CLOUD – Virtual Data Center

OPNSense

MANUAL DE UTILIZADOR

Reference: M_GP_303

Date: 11/02/2026

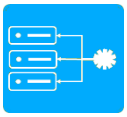
Version: 2.0

Controlo de Versões:

Versão	Data	Alterações
1.0	10-Jan-2025	na.
2.0	11-02-2026	Nova imagem Ar

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

Significado dos Símbolos utilizados

	INFORMAÇÃO	Informação adicional que se pretende relevar
	AVISO	Informação Importante que requer especial atenção
	NOTAS DE PROVISÃO	Apontamentos para a equipa de provisão
	NOTAS DE GESTÃO	Apontamentos para a gestão e/ou operação do serviço

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

ÍNDICE

1. MANUAL DE UTILIZADOR 6
2. INSTALAÇÃO DE INSTÂNCIA FIREWALL 7
2.1 Preparação vCloud 7
2.2 Instalação de instância de firewall 16
2.3 Configuração do router Edge 22
2.4 Ativação da instância de firewall 26
3. ACESSO À CONSOLA DA FIREWALL 28
4. ALTERAR PASSWORD 29
5. CONFIGURAÇÕES DE SEGURANÇA 30
5.1 NTP 30
5.2 DNS 30
5.3 SNMP 31
6. AUTENTICAÇÃO 2FA 33
6.1 Criar servidor de autenticação 33
6.2 Google authenticator 33
6.3 Configurar utilizador 33
6.4 Ativar autenticação no Google Authenticator 34
6.5 Ativar servidor de autenticação 36
7. CONEXÃO A REDE DO VDC 37
7.1 Adição de interface no virtual data center 37
7.2 Conexão à rede pretendida 39
7.3 Configuração da interface na OPNsense 42
8. PERMITIR TRÁFEGO PARA A INTERNET - SNAT 46
8.1 Configuração SNAT 46
8.2 Configuração regras de tráfego 46
9. PORT FORWARD – DNAT 47
10. OPENVPN ROAD WARRIOR 50
10.1 Criar certificados – Certificate Authority 50
10.2 Criar certificados – server certificate 51
10.3 Criar utilizadores da VPN e certificados associados 52
10.4 Criar chave estática 54
10.5 Adicionar servidor OpenVPN 55
10.6 Regras de firewall 56
10.7 Configuração dos dispositivos remotos 57
10.8 Ativar autenticação 2FA 59
11. WIREGUARD ROAD WARRIOR 61
11.1 Adicionar instância Wireguard 61
11.2 Configuração do Peer 62
11.3 Regras de firewall 64
11.4 Configuração do cliente 65
12. IPSEC VPN SITE-TO-SITE 71
12.1 Regras de firewall 71
12.2 Pre-Shared Keys 74

Serviço de apoio a clientes

portal.ar.pt

800 300 400

ar@ar.pt

12.3 Configuração do túnel 75
12.4 Interligação das sub-redes 78

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

1. MANUAL DE UTILIZADOR

Este documento tem como objetivo facilitar a utilização da instância de firewall OPNsense.

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. Para obter informações mais detalhadas, recomendamos que visite https://docs.opnsense.org

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

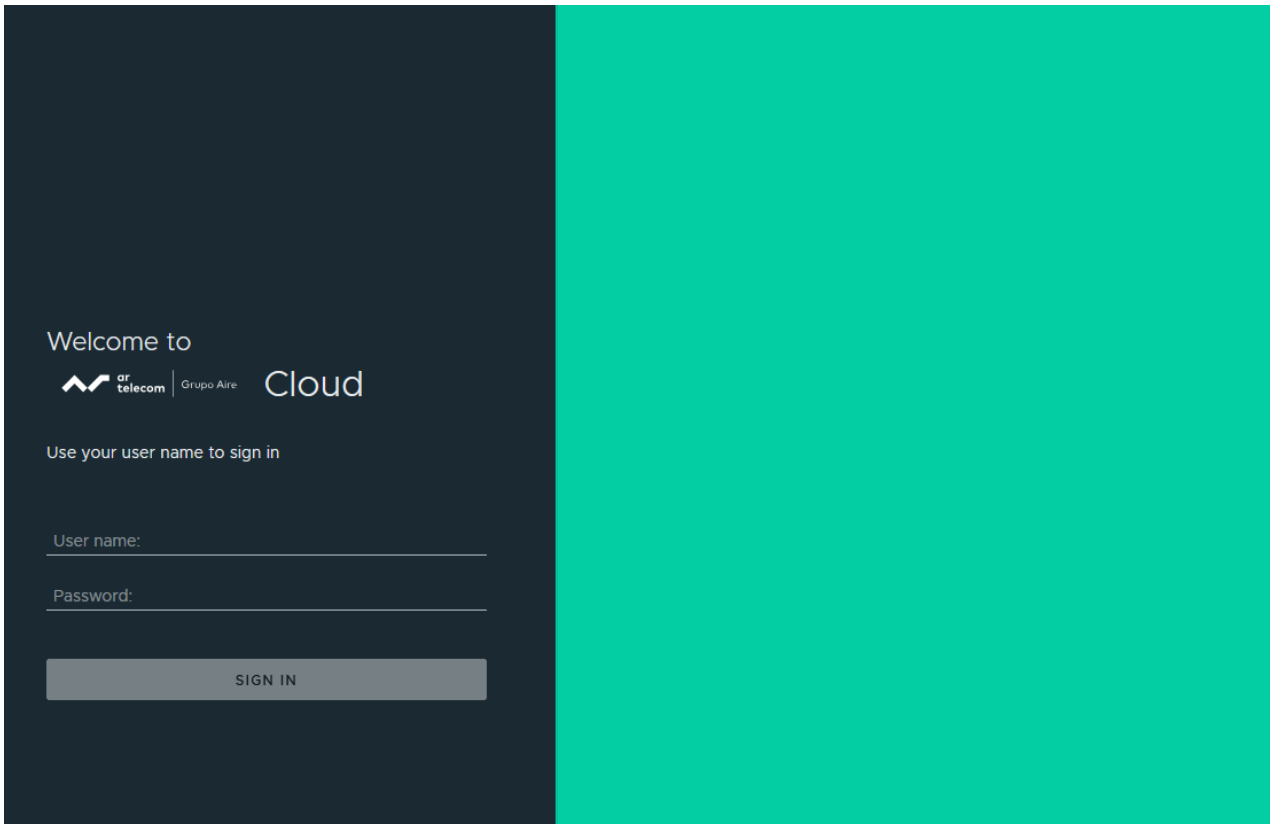
2. INSTALAÇÃO DE INSTÂNCIA FIREWALL

2.1 Preparação vCloud

A implementação de uma instância de firewall customizada implica algumas configurações específicas no router Edge do Virtual Data Center.

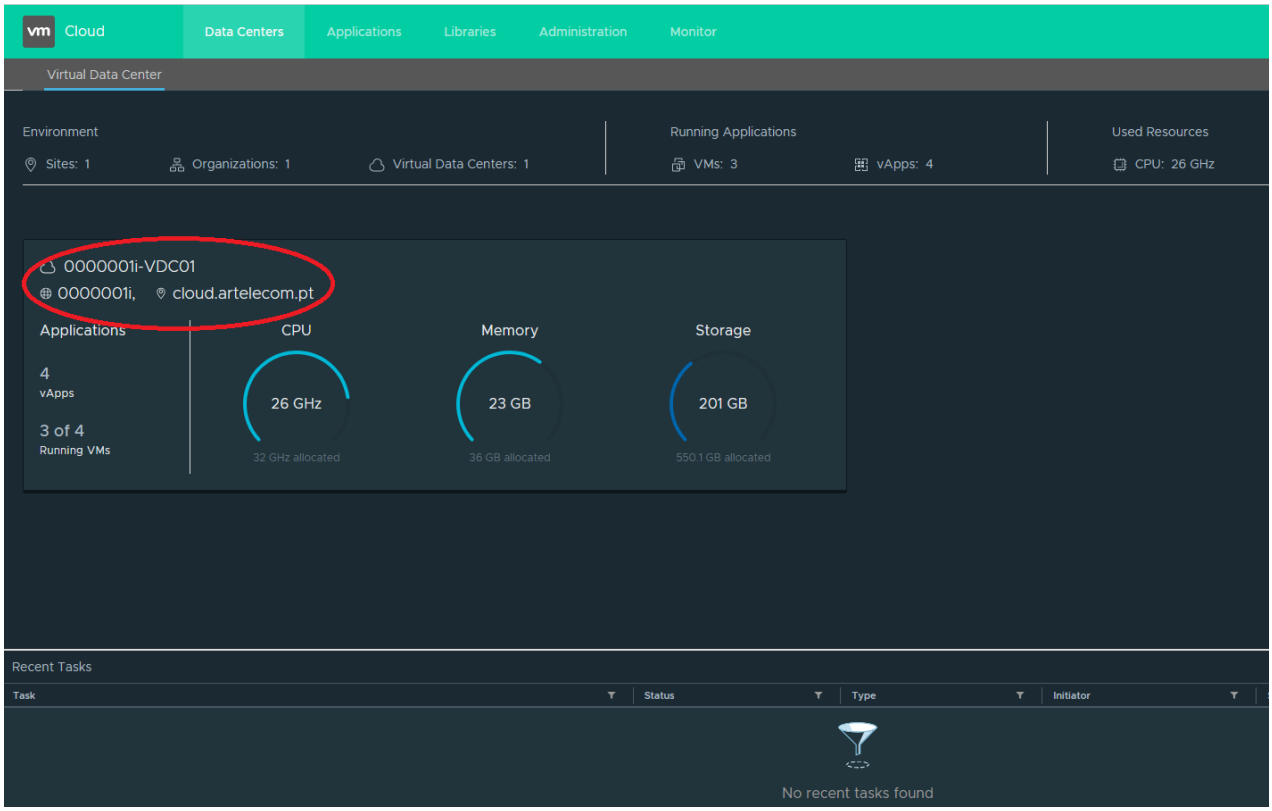
Os passos seguintes mostram o que é necessário configurar e como.

O primeiro passo é aceder à consola do virtual data center, usando o URL e credenciais que lhe foram enviados aquando da ativação do serviço VDC:



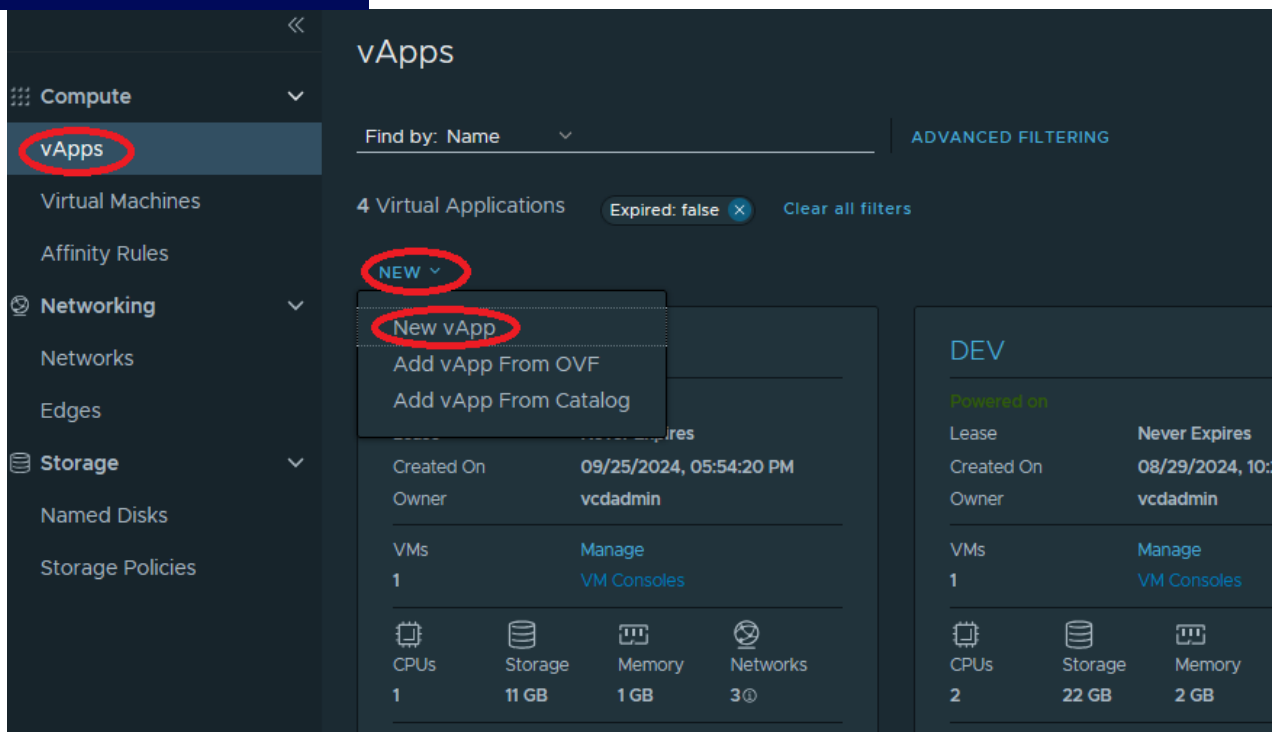
Após uma autenticação bem-sucedida, surge o painel inicial onde deve selecionar o VDC:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

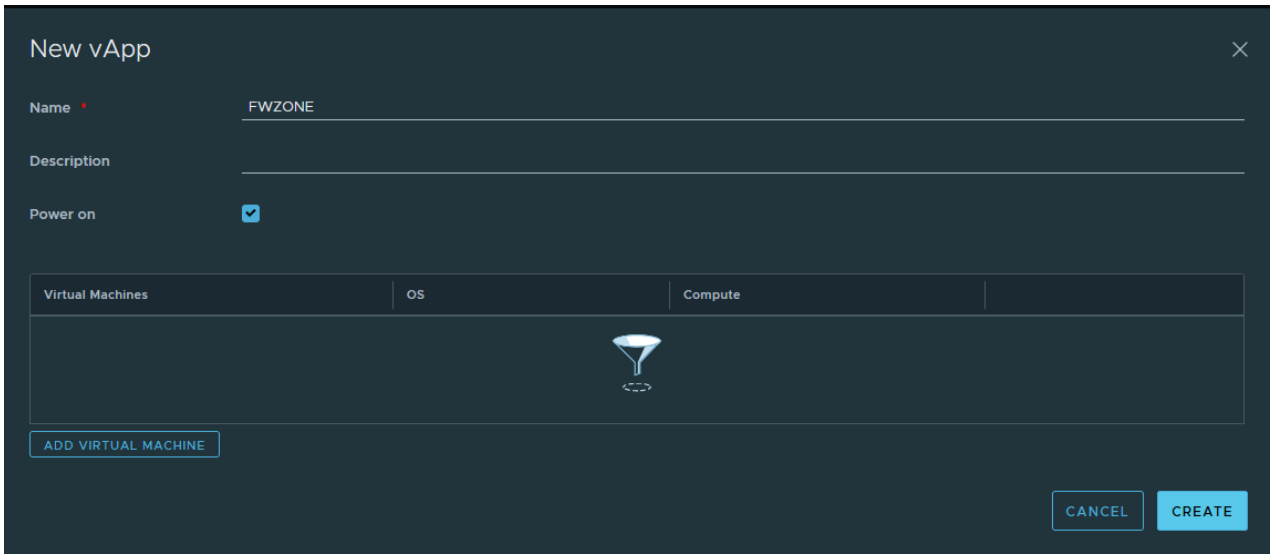


Recomendamos a criação de uma vApp específica para as instâncias de firewall. Para isso, carregar em cima de "vApps" no menu lateral esquerdo e de seguida em "NEW" e "New vApp":

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

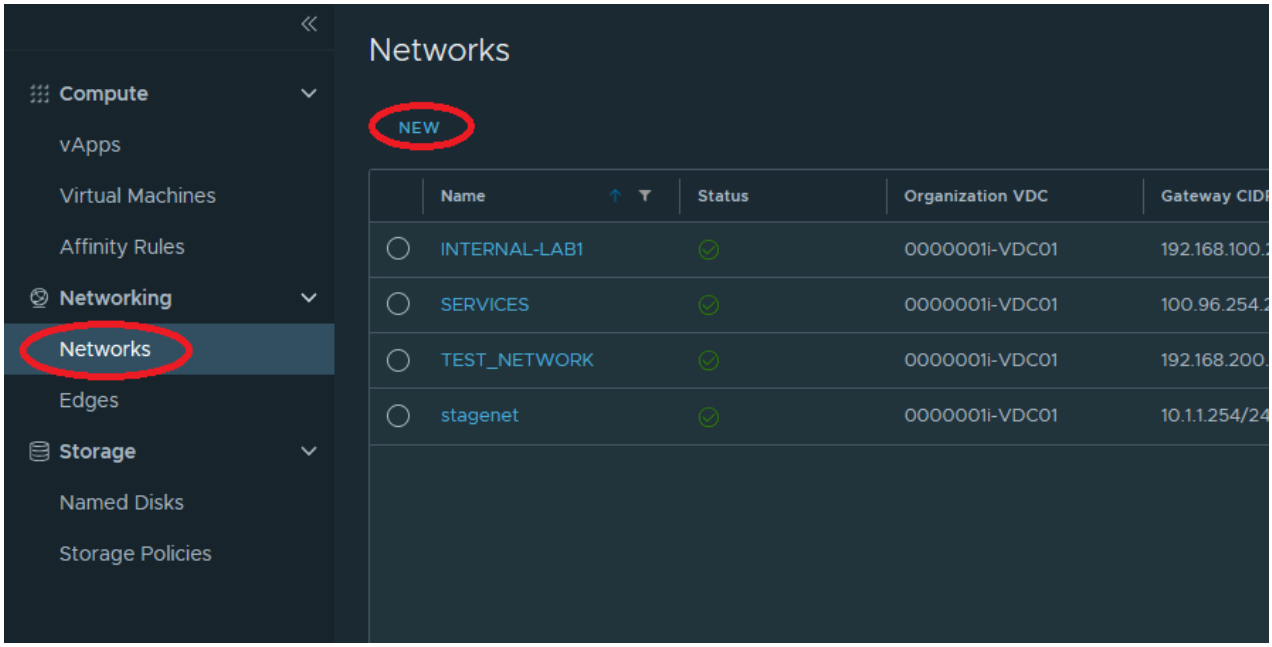


Dar um nome à vApp, selecionar opção "Power on" e "CREATE". Não adicionar nenhuma máquina virtual à vApp nesta fase.

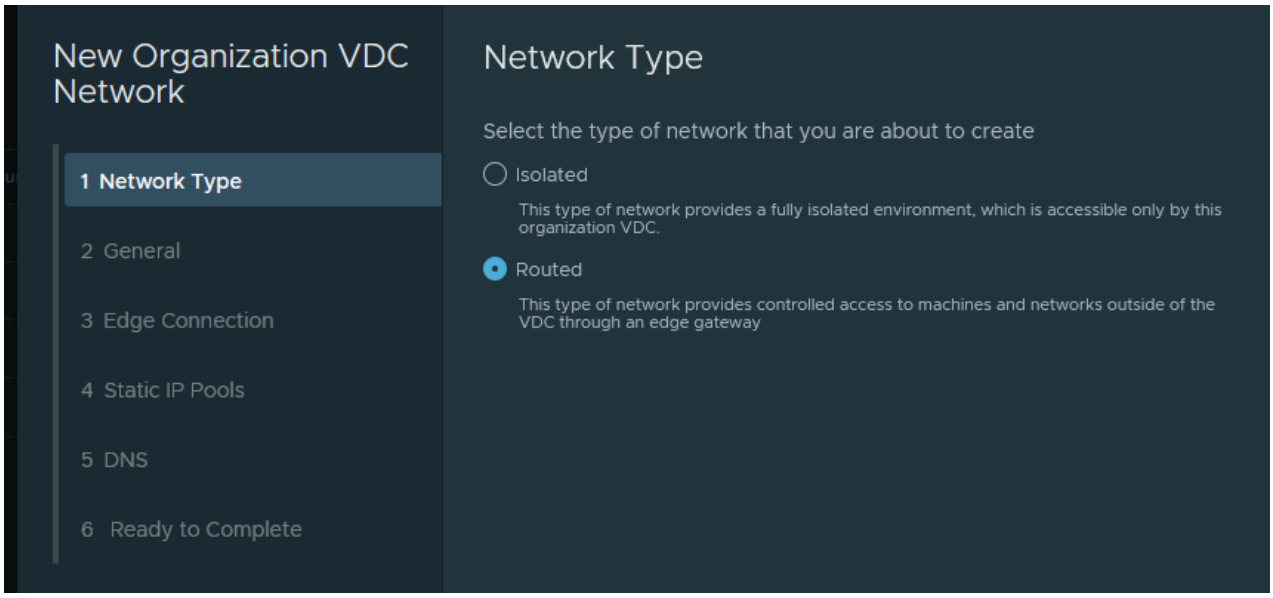


Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

Após a vApp estar criada, sugerimos adicionar uma rede específica para interligação da instância de firewall com o router Edge, caso ainda não esteja criada. Para isso, carregar em "Networks" no menu lateral esquerdo e depois em "NEW":

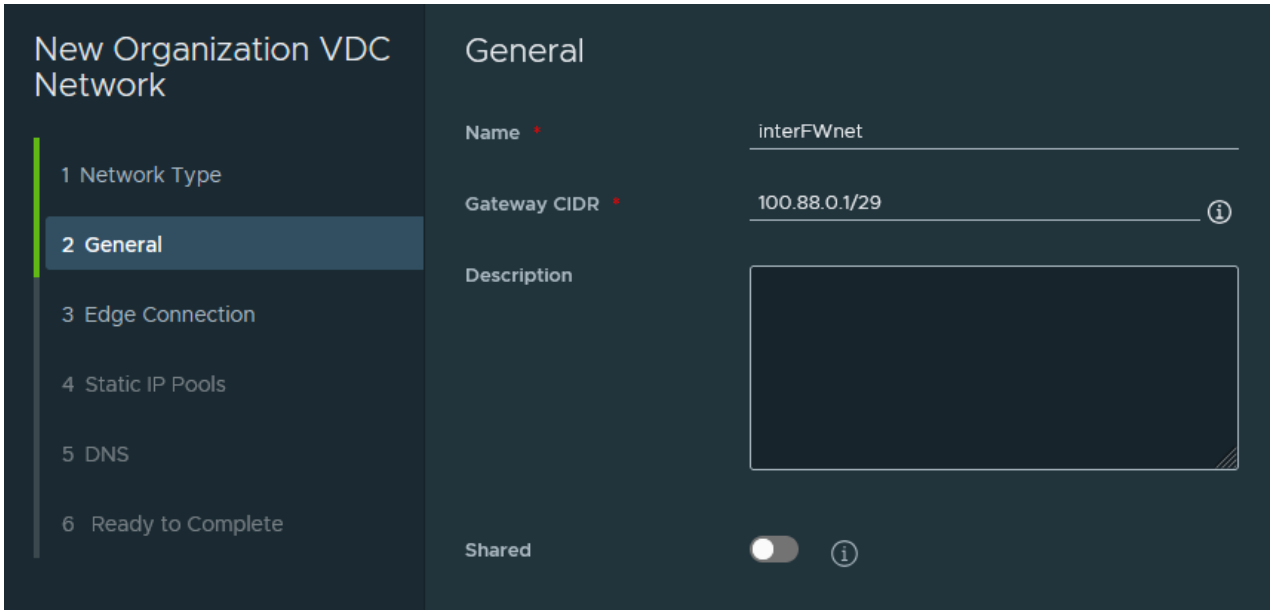


Escolher opção "Routed" para que seja criada a interface correspondente no router Edge:



No próximo passo escolhe-se um nome a dar à rede e o conjunto endereço/máscara de rede a dar à interface no router Edge:

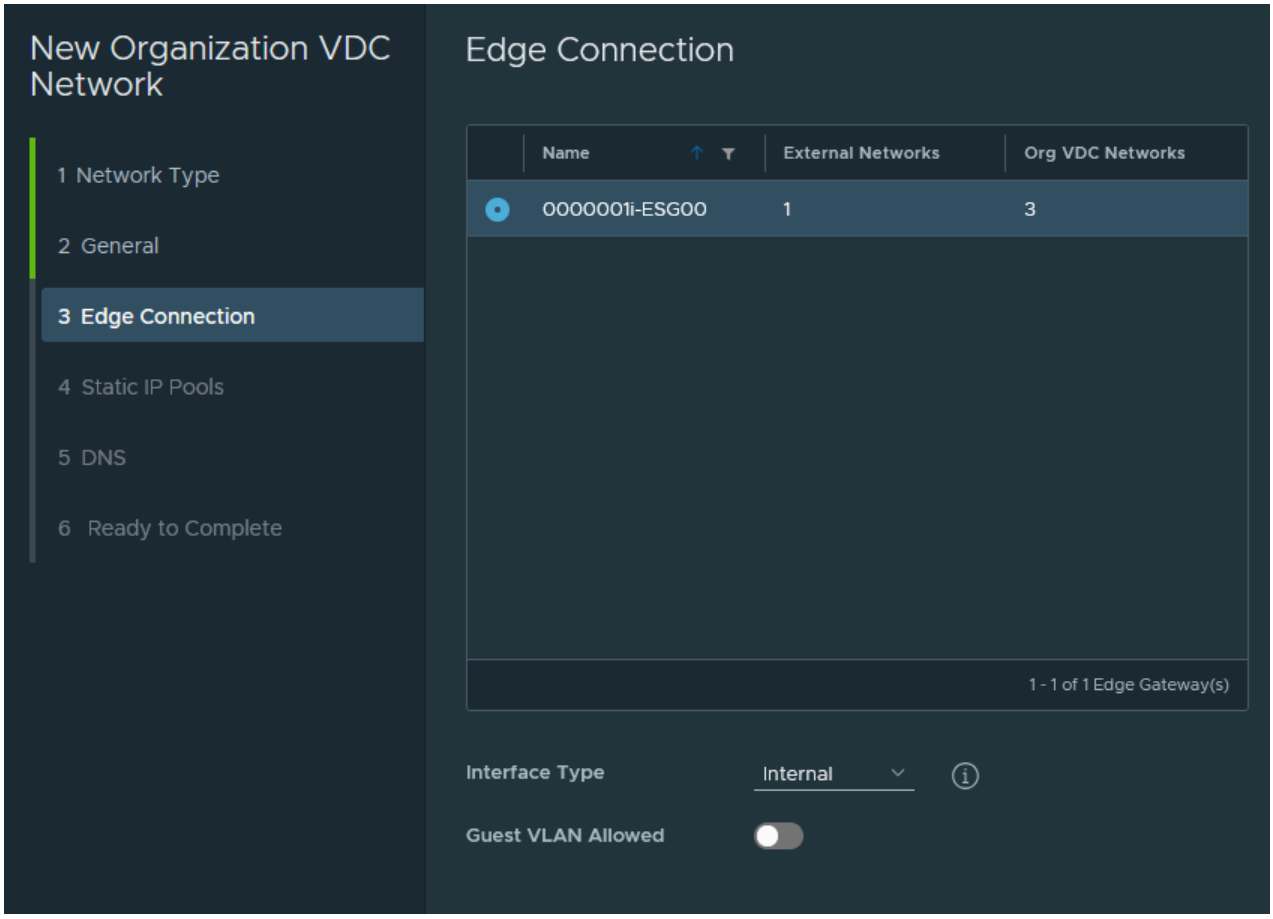
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



e em seguida escolher o router Edge, deixando o tipo de interface conforme está (Internal)

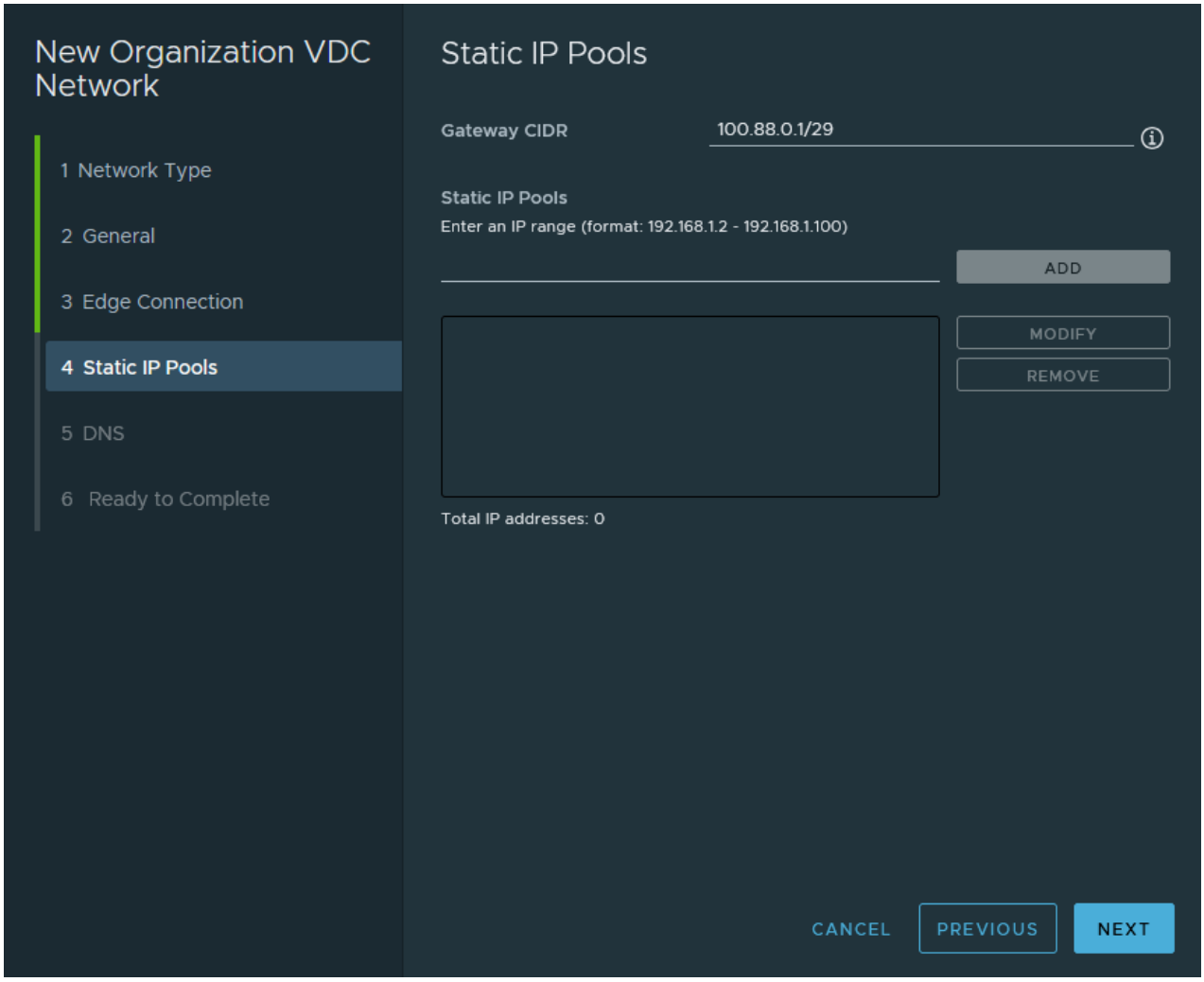
O template de firewall existente está configurado para uma rede de interligação ao router 100.88.0.0/29 em que 100.88.0.1 será o endereço do router e 100.88.0.2 o endereço da firewall. Caso não seja possível utilizar esta rede, escolher uma rede livre neste passo e posteriormente alterar o endereço na firewall.

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

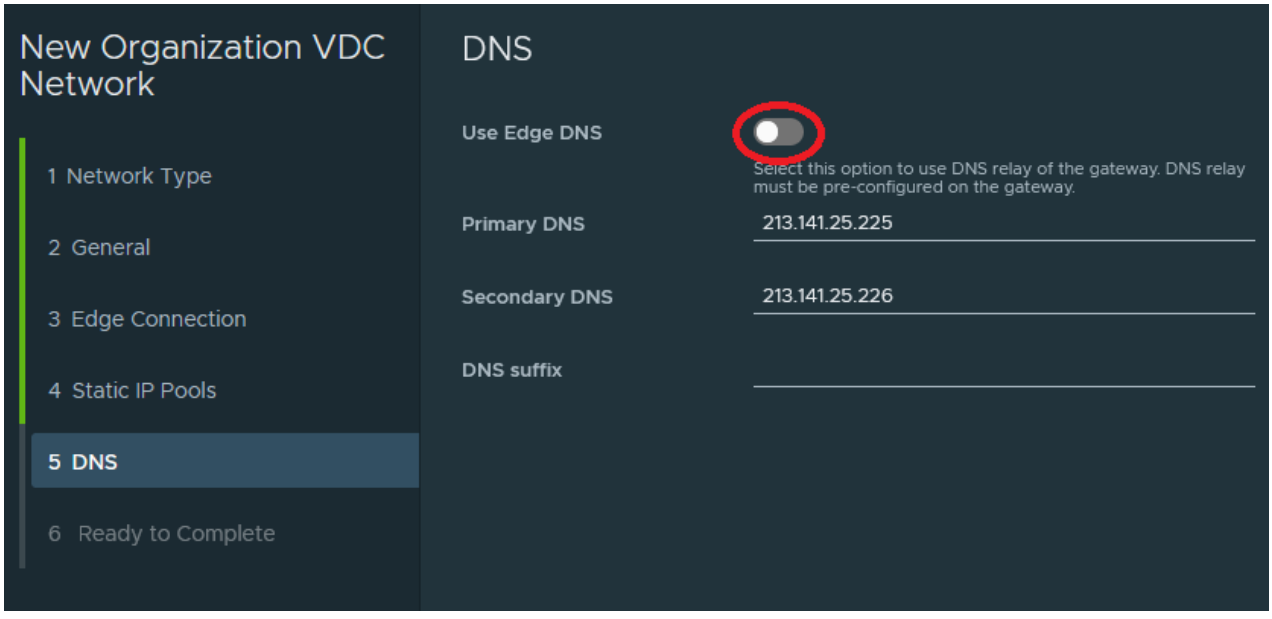


Não é necessária a criação de uma pool de endereços para atribuição às VMs, pelo que, deve-se fazer Next no quadro seguinte:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

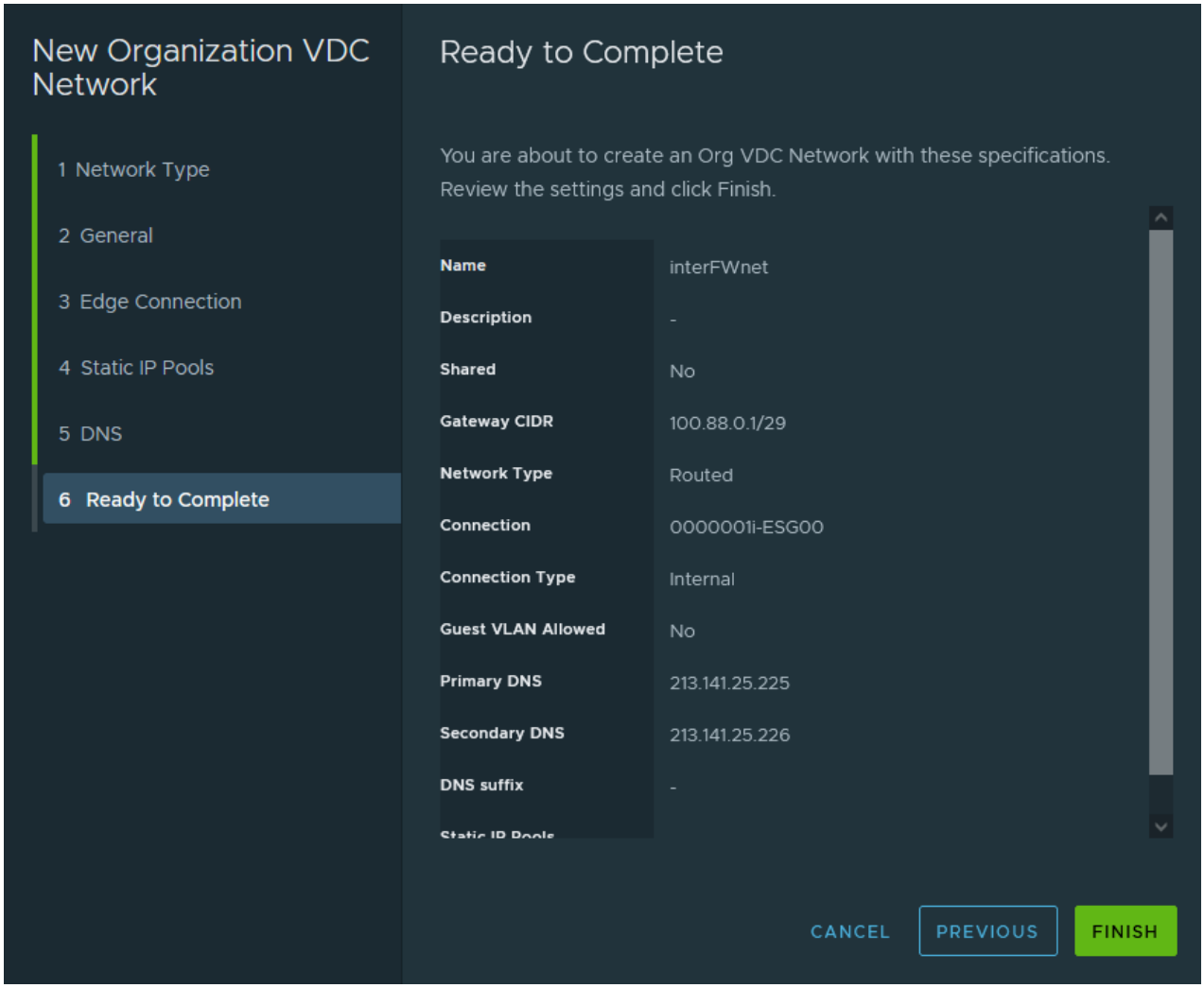


Para a configuração de DNS sugerimos os endereços DNS dos servidores da Ar, sendo necessário desativar a opção "Use Edge DNS":

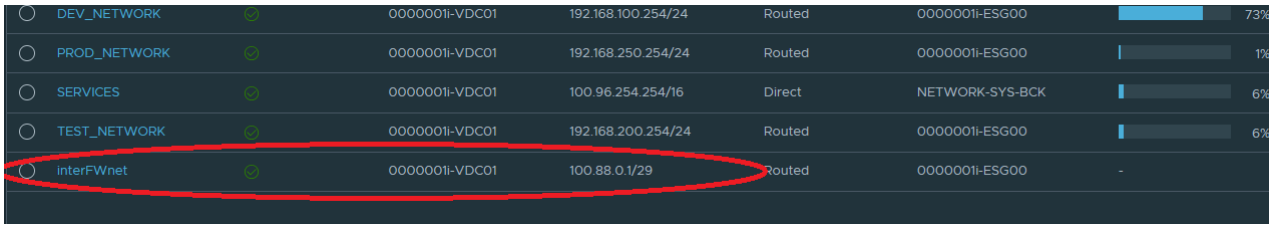


Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

Por fim, confirmar os dados introduzidos e concluir a configuração carregando em "FINISH":

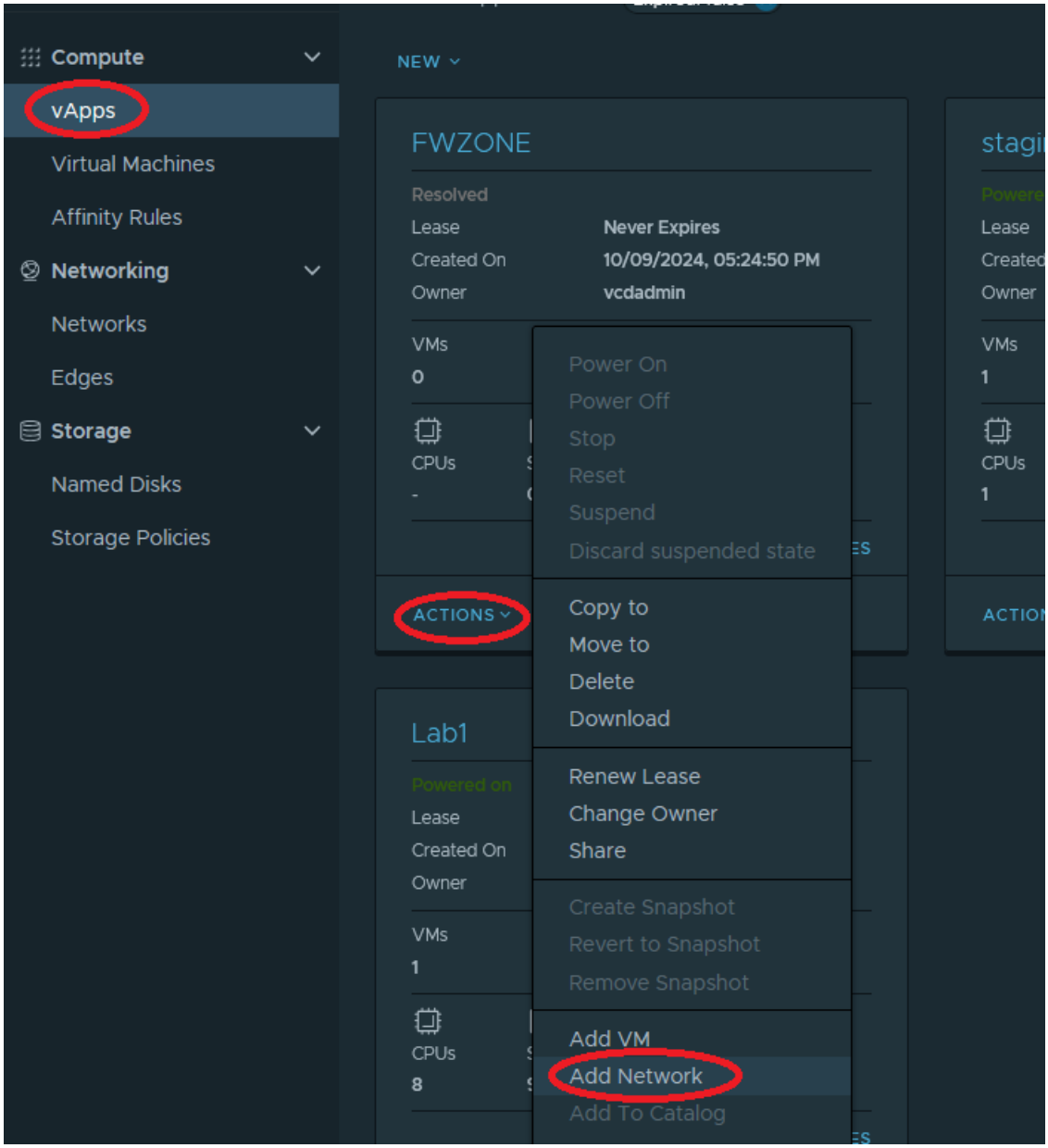


A partir deste momento a rede vai estar disponível na Organização para associação às vApps.



Esta rede necessita estar disponível para a instância de firewall a instalar, pelo que, tem de ser associada à vApp criada anteriormente e onde a firewall vai residir. Para isso, carregar em "vApps" no menu lateral esquerdo e em "ACTIONS" da vApp correspondente, seguido de "Add Network":

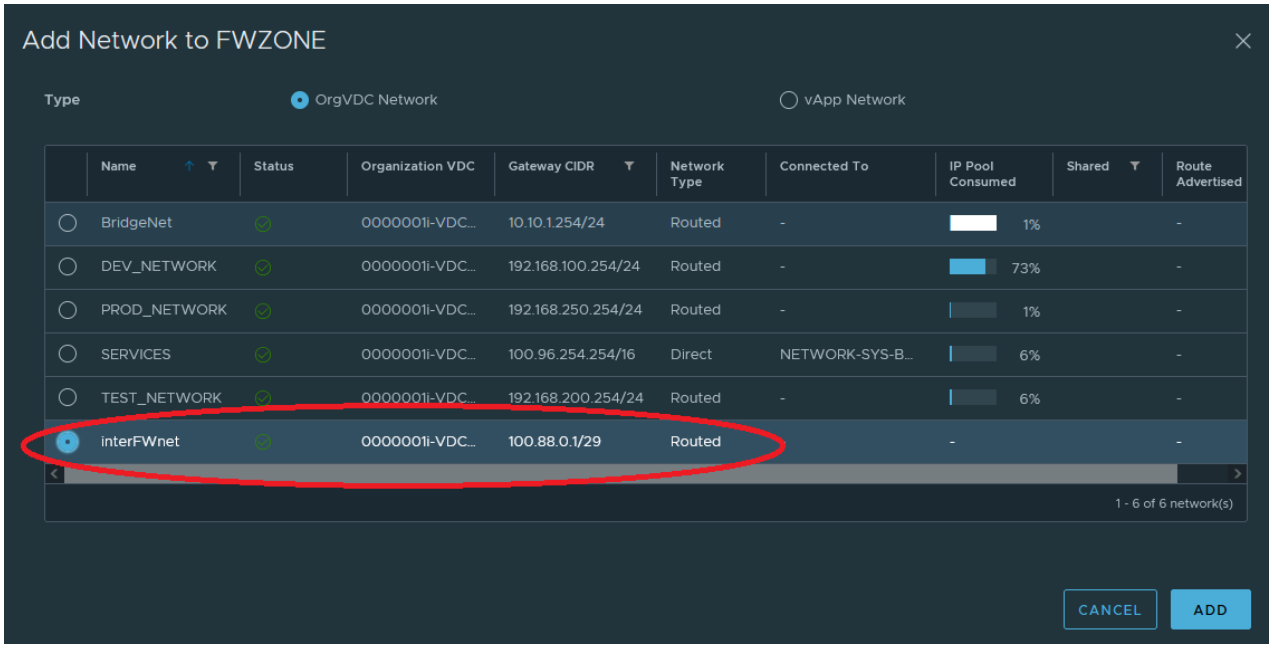
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



Selecionar opção "OrgVDC Network"

e escolher a rede criada anteriormente:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



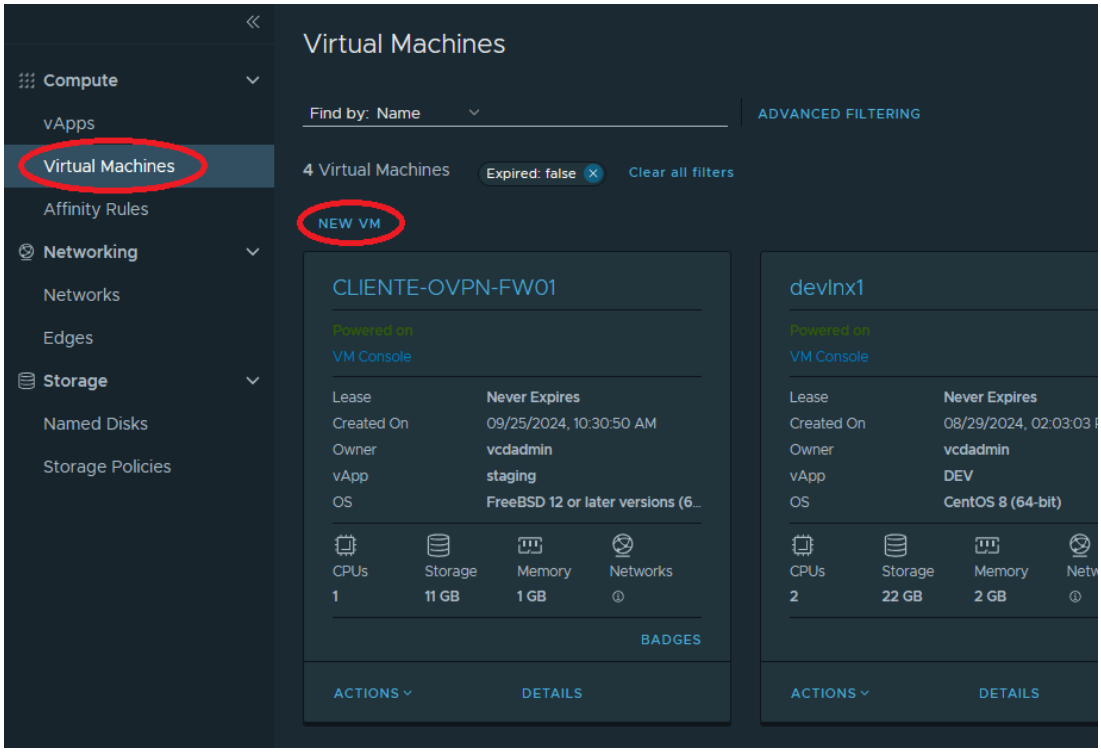
A partir deste momento, temos uma vApp criada com uma rede de interligação com o router Edge. O próximo passo será a instalação da instância de firewall.

2.2 Instalação de instância de firewall

Para facilitar esta instalação, a Ar disponibiliza um template de uma instância já preparada. Este template encontra-se no catálogo Network Appliances que não está disponível na ativação base do serviço VDC. Para ter acesso ao mesmo deverá solicitá-lo à equipa de suporte da Ar.

Para adicionar uma VM com instância de firewall OPNsense a partir do catálogo, ir a "Virtual Machines" no menu lateral esquerdo e escolher a opção "NEW VM":

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

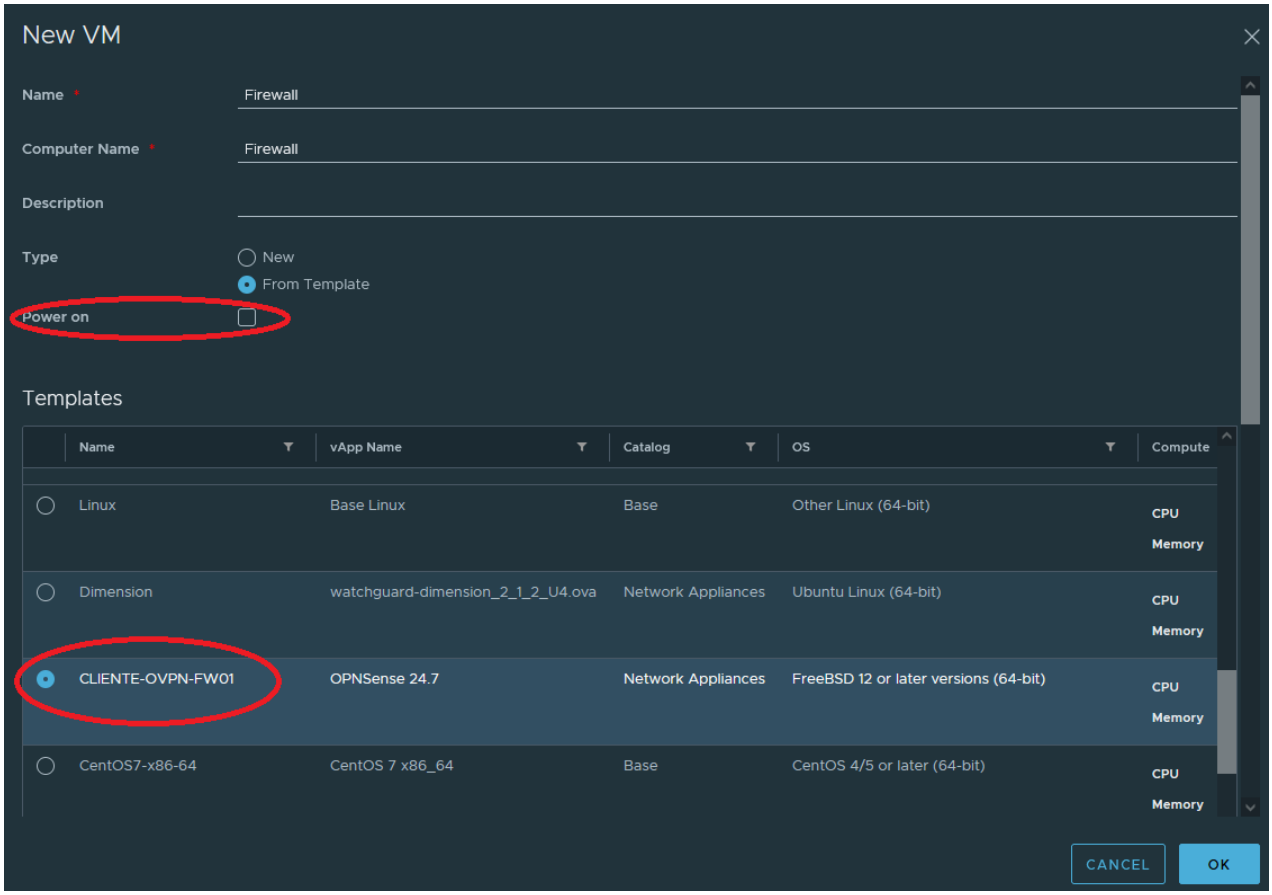


No quadro que aparece de seguida, é necessário fazer algumas configurações:

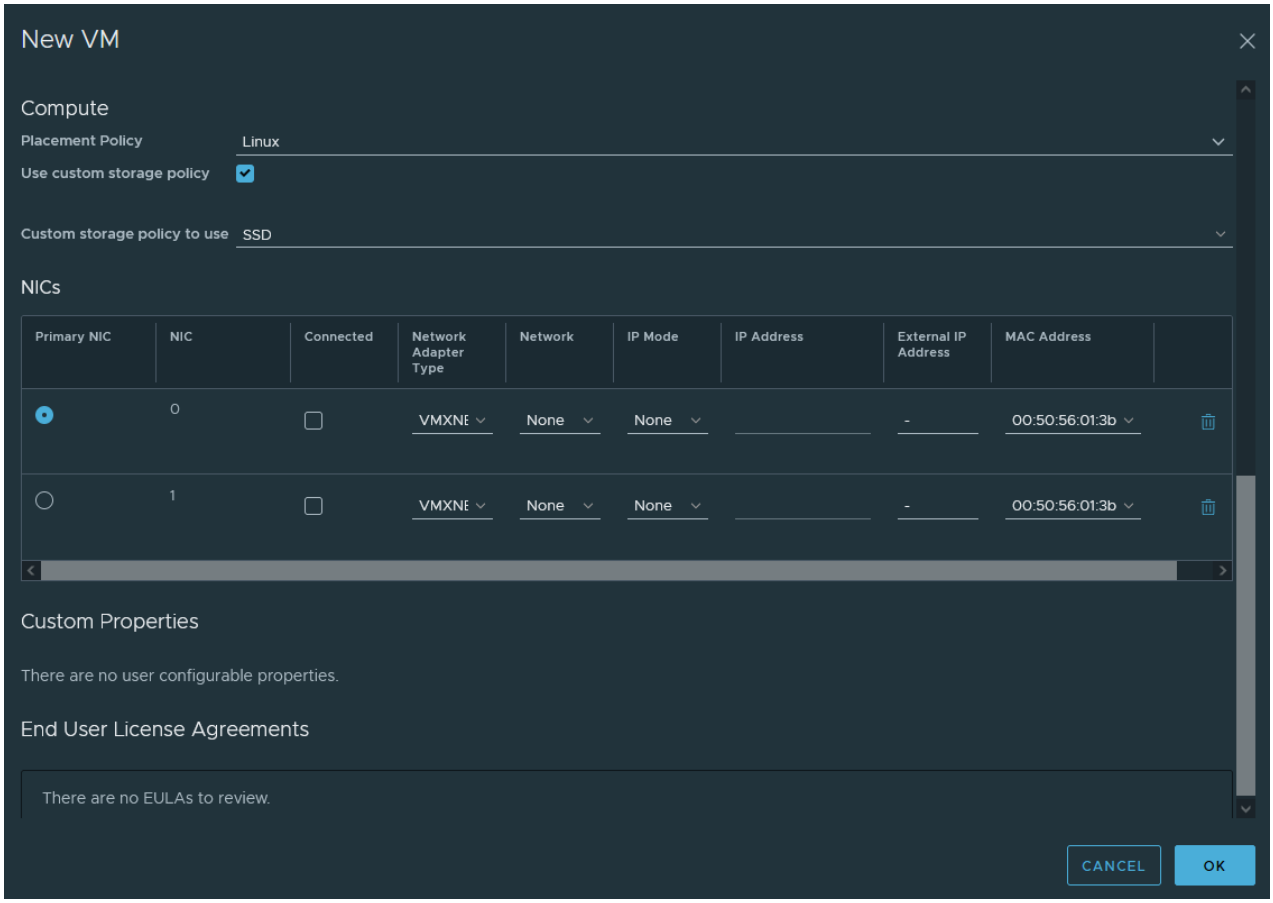
- dar um nome à instância de firewall
- deixar o campo Type em "From Template"
- desativar o "Power on"
- escolher o template "CLIENTE-OVPN-FW01"
- Alterar o "Placement Policy" para "Linux"
- Usar a política de storage que corresponde ao Tier de storage contratado: por exemplo "SSD"

Não é necessário configurar a secção de rede nesta fase.

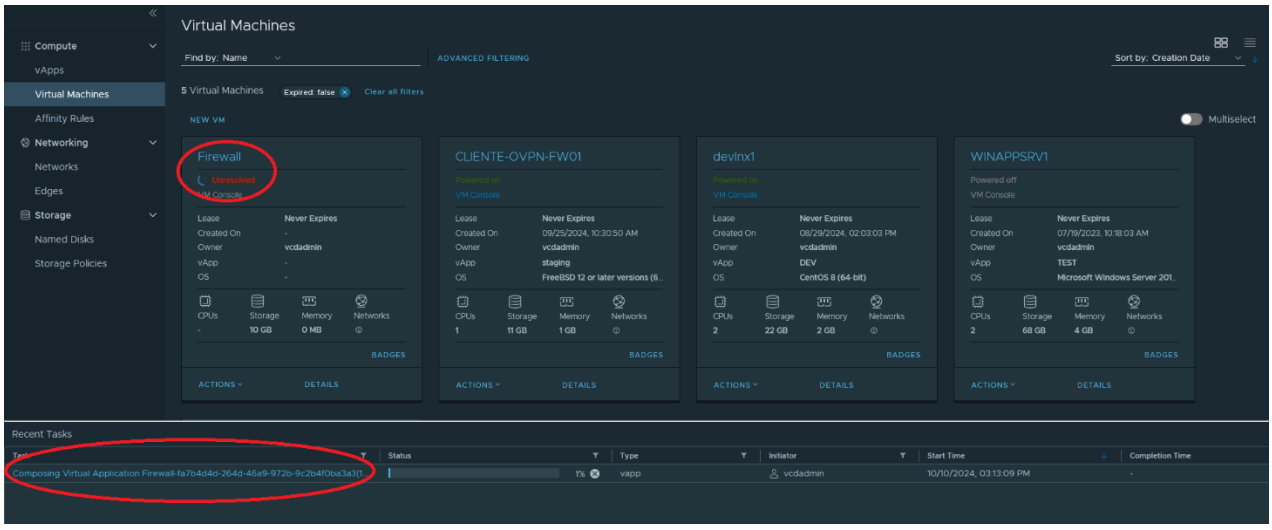
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



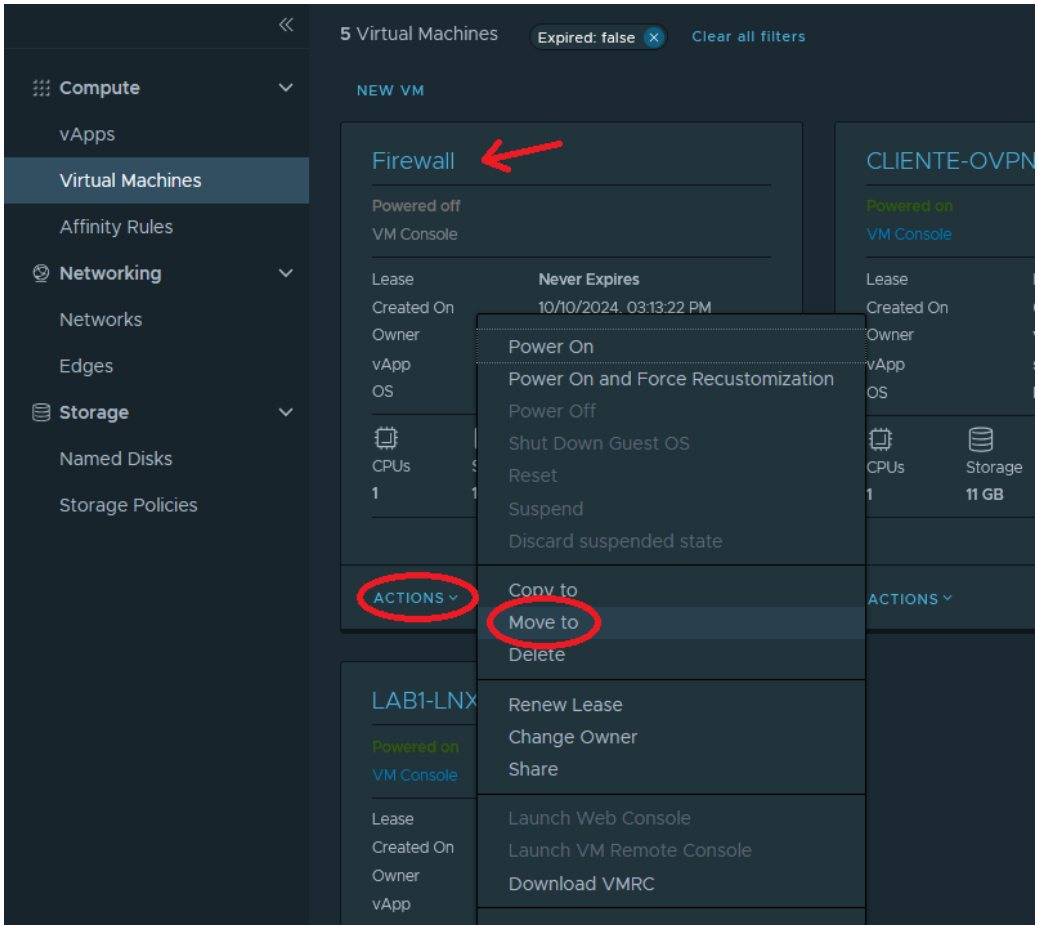
Após carregar em OK o sistema irá compor a VM

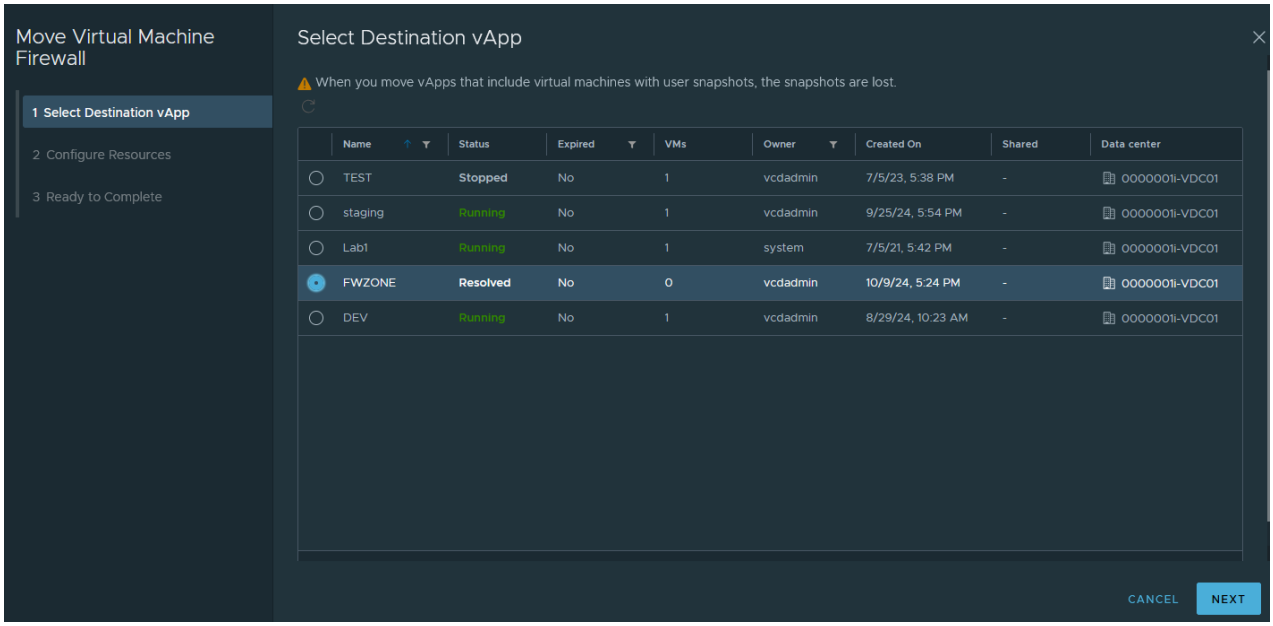


Por defeito, esta instância será criada com 1 vCPU e 1GB de memória, podendo estas quantidades ser alteradas após esta tarefa estar concluída ou mais tarde sempre que for necessário e houver recursos suficientes contratados.

O passo seguinte é o de mover a VM para a vApp pretendida (neste exemplo, vApp FWZONE):

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

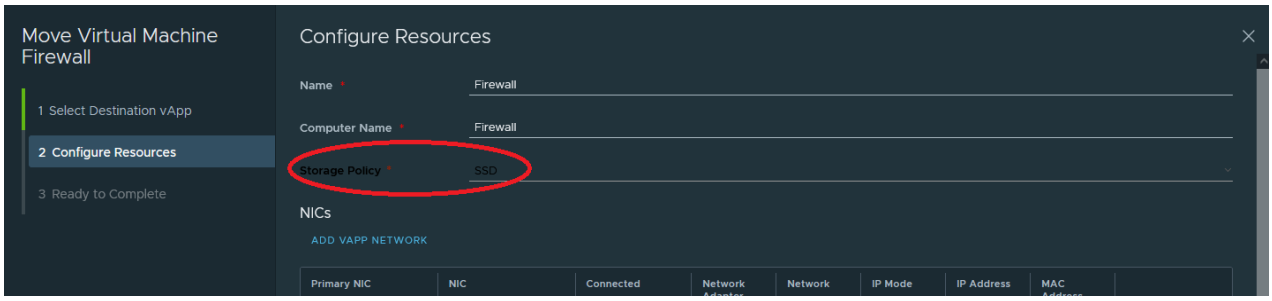


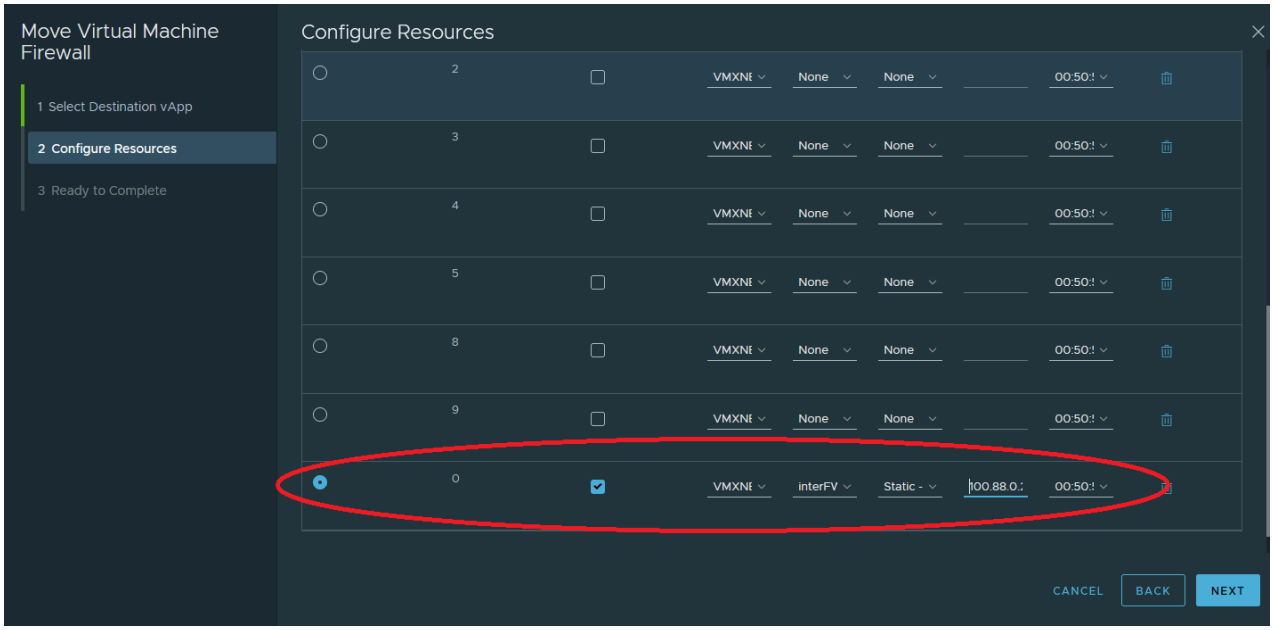


Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

É necessário voltar a configurar alguns parâmetros apesar de já o terem sido feitos anteriormente (necessário sempre que se move de vApps). Neste caso a Storage Policy e vamos configurar aqui as interfaces de redes. Para já configuramos apenas a ligação ao router Edge:

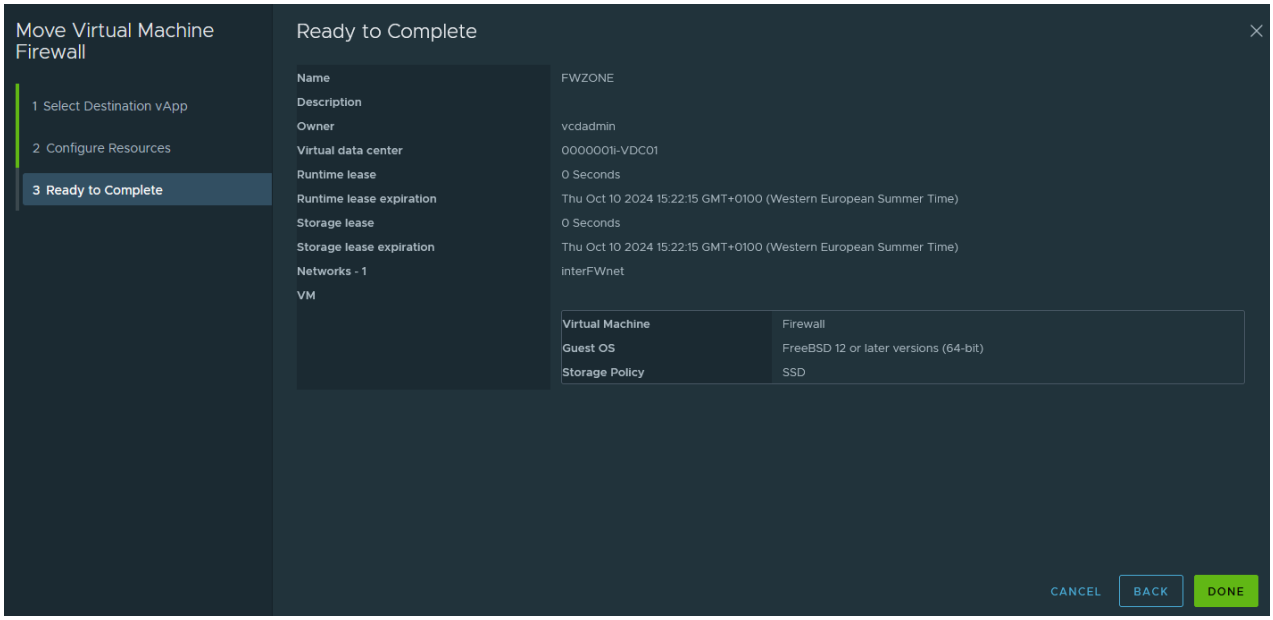
- NIC 0
- Primary NIC
- Connected
- Network Adapter Type: VMXNET3
- Network: selecionamos a rede criada anteriormente (neste exemplo, interFWnet)
- IP Mode: Static – Manual e introduzir o IP da firewall (10.10.10.2 no template mas pode ser alterado se necessário, em conformidade com a rede criada anteriormente)





Por fim, verificar as configurações e terminar com DONE:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

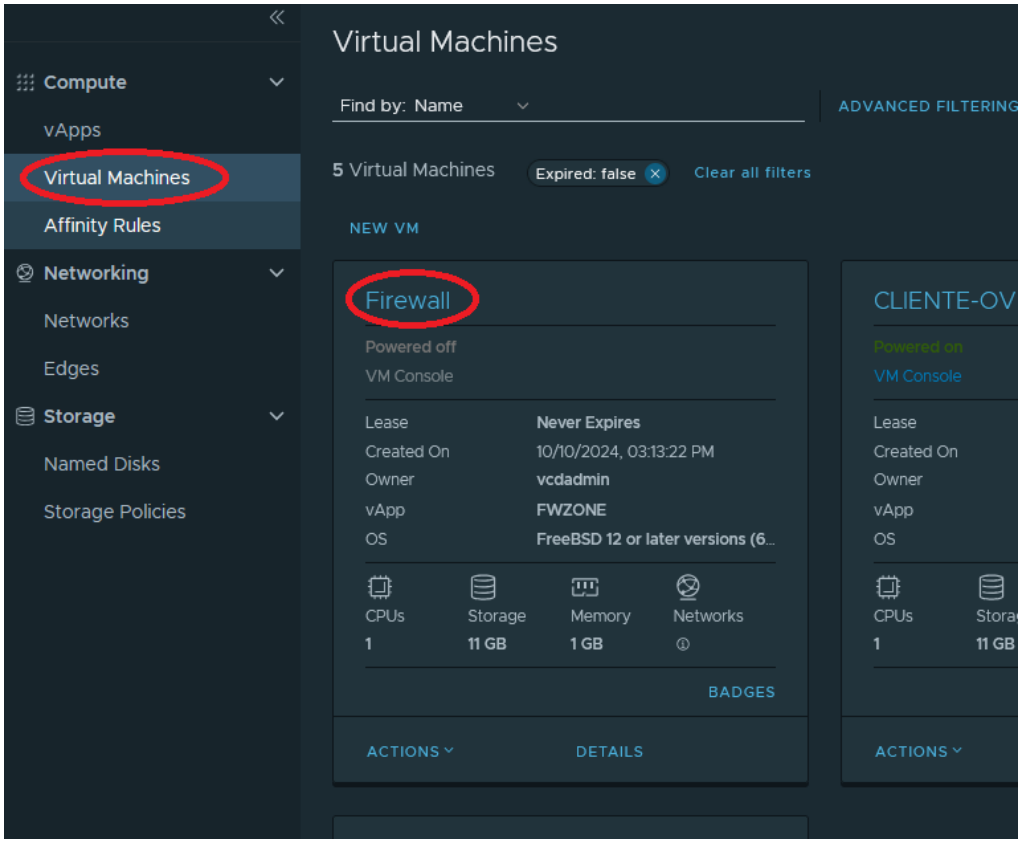


2.3 Configuração do router Edge

Neste ponto temos a instância de firewall instalada com conexão ao router.

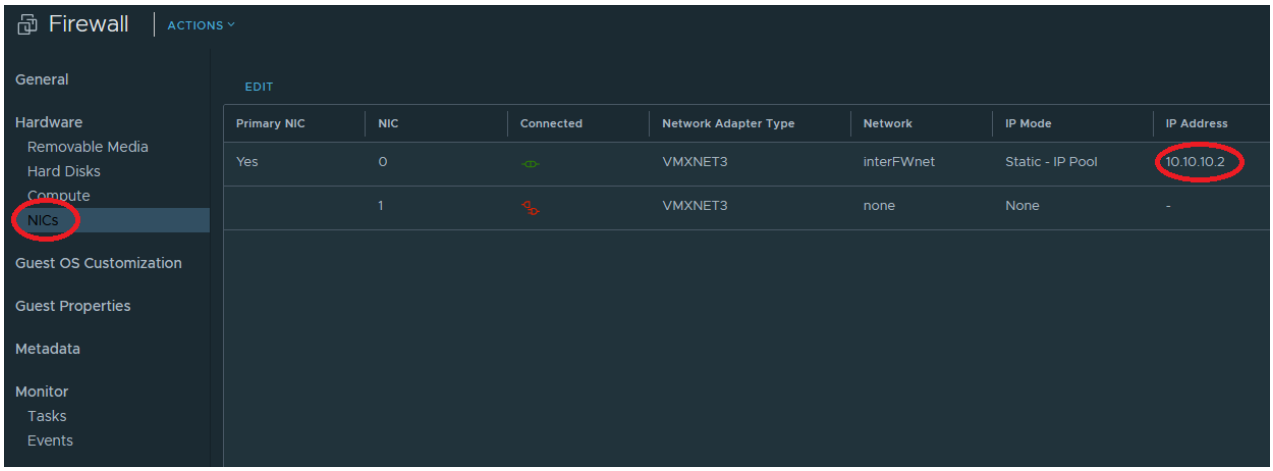
Falta configurar a conectividade lógica no router para permitir a passagem de tráfego de e para a firewall.

Podemos confirmar o endereço IP que configurámos para a firewall, indo a "Virtual Machines" e escolher a VM correspondente à firewall:



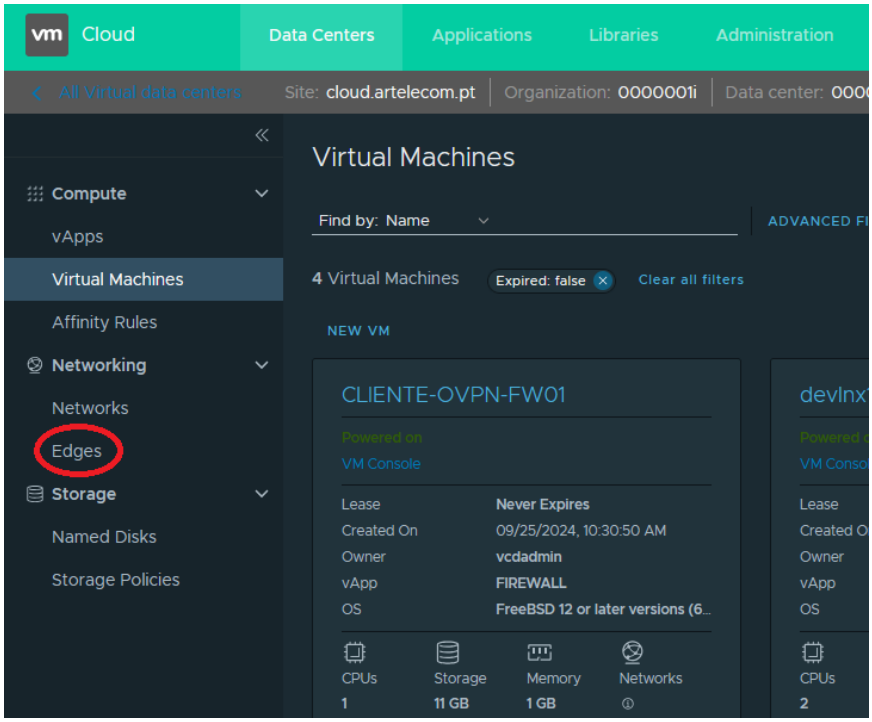
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

O endereço pode então ser consultado em NICs e corresponde ao IP Address da NIC 0 que se encontra ligada na rede que liga ao router, neste exemplo, interFWnet:



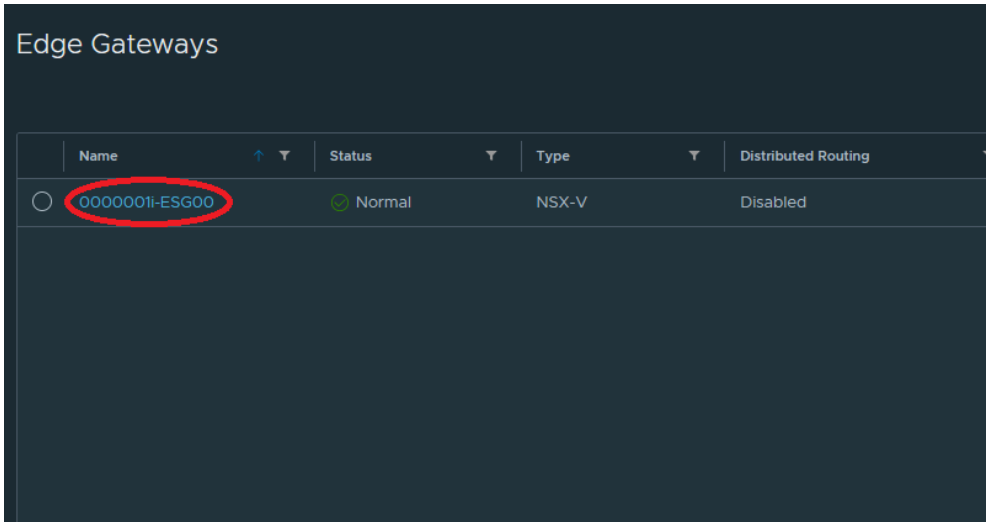
Neste caso, o endereço IP é 10.10.10.2

O passo seguinte é configurar o router Edge. Para isso, carregar em "Edges" no menu lateral esquerdo

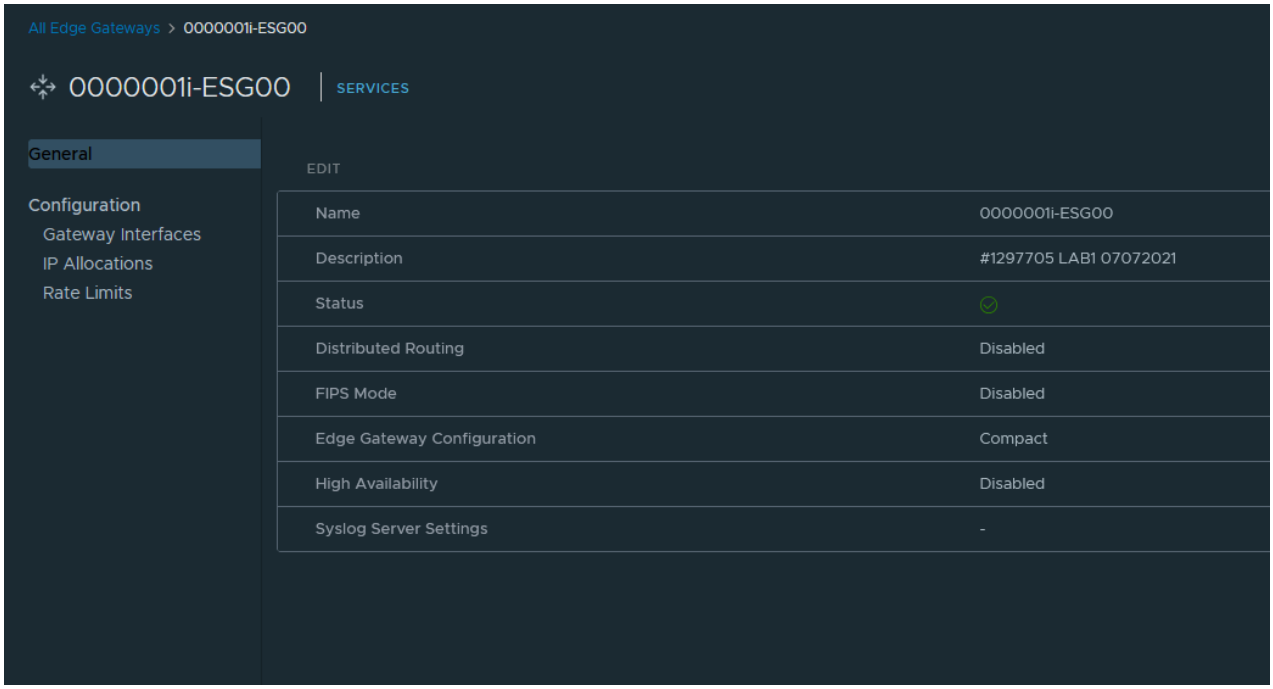


Vão ser mostrados os routers Edge atribuídos à sua organização e poderá carregar em cima dos mesmos para aceder à configuração:

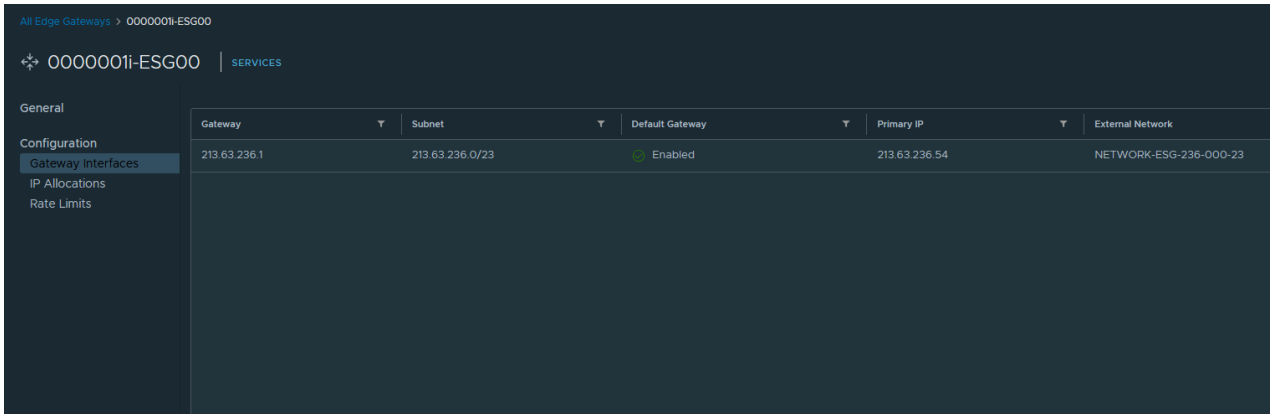
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

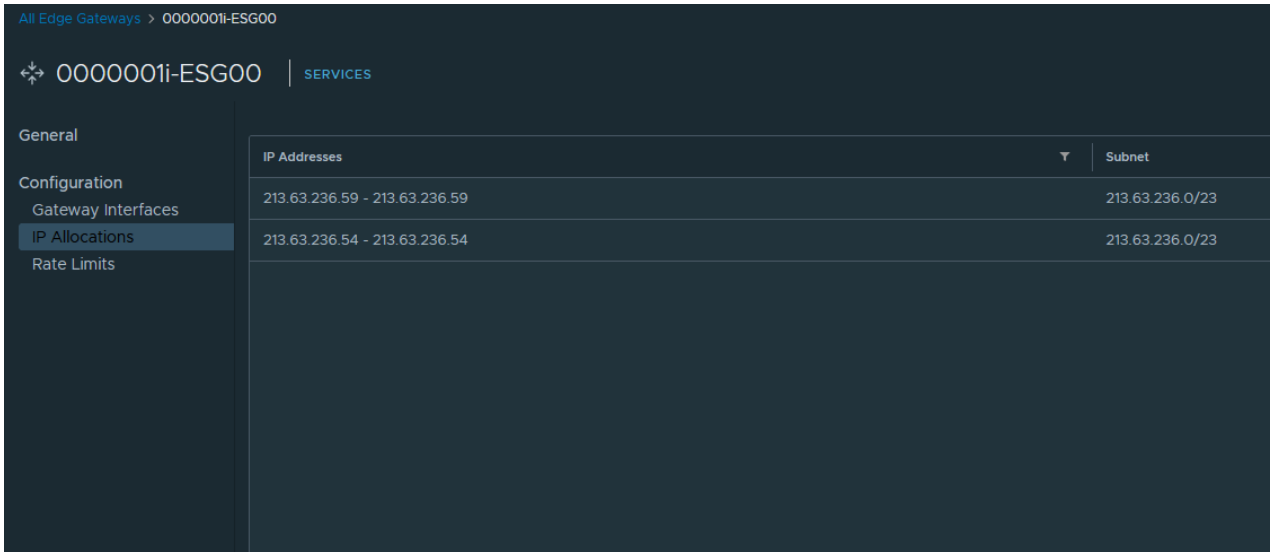


No ecrã que se segue pode-se consultar informações importantes que irão ser usadas nas configurações seguintes: Gateway interfaces e IP Allocations

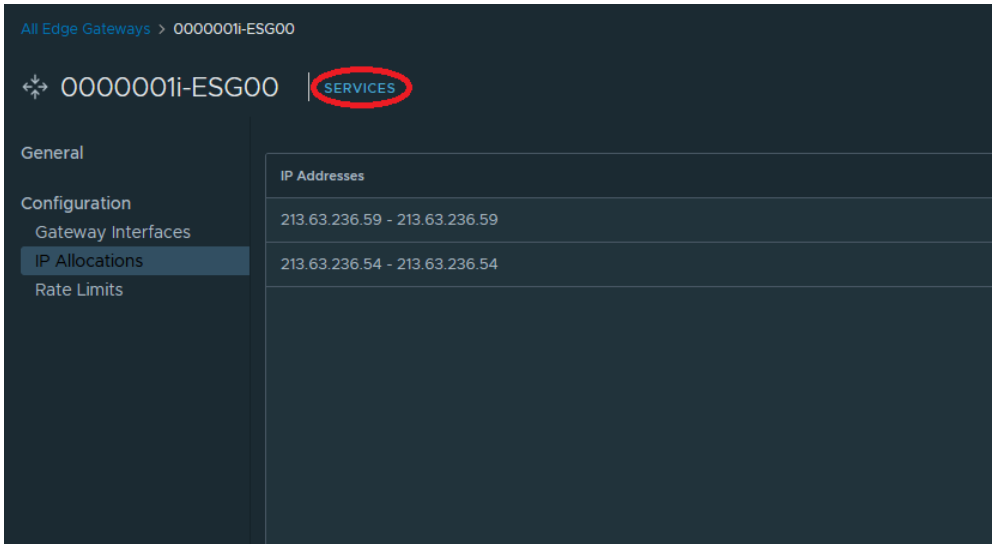


Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt





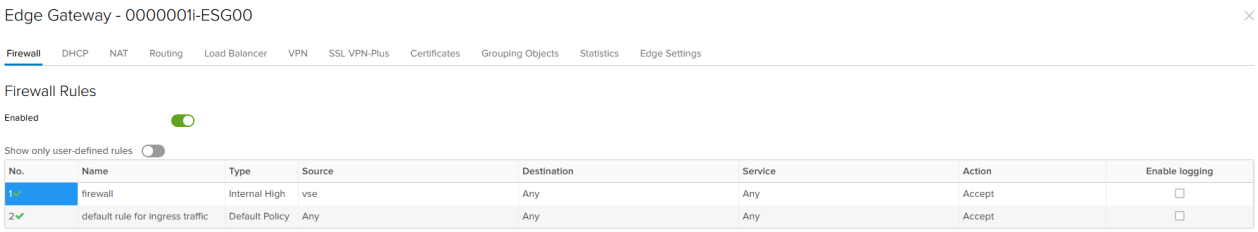
Para aceder aos menus de configuração carrega-se em "SERVICES" na barra superior:



Configuração de regras de firewall

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

Como o controlo do tráfego será feito pela firewall que instalámos, no menu de configuração "Firewall" apenas deve haver uma regra criada automaticamente e uma default policy permitindo tráfego de qualquer fonte, para qualquer destino e qualquer serviço:



Configuração das regras NAT

SNAT: deve existir uma única regra do IP da WAN da instância de firewall a usar (por exemplo, OPNsense) para o IP público do router Edge, para qualquer IP destino e qualquer porta destino:

ID	Type	Action	Applied on	Original		Translated		Protocol
				IP Address	Port	IP Address	Port	
196609	User-defined	SNAT	NETWORK-ESG-236-000-:	100.88.0.2	Any	213.63.236.54	Any	Any
196610	User-defined	DNAT	NETWORK-ESG-236-000-:	213.63.236.54	Any	100.88.0.2	Any	Any

DNAT: deve existir uma única regra do IP público do router Edge para o IP da WAN da instância de firewall a usar (por exemplo, OPNsense), qualquer protocolo, qualquer IP de origem e qualquer porta de origem:

ID	Type	Action	Applied on	Original		Translated		Protocol
				IP Address	Port	IP Address	Port	
196609	User-defined	SNAT	NETWORK-ESG-236-000-:	100.88.0.2	Any	213.63.236.54	Any	Any
196610	User-defined	DNAT	NETWORK-ESG-236-000-:	213.63.236.54	Any	100.88.0.2	Any	Any

Configuração DHCP

O serviço DHCP deve ficar inativo, não configurado

Configuração de Routing

O routing deve ficar no estado inativo, não configurado

Load Balancer

O Load Balancer deve ficar no estado inativo, não configurado

IPsec e SSL VPNs

Não devem ser configuradas quaisquer VPNs no router Edge, devendo para isso fazê-lo na instância de firewall a usar (por exemplo, OPNsense).

Certificados

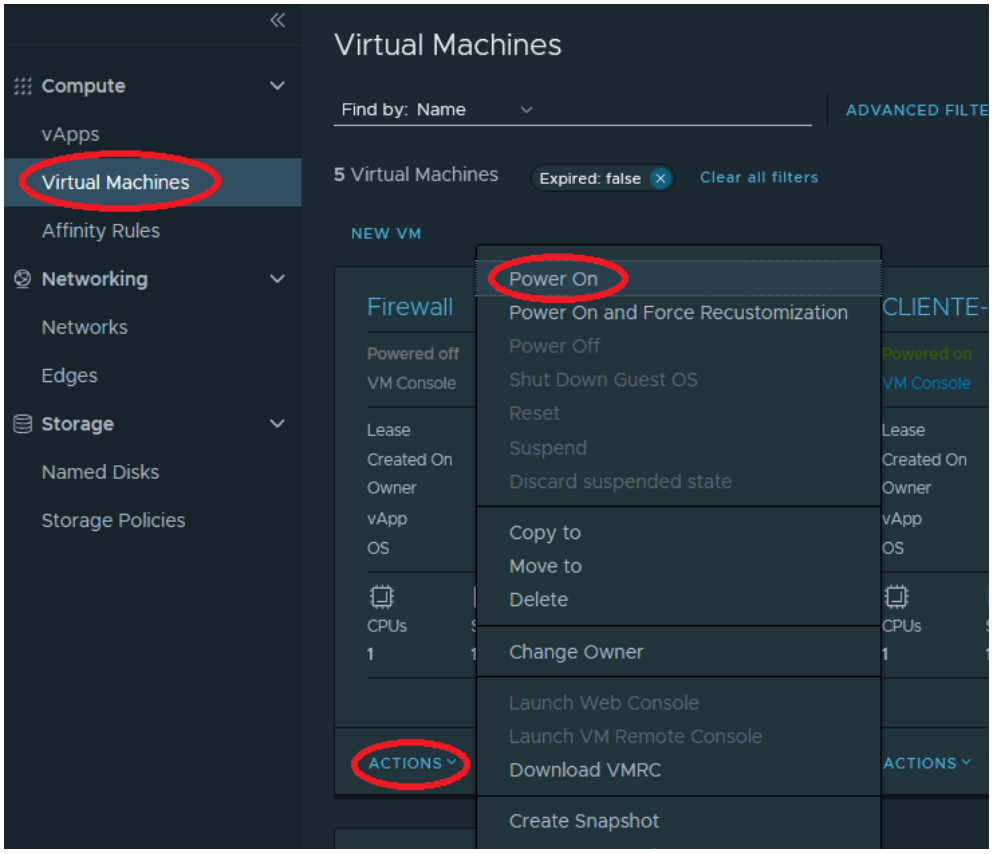
A configuração de certificados deve ficar conforme a configuração inicial efetuada pela Ar

2.4 Ativação da instância de firewall

Agora que a configuração de conectividade está concluída, vamos iniciar a firewall.

Ir a "Virtual Machines", escolher a VM correspondente e fazer "Power On":

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



A partir deste momento a firewall está ativa e pode ser configurada. Note-se que apenas existe conectividade com o router e irá ser necessário adicionar tantas interfaces de rede e respetiva ligação às redes da Organização quantas as que se queiram.

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

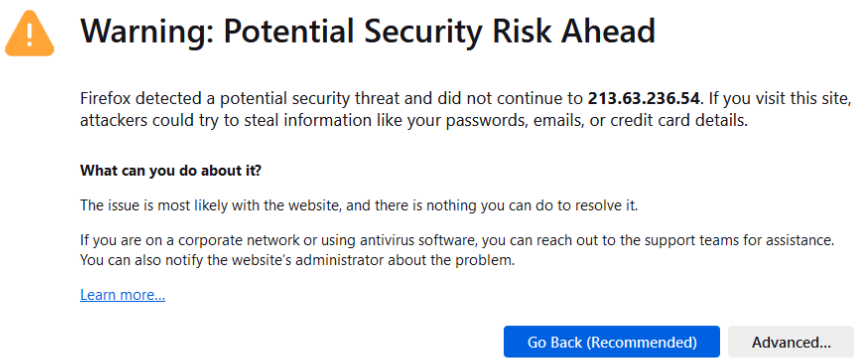
3. ACESSO À CONSOLA DA FIREWALL

Por defeito a firewall aceita ligação à consola por qualquer interface que possua e esteja ativada.

Este acesso é feito via browser em https ao endereço IP da interface em questão.

Para efeitos deste manual consideramos o IP público da firewall como sendo o 213.63.236.54, pelo que o acesso far-se-á através do URL https://213.63.236.54

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:

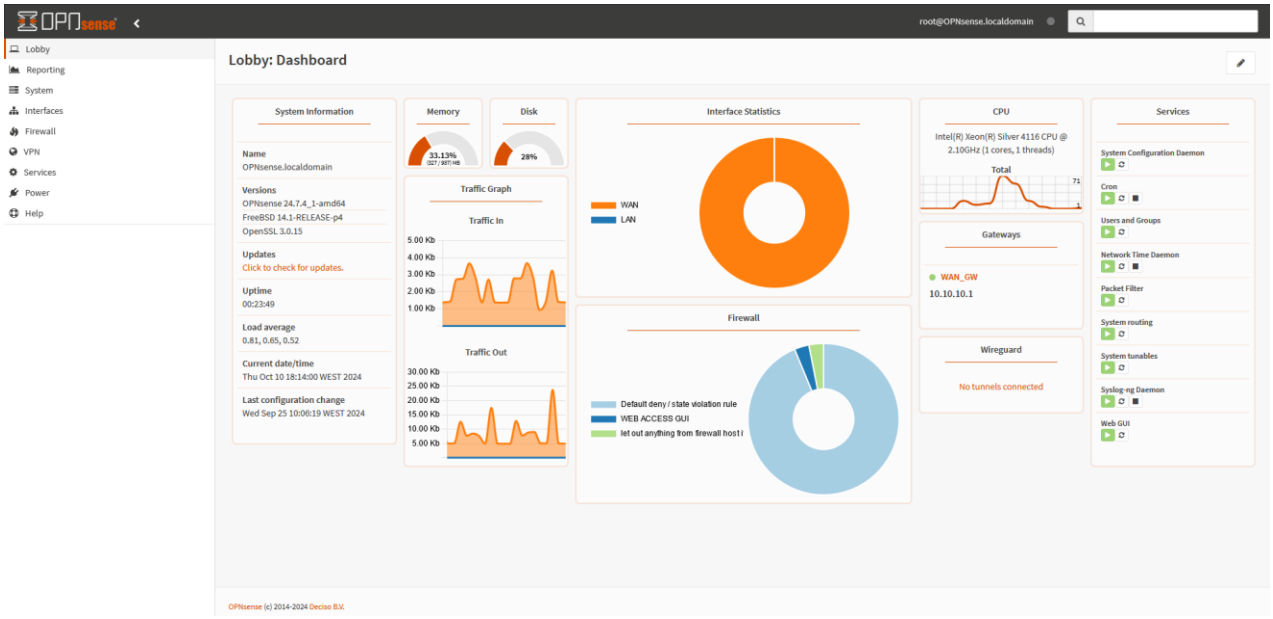
- **Username:** root
- **Password:** !OperJazz!

Recomendamos que altere a password após o primeiro login.

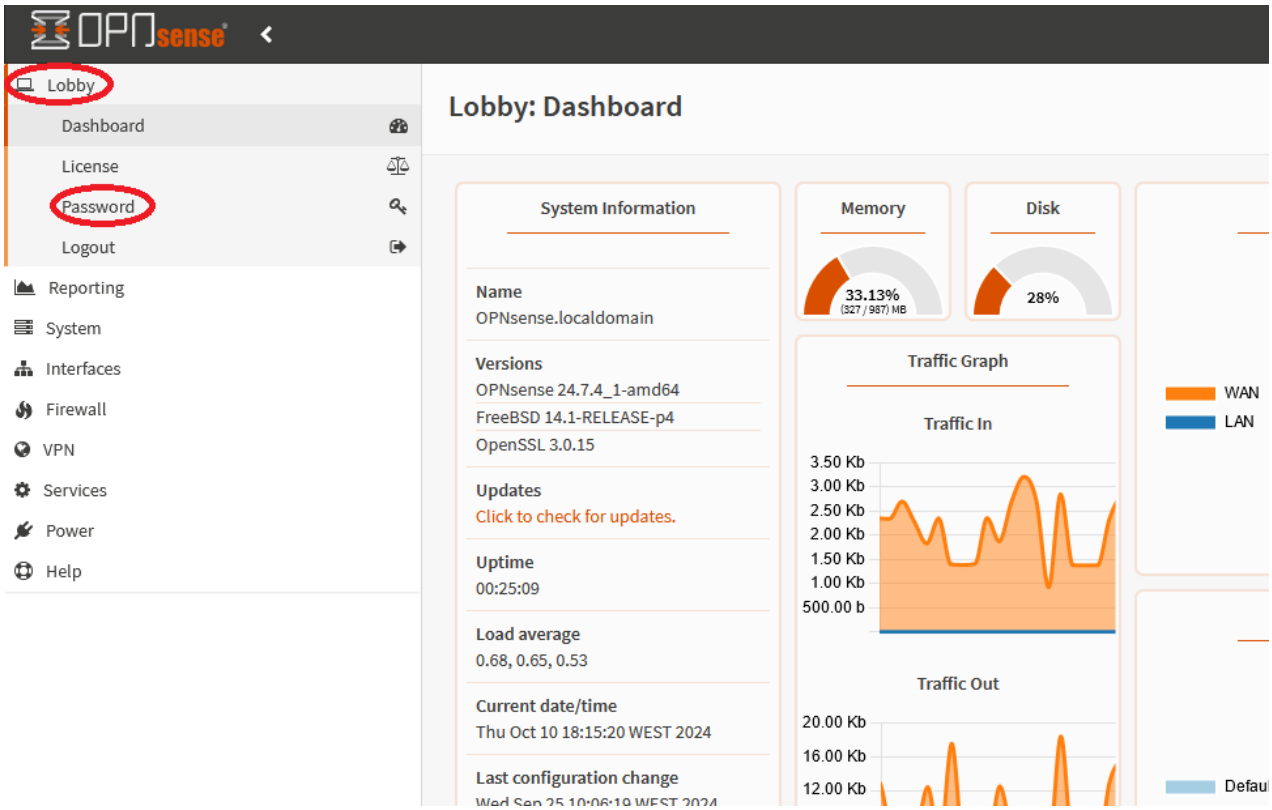
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

4. ALTERAR PASSWORD

Após o login será mostrado o dashboard e o menu a partir do qual poderá configurar a firewall:



Para mudar a password de acesso à consola, ir a "Lobby" e carregar em "Password":



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

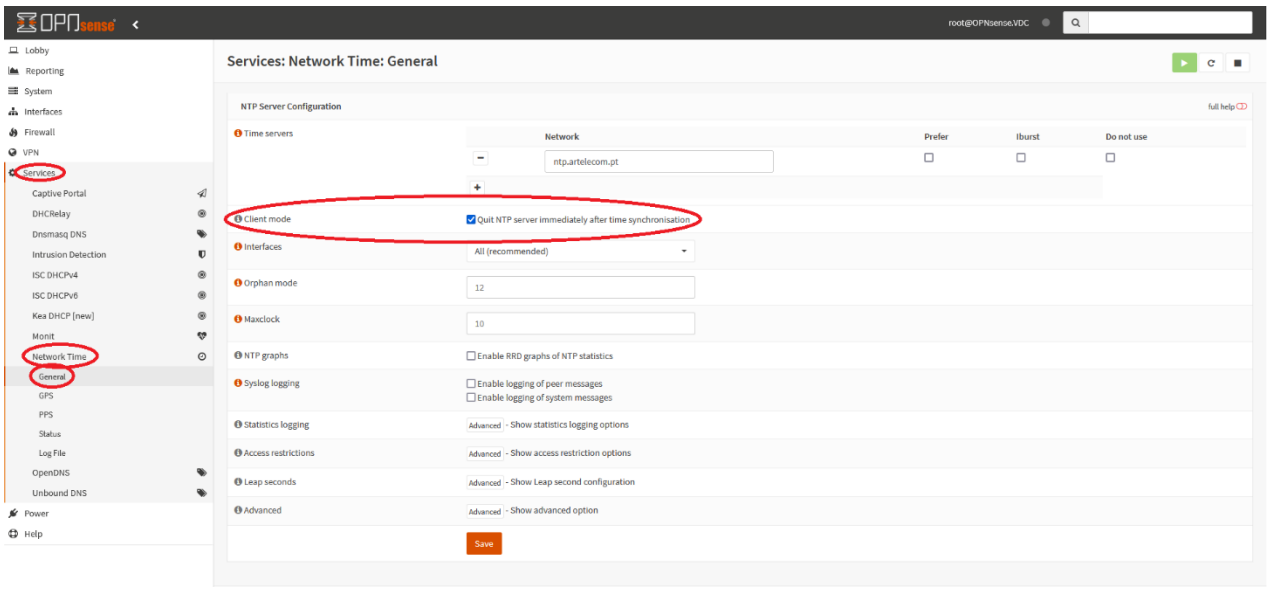
5. CONFIGURAÇÕES DE SEGURANÇA

É conveniente efetuar algumas alterações à configuração standard, por forma a minimizar o risco de ciber-ataques.

As configurações sugeridas nos pontos seguintes já estão implementadas nas últimas versões do template da OPNsense no VDC da Ar.

5.1 NTP

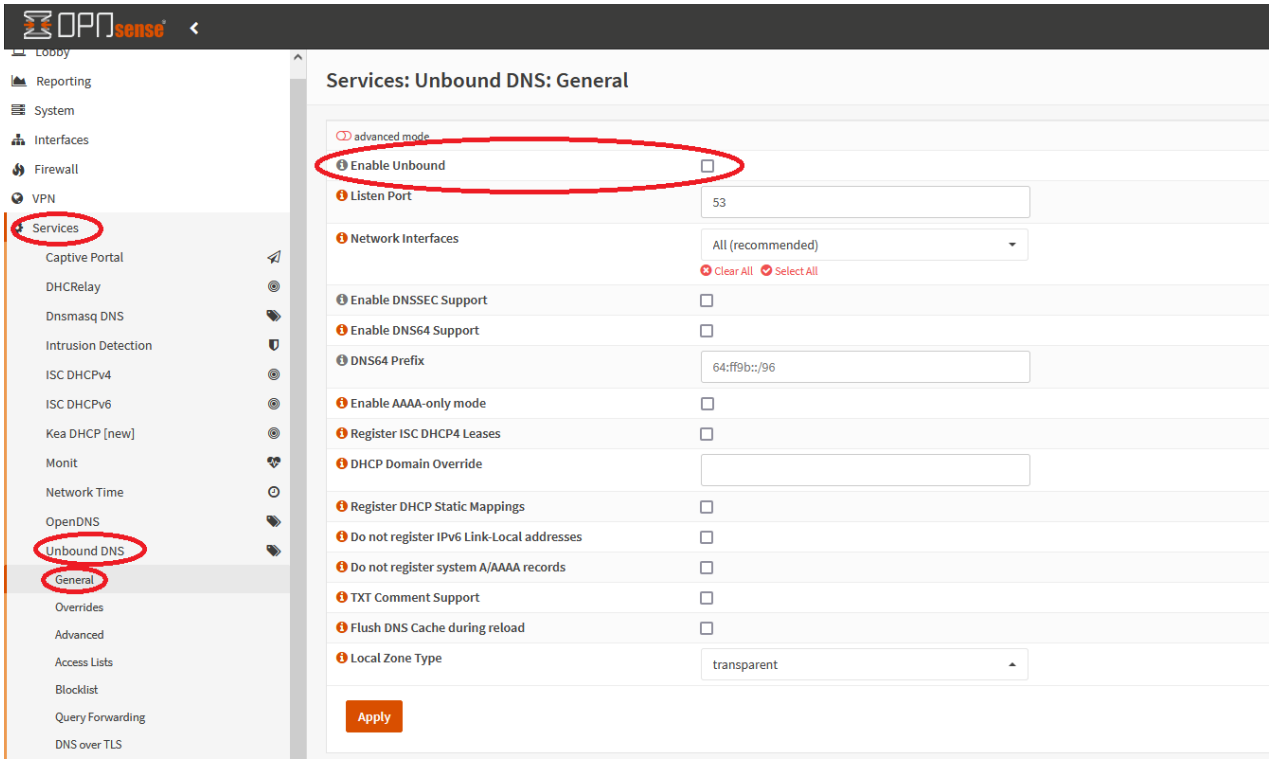
Para que a OPNsense não responda a pedidos NTP vindos do exterior, deve-se aplicar o modo cliente, indo a **Services** -> **Network Time** -> **General** e ativar o modo cliente:



5.2 DNS

Sugerimos que a função de unbound DNS esteja desligada, devendo confirmar isso em **Services** -> **Unbound DNS** -> **General**:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

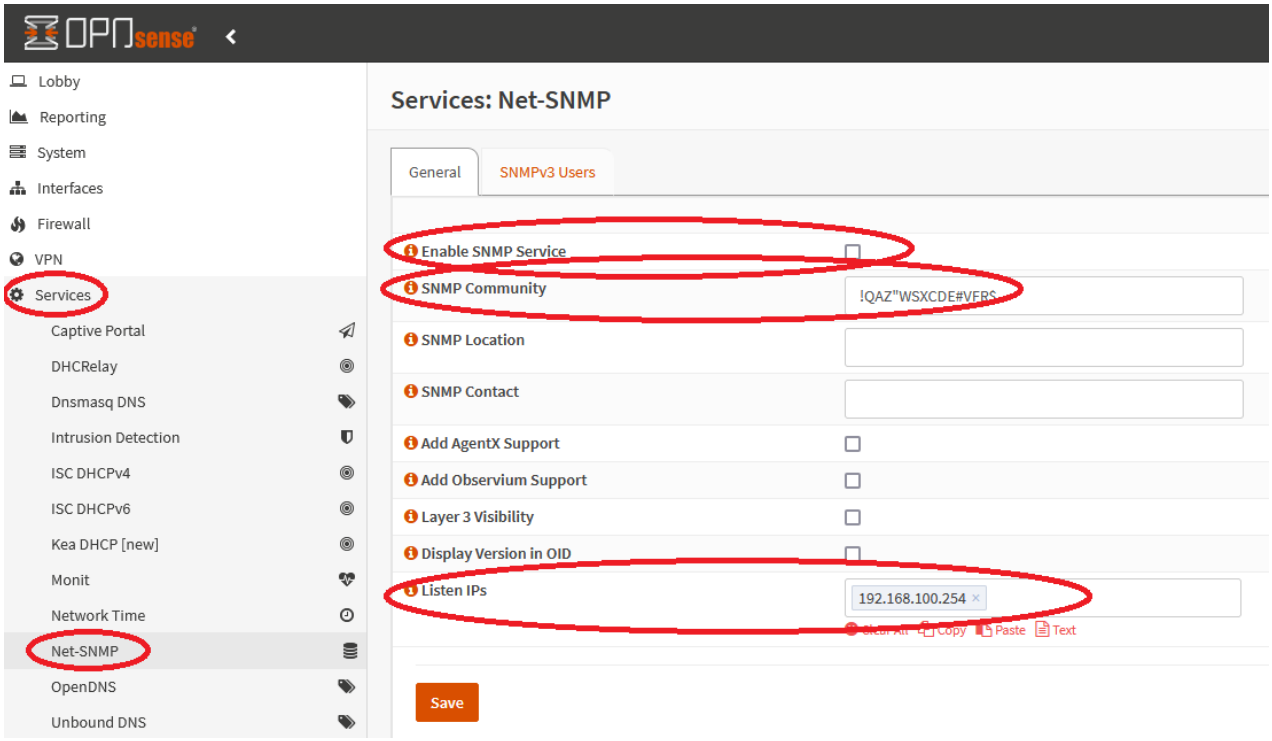


5.3 SNMP

Mesmo com o serviço SNMP desligado, recomendamos que seja definida uma *community* complexa e um IP de uma interface interna.

Para o fazer, ir a **Services -> Net-SNMP**:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



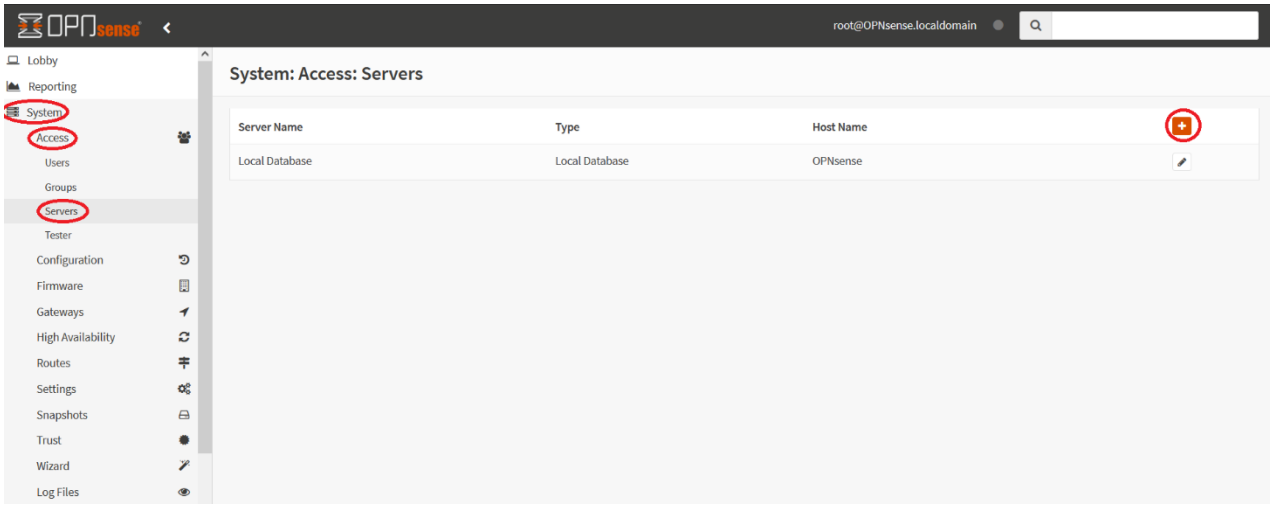
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

6. AUTENTICAÇÃO 2FA

Neste capítulo demonstra-se como configurar a autenticação de dois fatores que irá usar o Google Authenticator como autenticador. Todos os serviços à exceção do acesso à consola SSH irão utilizar esta solução.

6.1 Criar servidor de autenticação

O primeiro passo é criar um servidor de autenticação, indo a **System** -> **Access** -> **Servers** e carregar em **+**:



Preencher os campos conforme abaixo:

- Dar um nome ao servidor
- Type: Local + Timebased One Time Password
- Token length: deixar por defeito (6)
- Time window: deixar vazio
- Grace period: deixar vazio
- Reverse token order: deixar unchecked

6.2 Google authenticator

Instalar o Google Authenticator no dispositivo pretendido

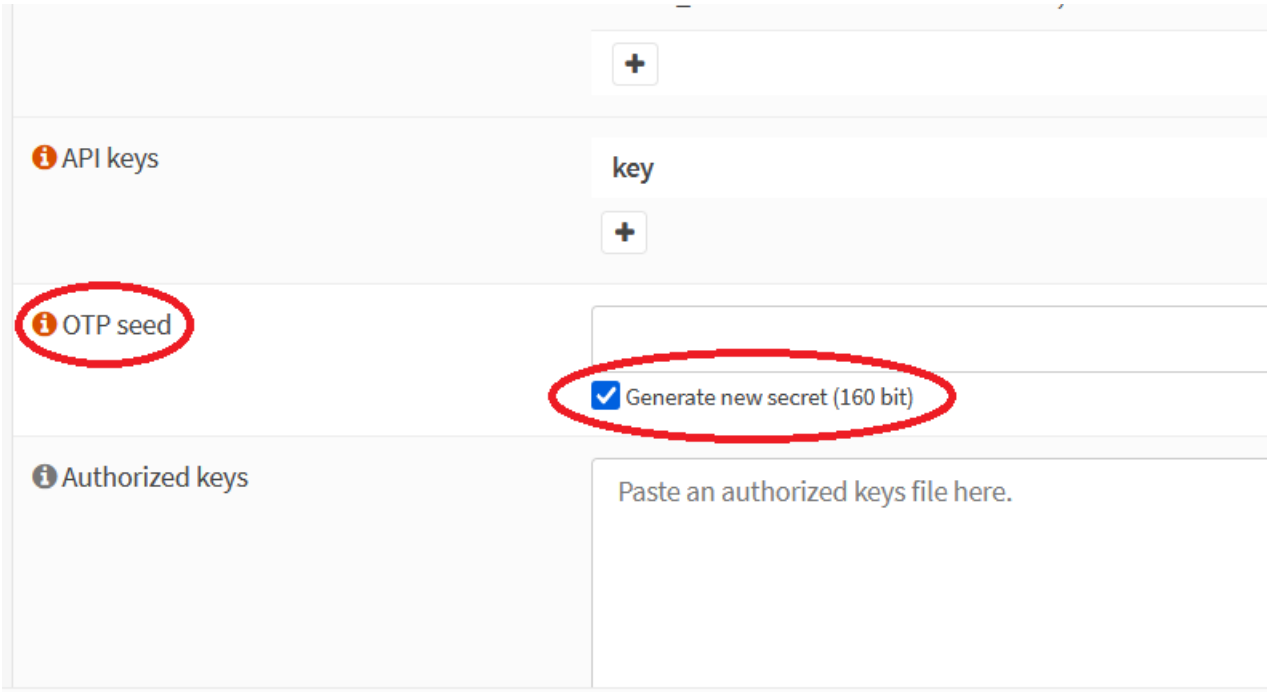
6.3 Configurar utilizador

O passo seguinte é configurar o utilizador (ou criar um novo).

Para isso, ir a **System** -> **Access** -> **Users** e criar um utilizador carregando em **+** ou editar o utilizador se já existia.

Para configurar a autenticação de dois fatores, ir a **OTP seed**, carregar em **Generate new (160bit) secret** e salvar.

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

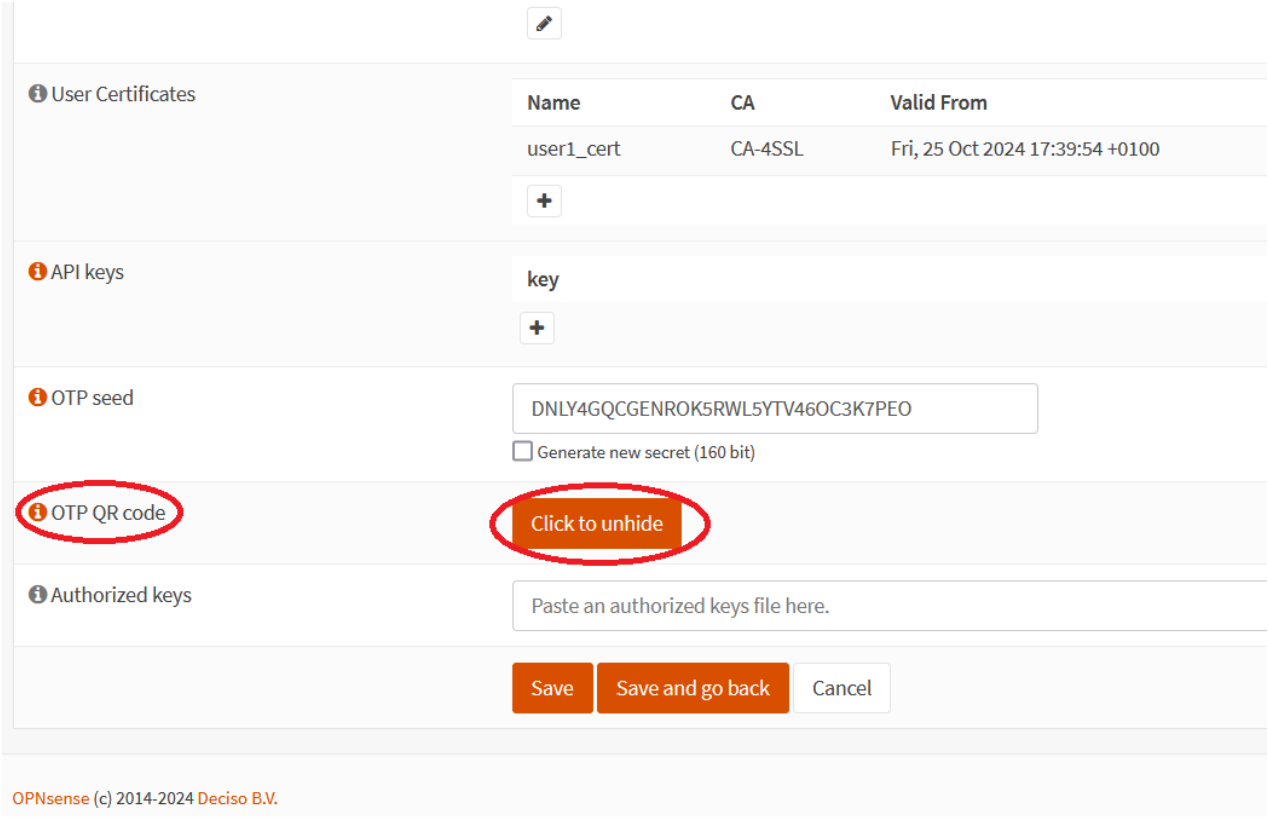


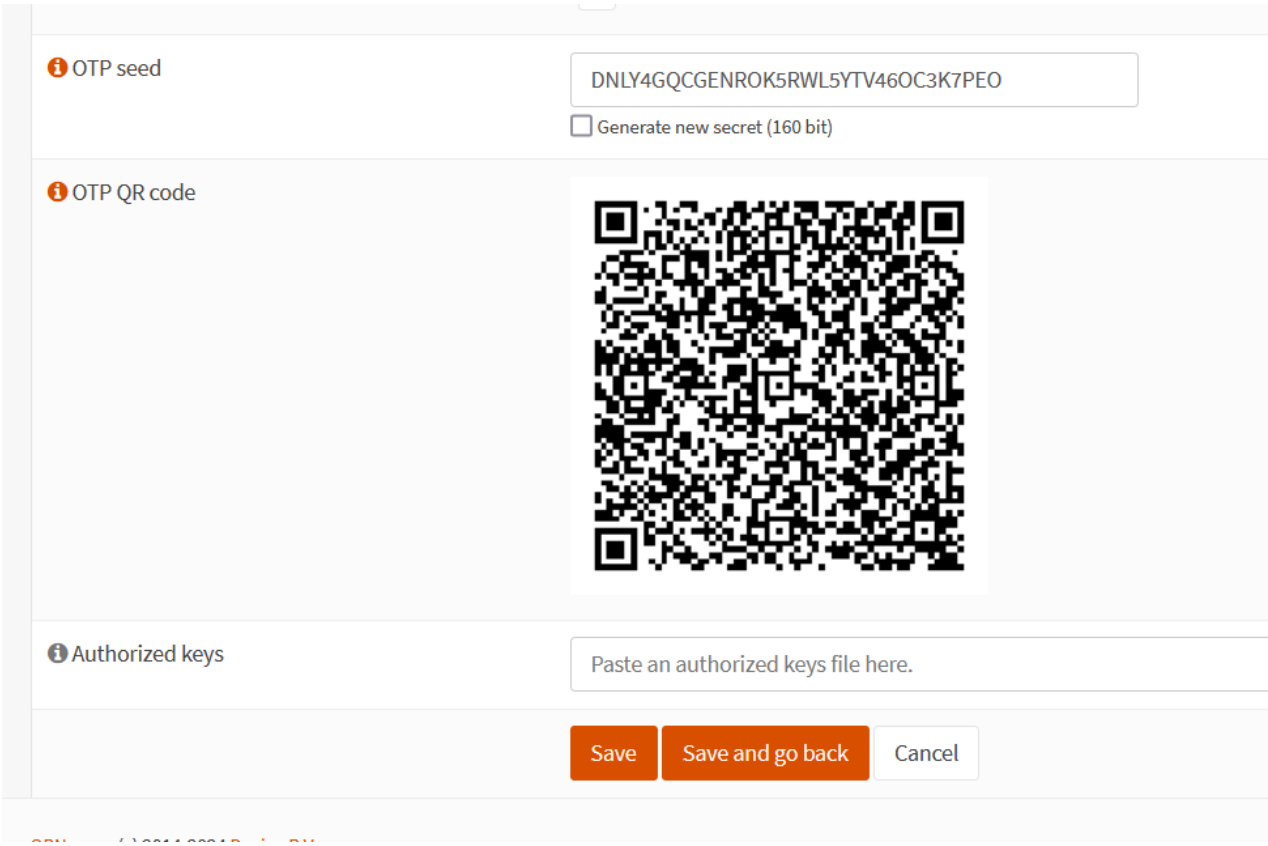
6.4 Ativar autenticação no Google Authenticator

Para possibilitar a autenticação, é necessário configurá-la no Google Authenticator.

Para isso, editar novamente o utilizador, ir até **OTP seed** e carregar em "**Click to unhide**" em **OTP QR code,** para mostrar o código QR a importar no Google Authenticator:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



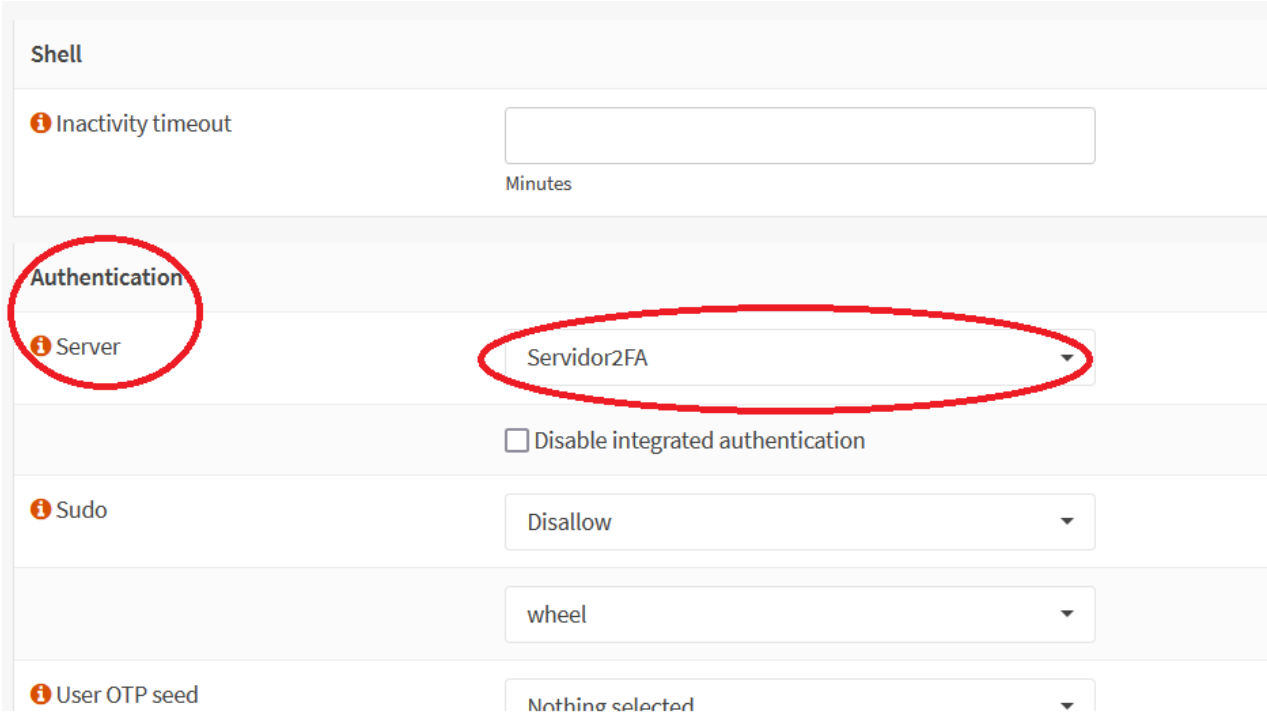


Agora apenas é necessário abrir a aplicação Google Authenticator no seu dispositivo e adicionar uma nova entrada com este código QR.

6.5 Ativar servidor de autenticação

Por defeito, a OPNsense usa o método de autenticação simples, usando a base de dados local.

Para definir a autenticação de dois fatores usando o servidor criado para esse efeito, deve-se ir a **System** -> **Settings** -> **Administration** e na secção **Authentication** escolher o servidor criado anteriormente e gravar:



A partir do momento em que se ativa o servidor de autenticação de dois fatores, todos os utilizadores necessitam do código do autenticador (neste exemplo, Google Authenticator) para efetuarem login, inclusivamente o utilizador **root**!

ANTES DE ATIVAR O SERVIDOR DE AUTENTICAÇÃO, DEVE-SE OBTER A OTP SEED E CONFIGURAR O AUTENTICADOR PARA O UTILIZADOR ROOT, conforme descrito nos pontos 6.3 e 6.4 !

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

7. CONEXÃO A REDE DO VDC

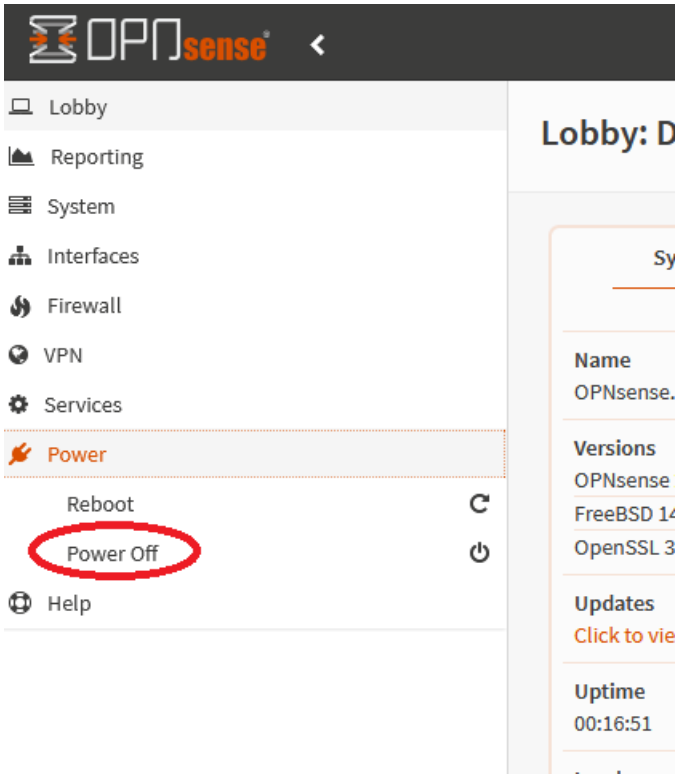
A firewall instalada irá gerir tráfego entre o exterior e as redes internas.

7.1 Adição de interface no virtual data center

O template de OPNsense da Ar já contempla o número máximo de interfaces possível, correspondendo a 10 NIC, pelo que, não é necessário executar este ponto. Apesar disso, optámos por apresentar o procedimento para referência ou alterações futuras.

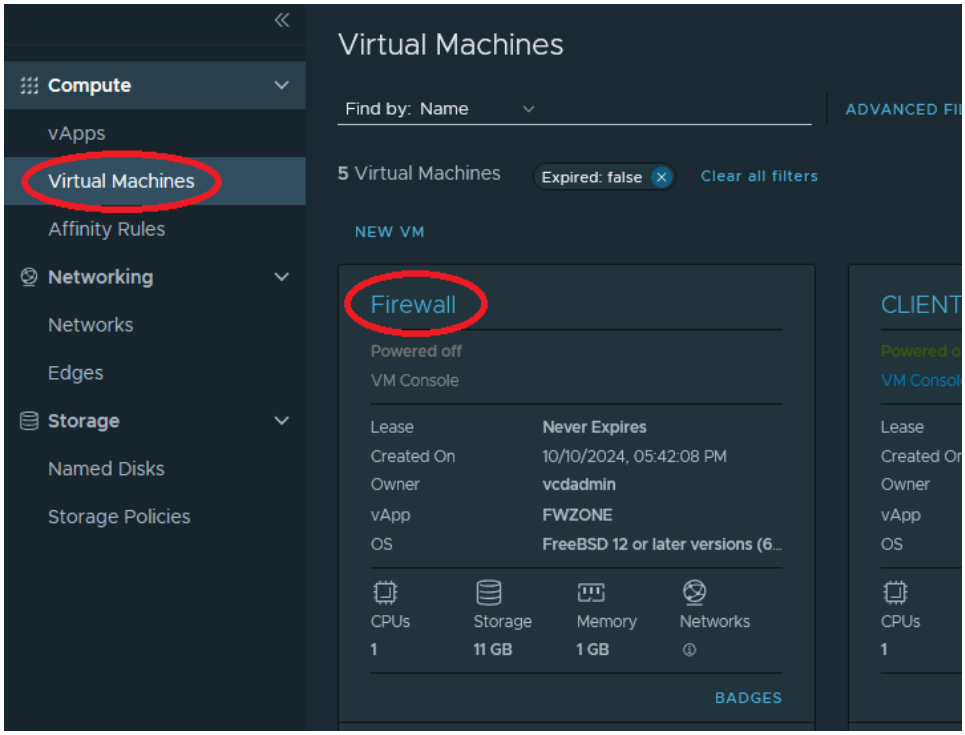
Esta operação tem de ser efetuada com a firewall em power off!

Aceder ao portal de gestão do virtual data center e garantir que a VM está desligada. Caso não esteja, desligá-la via portal de administração da mesma:

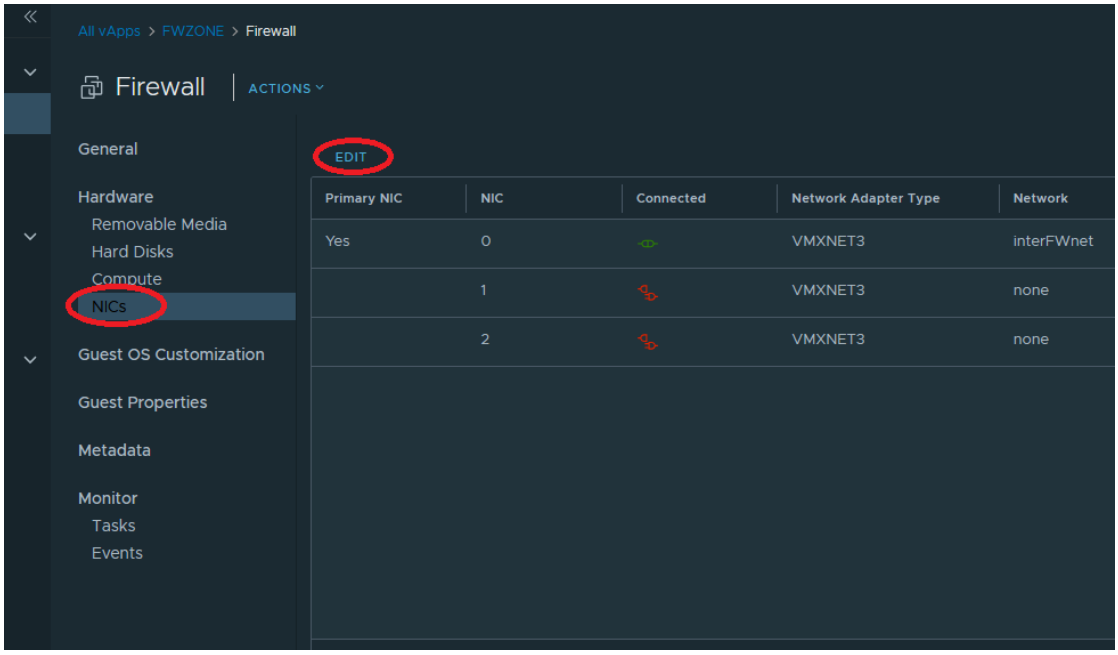


Assim que a mesma estiver em modo power off, para adicionar uma nova interface (NIC) à instância de firewall ir a "Virtual Machines" no menu lateral esquerdo, selecionar a VM com a firewall

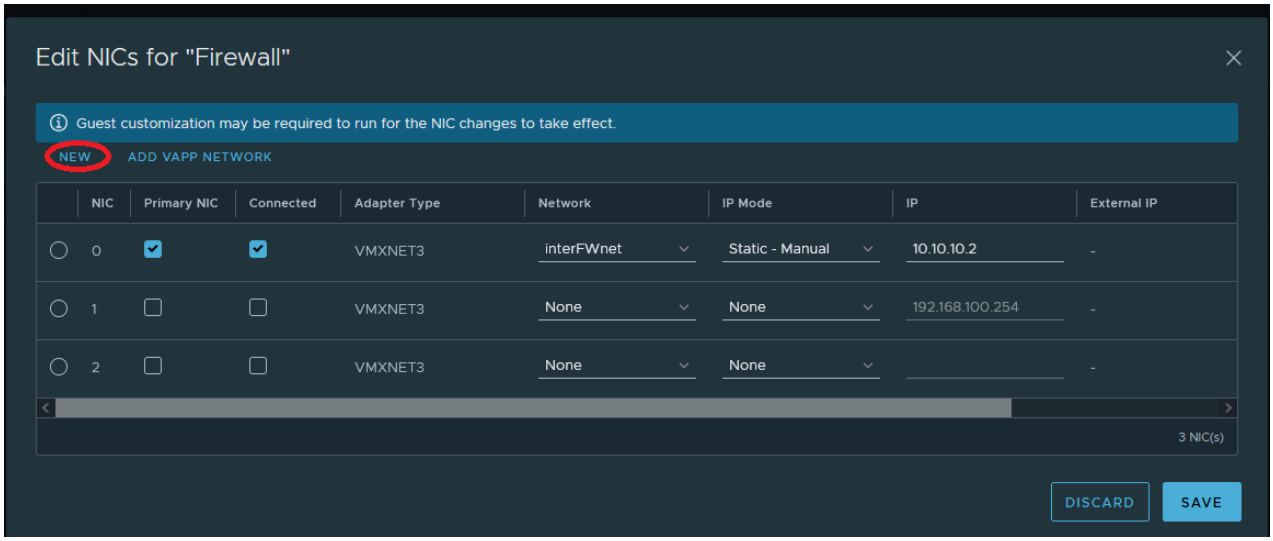
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



e para adicionar um novo interface, ir a "NICs" seguido de "EDIT" e posteriormente "NEW":



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



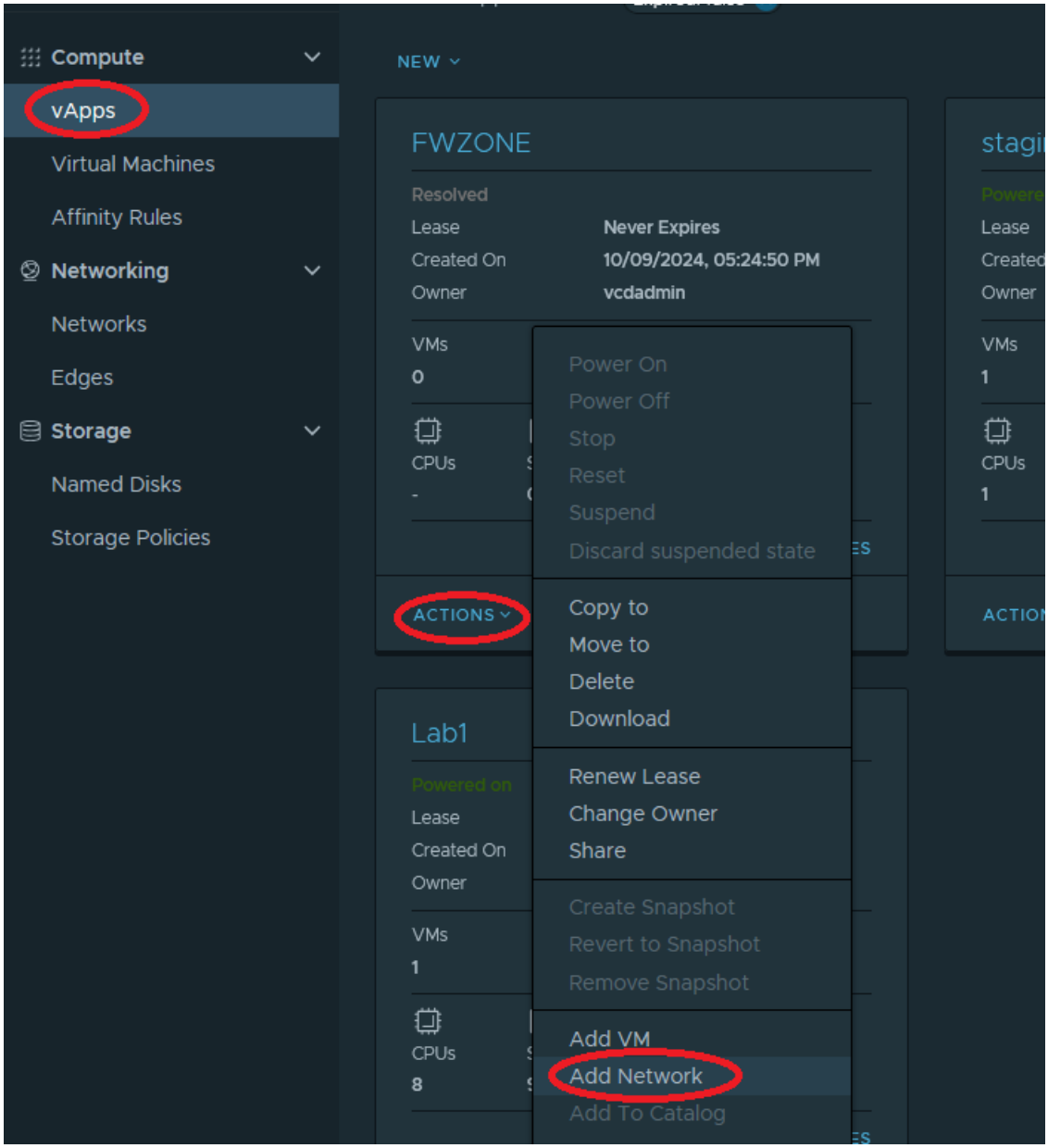
É possível adicionar NICs no vCloud com a máquina ligada mas a firewall ficará num estado corrompido. Para apagar interfaces no vCloud é necessário fazer primeiro o shutdown/power off.

7.2 Conexão à rede pretendida

Agora que a interface está criada é necessário ligá-la à rede pretendida. No caso da firewall não estar numa vApp onde esta rede já se encontre configurada, é necessário configurar a rede na vApp da firewall.

Para o fazer, carregar em "vApps" no menu lateral esquerdo e em "ACTIONS" da vApp correspondente, seguido de "Add Network":

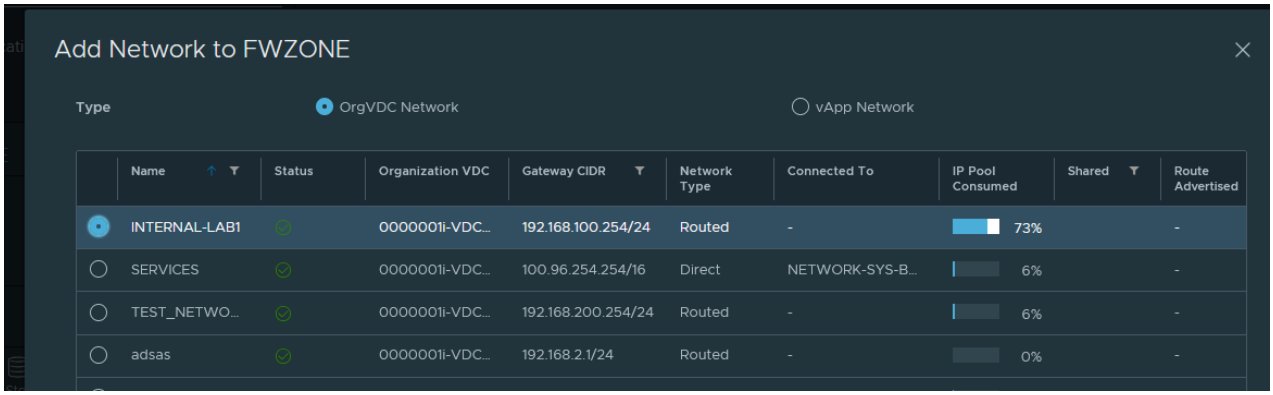
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



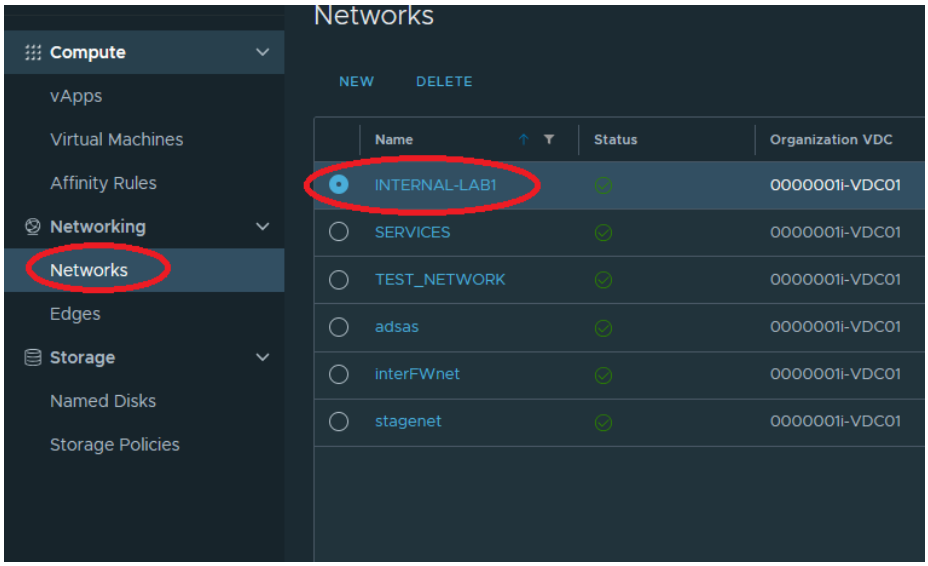
Selecionar opção "OrgVDC Network"

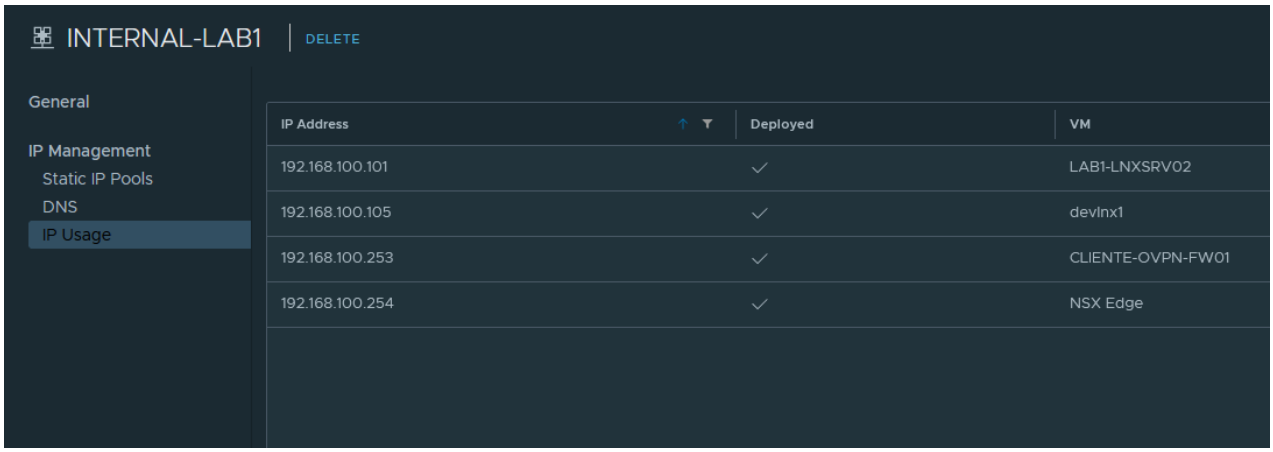
e escolher a rede pretendida:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



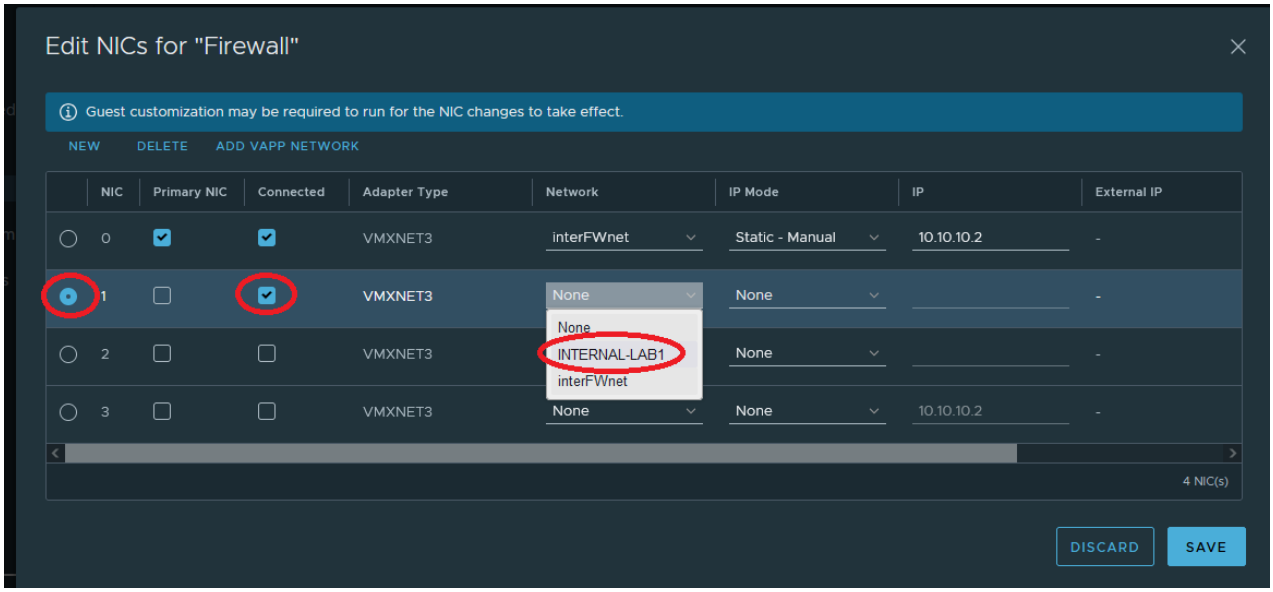
Agora é possível associar a NIC da firewall a esta rede, sendo necessário escolher um endereço IP para a mesma. Para saber os endereçamentos utilizados pode ir a "Networks" no menu lateral esquerdo, carregar na rede pretendida e depois em "IP Usage".



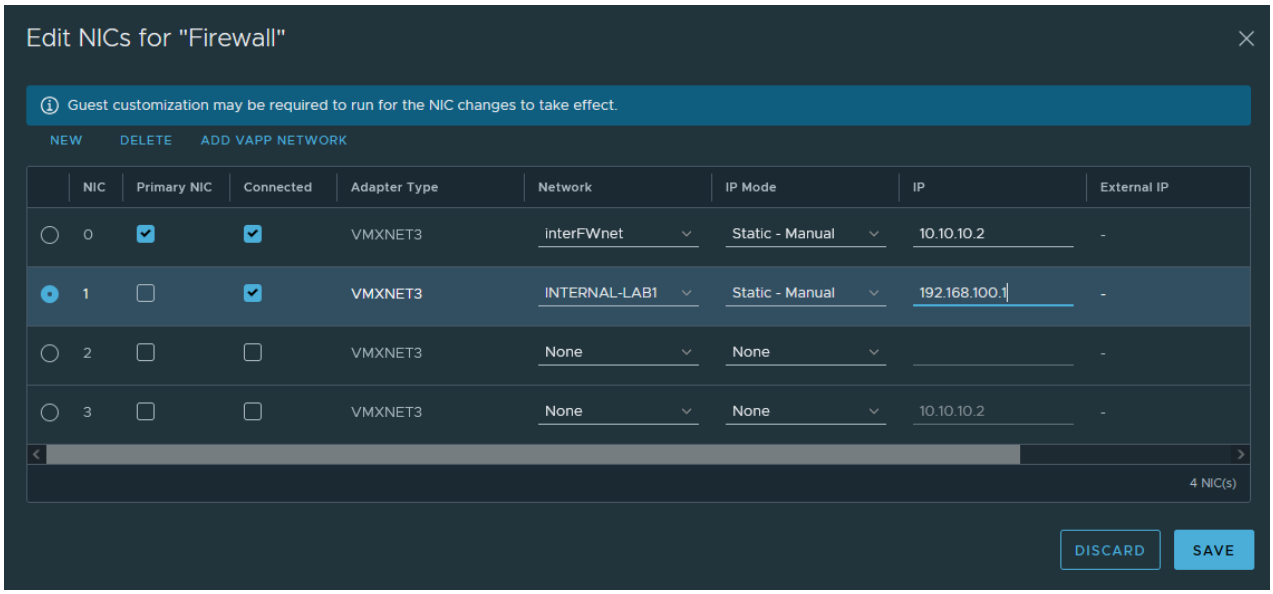


Escolhendo um IP disponível (por exemplo, 192.168.100.1), ir a "Virtual Machines" no menu lateral esquerdo, selecionar a VM com a firewall e ir a "NICs" seguido de "EDIT" e escolher uma interface e a rede pretendida:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



Pode optar-se por usar o IP obtido a partir da pool mas caso pretenda atribuir um específico deverá escolher o modo manual e indicar o IP escolhido:



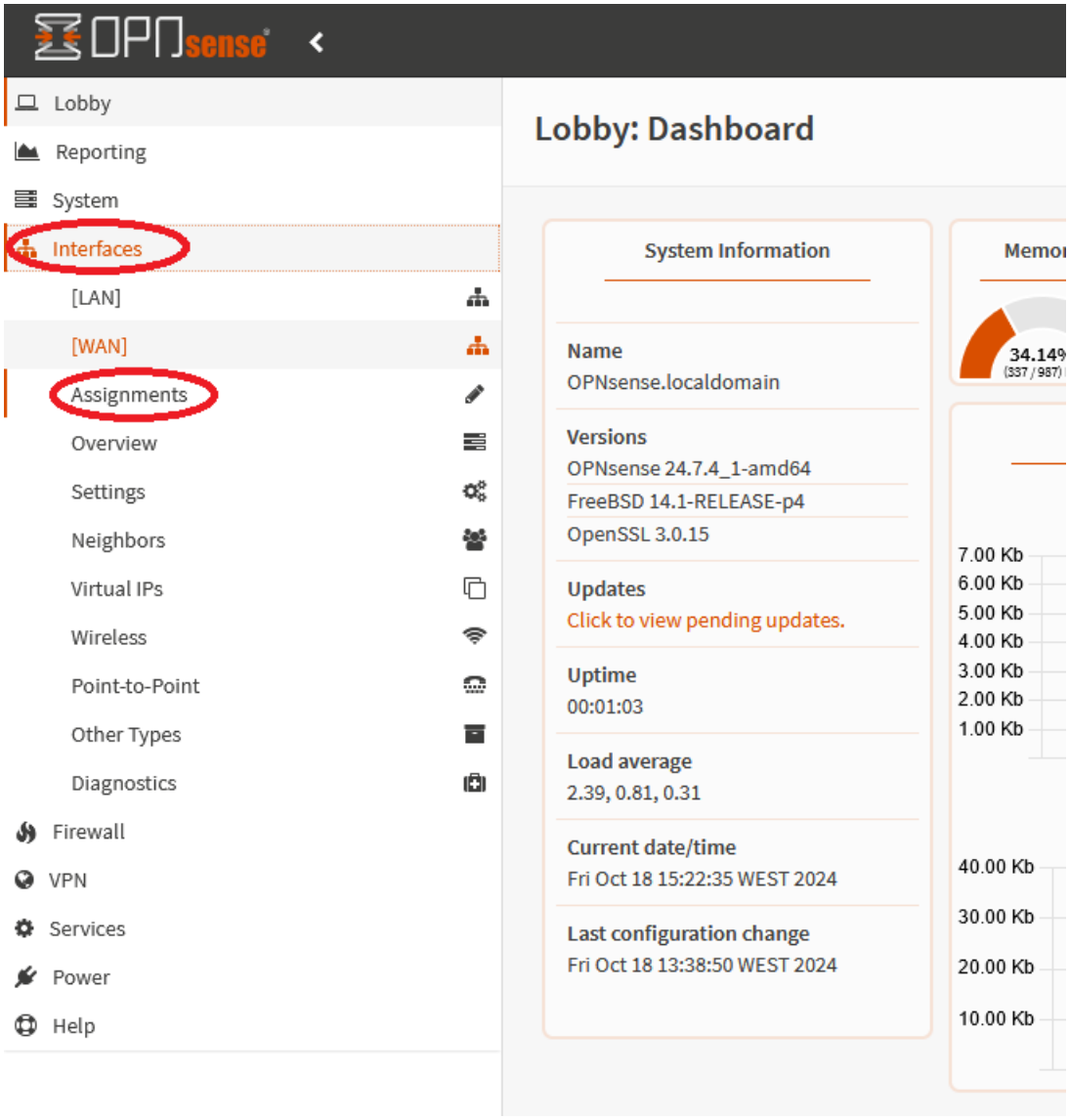
De seguida faz-se power on da firewall e configura-se a interface.

7.3 Configuração da interface na OPNsense

Depois de a OPNsense detetar a nova interface é necessário assigná-la e configurá-la.

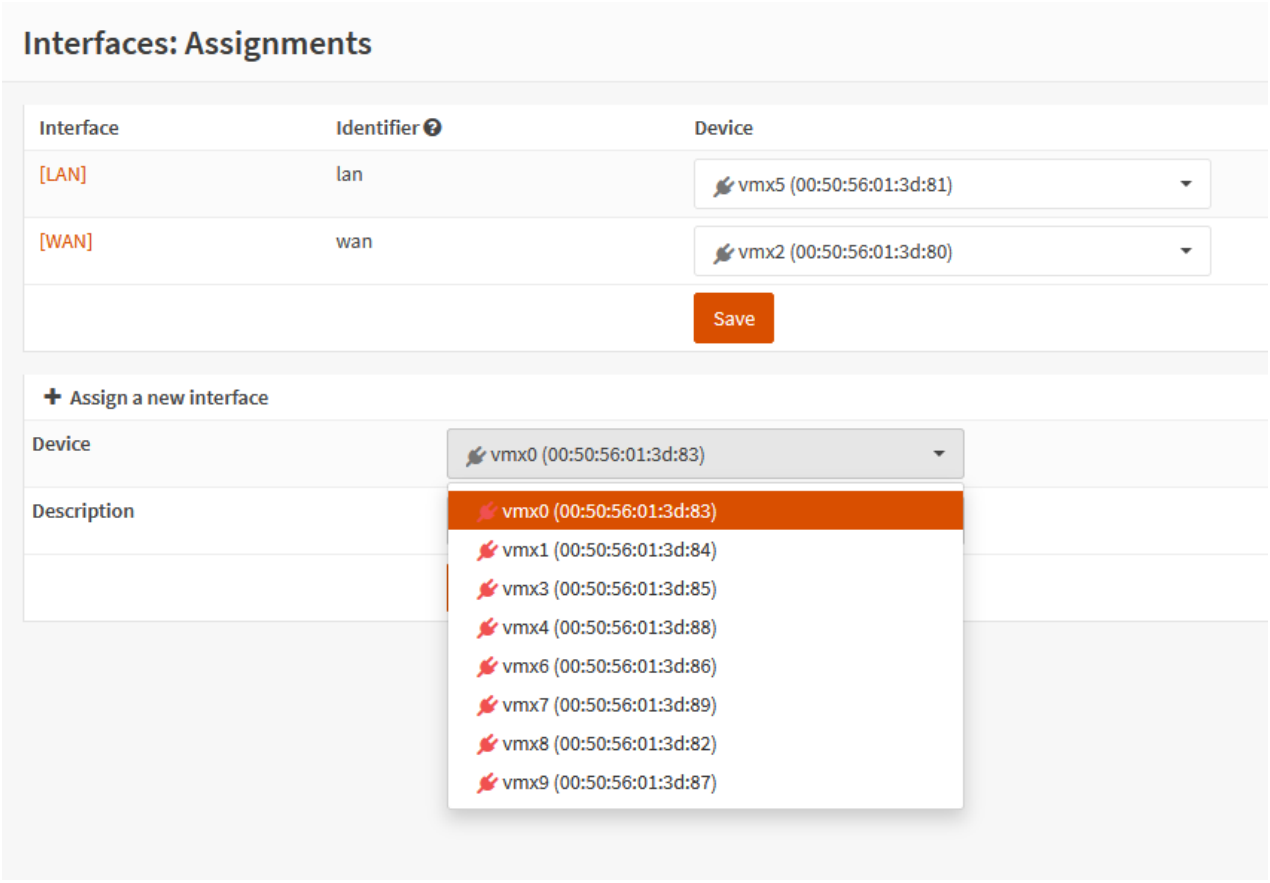
Para isso, aceder à consola da firewall e no menu lateral esquerdo escolher “Interfaces” e “Assignments”:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

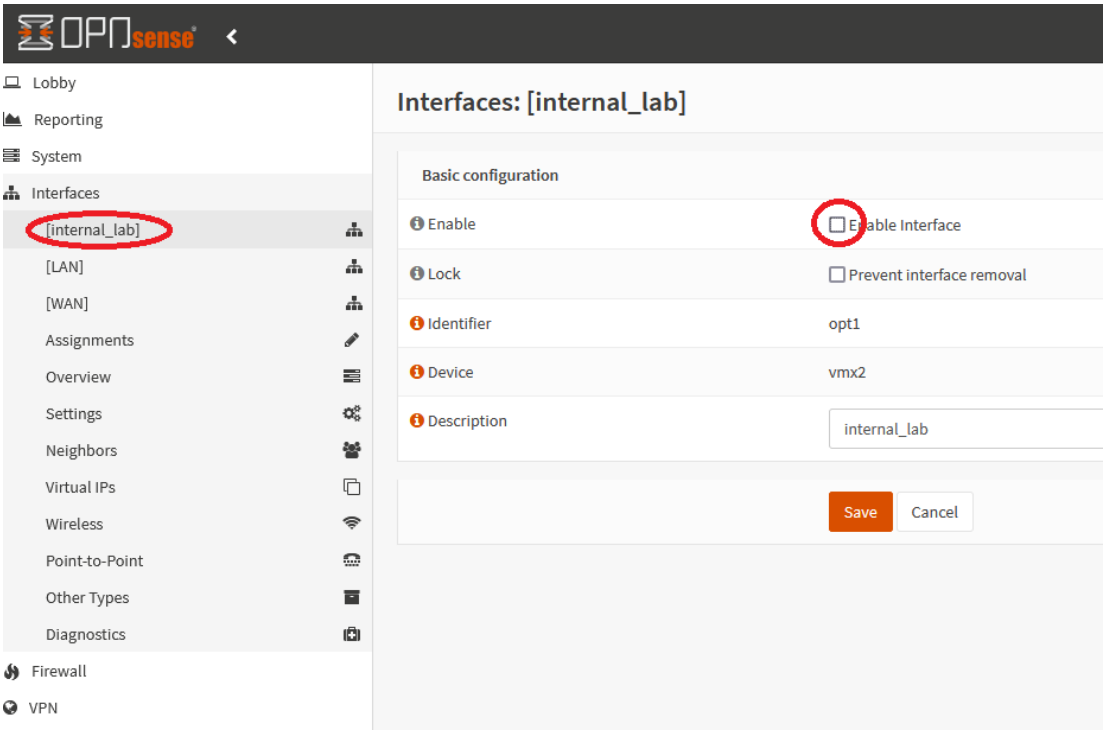


Vai surgir uma lista com as interfaces adicionadas, no campo *Device*:

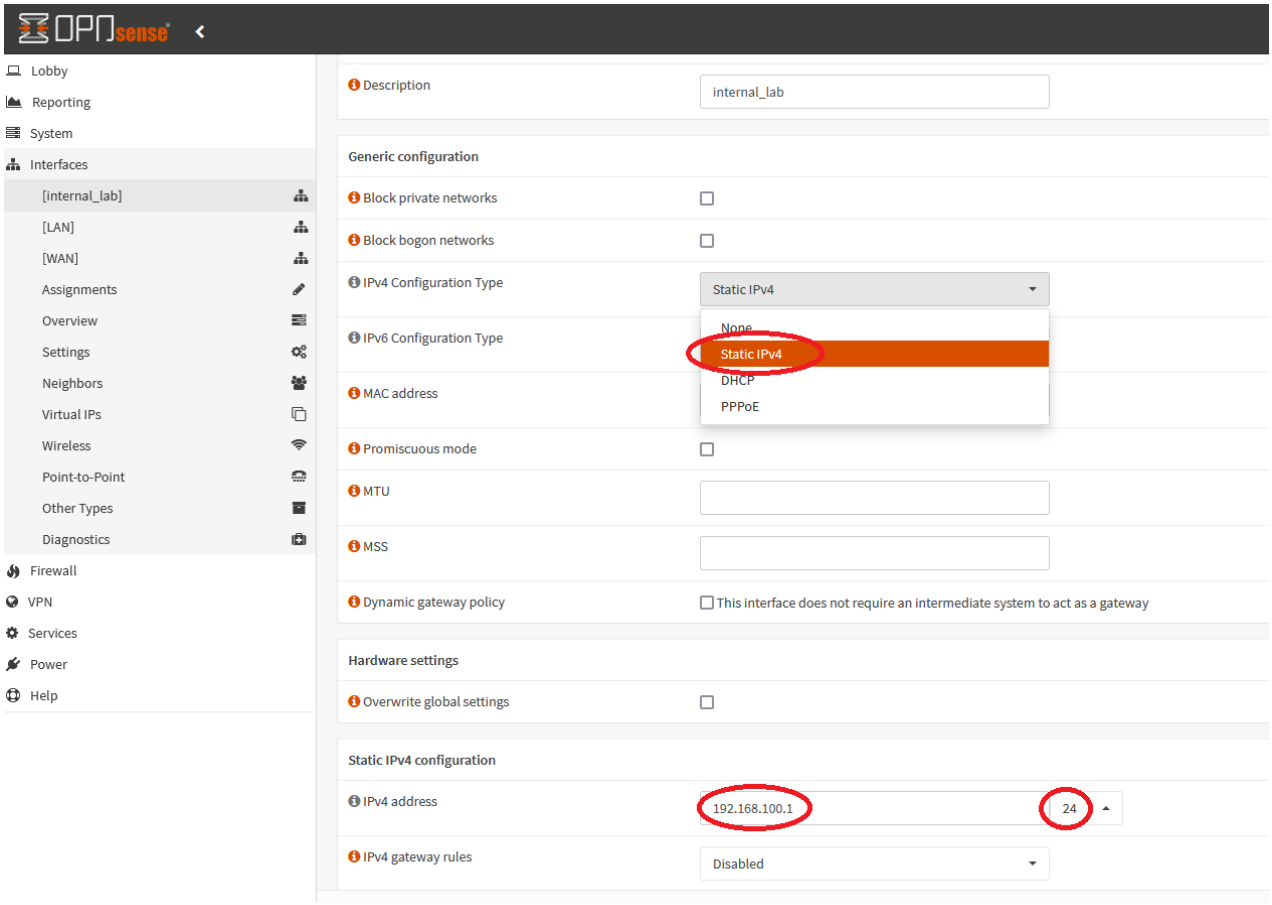
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



Depois de adicionada podemos ativar e configurá-la carregando sobre a descrição dada:



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



O passo seguinte é o da configuração das regras e serviços de firewall.

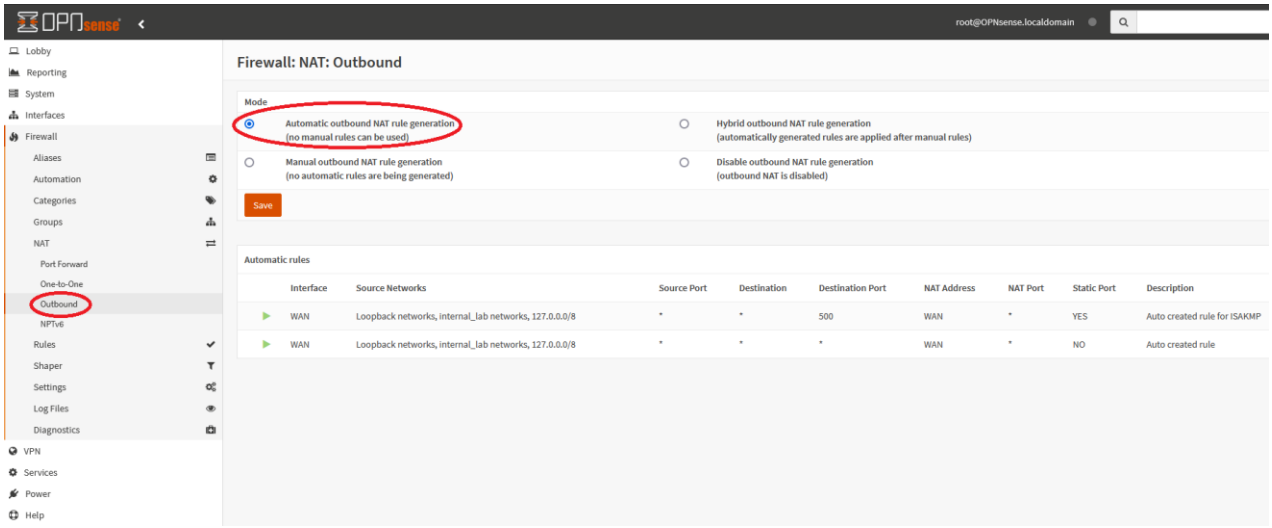
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

8. 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.

8.1 Configuração SNAT

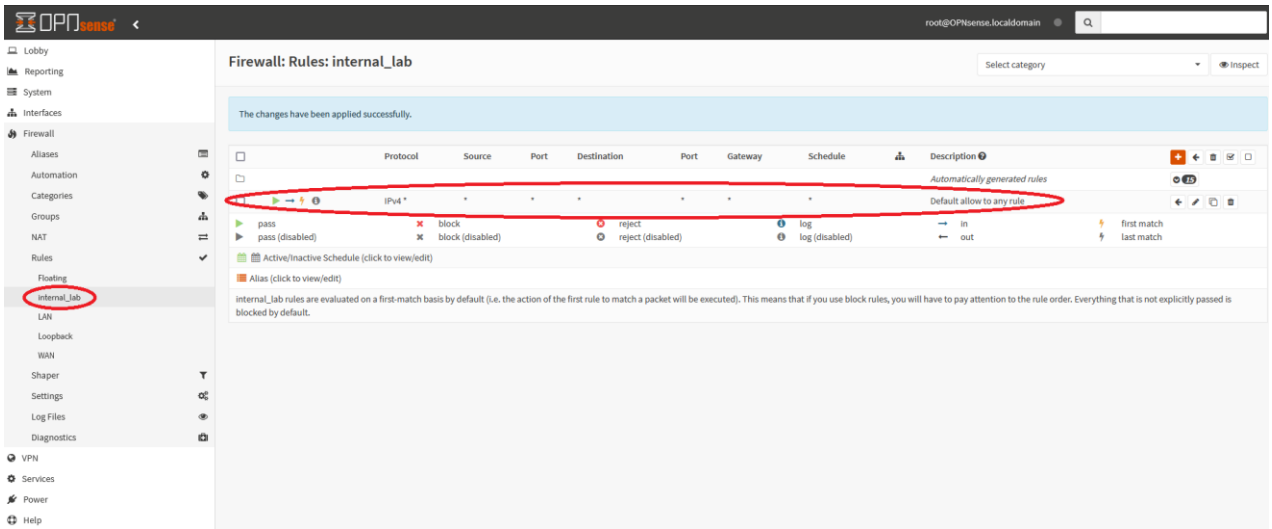
As regras SNAT são criadas automaticamente por defeito na configuração default da OPNsense. Isto pode ser visualizado indo ao menu Firewall -> NAT -> Outbound:



Caso pretenda alterar este comportamento pode fazê-lo neste quadro.

8.2 Configuração regras de tráfego

Da mesma forma, por defeito encontra-se criada a regra que permite a passagem do tráfego. Isto pode ser visualizado e modificado indo ao menu Firewall -> Rules e escolher a interface em questão:



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

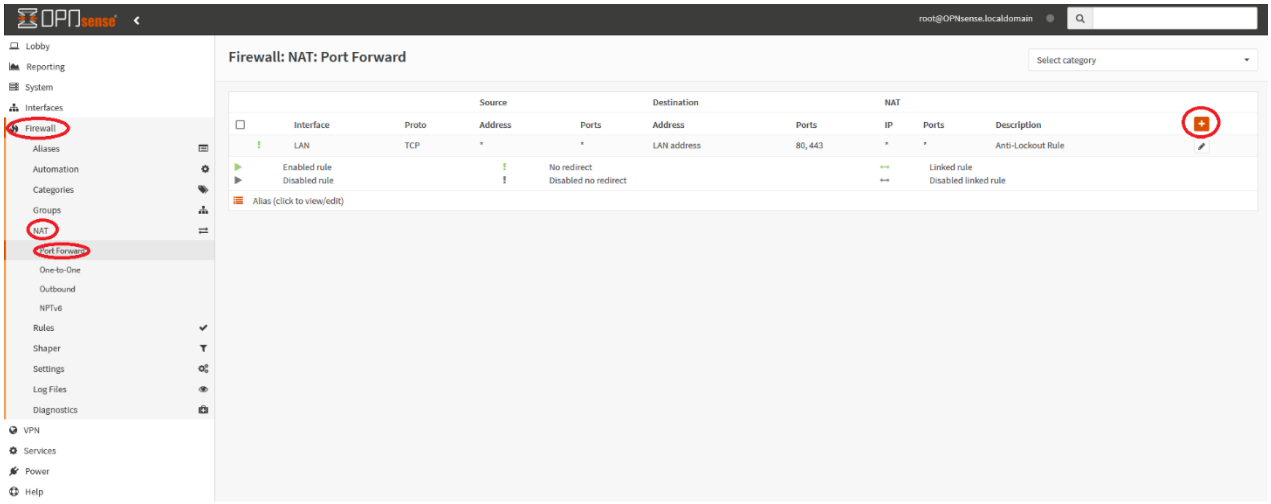
9. PORT FORWARD – DNAT

Para redirecionar acessos do exterior para uma determinada máquina numa rede interna, aceder à consola da OPNsense e no menu lateral esquerdo ir a "Firewall" -> "NAT" -> "Port Forward" e adicionar a nova regra.

Por exemplo:

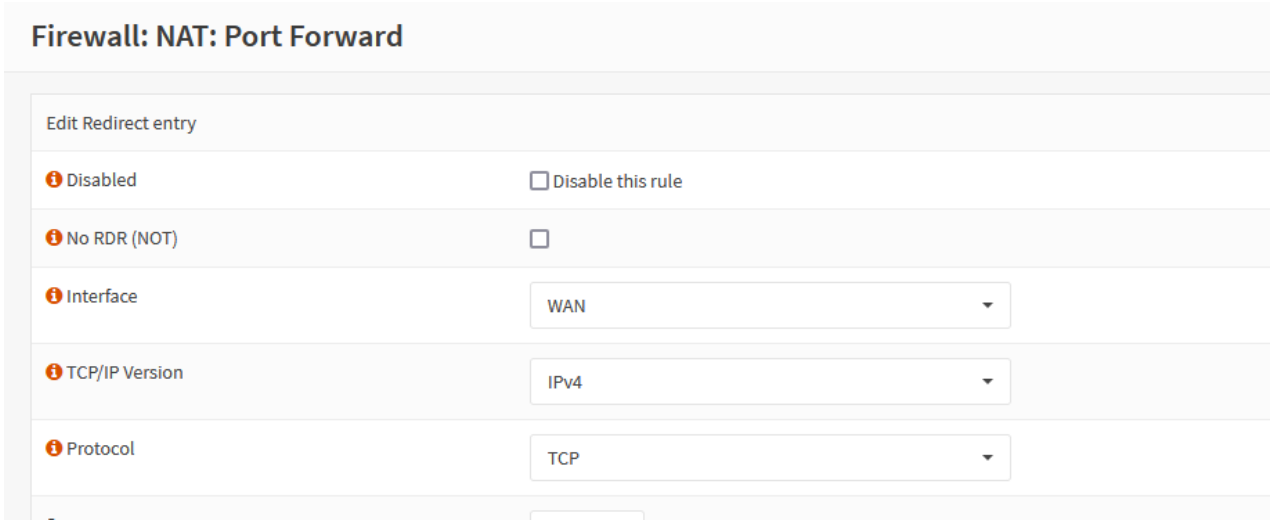
- Pretende-se criar um redireccionamento para a porta RDP de um servidor Windows
- Esse servidor tem o endereço IP interno 192.168.100.107
- A porta RDP é a 3389, no entanto, recomenda-se que a porta pública seja diferente, por exemplo, 10010

Para configurar esta regra, ir então ao quadro "Port Forward" e adicionar a regra:



Por defeito, a configuração inclui:

- a interface onde se vai aplicar o redireccionamento: WAN
- a versão de TCP/IP: IPv4
- o protocolo: TCP

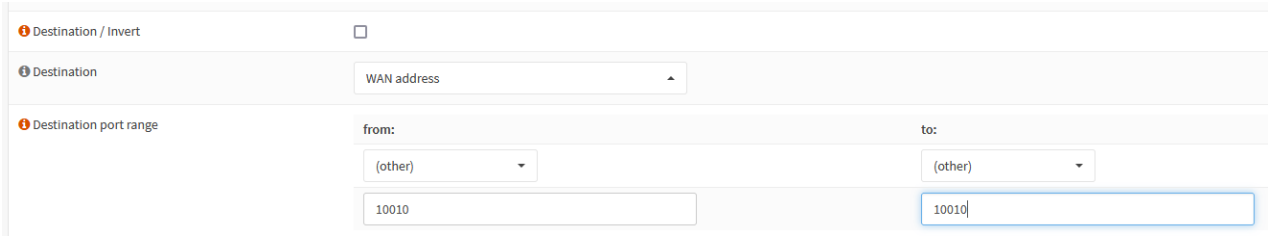


Para este exemplo não é necessário alterar estes parâmetros. Outros casos podem necessitar de valores diferentes (eventualmente alterar o protocolo).

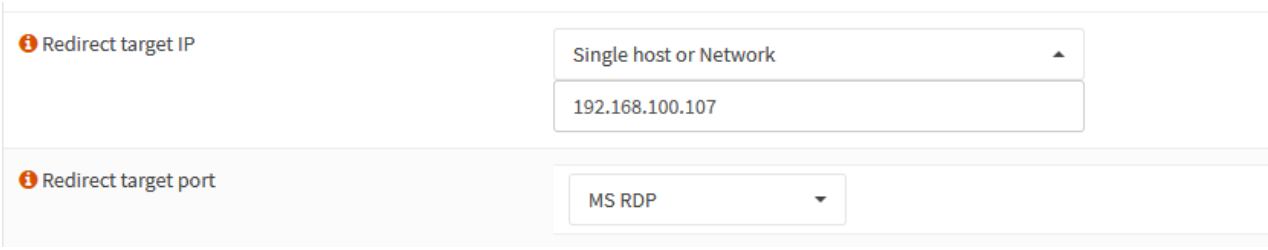
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

Neste quadro configura-se também qual o endereço e portas a redirecionar (Destination), ou seja, qual o IP da firewall e porta. Neste exemplo, temos o endereço IP externo da firewall 10.10.10.2 e a porta será 10010. Devemos optar por colocar em Destination o WAN address em vez o endereço IP para o caso de mudarmos o IP mais tarde.

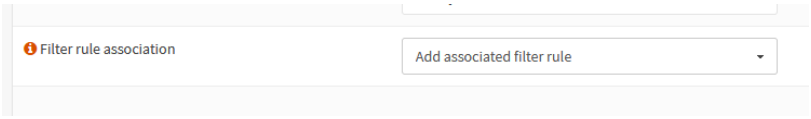
O IP da firewall a configurar é o que está, neste caso, atribuído à interface WAN. No entanto, o IP público que deverá ser usado para aceder a este serviço é o do router Edge do qual se fez NAT (no ponto 2.3 deste manual) para esta firewall, que corresponde neste exemplo a 213.63.236.54



No próximo passo configura-se o destino do tráfego redirecionado. Para isso, introduz-se o endereço IP do servidor destino e a porta do serviço no mesmo, neste exemplo, IP 192.168.100.107 e porta MS RDP (3389):



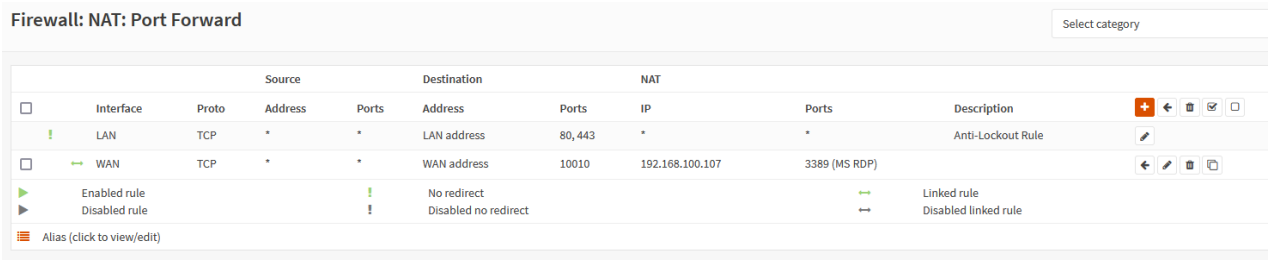
Por fim é necessário definir a regra que permite a passagem deste tráfego. Por defeito, está selecionada a opção para criar uma regra associada que permitirá este tráfego. Alterações à configuração deste DNAT serão refletidas na regra de firewall.



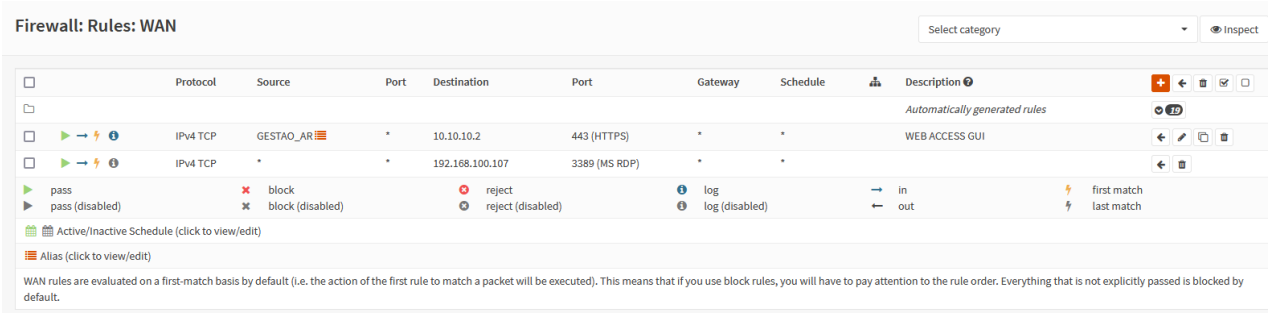
Fazendo "Save" e depois de aplicar as alterações, podemos ver o Port Forward e a correspondente regra de firewall aplicada na interface WAN:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

Firewall: NAT: Port Forward



Firewall: Rules: WAN



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

10. OPENVPN ROAD WARRIOR

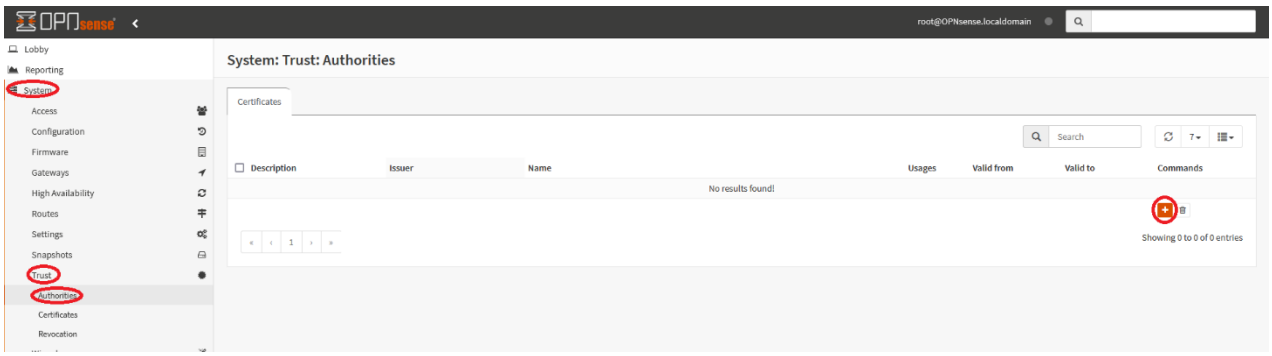
Uma VPN Road Warrior é uma VPN criada diretamente entre um dispositivo (normalmente PC ou dispositivo portátil) e uma rede, e é usada quando utilizadores individuais necessitam acesso a recursos de uma determinada rede.

Apresentam-se de seguida os passos para a sua configuração.

10.1 Criar certificados – Certificate Authority

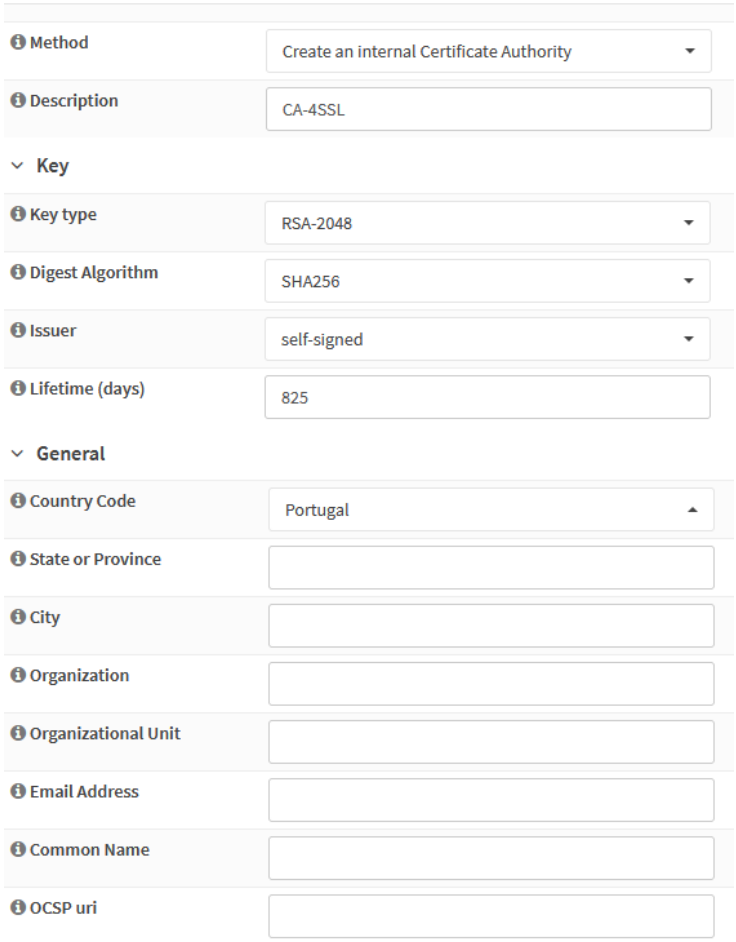
Como primeiro passo, vamos gerar a Certificate Authority (CA) para validar a identidade da instância servidor OpenVPN e autenticar certificados de utilizador.

Ir a "System" -> "Trust" -> "Authorities" e criar uma nova:



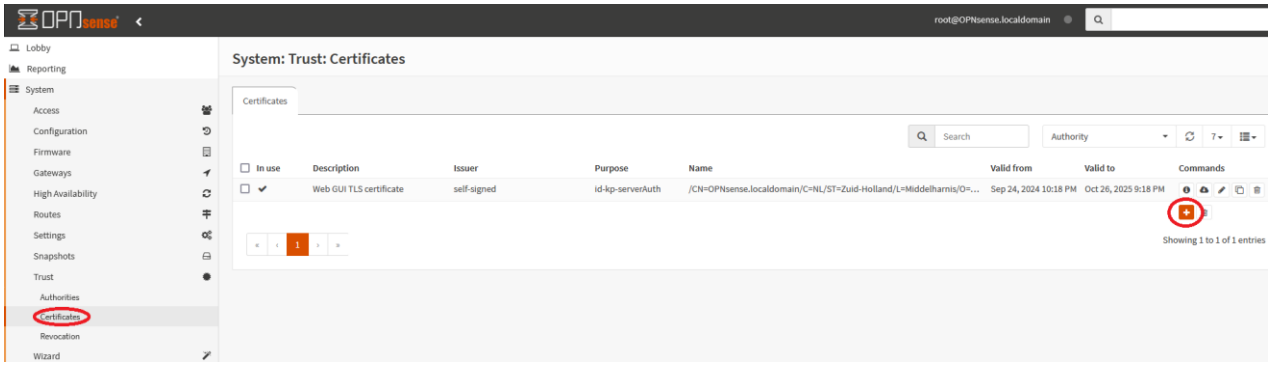
- Por defeito será criada uma autoridade do tipo *Internal*.
- Podemos alterar o tipo de chave e a duração, mas neste exemplo vamos deixar por defeito.
- Preencher os outros campos conforme pretendido

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

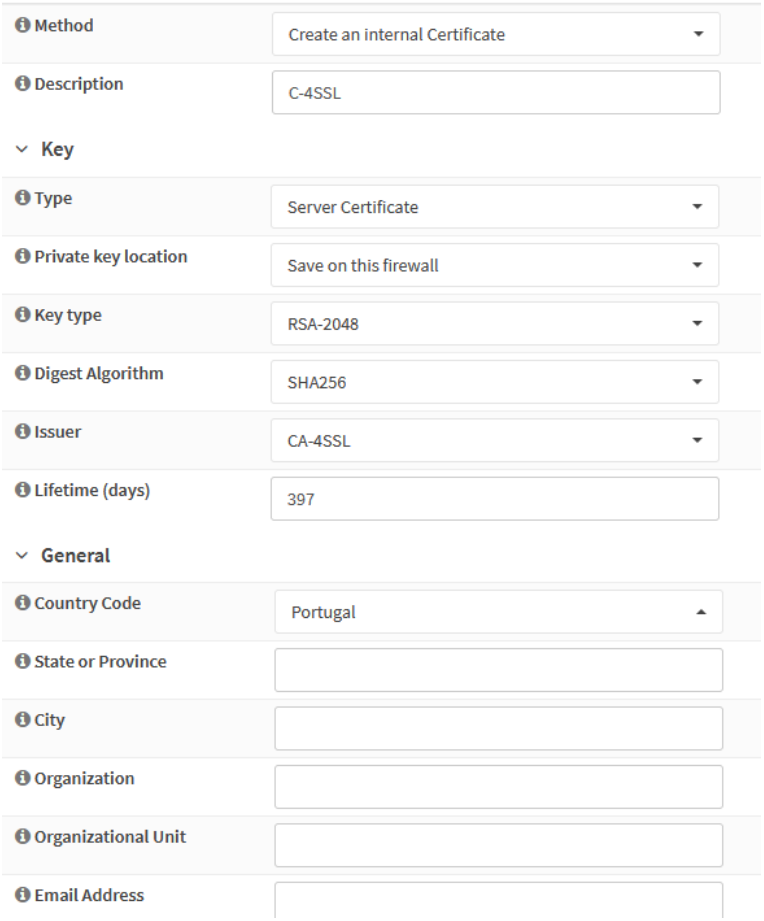


10.2 Criar certificados – server certificate

De seguida, vai-se gerar um certificado para o servidor, indo a "System" -> "Trust" -> "Certificates":



- Por defeito será criada um certificado do tipo *Internal*.
- Em *Type* escolher "Server Certificate"
- Em *Issuer* escolher a autoridade criada acima (neste exemplo, CA-4SSL)
- Preencher os outros campos conforme pretendido

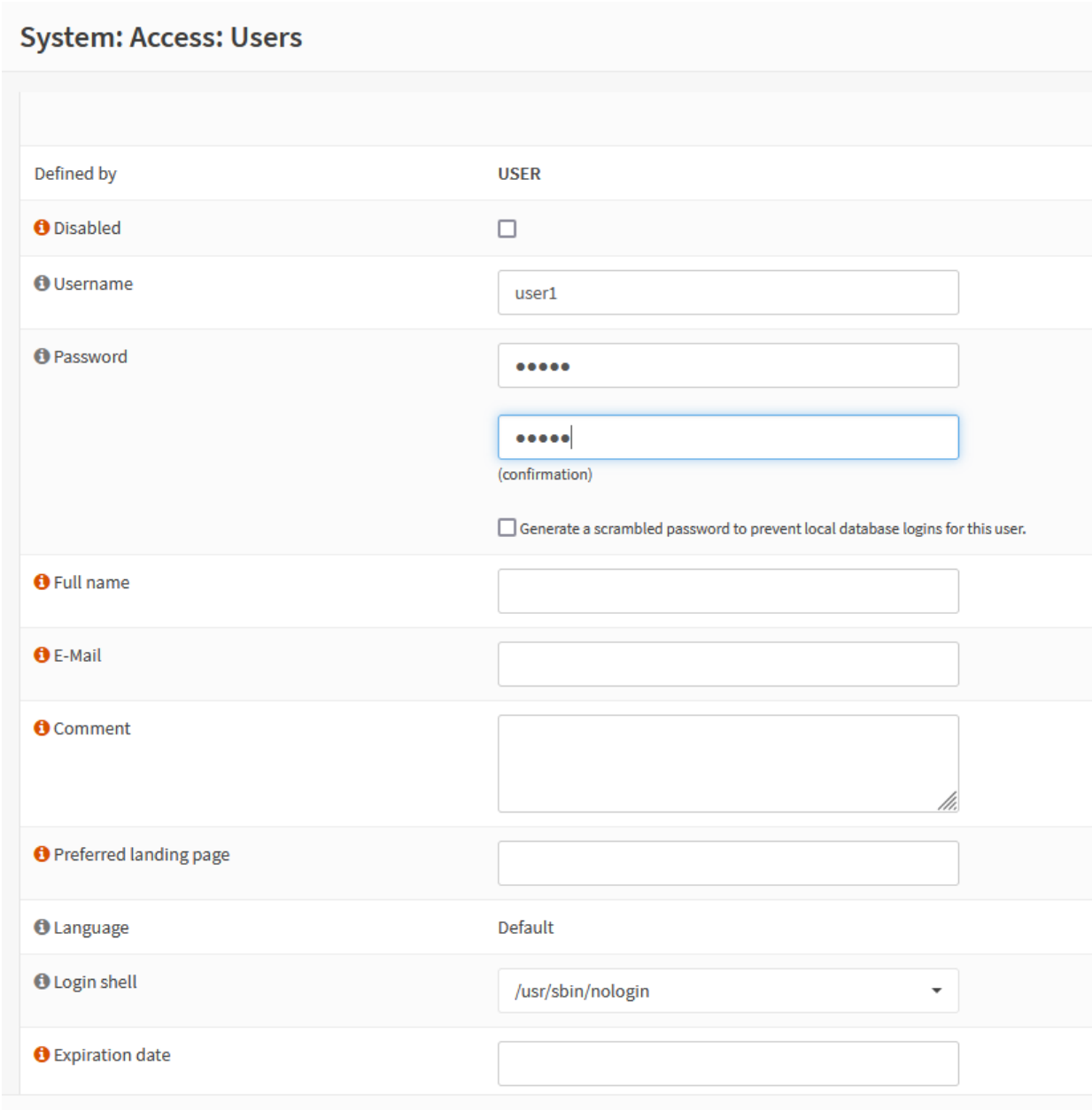


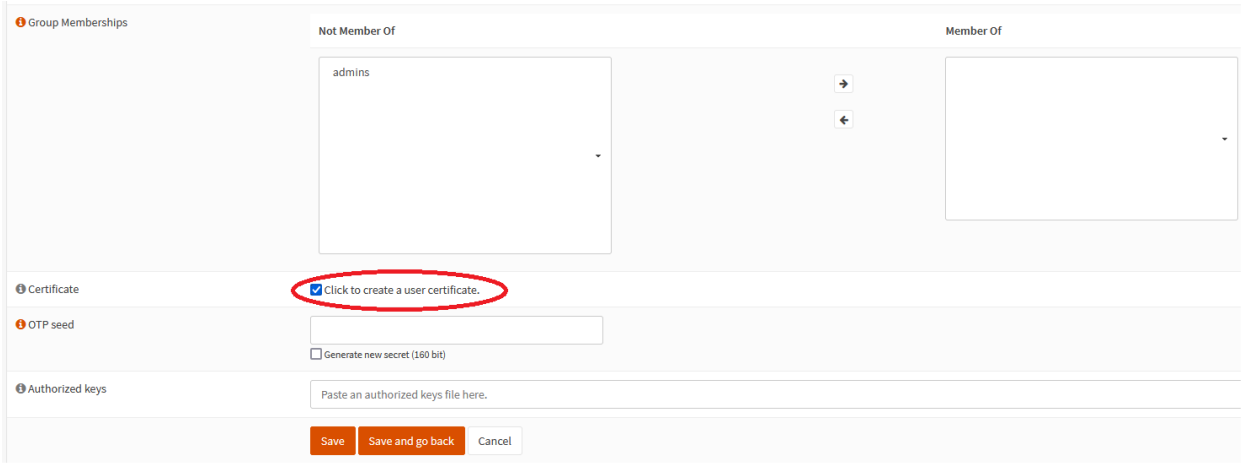
10.3 Criar utilizadores da VPN e certificados associados

Para adicionar utilizadores ir a "System" -> "Access" -> "Users":

- Dar um nome ao utilizador
- Pode-se usar apenas username e password ou também um certificado. Neste exemplo vamos criar um certificado específico para este utilizador, selecionando a opção "**Click to create a user certificate**".

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



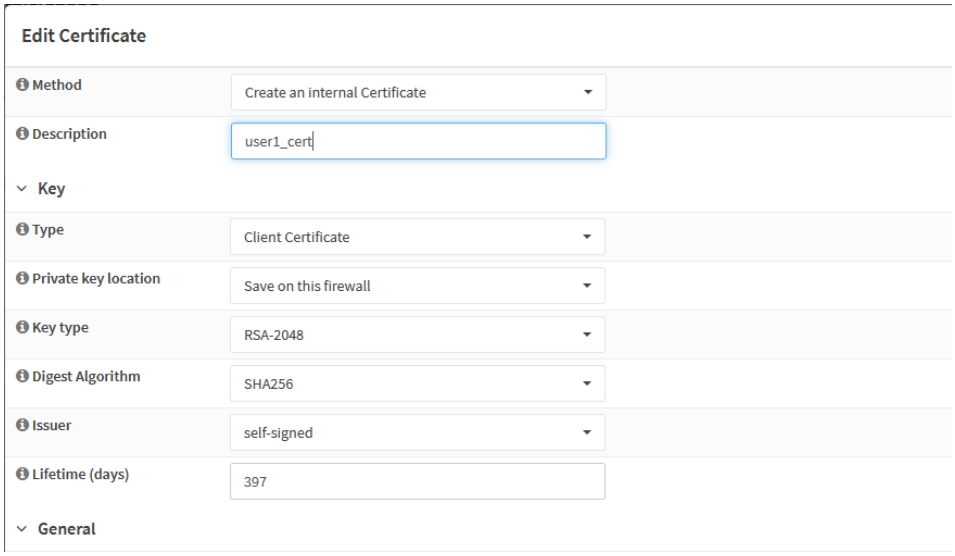


Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

Ao fazer "Save" para criar o utilizador, vai surgir uma nova janela com informações sobre o certificado, que podem ser modificadas antes de gravar.

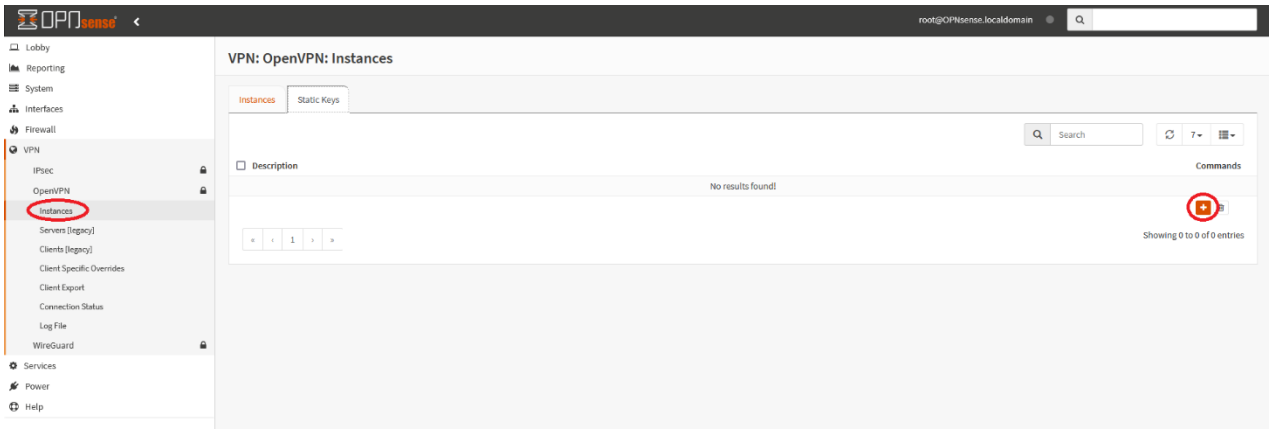
Escolher as opções:

- Method: internal
- Introduzir uma descrição
- Type: Client Certificate
- Issuer: escolher a CA criada anteriormente (CA-4SSL neste exemplo)



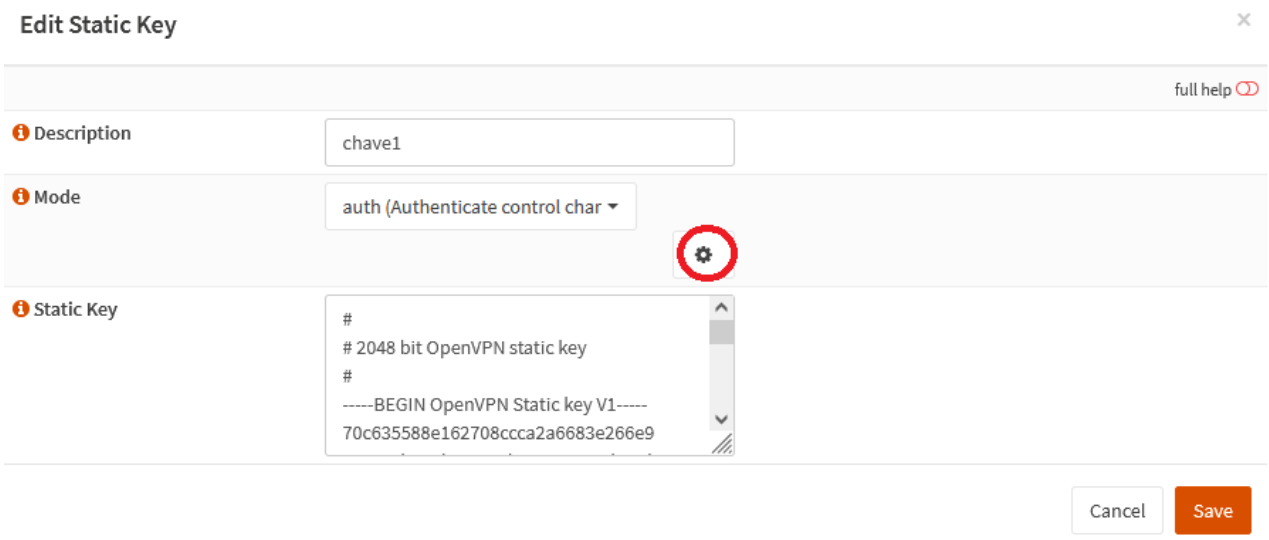
10.4 Criar chave estática

Ir a "VPN" -> "OpenVPN" -> "Instances" -> "Static Keys" e adicionar uma nova:



Neste passo deve-se introduzir uma descrição da chave, escolher o modo "auth" e carregar em  para a gerar:

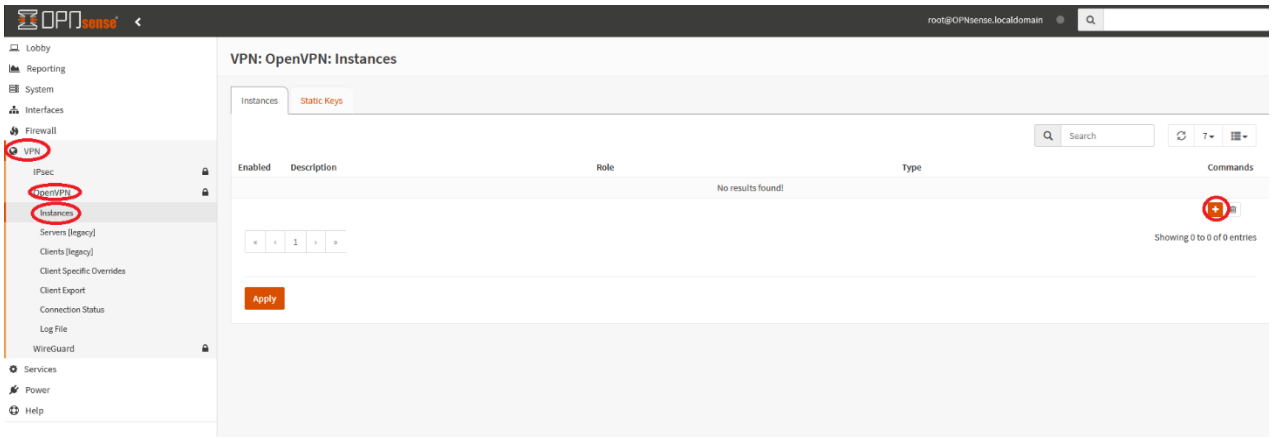
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



10.5 Adicionar servidor OpenVPN

Para adicionar uma instância de servidor OpenVPN, ir a "VPN" -> "OpenVPN" -> "Instances"

Criar uma instância carregando no sinal de "**+**":



Aqui, configuram-se os seguintes parâmetros:

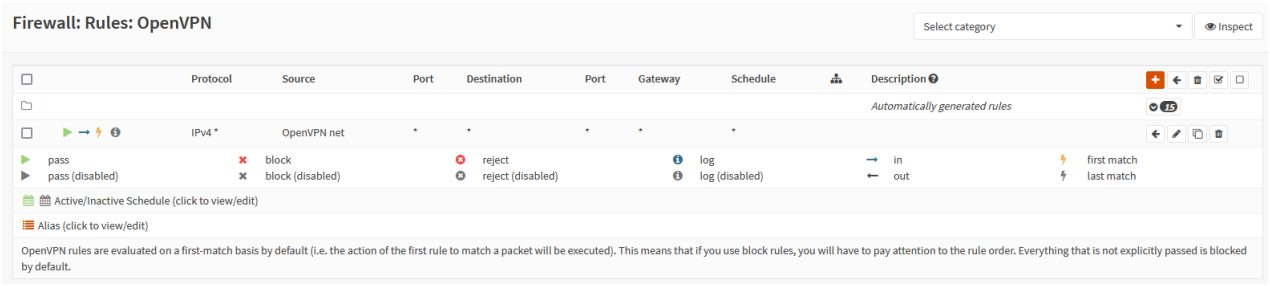
- Role: Server (aparece por defeito)
- Introduzir uma descrição para este servidor
- Protocol: deixar por defeito em UDP
- Port number: este campo pode ser deixado em branco para usar a porta default (1194). No caso de haver mais que uma instância, deve-se garantir que cada uma tem a sua porta, distinta de todas as outras.
- Type: deixar por defeito em TUN
- Bind address: pode ficar em branco o que quer dizer que vai responder em todos os endereços
- Server (IPv4): introduzir uma rede não utilizada, que será a rede do túnel (por ex. 10.1.1.0/24)
- Certificate: escolher o certificado criado anteriormente no ponto 10.2 (server certificate)
- TLS static key: escolher a chave criada anteriormente no ponto 10.4

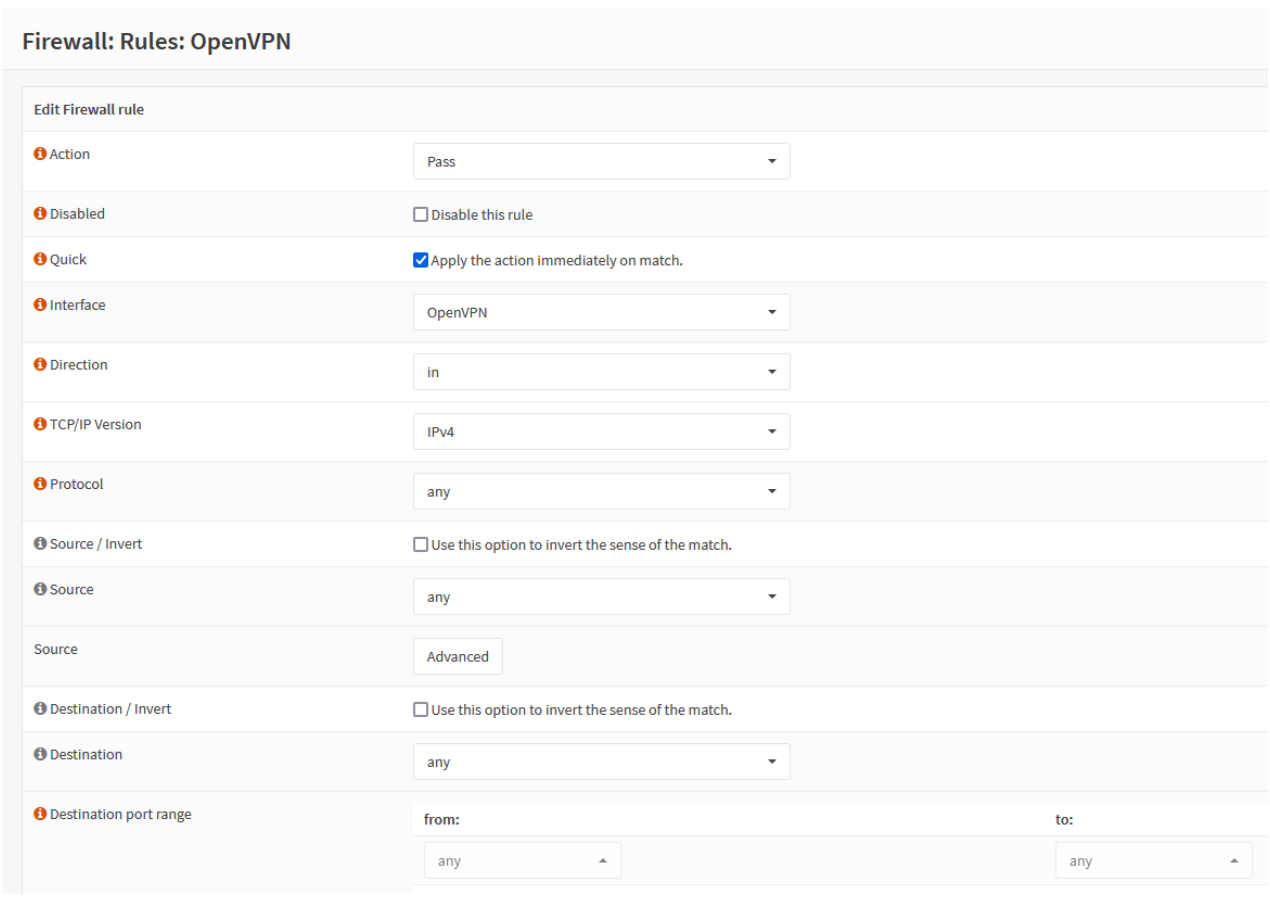
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

- Authentication: escolher “Local Database”
- Local Network: escolher a rede pretendida. Neste exemplo será 192.168.100.0/24

10.6 Regras de firewall

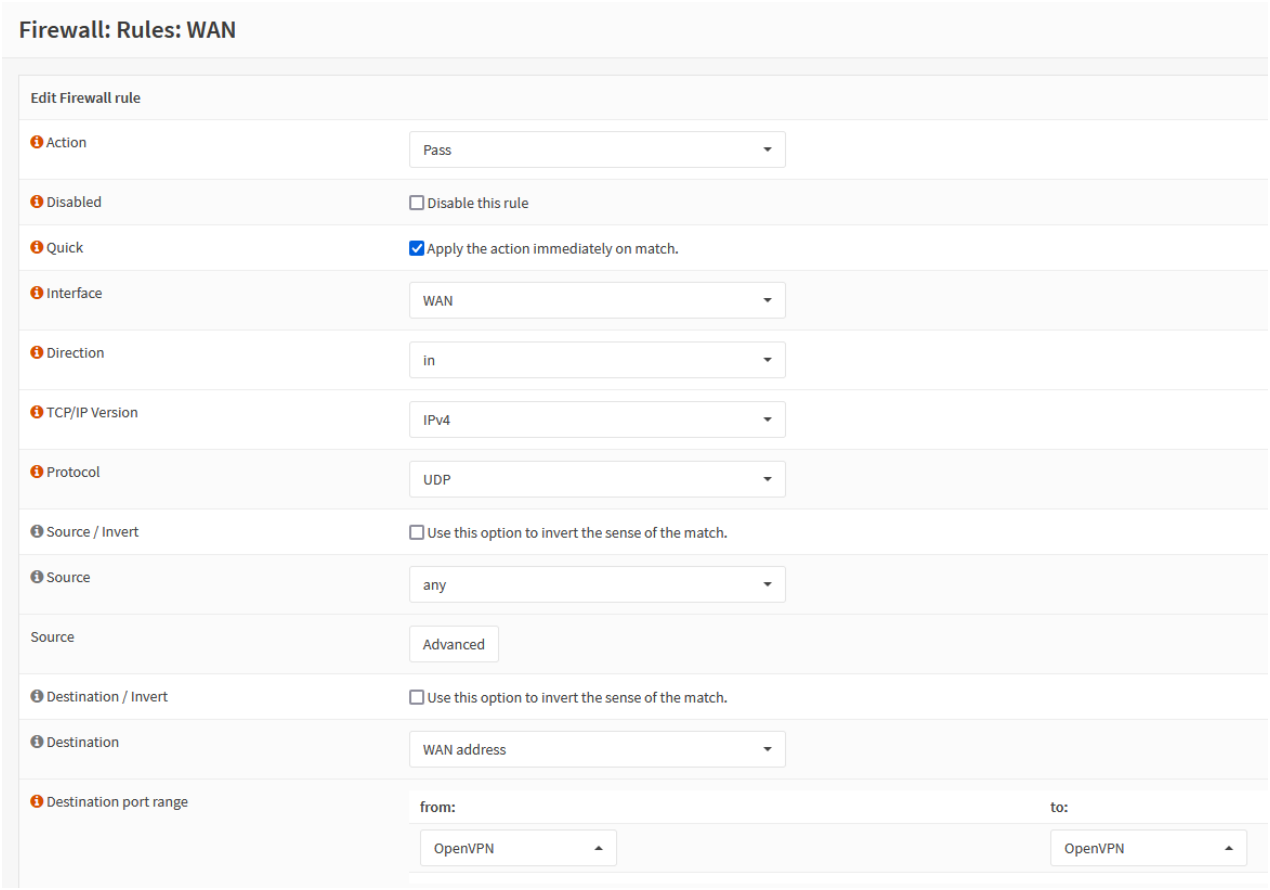
Finalmente, para permitir o tráfego nesta VPN, ir a “Firewall” -> “Rules” -> “OpenVPN” e criar uma regra, permitindo passagem de tráfego, direção “in”:

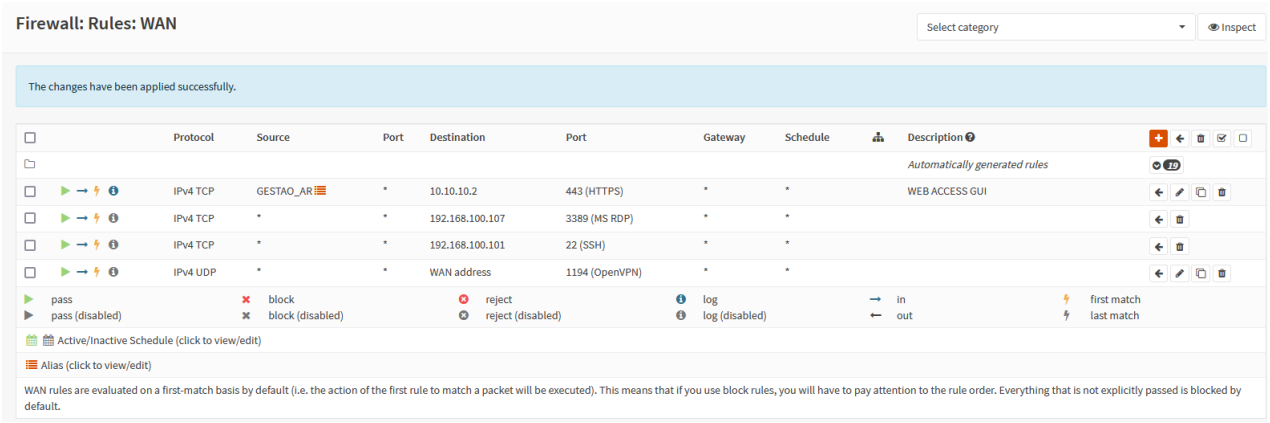




Criar também uma regra para permitir o tráfego OpenVPN na interface WAN: “Firewall” -> “Rules” -> “WAN” e criar uma regra, permitindo passagem de tráfego, direção “in”:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt





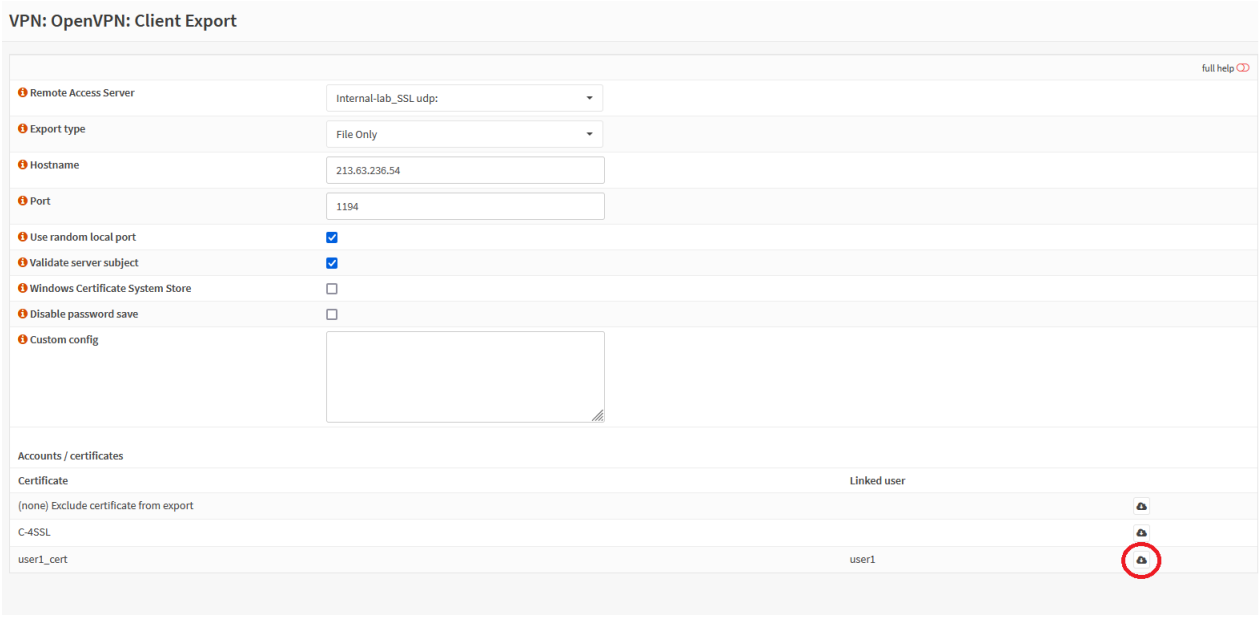
10.7 Configuração dos dispositivos remotos

Para exportar a configuração a utilizar nos dispositivos remotos ir a "**VPN**" -> "**OpenVPN**" -> "**Client Export**":

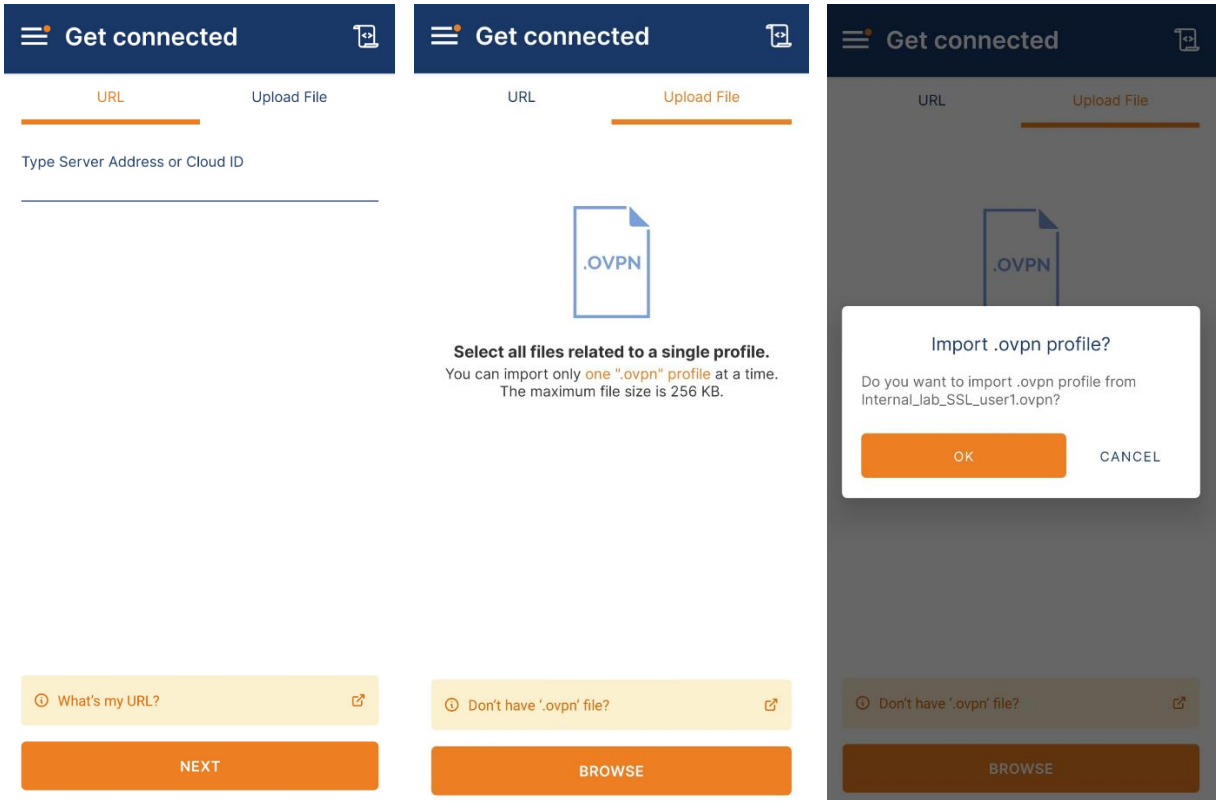
- Escolher o servidor
- Export type: escolher "File Only"
- Hostname: colocar o FQDN ou o endereço IP público do router Edge (213.63.236.54 neste exemplo)
- Port: colocar a porta definida anteriormente (1194 neste exemplo)

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

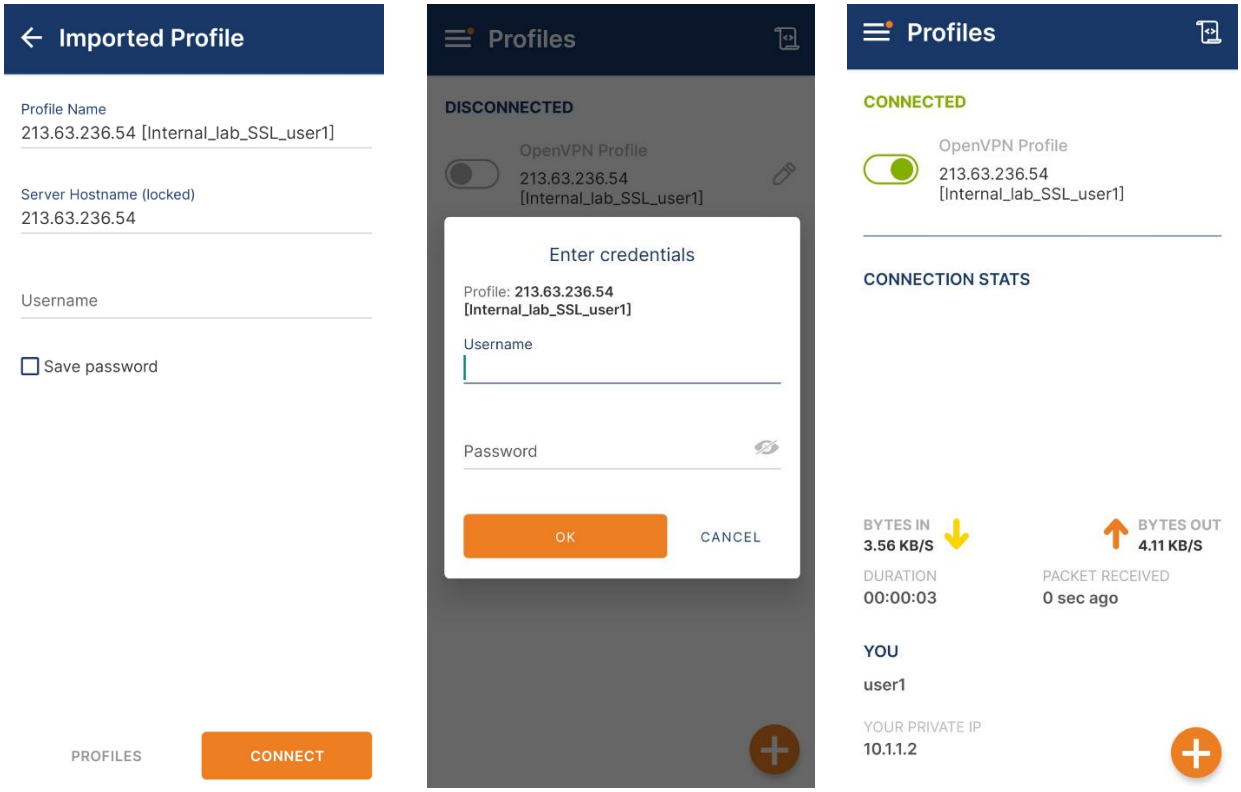
- Fazer download, carregando no ícone correspondente ao utilizador:



Para configurar o cliente OpenVPN, basta importar este ficheiro. Nas imagens abaixo mostra-se o exemplo no caso da aplicação num dispositivo móvel Android:



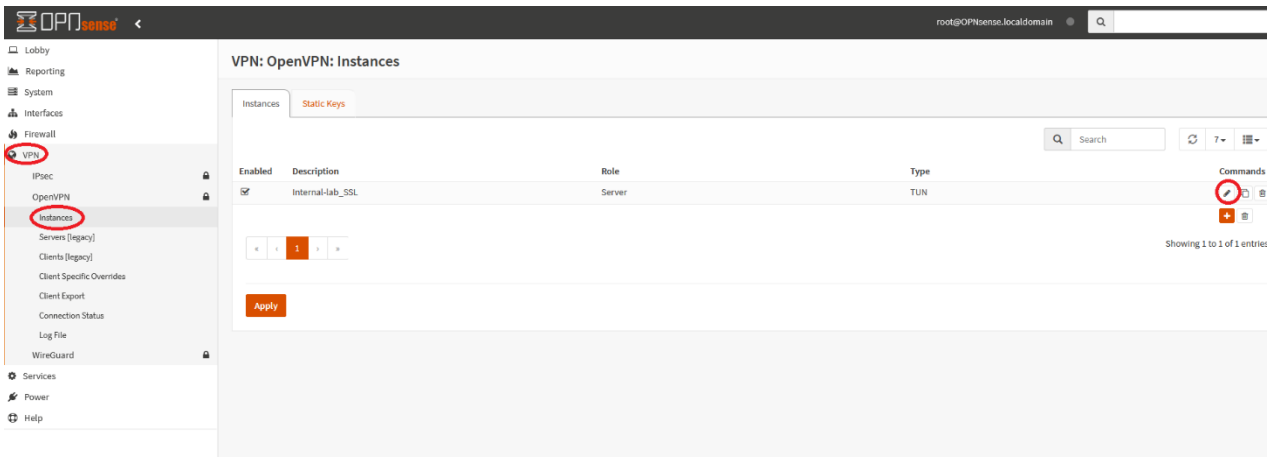
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



10.8 Ativar autenticação 2FA

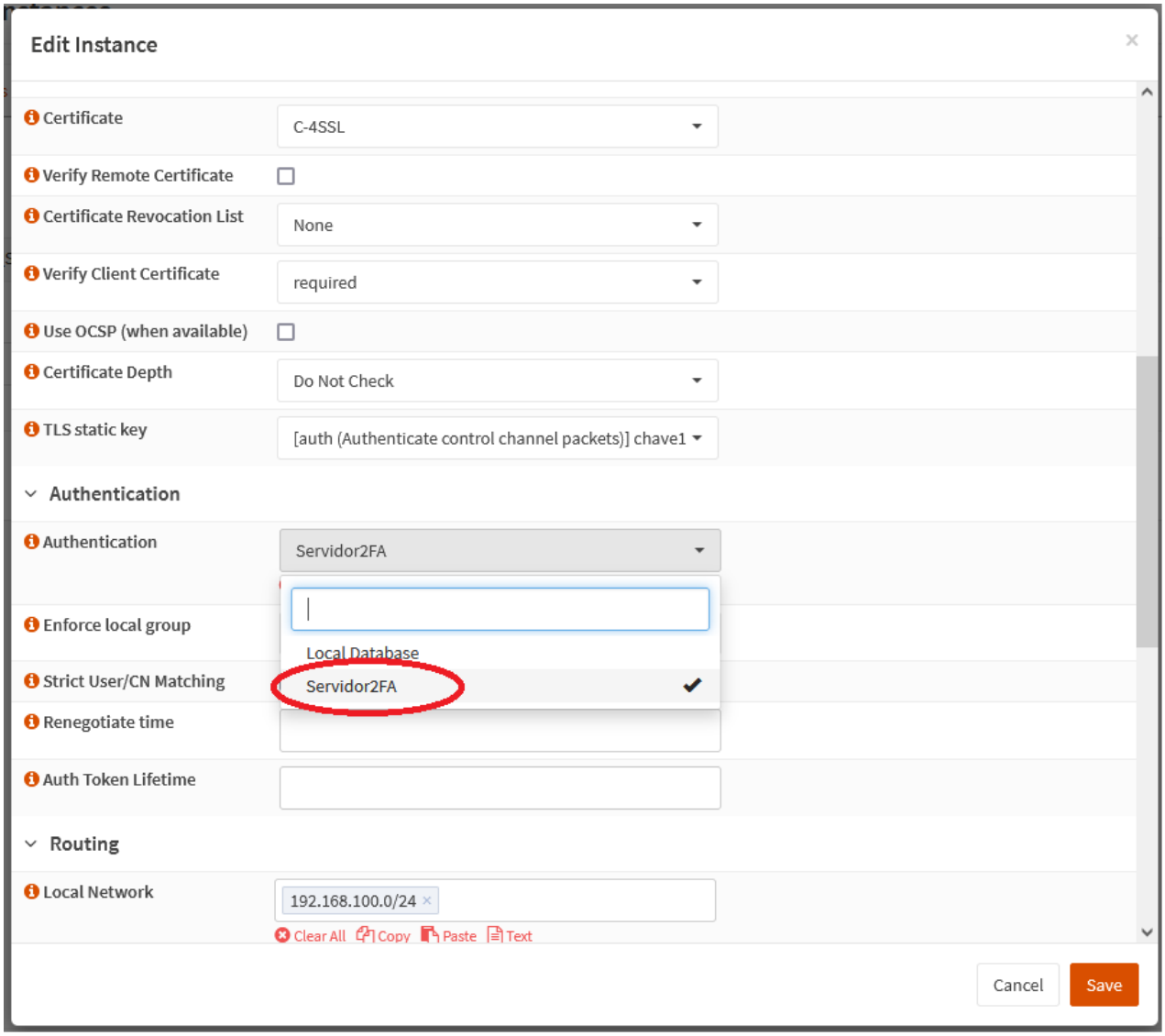
A autenticação de dois fatores pode ser aplicada ao nível da instância OpenVPN, sendo que, é possível existir mais do que uma instância. Pode por exemplo, existir uma instância com autenticação de dois fatores que irá ser utilizada por alguns utilizadores, e outra instância com autenticação simples que irá ser utilizada por outros utilizadores.

Para modificar o tipo de autenticação na instância OpenVPN ir a **VPN** -> **OpenVPN** -> **Instances** e editar a instância pretendida:



No quadro que aparece, navegar até à secção "Authentication" e escolher o servidor de autenticação pretendido:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



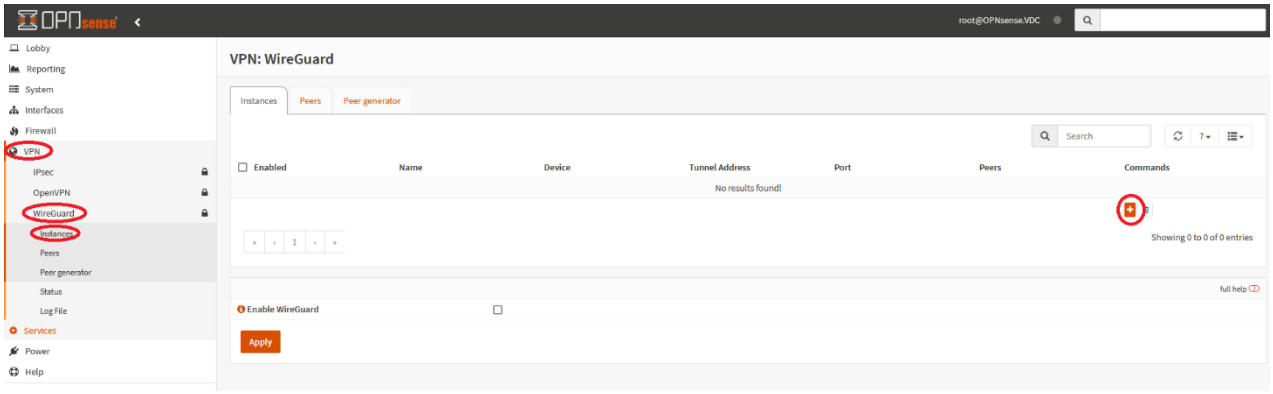
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

11. WIREGUARD ROAD WARRIOR

11.1 Adicionar instância Wireguard

Para adicionar uma instância de servidor Wireguard, ir a "VPN" -> "WireGuard" -> "Instances"

Criar uma instância carregando no sinal de "**+**":

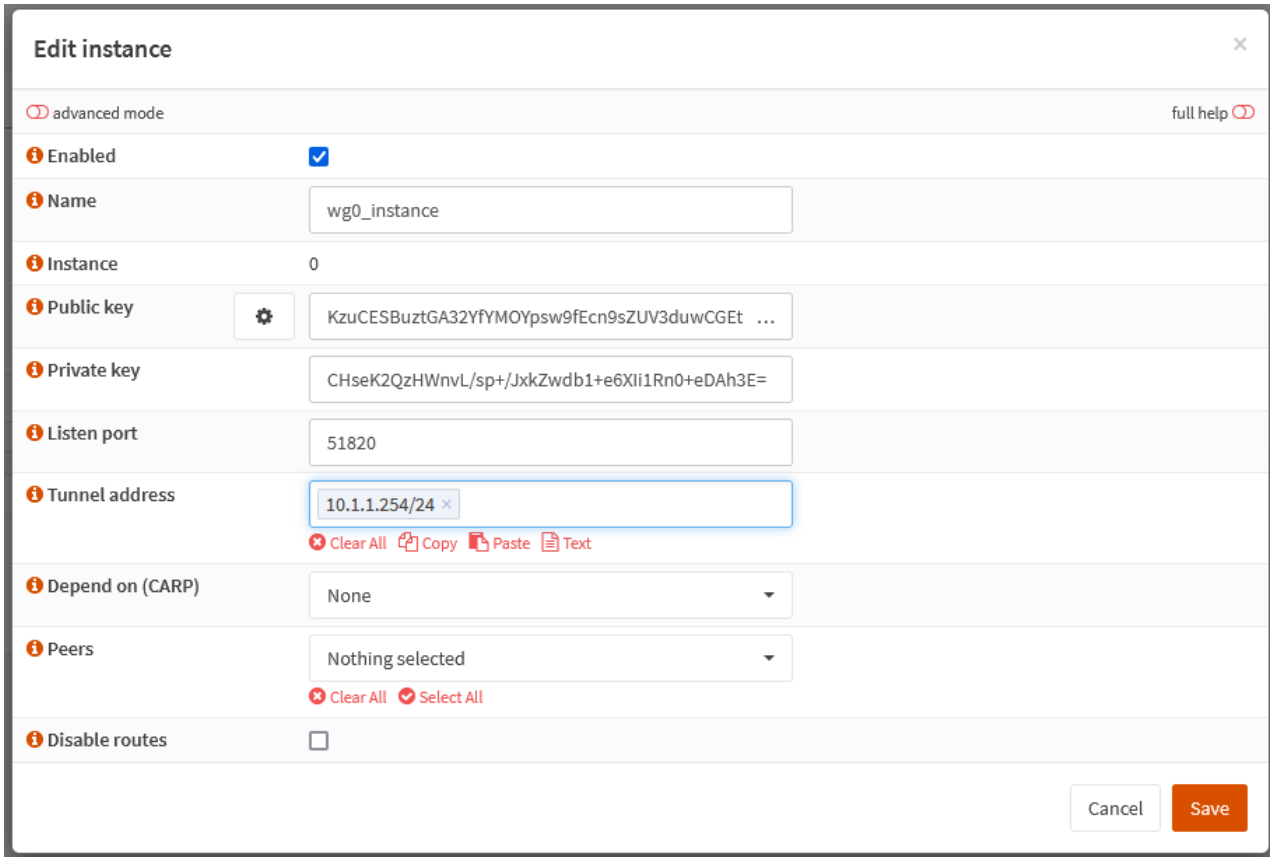


Aqui, configuram-se os seguintes parâmetros:

- Name: uma descrição para esta instância
- Public key: carregar na roda para gerar uma chave pública e a correspondente chave privada
- Listen Port: usar uma porta única, associada a esta instância (51820 ou superior)
- Tunnel address: introduzir um endereço de uma rede não utilizada, que será a rede do túnel (por ex. 10.1.1.254/24)
- Peers: deixar em branco nesta fase (serão configurados no próximo passo)

Não preencher o campo **DNS servers** que surge quando selecionamos o modo avançado. Ao fazê-lo, isto irá substituir a configuração de DNS da OPNsense.

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

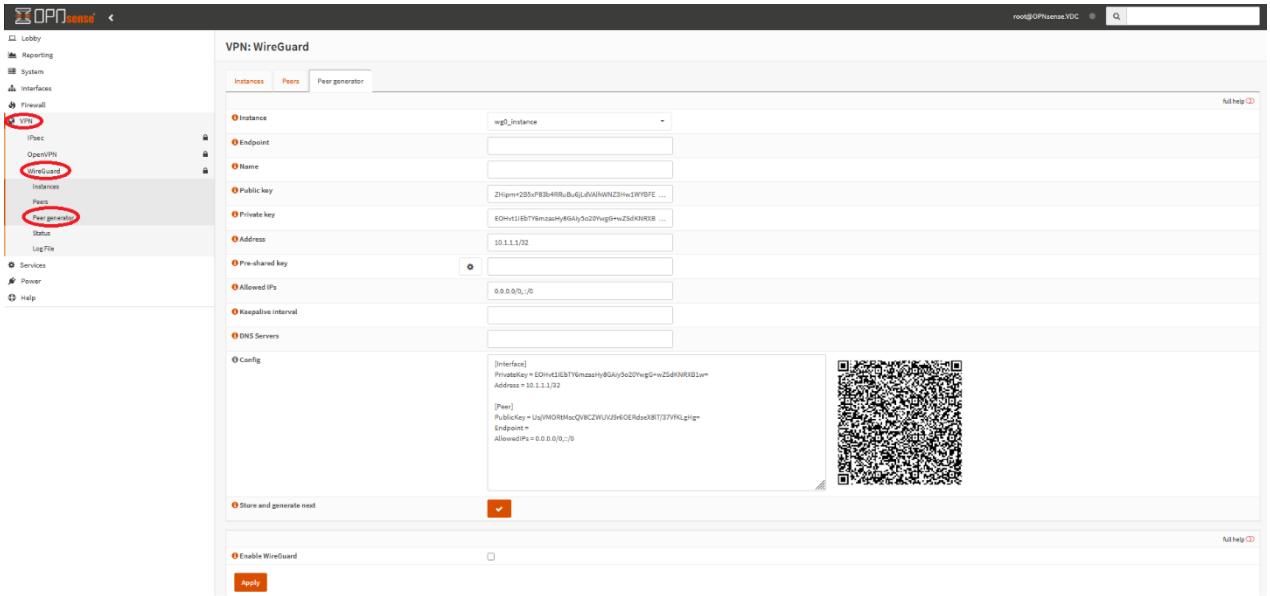


Copiar a chave pública para usar na configuração do cliente.

Terminar a configuração fazendo **Save** e **Apply**, fazendo **Enable WireGuard**

11.2 Configuração do Peer

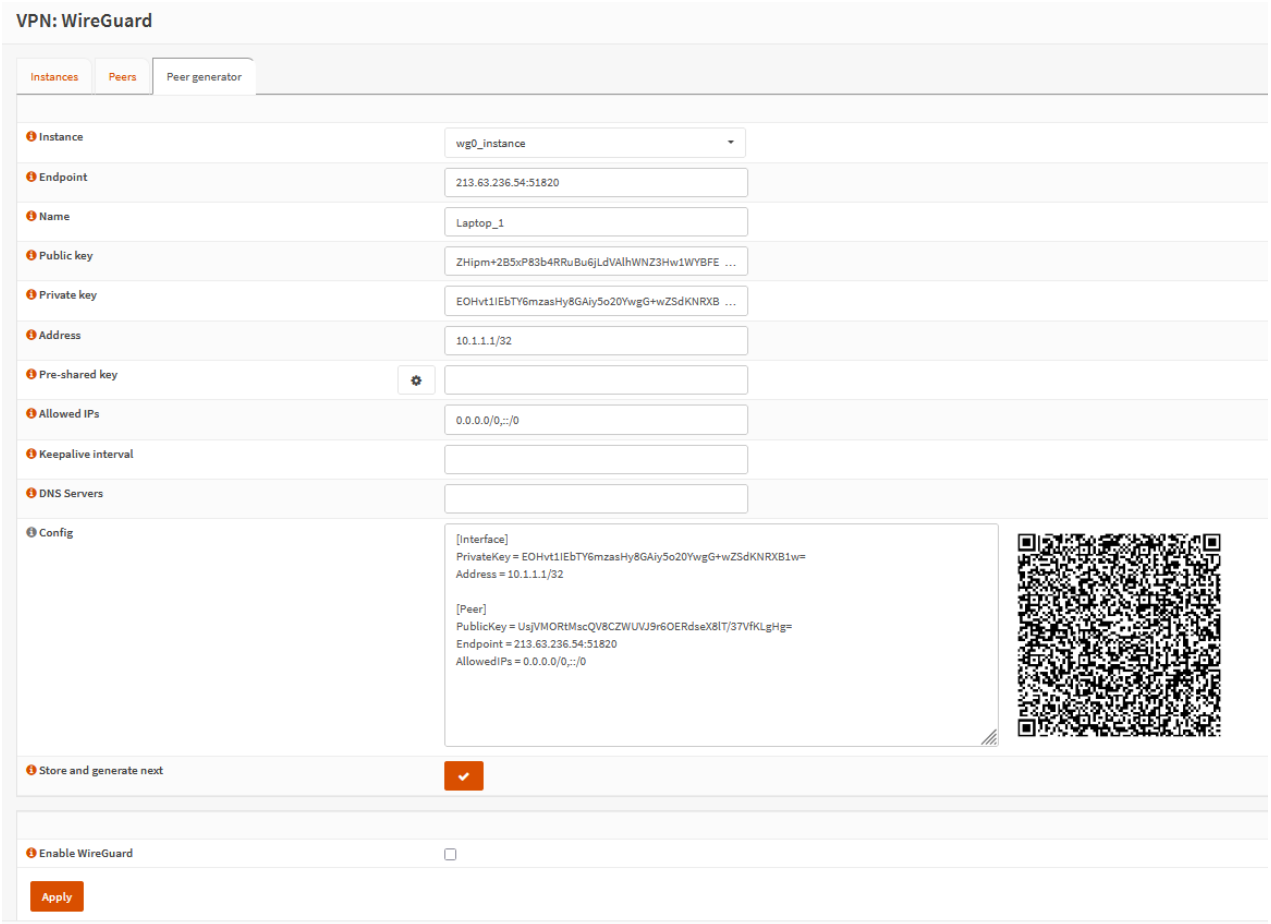
Para adicionar um peer, ir a "VPN" -> "WireGuard" -> "Peer generator":



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

Aqui configuram-se os parâmetros a passar ao cliente:

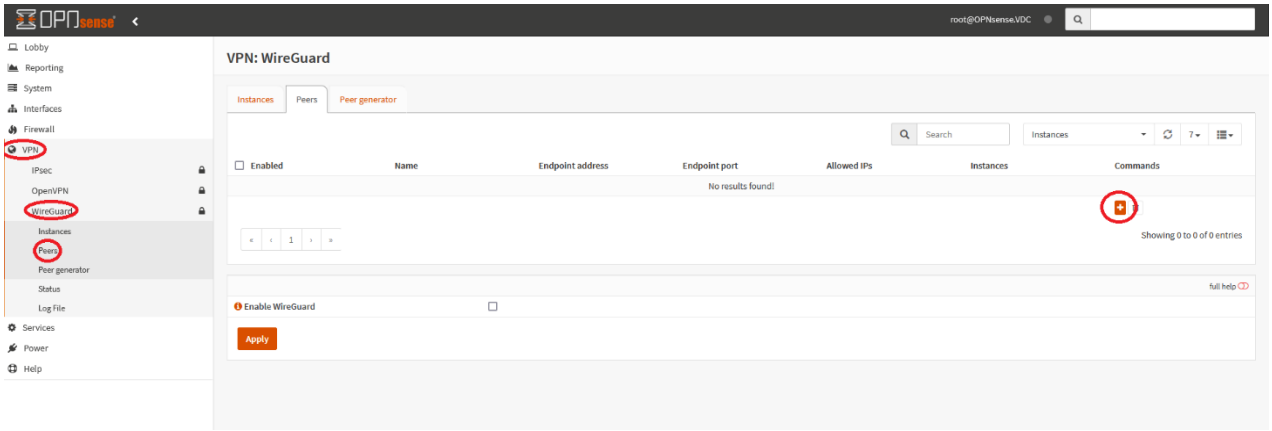
- Endpoint: o endereço IP ou FQDN e respetiva porta para aceder à instância Wireguard
- Name: a descrição deste peer
- Public e Private keys: geradas automaticamente
- Address: endereço IP do túnel no lado do peer
- Pre-shared key: opcional
- Allowed IPs: os IPs ou redes que irão passar pelo túnel



Carregar em **Store and generate next** e seguidamente em **Enable WireGuard**

Também se pode adicionar um peer indo a "VPN" -> "WireGuard" -> "Peers" e carregar no sinal de "**+**":

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

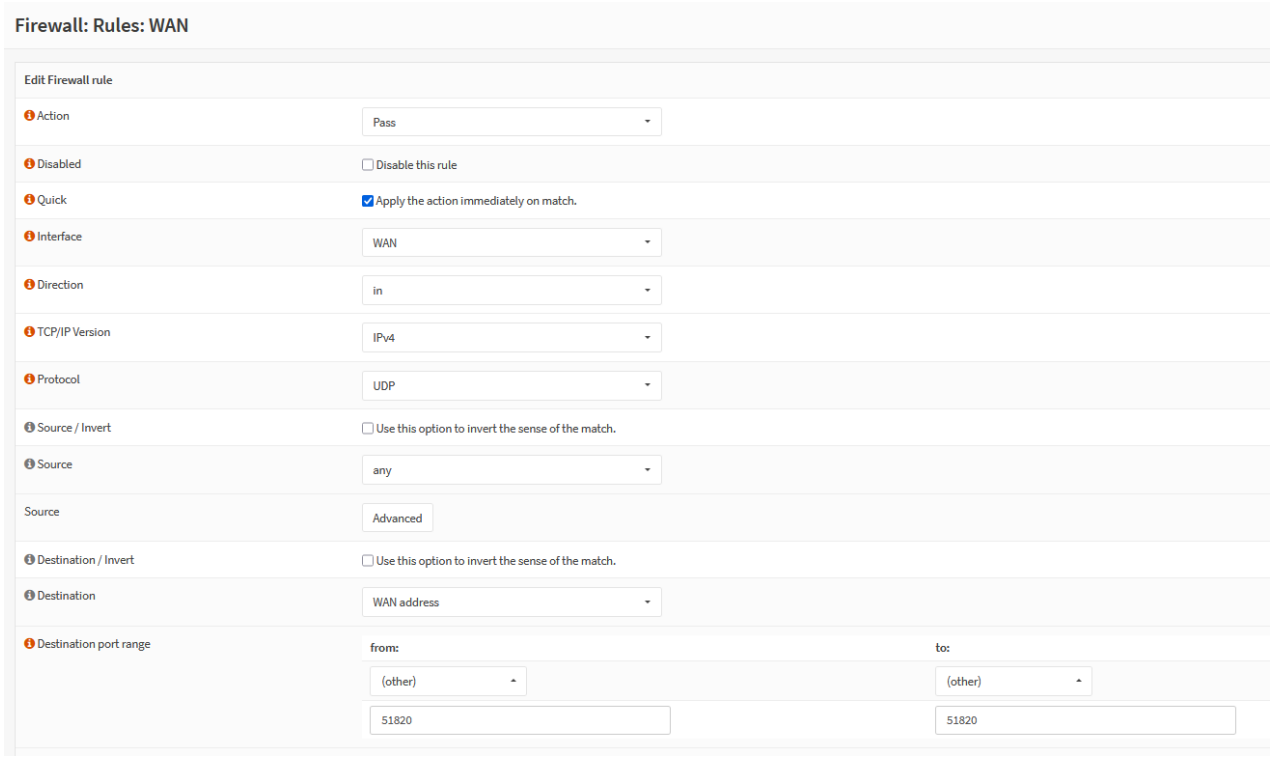


Configurar os seguintes parâmetros:

- Name: uma descrição para este peer
- Public key: carregar na roda para gerar uma chave pública e a correspondente chave privada
- Listen Port: usar uma porta única, associada a esta instância (51820 ou superior)
- Tunnel address: introduzir uma rede não utilizada, que será a rede do túnel (por ex. 10.1.1.0/24)
- Peers: deixar em branco nesta fase (serão configurados no próximo passo)

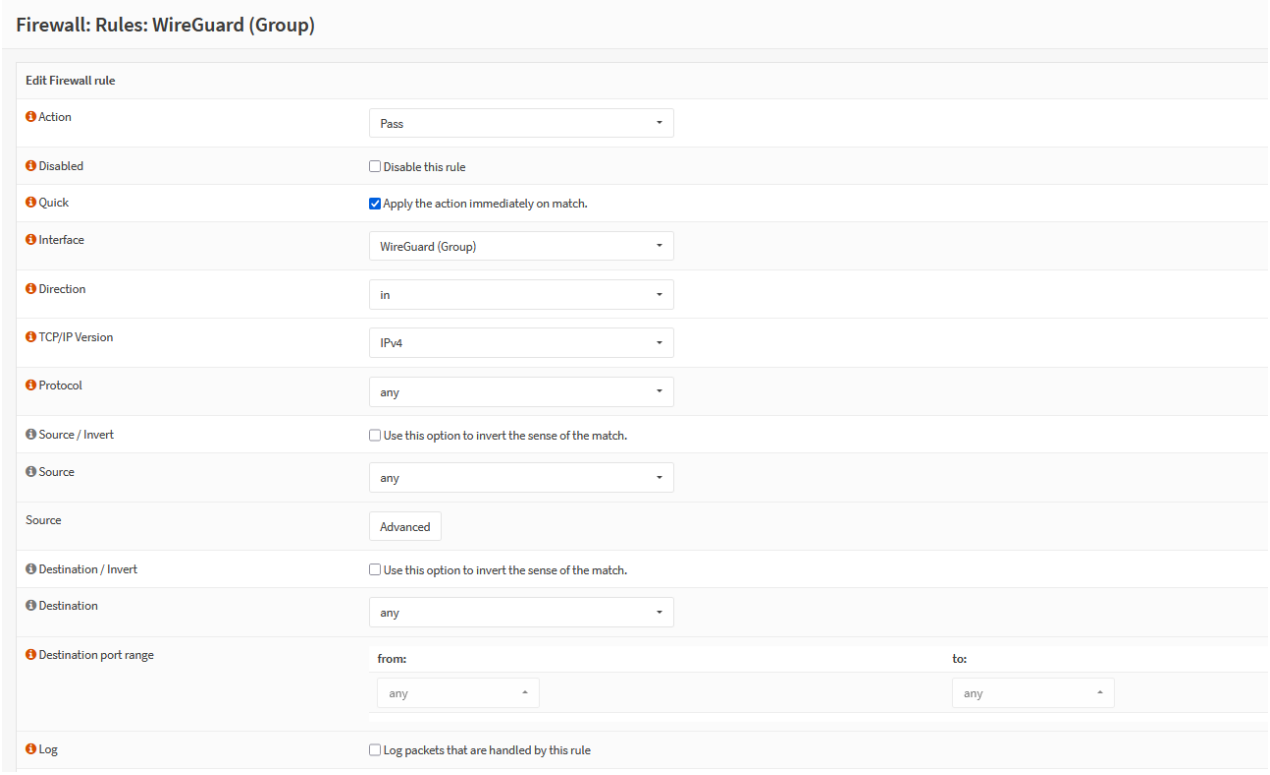
11.3 Regras de firewall

Para permitir o tráfego nesta VPN, ir a "Firewall" -> "Rules" -> "WAN" e permitir a entrada de tráfego UDP na porta escolhida para a instância Wireguard:



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

Também é necessário permitir tráfego no túnel Wireguard, indo a "Firewall" -> "Rules" -> "WireGuard (Group)" e permitir a entrada de tráfego:



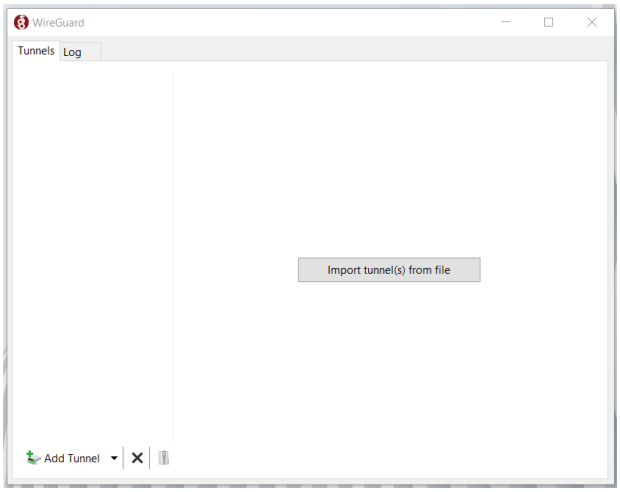
11.4 Configuração do cliente

O cliente wireguard pode ser descarregado em https://www.wireguard.com/install

Cliente Windows

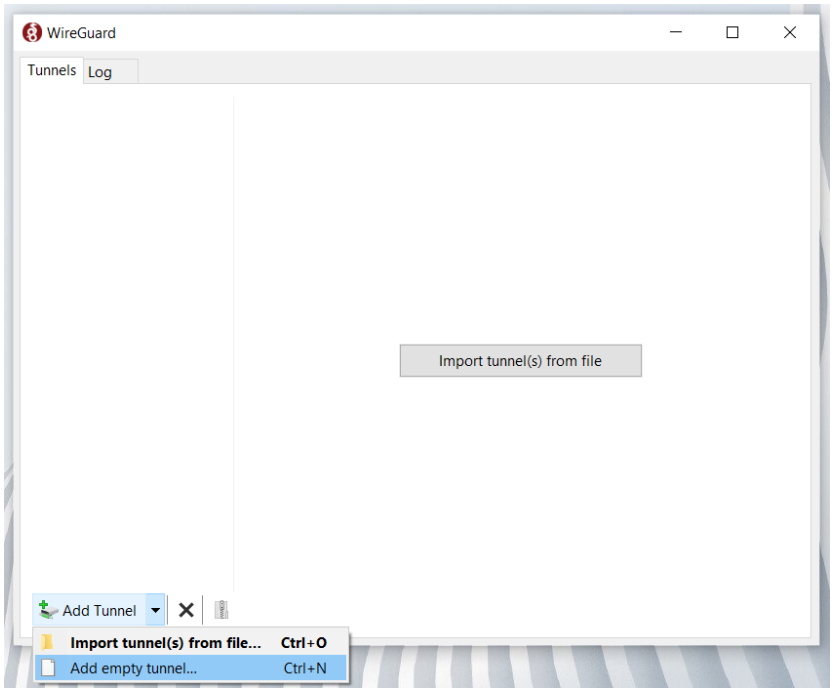
Recomendamos a instalação do pacote .msi. A instalação é bastante simples, bastando seguir as instruções.

Após concluída, surge um quadro pra configuração do túnel:



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

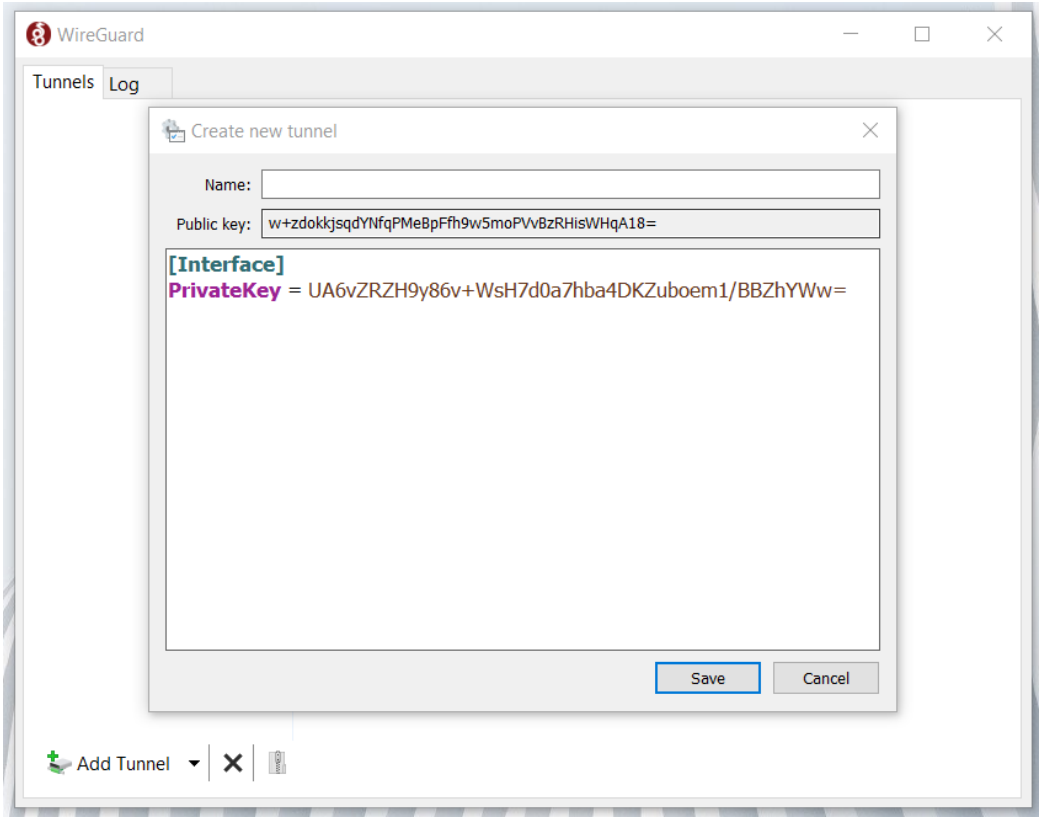
Como neste caso não existe ficheiro de configuração, devemos iniciar a criação do túnel expandindo o dropdown junto a "Add Tunnel" e escolher a opção "Add empty tunnel...":



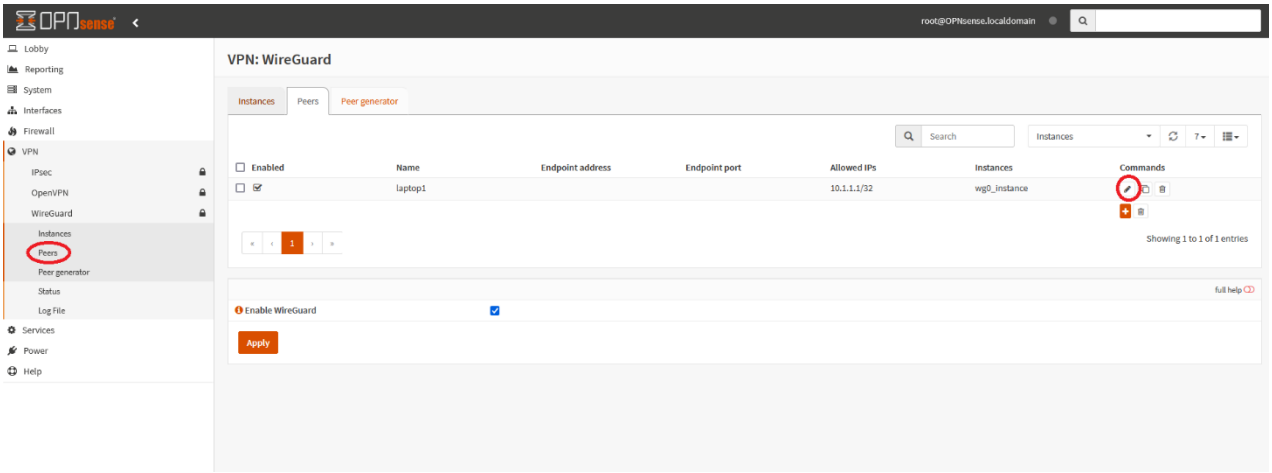
O processo de configuração á manual mas bastante simples.

O quadro seguinte mostra a situação inicial, onde é necessário dar um nome à ligação VPN, e mostra a chave pública que é necessária configurar no peer da OPNsense.

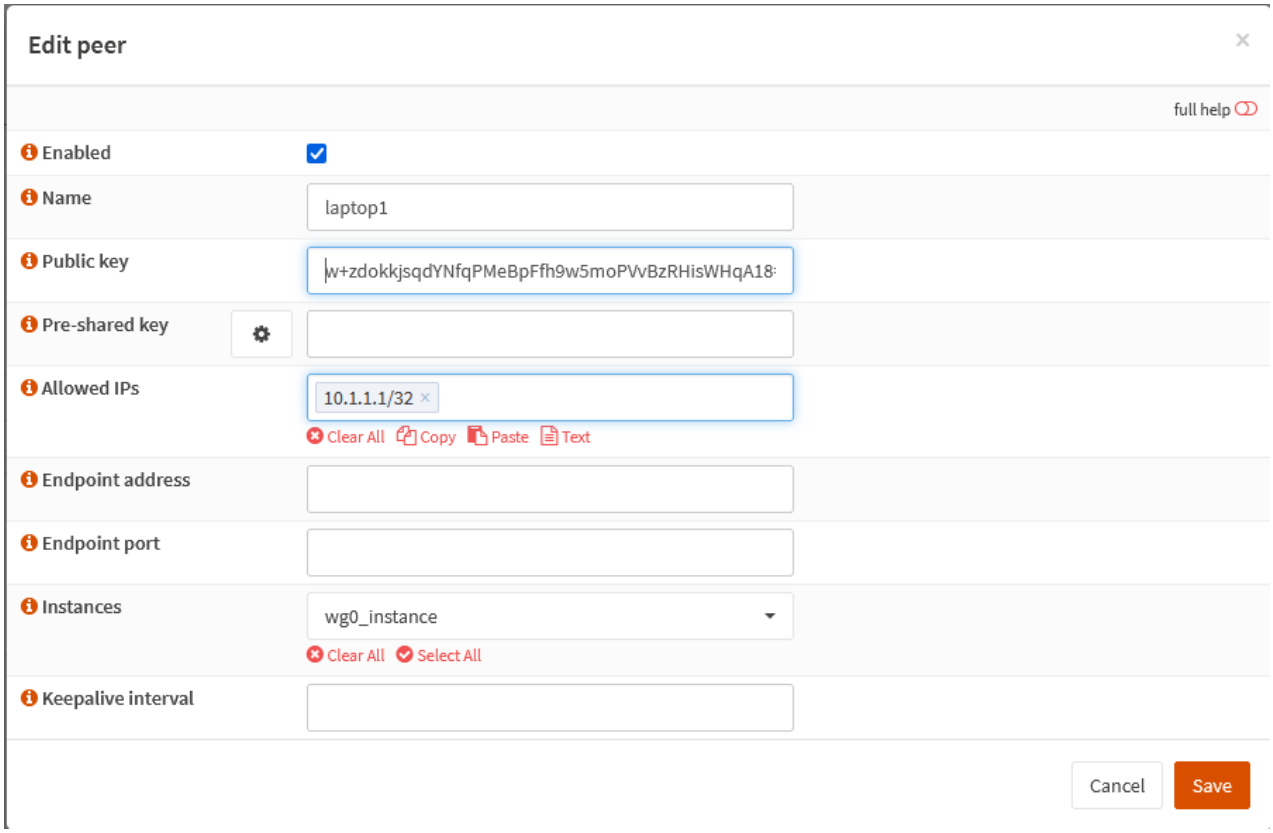
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



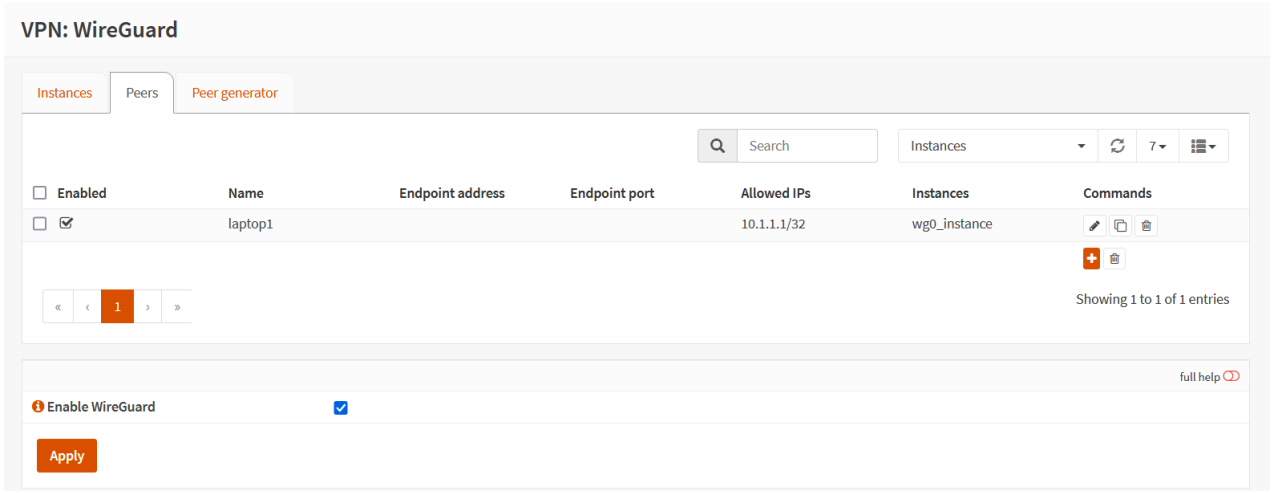
O passo seguinte é editar o Peer na OPNsense e introduzir a chave pública que aparece no cliente:



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



Fazer "Save" para guardar a configuração e depois Apply:

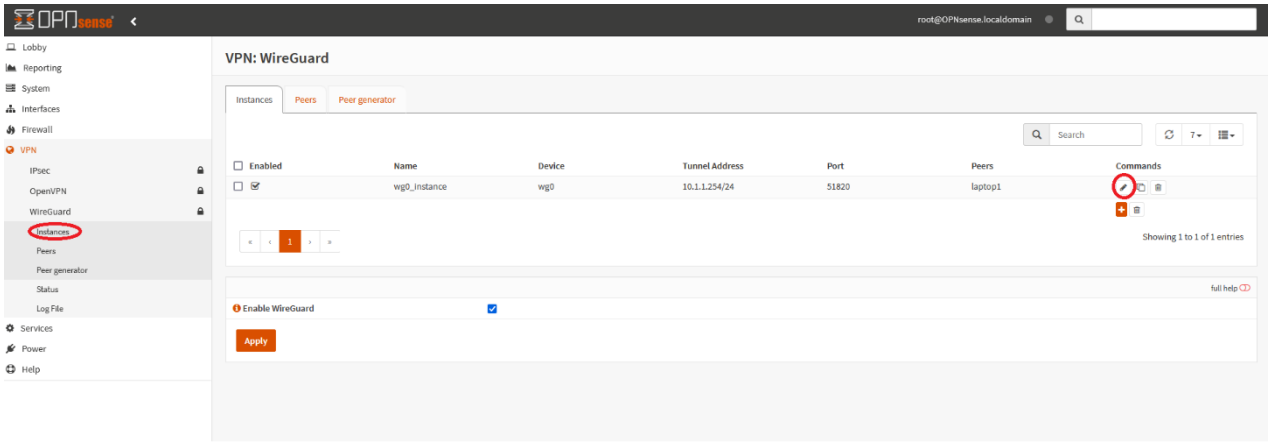


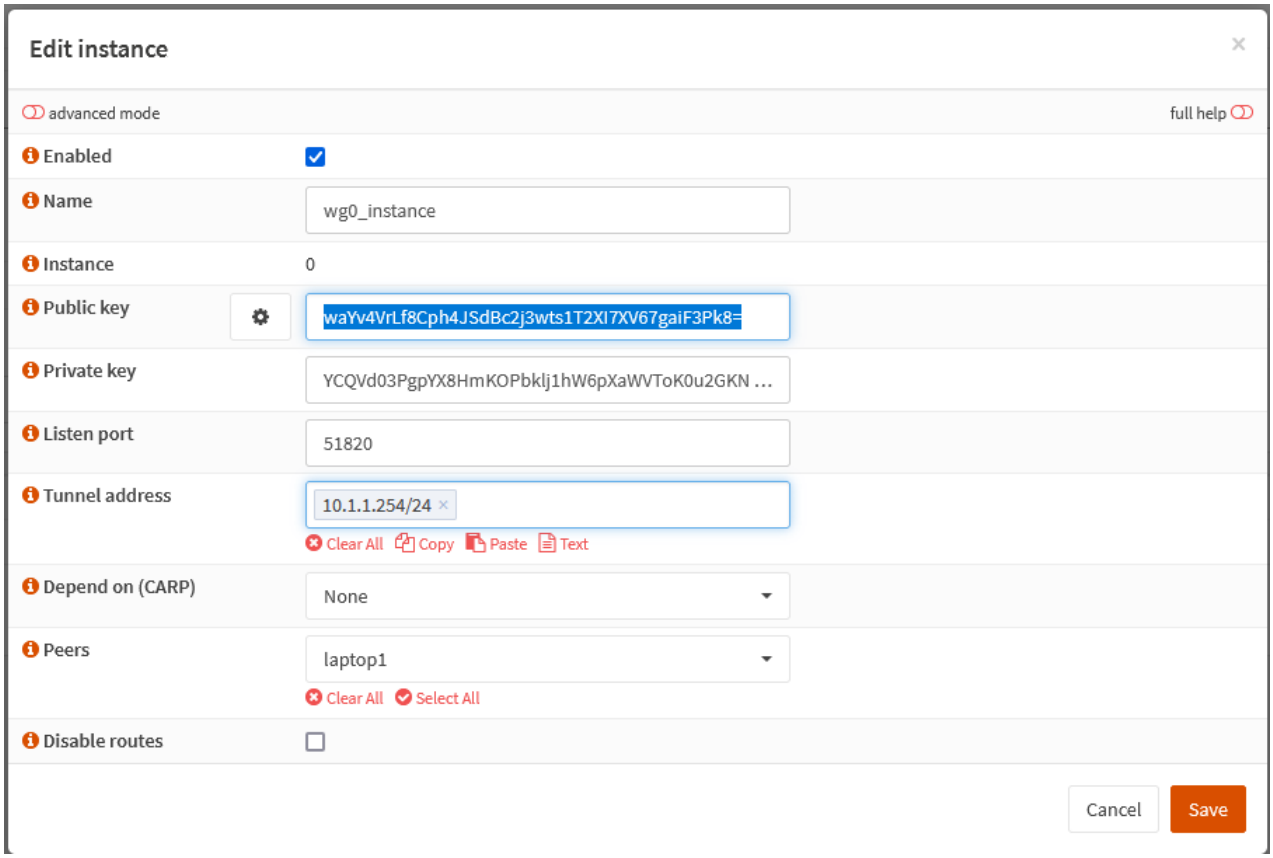
É necessário adicionar uma entrada correspondente ao endereço da VPN, que pode ser encontrado na configuração do peer na OPNsense, que neste caso corresponde a 10.1.1.1/32, como se pode ver no quadro acima. A configuração no cliente ficará como "Address = 10.1.1.1/32"

No cliente é ainda necessário criar uma nova secção "[Peer]" e debaixo dela:

- Introduzir a chave pública da instância Wireguard da OPNsense, no formato "PublicKey = chave pública". Esta chave pode ser encontrada na configuração da instância:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

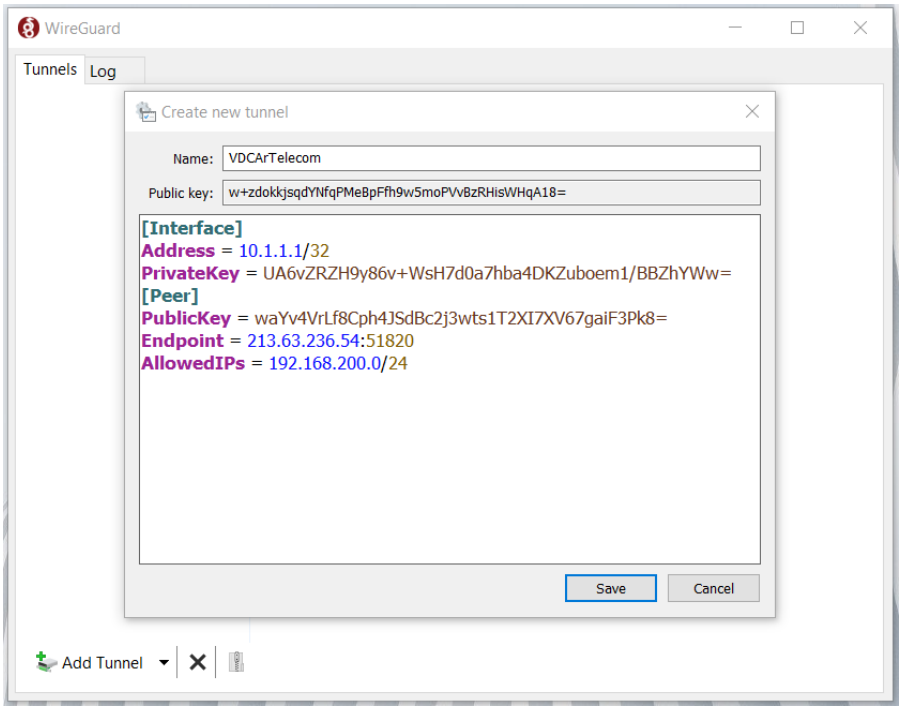




- Introduzir o endereço público e porta de acesso à instância wireguard, no formato "Endpoint = IP ou FQDN". Neste caso será 192.168.200.0/24
- Introduzir as redes a que o cliente terá acesso. Neste exemplo, iremos criar um túnel para a rede 192.168.200.x, pelo que, o formato a usar na configuração do cliente será "AllowedIPs = 192.168.200.0/24"

A configuração final ficará como se mostra abaixo:

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

12. 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.

Nos pontos seguintes demonstra-se como efetuar esta configuração.

12.1 Regras de firewall

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

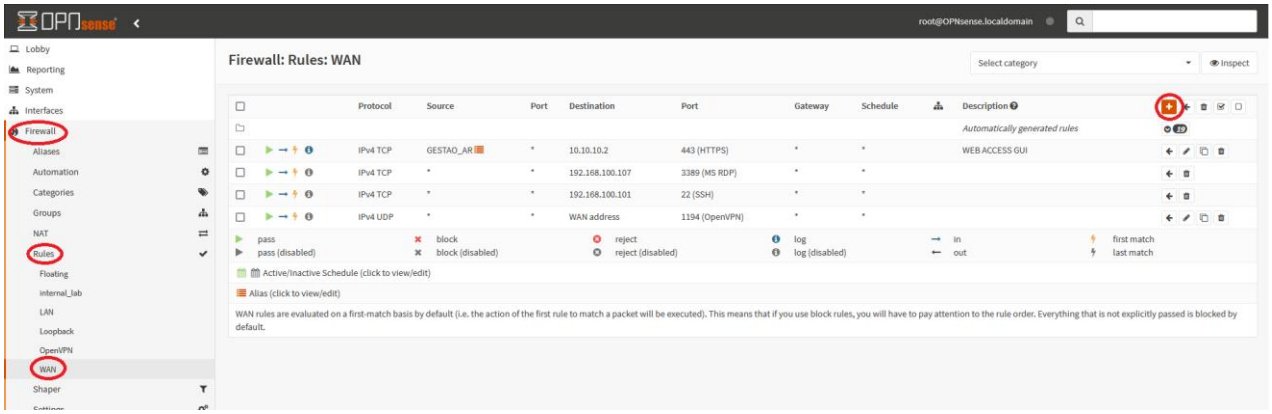
Este tráfego consiste de:

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

No caso da OPNsense a configuração fica como se mostra em baixo:

☐	▶ → ϟ ⓘ	IPv4 ESP	*	*	WAN address	*	*	*
☐	▶ → ϟ ⓘ	IPv4 TCP/UDP	*	*	WAN address	500 (ISAKMP)	*	*
☐	▶ → ϟ ⓘ	IPv4 TCP/UDP	*	*	WAN address	4500 (IPsec NAT-T)	*	*

Para o fazer, ir a **Firewall** -> **Rules** -> **WAN** e adicionar uma nova regra:

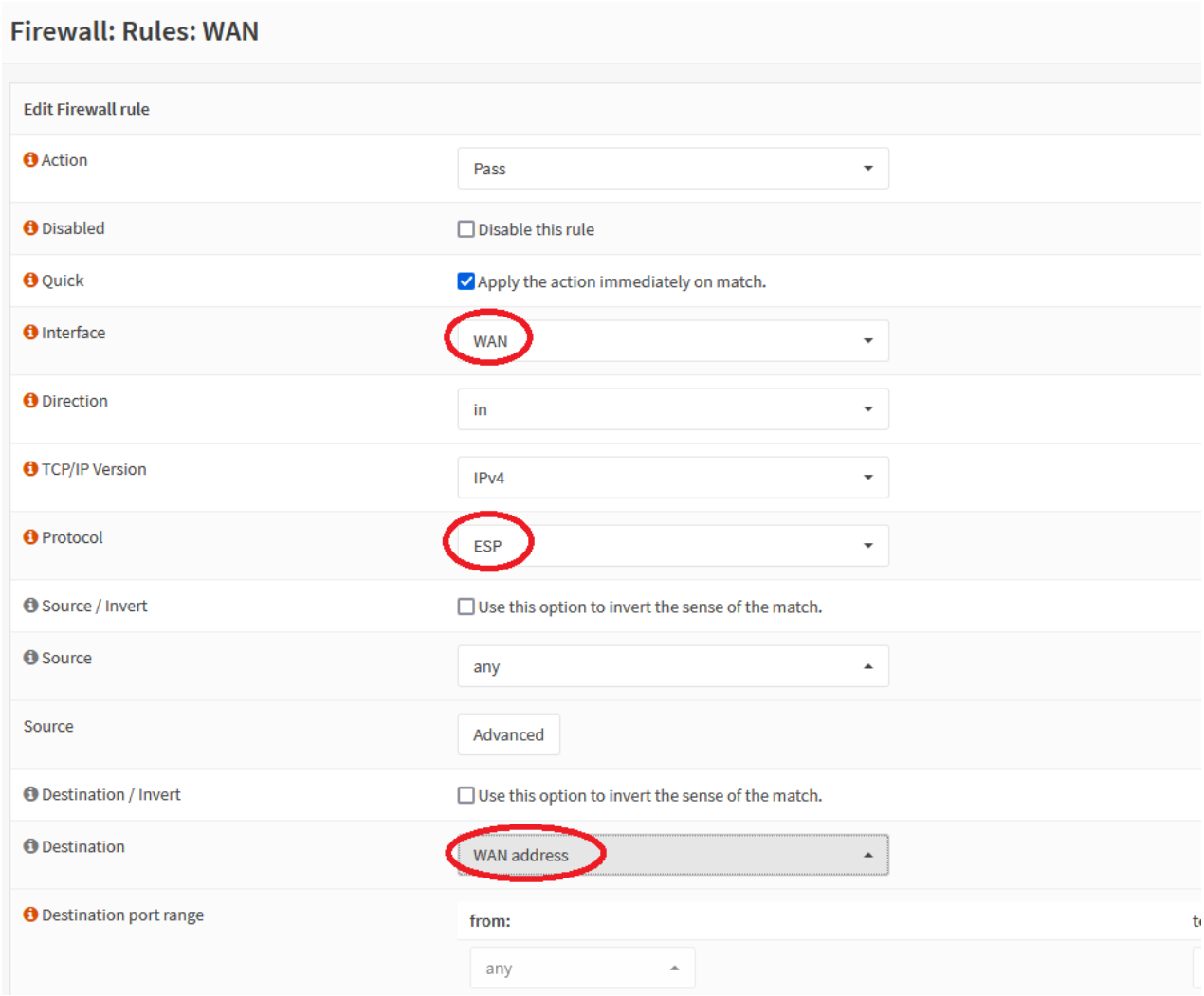


Protocolo ESP

Escolher:

- Interface: WAN
- Protocol: ESP
- Destination: WAN address
- Source: É possível limitar a ligação a um determinado IP de origem

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

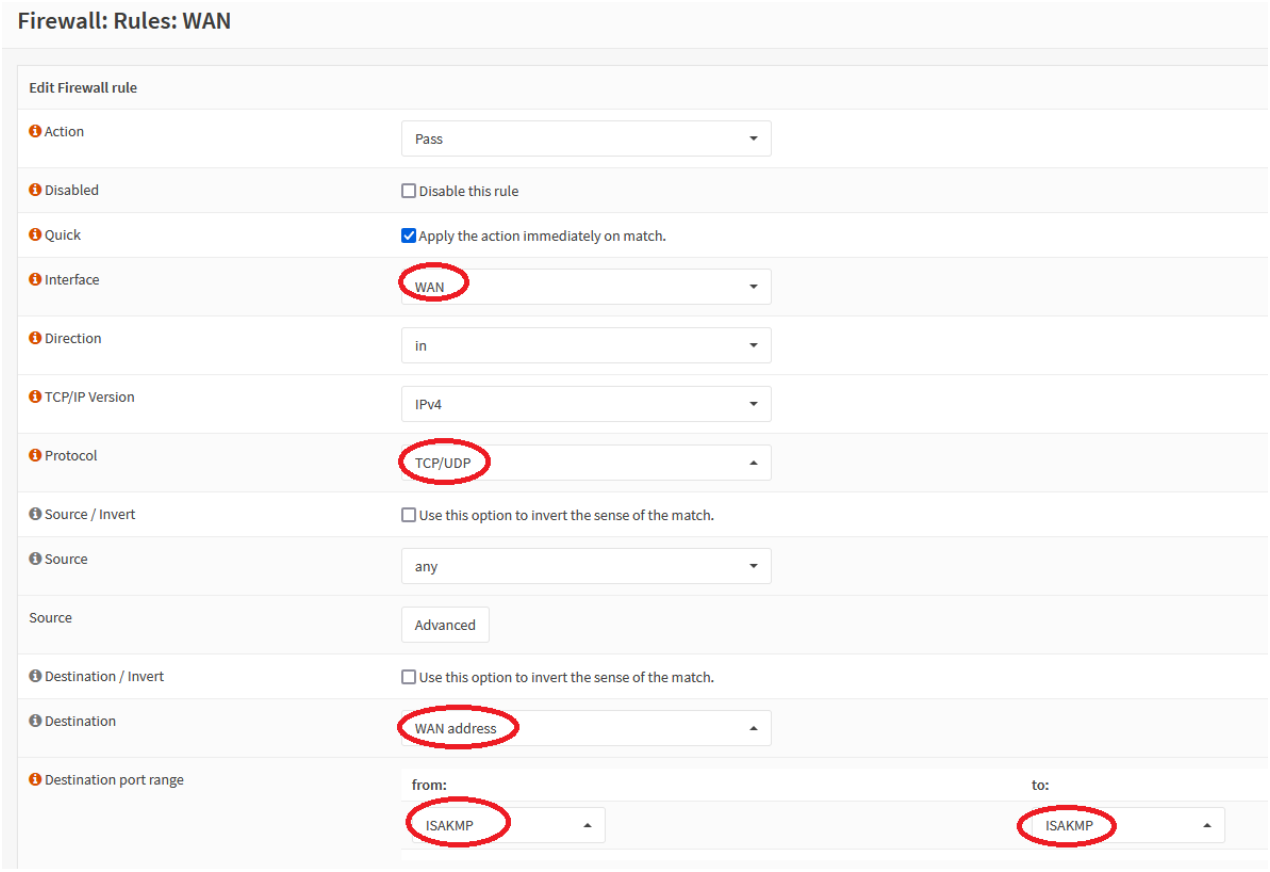


Tráfico UDP na porta 500 (ISAKMP)

Escolher:

- Interface: WAN
- Protocol: TCP/UDP
- Destination: WAN address
- Destination port range: ISAKMP
- Source: É possível limitar a ligação a um determinado IP de origem

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

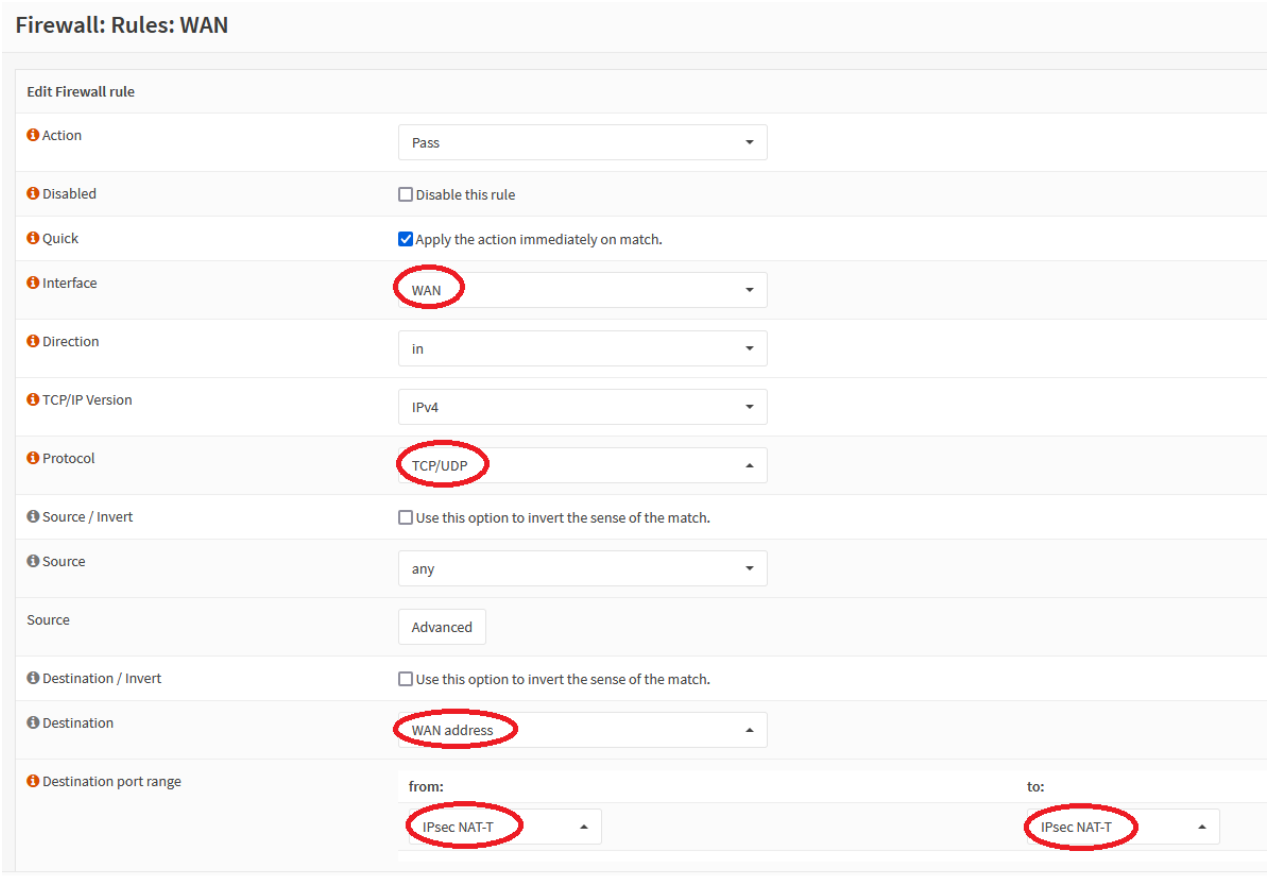


Tráfico UDP na porta 4500 (NAT-T)

Escolher:

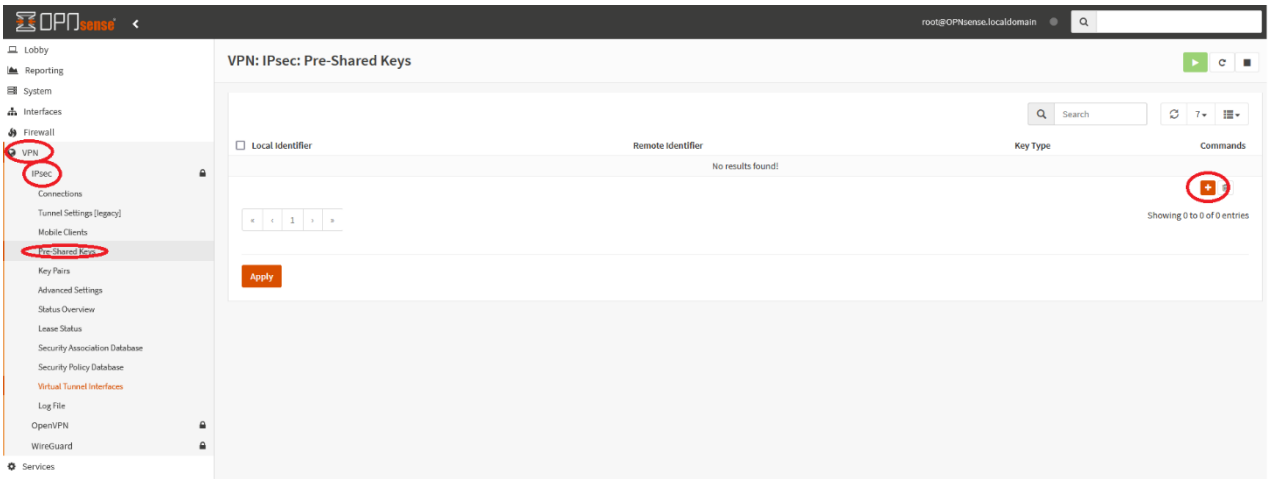
- Interface: WAN
- Protocol: TCP/UDP
- Destination: WAN address
- Destination port range: IPsec NAT-T
- Source: É possível limitar a ligação a um determinado IP de origem

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



12.2 Pre-Shared Keys

Para criar a PSK, ir a **VPN** -> **IPsec** -> **Pre-Shared Keys** e carregar em + para criar uma nova entrada:



Preencher os identificadores Local e Remoto. Por exemplo, o identificador local pode ser o IP público associado à firewall (NOTA: no caso do vCloud, este IP público corresponde ao IP público do router Edge) e o identificador remoto pode ser o IP público do dispositivo remoto.

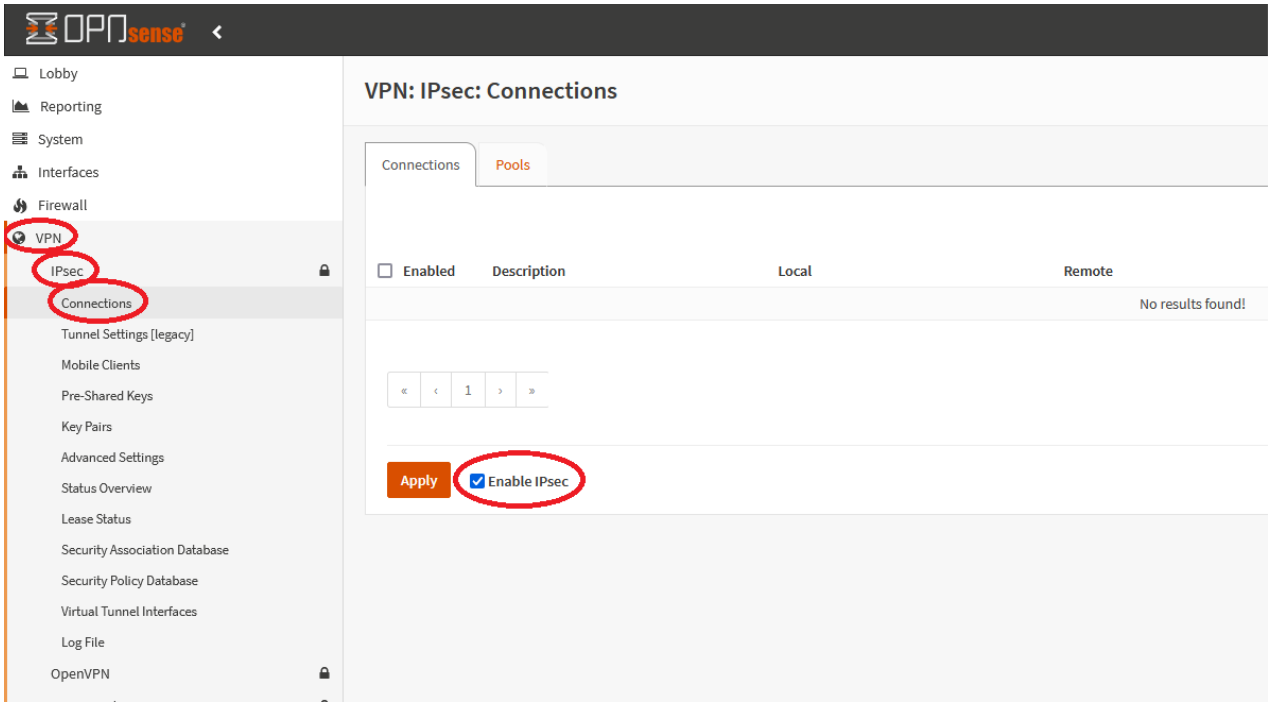
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

A chave PSK poderá ser gerada em qualquer ferramenta para o efeito e introduzida neste quadro.

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

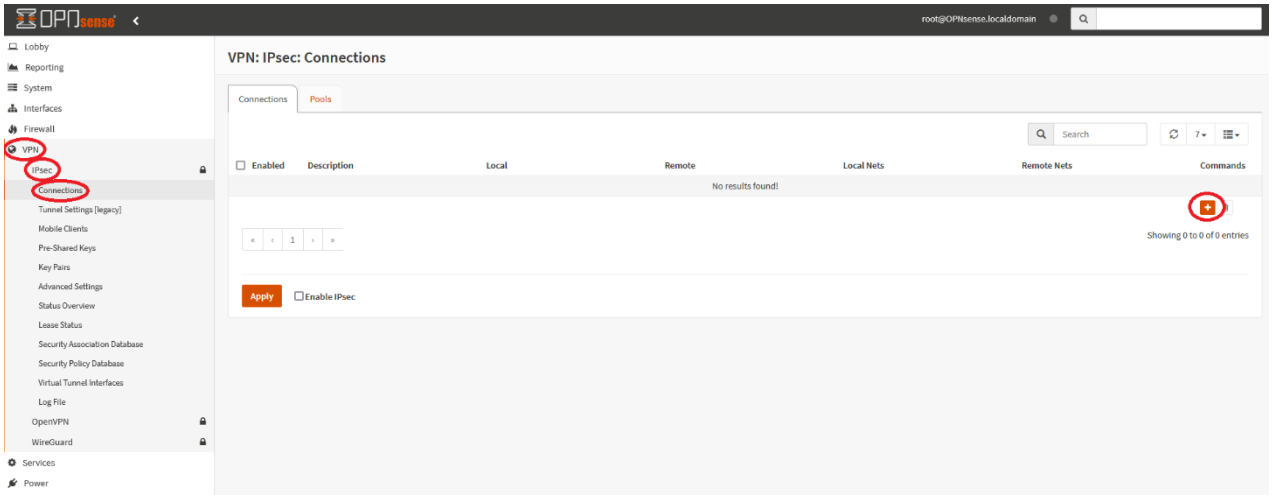
12.3 Configuração do túnel

Para definir o túnel IPsec configuramos a conexão, começando por ativar o IPsec em **VPN** -> **IPsec** -> **Connections**



Para configurar a ligação de túnel IPsec, no mesmo quadro adicionar uma nova ligação carregando em **+**:

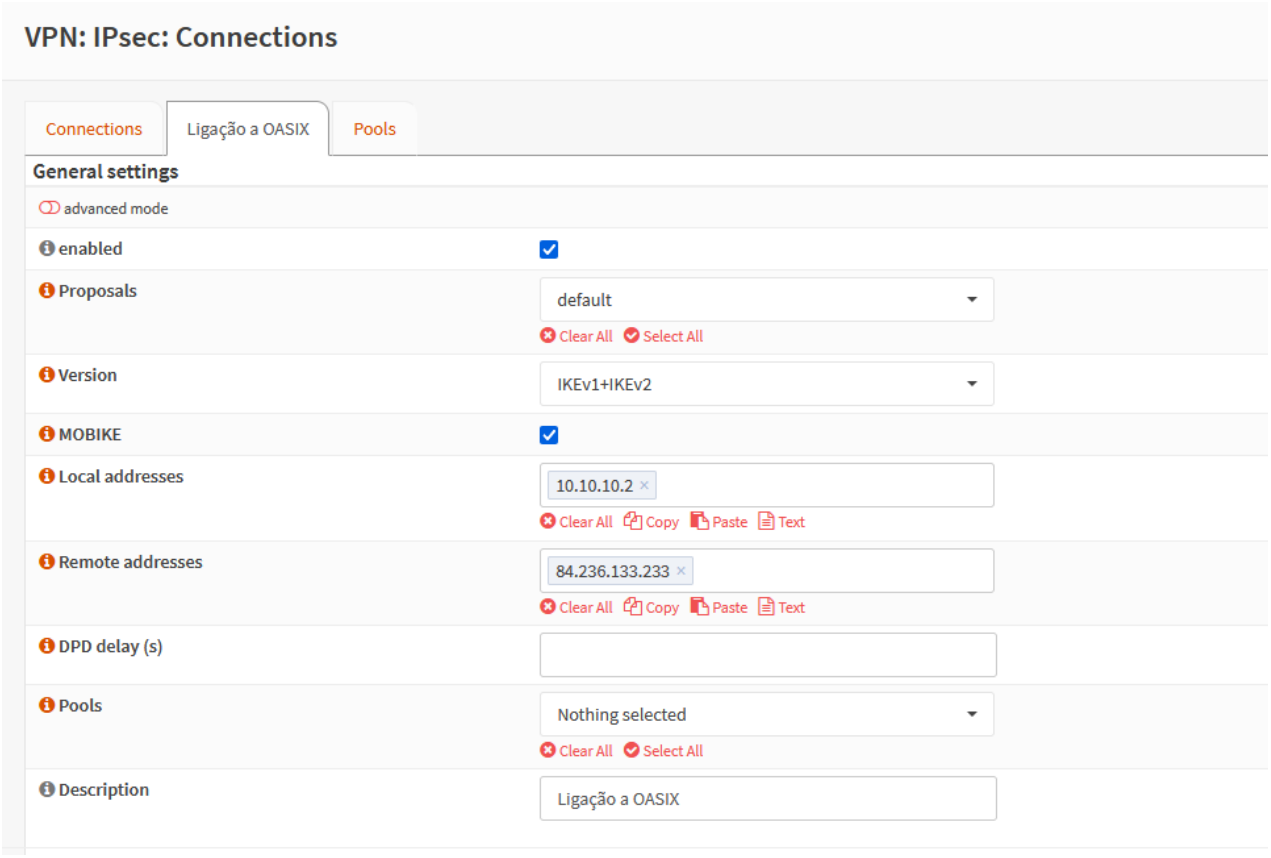
Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



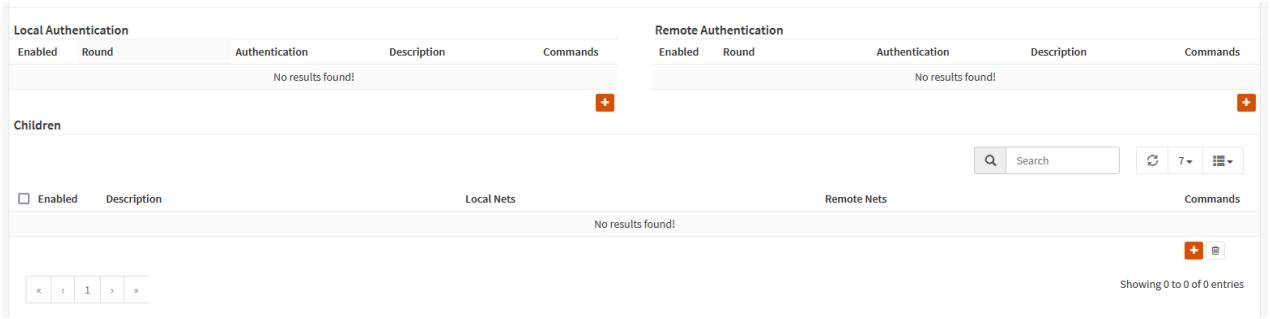
Surge um quadro de configuração em modo simples onde podemos efetuar as seguintes configurações:

- Proposals: é um conjunto de algoritmos a utilizar. O default corresponde a um conjunto de algoritmos considerados seguros, mas pode ser escolhido um conjunto que corresponda à configuração no destino (por exemplo, AES256, SHA512, 2048 bit – DH tipo 14).
- Version: por defeito IKEv1+IKEv2
- Local addresses: endereço da interface WAN da OPNsense (diferente do IP público do router Edge)
- Remote addresses: endereço público remoto
- Description: uma designação da ligação

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



Fazendo Save surge um novo quadro para configurar as autenticações local e remota.

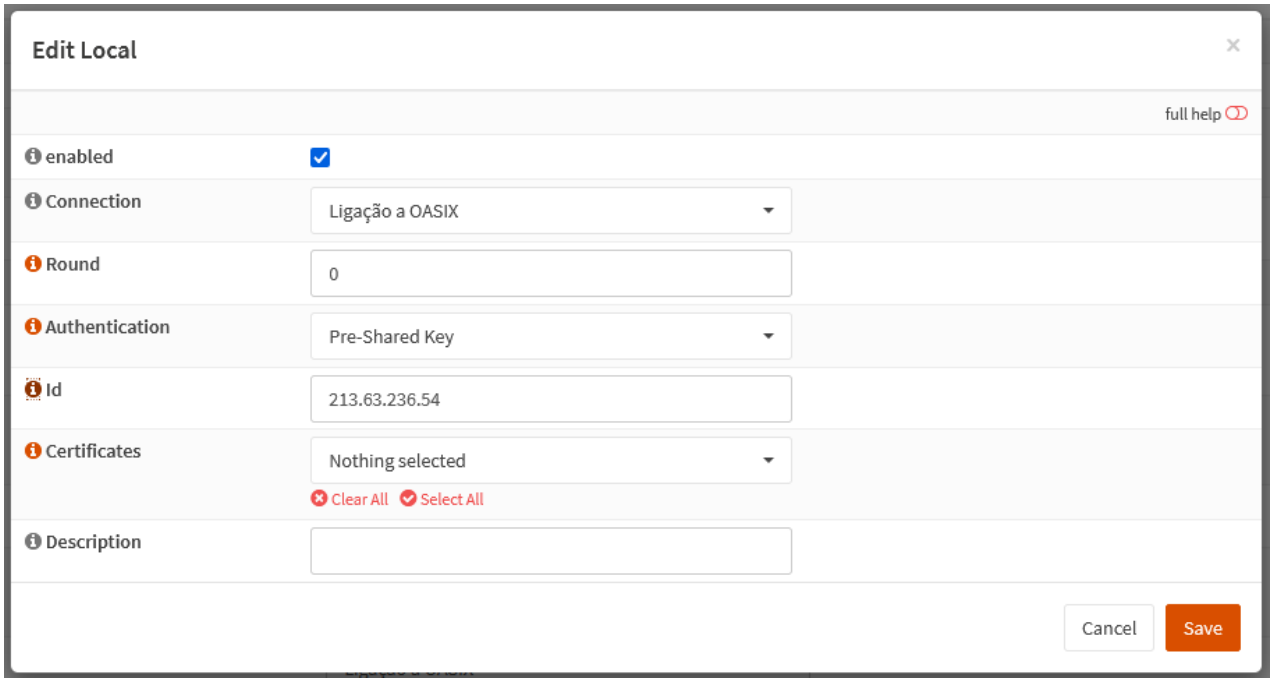


Carregando em **+** permite efetuar as respetivas configurações. Para a autenticação local:

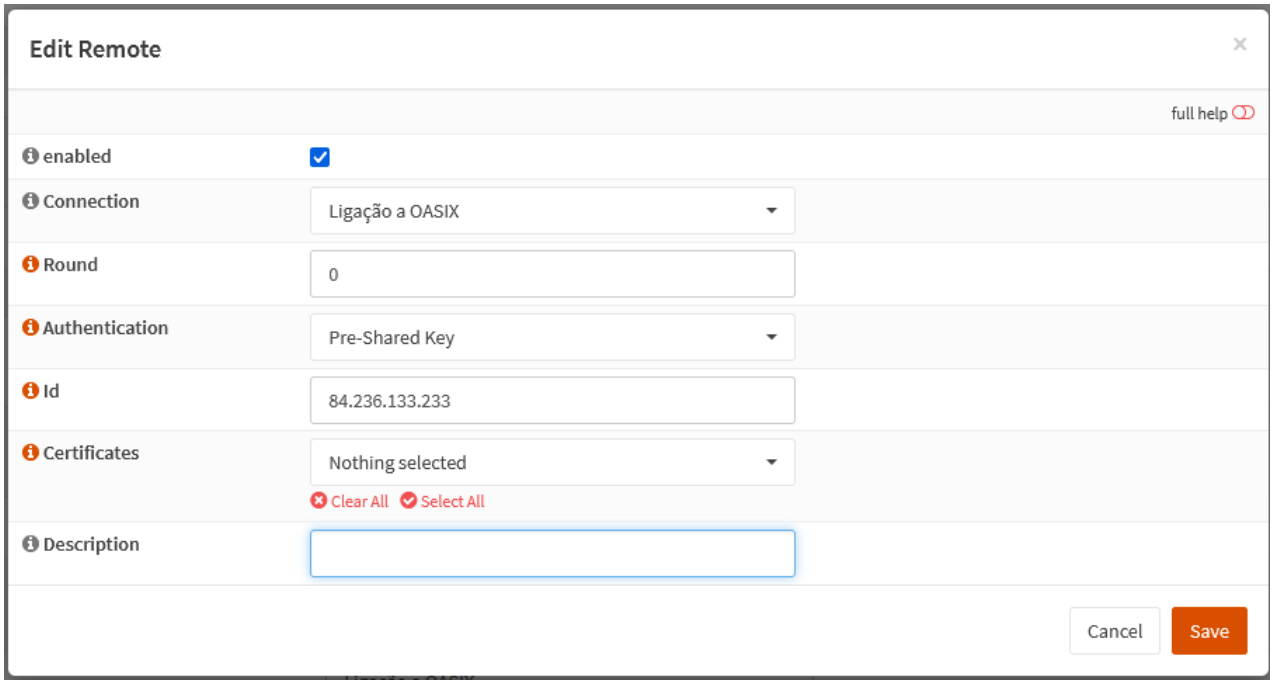
Escolher:

- Connection: a ligação criada anteriormente
- Authentication: Pre-Shared Key
- Id: tem de ser o mesmo que foi utilizado para a criação da Pre-Shared Key.
- Certificates: deixar sem seleção

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt



E o mesmo para a autenticação remota:



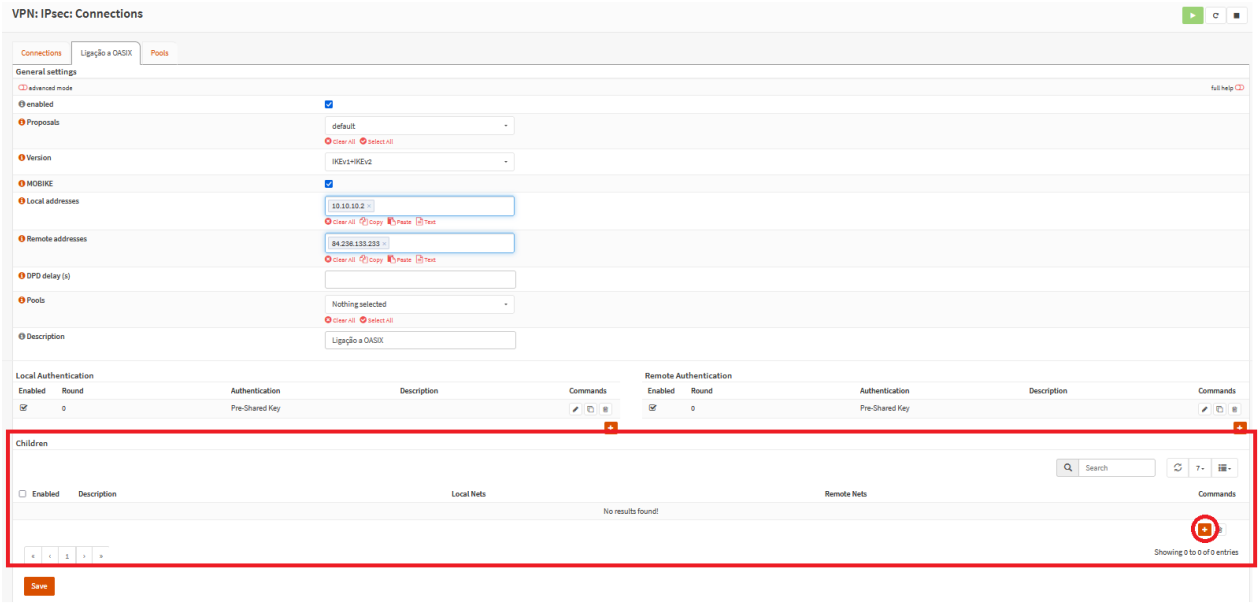
Finalizar fazendo "Save" e "Apply" garantindo que "Enable IPsec" se encontra ativado.

12.4 Interligação das sub-redes

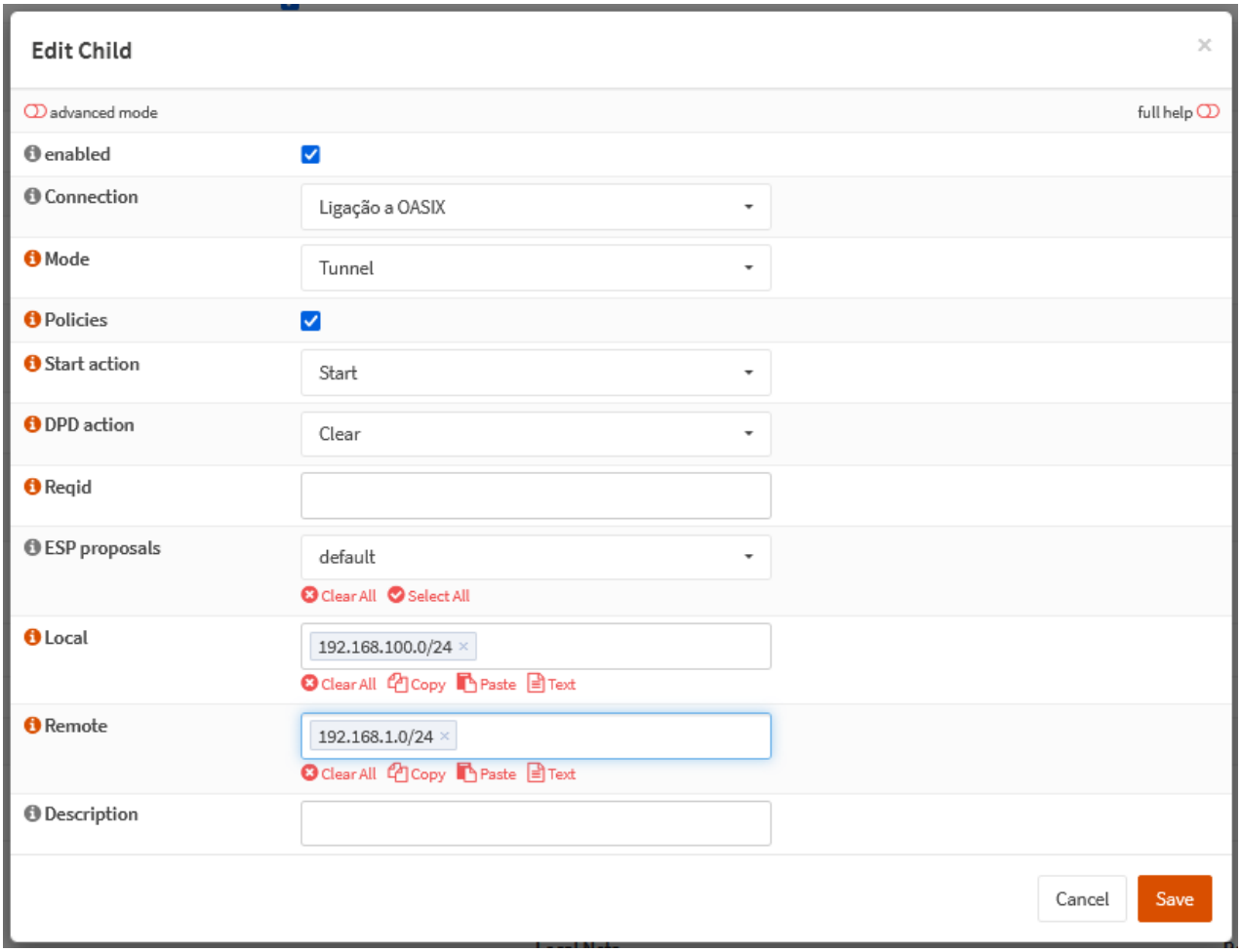
Agora que o túnel está configurado entre os dois dispositivos, podemos configurar as ligações entre as sub-redes. Isso é feito na OPNsense no sub-menu "**Children**".

Assim sendo, adicionar uma nova ligação carregando em "**+**":

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

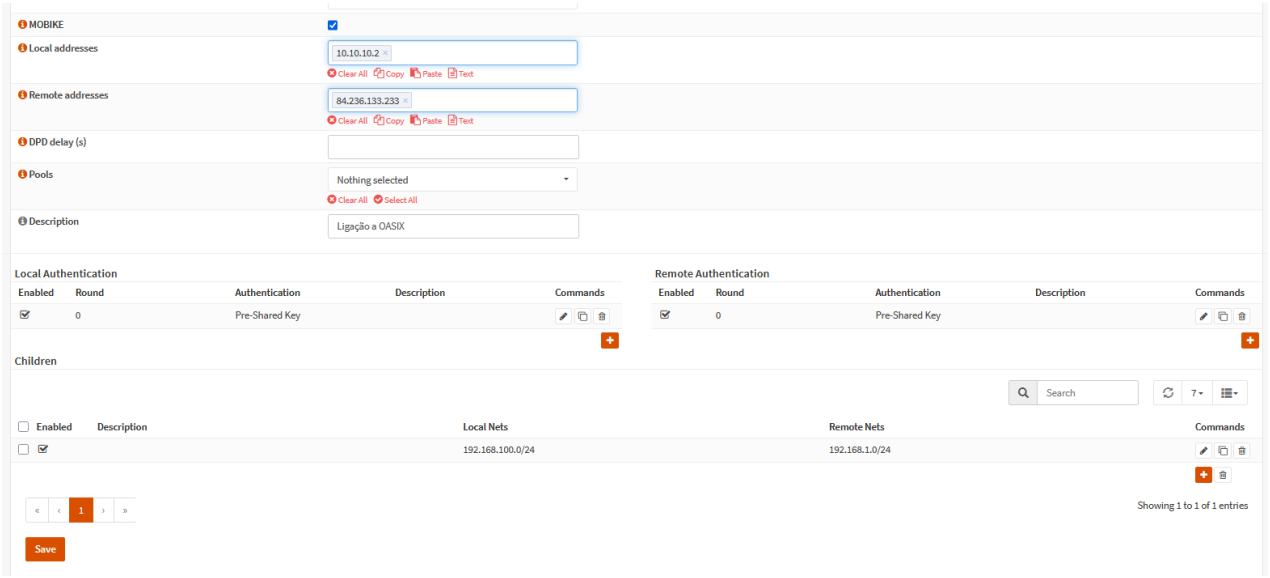


Introduzir as redes local e remota e fazer "**Save**":

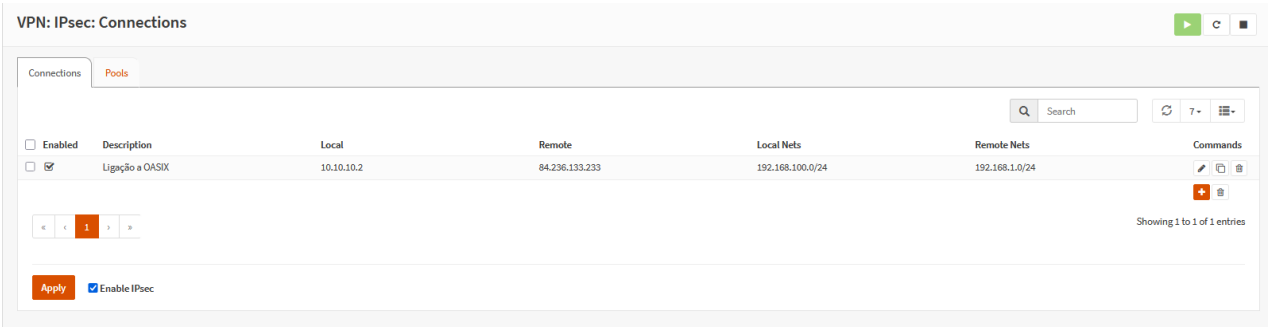


Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

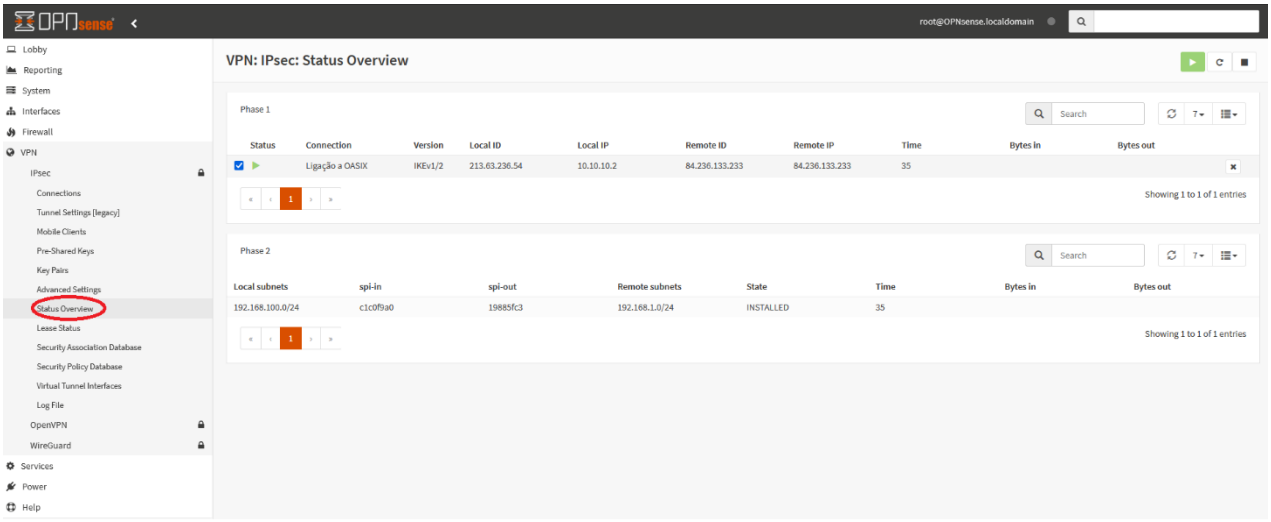
No quadro da Conexão fazer novamente “Save”:



E finalmente, “Apply” da configuração:



Podemos verificar a criação do túnel e respetiva conetividade em “**Status Overview**”:



Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt

O passo final é o de permitir o tráfego entre as duas sub-redes, permitindo o tráfego de entrada em **Firewall** -> **Rules** -> **IPsec**.

Serviço de apoio a clientes
portal.ar.pt
800 300 400
ar@ar.pt