

PARAMETRAGE DES REGLES IPCOP BOOKTIC

Paramétrage des règles IPCOP.

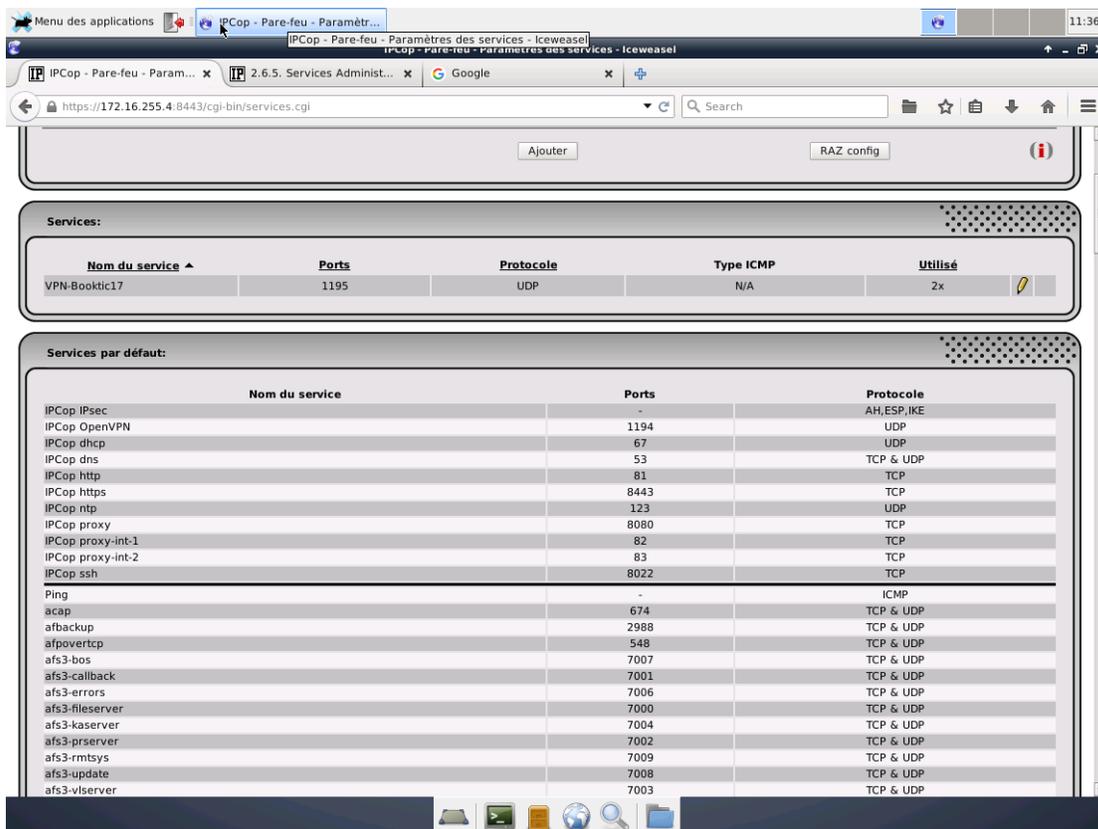
Pour créer les règles sur IPCOP, on effectue dans l'ordre ces opérations:

Paramétrage de la connexion VPN:

On commence par modifier les paramètres de connexion (port 1195 au lieu de 1194) sur les fichiers SRV.conf et client.conf du VPN de booktic.

on teste une connexion locale.

On crée ensuite un service (dans notre cas VPNbooktic17), afin d'autoriser la connexion.



The screenshot shows the IPCop web interface for service configuration. The browser address bar displays `https://172.16.255.4:8443/cgi-bin/services.cgi`. The interface includes a top navigation bar with buttons for 'Ajouter' and 'RAZ config'. Below this, there are two main sections: 'Services:' and 'Services par défaut:'. The 'Services:' section contains a table with one entry: 'VPN-Booktic17' on port 1195 using UDP. The 'Services par défaut:' section contains a larger table listing various default services and their protocols.

Nom du service	Ports	Protocole	Type ICMP	Utilisé
VPN-Booktic17	1195	UDP	N/A	2x

Nom du service	Ports	Protocole
IPCop IPsec	-	AH,ESP,IKE
IPCop OpenVPN	1194	UDP
IPCop dhcp	67	UDP
IPCop dns	53	TCP & UDP
IPCop http	81	TCP
IPCop https	8443	TCP
IPCop ntp	123	UDP
IPCop proxy	8080	TCP
IPCop proxy-int-1	82	TCP
IPCop proxy-int-2	83	TCP
IPCop ssh	8022	TCP
Ping	-	ICMP
acap	674	TCP & UDP
afbackup	2988	TCP & UDP
afpovertcp	548	TCP & UDP
afs3-bos	7007	TCP & UDP
afs3-callback	7001	TCP & UDP
afs3-errors	7006	TCP & UDP
afs3-filesystem	7000	TCP & UDP
afs3-kaserver	7004	TCP & UDP
afs3-prserver	7002	TCP & UDP
afs3-rmtsys	7009	TCP & UDP
afs3-update	7008	TCP & UDP
afs3-vlserver	7003	TCP & UDP

Menu des applications IPCop - Pare-feu - Paramétr... 11:37

IPCop - Pare-feu - Paramètres des services - Iceweasel

IPCop - Pare-feu - Param... x 2.6.5. Services Administr... x Google x

https://172.16.255.4:8443/cgi-bin/services.cgi

Pare-feu >> **Services**

Système Etat Réseau Services Pare-feu RPVs Journaux

Modifier les services:

Nom du service: VPN-Booktic17

Protocole: UDP Inverser:

Ports: 1195 Inverser:

Type ICMP: -- Types d'ICMP valides --

Mise à Jour RAZ config

Services:

Nom du service	Ports	Protocole	Type ICMP	Utilisé
VPN-Booktic17	1195	UDP	N/A	2x

Services par défaut:

Nom du service	Ports	Protocole
IPCop IPsec	-	AH,ESP,IKE
IPCop OpenVPN	1194	UDP
IPCop dhcp	67	UDP
IPCop dns	53	TCP & UDP
IPCop http	81	TCP
IPCop https	8443	TCP
IPCop ntp	123	UDP
IPCop proxy	8080	TCP
IPCop_proxy-int-1	82	TCP

Une fois le service établi, on crée un transfert de port:

The screenshot displays the IPCop configuration interface for the firewall. The browser window shows the URL `https://172.16.255.4:8443/cgi-bin/fwrules.cgi`. The interface is divided into several sections for configuring firewall rules:

- Trafic en sortie:** A table with 3 rules. Rule 1: Source 172.16.10.1, Destination Any: domain. Rule 2: Source 172.16.10.7, Destination Any: http. Rule 3: Source 172.16.10.7, Destination Any: https.
- Accès IPCop:** A table for external access to the firewall.
- Trafic Interne:** A table for internal traffic rules.
- Transferts de ports:** A table with 1 rule. Rule 1: Source Any, Destination interne 172.16.10.10: VPN-Booktic17.
- Accès Externe IPCop:** A table for external access to services.

Légende:

- Règle d'acceptation standard
- Règle d'Interdiction
- Règle de Journaliser, seulement Journaliser
- Règle avancée acceptée, Pare-Feu ouvert
- Activé (cliquer pour désactiver)
- Désactivé (cliquer pour activer)
- Journalisé Activé (cliquer pour désactiver)
- Journalisé Désactivé (cliquer pour activer)

On doit établir un nouveau service car IPcop possède son propre serveur VPN sur le port 1194

Menu des applications | IPCop - Configuration du Pare-Feu - Iceweasel | 11:49

IPCop - Configuration du Pare-Feu - Iceweasel

https://172.16.255.4:8443/cgi-bin/fwrules.cgi

Source

- Adresse: Any
- Format d'adresse: IP Adresse Source (MAC ou IP ou réseau):

Port source utilisé:
Port source:

Destination externe IPCop

Alias IP: Red Address

- Services: VPN-Booktic17
- Services par défaut: -- Services par défaut --

Destination interne

réseau interne

Interface par défaut: VERT

Adresse IP de destination: 172.16.10.10

- Services: VPN-Booktic17
- Services par défaut: -- Services par défaut --

Additionnel

- Règle activée
- La règle de Journaliser

Remarque:

⚠ Ce champ peut être vide.

Taskbar: Computer, Terminal, File Manager, Network, Search, Mail

On change le port du VPN dans les certificats client et serveur et on vérifie la connexion en activant le VPN, et on vérifie la connexion. Si le message Initialization Sequence Completed s'affiche, c'est gagné !....

On crée ensuite les règles les unes après les autres:

http, https: uniquement le serveur proxy (172.16.10.7)

Pour tester on peut utiliser les commandes suivantes:

sur ipcop, iptables -F, telnet, nslookup, tcpdump

The screenshot shows the IPCop configuration interface in a web browser. The page title is "IPCop - Configuration du Pare-Feu - Iceweasel". The browser address bar shows the URL "https://172.16.255.4:8443/cgi-bin/fwrules.cgi". The main content area is titled "Règles actuelles:" and contains several sections of firewall rules:

- Trafic en sortie:** A table with 4 rules. Each rule has a "VERT" status, a source IP of 172.16.10.1 or 172.16.10.7, a "Rouge" destination interface, and a specific destination (domain, http, https, Ping). Each rule has a set of action icons (checkbox, X, pencil, trash, up arrow).
- Accès IPCop:** A table with columns for #, Réseau Interface, Source, Destination, Remarque, and Action.
- Trafic Interne:** A table with columns for #, Réseau Interface, Source, Réseau Interface, Destination, Remarque, and Action.
- Transferts de ports:** A table with 1 rule. The source is "Tout", the destination interface is "VERT", and the destination is "172.16.10.10 : VPN-Booktic17".
- Accès Externe IPCop:** A table with columns for #, Réseau Interface, Source, Destination, Remarque, and Action.

At the bottom of the interface, there are four legend items: "Règle d'acceptation" (green arrow), "Règle d'interdiction" (red arrow), "Règle de journaliser," (green arrow), and "Règle avancée acceptée," (red arrow).

Ne pas oublier d'autoriser le serveur proxy sur le http et https Les règles une fois établies:

The screenshot shows the IPCop web interface for configuring services. The browser window title is "IPCop - Pare-feu - Paramètres des services - Iceweasel". The address bar shows the URL "https://172.16.255.4:8443/cgi-bin/services.cgi".

Services:

Nom du service	Ports	Protocole	Type ICMP	Utilisé
VPN-Booktic17	1195	UDP	N/A	2x
Web-booktic17	8081	TCP	N/A	2x

Services par défaut:

Nom du service	Ports	Protocole
IPCop IPsec		AH,ESP,IKE
IPCop OpenVPN	1194	UDP
IPCop dhcp	67	UDP
IPCop dns	53	TCP & UDP
IPCop http	81	TCP
IPCop https	8443	TCP
IPCop ntp	123	UDP
IPCop proxy	8080	TCP
IPCop proxy-int-1	82	TCP
IPCop proxy-int-2	83	TCP
IPCop ssh	8022	TCP
Ping	-	ICMP
acap	674	TCP & UDP
afbackup	2988	TCP & UDP
afpovertcp	548	TCP & UDP
afs3-bos	7007	TCP & UDP

Afin que l'on puisse se connecter de l'extérieure vers la dmz, on définit un nouveau service:

The screenshot displays the IPCop configuration interface for a firewall. The browser address bar shows the URL `https://172.16.255.4:8443/cgi-bin/fwrules.cgi`. The main content area is titled "Transferts de ports:" and contains a table of port forwarding rules. Below this is a section for "Accès Externe IPCop:" with a single rule for HTTP access. A legend at the bottom explains the icons used in the interface.

#	Réseau Interface	Source	Réseau Interface	Destination interne	Remarque	Action
1	Tout	Any	VERT	172.16.10.10 : VPN-Booktic17		<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2	Tout	Any	ORANGE	192.168.10.3 : http		<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Destination externe IPCop: Red Address : Web-booktic17

#	Réseau Interface	Source	Destination	Remarque	Action
1	Rouge	Any	IPCop : Web-booktic17		<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Légende:

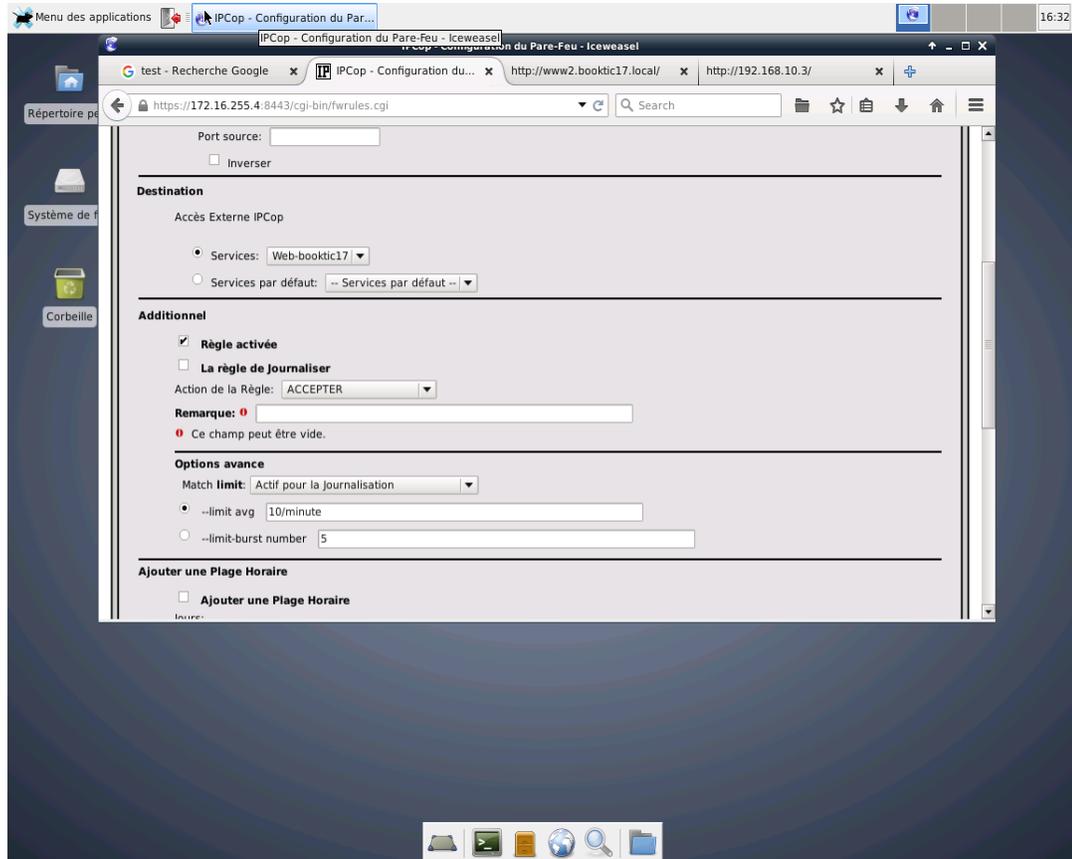
- Règle d'acceptation standard
- Règle d'interdiction
- Règle de journaliser, seulement journaliser
- Règle avancée acceptée, Pare-Feu ouvert
- Activé (cliquer pour désactiver)
- Désactivé (cliquer pour activer)
- Journalisé Activé (cliquer pour désactiver)
- Journalisé Désactivé (cliquer pour activer)
- Modifier
- Copier une règle
- Supprimer
- Monter
- Vers le bas

sourceforge

Connecté (0d 5h 25m 32s)
2016-04-22 18:30:43

IPCop v2.1.8 © 2001-2015 The IPCop Team

On crée ensuite une règle d'accès externe:



Menu des applications | IPCop - Configuration du Pare-Feu - Iceweasel | 16:34

IPCop - Configuration du Pare-Feu - Iceweasel

test - Recherche Google | IPCop - Configuration du Pare-Feu - Iceweasel | http://www2.booktic17.local/ | http://192.168.10.3/

https://172.16.255.4:8443/cgi-bin/fwrules.cgi

Adresse: Any
 Format d'adresse: IP Adresse Source (MAC ou IP ou réseau):

Port source utilisé:
Port source:

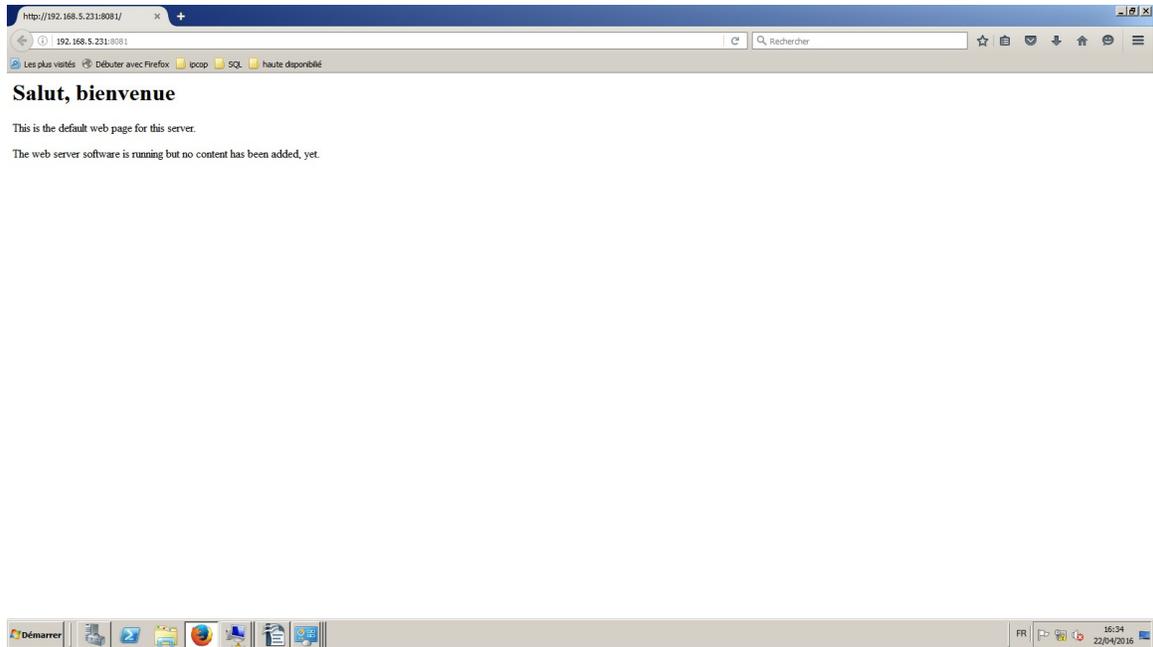
Destination externe IPCop
Alias IP: Red Address
 Services: Web-booktic17
 Services par défaut: Services par défaut

Destination interne
réseau interne
Interface par défaut: ORANGE
Adresse IP de destination: 192.168.10.3
 Services: VPN-Booktic17
 Services par défaut: http (80)

Additionnel
 Active-est-actif



Puis on créé un transfert de port vers la machine du failover:



Vue des règles:

Menu des applications | IPCop - Configuration du Pare-Feu - Ickeaseel | 16:36

IPCop - Configuration du Pare-Feu - Ickeaseel

test - Recherche Google | IPCop - Configuration du... | http://www2.booktic17.local/ | http://192.168.10.3/

https://172.16.255.4:8443/cgi-bin/fwrules.cgi

#	Réseau Interface	Source	Réseau Interface	Destination	Remarque	Action
1	VERT	172.16.10.1	ROUGE	Any : domain		<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
2	VERT	172.16.10.7	ROUGE	Any : http		<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
3	VERT	172.16.10.7	ROUGE	Any : https		<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
4	VERT	172.16.10.7	ROUGE	Any : Ping		<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Acces IPCop:

#	Réseau Interface	Source	Réseau Interface	Destination	Remarque	Action
1	VERT	Any	ORANGE	Any		<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Trafic Interne:

#	Réseau Interface	Source	Réseau Interface	Destination	Remarque	Action
1	VERT	Any	ORANGE	Any		<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Transferts de ports:

#	Réseau Interface	Source	Réseau Interface	Destination interne	Remarque	Action
1	Tout	Any	VERT	172.16.10.10 : VPN-Booktic17		<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
2	Tout	Any	ORANGE	192.168.10.3 : http		<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Destination externe IPCop: Red Address : Web-booktic17

Accès Externe IPCop:

#	Réseau Interface	Source	Réseau Interface	Destination	Remarque	Action
1	ROUGE	Any	IPCop	IPCop : Web-booktic17		<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Légende:

- Règle d'acceptation standard
- Règle d'interdiction
- Règle de Journaliser, seulement Journaliser
- Règle avancée acceptée, Pare-Feu ouvert
- Activé (cliquer pour désactiver)
- Désactivé (cliquer pour activer)
- Journalisé Activé (cliquer pour désactiver)
- Journalisé Désactivé (cliquer pour activer)
- Modifier
- Copier une règle
- Supprimer
- Monter
- Vers le bas

Connecté (0d 5h 30m 13s)
2016-04-27 10:35:24