Labo Firewall pfSense (90 min)

1	Objectifs	sudo ./c 2

Déterminer la configuration par défaut du firewall pfSense
Etudier les fonctions évoluées (liste blanche, …) du service DHCP
Utiliser une machine virtuelle (VM) CentOS sur le PC Windows afin de simuler un PC physique de test

Ce travail s'effectue par **groupe de 2**, vous disposez de 2 PC (voir étiquette jaune sur face avant)

- PC **A2-A16** (appelé **PC-Firewall**) sur lequel vous allez installer le logiciel gratuit **pfSense**
- PC **A20-A30** sous Windows7 (appelé **PC-Win**) pour administrer et tester ce firewall

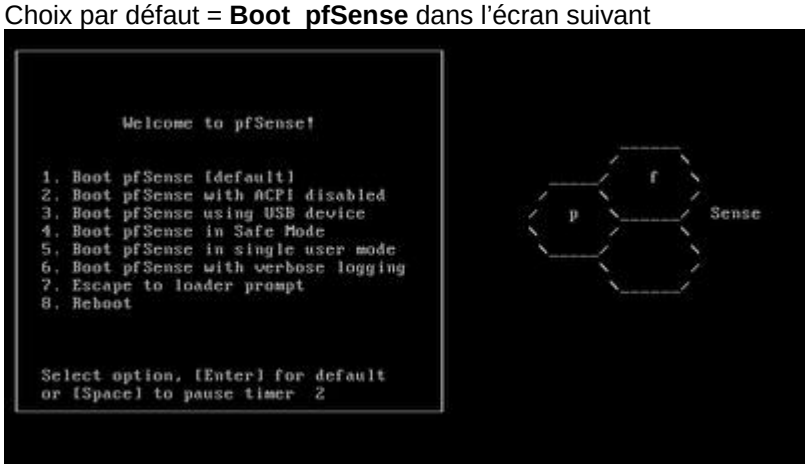
2	Démarrage du firewall	10 min

Action

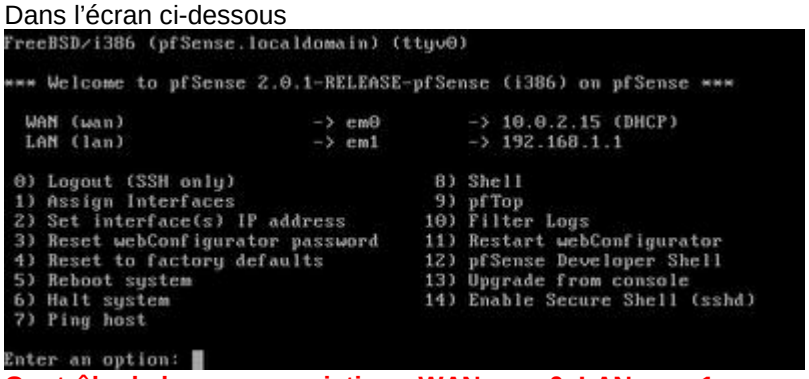
Allumer ou redémarrer le **PC-Firewall**
Dans le menu, choisir l'image **pfSense-2.0-1**

Après redémarrage conserver l'option Disque_Dur

Choix par défaut = **Boot pfSense** dans l'écran suivant



Dans l'écran ci-dessous



Contrôler la bonne association : WAN – em0, LAN – em1

Q_2a Quelles valeurs obtenez-vous pour les adresses IP ?

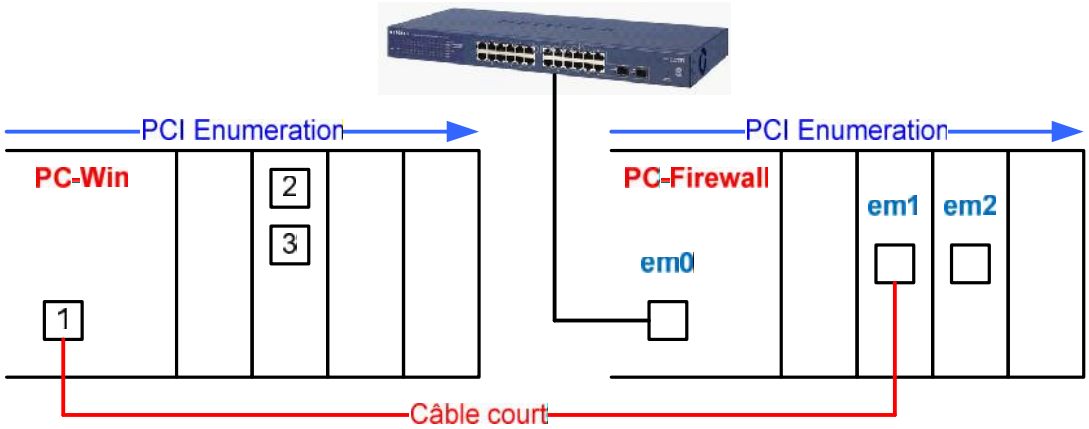
Q_2b Qui a configuré l'adresse IP de l'interface WAN ?

Q_2c Qui a configuré l'adresse IP de l'interface LAN ?

3	Configuration réseau	10 min

Action Allumer le **PC-Win**
Ouvrir une session avec Username=**albert** password=**admin**
Copier le dossier `\\10.2.1.1\doclabo\Secu\Firewall` sur le bureau

Débrancher le câble relié au port Ethernet de la carte mère
Utiliser un câble court pour relier PC-Win (carte mère) à PC-Firewall



Remarque Contrôler que le port Ethernet em0 (carte mère de PC-Firewall) est bien raccordé à l'intranet du labo

Q_3a Quelle est l'adresse IP de votre **PC-Win** ?

Test Sur **PC-Win**, contrôlez avec le navigateur **Chrome** (taskbar) l'accès à www.hes-so.ch
Des blocages, dus à IE, ont été observés

4	Administration via WebGUI	30 min

Action Avec le navigateur Chrome
Sélectionner **http://192.168.1.1**
Ignorer l'avertissement lié au certificat
User = **admin** pass = **pfsense**

Q_4a Quelle adresse IP avez-vous sélectionné ?

Q_4b L'adresse IP ci-dessus répond-elle au ping envoyé depuis **PC-Win** ?

Q_4c Quelles sont les principales informations de la page par défaut appelée Dashboard ?

Q_4d Quelle est l'utilité de la page Status – Interfaces ?

Q_4e Quelle est l'adresse IP de l'interface WAN ?

Q_4f Quelle est l'utilité de la page Status – Gateways ?

Q_4g Quels sont les services actifs ?

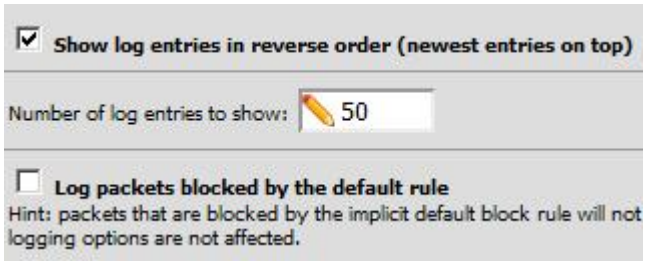
Q_4h Quel est le serveur DNS utilisé par le **PC-Win** ?

Q_4i Combien le serveur DHCP peut-il fournir d'adresses IP différentes ?

Q_4j Quelle est la règle qui autorise les flux précédents ?

Q_4k Quel est le mode par défaut des logs du firewall ?

Action Dans Status – System logs – Settings, modifier les champs suivants



Puis Save – Close
Dans Status – System logs – Firewall : Clear log

Q_4l Sous Firewall – Rules - LAN à quoi sert la règle Anti-Lockout Rule

5	**Afficher la table d'état**	**10 min**

Action Sur le **PC-Firewall**
Choisir l'option 8 (Shell)
Typer **`pftop -f icmp`**

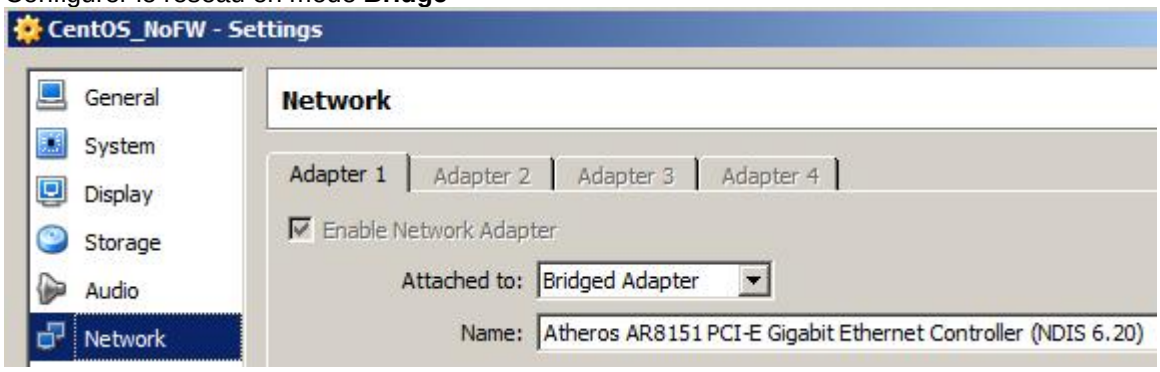
Q_5a Comment interprétez-vous cet affichage ?

Action Sur le **PC-Win**
Effectuer **`ping 10.10.10.10`**

Q_5b Comment interprétez-vous cet affichage ?
Q_5c Quelle est la durée du timeout ?

6	**Configuration réseau de VirtualBox**	**10 min**

Action Sur le **PC-Win,** clic sur **CentOS_NoFW.ova** (dossier copié sur le bureau) pour lancer Vbox et charger cette VM
Import
Configurer le réseau en mode **Bridge**



Contrôler que cette VM utilise la bonne interface physique Atheros

Remarque Les info utiles (username = **root**, password = **rootroot** , …) se trouvent dans le champ **Description**
Cette VM exécute le système d'exploitation CentOS 6.4 sans interface GUI

Action Start pour démarrer cette VM
Ouvrir une session
Entrer ifconfig pour contrôler que l'interface eth0 est bien configuré via DHCP
Noter cette valeur
Effectuer un ping sur l'interface LAN

Status – DHCP Leases dans l'administration du firewall, afficher la liste des adresses IP allouées

Q_6a Combien avez-vous d'adresses IP allouées ?

7	Liste blanche	20 min

Objectif **Seul le PC autorisé (PC-Win) dans la liste sera pris en compte par les règles du firewall**
La VM permettra de tester l'exclusion de celle-ci

Important **Choisir une nouvelle adresse IP pour PC-Win hors de l'intervalle utilisé par le serveur DHCP**

Action Sélectionner Services – DHCP Server pour ajouter en bas de page les informations utiles

Save – Apply changes

Q_7a Comment avez-vous procédé ?

Typer **`ipconfig /renew`** dans un cmd (Run as administrator)

Depuis la VM, effectuer un ping sur l'interface LAN

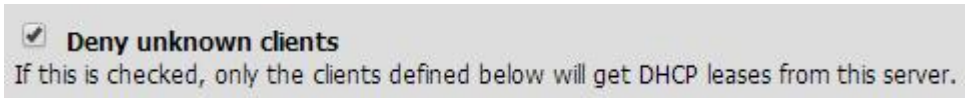
Important **Configurer vos fenêtres pour voir simultanément cette VM (ping) et l'interface web d'admin**

Dans Services – DHCP Server, activer 

Save

Tests ping depuis la VM
ping depuis PC-Win
Status – DHCP leases

Action Observer l'effet de

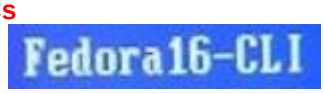


Tests comme précédemment

Q_7b Quelle est l'utilité pratique de Deny unknown clients ?

Important	**Poste de travail dans l'état initial**	**A faire à la fin**

Enlever le câble court reliant PC-Win (carte mère) à PC-Firewall
Brancher le câble enlevé au §2 au port Ethernet de la carte mère
Redémarrer les 2 PCs

Sélectionner l'image 

	A faire chez soi

Objectif Représenter le schéma de l'installation utilisée qui doit contenir

- Un bloc (rectangle) pour chaque entité physique (PC-Win, …)
- Les identifiants des ports Ethernet utilisés
- Toutes les adresses IP utiles
- Tous les subnet masks
- L'adresse IP des routeurs utilisés