

Implémentation d'un IDS/IPS avec Suricata sur pfSense

Protection Active du Périmètre Réseau — pfSense (10.11.3.17) — Bloc 3 SISR — Sécurité

Suricata IDS/IPS | Emerging Threats Open | Block Offenders | Pattern Matching | SOC

EN-TÊTE — TABLEAU RÉCAPITULATIF

Champ	Valeur
Candidat	BTS SIO option SISR — Session 2026
Entreprise	SIO SISR
Objet	Implémentation d'un IDS/IPS Suricata sur pfSense — Protection active du périmètre
Équipement cible	pfSense — 10.11.3.17 — Pare-feu / Routeur
Supervision associée	SRV-ZABBIX — 10.11.3.19 — Centralisation logs rsyslog (UDP/514)
Outil IDS/IPS	Suricata (package pfSense) — Signatures Emerging Threats Open
Référentiel SISR	Bloc 3 — Cybersécurité / Sécurité des infrastructures réseau
Date	Mai 2026
Fiche n°	E6 — Supervision, Maintenance et Sécurité

I. OBJECTIF TECHNIQUE — IDS vs IPS : Détection vs Prévention

Un **IDS (Intrusion Detection System)** analyse le trafic réseau en temps réel par **pattern matching** — comparaison des flux avec une base de **signatures** connues (ex: Emerging Threats). Lorsqu'une correspondance est trouvée, l'IDS génère une alerte mais laisse passer le trafic. Il est passif. Un **IPS (Intrusion Prevention System)** va plus loin : il **bloque (drop)** activement les paquets malveillants en temps réel et peut bannir l'IP source. Suricata, déployé sur pfSense, peut fonctionner dans ces deux modes.

Comparatif — IDS (Détection) vs IPS (Prévention)

Critère	IDS — Mode Alerte	IPS — Mode Blocage
Mode de fonctionnement	Passif — analyse et alerte uniquement	Actif — analyse, alerte ET bloque/drop
Action sur le trafic	Laisse passer — génère une alerte Zabbix	Bloque le paquet — bannit l'IP source
Méthode de détection	Pattern matching sur signatures connues	Pattern matching + action drop immédiate
Risque de faux positifs	Limité — trafic légitime non bloqué	Élevé — un faux positif bloque un flux légitime
Impact sur performances	Faible — lecture seule du trafic	Modéré — inspection profonde (DPI) du flux
Cas d'usage SISR	Audit, détection, forensics, SOC passif	Protection active, conformité, SOC actif
Suricata pfSense	Mode "Alert only" — onglet Alerts	Mode "Block Offenders" — onglet Blocks

II. INSTALLATION ET CONFIGURATION — Suricata sur pfSense

Étape 1 — Installation du package Suricata

🔗 Navigation : pfSense (<https://10.11.3.17>) > System > Package Manager > Available Packages

Navigation dans l'interface web pfSense :

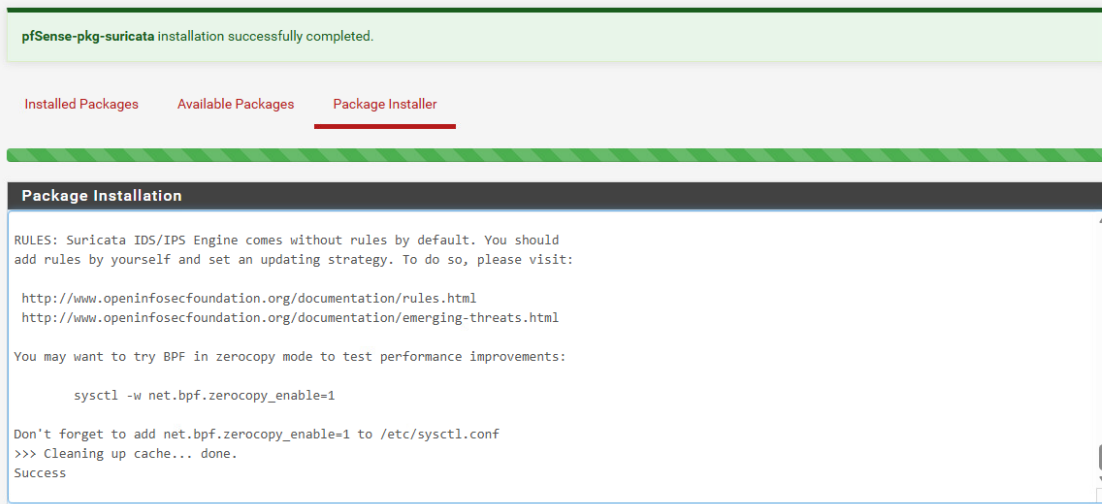
1. Se connecter sur <https://10.11.3.17> avec le compte admin
2. Menu : System
3. Sous-menu : Package Manager
4. Onglet : Available Packages
5. Rechercher : suricata
6. Cliquer sur [Install] en face du package "suricata"
7. Confirmer en cliquant sur [Confirm]

Attendre la fin de l'installation (barre de progression)

Le package Suricata s'ajoute dans : Services > Suricata

✅ Package Suricata installé — accessible dans Services > Suricata.

[Capture n°1: pfSense Package Manager — Package Suricata listé et bouton [Install] visible.]



Étape 2 — Configuration des signatures via Emerging Threats Open

🔗 Navigation : pfSense > Services > Suricata > Global Settings

Paramètres à configurer dans l'onglet Global Settings :

— Section : IDS Policy —

Enable Suricata pkg : ☒ Cocher

— Section : Emerging Threats Open (ETOpen) —

Install ETOpen Emerging Threats rules : ☒ Cocher

Emerging Threats Open est un ensemble de signatures gratuites

maintenu par la communauté Proofpoint

Couvre : exploits, malware, scan de ports, botnet, DoS...

— Section : Update Interval —

Rules Update Interval : 12 hours (mise à jour des signatures)

— Section : Logging —

Send Alerts to System Log : ☒ Cocher

→ Les alertes Suricata seront envoyées vers rsyslog / Zabbix

Cliquer sur [Save] puis sur [Update Rules] pour télécharger les signatures

⚠ PERFORMANCES : *Emerging Threats Open contient plusieurs milliers de signatures. Sur du matériel limité (pfSense sur VM ou routeur bas de gamme), activer uniquement les catégories pertinentes pour l'environnement (ex: scan, exploit, malware) afin de limiter l'impact CPU de l'inspection DPI (Deep Packet Inspection).*

☒ **Signatures Emerging Threats Open téléchargées et indexées par Suricata — base de détection opérationnelle.**

[Capture n°2 : Suricata Global Settings — ETOpen coché et statut des règles après [Update Rules] affichant le nombre de signatures chargées.

Please Choose The Type Of Rules You Wish To Download

Install ETOpen Emerging Threats rules

☒ ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro.

☐ Use a custom URL for ETOpen downloads

Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETOpen rules.

Rules Update Settings

Update Interval

12 HOURS

Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Hint: In most cases, every 12 hours is a good choice.

Update Start Time

00:41

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.

Live Rule Swap on Update

☐ Enable "Live Swap" reload of rules after downloading an update. Default is Not Checked

When enabled, Suricata will perform a live load of the new rules following an update instead of a hard restart. If issues are encountered with live load, uncheck this option to perform a hard restart of all Suricata instances following an update.

GeoLite2 DB Update

☐ Enable downloading of free GeoLite2 Country IP Database updates. Default is Not Checked

When enabled, Suricata will automatically download updates for the free GeoLite2 country IP database.

If you have a subscription for more current GeoIP2 updates, uncheck this option and instead create your own process to place the required database file in /usr/local/share/suricata/GeoLite2/.

General Settings

Remove Blocked Hosts Interval

NEVER

Please select the amount of time you would like hosts to be blocked. Note this setting is only applicable when using Legacy Mode blocking! This setting is ignored when using Inline IPS Mode.

Hint: in most cases, 1 hour is a good choice.

Log to System Log

☒ Copy Suricata messages to the firewall system log.

Log Facility

SYSLOG

Select system log facility to use for reporting. Default is LOCAL1.

Log Priority

NOTICE

Select system log Priority (Level) to use for reporting. Default is NOTICE.

Keep Suricata Settings After Deinstall

☒ Settings will not be removed during package deinstallation.

Clear Blocked Hosts After

☒ Click to clear all blocked hosts added by Suricata when removing the package. Default is checked.

Étape 3 — Paramétrage de l'interface LAN pour Suricata



Navigation : pfSense > Services > Suricata > Interfaces > Add (LAN)

Créer une interface Suricata sur LAN : 1. Services > Suricata > onglet Interfaces 2. Cliquer sur [+ Add]

— Onglet LAN Settings — Enable : ☒ Cocher Interface : LAN

(Surveillance du réseau interne / Zero Trust) Description : Suricata LAN – IDS/IPS Détection Interne

☑ **Interface LAN configurée dans Suricata — mode IDS actif (alerte sans blocage). Suricata inspecte maintenant le trafic LAN en temps réel.**

[Capture n°3 : Suricata Interfaces — Interface LAN listée avec statut Running (icône verte).

Interface Settings Overview						
	Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
☐	WAN (vmx1)	  	AUTO	LEGACY MODE	Suricata WAN – IDS/IPS Périphère	  
☐	LAN (vmx0)	  	AUTO	LEGACY MODE	LAN	  

 Add  Delete

Étape 4 — Activation des catégories de signatures ETOpen

 **Navigation : Suricata > Interfaces > LAN > LAN Rules**

Sélectionner les catégories de signatures à activer :

1. Suricata > Interfaces > cliquer sur l'icône [crayon] de LAN
2. Onglet : LAN Rules

Catégories ETOpen recommandées pour ce contexte :

- [✓] emerging-scan.rules → Détection de scans de ports (Nmap, Masscan...)
- [✓] emerging-exploit.rules → Tentatives d'exploitation de vulnérabilités
- [✓] emerging-malware.rules → Communications malware / C2
- [✓] emerging-dos.rules → Attaques par déni de service
- [✓] emerging-policy.rules → Violation de politiques réseau
- [✓] emerging-trojan.rules → Détection de chevaux de Troie

Cliquer sur [Save] pour appliquer les règles sélectionnées

Redémarrer l'interface : Services > Suricata > Interfaces > [Stop] > [Start]

⚠ FAUX POSITIFS : Certaines règles ETOpen peuvent générer des faux positifs (alertes sur du trafic légitime). Il est recommandé de démarrer en mode IDS et d'analyser les alertes pendant 24-48h avant d'activer le mode IPS (Block Offenders). Les faux positifs doivent être supprimés via l'onglet Suppress avant le passage en IPS.

☑ **Catégories de signatures activées — Suricata charge les règles et commence l'inspection du trafic WAN.**

III. ACTIVATION DU MODE IPS — Configuration de Block Offenders

Le passage en mode **IPS** s'effectue via l'option "**Block Offenders**" de Suricata. Lorsqu'elle est activée, Suricata envoie automatiquement à pfSense une demande de **blocage (drop)** de l'IP source à chaque fois qu'une signature est déclenchée. L'IP est ajoutée à une table de blocage et tous ses paquets suivants sont rejetés sans traitement. Cette action est enregistrée dans l'onglet **Blocks** de Suricata.

Étape 5 — Activation de Block Offenders (mode IPS)

 **Navigation : Suricata > Interfaces > LAN > LAN Settings > Block Settings**

PRÉREQUIS : Analyser les alertes (onglet Alerts) pendant 24-48h

et supprimer les faux positifs avant d'activer cette option.

— Section : Block Settings —

Block Offenders : [✓] COCHER → Passage en mode IPS actif

Kill States : ☒ Cocher
→ Supprime également les états de connexion actifs de l'IP bloquée

Which IP to Block : SRC (bloquer l'IP SOURCE attaquante)
Options : SRC / DST / BOTH – choisir SRC pour bloquer l'attaquant

— Section : Block Settings – Durée —

Block Repeat Offenders : ☒ Cocher
Remove Blocked Hosts Interval: 3600 (durée du bannissement en secondes = 1h)
→ Après 1h, l'IP est automatiquement débannie
→ En production : augmenter à 86400 (24h) selon la politique sécurité

Cliquer sur [Save]
Redémarrer l'interface : Suricata > Interfaces > [Stop] puis [Start] sur WAN

⚠ ATTENTION CRITIQUE — MODE IPS : Une fois Block Offenders activé, toute correspondance de signature entraîne un blocage immédiat. Si l'IP du serveur Zabbix (10.11.3.19) ou d'un équipement légitime déclenche une règle par erreur (faux positif), il sera banni automatiquement. Toujours ajouter les IPs internes en liste blanche (Whitelist) avant activation.

Ajouter les IPs internes en liste blanche (Pass List) :
Suricata > Pass Lists > [Add]

Description : Whitelist Infrastructure Interne
IPs / Subnets à inclure :
10.11.3.19/32 → SRV-ZABBIX (supervision)
10.11.3.17/32 → pfSense lui-même
127.0.0.0/8 → Loopback

Associer cette Pass List à l'interface LAN :
Suricata > Interfaces > LAN > LAN Settings
> Pass List : sélectionner "Whitelist Infrastructure Interne"

☑ Mode IPS activé — Block Offenders opérationnel — Pass List appliquée pour protéger les équipements internes contre les faux positifs.

[Capture n°5 : Suricata LAN Settings — Block Offenders coché, Kill States coché, Which IP to Block = SRC, Remove Blocked Hosts Interval = 3600.]

Alert and Block Settings	
Block Offenders	☒ Checking this option will automatically block hosts that generate a Suricata alert.
IPS Mode	Legacy Mode Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode. 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 Suricata 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 include: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.
Kill States	☒ Checking this option will kill firewall states for the blocked IP. Default is Checked.
Which IP to Block	SRC Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.
Block On DROP Only	☐ Checking this option will insert blocks only when rule signatures having the DROP action are triggered. When not checked, any rule action (ALERT or DROP) will generate a block of the offending host. Default is Not Checked.
IP Pass List	default View List Choose the Pass List you want this interface to use. Addresses in a Pass List are never blocked. Select "none" to prevent use of a Pass List. The default Pass List adds Gateways, DNS servers, locally-attached networks, the WAN IP, VPNs and VIPs. Create a Pass List with an alias to customize whitelisted IP addresses. This option will only be used when block offenders is on. Choosing "none" will disable Pass List generation.
Enable Passlist Debugging Log	☐ Checking this option will enable detailed Passlist operations logging to file /var/log/suricata/suricata_vmx15874/passlist_debug.log. Default is Not Checked.

IV. PHASE DE VALIDATION (AUDIT) — Nmap, Alertes et Blocages

La validation consiste à simuler une attaque réseau contrôlée depuis une machine externe au périmètre et à vérifier que Suricata détecte l'attaque (onglet **Alerts**) et bannit l'IP source (onglet **Blocks**). L'outil **Nmap** en mode agressif est idéal pour déclencher les signatures de détection de scan.

Étape 6 — Simulation d'un scan agressif avec Nmap

Navigation : Machine externe (hors réseau interne) — Terminal Kali Linux / Debian

```
# PRÉREQUIS : Utiliser une machine de test interne dont l'IP a été volontairement exclue de la liste
# blanche (Pass List) de Suricata.
# (ou une VM en réseau externe simulé)
# NE PAS utiliser une IP comprise dans la Pass List Suricata

# Scan Nmap agressif – déclenche les règles emerging-scan :
nmap -A -T4 --script=vuln 10.11.3.17

# Explications des options :
-A          : Scan agressif (OS, version, scripts, traceroute)
-T4         : Timing rapide (génère beaucoup de paquets)
--script=vuln : Scripts NSE de détection de vulnérabilités

# Alternative – scan SYN furtif (aussi détecté) :
nmap -sS -sV -p 1-65535 10.11.3.17

# Scan UDP (déclenche d'autres règles) :
nmap -sU -T4 --top-ports 100 10.11.3.17

# Résultat attendu côté Nmap : connexions bloquées / timeouts
# (une fois Block Offenders actif, Nmap ne reçoit plus de réponses)
```

⚠ CADRE LÉGAL : Ce test doit être réalisé UNIQUEMENT sur une infrastructure dont vous êtes l'administrateur

(environnement de lab BTS). Scanner des équipements sans autorisation est une infraction pénale (article 323-1 du Code pénal français).

[Capture n°6 : Terminal Kali/Debian — Commande Nmap -A -T4 --script=vuln 10.11.3.17 en cours d'exécution.

Étape 7 — Vérification des alertes dans l'onglet Suricata Alerts

 Navigation : pfSense > Services > Suricata > Alerts

Consulter les alertes générées par Suricata :

1. Services > Suricata > onglet Alerts

Colonnes à contrôler :

Timestamp : horodatage de l'alerte (doit correspondre au scan Nmap)

Interface : LAN

Source IP : IP de la machine Nmap (IP externe)

Dest IP : 10.11.3.17 (pfSense)

Proto : TCP ou UDP

Description : [2100366] ET SCAN NMAP -sV version scan (ou similaire)

Action : Alert (mode IDS) ou Drop (mode IPS actif)

Signature typiquement déclenchée par Nmap :

ET SCAN Nmap Scripting Engine User-Agent Detected

ET SCAN NMAP -sS window 1024

ET SCAN Potential SSH Scan

Filtrer les alertes par IP source :

→ Utiliser le champ de filtre en haut de la page

☒ **Alertes visibles dans l'onglet Suricata Alerts — signatures Emerging Threats déclenchées par le scan Nmap — horodatage cohérent.**

[Capture n°7 : Suricata Alerts — Tableau des alertes avec IP source Nmap, signature ET SCAN détectée, action Alert ou Drop visible.

Last 250 Alert Entries. (Most recent entries are listed first)										
Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
05/12/2026 21:07:46		1	TCP	Web Application Attack	10.11.3.23  	6583	10.11.3.17  	80	1:2024364  	ET SCAN Possible Nmap User-Agent Observed
05/12/2026 21:07:46		1	TCP	Web Application Attack	10.11.3.23  	6584	10.11.3.17  	80	1:2024364  	ET SCAN Possible Nmap User-Agent Observed
05/12/2026 21:07:46		1	TCP	Web Application Attack	10.11.3.23  	6581	10.11.3.17  	80	1:2024364  	ET SCAN Possible Nmap User-Agent Observed
05/12/2026 21:07:46		1	TCP	Web Application Attack	10.11.3.23  	6582	10.11.3.17  	80	1:2024364  	ET SCAN Possible Nmap User-Agent Observed
05/12/2026 21:07:46		1	TCP	Web Application Attack	10.11.3.23  	6578	10.11.3.17  	80	1:2024364  	ET SCAN Possible Nmap User-Agent Observed
05/12/2026 21:07:46		1	TCP	Web Application Attack	10.11.3.23  	6577	10.11.3.17  	80	1:2024364  	ET SCAN Possible Nmap User-Agent Observed
05/12/2026 21:07:46		1	TCP	Web Application Attack	10.11.3.23  	6574	10.11.3.17  	80	1:2024364  	ET SCAN Possible Nmap User-Agent Observed

Étape 8 — Preuve du bannissement dans l'onglet Blocks

 **Navigation : pfSense > Services > Suricata > Blocks**

Vérifier le bannissement de l'IP attaquante :

1. Services > Suricata > onglet Blocks

Colonnes à contrôler :

Timestamp : horodatage du bannissement

Blocked IP : IP de la machine Nmap (confirmée bannie)

Reason : Description de la signature ayant déclenché le blocage

Interface : LAN

Vérifier également dans pfSense que la table de blocage est alimentée :

Diagnostics > Tables > snort2c (ou suricata_block)

→ L'IP de la machine Nmap doit apparaître dans cette table

Test de confirmation : retenter un ping depuis la machine bloquée :

ping 10.11.3.17

Résultat attendu : Request timeout – IP bannie, paquets droppés

☒ **IP Nmap listée dans Blocks — Table de bannissement pfSense alimentée — le mode IPS est confirmé opérationnel.**

[Capture n°8 : Suricata Blocks — IP source Nmap listée avec horodatage et raison du blocage.

InterfacesGlobal SettingsUpdatesAlertsBlocksFilesPass ListsSuppressLogs ViewLogs MgmtSID Mgmt

SyncIP Lists

Blocked Hosts Log View Settings

Save or Remove Hosts

Download

All blocked hosts will be saved

Clear

All blocked hosts will be cleared

Save Settings

Save

Save auto-refresh and view settings

☒ Refresh

Default is ON

500

Number of blocked entries to view.
Default is 500

Last 500 Hosts Blocked by Suricata

Note: Only blocked IP addresses from Legacy Mode interfaces are shown! For inline IPS mode interfaces, dropped IP addresses are highlighted on the ALERTS tab.

Blocked IP	Block Date/Time	Block Alert Description	Block Rule GID:SID	Remove Block
10.11.3.23	05/12/2026 21:15:47	SURICATA ICMPv4 unknown code	1:2200025	✖

[Capture n°9 : pfSense Diagnostics > Tables > snort2c — IP de la machine Nmap visible dans la table de blocage.

Snort2c Table

IP Address	
10.11.3.18	
10.11.3.23	
150.171.27.10	
172.217.22.174	

Étape 9 — Intégration avec la centralisation de logs Zabbix (SRV-ZABBIX)

Navigation : SRV-ZABBIX — Terminal SSH + Interface Web Zabbix

Les alertes Suricata sont envoyées vers rsyslog si "Send Alerts to System Log" est coché
(configuré étape 2 et 3)

Vérifier la réception des alertes Suricata sur SRV-ZABBIX :
tail -f /var/log/pfsense.log | grep -i suricata
ou
tail -f /var/log/syslog | grep -i suricata

Exemple d'alerte Suricata dans syslog :
May 12 14:00:05 pfSense suricata[12345]: [1:2100366:7] ET SCAN NMAP...

Dans Zabbix – créer un item dédié aux alertes Suricata :
Key : log[/var/log/pfsense.log,suricata,,,skip]
→ Filtre sur le mot "suricata" pour ne remonter que les alertes IDS/IPS

Trigger Zabbix pour alerter sur chaque détection Suricata :
Expression : {SRV-ZABBIX:log[/var/log/pfsense.log,suricata,,,skip].strlen()}>0
Severity : High
Description: Suricata IDS/IPS – Intrusion ou scan détecté sur pfSense WAN

☒ Alertes Suricata intégrées dans Zabbix via rsyslog — supervision IDS/IPS et centralisation de logs unifiées sur SRV-ZABBIX.

[Capture n°10 : SRV-ZABBIX — tail -f /var/log/pfsense.log grep suricata — alertes Suricata visibles en temps réel.
→

10.11.3.19/zabbix/history.php?action=showvalues&items%5B%5D=53705

Résumer

Afficher comme Valeurs

Format texte

Conversation

Zabbix server: Syslog pfSense — Logs Pare-feu (filterlog)

Liste d'éléments

Zabbix server: Syslog pfSense — Logs Pare-feu (filterlog)

Sélectionner

Valeur

Sélectionné

Afficher sélections

Appliquer

Réinitialiser

Horodateur	Heure locale	Valeur
12/05/2026 20:56:05	2026-05-12T20:55:56+00:00	_gateway filterlog[25935]: 4,,,1000000103,vmx1,match,block,in,4,0x0,,64,40169,0,none,1,icmp,29,10.10.101.4,10.10.101.3,request,50983,306569
12/05/2026 20:56:05	2026-05-12T20:55:56+00:00	_gateway filterlog[25935]: 4,,,1000000103,vmx1,match,block,in,4,0x0,,64,38521,0,none,1,icmp,29,10.10.101.56,10.10.255.255,request,58546,555869
12/05/2026 20:56:05	2026-05-12T20:55:56+00:00	_gateway filterlog[25935]: 4,,,1000000103,vmx1,match,block,in,4,0x0,,64,48984,0,none,1,icmp,29,10.10.101.4,10.10.101.3,request,50983,306559
12/05/2026 20:56:05	2026-05-12T20:55:55+00:00	_gateway suricata[23269]: message repeated 3 times: [[1:2231000:1] SURICATA QUIC failed decrypt [Classification: Generic Protocol Command Decode] [Priority: 3] [UDP] 10.10.101.3:45528 -> 151.101.129.91:443]
12/05/2026 20:56:05	2026-05-12T20:55:55+00:00	_gateway suricata[23269]: [1:2231000:1] SURICATA QUIC failed decrypt [Classification: Generic Protocol Command Decode] [Priority: 3] [UDP] 10.10.101.3:45528 -> 151.101.129.91:443
12/05/2026 20:56:05	2026-05-12T20:55:55+00:00	_gateway suricata[23269]: message repeated 4 times: [[1:2231000:1] SURICATA QUIC failed decrypt [Classification: Generic Protocol Command Decode] [Priority: 3] [UDP] 10.10.101.3:27605 -> 151.101.1.91:443]
12/05/2026 20:56:05	2026-05-12T20:55:55+00:00	_gateway suricata[23269]: [1:2231000:1] SURICATA QUIC failed decrypt [Classification: Generic Protocol Command Decode] [Priority: 3] [UDP] 10.10.101.3:27605 -> 151.101.1.91:443

V. BILAN ET ARGUMENTAIRE — Bloc 3 Sécurité & Démarche SOC

#	Action réalisée	Résultat observé	Statut
1	Installation package Suricata sur pfSense	Suricata accessible dans Services > Suricata	OK
2	Configuration signatures Emerging Threats Open	Règles téléchargées et indexées — base de signatures opérationnelle	OK
3	Paramétrage interface LAN (mode IDS)	Interface LAN active — statut Running — alerte sans blocage	OK
4	Sélection catégories rules (scan, exploit, malware)	Règles ETOpen actives sur l'interface LAN	OK
5	Activation Block Offenders (mode IPS) + Pass List	IPS actif — IPs internes whitelistées — bannissement configuré	OK
6	Scan Nmap agressif depuis machine externe	Scan effectué — paquets Nmap injectés sur 10.11.3.17	OK
7	Vérification alertes dans Suricata Alerts	Signatures ET SCAN déclenchées — alertes horodatées visibles	OK
8	Preuve blocage IP Nmap dans onglet Blocks	IP Nmap bannie — table snort2c alimentée — paquets dropped	OK
9	Intégration alertes Suricata dans Zabbix (rsyslog)	Alertes IDS/IPS visibles dans Monitoring > Latest data Zabbix	OK

Argumentaire Jury — Bloc 3 SISR (Sécurité) & Démarche SOC

► **Défense en profondeur (Bloc 3)** — En déployant la sonde Suricata sur l'interface LAN, la politique de sécurité adopte une approche "Zero Trust". L'IPS ne se contente pas de surveiller les menaces extérieures, il analyse également les comportements suspects provenant des postes internes (ex: mouvement latéral, scan interne, ou poste infecté).

► **Non-répudiation et traçabilité** — Chaque alerte Suricata est horodatée, signée par une règle identifiée (SID), et transmise via Syslog à SRV-ZABBIX. Cette chaîne garantit la non-répudiation des événements de sécurité et constitue une preuve d'audit exploitable.

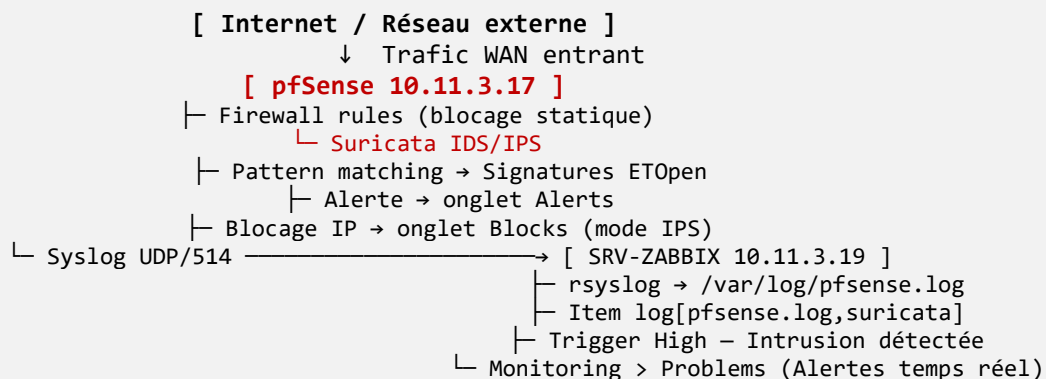
► **Intégration dans une démarche SOC** — La combinaison pfSense (IDS/IPS Suricata) + Zabbix (centralisation Syslog) constitue un SOC (Security Operations Center) miniature : détection, corrélation, historisation et alerte en

temps réel sur un tableau de bord unique.

► **Gestion des faux positifs** — La démarche en deux temps (IDS d'abord, IPS ensuite) démontre la maturité de l'approche : analyser les faux positifs avant d'activer le blocage évite les interruptions de service causées par des règles trop agressives.

► **Recommandations ANSSI** — Cette configuration suit les recommandations ANSSI (Guide de sécurisation des systèmes d'information) sur la mise en place de mécanismes de détection d'intrusion et la journalisation des événements de sécurité.

Architecture SOC déployée — Chaîne de supervision et sécurité



Conclusion technique — Mots-clés BTS SIO SISR

L'implémentation de **Suricata IDS/IPS** sur pfSense transforme le périmètre réseau d'une protection statique (règles pare-feu) vers une **protection active et dynamique** basée sur de la **détection comportementale par signatures**. L'intégration avec Zabbix via Syslog construit une chaîne de supervision complète répondant aux exigences du **Bloc 3 SISR** et d'une démarche **SOC (Security Operations Center)** professionnelle.

🔑 **Mots-clés jury** : IDS • IPS • Suricata • Pattern matching • Signatures • Drop • Block Offenders • Emerging Threats • Faux positifs • Non-répudiation • SOC • DPI • Syslog • Bloc 3 SISR • ANSSI • pfSense