
🛡️ **Sécurité et Sensibilisation**

Firewalls, IDS et Formation des Utilisateurs

Objectif : intégrer la sécurité au cœur des pratiques quotidiennes pour prévenir les incidents et renforcer la résilience du système d'information.

🔥 **1. Les Firewalls (Pare-feux)**

➤ **Rôle**

Les firewalls constituent la **première ligne de défense** du réseau.
Ils contrôlent les flux entrants et sortants selon des règles prédéfinies, empêchant ainsi tout accès non autorisé.

➤ **Types de pare-feux**

Type	Description	Exemple
Pare-feu réseau	Filtre les paquets entre réseaux (LAN, WAN, Internet)	Cisco ASA, Fortinet, pfSense
Pare-feu applicatif (WAF)	Analyse les requêtes HTTP/HTTPS au niveau applicatif	ModSecurity, AWS WAF
Pare-feu personnel	Protège les postes utilisateurs	Windows Defender Firewall

➤ **Bonnes pratiques**

- Bloquer tous les ports inutilisés et autoriser uniquement le nécessaire (principe du **moindre privilège**)
- Mettre à jour régulièrement les signatures et règles de filtrage
- Surveiller les logs et activer les alertes d'anomalie

🕵️ **2. Les IDS/IPS (Intrusion Detection/Prevention Systems)**

➤ **Rôle**

Les IDS (et leur version proactive IPS) surveillent en continu le trafic réseau ou les activités système pour **détecter les comportements suspects**.

➤ **Types d'IDS**

Type	Fonction	Exemple
NIDS (Network IDS)	Analyse le trafic réseau	Snort, Suricata

Type	Fonction	Exemple
HIDS (Host IDS)	Surveille les fichiers et processus d'un hôte spécifique	OSSEC, Wazuh

➤ **Fonctionnement**

1. Collecte des données réseau et systèmes
2. Analyse comportementale ou par signatures
3. Détection d'anomalies
4. Génération d'alertes (et blocage pour IPS)

➤ **Bonnes pratiques**

- Définir une politique claire de réponse aux alertes
- Coupler IDS/IPS avec un **SIEM** (ex. : Wazuh + Graylog) pour centraliser les logs
- Réaliser des tests d'intrusion pour ajuster les signatures

🧠 **3. Sensibilisation et Formation des Utilisateurs**

➤ **Pourquoi ?**

Les utilisateurs représentent souvent **le maillon le plus faible** en cybersécurité.
Une simple erreur humaine (clic sur un lien, mot de passe faible, partage de fichier sensible) peut compromettre tout un système.

➤ **Objectifs de la sensibilisation**

- Adopter des **réflexes de sécurité** au quotidien
- Identifier les **tentatives d'hameçonnage (phishing)**
- Comprendre les **risques liés aux données** et à la navigation

➤ **Moyens d'action**

- **Sessions de formation régulières** (courtes et pratiques)
- **Simulations d'attaques** (phishing tests)
- **Affichage de guides simples** dans les bureaux ou plateformes internes
- **Campagnes de communication** (email, affiches, vidéos courtes)

➤ **Bonnes pratiques utilisateur**

✅ Utiliser des mots de passe forts (et un gestionnaire de mots de passe)
✅ Verrouiller sa session lorsqu'on s'absente
✅ Ne jamais brancher de périphériques USB inconnus
✅ Signaler toute activité suspecte au service informatique

🧩 4. Intégration dans la stratégie globale de sécurité

Une sécurité efficace repose sur une approche **multi-couches** :

1. **Prévention** → Firewalls, mises à jour, segmentation réseau
2. **Détection** → IDS/IPS, SIEM, alertes
3. **Réaction** → Plans de réponse et procédures d'incident
4. **Formation** → Sensibilisation continue des utilisateurs

🛠️ 5. Exemple d'implémentation pratique (Windows Server + Réseau d'entreprise)

1. 🔧 **Installer un pare-feu réseau (pfSense ou Fortinet)**
    - Créer des règles :
        - Autoriser le trafic web (HTTP/HTTPS)
        - Bloquer les connexions non sollicitées
    - Mettre en place une DMZ pour les serveurs exposés
2. 🧩 **Déployer un IDS (ex : Wazuh ou Snort)**
    - Surveiller les journaux système, authentifications, et connexions réseau
    - Configurer des alertes email/SMS
3. 👥 **Lancer une campagne de sensibilisation**
    - 1 atelier mensuel de 30 min
    - 1 test de phishing tous les trimestres
    - 1 guide PDF « Sécurité au quotidien » diffusé à tous les employés

---

🧭 Conclusion

La sécurité ne repose pas uniquement sur la technologie, mais sur **l'humain, la discipline et la culture de vigilance**.
Un pare-feu protège le réseau, un IDS détecte les menaces, mais **l'utilisateur averti** reste le meilleur bouclier contre les attaques.