

Système de détection d'intrusion SNORT



Table des matières

Contexte StadiumCompany	2
Cahier des charges Stadiumcompany	4
Mission 6	5
Solution :	6
Projet	6
Objectif du projet.....	6
Mise en place du service Snort	7
Inscription sur Snort.....	7
Installation de Snort	8
Test d'intrusion	15
Conclusion	16

Contexte StadiumCompany

StadiumCompany gère un grand stade et avait initialement mis en place un réseau de communication avancé lors de la construction. Cependant, au fil du temps, l'entreprise a ajouté de nouveaux équipements et augmenté les connexions sans tenir compte de ses objectifs commerciaux à long terme ni de la conception de son infrastructure réseau. Cela a conduit à des problèmes de bande passante et de gestion du trafic, limitant la capacité de la société à offrir des services de qualité.

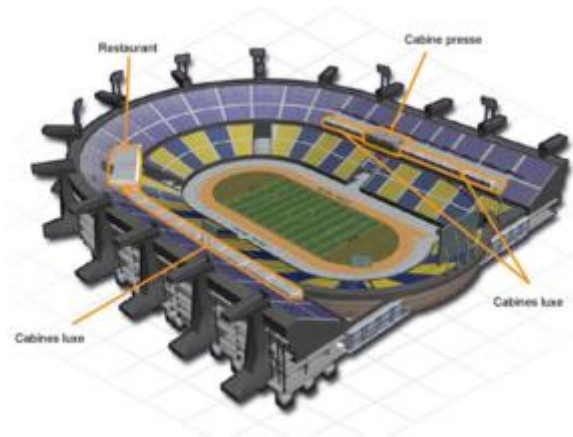


Maintenant, la direction de StadiumCompany souhaite améliorer la satisfaction de ses clients en introduisant de nouvelles technologies et en permettant l'organisation de concerts, mais le réseau actuel ne le permet pas. Sachant qu'elle ne possède pas l'expertise nécessaire en matière de réseau, la direction a décidé de faire appel à des consultants réseau pour concevoir, gérer et mettre en œuvre ce projet en trois phases.

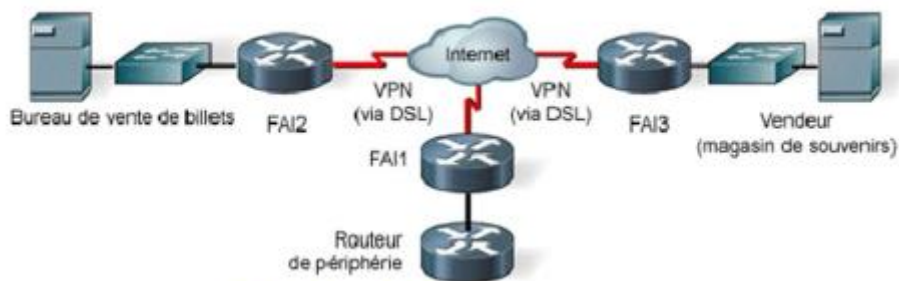
La première phase consiste à planifier le projet et à préparer une conception réseau de haut niveau. Pour cela, StadiumCompany a engagé NetworkingCompany, une société spécialisée en conception de réseaux, qui a interrogé le personnel du stade pour comprendre l'organisation et les installations.



StadiumCompany emploie 170 personnes à temps plein, dont 35 dirigeants et responsables, ainsi que 135 employés. Ils ont également recours à environ 80 intérimaires pour des événements spéciaux. Tous les employés, à l'exception des préposés au terrain et des gardiens, utilisent des PC et des téléphones connectés à un PABX vocal numérique



Le stade propose des installations pour deux équipes sportives, une équipe visiteuse, un restaurant de luxe et un fournisseur de concessions. Il dispose également de deux sites distants, une billetterie en centre-ville et une boutique de souvenirs, connectés via DSL à un FAI local.



Le stade est construit sur deux niveaux, avec des locaux techniques reliés par des câbles à fibre optique en raison de sa grande taille. Les équipes sportives ont leurs bureaux et installations, tandis que le restaurant de luxe loue également des bureaux auprès de StadiumCompany

En résumé, StadiumCompany souhaite moderniser son réseau pour répondre aux besoins actuels et futurs, et a fait appel à des experts pour le guider à travers ce processus de mise à niveau.

Cahier des charges Stadiumcompany

Le Cahier des Charges de StadiumCompany révèle votre intégration au sein de la division Systèmes d'Information (SI) de l'entreprise pour cette année. Votre mission centrale consistera à assumer la responsabilité de l'administration des systèmes et des réseaux informatiques.

StadiumCompany se compose de plusieurs sites distincts, chacun ayant un rôle spécifique :

1. Site 1 : Stade - Ce site est le cœur de l'entreprise, abritant l'hébergement informatique, le siège social et le centre administratif. Il est le pivot autour duquel s'articulent toutes les opérations et activités de l'entreprise.

2. Site 2 : Billetterie - Ce site est dédié à la gestion des ventes de billets, un élément essentiel pour les événements sportifs et les spectacles organisés au stade.

3. Site 3 : Magasin - Ce site est spécialement conçu pour la vente d'articles souvenirs, offrant aux fans et aux visiteurs la possibilité d'acheter des produits liés à l'équipe ou aux événements.

Le Cahier des Charges insiste sur la nécessité de documenter les différentes solutions retenues pour le projet en fonction de leur niveau de complexité. Cette approche méthodique garantira que chaque aspect de l'infrastructure informatique soit clairement spécifié et que les procédures soient consignées de manière exhaustive. Cela s'inscrit dans la vision globale adoptée par StadiumCompany pour assurer une gestion efficace et cohérente de ses ressources informatiques.

Votre rôle au sein de cette mission sera d'une importance cruciale, car vous devrez contribuer à façonner et à maintenir l'infrastructure technologique qui soutient les opérations de l'entreprise et qui permet de répondre aux défis uniques posés par chaque site.

Mission 6 : Sécurisation de l'Interconnexion du Réseau de Stadiumcompany avec Internet

Contexte : Après avoir mis en place l'architecture réseau interne du site du stade, le Directeur des Systèmes d'Information (DSI) de StadiumCompany souhaite désormais interconnecter le réseau de l'entreprise avec Internet. Cette expansion vers Internet offre de nombreux avantages, mais elle expose également l'entreprise à de nouvelles menaces en matière de sécurité. Il est donc essentiel d'intégrer la sécurité au sein de l'architecture réseau pour réduire ces risques.

Définition du besoin : Le DSI de StadiumCompany souhaite réaliser une étude complète des risques liés à l'accès à Internet, en prenant en compte les éléments de sécurité suivants :

1. **Mise en place d'une DMZ :** Création d'une zone démilitarisée (DMZ) contenant un ensemble de serveurs accessibles depuis l'extérieur, en particulier le serveur web.
2. **Restriction de l'accès au réseau interne :** L'environnement du réseau interne du stade doit être accessible uniquement aux acteurs de l'entreprise.
3. **Hébergement en interne des serveurs :** Les serveurs exécutant les applications et les besoins de StadiumCompany sont hébergés en interne.
4. **Accès Internet pour les collaborateurs :** Les employés de l'entreprise sont autorisés à accéder à Internet à partir du réseau interne.
5. **Accès Internet restreint pour les utilisateurs du réseau Wi-Fi Visiteurs :** Les utilisateurs du réseau Wi-Fi Visiteurs ont un accès limité, uniquement à Internet.

Travail à réaliser : Pour répondre à ces besoins, les tâches suivantes doivent être accomplies :

1. **Identification des Risques :** Il est essentiel d'identifier les risques potentiels associés à l'interconnexion avec Internet. Cela comprend la menace de cyberattaques, d'intrusions, de fuites de données, etc.
2. **Détermination de la Démarche de Sécurité :** Élaboration d'une démarche visant à réduire ces risques. Cela inclut la mise en place de pare-feux, de systèmes de détection d'intrusions, de systèmes de prévention des intrusions, et d'autres mesures de sécurité.
3. **Définition de la Problématique de l'Accès à Internet :** Élaboration d'une stratégie de sécurité pour gérer l'accès au réseau Internet à partir d'un réseau privé, en garantissant la confidentialité, l'intégrité et la disponibilité des données.
4. **Conception de la Politique de Filtrage :** Définition d'une politique de filtrage des flux de données conformément aux exigences du cahier des charges. Cette politique devrait déterminer quels types de trafic sont autorisés ou bloqués.
5. **Adaptation de la Maquette :** Mise à jour de l'architecture réseau actuelle en fonction de la solution proposée, en intégrant les éléments de sécurité nécessaires pour garantir la protection du réseau et des données.

La réalisation de cette mission est cruciale pour assurer la sécurité de l'entreprise dans un environnement connecté à Internet, en réduisant les risques potentiels et en mettant en place les contrôles de sécurité adéquats.

Solution :

Qu'est-ce que Snort ?

SNORT est un système de détection d'intrusion basé sur un réseau et écrit en langage de programmation C. Il a été développé en 1998 par Martin Roesch. Il est maintenant développé et maintenu par Cisco. Il peut également être utilisé comme un renifleur de paquets pour surveiller le système en temps réel. L'administrateur réseau peut l'utiliser pour surveiller tous les paquets entrants et trouver ceux qui sont dangereux pour le système. Il est basé sur l'outil de capture de paquets de la bibliothèque. Les règles sont assez faciles à créer et à mettre en œuvre et il peut être déployé dans n'importe quel système d'exploitation et n'importe quel environnement réseau.

Snort est considéré comme un renifleur de paquets qui surveille le trafic réseau, examinant de près chaque paquet pour détecter une charge utile dangereuse ou des anomalies suspectes. Longtemps leader parmi les outils de prévention et de détection des intrusions en entreprise, les utilisateurs peuvent compiler Snort sur la plupart des systèmes d'exploitation (OS) Linux ou Unix et Windows.

Quels sont les avantages de l'utilisation de Snort dans votre environnement ?

Le système de détection et d'intrusion réseau Snort offre de nombreux avantages aux organisations qui le déploient sur leurs réseaux.

1. Haute précision : Snort étant un projet open-source, il y a un effort constant pour l'améliorer et modifier certaines de ses fonctionnalités pour une plus grande précision. Plusieurs équipes de sécurité améliorent le logiciel par le biais de la communauté Snort, dispersée dans le monde entier.
2. Grande adaptabilité : La possibilité d'ajouter de nouvelles fonctionnalités à Snort en accédant à son code source donne à Snort un avantage significatif sur ses concurrents. Cette méthode pourrait permettre à Snort de gérer n'importe quel système de sécurité réseau.
3. Réponse rapide : Grâce à ses mécanismes de protection en temps réel, Snort peut protéger le système contre toute nouvelle menace ou logiciel malveillant. Le groupe de recherche et de renseignement sur la sécurité Talos de Cisco (Talos) est l'une des plus grandes caractéristiques de Snort ; il peut détecter de nouvelles attaques en mettant à jour Snort avec de nouvelles menaces toutes les heures.

Pour conclure, Snort est un système de détection d'intrusion réseau (IDS) très utilisé, car c'est l'un des meilleurs outils de chasse aux cybermenaces disponibles sur le marché. De plus, Snort est un logiciel libre et gratuit. Par conséquent, toute organisation disposant d'un budget limité peuvent utiliser Snort comme solution IDS/IPS.

[Source](#)

Projet

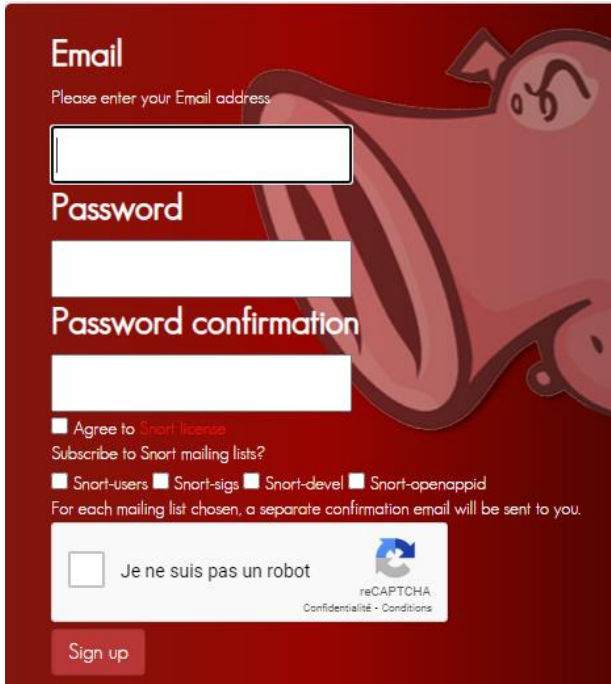
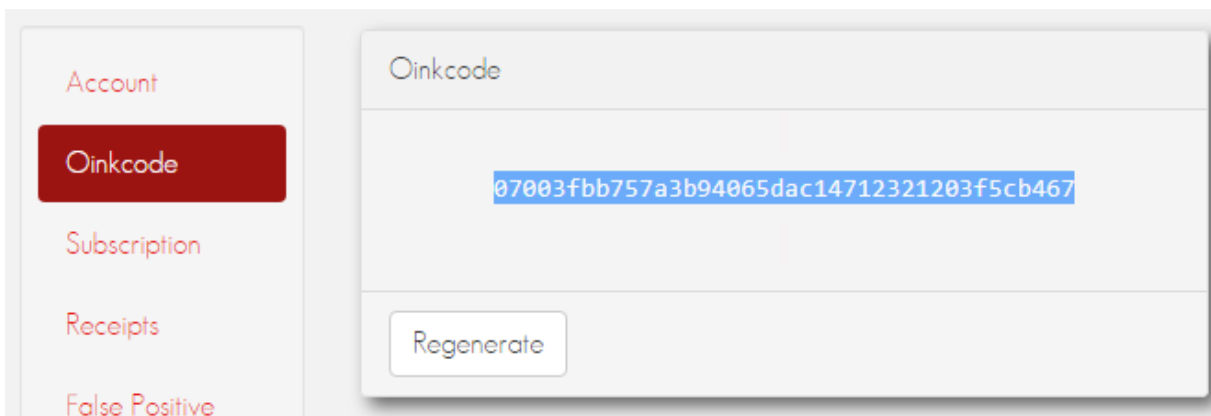
Objectif du projet

L'objectif du projet est de mettre en place un système de détection d'intrusion afin de prévenir les attaques malveillantes sur le réseau de StadiumCompany ainsi permettant aux utilisateurs de bénéficier d'un réseau sécurisé.

Mise en place du service Snort

Inscription sur Snort

On va d'abord créer un compte chez Snort qui nous fournira une clé (**Snort Oinkmaster Code**) pour notre configuration. Une fois le formulaire d'inscription fait, un mail est envoyé puis on se connecte (<https://www.snort.org/>) avec nos identifiants pour récupérer notre clé.

The image shows the Snort registration form. It has a dark red background with a cartoon pig illustration. The form includes fields for 'Email', 'Password', and 'Password confirmation'. Below these are checkboxes for 'Agree to Snort license', 'Subscribe to Snort mailing lists?', and four specific mailing lists: 'Snort-users', 'Snort-sigs', 'Snort-devel', and 'Snort-openappid'. There is a reCAPTCHA section with the text 'Je ne suis pas un robot' and a 'Sign up' button at the bottom.The image shows the Snort Oinkcode page. On the left is a sidebar with links: 'Account', 'Oinkcode', 'Subscription', 'Receipts', and 'False Positive'. The main area is titled 'Oinkcode' and displays a long alphanumeric string: '07003fbb757a3b94065dac14712321203f5cb467'. Below this string is a 'Regenerate' button.

Installation de Snort

On va dans **System > Packet Manager > Available Packages > Snort**

Search

Search term

Both

Search Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

tection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.

+ Install

On va dans **Services > Snort** pour configurer Snort

Services ▾

Auto Config Backup

Captive Portal

DHCP Relay

DHCP Server

DHCPv6 Relay

DHCPv6 Server

DNS Forwarder

DNS Resolver

Dynamic DNS

IGMP Proxy

NTP

PPPoE Server

Router Advertisement

Shellcmd

SNMP

Snort

On part ensuite dans l'onglet **Global Settings**, on télécharge les règles gratuites en cochant les cases suivantes :

- **Enable Snort VRT**
- **Enable Snort GPLv2**
- **Enable ET Open**

Snort Subscriber Rules

Enable Snort VRT

☒ Click to enable download of Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

Snort Oinkmaster Code

Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

Enable Snort GPLv2

☒ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open

☒ Click to enable download of Emerging Threats Open rules

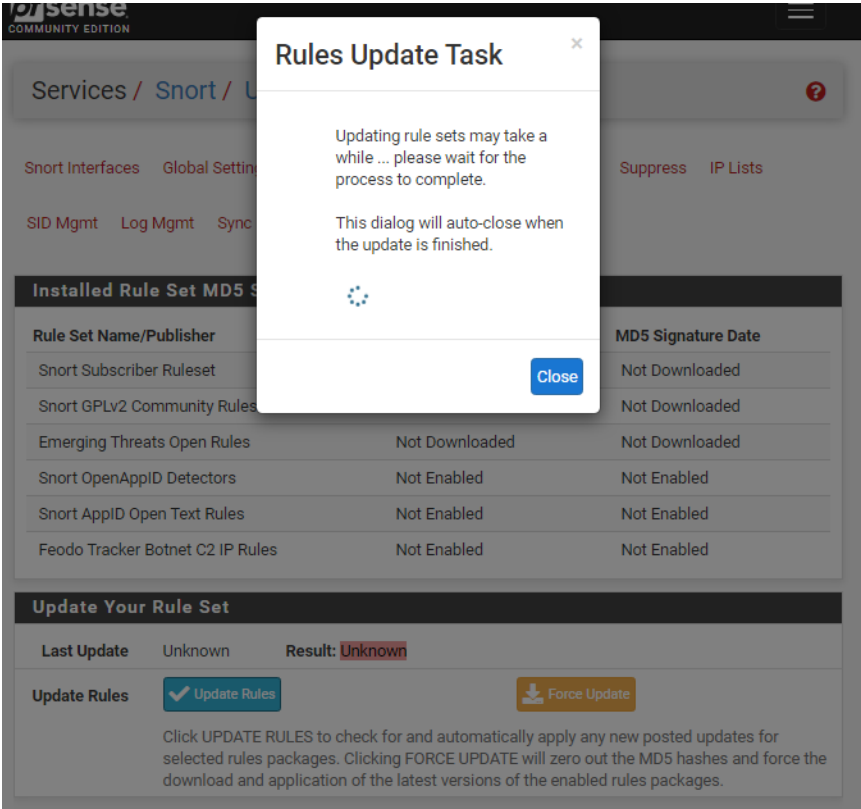
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

À partir de la section **Rules Update Settings**, on configure les paramètres tels :

- **Update Interval = 1 DAY**
- **Update Start Time = 00:01**
- **Hide Deprecated Rules Categories = Coché**
- **Remove Blocked Hosts Interval = 1 HOUR**
- **Start/Shutdown Logging = Coché**

Rules Update Settings	
Update Interval	<div>1 DAY</div> <div>Please select the interval for rule updates. Choosing NEVER disables auto-updates.</div>
Update Start Time	<div>00:01</div> <div>Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.</div>
Hide Deprecated Rules Categories	<input checked="" type="checkbox"/> Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification	<input type="checkbox"/> Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.
General Settings	
Remove Blocked Hosts Interval	<div>1 HOUR</div> <div>Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.</div>
Remove Blocked Hosts After Deinstall	<input type="checkbox"/> Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	<input checked="" type="checkbox"/> Click to retain Snort settings after package removal.
Startup/Shutdown Logging	<input checked="" type="checkbox"/> Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.
<div>Save</div>	

On met à jour nos règle dans **Update > Update rules**



Les règles ont bien été appliquées

Installed Rule Set MD5 Signature		
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	17d6b35e5f145e8493ea00c16469e6a5	Monday, 06-May-24 00:46:36 CEST
Snort GPLv2 Community Rules	88526492e0f0cda2d371e26dfaafbf1b	Monday, 06-May-24 00:46:36 CEST
Emerging Threats Open Rules	61b23f2afe4cf1de7b16ab6adba2a578	Monday, 06-May-24 00:46:37 CEST
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set		
Last Update	May-06 2024 00:46	Result: Success

Snort n'est pas encore configuré sur des interfaces via **View Log**

Rules Update Log

```
Installation of Snort Subscriber rules completed.  
Extracting and installing Snort GPLv2 Community Rules.  
Installation of Snort GPLv2 Community Rules completed.  
Extracting and installing Emerging Threats Open rules.  
Installation of Emerging Threats Open rules completed.  
Copying new config and map files...  
Warning: No interfaces configured for Snort were found.  
Rules update has finished. Time: 2024-05-06 00:46:37
```

Close

On va aller sur **Snort Interfaces** pour choisir les interfaces sur lesquelles Snort va analyser le trafic réseau

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists

SID Mgmt Log Mgmt Sync

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
-----------	--------------	---------------	---------------	-------------	---------

+ Add

On coche les paramètres à activer

General Settings	
Enable	<input checked="" type="checkbox"/> Enable interface
Interface	<div>WAN (em0) ▼</div> <p>Choose the interface where this Snort instance will inspect traffic.</p>
Description	<div>WAN</div> <p>Enter a meaningful description here for your reference.</p>
Snap Length	<div>1518</div> <p>Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.</p>
Alert Settings	
Send Alerts to System Log	<input checked="" type="checkbox"/> Snort will send Alerts to the firewall's system log. Default is Not Checked.
System Log Facility	<div>LOG_AUTH ▼</div> <p>Select system log Facility to use for reporting. Default is LOG_AUTH.</p>
System Log Priority	<div>LOG_ALERT ▼</div> <p>Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.</p>
Enable Packet Captures	<input checked="" type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Packet Capture File Size	<div>128</div> <p>Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em054898 is rotated and a new file opened.</p>
Enable Unified2 Logging	<input type="checkbox"/> Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked. Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.
Block Settings	
Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	<div>Legacy Mode ▼</div> <p>Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.</p> <p>Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtetnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.</p>
Kill States	<input checked="" type="checkbox"/> Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	<div>BOTH ▼</div> <p>Select which IP extracted from the packet you wish to block. Default is BOTH.</p>

Dans l'onglet **Wan Categories**, on effectue la suite de la configuration et **Save** tout en bas :

- **Resolve Flowbit** : Cette option sert à activer automatiquement les règles pour les flowbits utilisera les règles activées et choisies
- **IPS Policy Selection** : Cette option sert à choisir la politique IPS, elle désactive cependant les règles **Snort Text Rules**, **Snort OS Rules**, on coche **Select All**

Les politiques Snort IPS sont Connectivity, Balanced, Sécurité et Max-Detect:

1. **Connectivity** bloque la plupart des menaces majeures avec peu ou pas de faux positifs.
2. **Balanced** est une bonne politique de départ. Il est rapide, a un bon niveau de couverture de base et couvre la plupart des menaces. Il inclut toutes les règles de Connectivity.
3. **Sécurité** est une politique stricte. Il contient tout ce qui se trouve dans les deux premiers plus les règles de type politique telles qu'un objet Flash dans un fichier Excel.
4. **Max-Detect** est une stratégie créée pour tester le trafic réseau via votre appareil. Cette politique doit être utilisée avec prudence sur les systèmes de production !

Automatic Flowbit Resolution

Resolve Flowbits

☒ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
 Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Snort Subscriber IPS Policy Selection

Use IPS Policy

☒ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.

 Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection

Balanced
▼

Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect. Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

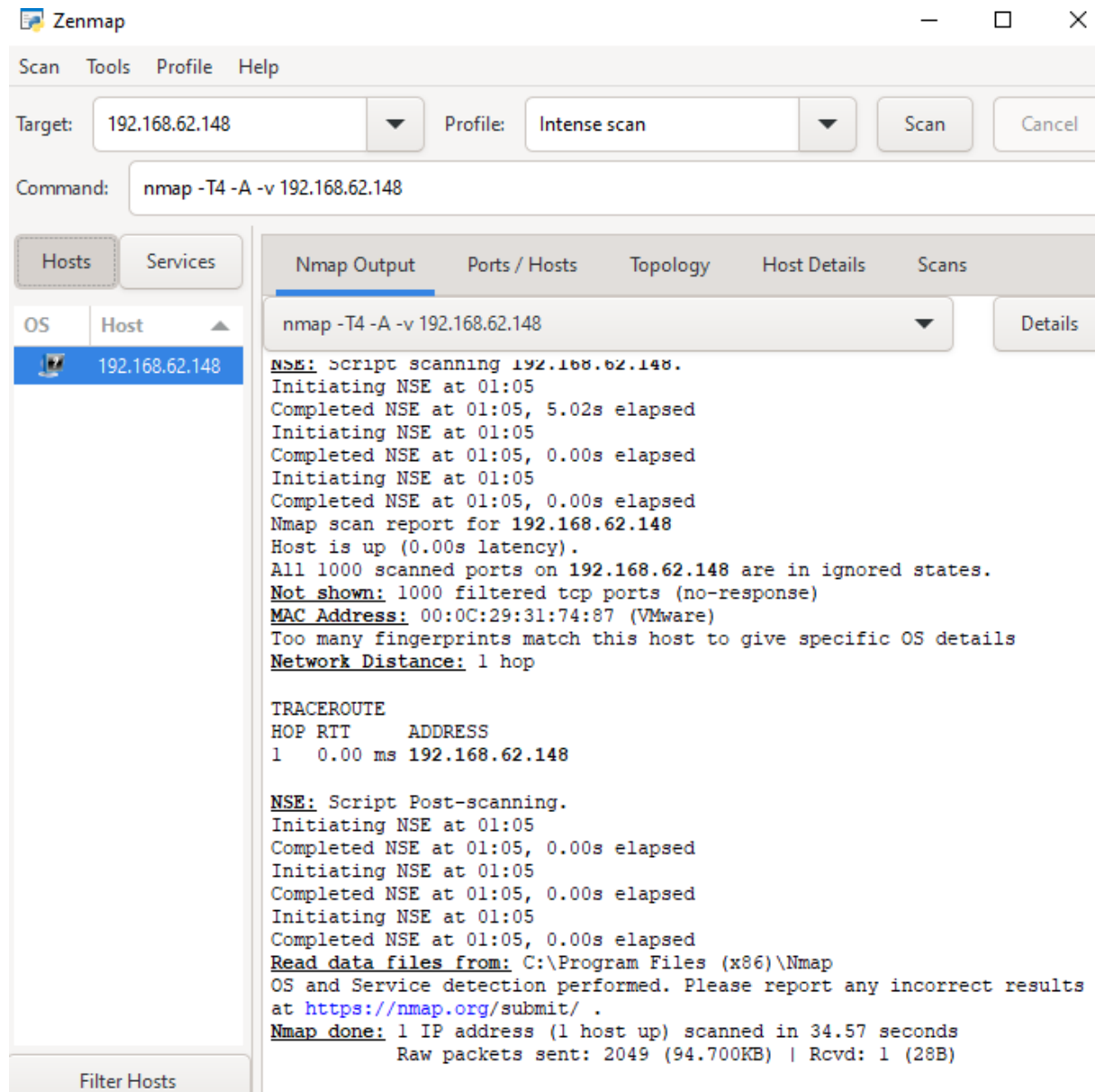
On démarre ensuite l'interface Snort (**Snort Interfaces**)

Interface Settings Overview					
Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)		AC-BNFA	LEGACY MODE	WAN	

























Interface Settings Overview					
Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)		AC-BNFA	LEGACY MODE	WAN	



Test d'intrusion

On installe sur une machine vierge un utilitaire nmap (**Zenmap**) qui scanner les ports de PfSense
On lance le scan sur l'interface WAN



Les alertes sont remontées et l'assaillant (notre machine) a été bloqué

10 Entries in Active Log								
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort
2024-05-06 01:33:38		2	TCP	Potentially Bad Traffic	192.168.62.149   	64228	192.168.62.148  	1521
2024-05-06 01:33:38		2	TCP	Potentially Bad Traffic	192.168.62.149   	64228	192.168.62.148  	1521
2024-05-06 01:33:38		2	TCP	Potentially Bad Traffic	192.168.62.149   	64226	192.168.62.148  	1521
2024-05-06 01:33:38		2	TCP	Potentially Bad Traffic	192.168.62.149   	64226	192.168.62.148  	1521

Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)			
#	IP	Alert Descriptions and Event Times	Remove
1	192.168.62.149 	ET SCAN Suspicious inbound to mySQL port 3306 – 2024-05-06 01:33:15 ET SCAN Potential VNC Scan 5900-5920 – 2024-05-06 01:33:27	
1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.			

Conclusion

La mise en place d'un système de détection d'intrusion permet de mieux gérer les attaques réseaux et prévenir ces dernières afin d'assurer la continuité du service réseau de StadiumCompany. De plus, Snort propose une interface facile d'utilisation rendant la tâche plus simple au service informatique