1. Mise en œuvre du filtrage pour le contexte

Vous devez mettre en oeuvre une politique de filtrage protocolaire avec votre pare-feu Stormshield en tenant compte des recommandations de l'ANSSI.

1.1. Configuration de votre infrastructure

Vous avez dans la DMZ :

- un serveur NS0 qui a autorité sur la zone DNS de votre agence
- un serveur Web
- etc.

Vous avez dans le VLAN Serveurs :

- un serveur DHCP
- un contrôleur de domaine Active Directory pour votre agence
- etc.

Vous avez dans le VLAN Utilisateurs :

- un résolveur DNS0
- un agent-relais DHCP

Pour ces différents serveurs, respectez le plan d'adressage défini dans ces VLAN et utilisez des adresses IP statique mises à disposition pour chaque équipe.

Lien : Ressources pour le APs

1.2. Mise en oeuvre d'une politique de filtrage

La mise en oeuvre de votre politique de filtrage doit s'appuyer sur les recommandations de l'ANSII.

Complétez ce document avec les règles à mettre en oeuvre :

politiquefiltrage.odt

1.2.1. Section 1 – Règles d’autorisation des flux à destination du pare-feu

- autoriser les flux d'administration (https 443 en TCP, éventuellement ssh 22 en TCP) pour un PC identifié comme **PC d'administration** ;
- **autorisez** les flux vers :
  - le serveur **Web** (http 80 en TCP) avec une **redirection de port**,
  - le serveur **DNS** (dns 53 en UDP) avec une **redirection de port**.
- Pour des tests, les utilisateurs des autres réseaux sont autorisés à **pinger** l’interface externe de votre SNS ; cet événement devra lever une alarme mineure.

1.2.2. Section n°2 - Règles d’autorisation des flux émis par le pare-feu

Pour l'instant, ne définissez pas de règles

1.2.3. Section n°3 Règle de protection du pare-feu

- **Bloquer** tout ce qui arrive sur les interfaces du SNS suite aux autorisations définies dans la section 1. Cela est impératif pour prévenir l’ouverture de flux non légitimes à destination de la passerelle.
- journaliser cette règle afin de conserver la trace de ces flux illégitimes.

1.2.4. Section n°4 Règles d’autorisation des flux métiers

- autoriser depuis le poste administrateur :
  - les flux d'administration (22 SSH en TCP ; 3389 RDP en TCP - bureau à distance) vers les serveurs (DNS, résolveur DNS, serveur Web, DHCP, agent-relais, contrôleur Active Directory)
  - les flux vers le serveur de temps de l'Université de Tours qui a l'adresse IP 193.52.212.3 et port UDP 123.

- Interdire au PC d'administation l'accès à tout autre réseau (Ici Internet). En effet, ce poste ayant des privilèges élevés sur le réseau, le fait de lui bloquer entre autres l'accès internet permet de réduire considérablement sa surface d'attaque.
- seul le **serveur récursif DNS** peut rediriger les requêtes des clients vers le **serveur DNS cub.fr**.
- les autres ordinateurs doivent pouvoir utiliser le **résolveur DNS** du VLAN serveurs
- pour l'instant autoriser les flux des réseaux internes vers Internet (http 80, https 443 en TCP).

- autoriser les flux des réseaux internes vers le serveur de temps.
- les serveurs de la **DMZ** :
    - ne doivent pas avoir accès au réseau utilisateurs sauf pour le résolveur DNS. En cas de compromission d'un des serveurs hébergés, il doit être impossible de pouvoir remonter vers un des VLAN de l'entreprise.
    - doivent pouvoir accéder à Internet et au **serveur de temps**
- pour pouvoir effectuer des **tests**, autorisez le **protocole ICMP** depuis les **réseaux internes**

1.2.5. Section n°5 Règles "antiparasites" (facultatif)

Pour l'instant, ne définissez pas de règles

1.2.6. Section n°6 Règle d'interdiction finale

L'ajout d'une règle explicite d'interdiction finale journalisée garantit l'application du modèle de sécurité positif (tout ce qui n'a pas été autorisé précédemment est interdit) et permet de conserver la trace des flux non légitimes.

- **Vérifiez** que toutes les VM (serveurs et clients) accèdent à Internet : configurer le NAT dynamique ;
- Vos serveurs NS0 et Web doivent être **accessibles depuis Internet (CUB WAN)** : configurez du NAT sur destination (redirection de ports) ;

1.3. Implémentation de nouveaux besoins

Suite à une analyse des besoins de l'entreprise et des fonctionnalités avancées de l'appliance Stormshield, vous prenez en compte les besoins suivants.

- Interdire explicitement les plages d'adresses du groupe RFC 5735 provenant d'Internet.
- 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.
- L'ensemble des hôtes du site ont interdiction de pouvoir émettre des requêtes vers des machines sur Internet considérées comme Botnet, Malware, Scanneur, Noeud de sortie Tor, Anonymiseur ou Phishing.

1.3.1. Retour

- Mise en oeuvre de l'UTM Stormshield

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/activite4filtrage

Last update: **2025/11/11 20:39**