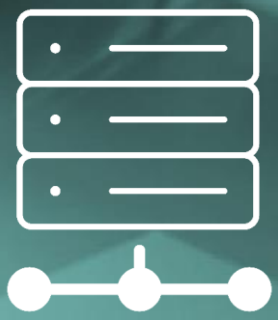
ar telecom
Grupo Aire

CLOUD – Virtual Data Center

Router Multi Serviços

MANUAL DE UTILIZADOR



CLOUD

Reference: M_GP_304

Date: 23/06/2025

Version: 1.1

Controlo de Versões:

Versão	Data	Alterações
1.0	11-Jun-2025	na.
1.1	23-Jun-2025	Versão revista

Significado dos Símbolos utilizados

 INFORMAÇÃO	Informação adicional que se pretende relevar
 AVISO	Informação Importante que requer especial atenção

ÍNDICE

1. MANUAL DE UTILIZADOR

Este documento tem como objetivo facilitar a utilização do router multiserviços Mikrotik.

Este manual é uma versão simplificada da documentação oficial, adaptada para os cenários mais comuns e no âmbito de utilização no ambiente Virtual Data Center da Ar Telecom.

A instância de Mikrotik fornecida pela Ar Telecom é uma versão simplificada, customizada para os cenários predominantes no ambiente de virtual data center.

As configurações apresentadas neste manual consideram a existência de apenas um IP público.

Para obter informações mais detalhadas, recomendamos que consulte a documentação oficial.

O seu router é entregue pré-configurado juntamente com a criação da vApp no VDC. Este manual pretende dar a conhecer algumas configurações específicas.

A configuração base inclui o seguinte:

- Permite tráfego das redes internas da vApp para a internet (SNAT)
- Permite redireccionamento de portas (DNAT)
- Regras de firewall
- Serviço OpenVPN pronto a funcionar:
  - Servidor ativo em modo split-tunnel
  - 10 utilizadores VPN pré-configurados
  - Configuração dos clientes OpenVPN simplificada
- VPNs WireGuard:
  - Interface criada e pronta a ativar
  - Instruções simples de configuração
  - Permite VPNs road-warrior (para PCs, smartphones, etc)
  - Permite VPNs ponto-a-ponto (interligação de redes router a router)
- VPNs IPsec:
  - Instruções simples de configuração
  - Permite VPNs ponto-a-ponto (interligação de redes router a router)

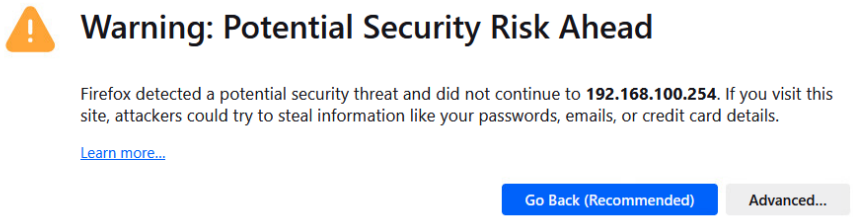
2. ACESSO

Por razões de segurança, o Mikrotik não vai aceitar acesso à consola de configuração através do IP público. A Ar Telecom entrega a solução com acesso permitido a partir da rede privada da vApp. Para aceder à consola, utilizar então um browser e o endereço:

https:*endereço_privado_do_Mikrotik*:10300.

Esta informação é enviada no email de provisão do serviço.

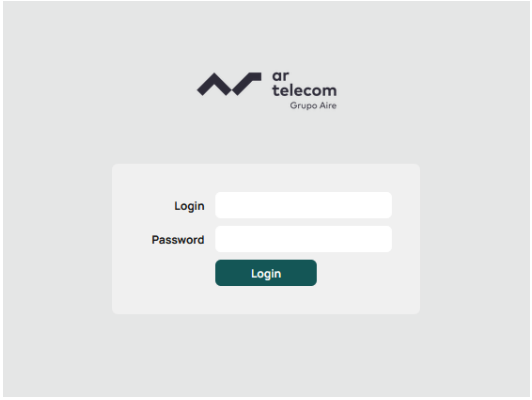
Caso não tenha disponível uma VM com ambiente gráfico e browser, o acesso deverá ser feito via VPN. Para obter os detalhes da configuração VPN a utilizar deve entrar em contacto com o suporte da Ar Telecom. Depois da ligação VPN estar ativa, o acesso à consola faz-se utilizando o URL indicado anteriormente. O certificado SSL utilizado é gerado internamente, pelo que, irá receber uma notificação de ligação com risco potencial. Poderá ignorar e caso pretenda, posteriormente adquirir e instalar um certificado válido.



Surgirá então a janela para introdução de credenciais que por defeito, são:

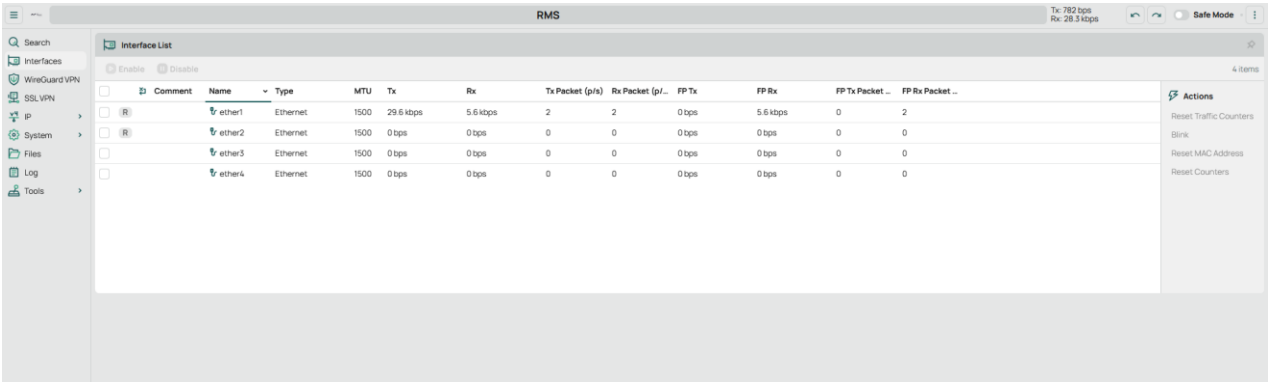
- Username: admin_cliente
- Password: enviada aquando da provisão do serviço

Recomendamos que altere a password após o primeiro login.

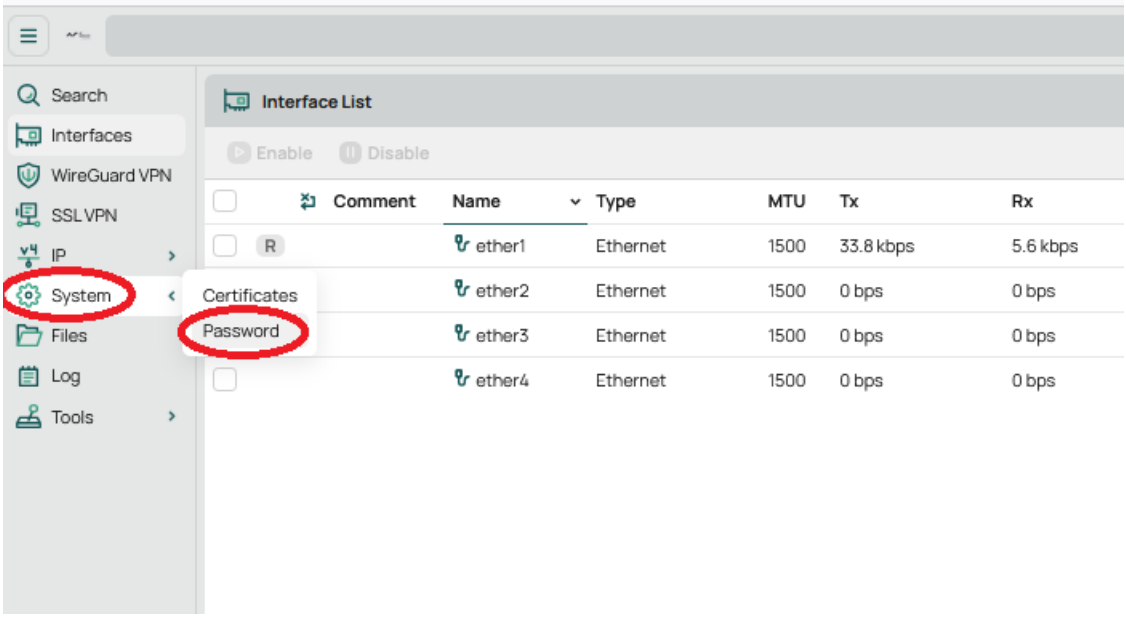


3. ALTERAR PASSWORD

Após o login será mostrado o ecrã de interfaces:



Para mudar a password de acesso à consola, ir a System no menu lateral esquerdo e carregar em Password:



4. CONEXÃO A REDE DO VDC

O router instalado irá gerir o tráfego entre o exterior e as redes internas. A versão provisionada pela Ar Telecom já contempla quatro interfaces, sendo a primeira (ether1) utilizada para conexão com o exterior, e as restantes utilizadas para redes internas do VDC.

Com a provisão de uma nova vApp é entregue uma instância de router multi serviços já com as interfaces de rede configurados e conectados às redes privadas dessa vApp, sendo que, tipicamente existe uma rede privada por vApp, correspondendo à interface ether2 no router.

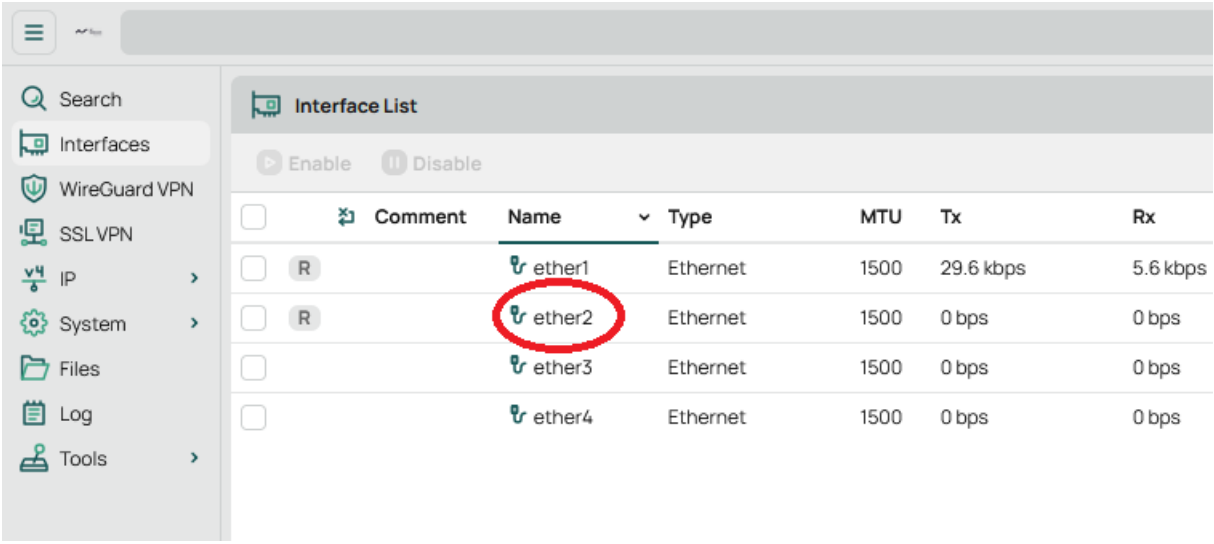
Caso seja necessário adicionar mais que três interfaces privadas e até ao limite de nove, deve contactar o suporte da Ar Telecom.

As instruções seguintes aplicam-se apenas se criar redes privadas adicionais.

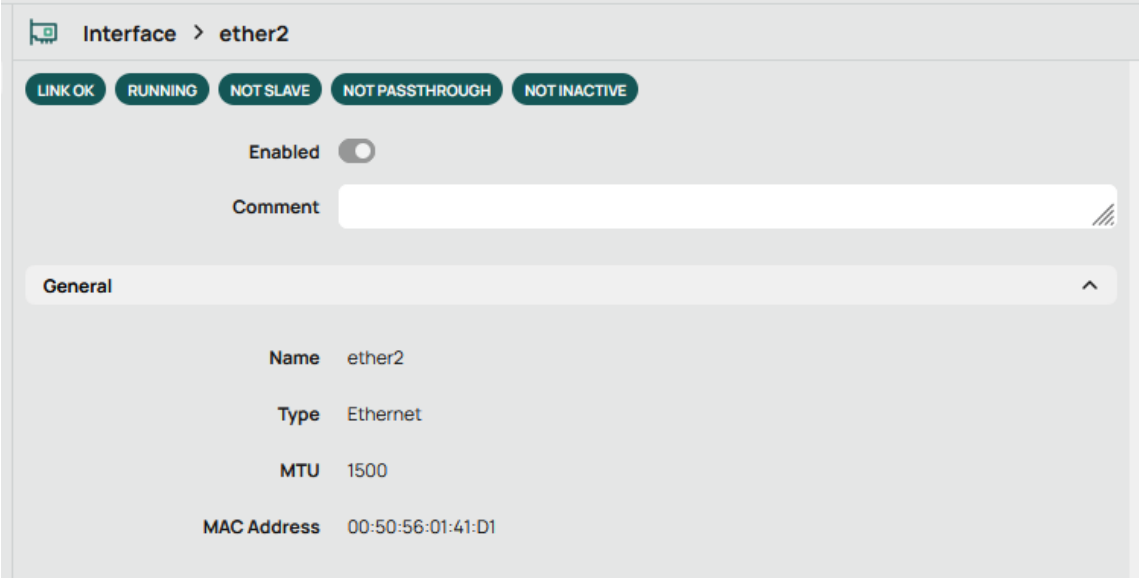
4.1 Interfaces

A numeração das interfaces no Mikrotik começa em 1 e no VDC em 0, e a correspondência entre as interfaces do Mikrotik e do VDC é feita por ordem, ou seja, a 1 do Mikrotik corresponde à 0 do VDC, a 2 do Mikrotik corresponde à 1 do VDC e por aí fora. Isto pode ser confirmado verificando os MAC addresses.

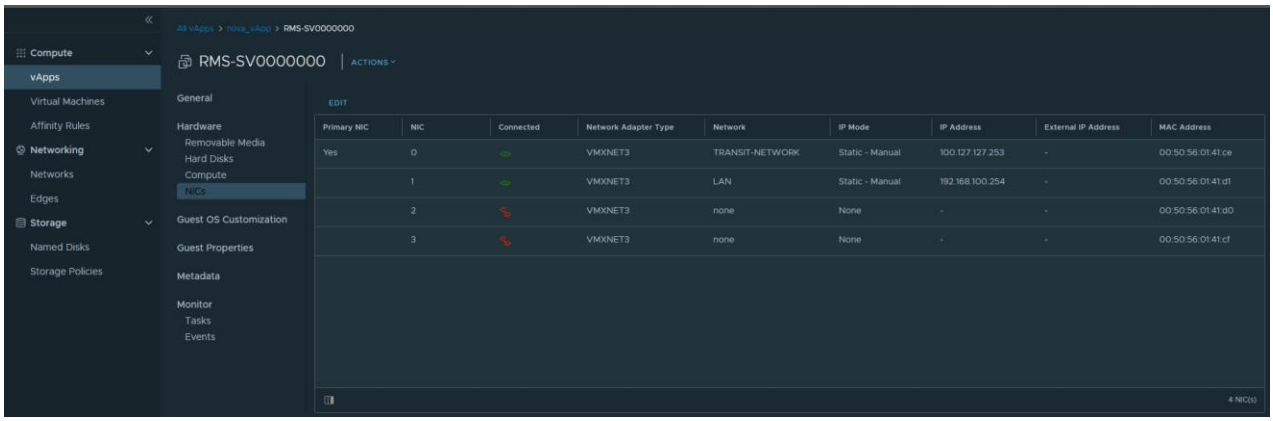
Para ver o MAC address das interfaces no Mikrotik, clicar na interface:



verificar os detalhes:



e confirmar com o MAC no VDC:



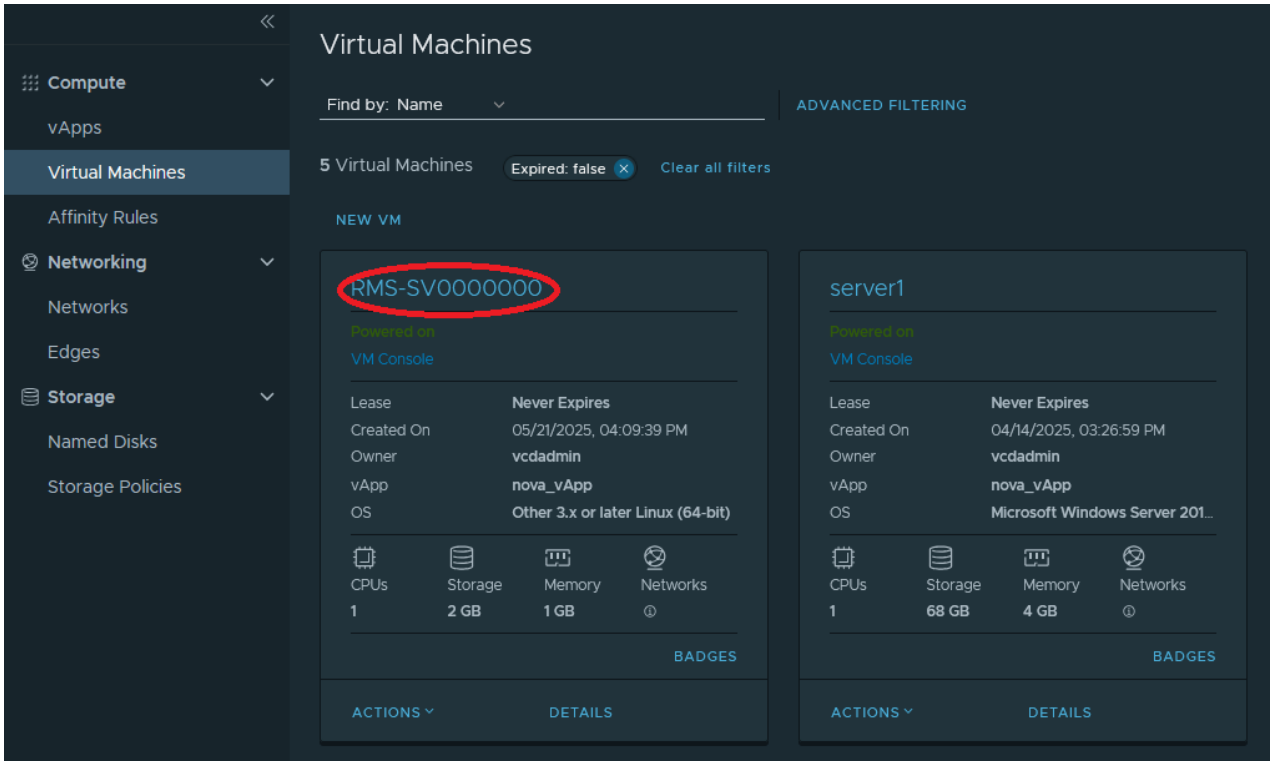
4.2 Conexão à rede privada no vCloud

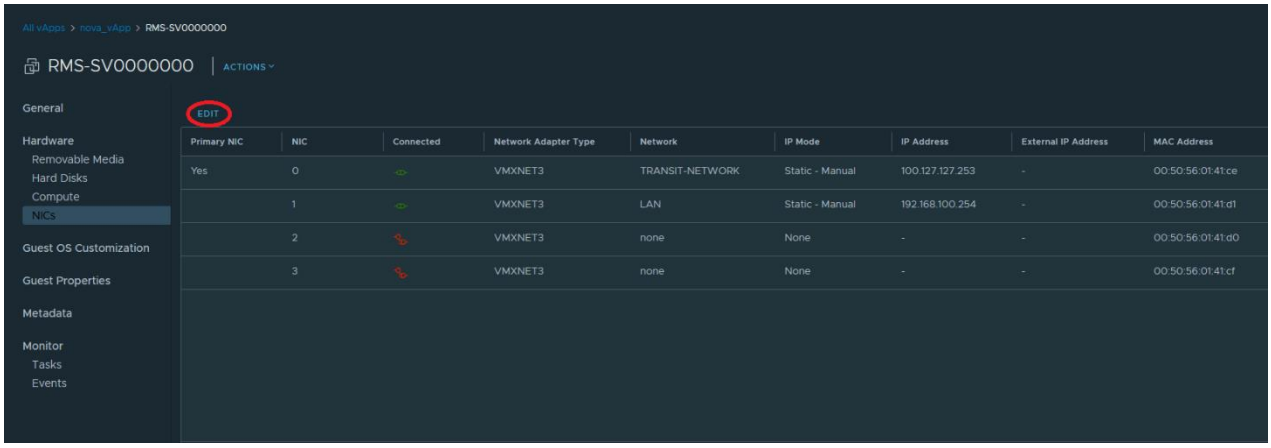
Durante o processo de provisão efetuado pela Ar Telecom, efetuam-se as conexões para o exterior e para as redes privadas solicitadas na vApp.

Caso posteriormente pretenda criar mais redes na vApp com consequente conexão ao router Mikrotik, deve seguir um procedimento muito simples que passamos a descrever.

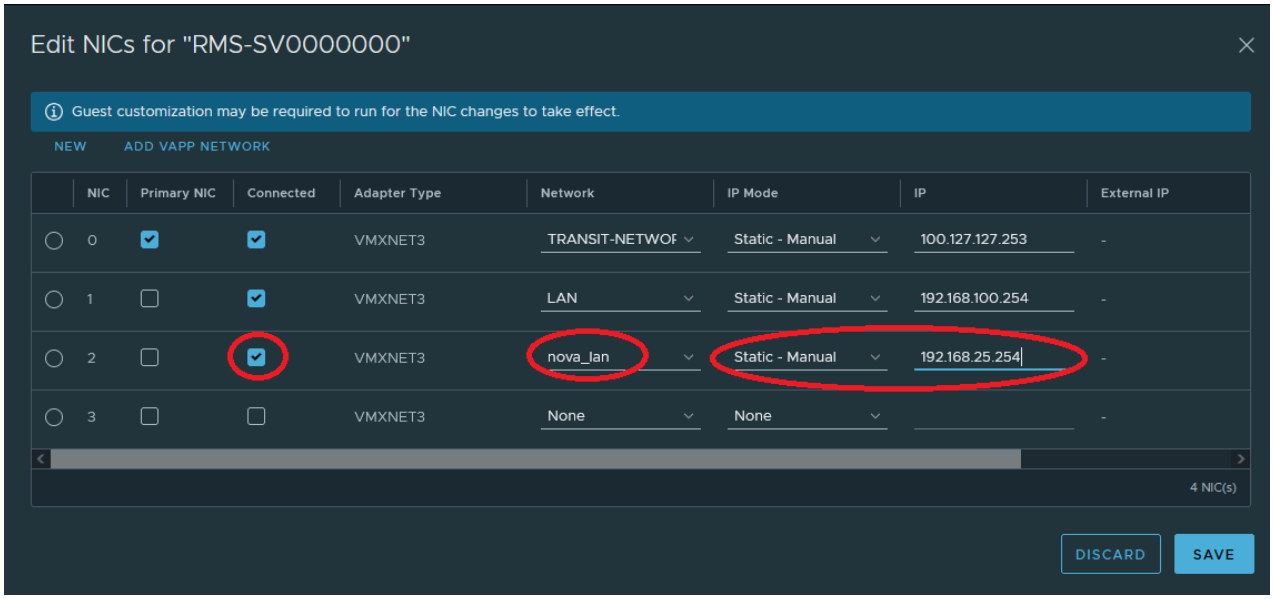
O primeiro passo é obviamente a criação da rede na vApp (vApp Network). Para efeitos deste manual, vamos considerar uma rede denominada "nova_lan" com endereçamento 192.168.25.0/24.

De seguida, no portal vCloud associa-se a interface da VM com o Mikrotik à rede pretendida. Clica-se na VM correspondente ao Mikrotik e posteriormente edita-se a configuração das NICs:



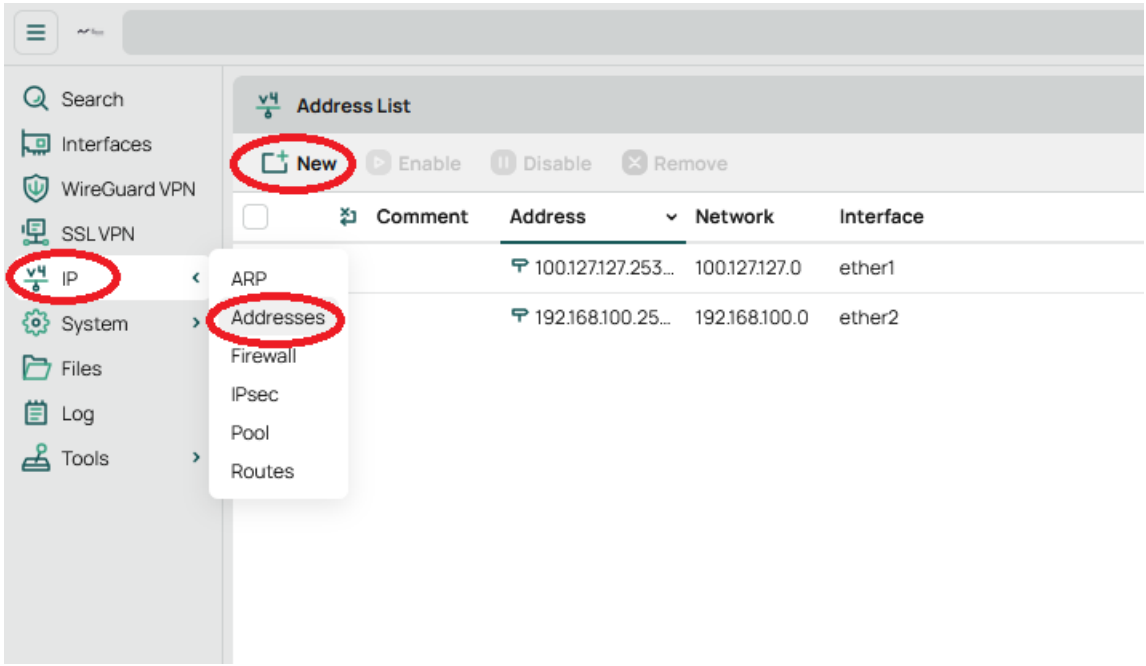


Neste caso e sendo que já existem duas interfaces ativas (a 0 para o acesso exterior e a 1 para a rede LAN criada no processo de provisão), vamos configurar a interface 2 e associá-la à rede recentemente criada, selecionando "Connected", a rede pretendida e o endereçamento IP:



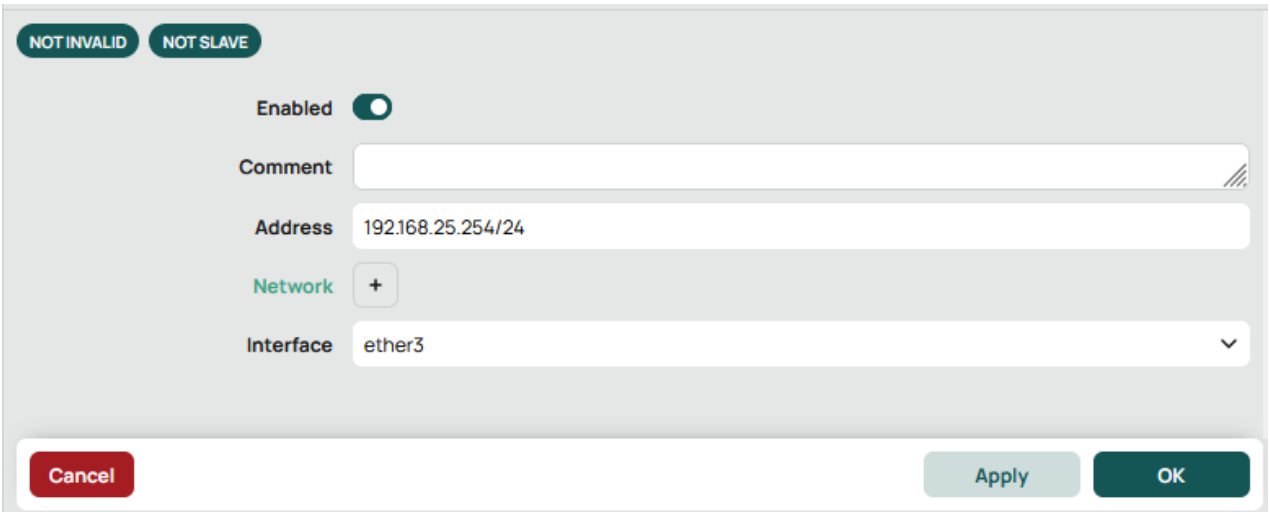
4.3 Configuração da interface no Mikrotik

Para configurar o endereçamento da interface, aceder à consola e no menu lateral esquerdo escolher IP -> Addresses e adicionar uma nova carregando em **New**.



Preencher com os dados pretendidos, neste exemplo:

- Enabled
- Address: 192.168.25.254/24
- Interface: escolher a interface pretendida, neste exemplo, ether3



Terminar fazendo Apply e OK.

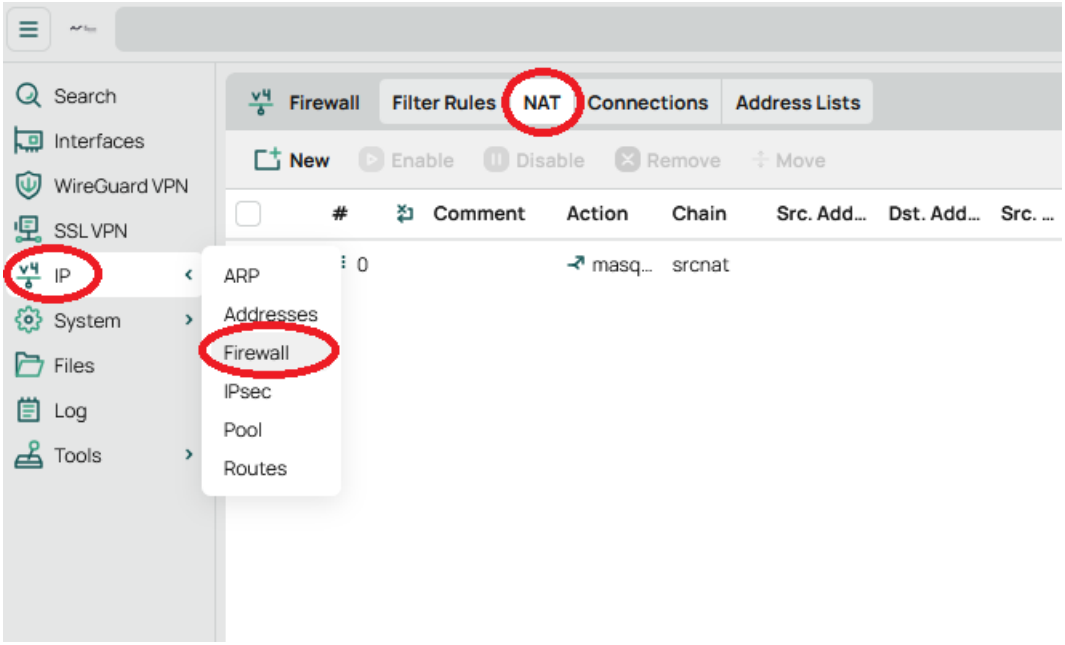
5. PERMITIR TRÁFEGO PARA A INTERNET - SNAT

Para permitir a saída de tráfego para a rede pública, é necessário existir uma regra SNAT e permitir o tráfego para cada uma das redes privadas (internas do VDC) a que se pretenda dar este acesso. A Ar Telecom entrega o serviço com uma regra já criada que efetua o SNAT de qualquer rede interna, mesmo que seja criada posteriormente, e uma regra de firewall que permite o tráfego apenas das redes internas da vApp provisionada.

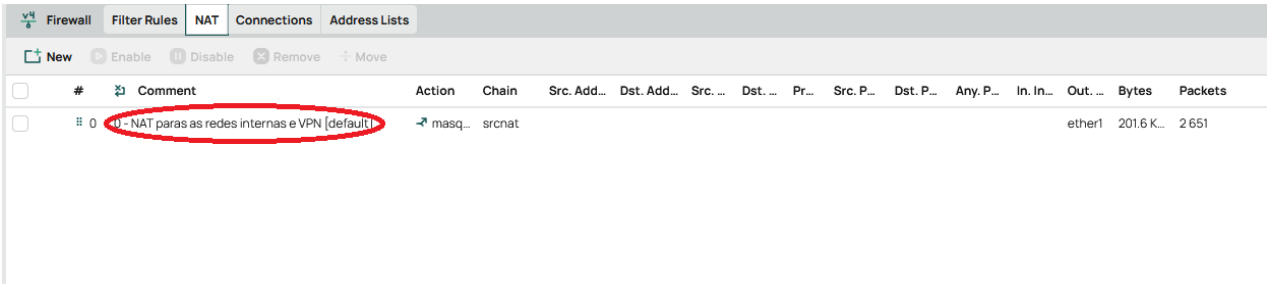
De qualquer forma, pode encontrar em baixo informação de como o fazer se posteriormente efetuar alguma alteração.

5.1 Configuração SNAT

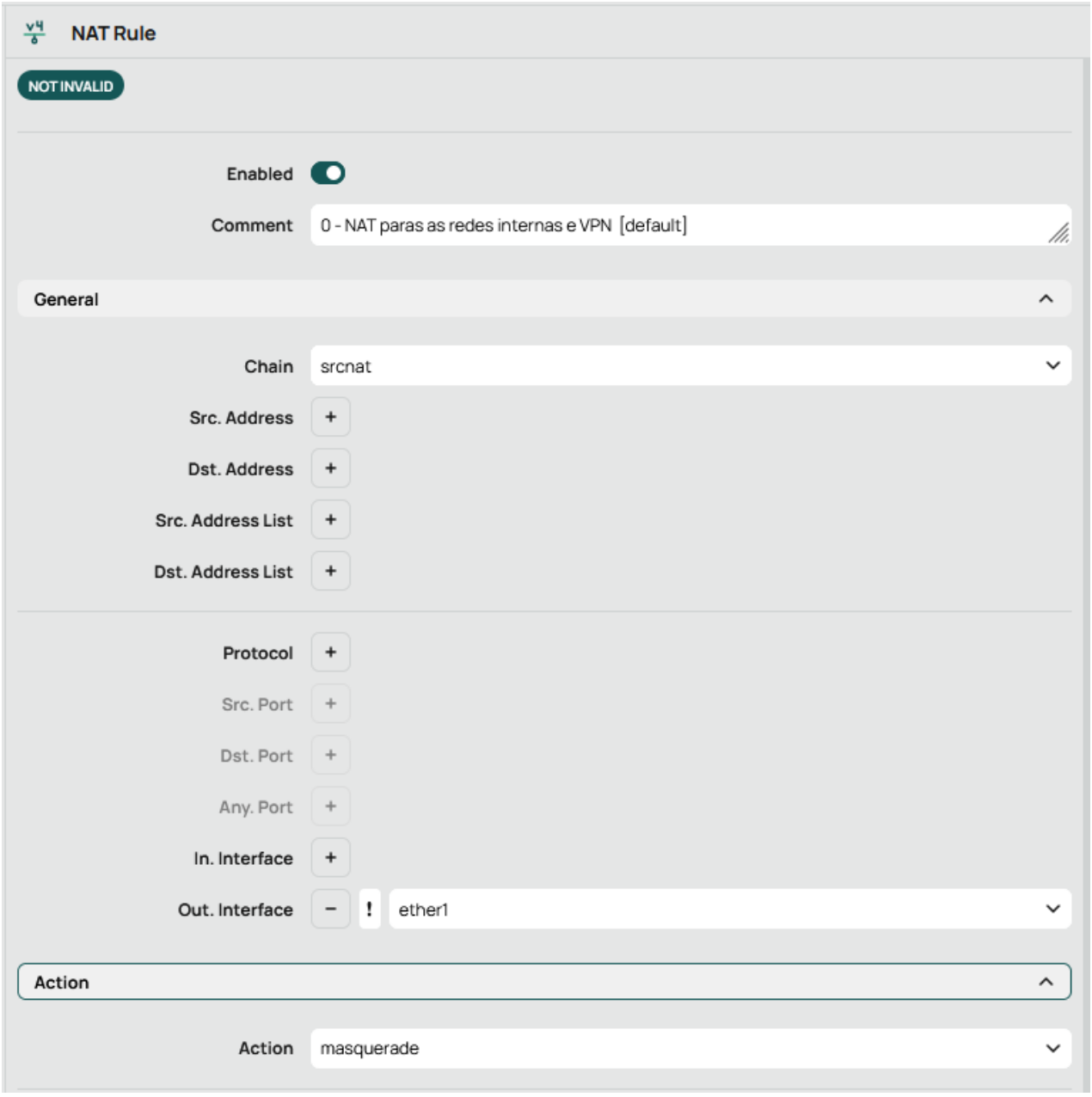
As regras SNAT para as redes solicitadas durante a provisão são criadas pela equipa da Ar Telecom. Posteriormente, caso pretenda alterar ou criar regras diferentes, poderá fazê-lo indo ao menu lateral esquerdo e clicar IP -> Firewall e seguidamente no tab NAT:



A configuração inicial consiste numa regra que mascara o IP de todo o tráfego que sai para o exterior com o IP atribuído ao router, independentemente da rede interna. Para verificar essa configuração, clica-se na regra apresentada:



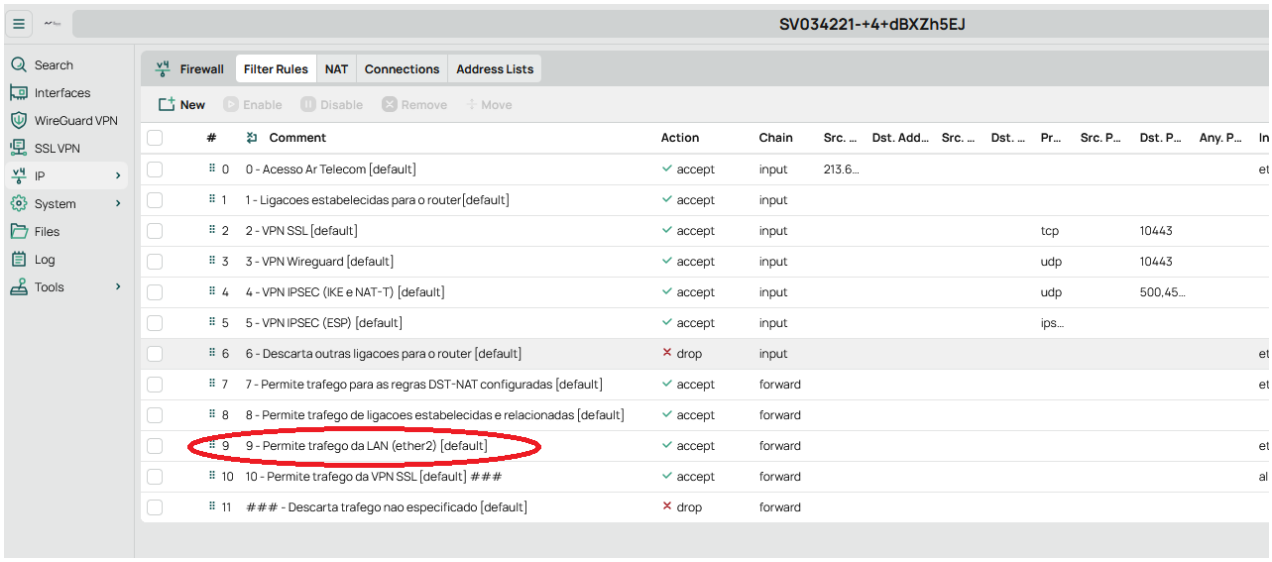
sendo a configuração como se mostra a seguir:

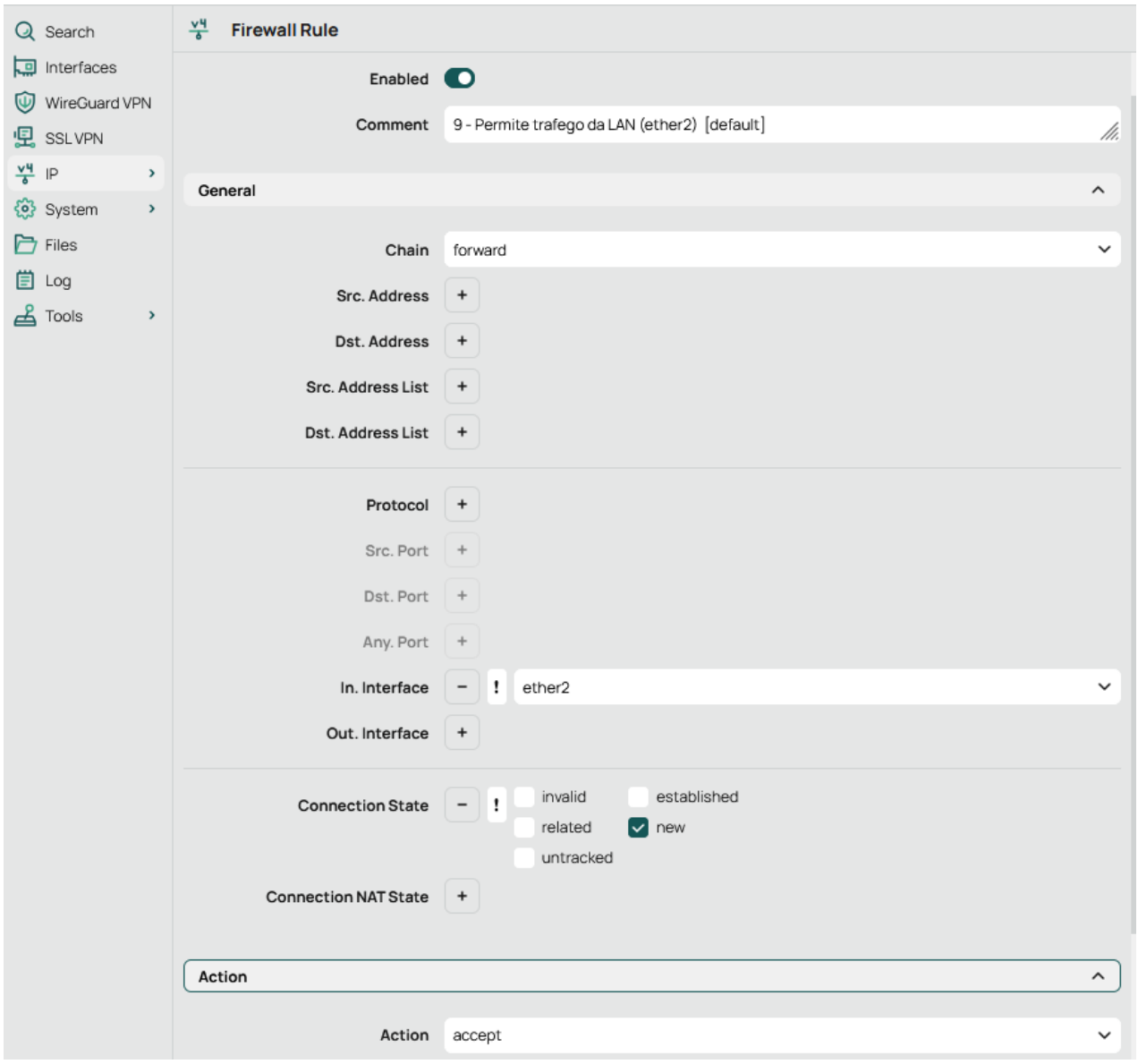


5.2 Configuração regras de tráfego

A Ar Telecom entrega o Mikrotik com algumas regras pré-configuradas, nomeadamente, permitindo o tráfego de saída a partir das redes internas criadas na vApp no momento da provisão. Havendo apenas uma como neste exemplo, isso equivale à interface ether2 no router.

Para verificar ou modificar essa configuração, poderá fazê-lo indo ao menu lateral esquerdo e clicar IP -> Firewall e seguidamente no tab Filter Rules, clicando depois na regra apresentada:

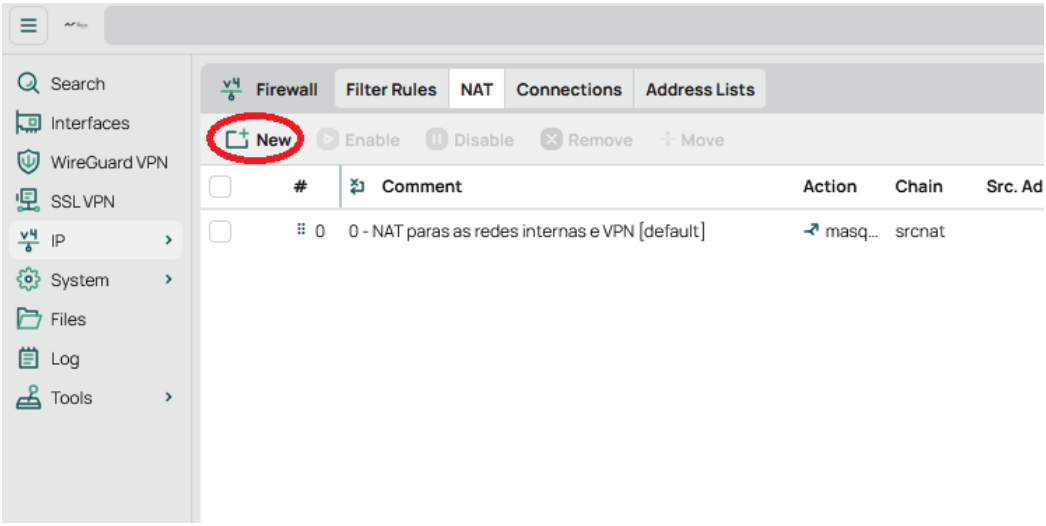




6. PORT FORWARD – DNAT

Para redirecionar acessos do exterior para uma determinada máquina numa rede interna, é necessário configurar regras DNAT e permitir o tráfego.

Para o fazer, aceder à configuração de regras NAT no menu lateral esquerdo e clicar IP -> Firewall e seguidamente no tab NAT. Seguidamente clicar em New e preencher o quadro em conformidade.



No nosso exemplo, vamos redirecionar a porta 10301 para a porta RDP (3389) de um servidor Windows na rede LAN com o endereço 192.168.100.53.

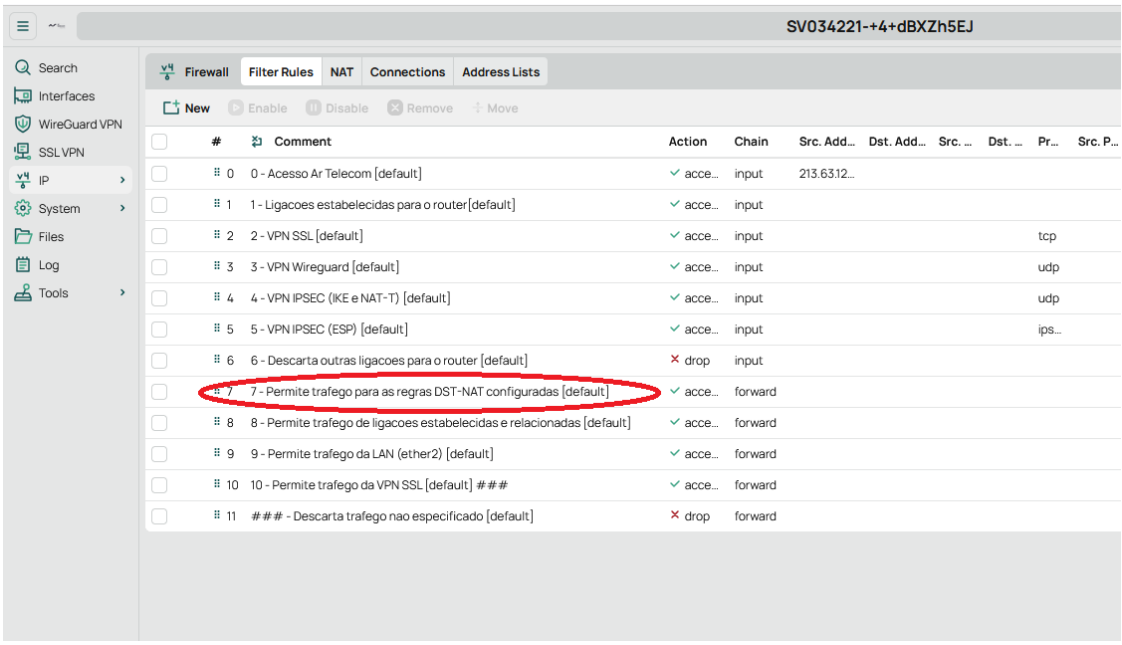
General

- Chain deve ser dstnat
- Src. Address fica vazio se quisermos permitir o acesso de qualquer IP
- Dst. Address vamos deixar vazio pois vamos redirecionar o que chegar à interface ether1
- Protocolo: TCP
- Dst. Port: a porta que irá ser redirecionada. No nosso exemplo, 10301
- In. Interface: a interface onde se vai aplicar o redireccionamento. Deverá ser ether1

Action

- Action: dst-nat
- To Addresses: o endereço do servidor para onde vai ser redirecionado
- To Ports: a porta destino no servidor para onde vai ser redirecionado

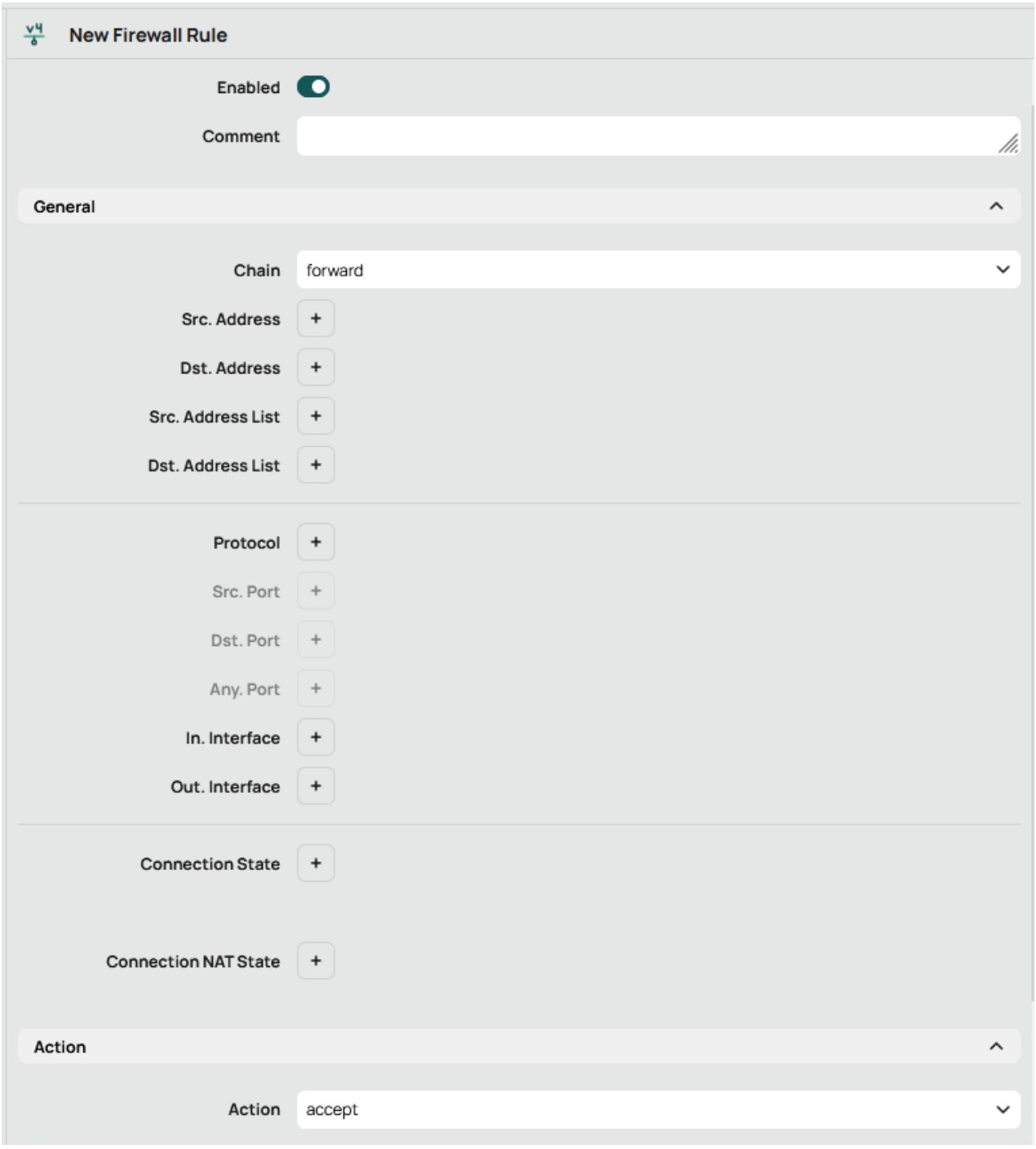
Por fim é necessário definir uma regra que permite a passagem deste tráfego. A Ar Telecom entrega o Mikrotik com uma regra pré-configurada que permite a passagem de todo o tráfego DNAT. Isso pode ser verificado e modificado clicando na regra:



7. REGRAS DE FIREWALL

Além das regras NAT é possível definir regras mais complexas de filtragem de tráfego. Estas regras são geridas no quadro Filter Rules, acessível através do menu lateral esquerdo e clicando IP -> Firewall -> tab Filter Rules.

Aqui podemos ver e editar as regras existentes, assim como criar novas regras. Para criar uma nova regra, clicar em New e configurar de acordo com o pretendido.

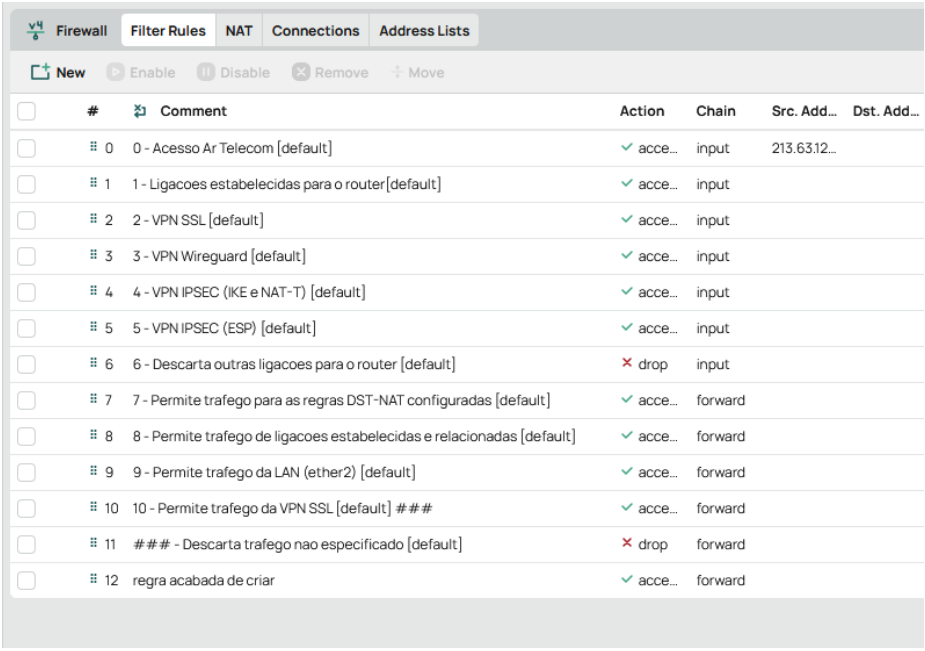


Atenção a um parâmetro da configuração (Chain) que deve ser compreendido da seguinte forma:

Chain:

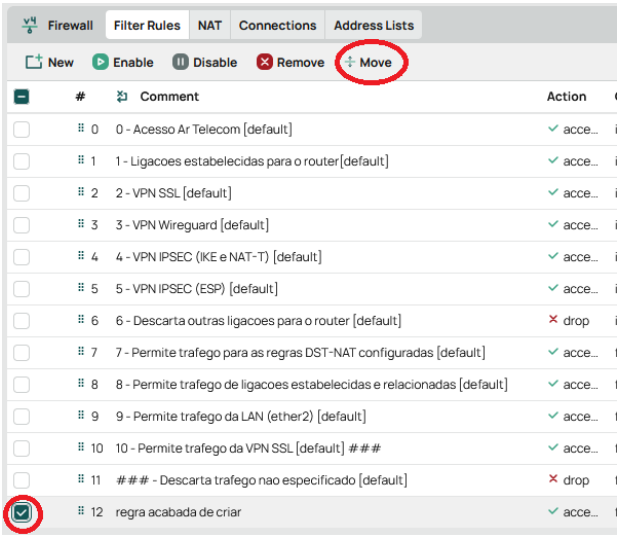
- Input: tráfego que entra com destino a serviços no router
- output: tráfego originado pelo router
- forward: tráfego que atravessa o router

Carregando no botão OK a regra será criada e colocada no fim da lista de regras.

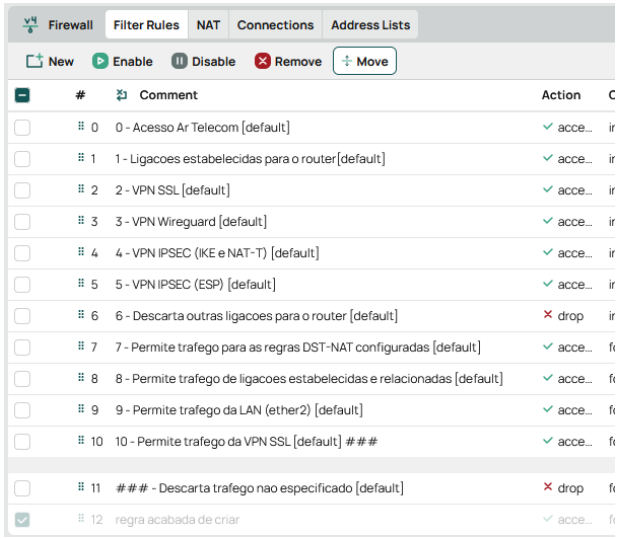


#	Comment	Action	Chain	Src. Add...	Dst. Add...
0	0 - Acesso Ar Telecom [default]	acce...	input	213.63.12...	
1	1 - Ligacoes estabelecidas para o router[default]	acce...	input		
2	2 - VPN SSL [default]	acce...	input		
3	3 - VPN Wireguard [default]	acce...	input		
4	4 - VPN IPSEC (IKE e NAT-T) [default]	acce...	input		
5	5 - VPN IPSEC (ESP) [default]	acce...	input		
6	6 - Descarta outras ligacoes para o router [default]	drop	input		
7	7 - Permite trafego para as regras DST-NAT configuradas [default]	acce...	forward		
8	8 - Permite trafego de ligacoes estabelecidas e relacionadas [default]	acce...	forward		
9	9 - Permite trafego da LAN (ether2) [default]	acce...	forward		
10	10 - Permite trafego da VPN SSL [default] ###	acce...	forward		
11	### - Descarta trafego nao especificado [default]	drop	forward		
12	regra acabada de criar	acce...	forward		

Como a execução das regras é feita top-to-bottom e a última regra existente descarta todo o tráfego novo (ação drop), é necessário movê-la uma posição para cima. Para o fazer, seleciona-se a mesma, clica-se em Move ou carrega-se em cima da regra, e arrasta-se para a posição pretendida.



#	Comment	Action
0	0 - Acesso Ar Telecom [default]	acce...
1	1 - Ligacoes estabelecidas para o router[default]	acce...
2	2 - VPN SSL [default]	acce...
3	3 - VPN Wireguard [default]	acce...
4	4 - VPN IPSEC (IKE e NAT-T) [default]	acce...
5	5 - VPN IPSEC (ESP) [default]	acce...
6	6 - Descarta outras ligacoes para o router [default]	drop
7	7 - Permite trafego para as regras DST-NAT configuradas [default]	acce...
8	8 - Permite trafego de ligacoes estabelecidas e relacionadas [default]	acce...
9	9 - Permite trafego da LAN (ether2) [default]	acce...
10	10 - Permite trafego da VPN SSL [default] ###	acce...
11	### - Descarta trafego nao especificado [default]	drop
12	regra acabada de criar	acce...



#	Comment	Action
0	0 - Acesso Ar Telecom [default]	acce...
1	1 - Ligacoes estabelecidas para o router[default]	acce...
2	2 - VPN SSL [default]	acce...
3	3 - VPN Wireguard [default]	acce...
4	4 - VPN IPSEC (IKE e NAT-T) [default]	acce...
5	5 - VPN IPSEC (ESP) [default]	acce...
6	6 - Descarta outras ligacoes para o router [default]	drop
7	7 - Permite trafego para as regras DST-NAT configuradas [default]	acce...
8	8 - Permite trafego de ligacoes estabelecidas e relacionadas [default]	acce...
9	9 - Permite trafego da LAN (ether2) [default]	acce...
10	10 - Permite trafego da VPN SSL [default] ###	acce...
11	### - Descarta trafego nao especificado [default]	drop
12	regra acabada de criar	acce...

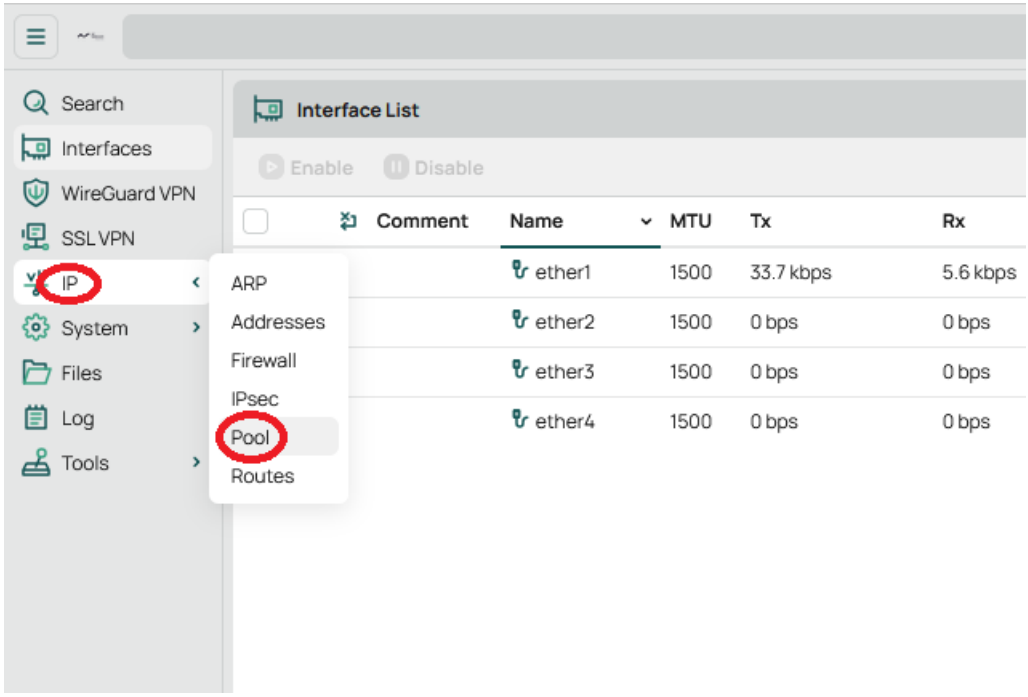
8. OPENVPN ROAD WARRIOR (PPP/SSL VPN)

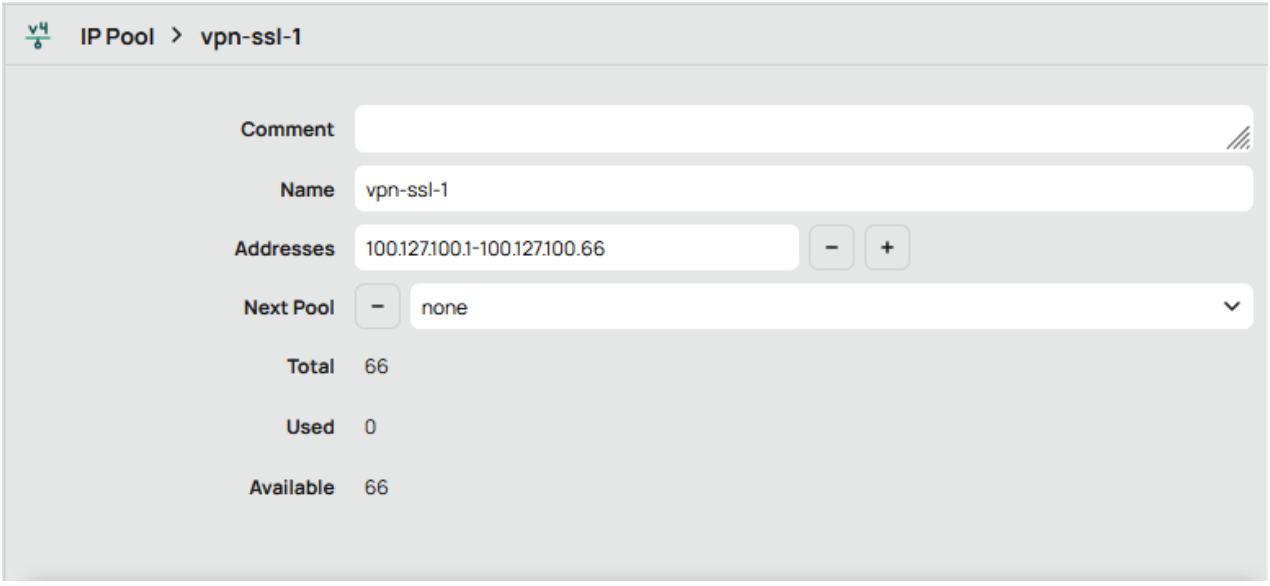
Uma VPN Road Warrior OpenVPN requer certificados SSL/TLS para encriptação, nomeadamente, uma Certificate Authority (CA), um certificado de servidor e um certificado de cliente.

A Ar Telecom entrega o serviço com estes certificados já criados.

8.1 Configurar endereçamento IP do túnel OpenVPN

Para criar uma gama de endereços IP a atribuir aos clientes OpenVPN que se conectam, ir ao menu lateral esquerdo e clicar em IP -> Pool. O serviço é entregue já com esta pool criada (100.127.100.1-100.127.100.66), o que pode ser verificado acedendo à configuração:

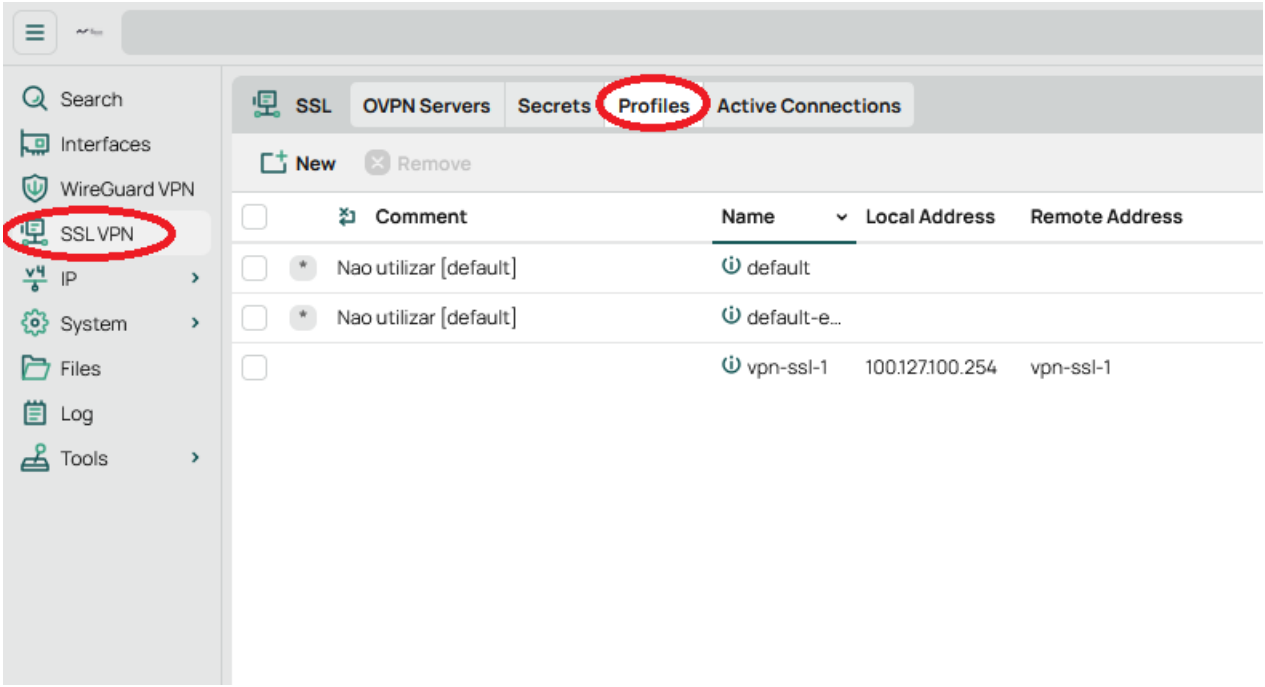


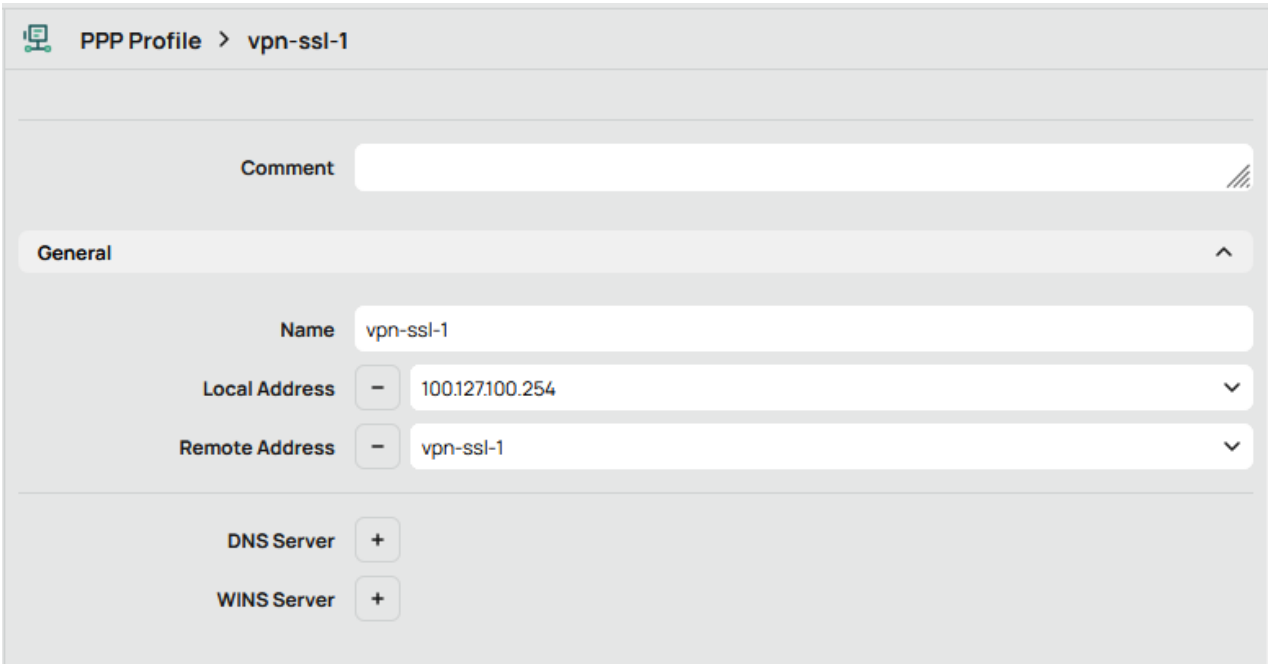


8.2 Perfil VPN

O passo seguinte obriga à criação de um perfil VPN que já se encontra criado no serviço entregue.

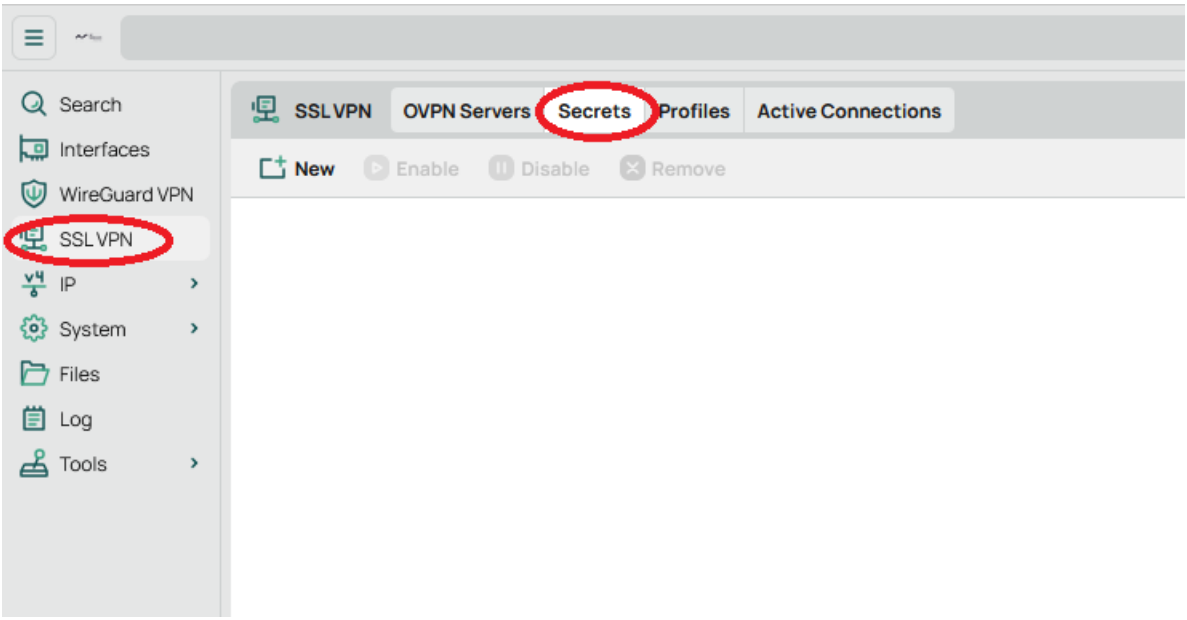
Para o verificar, aceder ao menu lateral esquerdo e clicar em SSL VPN e depois no tab Profiles:



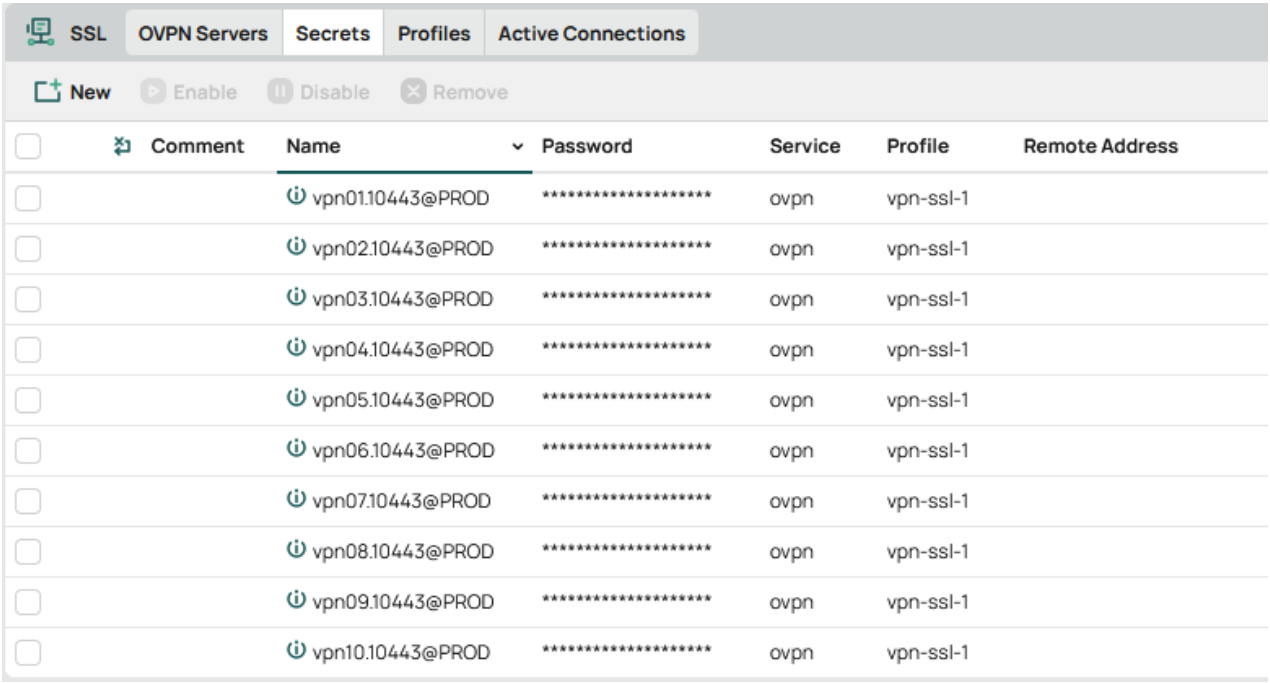


8.3 Utilizadores da VPN

Para gerir os utilizadores VPN ir ao menu lateral esquerdo e clicar em SSL VPN e depois no tab Secrets:



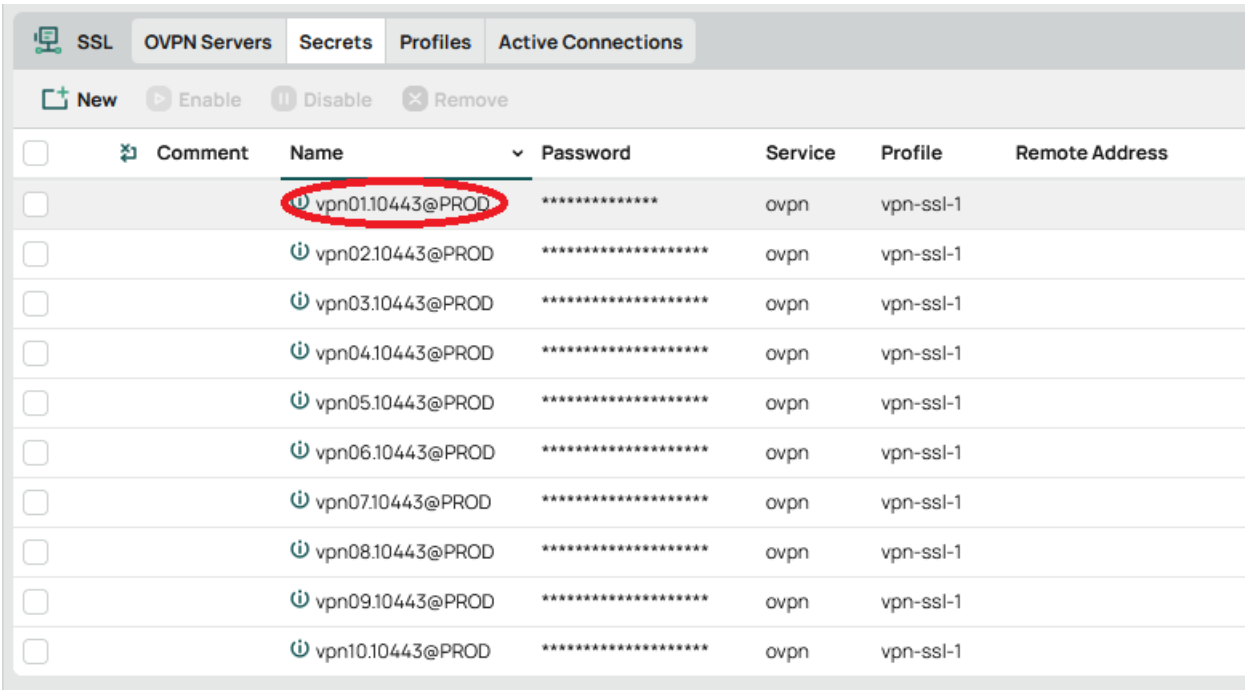
Podemos verificar que existem já dez utilizadores pré-criados, prontos a ser usados:

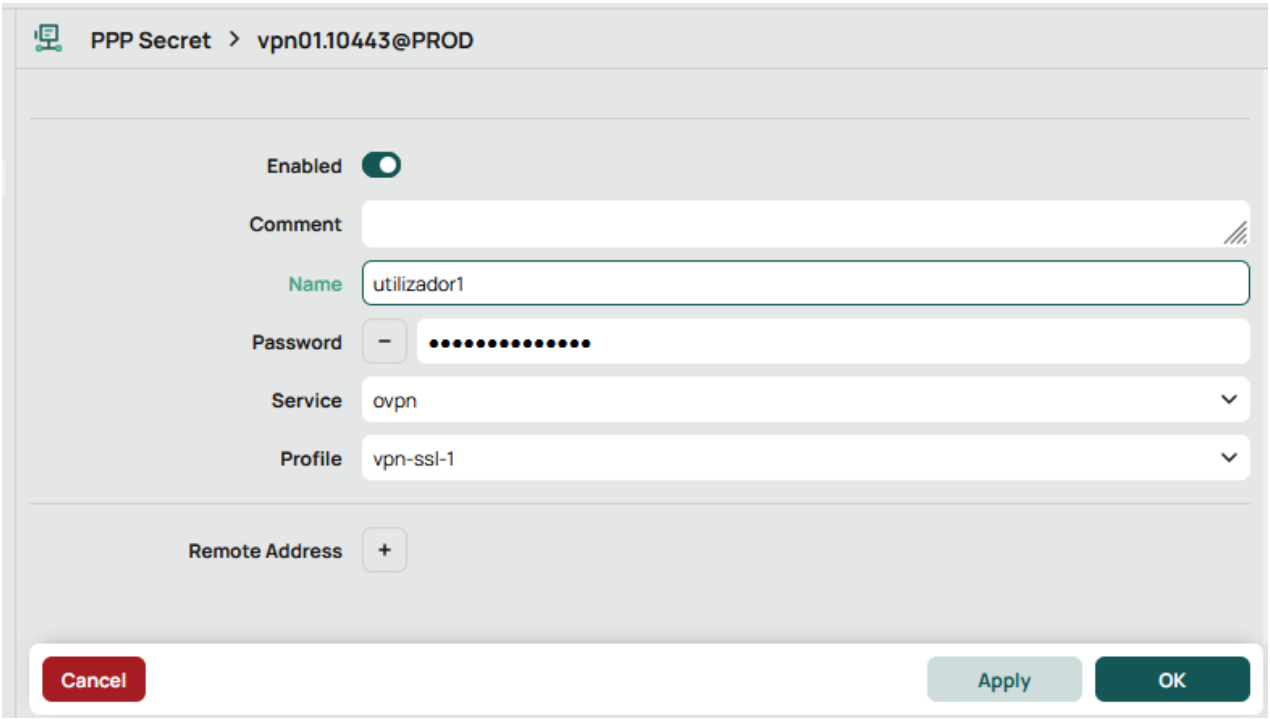


Comment	Name	Password	Service	Profile	Remote Address
	vpn01.10443@PROD	**********	ovpn	vpn-ssl-1	
	vpn02.10443@PROD	**********	ovpn	vpn-ssl-1	
	vpn03.10443@PROD	**********	ovpn	vpn-ssl-1	
	vpn04.10443@PROD	**********	ovpn	vpn-ssl-1	
	vpn05.10443@PROD	**********	ovpn	vpn-ssl-1	
	vpn06.10443@PROD	**********	ovpn	vpn-ssl-1	
	vpn07.10443@PROD	**********	ovpn	vpn-ssl-1	
	vpn08.10443@PROD	**********	ovpn	vpn-ssl-1	
	vpn09.10443@PROD	**********	ovpn	vpn-ssl-1	
	vpn10.10443@PROD	**********	ovpn	vpn-ssl-1	

As passwords iniciais encontram-se disponíveis num ficheiro de configuração que iremos ver mais à frente. Opcionalmente podemos alterar a password e o nome.

Para o fazer, clicar no utilizador pretendido e preencher o quadro que aparece:





Terminar com Apply e OK.

8.4 Servidor OVPN

O servidor OVPN está já configurado e ativo.

Para verificar a configuração, aceder a SSL VPN, depois no tab OVPN Servers e carregar na configuração existente:

Aqui devemos ter em atenção o seguinte:

- Redirect Gateway - existem duas opções: disabled e def1

  Full tunnel VPN – def1

  Nesta configuração todo o tráfego do cliente será redirecionado para o túnel. Isto implica que se o cliente quiser aceder à internet, terá de criar uma regra de firewall que permita o tráfego.

  Split tunnel VPN – disabled

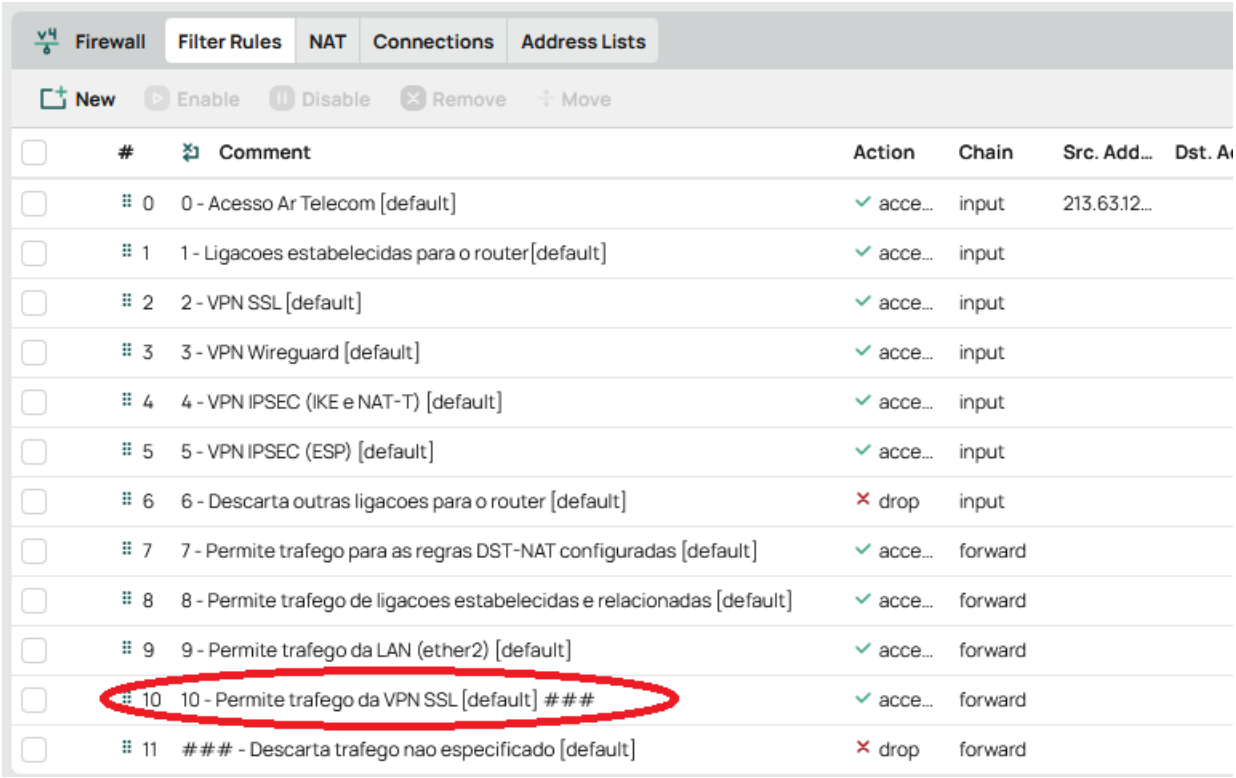
  Nesta configuração apenas o tráfego para as redes explicitamente indicadas passa pelo túnel, saindo todas as outras pelo default gateway, nomeadamente, o acesso à internet. É necessário criar uma regra de firewall que permita o tráfego para as redes internas.

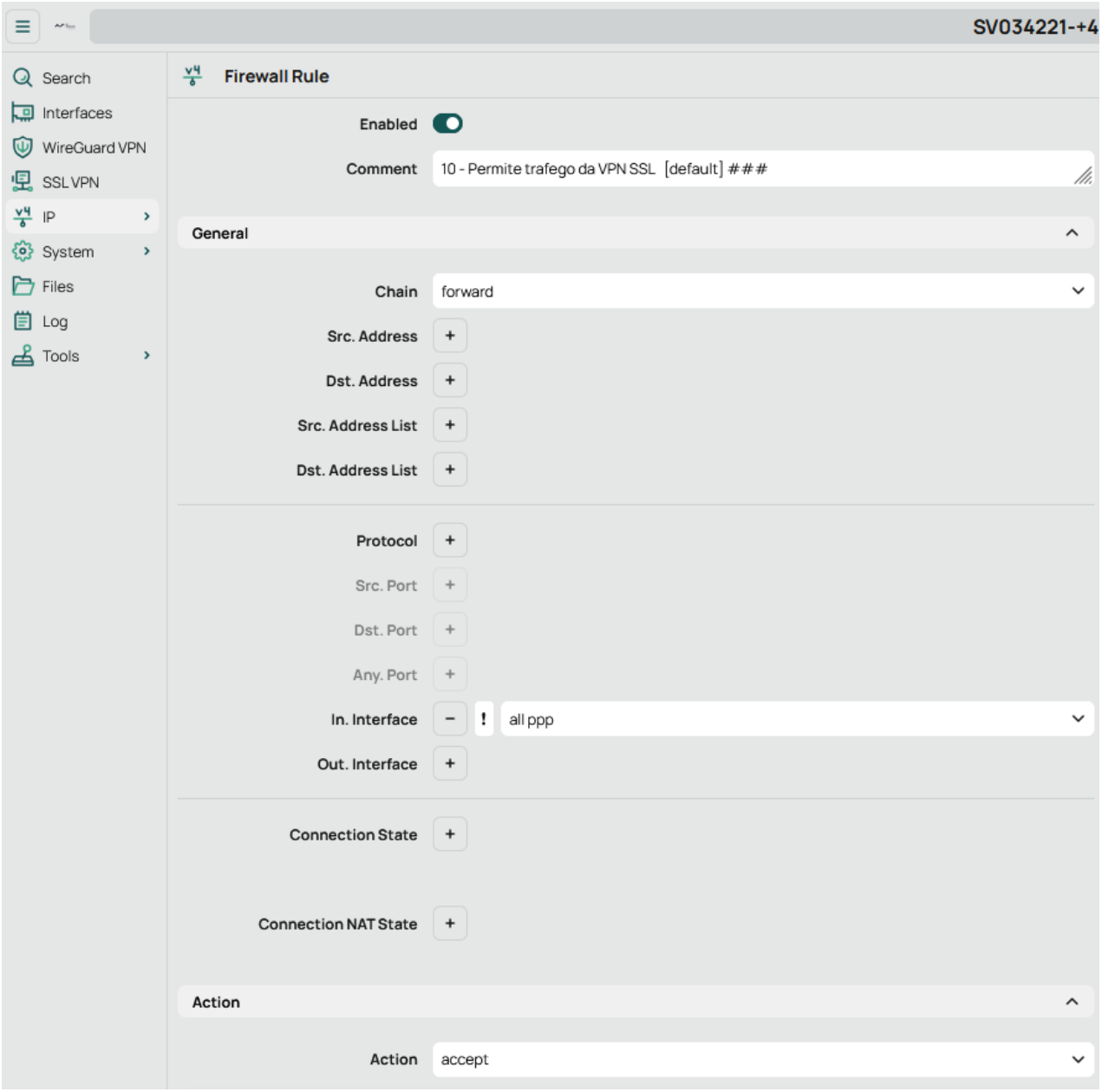
- Push Routes: no caso de configuração em Split tunnel é necessário informar ao cliente a que redes remotas se pode ligar, ou seja, para que redes o tráfego deve ser redirecionado pelo túnel. No nosso exemplo, usamos a configuração Split tunnel sendo a rede no VDC a 192.168.100.0/24.

8.5 Regras de firewall

Estando o túnel configurado, é necessário permitir o tráfego do túnel para as redes internas.

A regra de firewall que o permite encontra-se já configurada:



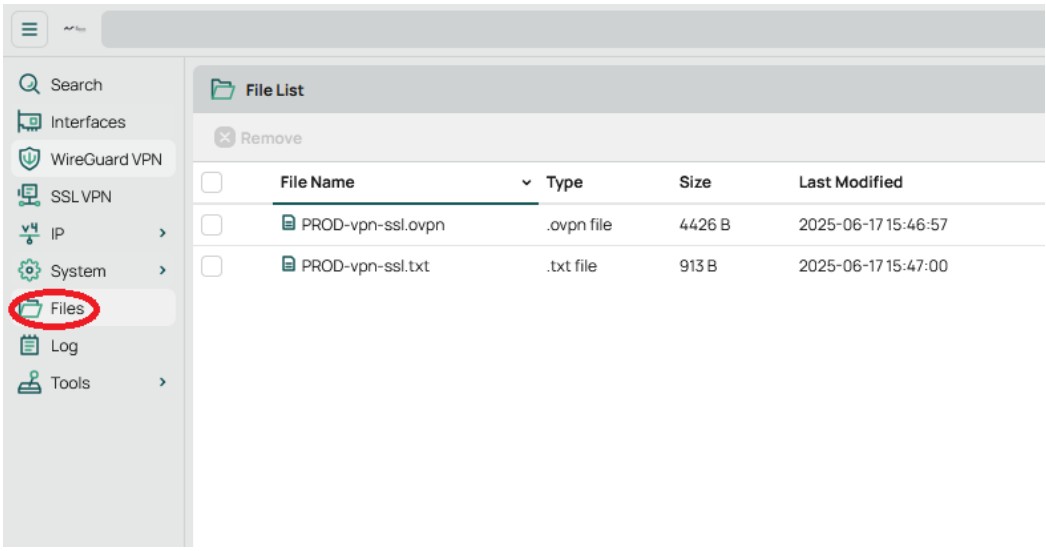


8.6 Configuração dos dispositivos remotos

Todos os clientes OpenVPN irão utilizar a mesma configuração e o mesmo certificado de cliente, distinguindo-se entre si pelo conjunto de credencias utilizador/password indicados atrás.

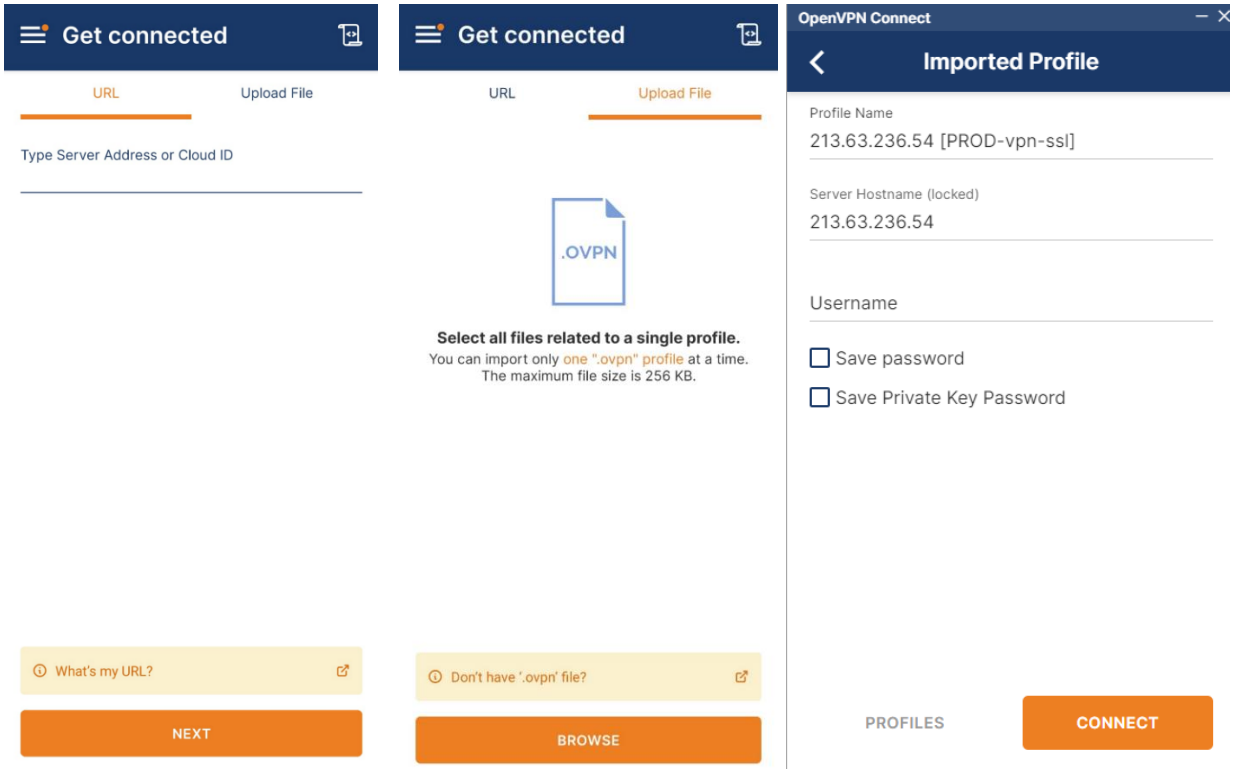
Para facilitar o processo de configuração dos clientes OpenVPN, o serviço Mikrotik é entregue pré-configurado com os parâmetros explicados anteriormente, e disponibiliza ainda dois ficheiros: um de configurações gerais do router e outro ficheiro de configuração .ovpn.

Para obter os ficheiros necessários para a configuração dos clientes OpenVPN, ir ao menu lateral esquerdo e escolher Files:

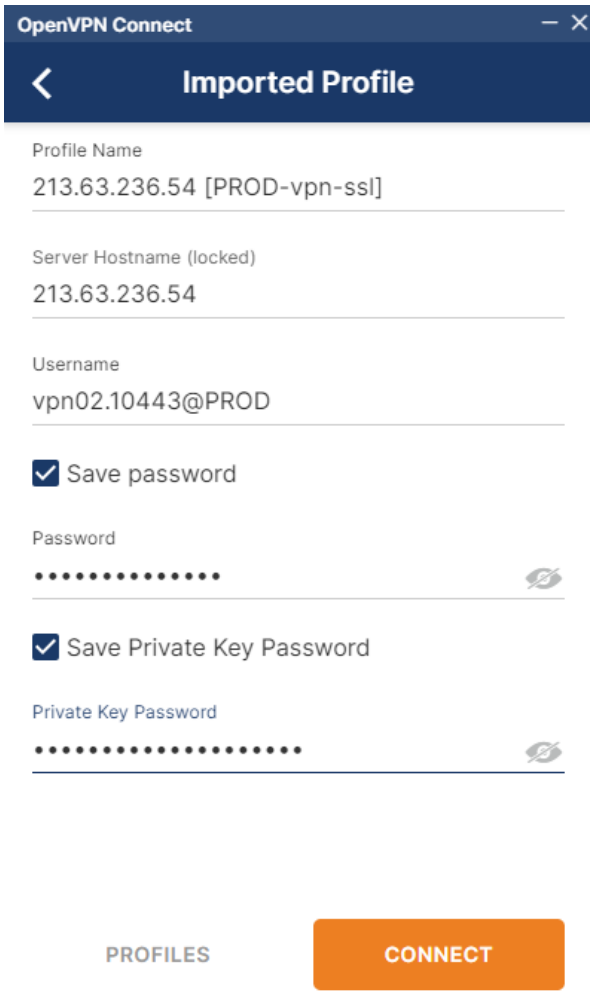


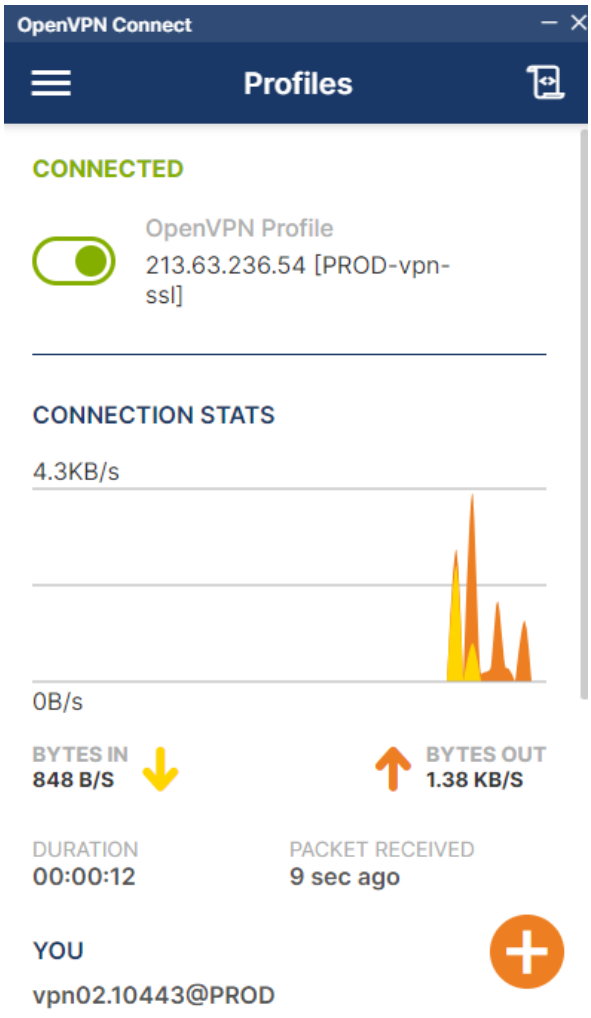
Aqui pode verificar a existência dos mesmos e descarregá-los.

Para configurar os clientes OpenVPN, é necessário importar o ficheiro .ovpn. Nas imagens abaixo mostra-se o exemplo no caso da aplicação OpenVPN Connect, igual para Windows e Android:



Depois de importado o ficheiro .ovpn é necessário introduzir o utilizador e respetiva password, assim como a chave privada da ligação. Estes dados podem ser encontrados no ficheiro [*vApp*]-vpn-ssl.txt.

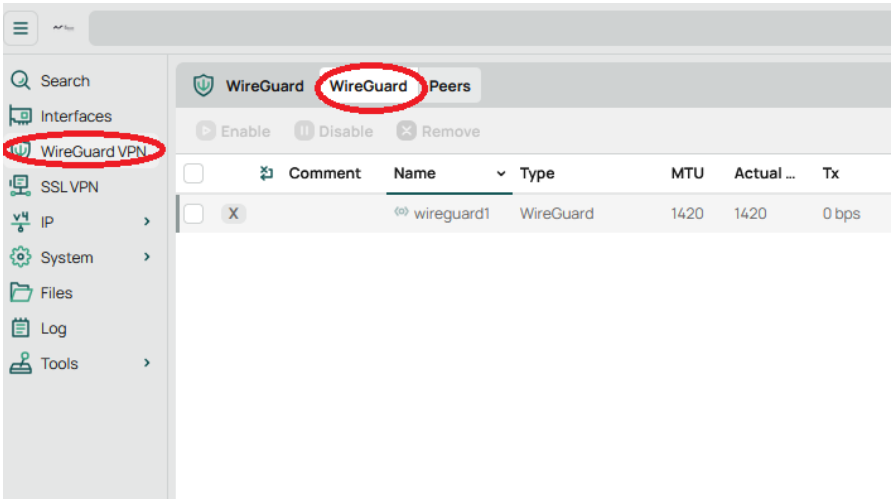




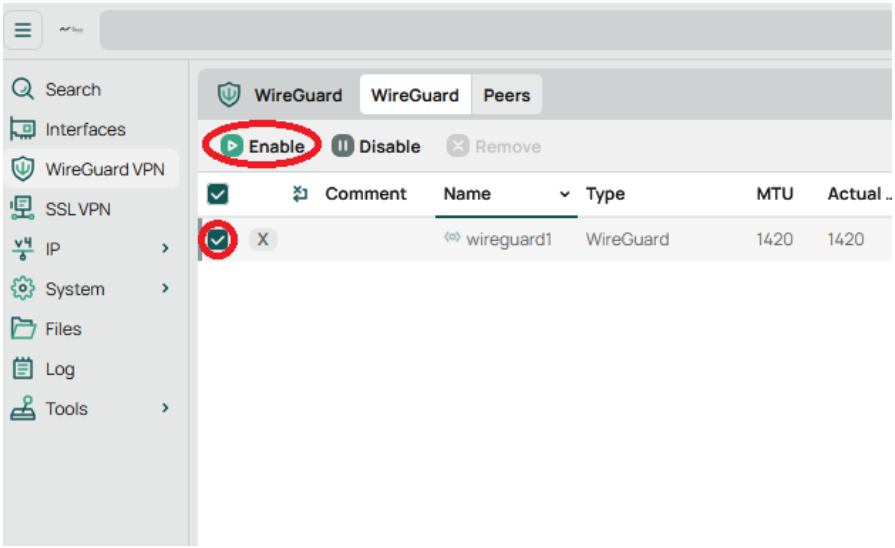
9. WIREGUARD

9.1 Interface Wireguard

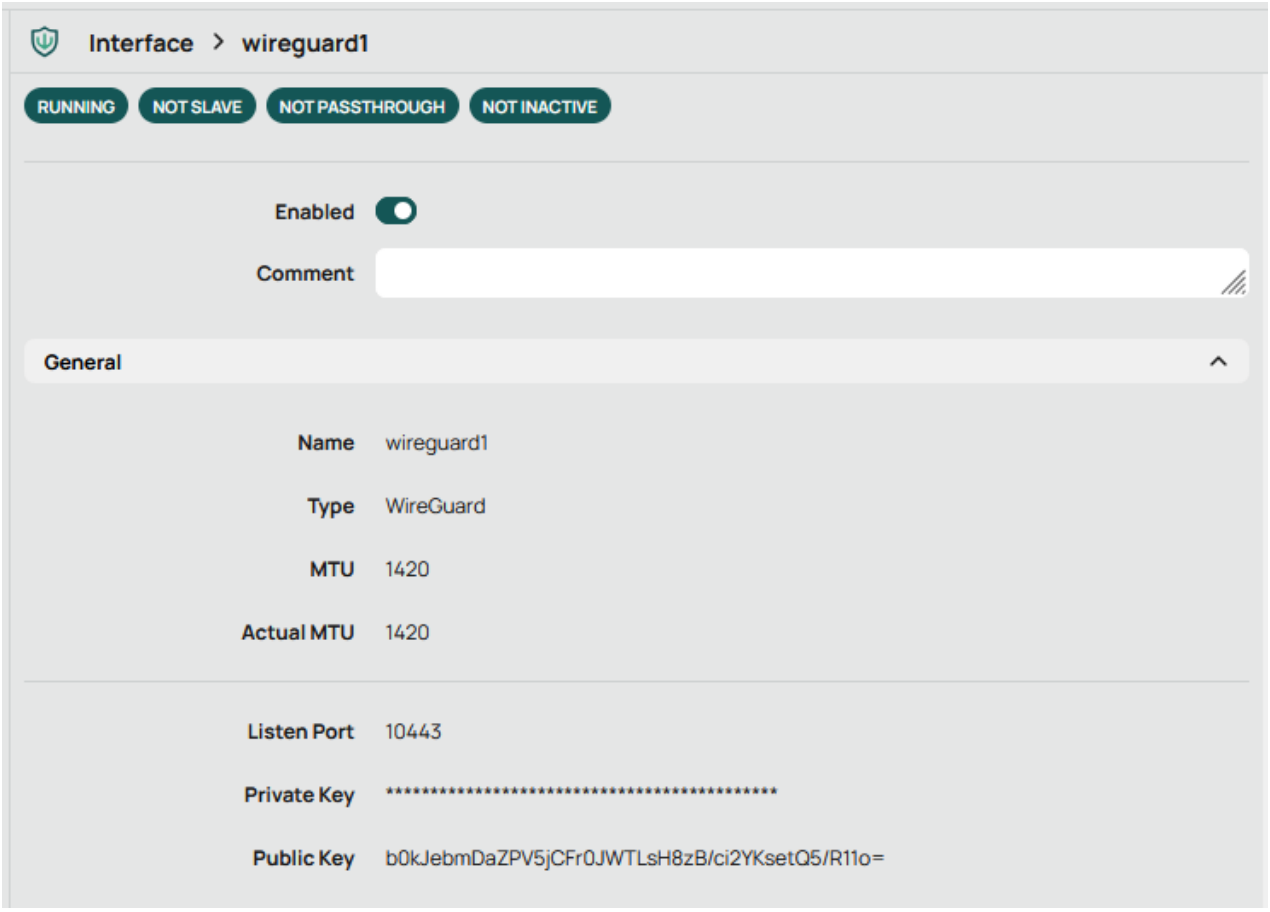
Para simplificar configurações WireGuard, o router Mikrotik é disponibilizado já com uma interface WireGuard criada. Esta interface encontra-se desabilitada por razões de segurança, mas pode ser ativada quando necessário. Para verificar a configuração e/ou ativar a interface, ir ao menu lateral esquerdo e clicar em WireGuard VPN, tab WireGuard:



Para ativar a interface, basta selecioná-la e clicar em **Enable**.

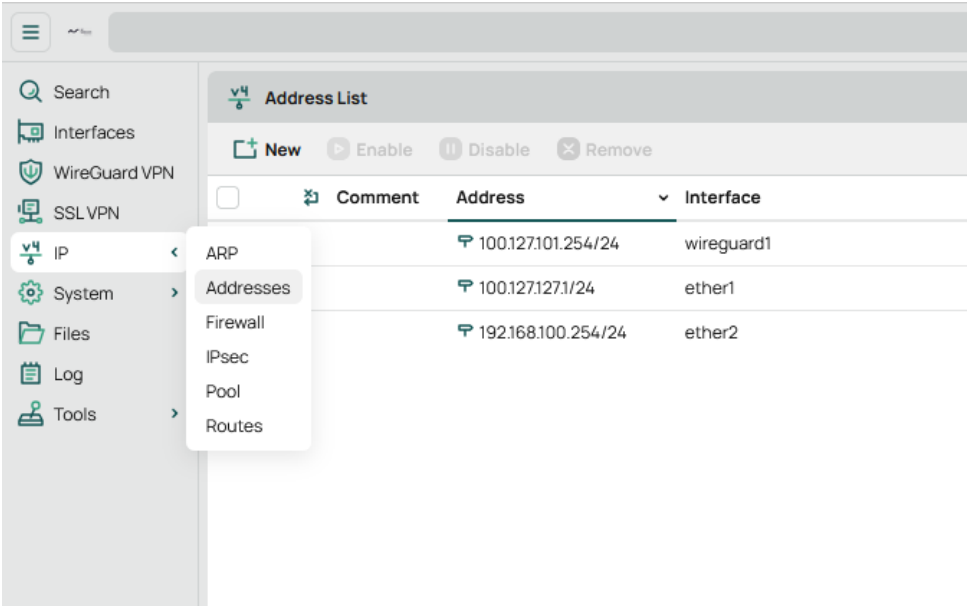


Para ver a configuração basta clicar sobre a interface:



9.2 Endereçamento IP da interface Wireguard

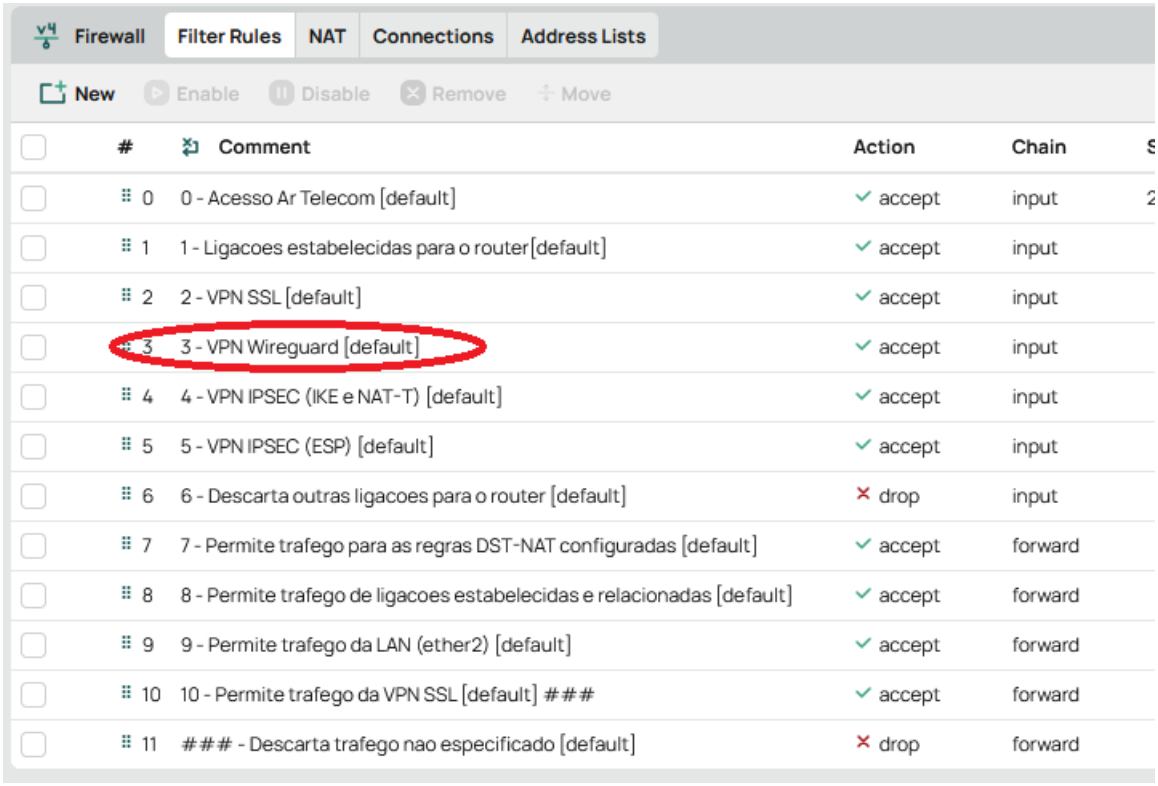
A interface WireGuard necessita de um endereço IP associado, o que é feito durante o processo de provisão. Para verificar o endereçamento utilizado, ir ao menu e clicar em IP -> Addresses:



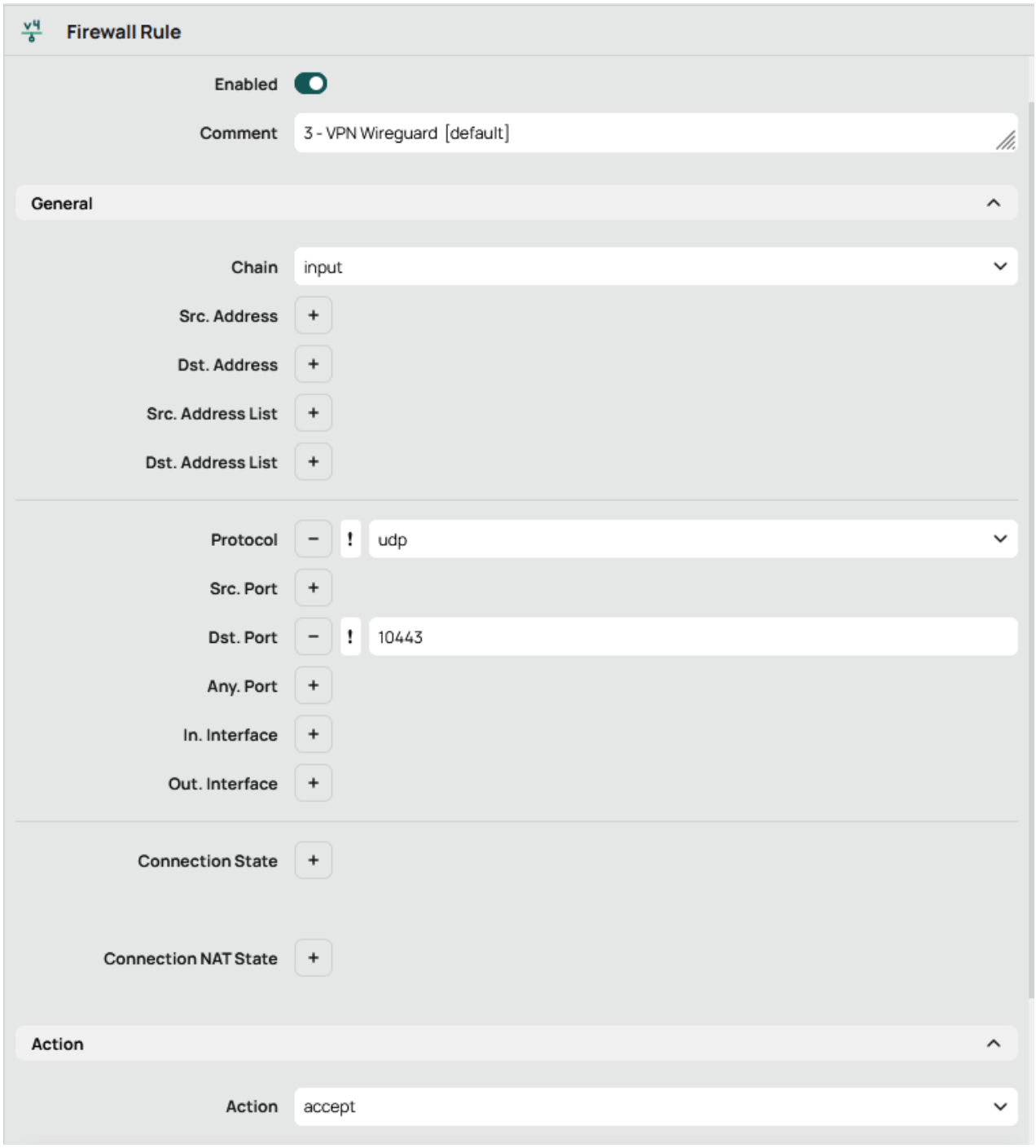
9.3 Regras de firewall

Estando o túnel configurado, é necessário permitir o tráfego WireGuard. Para isso são necessárias duas regras: uma para permitir entrada de tráfego WireGuard e outra para permitir tráfego WireGuard para a(s) rede(s) interna(s). Estas regras estão já criadas e ativas, como se pode ver na configuração, indo ao menu lateral esquerdo e clicar IP -> Firewall -> tab Filter Rules:

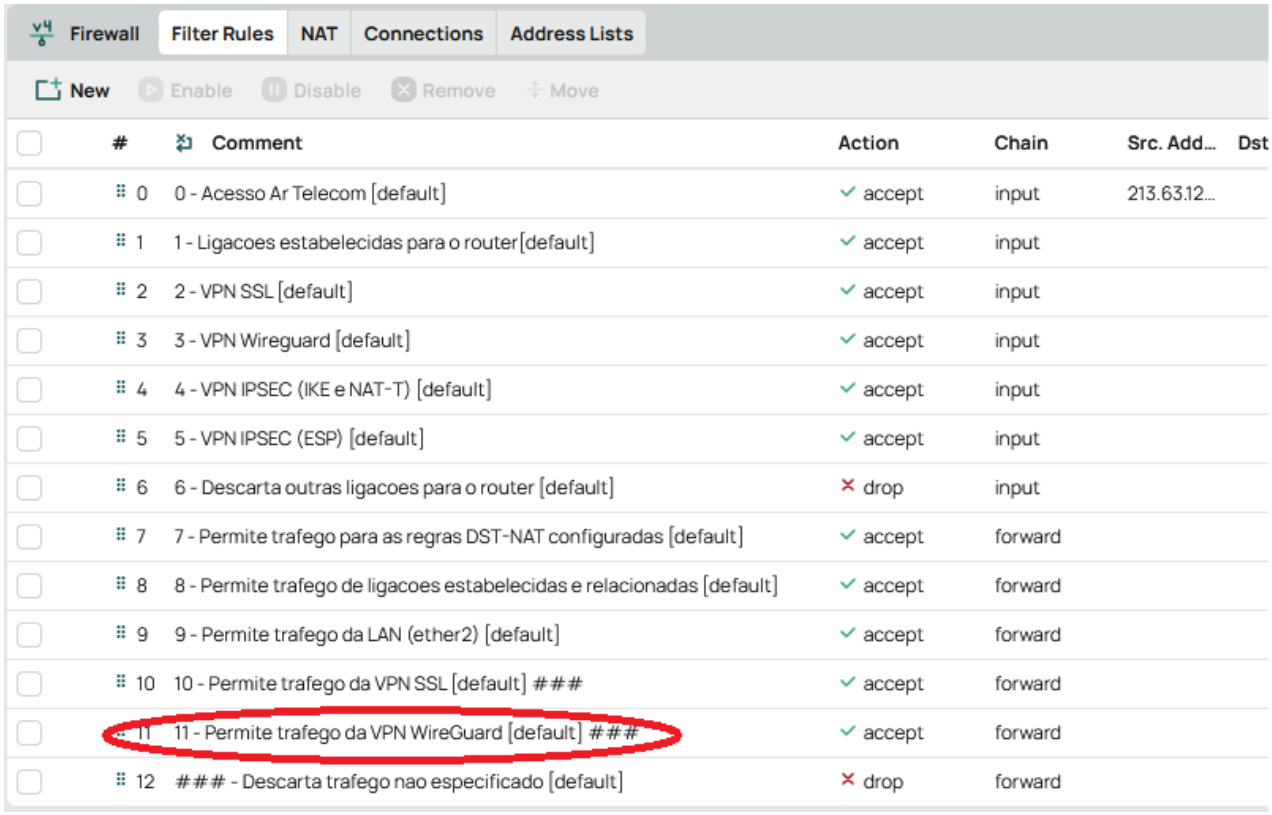
Regra 1: permitir tráfego WireGuard



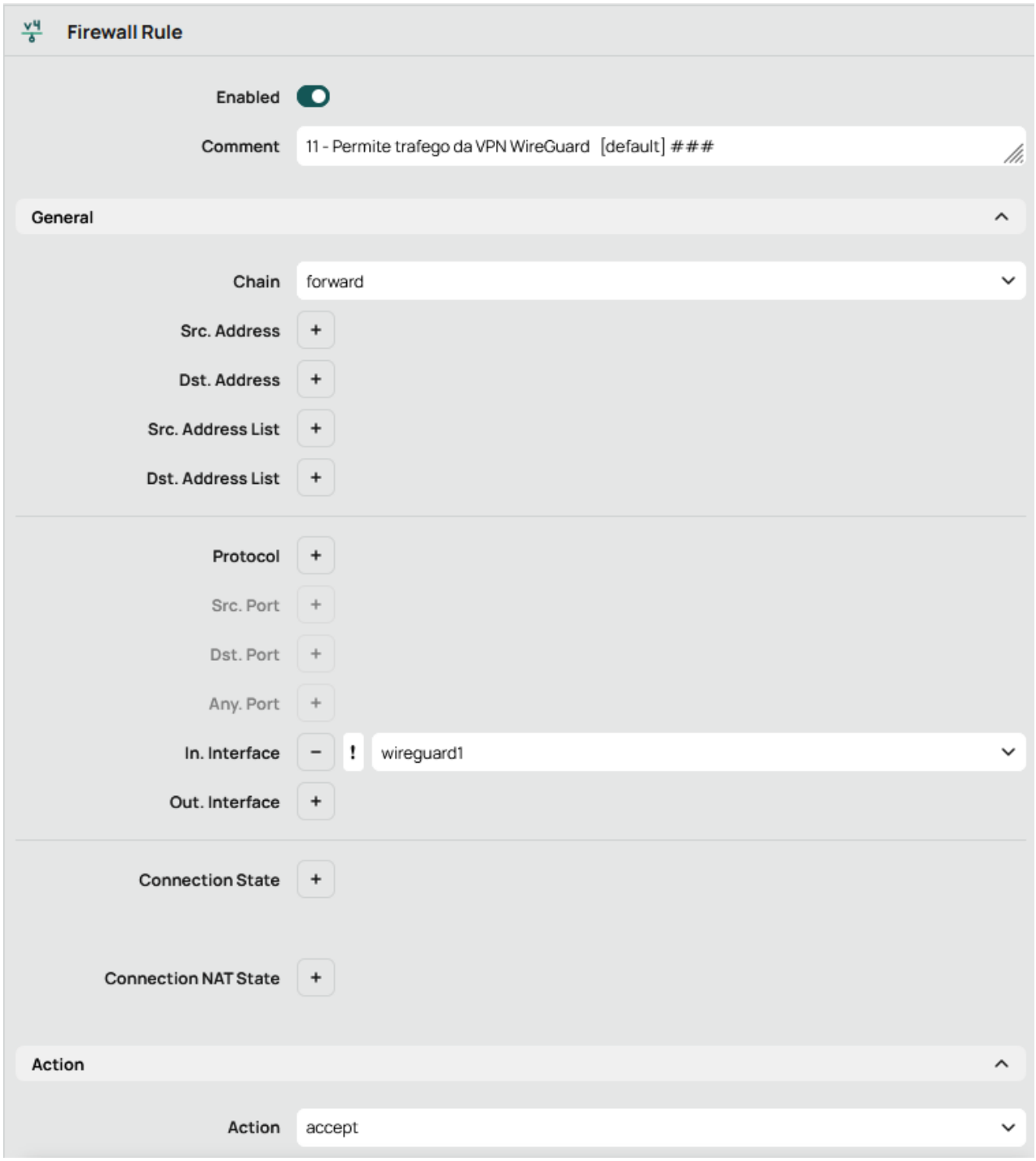
#	Comment	Action	Chain
0	0 - Acesso Ar Telecom [default]	accept	input
1	1 - Ligacoes estabelecidas para o router[default]	accept	input
2	2 - VPN SSL [default]	accept	input
3	3 - VPN Wireguard [default]	accept	input
4	4 - VPN IPSEC (IKE e NAT-T) [default]	accept	input
5	5 - VPN IPSEC (ESP) [default]	accept	input
6	6 - Descarta outras ligacoes para o router [default]	drop	input
7	7 - Permite trafego para as regras DST-NAT configuradas [default]	accept	forward
8	8 - Permite trafego de ligacoes estabelecidas e relacionadas [default]	accept	forward
9	9 - Permite trafego da LAN (ether2) [default]	accept	forward
10	10 - Permite trafego da VPN SSL [default] ###	accept	forward
11	### - Descarta trafego nao especificado [default]	drop	forward



Regra 2: permitir tráfego vindo do túnel WireGuard



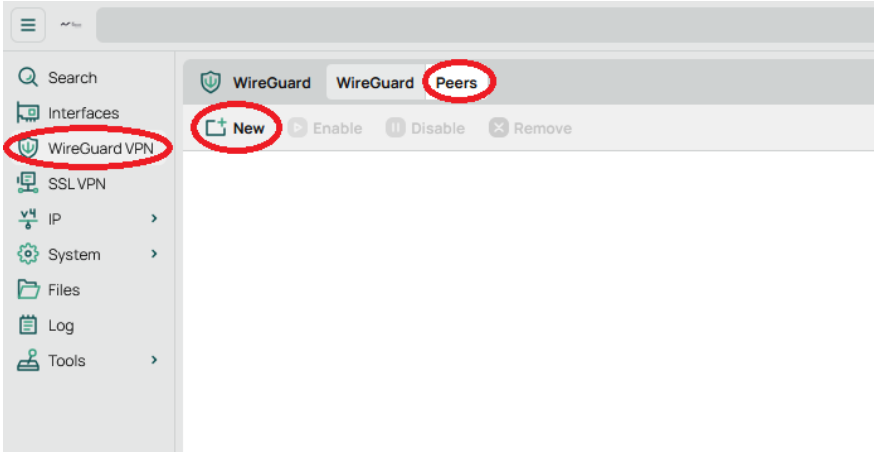
#	Comment	Action	Chain	Src. Add...	Dst
0	0 - Acesso Ar Telecom [default]	accept	input	213.63.12...	
1	1 - Ligacoes estabelecidas para o router[default]	accept	input		
2	2 - VPN SSL [default]	accept	input		
3	3 - VPN Wireguard [default]	accept	input		
4	4 - VPN IPSEC (IKE e NAT-T) [default]	accept	input		
5	5 - VPN IPSEC (ESP) [default]	accept	input		
6	6 - Descarta outras ligacoes para o router [default]	drop	input		
7	7 - Permite trafego para as regras DST-NAT configuradas [default]	accept	forward		
8	8 - Permite trafego de ligacoes estabelecidas e relacionadas [default]	accept	forward		
9	9 - Permite trafego da LAN (ether2) [default]	accept	forward		
10	10 - Permite trafego da VPN SSL [default] ###	accept	forward		
11	11 - Permite trafego da VPN WireGuard [default] ###	accept	forward		
12	### - Descarta trafego nao especificado [default]	drop	forward		



9.4 Configuração Road Warrior

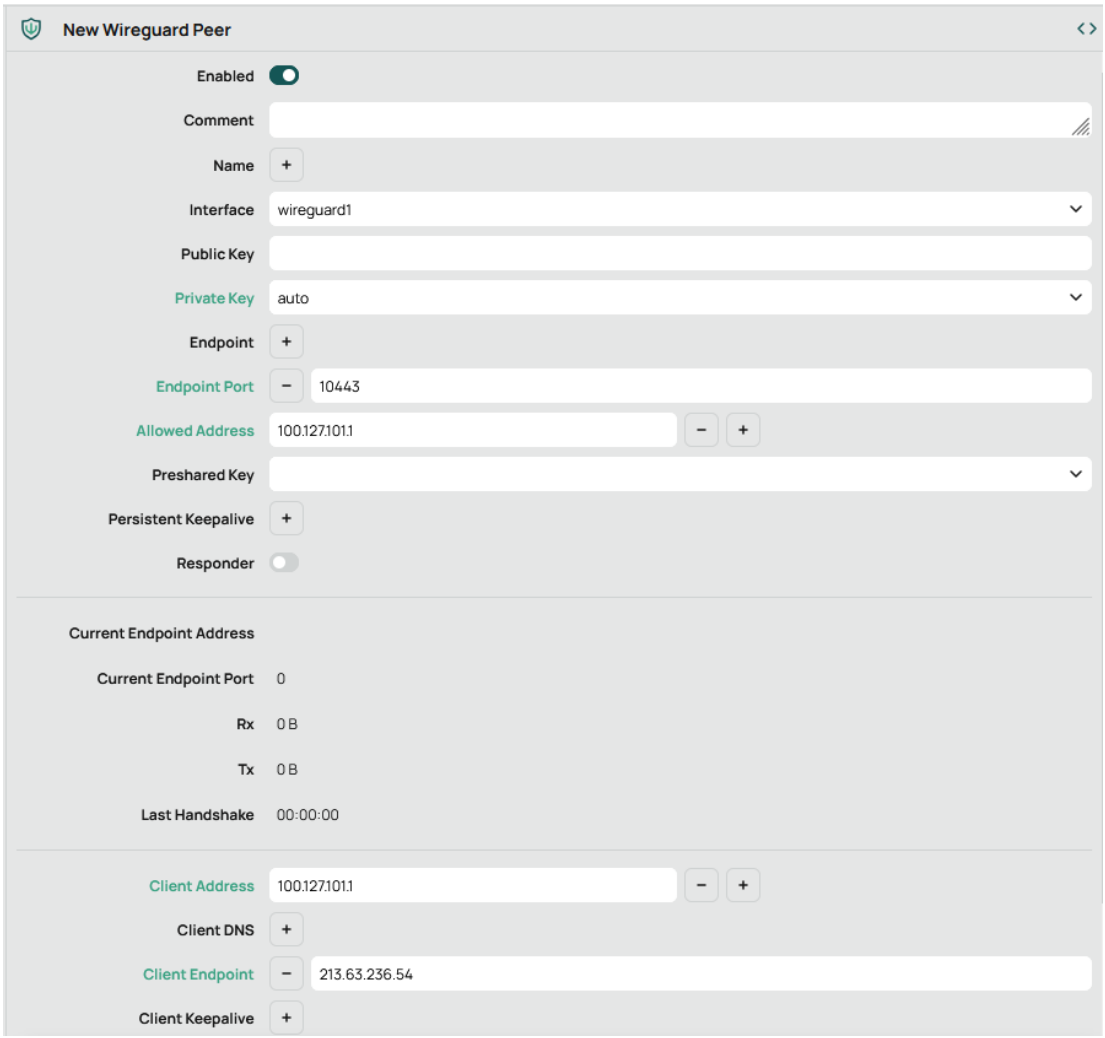
9.4.1 Configuração dos Peers no Mikrotik

Para adicionar um peer, ir ao menu lateral esquerdo, clicar em WireGuard VPN -> tab Peers e depois em New:



De seguida, configuram-se os parâmetros relevantes:

- Interface: a interface WireGuard a usar por este peer
- Name (opcional): a descrição deste peer
- Private key: selecionar auto para ser gerada automaticamente ao gravar a configuração
- Endpoint Port: a porta configurada na interface WireGuard, no nosso exemplo, 10443
- Allowed Address: um IP da rede do túnel a atribuir ao Peer, no nosso exemplo vamos usar 100.127.101.1
- Pre-shared key: opcional
- Client Address: o mesmo IP da rede do túnel configurado como Allowed Address, no nosso exemplo, 100.127.101.1
- Client Endpoint: o IP público que está associado ao Mikrotik

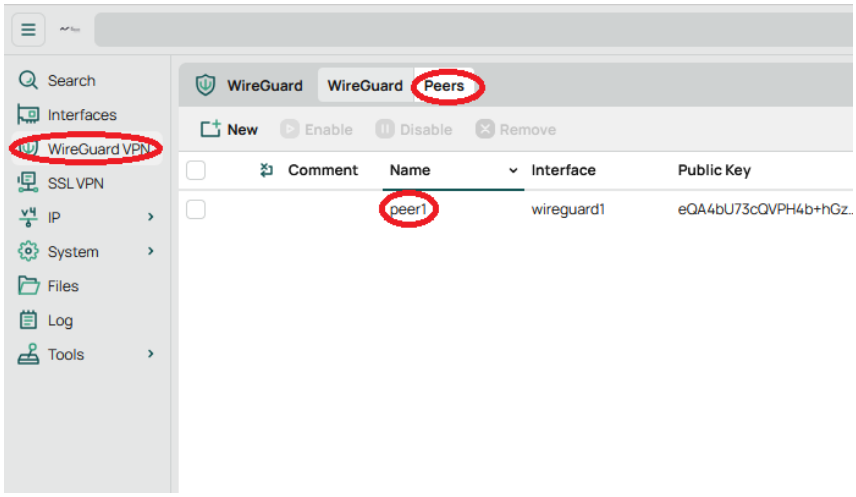


9.4.2 Configuração dos clientes

O cliente WireGuard para as diversas plataformas pode ser descarregado em https://www.wireguard.com/install

Dados para a configuração

Os dados necessários para a configuração dos clientes WireGuard podem ser encontrados no detalhe do Peer, acessível após a sua criação, acedendo ao menu lateral esquerdo e clicando em WireGuard VPN, tab Peers e depois no Peer que se pretende configurar:



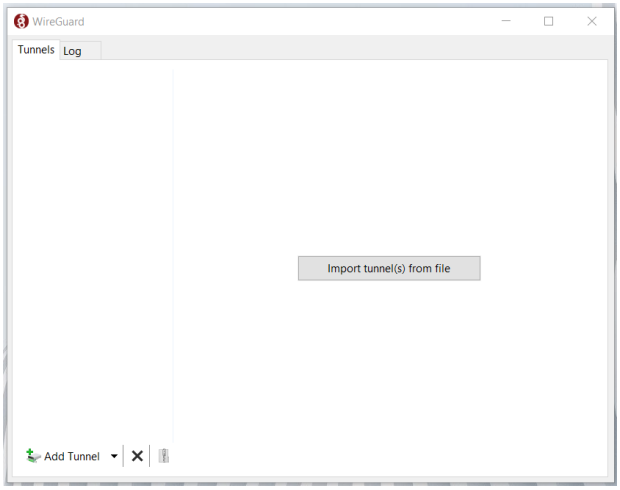
Na secção final dos detalhes é possível encontrar a configuração a efetuar nos clientes em modo texto e em código QR:

A configuração apresentada corresponde a um full-tunnel, ou seja, todo o tráfego do cliente é redirecionado para o túnel, inclusivamente o tráfego para a internet (AllowedIPs = 0.0.0.0/0). Nos exemplos apresentados não existe regra de firewall que o permita, pelo que, esse tráfego será bloqueado. Recomendamos que na configuração dos clientes (apresentada mais à frente) se substitua este parâmetro para que permita apenas o tráfego para a rede interna pretendida (nos exemplos deste manual, a rede 192.168.100.0/24).

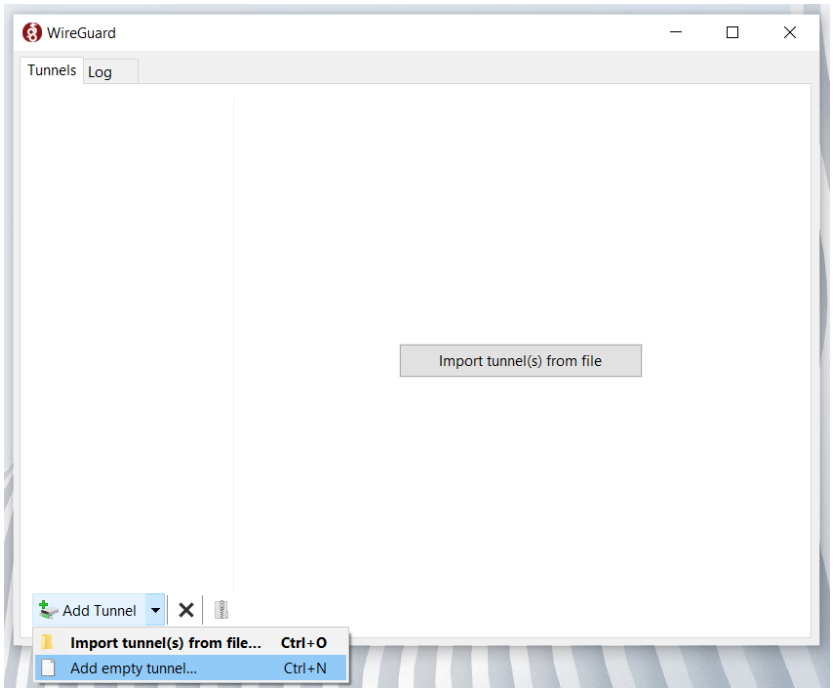
Esta página não permite copiar diretamente o texto para o clipboard. Sugerimos usar uma extensão de leitor de códigos QR no browser ou mudar para o modo "Reader View" no caso de estar a usar Firefox ou "Reading Mode" no caso de estar a usar o Chrome.

Cliente Windows

Após a instalação concluída, surge um quadro para configuração do túnel:

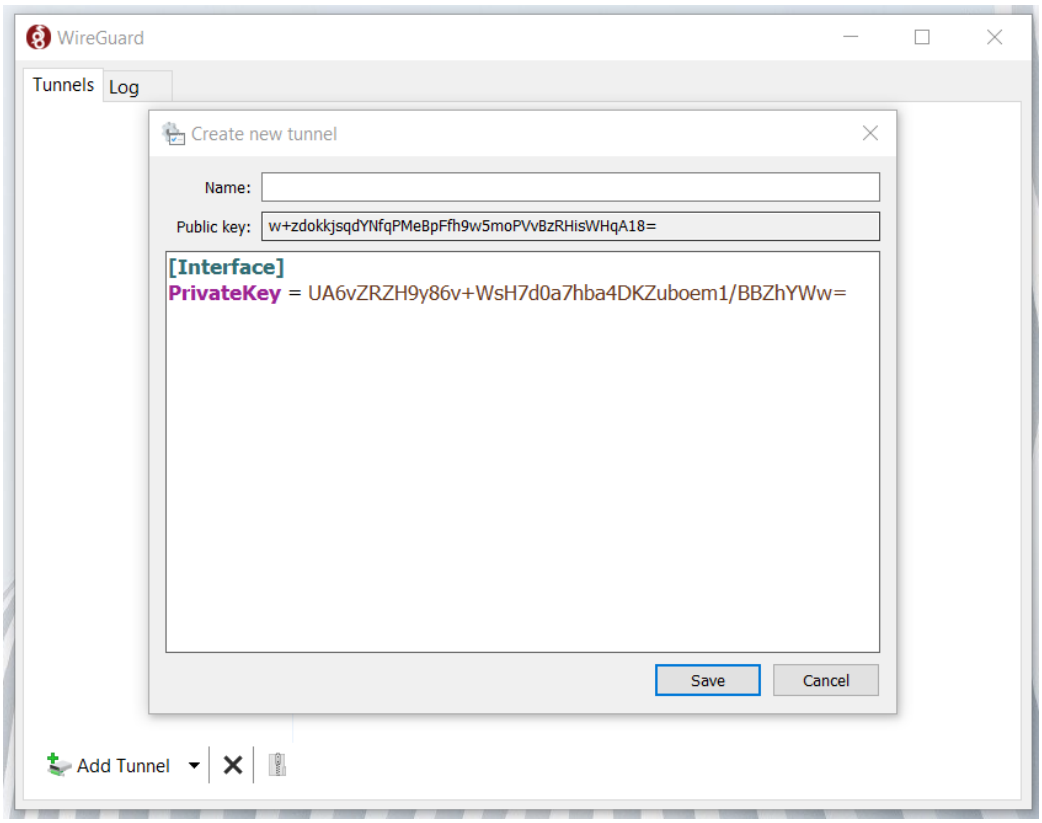


Como neste caso não existe ficheiro de configuração, devemos iniciar a criação do túnel expandindo o dropdown junto a "Add Tunnel" e escolher a opção "**Add empty tunnel...**":

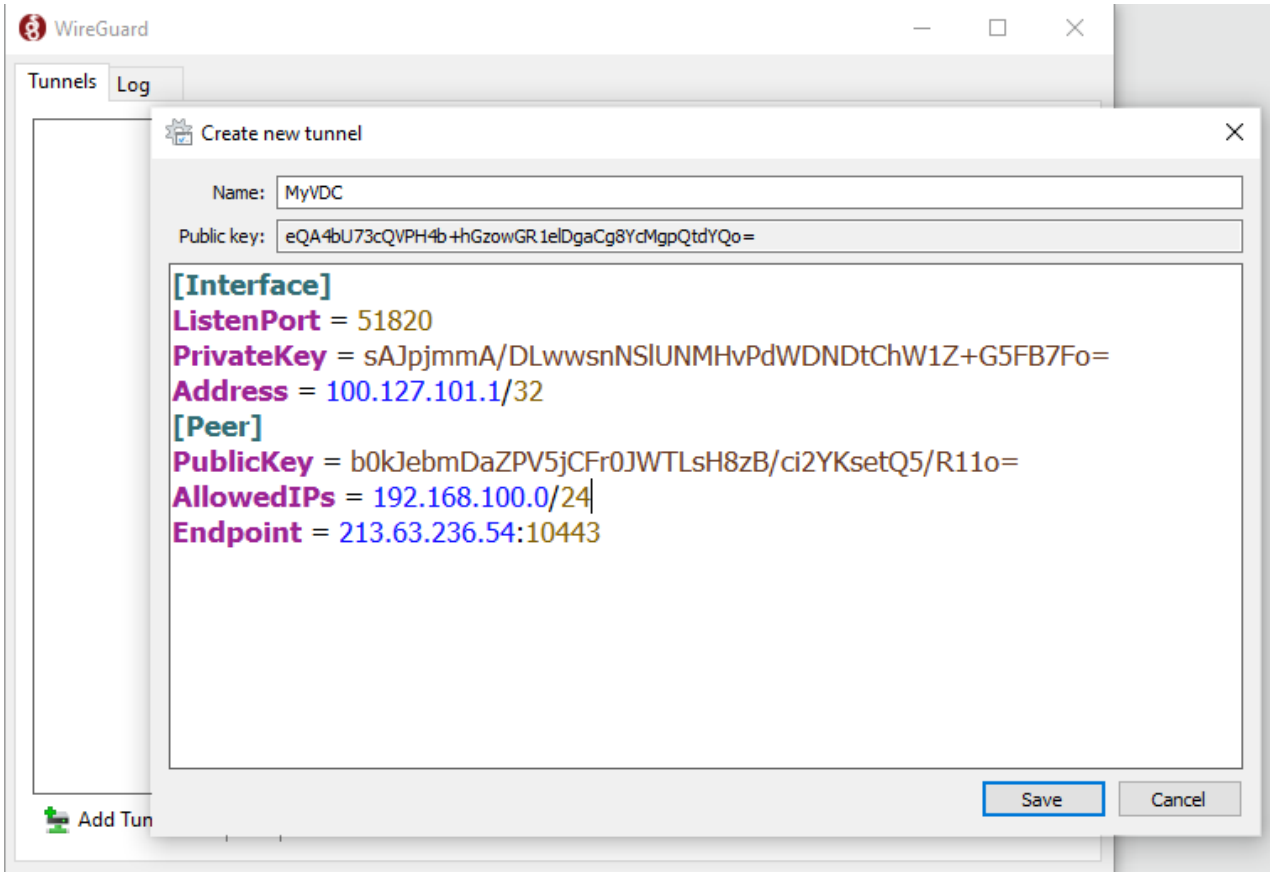


O processo de configuração é manual, mas bastante simples.

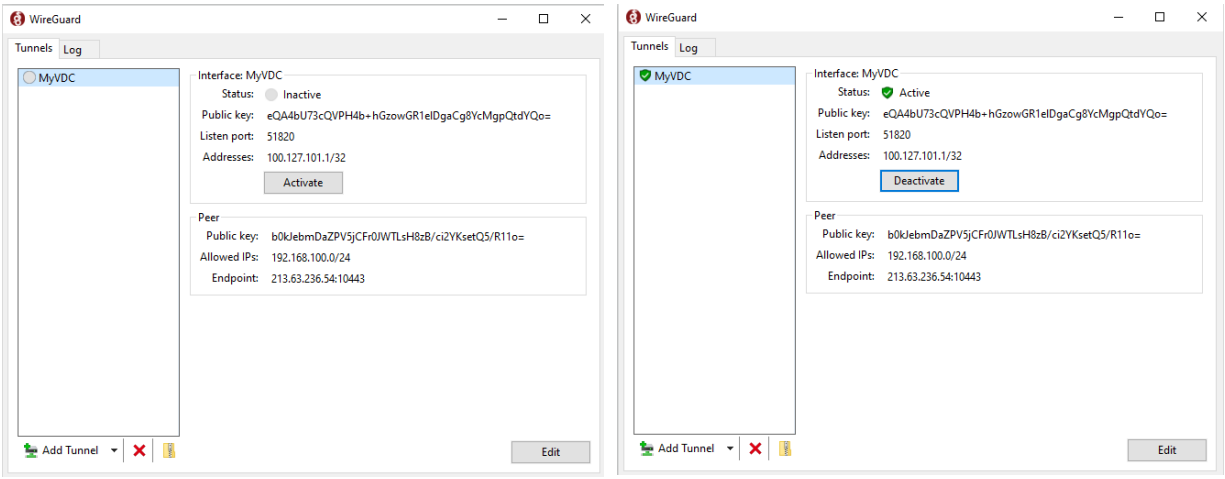
O quadro seguinte mostra a situação inicial, onde é necessário dar um nome e configurar a ligação VPN.



Aqui dá-se um nome à ligação, substitui-se o texto apresentado pelo copiado anteriormente do Peer e sugerimos modificar os AllowedIPs em conformidade, no nosso exemplo, 192.168.100.0/24



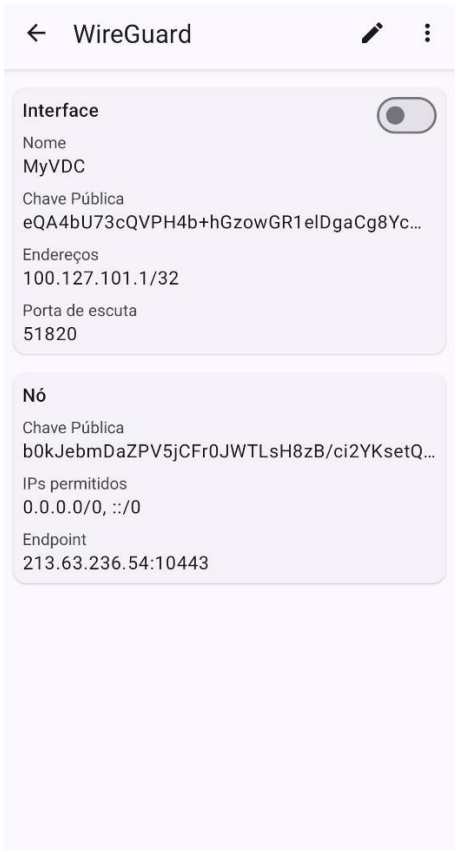
Fazendo Save o túnel encerra-se a configuração do túnel e é possível ativá-lo:



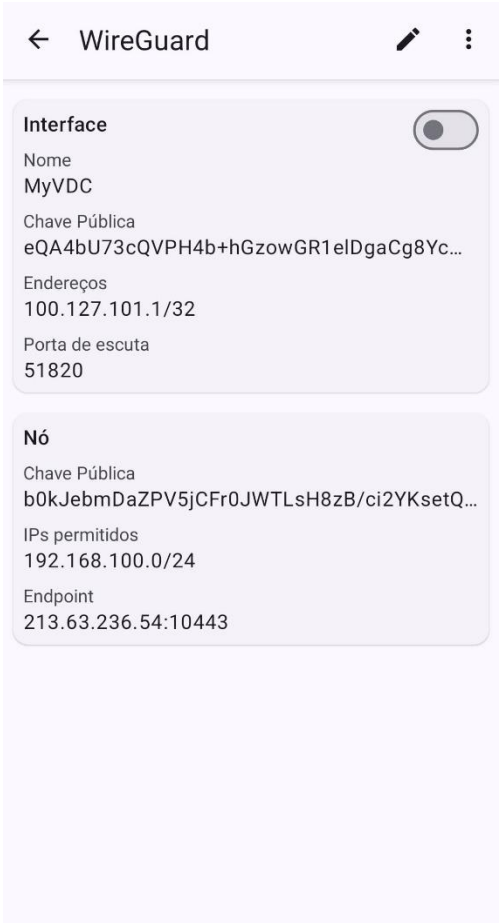
Cliente Android

Após a instalação da App concluída, surge um quadro para configuração do túnel. Clicando em "+" para criar a configuração de um novo túnel surgem as opções disponíveis, podendo carregar um ficheiro de configuração ou lendo um código QR:

O ficheiro de configuração é um ficheiro de texto com a extensão .conf cujo conteúdo é o mesmo que se utiliza para a configuração dos clientes Windows exemplificado anteriormente. Alternativamente, podemos digitalizar o código QR, sendo apenas necessário dar um nome à ligação.



Sugerimos editar a configuração e modificar os AllowedIPs em conformidade, no nosso exemplo, 192.168.100.0/24:



9.5 Configuração ponto a ponto

Também é possível configurar um router/firewall num site remoto para implementar um túnel permanente entre os dois.

Os parâmetros de configuração nos dois sites têm de estar perfeitamente concordantes, pelo que, recomendamos fazer um diagrama da solução e uma tabela prévia com as configurações a efetuar. De seguida apresenta-se, como exemplo, um diagrama de solução e respetivas configurações.

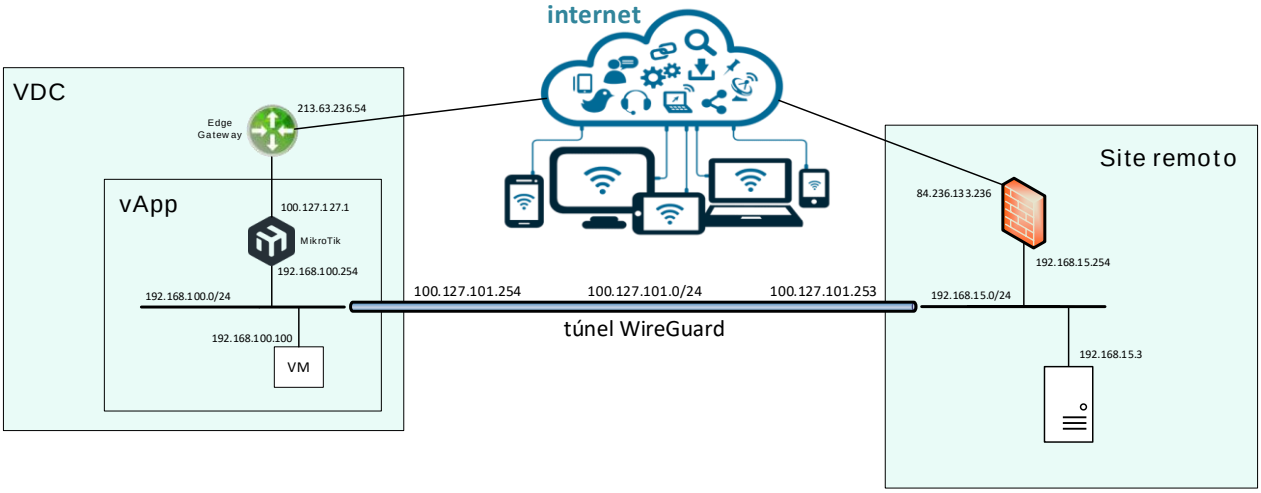


Tabela de configurações

Site VDC – Mikrotik no VDC	
IP público	213.63.236.54
IP rede trânsito	100.127.127.1
IP na rede do túnel	100.127.101.254
IP LAN local	192.168.100.254
LAN local	192.168.100.0/24
Public Key	a definir
Private Key	a definir

Site Remoto	
IP público	84.236.133.236
IP rede trânsito	n/a
IP na rede do túnel	100.127.101.253
IP LAN local	192.168.15.254
LAN local	192.168.15.0/24
Public Key	a definir
Private Key	a definir

WireGuard	
Porta	10443
Protocolo	UDP
Rede do túnel WireGuard	100.127.101.0/24

As chaves pública e privada no Mikrotik serão geradas ao criar a instância de WireGuard e terão de ser configuradas no dispositivo no site remoto.

A configuração do Peer no Mikrotik permite gerar as chaves ou introduzir chaves já existentes. A opção a utilizar depende do dispositivo remoto que se estiver a configurar, se permite introduzir as chaves geradas aqui ou se ele próprio as gera, sendo que neste último caso, teremos de as introduzir no Mikrotik.

9.5.1 Regras de firewall

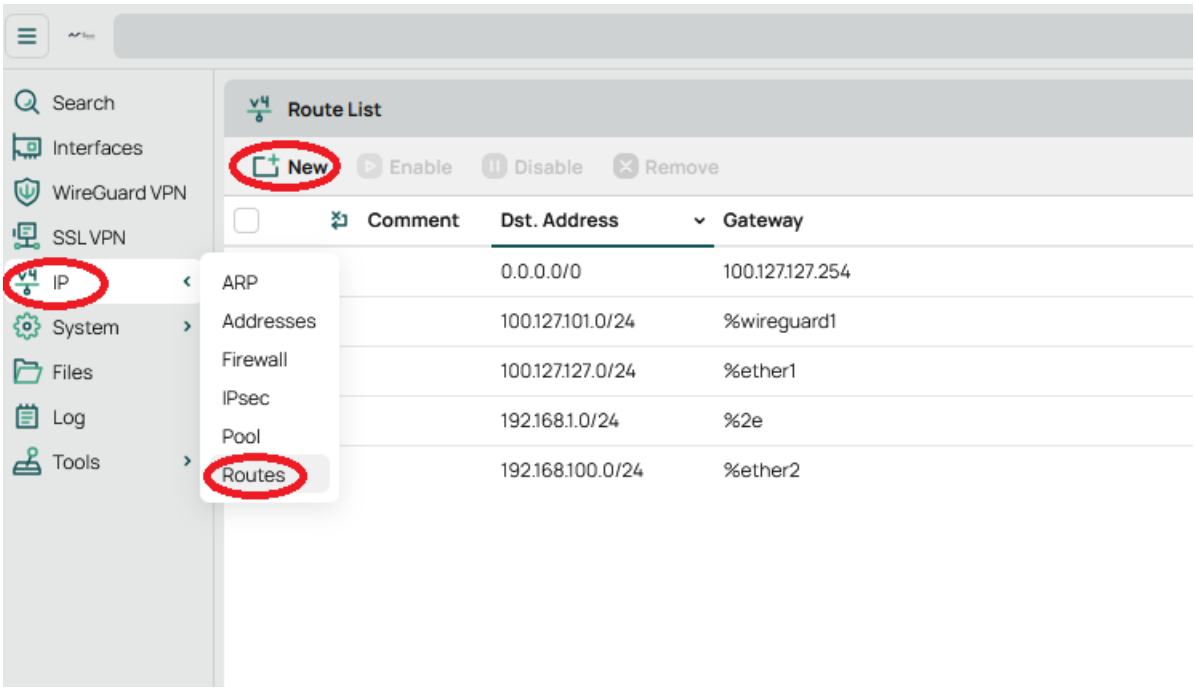
Além das regras de firewall criadas anteriormente, é necessário adicionar uma nova regra que permita a saída do tráfego WireGuard para a LAN remota.

Da mesma forma, no dispositivo remoto, é necessário criar uma regra que permita a entrada e saída de tráfego pela interface WireGuard.

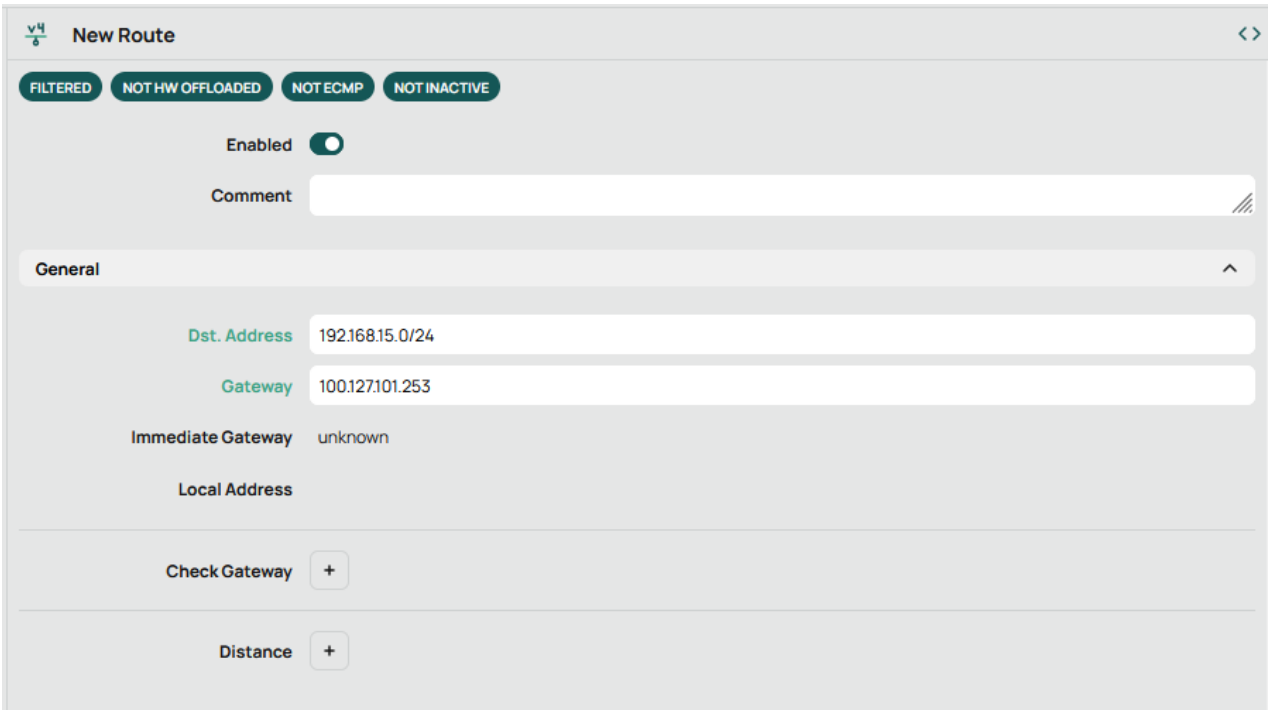
9.5.2 Configuração de rotas

Outro passo fundamental é a configuração do roteamento do tráfego com destino à LAN remota para o endereço IP do túnel no dispositivo remoto.

Para o fazer, aceder ao menu lateral esquerdo e em IP -> Routes fazer New:



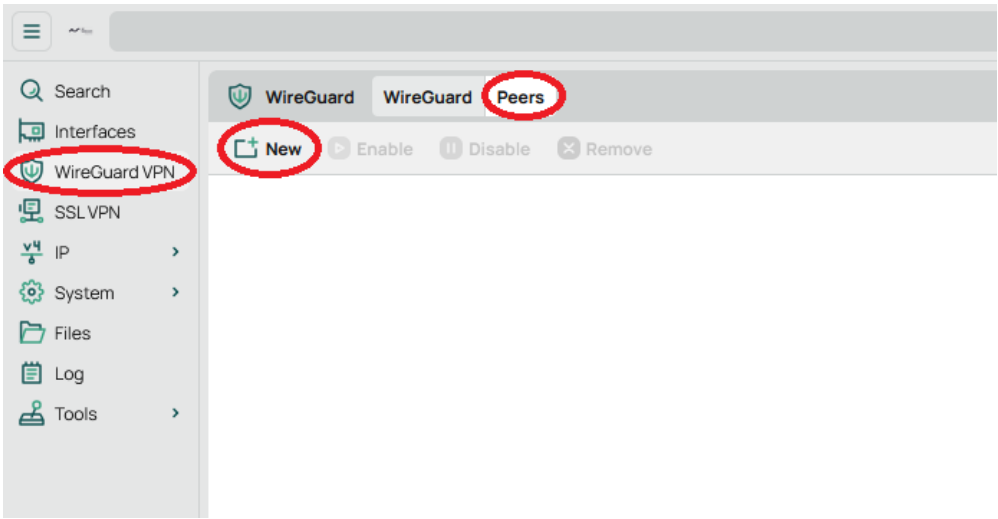
Configurar então uma rota de forma que o tráfego com destino à LAN remota seja encaminhado para o IP do túnel remoto (192.168.15.0/24 e 100.127.101.253 no nosso exemplo, respetivamente).



9.5.3 Configuração do Peer

No caso da configuração de um Peer com estabelecimento de túnel ponto a ponto vamos adicionar alguns parâmetros à configuração de Peer no Mikrotik.

Fazendo então WireGuard VPN -> tab Peers e depois em New:

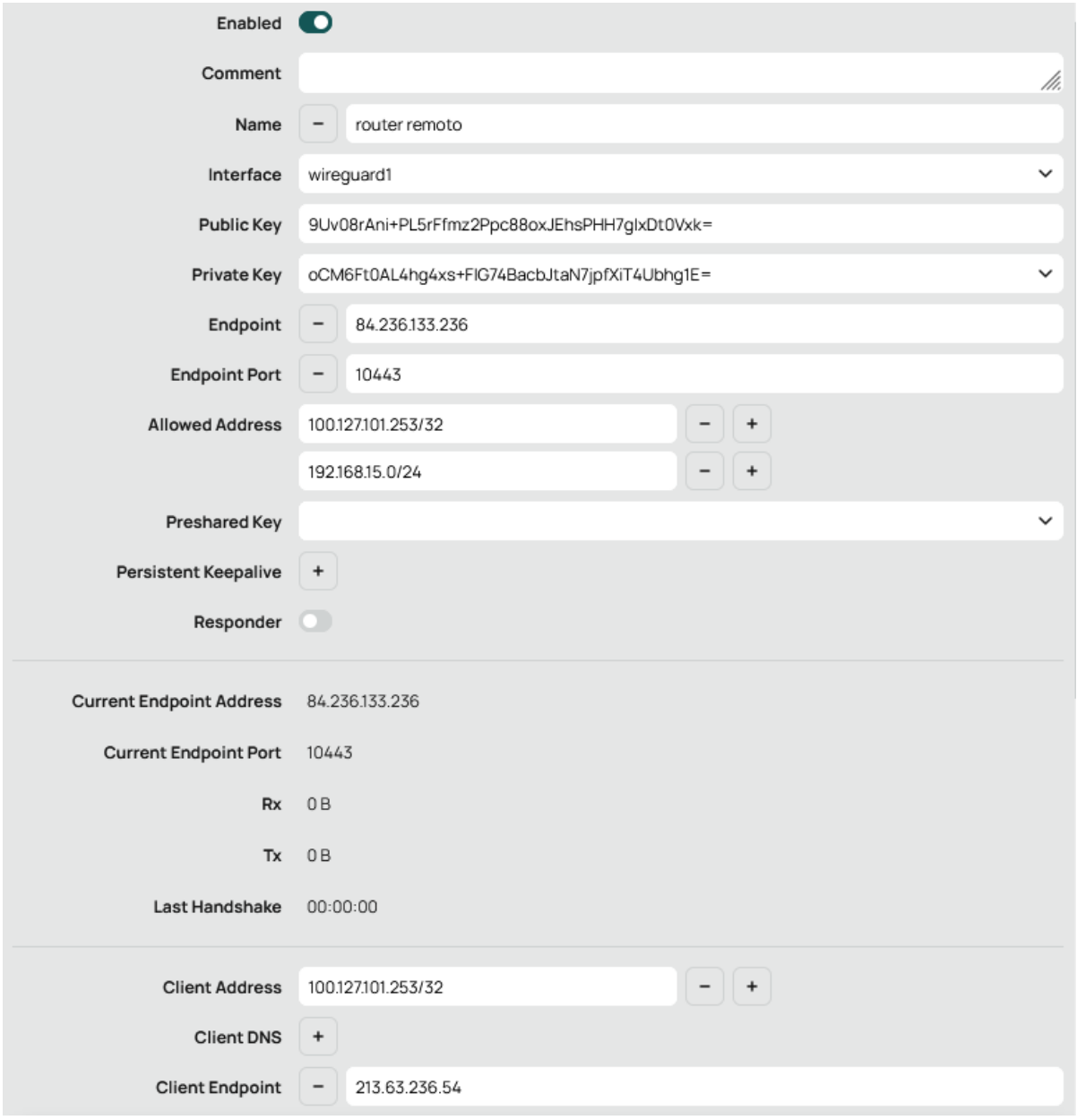


Configuramos os parâmetros como se exemplifica abaixo:

- Name (opcional): a descrição do dispositivo remoto
- Interface: a interface WireGuard a usar por este peer
- Public Key e Private Key: aqui podemos selecionar auto para serem gerados automaticamente ao gravar a configuração ou podemos introduzir as chaves já geradas no

dispositivo remoto. O importante lembrar é que as chaves pública e privada aqui introduzidas têm de ser as mesmas do serviço Wireguard no dispositivo remoto.

- Endpoint: o endereço IP público do dispositivo remoto
- Endpoint Port: a porta configurada no interface WireGuard, no nosso exemplo, 10443
- Allowed Address:
    - o IP da rede do túnel no dispositivo remoto, no nosso exemplo 100.127.101.253
    - a rede LAN no dispositivo remoto, no nosso exemplo 192.168.15.0/24
- Client Address: o mesmo IP da rede do túnel configurado como Allowed Address, no nosso exemplo, 100.127.101.253
- Client Endpoint: o IP público que está associado ao Mikrotik



10. IPSEC VPN SITE-TO-SITE

Uma ligação site-to-site IPsec permite a conetividade de rede entre dois locais com IPs públicos fixos e em que as redes a ligar têm endereçamentos distintos. Os parâmetros de configuração nos dois sites têm de estar perfeitamente concordantes, pelo que, recomendamos fazer um diagrama da solução e uma tabela prévia com as configurações a efetuar. No exemplo usado neste manual vamos considerar os parâmetros como se indicam abaixo.

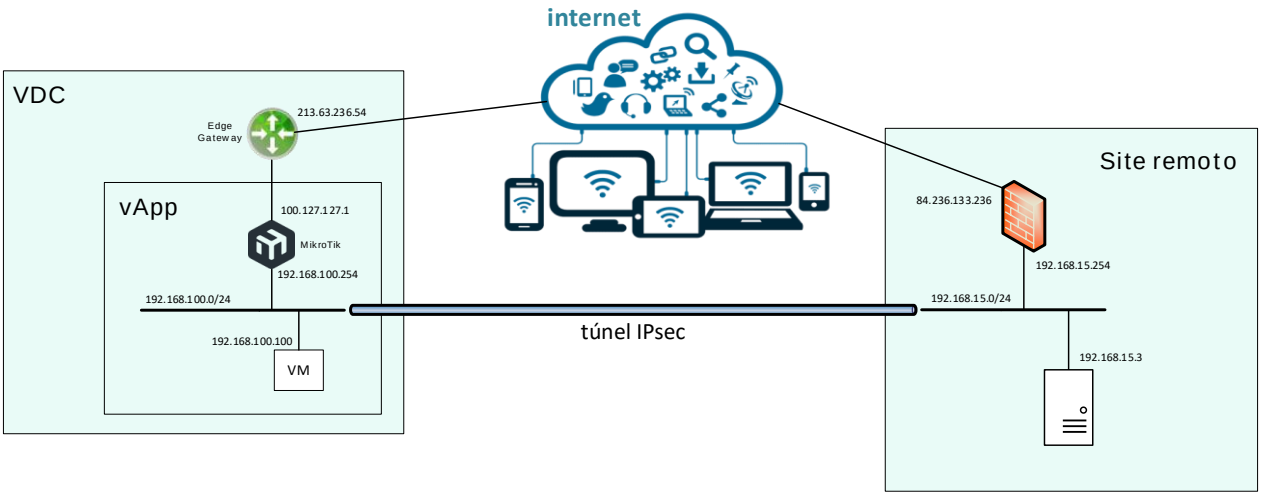


Tabela de configurações

IPsec Phase 1	
Hash Algorithms	sha256
PRF Algorithms	sha256
Encryption Algorithm	aes-256
DH Group	modp2048
DPD Interval	8 seconds
DPD Maximum Failures	4
NAT Traversal	Sim
IPsec Phase 2	
Auth. Algorithms	sha256
Encryption Algorithm	aes-256
PFS Group	modp2048 DH (DH group 14)
Lifetime	30 minutos

Site VDC – Mikrotik no VDC	
IP público	213.63.236.54
IP rede trânsito	100.127.127.1
IP LAN local	192.168.100.254
LAN local	192.168.100.0/24
ID	213.63.236.54

Site Remoto	
IP público	84.236.133.236
IP rede trânsito	n/a
IP LAN local	192.168.15.254
LAN local	192.168.15.0/24
ID	84.236.133.236

Pre-Shared Key	
PSK	ArTelecom2025
Exchange Mode	
IKE	IKEv2

A chave PSK poderá ser gerada em qualquer ferramenta para o efeito.

Por exemplo, https://delinea.com/resources/password-generator-it-tool.

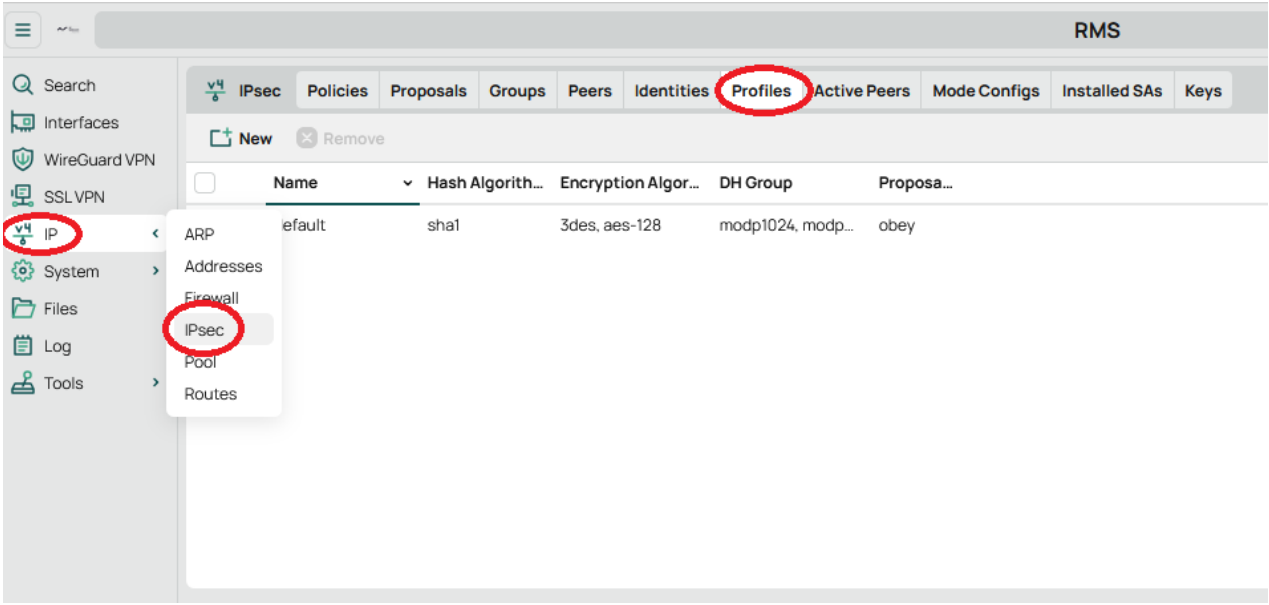
Neste exemplo usamos uma chave simples.

Nos pontos seguintes demonstra-se como efetuar esta configuração.

10.1 Configuração de perfis - IPsec Phase 1

A configuração de perfis serve para definir os parâmetros da Phase 1 da conexão IPsec.

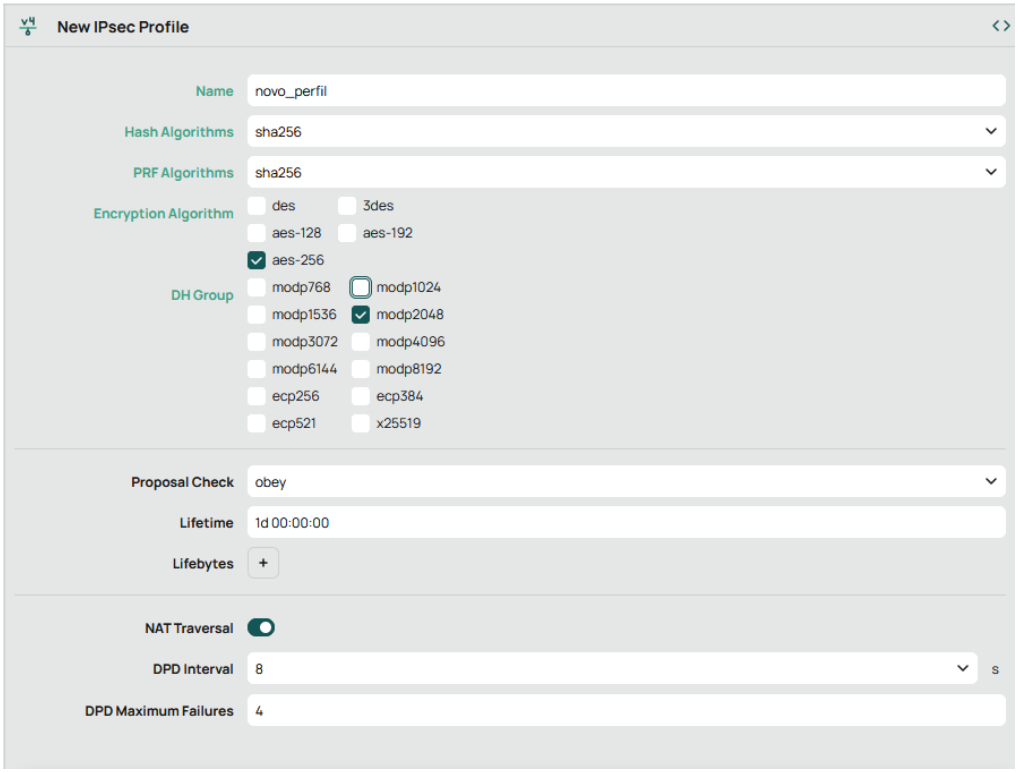
No menu lateral esquerdo em IP -> IPsec e depois no tab Profiles podemos ver um perfil *default* pré-configurado:



Carregando no perfil, podemos ver e alterar a configuração. Vamos em vez disso, criar um perfil novo carregando em New, deixando o default inalterado. Os parâmetros devem ser configurados em conformidade com a tabela de configurações criada inicialmente.

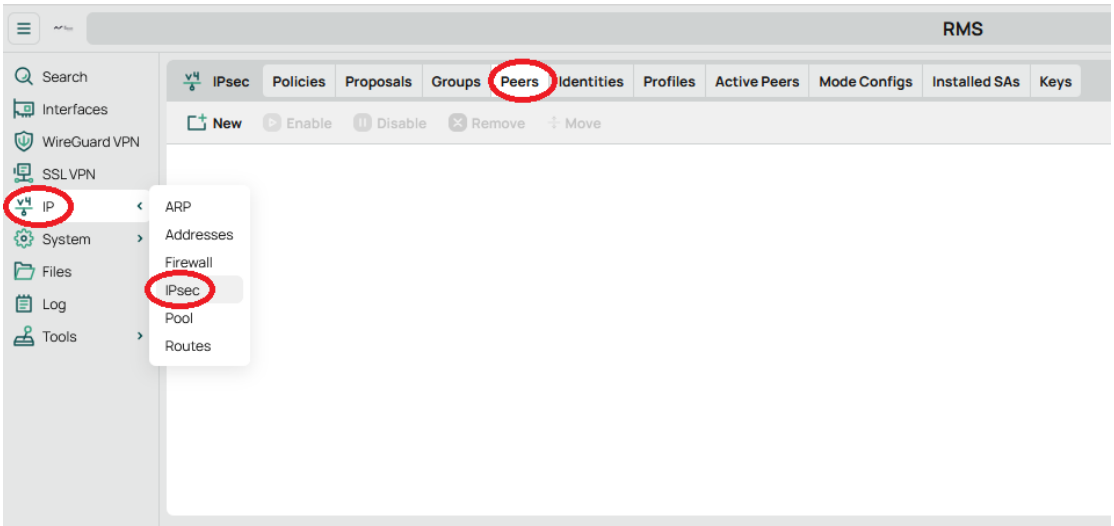
- Name: novo_perfil
- Hash Algorithms: sha256
- PRF Algorithms: sha256
- Encryption Algorithm: aes-256
- DH Group: modp2048

- NAT Traversal: como o Mikrotik se conecta ao exterior através de um Edge Gateway é mandatório que esta opção esteja ativa
- DPD Interval: 8 seconds
- DPD Maximum Failures: 4

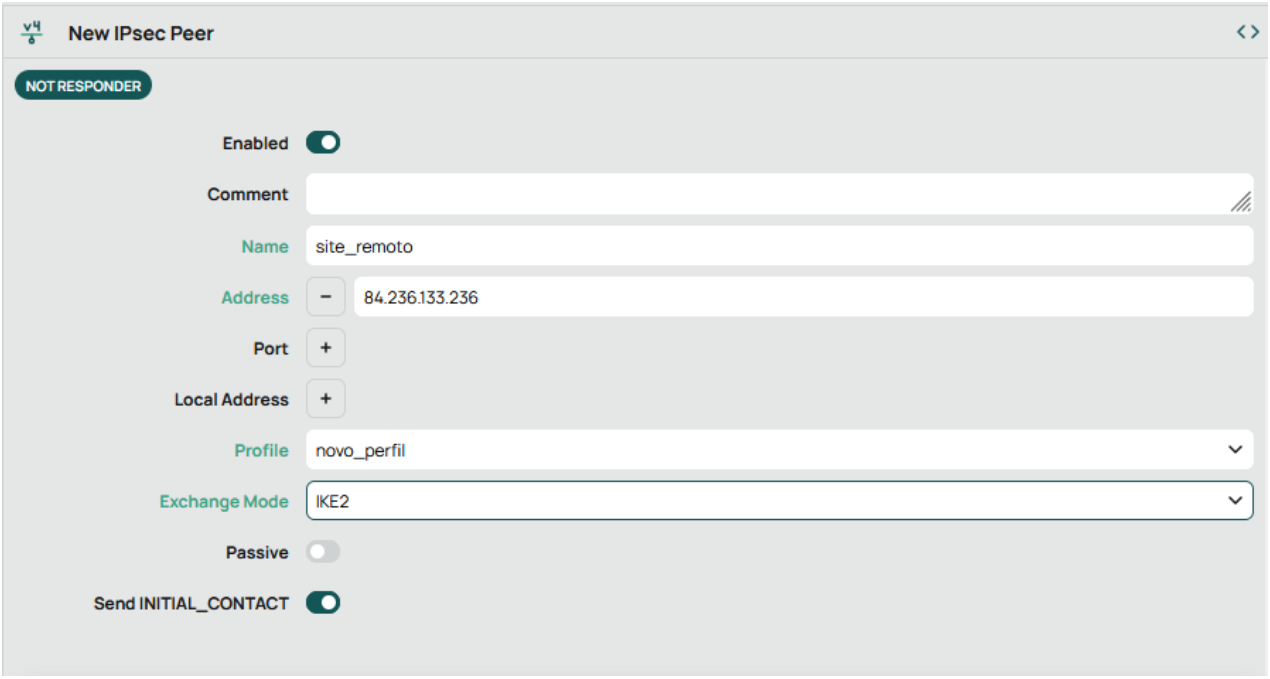


10.2 Criação do dispositivo remoto

Para adicionar um dispositivo remoto, ir ao menu lateral esquerdo e clicar em IP -> IPsec, tab Peers e New:



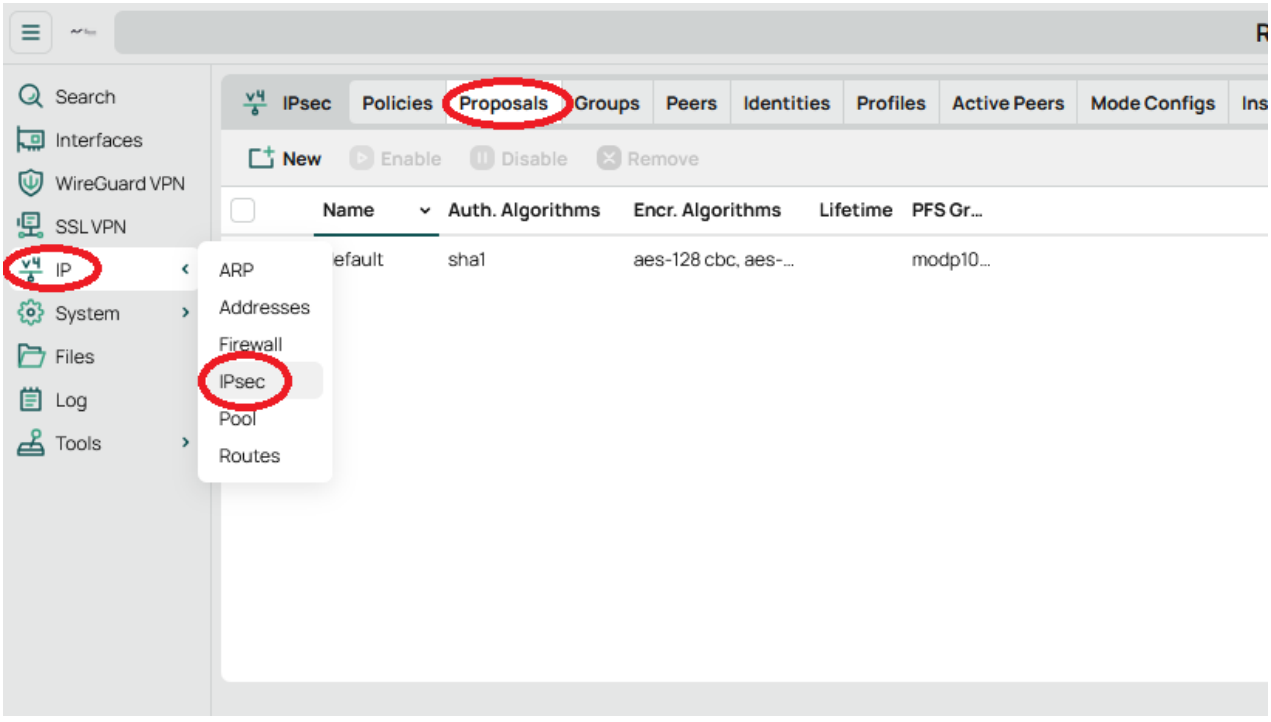
Preencher o quadro de acordo com a tabela de configurações criada inicialmente e usando o perfil do ponto anterior (não esquecer o Exchange Mode que no nosso exemplo é IKE2):



10.3 Configuração de Proposals - IPsec Phase 2

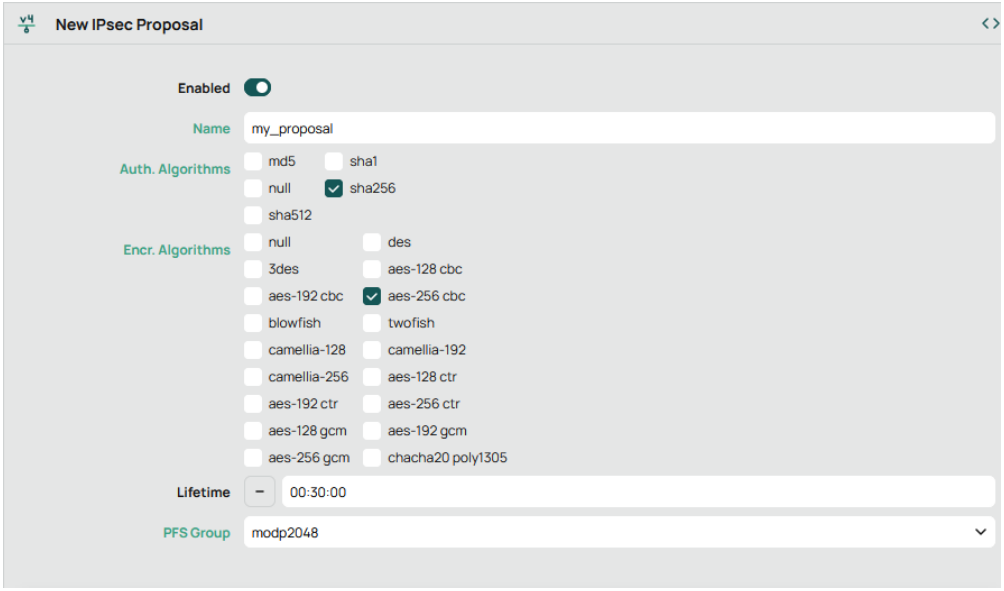
A configuração de Proposal serve para definir os parâmetros da Phase 2 da conexão IPsec.

No menu lateral esquerdo em IP -> IPsec e depois no tab Proposals podemos ver uma configuração *default* pré-definida:



Carregando na Proposal, podemos ver e alterar a configuração. Vamos em vez disso, criar uma nova carregando em New, deixando a default inalterada. Os parâmetros devem ser configurados em conformidade com a tabela de configurações criada inicialmente.

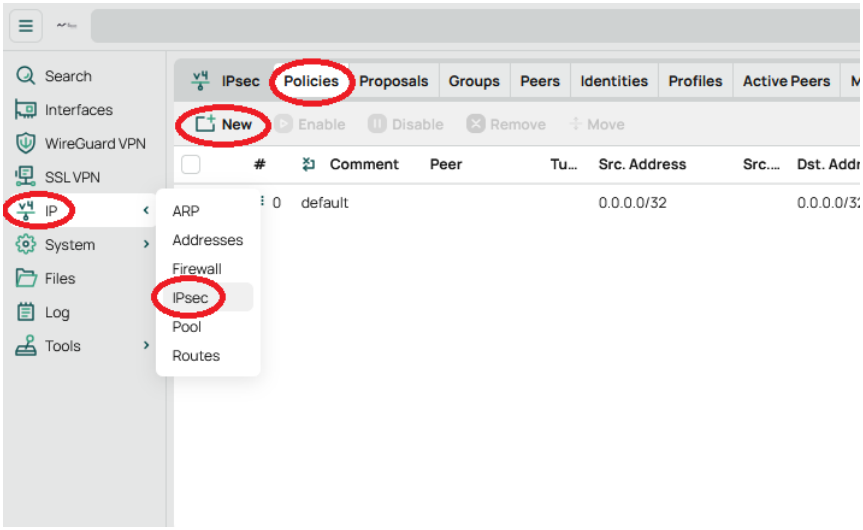
- Name: my_proposal
- Auth. Algorithms: sha256
- Encryption Algorithm: aes-256 cbc
- Lifetime: 30 minutos
- PFS Group: modp2048



10.4 Policies

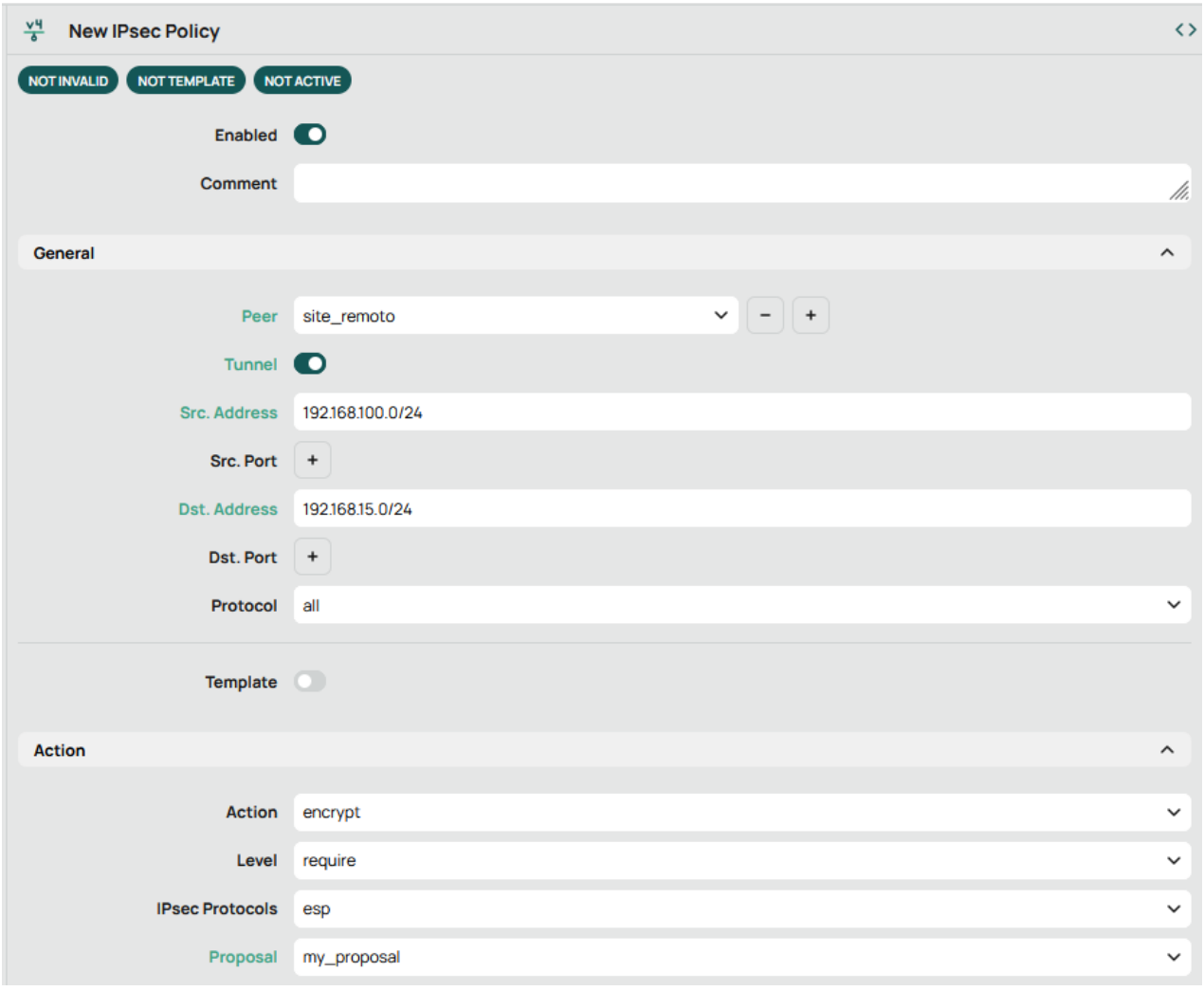
Aqui vamos configurar a relação entre as redes locais nos dois sites.

Indo ao menu lateral esquerdo em IP -> IPsec e depois no tab Policies encontramos uma política default que não é possível transformar em política ativa, pelo que, vamos criar uma nova:



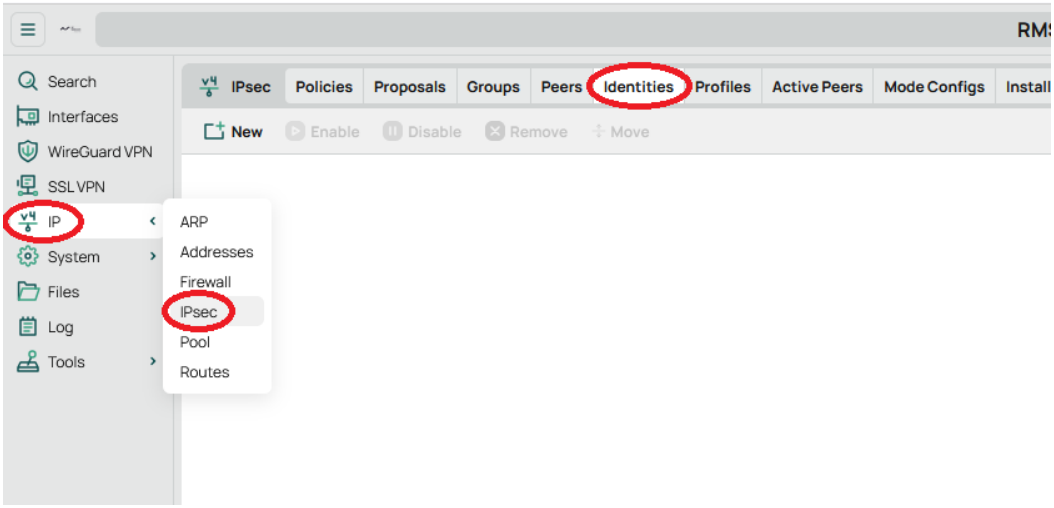
Aqui introduzimos:

- Peer: no nosso exemplo, *site_remoto*
- Ativamos a opção Tunnel
- Src. Address: a rede local no VDC, no nosso exemplo, 192.168.100.0/24
- Dst. Address: a rede local no destino, no nosso exemplo, 192.168.15.0/24
- Action: encrypt
- Level: require
- IPsec Protocols: esp
- Proposal: a definida no ponto anterior

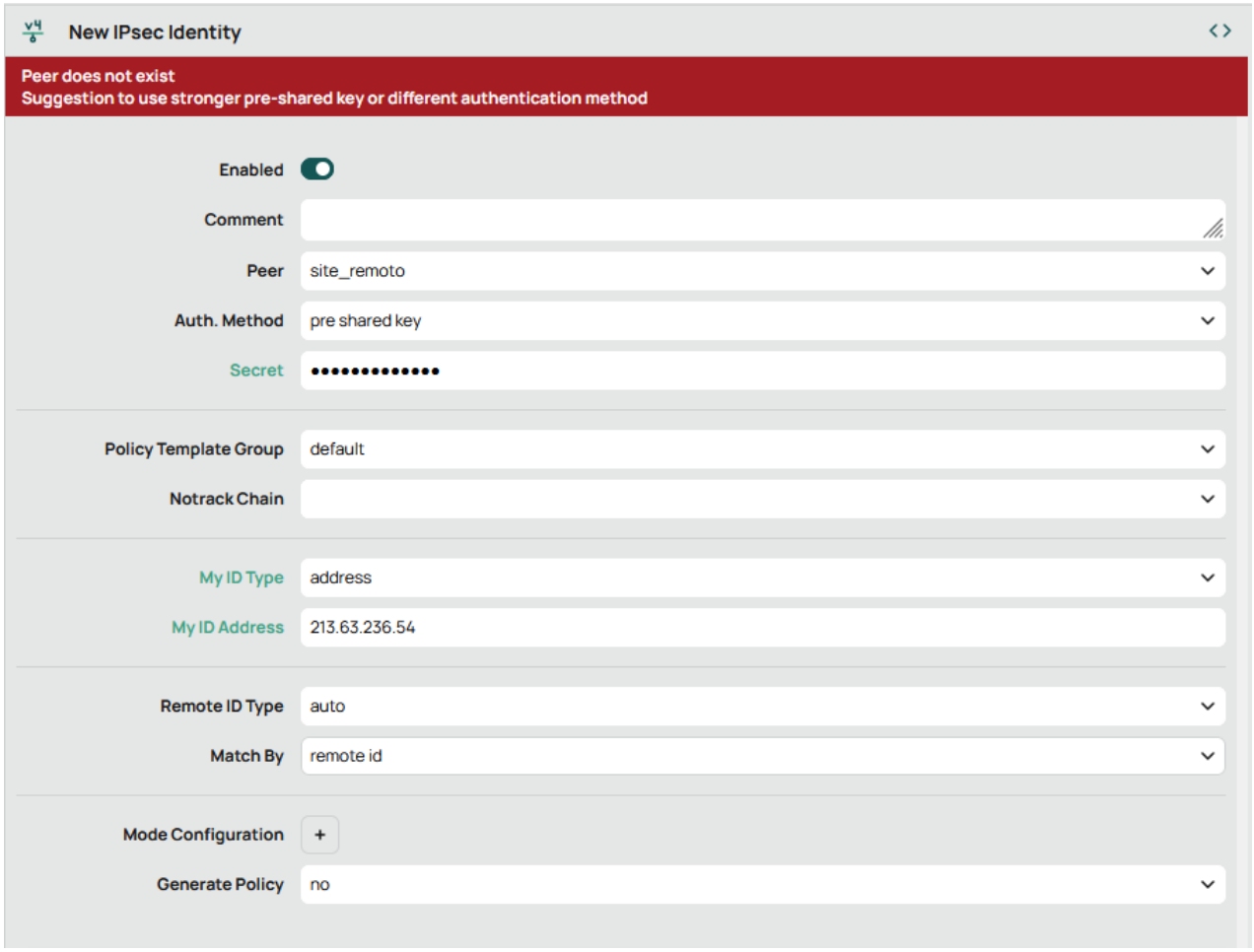


10.5 Pre-Shared Keys

Para relacionar uma PSK com um dispositivo remoto, ir ao menu lateral esquerdo e clicar em IP -> IPsec e depois no tab Identities:



Clicar em **New** para adicionar uma entrada e preencher conforme definido, terminando com OK. O Remote ID Type pode ficar como *auto* mas devemos alterar o My ID Type para *address* e em My ID Address devemos colocar o IP público associado. Isto porque o Mikrotik se encontra atrás de uma Edge Gateway com NAT ativo.



A mensagem "Peer does not exist" apesar de estar selecionado o Peer configurado antes ("site_remoto" neste exemplo) é normal e desaparece depois de se gravar a configuração com OK.

10.6 Regras de firewall

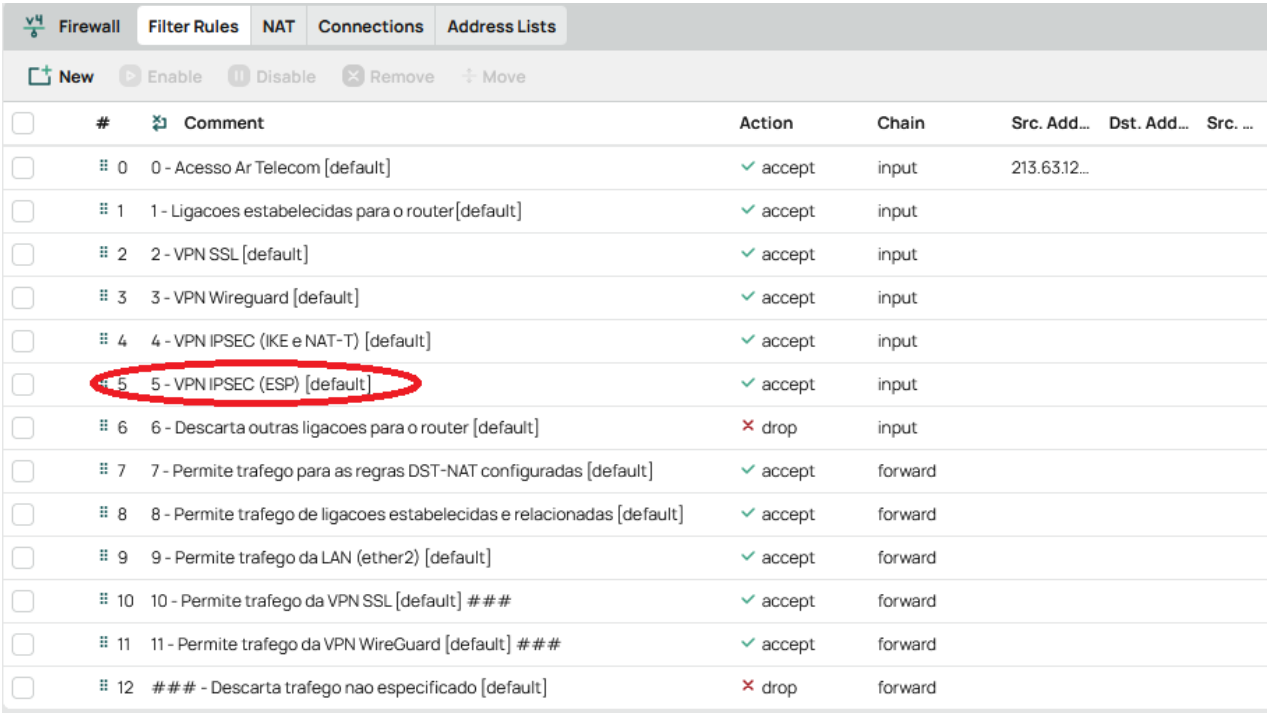
É necessário garantir que seja permitido o tráfego IPsec à entrada da firewall em ambos os sites.

Este tráfego consiste de:

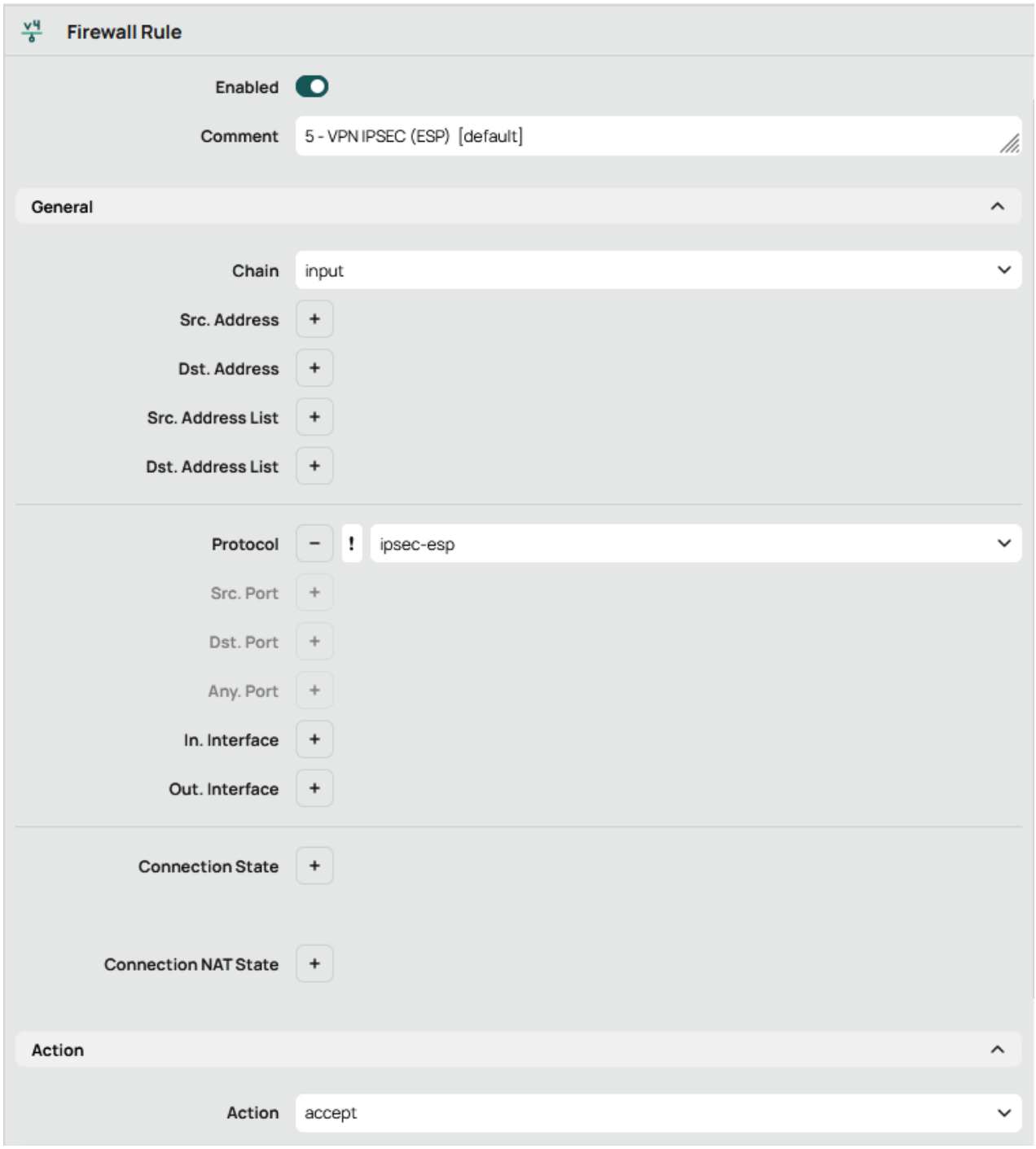
- Protocolo ESP (IPsec)
- Tráfico UDP na porta 500 (ISAKMP)
- Tráfico UDP na porta 4500 (NAT-T)

Estas regras de firewall estão já criadas no serviço entregue pela Ar Telecom, o que pode ser comprovado verificando as mesmas em IP -> Firewall, tab Filter Rules:

Protocolo ESP



#	Comment	Action	Chain	Src. Add...	Dst. Add...	Src. ...
0	0 - Acesso Ar Telecom [default]	accept	input	213.63.12...		
1	1 - Ligacoes estabelecidas para o router [default]	accept	input			
2	2 - VPN SSL [default]	accept	input			
3	3 - VPN Wireguard [default]	accept	input			
4	4 - VPN IPSEC (IKE e NAT-T) [default]	accept	input			
5	5 - VPN IPSEC (ESP) [default]	accept	input			
6	6 - Descarta outras ligacoes para o router [default]	drop	input			
7	7 - Permite trafego para as regras DST-NAT configuradas [default]	accept	forward			
8	8 - Permite trafego de ligacoes estabelecidas e relacionadas [default]	accept	forward			
9	9 - Permite trafego da LAN (ether2) [default]	accept	forward			
10	10 - Permite trafego da VPN SSL [default] ###	accept	forward			
11	11 - Permite trafego da VPN WireGuard [default] ###	accept	forward			
12	### - Descarta trafego nao especificado [default]	drop	forward			



Tráfico UDP na porta 4500 (NAT-T) e 500 (ISAKMP)

Firewall | Filter Rules | NAT | Connections | Address Lists

New | Enable | Disable | Remove | Move

#	Comment	Action	Chain	Src. Add...	Dst. Add...	Src
0	0 - Acesso Ar Telecom [default]	accept	input	213.63.12...		
1	1 - Ligacoes estabelecidas para o router[default]	accept	input			
2	2 - VPN SSL [default]	accept	input			
3	3 - VPN Wireguard [default]	accept	input			
4	4 - VPN IPSEC (IKE e NAT-T) [default]	accept	input			
5	5 - VPN IPSEC (ESP) [default]	accept	input			
6	6 - Descarta outras ligacoes para o router [default]	drop	input			
7	7 - Permite trafego para as regras DST-NAT configuradas [default]	accept	forward			
8	8 - Permite trafego de ligacoes estabelecidas e relacionadas [default]	accept	forward			
9	9 - Permite trafego da LAN (ether2) [default]	accept	forward			
10	10 - Permite trafego da VPN SSL [default] ###	accept	forward			
11	11 - Permite trafego da VPN WireGuard [default] ###	accept	forward			
12	### - Descarta trafego nao especificado [default]	drop	forward			

Firewall Rule

Enabled

Comment: 4 - VPN IPSEC (IKE e NAT-T) [default]

General

Chain: input

Src. Address: +

Dst. Address: +

Src. Address List: +

Dst. Address List: +

Protocol: − ! udp

Src. Port: +

Dst. Port: − ! 500,4500

Any. Port: +

In. Interface: +

Out. Interface: +

Connection State: +

Connection NAT State: +

Action

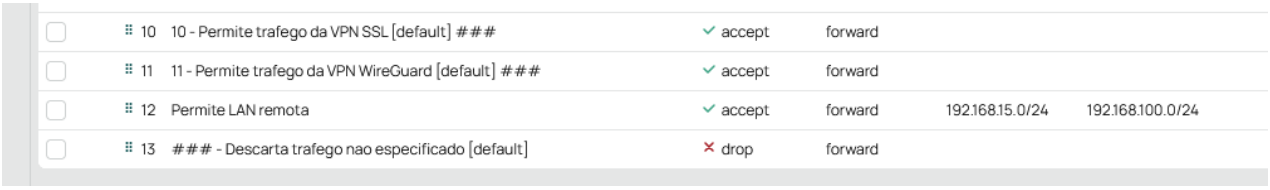
Action: accept

Tráfico entre as redes locais

A passagem de tráfego da rede local para a rede destino já está permitido na regra que permite as ligações da LAN para fora, pelo que, apenas precisamos permitir o tráfego da rede local remota. Criar então uma regra com a seguinte configuração:

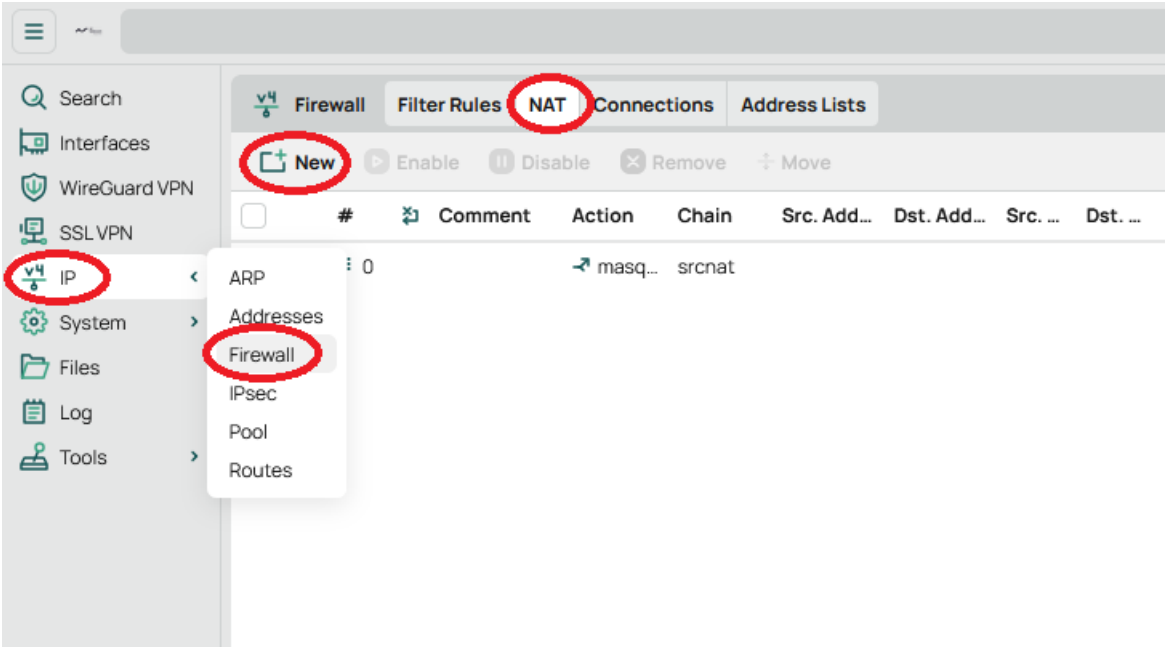
- Comment: colocar uma descrição que facilite a identificação da regra, por exemplo, "Permite LAN remota"
- Chain: forward
- Src. Address: 192.168.15.0/24
- Dst. Address: 192.168.100.0/24
- Action: accept

Não esquecer de mover as regras anteriormente criadas para a posição anterior à regra de drop (deny all):



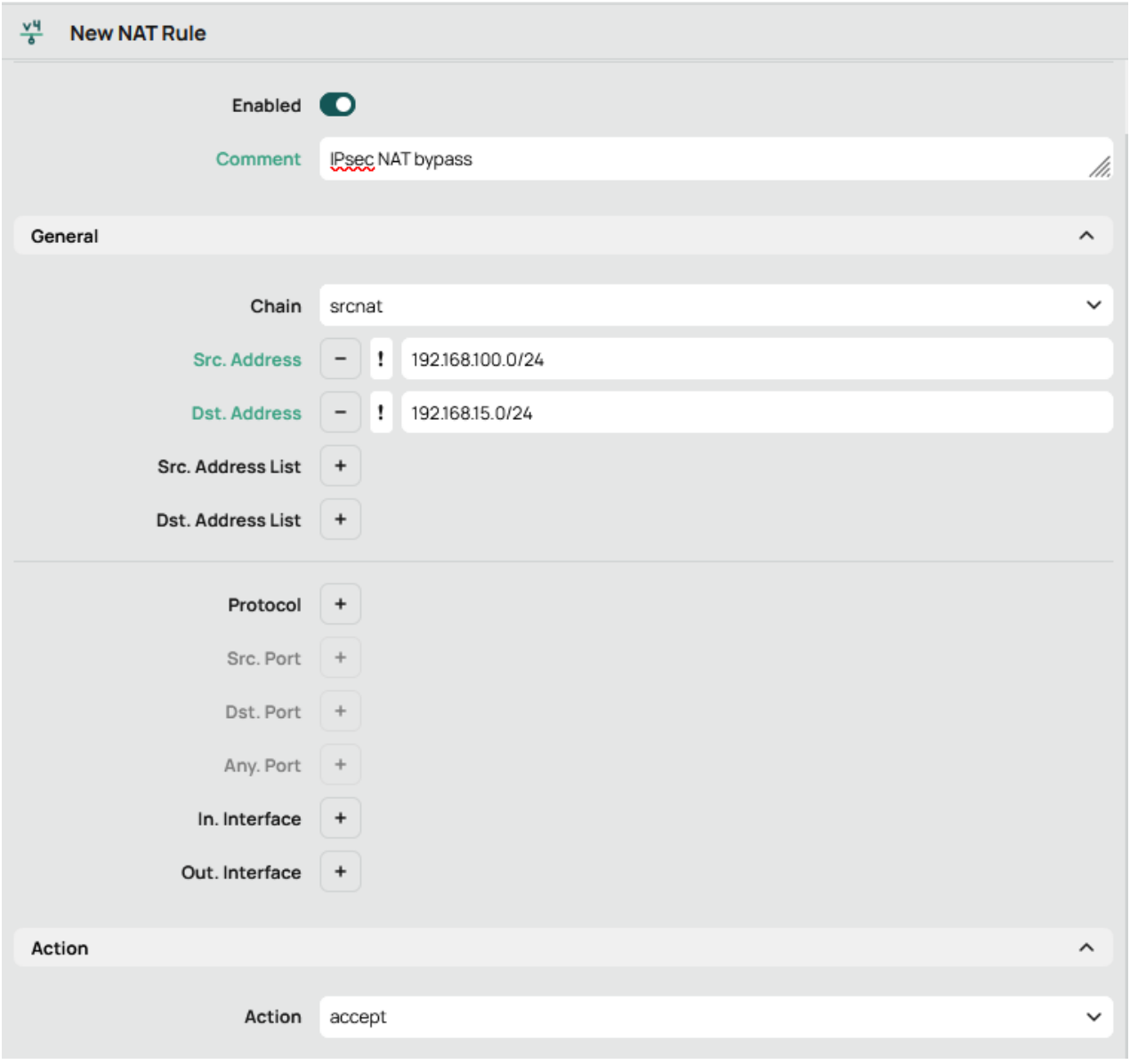
Evitar NAT entre as redes locais

É preciso garantir que o tráfego que passa no túnel IPsec não é alterado pelas regras NAT. Para o fazer, ir ao menu lateral esquerdo e clicar IP -> Firewall -> tab NAT, clicando depois em New :



Configurando da seguinte forma

- Comment: colocar uma descrição que facilite a identificação da regra, por exemplo, "IPsec NAT bypass"
- Chain: srcnat
- Src. Address: 192.168.100.0/24
- Dst. Address: 192.168.15.0/24
- Action: accept



De seguida move-se a regra para o topo para garantir que é executada antes do NAT geral: