Contexte de la situation professionnelle : Contexte TiersLieux
La société Tiers Lieux dispose de plusieurs sites départementaux répartis sur la France.

Mission AccesInternetSécurisé Partie 1: Vous êtes chargé de mettre en place l'accès à Internet au niveau de votre agence. Vous mettrez en place la NAT, la redirection DNS, les règles de filtrage de ports, le portail captif et/ou le proxy transparent permettant cet accès contrôlé et sécurisé.

Opérations de base à réaliser :

- Mettre en place la NAT afin de pouvoir accéder à Internet depuis n'importe quel vlan
- Le protocole ICMP doit être interdit sur l'interface publique du parefeu
- Le protocole DNS doit être autorisé en entrée et en sortie du parefeu
- La redirection DNS doit être supportée afin de résoudre n'importe quel domaine et accéder à n'importe quel site internet en HTTP ou HTTPS
- Proposer un ensemble de règles pour le filtrage d'URL et le filtrage applicatif afin d'interdire l'accès aux réseaux sociaux, aux sites de e-commerces… pendant les horaires de bureau (7h-17h)
- La configuration de la solution de proxy doit être en proxy transparent et ne pas pouvoir être contournée par le paramétrage réseau et/ou navigateur des postes

Implémentation de nouveaux besoins
le RSSI vous demande de prendre en compte les besoins suivants.

A) Interdire explicitement les plages d'adresses du groupe RFC 57351 provenant d'Internet.

B) Toutes les machines provenant d'Internet et ayant une réputation de Botnet, Malware, Scanneur, Noeud de sortie Tor, Anonymiseur ou Phishing ont interdiction d'accéder à l'interface externe du firewall.

C) L'ensemble des hôtes du site de TiersLieux ont interdiction de pouvoir émettre des requêtes vers des machines sur Internet considérées comme Botnet, Malware, Scanneur, Noeud de sortie Tor, Anonymiseur ou Phishing.

Productions attendues semestre 1:

- Produire la liste des tâches à réaliser, le schéma du réseau et son plan d'adressage
- Mettre en place les fonctionnalités demandées (filtrage URL…) et les tester
- Montrer que les protocoles DNS et ICMP sont contrôlés comme demandé. Produire la capture de trames (éventuellement les logs) qui le prouve.
- Montrer que l'accès internet ne peut se faire que via le portail captif. Produire la capture de trames (éventuellement les logs) qui le prouve.
- Montrer que l'accès internet ne peut se faire que via le proxy transparent. Produire la capture de trames (éventuellement les logs) qui le prouve.

Ressources :
TD Firewall, Proxy, NAT, Annexe Iptables
Fiches Support Stormshield

Logiciels possibles :
parefeu Stormshield SNS virtuel ou physique