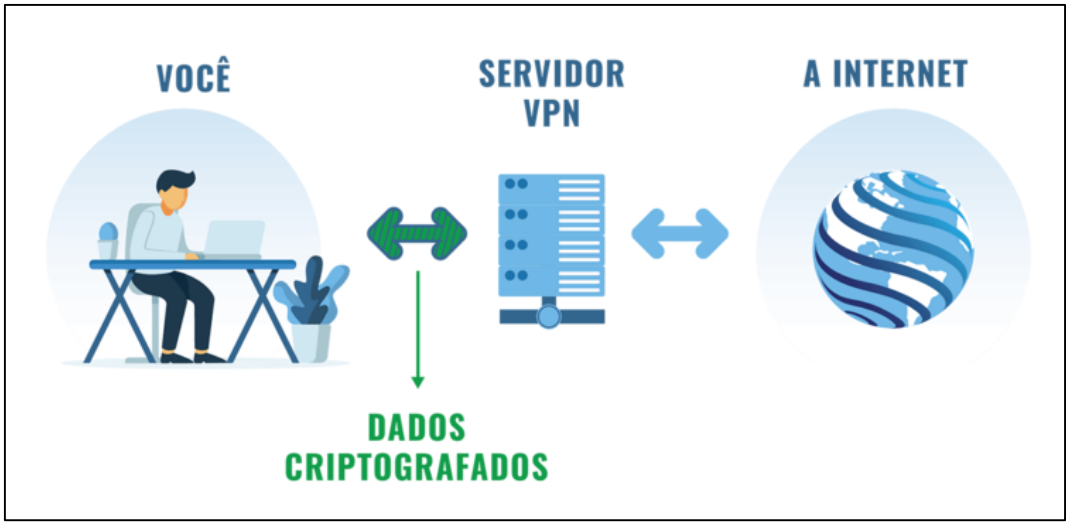
5.5 VPN

Uma *VPN*, sigla do termo em inglês *Virtual Private Network*, é exatamente o que a tradução do nome diz, uma rede privada virtual. Um serviço de rede intermediário opcional entre o usuário e a internet, que oferece ferramentas adicionais de criptografia e navegação segura e sigilosa.

Como a internet é uma rede pública e um tanto insegura, faz-se necessário a criação de mecanismos de segurança para que as informações trocadas entre os dispositivos em uma *VPN* não possam ser interceptadas e lidas por outras pessoas.

A criptografia é a proteção mais utilizada, pois ela garante que os dados transmitidos por um dos dispositivos da rede sejam os mesmos que os demais dispositivos irão receber. Depois de serem criptografados, esses dados são encapsulados e transmitidos pela internet, utilizando o protocolo de tunelamento escolhido, neste caso o *OpenVPN*, até encontrarem seu destino final. A Figura 54 ilustra um exemplo básico de conexão *VPN*.

Figura 54. Conexão *VPN*



Fonte: Os autores

5.5.1 Configurações iniciais da VPN

Para iniciar o serviço *VPN*, foi necessário preparar o *routerboard* com configurações mais específicas. Para isso, foram alterados alguns parâmetros básicos e que foram descritos no decorrer desta seção.

5.5.1.1 Identificação do túnel entre os routerboards

Foi necessário informar quais os endereços seriam utilizados para identificar o túnel *VPN* entre matriz e filial. A Tabela 5 foi construída para auxiliar-nos no momento da configuração deste túnel e foi descrita com mais detalhes na seção 5.5.1.4.

Tabela 5. *Hostnames* e endereços IP para o túnel *VPN*

TÚNEL VPN	MATRIZ	FILIAL
IP Externo - VIVO	201.1.127.10	201.1.127.130
DDND - No-IP	quatrocambalhotas-mz.ddns.net	quatrocambalhotas-mz.ddns.net
IP da WAN	192.168.15.11	192.168.15.131
IP do TÚNEL (M <=> F)	172.201.15.1	172.201.15.2
IP da LAN	192.168.1.0/24	192.168.2.0/24

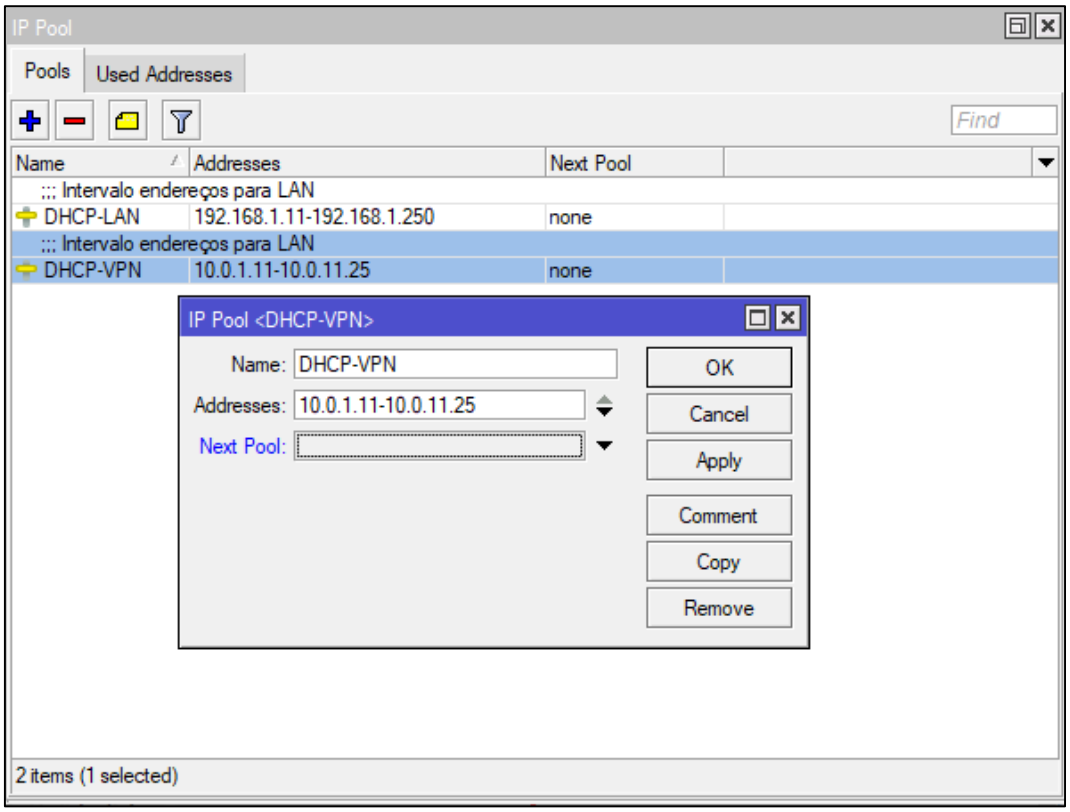
Fonte: Os autores

5.5.1.2 Intervalo de endereços DHCP (Pool)

Foi criado um novo *pool* de endereços para ser utilizado nas conexões *VPN* do tipo *client-to-site*. Esses endereços serão entregues via *Profile*, que desempenha um papel semelhante ao serviço *DHCP*, porém atuando apenas nas conexões *VPN client-*

to-site. Navegado pelo menu *IP > Pool > Add (+)* e, em *New IP Pool*, foi adicionado o intervalo de endereços IP, que inicia em **10.0.1.11** e vai até o **10.0.1.25** no parâmetro *Address*. Foi nomeado esse intervalo para ***DHCP-VPN*** e salvo esta através dos botões *Apply* e *OK*, conforme exibe a Figura 55. Importante a utilização do **hífen (-)** na definição deste intervalo, entre o endereço IP de início e o endereço final.

Figura 55. IP *Pool* - Intervalo de endereços IP para *VPN*

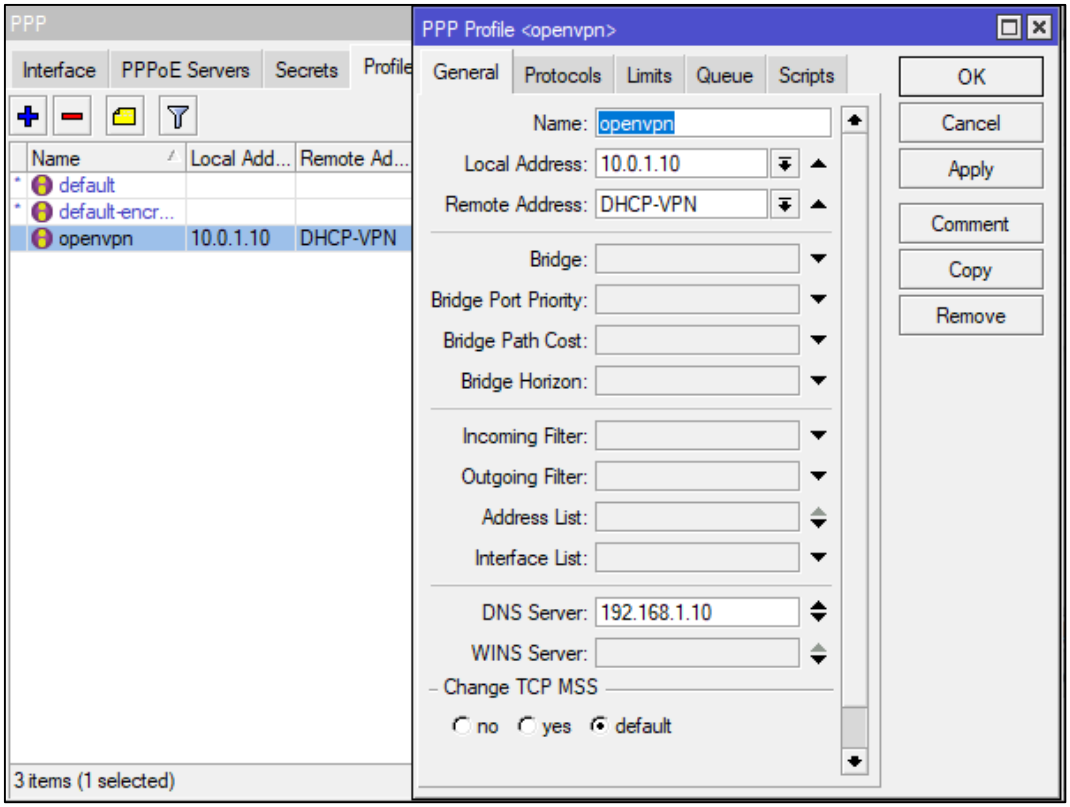


Fonte: Os autores

5.5.1.3 Perfil na VPN

Logo após a criação do *pool* de endereços para a *VPN*, foi preciso adicionar um perfil que será responsável por distribuir os endereços IP para as conexões remotas, função parecida ao do *DHCP,* na rede local. Para isso, foi acessado o item *PPP*, no menu vertical e, na aba *Profiles*, clicado no botão *Add (+).* Esse perfil foi nomeado como ***openvpn***, informado o endereço IP local **10.0.1.10** e selecionado o *pool* ***DHCP-VPN***. Em *DNS Server*, foi informado o endereço IP **192.168.1.10** do servidor *DNS*. As alterações foram salvas através dos botões *Apply* e *OK*. A Figura 56 exibe a criação desse perfil.

Figura 56. Gerenciamento de perfil *PPP*

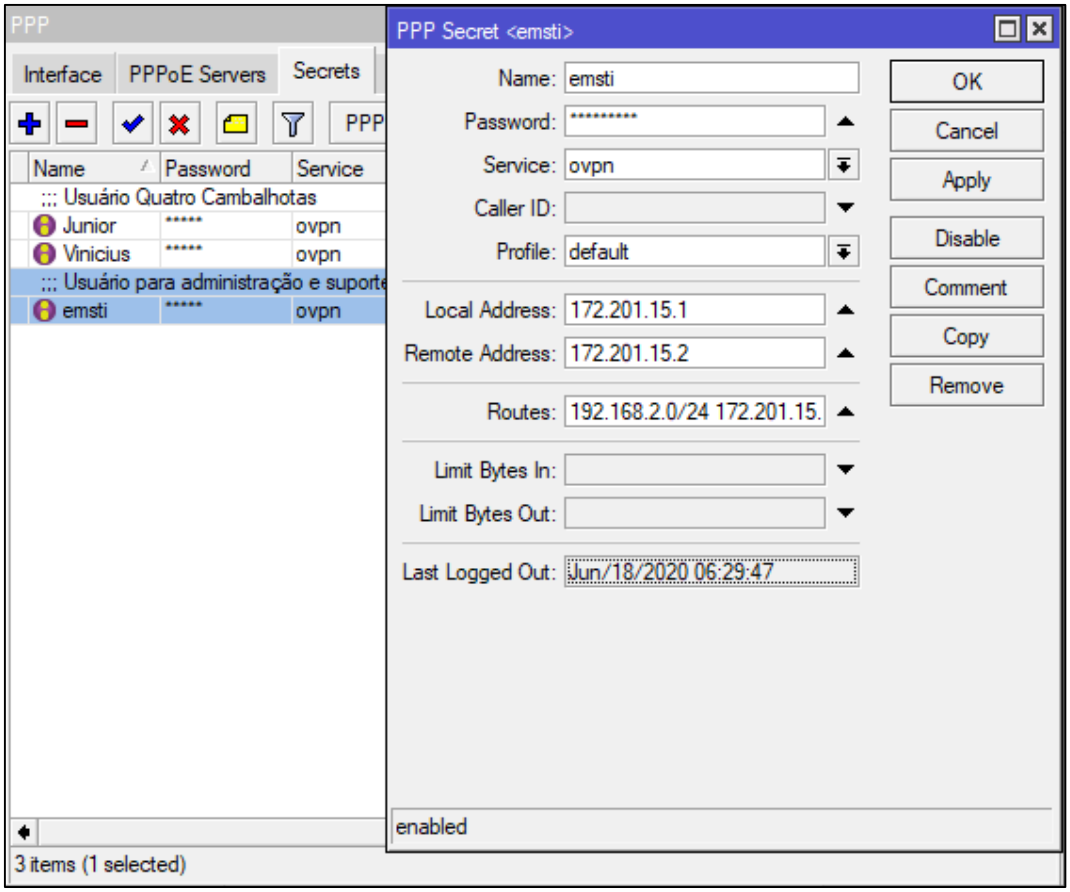


Fonte: Os autores

5.5.1.4 Credencial (PPP Secrets)

Nesta etapa foi criado o usuário **emsti**, que foi utilizado para a autenticação do túnel *VPN*, entre a matriz e a filial. Para adiciona-lo, foi navegado pelo menu *PPP* > *Secrets* e clicado no botão *Add (+).* Em *Name*, foi digitado o nome **emsti**, criado uma senha em *Password* e adicionados os endereços IP **172.201.15.1** e **172.201.15.2** nos campos *Local Address* e *Remote Address*, respectivamente. A rota entre os locais foi definida através dos endereços IP **192.168.2.0/24 172.201.15.2 1**, que são correspondentes aos parâmetros *Dst. Address*, *Gateway* e *Distance* do item *New Route,* no menu *IP* > *Routes*. A Figura 57 exibe o momento desta configuração.

Figura 57. Gerenciamento de usuários *VPN*



Fonte: Os autores

5.5.1.5 Certificados

Certificados são necessários para prover uma conexão segura na *VPN*. São eles que garantem a confidencialidade, integridade e a disponibilidade da informação. Esses requisitos são os pilares de segurança da informação. O serviço *OpenVPN* solicita a criação mínima de três certificados para prover uma conexão segura:

- Autoridade certificadora;
- Servidor;
- Cliente.

Foi configurado primeiro o certificado da autoridade certificadora (*CA*), que será utilizado para assinar e validar digitalmente os outros dois. Para isso, foi acessado o menu *System* > *Certificates* e na guia *Certificates*, o botão *Add (+)* foi clicado. Foram preenchidos com os valores disponíveis e relacionados na Tabela 6 os parâmetros nas abas *General* e *Key Usage*.

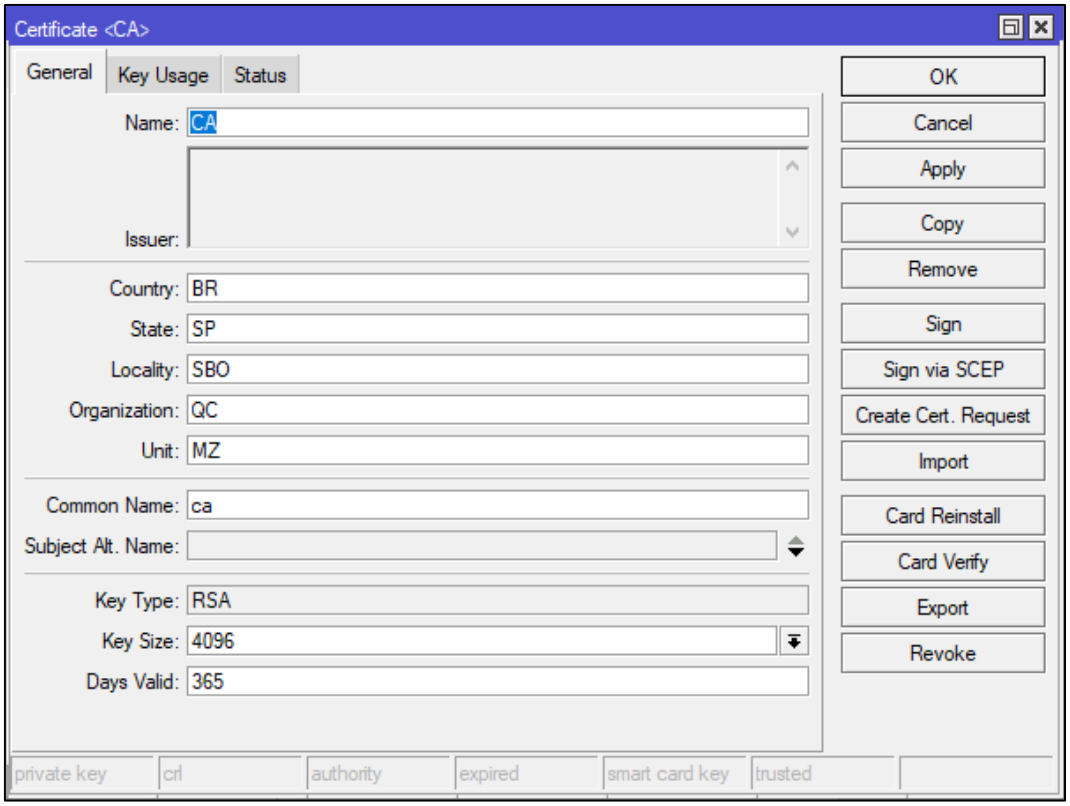
Tabela 6. Valores para o certificado CA

Certificate (Certificado)	
CA - Certification authority	**Autoridade certificadora (AC)**
General (Geral)	
Name (Nome)	CA
Country (País)	BR
State (Estado)	SP
Locality (Localidade)	S B O
Organization (Organização)	QC
Unit (Unidade)	MZ
Common name (Nome comum)	ca
Subject Alt. Name (Nome alternativo)	-
Key Type (Tipo de chave)	RSA
Key Size (Tamanho da chave)	4096
Days Valid (Dias válidos)	365
Key Usage (uso de chave)	
Enable (Habilitado)	Key Cert. Sign
Enable (Habilitado)	CRL Sign
Security	
Enable (Habilitado)	Trusted (Confiável)

Fonte: Os autores

A Figura 58 ilustra os campos preenchidos na guia *General*. O botão *Apply* foi clicado para salvar as informações e, em seguida, alternado para a guia, *Key Usage*.

Figura 58. Certificado CA – *General*

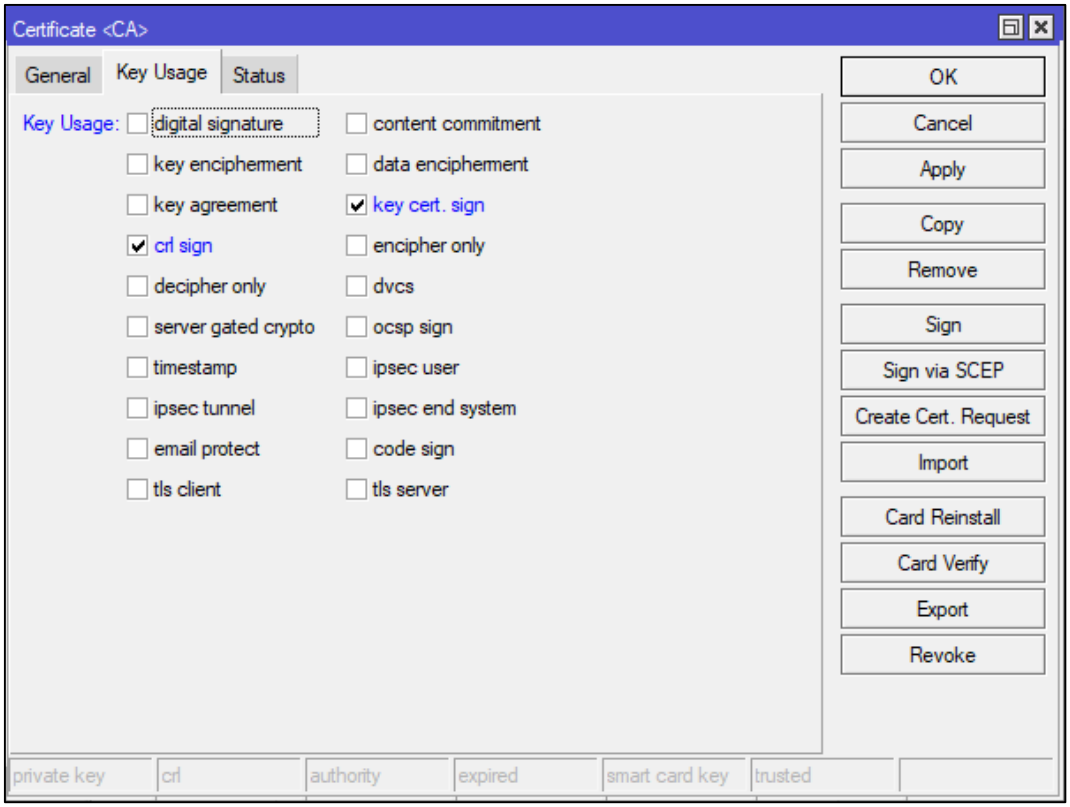


Fonte: Os autores

Em *Key Usage*, com exceção de **CRL Sign** e **Key Cert.Sign**, todos os demais itens foram desmarcamos e a configuração salva através dos botões *Apply* e *OK*.

A Figura 59 ilustra as alterações realizadas na guia *Key Usage*.

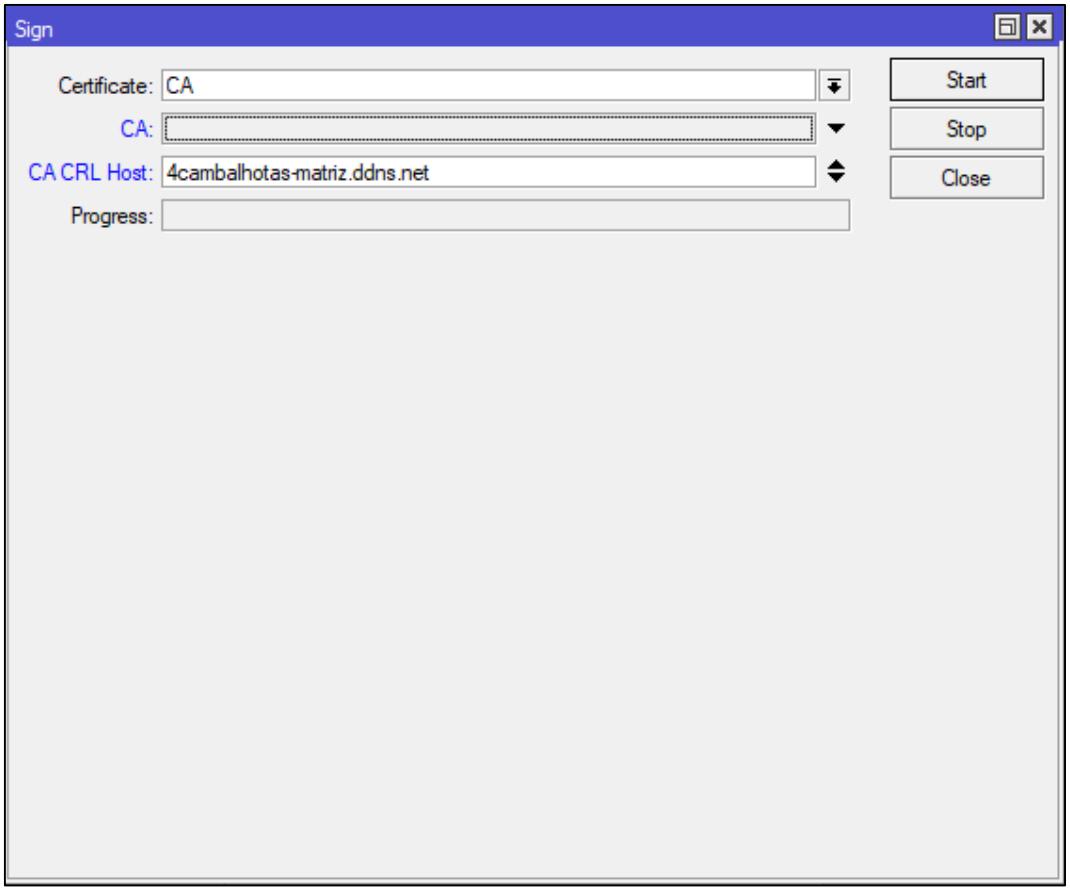
Figura 59. Certificado CA – *Key Usage*



Fonte: Os autores

Em seguida, o certificado *CA* foi assinado digitalmente, através do botão *Sign*, disponível na aba *General*. Em *CA CRL Host*, foi informado o endereço *DDNS* **4cambalhotas-matriz.ddns.net** e clicado no botão *Start*. O término desse processo é indicado através do *status* ***Done*** no campo *Progress*. Para finalizar, um clique no botão *Close*. Esse processo de assinatura foi ilustrado na Figura 60.

Figura 60. Assinando o certificado CA



Fonte: Os autores

Após assinado, o certifica *CA* assumiu o valor ***Trusted***, disponível na aba *General*, em *Certificate <CA>,* dispensando sua marcação manual.

Em seguida, foi criado o certificado *SERVER*, utilizando o mesmo processo de criação do certificado *CA*. Foram utilizadas as informações da Tabela 7 neste item.

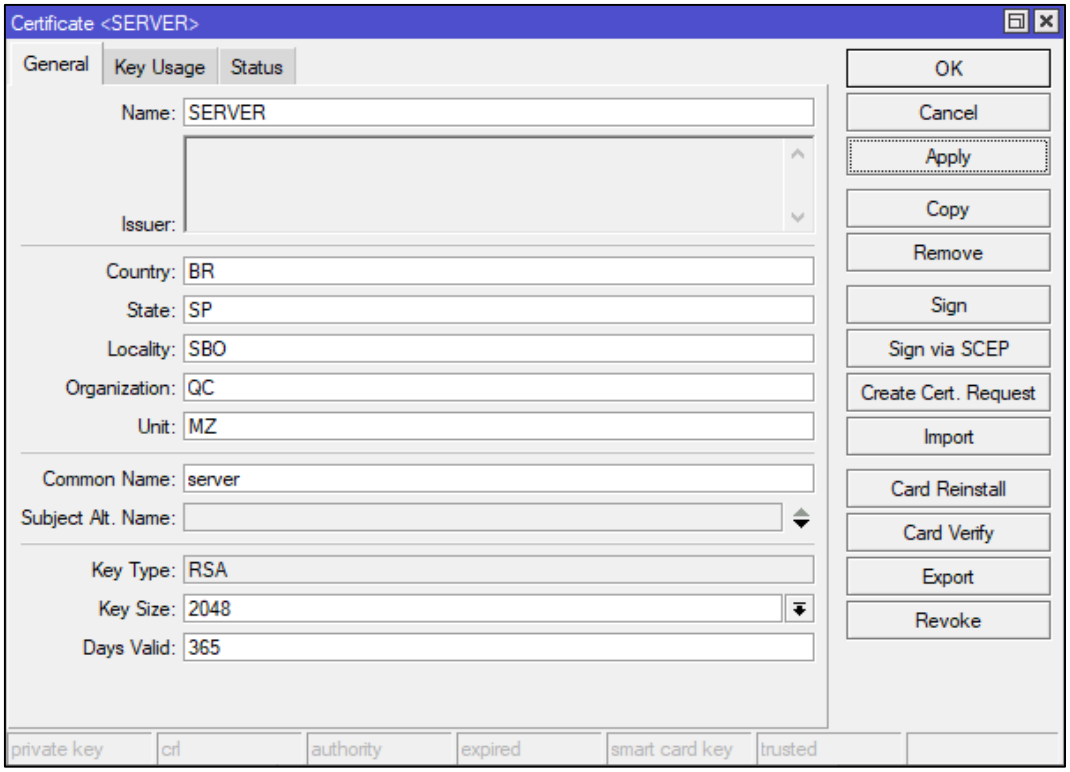
Tabela 7. Valores para o certificado SERVER

Certificate (Certificado)	
SERVER - Server	**Servidor**
General (Geral)	
Name (Nome)	SERVER
Country (País)	BR
State (Estado)	SP
Locality (Localidade)	S B O
Organization (Organização)	QC
Unit (Unidade)	MZ
Common name (Nome comum)	server
Subject Alt. Name (Nome alternativo)	-
Key Type (Tipo de chave)	RSA
Key Size (Tamanho da chave)	4096
Days Valid (Dias válidos)	365
Key Usage (uso de chave)	
Enable (Habilitado)	Digital Signature
Enable (Habilitado)	Key Encipherment
Enable (Habilitado)	TLS Server
Security	
Enable (Habilitado)	Trusted (Confiável)

Fonte: Os autores

A Figura 61 exibe as configurações que foram realizadas na aba *General*, do certificado *SERVER*.

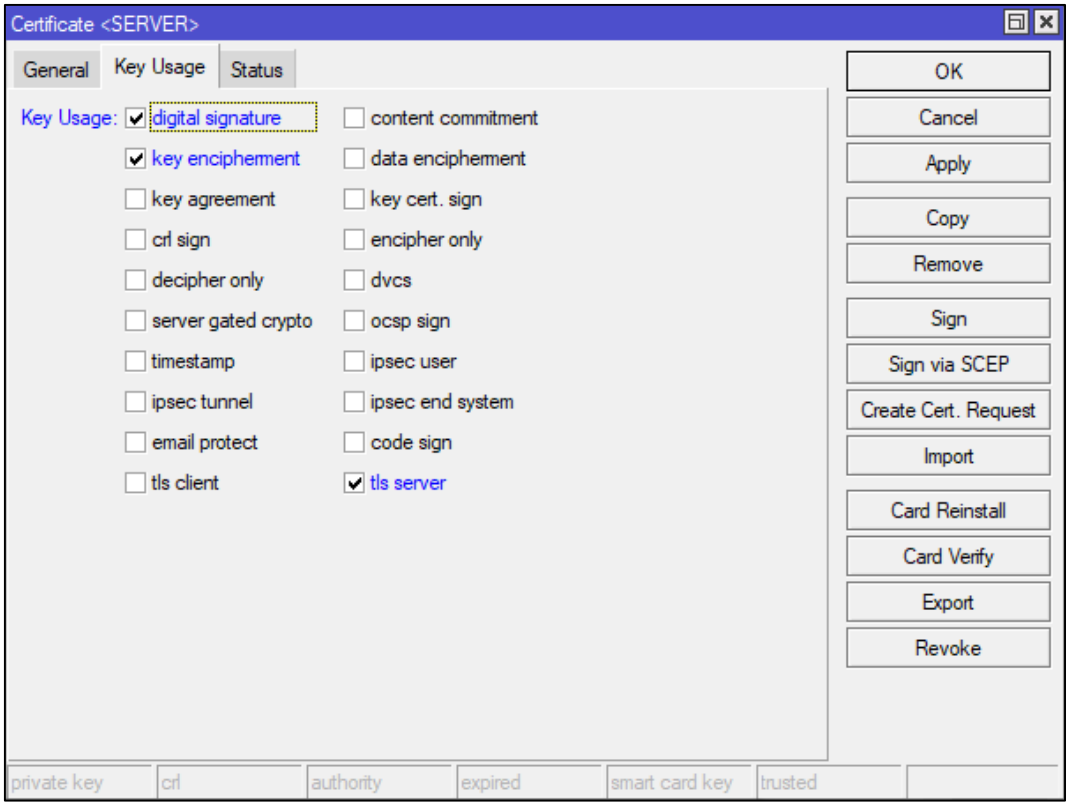
Figura 61. Certificado SERVER – *General*



Fonte: Os autores

Na aba *Key Usage*, foram marcadas apenas as opções *Digital Signature*, *Key Encipherment* e *TLS Server*, conforme ilustradas na Figura 62 e, através dos botões *Apply* e *OK*, as alterações foram salvas.

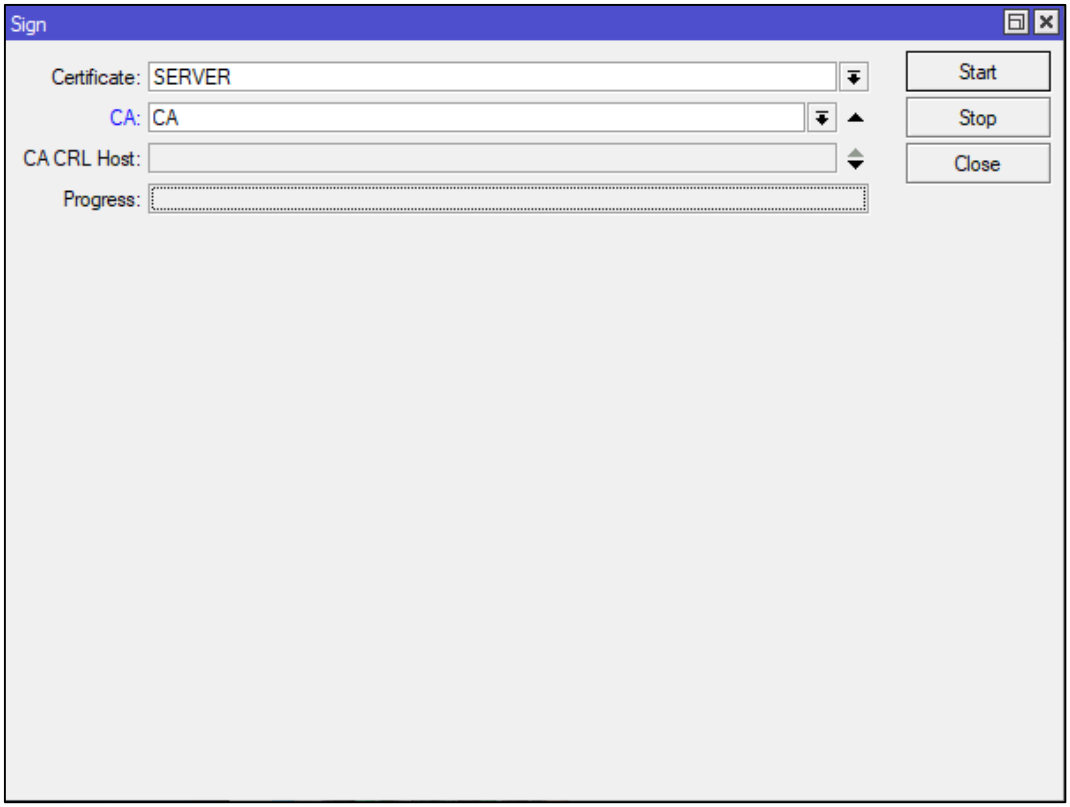
Figura 62. Certificado SERVER – *Key Usage*



Fonte: Os autores

Logo após, este certificado foi assinado, através do clique no botão *Sign* na aba *General* e da seleção do certificado ***CA*** no campo *CA*. O processo foi iniciado quando clicado o botão *Start* e, ao término, o botão *Close*. A Figura 63 exibe o momento da assinatura do certificado *Server*.

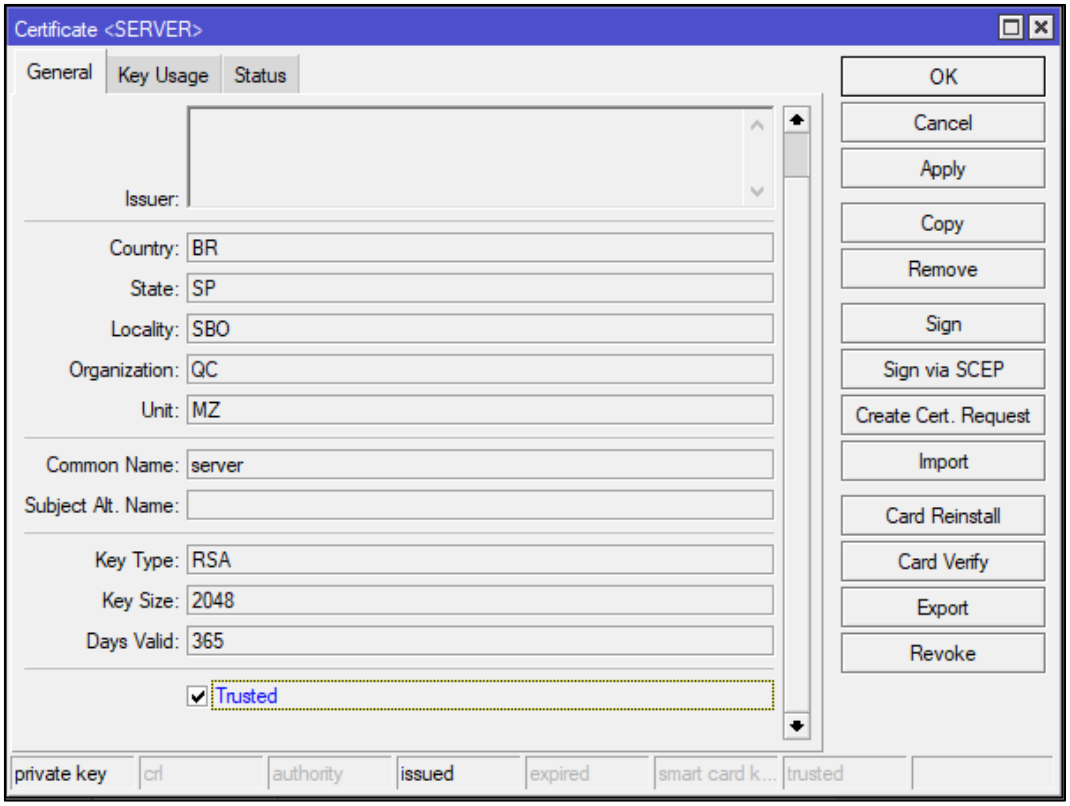
Figura 63. Assinando o certificado SERVER



Fonte: Os autores

O certificado *SERVER* foi marcado como **confiável**, na caixa *Trusted*, na aba *General*, em *Certificate <SERVER>*, conforme ilustrado na Figura 64.

Figura 64. Confiabilidade do certificado SERVER



Fonte: Os autores

Essa etapa foi finalizada com a criação do certificado *CLIENT*. Foi utilizada a Tabela 8 para o apoio no preenchimento das informações nos campos necessários.

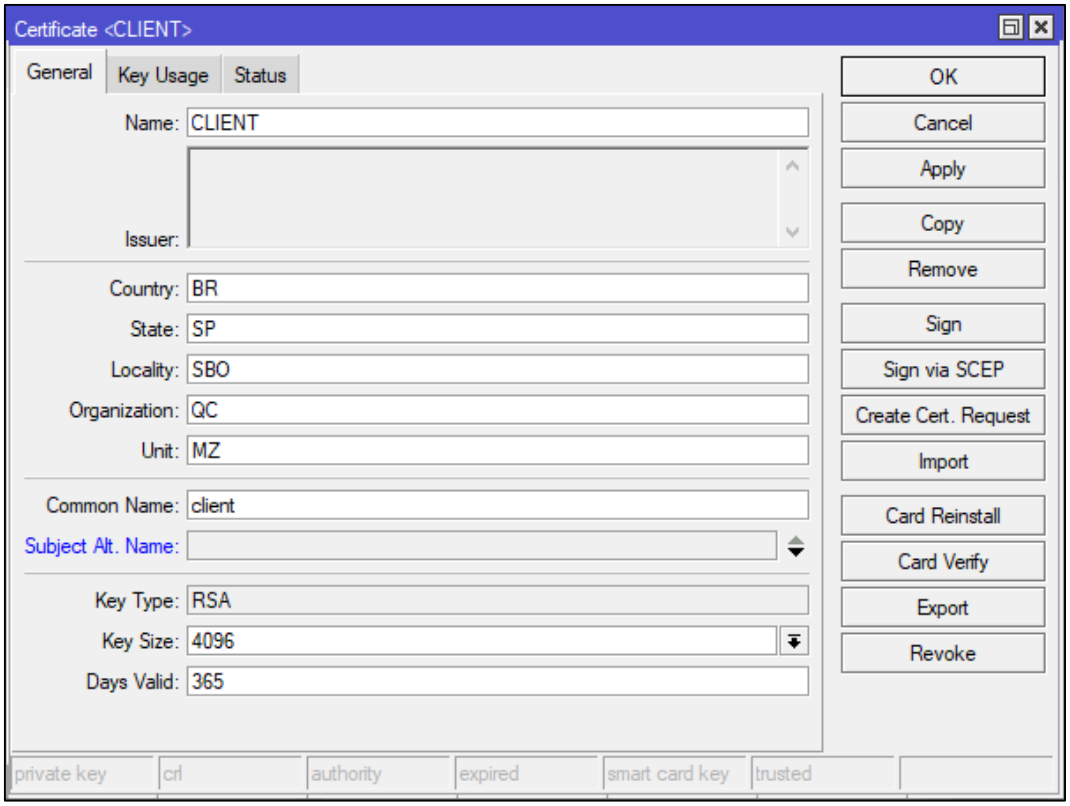
Tabela 8. Valores para o certificado CLIENT

Certificate (Certificado)	
CLIENT - Client	**Cliente**
General (Geral)	
Name (Nome)	CLIENT
Country (País)	BR
State (Estado)	SP
Locality (Localidade)	S B O
Organization (Organização)	QC
Unit (Unidade)	MZ
Common name (Nome comum)	client
Subject Alt. Name (Nome alternativo)	-
Key Type (Tipo de chave)	RSA
Key Size (Tamanho da chave)	4096
Days Valid (Dias válidos)	365
Key Usage (uso de chave)	
Enable (Habilitado)	TLS Client
Security	
Enable (Habilitado)	Trusted (Confiável)

Fonte: Os autores

A Figura 65 exibe os campos que foram preenchidos em *General*. Em seguida, foi clicado em *Apply* para salvar as alterações e alternado para a guia *Key Usage*.

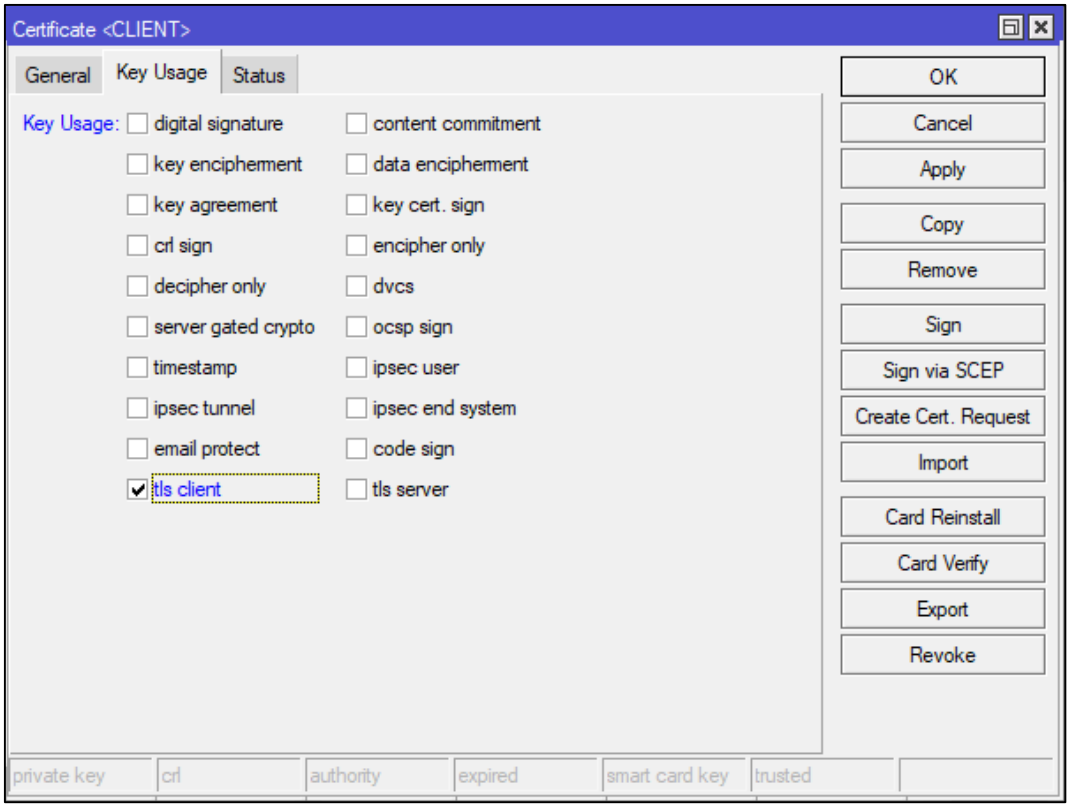
Figura 65. Certificado CLIENT – *General*



Fonte: Os autores

Em *Key Usage*, apenas a opção ***TLS Client*** foi marcada, conforme ilustra a Figura 66. As configurações foram salvas com a ajuda dos botões *Apply* e *OK*.

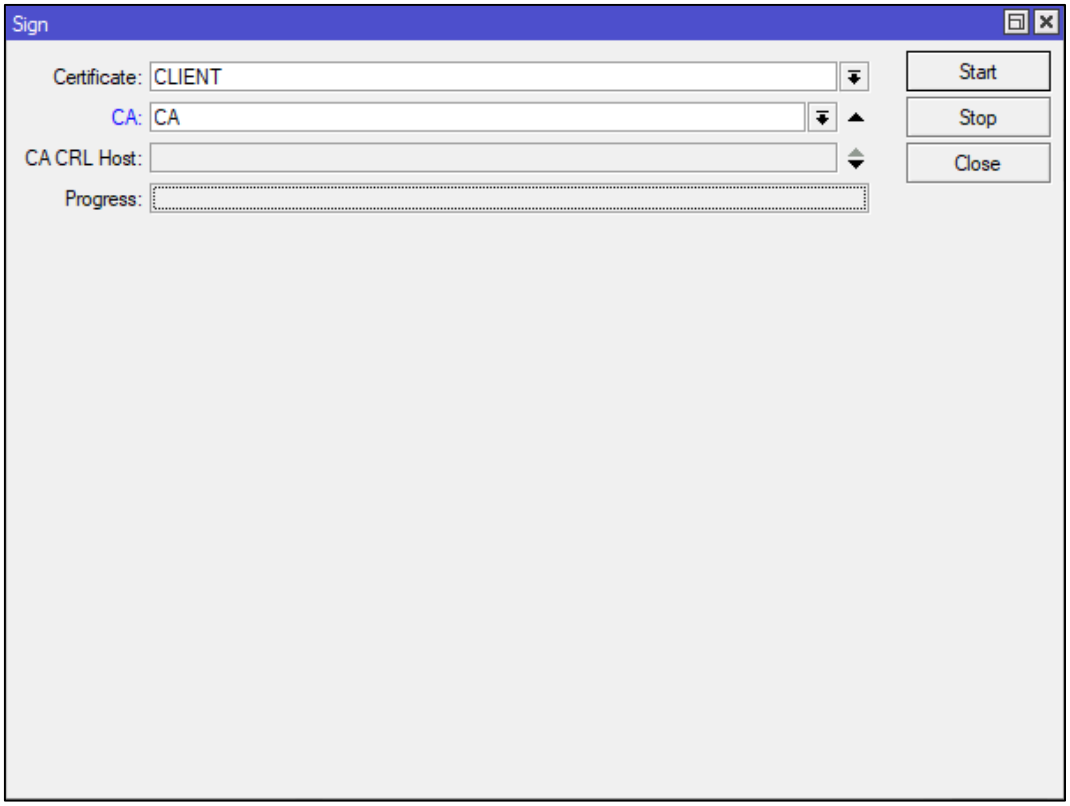
Figura 66. Certificado CLIENT – *Key Usage*



Fonte: Próprio autor

Este certificado também foi assinado, através do botão *Sign* na aba *General* e selecionado o certificado ***CA***, no campo *CA*. O processo foi iniciado pelo botão *Start* e ao seu término, o botão *Close* foi clicado. A Figura 67 exibe parte deste processo.

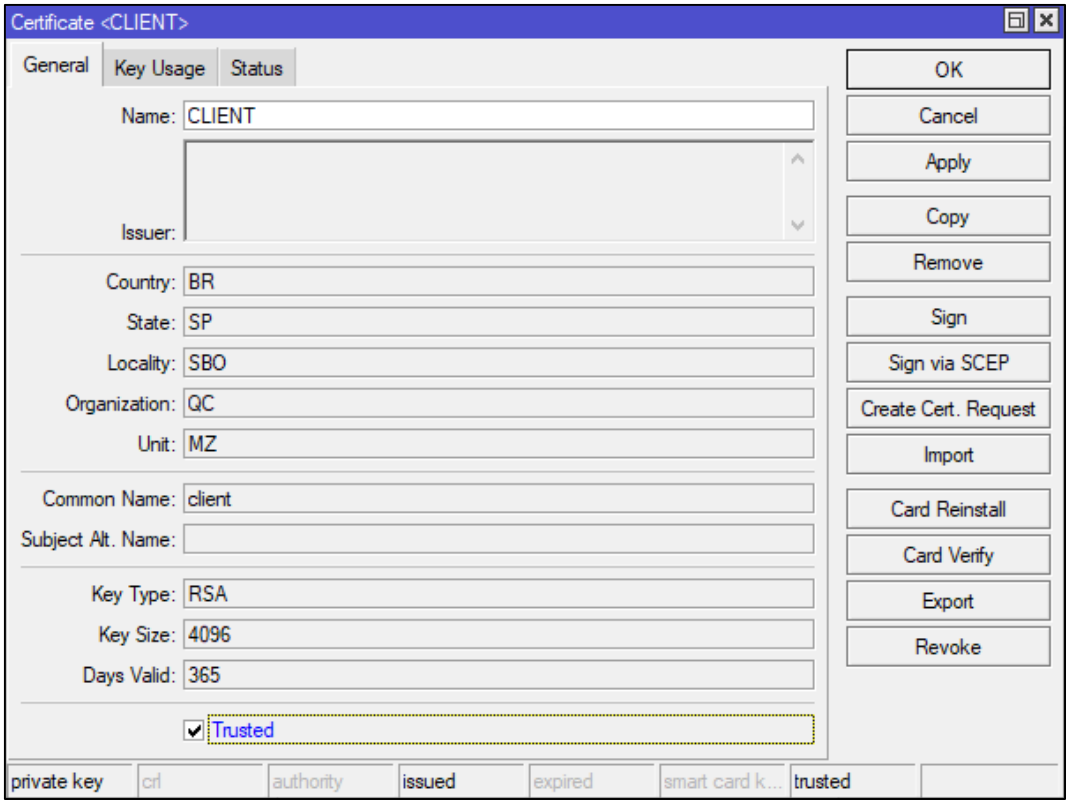
Figura 67. Assinando o certificado CLIENT



Fonte: Os autores

O certificado *CLIENT* foi marcado como **confiável**, na aba *General* quando clicado na caixa *Trusted*, conforme ilustrado na Figura 68.

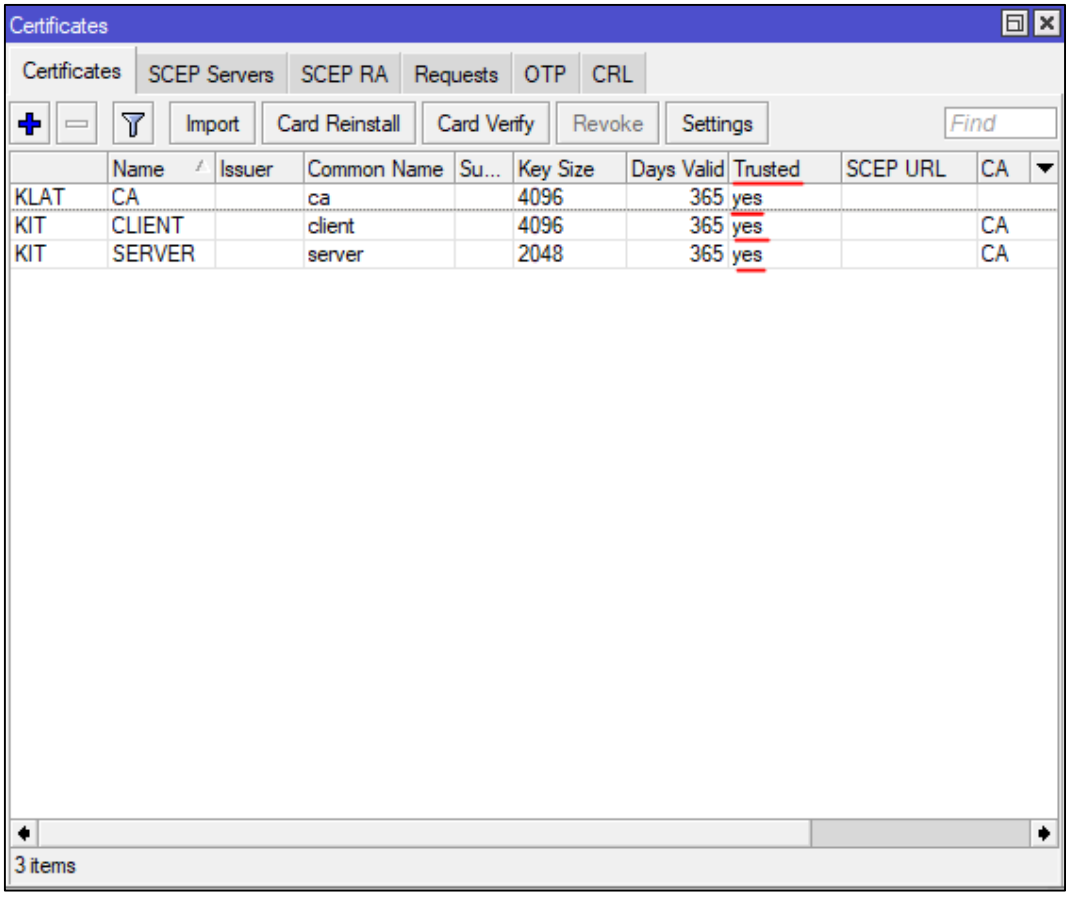
Figura 68. Confiabilidade do certificado CLIENT



Fonte: Os autores

Os três certificados foram ilustrados na Figura 69. A coluna *Trusted* foi destacada para indicar a importância de deixar os certificados marcados como confiáveis.

Figura 69. Certificados CA, SERVER e CLIENT



Fonte: Os autores

5.5.2 OpenVPN

O *OpenVPN*, que significa em sua tradução como rede virtual privada de código-fonte aberto, é um protocolo de *VPN* bem popular. Essa fama pode ter relação ao seu código-fonte ser aberto e à sua criptografia ser robusta e de alto nível. O *OpenVPN* é suportado pelas principais plataformas operacionais, como o Microsoft Windows, o MacOS e a maioria das distribuições Linux. Esse protocolo também é suportado por sistemas operacionais móveis, como o *Android* e o *iOS*, da Apple.

É fato que uma das principais funções do protocolo de *VPN* é fornecer uma criptografia de dados de nível elevado. Neste quesito, o *OpenVPN* tem um ótimo desempenho, pois utiliza uma criptografia de *256-bit* através de *OpenSSL*. Além disso, a maioria dos serviços de *VPN* disponíveis no mercado já suportam o *OpenVPN*.

Os protocolos *TCP* e *UDP* suportam o *OpenVPN*, mas é preciso entender em qual situação utiliza-lo. Entenda a diferença:

- *OpenVPN-TCP* é o protocolo mais utilizado e o mais confiável. Utilizar uma porta TCP significa que cada pacote de dados, individualmente, precisa ser aprovado pela parte receptora, antes que um novo possa ser enviado. Isso torna a conexão mais confiável e segura, porém tende a ser mais lenta.
- *OpenVPN-UDP* é significativamente mais rápido que o *OpenVPN-TCP*. Todos os pacotes de dados são enviados sem precisar de aprovação da parte receptora. O resultado é uma conexão *VPN* mais veloz, mas com certa perda de estabilidade e confiabilidade, pois não existe a confirmação de que todos os pacotes foram recebidos.

Em resumo, algumas vantagens e desvantagens do *OpenVPN* foram destacadas:

+ Serviço *VPN* muito seguro;

+ Suportado por muitos *softwares* e por praticamente todos os provedores de *VPN* modernos;

+ Suportado por quase todos os sistemas operacionais do mercado;

+ Amplamente testado, fiscalizado e modernizado;

+ Comunidade ativa e fóruns muito bem organizados;

– Às vezes necessita de *software* adicional;

Diferente de outras soluções de *VPN*, o *OpenVPN* utiliza uma única porta de entrada, a 1194, mesmo que sejam utilizadas várias *VPNs* simultaneamente. Isso facilita bastante a configuração do *firewall* ou do roteamento de portas no equipamento. Essa porta pode ser alterada, caso necessário e sem nenhum impacto.

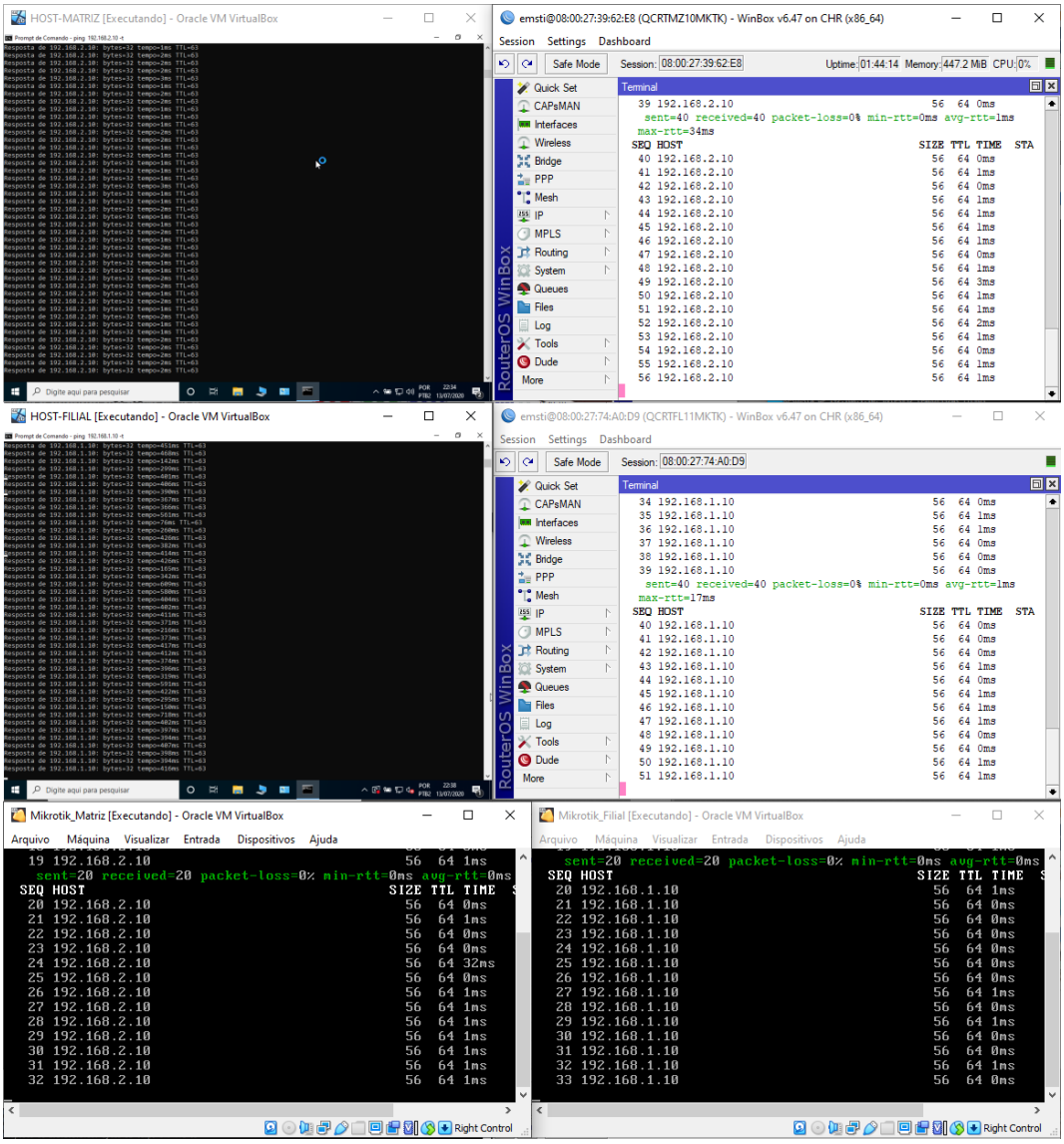
5.5.2.1 Configuração do serviço OpenVPN

O serviço *OpenVPN* foi iniciado, para as conexões *site-to-site* e *cliente-to-site*, com o ajuste dos últimos itens de configuração. Foram eles:

- Exportação dos certificados criados no *routerboard* da matriz;
- Habilitação do servidor *OpenVPN* no *routerboard* da matriz;
- Criação da interface *OpenVPN Client* no *routerboard* da filial.

A Figura 70 exibe uma cadeia de testes *ping* realizados entre os *routerboards* da matriz e filial e também entre os notebooks, cada um em sua rede local, após a criação do túnel via *OpenVPN*.

Figura 70. Visão geral do teste *ping* entre os equipamentos

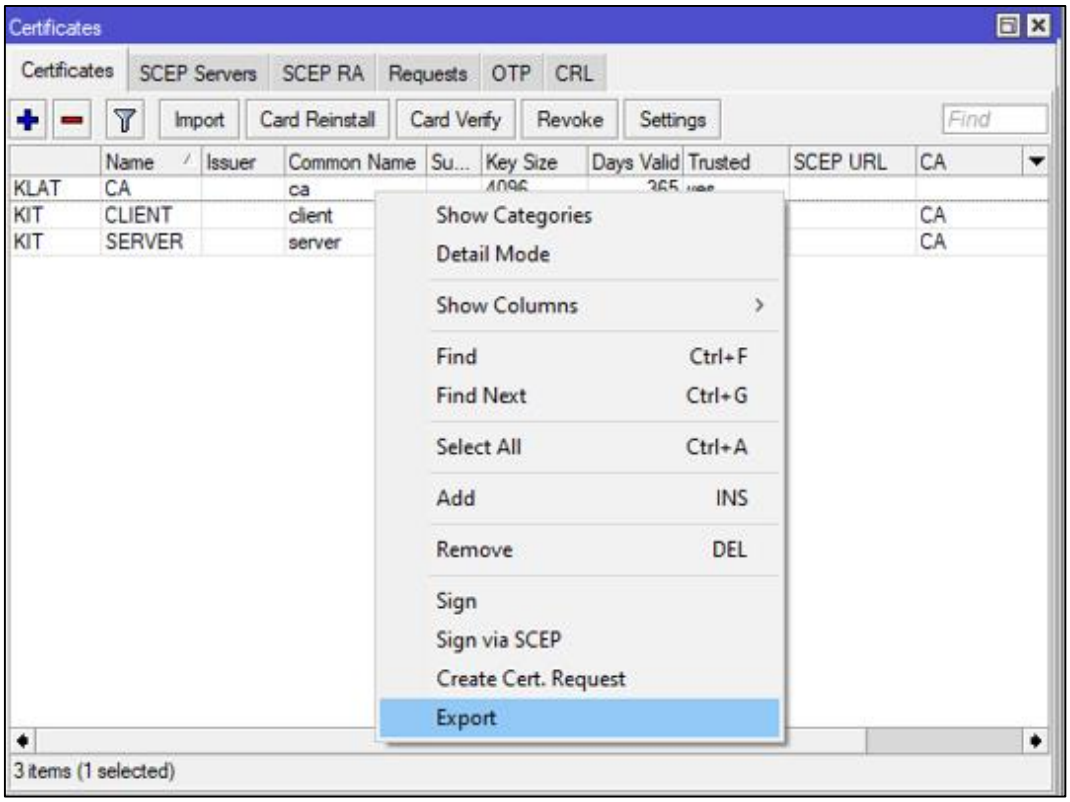


Fonte: Os autores

5.5.2.2 Exportação dos certificados

Os certificados criados no *routerboard* da matriz foram exportados para serem utilizados na conexão *VPN cliente-to-site*, via aplicativo *OpenVPN* instalado nos notebooks dos sócios da Quatro Cambalhotas. Para esta ação, foi acessado o menu *System* > *Certificates* e na aba *Certificates*, foi clicado com o botão direito sobre o certificado ***CA*** e selecionado a opção ***Export***, conforme ilustrado na Figura 71.

Figura 71. Exportando o certificado CA

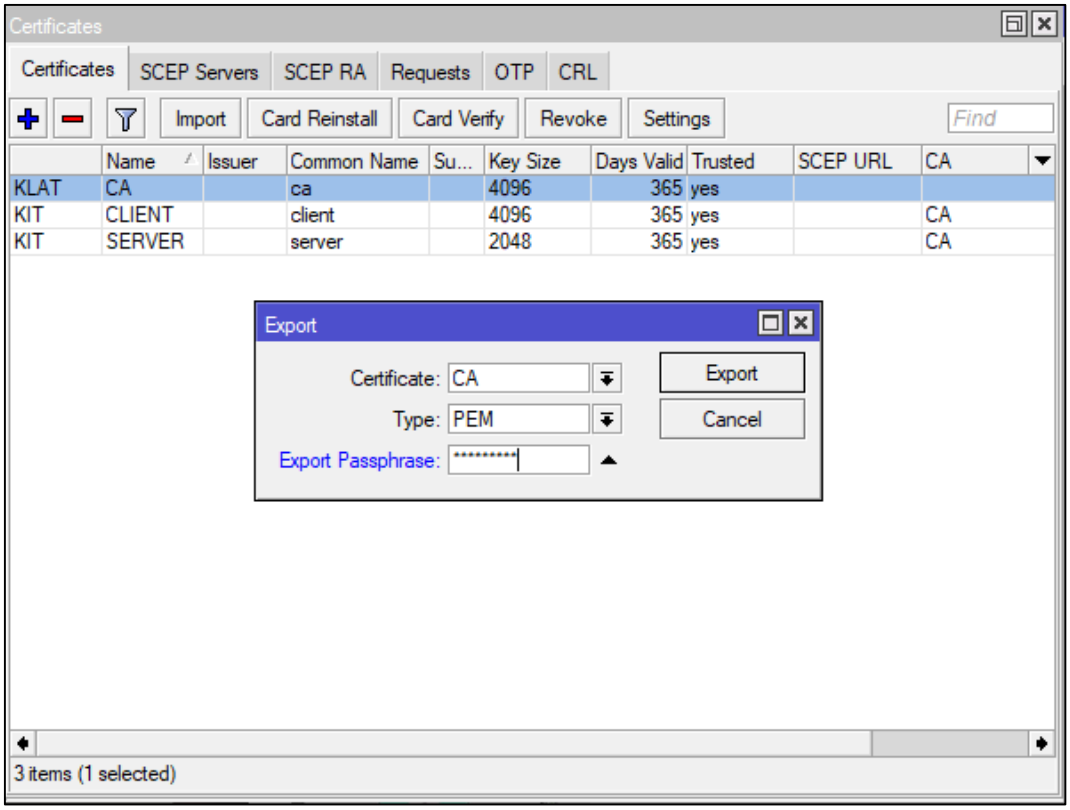


Fonte: Os autores

A Figura 72 ilustra a janela *Export*. Em *Export*, foi escolhido o método **PEM**[16] no campo *Type*, inserida uma **senha** em *Export Passphrase* e clicado no botão *Export* para concluir o processo de exportação.

[16] O *PEM*, sigla do termo em inglês *Privacy-Enhanced Mail*, é um formato de arquivo utilizado para armazenar e enviar chaves criptográficas, certificados e outros dados, com base em um conjunto de padrões IETF de 1993, que o definem como correio com privacidade aprimorada.

Figura 72. Senha de exportação do certificado

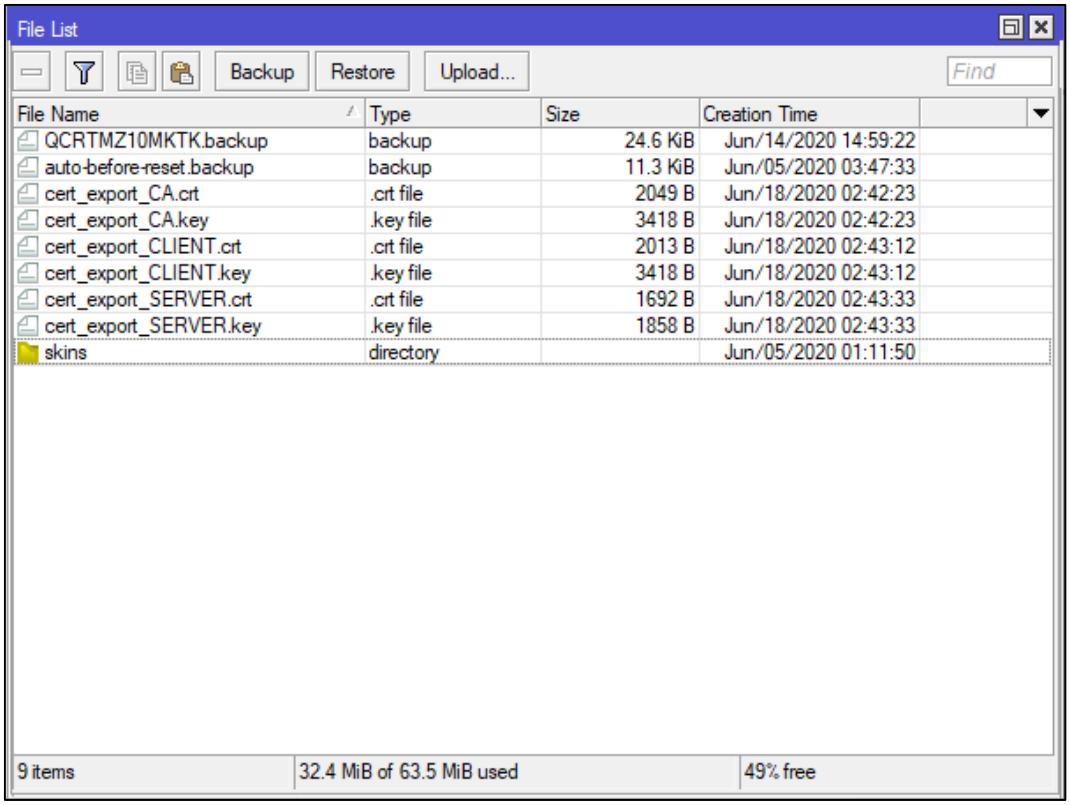


Fonte: Os autores

Esse processo foi reutilizado para exportar os certificados *SERVER* e *CLIENT*. Foi utilizada a mesma **senha** no campo *Passphrase* e o método de armazenamento ***PEM***, no campo *Type*.

A Figura 73 exibe o repositório *File List*, local onde os certificados exportados foram disponibilizados. Esses arquivos foram utilizados um pouco mais adiante, durante o processo de criação da conexão via aplicativo *OpenVPN*.

Figura 73. Repositório de arquivos *File List*

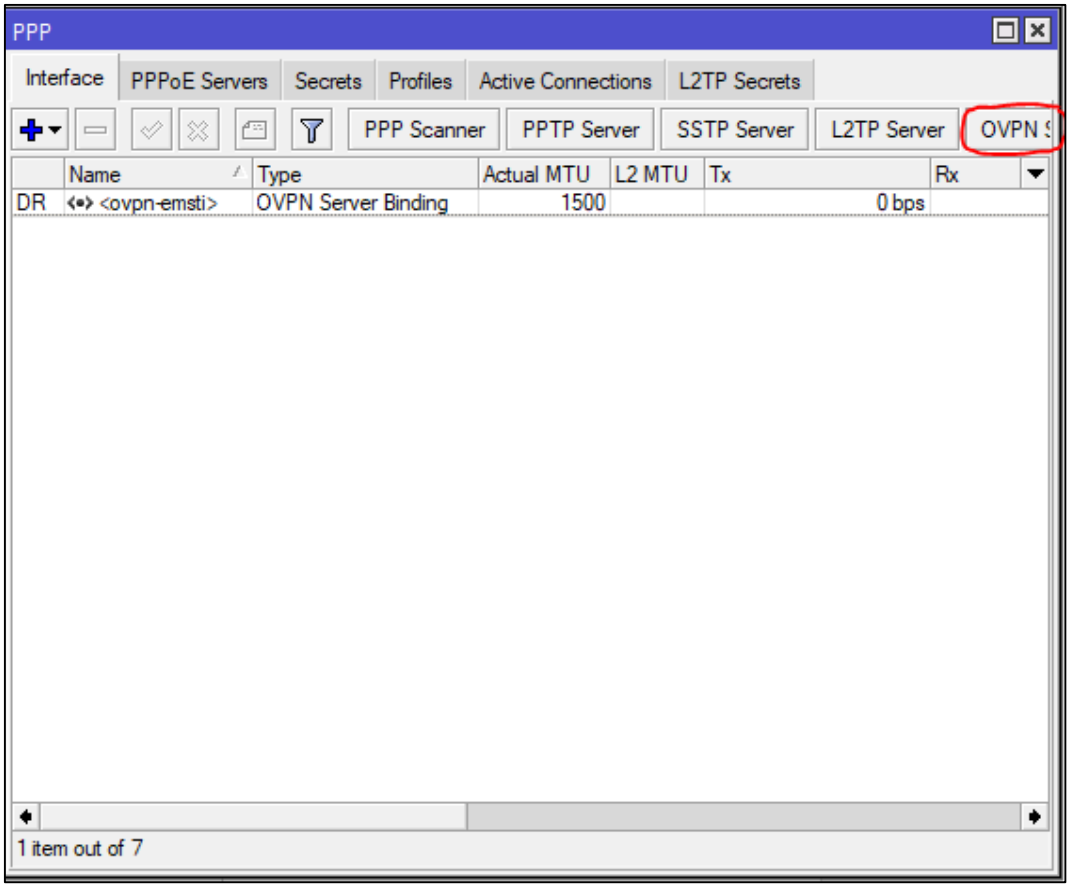


Fonte: Os autores

5.5.2.3 Servidor OpenVPN

Para habilitar o servidor, foi acessado o menu *PPP* e, na aba *Interface*, foi clicado o botão **OVPN Server**, ilustrado com destaque na Figura 74.

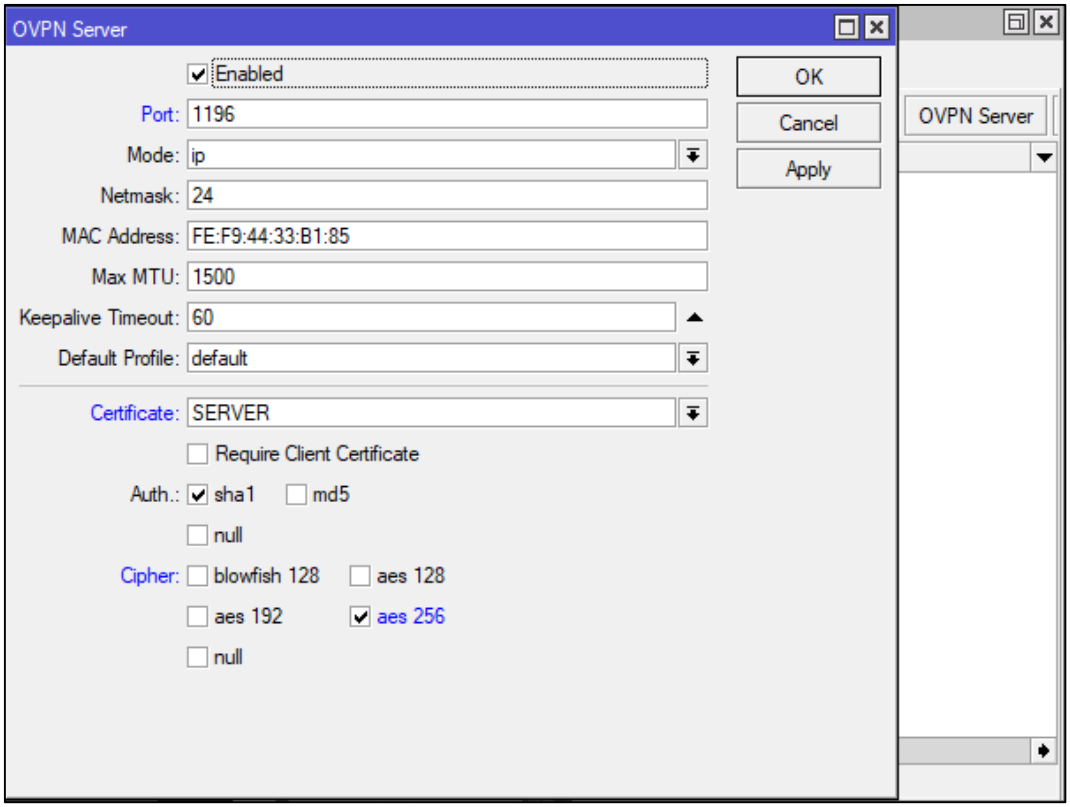
Figura 74. Serviços disponíveis em *PPP*



Fonte: Os autores

Em *OVPN Server*, foi marcada a caixa *Enabled* e alterada a porta padrão **1194** para **1196**. O certificado ***SERVER*** foi escolhido no campo *Certificate* e marcada a opção ***sha1*** em *Authentication*, juntamente com a cifra ***aes256***, em *Cipher*. As alterações foram salvas após um clique no botão *Apply* e no botão *OK*. A Figura 75 exibe o processo de habilitação do *OpenVPN Server*.

Figura 75. Habilitando o servidor *OpenVPN*

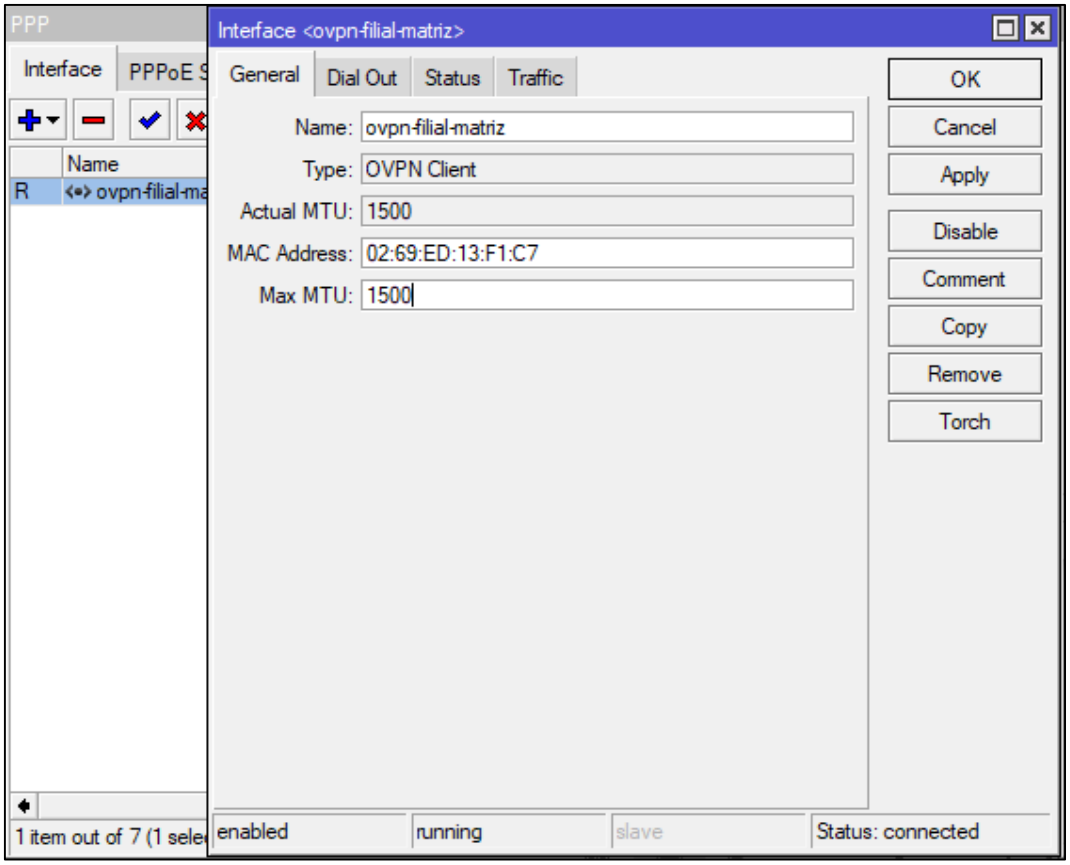


Fonte: Os autores

5.5.2.4 Interface OpenVPN Client

Agora, no *routerboard* da filial, foi configurado o túnel *VPN* que interliga os dois *routerboards*. Para esta tarefa, foi acessado o menu *PPP > Interface*, clicado no botão *Add (+)* e, em seguida, escolhida a opção ***OpenVPN Client*.** Em *New Interface*, a interface recebeu o nome ***ovpn-filial-matriz*** no campo *Name*. As alterações foram aplicadas com um clique no botão *Apply*. A Figura 76 ilustra o momento das configurações na guia *General*, em *New Interface*.

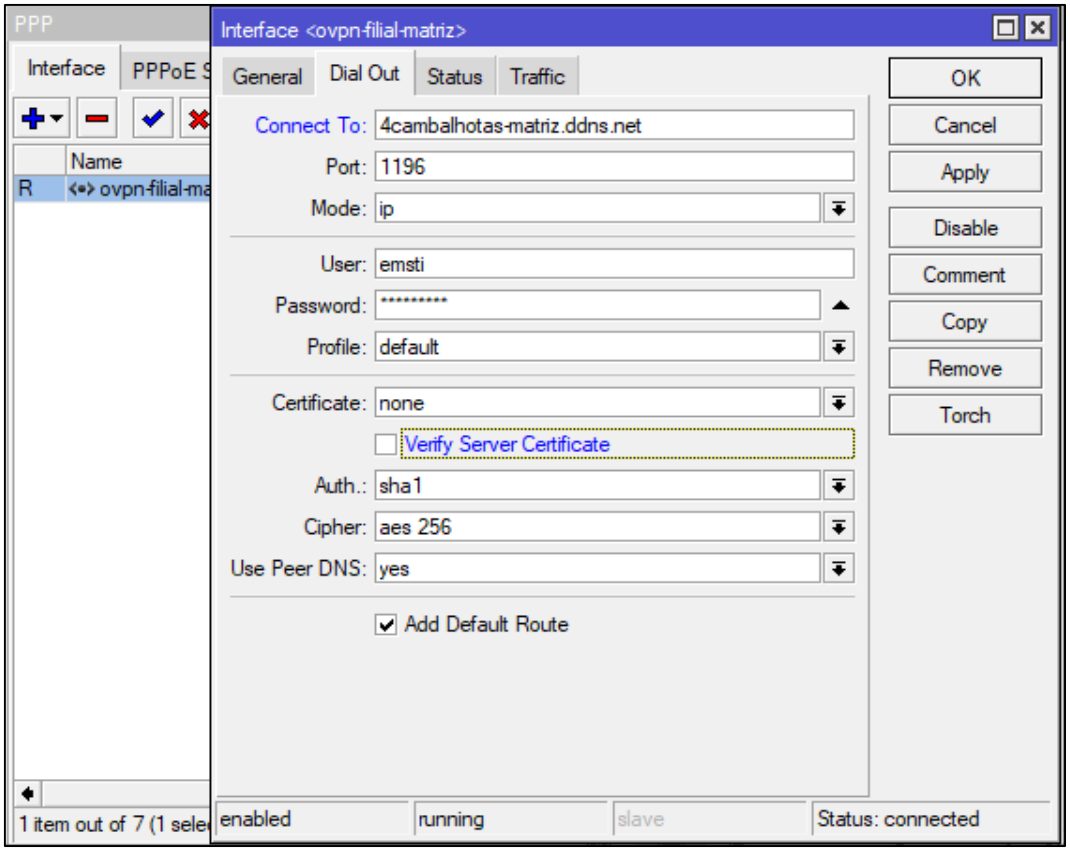
Figura 76. Interface *OpenVPN Client – General*



Fonte: Os autores

Alternado para a guia *Dial Out*, no campo *Connect To*, foi informado o endereço *DDNS* **4cambalhotas-matriz.net.br** e a porta **1196**, em *Port*. Informado o **usuário** e **senha** criados em *Secrets*, na seção 5.5.1.4, nos campos respectivos *User* e *Password*. Foram atribuídos os valores ***sha1***, ***aes266***, ***yes*** aos parâmetros *Auth*., *Cipher*, *Use Peer DNS* e, em *Add Default Route*, esta caixa foi marcada. As configurações foram salvas através dos botões *Apply* e *OK*. Essas alterações realizadas podem ser visualizadas na Figura 77.

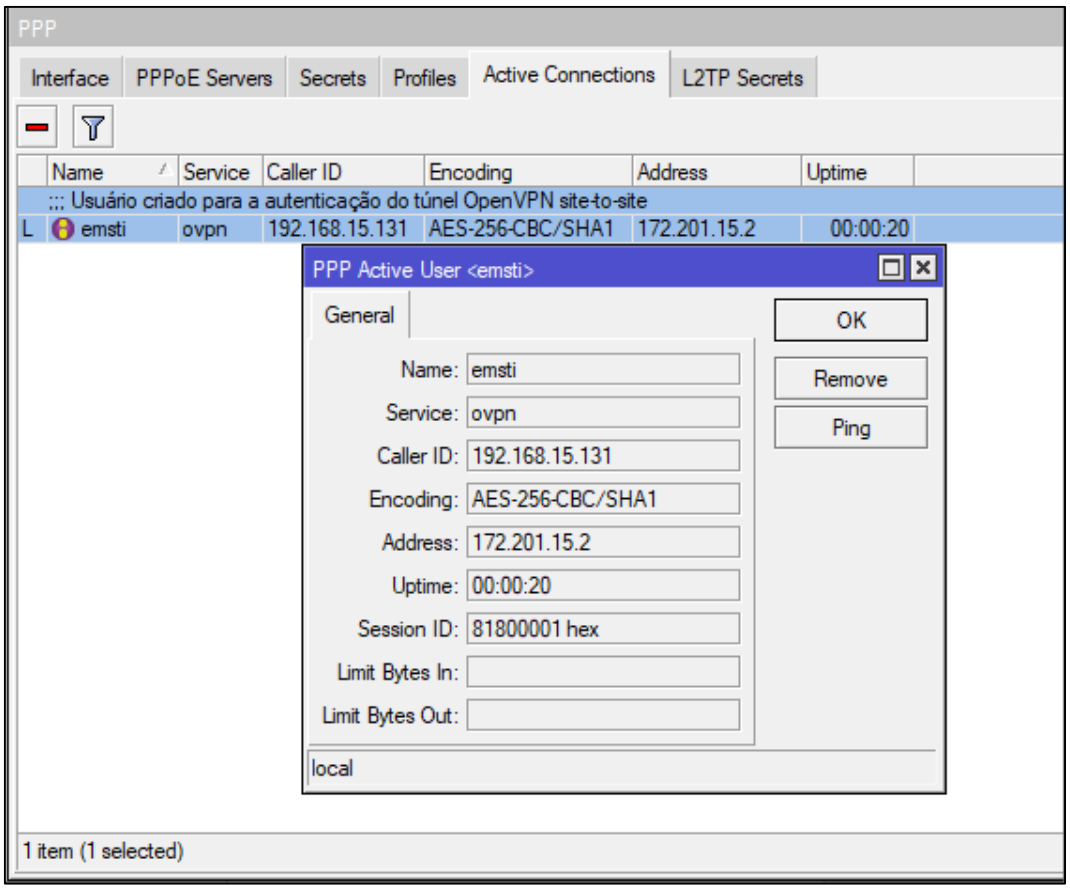
Figura 77. Interface *OpenVPN Client – Dial Out*



Fonte: Os autores

Retornado ao *routerboard* da matriz para conferir se a conexão foi estabelecida, foi acessado o menu *PPP > Active Connections*. Em *Active Connections*, foi possível visualizar uma sessão criada pelo usuário **emsti**. A Figura 78 evidencia a conexão firmada entre filial e matriz.

Figura 78. Conexão ativa do túnel filial-matriz



Fonte: Os autores

5.5.3 Aplicativo OpenVPN para acesso remoto

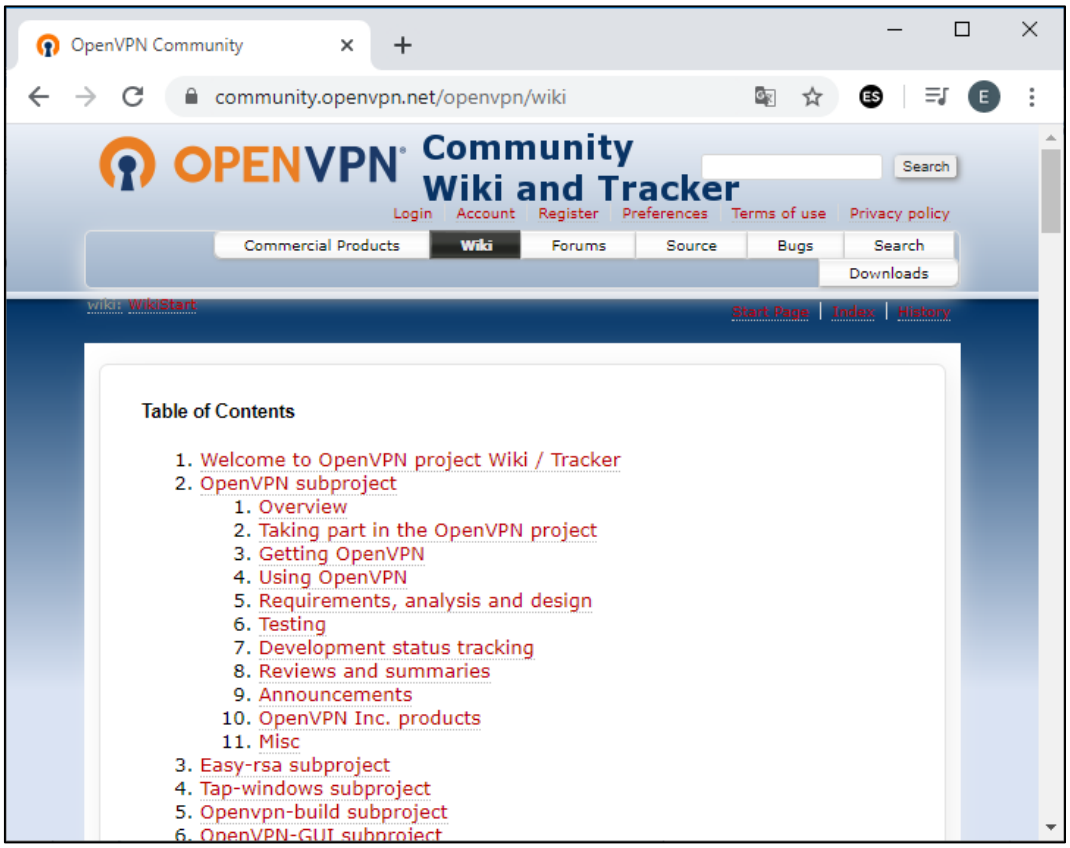
O aplicativo *OpenVPN* oferece, de maneira gráfica e bem intuitiva, a facilidade em prover uma conexão - virtual, privada e segura - entre o equipamento convidado até o equipamento hospedeiro do serviço de *VPN*, podendo este ser um roteador, *firewall* ou servidor.

Através dessa conexão, é possível acessar todos os recursos e serviços em rede compartilhados, à qual o usuário possui permissão, tais como arquivos, sistemas ou dispositivos em uma rede privada, podendo esta ser a do escritório ou empresa onde trabalha e até mesmo a de sua residência, caso possua tal necessidade.

O *OpenVPN* é gratuito e sem necessidade de uso de licença. Sua comunidade destaca-se pela organização, documentação e colaboratividade. É muito fácil

encontrar ajuda no *FAQ*[17], fóruns ou em sua *wiki*[18]. A Figura 79 ilustra a página da comunidade *OpenVPN*.

Figura 79. Página oficial da Comunidade *OpenVPN*



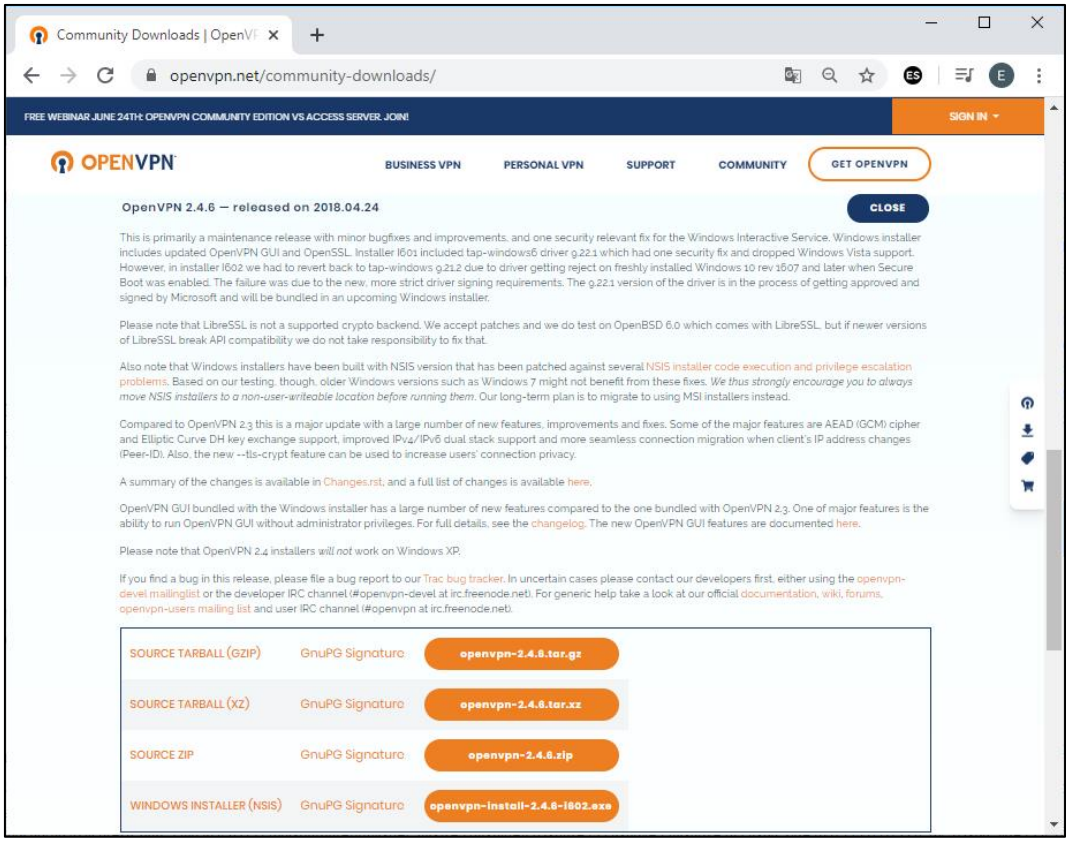
Fonte: Os autores

5.5.3.1 Download do programa

O aplicativo do *OpenVPN* está disponível em seu site oficial[19]. Foi navegado até a área de *downloads*[20] e baixada a **versão 2.4.6**. O arquivo foi salvo na pasta *Downloads*, padrão no Windows 10. A Figura 80 mostra os detalhes da **versão 2.4.6**.

[17] Sigla do termo em inglês *Frequently Asked Questions*. Em nosso idioma, as perguntas frequentes.
[18] O termo *wiki*, que foi baseado no termo havaiano *wiki-wiki*, que significa rápido, é utilizado para indicar uma coleção de muitas páginas interligadas, onde cada uma delas pode ser visitada e editada por qualquer pessoa, a partir de um navegador de internet, o que a torna bastante prática para atualização do conteúdo ou reedição da estrutura da página, de acordo com a vontade do usuário.
[19] Disponível na URL <https://openvpn.net/>.
[20] Disponível na URL <https://openvpn.net/client-connect-vpn-for-windows/>.

Figura 80. Área de downloads na página oficial do OpenVPN



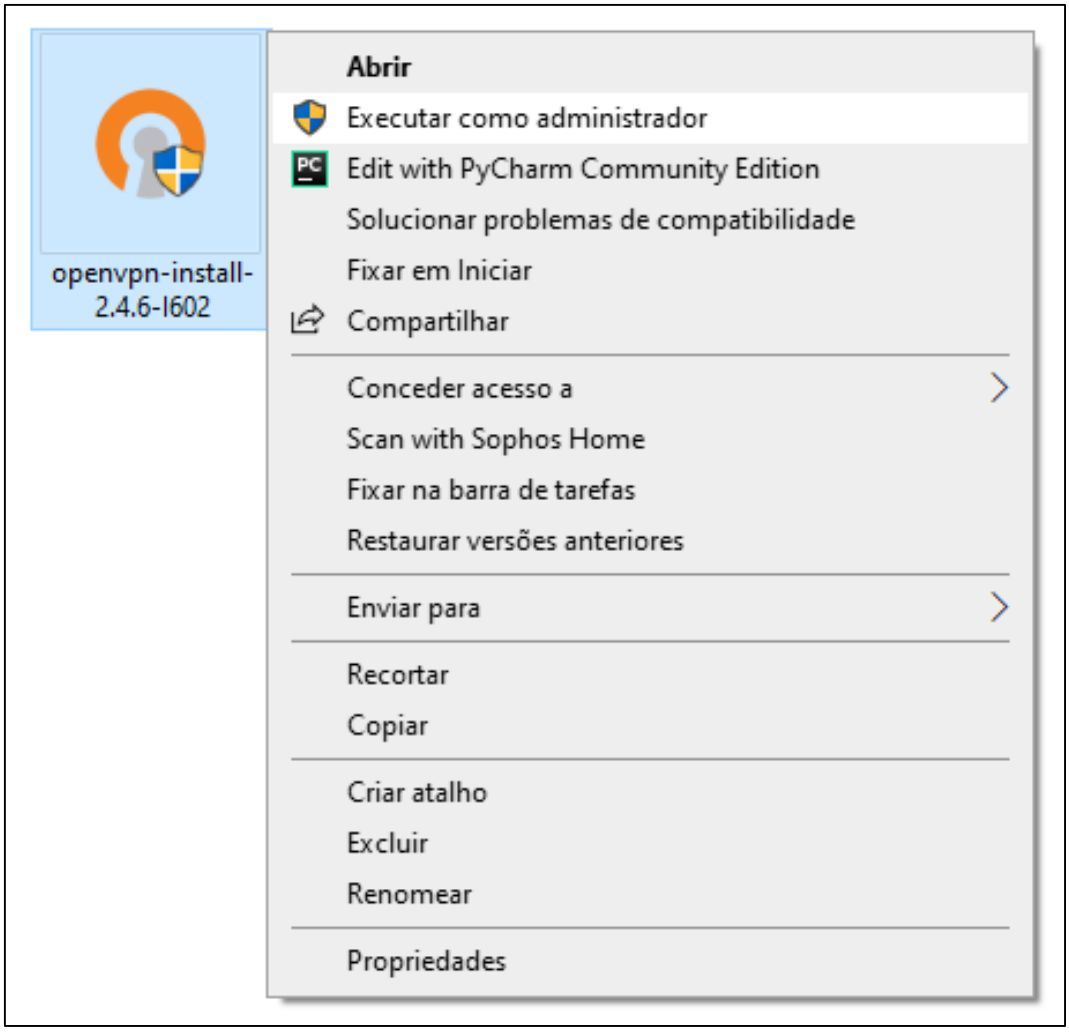
Fonte: Os autores

A instalação do aplicativo foi muito simples e tranquila. O passo-a-passo foi descrito na próxima sessão.

5.5.3.2 Instalação do programa

O arquivo ***openvpn-install-2.4.6-I602.exe*** foi executado em modo administrador no Windows 10, para garantir que todos os componentes fossem instalados sem impeditivos. Para isso, foi clicado com o botão direito sobre o ícone do arquivo e escolhida a opção **Executar como administrador**, conforme ilustrado na Figura 81.

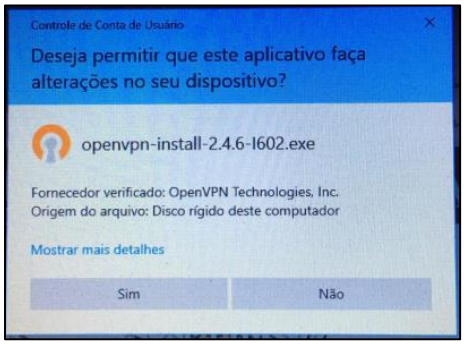
Figura 81. Execução de arquivo em modo administrador



Fonte: Os autores

Uma notificação do Windows 10, sobre a execução do arquivo em modo administrador, foi exibida. O botão *Sim* foi clicado para autorizar esta ação. A Figura 82 exibe a notificação gerada durante a instalação do aplicativo.

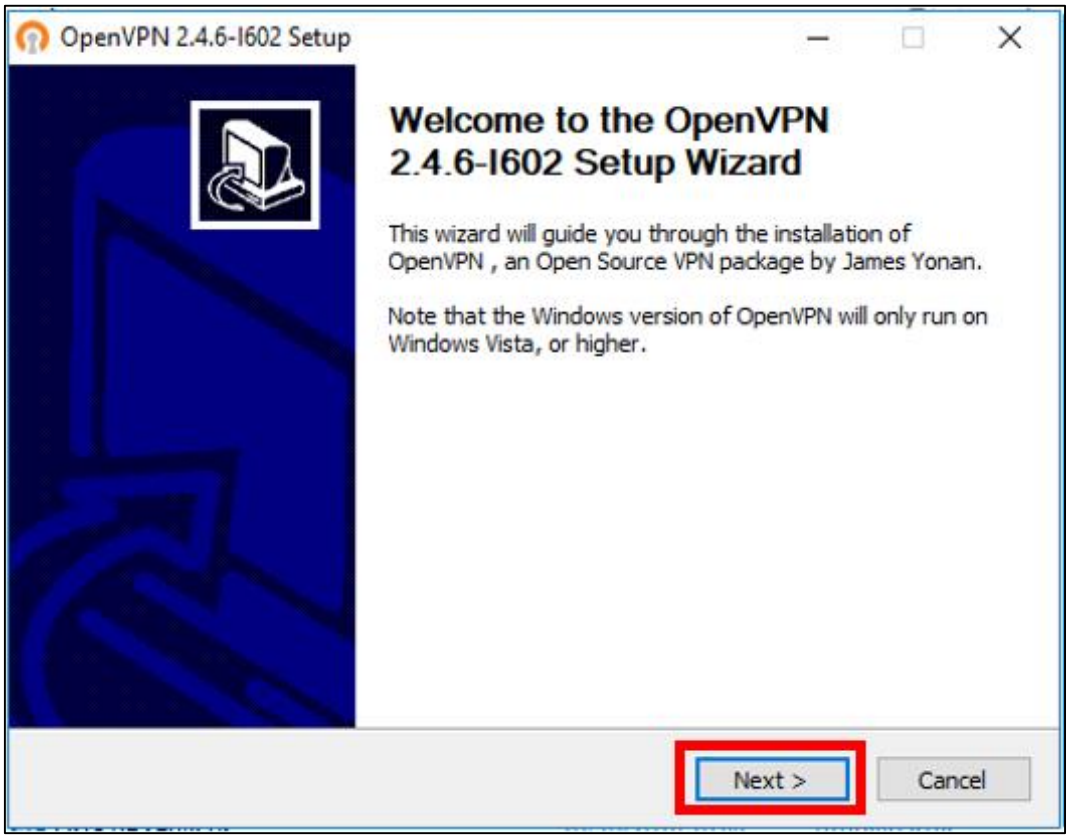
Figura 82. Controle de Conta de usuário



Fonte: Os autores

Após a autorização, o assistente de instalação do *OpenVPN* foi iniciado. Foi clicado no botão *Next* para prosseguir com a instalação, conforme exibe a Figura 83.

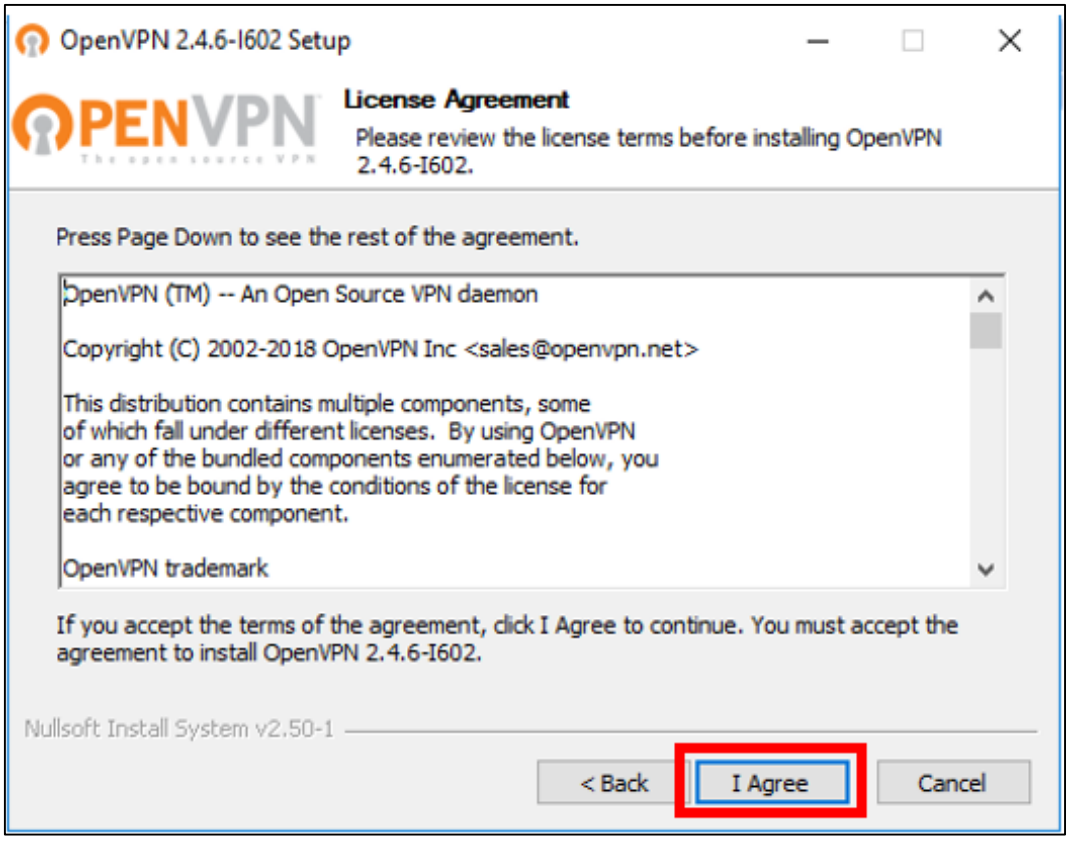
Figura 83. Instalação do *OpenVPN client* – Passo 01



Fonte: Os autores

A Figura 84 ilustra a tela do contrato de acordo de uso de licença. Para concordar com os termos do contrato, foi clicado no botão *I Agree* para prosseguir com a instalação.

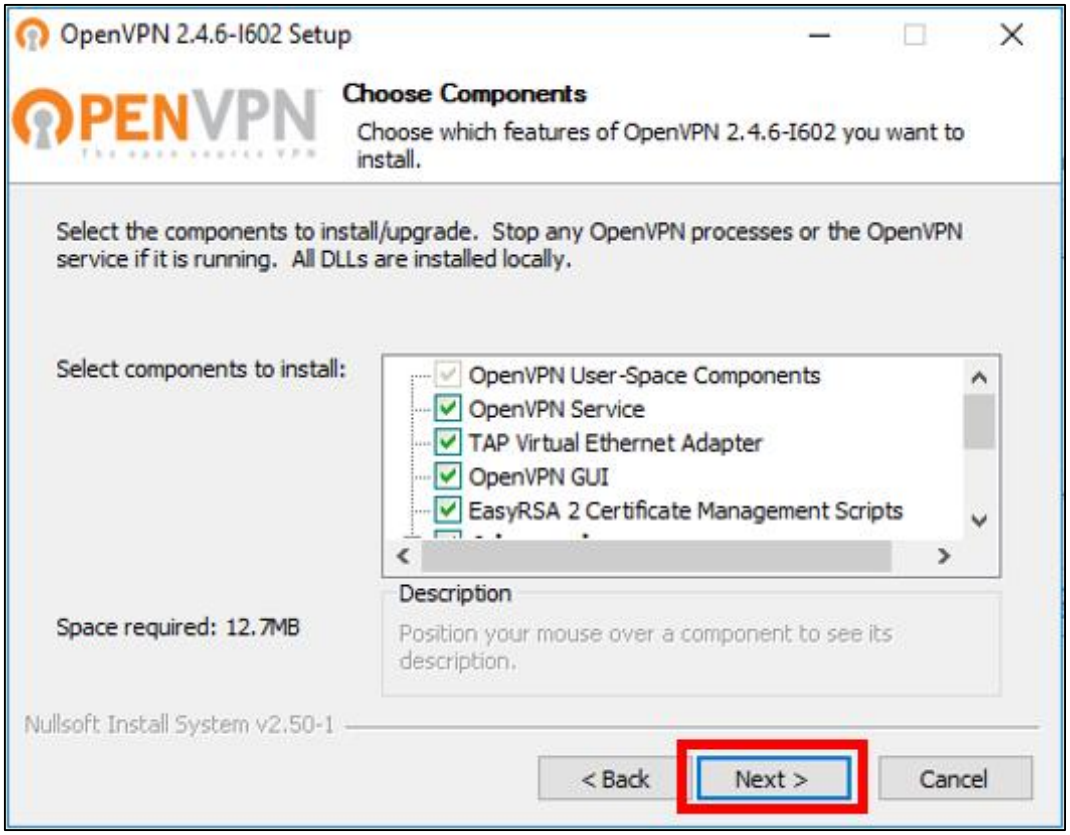
Figura 84. Instalação do *OpenVPN client* – Passo 02



Fonte: Os autores

Foram mantidas todas as opções marcadas, para que os componentes padrões fossem instalados. No entanto, é possível personalizar a instalação, porém, neste caso, não foi feito. A Figura 85 exibe esse momento da instalação.

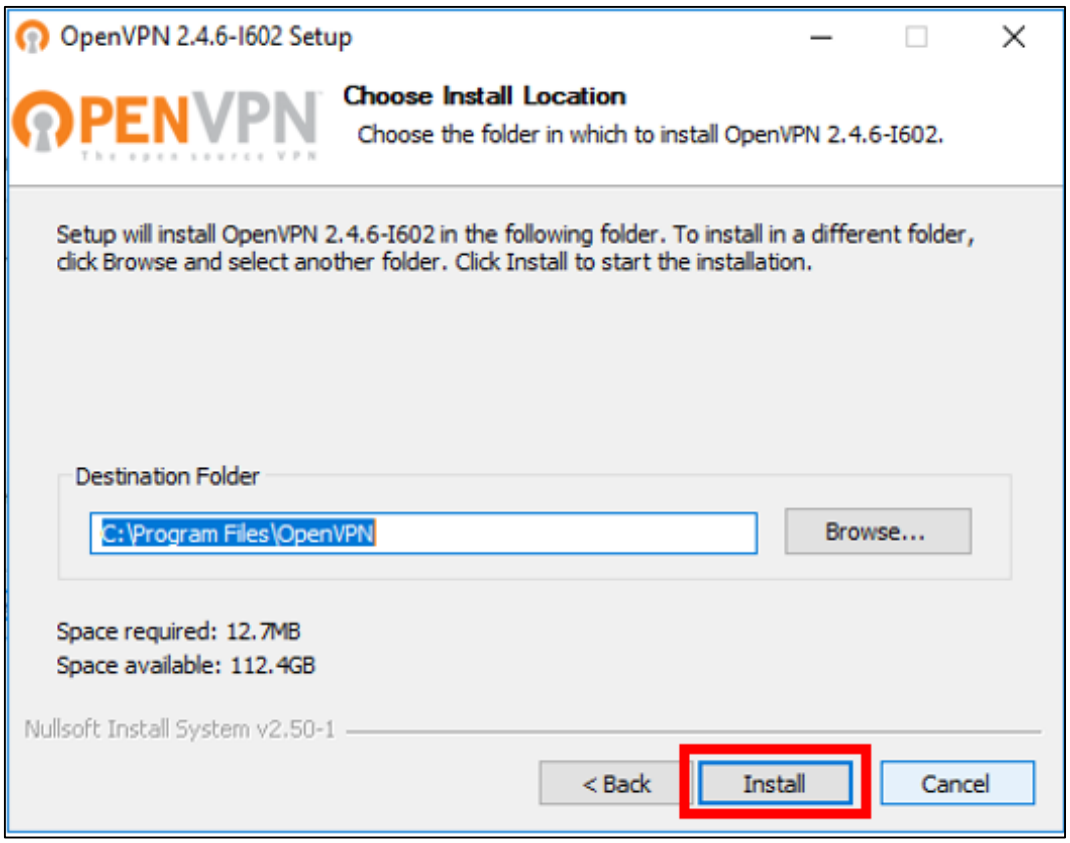
Figura 85. Instalação do *OpenVPN client* – Passo 03



Fonte: Os autores

Foi optado por deixar a instalação ser realizada em sua pasta de destino padrão ***C:\Arquivos de Programas\OpenVPN*** com o clique no botão *Install*. O aplicativo ocupa pouco espaço em disco. Seu tamanho pode ser observado na Figura 86.

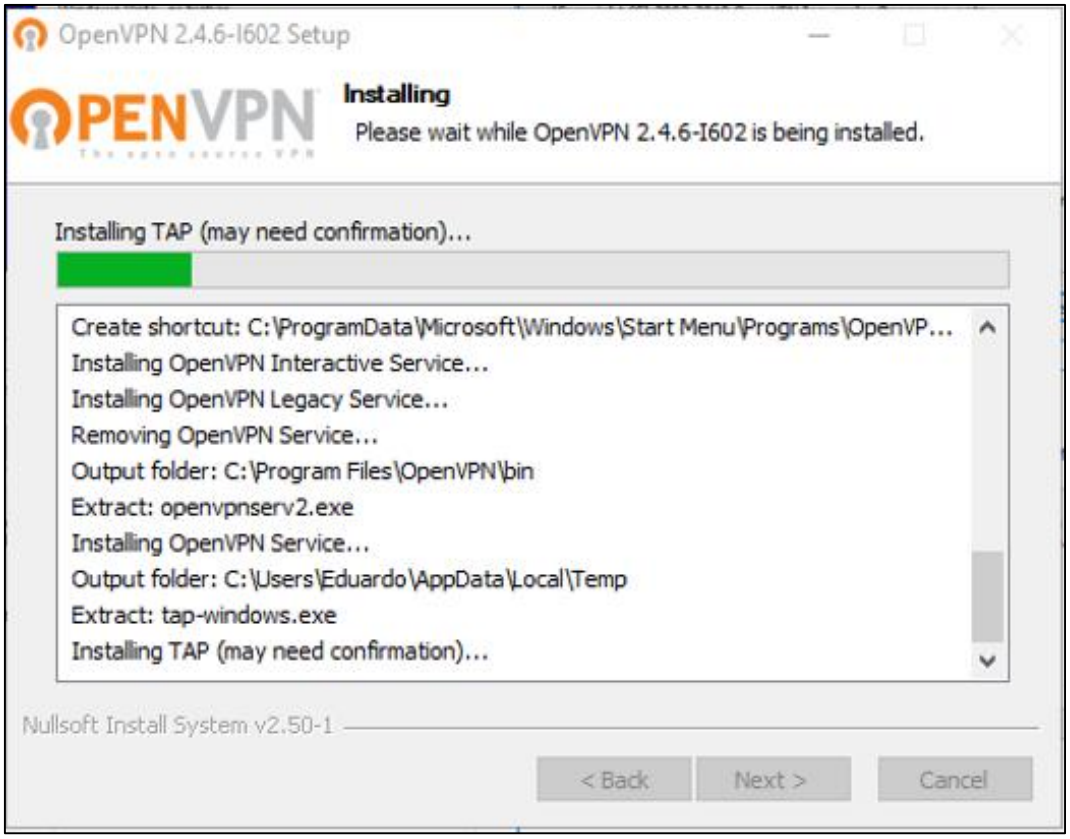
Figura 86. Instalação do *OpenVPN client* – Passo 04



Fonte: Os autores

O processo de instalação dos serviços e componentes foi aguardado até nossa próxima intervenção junto ao assistente. A Figura 87 ilustra o momento de instalação de cada item necessário para o funcionamento do *OpenVPN*.

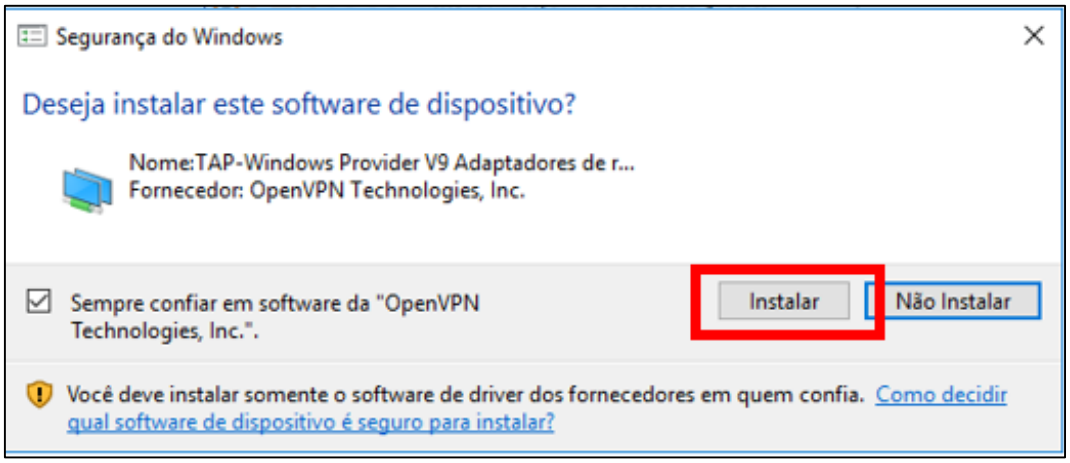
Figura 87. Instalação do *OpenVPN client* – Passo 05



Fonte: Os autores

O Windows 10 emitiu um novo alerta de segurança, conforme ilustrado na Figura 88, onde questionou se de acordo a instalação de *software* para dispositivo, no caso um adaptador de rede, que será o responsável pela criação do túnel *VPN*. Concordado com esta ação, quando clicado o botão *Install*.

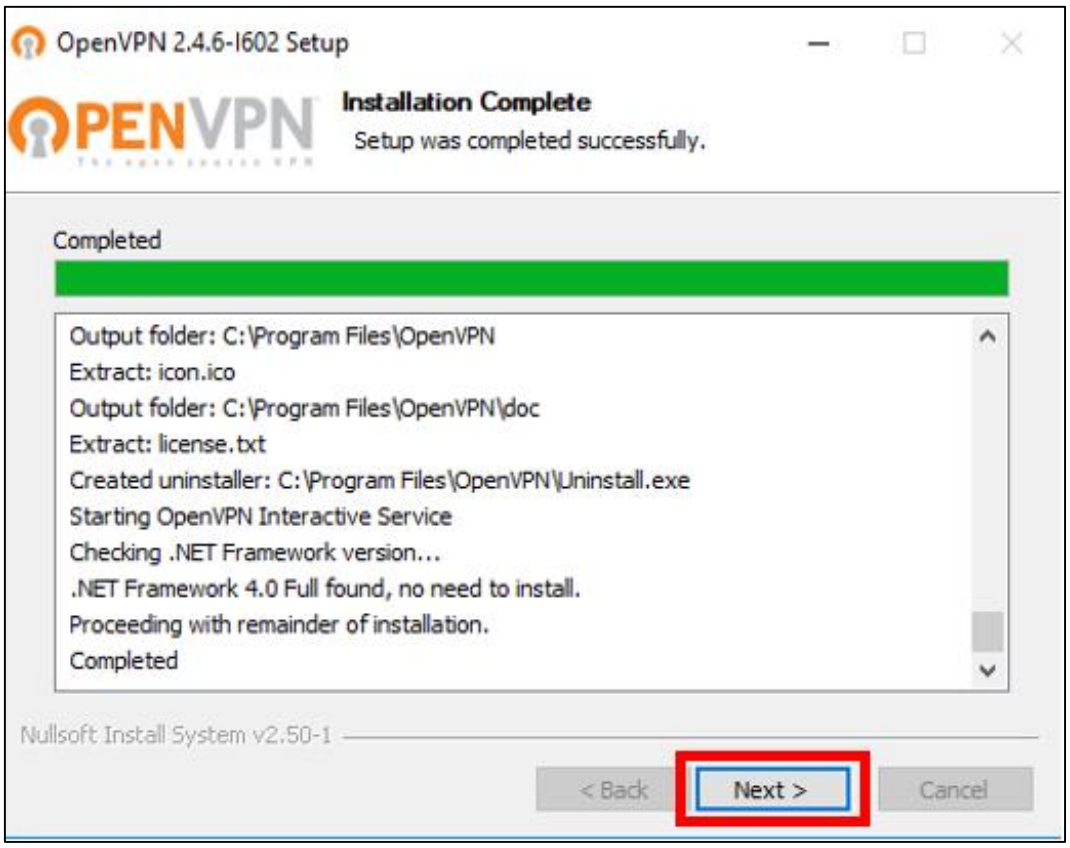
Figura 88. Instalação do *OpenVPN client* – Passo 06



Fonte: Os autores

Foi aguardado mais alguns instantes até a instalação terminar. O botão *Next* foi clicado para finalizar este processo. A Figura 89 exibe o status completo da instalação do aplicativo.

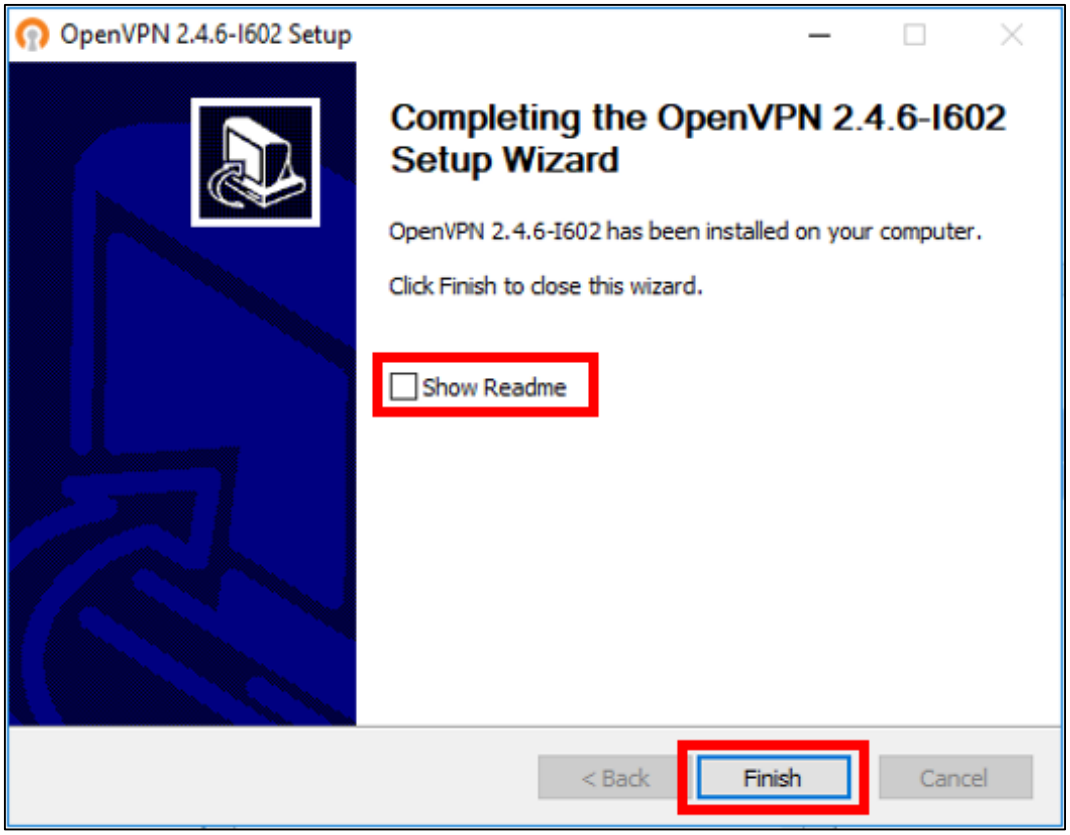
Figura 89. Instalação do *OpenVPN client* – Passo 07



Fonte: Os autores

A opção para abrir um arquivo de leitura, contendo informações sobre o *OpenVPN*, ao término da instalação pode ser desmarcado em *Show Readme*. Essa opção foi desmarcada e, para finalizar, o botão *Finish* foi utilizado. Essa último passo do assistente de instalação pode ser visualizado na Figura 90.

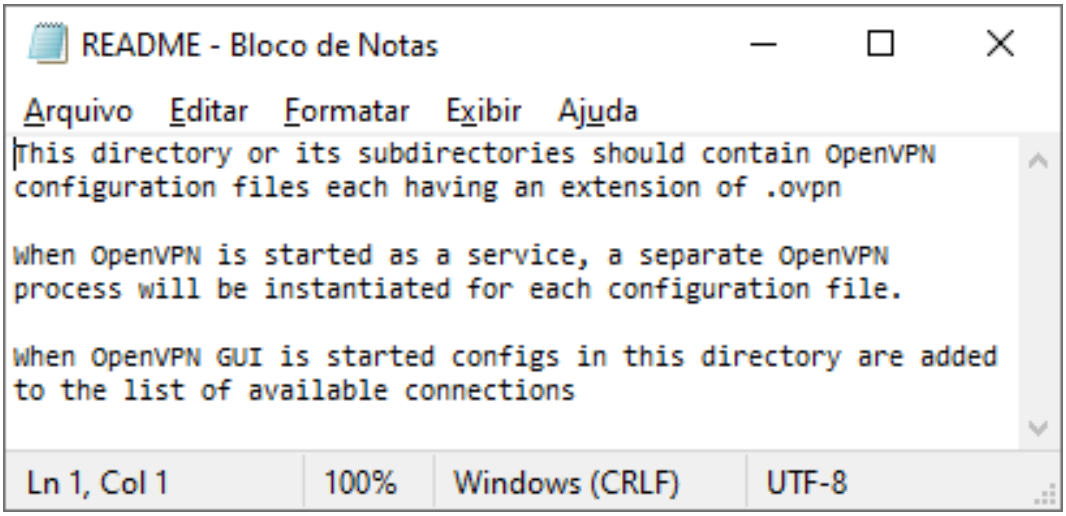
Figura 90. Instalação do *OpenVPN client* – Passo 08



Fonte: Os autores

A Figura 91 exibe o conteúdo do arquivo **README.txt**. Ele foi aberto a partir de seu diretório em ***C:\Program Files\OpenVPN\config***, minutos após o término da instalação do aplicativo *OpenVPN*.

Figura 91. Conteúdo do arquivo *README.txt*

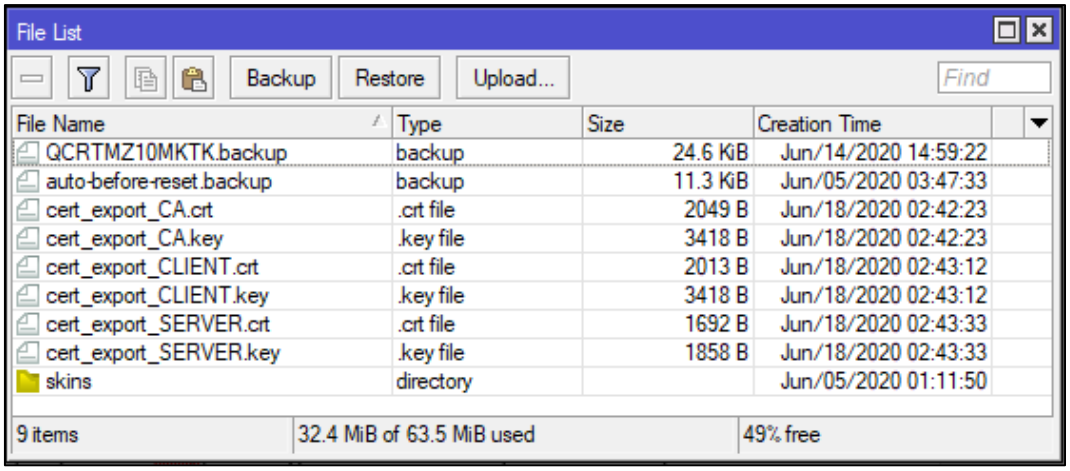


Fonte: Os autores

5.5.3.3 Cópia dos certificados do diretório padrão do routerboard

Os certificados criados na seção 5.5.1.5 e exportados na seção 5.5.2.2, foram utilizados nessa etapa da configuração. Após exportados, eles ficam armazenados no *RouterOS* no menu *Files* > *File List*. Sempre que é necessário trocar arquivos com o *routerboard* via *WinBox*, esse repositório é utilizado. Na Figura 92 este repositório pode ser visualizado. O menu *Files* fica localizado na barra vertical no *WinBox*.

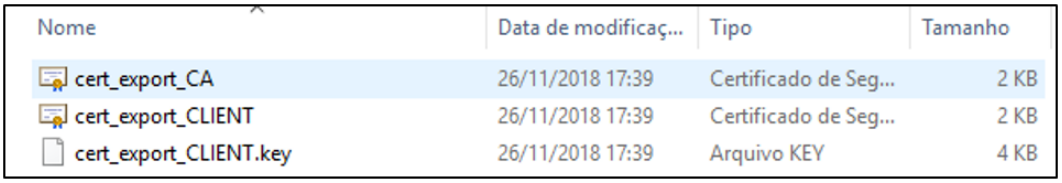
Figura 92. Diretório de arquivos do *routerboard* – *File List*



Fonte: Os autores

Foram copiados os arquivos **cert_export_CA.crt**, **cert_export_CLIENT.crt** e **cert_export_CLIENT.key** deste diretório *File List* para o nosso notebook, em uma pasta qualquer, em **Meus documentos**. A Figura 93 exibe os certificados e chave copiados para a pasta em Meus Documentos.

Figura 93. Lista de certificados copiados do *routerboard*



Fonte: Os autores

Dando continuidade ao processo de configuração, a pasta *Config*, no diretório da instalação do *OpenVPN,* foi acessada para a realização da cópia dos certificados

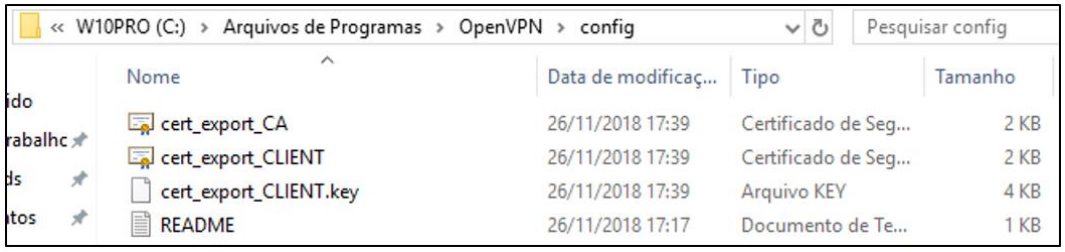
(arquivos *.crt) e a chave (arquivo *.key). A Figura 94 exibe que existe apenas um arquivo, o **README.txt**, antes de finalizada a cópia dos arquivos.

Figura 94. Local de instalação da pasta *Config*

Fonte: Os autores

Os arquivos necessários foram copiados para a pasta *Config*. É possível notar agora a quantidade de arquivos nesta pasta, através da ilustração na Figura 95.

Figura 95. Certificados adicionados na pasta *Config*

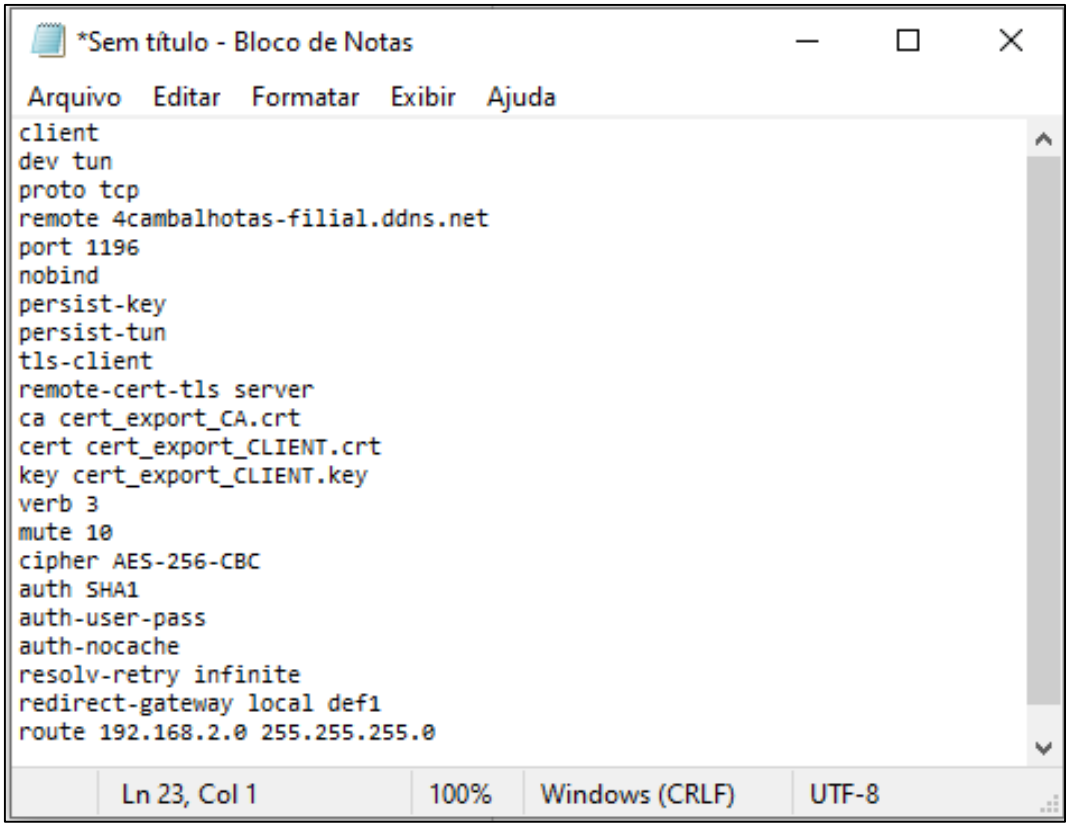


Fonte: Os autores

5.5.3.4 Configuração da conexão

Um arquivo com os parâmetros para a conexão é obrigatório. Com a ajuda de um arquivo modelo que possuímos em nosso repositório, foi criado um script dentro do **Bloco de Notas**, no Windows 10, e foram alteradas apenas as informações correspondentes, com base na Tabela 1, em suas respectivas linhas. A Figura 96 exibe o conteúdo deste arquivo-modelo, utilizado na criação do arquivo de conexão.

Figura 96. Arquivo modelo para configuração da conexão *OpenVPN*



Fonte: Os autores

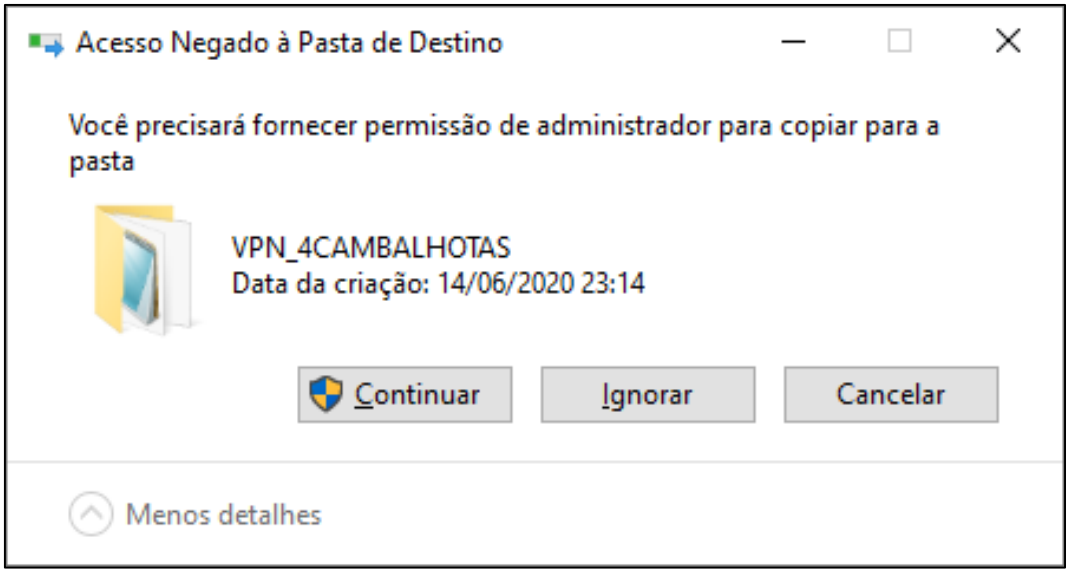
Preenchido o script com as devidas informações, o arquivo com o nome **4CAMBALHOTAS.ovpn** foi salvo na **Área de Trabalho** do Windows 10. A extensão ***.ovpn*** foi automaticamente associada ao aplicativo *OpenVPN*. A Figura 97 exibe o ícone do arquivo de conexão que foi criado.

Figura 97. Arquivo de conexão *OpenVPN*

Fonte: Os autores

Esse arquivo foi copiado para a pasta ***Config***, em ***C:\Program Files\OpenVPN\config*.** Um alerta de permissão de acesso foi exibido. Essa cópia foi autorizada ao clicar no botão Continuar, conforme ilustrado na Figura 98**.**

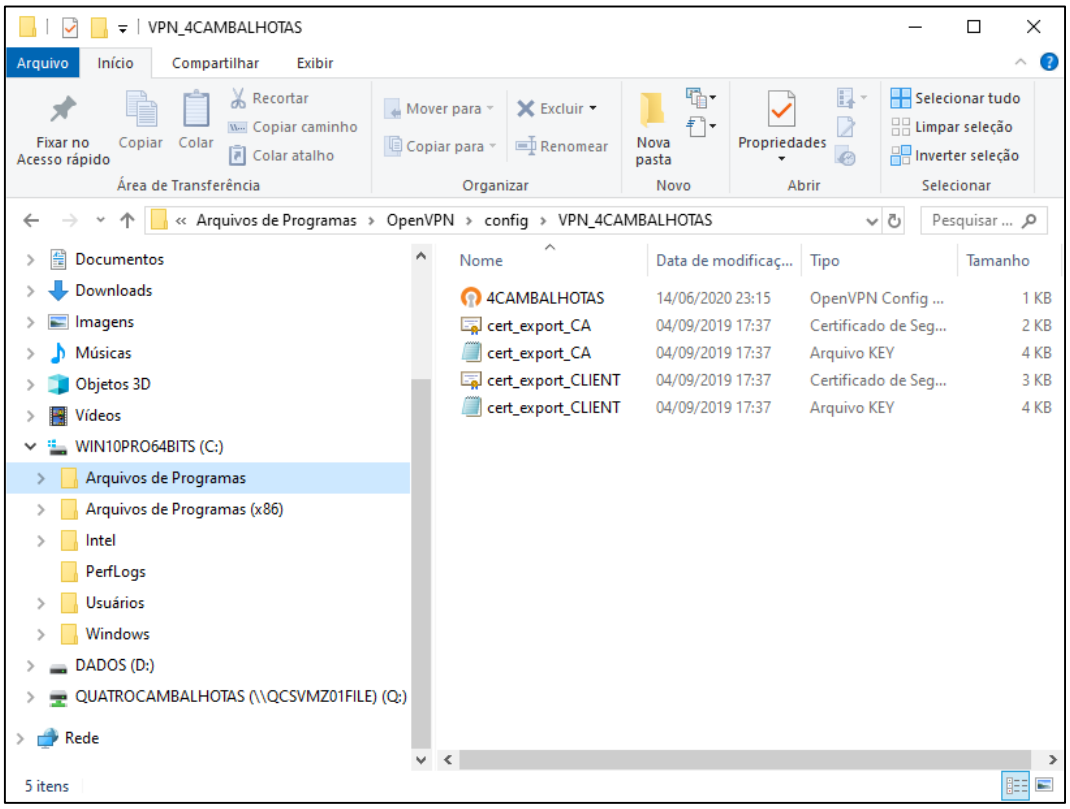
Figura 98. Aviso de permissão de acesso à pasta *Config*



Fonte: Os autores

A Figura 99 exibe como ficou o diretório ***Config*** após a adição do arquivo de configuração **4CAMBALHOTAS.ovpn**. A partir desta etapa da configuração, foi possível dar início aos testes de conexão.

Figura 99. Diretório de configuração do *OpenVPN*



Fonte: Os autores

5.5.3.5 Teste de conexão OpenVPN

Um teste para validar o funcionamento da *VPN client-to-site*, entre o notebook do cliente, desta vez fora de sua rede corporativa, para o site da matriz, de modo a acessar os dados no servidor de arquivos, foi realizado. Para conectar, o aplicativo *OpenVPN GUI* foi executado a partir do atalho disponibilizado na **Área de trabalho** (*Desktop*). A Figura 100 ilustra o atalho que foi criado após a instalação do aplicativo.

Figura 100. Atalho do aplicativo *OpenVPN*

Fonte: Os autores

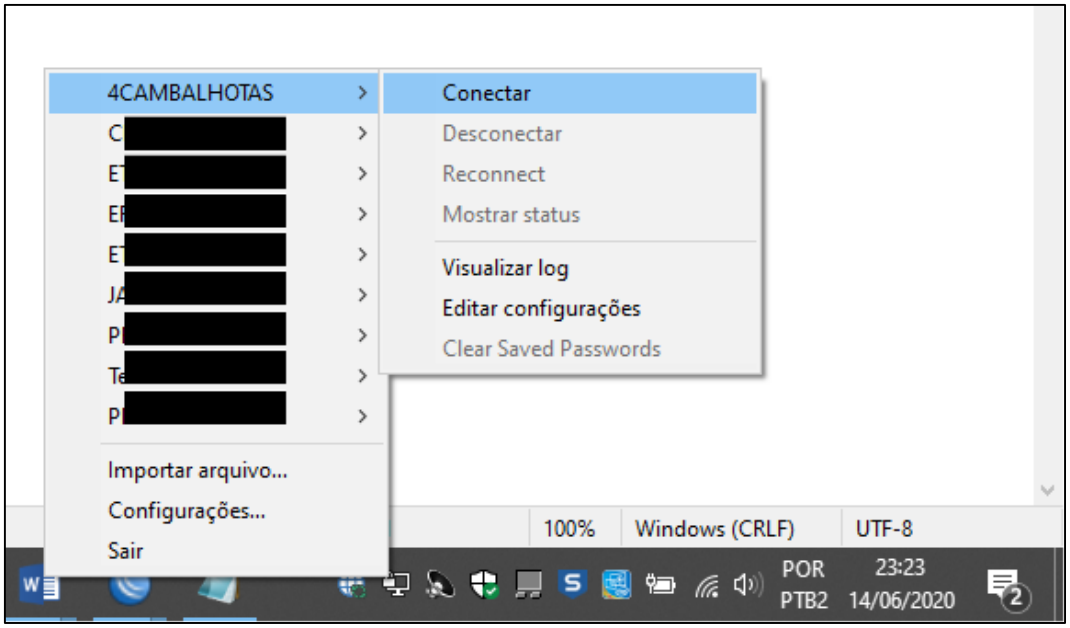
Logo após executado, o *OpenVPN* disponibilizou um ícone na área de notificação (bandeja) do Windows 10. A Figura 101 ilustra o ícone nesta bandeja.

Figura 101. Ícone *OpenVPN* na área de notificação

Fonte: Os autores

Clicado com o botão direito do mouse sobre o ícone para abrir seu menu de opções, foi escolhida a conexão **4CAMBALHOTAS**, definida anteriormente, e clicado em Conectar. Esse processo foi evidenciado e pode ser visualizado na Figura 102.

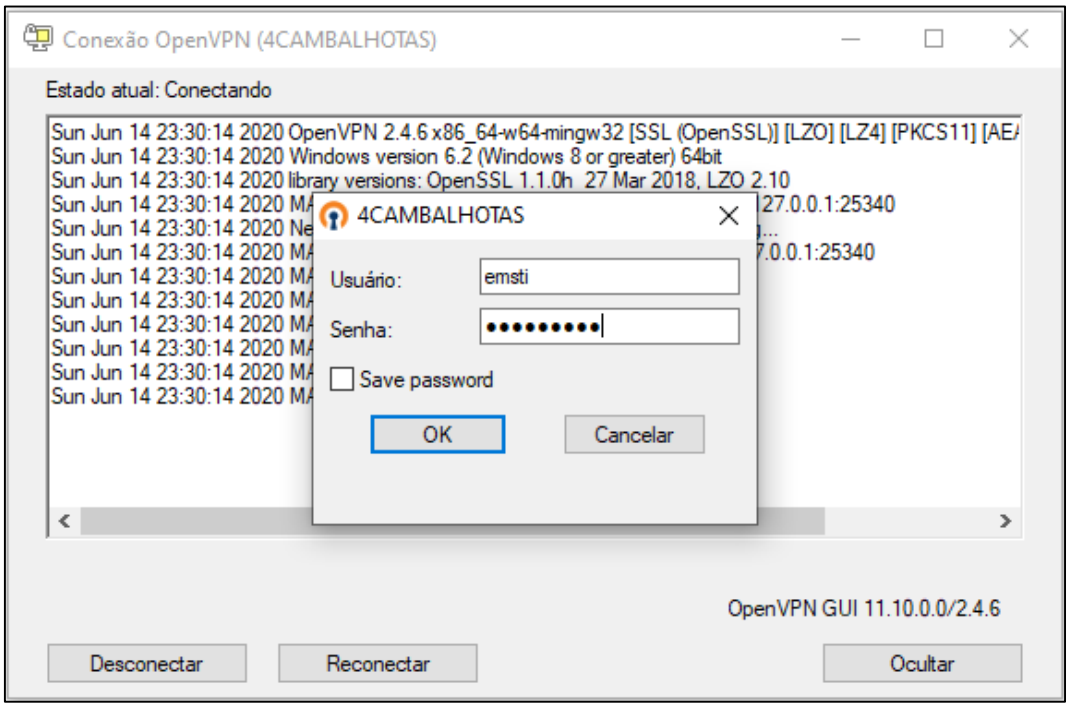
Figura 102. Método de conexão do *OpenVPN*



Fonte: Os autores

A credencial para a conexão foi solicitada. Mediante isto, foi informado nosso **usuário** e **senha** e clicado no botão *OK*. Uma nova solicitação de senha foi requerida e, após inserida, foi clicado novamente em *OK*. A Figura 103 exibe esse processo.

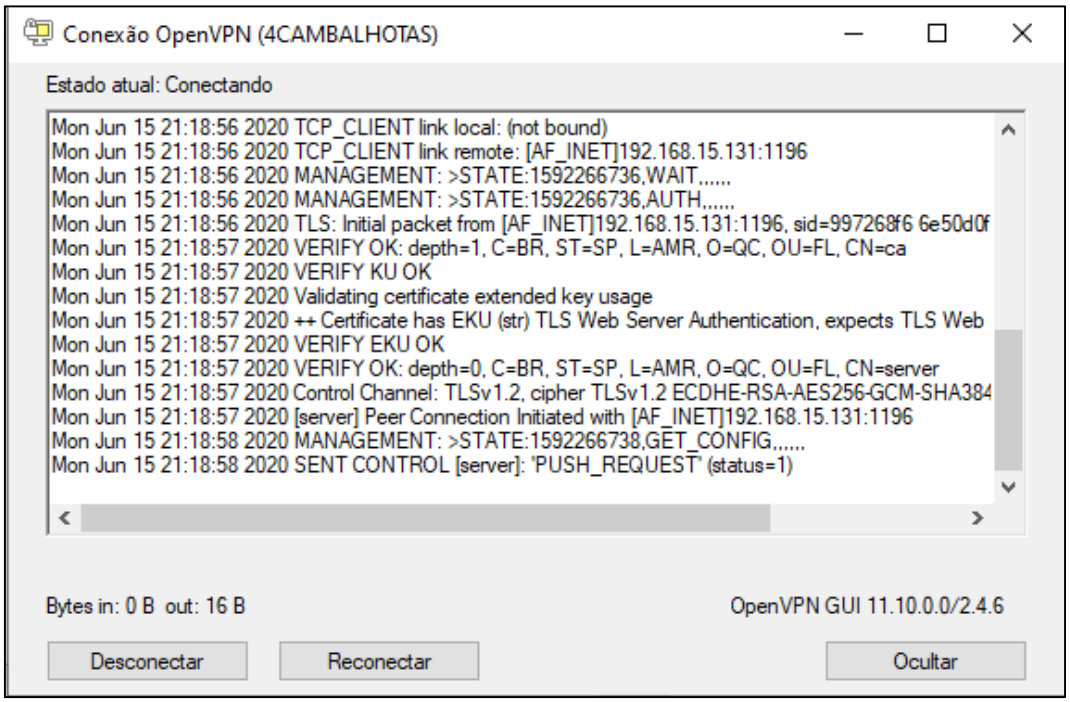
Figura 103. Janela de autenticação do *OpenVPN*



Fonte: Os autores

O processo de conexão levou apenas alguns segundos. A Figura 104 ilustra o processo realizado para prover a conexão.

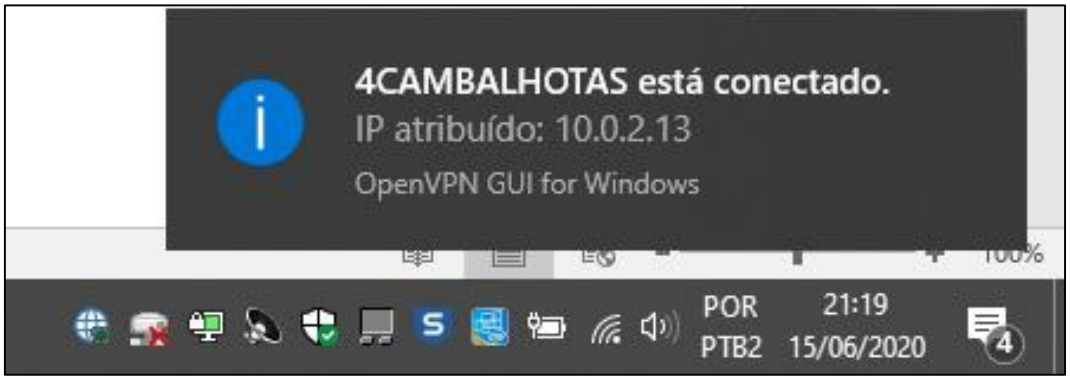
Figura 104. Progresso da conexão *OpenVPN*



Fonte: Os autores

Com a conexão estabelecida, a cor do ícone na bandeja do Windows 10 mudou para o **verde**. Logo em seguida, um aviso foi exibido, informando que o acesso foi concedido e que um IP **10.0.2.13** para essa sessão foi atribuído na interface de rede virtual do notebook do cliente, como mostra a Figura 105.

Figura 105. Resultado da conexão *OpenVPN*



Fonte: Os autores

O ícone na bandeja pode apresentar três cores: O **cinza** indica que não existe conexão, o **amarelo** indica que a conexão está em andamento ou em processo de reconexão e o **verde** indica que a conexão foi concedida. A Figura 106 ilustra o status da conexão.

Figura 106. Status de conexão *OpenVPN*

Fonte: Os autores

6 Resultados

Conforme planejado, foram realizados alguns testes de conectividade para evidenciar os resultados alcançados. Para esses testes, foi utilizada a ferramenta de ***prompt* de comando**, de codinome *CMD*[21], onde o comando *ping*[22] foi empregado.

A Tabela 9, logo abaixo, possui o inventário atualizado de equipamentos da Quatro Cambalhotas. Foi com base nesta tabela que foram realizados os testes, escolhendo alguns equipamentos mais relevantes para evidenciar os resultados.

Tabela 9. Inventário atualizado dos equipamentos da QC

INVENTÁRIO - HOST x IP					
HOSTNAME	**TIPO**	**LOCAL**	**IDENTIFICAÇÃO**	**FUNÇÃO**	**IP**
QCSVMZ01FILE	Servidor	Matriz	01	Servidor de arquivos	192.168.1.5
QCNBMZ02DSGR	Notebook	Matriz	02	Designer	DHCP
QCNBFL03SFTS	Notebook	Filial	03	Atendimento	DHCP
QCPRMZ04DSGR	Printer	Matriz	04	Impressora laser	192.168.1.4
QCPRFL05ATTO	Printer	Filial	05	Atendimento	192.168.2.4
QCPTMZ06DSGR	Plotter	Matriz	06	Plotter de recorte	192.168.1.6
QCPTMZ07DSGR	Plotter	Matriz	07	Plotter de recorte	192.168.1.7
QCPTMZ08DSGR	Plotter	Matriz	08	Plotter de recorte	192.168.1.8
QCRTMZ09TPLK	Roteador	Matriz	09	Wifi da recepção	192.168.1.9
QCRTMZ10MKTK	Roteador	Matriz	10	Routerboard Mikrotik	192.168.1.10
QCRBFL11MKTK	Roteador	Filial	11	Routerboard Mikrotik	192.168.2.10
QCRTFL12TPLK	Roteador	Filial	12	Wifi da recepção	192.168.2.9
QCDRFL13CFTV	DVR	Filial	13	CFTV Salão Festas	192.168.2.3

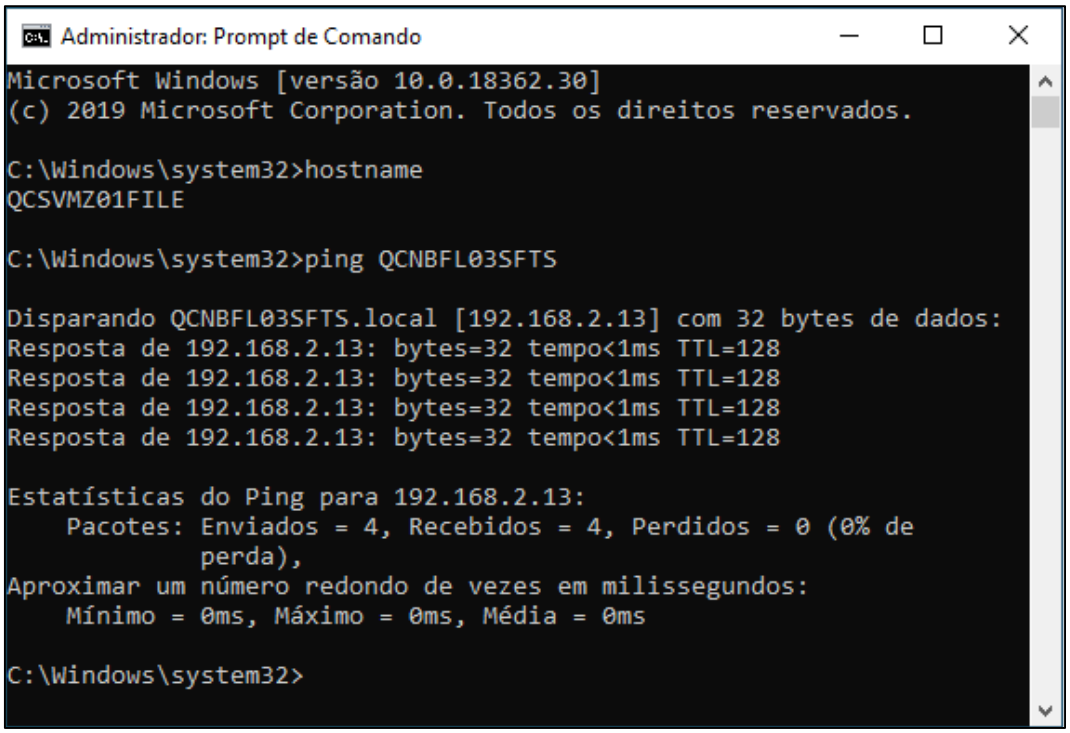
Fonte: Os autores

[21] Sigla abreviada do termo em inglês *Command* - *CMD*. É um interpretador de linha de comando no OS/2 e de sistemas baseados no Windows NT (incluindo Windows 2000, XP, Server 2003 e adiante até o mais recente Windows 10).
[22] *Ping* é um comando usado para medir o tempo de resposta da conexão do seu computador com outros dispositivos na rede local ou na internet. Este comando envia pequenos pacotes de dados para sites ou endereços de IP e calcula em quantos milissegundos (ms) o alvo demora para responder.

Para o teste, foi disparado do notebook conectado na rede local da filial, um *ping* para o servidor de arquivos, conectado na rede local da matriz, o qual retornou êxito na recepção dos pacotes.

A Figura 107 ilustra o *ping* do servidor da matriz para o notebook alvo da filial.

Figura 107. Teste *Ping* entre servidor de arquivos e notebook da filial

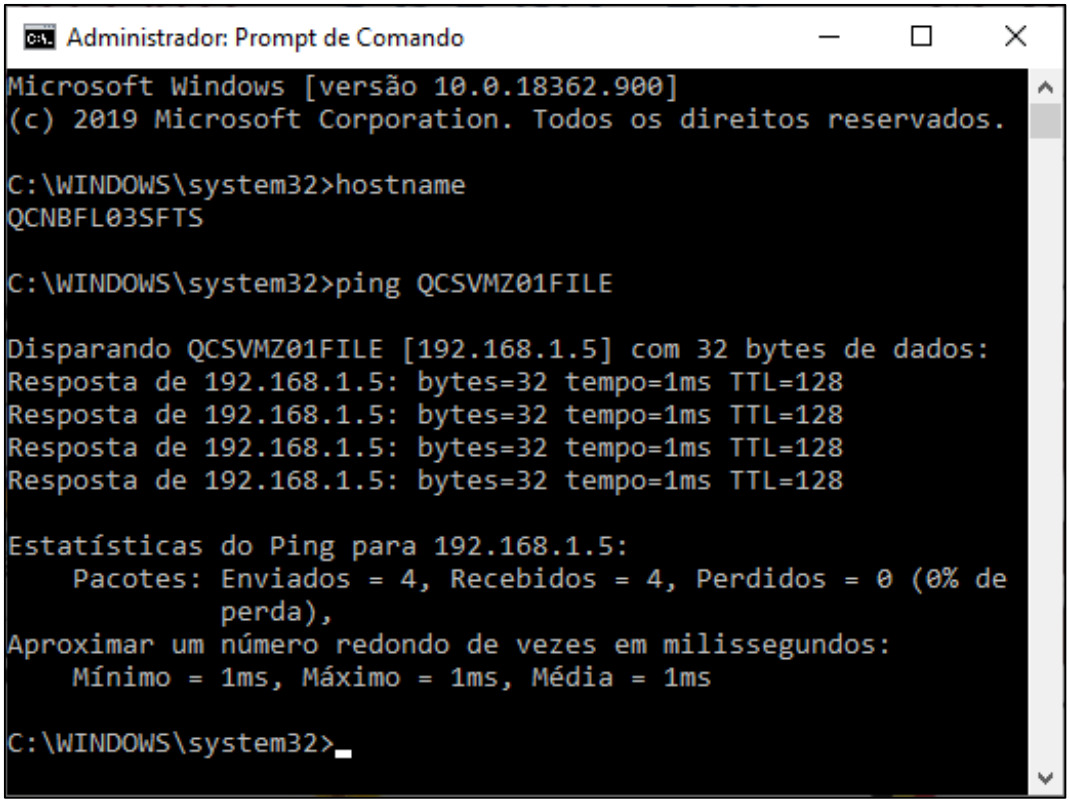


Fonte: Os autores

O mesmo teste foi feito para o caminho reverso, do notebook conectado na rede local da matriz foi disparado um *ping* para o notebook conectado na rede local da filial, o qual este também retornou sucesso na recepção dos pacotes.

A Figura 108 ilustra o *ping* do notebook da filial para o servidor alvo da matriz.

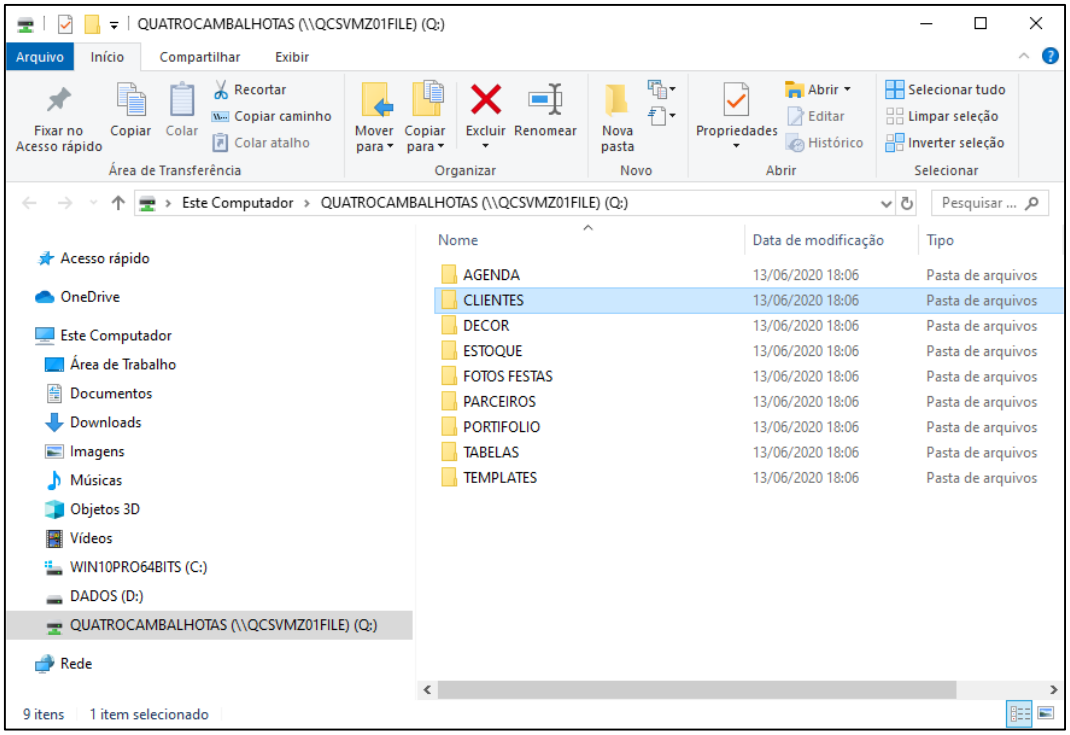
Figura 108. Teste *Ping* entre notebook da filial e servidor de arquivos



Fonte: Os autores

Com a comunicação entre os locais estabelecida pela *VPN*, foi possível mapear, no notebook de atendimento no salão de festas, o compartilhamento do servidor de arquivos, localizado na matriz. A Figura 109 evidencia o mapeamento que foi configurado no notebook.

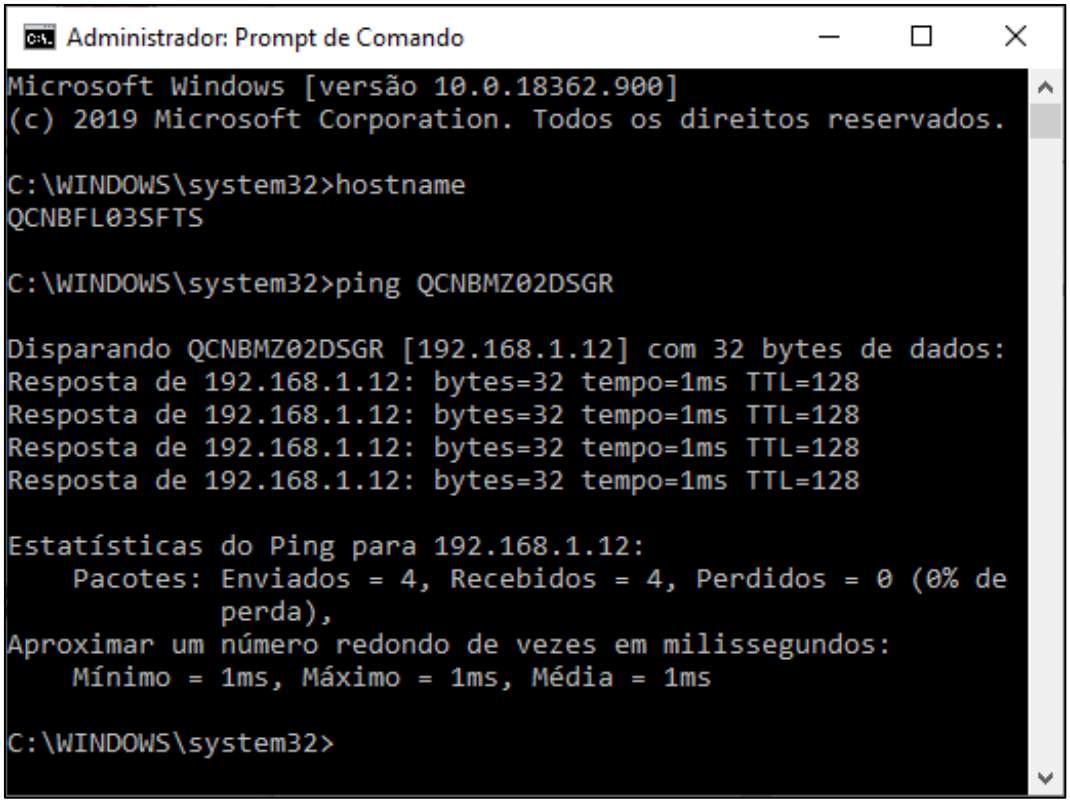
Figura 109. Mapeamento do diretório compartilhado no servidor



Fonte: Os autores

Um teste *ping* entre o notebook conectado na rede local da filial e o notebook conectado na rede local da matriz foi realizado. O resultado foi ilustrado na Figura 110.

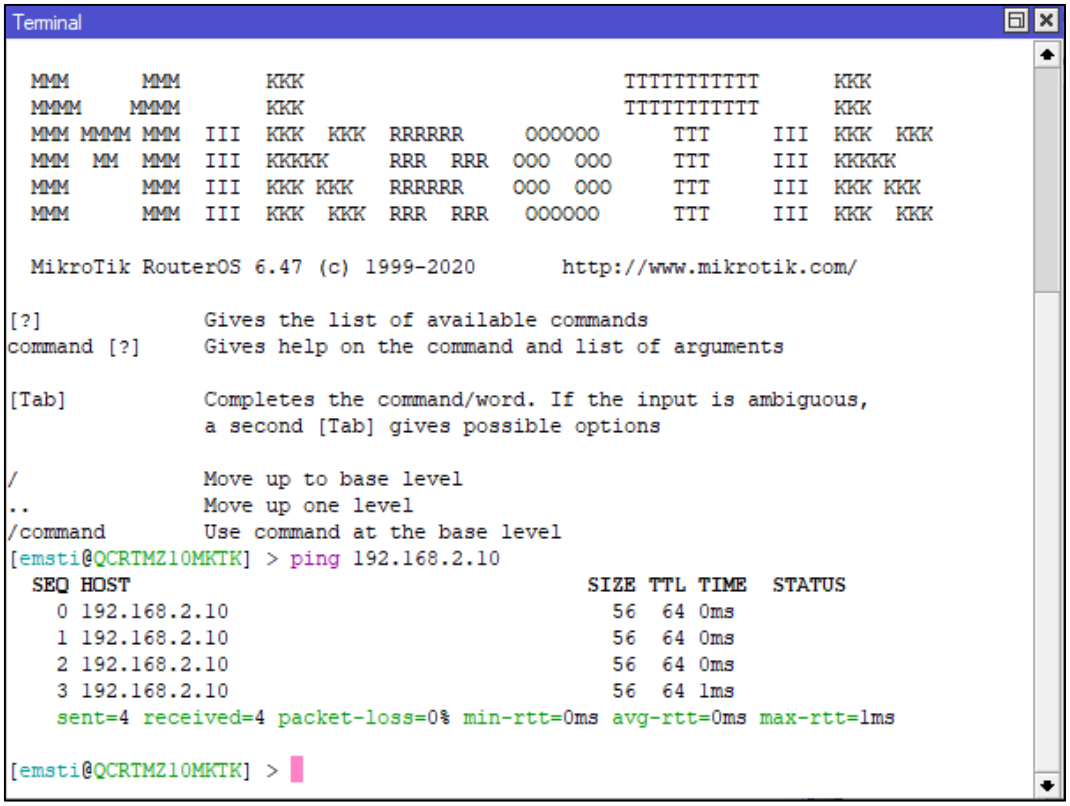
Figura 110. Teste *Ping* entre notebook da filial e notebook da matriz



Fonte: Os autores

Para validar a comunicação entre os *routerboards*, foi realizado um teste de *ping* via *New Terminal*, através do *WinBox*. A Figura 111 exibe o comando *ping* da console do *routerboard* da matriz para o endereço IP **192.168.2.10** da *bridge* da rede local (*LAN*) da filial.

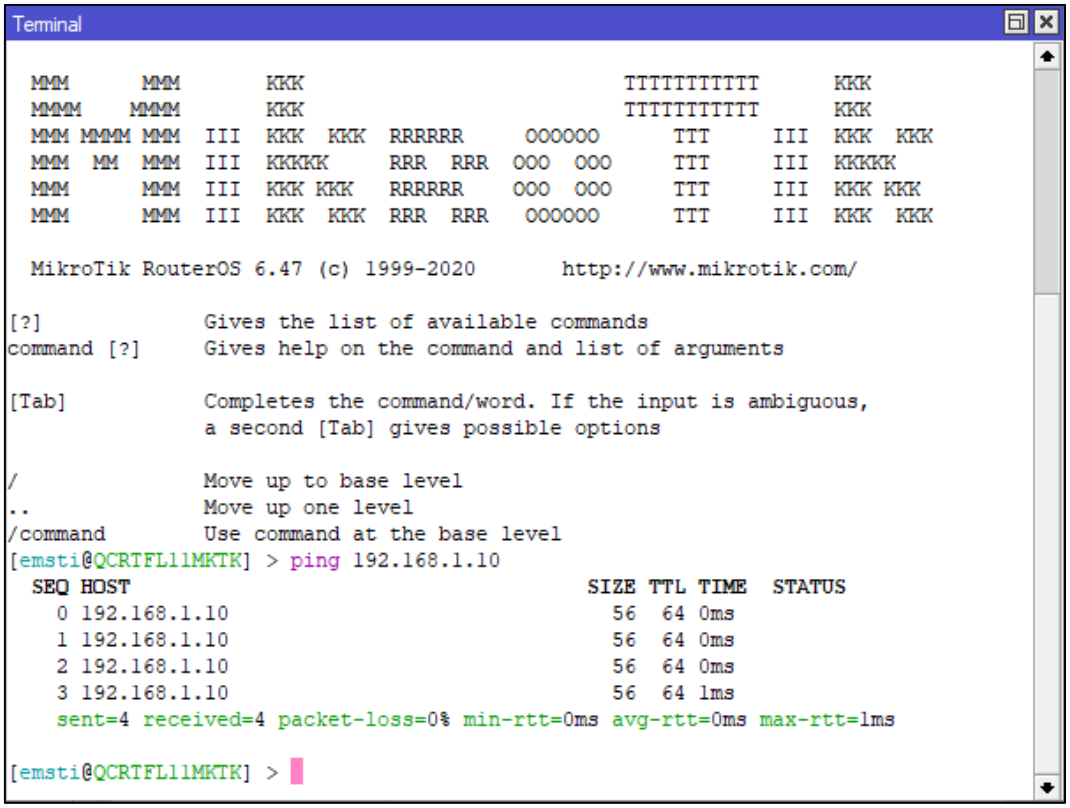
Figura 111. Ferramenta *New Terminal* no *routerboard* da matriz



Fonte: Os autores

O caminho reverso também foi feito, utilizando o mesmo teste, agora da console do *routerboard* da filial para o endereço IP **192.168.1.10** da *bridge* da rede local (*LAN*) da matriz. A Figura 112 exibe o resultado desse teste.

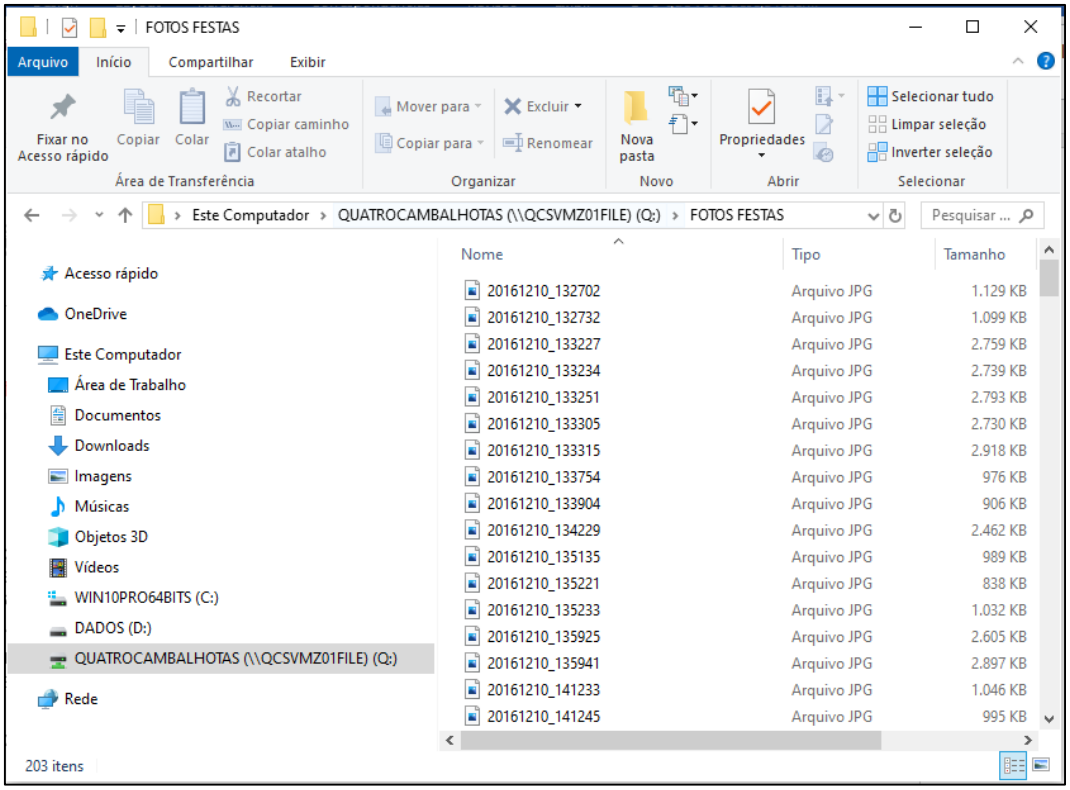
Figura 112. Ferramenta *New Terminal* no *routerboard* da filial



Fonte: Os autores

A Figura 113 exibe que foi possível acessar o diretório de arquivos, do compartilhamento existente no servidor. A pasta **FOTOS FESTAS** foi acessada e o seu conteúdo foi exibido.

Figura 113. Acesso ao diretório FOTOS FESTAS



Fonte: Os autores

A partir de agora, todos os serviços e recursos que forem instalados e compartilhados na rede da Quatro Cambalhotas, poderão ser acessados de qualquer um dos endereços, com esta implantação.

Embora executado um projeto simples e de baixo investimento, utilizando equipamentos com valores acessíveis e programa sem custo com licença, o objetivo foi alcançado e a expectativa do cliente atendida, entregando uma *VPN* estável e segura.

Segundo o sócio Vinícius, a *VPN* proporcionou a liberdade que ele precisava, pois liberou-o do compromisso de estar sempre disponível no salão de festas ou no ateliê de criação e em horários fixos ou agendados. Agora ele não precisa se preocupar se um cliente precisar de um atendimento mais exclusivo, em um horário especial, pois a informação de sua empresa estará disponível sempre que precisar, livrando-se das barreiras físicas que vivenciou até então, antes deste projeto.

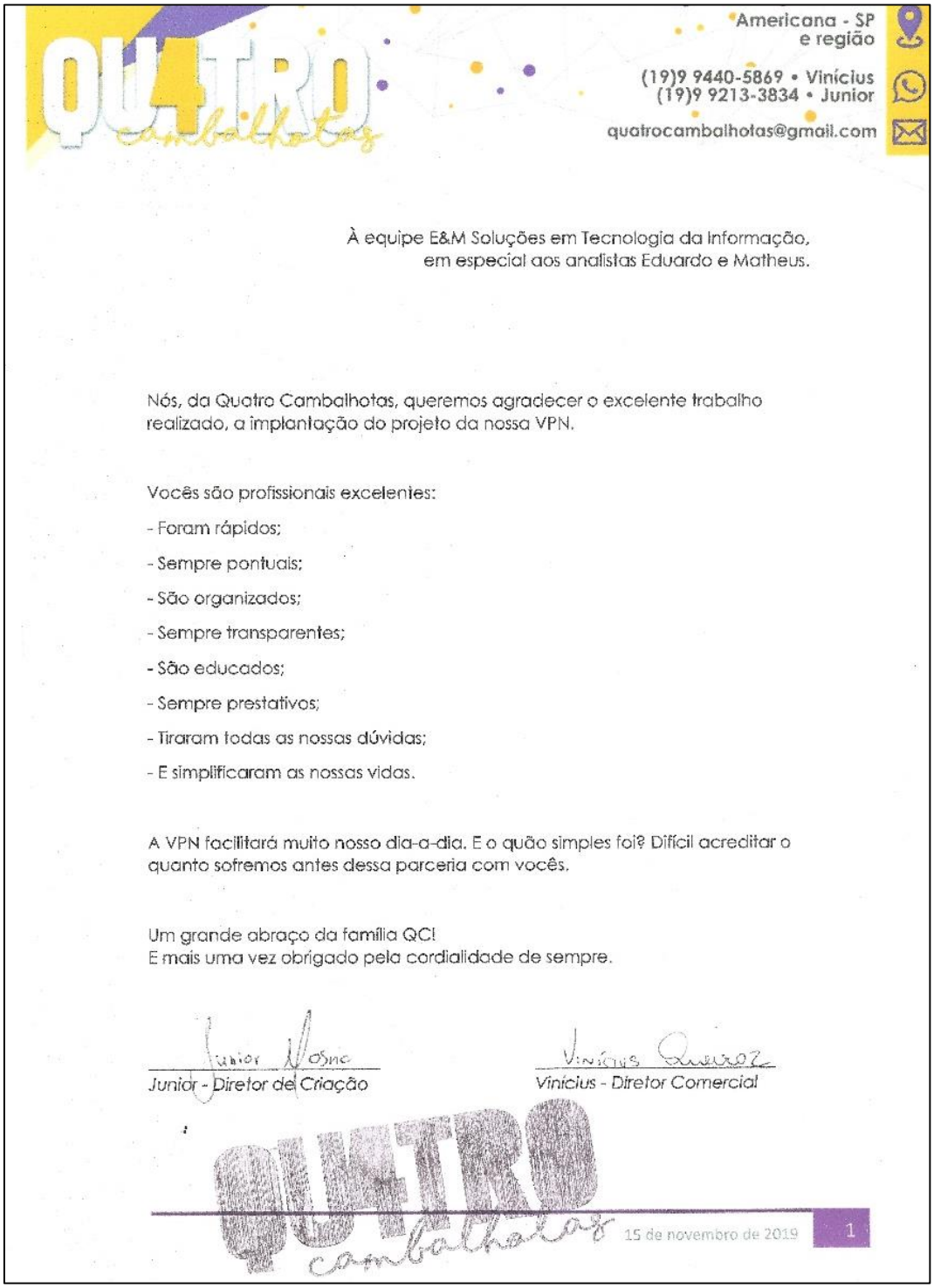
Para ele, além do ganho de tempo diário, a *VPN* ajudará a reduzir o número de visitas que o cliente precisa para aprovar as artes criadas pelos *designers*, pois agora

essas alterações poderão ser feitas imediatamente, na presença do cliente, durante essas visitas, fora da estrutura interna da Quatro Cambalhotas.

Já para o sócio Junior, o fato de estar no conforto de sua residência, após o horário comercial, ou até mesmo num final de semana, com a mente mais tranquila e criativa, poder acessar os arquivos da empresa para atualizar o portfólio da Quatro Cambalhotas nas mídias sociais foi um dos maiores benefícios que a *VPN* pôde proporcionar em seu dia-a-dia. *“Poder fechar o ateliê de criação as 18:00h e terminar o trabalho de casa, se necessário, foi uma grande conquista”,* completou Junior.

A Quatro Cambalhotas ficou satisfeita com o resultado final e elogiou, formalmente, o trabalho realizado pelos analistas da E&M, nas pessoas de Eduardo e Matheus. A Figura 114 exibe a carta de agradecimento redigida pelo cliente.

Figura 114. Carta de agradecimento do cliente



QUATRO cambalhotas

Americana - SP
e região

(19)9 9440-5869 • Vinícius
(19)9 9213-3834 • Junior

quatrocambalhotas@gmail.com

À equipe E&M Soluções em Tecnologia da Informação,
em especial aos analistas Eduardo e Matheus.

Nós, da Quatro Cambalhotas, queremos agradecer o excelente trabalho realizado, a implantação do projeto da nossa VPN.

Vocês são profissionais excelentes:

- Foram rápidos;
- Sempre pontuais;
- São organizados;
- Sempre transparentes;
- São educados;
- Sempre prestativos;
- Tiraram todas as nossas dúvidas;
- E simplificaram as nossas vidas.

A VPN facilitará muito nosso dia-a-dia. E o quão simples foi? Difícil acreditar o quanto sofremos antes dessa parceria com vocês.

Um grande abraço da família QC!
E mais uma vez obrigado pela cordialidade de sempre.

Junior - Diretor de Criação

Vinícius - Diretor Comercial

QUATRO cambalhotas

15 de novembro de 2019 1

Fonte: Os autores

7 Conclusões e considerações finais

Tão importante quanto poder acessar seu ambiente de trabalho remotamente é poder fazê-lo isso de maneira segura e eficiente, de modo que o conteúdo das informações possa estar protegido contra interceptações indevidas e não autorizadas. Isso garante a confidencialidade, integridade e disponibilidade da informação, que são os pilares da segurança da informação. E isso é altamente recomendável nos dias de hoje.

Estamos vivendo em uma era onde a mobilidade da informação está no smartphone que seguramos na mão, no notebook que carregamos na mochila ou até mesmo na TV, que está conectada na internet, na rede local da nossa casa. O maior objetivo está em como proteger toda essa informação.

Buscar por mecanismos confiáveis, que oferecem segurança e protegem a informação, nem sempre é uma tarefa fácil, pois geralmente estes recursos não são ofertados no mercado em um valor acessível a realidade financeira de nossos clientes.

E cada vez mais os nossos clientes estão mudando a forma como trabalham, desprendendo-se dos escritórios tradicionais e passando a trabalhar mais tempo em casa, no regime *home-office*, ou até mesmo viajando, visitando seus parceiros de negócios, fornecedores e clientes.

Nosso desafio neste projeto foi encontrar uma solução que atendesse a necessidade do cliente Quatro Cambalhotas, que está iniciando e apostando num novo segmento de mercado e, devido ao alto investimento feito no salão de festas, não reservou a devida quantia para ser empregada na tecnologia da informação da empresa.

Mediante esta situação, a E&M Soluções em tecnologia da informação encontrou uma solução e aplicou-a em um projeto, que foi apresentado e aprovado pelo cliente. E, ao decorrer das etapas de implantação, pudemos observar que, mesmo não investindo tanto com a aquisição de equipamentos mais sofisticados, foi possível atingir a expectativa do cliente, com a entrega de um projeto simples, estável e confiável.

A combinação do *hardware* Mikrotik com a associação do *software OpenVPN* foi uma escolha assertiva. Essa decisão, além de envolver os aspectos financeiros e técnicos, que eram premissas para a execução do projeto, entregou uma *VPN* estável, segura, eficaz e barata. Isso possibilitou que os sócios pudessem ter mais mobilidade da informação entre os endereços da empresa e proporcionar um atendimento mais

personalizado e íntimo, de modo que agora eles podem acessar a Quatro Cambalhotas de qualquer lugar e a qualquer momento, quando reservarem um horário com seus clientes para apresentarem seus produtos.

Concluindo, a *VPN* pode designar-se em uma alternativa segura para transmitir dados através de redes privadas ou públicas, uma vez que já ofertam recursos de autenticação e criptografia, com diversos níveis de segurança, proporcionando a eliminação dos links dedicados, de longa distância e de custos elevados, na conexão de *WANs*. Todavia, em aplicações onde o tempo de transmissão é uma questão crítica, o uso de VPN através de redes externas ainda deve ser analisado com cautela, pois podem ocorrer problemas de performance e atrasos na transmissão dos dados, sobre os quais a empresa não tem nenhum tipo de gestão ou controle, comprometendo a qualidade desejada nos serviços corporativos. Posto isto, a decisão de implementar ou não uma VPN requer uma análise criteriosa dos requisitos, principalmente daqueles que estão relacionados à segurança, confiabilidade, custos, qualidade de serviço e facilidade de utilização, que podem variar de acordo com a situação e o ramo de atuação de cada empresa.

REFERÊNCIAS BIBLIOGRÁFICAS:

CISCO. “**O que é um firewall?”**. Disponível em: https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html. Acesso em: 14 nov. 2019.

FOROUZAN, Behrouz. **Comunicação de Dados e Redes de Computadores**. Tradução Ariovaldo Griesi. 4. ed. Porto Alegre: AMGH, 2010. Tradução de: Data Communications and Networking.

KUROSE, James; ROSS, Keith. **Redes de computadores e a Internet: uma abordagem top-down**. Tradução Daniel Vieira. 6. ed. São Paulo: Pearson, 2013. Tradução de: Computer networking: a top-down approach.

MIKROTIK. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2020. Disponível em: https://pt.wikipedia.org/w/index.php?title=Mikrotik&oldid=57885283. Acesso em: 14 nov. 2019.

MIKROTIK. **RB750Gr3**. Disponível em:https://mikrotik.com/product/RB750Gr3. Acesso em: 14 nov. 2019.

MIKROTIK. **Dynamic DNS Update Script for No-IP DNS**. Disponível em: https://wiki.mikrotik.com/wiki/Dynamic_DNS_Update_Script_for_No-IP_DNS. Acesso em: 14 nov. 2019.

MIKROTIK. **Main Page**. Disponível em: https://wiki.mikrotik.com/wiki/Main_Page. Acesso em: 14 nov. 2019.

MIKROTIK. **Manual:Securing Your Router**. Disponível em: https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router. Acesso em: 14 nov. 2019.

MIKROTIK. **OpenVPN.** Disponível em: https://wiki.mikrotik.com/wiki/OpenVPN. Acesso em: 14 nov. 2019.

OPENVPN. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2020. Disponível em: https://pt.wikipedia.org/w/index.php?title=OpenVPN&oldid=57551076. Acesso em: 14 nov. 2019.

OPENVPN. **Página Principal**. Disponível em: https://openvpn.net/. Acesso em: 14 nov. 2019.

SAYEED, Abu. **MikroTik OpenVPN Setup with Windows Client**. Disponível em: https://systemzone.net/mikrotik-openvpn-setup-with-windows-client/. Acesso em: 14 nov. 2019.

SAYEED, Abu. **MikroTik OpenVPN Setup with Windows Client**. Youtube. Disponível em: https://www.youtube.com/watch?v=6l1sYGLrlz0. Acesso em: 14 nov. 2019.

SAYEED, Abu. **MikroTik Site to Site OpenVPN Server Setup.** Disponível em: https://systemzone.net/mikrotik-site-to-site-openvpn-server-setup-routeros-client/. Acesso em: 14 nov. 2019.

SAYEED, Abu. **MikroTik Site to Site OpenVPN Server Configuration.** Youtube**.** Di sponível em: https://www.youtube.com/watch?v=-RZfqIQ6PeA. Acesso em: 14 de nov. 2019. 18:26.

TANENBAUM, Andrew. **Redes de computadores**. Tradução Vandenberg D. de Souza. 4. ed. São Paulo: Campus, 2003. Tradução de: Computer Networks.