orange Business Services

Flexible Engine
pfSense open source virtual firewall appliance deployment guide

Objectives

The document has for purpose to

- **describe** how to deploy and configure pfSense appliance on Flexible Engine
- **explain** how to access the web interface from Internet
- **propose** example network designs to use pfSense to filter traffic between WAN, FE DMZ VPC, FE Private VPC and Internet

Content

Objectives.. 1

1. Introduction.. 3

2. pfSense image deployment on Flexible Engine 3

2.1. Prerequisites 3

2.2. pfSense ECS creation 4

2.3. pfSense initial configuration 5

3. pfSense configuration to access web interface from internet 7

4. VPC route table configuration to allow protected ECS to use pfSense as an Internet NAT gateway 10

5. pfSense network design on Flexible Engine examples 12

5.1. Single VPC 12

5.2. Multiple VPC 13

6. FAQ 14

How to associate several public IP addresses to pfSense WAN interface? 14

Is it possible to use pfSense to filter traffic between subnets in a VPC? 14

Is it possible to set a pfSense High Availability cluster in Flexible Engine? 14

1. Introduction

pfSense software is an open-source firewall with over 1 million active installations in enterprise-level organizations, higher education institutions, and government agencies worldwide.

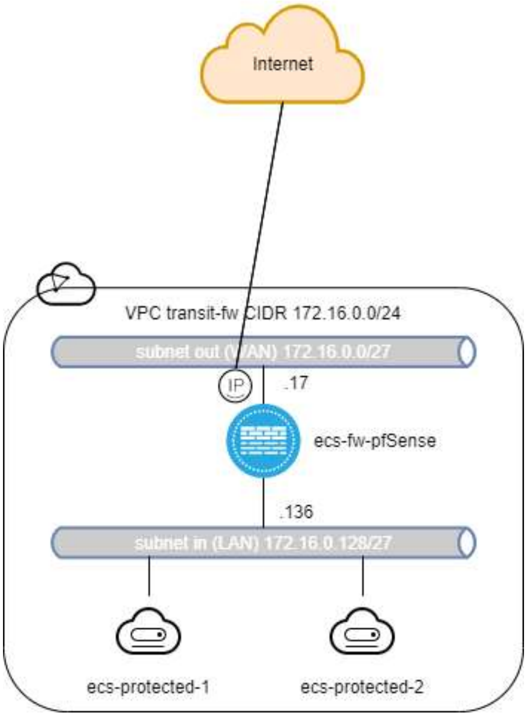
pfSense software delivers advanced firewall, VPN, and routing functionality in your cloud-based infrastructure with features including intrusion detection and prevention, load balancing, traffic shaping, GeoIP blocking, dual-stack IPv4 and IPv6 support, DHCP and DNS server, Domain Name blacklisting, multiple VPN tunnels using IPsec and OpenVPN, web content filtering, and more.

Please refer to the pfSense website for more information

2. pfSense image deployment on Flexible Engine

2.1.Prerequisites

Before deploying a pfSense appliance on Flexible you must define a network design corresponding to your needs.
Here is a simple and minimal network design example on which this deployment guide is based on:


Internet
VPC transit-fw CIDR 172.16.0.0/24
subnet out (WAN) 172.16.0.0/27
IP
.17
ecs-fw-pfSense
.136
subnet in (LAN) 172.16.0.128/27
ecs-protected-1
ecs-protected-2

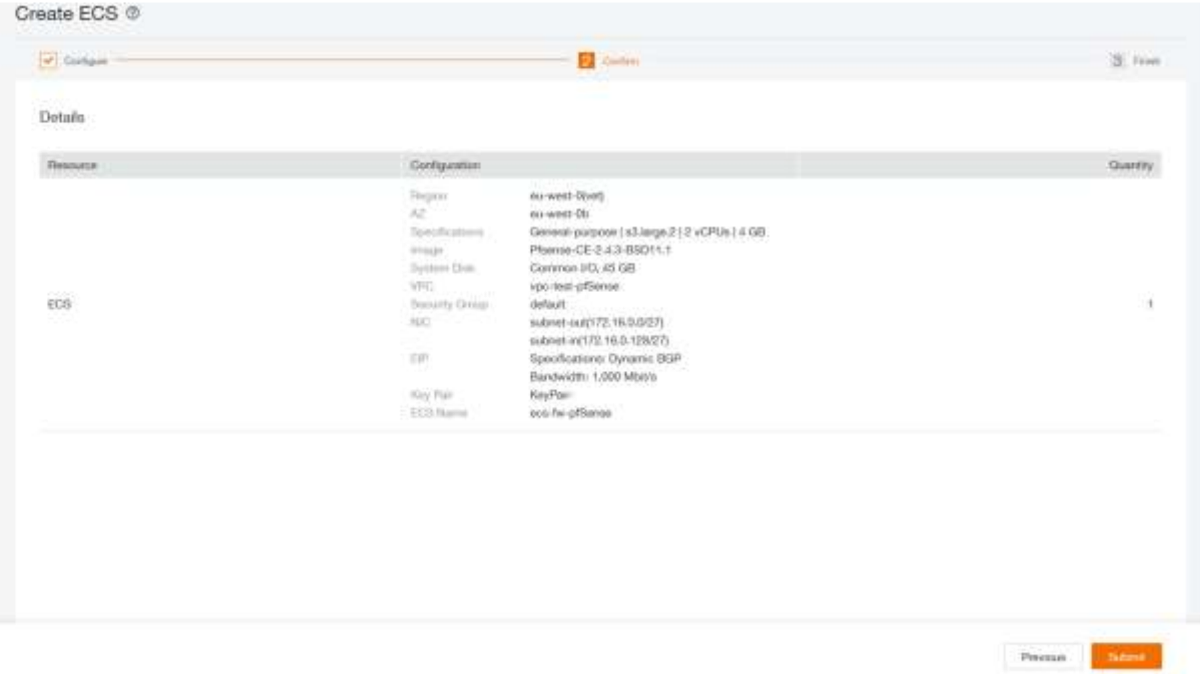
In this example we need 1 VPC with CIDR 172.16.0.0/24 with 2 subnets. A subnet “out” with CIDR 172.16.0.0/27 on which pfSense WAN network interface will be attached and a subnet “in” with CIDR 172.16.128.0/27 on which pfSense LAN network interface will be attached. An EIP will be attached on the WAN network interface to give pfSense internet connectivity.
The objective here is for pfSense to protect internet access of ECS attached to the subnet “in”.

In order to create the pfSense ECS instance, you will need a SSH Key-Pair. The SSH Key Pair will only be used for ECS creation; it can’t be used to SSH login on pfSense instances without further configuration.
https://docs.prod-cloud-ocb.orange-business.com/en-us/usermanual/ecs/en-us_topic_0014250631.html

In order to allow network flows, you will need to associate a Security Group to each network interface of your pfSense instance. Since pfSense is a firewall, you can use a non-filtering Security Group:
https://docs.prod-cloud-ocb.orange-business.com/en-us/usermanual/ecs/en-us_topic_0140323151.html

2.2.pfSense ECS creation

Using Flexible Engine Console create an ECS with the following parameters:

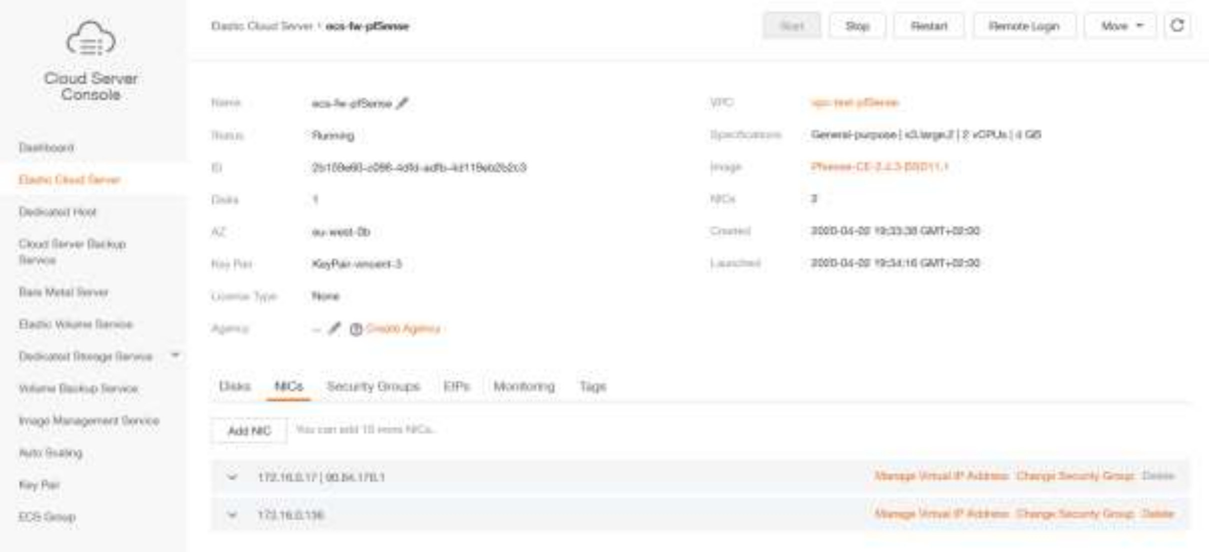


Create ECS

Details

Resource	Configuration		Quantity
ECS	Region AZ Specifications Image System Disk VPC Security Group NIC EIP Key Pair ECS Name	eu-west-0(vet) eu-west-0b General-purpose | s3.large.2 | 2 vCPUs | 4 GB Pfsense-CE-2.4.3-BSD11.1 Common I/O, 45 GB vpc-test-pfSense default subnet-out(172.16.0.0/27) subnet-in(172.16.0.128/27) Specifications: Dynamic BGP Bandwidth: 1,000 Mbit/s KeyPair ecs-fw-pfSense	1

Once the ECS is created go the “NICs” tab of the ECS details page:



Name ecs-fw-pfSense

Status Running

ID 2b159e60-c096-4d9d-adfb-4d119eb2b2c3

Disks 1

AZ eu-west-0b

Key Pair KeyPair-vincent-3

License Type None

Agency -- Create Agency

VPC vpc-test-pfSense

Specifications General-purpose | s3.large.2 | 2 vCPUs | 4 GB

Image Pfsense-CE-2.4.3-BSD11.1

NICs 2

Created 2020-04-02 19:33:38 GMT+02:00

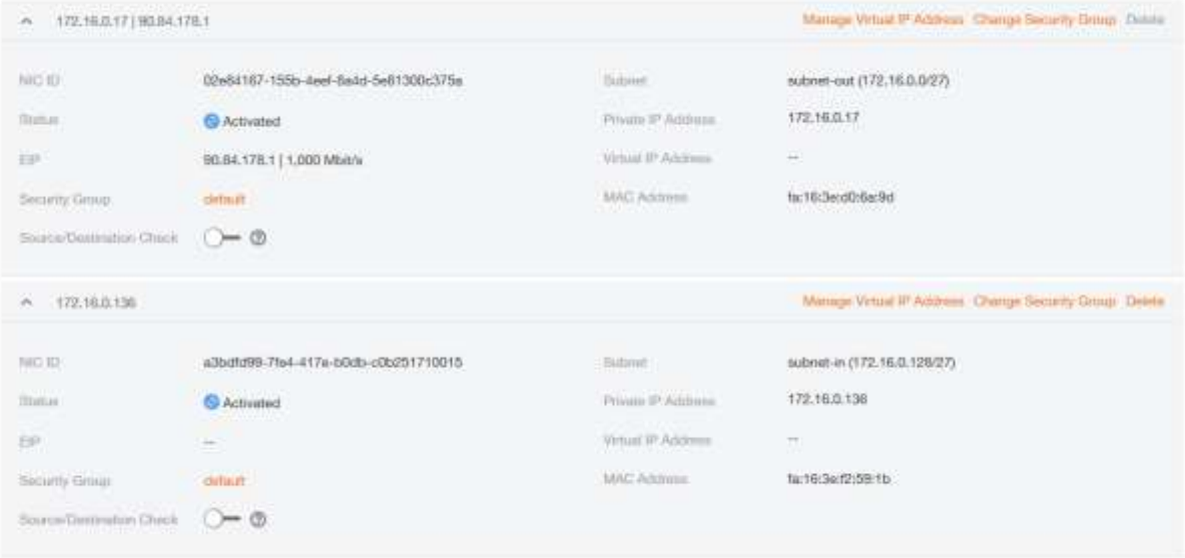
Launched 2020-04-02 19:34:16 GMT+02:00

You can add 10 more NICs.

172.16.0.17 | 90.84.178.1 Manage Virtual IP Address Change Security Group Delete

172.16.0.136 Manage Virtual IP Address Change Security Group Delete

And disable the “Source/Destination” parameter on each NIC as pfSense ECS will serve as NAT gateway for the protected ECS:



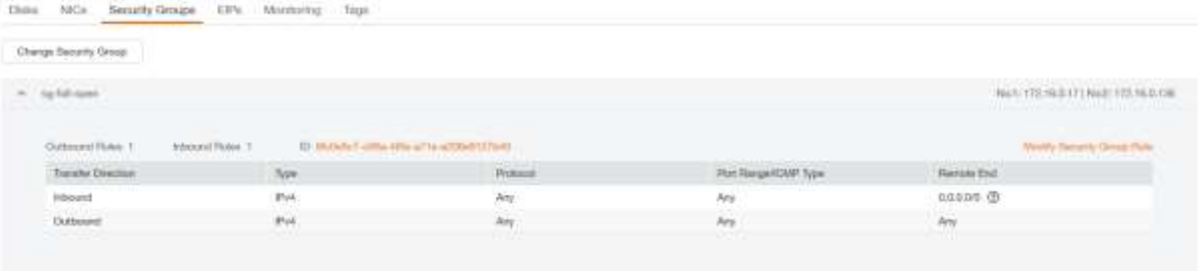
172.16.0.17 | 90.84.178.1

NIC ID	02e84167-155b-4eef-8a4d-5e81300c375a	Subnet	subnet-out (172.16.0.0/27)
Status	Activated	Private IP Address	172.16.0.17
EIP	90.84.178.1 | 1,000 Mbit/s	Virtual IP Address	--
Security Group	default	MAC Address	fa:16:3e:d0:6a:9d
Source/Destination Check	○		

172.16.0.136

NIC ID	a3bdfd99-7fe4-417e-b0db-c0b251710015	Subnet	subnet-in (172.16.0.128/27)
Status	Activated	Private IP Address	172.16.0.136
EIP	--	Virtual IP Address	--
Security Group	default	MAC Address	fa:16:3e:f2:59:1b
Source/Destination Check	○		

On the “Security Groups” tab, associate a security group to the network interfaces:



sg-full-open

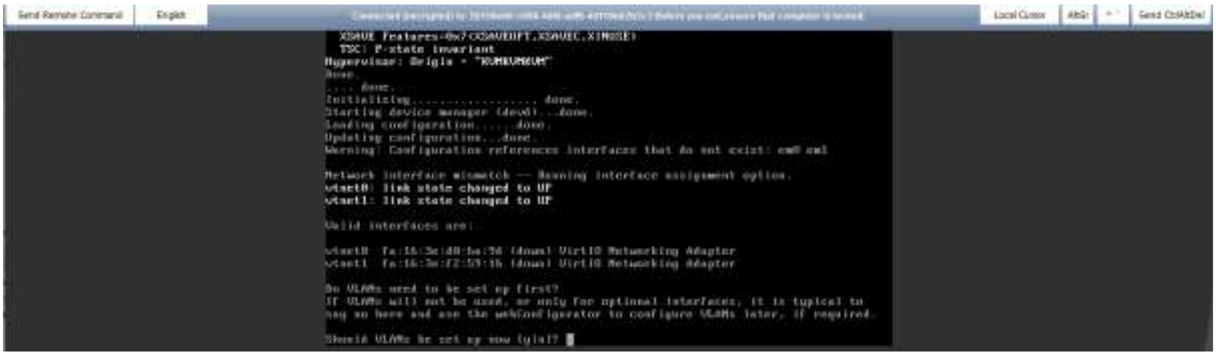
NIC1: 172.16.0.17 | NIC2: 172.16.0.136

Outbound Rules: 1   Inbound Rules: 1   ID: [illegible]

Transfer Direction	Type	Protocol	Port Range/ICMP Type	Remote End
Inbound	IPv4	Any	Any	0.0.0.0/0
Outbound	IPv4	Any	Any	Any

2.3.pfSense initial configuration

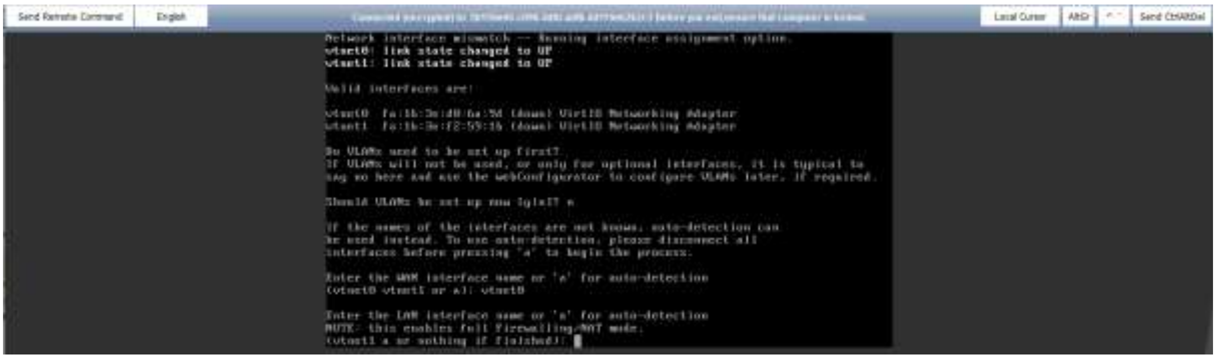
You can start configuring pfSense using “Remote Login” from the Flexible Engine console:



```
  XSAVE Features=0x7<XSAVEOPT,XSAVEC,XINUSE>
  TSC: P-state invariant
Hypervisor: Origin = "KVMKVMKVM"
done.
.... done.
Initializing................... done.
Starting device manager (devd)...done.
Loading configuration......done.
Updating configuration...done.
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.
vtnet0: link state changed to UP
vtnet1: link state changed to UP

Valid interfaces are:

vtnet0  fa:16:3e:d0:6a:9d (down) VirtIO Networking Adapter
vtnet1  fa:16:3e:f2:59:1b (down) VirtIO Networking Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]?
```

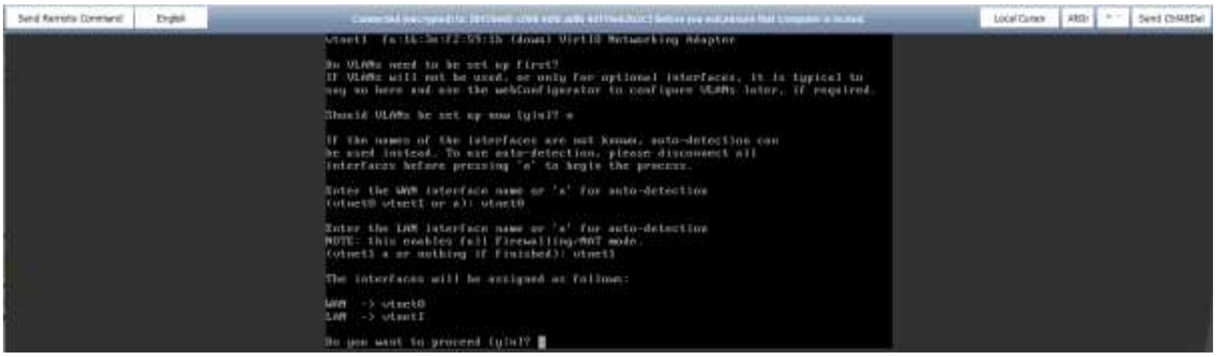
We don’t need to set up VLANs since they are not applicable in Flexible Engine network, so you can answer ‘n’ here.

We now define which network interface will be the WAN interface, so you can answer ‘vtnet0’ here since this network interface is attached to subnet “out” and has an EIP bound:



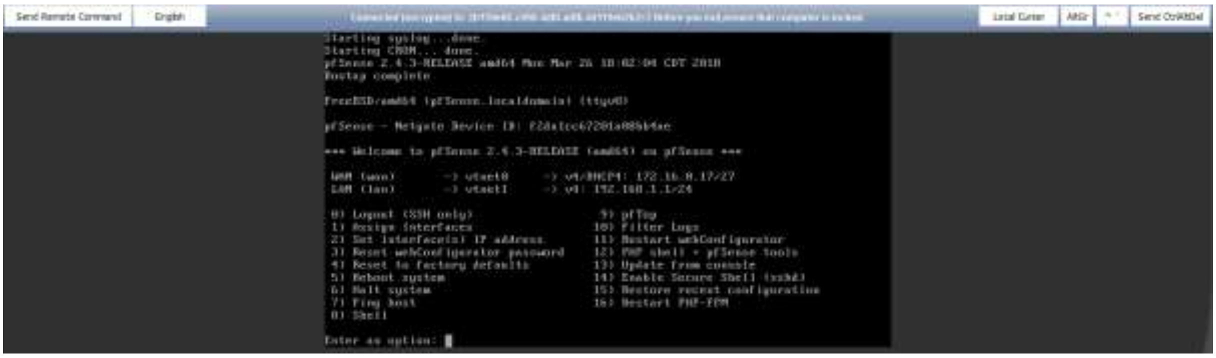
```
Network interface mismatch -- Running interface assignment option.
vtnet0: link state changed to UP
vtnet1: link state changed to UP

Valid interfaces are:

vtnet0  fa:16:3e:d8:6a:5d (down) VirtIO Networking Adapter
vtnet1  fa:16:3e:f2:59:1b (down) VirtIO Networking Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vtnet0 vtnet1 or a): vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 a or nothing if finished):
```

We now define which network interface will be the LAN interface, so you can answer ‘vtnet1’ since this network interface is attached to subnet “in”:



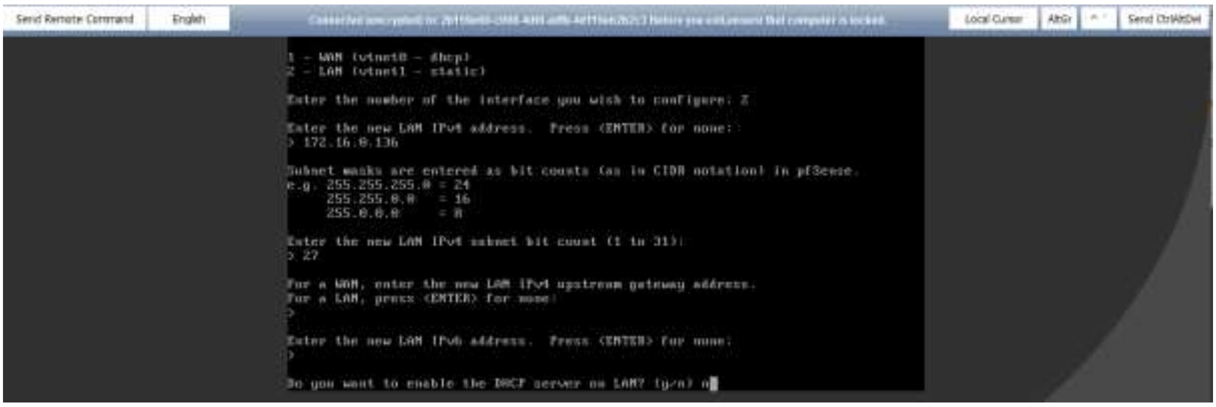
```
vtnet1  fa:16:3e:f2:59:1b (down) VirtIO Networking Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vtnet0 vtnet1 or a): vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 a or nothing if finished): vtnet1

The interfaces will be assigned as follows:

WAN  -> vtnet0
LAN  -> vtnet1

Do you want to proceed [y|n]?
```

After confirmation we can see the WAN interface has been configured with DHCP and the LAN interface with a default static configuration. So we need to configure the LAN interface with menu 2:



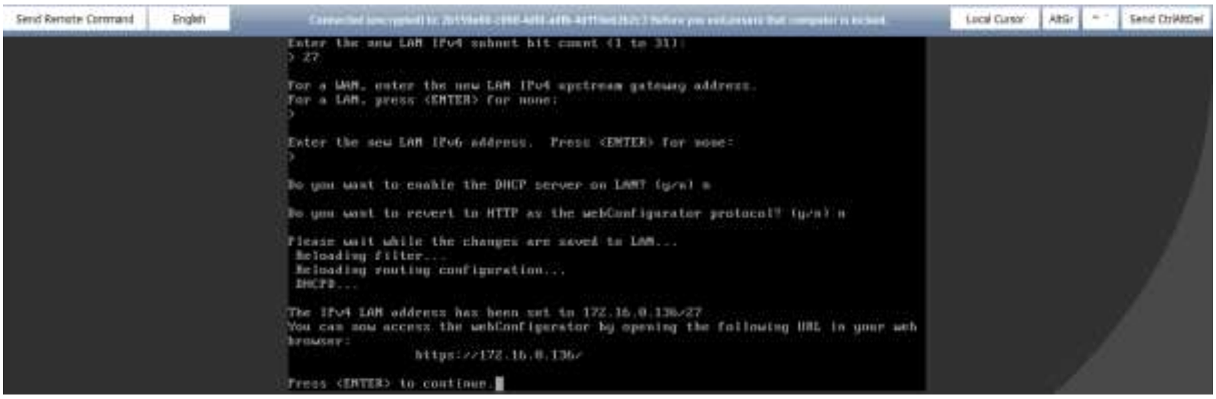
```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.3-RELEASE amd64 Mon Mar 26 18:02:04 CDT 2018
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

pfSense - Netgate Device ID: f2da1cc67201a08bb4ae

*** Welcome to pfSense 2.4.3-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 172.16.0.17/27
 LAN (lan)       -> vtnet1     -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

LAN interface must be configured manually using the IP address and mask which would have been received by DHCP.
In single VPC network configuration, upstream gateway should not be configured and DHCP server should never be activated on LAN interface:



```
1 - WAN (vtnet0 - dhcp)
2 - LAN (vtnet1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 172.16.0.136

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 27

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
```

If you don’t revert to HTTP as the webconfigurator protocol, it will be accessible in HTTPS though the LAN interface private IP:



```
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 27

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 172.16.0.136/27
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://172.16.0.136/

Press <ENTER> to continue.
```

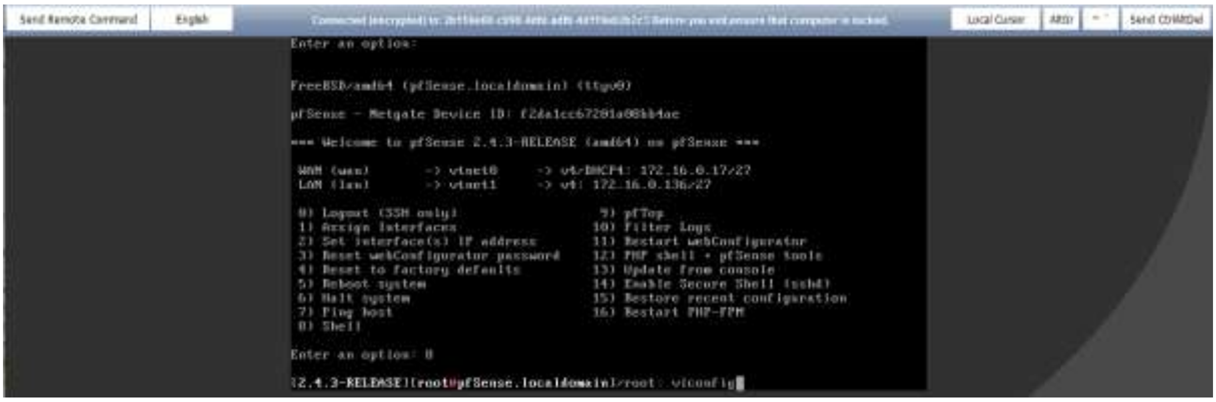
3. pfSense configuration to access web interface from internet

By default webconfigurator is only accessible from LAN interface. It can be configured to be accessible also on WAN interface but for initial configuration we need a way to access it from LAN interface.
There a few options:

- Deploy a ECS on the LAN subnet and from a remote login open the webconfigurator webpage with LAN interface private IP address
- Set up an IPsec tunnel between VPC and remote site using Flexible Engine VPNaaS feature (https://docs.prod-cloud-ocb.orange-business.com/en-us/vpn/index.html) to remotely access webconfigurator webpage with LAN interface private IP address
- Bound an EIP to LAN network interface

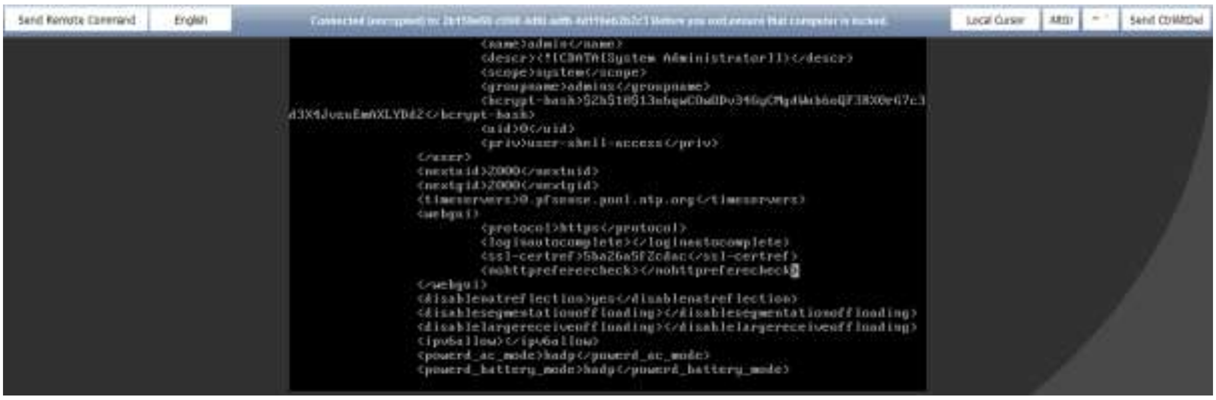
This is the last option which is described in this guide:
First you need to configure pfSense in order to disable “HTTP Referrer Check” using remote login.
You can do that by editing the “config.xml” file using “viconfig” command from the shell.

From the “Remote login” Flexible Engine console open a shell and run the “viconfig” command:



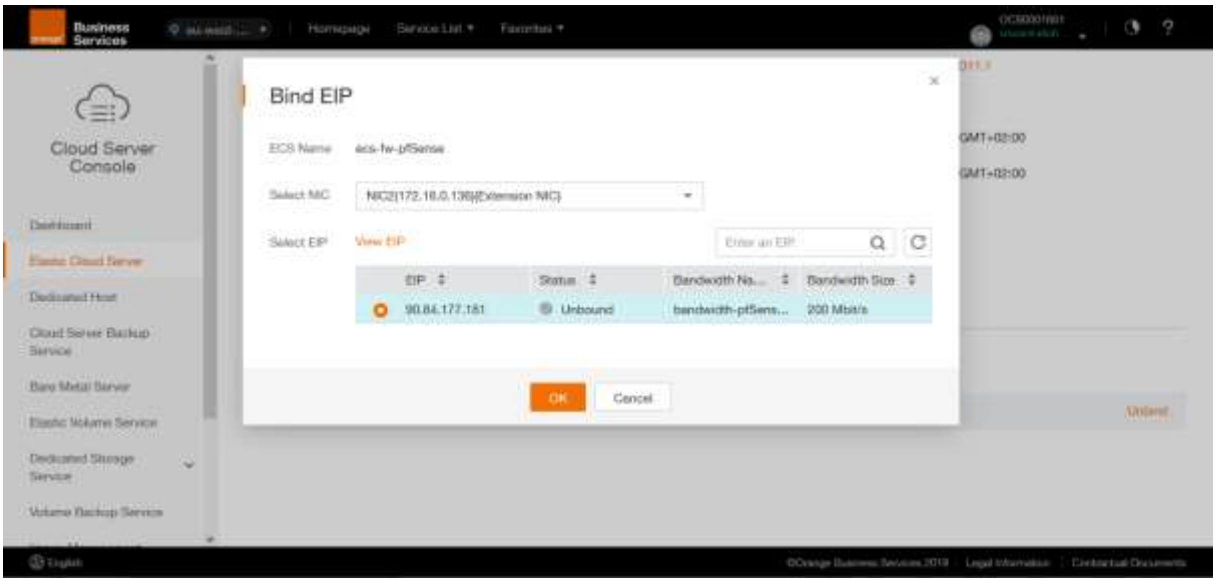
```
Enter an option:


FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

pfSense - Netgate Device ID: f2da1cc67281a08bb4ac

*** Welcome to pfSense 2.4.3-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 172.16.0.17/27
 LAN (lan)       -> vtnet1     -> v4: 172.16.0.136/27

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 8

[2.4.3-RELEASE][root@pfSense.localdomain]/root: viconfig
```

Scroll down to “<webgui>” section and add a line with “<nohttpreferercheck></nohttpreferercheck>”:



```
                <name>admin</name>
                <descr><![CDATA[System Administrator]]></descr>
                <scope>system</scope>
                <groupname>admins</groupname>
                <bcrypt-hash>$2b$10$13mbgwCDwDDv346yCMgdWkb6oQF38X0rG7c3
d3X4JuzuEmAXLYDd2</bcrypt-hash>
                <uid>0</uid>
                <priv>user-shell-access</priv>
        </user>
        <nextuid>2000</nextuid>
        <nextgid>2000</nextgid>
        <timeservers>0.pfsense.pool.ntp.org</timeservers>
        <webgui>
                <protocol>https</protocol>
                <loginautocomplete></loginautocomplete>
                <ssl-certref>5ba26a5f2c4ac</ssl-certref>
                <nohttpreferercheck></nohttpreferecheck>
        </webgui>
        <disablenatreflection>yes</disablenatreflection>
        <disablesegmentationoffloading></disablesegmentationoffloading>
        <disablelargereceiveoffloading></disablelargereceiveoffloading>
        <ipv6allow></ipv6allow>
        <powerd_ac_mode>hadp</powerd_ac_mode>
        <powerd_battery_mode>hadp</powerd_battery_mode>
```

Now you create EIP and bound it to LAN interface of pfSense ECS:



Bind EIP

ECS Name: ecs-fw-pfSense

Select NIC: NIC2(172.16.0.136)(Extension NIC)

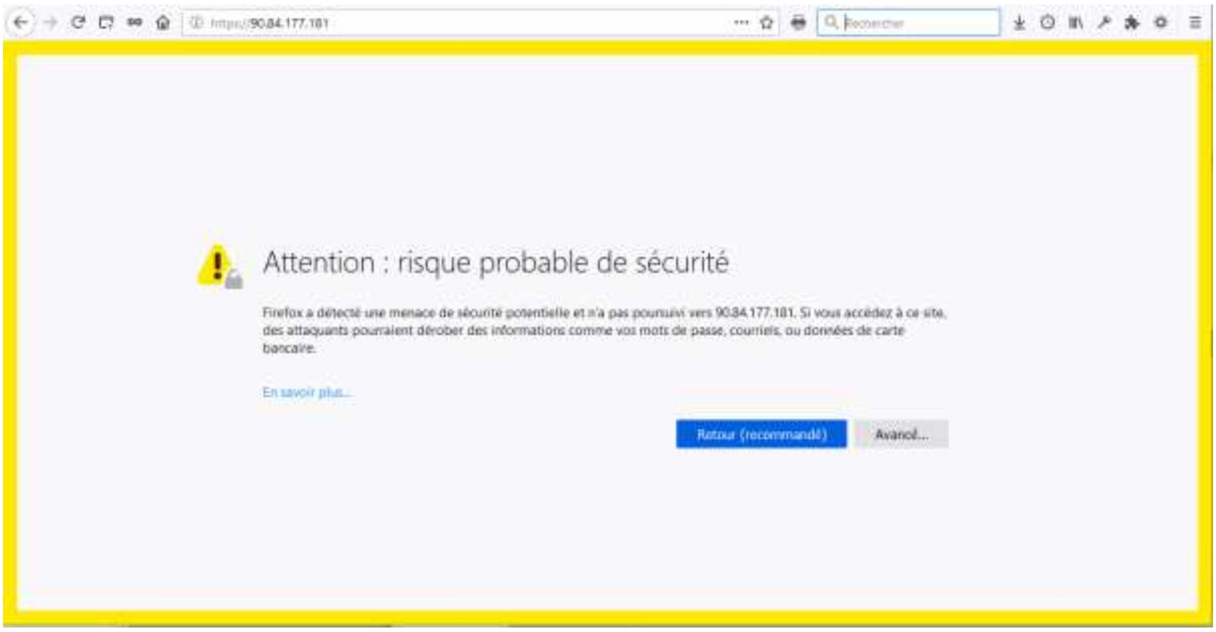
Select EIP: View EIP

Enter an EIP

	EIP	Status	Bandwidth Na...	Bandwidth Size
●	90.84.177.181	Unbound	bandwidth-pfSens...	200 Mbit/s

OK   Cancel

Then you can open the webconfigurator page from the browser of your workstation:



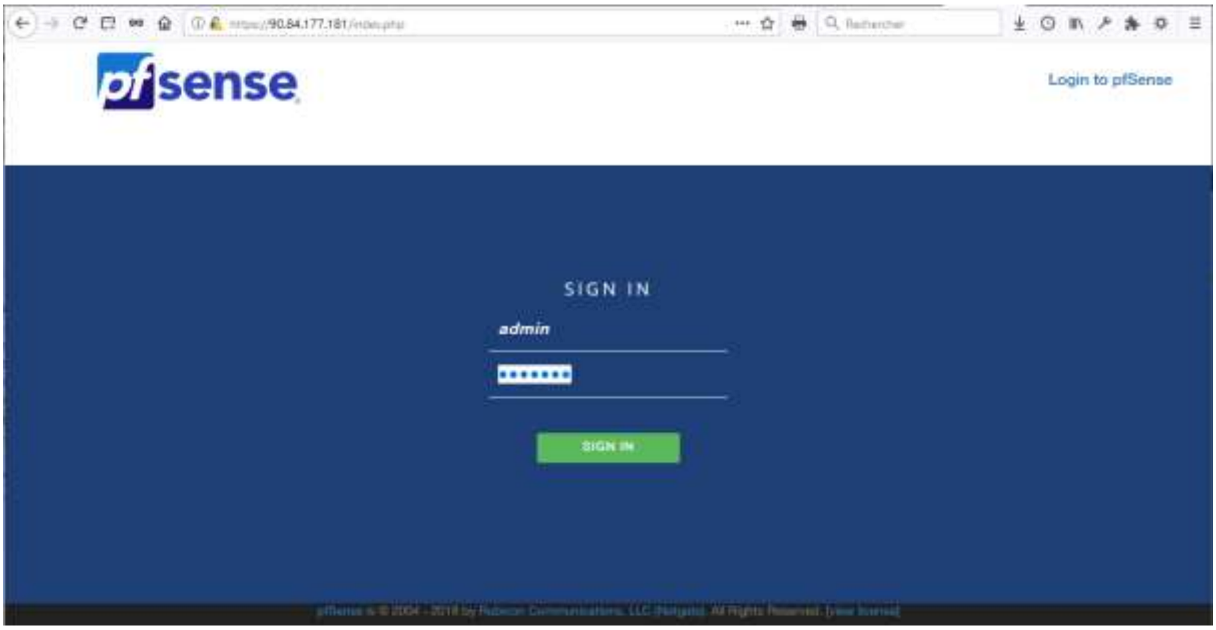
Attention : risque probable de sécurité

Firefox a détecté une menace de sécurité potentielle et n'a pas poursuivi vers 90.84.177.181. Si vous accédez à ce site, des attaquants pourraient dérober des informations comme vos mots de passe, courriels, ou données de carte bancaire.

En savoir plus…

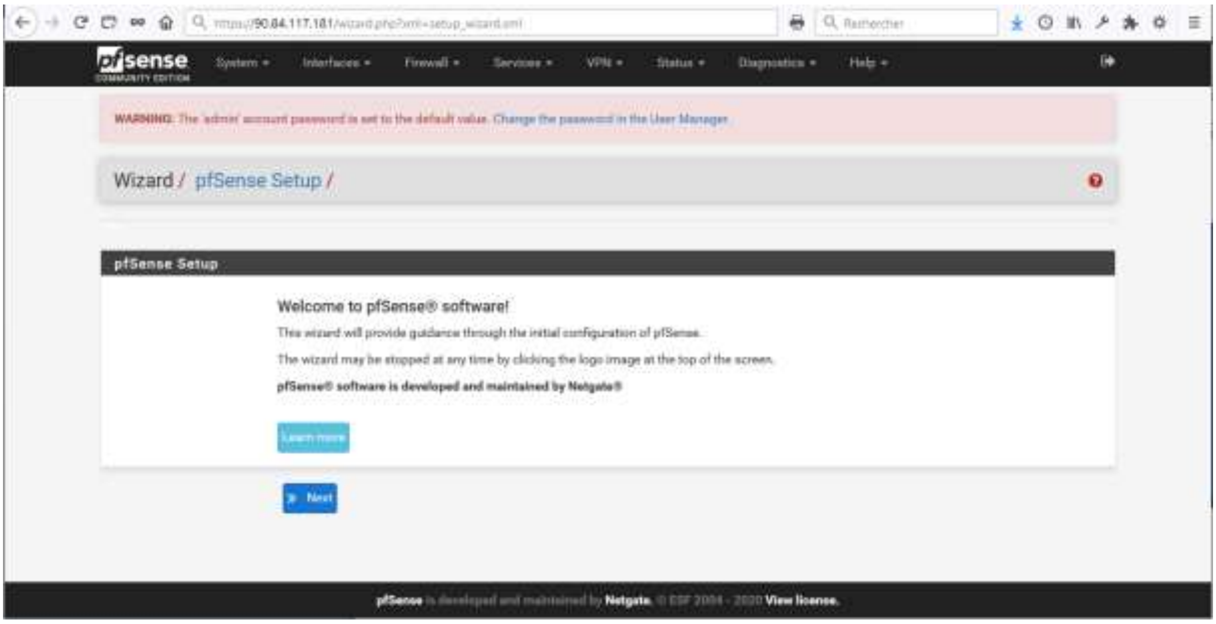
Retour (recommandé)   Avancé…

At initial configuration, the webconfigurator SSL certificate is a default self-signed certificate so you need to tell your browser to accept this untrusted certificate to display login page and authenticate with default credentials (username=admin and password=pfsense):



pfSense is © 2004 - 2018 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]

After first login it’s strongly recommended to **customize the admin password** before doing anything else especially when your webconfigurator is accessible by anyone on the internet through EIP address.
You can do this by running the “Setup Wizard” which will also allow you to start configuring your pfSense instance for you own purpose.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Welcome to pfSense® software!

This wizard will provide guidance through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

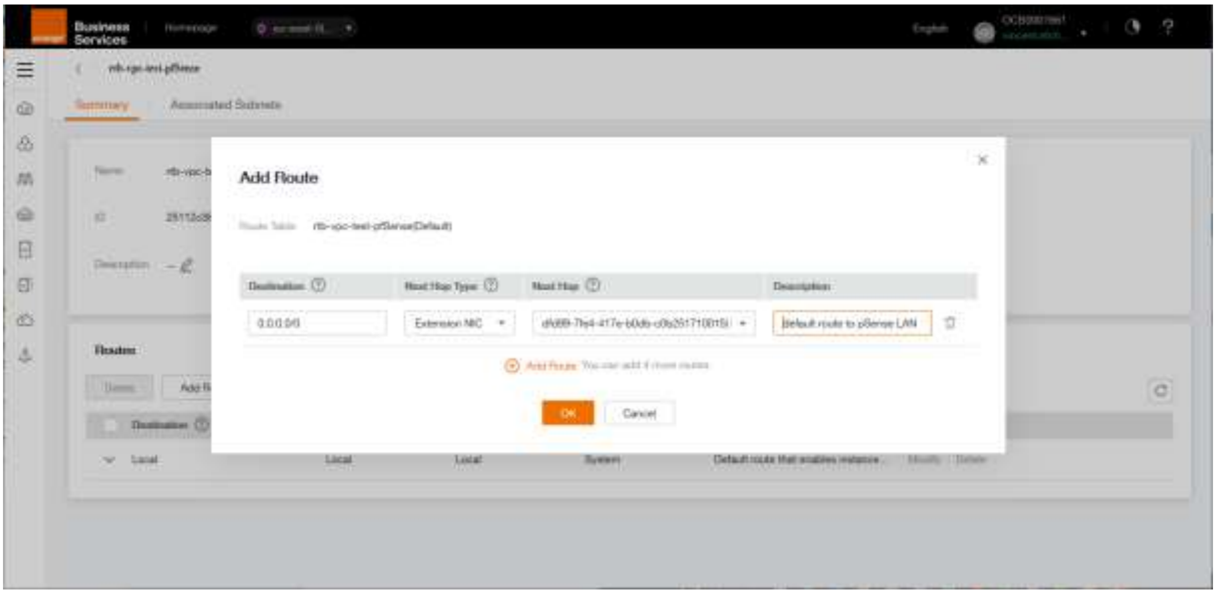
pfSense® software is developed and maintained by Netgate®

pfSense is developed and maintained by **Netgate.** © ESF 2004 - 2020 **View license.**

For further configuration information you can use pfSense online documentation:
https://docs.netgate.com/

4. VPC route table configuration to allow protected ECS to use pfSense as an Internet NAT gateway

In order to use pfSense as an Internet NAT gateway for protected ECS deployed on subnet “in” of the VPC you need to add a custom route in the VPC route table to send the internet traffic from the protected ECS attached to subnet “in” to the LAN network interface of your pfSense ECS:

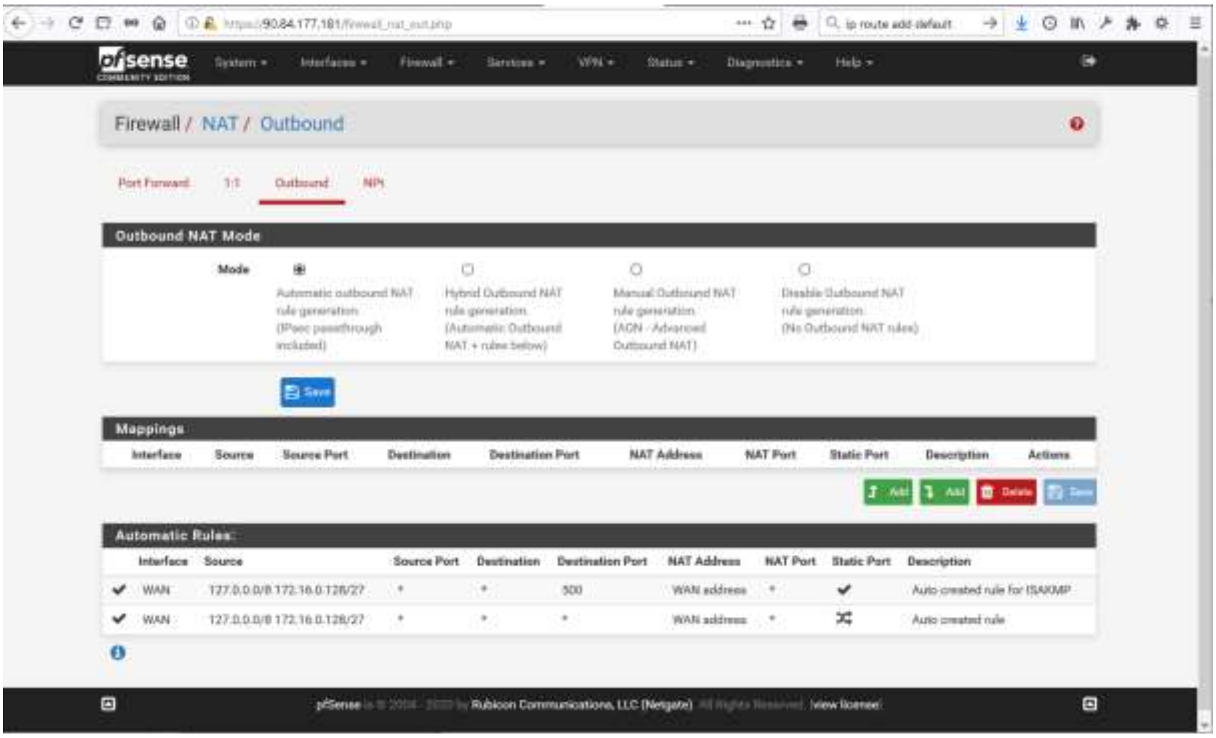


Add Route

Route Table rtb-vpc-test-pfSense(Default)

Destination	Next Hop Type	Next Hop	Description
0.0.0.0/0	Extension NIC	dfd69-7fe4-417e-b0db-c0b25171001[illegible]	Default route to pfSense LAN

In pfSense webconfigurator verify that automatic outbound NAT rule generation is selected and that a rule with subnet “in” exists on WAN interface:



Firewall / NAT / Outbound

Outbound NAT Mode

Mode: ● Automatic outbound NAT rule generation. (IPsec passthrough included) ○ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below) ○ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT) ○ Disable Outbound NAT rule generation. (No Outbound NAT rules)

Mappings

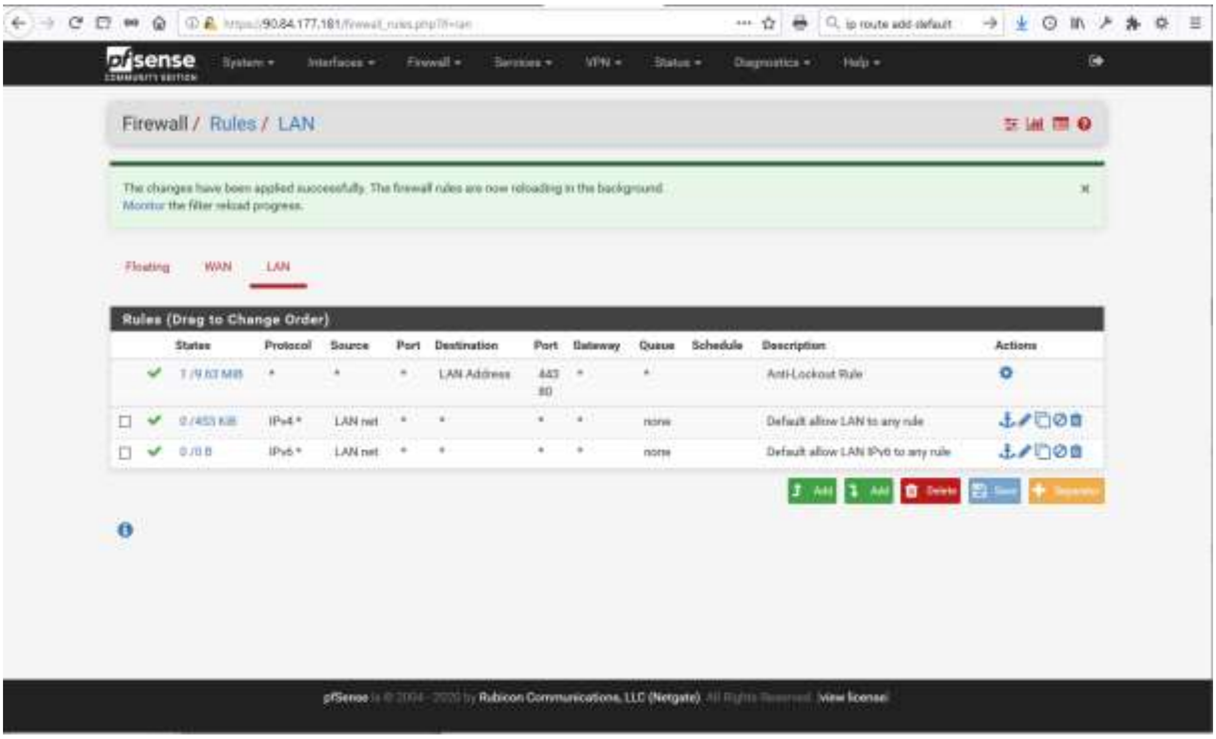
Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions

Automatic Rules:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 172.16.0.128/27	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 172.16.0.128/27	*	*	*	WAN address	*	⤮	Auto created rule

https://90.84.177.181/firewall_nat_out.php
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Port Forward
1:1
Outbound
NPt
Save
Add
Add
Delete
Save
pfSense is © 2004 - 2020 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]

In pfSense webconfigurator verify that a firewall rule exists on LAN interface to allow traffic on LAN net:



https://90.84.177.181/firewall_rules.php?if=lan

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules (Drag to Change Order)

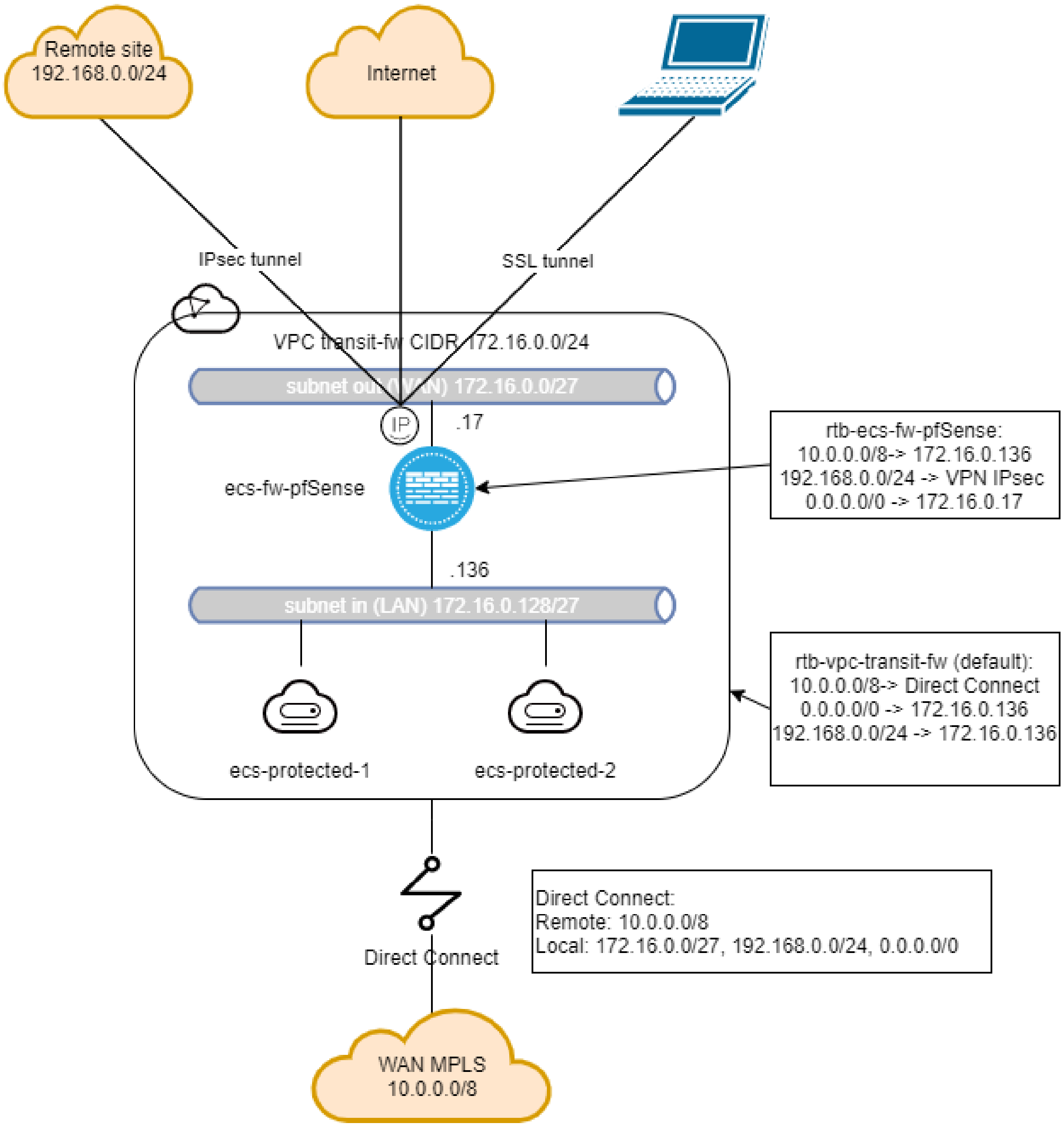
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1 /9.63 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
□	✓	0 /453 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

pfSense is © 2004 - 2020 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]

Now you can deploy protected ECS on subnet “in” which will use pfSense instance as an Internet NAT gateway and define some fine-tuned firewall rules to filter egress and ingress internet traffic for them.

5. pfSense network design on Flexible Engine examples

5.1. Single VPC

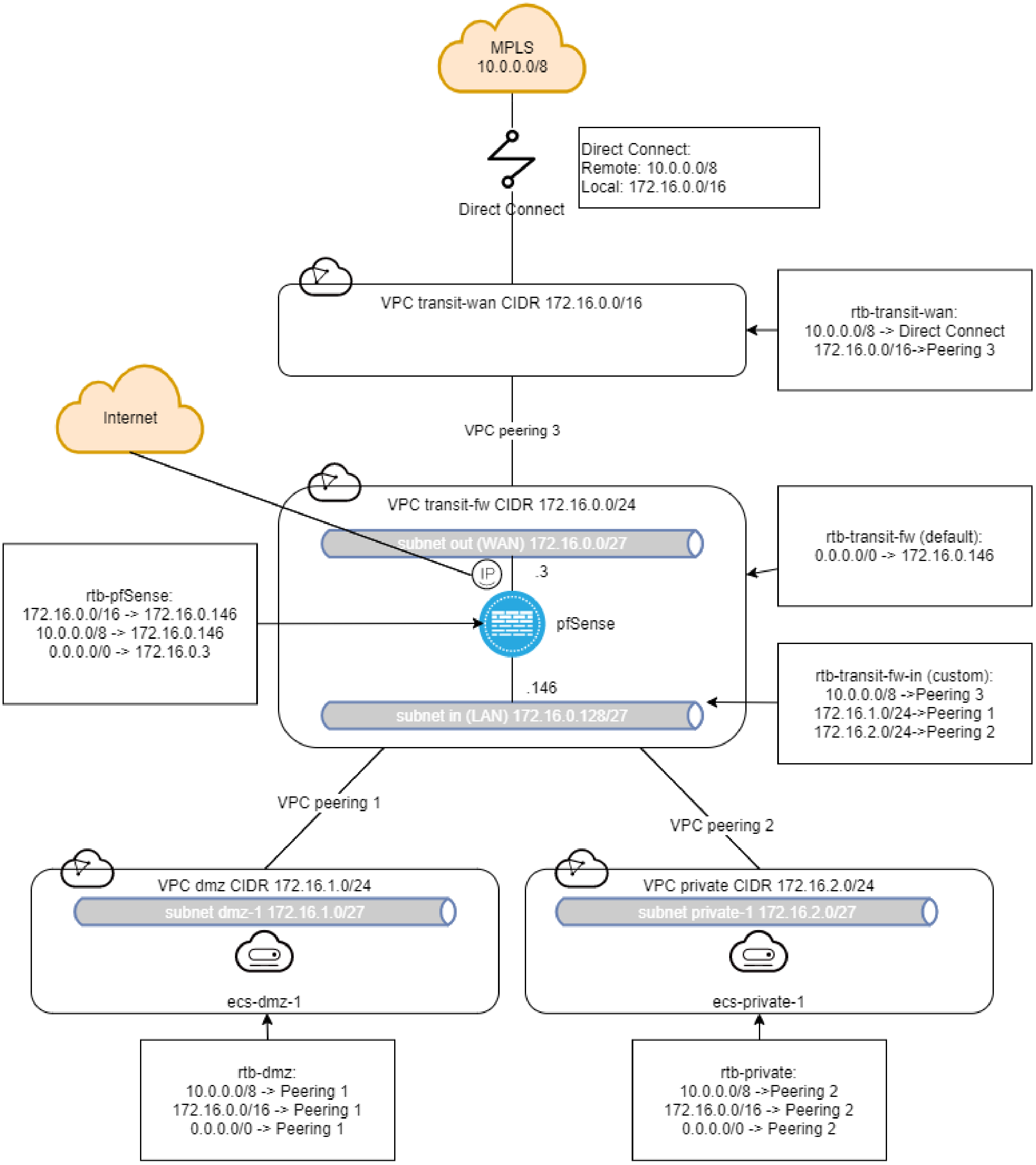


In this example pfSense instance is used for several purposes:

- It allows ingress and egress internet traffic for the protected ECS in the VPC
- It allows ingress and egress internet traffic for WAN MPLS resources
- It allows interconnect between a Remote site and protected ECS in the VPC and WAN MPLS resources though an IPsec tunnel
- It allows access to the protected ECS in the VPC, Remote site and WAN MPLS resources to nomad users through a SSL tunnel

Please note that, in this configuration, traffic between protected ECS in the VPC and MPLS WAN resources is not filtered by the pfSense instance.

5.2.Multiple VPC



In this advanced example pfSense instance is used to filter all the traffic between the all the VPCs, the MPLS WAN and Internet.

For this, we introduce the “Subnet Level Based Routing” concept by creating a custom route table attached to subnet “in” of the transit-fw VPC.

In the default route table of the transit-fw VPC, there is only a default route to send all the traffic entering the VPC to the LAN interface of pfSense instance.

All the routes toward the other VPCs are set in the custom route so that the traffic going out from the VPC can be routed only after being filtered.

6. FAQ

How to associate several public IP addresses to pfSense WAN interface?

You can add extra WAN network interfaces with EIP bound to your pfSense instance:
https://docs.prod-cloud-ocb.orange-business.com/en-us/usermanual/ecs/en-us_topic_0092497777.html
https://docs.netgate.com/pfsense/en/latest/routing/multi-wan.html

You can also use virtual IPs with EIPs bound associated with one WAN network interface:
https://docs.prod-cloud-ocb.orange-business.com/usermanual/vpc/en-us_topic_0097594610.html
https://docs.netgate.com/pfsense/en/latest/firewall/virtual-ip-address-feature-comparison.html

Is it possible to use pfSense to filter traffic between subnets in a VPC?

No, it’s not possible. Only FE Network ACL feature allows inter-subnet filtering.

Is it possible to set a pfSense High Availability cluster in Flexible Engine?

No, it’s not possible. Flexible Engine SDN doesn’t support CARP protocol.