Pfsense permet de réaliser un filtrage par protocole(s), port(s),..., sur chaque interface. Pour cela, il faut paramétrer les règles dans l'onglet Firewall/Rules.

Les règles fonctionnent de manière hiérarchique. En effet, Pfsense va « lire » les règles de haut en bas, et dès qu'il trouvera une règle s'appliquant au trafic, il l'appliquera. Par exemple, avec deux règles, une bloquant le protocole https, et l'autre l'autorisant, Pfsense appliquera la première qu'il rencontrera (la plus haute)

Firewall: Rules

Floating | WAN | LAN_MIXTE | DMZ

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN_MIXTE Address	80	*	*		Anti-Lockout Rule
		*	LAN_MIXTE net	*	*	*	*	none		Default allow LAN to any rule
		TCP	*	443 (HTTPS)	*	*	*	none		Bloquer le HTTPS
		TCP	*	443 (HTTPS)	*	*	*	none		Autoriser le HTTPS
		*	*	*	*	*	*	none		Tout bloquer depuis le LAN

Ici, la règle appliquée est celle bloquant le https.

Par défaut, Pfsense bloque tout trafic sur l'interface WAN et autorise tout trafic du LAN :

Règles par défaut sur l'interface WAN

Règles par défaut sur l'interface LAN

Firewall: Rules: Edit

Edit firewall 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 (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	LAN Choose on which interface packets must come in to match this rule.
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	**not** Use this option to invert the sense of the match. Type: any Address: / 31
Destination	**not** Use this option to invert the sense of the match. Type: any Address: / 31
Log	**Log packets that are handled by this rule** Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	Tout bloquer depuis le LAN You may enter a description here for your reference.

Afin de réaliser un « meilleur » filtrage, il est d'abord conseillé de bloquer tout trafic et d'ensuite autoriser un à un les ports et/ou protocole.

Concernant les deux règles par défaut du LAN, il ne faut surtout pas désactiver la règle « Anti-Lockout », qui permet de se connecter à l'interface web de Pfsense via un autre PC (sous peine de devoir reconfigurer voir réinstaller Pfsense).

Par contre, la seconde règle est celle qui autorise tout le trafic. Il faut donc soit la désactiver, soit la supprimer (je l'avais dans un premier temps désactivée car au besoin, j'avais juste à la réactiver pour avoir de nouveau accès à Internet rapidement)

Pour la supprimer, cliquez sur la croix correspondant à la règle, et validez le message de confirmation de suppression :

Cliquez sur la croix surlignée pour supprimer la règle

Pour uniquement la désactiver, cliquez sur la règle puis sur le bouton « e ». L'écran suivant arrive :

Firewall: Rules: Edit

Edit Firewall rule	
Action	Pass 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	LAN Choose on which interface packets must come in to match this rule.
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
Source	**not** Use this option to invert the sense of the match. Type: LAN subnet Address: / 31
Destination	**not** Use this option to invert the sense of the match. Type: any Address: / 31
Log	**Log packets that are handled by this rule** Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).

Ensuite, il faudra créer une règle qui bloque tout. En effet, comme cela, tout le trafic ne répondant pas à une règle définie dans pfsense sera automatiquement bloqué par cette règle-ci.

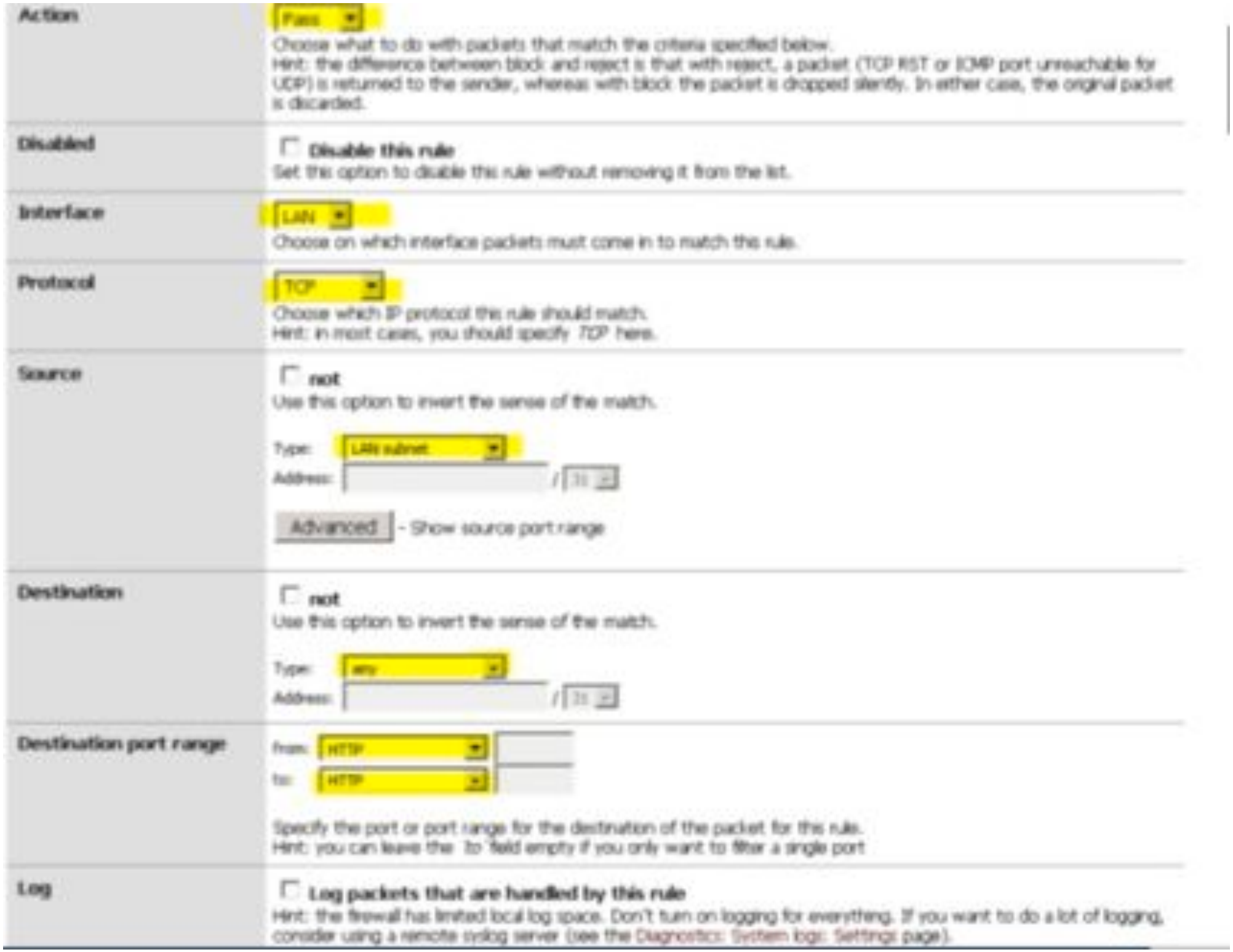
Il est donc impératif de positionner cette règle en dernière position sur la liste de toutes les règles.

Cliquez donc sur le bouton « + »

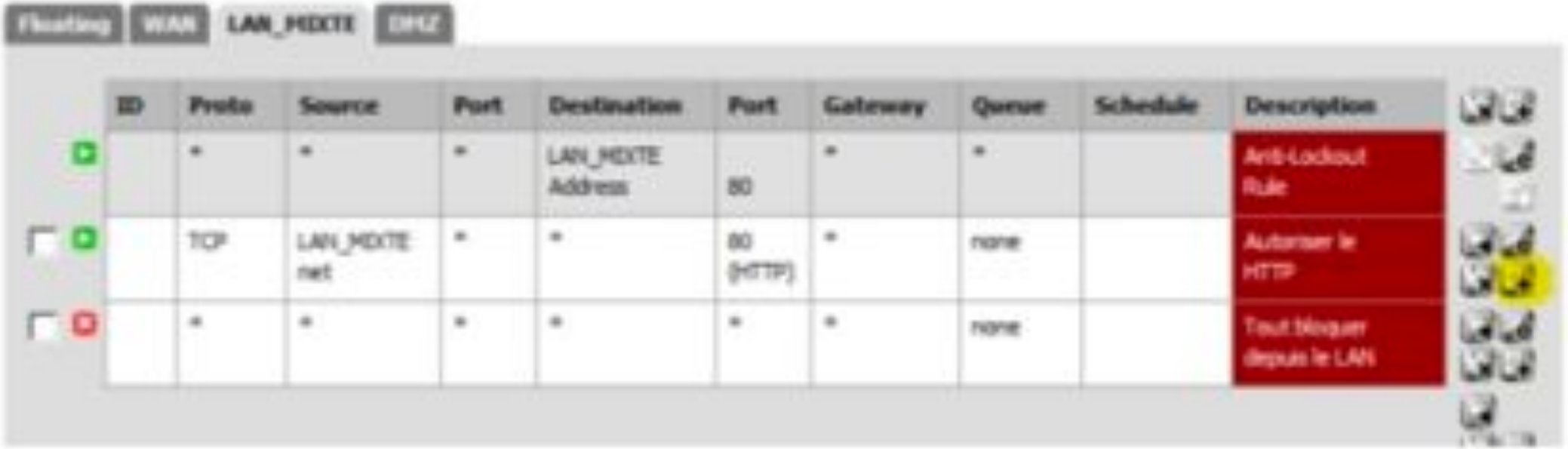
A ce stade-ci, tout trafic depuis le LAN est bloqué.

Règles avec tout le trafic bloqué

Désormais, il va falloir créer une règle par port, protocole, ... C'est-à-dire pour chaque besoin spécifique.


Action
Pass
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
LAN
Choose on which interface packets must come in to match this rule.
Protocol
TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.
Source
not
Use this option to invert the sense of the match.
Type:
LAN subnet
Address:
/ 31
Advanced
- Show source port range
Destination
not
Use this option to invert the sense of the match.
Type:
any
Address:
/ 31
Destination port range
From:
HTTP
To:
HTTP
Specify the port or port range for the destination of the packet for this rule.
Hint: you can leave the 'to' field empty if you only want to filter a single port
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).

Ensuite, pour plus de facilité, il est possible de cliquer sur le bouton « + » suivant pour créer un « clone » d'une règle existante (pratique lorsque l'on crée des règles qui diffèrent uniquement sur le port par exemple)



Voici, à titre d'exemple, les règles en vigueur pour le réseau pédagogique du lycée de Montauban :

☐	TCP	LAN net	*	*	80 (HTTP)	*	none		HTTP	
☐	TCP/UDP	LAN net	*	*	3128	*	none		Squid	
☐	TCP	LAN net	*	facebook	443 (HTTPS)	*	none	☐ toujours vous	Bloquer le HTTPS de facebook	
☐	TCP	LAN net	*	viedemerde	443 (HTTPS)	*	none		Bloquer le HTTPS de vie de merde	
☐	TCP	LAN net	*	*	443 (HTTPS)	*	none		HTTPS	
☐	TCP/UDP	LAN net	*	*	53 (DNS)	*	none		DNS	
☐	TCP	LAN net	*	*	510	*	none		FirstClass	
☐	ICMP	LAN net	*	*	*	*	none		Ping	
☐	*	*	*	*	*	*	none		Tout bloquer depuis le LAN	
☐	*	LAN net	*	*	*	*	none		Default allow LAN to any rule	

Règles en vigueur sur le réseau pédagogique du lycée de Montauban au 03 mai 2012

Ports & Protocoles	***Services***
TCP : 80	HTTP (pas obligatoire si proxy transparent)
TCP : 110	POP3
TCP : 25	SMTP
TCP : 443	HTTPS
TCP & UDP : 22	SSH
TCP & UDP : 21	FTP
TCP & UDP : 119	NNTP
TCP : 143	IMAP
TCP & UDP : 123	NTP
TCP : 510	FirstClass
TCP : 81	Nocia/Page de redirection SquidGuard
TCP : 1717	Module Java d'EVA
TCP : 1494	Luciole
UDP : 10000	Magellan
TCP : 264	Prisme / EPICEA
TCP : 256	Prisme / EPICEA
TCP : 709	Prisme / EPICEA
UDP : 2746	Prisme / EPICEA

UDP & TCP : 500	(Isakmp) Prisme / EPICEA / Magellan
TCP : 389	(LDAP) Prisme / EPICEA
TCP & UDP : 8080	Webcache
TCP & UDP : 8081	tproxy
TCP : 18231, 18232, 18233, 18234	Checkpoint
TCP & UDP : 53	DNS
TCP & UDP : 800	Proxy Squid
TCP : 1863	MSN Messenger
TCP: 1495	Citrix
TCP: 2598	Citrix