PARAMETRAGE DES REGLES IPCOP BOOKTIC

Paramétrage des règles IPCOP.

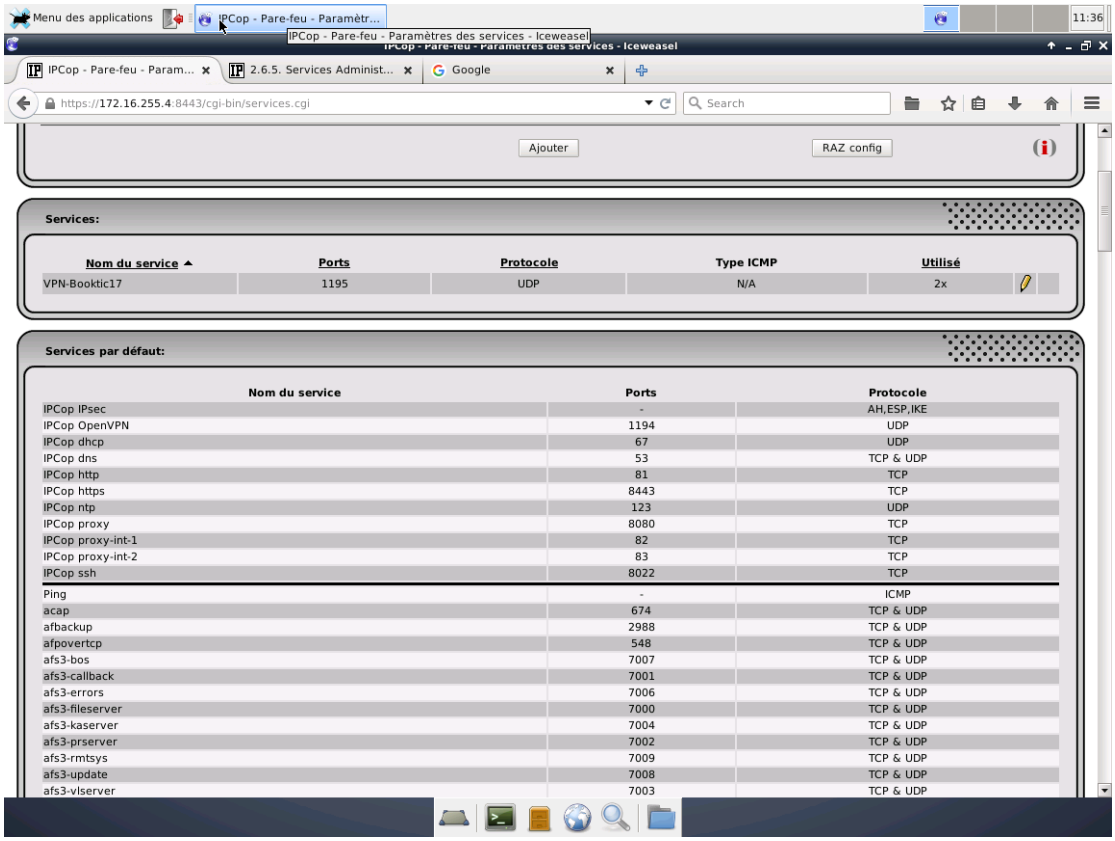
Pour créer les règles sur IPCOP, on effectue dans l'ordre ces opérations:

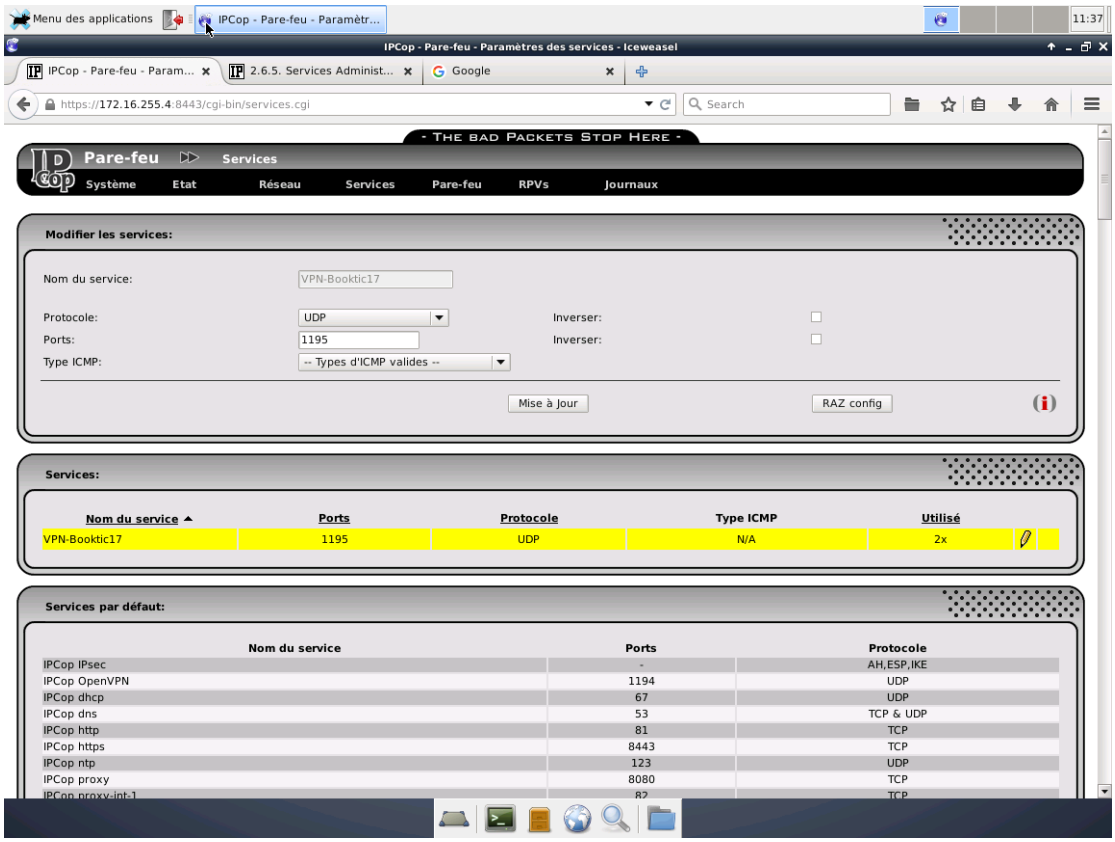
Paramétrage de la connexion VPN:

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.

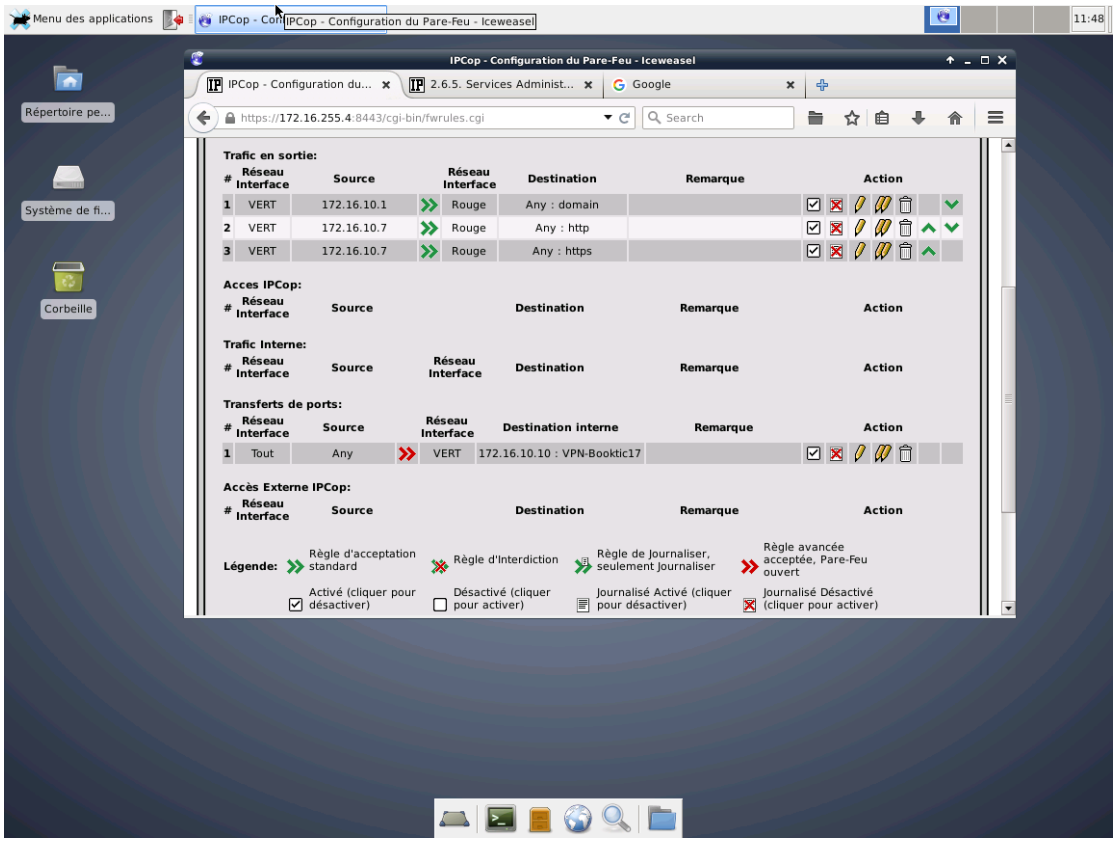
on teste une connexion locale.

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



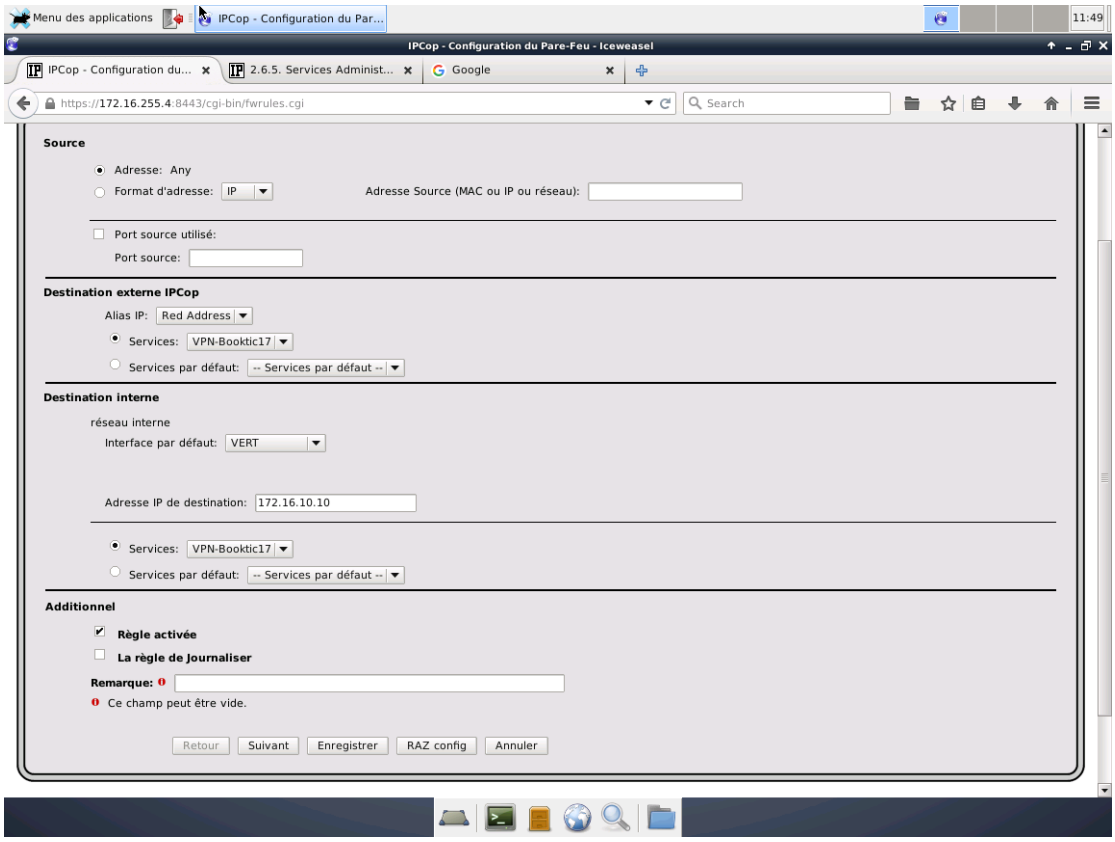

Menu des applications
IPCop - Pare-feu - Paramètr...
11:37
IPCop - Pare-feu - Paramètres des services - Iceweasel
IPCop - Pare-feu - Param...
2.6.5. Services Administ...
Google
https://172.16.255.4:8443/cgi-bin/services.cgi
Search
- THE BAD PACKETS STOP HERE -
Pare-feu
Services
Système
Etat
Réseau
Services
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 créé un transfert de port:



:

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


Menu des applications
IPCop - Configuration du Par...
11:49
IPCop - Configuration du Pare-Feu - Iceweasel
IPCop - Configuration du...
2.6.5. Services Administ...
Google
https://172.16.255.4:8443/cgi-bin/fwrules.cgi
Search
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.
Retour
Suivant
Enregistrer
RAZ config
Annuler

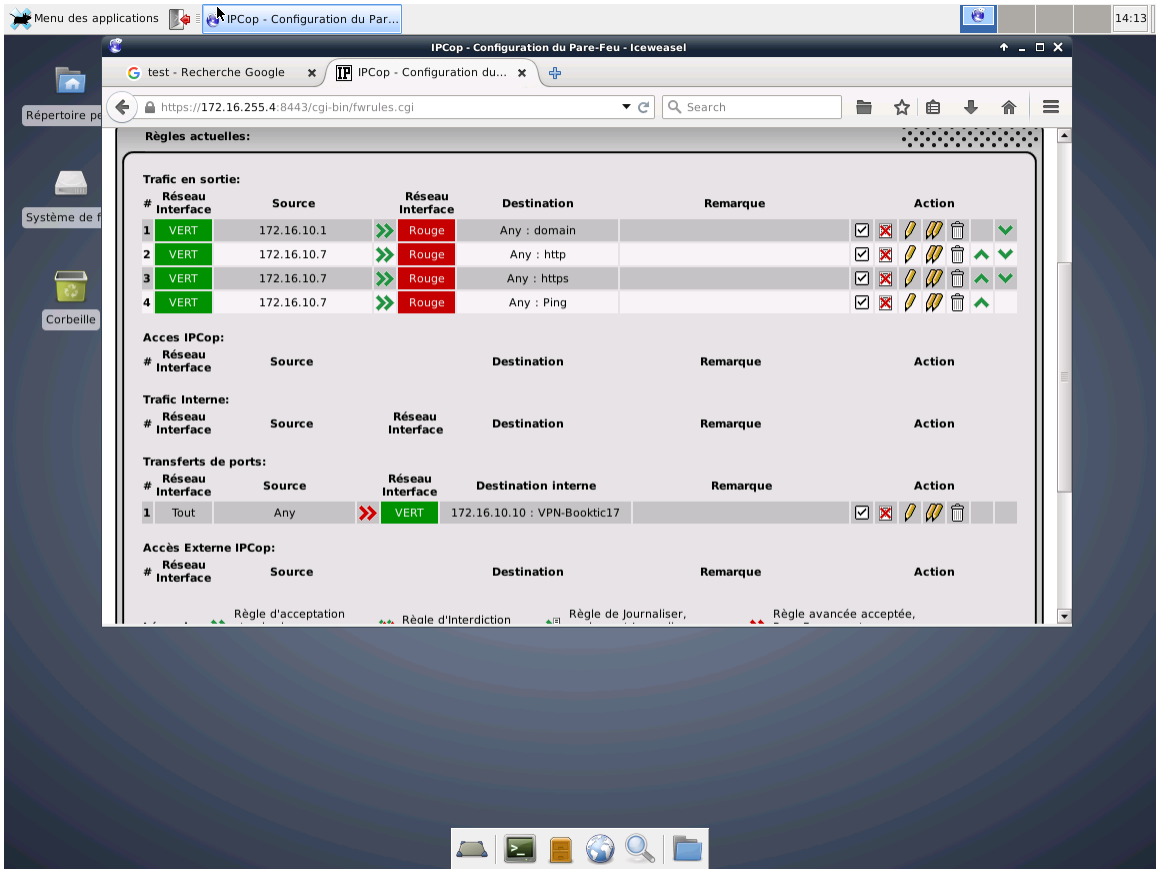
On change le port du VPN dans les certificats client et serveur et on vérifie la connexion en activant le VPN, et on vérifie la connexion.S i le message Initialization Sequence Completed s'affiche, c'est gagné !....

On créé ensuite les règles les unes après les autres:

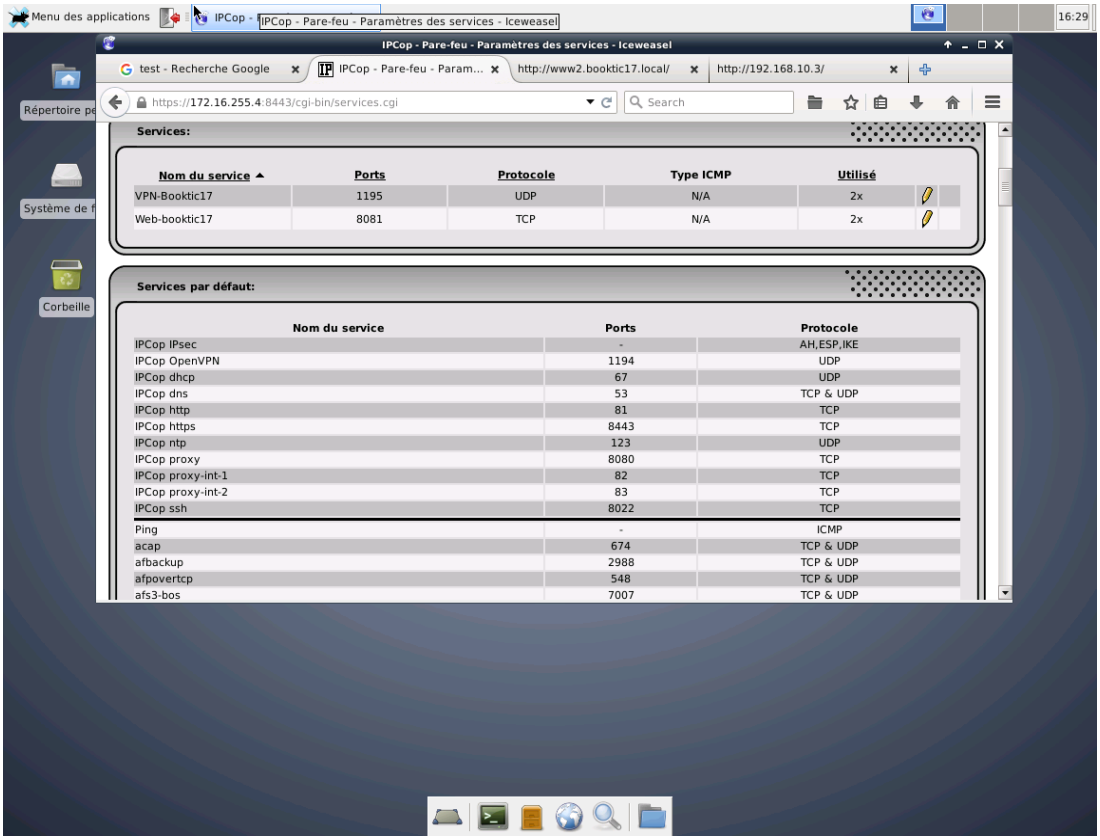
http, https: uniquement le serveur proxy (172.16.10.7)

Pour tester on peut utiliser les commandes suivantes:

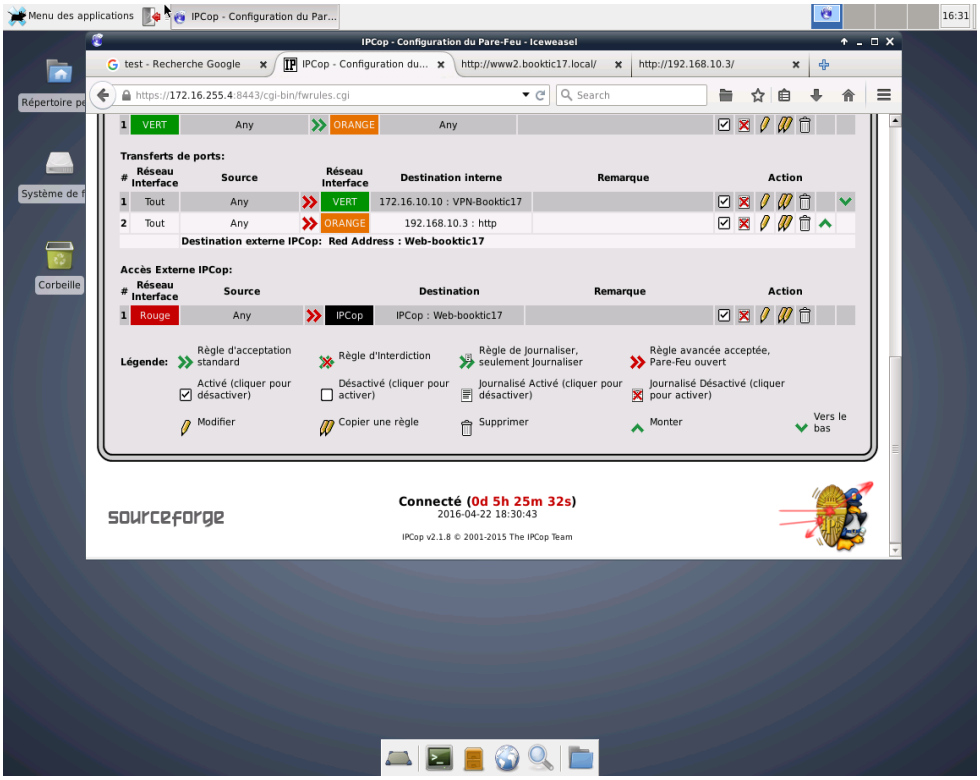
sur ipcop, iptables -F,telnet,nslookup,tcpdump



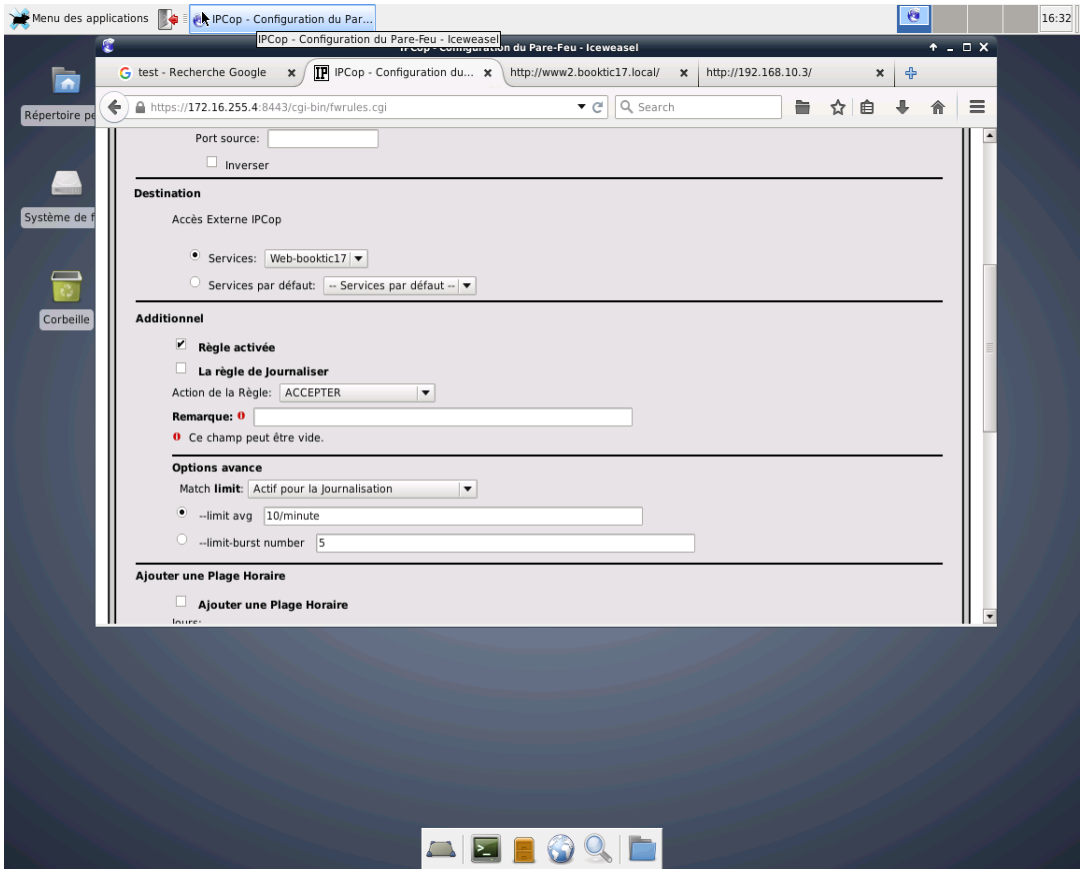
Ne pas oublier d'autoriser le serveur proxy sur le http et https Les règles une fois établies:

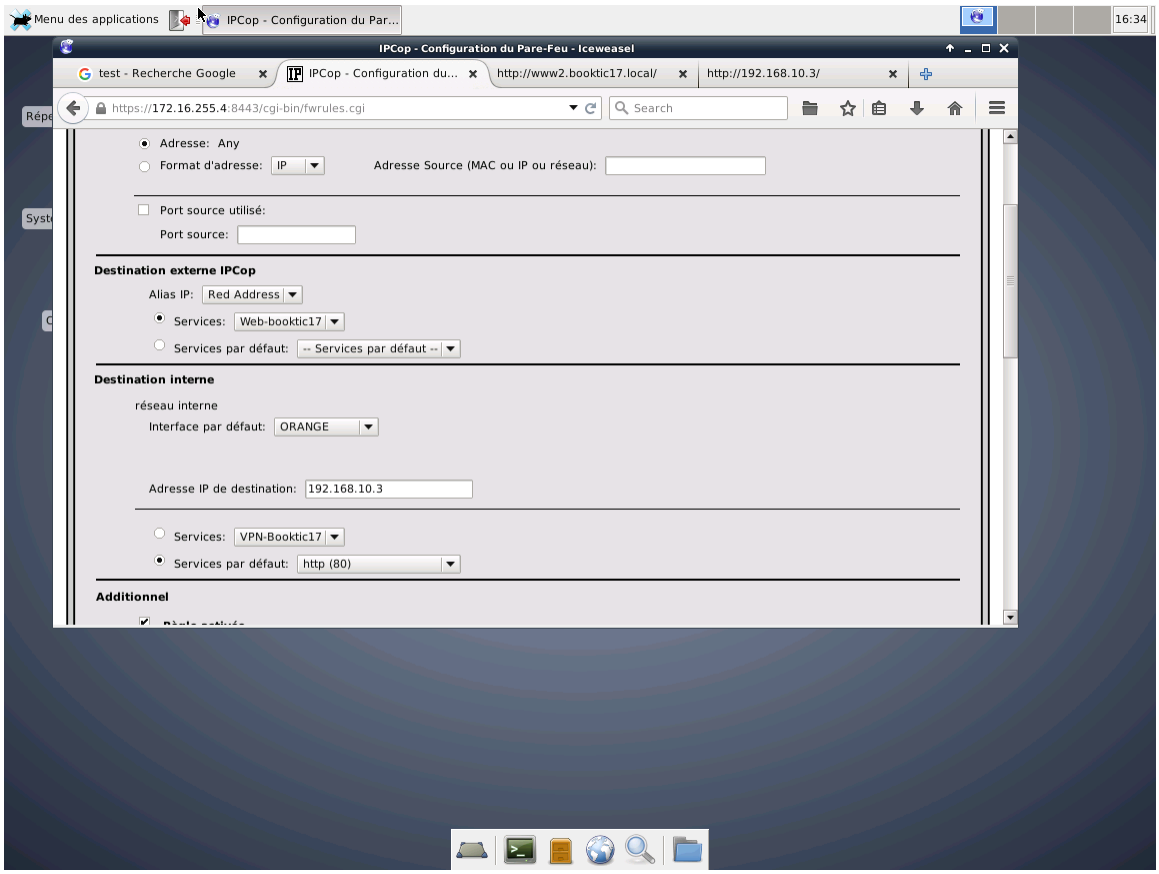


Afin que l'on puisse se connecter de l'extérieure vers la dmz, on définit un nouveau service:

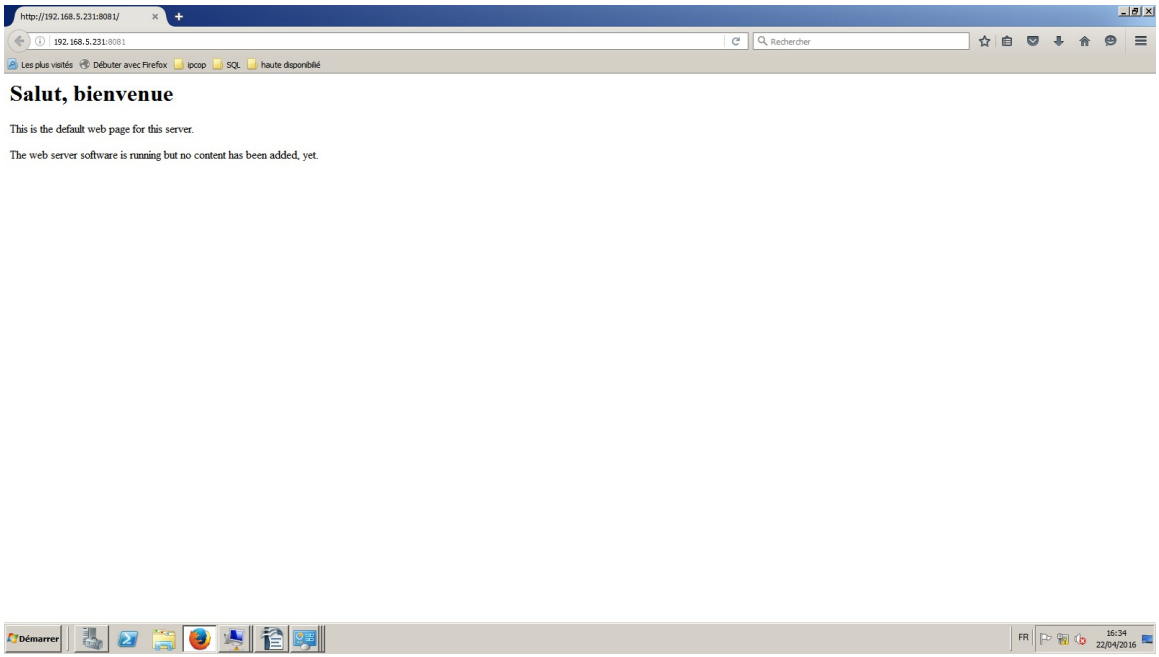


On créé ensuite une règle d'accès externe:




Menu des applications
IPCop - Configuration du Par...
16:34
IPCop - Configuration du Pare-Feu - Iceweasel
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
Search
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

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



Vue des règles: