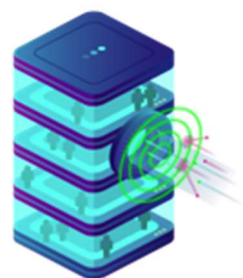


Documentation UF infrastructure réseaux
Projet 2

Ynov Campus

Victor-Emmanuel Sedaros

Samy Lacombe



pfSense

Le Dashboard central de pfSense nous donne des informations sur le système, l'état des interfaces.

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.10.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: a89e63938ae970929509
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.5.0-RELEASE (amd64) built on Tue Feb 16 08:56:29 EST 2021 FreeBSD 12.2-STABLE Version 2.5.1 is available. Version information updated at Tue May 4 16:16:24 CEST 2021
CPU Type	Intel(R) Core(TM) i7-9700K CPU @ 3.60GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	03 Hours 15 Minutes 25 Seconds
Current date/time	Tue May 4 17:30:48 CEST 2021
DNS server(s)	• 127.0.0.1
Last config change	Tue May 4 17:30:17 CEST 2021
State table size	0% (0/45000) Show states
MBUF Usage	0% (3330/1000000)

Netgate Services And Support

Contract type: [Community Support](#)
[Community Support Only](#)

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7/365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#).

Interfaces

WAN	1000baseT <full-duplex>	192.168.1.100
LAN	1000baseT <full-duplex>	192.168.10.1
DMZ	1000baseT <full-duplex>	10.0.0.1

Afin de vérifier l'état des Interfaces, il faut voir dans status > Interfaces

Status / Interfaces

WAN Interface (wan, em0)

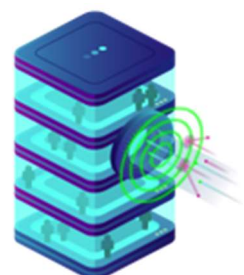
Status	up
MAC Address	08:00:27:0f:76:ef
IPv4 Address	192.168.1.100
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80:a00:27ff:fe0f:76ef%em0
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	47060/48240 (3.43 MiB/2.10 MiB)
In/out packets (pass)	47060/48240 (3.43 MiB/2.10 MiB)
In/out packets (block)	0/6 (0 B/240 B)
In/out errors	0/0
Collisions	0

LAN Interface (lan, em1)

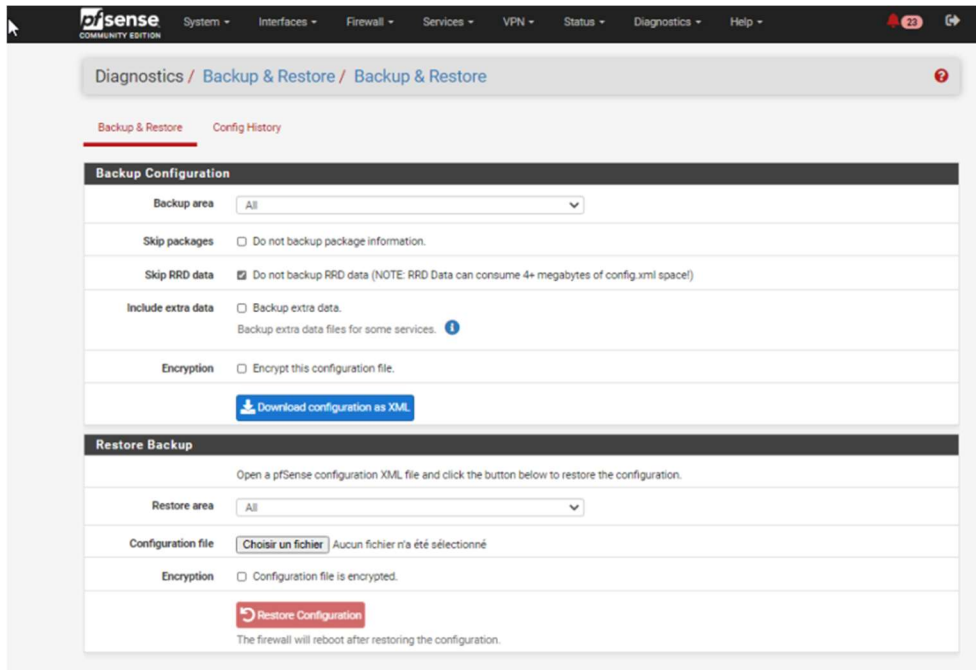
Status	up
MAC Address	08:00:27:06:12:af
IPv4 Address	192.168.10.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80:1:1%em1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	14243/18258 (895 KiB/9.69 MiB)
In/out packets (pass)	14243/18258 (895 KiB/9.69 MiB)
In/out packets (block)	0/5 (0 B/200 B)
In/out errors	0/0
Collisions	0

DMZ Interface (opt1, em2)

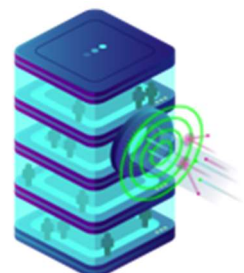
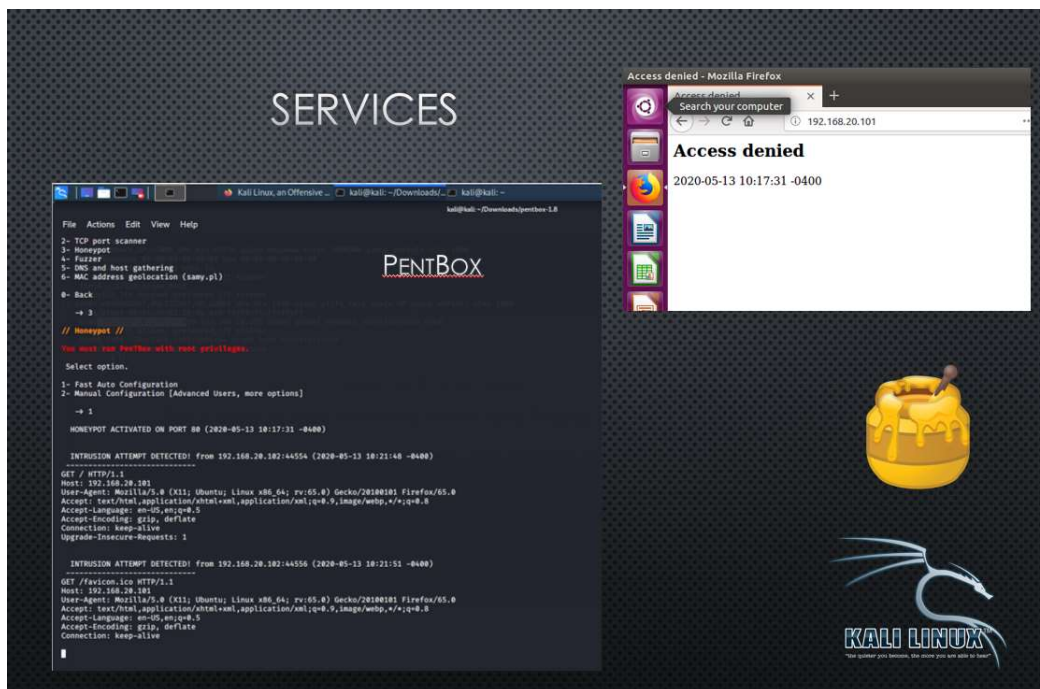
Status	up
MAC Address	08:00:27:77:3a:7c
IPv4 Address	10.0.0.1
Subnet mask IPv4	255.255.255.248
IPv6 Link Local	fe80:a00:27ff:fe77:3a7c%em2



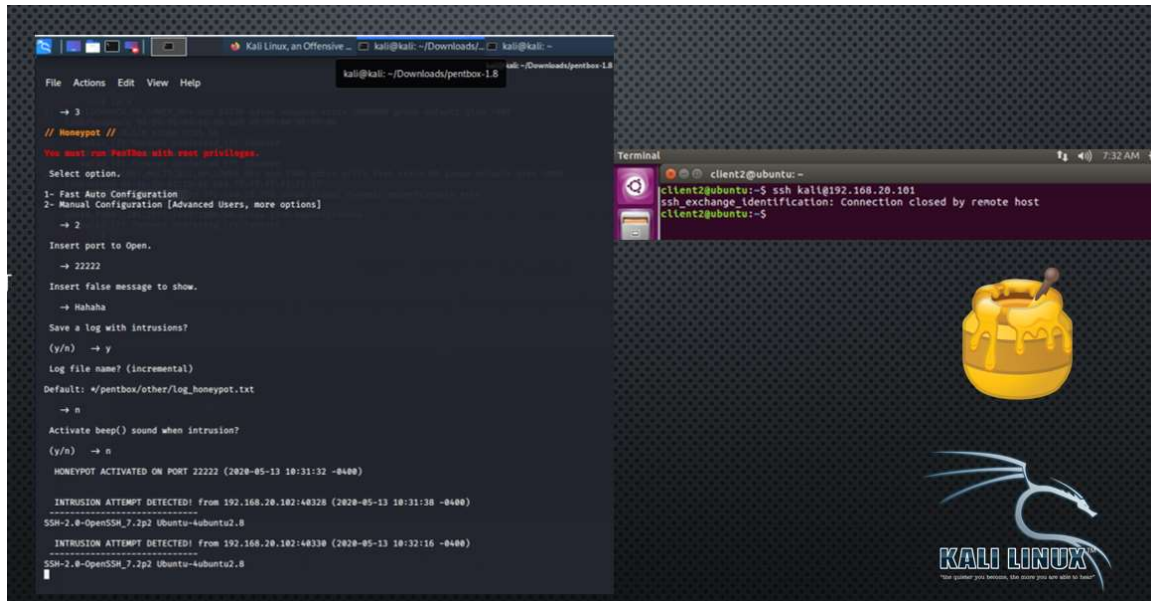
Pour effectuer un backup des configurations, la partie Diagnostics > backup and restore permet d'effectuer une sauvegarde des configurations actuelles



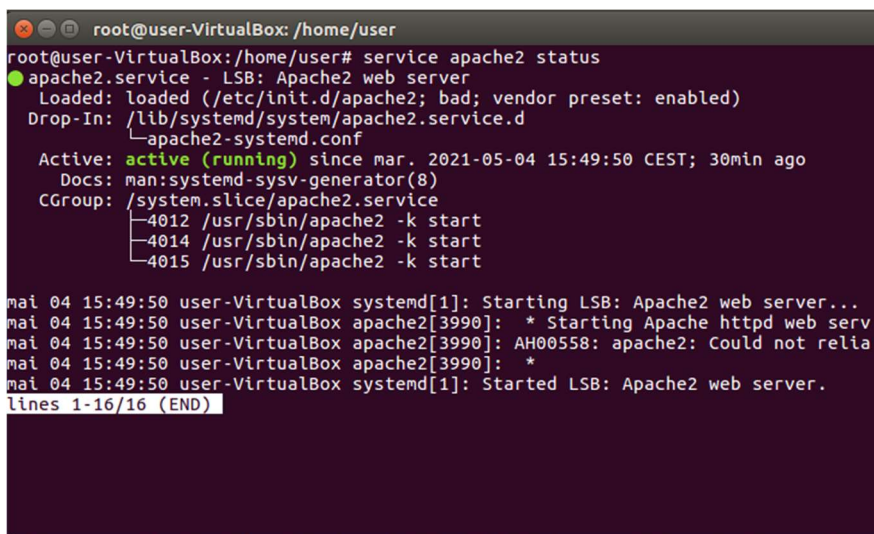
Afin de tester l'Honeypot, je me connecte à l'adresse IP du serveur sur le port 80, la connexion est refusée et je peux apercevoir un retour dans le prompt m'indiquant les informations de la machine attaquante.



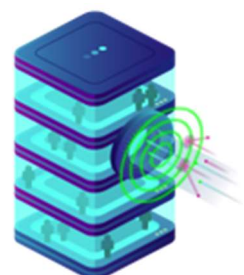
Cela est aussi valable pour l'accès en SSH, la connexion est refusée avec une alerte instantanée dans le prompt

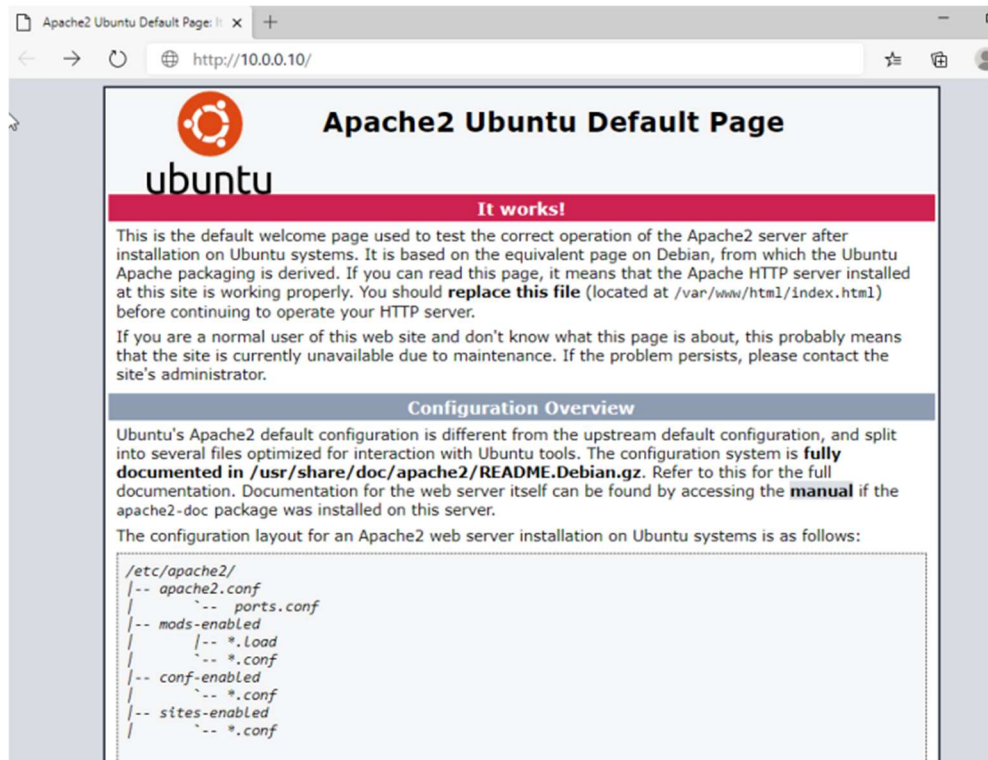


Pour checker si le service Web Apache est actif, il faut lancer la commande **service apache2 status** sur le serveur Web.

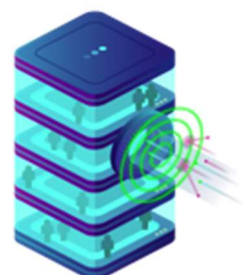
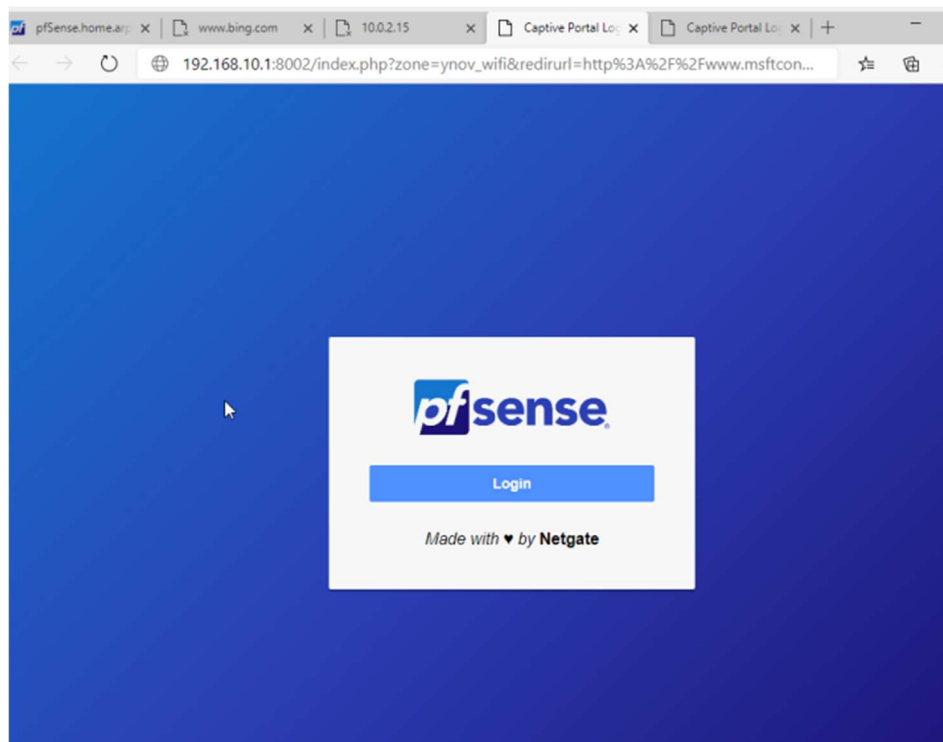


J'accède à la page web du serveur depuis le LAN et le WAN avec son IP : 10.0.0.10

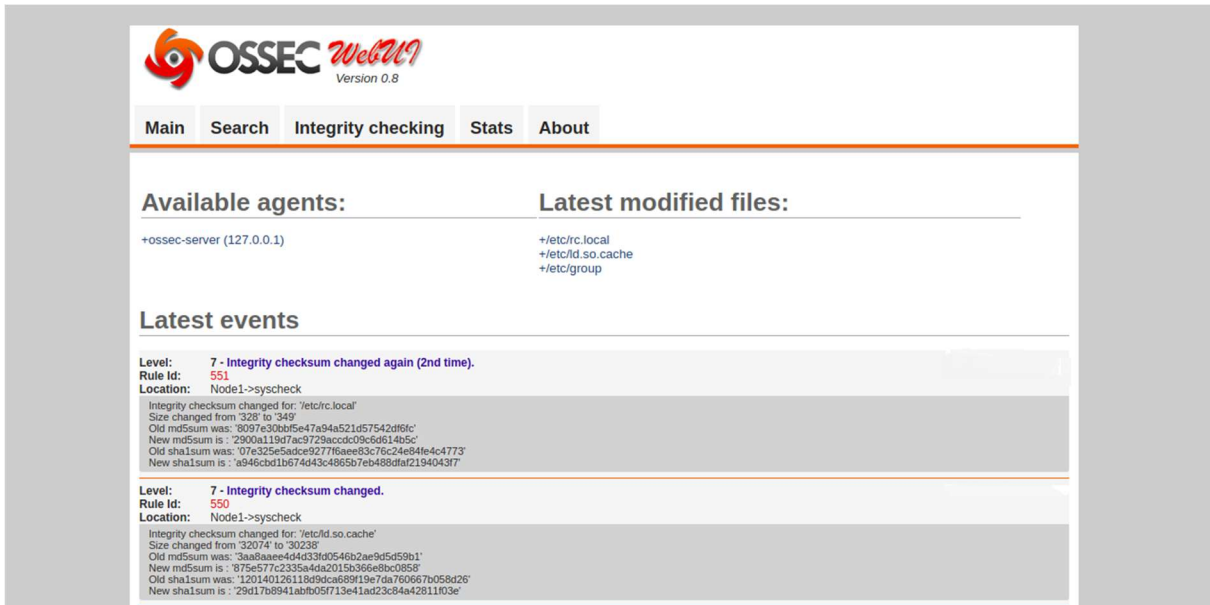




Afin de tester le portail captif, je lance une recherche sur un navigateur web, je suis automatiquement redirigé vers la page de portail captif qui me demande de m'authentifier avant



Pour la partie Ossec, on peut accéder à la webUI avec l'IP de HIDS en question.



The screenshot displays the OSSEC WebUI interface. At the top, the OSSEC logo and "Version 0.8" are visible. Below the logo is a navigation bar with tabs: Main, Search, Integrity checking, Stats, and About. The main content area is divided into three sections:

- Available agents:** Shows a single agent: "+ossec-server (127.0.0.1)".
- Latest modified files:** Lists three files: "+/etc/rc.local", "+/etc/ld.so.cache", and "+/etc/group".
- Latest events:** Displays two event entries, both at Level 7.

Event 1:

- Level: 7 - Integrity checksum changed again (2nd time).
- Rule Id: 551
- Location: Node1->syscheck
- Integrity checksum changed for: '/etc/rc.local'
- Size changed from '328' to '349'
- Old md5sum was: '8987e30bbf5e47a94a521d57542df6fc'
- New md5sum is: '2900a119d7ac9729accdc09c6d614b5c'
- Old sha1sum was: '07e325e5adce9277f6aee83c76c24e84fe4c4773'
- New sha1sum is: 'a946cbb1b674d43c4865b7eb488d1a219404317'

Event 2:

- Level: 7 - Integrity checksum changed.
- Rule Id: 550
- Location: Node1->syscheck
- Integrity checksum changed for: '/etc/ld.so.cache'
- Size changed from '32074' to '30238'
- Old md5sum was: '3aa8aaee4d4d33f00546b2ae9d5d59b1'
- New md5sum is: '875e577c2335a4da2015b366e8bc0858'
- Old sha1sum was: '120140126118d9dca689f19e7da760667b058d26'
- New sha1sum is: '29d17b8941abb0c9f713e41ad23c84e4281103e'

