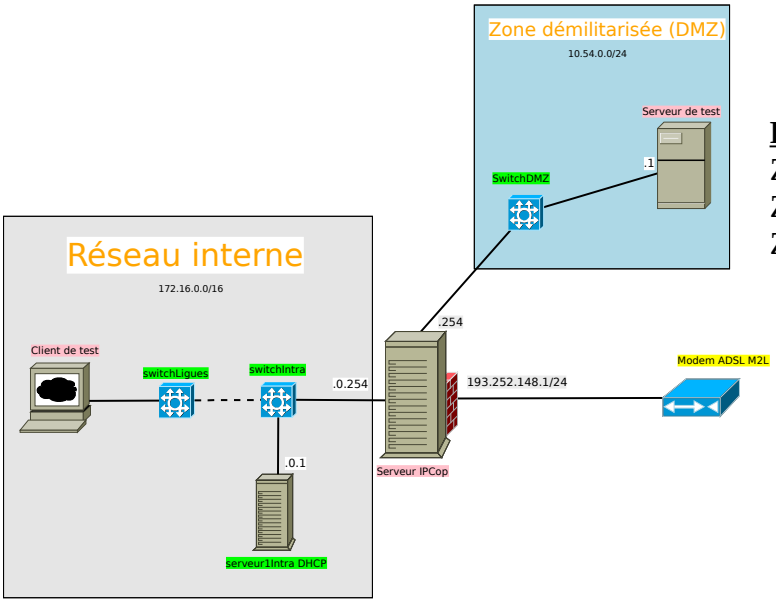
Tests et validation de la solution de pare-feu à états IPCop

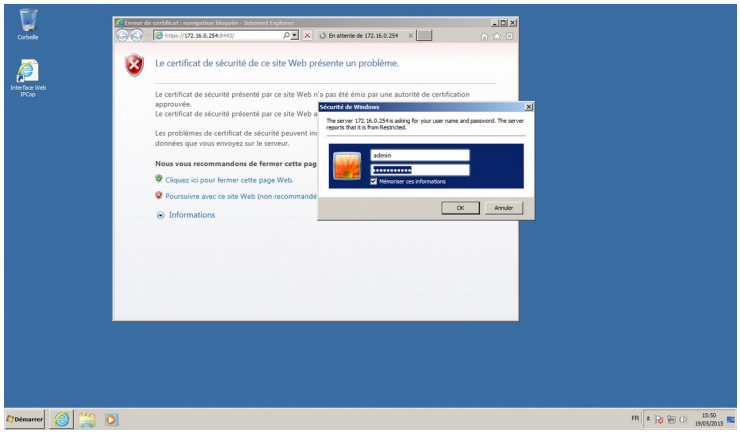
Pour rappel, voici le schéma actuel du réseau avec le pare-feu à états IPCop d'installé :

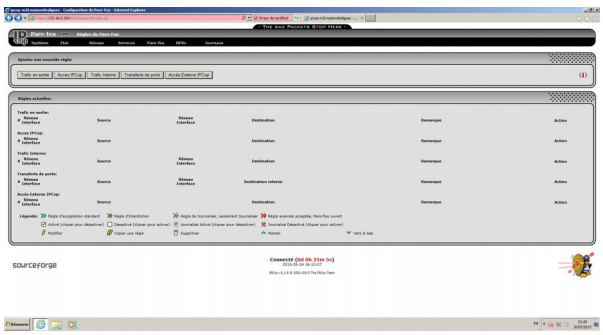


Petit rappel :
Zone vert : Réseau interne
Zone orange : Zone démilitarisée (DMZ)
Zone rouge : Zone en amont du serveur IPCop

Afin de démontrer le bon fonctionnement du pare-feu à états IPCop, je vais dans un premier temps bloquer les requêtes de ping sortants du réseau vert et le port 443 utilisé par les connexions cryptés de type SSL (https).

Via un navigateur, j'**accède à l'interface web du pare-feu IPCop** (**http://172.16.0.254:8443**) **depuis un client de la zone verte.**

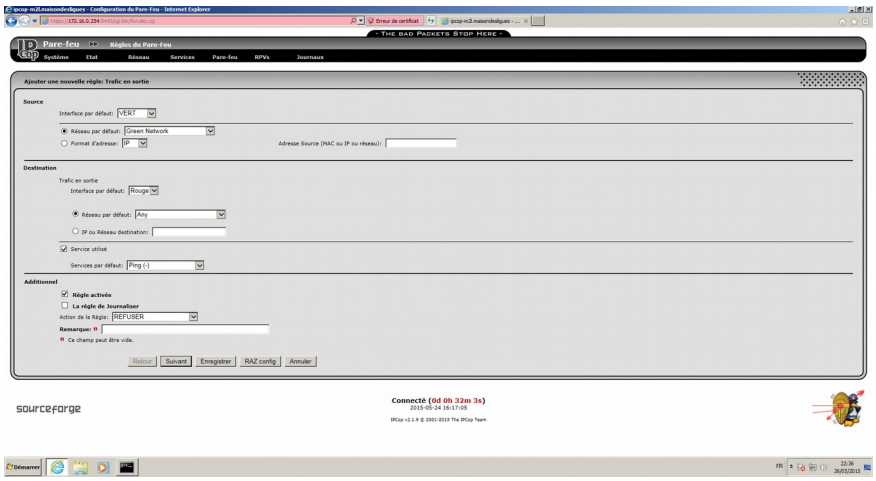




Une fois authentifié, je me rends dans **Pare-feu → Règles du pare-feu**

Dans « Ajouter une nouvelle règle: », je clique sur le bouton « **Trafic en sortie** »

Je complète ensuite avec les informations suivantes :



Source:
Interface: Green
Adresse: Green Network

Destination: Trafic en sortie
Interface: Red
Adresse IP: Any
Service: **Ping**

Action de la Règle: **REFUSER**
Règle activée: on
La règle de Journaliser: off
Remarque:

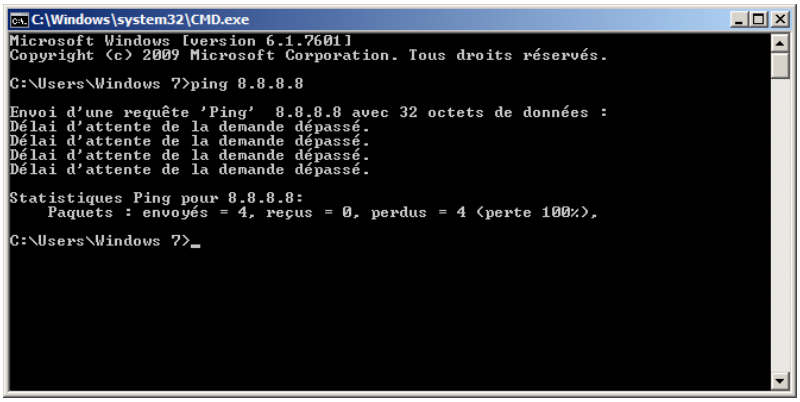
Une fois fait, je clique sur le bouton « **Enregistrer** ». Puis je recommence cette fois-ci pour bloquer le port **443 (https)**.

Source:
Interface: Green
Adresse: Green Network

Destination: Trafic en sortie
Interface: Red
Adresse IP: Any
Service: **https (443)**

Action de la Règle: **REFUSER**
Règle activée: on
La règle de Journaliser: off
Remarque:

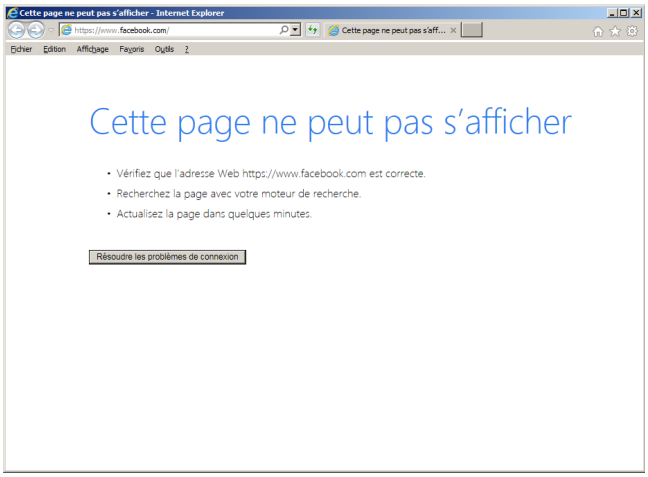
Une fois créées, les règles sont immédiatement actives.



Afin de vérifier le bon fonctionnement de la première règle qui bloque les pings.

J'essaie donc de pinger le serveur DNS de Google ayant pour adresse 8.8.8.8 depuis un client du réseau vert.

Comme vous pourrez le voir sur la capture d'écran ci-contre, les requêtes de ping n'aboutissent pas. Le filtre est donc a priori actif.



Afin de vérifier le bon fonctionnement de la deuxième règle qui bloque les connexions cryptés de type SSL (https), j'essaie d'accéder à une URL https, https://www.facebook.com . Comme vous pourrez le voir sur la capture d'écran ci-contre, le navigateur ne peut afficher cet URL. Le filtre est donc a priori actif.

Après désactivation ou suppression de ces deux règles dans l'interface web, les requêtes de ping et les connexions aux urls https se font naturellement. Ainsi, le pare-feu IPCop est bel et bien actif sur le réseau et fonctionne correctement selon la configuration à laquelle il est soumis.