

GUIDE D'UTILISATION DE WINSOCK FIREWALL

(Created by Sébastien SOULIER)

- 1. Comment démarrer et arrêter le FireWall
 - 1. Comment démarrer le FireWall
 - 2. Comment arrêter le FireWall
- 2. <u>Création et modification des règles</u>
 - 1. Format des règles du FireWall
 - 1. Format des règles IP
 - 2. Format des règles applicatives
 - 2. Création et modification des règles du FireWall
 - 1. Créer et modifier les règles IP
 - 2. Créer et modifier les règles applicatives
- 3. Choisir le niveau de sécurité
- 4. Interface des logs
- 5. Interface des répertoires partagés
- 6. Fonctions de scanneur de ports

I. Comment démarrer et arrêter le FireWall

Vous pouvez démarrer Isafer Winsock FireWall à partir du menu Démarrer de Windows de la même manière que n'importe quel autre logiciel. Une fois l'application lancée, elle apparaît en bas, à droite de la barre des tâches, parmi les autres icônes. Un clic sur cet icône laisse apparaître la fenêtre principale du logiciel.

1. Comment démarrer le FireWall

Le petit écran à droite de la fenêtre principale vous indique l'état du firewall. Si le firewall est arrêté (Firewall is stopped), cliquez sur le bouton 'start' pour le démarrer.



2. Comment arrêter le FireWall

Le petit écran à droite de la fenêtre principale vous indique l'état du firewall. Si le firewall est en marche

(Firewall is started), cliquez sur le bouton 'stop' pour l'arrêter.



II. Création et modification des règles

L'interface de création et de modification de règles est accessible par le bouton 'option'.

2-Safer	SRFE INTERVET	×		
Safer - F/W	Log 🔝 Shared Folder	rs 🛛 📑 Port Sca	n	
1. IP Rule :				
2. Application Rule :	PUILINU.	Роптуре	Permission	
Application Path	4	Permi	ission	
Add Ru	le 🔒 Delete R	Rule		

Il y a cinq onglets dans la fenêtre des options. Le premier contient la liste de deux types de règles, les règles de filtrage de paquets et les règles de filtrage applicatif.

1. Format des règles du FireWall

a. Format des règles IP

Dans la liste des règles IP, il y a 4 colonnes. La première colonne correspond aux adresses IP sur lesquelles la règle va s'appliquer. La seconde correspond aux ports. La troisième correspond au protocole

que l'on veut contrôler. La dernière montre l'action à effectuer sur le paquet IP s'il correspond aux trois autres colonnes. Si l'action est autoriser (Allow) le paquet sera autorisé à dialoguer avec votre PC. Si l'action est interdire (Deny) le paquet sera jeté.

b. Format des règles applicatives

Une règle applicative a uniquement deux paramètres. Le premier est le chemin complet de l'application. L'autre l'action à effectuer. Si l'action est autoriser (allow), l'application sera autorisée à accéder au réseau. Si l'action est interdire (deny), l'application ne pourra pas accéder au réseau. La valeur par défaut pour les deux types de règle dépend du niveau de sécurité choisi. Ce point sera plus détaillé dans la section <u>Choisir le niveau de sécurité</u>.

💁 iSafer - F/W				
🔹 💀 FAV Rule Set 🛛 💊 Security Level 🛛 🔅 Firewall Log	g 🛛 🔊 Shared Folder	s 🛛 🥳 Port Sca	n	
Rule Set				
1. IP Rule :				
IP Address	Port No.	Port Type	Permission	
A 045.045.045.045 ~ 045.045.045	1~1	TCP/UDP	ALLOW	
2. Application Rule :				
Application Path		Permi	ission	
Clprogram files\isafer\unwise.exe		DE	NY	
Ndd Rule	🔒 Delete R	ule		

Dans l'onglet de gestion des règles, il y a deux boutons : ajouter (Add) et supprimer (Delete). Il permettent respectivement d'ajouter et supprimer des règles. Un clic droit sur une règle permet de la modifier.

2. Création et modification des règles du firewall

Cliquez sur le bouton ajouter (Add) de l'onglet de gestion des règles pour obtenir la fenêtre suivante :

💁 iSafer - FireWall Rule Editor	×
👫 IP Rule 🕔 Application Rule	
Input IP Address/Port Range and permission to create a firewall rule	
 Rule for single IP Address Rule for a range of IP Addresses Rule applied to all IP Addresses 	
From IP: To IP: 45 . 45 . 45 . 45 ~	
 Rule for a single Port Rule for a range of ports Rule applied to all ports 	
From Port: To Port: 00001 ~ 65535	
 Allow Access Deny Access 	
🧭 OK 🇐 Cancel	

a. Créer et modifier les règles IP

Dans la fenêtre d'ajout de règles IP il y a 3 champs à remplir :

- Plage IP.
 - Il y a 3 options pour la plage IP:
 - IP unique, l'utilisateur peut entrer une IP
 - Plage IP, l'utilisateur peut entrer les deux extrémités d'un plage IP
 - Toutes les adresses IP, corresponds à la plage IP maximale [000.000.000.001-255.255.255.255]
- Plage de Ports.

Une plage de ports se configure de la même façon qu'une plage IP. Il y a 3 options :

- Port unique
- Plage de ports
- Tous les ports, ce qui correspond à la plage de ports [0, 6635]
- Action

En choisissant un des deux boutons radio, l'utilisateur va choisir l'action à effectuer pour la règle : 'Deny' (interdire) or 'Allow' (autoriser).

Après avoir fini la création d'une règle, cliquer sur ajouter (Add) ajoutera votre nouvelle règle à la liste de règles déjà présentes et la prendra en compte alors que cliquer sur annuler (Cancel) fermera la fenêtre sans modification.

b. Créer et modifier les règles applicatives

Dans l'autre onglet, 'Application Rule' (règle applicative), vous pouvez créer des règles pour chaque application logicielle.

💁 iSafer - FireWall Rule Editor	×
🐇 IP Rule 🔇 Application Rule	
Create new firewall rule for specific application	
Application path:	
🔐 Browse	
Permission:	
 Allow 	
C Deny	
🧭 OK 🧐 Cancel	

Pour créer une règle applicative, il faut d'abord spécifier manuellement le chemin complet vers l'application ou en cliquant sur le bouton parcourir (browse). Ensuite, il faut choisir avec le bouton radio l'action à effectuer autoriser (allow) ou interdire (deny). Et finalement, il faut cliquer sur le bouton ajouter (Add) pour que la règle soit prise en compte. Comme précédemment le bouton annuler (cancel) permet d'annuler l'ajout de la règle.

III. Choisir le niveau de sécurité

Le deuxième onglet de la fenêtre des options est utilisée pour définir le niveau de sécurité. Il y a trois niveaux de sécurité :

Niveau de Sécurité	Description
High (élevé)	A ce niveau, tout est interdit par défaut sauf ce qui est explicitement autorisé par l'utilisateur au moyen des règles.

Medium	Les ports communs comme HTTP, FTP, SMTP sont autorisés par défaut sauf s'ils sont
(moyen)	interdits par des règles de l'utilisateur.
Low (bas)	A ce niveau, tout est autorisé par défaut sauf ce qui est explicitement interdit par l'utilisateur au moyen des règles.

Après avoir sélectionné le niveau de sécurité désiré, cliquer sur le bouton ajouter (add) permet d'appliquer le changement.



IV. Interface des logs

Le troisième onglet de la fenêtre des options apporte à l'utilisateur les avantages d'une interface de lecture de fichiers de logs. Ici, l'utilisateur peut voir les informations sur les logs et a la possibilité d'ajouter des règles IP et applicatives.

Une ligne de log contient les informations décrites dans le tableau ci-dessous :

Type d'information	Description
Time (Date)	Date de création de la ligne de log
Direction	Direction du flux de données : IN indique un flux partant d'une machine distante vers la machine locale et OUT indique un flux partant de la machine locale vers une machine distante

Permission (Action)	L'action effectuée pour le paquet traité : interdit (deny) ou autorisé (allow)
IP	Adresse IP de la machine distante
Hostname (Nom de la machine)	Nom de la machine distante
Port	Numéro de port de la machine distante
Application Path (chemin de l'application)	Chemin de l'application locale dialoguant avec la machine distante
Bytes sent (Octets envoyés)	Nombre d'octets envoyés par la machine locale
Bytes received (Octets reçus)	Nombre d'octets reçus par la machine locale
Socket number (Numéro de port)	Numéro du port utilisé pour la communication

Par défaut les attributs date, IP et port apparaissent dans toutes les lignes de logs, les autres attributs sont optionnels. L'utilisateur peut choisir d'afficher ou non les attributs grâce au menu Show/Hide columns (Afficher/Cacher les colonnes) en faisant un clic droit sur le fond de la fenêtre.

💁 iSafer - F/W			1.1. 16			
🐋 FAV Rule Se	t 🛛 🐋 Secu	urity Level 🛛 🕏	🏃 Firewall Log 🛛 🔊	Shared Folders 🥂 🛃 I	Port Scan	
FAV Log	1970	<i></i>	1.57	12. 1		- -
Time	Direction	Permissi	IP	HostName	Port	Application Path
10:36:02:806	OUT	DENY	172.20.5.14	172.20.5.14	389	c:\winnt\system32\lsa
10:36:02:816	OUT	ALLOW	172.20.5.12	172.20.5.12	53	c:\winnt\system32\ser
10:36:02:816	OUT	DENY	172.20.5.12	172.20.5.12	389	c:\winnt\system32\lsa
10:36:02:816	OUT	DENY	172.20.5.13	172.20.5.13	389	c:\winnt\system32\lsa
10:36:02:826	OUT	DENY	172.18.7.10	172.18.7.10	389	c:\winnt\system32\lsa
10:36:03:877	OUT	ALLOW	172.20.5.12	172.20.5.12	53	c:\winnt\system32\ser
10:36:05:169	OUT	ALLOW	172.20.5.14	172.20.5.14	135	c:\winnt\system32\lsa
10:36:05:179	OUT	DENY	172.20.5.14	172.20.5.14	1025	c:\winnt\system32\lsa
10:36:05:179	OUT	ALLOW	172.20.5.14	172.20.5.14	135	c:\winnt\system32\lsa
10:36:05:199	OUT	DENY	172.20.5.14	172.20.5.14	1025	c:\winnt\system32\lsa
10:36:05:199	OUT	ALLOW	172.20.5.12	172.20.5.12	53	c:\winnt\system32\ser
•						•

Le clic droit permet aussi d'atteindre le menu de création de règles comme le montre la figure suivante :

FW Rule Set Security Level Firewall Log Shared Folders Port Scan FW Log Ime Direction Permissi IP Port Application Path Ime Direction Permissi IP Port Application Path Ime Direction Permissi IP Port Application Path Image: Internet intern	🂁 iSafer - F/W						
FW Log Direction Permissi IP Port Application Path Image: 10:40:07:177 OUT ALLOW 192.168.250.19 8080 c:tprogram files\mozilla firefoxtfirefox.exe Add IP rule Add application rule Add application rule Show/Hide Columns Image: Clear log	🐟 FAV Rule Se	t 🛛 🐋 Secu	rity Level 🛛 🔅	🏃 Firewall Log 🛛 👔	这 Shared Fo	olders 🛛 🥑 Port Scan	
Time Direction Permissi IP Port Application Path ALLOW 192.168.250.19 8080 c:\program files\mozilla firefox\firefox.exe ddd IP rule Add application rule Add application rule Show/Hide Columns Clear log	FAV Log					·	•
Image: No:40:07:177 OUT ALLOW 192.168.250.19 8080 c:\program files\tmozilla firefox\tfirefox.exe Add IP rule Add application rule Add application rule Show/Hide Columns Image: Clear log	Time	Direction	Permissi	IP	Port	Application Path	
	2 10:40:07:177	OUT	ALLOW	192.168.250.19	8080	c:\program files\mozilla ide ication rule 2 Columns	a firefox(firefox.exe

V. Interface des répertoires partagés

Le quatrième onglet de la fenêtre des options est une interface pour les répertoires partagés. Elle vous permet de lister vos répertoires partagés, stopper le partage, fournir les propriétés des répertoires et se déplacer dans un répertoire spécifique.

<u>5</u>	iSafer - F/W							
	😿 F/W Rule Set 💧	👈 Secur	ity Level	💸 Firewall Log	🔊 Shared Folders	🥃 Port Scar	n	
Г	Shared folder Mar	nager				·		
	Share name		Share Pa	th			Notes	
	📫 Partage		C:\Partag	e				
	J							_
	1	Open		Properties	🌱 Unsha	re	😥 Refresh	

VI. Fonctions de scanneur de ports

Le dernier onglet de la fenêtre des options propose un petit utilitaire de scanneur de ports. Il permet de scanner ses propres ports pour déterminer quels services sont actifs sur la machine locale. C'est très pratique pour savoir si un port bizarre est ouvert et si des logiciels spéciaux, non autorisés sont à l'écoute. Il y a 3 boutons. Le premier, ports usuels (Common ports), scan les ports les plus courants. Le deuxième scan les ports utilisés fréquemment par les portes dérobées et le dernier scan les deux types de ports.

r FAV Rule Set 📔 🐋 Security Level 📔 😻 Firewall Log 🛛 🔝 S	hared Folders 🛛 🛒 Port	Scan	
Network Port Information			
Service	Port Number	Status	
🍓 Daytime	13	Close	
🖣 File Transfer (Default Data)	20	Close	
🖣 File Transfer [Control]	21	Close	
🍓 Unassigned	22	Close	
🧃 Telnet	23	Close	
🍓 any private mail system	24	Close	
🧃 Simple Mail Transfer	25	Close	
🧃 NSW User System FE	27	Close	
NSG ICP	29	Close	
NSG Authentication	31	Close	
🧃 Display Support Protocol	33	Close	
🧃 any private printer server	35	Close	
🧃 Time	37	Close	-
any private printer server Time	35 37	Close Close	