



S E C U R I N E T S
Club de la sécurité informatique
INSAT

Atelier IPCOP

IPCOP : distribution Linux complète à noyau allégé orientée pour des objectifs de sécurité.

1. Caractéristiques :

Pare feu	Stable
Client DHCP	Obtention automatique d'une adresse IP pour Ipcop
Serveur DHCP	Attribution des adresses IP aux machines du réseau interne
Serveur DNS	Résolution des noms des domaines
Proxy	Accélérer l'accès au web
IDS	Détection des intrusions
Configuration de la bande passante	Réserver des parties plus intéressantes que des autres pour les services « gourmands » tels que FTP
Segmentation du réseau	Vert (réseau protégé) ; Bleu (Wifi) ; Orange (zone DMZ) ; Rouge (réseau de connexion à l'Internet).

2. Méthodes d'accès :

Pour accéder à IPCOP, nous disposons de deux possibilités requises par ce système :

- A travers une ligne de commande



S E C U R I N E T S
Club de la sécurité informatique
INSAT

- A travers une interface graphique tout en saisissant dans un navigateur l'adresse IP de l'interface VERTE, ou bien le nom d'hôte du serveur IPCop suivi du numéro de port 445 (https/secure) ou 81.

3. Onglets :

Les pages web d'administration d'IPCop sont accessibles par des onglets en haut de l'écran :

Système	Configuration du système et fonctions associées à IPCop.
Etat	Présentation détaillée de l'état de plusieurs éléments de votre serveur IPCop.
Réseau	Configuration/Administration de vos paramètres de connexion.
Services	Configuration/Administration de nombreux services optionnels de votre serveur IPCop.
Pare-feu	Configuration/Administration de la fonction pare-feu de votre serveur IPCop.
RPVs	Configuration/Administration de votre éventuel Réseau Privé Virtuel.
Journaux	Consultation de tous les journaux d'évènements générés par votre serveur IPCop (pare-feu, sonde de détection d'intrusion, etc).

4. Potentialités d'IPCOP :

- **Systeme de detection d'intrusion (IDS):** IPCop intègre un puissant système de détection d'intrusion nommé Snort. Il offre également la possibilité de contrôler les paquets réseau sur toutes les interfaces, il suffit de cocher ceci dans l'interface graphique système de détection des intrusions.



S E C U R I N E T S
Club de la sécurité informatique
INSAT

En effet, Snort est connu par sa capacité d'effectuer en temps réel des analyses de trafic et de logger les paquets sur un réseau IP. Il peut effectuer des analyses de protocole, recherche/correspondance de contenu et peut être utilisé pour détecter une grande variété d'attaques et de sondes comme des dépassements de buffers, scans mais il faut toujours envisager une mise à jour régulière pour assurer sa fiabilité.

- *Pare-feu*: Cet onglet nous permet de présenter les fonctionnalités pour contrôler les flux traversant notre pare-feu.

Transferts de ports	Permet seulement d'ouvrir à l'extérieur des ports de votre machine IPCop mais pas vos réseaux VERT ou ORANGE.
Accès externes	La configuration d'accès de maintenance de votre IPCop depuis l'extérieur
Accès à la DMZ	Paramétrer les accès au réseau VERT depuis la DMZ.
Accès au réseau BLEU	Permet de connecter un point d'accès sans-fil à IPCop.
des options d u pare-feu	Permet de configurer plus finement certains comportements du pare-feu.

- *Lissage de Traffic 'Shaping'*: Il nous permet d'assigner des priorités aux flux IP traversant le pare-feu. IPCop fait appel pour cela à WonderShaper afin de minimiser la latence au ping et garantir que les services interactifs.



S E C U R I N E T S
Club de la sécurité informatique
INSAT

IPcop gère ce phénomène tout en assignant des priorités aux flux. Ces derniers seront regroupés en trois catégories de priorités différentes : Haute, Moyenne et Basse.

- **Virtual Private Networks (VPNs)** ou Réseau Privé Virtuel (RPV) : IPCop peut facilement établir des VPNs (Virtual Private Network) avec d'autres serveurs IPCop. Il suffit de saisir les différentes données utiles pour l'établissement de la connexion. En effet un VPN est une extension des réseaux locaux qui procure une norme de sécurité en télécommunications. Il repose sur le protocole appelé "protocole de tunneling". Son principe consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel.