PLOUZENNEC Eliaz

TP : FIREWALL PFSENSE

29/09/24

Introduction :	. 2
Etape 1 : Installer et configurer le Firewall PFSENSE	. 3
Etape 2 : Vérification de l'accès à internet	.4
Etape 4 : Test de blocage du site internet ECOLE DIRECTE (par exemple) - Etude du	
fonctionnement du filtrage URL	.4

Introduction :

Objectif : Installer et Configurer un Firewall PFSENSE dans une infrastructure virtuelle.

Un schéma est présenté au tableau à l'ensemble des étudiants avec des explications.

Adressage de l'infrastructure :

- Passerelle : 192.168.0.253
- Adresse IP WAN du Firewall : 192.168.0.172
- Adresse IP LAN : 172.16.1.253 (/16)
- Adresse IP du poste derrière le FIREWALL : 172.16.1.1 (/16)

Etape 1 : Installer et configurer le Firewall PFSENSE

Suivre l'installation et au moment de reboot, il faut éjécter virttuellement le disque pour ne pas redemarrer la configuration.

On arrive sur cette page:



Où on configure l'entrée WAN, en acces par pont vers le réseau de la salle, ici en gateway 192.168.0.172.

Puis on ajoute un LAN, qui mènera vers les machines, connectées en réseau interne, où le par feu fera effet, vers le réseau 172.16.0.0, on créé le gateway 172.16.1.253/16

Ainsi, coté windows 7, on met la carte réseau en réseau interne aussi, et on va pour configurer le réseau:

Propriétés de : Protocole Internet version	on 4 (TCP/IPv4)										
Général											
Les paramètres IP peuvent être déterr réseau le permet. Sinon, vous devez d appropriés à votre administrateur rése	ninés automa, quement si votre emander les paramètres IP au.										
Obtenir une adresse IP automatiquement											
Utiliser l'adresse IP suivante :											
Adresse IP :	172 . 16 . 1 . 1										
Masque de sous-réseau :	255.255.0.0										
Passerelle par défaut :	172 . 16 . 1 . 253										
Obtenir les adresses des serveurs	s DNS automatiquement										
O Utiliser l'adresse de serveur DNS s	suivante :										
Serveur DNS préféré :	8.8.8.8										
Serveur DNS auxiliaire :	· · ·										
🔲 Valider les paramètres en quittar	Avancé										
	OK Annuler										

Ici il suffit de mettre une ip au choix dans le réseau 172.16.0.0/16, ici 172.16.1.1, puis de mettre la passerelle qu'on vient de créer sur le pfsense, dans le LAN, donc 172.16.1.253

Etape 2 : Vérification de l'accès à internet

😆 Get Firefox for desktop — Mozilla (US)

No shady privacy policies or back doors for advertisers. Just a lightning fast browser that doesn't sell you out.

Firefox is no longer supported on Windows 8.1 and

Please download Firefox ESR (Extended Support Relea

Download Firefox ESR 32-bit

Download a different build

Firefox Privacy Notice

Download options and other languages

Pour accéder à un navigateur on va prendre firefox car il eiste en x32, compatible avec la windows 7.

Etape 3 : Test de blocage du site internet ECOLE DIRECTE (par exemple) - Etude du fonctionnement du filtrage URL

Pour la suite on va accéder à l'interface du firewall depuis firefox, sur la machine virtuelle, pour accéder à cette interface il suffit de rentrer l'adresse du gateway, on rentre donc 172.16.1.253, pour arriver sur cette page:

$\leftarrow \ \ \rightarrow$	C	08	172.16.1.253/index.php
D		nc	ρ
	301	15	~ ,
			SIGNIN
			admin
			•••••

Avec comme user: admin, mdp : pfsense

Firewall /	Aliases / Edit	0
Properties		
Name	ecoled The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".	
Description	block ecole d A description may be entered here for administrative reference (not parsed).	
Туре	Host(s)	~

Pour bloquer ecoledirecte.com j'ai créé un alias pour commencer, cet alias permet de bloquer son url

Host	Domain	IP	Description	Actions
ecoledirecte	com	152.228.241.34		e 🖉 🗇
www	ecoledirecte.com	152.228.241.34		e 🖉
				+ Ad
Domain Ove	errides			
Domain	IP	Des	cription	Actions
ecoledirecte.co	m 152.228	.241.34		e 🖉 🖄
				+ Ad
:\Users\plo	ouzennec>ping ecol	ledirecte.com		
nvoi d'une éponse de 1 éponse de 1	requête 'ping' Si 152.228.241.28 : 152.228.241.28 : 0	ur ecoledirecte. octets=32 temps= octets=32 temps=:	com [152.228.2 10 ms TTL=46 10 ms TTL=46	41.28] avec 32

Ensuite j'ai fait en sorte de bloquer son dns, avec son nom de domaine en meme temps, et pour trouver son ip à ecoledirecte j'ai juste fait un ping de son url (il y a plusieurs dns, pour cette raison qu'on bloque directement l'url)

Host(s)	
Hint	Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.
IP or FQDN	www.ecoledirecte.com Entry added Wed, 02 Oct 2024 09

Ici on block directement l'url

Firewall /	Rules / Edit	≞ 🔟 🗏 🚷
Edit Arewall	Rule	
Action	Block	~
	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 (T port unreachable for UDP) is returned to the sender, whereas with block the silently. In either case, the original packet is discarded.	CP RST or ICMP e packet is dropped
Disabled	Disable this rule Set this option to disable this rule without removing it from the list.	
Interface	ECOLE Choose the interface from which packets must come to match this rule.	~
Address Family	IPv4 Select the Internet Protocol version this rule applies to.	~
Protocol	Any	~

Enfin on peut aller dans firewall/rules pour y ajouter notre regle de par feu, on créé cette regle bien dans l'interface où on veut bloquer, puis dans cette création on fait en sorte de bloquer par IP^{°°}, dans tous les protocols, sur l'interface ECOLE (nouveau nom de l'interface).

Source						
Source	Invert match.	any	~	Source Address	/	~
Destination						
Destination	Invert match.	Single host or alias	~	ecoled	1	~

Dans source on met tout le monde, et dans la destination on met l'alias qu'on a créé auparavant, cet alias "ecoled"

Firewall / Rules / ECOLE										≢ <u>1</u> 11 (•	
Floa	ting	WAN	ECOLE									
Ru	les	(Drag t	o Chang	e Orde	r)							
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	*	2 /2.27 MiB	*	*	*	ECOLE Address	80	*	*		Anti- Lockout Rule	0

Apres cette règle créé, on la met le plus haut possible dans les regles, en deuxieme (premiere place est prise)

The connection has timed out

An error occurred during a connection to www.ecoledirecte.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

La page est maintenant bloquée.