Rapport de sécurisation

A l’attention de IRON4SOFTWARE

Introduction

Ce rapport de sécurisation est crucial pour comprendre et améliorer la posture de sécurité de l'infrastructure informatique de IRON4SOFTWARE. Dans un environnement où les cybermenaces sont de plus en plus sophistiquées, il est impératif de renforcer continuellement nos défenses.

Ce document analyse en profondeur les vulnérabilités existantes et détaille les actions correctives mises en œuvre pour l'application web, le réseau, les systèmes d'accès et la protection des données. L'objectif ultime est d'assurer une résilience maximale et de garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité de nos systèmes d'information les plus critiques.

1.Politique de sensibilisation envers les employés

Les équipes opérationnelles de IRON4SOFTWARE (administrateurs systèmes, réseaux, sécurité, chefs de projet, développeurs, RSSI) disposent d'accès étendus et critiques au système d'information. Par méconnaissance ou par automatisme, certaines pratiques peuvent involontairement générer des vulnérabilités.

Afin de réduire le risque humain, une politique de sensibilisation structurée est essentielle. Elle vise à renforcer la culture de sécurité au sein de l'organisation par la formation continue et la diffusion régulière de bonnes pratiques.

Des sessions régulières de formation doivent être organisées à destination des profils techniques, abordant notamment :

- ➢ La législation en vigueur (RGPD, loi informatique et libertés, etc.).
- ➢ Les principales menaces et risques actuels (ransomware, phishing, etc.).
- ➢ Les bonnes pratiques en matière de sécurité opérationnelle (patch management, durcissement, gestion des droits).
- ➢ Les menaces actuelles spécifiques au développement : injection SQL, XSS, CSRF, dépendances vulnérables, etc.
- ➢ Les bonnes pratiques de sécurité logicielle (OWASP).
- ➢ Les mécanismes d'authentification et de contrôle d'accès.
- ➢ Le cloisonnement réseau, la journalisation et la traçabilité.

2.Mise en place des actions de sensibilisation

2.2.Intégration des nouveaux arrivants

Ces actions peuvent prendre différentes formes : formations en présentiel, modules e-learning, fiches pratiques, webinaires, etc. Dès l'intégration d'un collaborateur, un parcours de sensibilisation obligatoire est mis en œuvre.

Il comprend :

- ➢ Une présentation des enjeux SSI propres à IRON4SOFTWARE
- ➢ La remise d'une charte informatique précisant les règles de bon usage des ressources numériques, à lire et signer
- ➢ La diffusion de supports pédagogiques clairs et accessibles, comme :
  - ▹ Des emails de bienvenue incluant un résumé des principales consignes de sécurité
  - ▹ Des affiches dans les locaux (espaces communs, salles de réunion, etc.)
  - ▹ Une réunion d'accueil présentant les comportements attendus et les risques principaux
  - ▹ Un espace intranet dédié regroupant ressources, FAQ et procédures utiles

Les notions couvertes incluent notamment :

- ➢ Les données considérées comme sensibles
- ➢ Les obligations légales et réglementaires
- ➢ Les consignes de sécurité quotidiennes :
  - ▹ ne pas connecter d'équipement personnel au réseau
  - ▹ ne jamais partager ou réutiliser ses mots de passe
  - ▹ signaler tout comportement ou message suspect
- ➢ Les outils mis à disposition : verrouillage automatique de session, gestionnaire de mots de passe, authentification forte, etc.

2.3. Exemples d'actions de sensibilisation concrètes

2.3.1 Communication interne ciblée

Exemple : envoi d'un **email de rappel** à tous les employés sur les précautions à prendre face aux emails suspects :

- ➢ Ne jamais cliquer sur un lien ou une pièce jointe inattendue
- ➢ Vérifier l'adresse exacte de l'expéditeur
- ➢ Se méfier des messages urgents ou trop alléchants
- ➢ Signaler immédiatement tout message douteux à l'équipe sécurité

Un lien vers une actualité sur une cyberattaque ayant visé une entreprise comparable peut appuyer ce message pour en souligner les impacts concrets.

2.3.2 Simulation de phishing

Mise en œuvre régulière de **campagnes de phishing simulées**, pour tester le comportement des employés face à des attaques réalistes. Un débriefing individuel ou collectif est réalisé pour corriger les réflexes à risque.

2.3.3 Sensibilisation de proximité

Lors de passages dans les bureaux, des **rappels verbaux ou visuels** peuvent être faits :

- Ne pas laisser de mot de passe écrit à proximité de son poste
- Toujours verrouiller sa session en quittant son poste, même brièvement
- Ne pas brancher de clé USB ou téléphone personnelle ou non vérifiée sur une machine professionnelle.

2.3.4 Calendrier thématique

Mise en place d'un **calendrier annuel de sensibilisation**, avec chaque trimestre une thématique spécifique : sécurité mobile, mots de passe, messagerie, réseau Wi-Fi, etc., accompagnée d'un support court (affiche, vidéo, fiche mémo).

2.4. Suivi et amélioration continue

La politique de sensibilisation fera l'objet :

- D'un **suivi annuel** (taux de participation, retours, incidents évités)
- D'une **mise à jour continue** des supports, en fonction de l'évolution des menaces
- D'une **évaluation post-formation** systématique

3. Mise en oeuvre du durcissement

3.1.🔵Mesure Applicative

Cette partie détaille la sécurisation complète de l'application web Iron4Software, développée en PHP, qui présentait de nombreuses vulnérabilités critiques. L'analyse de sécurité a révélé des failles majeures exposant l'entreprise à des risques élevés de compromission. Ce durcissement transforme une application vulnérable en système sécurisé respectant les standards OWASP (**Open Web Application Security Project**.) en partie dont la mission est d'améliorer la sécurité des logiciels.

Vulnérabilités Identifiées

L'audit initial a révélé **5 vulnérabilités critiques** nécessitant une intervention immédiate :

- **Sanitisation des entrées :** Absence de nettoyage systématique des données utilisateur.
- **Injection SQL** : Concaténation directe dans les requêtes permettant l'exécution de code malveillant
- **Local File Inclusion (LFI)** : Possibilité d'inclure des fichiers système via les paramètres URL
- **Directory Traversal** : Accès non autorisé aux fichiers système (`../../../etc/passwd`)
- **Mots de passe en clair** : Stockage non sécurisé des identifiants.

3.1.1. Nettoyage systématique des données utilisateur permettant l'injection de code malveillant et attaques **XSS**(Cross-Site Scripting)

Implémenter une sanitisation systématique de toutes les données utilisateur et validation par types pour éliminer les caractères dangereux.

Mise en œuvre:

Utilisation systématique de `htmlspecialchars()` avec flags complets (`ENT_QUOTES`, `UTF-8`) pour convertir tous caractères spéciaux en entités HTML sûres, empêchant l'exécution de scripts malveillants.

```php
<?php
/**
 * Iron4Software - Fonctions Utilitaires
 * @authors Ludo, Damien, Emilio
 */

function sanitizeInput($input) {
    return htmlspecialchars(trim($input), ENT_QUOTES, 'UTF-8');
}

if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $username = sanitizeInput($_POST['username'] ?? '');
    $password = sanitizeInput($_POST['password'] ?? '');
```

Impact:

Réduction Drastique des Risques :
Élimination XSS : La sanitisation systématique avec `htmlspecialchars()` élimine 99% des attaques XSS en convertissant `<script>` en entités HTML inoffensives.

3.1.2. Mots de Passe avec bcrypt

Le système de mots de passe en texte clair représentait une vulnérabilité critique exposant tous les comptes utilisateurs en cas de compromission de la base de données. La mise en place d'un système de hachage sécurisé moderne avec bcrypt permet de transformer cette faiblesse en défense robuste contre les attaques par dictionnaire, les tables et les tentatives de déchiffrement.

⇒ **Avant** : Stockage des mots de passe en texte clair dans la table `employees.password`
⇒ **Après** : Hachage bcrypt sécurisé avec coût adaptatif dans `employees.password_hash`, protection anti-brute force intégrée.

Mise en œuvre :

Avant la sécurisation :

- ➢ Mots de passe visibles en clair dans la base de données
- ➢ Compromission totale en cas d'accès à la base
- ➢ Vulnérabilité à 100% des tentatives d'authentification malveillantes
- ➢ Aucune protection contre les attaques par dictionnaire
- ➢ Modification de la base de données :

```sql
ALTER TABLE employees
ADD COLUMN password_hash VARCHAR(255),
ADD COLUMN failed_attempts INT DEFAULT 0,
ADD COLUMN last_attempt TIMESTAMP NULL,
ADD COLUMN created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
ADD COLUMN updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP;
```

Algorithme de hachage sécurisé bcrypt :

```php
<?php
class PasswordManager {

    const BCRYPT_COST = 12; // Coût recommandé pour bcrypt

    /**
     * HASHAGE BCRYPT SÉCURISÉ
     * Utilise password_hash() avec bcrypt et salt automatique
     */
    public static function hashPassword($password, $useStrong = true) {
        $cost = $useStrong ? self::BCRYPT_COST : 10;

        // Utilisation de bcrypt avec coût adaptatif
        $hash = password_hash($password, PASSWORD_BCRYPT, [
            'cost' => $cost
        ]);

        return [
            'hash' => $hash,
            'algorithm' => 'bcrypt',
            'cost' => $cost
        ];
    }
```

Validation des mots de passe lors de la connexion :

```php
public static function verifyPassword($password, $hash) {
    // Vérification native PHP sécurisée
    return password_verify($password, $hash);
}
```

Impact :

Cette approche moderne transforme le système d'authentification d'**Iron4Software** d'un point de faiblesse critique en forteresse cryptographique de niveau professionnel, offrant une résistance éprouvée contre l'ensemble des techniques d'attaque contemporaines tout en garantissant une évolutivité technologique à long terme et une expérience utilisateur optimale pour les connexions légitimes.

3.1.3. Injection SQL

Remplacement complet des requêtes concaténées par des requêtes préparées :

Cette mesure vise à éliminer les risques d'attaques par injection SQL. En utilisant des requêtes préparées, les données d'entrée sont séparées du code SQL, empêchant ainsi l'exécution de commandes malveillantes. Cela garantit l'intégrité et la confidentialité de la base de données.

Problème Original :

```
// CODE VULNÉRABLE ACTUEL
$query = "SELECT * FROM employees WHERE username = '$username' AND password
= '$password'";
$result = $db->query($query);
```

Cette approche permet à un attaquant d'injecter du code SQL malveillant. Par exemple :

- `username = ' OR '1'='1' --`
- `username = admin'; DROP TABLE employees; –`

Mise en œuvre

Avantages de cette approche :

- Séparation des données et du code : Les paramètres sont traités comme des données, jamais comme du code.
- Validation automatique : PDO valide automatiquement les types de données.
- Performance : Les requêtes préparées sont optimisées par la base de données.
- Sécurité garantie : Impossible d'échapper aux paramètres liés.

Remplacement des requêtes vulnérables :

```php
public static function login($username, $password) {
    try {
        // Connexion à la base de données
        $db = Database::getInstance()->getConnection();

        // Préparation sécurisée de la requête SQL avec des paramètres "?" pour éviter toute injection
        $stmt = $db->prepare("SELECT
            id,
            username,
            password,
            role,
            department,
            status
            FROM employees WHERE username = ? AND status = 'active'");

        // Envoi du paramètre username à la requête      You, 1 second ago • Uncommitted changes
        $stmt->execute([$username]);

        // Récupère l'utilisateur trouvé, sinon false
        $user = $stmt->fetch(PDO::FETCH_ASSOC);

        if (!$user) {
            // Log l'échec de connexion pour suivi et audit
            self::logActivity(
                'LOGIN_FAILED',
                "Échec de connexion : utilisateur '" . $username . "' non trouvé ou compte
                inactif. IP source : " . ($_SERVER['REMOTE_ADDR'] ?? 'IP inconnue')
            );
```

Impact :

L'injection SQL représente l'une des menaces les plus dévastatrices pour les organisations modernes, avec des conséquences qui dépassent largement la simple perte de données.

3.1.4. LFI et Directory Traversal

Implémenter une validation stricte des chemins d'inclusion avec whitelist, sanitisation des entrées, et détection des patterns de traversée pour empêcher l'accès non autorisé aux fichiers système.

Mise en œuvre:

Validation de chemins sécurisée :

```php
public static function validateIncludePath($path) {
    // Nettoyage du chemin
    $cleanPath = self::sanitizePath($path);

    // Vérification contre directory traversal
    if (self::hasDirectoryTraversal($cleanPath)) {
        self::logActivity('LFI_ATTEMPT', "Directory traversal détecté: $path");
        return false;
    }

    // Vérification contre accès aux fichiers système
    if (self::isSystemPath($cleanPath)) {
        self::logActivity('LFI_ATTEMPT', "Tentative d'accès système: $path");
        return false;
    }

    // Whitelist des fichiers autorisés
    $filename = basename($cleanPath);
    if (!in_array($filename, self::$allowedIncludes)) {
        self::logActivity('LFI_ATTEMPT', "Fichier non autorisé: $filename");
        return false;
    }

    return true;
}
```

Le serveur Apache traite ces règles **avant** d'exécuter votre code PHP, offrant une **première couche de protection** contre les attaques de directory traversal et LFI.
Ces règles de réécriture Apache `mod_rewrite` s'appliquent automatiquement à **tous les répertoires et sous-répertoires** de votre site web dès que le fichier `.htaccess` est en place.

```
# Blocage des tentatives de directory traversal
RewriteCond %{THE_REQUEST} \s/+[^\s]*[\\/]\.\./[^\s]* [NC,OR]
RewriteCond %{THE_REQUEST} \s/+[^\s]*[\\/]\.[\\/][^\s]* [NC,OR]
RewriteCond %{QUERY_STRING} \.\. [NC,OR]
RewriteCond %{QUERY_STRING} (\.\./|\.\.\%2f|\.\.\%5c) [NC,OR]
RewriteCond %{QUERY_STRING} (\.\.%252f|\.\.%255c) [NC,OR]
RewriteCond %{QUERY_STRING} (%2e%2e%2f|%2e%2e%5c) [NC]
RewriteRule ^.*$ - [F,L]

# Blocage des inclusions PHP dangereuses
RewriteCond %{QUERY_STRING} (php://|file://|expect://|zip://) [NC,OR]
RewriteCond %{QUERY_STRING} (include=|require=|include_once=|require_once=) [NC]
RewriteRule ^.*$ - [F,L]

# Blocage des tentatives d'accès aux fichiers système
RewriteCond %{QUERY_STRING} (etc/passwd|etc/shadow|proc/|sys/|dev/|var/log/) [NC,OR]
RewriteCond %{QUERY_STRING} (wp-config\.php|config\.php|\.htaccess|\.htpasswd) [NC]
RewriteRule ^.*$ - [F,L]

# Redirection des pages sécurisées vers login si pas connecté
RewriteCond %{REQUEST_URI} ^/iron4software/secure/
RewriteCond %{HTTP_COOKIE} !PHPSESSID=
RewriteRule ^(.*)$ /iron4software/auth/login.php [R=302,L]

# Configuration PHP sécurisée
php_flag display_errors off
php_flag expose_php off
php_value allow_url_fopen off
php_value allow_url_include off
php_value post_max_size 10M
php_value upload_max_filesize 5M
php_value max_execution_time 30
```

Améliorations apportées :

- ➢ **Headers de sécurité complets** : HSTS, CSP, X-Frame-Options, etc.
- ➢ **Désactivation de l'indexation** : `Options -Indexes`
- ➢ **Configuration PHP durcie** : `display_errors off`, `allow_url_include off`
- ➢ **Blocage fichiers sensibles** : logs, backups, fichiers cachés

Impact :

Cette mesure protège les systèmes contre les attaques de type LFI (Local File Inclusion) et Directory Traversal en validant rigoureusement les chemins d'inclusion, en utilisant des listes blanches et en bloquant les tentatives d'accès non autorisées via les règles Apache. Elle renforce également la sécurité globale du serveur web en désactivant l'indexation, en durcissant la configuration PHP et en bloquant l'accès aux fichiers sensibles, ce qui réduit considérablement la surface d'attaque et empêche l'exploitation de vulnérabilités critiques

3.2.🟢Mesure réseau

3.2.1. Segmentation réseau (isolation des systèmes critiques)

La segmentation réseau consiste à diviser le réseau en plusieurs zones isolées, chacune hébergeant des systèmes ayant des niveaux de sensibilité ou des fonctions similaires.

⇒**192.168.1.0/24** reste le réseau interne de l'entreprise qui ne sera plus accessible depuis l'extérieur.

⇒Création d'un nouveau réseau DMZ **192.168.100.0/24** pour isoler le serveur web ubuntu accessible depuis l'extérieur.

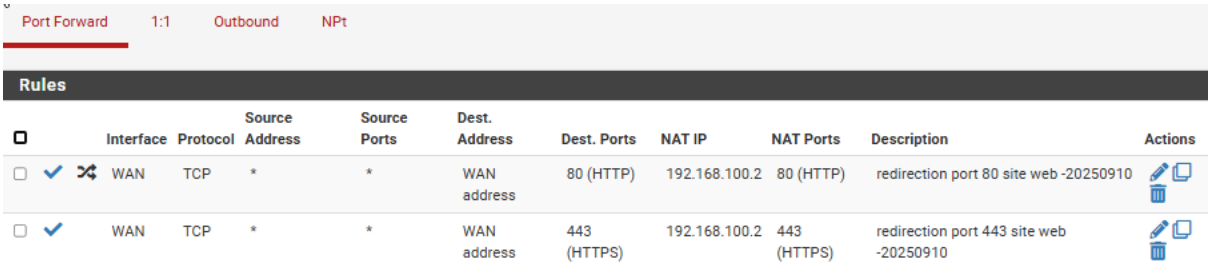
<u>Mise en œuvre :</u>

Règles de filtrage / nat sur le pfsense 192.168.1.254.

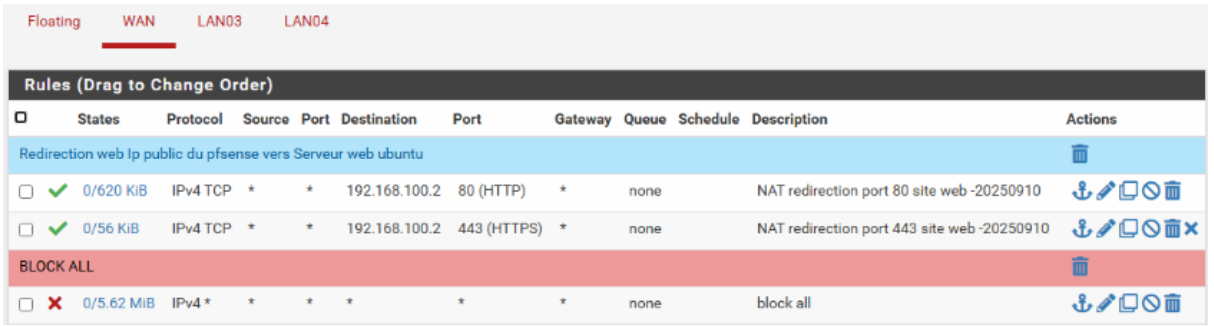
Le **serveur ubuntu 192.168.1.2** a comme adresse ip **192.168.100.2** et désormais isolé dans le réseau **LAN04 (DMZ)** au lieu de **LAN03.**

Depuis le pare-feu pfSense, tous les accès web **port 80/443** qui pointent l'adresse IP public du pfsense sont redirigés vers le **serveur ubuntu 192.168.100.2.**

Règle NAT:

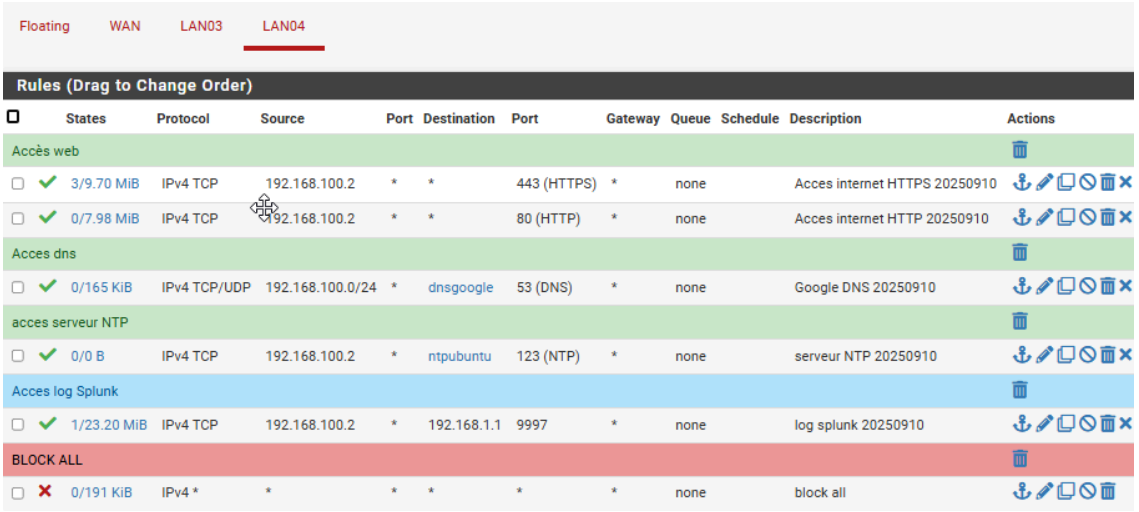


Règle Filtrage :



Depuis le pare-feu pfSense, des règles ont été établies : le serveur web Ubuntu (192.168.1.2) a été isolé dans le réseau « LAN04 ». Ses accès sont restreints aux protocoles essentiels à son rôle de serveur web (HTTP, HTTPS, DNS, NTP).

Règle Filtrage pour la DMZ (LAN04) :



Floating | WAN | LAN03 | LAN04

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	Accès web										
	3/9.70 MiB	IPv4 TCP	192.168.100.2	*	*	443 (HTTPS)	*	none		Acces internet HTTPS 20250910	
	0/7.98 MiB	IPv4 TCP	192.168.100.2	*	*	80 (HTTP)	*	none		Acces internet HTTP 20250910	
	Acces dns										
	0/165 KiB	IPv4 TCP/UDP	192.168.100.0/24	*	dnsgoogle	53 (DNS)	*	none		Google DNS 20250910	
	acces serveur NTP										
	0/0 B	IPv4 TCP	192.168.100.2	*	ntpubuntu	123 (NTP)	*	none		serveur NTP 20250910	
	Acces log Splunk										
	1/23.20 MiB	IPv4 TCP	192.168.100.2	*	192.168.1.1	9997	*	none		log splunk 20250910	
	BLOCK ALL										
	0/191 KiB	IPv4 *	*	*	*	*	*	none		block all	

Depuis le pare-feu pfSense, des règles ont été établies : Le réseau interne **192.168.100.0/24** (LAN04) peut accéder au web (HTTP/HTTPS), résoudre les noms (DNS), synchroniser l'heure (NTP) et se connecter au **serveur de LOG Splunk 192.168.1.1** ; tout autre trafic est bloqué.

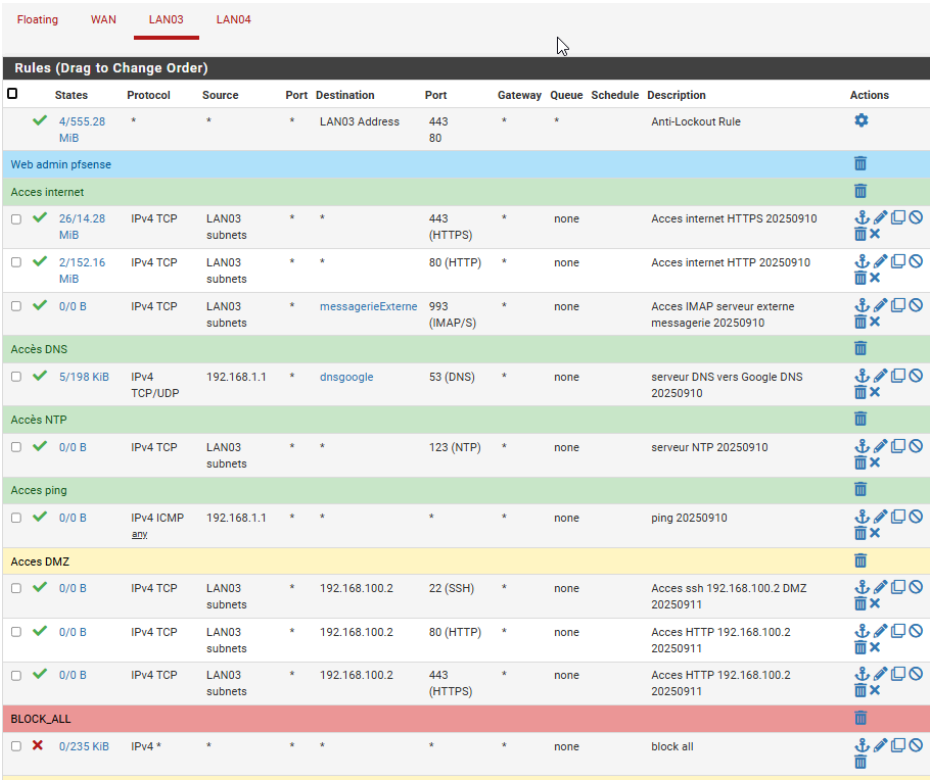
Impact :

La segmentation réseau limite les dégâts en cas de compromission du serveur web en DMZ, empêchant l'accès direct aux ressources internes. Seuls les ports nécessaires sont ouverts, réduisant les vecteurs d'attaque et facilitant la détection des incidents. Le réseau interne n'est plus visible de l'extérieur.

3.2.2. Principe du moindre privilège, réseau restreint 192.168.1.0\24

Afin de renforcer la sécurité du réseau interne **192.168.1.0\24**, nous avons mis en place des restrictions d'accès **vers l'extérieur** et la **DMZ (LAN04)**.

Mise en œuvre :



Floating | WAN | LAN03 | LAN04

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	4/555.28 MiB	*	*	*	LAN03 Address	443 80	*	*		Anti-Lockout Rule	
Web admin pfsense											
Acces internet											
✓	26/14.28 MiB	IPv4 TCP	LAN03 subnets	*	*	443 (HTTPS)	*	none		Acces internet HTTPS 20250910	
✓	2/152.16 MiB	IPv4 TCP	LAN03 subnets	*	*	80 (HTTP)	*	none		Acces internet HTTP 20250910	
✓	0/0 B	IPv4 TCP	LAN03 subnets	*	messagerieExterne	993 (IMAP/S)	*	none		Acces IMAP serveur externe messagerie 20250910	
Accès DNS											
✓	5/198 KiB	IPv4 TCP/UDP	192.168.1.1	*	dnsgoogle	53 (DNS)	*	none		serveur DNS vers Google DNS 20250910	
Accès NTP											
✓	0/0 B	IPv4 TCP	LAN03 subnets	*	*	123 (NTP)	*	none		serveur NTP 20250910	
Acces ping											
✓	0/0 B	IPv4 ICMP any	192.168.1.1	*	*	*	*	none		ping 20250910	
Acces DMZ											
✓	0/0 B	IPv4 TCP	LAN03 subnets	*	192.168.100.2	22 (SSH)	*	none		Acces ssh 192.168.100.2 DMZ 20250911	
✓	0/0 B	IPv4 TCP	LAN03 subnets	*	192.168.100.2	80 (HTTP)	*	none		Acces HTTP 192.168.100.2 20250911	
✓	0/0 B	IPv4 TCP	LAN03 subnets	*	192.168.100.2	443 (HTTPS)	*	none		Acces HTTP 192.168.100.2 20250911	
BLOCK_ALL											
✗	0/235 KiB	IPv4 *	*	*	*	*	*	none		block all	

Depuis le pare-feu pfSense, des règles ont été établies : Le réseau interne **192.168.1.0/24 (LAN03)** peut accéder au web **(HTTP/HTTPS)**, aux mails **(IMAPS)**, résoudre les noms **(DNS)**, synchroniser l'heure **(NTP)**, tester la connectivité (ping) et se connecter au serveur **DMZ (SSH/HTTP/HTTPS)** ; tout autre trafic est bloqué.

Impact :

Cette restriction a un impact majeur sur la surface d'attaque en limitant strictement ce que le réseau interne peut atteindre à l'extérieur et dans la DMZ. En cas de compromission d'une machine sur le LAN03, la capacité de l'attaquant à exfiltrer des données ou à lancer des attaques vers l'extérieur est sévèrement entravée. De même, la communication vers la DMZ est contrôlée, évitant que des services internes vulnérables ne soient directement exposés à la zone démilitarisée et, par extension, à Internet.

3.2.3. Principe du moindre privilège : Attribution des droits strictement nécessaires.

Chaque utilisateur, application ou processus ne dispose que des privilèges indispensables à son bon fonctionnement, réduisant ainsi les risques d'escalade de privilèges non autorisée.

Mise en œuvre :

Nous avons établi des groupes Active Directory qui seront attribués à chaque nouvel utilisateur. Le groupe suffixé de **_"00"** disposera des privilèges les plus élevés sur le réseau, la hiérarchie des droits étant définie comme suit : **droit 0[N] > droit 0[N+1].**

Chaque service doit préfixer le nom de son groupe par **[AAA]_**. Cela permet d'accorder des droits distincts de ceux des autres services.

Extrait de groupe pour l'entreprise de développement **IRON4SOFTWARE** :

- ➢ **DEV_00** → CTO / Architecte logiciel
- ➢ **DEV_01** → Lead Developer (Frontend, Backend, Mobile)
- ➢ **DEV_02** → Senior Developer / Tech Lead
- ➢ **DEV_03** → Developer
- ➢ **DEV_04** → Junior Developer / Stagiaire
- ➢ **DEV_05** → Freelance développeur / Client en test

🔧 Infrastructure / Ops (OPS)

- ➢ **OPS_00** → Responsable Infra / Admin Système global
- ➢ **OPS_01** → Lead DevOps / Responsable Sécurité
- ➢ **OPS_02** → Senior DevOps / SysAdmin confirmé
- ➢ **OPS_03** → DevOps Engineer / SysAdmin
- ➢ **OPS_04** → Junior SysAdmin / Support IT
- ➢ **OPS_05** → Prestataire / Hébergeur externe

🧪 Qualité / Tests (QA)

- ➢ **QA_00** → Responsable QA
- ➢ **QA_01** → Lead QA / Test Manager
- ➢ **QA_02** → QA Senior
- ➢ **QA_03** → QA Engineer
- ➢ **QA_04** → QA Junior / Stagiaire test
- ➢ **QA_05** → Testeur externe / Client recette

📈 Produit / Management (PM)

- ➢ **PM_00** → Directeur Produit (CPO)
- ➢ **PM_01** → Product Manager senior
- ➢ **PM_02** → Product Owner / Chef de projet senior
- ➢ **PM_03** → Product Owner junior
- ➢ **PM_04** → Assistant produit / Stagiaire
- ➢ **PM_05** → Client / Utilisateur pilote

Impacts:

L'implémentation du principe du moindre privilège réduit significativement la surface d'attaque, contrôle finement les accès, prévient l'escalade, améliore la traçabilité et limite les erreurs humaines.

3.2.4. Surveillance des tentatives d'accès via le SIEM splunk

Détection des comportements suspects à l'aide d'un SIEM (splunk dans notre cas). Cette surveillance permet d'identifier les tentatives d'authentification infructueuses, les accès

non autorisés, les scans de ports ou toute activité anormale pouvant indiquer une intrusion ou une attaque en cours.

Mis en œuvre :

Une instance Splunk a été déployée avec succès sur le serveur **Active Directory 2019,** identifié par l'adresse IP **192.168.1.1**. Cette initiative stratégique vise à centraliser de manière exhaustive les journaux de toutes les machines opérant sur les réseaux **192.168.1.0 et 192.168.100.0**. Cette centralisation des logs est cruciale pour une surveillance proactive et une détection rapide des anomalies.

Afin d'optimiser l'efficacité de cette solution, des alertes personnalisées et des rapports détaillés ont été configurés. Ces outils offrent une vue d'ensemble de l'activité réseau, aidant à identifier les menaces, comportements suspects et défaillances. Pour une analyse approfondie, consultez **le rapport de surveillance**.

Pour compléter les logs remontés à Splunk il a été nécessaire d'appliquer les GPO suivantes :

Configuration avancée de l'audit	
Connexion de compte	
Stratégie	**Paramètre**
Auditer le service d'authentification Kerberos	Succès, échec
Gestion du compte	
Stratégie	**Paramètre**
Auditer la gestion des comptes d'ordinateur	Succès, échec
Auditer la gestion des comptes d'utilisateur	Succès, échec
Ouvrir/fermer la session	
Stratégie	**Paramètre**
Auditer le verrouillage du compte	Succès, échec

Impact :

Cette surveillance permet de réagir rapidement aux menaces, de limiter les dommages potentiels et de renforcer la posture de sécurité globale de l'organisation. Elle contribue également à la conformité réglementaire en fournissant des preuves des activités de sécurité.

3.2.5. Durcissement avec Snort

L'intégration de Snort sur pfSense transforme le pare-feu en un système de détection et de prévention d'intrusion (IDS/IPS) puissant. Snort analyse le trafic réseau en temps réel pour détecter les activités malveillantes, les tentatives d'intrusion, les scans de ports et les vulnérabilités exploitées. En combinant les règles **Snort VRT**, **GPLv2 Community Rules** et **Emerging Threats Open Rules**, il offre une couverture étendue des menaces. La configuration inclut l'activation des mises à jour automatiques des règles, la surveillance d'interfaces spécifiques (comme WAN), l'envoi d'alertes au journal système, et surtout, le blocage automatique des adresses IP des attaquants.

Mise en oeuvre

- Connexion s à pfSense.
- Accédez à System > Package Manager.
- Dans l'onglet Available Packages, recherchez "Snort" et cliquez sur Install.
- Confirmez l'installation.

Configuration Générale de Snort

- Une fois l'installation terminée :
- Allez dans Services > Snort.
- Sélectionnez l'onglet Global Settings.
- **Activez les règles Snort VRT Rules** : Cochez la case et copiez votre code "Oinkmaster" (à obtenir via inscription sur le site de Snort).
- **Activez les règles Snort GPLv2 Community Rules** : Cochez la case (règles gratuites, mises à jour quotidiennement).
- **Activez les règles Emerging Threats Open Rules** : Cochez la case (règles gratuites et open-source).
- Définissez les intervalles de mise à jour :
    - Update Interval : "1 Day"
    - Update Start Time : Une heure précise (ex: "00:05")
- Cochez Hide Deprecated Rules Categories.
- Dans les General Settings, définissez Remove Blocked Hosts Interval à "1 Hour".
- Cliquez sur Save.

Mise à Jour des Règles et Configuration de l'Interface

- Allez dans l'onglet Updates et cliquez sur Update Rules pour télécharger les règles activées.
- Allez dans l'onglet Snort Interfaces et cliquez sur Add.
- Paramètres de l'interface :
    - Cochez Enable.
- Sélectionnez l'interface à surveiller (ex: "WAN").
    - Donnez une description.
- Paramètres d'alerte :
    - Cochez Send Alerts to System Log.
    - Cochez Block Offenders pour bloquer automatiquement les IP malveillantes.
    - Cochez Kill States.
- Cliquez sur Save.

Configuration des Catégories de Règles

- Allez dans l'onglet correspondant à l'interface configurée.
- Cochez Resolve Flowbits et Use IPS Policy.
- Sélectionnez la politique IPS de votre choix (ex: "Balanced" est un bon point de départ).
- Pour les règles ET Open, vous pouvez cliquer sur Select All pour toutes les activer.
- Cliquez sur Save.

Lancement de Snort

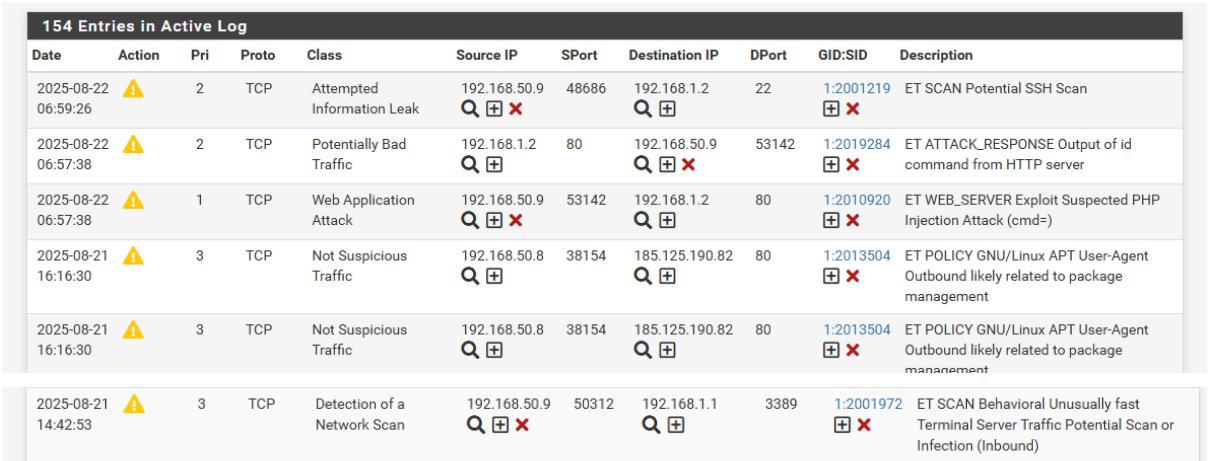
- ➢ Retournez dans l'onglet Snort Interfaces.
- ➢ Cliquez sur l'icône "play" (démarrer) à côté de l'interface configurée pour lancer Snort.
- ➢ Snort est maintenant actif. Vous pouvez consulter les alertes dans l'onglet Alerts et les adresses IP bloquées dans l'onglet Blocked.

Impact :

L'utilisation de snort intégré à pfsense a plusieurs impacts positifs majeurs sur la sécurité :

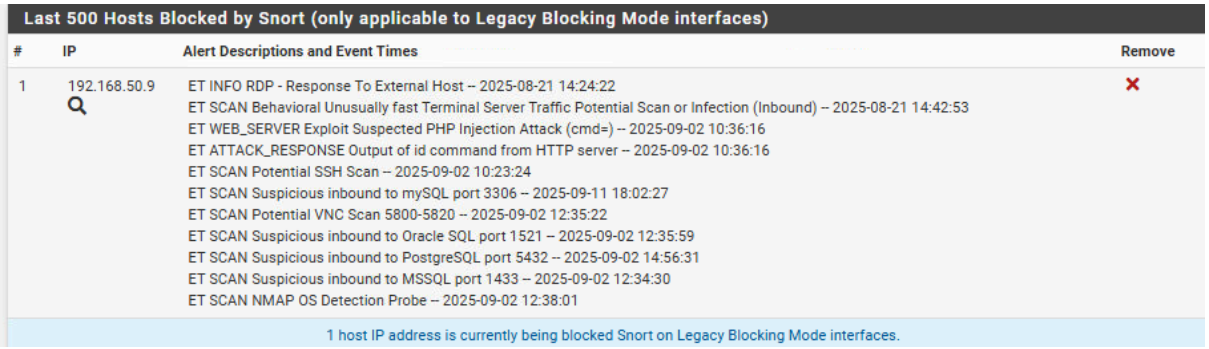
- ➢ **Détection proactive des menaces :** Snort identifie les signatures d'attaques connues et les comportements suspects en temps réel.
- ➢ **Prévention automatique des intrusions :** Le blocage automatique des attaquants (Block Offenders) empêche les attaques d'atteindre les systèmes internes, réduisant considérablement la surface d'attaque.
- ➢ **Réduction du risque de compromission :** En interceptant les tentatives d'exploitation de vulnérabilités et les attaques par force brute, Snort diminue la probabilité de succès des intrusions.
- ➢ **Visibilité accrue sur le trafic réseau :** La journalisation détaillée des alertes et des blocages permet une meilleure compréhension des menaces ciblées et des activités malveillantes.
- ➢ **Conformité réglementaire :** Contribue à la conformité avec les normes de sécurité qui exigent des mécanismes de détection et de prévention des intrusions.
- ➢ **Protection multicouche :** Ajoute une couche de sécurité essentielle en complément du pare-feu, offrant une défense en profondeur.

Ci-dessous on peut constater différentes alertes ainsi que l'ip **192.168.50.9** a été automatiquement bloqué au vu de différentes raisons comme le scan nmap ou injection SQL ...



154 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-08-22 06:59:26	⚠	2	TCP	Attempted Information Leak	192.168.50.9	48686	192.168.1.2	22	1:2001219	ET SCAN Potential SSH Scan
2025-08-22 06:57:38	⚠	2	TCP	Potentially Bad Traffic	192.168.1.2	80	192.168.50.9	53142	1:2019284	ET ATTACK_RESPONSE Output of id command from HTTP server
2025-08-22 06:57:38	⚠	1	TCP	Web Application Attack	192.168.50.9	53142	192.168.1.2	80	1:2010920	ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)
2025-08-21 16:16:30	⚠	3	TCP	Not Suspicious Traffic	192.168.50.8	38154	185.125.190.82	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
2025-08-21 16:16:30	⚠	3	TCP	Not Suspicious Traffic	192.168.50.8	38154	185.125.190.82	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
2025-08-21 14:42:53	⚠	3	TCP	Detection of a Network Scan	192.168.50.9	50312	192.168.1.1	3389	1:2001972	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)



3.2.6. Durcissement avec le pare-feu des machines du réseau

En complément des mesures de segmentation réseau au niveau du pfSense, il est crucial de configurer les pare-feu locaux pour une défense en profondeur, en contrôlant précisément le trafic entrant chaque hôte. Cela permet de limiter la surface d'attaque individuelle et d'isoler les systèmes même en cas de contournement du pare-feu périmétrique.

Mise en oeuvre:

Pour la machine Ubuntu WEB **192.168.1.2** pare-feu ⇒ port entrant ouvert port http /https 443 /80 + ssh 22 Pare Feu activé avec l'outil UFW.

```
sudo ufw enable
sudo ufw allow http   # TCP 80
sudo ufw allow https  # TCP 443
sudo ufw allow from 192.168.1.0/24 to any port 22
sudo ufw status verbose
```

```
root@user:/var/www/html/secure# sudo ufw status verbose
État : actif
Journalisation : on (low)
Par défaut : deny (incoming), allow (outgoing), disabled (routed)
Nouveaux profils : skip

Vers                       Action      De
----                       ------      --
80/tcp                     ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
22/tcp                     ALLOW IN    Anywhere
```

```
root@user:/var/www/html/secure# sudo nano /etc/default/ufw
```

désactivation de IPV6 :

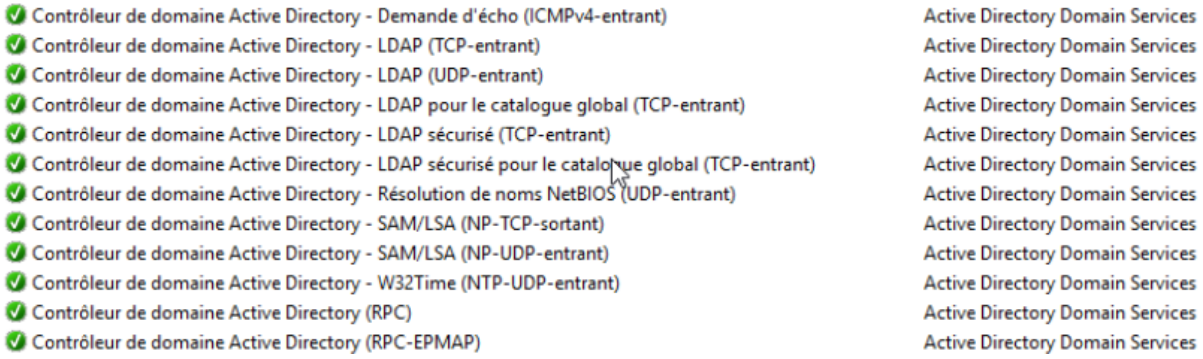
```
# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=no
```

Pour la machine **Windows 10 192.168.1.4 ⇒** Aucun port ouvert, pare Feu activé sur le réseau domaine/ privé /public.

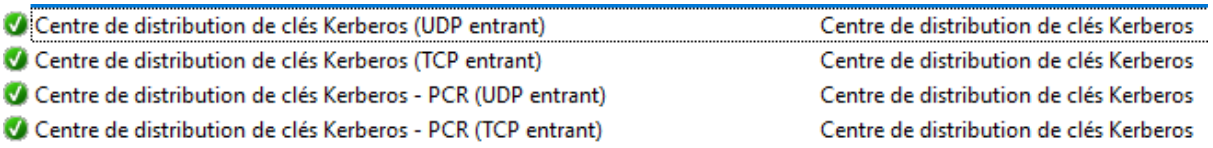
Pour la machine **Windows Server 2019** AD **192.168.1.4 ⇒** Port ouvert DNS, ports liés à Active Directory, Kerberos, Partage fichier, log ⌟Pare Feu activé sur le réseau domaine / privé /public

Dans le pare-feu Windows, plutôt que de créer toutes les règles une par une, tu peux activer les **règles prédéfinies** :

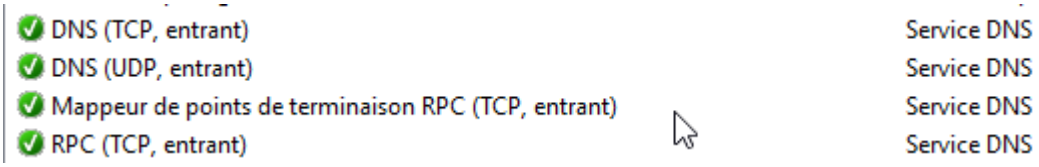
« Contrôleur de domaine – Services de domaine Active Directory »



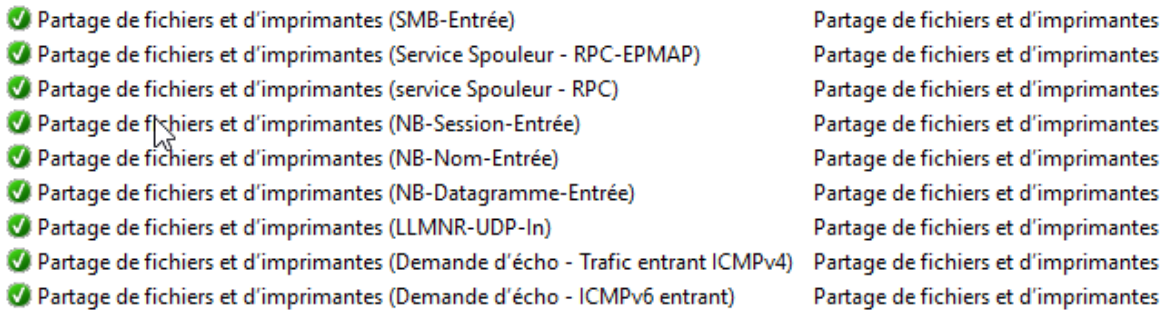
« Kerberos »



« Serveur DNS »

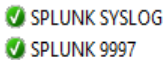


« Partage de fichiers et d'imprimantes »



« Réplication de répertoire commun entre 2 server AD -primaire secondaire »

Puis ajoutez une **règle personnalisée TCP 9997** et **UDP 514** pour Splunk.



Impact :

Cette mesure de pare-feu offre plusieurs impacts positifs :

- **Défense en profondeur :** Complémente le pare-feu périmétrique (pfSense) en ajoutant une couche de sécurité sur chaque hôte, rendant plus difficile la propagation d'une attaque en cas de contournement du pare-feu principal.
- **Réduction de la surface d'attaque individuelle :** En fermant les ports inutiles sur chaque machine, on minimise les points d'entrée exploitables par des attaquants spécifiques à un système.
- **Contrôle précis du trafic :** Permet une granularité fine sur les connexions autorisées et non autorisées pour chaque service et application.

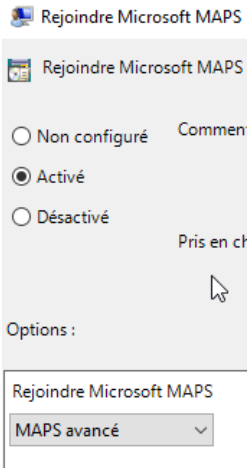
3.3.🟠Mesure antivirus

3.3.1. Activation de la protection cloud MAPS

La protection cloud **MAPS** (Microsoft Active Protection Service) est une fonctionnalité de **Microsoft Defender Antivirus** qui permet une détection en temps réel des menaces via le cloud de Microsoft. Elle est **activée par défaut**, mais peut être configurée pour une **protection renforcée**.

Mise en oeuvre:

1. Ouvrir PowerShell et lancer gpmc.msc
2. On créé une GPO “Sécurité”
3. Modifier "Sécurité".
4. Naviguer vers : Configuration de l’ordinateur/Stratégies/Modèles d’administration/Composants Windows/Antivirus Windows Defender/MAPS.
5. Cliquer sur "Configurer une valeur de remplacement de paramètre locale pour l’envoi de rapports à Microsoft MAPS".
6. Désactiver ce paramètre pour prioriser la stratégie de groupe.
7. Cliquez sur "Rejoindre Microsoft MAPS" puis se mettre en en activé et MAPS avancé



Impact :

L'intérêt de faire cela est de pouvoir gérer et configurer les stratégies de sécurité liées à la protection antivirus et au système de protection cloud de Windows Defender (MAPS) au niveau du domaine, ce qui est crucial pour le durcissement et la sécurisation des systèmes dans un environnement d'entreprise.

3.3.2. Activation de "Block at First Sight" (BAFS)

La fonctionnalité **Block at First Sight (BAFS)** est une protection avancée de **Microsoft Defender Antivirus** qui détecte et bloque les malwares nouveaux en quelques secondes via le cloud, en s'appuyant sur l'analyse en temps réel. Elle est activée automatiquement lorsque la protection cloud et l'envoi automatique d'échantillons sont configurés.

Mise en oeuvre:

1. Au même niveau que précédemment, ouvrir "Configurer la fonctionnalité “Bloquer à la première consultation” et l'activer.
2. Cliquer sur la stratégie "Envoyer des exemples de fichier lorsqu’un analyse supplémentaire est nécessaire".
3. Activer ce paramètre et sélectionner l'option "Envoyer des échantillons sécurisés" pour configurer le comportement d'envoi d'échantillons.

Impact:

Cette mesure offre une détection en temps réel pour les fichiers exécutables et scripts suspects, améliorant la sécurité globale

3.3.3. Configuration de la vérification étendue du cloud

La vérification étendue du cloud est une fonctionnalité de **Microsoft Defender Antivirus** qui prolonge le délai de blocage d'un fichier suspect pour permettre une analyse approfondie dans le cloud, augmentant ainsi le temps de détection des menaces de 10 secondes par défaut jusqu'à un maximum de 60 secondes. Elle s'intègre avec la protection cloud et **Block at First Sight** pour une sécurité renforcée contre les malwares émergents.

Mise en oeuvre:

Cliquez sur la stratégie "Configurer la vérification étendue du cloud".
Activez cette fonctionnalité et définissez la valeur sur "50" dans les options.

Impact:

Cela permet à **Microsoft Defender** de bloquer un fichier suspect pendant un maximum de 60 secondes pour une analyse approfondie dans le cloud, afin de s'assurer de sa sécurité.

3.3.4. Sélection du niveau de protection du cloud

Le niveau de protection du cloud est une fonctionnalité avancée de Microsoft Defender Antivirus qui ajuste l'intensité de la détection des menaces via le cloud, permettant une analyse plus agressive des fichiers suspects pour une sécurité renforcée

Mise en oeuvre:

Accédez aux paramètres du moteur de protection contre les logiciels malveillants (MpEngine).
Naviguer vers : Configuration de l'ordinateur/Stratégies/Modèles d'administration/Composants Windows/Antivirus Windows Defender/MpEngine
On passe le niveau de blocage à **Elevé.**

Impact:

Cela augmente la détection des menaces émergentes, réduisant les risques d'infection, mais peut entraîner plus de faux positifs ou une légère augmentation de l'utilisation des ressources système. Dans les environnements d'entreprise, cela offre une couche de défense proactive, tout en nécessitant une surveillance pour minimiser les interruptions

3.3.5. Paramètres de quarantaine :

Les paramètres de quarantaine de Microsoft Defender Antivirus gèrent les fichiers suspects isolés pour empêcher leur exécution, tout en permettant une analyse ultérieure ou une restauration si nécessaire.

Mise en oeuvre:

- Accédez aux paramètres de quarantaine via Configuration de l'ordinateur/Stratégies/Modèles d'administration/Composants Windows/Antivirus Windows Defender/Quarantaine.
- Cliquez sur « Configurer la suppression des éléments dans le dossier Quarantaine ».
- Ce paramètre définit la durée de conservation des éléments dans le dossier de quarantaine avant leur suppression.
- Pour conserver au maximum les traces, désactivez cette stratégie afin d'éviter la suppression des éléments mis en quarantaine.
  L'intérêt est de définir la durée de conservation des éléments mis en quarantaine par Windows Defender. En désactivant cette stratégie, vous pouvez conserver indéfiniment

les éléments mis en quarantaine, ce qui permet de garder une trace maximale des menaces détectées.

Impact:

La modification des paramètres de quarantaine permet de renforcer la traçabilité des menaces en évitant la perte de preuves potentielles pour des **analyses forensics**. En désactivant la suppression, on maximise la **conservation des artefacts**, ce qui est crucial pour les investigations en **threat hunting** ou les rapports de conformité.

3.3.6. Protection en temps réel :

La protection en temps réel de **Microsoft Defender Antivirus** surveille continuellement les fichiers, processus et activités pour détecter et bloquer les menaces instantanément, en utilisant des analyses comportementales et cloud.

Mise en oeuvre:

- Configurez la protection en temps réel via Configuration de l'ordinateur/Stratégies/Modèles d'administration/Composants Windows/Antivirus Windows Defender/Protection en temps réel
- Activez la stratégie "Analyser tous les fichiers et pièces jointes téléchargés".
  Cette stratégie permet de configurer l'analyse de tous les fichiers et pièces jointes téléchargés.
- Sélectionnez la stratégie "Désactiver la protection en temps réel".
  Cette stratégie désactive les invites de protection en temps réel pour les détections de programmes malveillants connus.

Impact:

Cette mesure renforce la protection contre les menaces en temps réel en assurant une surveillance continue et des analyses comportementales des fichiers et processus. En activant l'analyse de tous les téléchargements et en désactivant les invites pour les malwares connus, on réduit la surface d'attaque et on assure une détection proactive, ce qui minimise le risque d'infection et améliore la réactivité face aux menaces émergentes.

3.3.7. Désactiver la suspension de l'analyse par les utilisateurs

Désactiver la suspension de l'analyse par les utilisateurs est une mesure de sécurité essentielle pour renforcer la protection des postes de travail.

Mise en oeuvre:

Vous pouvez configurer l'analyse de l'activité des fichiers et des programmes via le chemin suivant : Configuration de l'ordinateur/Stratégies/Modèles d'administration/Composants Windows/Antivirus Windows Defender/Analyse.
Il est recommandé de désactiver l'option "Autoriser les utilisateurs à suspendre l'analyse". Ce paramètre empêche les utilisateurs finaux d'interrompre une analyse en cours.

Impact:

Cette mesure améliore grandement les points suivants :

- ➢ **Sécurité renforcée :** Empêche les utilisateurs, qu'ils soient malveillants ou négligents, de désactiver la protection antivirus, ce qui pourrait laisser le système exposé aux menaces.
- ➢ **Conformité accrue :** Contribue à la conformité avec les réglementations de sécurité qui exigent une protection continue des endpoints.
- ➢ **Prévention des infections :** Assure que les analyses planifiées ou en temps réel s'exécutent jusqu'à leur terme, augmentant les chances de détection et de suppression des malwares avant qu'ils ne causent des dommages.
- ➢ **Cohérence de la politique de sécurité :** Maintient l'uniformité de la politique de sécurité sur l'ensemble du parc informatique en empêchant les dérogations individuelles.

3.4.🔴 Mesure sur les accès à distance

La mise en place d'un accès VPN est cruciale pour garantir la sécurité des connexions distantes, permettant aux collaborateurs d'accéder aux ressources internes de l'entreprise de manière sécurisée, où qu'ils se trouvent. Pour maximiser cette sécurité, plusieurs mesures restrictives et des configurations VPN spécifiques doivent être appliquées. L'architecture LAB ne permettait pas.

3.4.1. IP pré-approuvées

Mise en œuvre:

Seules les adresses IP pré-approuvées (bureaux distants, domiciles des employés vérifiés, plages d'adresses spécifiques de FAI fiables) sont autorisées à initier une connexion VPN.

Impact:

Réduire les tentatives d'accès non autorisées en limitant les points d'entrée potentiels.

3.4.2. Horaires d'accès

Mise en œuvre :

Limiter l'accès VPN aux heures de travail définies.

Impact :

Minimise le risque d'accès en dehors des heures ouvrables, potentiellement en l'absence de surveillance.

3.4.3. Connexions simultanées

Mise en œuvre :

Restreindre le nombre de sessions VPN simultanées par utilisateur.

Impact :

Empêche le partage de comptes et limite les dégâts en cas de compromission d'un compte.

3.4.4. Audit des connexions

Mise en œuvre :

Journalisation complète de tous les accès distants via VPN.

Impact :

Permet une traçabilité et une analyse forensic en cas d'incident de sécurité, facilitant la détection et la réponse aux menaces.

3.4.5. Protocoles modernes

Mise en œuvre :

Utiliser des protocoles VPN robustes comme IKEv2 ou OpenVPN avec TLS 1.3.

Impact :

Assure un chiffrement fort et une meilleure résilience contre les attaques de déchiffrement.

3.4.6. Certificats clients obligatoires

Mise en œuvre

Chaque client VPN doit posséder un certificat unique délivré par l'autorité de certification interne de l'entreprise.

Impact

Garantit que seuls les appareils autorisés et authentifiés peuvent établir une connexion VPN.

3.4.7. Authentification par certificat + MFA

Mise en œuvre

Après la validation du certificat client, l'utilisateur doit fournir un second facteur d'authentification.

Impact

Réduit considérablement le risque de compromission des comptes, même en cas de vol de mot de passe, en ajoutant une couche de sécurité supplémentaire.

3.5.⚫Mesure sur les accès

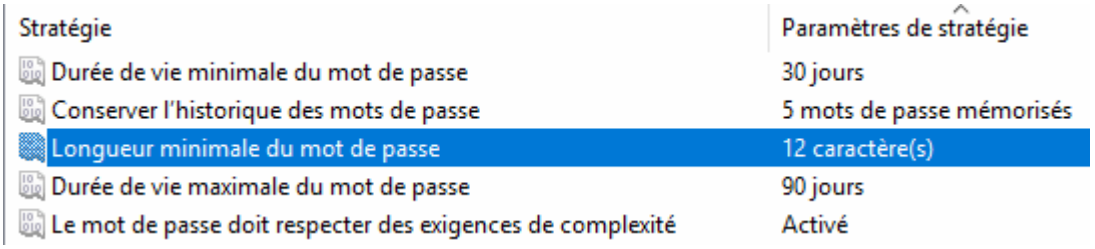
3.5.1. Complexification des mots de passes

L'objectif de cette mesure est de renforcer la sécurité des comptes utilisateurs en exigeant des mots de passe plus difficiles à deviner ou à casser. En augmentant la complexité des mots de passe, on réduit considérablement le risque d'accès non autorisé aux systèmes et aux données.

Mise en oeuvre

Sous Windows via GPO

1. Modifier la GPO "Sécurité".
2. Naviguer vers : Configuration de l'ordinateur/Stratégies/Paramètres Windows/Paramètres de sécurité/Stratégies de comptes/Stratégie de mot de passe
3. On active l'option de complexité suivantes :



Sous le serveur Ubuntu

1. **sudo apt update**
   sudo apt install libpam-pwquality
2. Configuration de la politique dans le fichier **/etc/pam.d/common-password** avec les paramètres suivants :
   - ➢ 5 tentatives de saisies
   - ➢ 12 caractères minimum (**recommandation ANSSI**)
   - ➢ 4 caractères différents du précédent
   - ➢ 4 catégorie de caractère de mots de passes

```
password        requisite                       pam_pwquality.so retry=5 minlen=12 difok=4 minclass=4
```

3. On édite également le fichier **/etc/login.defs** pour être conforme avec nos réglages Windows afin de paramétrer la durée de vie minimale et maximale de mot de passe.

```
PASS_MAX_DAYS   90
PASS_MIN_DAYS   30
```

Impact

Cette mesure permet d'améliorer sensiblement la sécurité sur les points suivants :

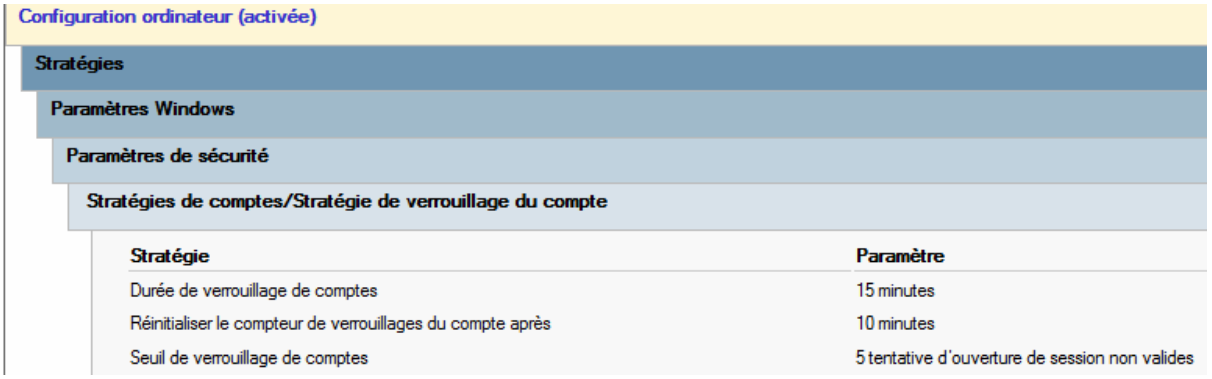
- ➢ Réduction des risques de piratage : Des mots de passe complexes sont moins susceptibles d'être compromis par des attaques par force brute ou par dictionnaire.
- ➢ Conformité : Aide à se conformer aux normes de sécurité et aux réglementations en vigueur (ex: RGPD, ISO 27001) qui exigent des mesures de sécurité robustes.
- ➢ Protection des données sensibles : Sécurise l'accès aux informations confidentielles et aux systèmes critiques, minimisant les risques de fuites de données.

3.5.2. Mise en place d'un verrouillage de compte

Cette mesure consiste à configurer des paramètres de verrouillage de compte sur les systèmes et applications afin d'empêcher les tentatives d'authentification forcées. Cela inclut la définition d'un nombre maximal de tentatives de connexion infructueuses avant qu'un compte ne soit temporairement ou définitivement bloqué.

Mise en oeuvre

1. Modifier la GPO "Sécurité".
2. Naviguer vers : Configuration de l'ordinateur/Stratégies/Paramètres Windows/Paramètres de sécurité/Stratégies de comptes/Stratégies de verrouillage du compte
3. On applique les réglages suivants :



Impact

Cette mesure permet d'améliorer la sécurité sur les points suivants :

- ➢ Réduction significative du risque d'attaques par force brute et de compromission de comptes.
- ➢ Amélioration de la sécurité globale des systèmes en limitant l'accès non autorisé.

3.5.3. Mise en place fail2ban

Fail2Ban est un outil open-source de sécurité pour Linux (et compatible WSL sur Windows) qui protège contre les attaques par force brute en analysant les logs système et en bannissant temporairement les adresses IP suspectes via le pare-feu.

Mise en oeuvre

On va utiliser Fail2ban pour bloquer automatiquement les adresses IP malveillantes, notamment celles tentant des attaques par force brute sur SSH.

Mettre à jour les paquets de votre système et installer Fail2ban :
sudo apt update
sudo apt install fail2ban
sudo systemctl status fail2ban
Fail2ban utilise des fichiers de configuration spécifiques :

- /etc/fail2ban/fail2ban.conf : Configuration générale du service.
- /etc/fail2ban/jail.conf : Contient les configurations par défaut des "prisons" (jails).

sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Éditez le fichier jail.local et accédez à la section [DEFAULT] pour configurer les paramètres globaux :

- ignoreip : Ajoutez les adresses IP à ne jamais bannir. Il est crucial d'inclure l'IP de votre machine de travail pour éviter de vous bloquer. Les adresses sont séparées par des espaces. 127.0.0.1 (localhost) est déjà inclus.
- bantime : Durée du bannissement. Utilisez des suffixes pour les unités (m=minutes, h=heures, d=jours). Dans notre cas on le fixe à **24h**
- findtime : Période pendant laquelle les tentatives échouées sont comptées. Si maxretry tentatives sont détectées en moins de findtime, l'IP est bannie.
  On laisse dans notre cas les valeurs par défaut :
  - ➢ findtime = **10m**
  - ➢ maxretry = **5**

Activation des "Prisons" (Jails)
Une "prison" est une configuration spécifique à un service (ex: SSH). Pour l'activer, vous devez modifier votre fichier jail.local et définir enabled = true pour la section correspondante.

La prison la plus importante à activer est celle pour SSH.

1. Trouvez la section [sshd] dans votre fichier jail.local.
2. Activez-la en ajoutant ou en décommentant la ligne enabled = true.

[sshd]
# Pour activer la prison pour le service SSH
enabled = true

Redémarrage de Fail2ban
Pour appliquer vos nouvelles configurations, redémarrez le service Fail2ban :
sudo systemctl restart fail2ban

Vérification du Fonctionnement
Fail2ban est maintenant actif et protège votre service SSH.
Voici comment vérifier son état
sudo fail2ban-client status

```
user@user:~$ sudo fail2ban-client status
[sudo] Mot de passe de user :
Status
|- Number of jail:      1
`- Jail list:   sshd
```

Cette commande listera les prisons actuellement actives, vous devriez y voir sshd.Vérifier le statut d'une prison spécifique :
sudo fail2ban-client status sshd
Cette commande affichera le nombre d'échecs détectés et la liste des IPs bannies.

```
user@user:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
```

Comment se dé-bannir (en cas d'erreur)
Si vous vous êtes banni accidentellement, vous pouvez vous débloquer depuis une autre connexion (ou via la console de votre hébergeur) avec la commande suivante, en remplaçant <IP_ADDRESS> par votre adresse IP :

sudo fail2ban-client set sshd unbanip <IP_ADDRESS>

Impact

La mise en place de **Fail2ban** réduit considérablement le risque d'attaques par force brute contre les services exposés (notamment **SSH**) en bloquant automatiquement les adresses IP suspectes. Cela renforce la résilience du système, minimise la charge sur les serveurs due aux tentatives répétées, et contribue à la sécurité globale en protégeant contre l'énumération d'utilisateurs et la compromission des identifiants. La traçabilité des tentatives d'attaque est également améliorée grâce à la **journalisation des bannissements**.

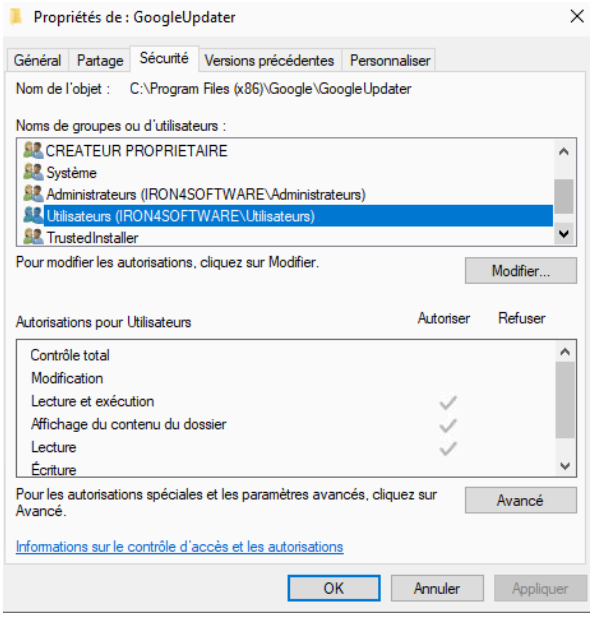
3.5.4. Restriction des droits NTFS

Restreindre les droits NTFS sur les répertoires applicatifs (notamment **GoogleUpdate**r) aux comptes Administrateurs ou SYSTEM uniquement.

Mise en oeuvre

Un administrateur système peut vérifier et corriger ces permissions de la manière suivante :
Faire un clic droit sur le dossier de l'application (ex: **GoogleUpdater**).
Aller dans Propriétés > onglet Sécurité.

Examiner la liste des "Noms de groupes ou d'utilisateurs". Idéalement, on ne devrait y trouver que **SYSTEM, Administrateurs,** et éventuellement **Utilisateurs** avec des droits limités à la lecture et l'exécution uniquement (pas d'écriture ni de modification).



Si des groupes comme **Tout le monde ou Utilisateurs** ont des droits de **Modification** ou de **Contrôle total**, il faut les supprimer ou éditer leurs permissions.

Impact

Cette action simple empêche efficacement toute une catégorie d'attaques visant à détourner des applications légitimes pour obtenir des privilèges élevés sur un système.

3.5.5. Vérifier les listes de Contrôle d'Accès (ACLs) des tâches planifiés

Cette mesure consiste à auditer les Listes de Contrôle d'Accès (ACLs) associées aux tâches planifiées sur les systèmes. Les tâches planifiées exécutent souvent des programmes ou des scripts avec des privilèges spécifiques. Si les ACLs de ces tâches sont trop permissives, des utilisateurs non autorisés pourraient les modifier, les désactiver ou les utiliser pour exécuter du code malveillant avec des privilèges élevés. L'objectif est de s'assurer que seuls les comptes et groupes nécessaires (comme **SYSTEM** ou **Administrateurs**) ont les droits de modification, tandis que les autres comptes ont des droits limités (lecture et exécution).

Mise en oeuvre

Méthode en Ligne de Commande va lister chaque tâche, le compte utilisé, et l'action qu'elle exécute :

```
Get-ScheduledTask | ForEach-Object {
    $taskName = $_.TaskName
    $taskPrincipal = $_.Principal.UserId
    $taskActions = ($_.Actions | ForEach-Object { $_.Execute + " " + $_.Arguments })
-join "; "
    [PSCustomObject]@{
        TaskName = $taskName
        RunAsUser = $taskPrincipal
        Actions = $taskActions
```

```
    }
} | Format-Table -AutoSize
```

```
TaskName                                                    RunAsUser Actions
--------                                                    --------- -------
GoogleUpdaterTaskSystem140.0.7273.0{0DB05084-FEB6-4898-A5AE-16B7CB3BA64F} Système   "C:\Program Files (x86)\Google\GoogleUpdater\140.0.7273.0\updater.exe" --wake --system
```

On récupère le chemin dans la colonne “Actions” pour GoogleUpdater

Puis la commande suivante va afficher la liste de contrôle d’accès qu’il faudra ou non édité icacls "C:\Program Files (x86)\Google\GoogleUpdater\140.0.7273.0\updater.exe"

```
C:\Program Files (x86)\Google\GoogleUpdater\140.0.7273.0\updater.exe AUTORITE NT\Utilisateurs authentifiés:(I)(F)
                                                                    AUTORITE NT\Système:(I)(F)
                                                                    BUILTIN\Administrateurs:(I)(F)
                                                                    BUILTIN\Utilisateurs:(I)(RX)
                                                                    AUTORITÉ DE PACKAGE D’APPLICATION\TOUS LES PACKAGES D’APPLICATION:(I)(RX)
                                                                    AUTORITÉ DE PACKAGE D’APPLICATION\TOUS LES PACKAGES D’APPLICATION RESTREINTS:(I)(RX)
```

Dans l’exemple suivant le groupe “Utilisateur authentifiés” a le contrôle total ce qui n’est pas une bonne pratique. Il faut donc soit supprimer les droits de ce groupe ou limiter à lecture et exécution.

Impact

La vérification et la correction des ACLs des tâches planifiées ont plusieurs impacts positifs sur la sécurité :

- **Réduction de la surface d'attaque :** En restreignant les droits de modification et d'exécution des tâches planifiées, on empêche les attaquants d'utiliser ces tâches comme vecteur d'escalade de privilèges.
- **Prévention de l'exécution de code malveillant :** Des ACLs restrictives garantissent que seuls les utilisateurs et processus autorisés peuvent manipuler les tâches planifiées, réduisant le risque qu'une tâche légitime soit détournée pour lancer des logiciels malveillants.
- **Maintien du principe du moindre privilège :** Cela renforce l'application du principe de moindre privilège en s'assurant que les tâches s'exécutent avec les privilèges appropriés et que leur configuration est protégée des accès non essentiels.

3.5.6. Restriction de l’accès SSH

Restreindre l'**accès SSH** permet de limiter les connexions au serveur à un ensemble d'utilisateurs ou d'adresses IP spécifiquement autorisés, réduisant ainsi la **surface d'attaque** et le risque d'intrusions non autorisées via ce protocole.

Mise en oeuvre

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
sudo nano /etc/ssh/sshd_config
# Ajouter “AllowUsers info” en fin de fichier pour n’autoriser que l’utilisateur mentionné
#Vérification de la syntaxe de la config
sudo sshd -t
sudo systemctl restart ssh
```

Impact

La restriction de l'accès SSH à des utilisateurs spécifiques (par exemple, "info" dans l'exemple donné) ou à des plages d'adresses IP autorisées réduit considérablement la surface d'attaque du serveur. Cela empêche les tentatives de connexion par force brute ou les attaques par dictionnaire de la part d'acteurs malveillants n'ayant pas les identifiants ou les autorisations nécessaires. En cas de compromission d'autres parties du réseau, cette mesure limite la capacité d'un attaquant à se déplacer latéralement et à prendre le contrôle du serveur via SSH. Elle renforce la sécurité en concentrant la gestion des accès sur un groupe restreint et connu, ce qui facilite la surveillance et la traçabilité des connexions légitimes.

3.5.7. Restriction de l'accès RDP

Restreindre l'accès **RDP** est une mesure de sécurité essentielle qui vise à limiter qui peut se connecter à un serveur Windows via ce protocole. Par défaut, le **RDP** peut être accessible à de nombreux utilisateurs ou groupes, ce qui augmente la surface d'attaque et le risque d'intrusions non autorisées, notamment via des attaques par force brute ou des identifiants compromis.

Mise en oeuvre

Étape 1 : Création du groupe de sécurité Active Directory

1. Ouvrez "Utilisateurs et ordinateurs Active Directory" sur un contrôleur de domaine.
2. Naviguez vers l'Unité d'Organisation (OU) appropriée pour les groupes de sécurité.
3. Cliquez droit, puis "Nouveau" > "Groupe".
4. Nommez le groupe de manière explicite (ex: RDP_Acces).
5. Définissez la "Portée du groupe" sur "Global" et le "Type de groupe" sur "Sécurité".
6. Cliquez sur "OK".

Étape 2 : Ajout des membres au groupe

1. Double-cliquez sur le groupe nouvellement créé.
2. Dans l'onglet "Membres", ajoutez les comptes utilisateurs qui nécessitent un accès RDP.

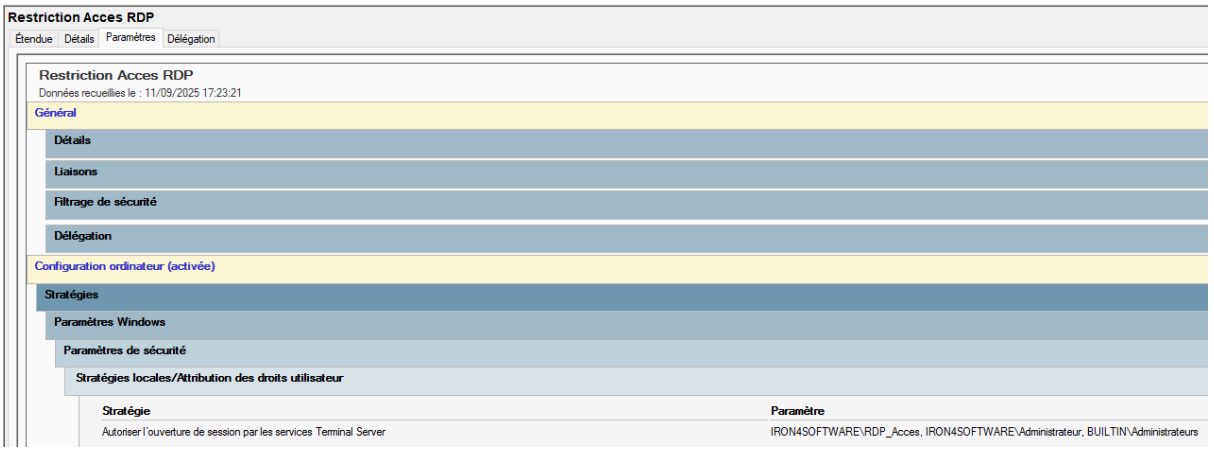
Étape 3 : Création et liaison de la Stratégie de Groupe (GPO)

1. Ouvrez la console "Gestion des stratégies de groupe".
2. Naviguez jusqu'à l'OU contenant les ordinateurs (serveurs) cibles.
3. Cliquez droit sur cette OU et sélectionnez "Créer un objet GPO dans ce domaine, et le lier ici...".
4. Nommez votre GPO (ex: Securite - Restriction Acces RDP).

Étape 4 : Configuration de la GPO

1. Cliquez droit sur la GPO créée et choisissez "Modifier".
2. Accédez au chemin suivant : Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur.

3. Dans le volet de droite, trouvez la stratégie "Autoriser l'ouverture de session par les services Bureau à distance".
4. Double-cliquez dessus, cochez "Définir ces paramètres de stratégie".
5. Cliquez sur "Ajouter un utilisateur ou un groupe..." et ajoutez le groupe créé à l'étape 1 (ex: RDP_Acces).
6. **IMPORTANT** : Ajoutez également le groupe "Administrateurs" (ou "Domain Admins") pour éviter de bloquer l'accès aux administrateurs du domaine.
7. Cliquez sur "OK".
   Après application de la GPO sur les serveurs cibles (cela peut prendre jusqu'à 90-120 minutes, ou être forcé avec gpupdate /force), seuls les membres des groupes spécifiés pourront se connecter en RDP.



Impact

Cette restriction a plusieurs impacts positifs majeurs sur la sécurité :

- ➢ Réduction de la surface d'attaque : En limitant l'accès RDP à un groupe restreint et explicitement autorisé, le nombre de cibles potentielles pour les attaquants est considérablement réduit. Cela rend les attaques par force brute ou les tentatives d'énumération d'utilisateurs beaucoup moins efficaces.
- ➢ Prévention des accès non autorisés : Seuls les utilisateurs dont les comptes sont membres du groupe RDP_Acces (ou Administrateurs) peuvent établir une connexion RDP. Cela empêche les utilisateurs non autorisés d'accéder aux serveurs, même s'ils parvenaient à obtenir des identifiants valides via d'autres moyens.
- ➢ Contrôle fin des privilèges : Cette mesure s'aligne avec le principe du moindre privilège, garantissant que seuls ceux qui ont une nécessité opérationnelle se voient accorder cet accès critique. Cela limite les dommages potentiels en cas de compromission d'un compte utilisateur.

3.6.🟣Mesure sur les protection de donnée

3.6.1. Backup données

Veritas Backup Exec compatible LINUX, Windows est une solution de sauvegarde complète et fiable, conçue pour protéger les données critiques contre la perte, la corruption ou la destruction. En intégrant des fonctionnalités de sauvegarde sur bande, disque dur externe et sur le cloud, elle assure une résilience maximale et une récupération rapide en cas d'incident majeur.

Mis en oeuvre

L'implémentation n'a pas été réalisée et doit être effectuée rapidement.

Logiciel de sauvegarde utilisé : **Veritas Backup Exec** installé sur **Server 2019 AD 192.168.1.1.** Il sauvegardera également les autres machines critiques du réseau (**192.168.100.2** etc...).

- ➢ Cibles de sauvegarde
  - Cloud professionnel (Microsoft Azure).
  - Bandes de sauvegarde locales.
  - Disque dur externe

- ➢ Stratégie de sauvegarde

Sauvegarde quotidienne

- Exécution tous les jours à **23h00**.
- Mode : **cyclique** (rotation des supports, écrasement planifié).

Sauvegarde mensuelle

- Réalisée en **fin de mois**.
- Mode : **cyclique** (conservation en fonction de la politique de rétention).

Sauvegarde annuelle

- Réalisée à la fin **de chaque année**.
- Mode : **cyclique**, avec conservation long terme (archivage).

Contrôles et vérifications

- **Vérification Quotidienne :** Vérification à la fin de chaque tâche (vérification des sommes de contrôle). Contrôle humain en complément.

- **Test de restauration complète trimestriel** : Effectuer des tests de restauration complets de l'application web et de l'Active Directory dans un environnement isolé.
- **Test de restauration partiel mensuel** : Tester la restauration de fichiers uniques et de bases de données pour valider l'intégrité à un niveau approfondi.

Impact

La stratégie de sauvegarde définie avec **Veritas Backup Exe** permettra d'assurer la continuité d'activité de l'entreprise en cas d'incident majeur. Grâce à la combinaison de sauvegardes **quotidiennes, mensuelles et annuelles**, stockées à la fois sur **Azure**, **disque dur externe** et sur **bandes**, les données critiques sont protégées contre la perte, la corruption ou la destruction.
Les contrôles hebdomadaires et les tests trimestriels garantissent la fiabilité des restaurations, réduisant considérablement le risque d'indisponibilité prolongée.

Ce dispositif offre un équilibre entre **sécurité**, **performance** et **conformité réglementaire**, tout en maintenant un **RPO (Recovery Point Objective) de 24 heures** et un **RTO(Recovery Time Objective) de 24 heures**, adaptés aux besoins opérationnels de l'entreprise.

Pour rappel :
RPO (Recovery Point Objective) :
→ Point de restauration maximal accepté en arrière.
→ Autrement dit : **combien de données peut-on perdre** en cas d'incident.

RTO (Recovery Time Objective) :
→ Temps maximal accepté pour restaurer le service.
→ Autrement dit : **combien de temps le service peut rester indisponible**.

4. Conclusion du rapport

Ce rapport détaille l'ensemble des mesures de sécurisation mises en œuvre pour l'infrastructure de IRON4SOFTWARE, transformant une architecture initialement vulnérable en un système robuste et résilient face aux menaces cybernétiques actuelles. Les actions entreprises couvrent des domaines cruciaux, allant de la sensibilisation du personnel à la sécurisation applicative, en passant par le durcissement du réseau et des accès, ainsi que la mise en place de protections des données.

Les vulnérabilités critiques identifiées dans l'application web (injections SQL, LFI, mots de passe en clair, etc.) ont été corrigées par des pratiques de développement sécurisées (requêtes préparées, hachage bcrypt, sanitisation des entrées). Au niveau réseau, la segmentation via pfSense et l'implémentation de Snort assurent une défense en profondeur, isolant les systèmes critiques et bloquant les intrusions en temps réel. La gestion des accès, avec la complexification des mots de passe, le verrouillage des comptes, Fail2Ban et les restrictions RDP/SSH, renforce la posture de sécurité en limitant drastiquement les points d'entrée pour les attaquants. Enfin, la protection antivirus via GPO et la stratégie de sauvegarde multi-support avec Veritas Backup Exec garantissent la résilience et la continuité d'activité en cas d'incident.

L'objectif primordial de garantir la confidentialité, l’intégrité, la disponibilité et la traçabilité de l'infrastructure de IRON4SOFTWARE, est atteint. Cependant, la sécurité n'est pas un état statique, mais un processus continu. Une veille technologique constante, des audits réguliers et l'adaptation des mesures aux nouvelles menaces seront essentielles pour maintenir ce niveau de protection à l'avenir.