INSTITUT UNIVERSITAIRE DES SCIENCES (IUS)

FACULTÉ DES SCIENCES ET DES TECHNOLOGIES (FST)

TITRE DU SUJET

Configuration d'un Pare-feu pfSense avec Cisco Packet Tracer.

<u>Cours : Réseau 2</u>

Étudiant : FABIEN Marie Beatrice

Professeur : Mr. Ismaël SAINT-AMOUR

Juin 2025

Projet 5 : Configuration d'un Pare-feu PfSense avec Cisco Packet Tracer

Objectifs du Projet

Dans Ce projet, on va :

1) Configurer un pare-feu **pfSense** dans Cisco Packet tracer pour sécuriser un réseau interne.

2) Comprendre les concepts de base des pare-feu, y compris les règles de filtrage, les NAT, les VLAN, et les services de sécurité.

3. Tester la connectivité et la sécurité du réseau en simulant des attaques et en vérifiant les règles de parefeu.

Livrables du Projet

1. **Diagramme de topologie réseau** : Schéma représentant la connexion entre les dispositifs internes, le pare-feu pfSense, et le réseau externe (Internet).
2. **Configuration complète du pare-feu** : Script ou document avec toutes les étapes de configuration de pfSense.
3. **Tests de sécurité** : Résultats des tests de connectivité et de sécurité pour valider les règles de pare-feu.
4. **Rapport technique** : Explication des règles de filtrage, des NAT, des VLAN, et des services de sécurité.
5. **Présentation** : Résumé des résultats du projet pour présentation en classe.

Rapport du Projet

Vous devez rédiger un rapport final contenant :

1. **La configuration réalisée** : Chaque étape de configuration de pfSense, y compris les règles de filtrage, les NAT, les VLAN, et les services de sécurité.
2. **Comparaison des fonctionnalités** : Différences entre les règles de filtrage basées sur les interfaces et les règles basées sur les VLAN.
3. **Importance du pare-feu** : Décrire pourquoi un pare-feu comme pfSense est essentiel pour la sécurité des réseaux et la protection contre les menaces externes.
4. **Limitations de la Simulation** : Mentionner que Cisco Packet Tracer simule le fonctionnement de pfSense mais ne reproduit pas entièrement les conditions réelles d'un réseau complexe.

Évaluation

Les critères d'évaluation incluent :

1. **La précision de la configuration** : Vérification que les règles de filtrage fonctionnent correctement et que le trafic est filtré selon les règles définies.
2. **L'analyse de sécurité** : Capacité à expliquer les règles de filtrage et leur impact sur la protection du réseau.
3. **La qualité du rapport** : Explication claire de la configuration et des conclusions tirées de l'expérience.
4. **Présentation des résultats** : Présentation en classe ou sous forme de diaporama pour partager les connaissances acquises.

1-Configurer un pare-feu pfSense dans Cisco Packet Tracer pour sécuriser un réseau interne.

Un **pare-feu** (ou **firewall** en anglais) est un **dispositif de sécurité réseau** conçu pour contrôler le trafic entrant et sortant d'un réseau informatique. Il agit comme une barrière entre un réseau interne fiable (par exemple un réseau d'entreprise) et un réseau externe non fiable (comme Internet), selon des règles de sécurité prédéfinies.

Le pare-feu a pour rôle de :

- **Filtrer le trafic réseau** selon des règles (adresses IP, ports, protocoles, etc.).
- **Bloquer les connexions non autorisées** et permettre celles qui sont sûres.
- **Prévenir les attaques** telles que les intrusions, les malwares, les scans de ports, etc.
- **Surveiller et enregistrer** les activités réseau suspectes.

Quelques types de Pare-feu.

1-Pare-feu à filtrage de paquets (Packet Filtering Firewall)

2. Pare-feu à inspection dynamique (Stateful Inspection Firewall)

3. Pare-feu applicatif (Application Layer Firewall ou Proxy)

4. Pare-feu personnel (ou logiciel)

5. Pare-feu matériel

6. Pare-feu de nouvelle génération (NGFW - Next Generation Firewall)

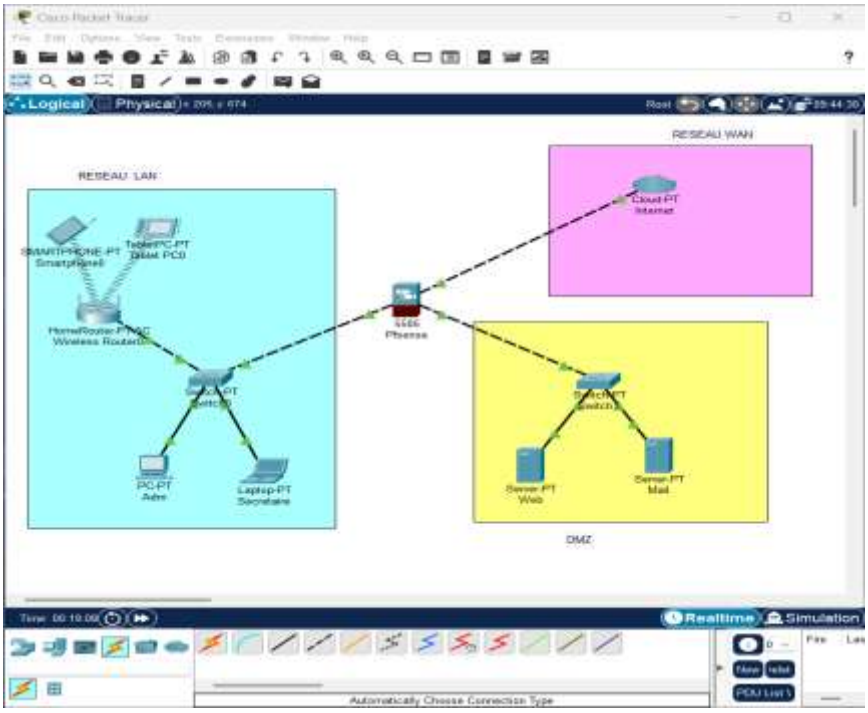
PfSense est un **pare-feu logiciel de type complet** basé sur **FreeBSD**. Il peut être installé sur un matériel dédié ou exécuté en tant que machine virtuelle.

PfSense peut intégrer des **fonctionnalités avancées**, comme :

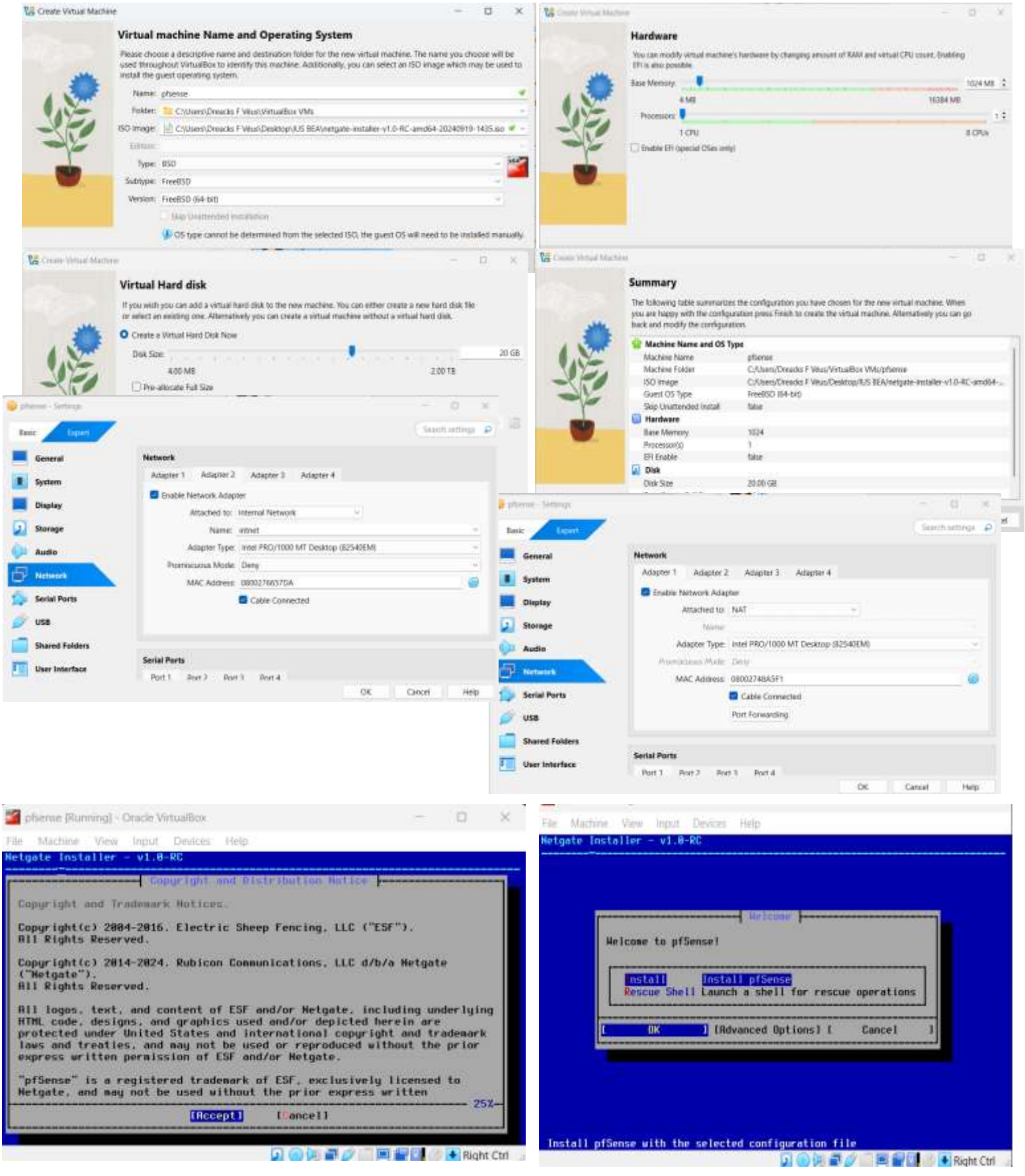
- IDS/IPS (Snort ou Suricata),
- VPN (IPsec, OpenVPN),
- Contrôle applicatif et filtrage web (via Squid, SquidGuard),
- Redondance et haute disponibilité (CARP),
- Portail captif, QoS, NAT avancé, etc.

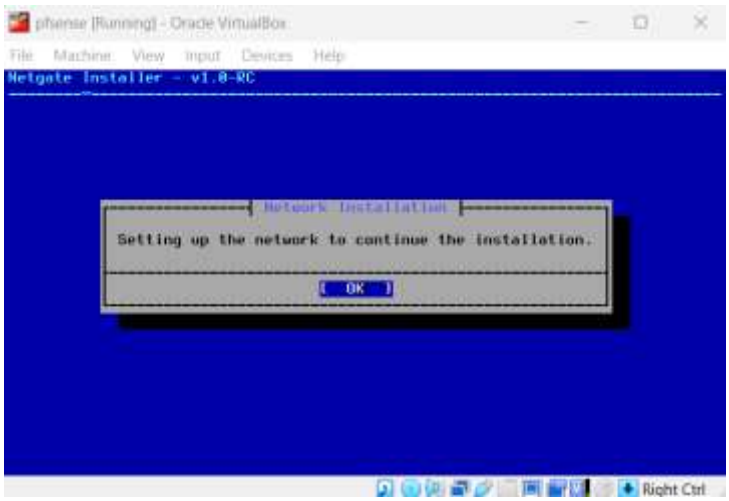
Exécution du Projet

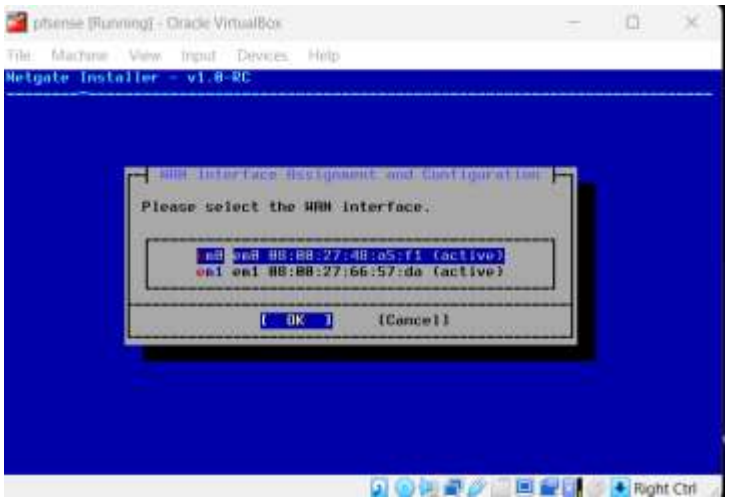
1-Topologie du projet

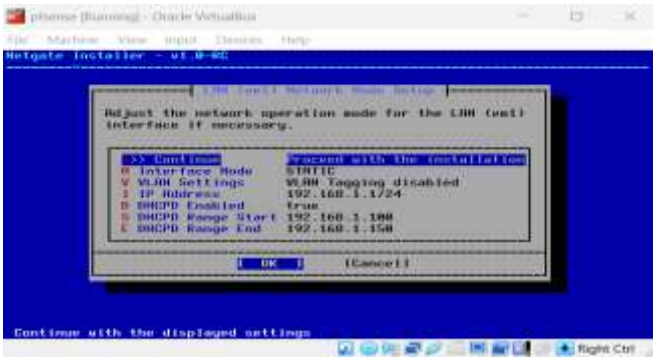


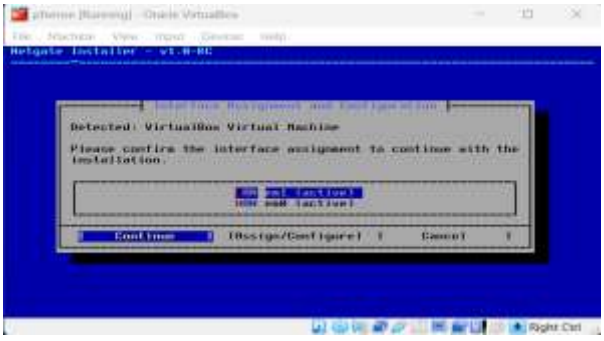
Installer et Configurer PfSense sur un VM

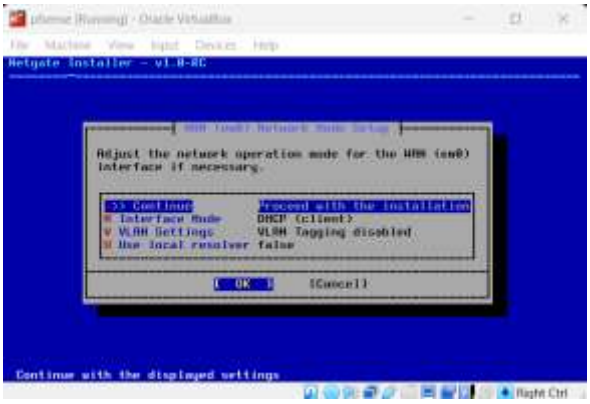


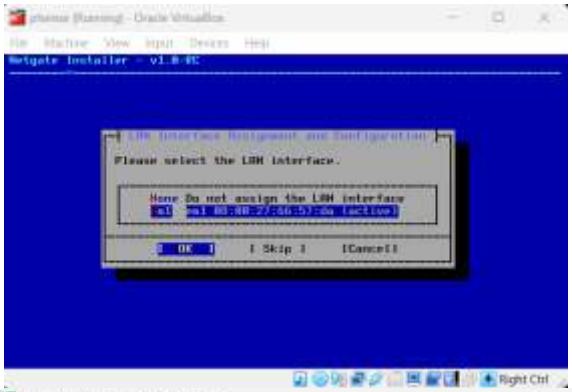

pfSense [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Netgate Installer - v1.0-RC
Network Installation
Setting up the network to continue the installation.
OK
Right Ctrl

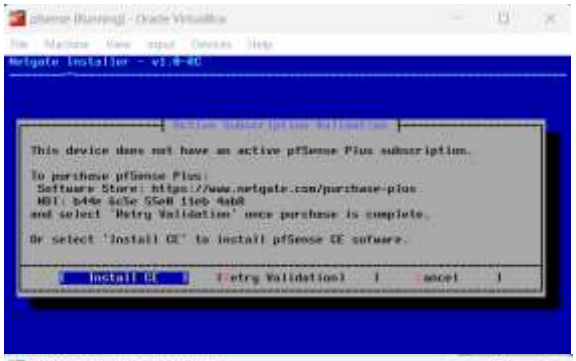

pfSense [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Netgate Installer - v1.0-RC
WAN Interface Assignment and Configuration
Please select the WAN interface.
em0 em0 08:00:27:48:a5:f1 (active)
em1 em1 08:00:27:66:57:da (active)
OK
Cancel
Right Ctrl

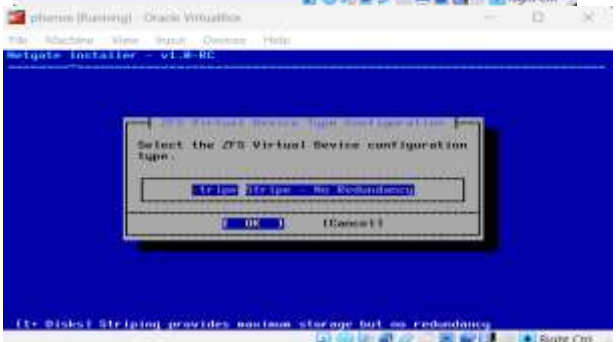

Netgate Installer - v1.0-RC
Adjust the network operation mode for the LAN (em1) interface if necessary.
>> Continue Proceed with the installation
I Interface Mode STATIC
V VLAN Settings VLAN Tagging disabled
I IP Address 192.168.1.1/24
D DHCPD Enabled true
S DHCPD Range Start 192.168.1.100
E DHCPD Range End 192.168.1.150
OK
Cancel
Continue with the displayed settings
Right Ctrl

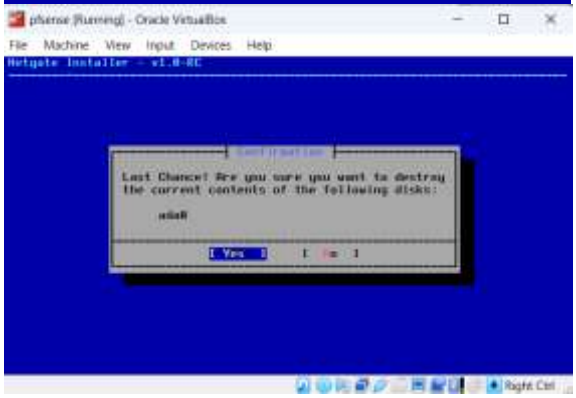

Netgate Installer - v1.0-RC
Detected: VirtualBox Virtual Machine
Please confirm the interface assignment to continue with the installation.
em0 em0 (active)
em1 em1 (active)
Continue
Assign/Configure
Cancel

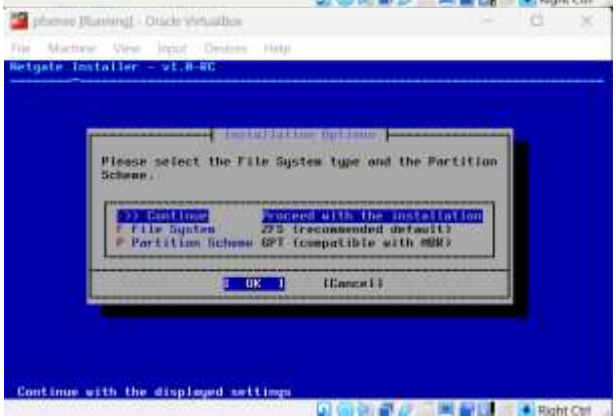

Netgate Installer - v1.0-RC
Adjust the network operation mode for the WAN (em0) interface if necessary.
>> Continue Proceed with the installation
I Interface Mode DHCP (client)
V VLAN Settings VLAN Tagging disabled
U Use local resolver false
OK
Cancel
Continue with the displayed settings
Right Ctrl

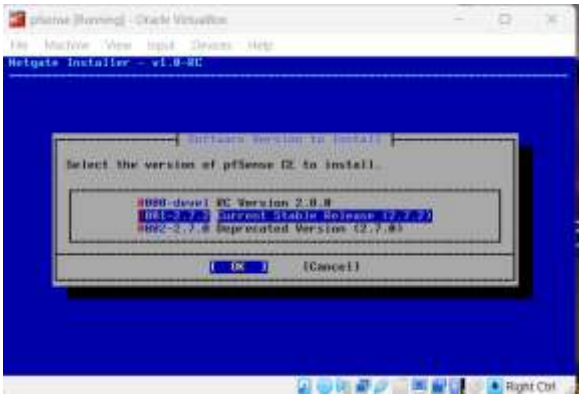

Netgate Installer - v1.0-RC
LAN Interface Assignment and Configuration
Please select the LAN interface.
None Do not assign the LAN interface
em1 08:00:27:66:57:da (active)
OK
Skip
Cancel
Right Ctrl

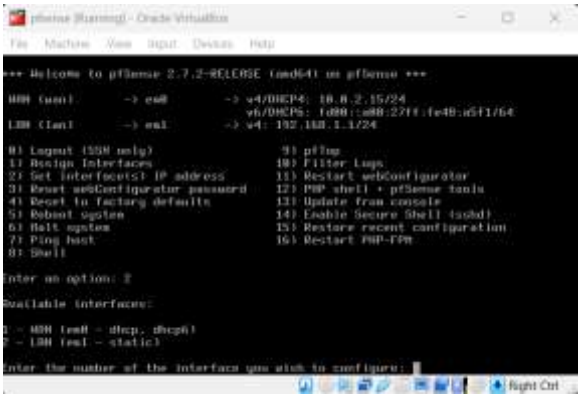

Netgate Installer - v1.0-RC
This device does not have an active pfSense Plus subscription.
To purchase pfSense Plus:
Software Store: https://www.netgate.com/purchase-plus
MAC: b44e 4c5e 55e0 11eb 4ab8
and select "Retry Validation" once purchase is complete.
Or select "Install CE" to install pfSense CE software.
Install CE
Retry Validation
Cancel

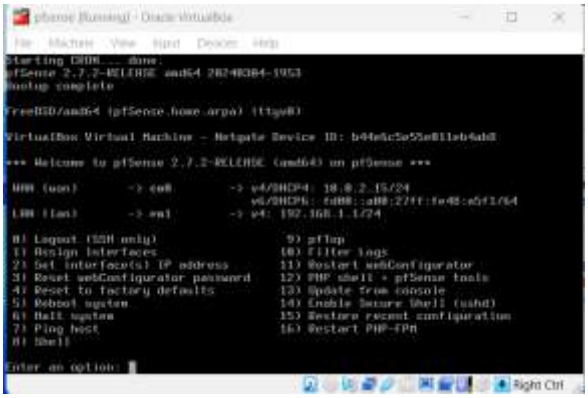

Netgate Installer - v1.0-RC
Select the ZFS Virtual Device configuration type.
stripe Stripe - No Redundancy
OK
Cancel
(1+ disks) Striping provides maximum storage but no redundancy
Right Ctrl

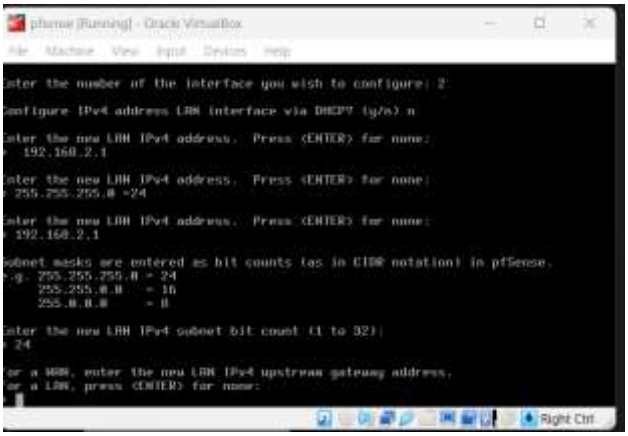

pfSense [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Netgate Installer - v1.0-RC
Last Chance! Are you sure you want to destroy the current contents of the following disks:
ada0
Yes
No
Right Ctrl

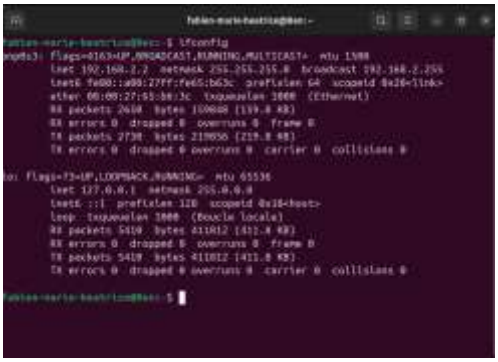

Netgate Installer - v1.0-RC
Installation Options
Please select the File System type and the Partition Scheme.
>> Continue Proceed with the installation
F File System ZFS (recommended default)
P Partition Scheme GPT (compatible with MBR)
OK
Cancel
Continue with the displayed settings
Right Ctrl

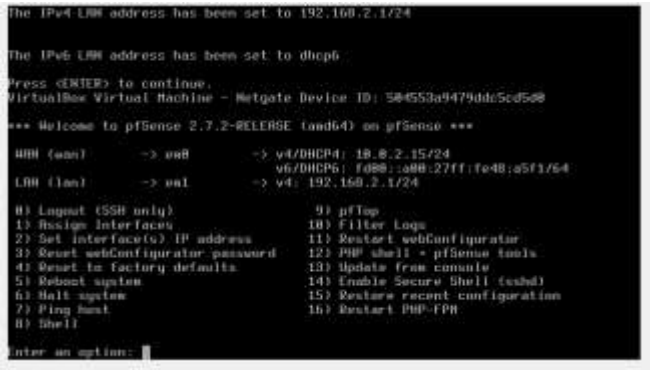

pfSense [Running] - Oracle VirtualBox
Netgate Installer - v1.0-RC
Select the version of pfSense CE to install.
2000-devel BE Version 2.8.0
2001-2.7.2 Current Stable Release (2.7.2)
2002-2.7.0 Deprecated Version (2.7.0)
[OK]
(Cancel)
Right Ctrl

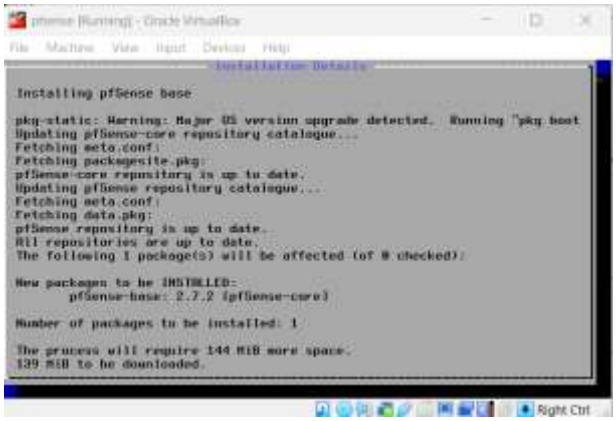

pfSense [Running] - Oracle VirtualBox
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
v6/DHCP6: fd00::a00:27ff:fe48:a5f1/64
LAN (lan) -> em1 -> v4: 192.168.1.1/24
0) Logout (SSH only) 9) pfTop
1) Assign Interfaces 10) Filter Logs
2) Set interface(s) 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: 2
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure:
Right Ctrl


pfSense [Running] - Oracle VirtualBox
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20240304-1953
Bootup complete
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: b40a6c5e55e811eb4a68
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
v6/DHCP6: fd00::a00:27ff:fe48:a5f1/64
LAN (lan) -> em1 -> 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:
Right Ctrl


pfSense [Running] - Oracle VirtualBox
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.2.1
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 255.255.255.0 =24
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.2.1
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 32):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
Right Ctrl

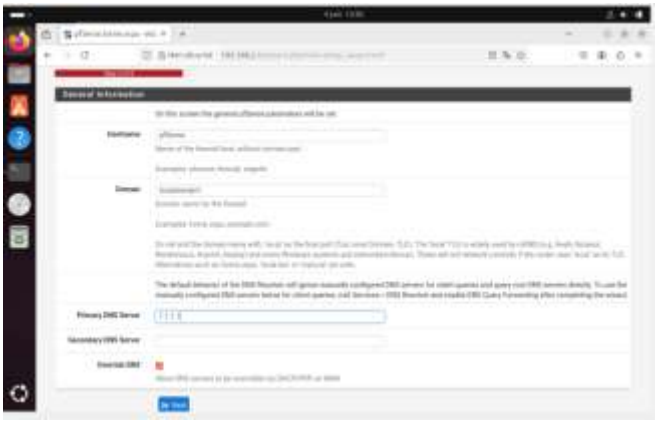

fabian-marie-beatrice@box:~
fabian-marie-beatrice@box:~ $ ifconfig
em0: flags=8863<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.2.2 netmask 255.255.255.0 broadcast 192.168.2.255
inet6 fe80::a00:27ff:fe65:b63c prefixlen 64 scopeid 0x20<link>
ether 08:00:27:65:b6:3c txqueuelen 1000 (Ethernet)
RX packets 2608 bytes 159608 (159.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2738 bytes 219856 (219.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Boucle locale)
RX packets 5310 bytes 411012 (411.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 5310 bytes 411012 (411.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
fabian-marie-beatrice@box: $


The IPv4 LAN address has been set to 192.168.2.1/24
The IPv6 LAN address has been set to dhcp6
Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 584553a9479ddc5cd5d0
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
v6/DHCP6: fd00::a00:27ff:fe48:a5f1/64
LAN (lan) -> em1 -> v4: 192.168.2.1/24
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:

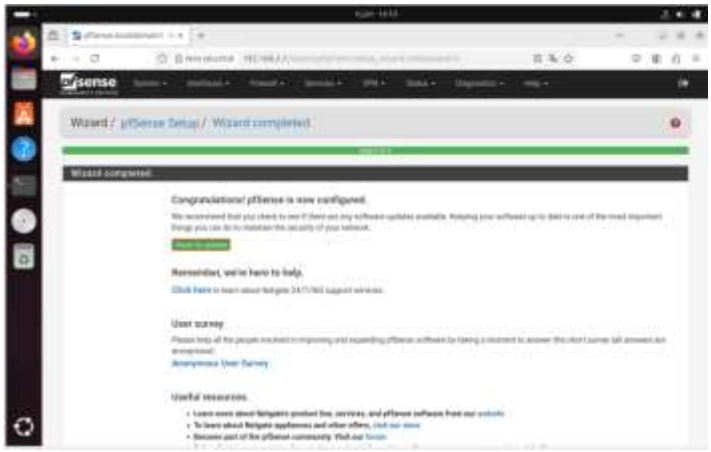

pfSense [Running] - Oracle VirtualBox
Installation Details
Installing pfSense base
pkg-static: Warning: Major OS version upgrade detected. Running "pkg boot
Updating pfSense-core repository catalogue...
Fetching meta.conf:
Fetching packagesite.pkg:
pfSense-core repository is up to date.
Updating pfSense repository catalogue...
Fetching meta.conf:
Fetching data.pkg:
pfSense repository is up to date.
All repositories are up to date.
The following 1 package(s) will be affected (of 0 checked):
New packages to be INSTALLED:
pfSense-base: 2.7.2 (pfSense-core)
Number of packages to be installed: 1
The process will require 144 MiB more space.
139 MiB to be downloaded.
Right Ctrl

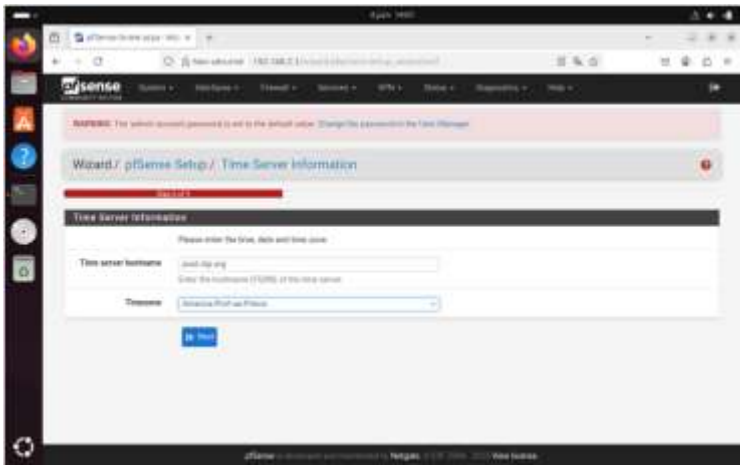

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 2 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 2 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 1 . 1 . 1 . 1
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel


pfsense
SIGN IN




Thank you!





1.Règles de filtrage

Des règles de filtrage ont été définies pour contrôler le trafic entre les différentes interfaces et VLANs :

- **Interface WAN** :
    - Blocage de tout le trafic entrant par défaut.
    - Ouverture du port 443 pour l'administration distante via HTTPS.
    - Autorisation du trafic VPN entrant si nécessaire.
- **Interface LAN** :
    - Autorisation du trafic sortant vers Internet.
    - Blocage de certains services à l'aide de règles spécifiques ou d'un proxy.
- **Règles spécifiques aux VLANs** :
    - VLAN 10 (Utilisateurs) : accès restreint à Internet.
    - VLAN 20 (Administrateurs) : accès total au réseau et aux services critiques.
    - VLAN 30 (Invités) : uniquement l'accès Internet est autorisé.

2. NAT (Network Address Translation)

Nous avons utilisé le **NAT dynamique (PAT)** :

- Chaque VLAN utilise une seule adresse IP publique via la traduction d'adresse de port.
- **Règles de redirection de port** mises en place :
    - Accès à un serveur Web interne depuis Internet (port 80 redirigé).
    - Accès à un serveur Mail interne (port 587 redirigé de façon contrôlée).

3. VLANs

Les VLANs sont associés à des sous-interfaces logiques du routeur ou du commutateur Layer 3 simulé dans Cisco Packet Tracer.

4. Services de Sécurité

Bien que Packet Tracer ne simule pas toutes les fonctions avancées de pfSense, nous avons représenté les services suivants :

- **DHCP Server par VLAN** : attribution dynamique des adresses IP.
- **DNS local** : résolution des noms interne au réseau.
- **Proxy filtrant (représenté via règles de filtrage)**.
- **VPN (représenté symboliquement)** : pour accès sécurisé au réseau interne.

2. Comparaison : Règles de filtrage par interface vs. par VLAN

Critère	Règles par Interface	Règles par VLAN
Cible	Interface physique (ex. LAN, WAN)	Réseaux logiques isolés
Gestion	Plus simple, surtout pour les petits réseaux	Plus complexe mais plus flexible
Segmentation	Moins précise	Très précise, favorise la sécurité par séparation des rôles
Utilisation	Environnements simples	Environnements professionnels multi-services

Les règles par VLAN permettent un **contrôle plus fin** du trafic, essentiel dans un réseau professionnel. Les règles par interface sont plus faciles à gérer mais moins flexibles.

3. Importance d’un Pare-feu comme pfSense

Un pare-feu tel que **pfSense** est **essentiel pour la sécurité réseau** :

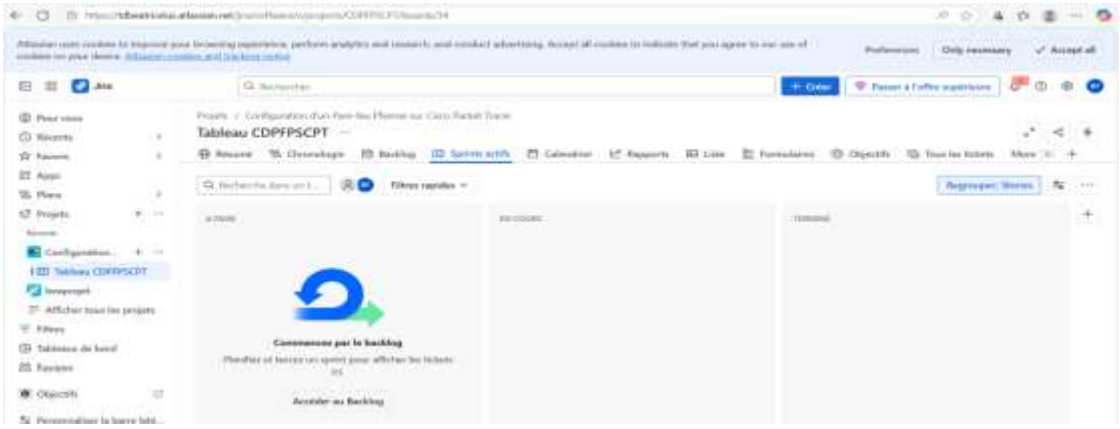
- **Contrôle du trafic** : autorise ou bloque les flux en fonction de politiques définies.
- **Protection contre les menaces externes** : évite les intrusions, attaques DDoS, scans de ports.
- **Segmentation réseau** : réduit les risques de propagation d’attaques internes.
- **Surveillance et alertes** : grâce aux logs, outils de détection d’intrusion, et au filtrage DNS.
- **Services supplémentaires** : VPN, proxy, gestion d’identité, filtrage web, etc.

Il agit comme une **barrière intelligente** entre le réseau interne et l’extérieur, tout en contrôlant les flux internes.

4. Limitations de la Simulation

Cisco Packet Tracer ne permet pas d’implémenter pfSense directement, et présente plusieurs limitations :

- Pas de machine virtuelle pfSense : Impossible d’émuler pfSense tel quel.
- Services simulés de façon approximative : VPN, proxy, IDS ne sont pas fonctionnels.
- Pas de plugins avancés (Snort, pfBlockerNG).
- Pas de gestion avancée des logs ou interfaces Web de configuration.
- Pas de trafic réel ni comportement réaliste du réseau (latence, goulot d’étranglement, attaques).



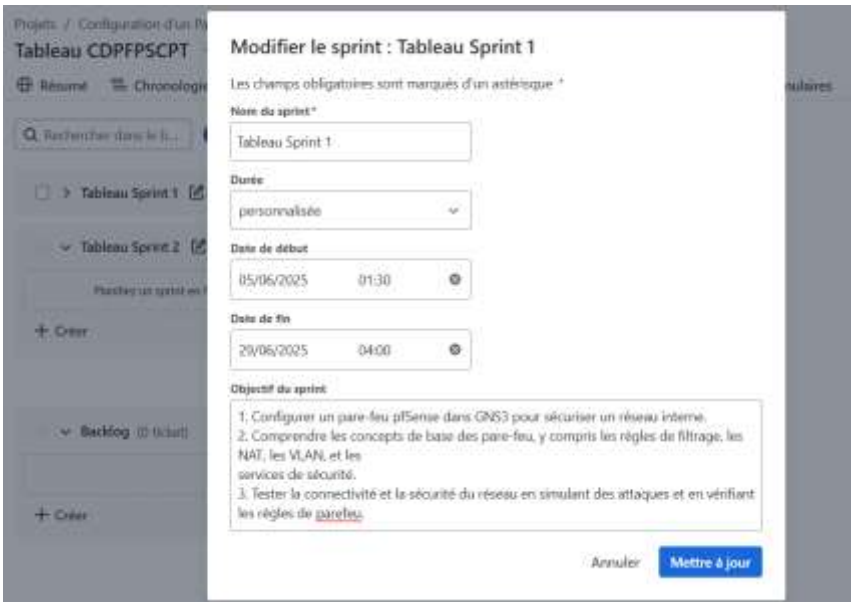
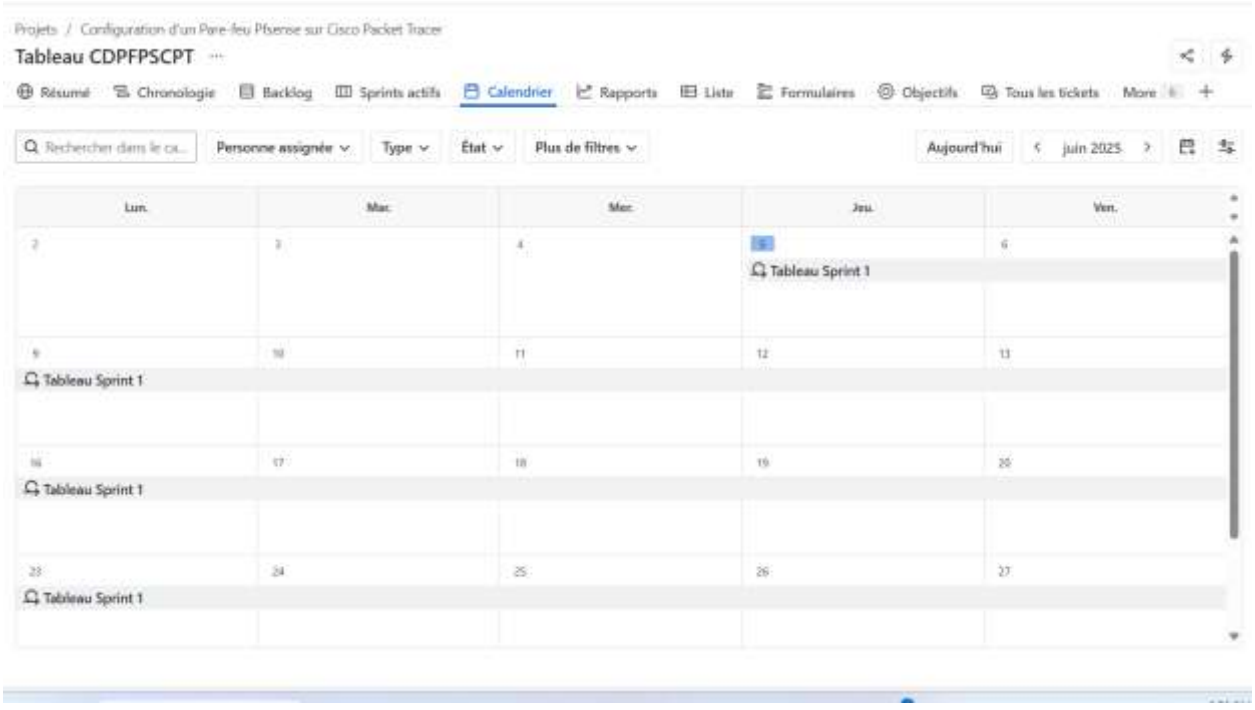
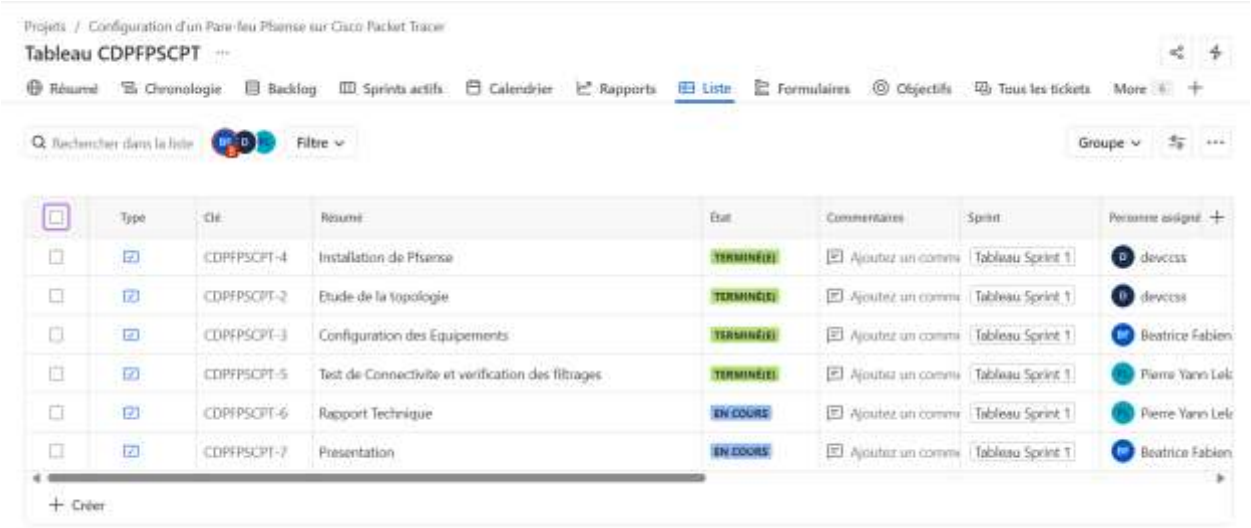


Tableau CDPFPSCPT
Modifier le sprint : Tableau Sprint 1
Les champs obligatoires sont marqués d'un astérisque *
Nom du sprint *
Tableau Sprint 1
Durée
personnalisée
Date de début
05/06/2025 01:30
Date de fin
29/06/2025 04:00
Objectif du sprint
1. Configurer un pare-feu pfSense dans GNS3 pour sécuriser un réseau interne.
2. Comprendre les concepts de base des pare-feu, y compris les règles de filtrage, les NAT, les VLAN, et les services de sécurité.
3. Tester la connectivité et la sécurité du réseau en simulant des attaques et en vérifiant les règles de pareFeu.
Annuler
Mettre à jour


Projets / Configuration d'un Pare-feu Pfsense sur Cisco Packet Tracer
Tableau CDPFPSCPT
Résumé
Chronologie
Backlog
Sprints actifs
Calendrier
Rapports
Liste
Formulaires
Objectifs
Tous les tickets
More
Personne assignée
Type
État
Plus de filtres
Aujourd'hui
juin 2025
Lun.
Mar.
Mer.
Jeu.
Ven.
Tableau Sprint 1



Conclusion

Ce projet a permis d'explorer les bases de la **sécurité réseau avec pfSense**, en abordant la configuration des règles de filtrage, du NAT, des VLANs et des services essentiels. Malgré les limites de Cisco Packet Tracer, nous avons pu comprendre l'architecture logique d'un pare-feu efficace et son rôle crucial dans la protection des réseaux. Et en utilisant Jira, j'ai pu utiliser un outil incontournable pour les équipes cherchant à structurer, suivre et améliorer la gestion de mes projets, tout en favorisant la collaboration, la transparence et l'agilité.