le cnam

SEC 102 - TP10
Veille

Date	Version	Description	Auteurs
11/06/2023	1	Retranscription collective des informations présentées en cours	Bartel Cantin Bialas Alexis Dufourt Marvin Faussurier Marc N'Guessan Jérémy

Sommaire

1. Contexte

Nous avons un serveur physique sur lequel nous faisons de la virtualisation avec l'hyperviseur Proxmox qui est basé sur du Debian, Debian étant une distribution fonctionnant sur un noyau Linux.

Proxmox virtualise toutes nos machines virtuelles qui fonctionne avec des cartes réseaux dédié puis un accès par pont pour internet.

2. Rappel de la Problématique

L'une des failles que nous avons détecté avec Nessus est que le serveur ouvre par défaut le port 8006 pour l'administration du serveur via une interface web.
Cela est tout à fait normale, il s'agit du port qui nous permet d'accéder à l'interface de gestion de Proxmox via une interface web.
Mais dans ce scénario, un attaquant effectuant un scan des ports afin de savoir lesquels sont ouvert remarquerai que le port 8006 est ouvert. Cela nous expose à un grand danger en matière de cybersécurité.
Par ailleurs, si nous poussons le raisonnement plus loin, ce petit scan donne à l'attaquant aguerri une information de haute importance. Le fait que par défaut Proxmox a le port 8006 pour l'administration des machines virtuelle indiquent à ce dernier que nous utilisons des serveurs de virtualisation. Cela permet à l'attaquant de cartographier le réseau.

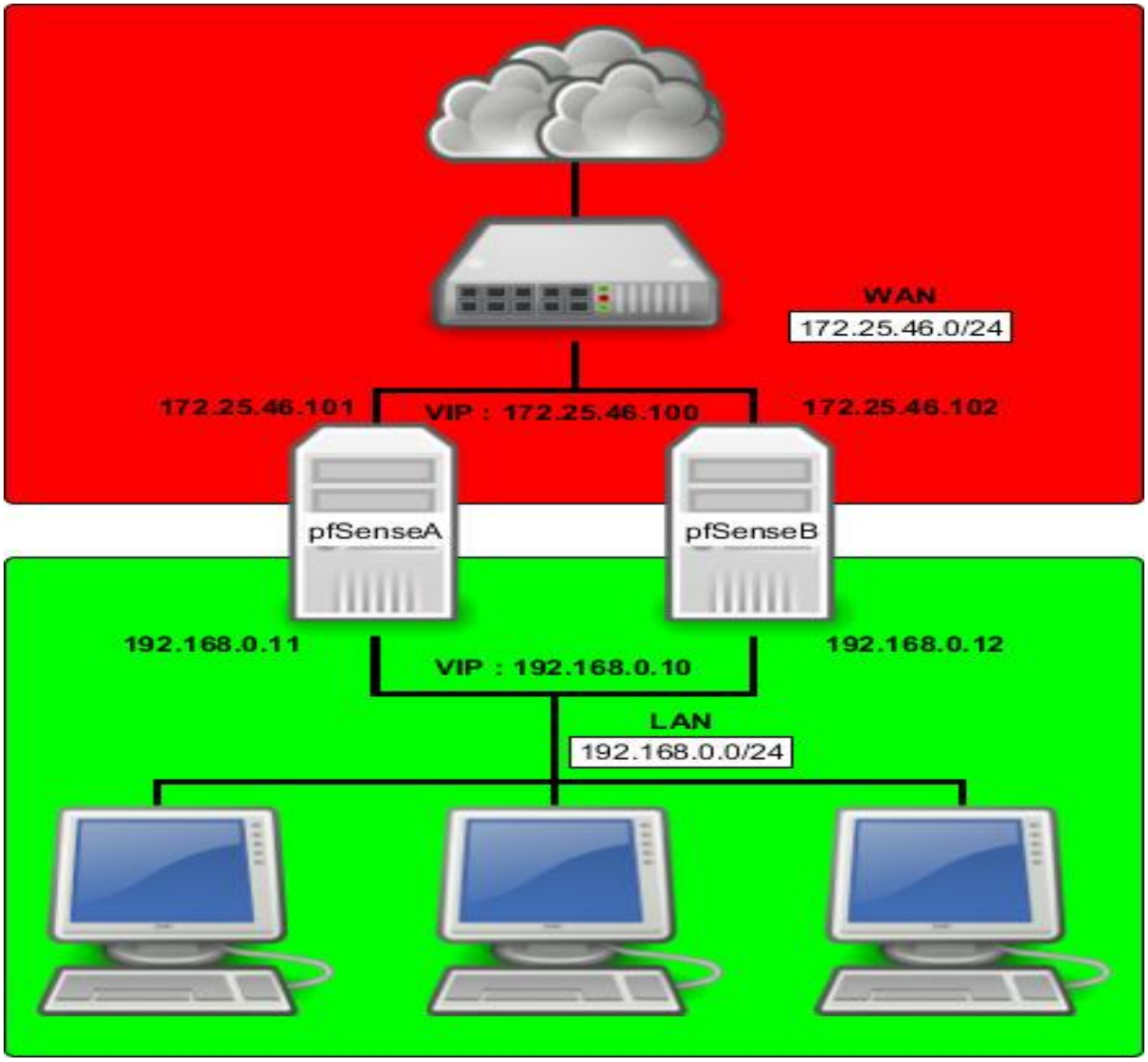
3. Solution(s)

Pour cela plusieurs mesures sont possibles. En voici une que nous proposons pour commencer. L'idée est de bloquer toutes tentative de scan de la part d'un client à l'extérieur du réseau car il ne doit surtout pas être en mesure de scanner le réseau. En revanche, dans notre LAN, une règle qui restreint le scan de port peu nous pénaliser dans le dépannage et l'administration de notre infrastructure réseau en cas de dépannage par exemple.

C'est pour cette raison que nous choisissons de mettre une sonde Snort au niveau de la panne WAN de notre pfSence afin de cibler les menaces en provenance du WAN qui a pour destination notre serveur dans notre LAN.
Ainsi un attaquant qui souhaite scanner notre LAN ne sera pas en mesure de réalisé cet exercice car le Pare-Feu Snort va bloquer ce dernier.

Aussi nous pouvons enregistrer le tout dans un fichier log afin d'avoir un historique de toutes les tentatives de connexion non autorisé comme il est présenté dans le schéma fournit plus tôt.

Ci-dessous, le schéma réseau sur lequel nous allons travailler :



4. Syntaxe & Explications de la règle :

En ce qui concerne la syntaxe de la règle, voici cette dernière :

```
alert icmp any any -> any any (msg:"Blocage des pings"; sid:1000009; rev:1; \
    icmp_type:8; icmp_code:0; \
    logto:"/var/log/snort/ping.log";)
```

Et l’explication de cette dernière :

- `alert icmp any any -> any any` : Cette partie spécifie que la règle s'applique aux paquets ICMP (ping) provenant de n'importe quelle adresse source (any) et envoyés à l'intérieur de notre réseau LAN.
- `msg:"Blocage des pings"` : C'est le message qui sera enregistré dans les logs pour indiquer le blocage des pings.
- `sid:1000009; rev:1;` : Ce sont des identifiants uniques pour la règle, utilisés par Snort pour l'identifier.
- `icmp_type:8; icmp_code:0;` : Spécifie le type et le code ICMP correspondant au ping standard.
- `logto:"/var/log/snort/ping.log";` : Cette partie indique à Snort de journaliser les détails des paquets ICMP bloqués dans le fichier `/var/log/snort/ping.log`.

5. Conclusion

En conclusion, Snort est un Pare-Feu avec énormément de ressources. Il peut fonctionner mode IDS (Intrusion Detection System) et/ou en mode IPS (Intrusion Prevention System).
Snort surveille le trafic réseau en temps réel pour détecter les activités malveillantes et les intrusions potentielles. Il utilise des règles préconfigurées pour identifier les signatures connues d'attaques, les tentatives de scans de ports, les exploitations de vulnérabilités, etc.

- Mode IDS : En mode IDS, Snort analyse le trafic réseau et génère des alertes lorsqu'il détecte des activités suspectes ou malveillantes. Ces alertes peuvent être consultées en temps réel ou enregistrées dans des fichiers de logs pour une analyse ultérieure.

- Mode IPS : En mode IPS, Snort agit de manière proactive pour bloquer les activités malveillantes en temps réel. Lorsqu'il détecte une menace, Snort peut prendre des mesures pour prévenir l'intrusion, telles que la mise en liste noire d'une adresse IP, la fermeture d'une connexion réseau, ou l'envoi d'un paquet de réinitialisation TCP.

Outre les règles préconfigurées, Snort permet aux utilisateurs de créer leurs propres règles personnalisées pour détecter des attaques spécifiques ou des schémas de trafic suspects. Cela offre une flexibilité pour adapter Snort à des environnements spécifiques.