BTS SIO — Option SISR — Fiche de Réalisation Professionnelle

Centralisation des Logs Pare-feu via Syslog

pfSense (10.11.3.17) → SRV-ZABBIX (10.11.3.19) — Traçabilité des accès réseau

Protocole Syslog UDP/514 | pfSense 2.7.x | Zabbix 6.x/7.x | Bloc 3 SISR — Sécurité & Traçabilité

EN-TÊTE — TABLEAU RÉCAPITULATIF	
Champ	**Valeur**
Candidat	BTS SIO option SISR — Session 2026
Entreprise	SIO SISR
Objet	Centralisation des logs pare-feu pfSense via Syslog vers SRV-ZABBIX
Source des logs	pfSense — 10.11.3.17 — Pare-feu / Routeur
Destination des logs	SRV-ZABBIX — 10.11.3.19 — Serveur de supervision
Protocole	Syslog — UDP port 514 (RFC 5424)
Référentiel SISR	Bloc 3 — Sécurité informatique / Traçabilité des accès réseau
Date	Mai 2026
Fiche n°	E6 — Supervision et Maintenance

I. THÉORIE — Supervision vs Centralisation de Logs

La **supervision** (via SNMP ou WMI) consiste à interroger périodiquement des équipements pour en extraire des indicateurs de performance (CPU, RAM, débit, statut de service). C'est un modèle **pull** : le serveur de supervision demande la donnée. La **centralisation de logs via Syslog** est à l'inverse un modèle **push** : l'équipement émet lui-même ses journaux dès qu'un événement se produit, sans attendre d'être interrogé. Ces deux mécanismes sont complémentaires et tous deux présents dans un dispositif SISR complet.

Comparatif — Supervision SNMP/WMI vs Centralisation de logs Syslog		
Critère	**Supervision (SNMP / WMI)**	**Centralisation de logs (Syslog)**
Modèle	Pull — le serveur interroge la cible	Push — la cible émet ses logs en temps réel
Données collectées	Métriques quantitatives (CPU, RAM, interfaces)	Événements qualitatifs (blocages, erreurs, connexions)
Protocole	SNMP UDP/161 ou WMI (RPC/DCOM)	Syslog UDP/514 (RFC 5424) ou TCP/514 sécurisé
Fréquence	Périodique (polling interval configurable)	Temps réel — envoi immédiat à chaque événement
Cas d'usage SISR	MCO, performances, disponibilité	Sécurité, traçabilité, audit des accès réseau
Apport Bloc 3 SISR	Détection de surcharge ou panne système	Preuve de conformité, détection d'intrusion, forensics

II. CONFIGURATION pfSense — Envoi des Logs vers SRV-ZABBIX

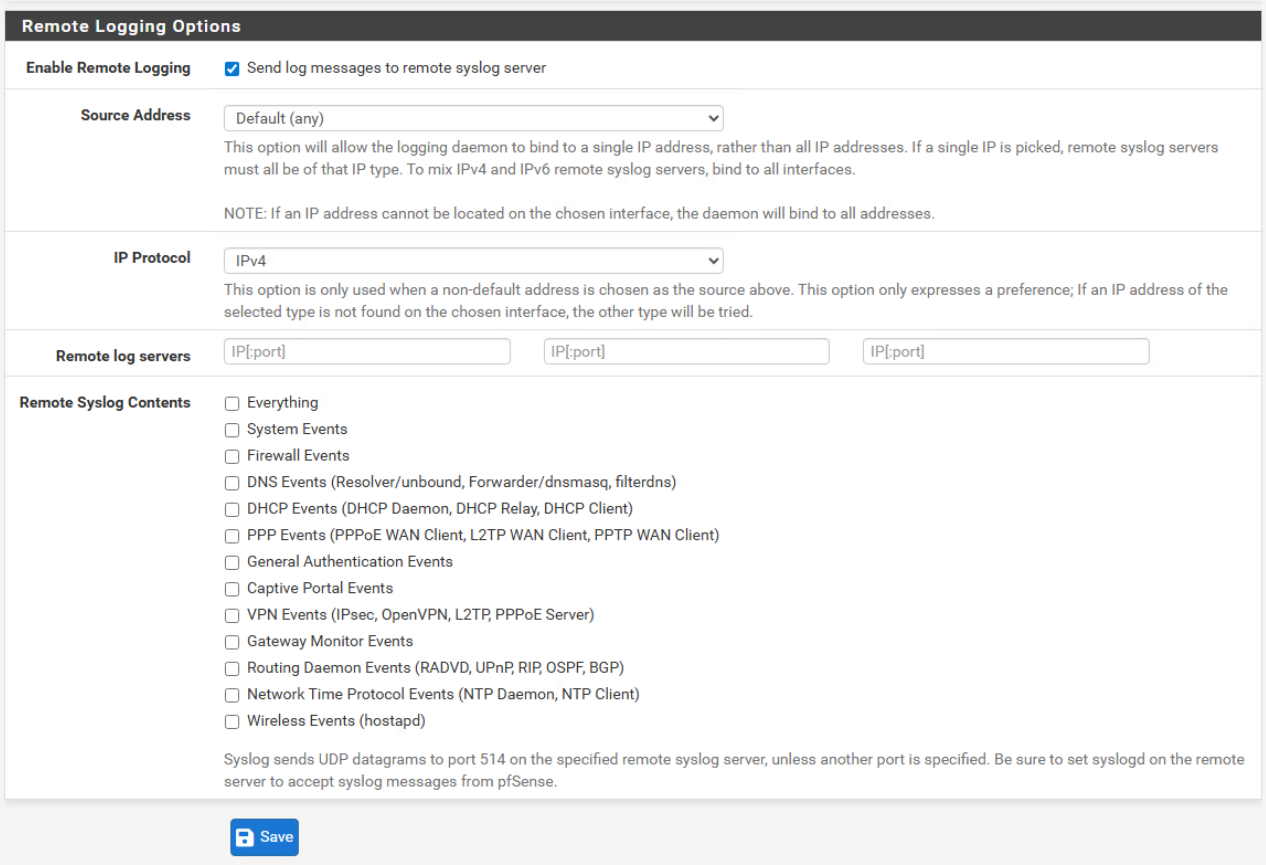
pfSense intègre nativement un émetteur Syslog. Il suffit de renseigner l'adresse IP du serveur de réception (SRV-ZABBIX — 10.11.3.19) dans les paramètres système pour que pfSense commence à envoyer ses journaux en **UDP sur le port 514**. La configuration s'effectue entièrement depuis l'interface web de pfSense, sans installation de paquet supplémentaire.

Étape 1 — Accès aux paramètres Syslog de pfSense

Navigation : pfSense — Interface Web (https://10.11.3.17) > Status > System Logs > Settings

```
# Navigation dans l'interface web pfSense :

1. Ouvrir un navigateur et accéder à https://10.11.3.17
2. Se connecter avec un compte admin
3. Menu : Status
4. Sous-menu : System Logs
5. Cliquer sur l'onglet : Settings

# → La page "System Logs – Settings" s'affiche
```

[Capture n°1: Interface web pfSense — Menu Status > System Logs > onglet Settings affichant la section "Remote Logging Options".



Étape 2 — Activation du Remote Logging et configuration du serveur Syslog

Navigation : pfSense > Status > System Logs > Settings > Remote Logging Options

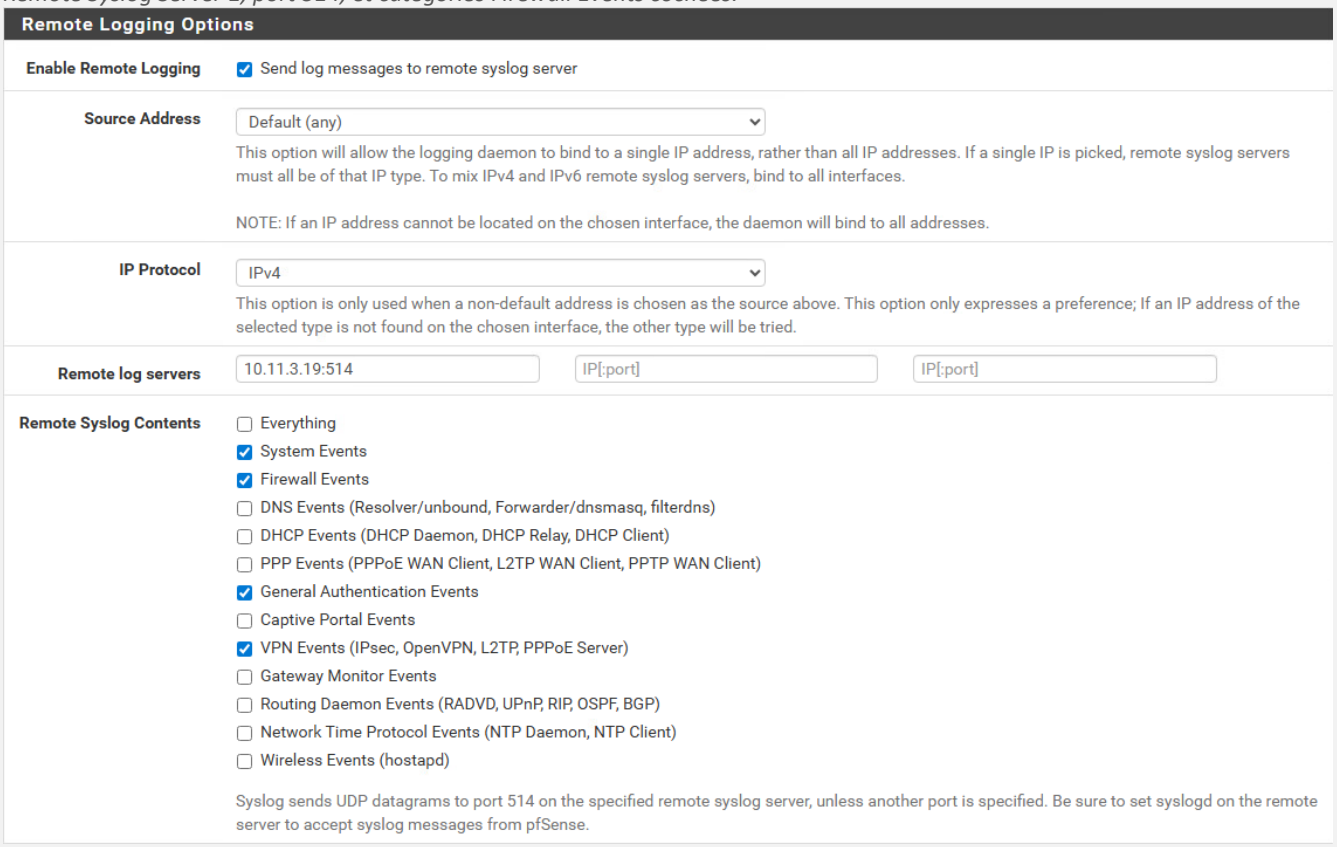
```
# Paramètres à configurer dans la section "Remote Logging Options" :

Enable Remote Logging     : [✓] Cocher la case

Source Address            : (laisser par défaut – interface LAN/WAN de pfSense)

IP Protocol               : IPv4
```

```
# Remote log servers (champ 1 sur 3 disponibles) :
Remote Syslog Server 1    : 10.11.3.19
Port                      : 514

# Syslog Contents — sélectionner les catégories à envoyer :
[✓] Firewall Events       ← PRIORITÉ — blocages et règles du pare-feu
[✓] General System Events ← Événements système généraux
[✓] Authentication Events ← Connexions / authentifications
[✓] VPN IPSEC   ← Optionnel selon le contexte

# Cliquer sur [Save] pour appliquer
```

⚠ UDP vs TCP : Par défaut, pfSense envoie les Syslog en UDP/514. L'UDP est non fiable (perte de paquets possible en cas de surcharge réseau). Pour un environnement de production critique, activer TLS Syslog (TCP/6514) si le récepteur le supporte. En contexte BTS/TP, UDP/514 est la configuration standard et suffisante.

☑ Remote Logging activé sur pfSense — cible : 10.11.3.19:514 — catégories Firewall Events et General System Events sélectionnées.

[Capture n°2: pfSense Settings — Section Remote Logging Options avec Enable Remote Logging coché, IP 10.11.3.19 saisie dans Remote Syslog Server 1, port 514, et catégories Firewall Events cochées.



Étape 3 — Vérification immédiate dans les logs pfSense

Navigation : pfSense > Status > System Logs > Firewall

```
# Vérifier que les logs de firewall sont bien générés localement :
1. Status > System Logs > onglet Firewall
2. Consulter les entrées — chaque règle de blocage génère une ligne

# Format d'une entrée Syslog pfSense (firewall) :
<timestamp> pfSense filterlog:
<in/out>,<interface>,<rule>,<proto>,<src_ip>,<dst_ip>,<src_port>,<dst_port>
```

```
# Exemple de log de blocage :
May 11 17:00:01 pfSense filterlog: 2,,1000000103,em0,match,block,in,4,0x0,,64,
    12345,0,none,6,tcp,60,192.168.1.100,10.11.3.17,54321,22,0
```

Logs locaux présents dans Status > System Logs > Firewall — les événements sont bien générés par pfSense.

[Capture n°3 : pfSense — Status > System Logs > Firewall — liste des dernières entrées de pare-feu.

System | Firewall | DHCP | Authentication | IPsec | PPP | PPPoE/L2TP Server | OpenVPN | NTP | Packages | Settings

Normal View | Dynamic View | Summary View

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✕	May 12 09:43:24	WAN	Default deny rule IPv4 (1000000103)	10.10.101.4	10.10.101.3	ICMP
✕	May 12 09:43:24	WAN	Default deny rule IPv4 (1000000103)	10.10.255.254:67	255.255.255.255:68	UDP
✕	May 12 09:43:24	WAN	Default deny rule IPv4 (1000000103)	10.10.101.56	10.10.255.255	ICMP
✕	May 12 09:43:24	WAN	Default deny rule IPv4 (1000000103)	10.10.101.4	10.10.101.3	ICMP
✕	May 12 09:43:25	WAN	Default deny rule IPv4 (1000000103)	10.10.101.4	10.10.101.3	ICMP
✕	May 12 09:43:25	WAN	Default deny rule IPv4 (1000000103)	10.10.101.56	10.10.255.255	ICMP
✕	May 12 09:43:25	WAN	Default deny rule IPv4 (1000000103)	10.10.101.4	10.10.101.3	ICMP
✕	May 12 09:43:25	WAN	Default deny rule IPv4 (1000000103)	10.10.101.56	10.10.255.255	ICMP

III. CONFIGURATION SRV-ZABBIX — Réception et Intégration Syslog

Sur SRV-ZABBIX (Debian/Linux), les logs Syslog envoyés par pfSense sont reçus par le démon **rsyslog**, qui les écrit dans un fichier dédié. Zabbix lit ensuite ce fichier via un item de type **log[...]** (agent) pour les intégrer dans sa base d'historique et les rendre consultables dans **Monitoring > Latest data**.

Étape 4 — Configuration de rsyslog pour recevoir les logs pfSense

Navigation : SRV-ZABBIX — Terminal SSH (root ou sudo)

```
# 1. Créer un fichier de configuration dédié pour pfSense
nano /etc/rsyslog.d/10-pfsense.conf

# --- Contenu du fichier 10-pfsense.conf (À copier dans nano) ---
# Activer la réception UDP sur le port 514
module(load="imudp")
input(type="imudp" port="514")

# Rediriger les logs venant de pfSense vers un fichier dédié
if $fromhost-ip == "10.11.3.17" then {
    action(type="omfile" file="/var/log/pfsense.log")
    stop
}
# ------------------------------------------------------------#
```

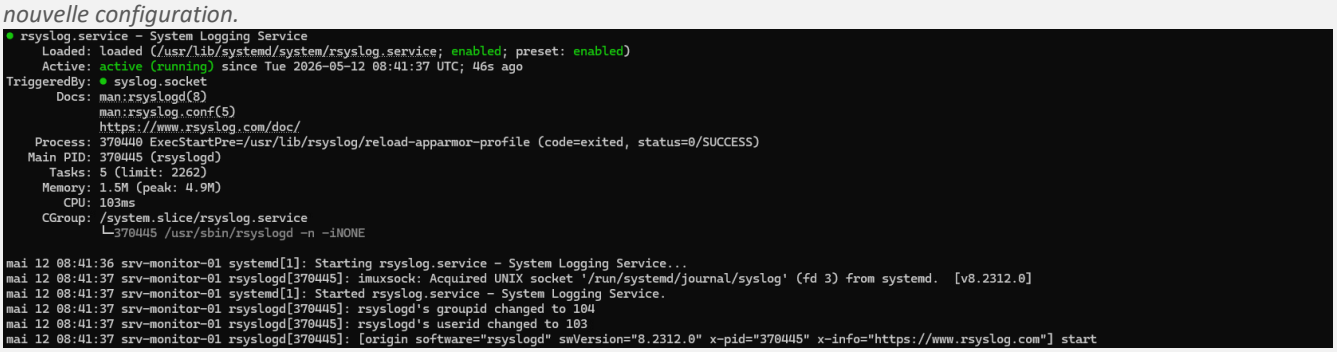
```
# Créer le fichier de log et attribuer les droits :
touch /var/log/pfsense.log
chmod 640 /var/log/pfsense.log
chown syslog:adm /var/log/pfsense.log

# Redémarrer rsyslog pour appliquer la configuration :
systemctl restart rsyslog
```

```
systemctl status rsyslog
# Résultat attendu : Active: active (running)
```

⚠ PARE-FEU SRV-ZABBIX : Si un pare-feu est actif sur SRV-ZABBIX (iptables/nftables), autoriser le trafic entrant UDP/514 : iptables -A INPUT -p udp --dport 514 -s 10.11.3.17 -j ACCEPT
Cette règle limite la réception aux logs de pfSense uniquement (moindre privilège).

☑ rsyslog configuré — réception UDP/514 activée — fichier /var/log/pfsense.log créé avec les droits adéquats.

[Capture n°4: Terminal SRV-ZABBIX — systemctl status rsyslog affichant Active: active (running) après redémarrage avec la nouvelle configuration.



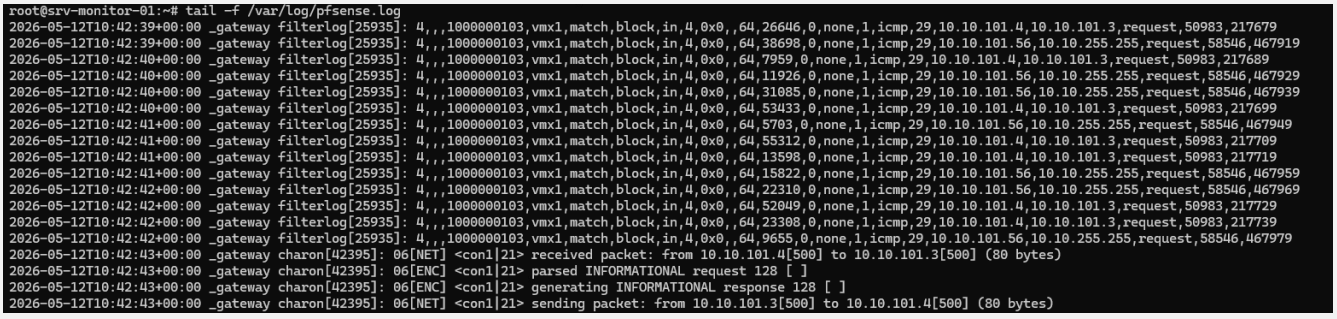
Étape 5 — Vérification de la réception des logs pfSense sur SRV-ZABBIX

Navigation : SRV-ZABBIX — Terminal SSH (root ou sudo)

```
# Surveiller en temps réel l'arrivée des logs pfSense :
tail -f /var/log/pfsense.log

# Résultat attendu (exemple d'entrée pfSense reçue) :
May 11 17:05:00 pfSense filterlog: 2,,1000000103,em0,match,block,in,...

# Si le fichier reste vide après 1 minute :
→ Vérifier que pfSense envoie bien sur 10.11.3.19 (étape 2)
→ Vérifier le port UDP/514 ouvert sur SRV-ZABBIX :
   ss -ulnp | grep 514
   # Résultat attendu : udp  UNCONN  0  0  0.0.0.0:514  ...

# Vérifier la connectivité réseau pfSense → SRV-ZABBIX :
# Depuis pfSense (Diagnostics > Ping) : ping 10.11.3.19
```

☑ Logs pfSense reçus et écrits dans /var/log/pfsense.log — réception Syslog fonctionnelle sur SRV-ZABBIX.

[Capture n°5 : Terminal SRV-ZABBIX — tail -f /var/log/pfsense.log affichant des entrées filterlog en temps réel avec l'Ip source 10.11.3.17.



Étape 6 — Création de l'Item Zabbix pour lire /var/log/pfsense.log

Navigation : Interface Web Zabbix > Configuration > Hosts > SRV-ZABBIX > Items > Create item

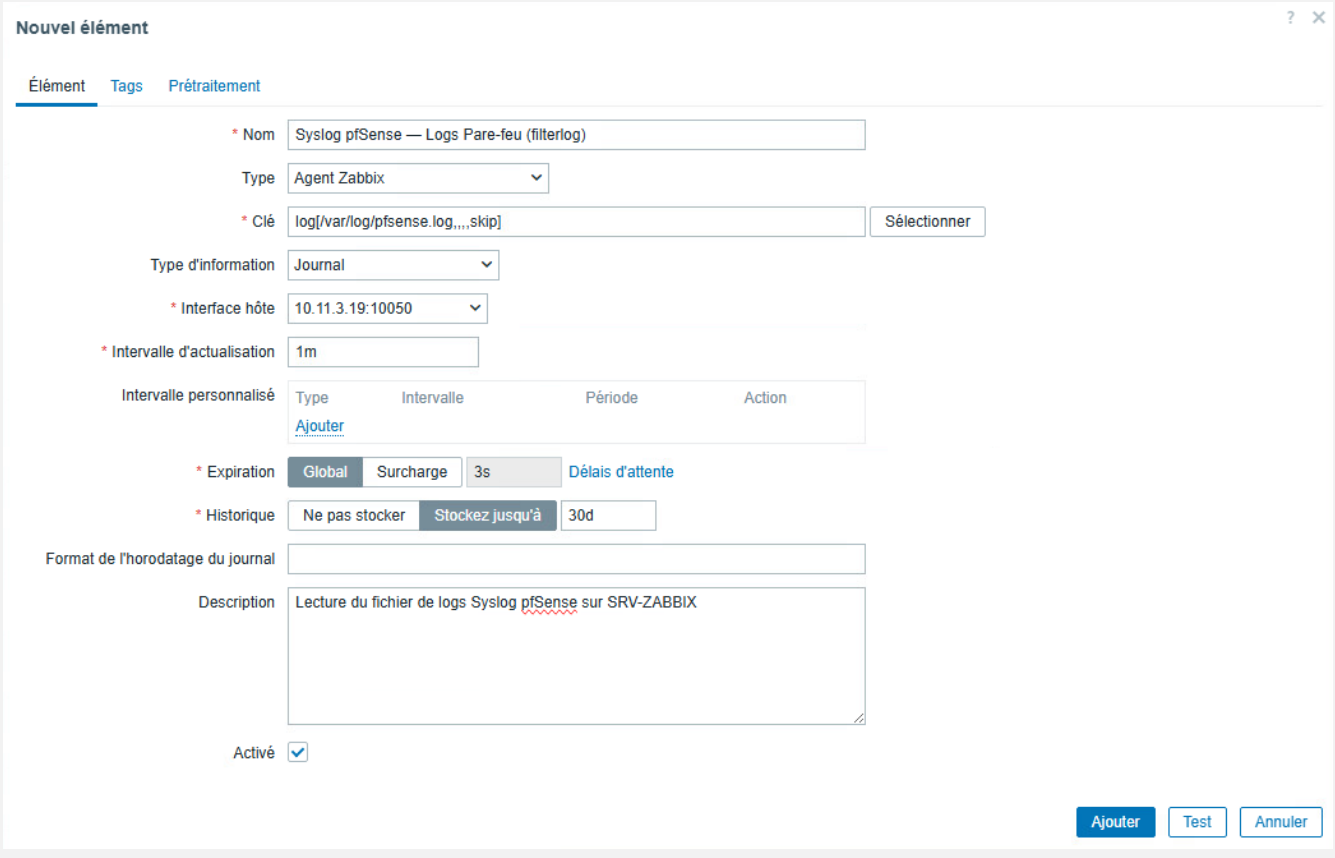
```
# Paramètres de l'item Zabbix à configurer :
```

```
Name                : Syslog pfSense — Logs Pare-feu (filterlog)
Type                : Zabbix agent  (agent installé sur SRV-ZABBIX)
Key                 : log[/var/log/pfsense.log,,,,skip]
Type of information: Log
Update interval     : 30s  (surveillance fréquente pour la sécurité)
History storage     : 30 days
Description         : Lecture du fichier de logs Syslog pfSense sur SRV-ZABBIX

# Syntaxe complète de la clé log[] :
log[file,<regexp>,<encoding>,<maxlines>,<mode>,<output>,<maxdelay>,<options>]

# Explication des paramètres utilisés :
  /var/log/pfsense.log  → fichier à surveiller
  (vide)                → pas de filtre regexp (toutes les lignes)
  (vide)                → encodage par défaut (UTF-8)
  (vide)                → maxlines par défaut
  skip                  → ne lit que les nouvelles lignes (ignore historique)

# Alternative — filtrer uniquement les blocages pfSense :
Key : log[/var/log/pfsense.log,block,,,,skip]
    → retourne uniquement les lignes contenant "block"
```

⚠ DROITS AGENT : L'agent Zabbix doit avoir les droits de lecture sur /var/log/pfsense.log. Si l'agent tourne sous le compte "zabbix", ajouter ce compte au groupe "adm" :
usermod -aG adm zabbix
systemctl restart zabbix-agent
Sans ce droit, la clé log[] retournera une erreur de permission.

☑ Item Zabbix créé — type Zabbix agent — clé log[/var/log/pfsense.log,,,,skip] — type Log — Zabbix commencera à ingérer les nouvelles lignes du fichier.

[Capture n°6 : Interface Zabbix — Formulaire Create item avec Name, Type (Zabbix agent), Key log[/var/log/pfsense.log,,,,skip] et Type of information (Log).



IV. VALIDATION — Génération d'un Blocage et Vérification dans Zabbix

La validation consiste à générer volontairement un événement de blocage sur pfSense et à vérifier que la ligne correspondante apparaît dans **Monitoring > Latest data** de Zabbix. Cela prouve la chaîne complète : pfSense → Syslog UDP/514 → rsyslog → /var/log/pfsense.log → agent Zabbix → base Zabbix.

Étape 7 — Générer un blocage sur pfSense

Navigation : pfSense > Firewall > Rules OU Diagnostics > Ping depuis une machine source

```
# Méthode 1 – Tentative de connexion bloquée (depuis CL-WIN11 ou tout poste) :
# Tenter d'accéder à un port bloqué par une règle pfSense

# Depuis CL-WIN11 (PowerShell) – tenter une connexion SSH vers pfSense :
Test-NetConnection -ComputerName 10.11.3.17 -Port 22
# Si SSH est bloqué → pfSense génère une entrée filterlog "block"

# Méthode 2 – Depuis pfSense, créer une règle de blocage temporaire :
# Firewall > Rules > LAN > Add rule :
  Action   : Block
  Protocol : TCP
  Source   : any
  Destination: This Firewall (WAN address)
  Port     : 22 (SSH)
  Description: TEST-SYSLOG-VALIDATION
# → Sauvegarder, puis tenter d'accéder à ce port depuis un client

# Méthode 3 – Trafic vers une IP inexistante (route par défaut bloquée) :
# Depuis CL-WIN11 : ping 10.11.99.99
# pfSense enregistre le trafic bloqué en sortie
```

⚠ IMPORTANT : S'assurer que la règle de test est supprimée après la validation. Laisser une règle de blocage incorrecte en production peut perturber le trafic légitime. Documenter la procédure de test dans le rapport de validation.

☑ **Blocage généré sur pfSense — entrée filterlog visible dans Status > System Logs > Firewall.**

[Capture n°7 : pfSense — Status > System Logs > Firewall — entrée de blocage "block" générée lors du test, avec IP source, destination et port visibles.

✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.1 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.2 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.6 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.3 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.7 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.4 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.5 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.8 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.9 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.10 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.11 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.12 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.13 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.14 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.3.17 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.17 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.18 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.19 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.20 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.21 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.22 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.24 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.23 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.25 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.26 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.27 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.30 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.28 ICMP
✓	May 12 12:30:03	LAN	TEST_LOG_ZABBIX (1778580717)	10.11.3.19	10.11.4.29 ICMP

]

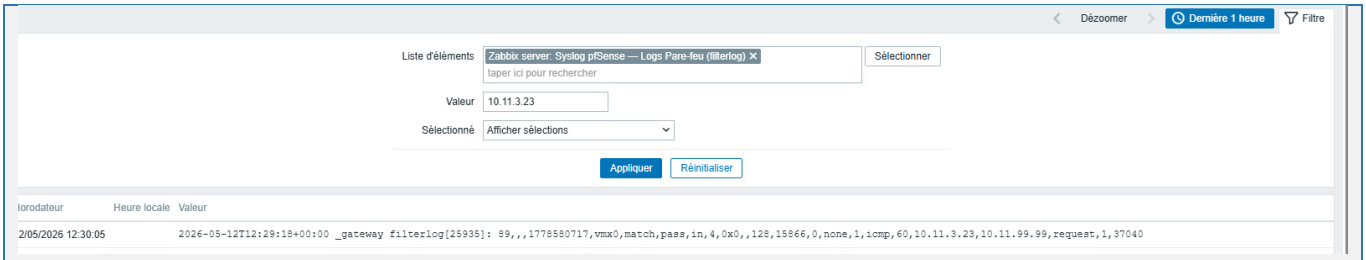
Étape 8 — Vérifier l'apparition du log dans Zabbix (Monitoring > Latest data)

Navigation : Interface Web Zabbix > Monitoring > Latest data > Host = SRV-ZABBIX

```
# Procédure de vérification dans Zabbix :
1. Monitoring > Latest data
2. Filtre : Host = SRV-ZABBIX
3. Filtre : Name = Syslog pfSense (ou filterlog)
4. Cliquer sur [Apply]

# Colonnes à contrôler :
Host       : SRV-ZABBIX
Name       : Syslog pfSense — Logs Pare-feu (filterlog)
Last value : [dernière ligne du log pfSense reçue]
Last check : [horodatage récent — quelques secondes après le test]

# Cliquer sur "History" de l'item pour voir toutes les entrées collectées :
→ Chaque ligne = un événement Syslog reçu depuis pfSense

# Exemple de valeur attendue dans Last value :
May 11 17:10:30 pfSense filterlog: 2,,1000000103,em0,match,block,in,4,...,10.11.3.100,10.11.3.17
```

☑ Entrée de blocage visible dans Monitoring > Latest data — la chaîne Syslog complète est validée : pfSense → rsyslog → Zabbix.

[Capture n°8 : Monitoring > Latest data — Ligne de l'item "Syslog pfSense" affichant l'entrée de blocage filterlog avec horodatage récent.



[Capture n°9 : Historique de l'item (clic sur History) — plusieurs entrées Syslog pfSense montrant la continuité de la collecte des logs.
→ Insérer ici la capture d'écran correspondante]

Étape 9 — Configurer un Trigger Zabbix sur les logs de blocage (optionnel avancé)

Navigation : Configuration > Hosts > SRV-ZABBIX > Triggers > Create trigger

```
# Trigger pour alerter sur chaque blocage pfSense détecté :

Name       : pfSense – Blocage détecté dans les logs Syslog
Expression : {SRV-ZABBIX:log[/var/log/pfsense.log,,,,skip].logseverity()}>0

# Alternative avec filtre sur le mot "block" :
Expression : find(/Zabbix server/log[/var/log/pfsense.log,,,,skip],,"like","block")=1

Severity   : Warning (ou High selon la politique de sécurité)
Description: Événement de blocage pare-feu détecté sur pfSense

# Ce trigger génèrera une alerte Zabbix visible dans :
Monitoring > Problems
→ Chaque blocage pfSense crée un événement Zabbix traçable et auditable
```

VALEUR AJOUTÉE JURY : La création de ce trigger transforme la simple collecte de logs en un mécanisme d'alerte en temps réel. C'est la différence entre une supervision passive (archivage des logs) et une supervision active (détection et notification d'incidents).

V. BILAN ET ARGUMENTAIRE — Bloc 3 SISR & Traçabilité des Accès

#	Action réalisée	Résultat observé	Statut
1	Activation du Remote Logging sur pfSense	IP 10.11.3.19:514 configurée, catégories Firewall Events cochées	☑ OK
2	Vérification des logs locaux pfSense	Entrées visibles dans Status > System Logs > Firewall	☑ OK
3	Configuration rsyslog (réception UDP/514)	rsyslog actif, fichier /var/log/pfsense.log créé et alimenté	☑ OK
4	Vérification réception SRV-ZABBIX	tail -f /var/log/pfsense.log affiche les entrées pfSense	☑ OK
5	Création item Zabbix log[/var/log/pfsense.log]	Item type Log actif sur SRV-ZABBIX	☑ OK
6	Génération d'un blocage test sur pfSense	Entrée filterlog "block" générée et visible	☑ OK
7	Vérification dans Monitoring > Latest data	Log de blocage présent — horodatage cohérent	☑ OK
8	Trigger Zabbix sur détection de	Alerte générée dans Monitoring >	☑ OK

	blocage	Problems	

Argumentaire oral — Lien avec le Bloc 3 SISR (Sécurité)

▶ **Traçabilité des accès réseau** — Les logs Syslog de pfSense constituent une preuve d'audit des règles pare-feu : chaque blocage est horodaté, tracé avec les IP source/destination et le port concerné.

▶ **Détection d'intrusion passive** — La corrélation des événements filterlog dans Zabbix permet d'identifier des tentatives répétées de connexion non autorisée (brute-force, scan de ports).

▶ **Non-répudiation** — L'horodatage par rsyslog sur SRV-ZABBIX garantit l'intégrité chronologique des journaux, même si pfSense venait à être compromis.

▶ **Conformité et MCO** — Cette démarche répond aux exigences RGPD et aux recommandations ANSSI sur la journalisation des équipements réseau en environnement professionnel.

▶ **Supervision active vs passive** — Le trigger Zabbix transforme la collecte passive de logs en alertes temps réel, s'intégrant dans un dispositif NOC complet.

Conclusion technique — Mots-clés BTS SIO SISR

La centralisation des logs pfSense via **Syslog UDP/514** vers SRV-ZABBIX complète le dispositif de supervision en ajoutant une dimension de **traçabilité et de sécurité** au-delà des simples métriques de performance. En intégrant ces logs dans Zabbix via la clé **log[]** et en créant un trigger sur les événements de blocage, l'administrateur dispose d'un mécanisme de détection d'incidents en temps réel, aligné avec les exigences du **Bloc 3 SISR — Sécurité** et les recommandations ANSSI sur la journalisation.

🎯 **Mots-clés jury :** *Syslog* • *UDP/514* • *rsyslog* • *filterlog* • *pfSense* • *Traçabilité* • *Non-répudiation* • *NOC* • *MCO* • *Bloc 3 SISR* • *ANSSI* • *log[] Zabbix* • *Supervision active*