GSB

IDS

Version <2.0>



Mise en place d'un système de détection d'intrusions

GSB	Version: <1.0>
IDS	Date: 08/03/2016

Historique des révisions

Date	Version	Description	Auteur
08/03/2016	<1.0>	Installation du package «Snort» et mise	Legrand Julien
08/03/2010	1.0>	en place des règles	Harismendy Brice
10/03/2016	<1.5>	Configuration du Pare-Feu	Legrand Julien
			Harismendy Brice
11/03/2016	<2.0>	Création de la liste blanche puis des	Legrand Julien
		règles de détection	Harismendy Brice

GSB	Version: <1.0>
IDS	Date: 08/03/2016

Table des matières

1. Introduction

- 1.1 Contexte du projet
- 1.2 Objectifs du document
- 1.3 Portée
- 1.4 Références

2. Éléments de configuration

- 2.1 Installation de "Snort" et mise à jour des règles
- 2.2 Configuration du Pare-Feu pour le réseau local
- 2.3 Création d'une "liste blanche" de l'IDS
- 2.4 Mise en place des dernières régles
 - 2.4.1 Configuration et activation des règles 9
 - 2.4.2 Démarrage du service "Snort" 10

3. Tests / Validations

- 3.1 Test par lancement de scan
- 3.2 Vérification des alertes

4. Conclusion

GSB	Version: <1.0>
IDS	Date: 08/03/2016

Mise en place d'un système de détection d'intrusions

1. Introduction

Nous allons maintenant mettre en place un IDS, c'est à dire un système de détection des intrusions sur notre Pfsense, avec un package du nom de «Snort». Celui-ci aura pour fonction d'analyser les communications entrantes ET sortantes du réseau pour se prémunir d'éventuelles attaques et aussi afin de créer une base de connaissance sur les attaques réussies pour ne pas qu'elles soient réitérées.

1.1 Contexte du projet

Nous reprenons ici le contexte du Pare-Feu / Proxy Pfsense, (cf. Compte-Rendu du sujet) et allons y ajouter un IDS pour prévenir plus efficacement des intrusions.

1.2 Objectifs du document

Le document à pour but de compléter celui du TP précédent sur les Pare-Feu / Proxy, et de démontrer la place que doit avoir une solution de supervision comme celle-ci.

1.3 Portée

Ce document est adressé ici aussi aux équipes techniques en charge de la sécurité d'un réseau et aux administrateurs qui souhaiteraient mettre en place la même solution.

1.4 Références

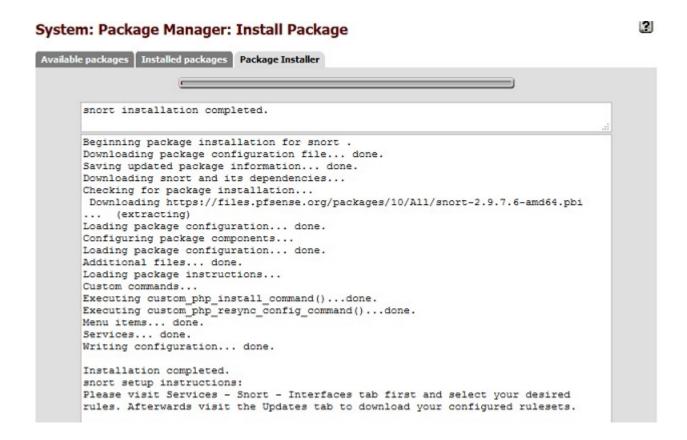
http://www.snort.org (Site officiel du package)

GSB	Version: <1.0>
IDS	Date: 08/03/2016

2. Éléments de configuration

2.1 Installation de "Snort" et mise à jour des règles

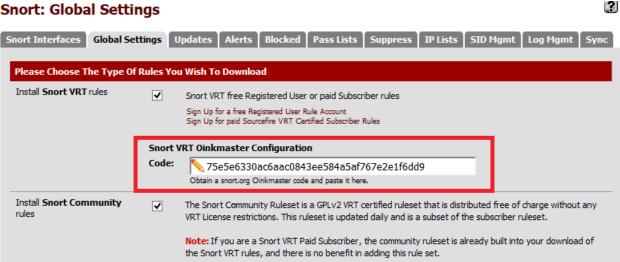
- Allez dans "System" > "Packages" > onglet "Available Packages" puis sélectionner "Snort" cliquez sur confirmer avant l'installation.



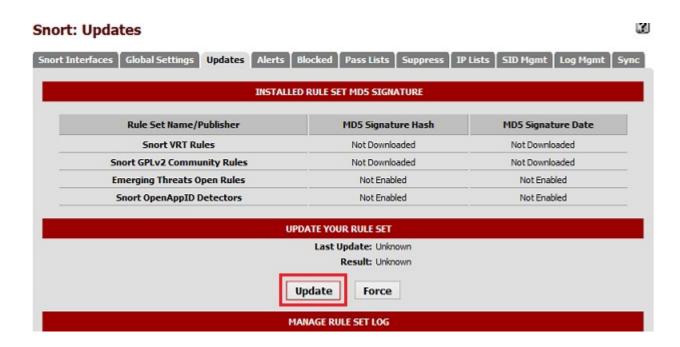
- Allez dans "Services" > "Snort" > onglet "Global Settings" > cochez "Install Snort VRT Rules" et "Install Snort Community Rules" (pour les installations, il vous faut créer un compte sur snort.org et dans le profil du compte allez dans le menu "Oinkcode" afin d'obtenir le code de téléchargement).

GSB	Version: <1.0>
IDS	Date: 08/03/2016

Snort: Global Settings



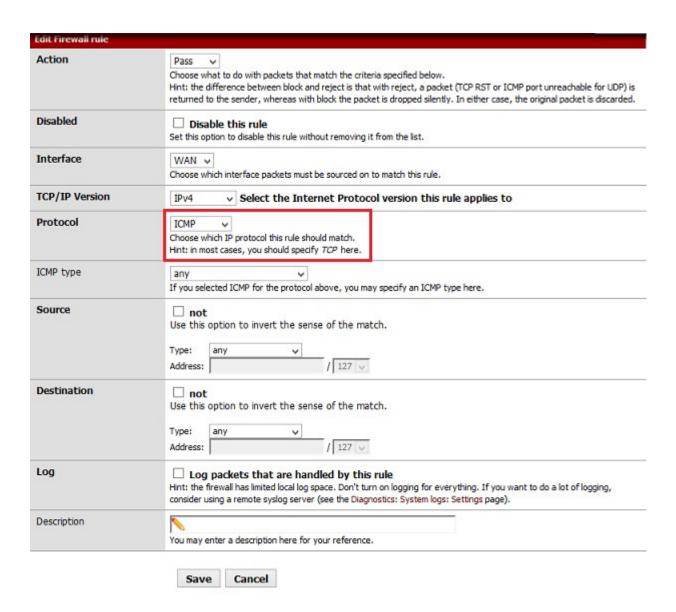
- Cliquez sur "Save" en bas de page.
- Allez enfin dans l'onglet "Updtate" et cliquez sur "Update"



GSB	Version: <1.0>
IDS	Date: 08/03/2016

2.2 Configuration du Pare-Feu pour le réseau local

- Ajoutez une règle sur l'interface WAN du Pare-Feu en allant dans "**FireWall**" > "**Rules**" > et dans l'onglet "**WAN**", créez une règle permettant les requètes ICMP dans le réseau local.

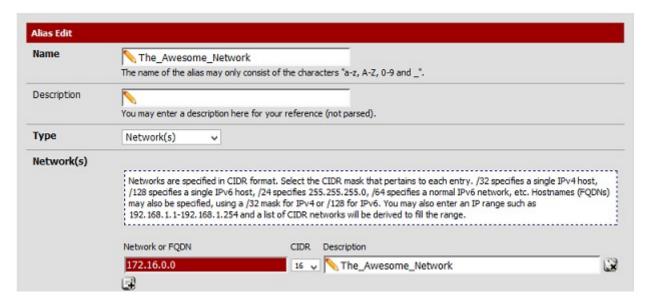


- Cliquez ensuite sur "Save" et "Apply Changes" (dans l'onglet "WAN").
- Allez enfin dans "**FireWall**" > "**Aliases**" > onglet "**IP**" > puis créez l'alias du nom du réseau (contenant ici notre VM) :

GSB	Version: <1.0>
IDS	Date: 08/03/2016

Firewall: Aliases: Edit



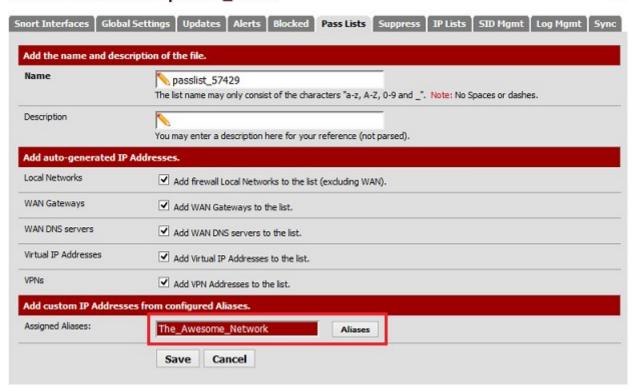


2.3 Création d'une "liste blanche" de l'IDS

- Allez dans "Services" > "Snort" > "Pass Lists" > créez une passlist et entrez l'alias crée précédemment.

Snort: Pass List Edit - passlist_57429





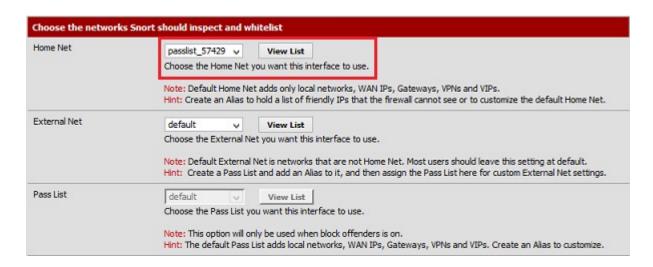
GSB	Version: <1.0>
IDS	Date: 08/03/2016

- Créez ensuite une interface à surveiller dans "**Snort Interfaces**" affectée au WAN. Puis mettre le nom de la "passlist" en bas dans "**Home Net**".

Snort: Interface - Edit Settings







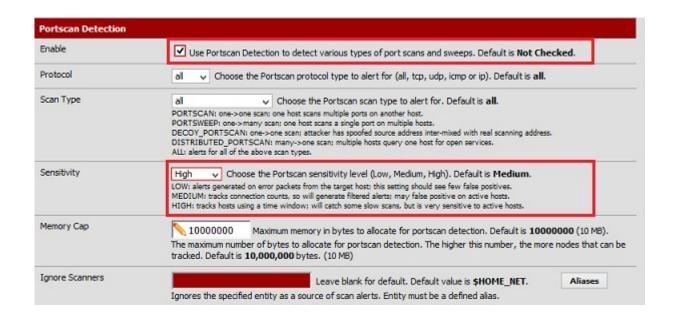
2.4 Mise en place des dernières régles

2.4.1 Configuration et activation des règles

- Allez dans "WAN Categories" et choisir "snort_scan.rules"
- Allez dans "WAN Preprocs" et cocher "Enable" dans "Portscan Detecion". Enfin, mettre "high" dans
- "Sensivity".

	snort_rservices.rules
	snort_scada.rules
✓	snort_scan.rules
	snort_server-apache.rules
	snort_server-iis.rules

GSB	Version: <1.0>
IDS	Date: 08/03/2016



2.4.2 Démarrage du service "Snort"

- Allez dans "Status" > "Services" puis démarrer le service.



GSB	Version: <1.0>
IDS	Date: 08/03/2016

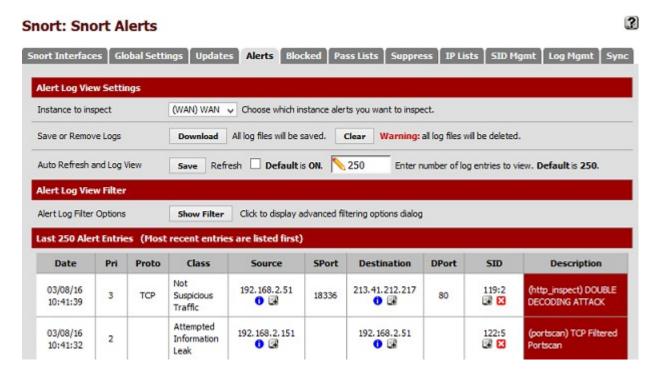
3. Tests / Validations

3.1 Test par lancement de scan

- On lance un test avec un scan sur "Zenmap" et on peut voir que l'IDS détecte le portscan.

3.2 Vérification des alertes

-Allez dans l'onglet "**Alerts**" de Snort ("**Services**" > "**Snort**"), on peut constater qu'il a bien détecté le portscan de "zenmap".



4. Conclusion

Nous avons mis en place un IDS qui permettra de vérifier la conformité des paquets et ainsi avoir un réseau plus sécurisé et une meilleure supervision. Un IDS permet de bloquer certaines attaques (portscan, arp, etc) couplé avec "squidguard" et un Pare-feu correctemment configuré, on obtient un réseau très sécurisé, il faut maintenant se poser la question de l'emplacement du Pare-Feu sur ce dit réseau.