



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

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

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

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

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>

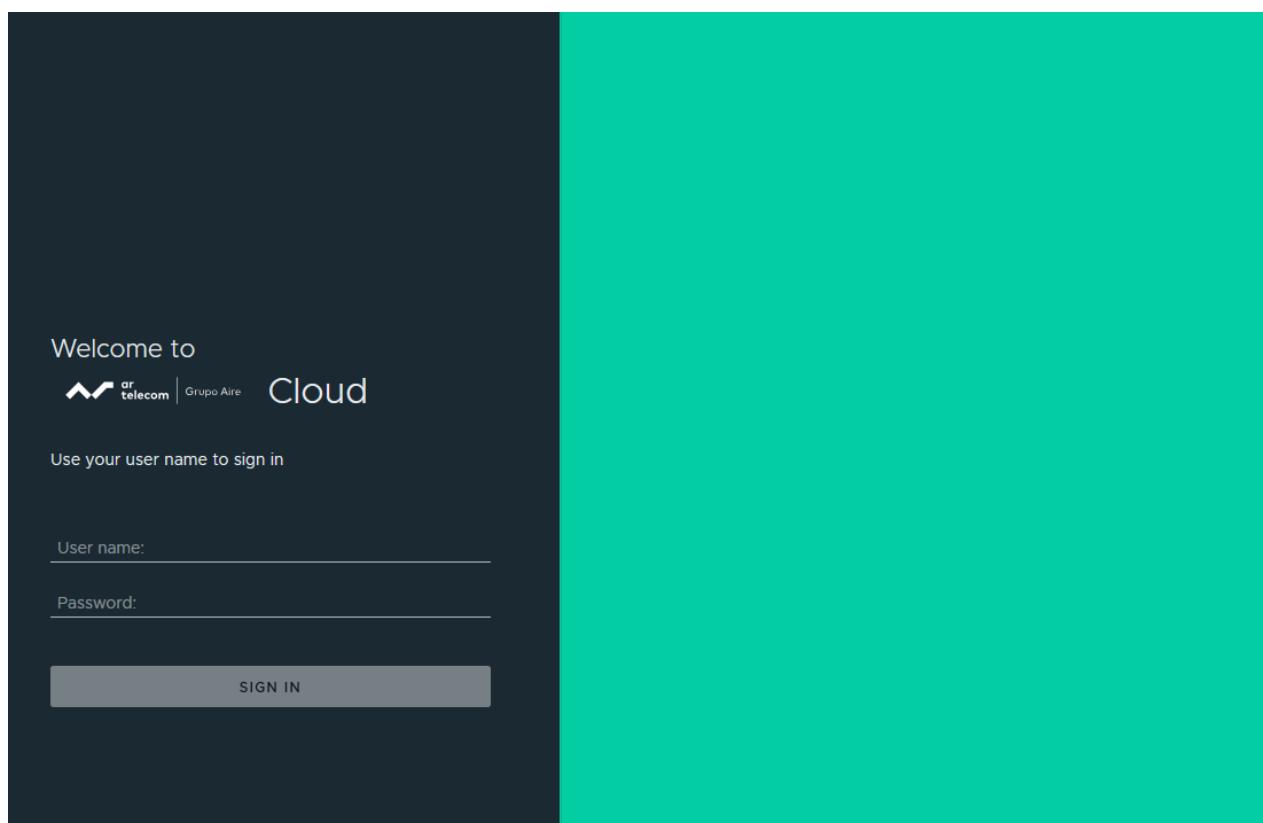
2. INSTALAÇÃO DE INSTÂNCIA FIREWALL

2.1 Preparação vCloud

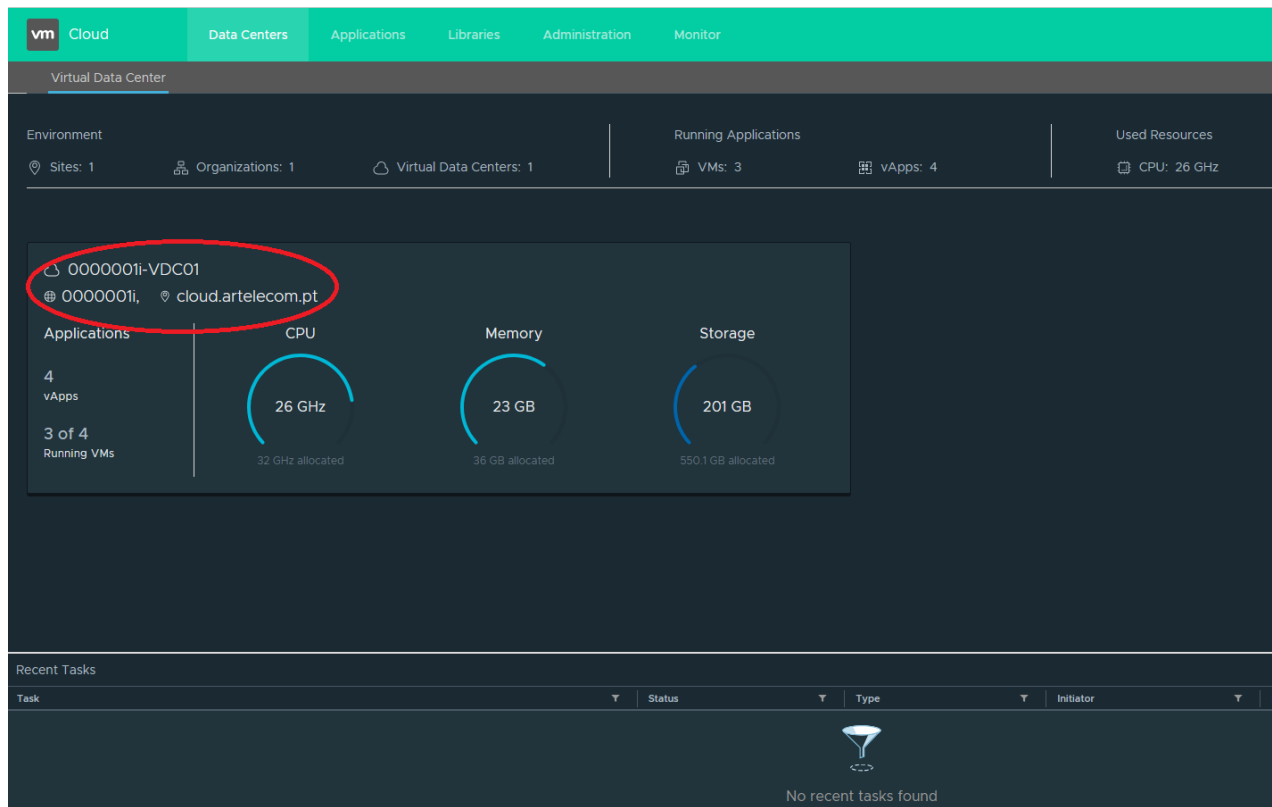
A implementação de uma instância de firewall customizada implica algumas configurações específicas no router Edge do Virtual Data Center.

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

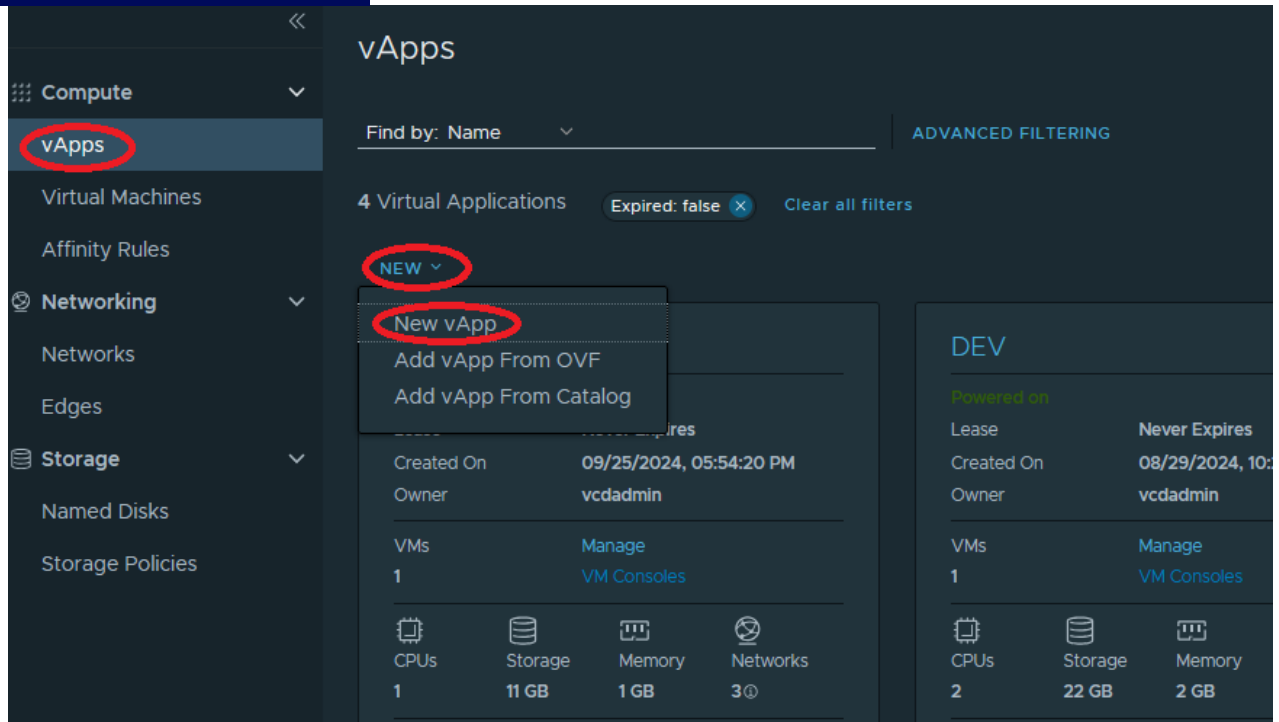
O primeiro passo é aceder à consola do virtual data center, usando o URL e credenciais que lhe foram enviados aquando da ativação do serviço VDC:



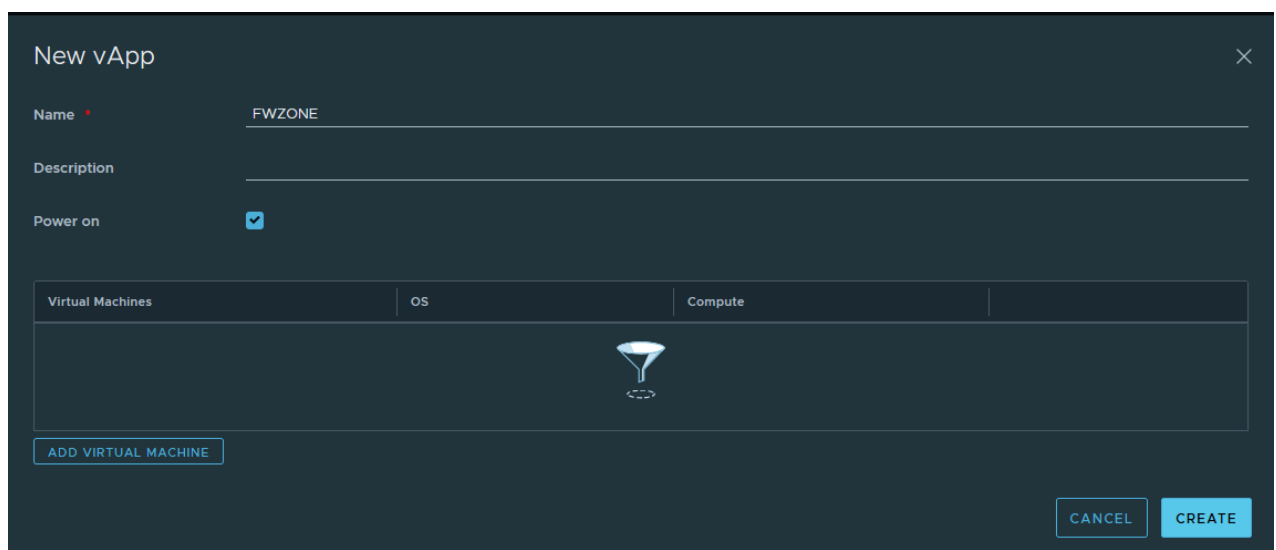
Após uma autenticação bem-sucedida, surge o painel inicial onde deve seleccionar o VDC:



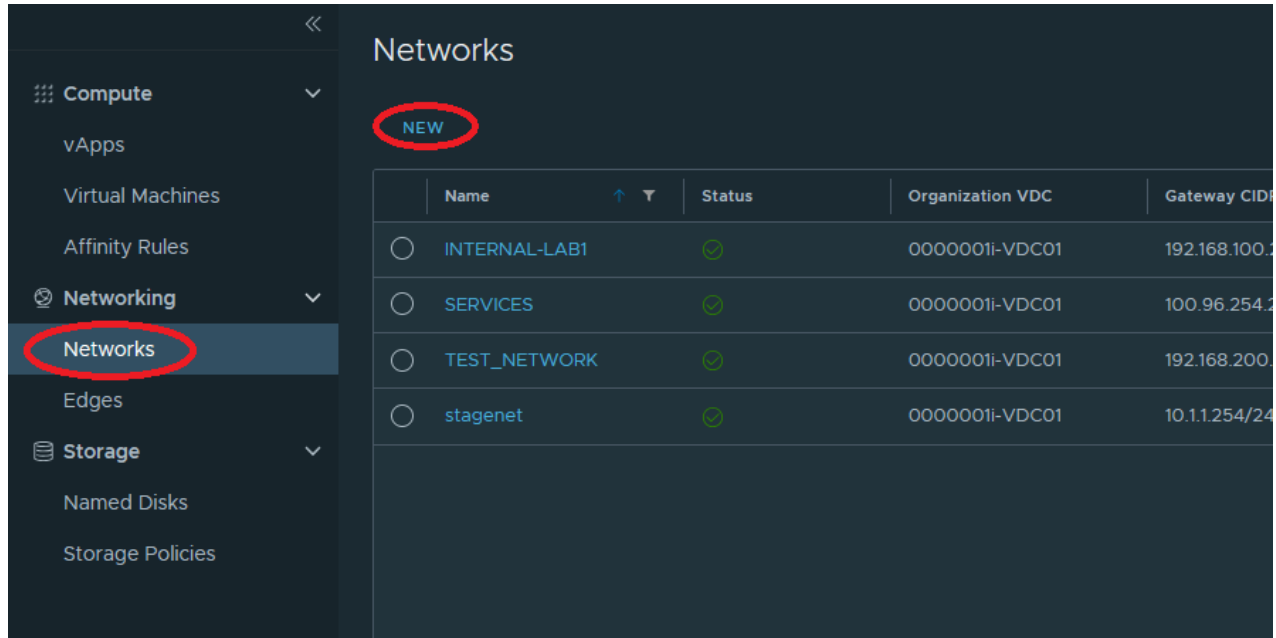
Recomendamos a criação de uma vApp específica para as instâncias de firewall. Para isso, carregar em cima de “vApps” no menu lateral esquerdo e de seguida em “NEW” e “New vApp”:



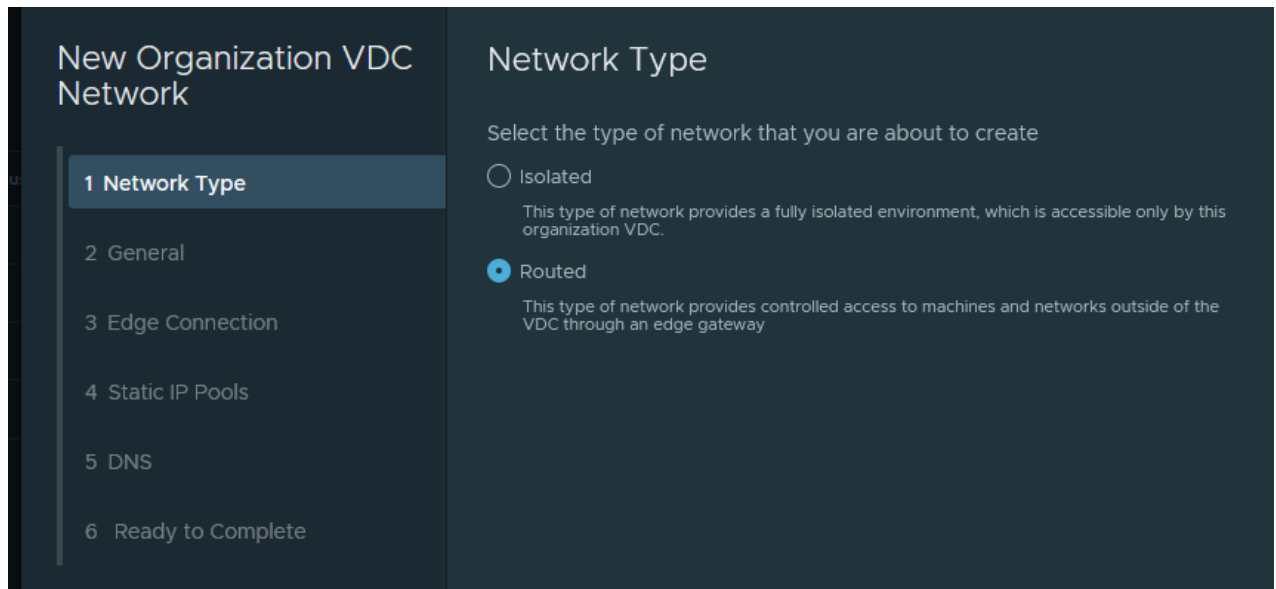
Dar um nome à vApp, seleccionar opção "Power on" e "CREATE". Não adicionar nenhuma máquina virtual à vApp nesta fase.



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:

New Organization VDC Network

- 1 Network Type
- 2 General**
- 3 Edge Connection
- 4 Static IP Pools
- 5 DNS
- 6 Ready to Complete

General

Name *

Gateway CIDR * ⓘ

Description

Shared ⓘ

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.

New Organization VDC Network

- 1 Network Type
- 2 General
- 3 Edge Connection**
- 4 Static IP Pools
- 5 DNS
- 6 Ready to Complete

Edge Connection

Name	External Networks	Org VDC Networks
0000001i-ESG00	1	3

1 - 1 of 1 Edge Gateway(s)

Interface Type: Internal

Guest VLAN Allowed:

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

New Organization VDC Network

- 1 Network Type
- 2 General
- 3 Edge Connection
- 4 Static IP Pools**
- 5 DNS
- 6 Ready to Complete

Static IP Pools

Gateway CIDR: ⓘ

Static IP Pools
Enter an IP range (format: 192.168.1.2 - 192.168.1.100)

Total IP addresses: 0

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

New Organization VDC Network

- 1 Network Type
- 2 General
- 3 Edge Connection
- 4 Static IP Pools
- 5 DNS**
- 6 Ready to Complete

DNS

Use Edge DNS ⓘ
Select this option to use DNS relay of the gateway. DNS relay must be pre-configured on the gateway.

Primary DNS:

Secondary DNS:

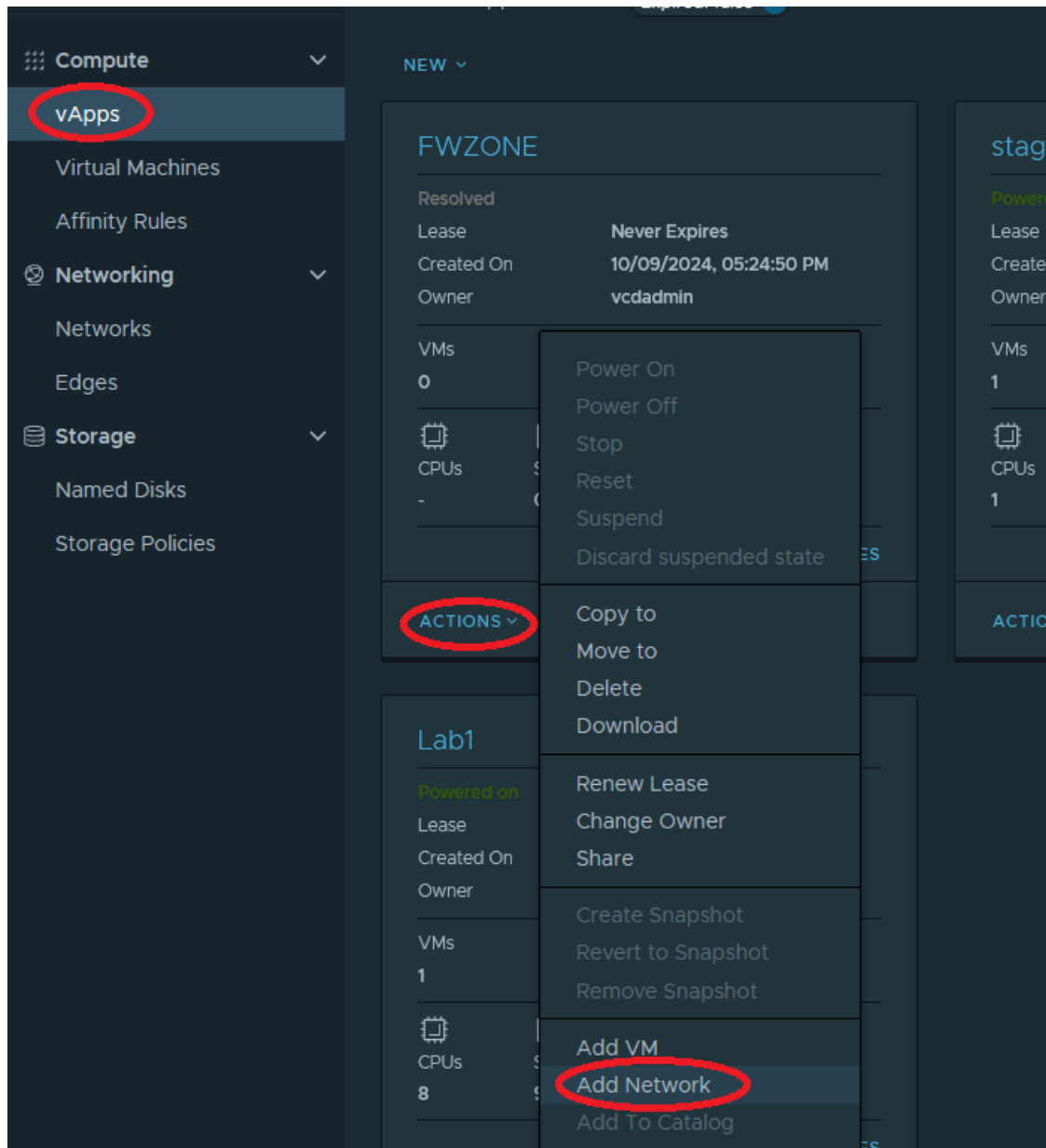
DNS suffix:

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.

<input type="radio"/>	DEV_NETWORK		0000001i-VDC01	192.168.100.254/24	Routed	0000001i-ESG00		73%
<input type="radio"/>	PROD_NETWORK		0000001i-VDC01	192.168.250.254/24	Routed	0000001i-ESG00		1%
<input type="radio"/>	SERVICES		0000001i-VDC01	100.96.254.254/16	Direct	NETWORK-SYS-BCK		6%
<input type="radio"/>	TEST_NETWORK		0000001i-VDC01	192.168.200.254/24	Routed	0000001i-ESG00		6%
<input type="radio"/>	interFWnet		0000001i-VDC01	100.88.0.1/29	Routed	0000001i-ESG00		-

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":



Selecionar opção "OrgVDC Network"



e escolher a rede criada anteriormente:

Add Network to FWZONE

Type OrgVDC Network vApp Network

Name	Status	Organization VDC	Gateway CIDR	Network Type	Connected To	IP Pool Consumed	Shared	Route Advertised
BridgeNet		0000001-VDC...	10.10.1.254/24	Routed	-	1%		-
DEV_NETWORK		0000001-VDC...	192.168.100.254/24	Routed	-	73%		-
PROD_NETWORK		0000001-VDC...	192.168.250.254/24	Routed	-	1%		-
SERVICES		0000001-VDC...	100.96.254.254/16	Direct	NETWORK-SYS-B...	6%		-
TEST_NETWORK		0000001-VDC...	192.168.200.254/24	Routed	-	6%		-
interFWnet		0000001-VDC...	100.88.0.1/29	Routed	-			-

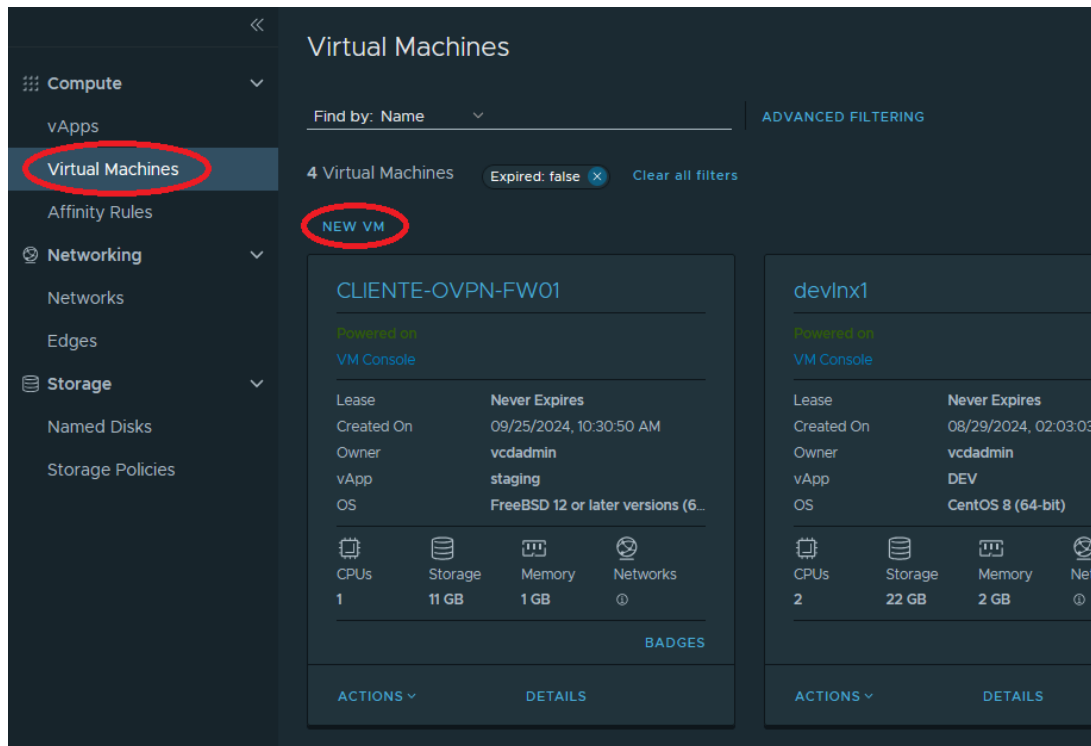
1 - 6 of 6 network(s)

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":



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.

New VM

Name

Computer Name

Description

Type New From Template

Power on

Templates

Name	vApp Name	Catalog	OS	Compute
<input type="radio"/> Linux	Base Linux	Base	Other Linux (64-bit)	CPU Memory
<input type="radio"/> Dimension	watchguard-dimension_2_1_2_U4.ova	Network Appliances	Ubuntu Linux (64-bit)	CPU Memory
<input checked="" type="radio"/> CLIENTE-OVPN-FW01	OPNSense 24.7	Network Appliances	FreeBSD 12 or later versions (64-bit)	CPU Memory
<input type="radio"/> CentOS7-x86-64	CentOS 7 x86_64	Base	CentOS 4/5 or later (64-bit)	CPU Memory

New VM

Compute

Placement Policy Linux

Use custom storage policy

Custom storage policy to use SSD

NICs

Primary NIC	NIC	Connected	Network Adapter Type	Network	IP Mode	IP Address	External IP Address	MAC Address
<input checked="" type="radio"/>	0	<input type="checkbox"/>	VMXNE	None	None		-	00:50:56:01:3b
<input type="radio"/>	1	<input type="checkbox"/>	VMXNE	None	None		-	00:50:56:01:3b

Custom Properties

There are no user configurable properties.

End User License Agreements

There are no EULAs to review.

Após carregar em OK o sistema irá compor a VM

Virtual Machines

Find by: Name

5 Virtual Machines

NEW VM

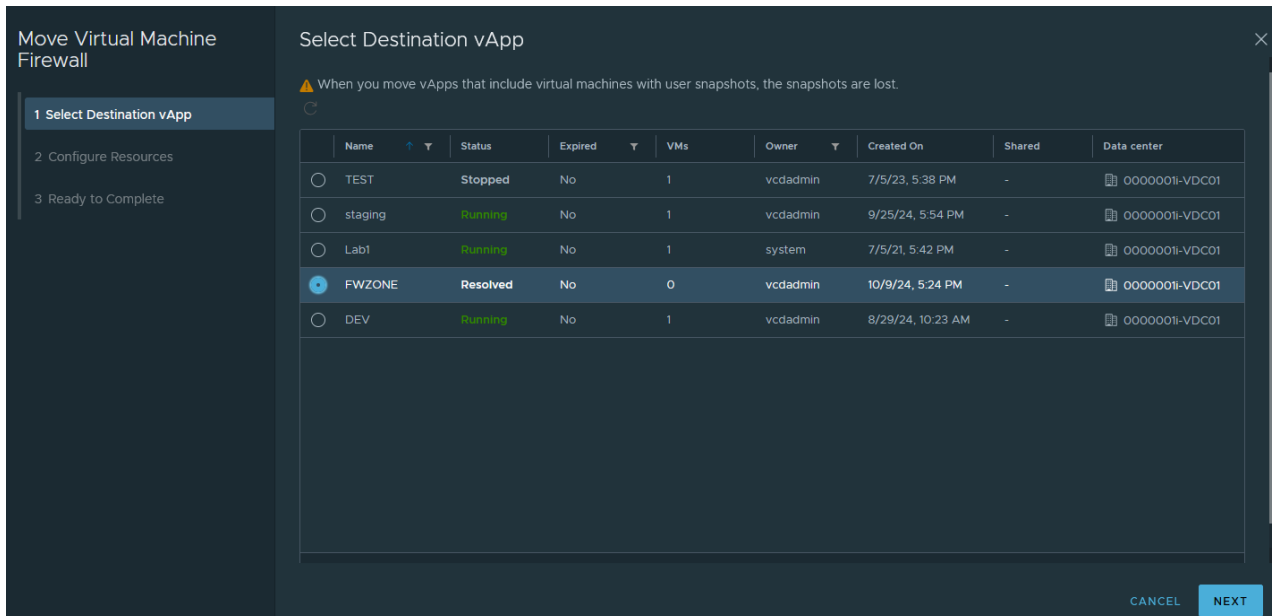
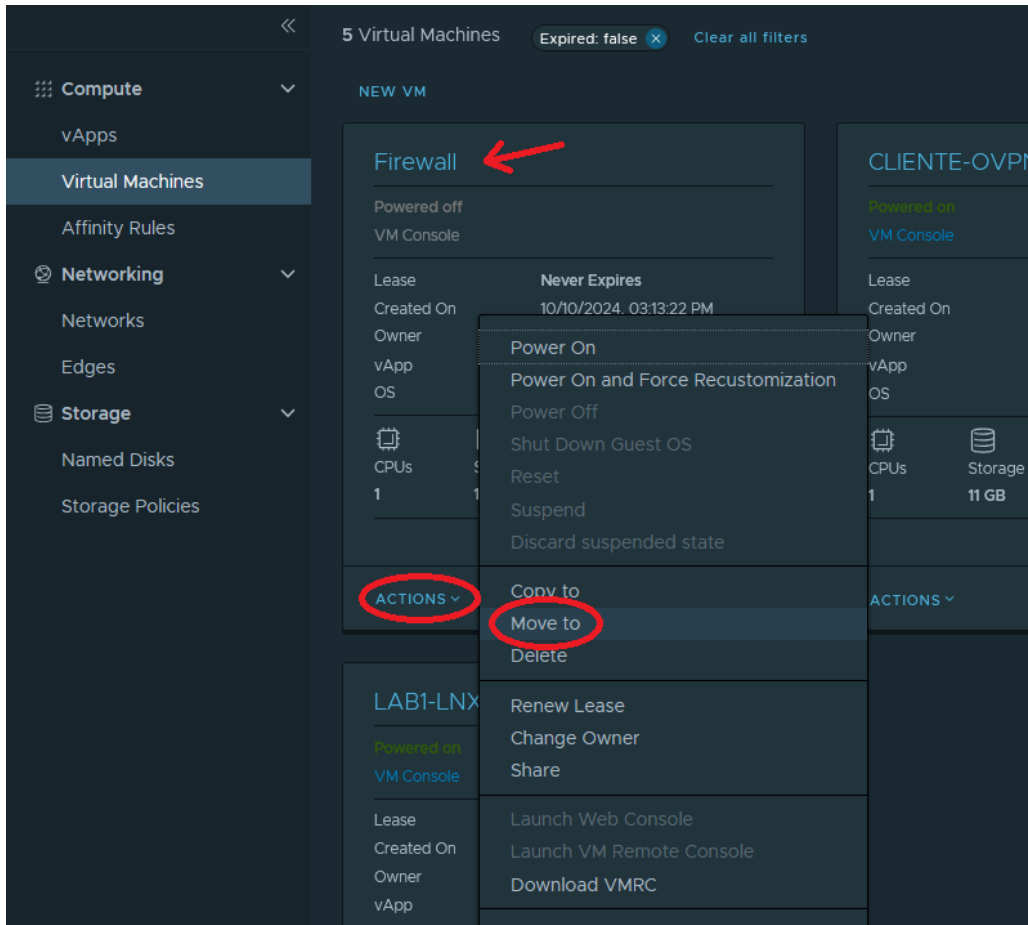
NAME	LEASE	NEVER EXPIRES	CREATED ON	OWNER	VAPP	OS	CPU	STORAGE	MEMORY	NETWORKS
Firewall	Never Expires	Never Expires	09/25/2024, 10:30:50 AM	vcdadmin	staging	FreeBSD 12 or later versions (6...	1	11 GB	1 GB	
CLIENTE-OVPN-FW01	Never Expires	Never Expires	08/29/2024, 02:03:03 PM	vcdadmin	DEV	CentOS 8 (64-bit)	2	22 GB	2 GB	
devinx1	Never Expires	Never Expires	07/19/2023, 10:18:03 AM	vcdadmin	TEST	Microsoft Windows Server 201...	2	68 GB	4 GB	
WINAPPSRV1	Never Expires	Never Expires								

Recent Tasks

Task	Status	Type	Initiator	Start Time	Completion Time
Composing Virtual Application Firewall-fb7b464d-264d-46a9-972b-9c2b4f0ba33311	Progress	vapp	vcdadmin	10/10/2024, 03:13:09 PM	

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.

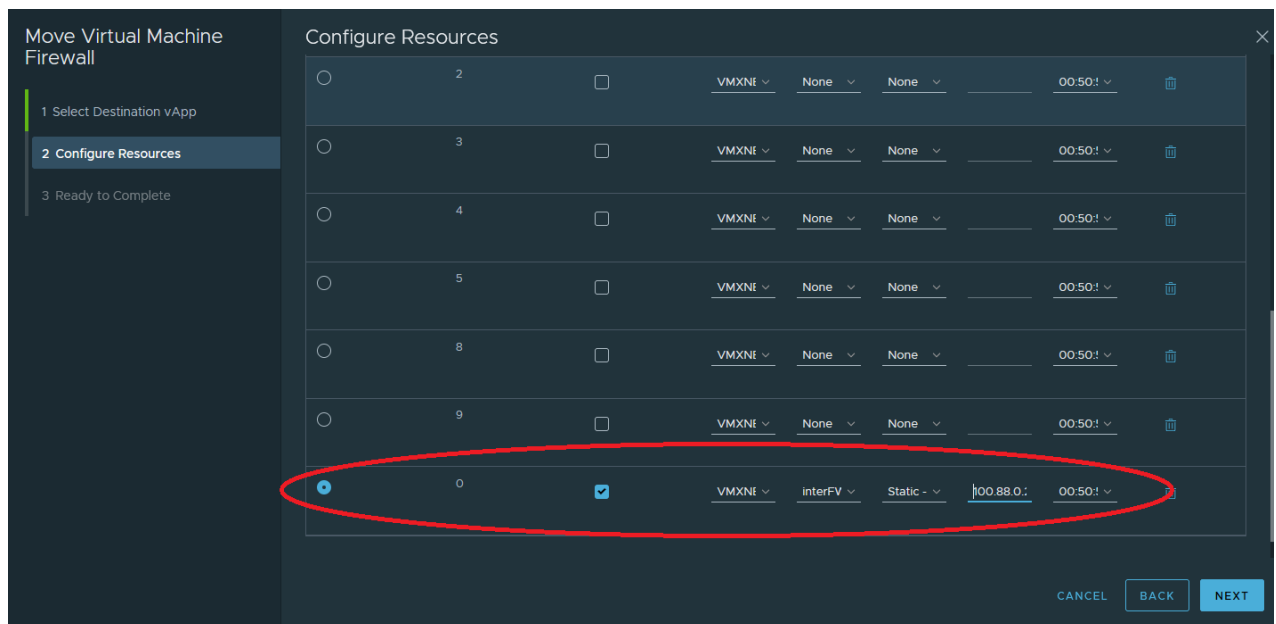
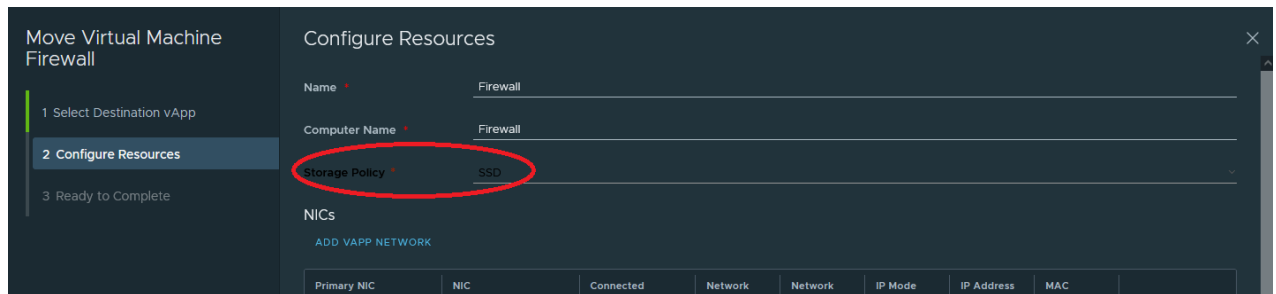
O passo seguinte é o de mover a VM para a vApp pretendida (neste exemplo, vApp FWZONE):



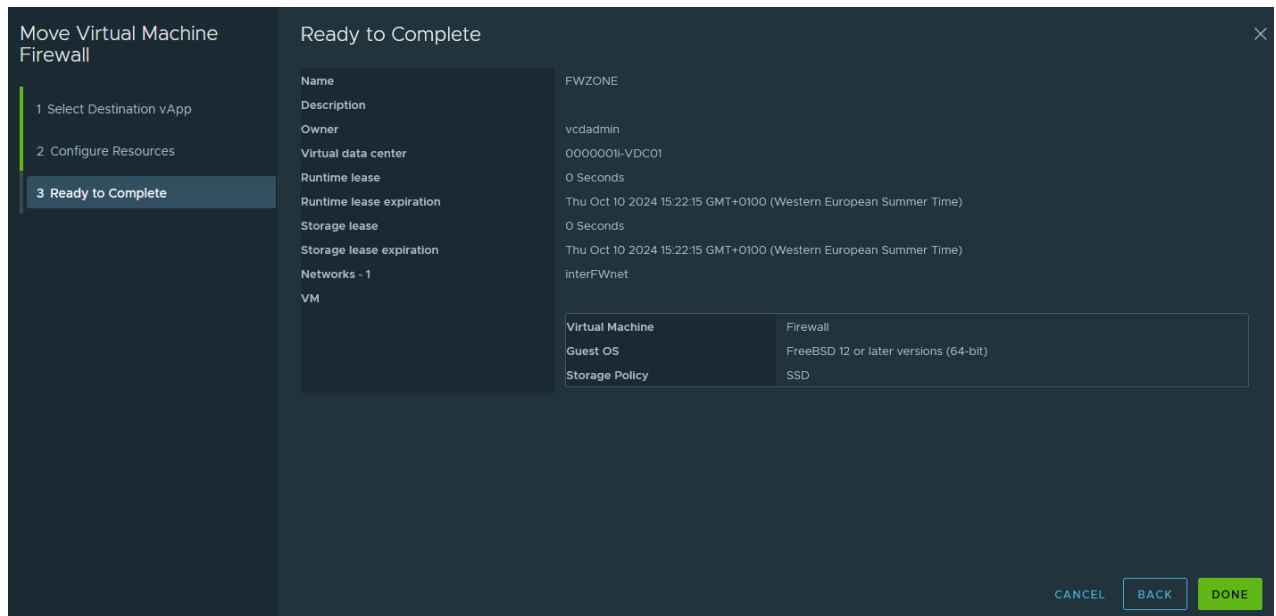
É necessário voltar a configurar alguns parâmetros apesar de já o terem sido feitos anteriormente (necessário sempre que se move de vApps). Neste caso a Storage Policy e vamos configurar aqui as interfaces de redes.

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:

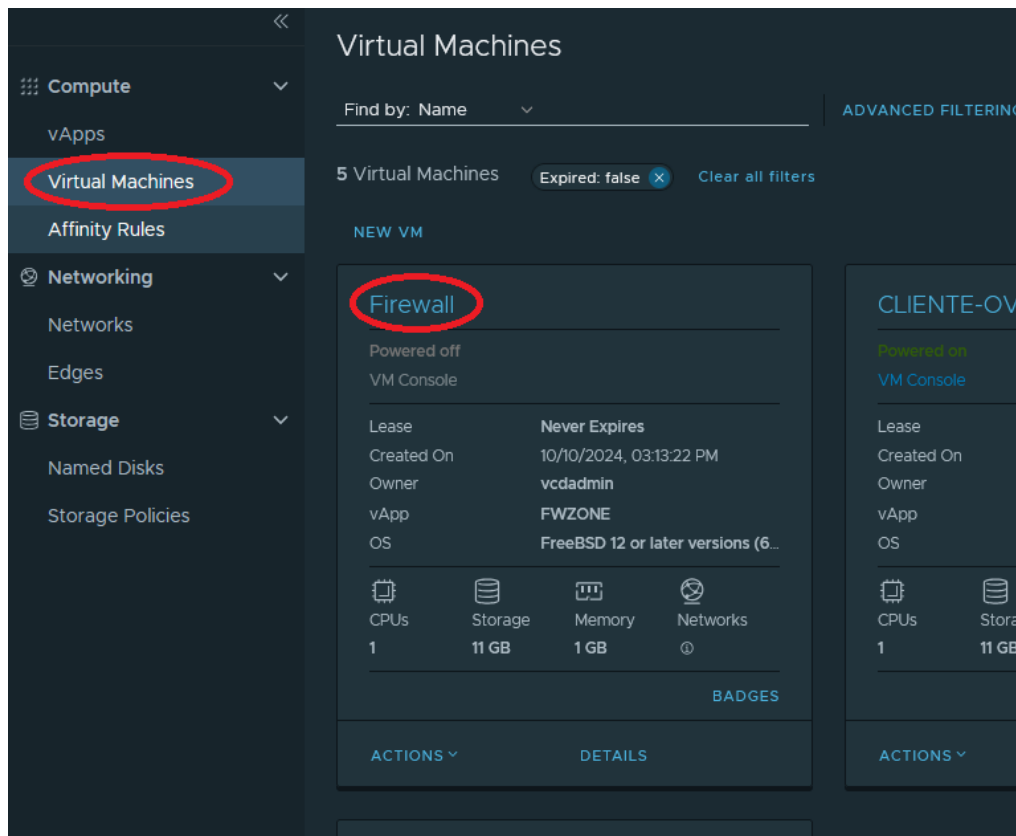


2.3 Configuração do router Edge

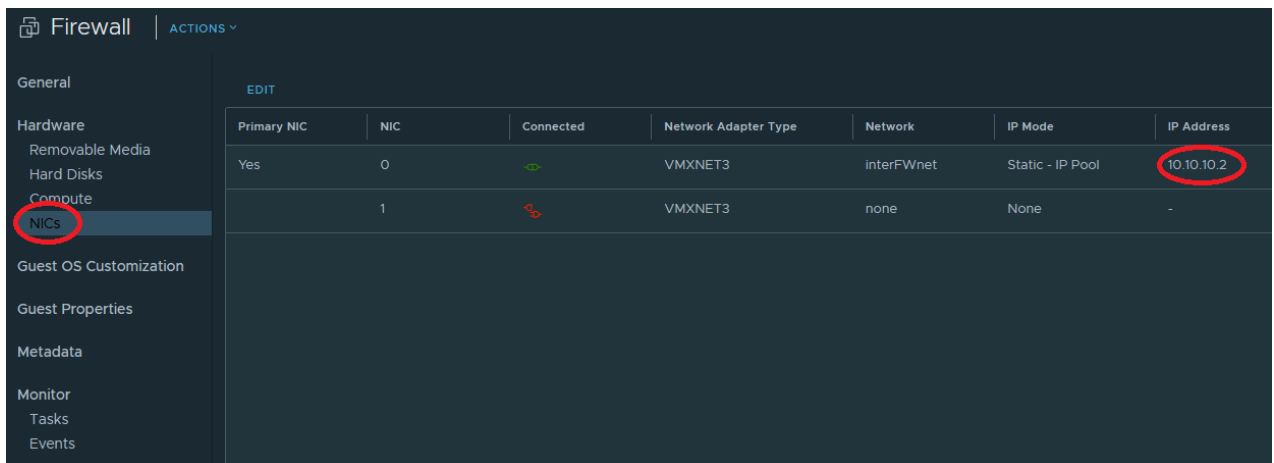
Neste ponto temos a instância de firewall instalada com conexão ao router.



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:



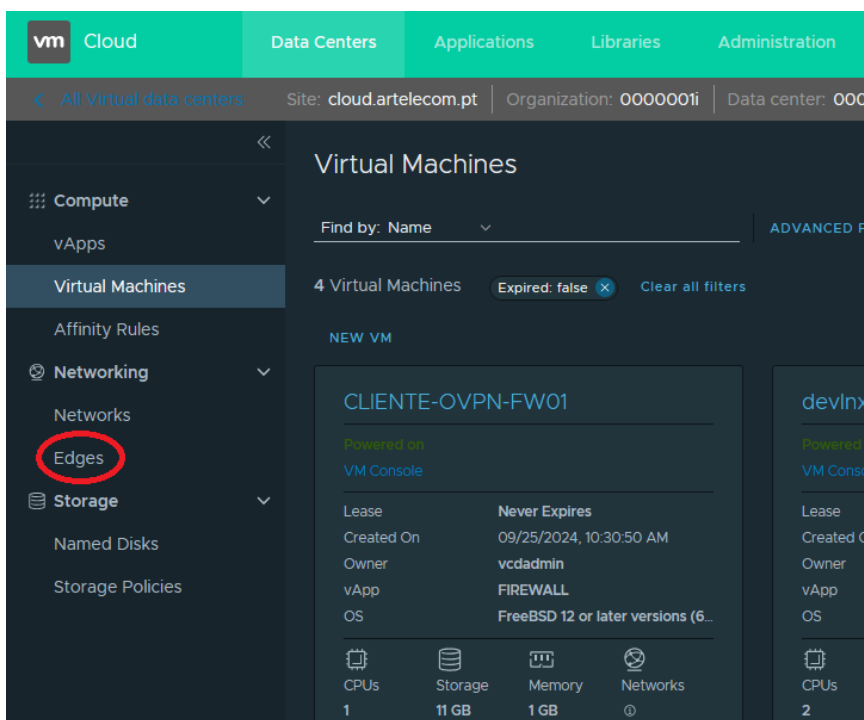
O endereço pode então ser consultado em NICs e corresponde ao IP Address da NIC 0 que se encontra ligada na rede que liga ao router, neste exemplo, interFWnet:



Primary NIC	NIC	Connected	Network Adapter Type	Network	IP Mode	IP Address
Yes	0		VMXNET3	interFWnet	Static - IP Pool	10.10.10.2
	1		VMXNET3	none	None	-

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:

Edge Gateways

Name	Status	Type	Distributed Routing
0000001i-ESG00	Normal	NSX-V	Disabled

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

All Edge Gateways > 0000001i-ESG00

0000001i-ESG00 | SERVICES

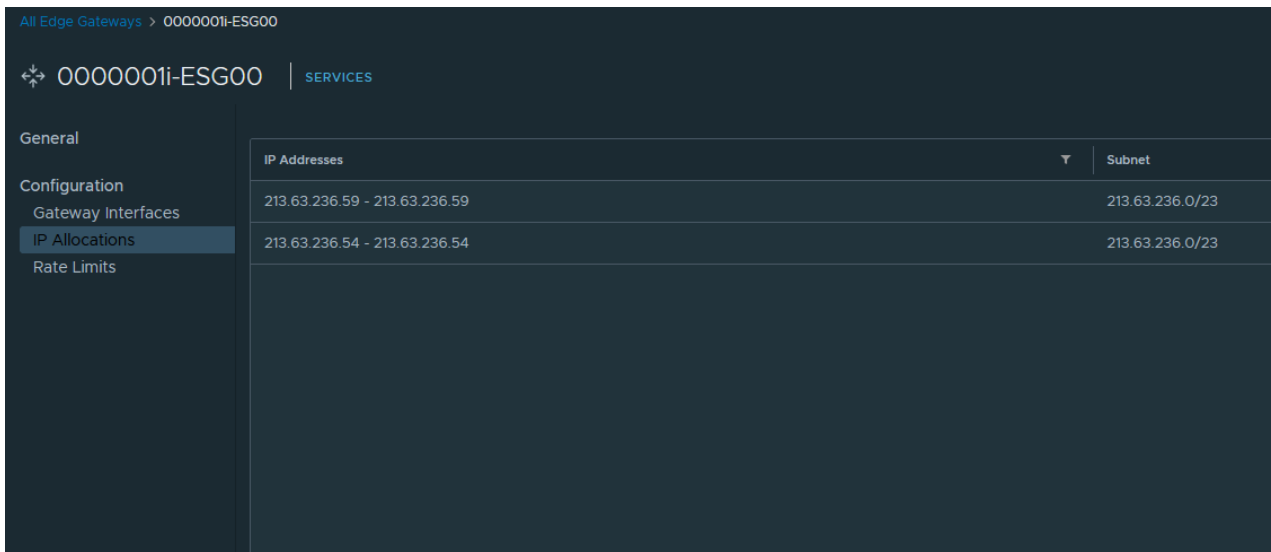
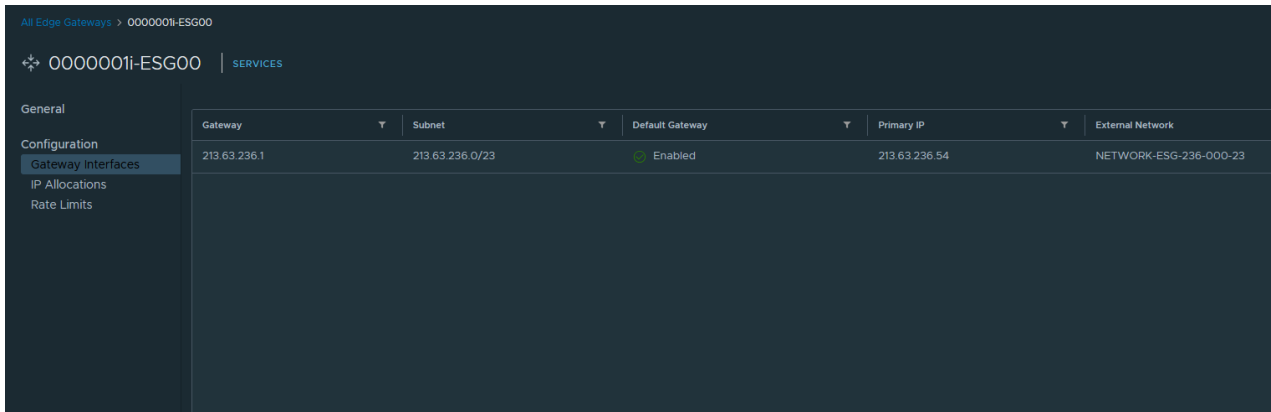
General

Configuration

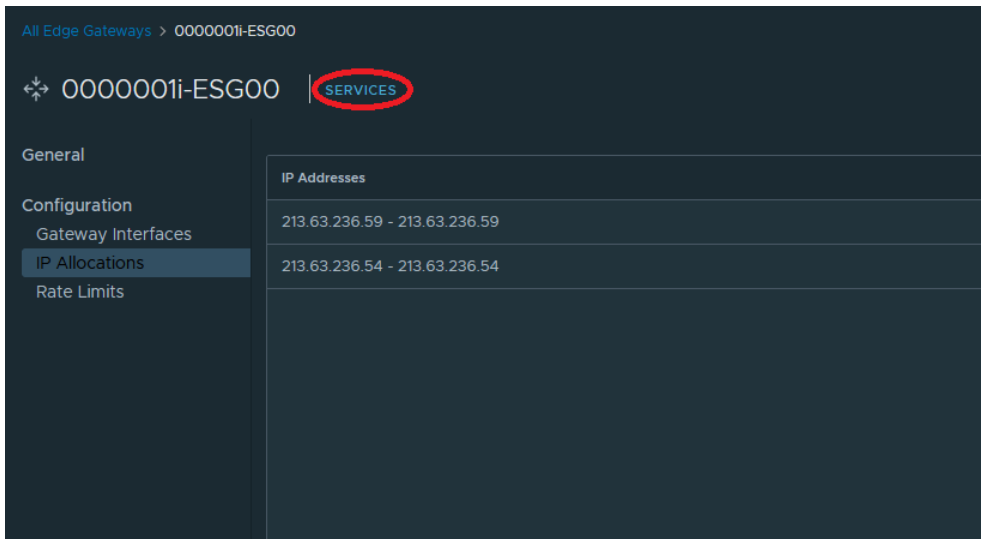
- Gateway Interfaces
- IP Allocations
- Rate Limits

EDIT

Name	0000001i-ESG00
Description	#1297705 LAB1 07072021
Status	Normal
Distributed Routing	Disabled
FIPS Mode	Disabled
Edge Gateway Configuration	Compact
High Availability	Disabled
Syslog Server Settings	-



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



Configuração de regras de firewall

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:

Edge Gateway - 0000001-ESG00

Firewall DHCP NAT Routing Load Balancer VPN SSL VPN-Plus Certificates Grouping Objects Statistics Edge Settings

Firewall Rules

Enabled

Show only user-defined rules

No.	Name	Type	Source	Destination	Service	Action	Enable logging
1	firewall	Internal High	vse	Any	Any	Accept	<input type="checkbox"/>
2	default rule for ingress traffic	Default Policy	Any	Any	Any	Accept	<input type="checkbox"/>

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).

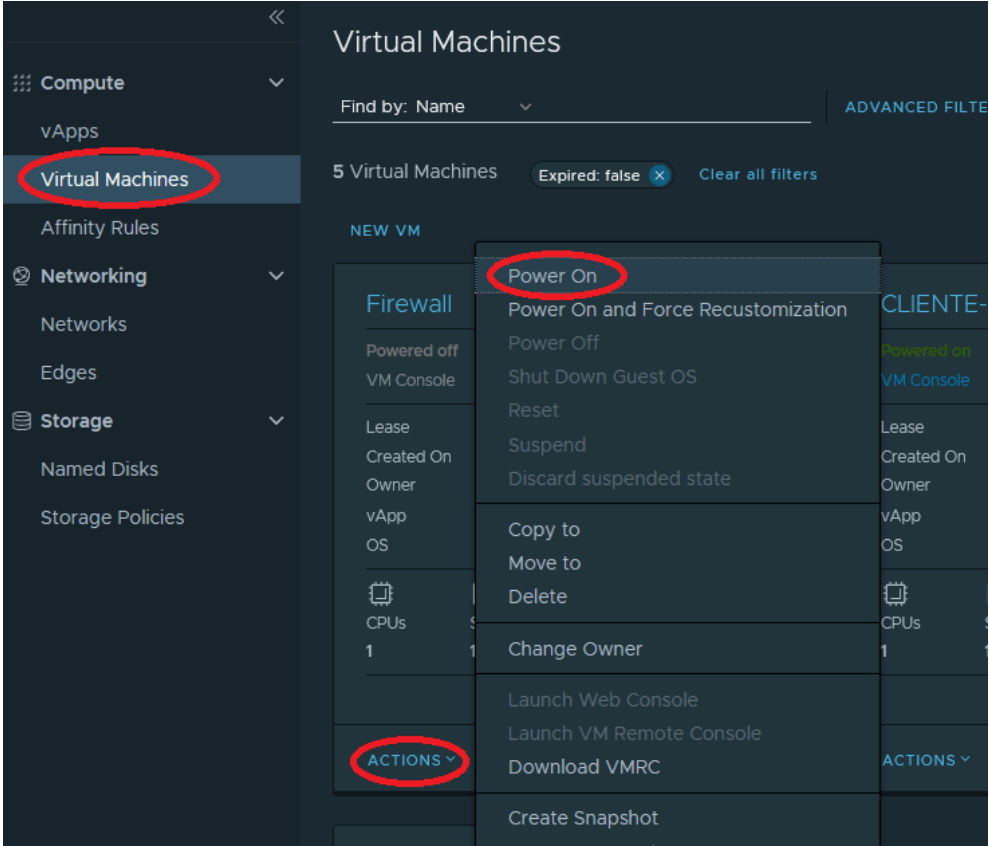
Certificados

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”:



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.

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.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **213.63.236.54**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

Go Back (Recommended)

Advanced...

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.

OPNsense

Username:

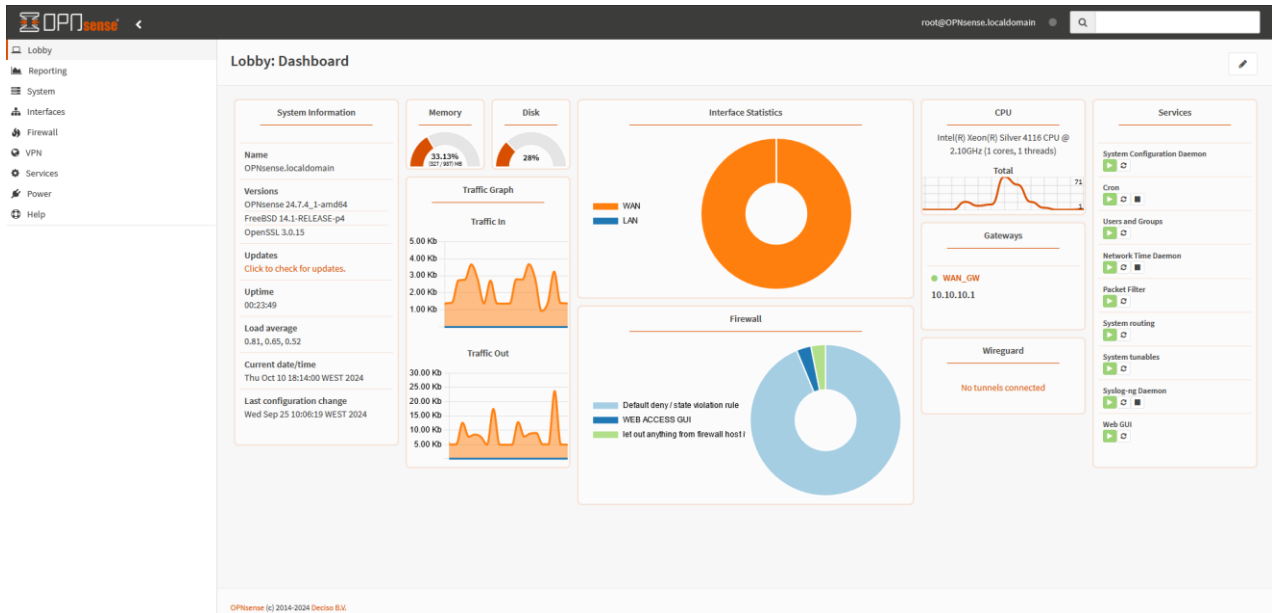
Password:

Login

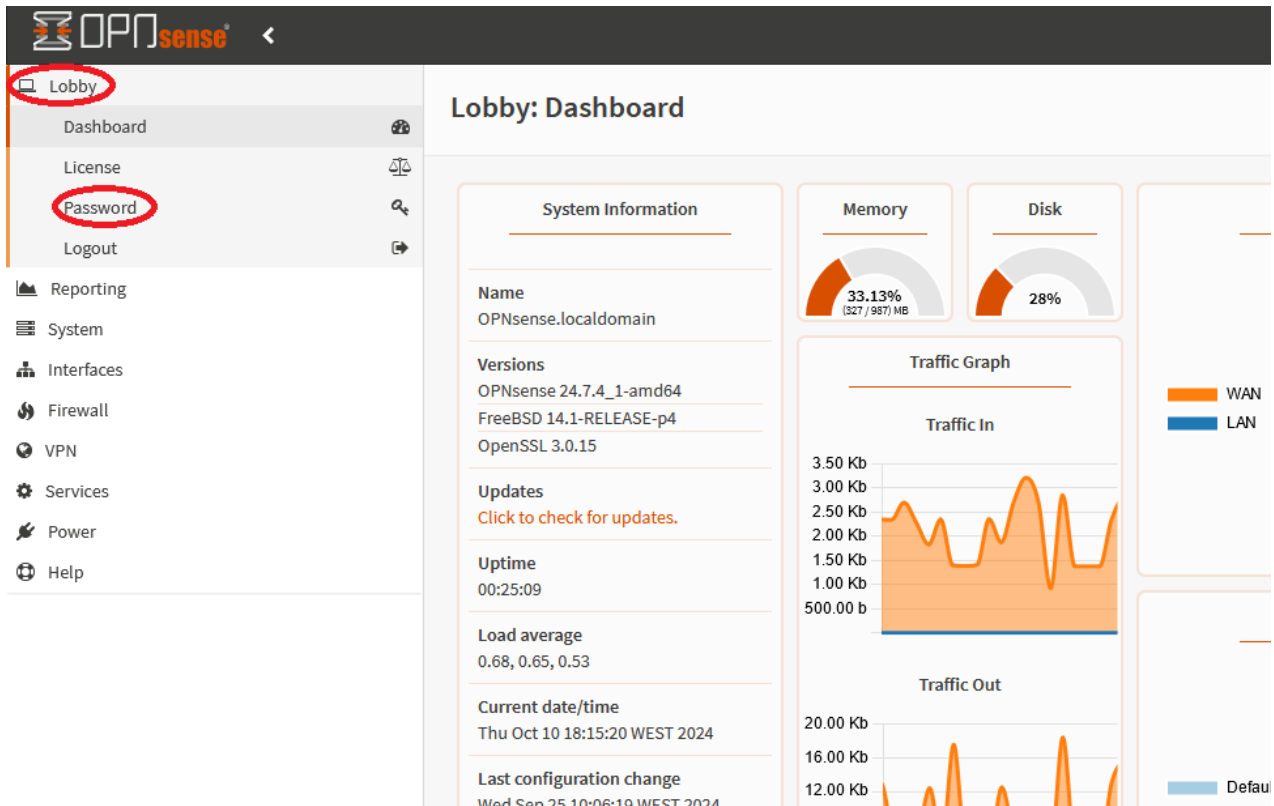
OPNsense (c) 2014-2024 Deciso B.V.

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":



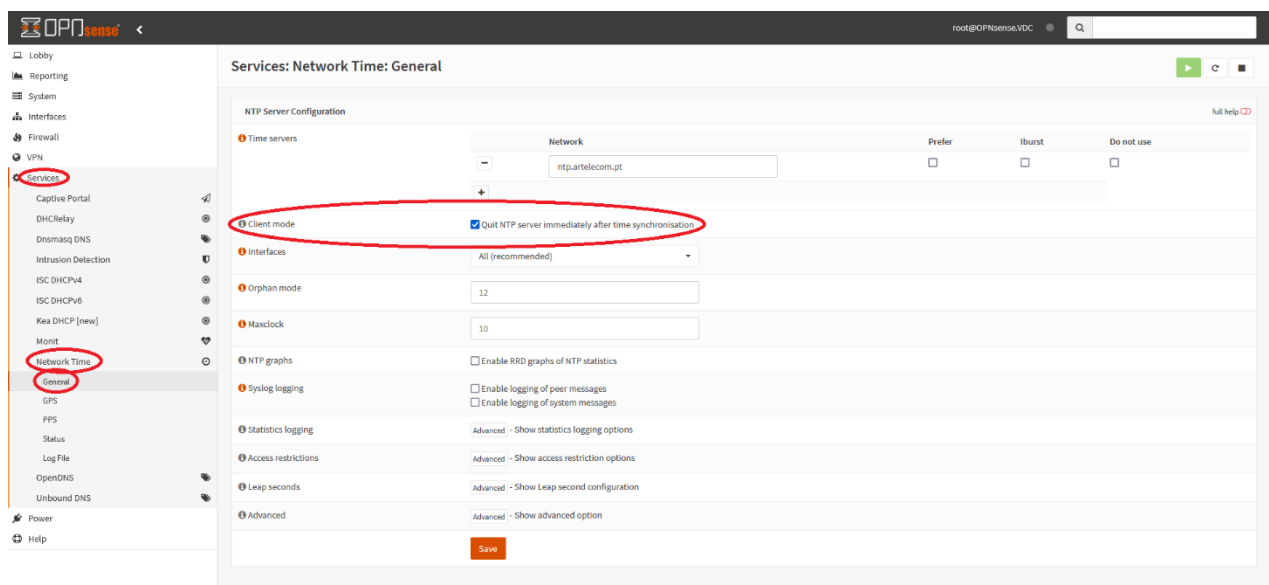
5. CONFIGURAÇÕES DE SEGURANÇA

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**:

The screenshot displays the OPNsense web interface. On the left sidebar, the 'Services' menu is expanded, and 'Unbound DNS' is selected, with its 'General' sub-tab also highlighted. The main content area shows the 'Services: Unbound DNS: General' configuration page. The 'Enable Unbound' checkbox is circled in red. Other visible settings include 'Listen Port' (53), 'Network Interfaces' (All (recommended)), 'Enable DNSSEC Support' (unchecked), 'Enable DNS64 Support' (unchecked), 'DNS64 Prefix' (64:ff9b::/96), 'Enable AAAA-only mode' (unchecked), 'Register ISC DHCP Leases' (unchecked), 'DHCP Domain Override' (empty), 'Register DHCP Static Mappings' (unchecked), 'Do not register IPv6 Link-Local addresses' (unchecked), 'Do not register system A/AAAA records' (unchecked), 'TXT Comment Support' (unchecked), 'Flush DNS Cache during reload' (unchecked), and 'Local Zone Type' (transparent). An 'Apply' button is located at the bottom of the configuration area.

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**:

Services: Net-SNMP

General | **SNMPv3 Users**

- Enable SNMP Service
- SNMP Community: !QAZ!WSXCDE#VFRS
- SNMP Location: [Empty]
- SNMP Contact: [Empty]
- Add AgentX Support
- Add Observium Support
- Layer 3 Visibility
- Display Version in OID
- Listen IPs: 192.168.100.254

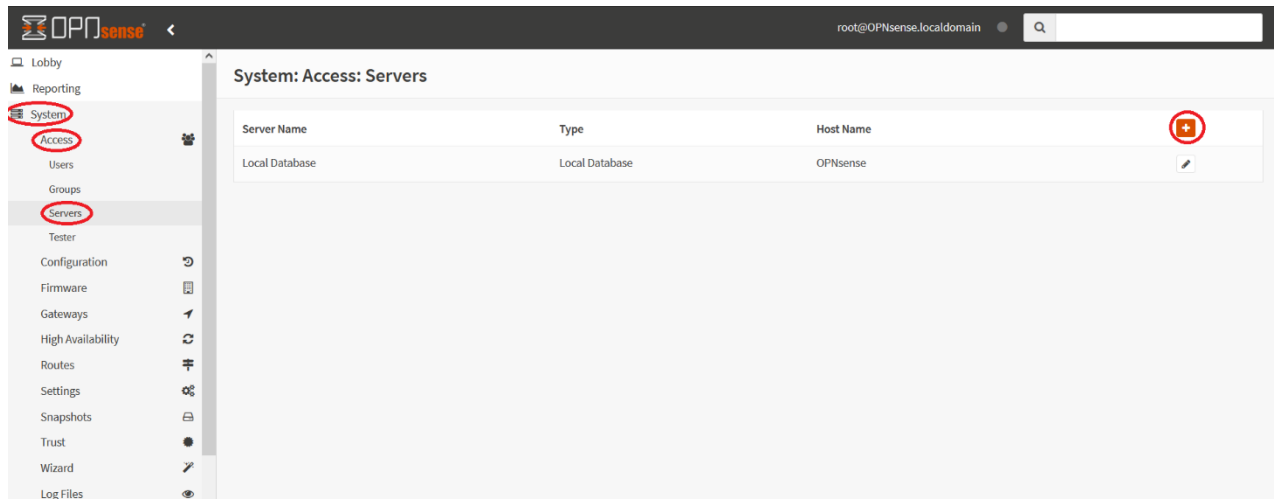
Save

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.

The screenshot shows a web interface with several sections. At the top, there is a '+' button. Below it is the 'API keys' section with a 'key' label and another '+' button. The 'OTP seed' section is highlighted with a red circle around the label. Below it, there is a checkbox labeled 'Generate new secret (160 bit)' which is also circled in red. At the bottom, there is the 'Authorized keys' section with a text area for pasting a file.

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:




User Certificates

Name	CA	Valid From
user1_cert	CA-4SSL	Fri, 25 Oct 2024 17:39:54 +0100



API keys


key



OTP seed

DNLY4GQC GENROK5RWL5YTV46OC3K7PEO

Generate new secret (160 bit)

OTP QR code 

Authorized keys

Paste an authorized keys file here.


OPNsense (c) 2014-2024 Deciso B.V.

OTP seed

DNLY4GQC GENROK5RWL5YTV46OC3K7PEO

Generate new secret (160 bit)

OTP QR code



Authorized keys

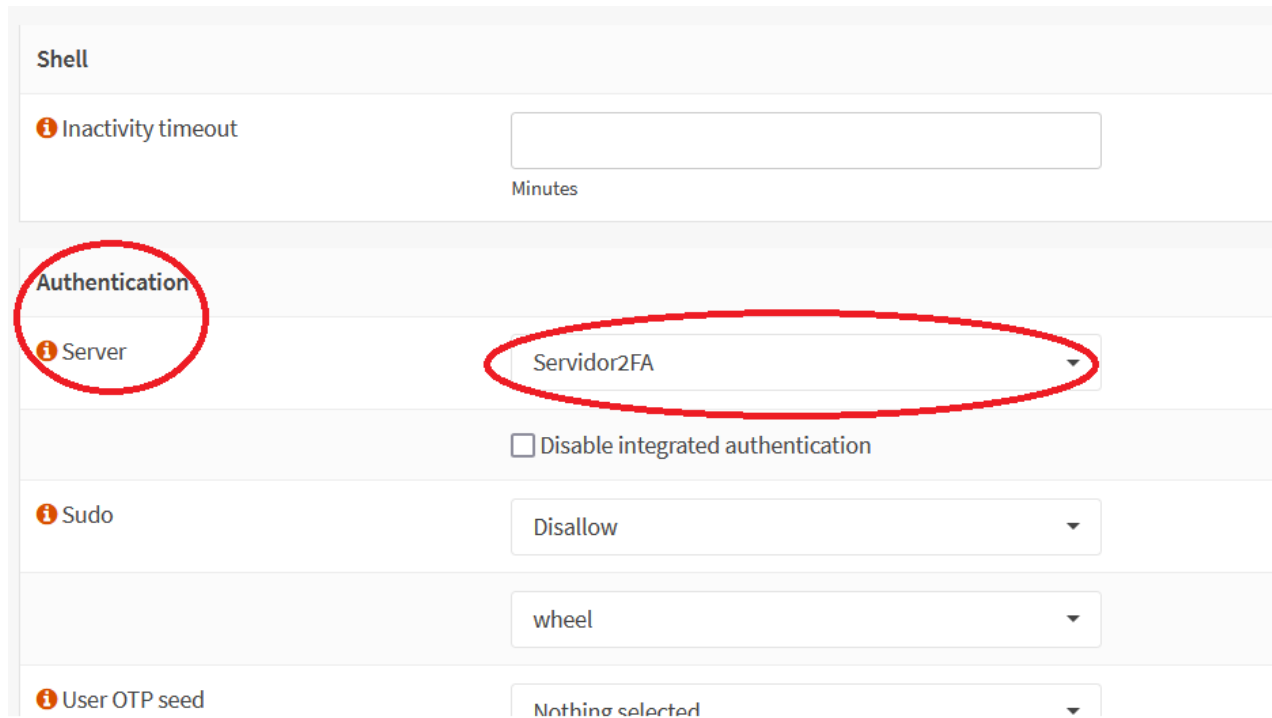
Paste an authorized keys file here.

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:



Shell

i Inactivity timeout
Minutes

Authentication

i Server

Disable integrated authentication

i Sudo

i User OTP seed



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 !

7. CONEXÃO A REDE DO VDC

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

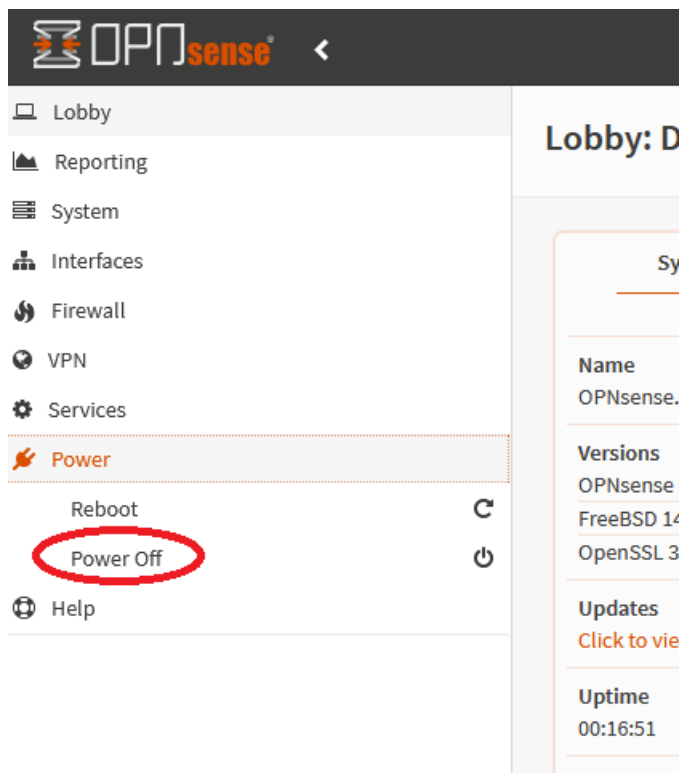
7.1 Adição de interface no virtual data center

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.

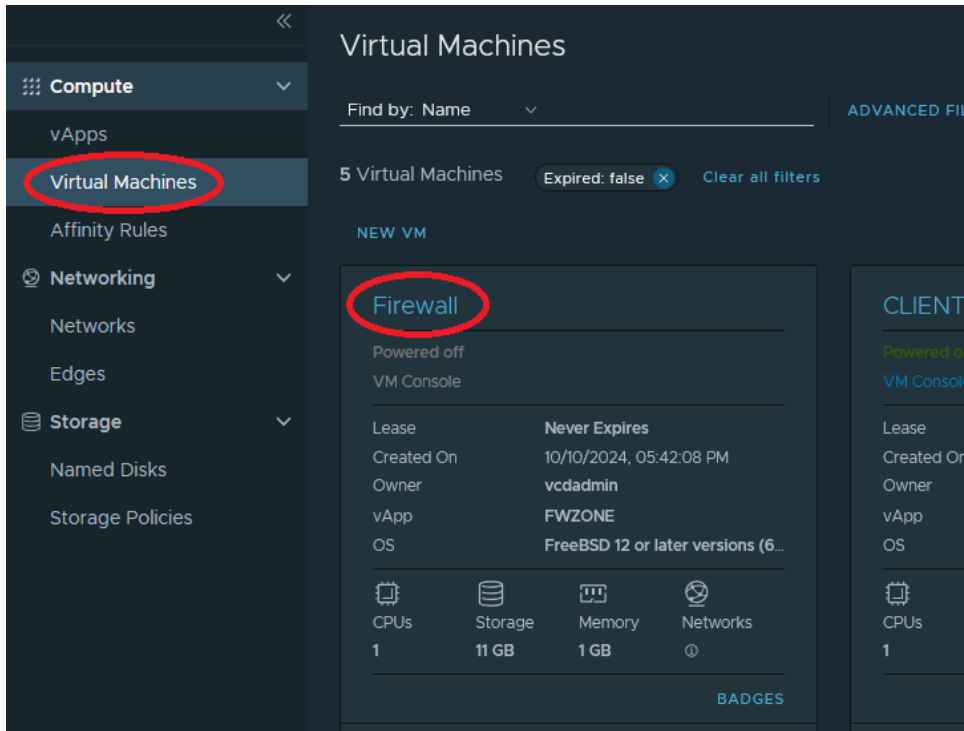


Esta operação tem de ser efetuada com a firewall em power off!

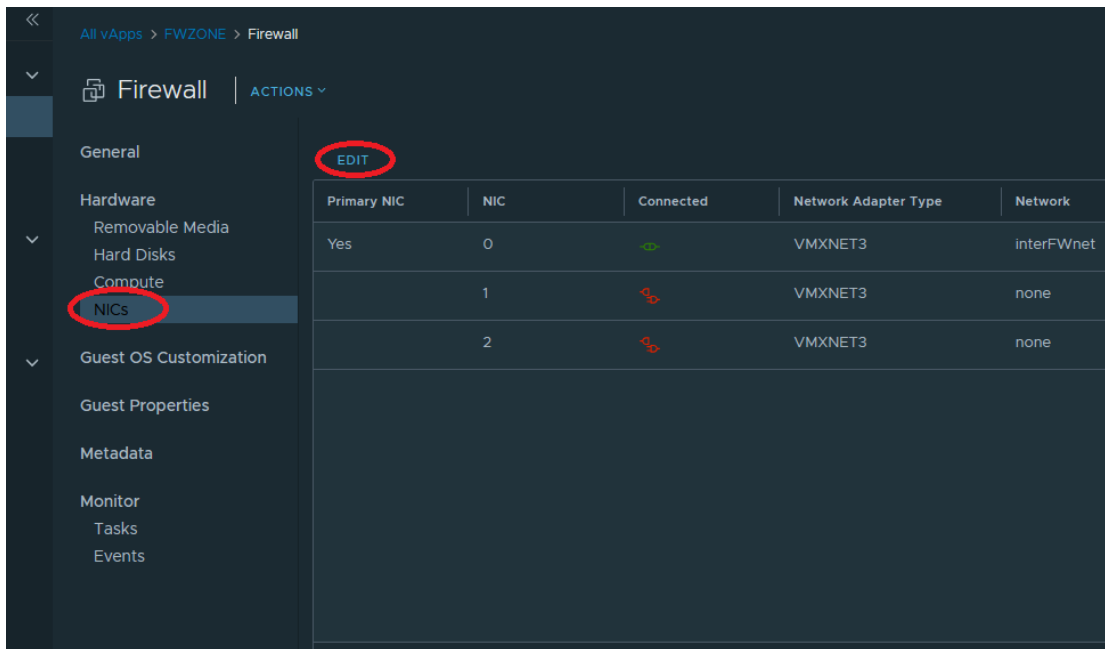
Aceder ao portal de gestão do virtual data center e garantir que a VM está desligada. Caso não esteja, desligá-la via portal de administração da mesma:



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, seleccionar a VM com a firewall



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



Edit NICs for "Firewall" ✕

ⓘ Guest customization may be required to run for the NIC changes to take effect.

NEW ADD VAPP NETWORK

NIC	Primary NIC	Connected	Adapter Type	Network	IP Mode	IP	External IP
<input type="radio"/> 0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	VMXNET3	interFWnet	Static - Manual	10.10.10.2	-
<input type="radio"/> 1	<input type="checkbox"/>	<input type="checkbox"/>	VMXNET3	None	None	192.168.100.254	-
<input type="radio"/> 2	<input type="checkbox"/>	<input type="checkbox"/>	VMXNET3	None	None		-

3 NIC(s)

DISCARD SAVE

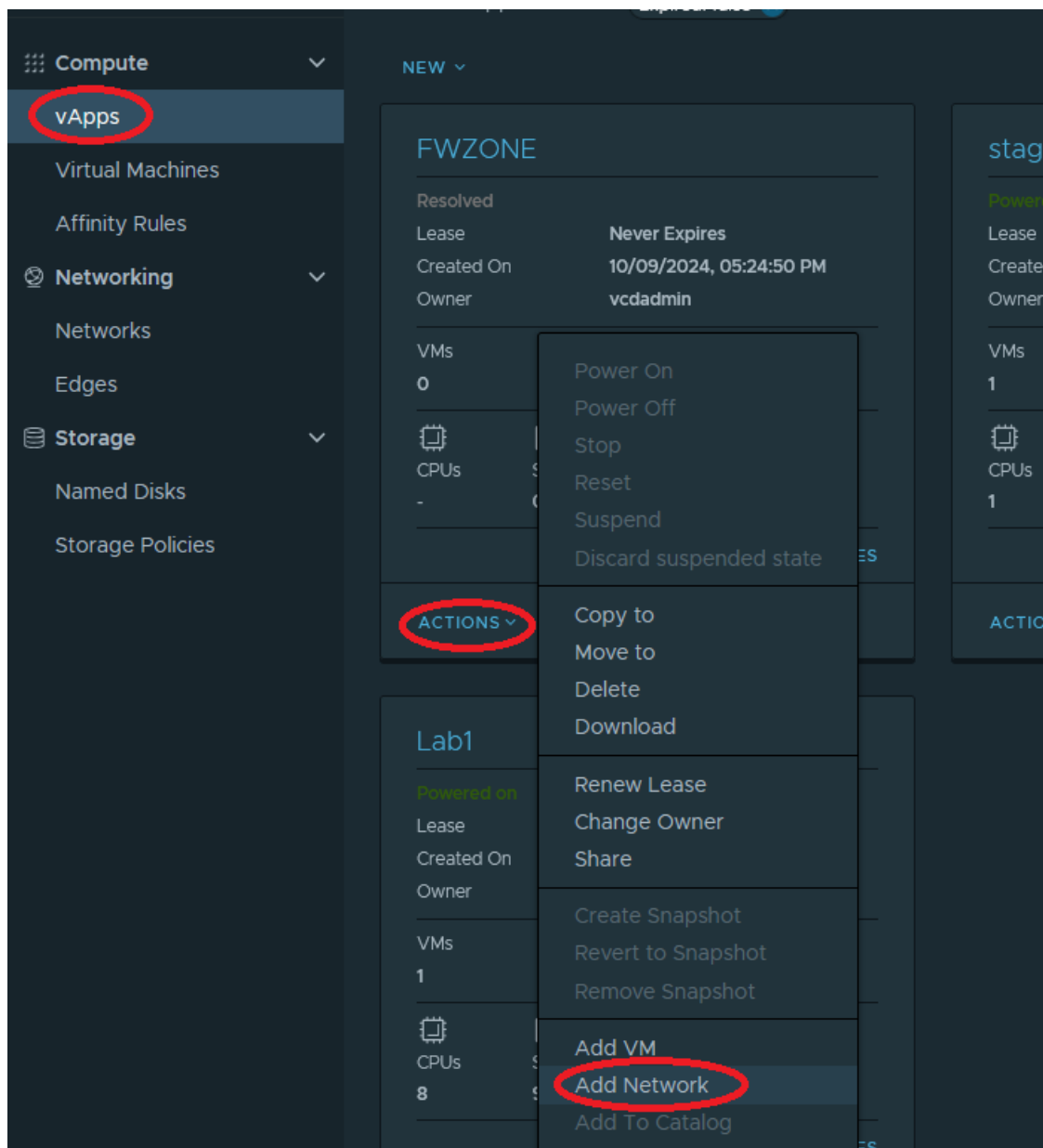


É possível adicionar NICs no vCloud com a máquina ligada mas a firewall ficará num estado corrompido. Para apagar interfaces no vCloud é necessário fazer primeiro o shutdown/power off.

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":



Selecionar opção "OrgVDC Network"



e escolher a rede pretendida:

atli Add Network to FWZONE X

Type OrgVDC Network vApp Network

Name	Status	Organization VDC	Gateway CIDR	Network Type	Connected To	IP Pool Consumed	Shared	Route Advertised
<input checked="" type="radio"/> INTERNAL-LAB1	●	0000001i-VDC...	192.168.100.254/24	Routed	-	<div style="width: 73%;"><div style="width: 73%;"></div></div> 73%		-
<input type="radio"/> SERVICES	●	0000001i-VDC...	100.96.254.254/16	Direct	NETWORK-SYS-BL...	<div style="width: 6%;"><div style="width: 6%;"></div></div> 6%		-
<input type="radio"/> TEST_NETWO...	●	0000001i-VDC...	192.168.200.254/24	Routed	-	<div style="width: 6%;"><div style="width: 6%;"></div></div> 6%		-
<input type="radio"/> adsas	●	0000001i-VDC...	192.168.2.1/24	Routed	-	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%		-

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".

Networks

NEW DELETE

Name	Status	Organization VDC
<input checked="" type="radio"/> INTERNAL-LAB1	●	0000001i-VDC01
<input type="radio"/> SERVICES	●	0000001i-VDC01
<input type="radio"/> TEST_NETWORK	●	0000001i-VDC01
<input type="radio"/> adsas	●	0000001i-VDC01
<input type="radio"/> interFWnet	●	0000001i-VDC01
<input type="radio"/> stagenet	●	0000001i-VDC01

INTERNAL-LAB1 DELETE

General

IP Management

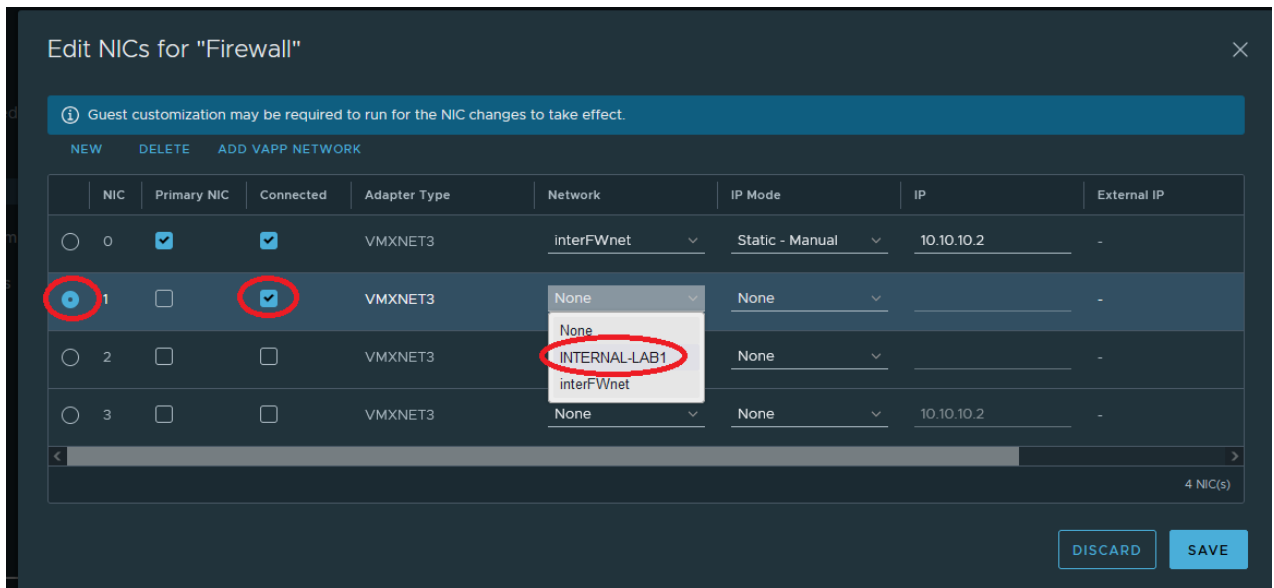
Static IP Pools

DNS

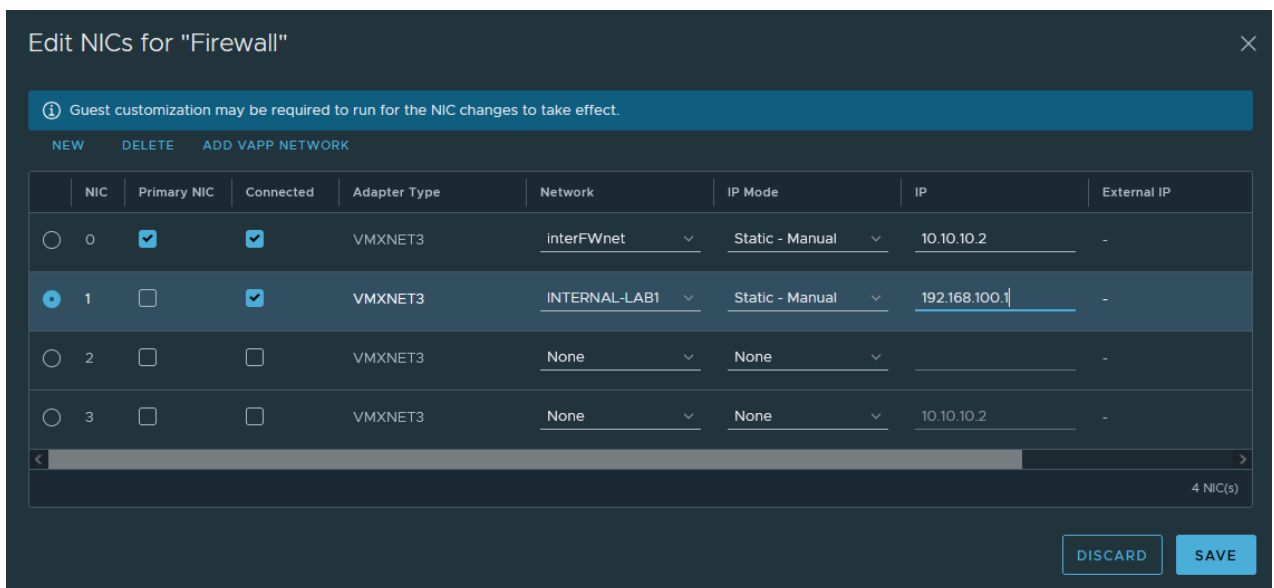
IP Usage

IP Address	Deployed	VM
192.168.100.101	<input checked="" type="checkbox"/>	LAB1-LNXSRV02
192.168.100.105	<input checked="" type="checkbox"/>	devlnx1
192.168.100.253	<input checked="" type="checkbox"/>	CLIENTE-OVPN-FW01
192.168.100.254	<input checked="" type="checkbox"/>	NSX Edge

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



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":

OPNsense

Lobby: Dashboard

System Information

Name
OPNsense.localdomain

Versions
OPNsense 24.7.4_1-amd64
FreeBSD 14.1-RELEASE-p4
OpenSSL 3.0.15

Updates
[Click to view pending updates.](#)

Uptime
00:01:03

Load average
2.39, 0.81, 0.31

Current date/time
Fri Oct 18 15:22:35 WEST 2024

Last configuration change
Fri Oct 18 13:38:50 WEST 2024

Memory
34.149 (337 / 987)

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

Interfaces: Assignments

Interface	Identifier	Device
[LAN]	lan	vmx5 (00:50:56:01:3d:81)
[WAN]	wan	vmx2 (00:50:56:01:3d:80)

[Save](#)

+ Assign a new interface

Device: vmx0 (00:50:56:01:3d:83)

Description:

- vmx0 (00:50:56:01:3d:83)
- vmx1 (00:50:56:01:3d:84)
- vmx3 (00:50:56:01:3d:85)
- vmx4 (00:50:56:01:3d:88)
- vmx6 (00:50:56:01:3d:86)
- vmx7 (00:50:56:01:3d:89)
- vmx8 (00:50:56:01:3d:82)
- vmx9 (00:50:56:01:3d:87)

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

The screenshot shows the OpenSense web interface. On the left, a sidebar menu has 'Interfaces' selected, and 'internal_lab' is highlighted with a red circle. The main content area is titled 'Interfaces: [internal_lab]' and shows the 'Basic configuration' section. In this section, the 'Enable Interface' checkbox is also highlighted with a red circle. Other configuration options include 'Lock', 'Identifier' (set to 'opt1'), 'Device' (set to 'vmx2'), and 'Description' (set to 'internal_lab'). At the bottom of the configuration area, there are 'Save' and 'Cancel' buttons.

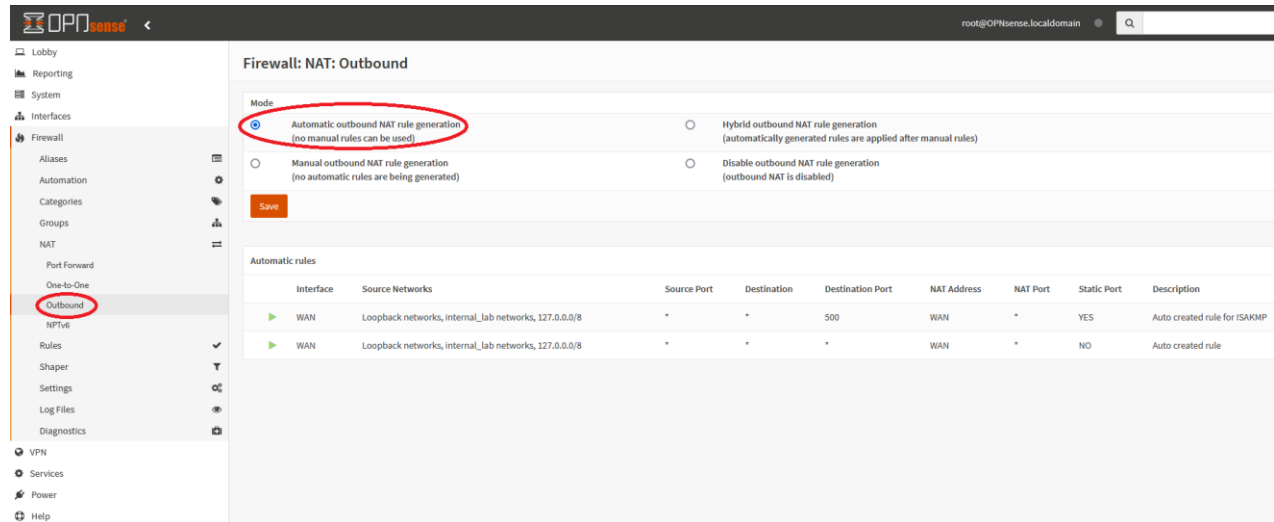
O passo seguinte é o da configuração das regras e serviços de firewall.

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

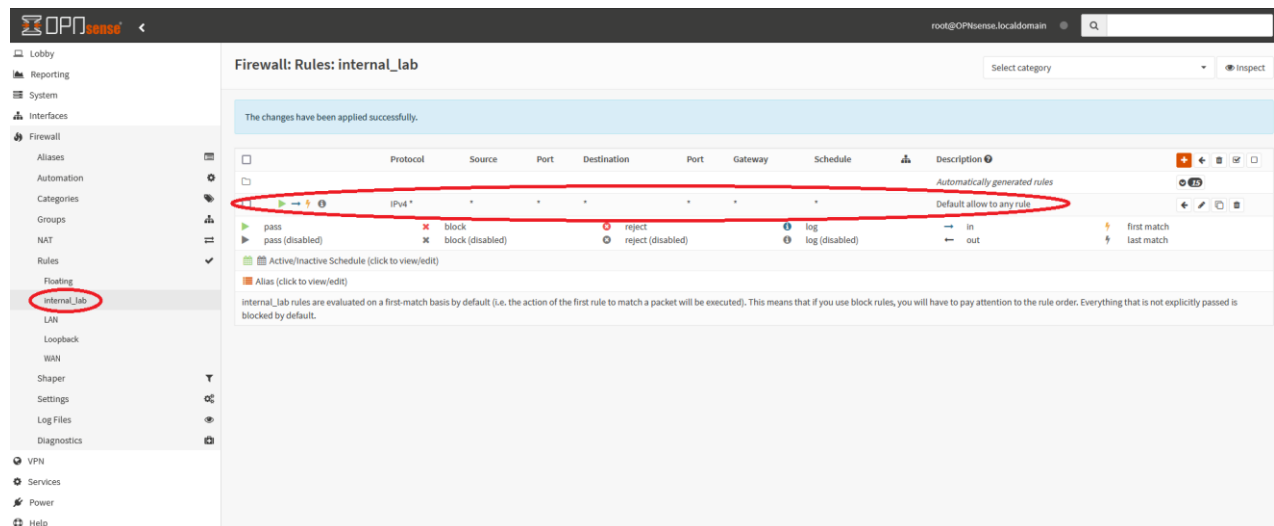
As regras SNAT são criadas automaticamente por defeito na configuração default da OPNsense. Isto pode ser visualizado indo ao menu Firewall -> NAT -> Outbound:



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:



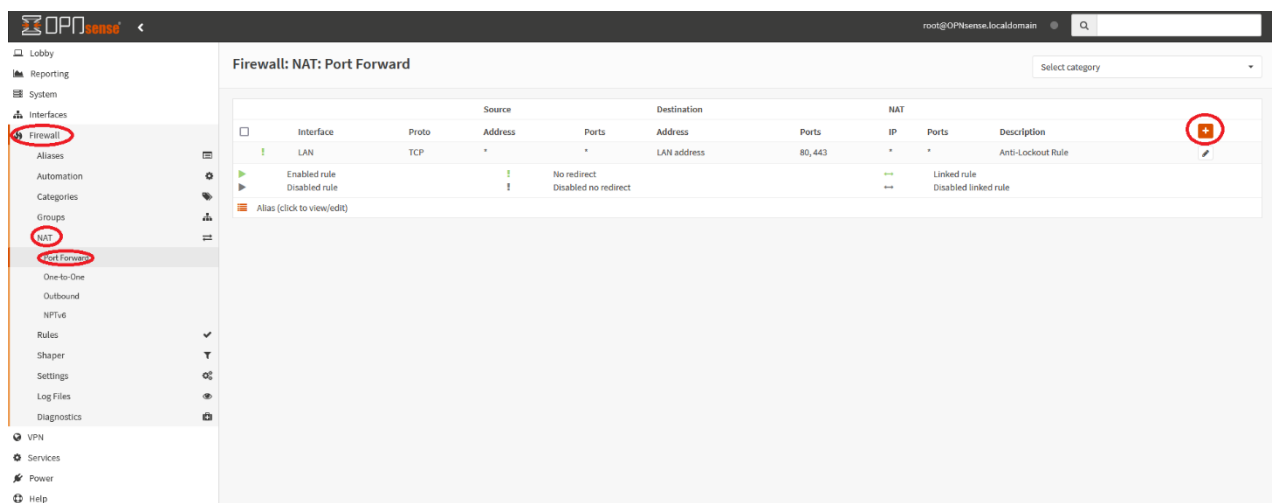
9. PORT FORWARD – DNAT

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:

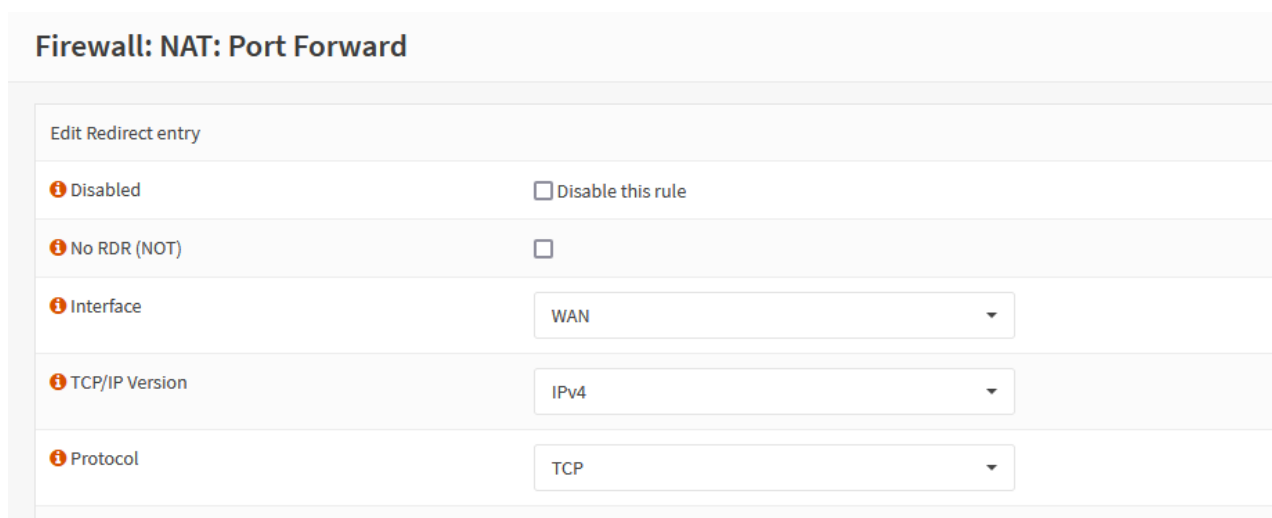
- Pretende-se criar um redireccionamento para a porta RDP de um servidor Windows
- Esse servidor tem o endereço IP interno 192.168.100.107
- A porta RDP é a 3389, no entanto, recomenda-se que a porta pública seja diferente, por exemplo, 10010

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).

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:

Firewall: NAT: Port Forward

Select category

	Source		Destination		NAT			Description	
<input type="checkbox"/>	Interface	Proto	Address	Ports	Address	Ports	IP	Ports	
<input type="checkbox"/>	LAN	TCP	*	*	LAN address	80, 443	*	*	Anti-Lockout Rule
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	10010	192.168.100.107	3389 (MS RDP)	
<input type="checkbox"/>	Enabled rule			<input type="checkbox"/>	No redirect			<input type="checkbox"/>	Linked rule
<input type="checkbox"/>	Disabled rule			<input type="checkbox"/>	Disabled no redirect			<input type="checkbox"/>	Disabled linked rule

Alias (click to view/edit)

Firewall: Rules: WAN

Select category

Inspect

<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
<i>Automatically generated rules</i>									
<input type="checkbox"/>	IPV4 TCP	GESTAO_AR	*	10.10.10.2	443 (HTTPS)	*	*	WEB ACCESS GUI	
<input type="checkbox"/>	IPV4 TCP	*	*	192.168.100.107	3389 (MS RDP)	*	*		
<input type="checkbox"/>	pass	<input type="checkbox"/>	block	<input type="checkbox"/>	reject	<input type="checkbox"/>	log	<input type="checkbox"/>	in
<input type="checkbox"/>	pass (disabled)	<input type="checkbox"/>	block (disabled)	<input type="checkbox"/>	reject (disabled)	<input type="checkbox"/>	log (disabled)	<input type="checkbox"/>	out

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

WAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

10. OPENVPN ROAD WARRIOR

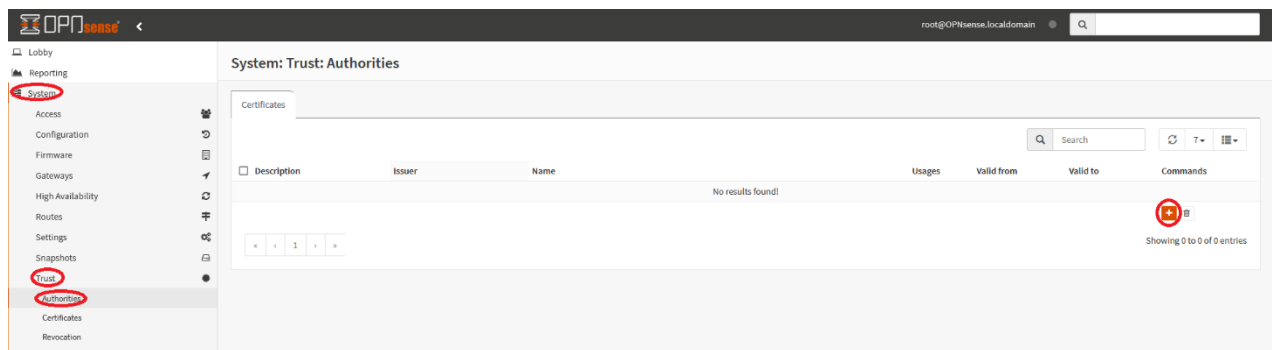
Uma VPN Road Warrior é uma VPN criada diretamente entre um dispositivo (normalmente PC ou dispositivo portátil) e uma rede, e é usada quando utilizadores individuais necessitam acesso a recursos de uma determinada rede.

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:

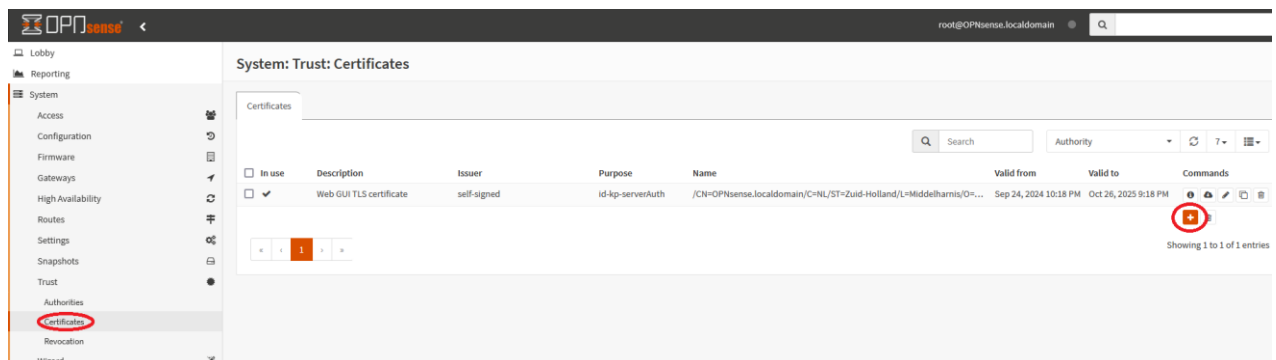


- Por defeito será criada uma autoridade do tipo *Internal*.
- Podemos alterar o tipo de chave e a duração, mas neste exemplo vamos deixar por defeito.
- Preencher os outros campos conforme pretendido

Method	Create an internal Certificate Authority
Description	CA-4SSL
Key	
Key type	RSA-2048
Digest Algorithm	SHA256
Issuer	self-signed
Lifetime (days)	825
General	
Country Code	Portugal
State or Province	
City	
Organization	
Organizational Unit	
Email Address	
Common Name	
OCSP uri	

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

Method	Create an internal Certificate
Description	C-4SSL
Key	
Type	Server Certificate
Private key location	Save on this firewall
Key type	RSA-2048
Digest Algorithm	SHA256
Issuer	CA-4SSL
Lifetime (days)	397
General	
Country Code	Portugal
State or Province	
City	
Organization	
Organizational Unit	
Email Address	

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, seleccionando a opção **"Click to create a user certificate"**.

System: Access: Users

Defined by	USER
i Disabled	<input type="checkbox"/>
i Username	<input type="text" value="user1"/>
i Password	<input type="password" value="....."/> <input type="password" value="....."/> (confirmation)
	<input type="checkbox"/> Generate a scrambled password to prevent local database logins for this user.
i Full name	<input type="text"/>
i E-Mail	<input type="text"/>
i Comment	<input type="text"/>
i Preferred landing page	<input type="text"/>
i Language	Default
i Login shell	<input type="text" value="/usr/sbin/nologin"/>
i Expiration date	<input type="text"/>

Group Memberships

Not Member Of	Member Of
<input type="text" value="admins"/>	<input type="text"/>

Certificate Click to create a user certificate.

OTP seed
 Generate new secret (100 bit)

Authorized keys

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)

Edit Certificate

ⓘ Method

ⓘ Description

▼ Key

ⓘ Type

ⓘ Private key location

ⓘ Key type

ⓘ Digest Algorithm

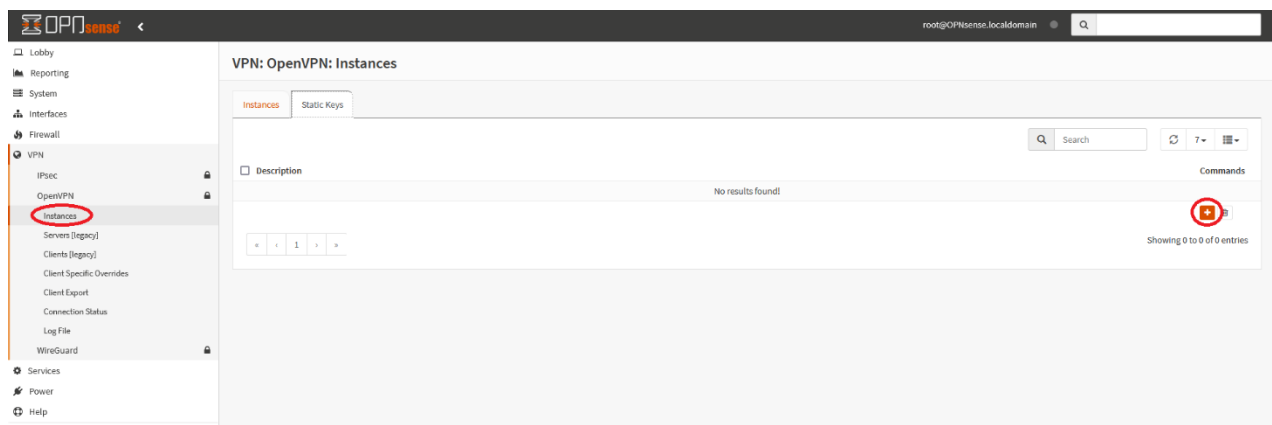
ⓘ Issuer


ⓘ Lifetime (days)

▼ General

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:

Edit Static Key ✕

[full help](#)

Description

Mode

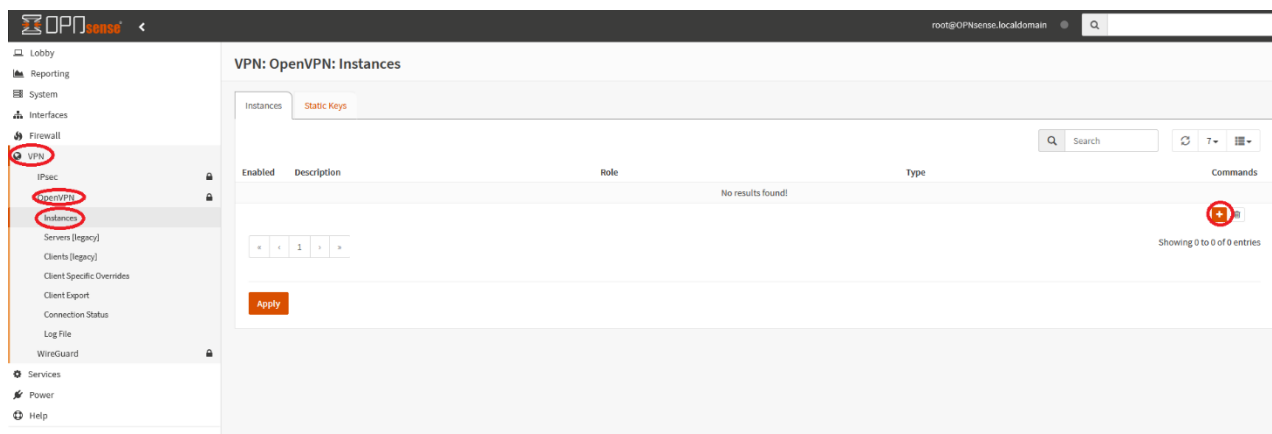
Static Key

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
70c635588e162708ccca2a6683e266e9
```

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

- 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":

Firewall: Rules: OpenVPN

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
IPv4 *	OpenVPN net	*	*	*	*	*	Automatically generated rules
pass	block		reject		log		in
pass (disabled)	block (disabled)		reject (disabled)		log (disabled)		out

OpenVPN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Firewall: Rules: OpenVPN

Edit Firewall rule

Action: Pass

Disabled: Disable this rule

Quick: Apply the action immediately on match.

Interface: OpenVPN

Direction: in

TCP/IP Version: IPv4

Protocol: any

Source / Invert: Use this option to invert the sense of the match.

Source: any

Source: Advanced

Destination / Invert: Use this option to invert the sense of the match.

Destination: any

Destination port range: from: any to: any

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":

Firewall: Rules: WAN

Edit Firewall rule

Action Pass

Disabled Disable this rule

Quick Apply the action immediately on match.

Interface WAN

Direction in

TCP/IP Version IPv4

Protocol UDP

Source / Invert Use this option to invert the sense of the match.

Source any

Source Advanced

Destination / Invert Use this option to invert the sense of the match.

Destination WAN address

Destination port range **from:** OpenVPN **to:** OpenVPN

Firewall: Rules: WAN

Select category Inspect

The changes have been applied successfully.

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
Automatically generated rules									
<input type="checkbox"/>	IPv4 TCP	GESTAO_AR	*	10.10.10.2	443 (HTTPS)	*	*	WEB ACCESS GUI	<input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	192.168.100.107	3389 (MS RDP)	*	*		<input type="checkbox"/>
<input type="checkbox"/>	IPv4 TCP	*	*	192.168.100.101	22 (SSH)	*	*		<input type="checkbox"/>
<input type="checkbox"/>	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	*		<input type="checkbox"/>

pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled) in out first match last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

WAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

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)

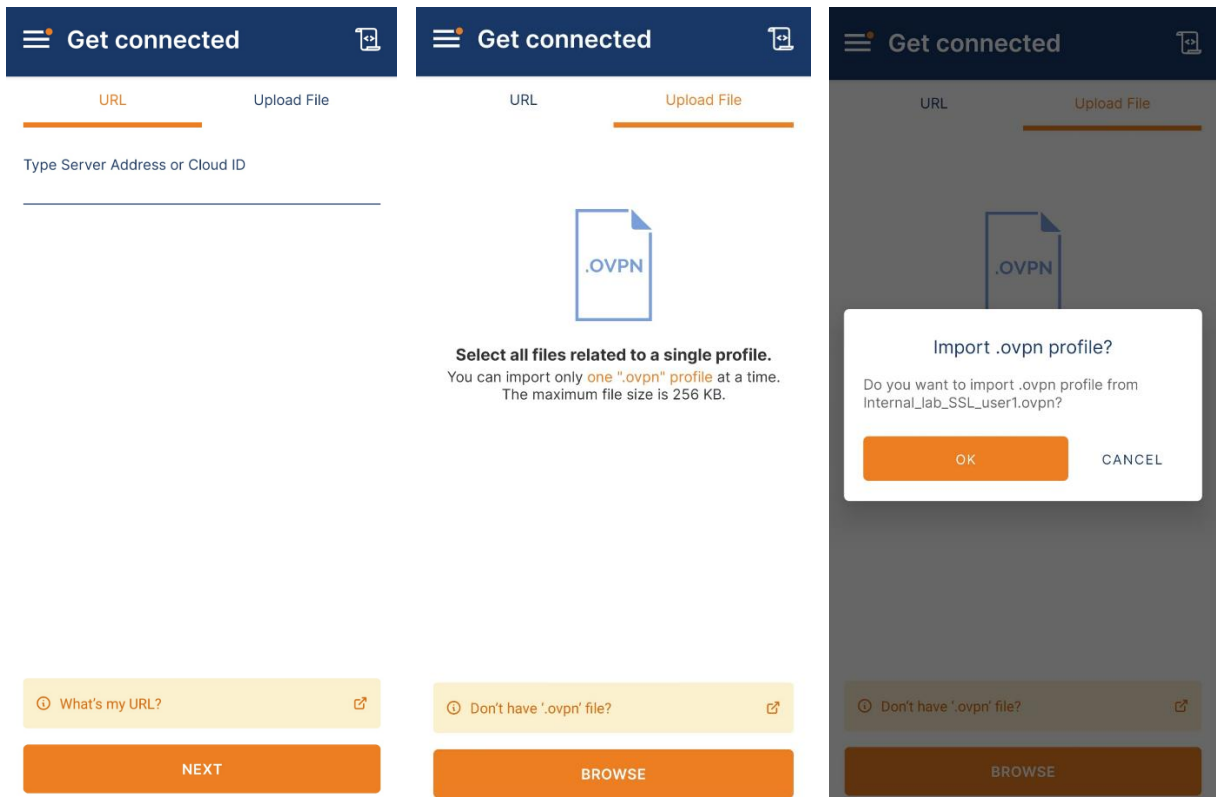
- Fazer download, carregando no ícone correspondente ao utilizador:

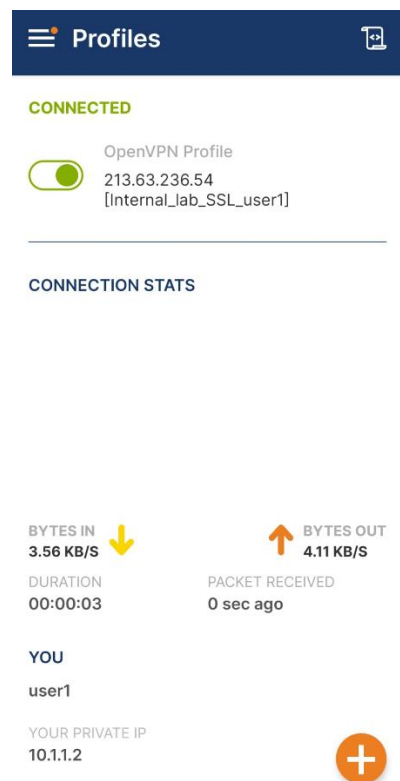
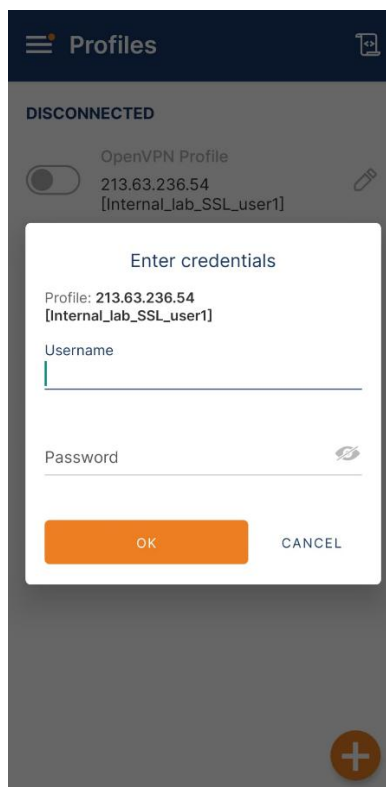
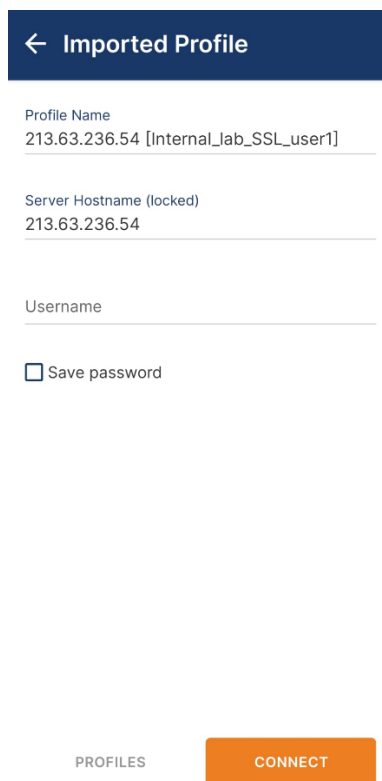
VPN: OpenVPN: Client Export full help

Remote Access Server	Internal-lab_SSL udp:
Export type	File Only
Hostname	213.63.236.54
Port	1194
Use random local port	<input checked="" type="checkbox"/>
Validate server subject	<input checked="" type="checkbox"/>
Windows Certificate System Store	<input type="checkbox"/>
Disable password save	<input type="checkbox"/>
Custom config	<div style="border: 1px solid #ccc; height: 40px;"></div>

Accounts / certificates	
Certificate	Linked user
(none) Exclude certificate from export	
C-4SSL	
user1_cert	user1

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

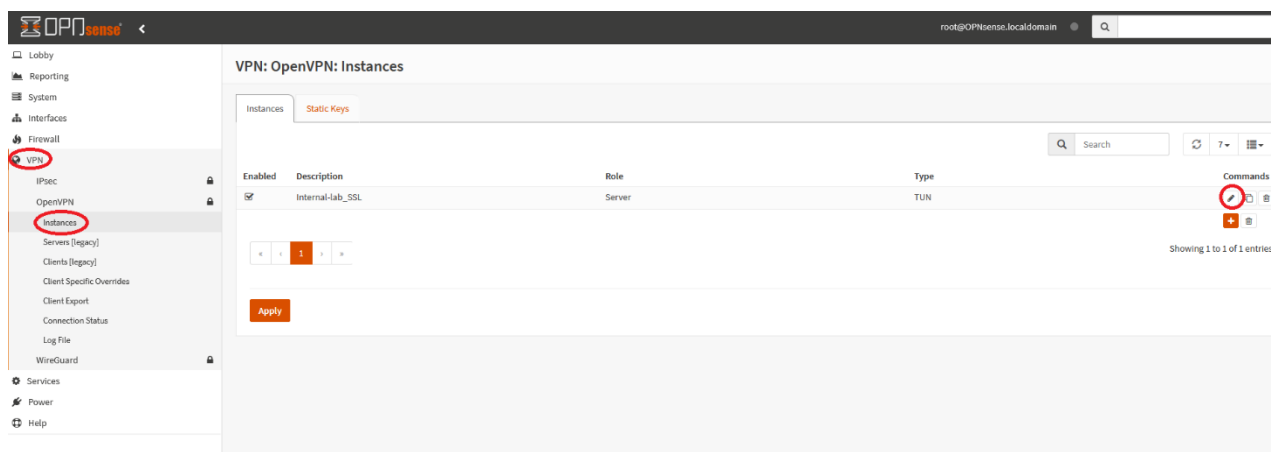




10.8 Ativar autenticação 2FA

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:

Edit Instance ✕

Certificate	C-4SSL
Verify Remote Certificate	<input type="checkbox"/>
Certificate Revocation List	None
Verify Client Certificate	required
Use OCSP (when available)	<input type="checkbox"/>
Certificate Depth	Do Not Check
TLS static key	[auth (Authenticate control channel packets)] chave1
Authentication	
Authentication	Servidor2FA
Enforce local group	<input type="text"/> <ul style="list-style-type: none"> Local Database <li style="border: 2px solid red; border-radius: 50%; padding: 2px;">Servidor2FA ✓
Strict User/CN Matching	<input type="checkbox"/>
Renegotiate time	<input type="text"/>
Auth Token Lifetime	<input type="text"/>
Routing	
Local Network	192.168.100.0/24

✖ Clear All 📄 Copy 📄 Paste 📄 Text

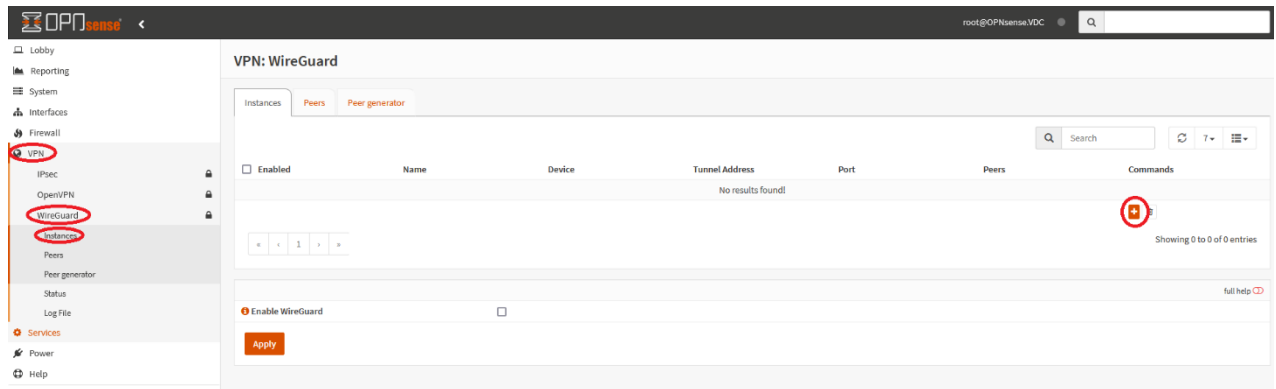
Cancel Save

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.

Edit instance ✕

Ⓞ advanced mode full help Ⓞ

Enabled

Name

Instance

Public key

Private key

Listen port

Tunnel address

✖ Clear All 📄 Copy 📄 Paste 📄 Text

Depend on (CARP)

Peers

✖ Clear All ✔ Select All

Disable routes

Cancel
Save

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":

OPN cestra

root@OPNcestra.VDC

- ↳ Lobby
- ↳ Reporting
- ↳ System
- ↳ Interfaces
- ↳ Firewall
- VPN
- ↳ IPsec
- ↳ OpenVPN
- WireGuard
- ↳ Instances
- ↳ Peers
- Peer generator
- ↳ Status
- ↳ Log File
- ↳ Services
- ↳ Power
- ↳ Help

VPN: WireGuard

Instances
Peers
Peer generator

Instance

Endpoint

Name

Public key

Private key

Address

Pre-shared key

Allowed IPs

Keepalive interval

DNS Servers

Config

```

[Interface]
PrivateKey = EDwv41ES7Y6mzashy8G4y3c27VgG5wvZ5dKXK0B1um
Address = 10.1.1.1/24

[Peer]
PublicKey = UqjMDRMtaQ8CZVUzH4CEEdseX8T37vKLP1g=
Endpoint =
AllowedIPs = 0.0.0.0::/0
                    
```

Store and generate qr ✔

Enable WireGuard

Apply

M_GP_303 v2.0

Página 62 de 81

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

VPN: WireGuard

Instances Peers Peer generator

Instance: wg0_instance

Endpoint: 213.63.236.54:51820

Name: Laptop_1

Public key: ZHipm+2B5xP83b4RRuBu6jLdVAlhWNZ3Hw1WYBFE ...

Private key: EOHvt1IEbTY6mzasHy8GAiy5o20YwgG+wZsdKNRxB ...

Address: 10.1.1.1/32

Pre-shared key:

Allowed IPs: 0.0.0.0/0,::/0

Keepalive interval:

DNS Servers:

Config

```
[Interface]
PrivateKey = EOHvt1IEbTY6mzasHy8GAiy5o20YwgG+wZsdKNRxB1w=
Address = 10.1.1.1/32

[Peer]
PublicKey = UsjVMORTMscQV8CZWUVJ9r6OERdseX8IT/37VfKlgHg=
Endpoint = 213.63.236.54:51820
AllowedIPs = 0.0.0.0/0,::/0
```

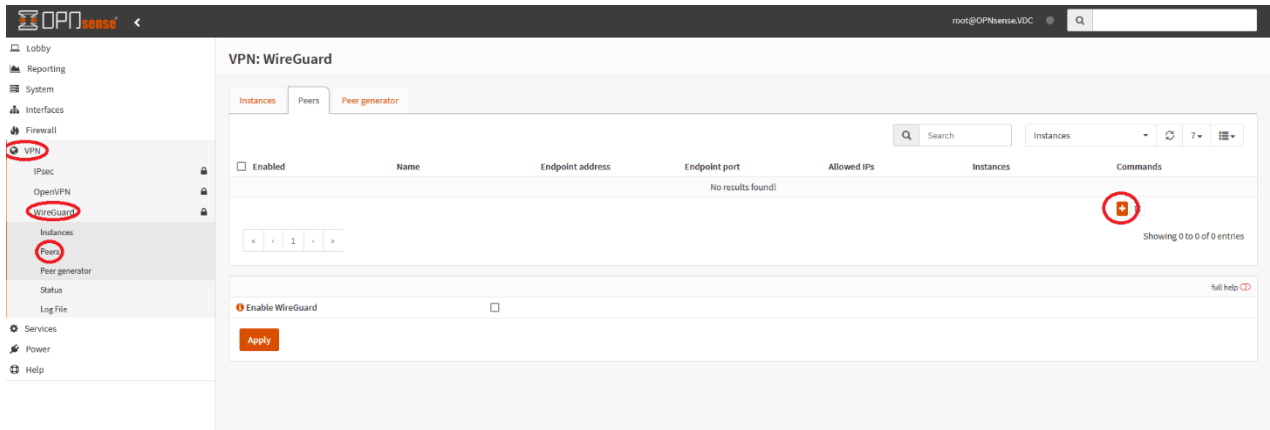
Store and generate next

Enable WireGuard

Apply

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 "+":

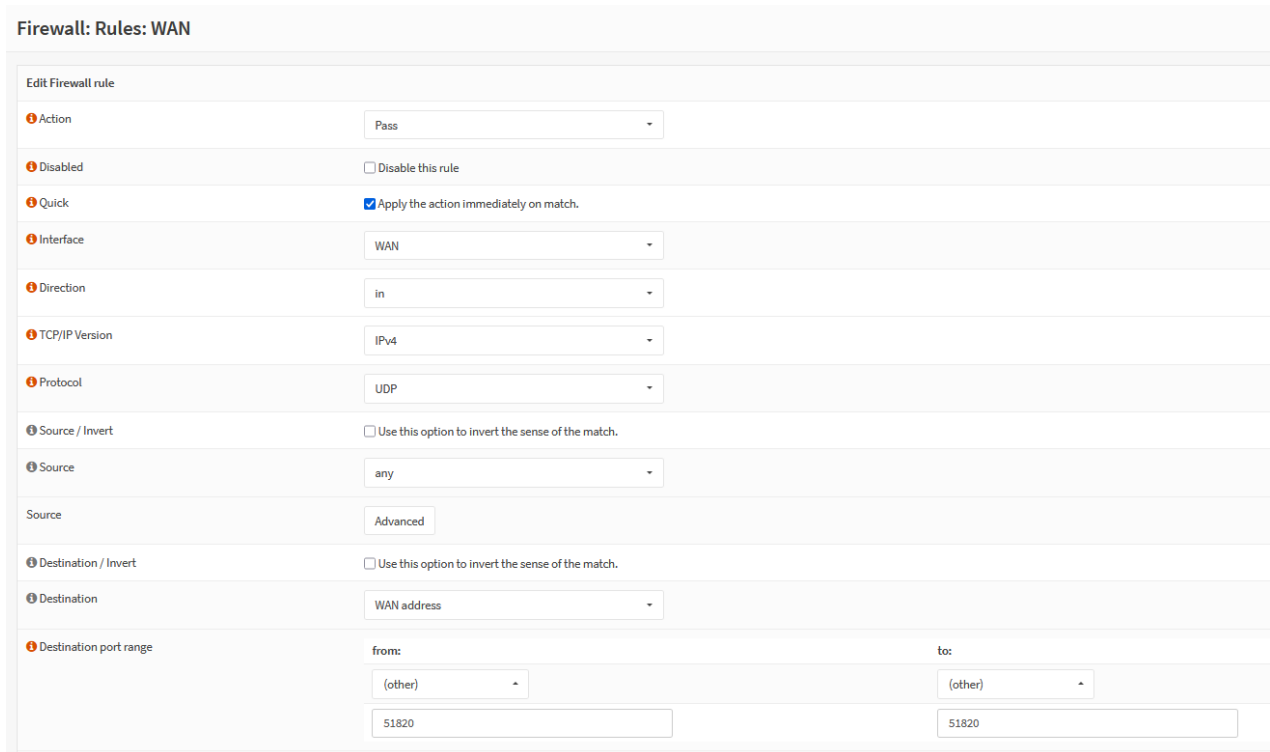


Configurar os seguintes parâmetros:

- 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:



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

Firewall: Rules: WireGuard (Group)

Edit Firewall rule

Action Pass

Disabled Disable this rule

Quick Apply the action immediately on match.

Interface WireGuard (Group)

Direction in

TCP/IP Version IPv4

Protocol any

Source / Invert Use this option to invert the sense of the match.

Source any

Source

Destination / Invert Use this option to invert the sense of the match.

Destination any

Destination port range from: any to: any

Log Log packets that are handled by this rule

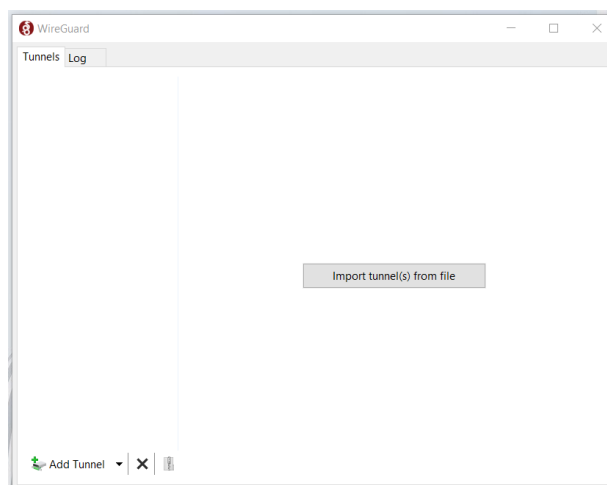
11.4 Configuração do cliente

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

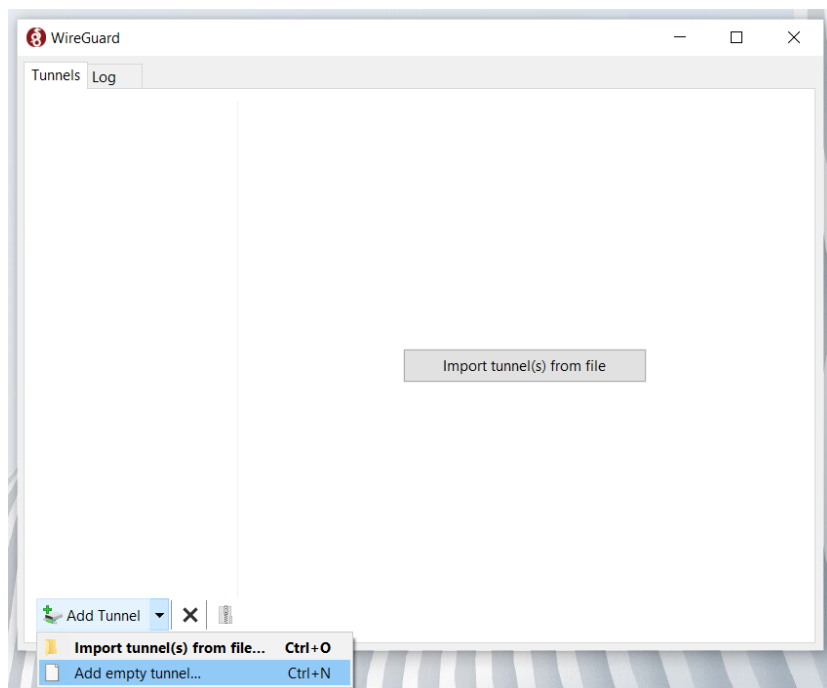
Cliente Windows

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

Após concluída, surge um quadro pra configuração do túnel:

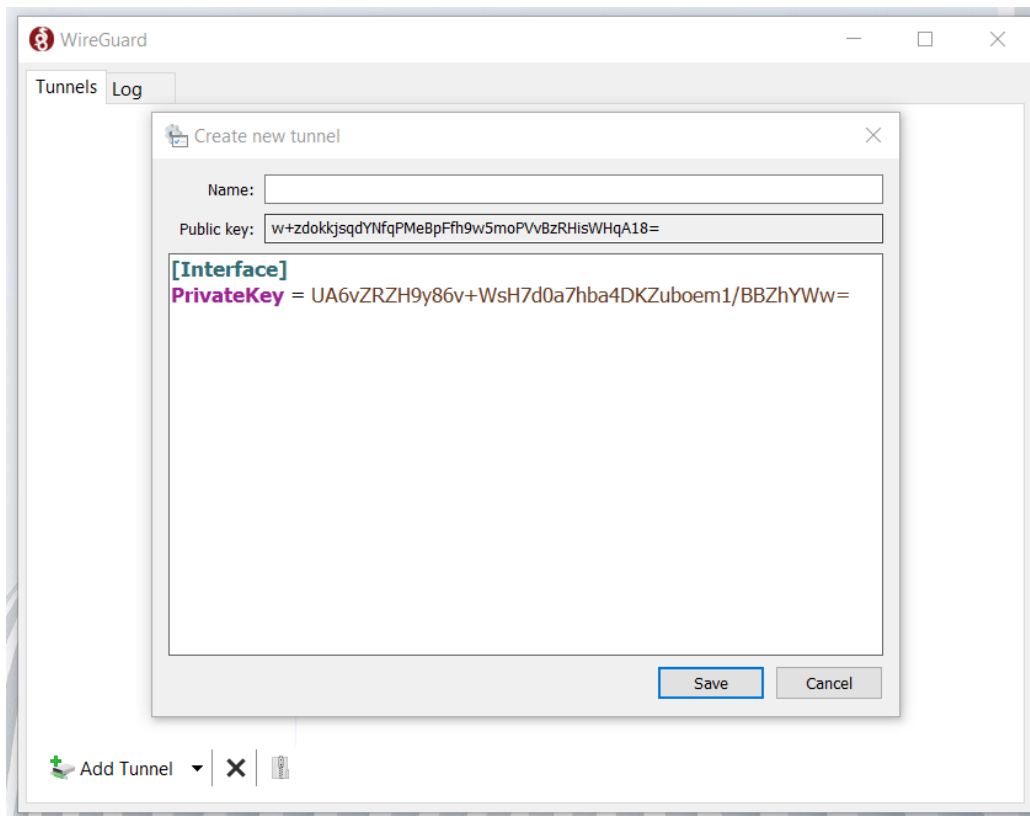


Como neste caso não existe ficheiro de configuração, devemos iniciar a criação do túnel expandindo o dropdown junto a "Add Tunnel" e escolher a opção "Add empty tunnel...":

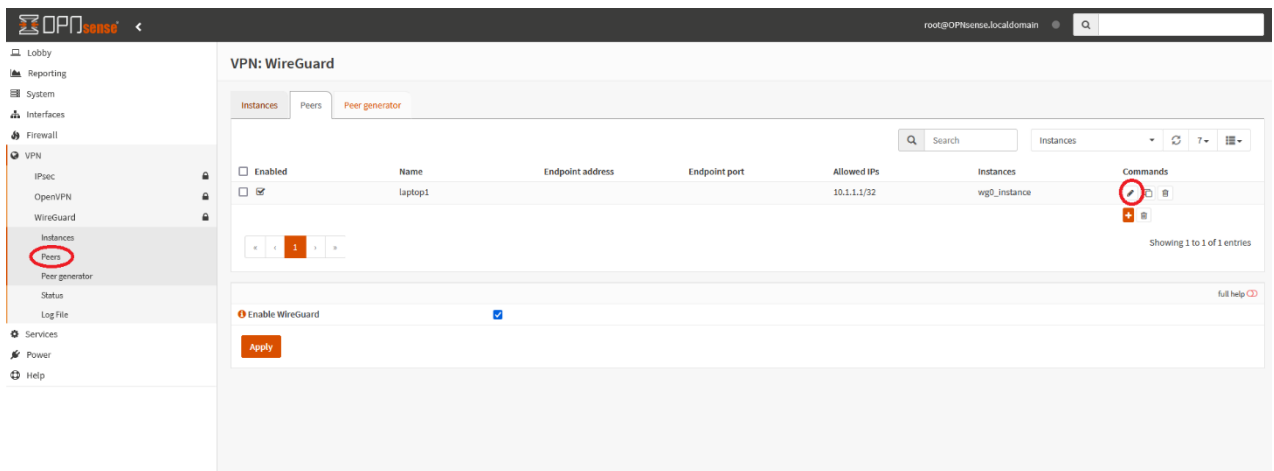


O processo de configuração é manual mas bastante simples.

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



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



Edit peer
✕

[full help](#)

Enabled

Name

Public key

Pre-shared key

Allowed IPs
✖ Clear All ✂ Copy 📄 Paste 📄 Text

Endpoint address

Endpoint port

Instances
✖ Clear All ✔ Select All

Keepalive interval

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

VPN: WireGuard

Instances
Peers
Peer generator

Instances
▼
↻
7
☰

<input type="checkbox"/>	Enabled	Name	Endpoint address	Endpoint port	Allowed IPs	Instances	Commands
<input checked="" type="checkbox"/>		laptop1			10.1.1.1/32	wg0_instance	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

« < 1 > »
Showing 1 to 1 of 1 entries

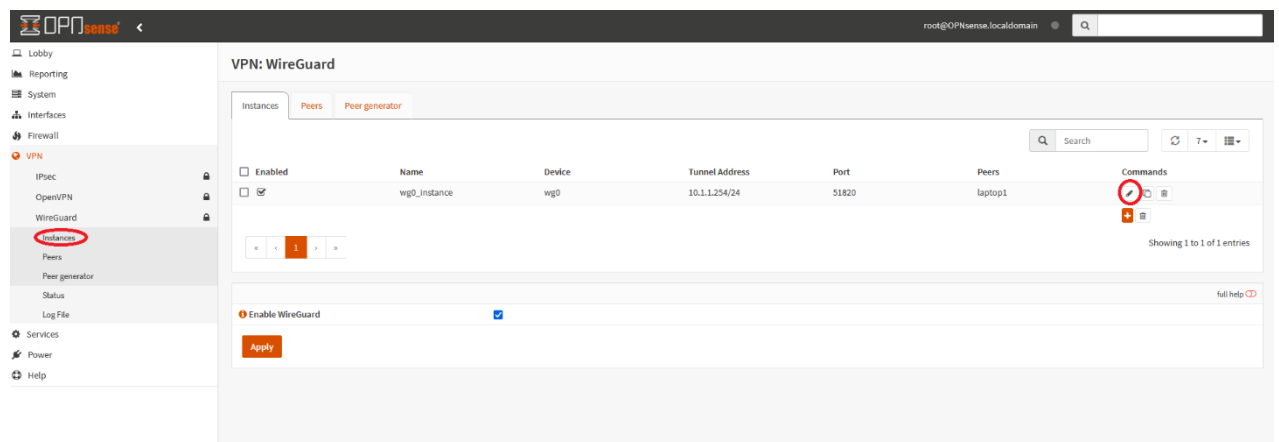
[full help](#)

Enable WireGuard

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:



Edit instance

advanced mode full help

Enabled

Name

Instance

Public key

Private key

Listen port

Tunnel address
✖ Clear All 📄 Copy 📄 Paste 📄 Text

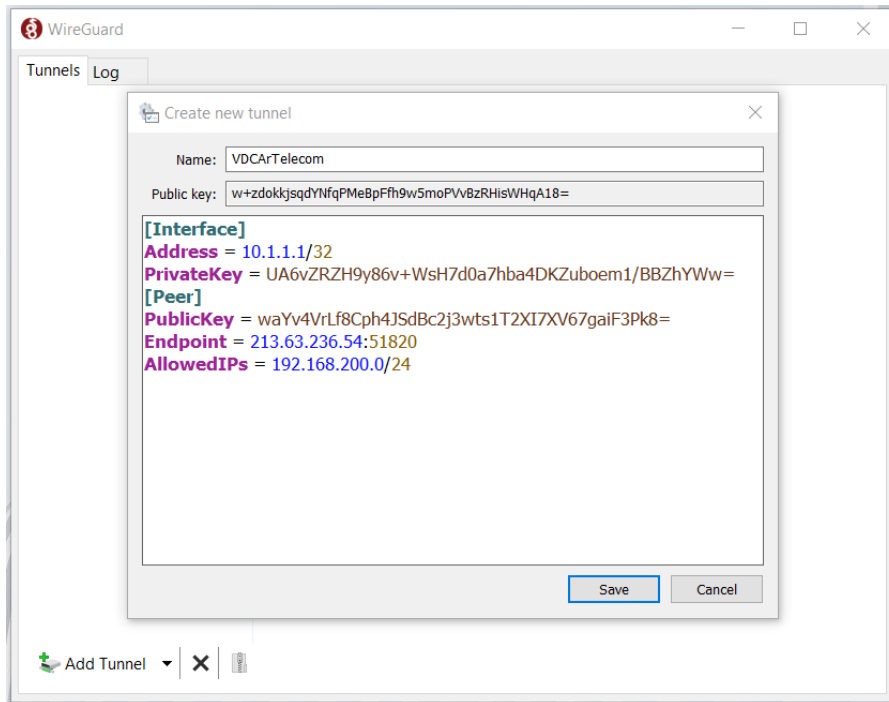
Depend on (CARP)

Peers
✖ Clear All ✔ Select All

Disable routes

- 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:



12. IPSEC VPN SITE-TO-SITE

Uma ligação site-to-site IPsec permite a conectividade 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
- Tráfego UDP na porta 500 (ISAKMP)
- Tráfego UDP na porta 4500 (NAT-T)

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

<input type="checkbox"/>		IPv4 ESP	*	*	WAN address	*	*	*
<input type="checkbox"/>		IPv4 TCP/UDP	*	*	WAN address	500 (ISAKMP)	*	*
<input type="checkbox"/>		IPv4 TCP/UDP	*	*	WAN address	4500 (IPsec NAT-T)	*	*

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

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
IPv4 TCP	GESTAO_AR	*	10.10.10.2	443 (HTTPS)	*	*	WEB ACCESS GUI
IPv4 TCP	*	*	192.168.100.107	3389 (MS RDP)	*	*	
IPv4 TCP	*	*	192.168.100.101	22 (SSH)	*	*	
IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	*	
pass	block (disabled)	reject	reject (disabled)	log	log (disabled)	in	first match
pass (disabled)	block (disabled)	reject	reject (disabled)	log	log (disabled)	out	last match

Protocolo ESP

Escolher:

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

Firewall: Rules: WAN

Edit Firewall rule	
Action	Pass
Disabled	<input type="checkbox"/> Disable this rule
Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.
Interface	WAN
Direction	in
TCP/IP Version	IPv4
Protocol	ESP
Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Source	any
Source	Advanced
Destination / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Destination	WAN address
Destination port range	from: any

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

Firewall: Rules: WAN

Edit Firewall rule

Action	Pass
Disabled	<input type="checkbox"/> Disable this rule
Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.
Interface	WAN
Direction	in
TCP/IP Version	IPv4
Protocol	TCP/UDP
Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Source	any
Source	Advanced
Destination / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Destination	WAN address
Destination port range	from: ISAKMP to: ISAKMP

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

Firewall: Rules: WAN

Edit Firewall rule

Action Pass

Disabled Disable this rule

Quick Apply the action immediately on match.

Interface WAN

Direction in

TCP/IP Version IPv4

Protocol TCP/UDP

Source / Invert Use this option to invert the sense of the match.

Source any

Source Advanced

Destination / Invert Use this option to invert the sense of the match.

Destination WAN address

Destination port range from: IPsec NAT-T to: IPsec NAT-T

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.

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>)

Edit pre-shared-key

full help

Local Identifier 213.63.236.54

Remote Identifier 84.236.133.233

Pre-Shared Key bB8u6Tj60uJL2RKYR0OCyiGMdds9gaEUs9Q2d3bRTT...

Type PSK

Cancel Save

12.3 Configuração do túnel

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

Connections

OPNsense

Lobby Reporting System Interfaces Firewall **VPN** IPsec **Connections** Tunnel Settings [legacy] Mobile Clients Pre-Shared Keys Key Pairs Advanced Settings Status Overview Lease Status Security Association Database Security Policy Database Virtual Tunnel Interfaces Log File OpenVPN

VPN: IPsec: Connections

Connections Pools

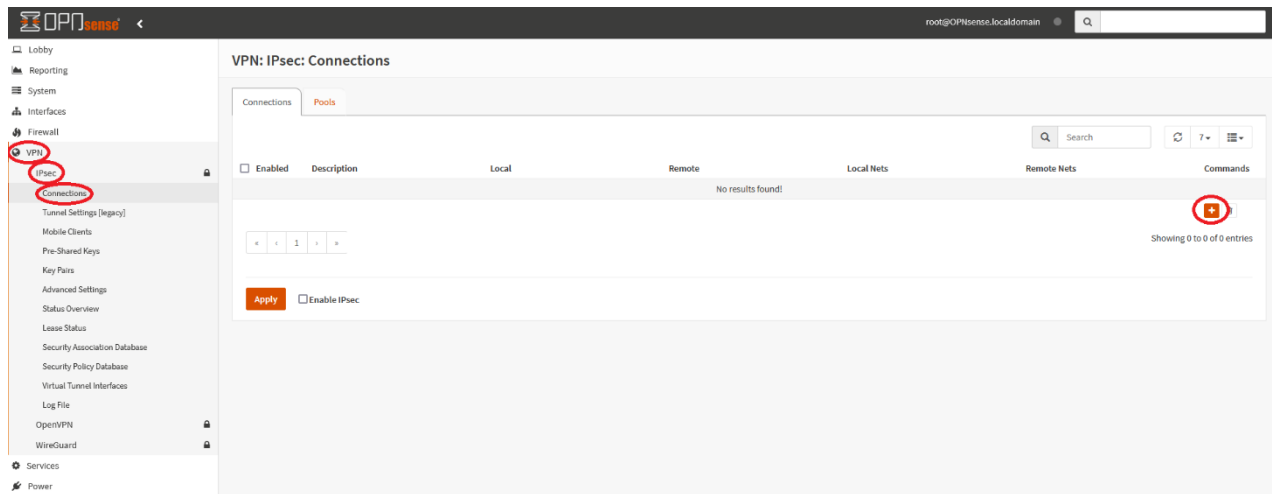
Enabled	Description	Local	Remote
<input type="checkbox"/>			

No results found!

« < 1 > »

Apply Enable IPsec

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



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

VPN: IPsec: Connections

[Connections](#)
[Ligação a OASIX](#)
[Pools](#)

General settings

advanced mode

enabled

Proposals default

Version IKEv1+IKEv2

MOBIKE

Local addresses 10.10.10.2

Remote addresses 84.236.133.233

DPD delay (s)

Pools Nothing selected

Description Ligação a OASIX

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

Local Authentication					Remote Authentication				
Enabled	Round	Authentication	Description	Commands	Enabled	Round	Authentication	Description	Commands
No results found!					No results found!				
<input type="button" value="+"/>					<input type="button" value="+"/>				
Children									
<input type="text" value="Search"/> <input type="button" value="7"/> <input type="button" value="List"/>									
Enabled	Description	Local Nets	Remote Nets	Commands					
No results found!					<input type="button" value="+"/>				
Showing 0 to 0 of 0 entries									

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

enabled	<input checked="" type="checkbox"/>
Connection	Ligação a OASIX
Round	0
Authentication	Pre-Shared Key
Id	213.63.236.54
Certificates	Nothing selected Clear All Select All
Description	

E o mesmo para a autenticação remota:

enabled	<input checked="" type="checkbox"/>
Connection	Ligação a OASIX
Round	0
Authentication	Pre-Shared Key
Id	84.236.133.233
Certificates	Nothing selected Clear All Select All
Description	

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 "+":

VPN: IPsec: Connections

Connections | Ligação a OASIX | Pools

General settings

advanced mode full help

enabled

Proposals: default

Version: IKEv1+IKEv2

MOBIKE:

Local addresses: 10.10.10.2

Remote addresses: 84.238.133.233

DPD delay (s):

Pools: Nothing selected

Description: Ligação a OASIX

Local Authentication				Remote Authentication			
Enabled	Round	Authentication	Description	Enabled	Round	Authentication	Description
<input checked="" type="checkbox"/>	0	Pre-Shared Key		<input checked="" type="checkbox"/>	0	Pre-Shared Key	

Children

Enabled Description Local Nets Remote Nets Commands

No results found!

Showing 0 to 0 of 0 entries

Save

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

Edit Child

advanced mode full help

enabled

Connection: Ligação a OASIX

Mode: Tunnel

Policies:

Start action: Start

DPD action: Clear

Reqid:

ESP proposals: default

Local: 192.168.100.0/24

Remote: 192.168.1.0/24

Description:

Cancel Save

No quadro da Conexão fazer novamente "Save":

E finalmente, "Apply" da configuração:

Podemos verificar a criação do túnel e respetiva conectividade em "Status Overview":

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