

## Sprint 2 - Installatie- en configuratiehandleidingen

### Configuratie passwordless ssh naar de firewall vanuit ICT linux

We openen een terminal venster in de ICT linux desktop.

We gaan een rsa key genereren zodat we zonder paswoord kunnen inloggen. We gebruiken daar het volgend commando voor.

```
# ssh-keygen -f pfsense -t rsa -b 4096
```

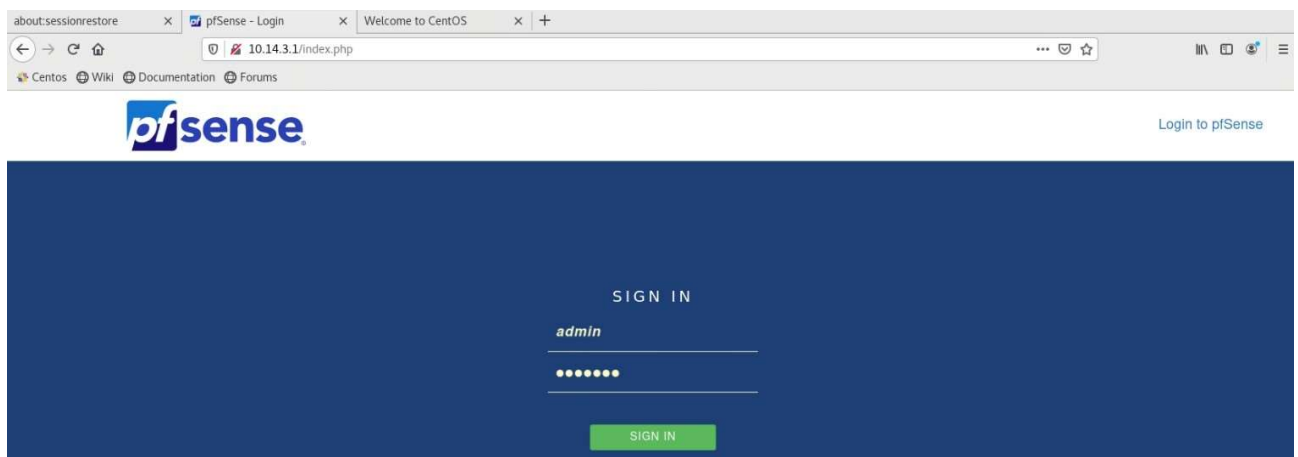
Er wordt gevraagd om een passphrase opgegeven. Dit doen we niet.

De -f in het commando staat voor de filename die je wilt geven, de -t voor het type, en de -b voor bytes voor de grootte van de key.

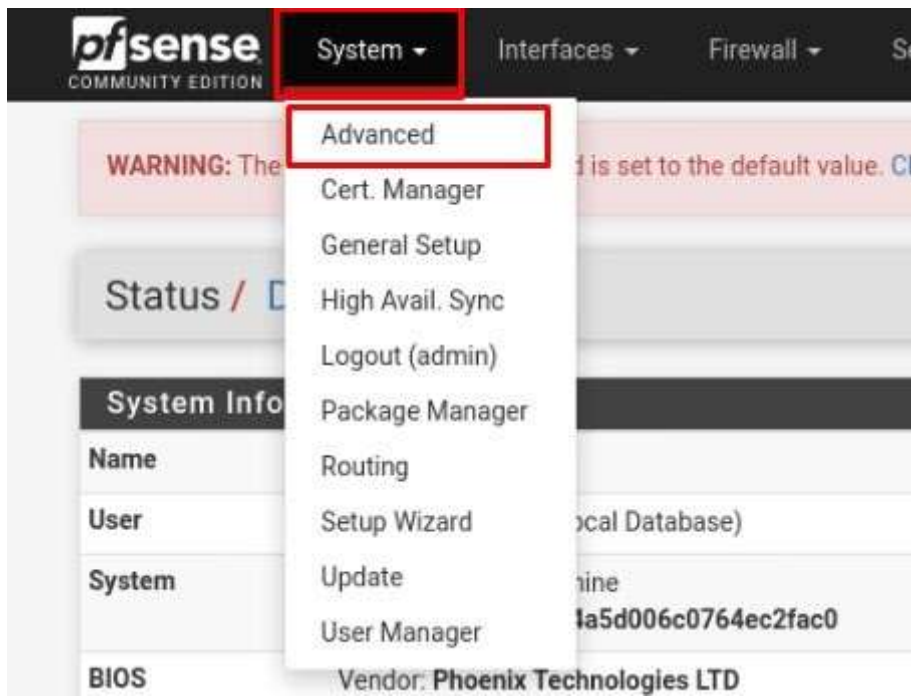
Nu met bovenstaand commando zijn er 2 key gemaakt 1 public en 1 private. De public met (.pub) extensie. Maar deze keys staan nu gewoon los in de homefolder. Deze gaan we nu verplaatsen naar de .ssh map. Volg onderstaand commando.

```
# cp pfs* /home/ICT/.ssh
```

Nu gaan we inloggen op de GUI van de firewall om de connectie toe te staan met een rsa key. Dus open je webbrowser en geef het IP van de default gateway in!



Klik sign in!



Navigeer naar System / advanced

**Secure Shell**

**Secure Shell Server** ☒ Enable Secure Shell

**SSHd Key Only** Public Key Only

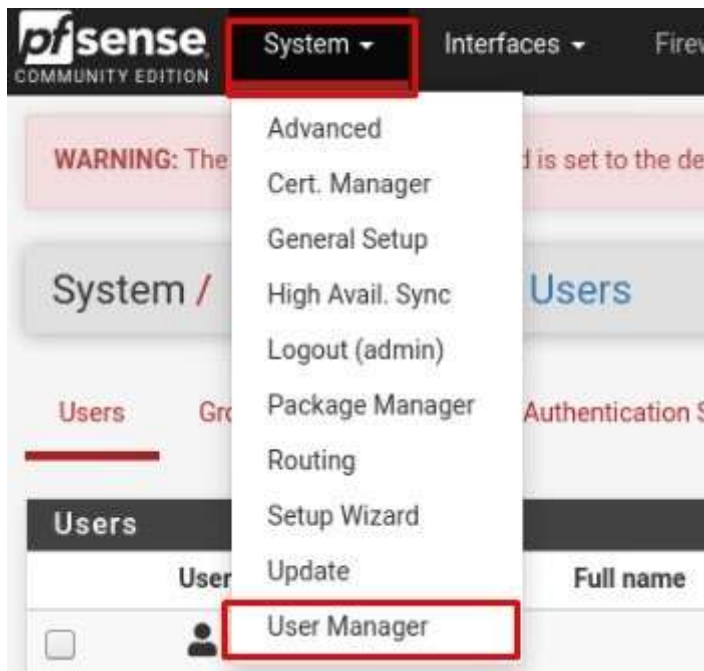
When set to *Public Key Only*, SSH access requires authorized keys and these keys must be access. If set to *Require Both Password and Public Key*, the SSH daemon requires both authentication. The default *Password or Public Key* setting allows either a valid password or a valid authorized

**Allow Agent Forwarding** ☐ Enables ssh-agent forwarding support.




**SSH port** 22

Note: Leave this blank for the default of 22.

Enable secure shell en zet de login op public key only! & save het bestand!



Navigeer nu naar de usermanager onder system / User Manager

<input type="checkbox"/>	ICT	✓	admins	
<input type="checkbox"/>	VPNuser	✓	admins	
<input type="checkbox"/>	admin	✓	admins	

Klik op edit op het account die waar je mee wilt dat deze kan inloggen. Als je nog geen account hebt klik dan op add, geef deze een naam en geef een password. (zie ook dat je de user toevoegt in de group admin)

Keys

Authorized SSH Keys

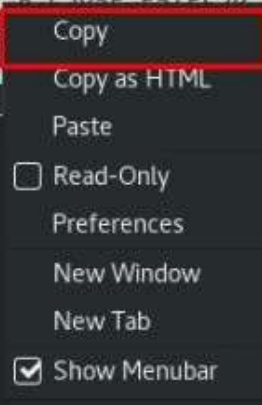
```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDbLoo1USy80QWN5nPT1D
mgp7gZ2XouMs958TKH5FHnPcvM9KG1ZoeW4GjLYVw/T
/R2rQUSVunk6ov57sHCrM
/P7s05xtuHBP7frDjNz6jzsJIvepFfSJ2w+W6EH92NGMHnXJv1
5m06v/7h1dvR
```

Enter authorized SSH keys for this user

IPsec Pre-Shared Key

Scroll naar "Keys" en dan zie je "Authorized ssh keys" hier moet je de public key plakken die je hebt aangemaakt op linux. Hiervoor gaan we terug naar de terminal.

```
[ICT@localhost ~]$ cat .ssh/pfsense.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDbLoo1USy80QWN5nPT1Dmgrp7gZ2XouMs958TKHSFHN
PcvM9KG1Zoew4GjLYVw/T/R2rQUSVunk6ov57sHCrm/P7s05xtuHBP7frDjNz6jzsJIvepFfSJ2w+W6E
H92NGMHnXJv15mq6x/7hldy8/e/tBHGzF7aKZ1yMp+gLHygIFv4A+KFTUTJ5Iwb415NZlrIJzkv7TE6A
n5y+YK3BzJuctV/rQAwDSMU87RrT8cgEWZM7CI5lYp0m//yHbiEn061dF9IIUscqsCB+624VNaRx9pQl
IJe+65WRYpHoD0k4fWki/0cSvA24E1LM4lhBrtdyBYPThLPYWNPAf7wF4WGCEvqB/sZ0arVaLUzVPqIr
XeLnW13g8ItP9w0UxbjlRUY6bkLVGQr44e+++BUJQ0cTURglpv6eJo7NcrDyPkd5I/ncQVCGEi6YSWF
VzVxp7Xxqi0P/LkcwTpmPl89TKB7mtJ1+cNZILGdVICdqqAPRqxGIwpsRCfre2cJR2k0CnV0J94enbSG
nwElbj07tgQal7DrxzVC...loafN/9VqT+vZoI8YzZ+Tu+2NqBN2pdE2rC6UbG4TgZ
LvKED+HvR2pwyqbWco+P...PMGWwemHTal2/cp4dondUkKlmnkFf4NvvpeSor0xAci
7w== ICT@localhost.s
[ICT@localhost ~]$
```

A context menu is overlaid on the terminal text, with 'Copy' highlighted in a red box. Other options include 'Copy as HTML', 'Paste', 'Read-Only' (unchecked), 'Preferences', 'New Window', 'New Tab', and 'Show Menubar' (checked).

Voer het commando `cat .ssh/pfsense.pub` uit

Kopieër de tekst en plak deze in het veld op de firewall. & sla de user op!

Nu moet je kunnen inloggen zonder password!

```
ICT@localhost:~
File Edit View Search Terminal Help
[ICT@localhost ~]$ ssh ICT@10.14.3.1
[2.5.0-RELEASE][ICT@pfSense.home.arpa]/home/ICT: echo succes
succes
[2.5.0-RELEASE][ICT@pfSense.home.arpa]/home/ICT: 
```

### Enable WAN SSH login

Navigeer op de firewall naar Firewall/rules/WAN

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ **Firewall ▾** Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is... Change the password in the User Manager.

Firewall / Rules / WAN

Floating **WAN** KLASSEN SERVERS DIRECTIE DMZ OpenVPN

Aliases  
NAT  
**Rules**  
Schedules  
Traffic Shaper  
Virtual IPs

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN connecteren naar ICT LAN wizard	

Add Add Delete Save Separator

Hier gaan we een regel toevoegen! Dus klik op add!

Zor ger voor dat de basis rules er als volgend uitzien.

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN connecteren naar ICT LAN wizard	

Add Add Delete Save Separator

Zorg er voor dat de basis rules er als volgend uitzien.

**Edit Firewall Rule**

**Action**   
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface**   
Choose the interface from which packets must come to match this rule.

**Address Family**   
Select the Internet Protocol version this rule applies to.

**Protocol**   
Choose which IP protocol this rule should match.

Zet de destination op "this firewall self"

En de destination port op ssh (22)

**Destination**

Destination ☐ Invert match This firewall (self) Destination Address /

**Destination Port Range** SSH (22)  SSH (22)

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.











Klik op save & apply changes!






Firewall / Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background.  
[Monitor the filter reload progress.](#)

Floating **WAN** KLASSEN SERVERS ICT SECRETERIAAT DIRECTIE DMZ OpenVPN

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN connecteren naar ICT LAN wizard	    
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	This Firewall	22 (SSH)	*	none			    

 Add  Add  Delete  Save  Separator

Nu zetten we de Linux desktop uit en zetten we deze in het routed netwerk gekregen van de pxl.

ICT-Linux Desktop

Summary Monitor Configure Permissions Datastores

Powered Off

Guest OS: CentOS 8 (64-bit)  
Compatibility: ESXi 6.7 and later (VM version 10.0.0)  
VMware Tools: Not running, version:11296 (64-bit)  
[More info](#)

DNS Name: localhost.sso1.local  
IP Addresses:  
Host: compute2.px1.local

Launch Web Console  
Launch Remote Console

VM Hardware

> CPU	2 CPU(s)
> Memory	4 GB, 0 GB mem
> Hard disk 1	25 GB
> Network adapter 1	Local Network 24-
CD/DVD drive 1	Disconnected
> Video card	8 MB
VMCI device	Device on the virtu
	virtual machine cor
> Other	Additional Hardwa
Compatibility	ESXi 6.7 and later (

Edit Settings...

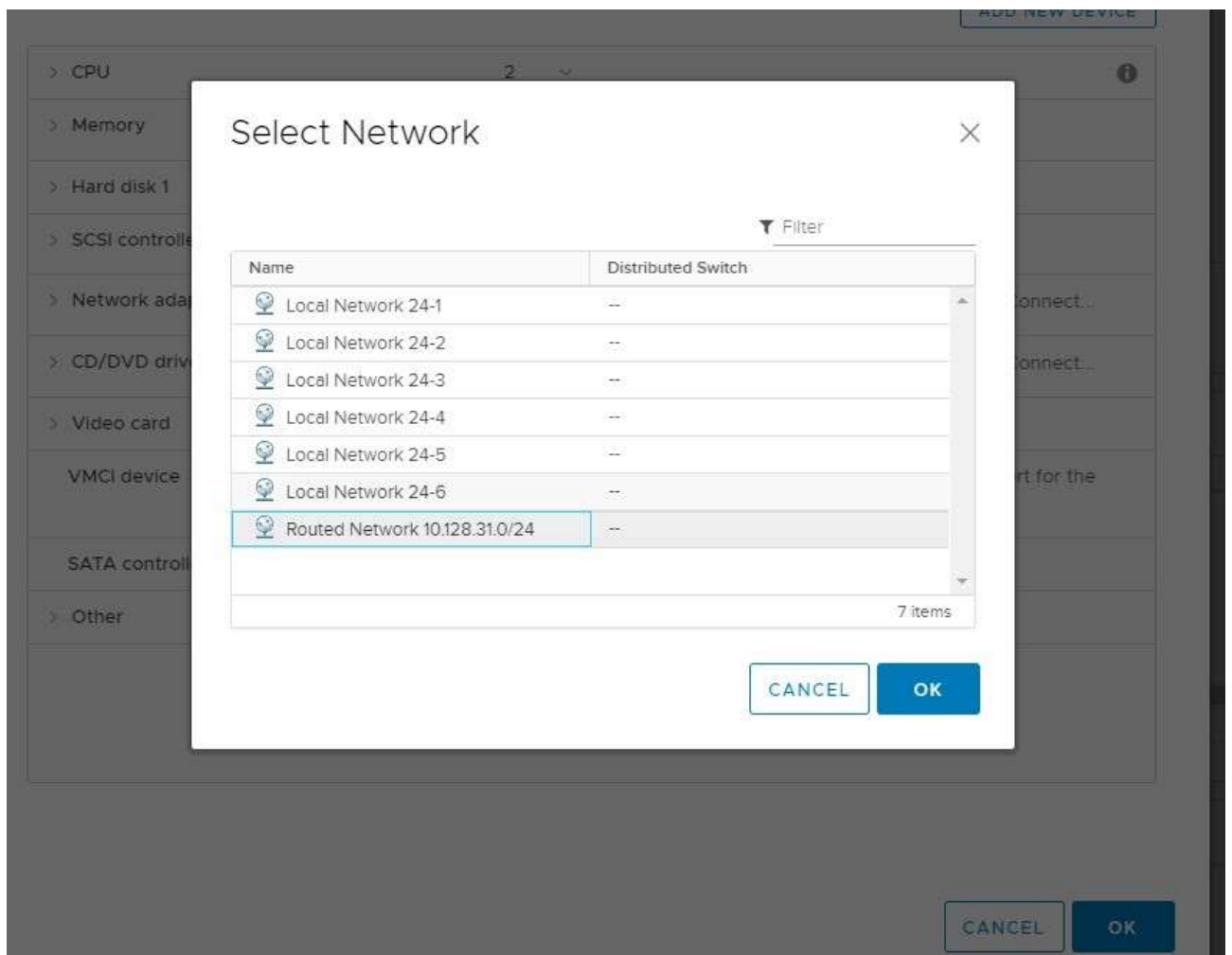
Related Objects

Host: compute2.px1.local

ACTIONS

- Power
- Guest OS
- Snapshots
- Open Remote Console
- Migrate...
- Clone
- Fault Tolerance
- VM Policies
- Template
- Compatibility
- Export System Logs...
- Edit Settings...
- Move to folder...
- Rename...
- Edit Notes...
- Tags & Custom Attributes
- Add Permission...
- Alarms
- Remove from Inventory
- Delete from Disk
- Update Manager

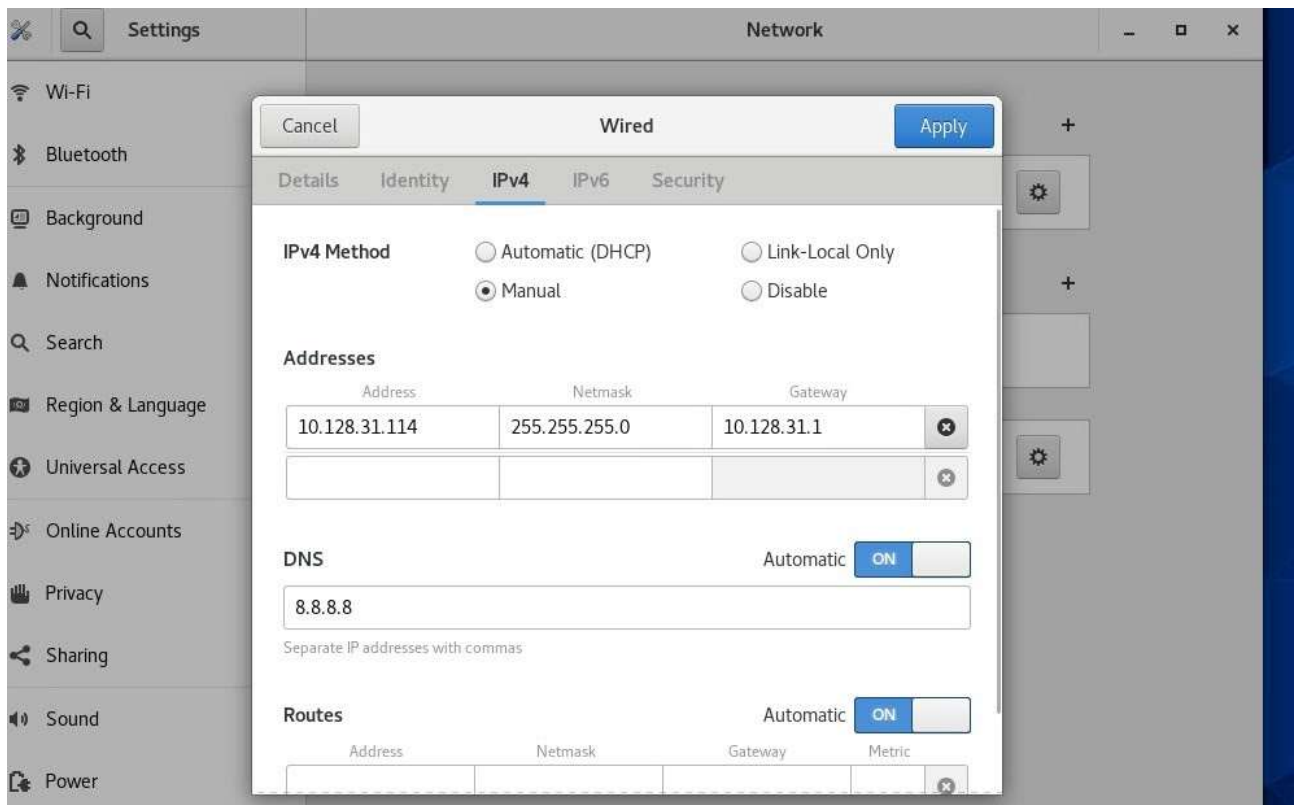




Zet nu je VM terug aan!

Zie dat je kan je desktop een werkend een ip hebt gegeven! En dat je kan pingen.





Nu gaan we kijken of we ssh verbinding kunnen maken

Dus # ssh ICT@"WAN adres van de Firewall" ons geval 10.128.31.14

```

ICT@localhost:~
File Edit View Search Terminal Help
[ICT@localhost ~]$ ssh ICT.....
.....: Name or service not known
[ICT@localhost ~]$ ssh ITC
ssh: Could not resolve hostname itc: Name or service not known
[ICT@localhost ~]$ ssh ICT@10.128.31.14
The authenticity of host '10.128.31.14 (10.128.31.14)' can't be established.
ED25519 key fingerprint is SHA256:RAkYM4JhT44jx5uNtnQKdMEf4lGtqnaUxJ//tEvtrC0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.128.31.14' (ED25519) to the list of known hosts.
[2.5.0-RELEASE][ICT@pfSense.home.arpa]/home/ICT:

```

En ook dit werkt!