Département du Système d'Information

CONTEXTE	●	**Pfsense**
SUJET	●	**Mise en service**
référence	●	*document d'exploitation.docx*
version	●	1
statut	●	Terminé
créé le	●	*12/11/2020 11:03:00*
par	●	Hugo Sanchez
mis à jour le	●	*16/06/2024 16:10:00*
par	●	Hugo SANCHEZ
validé le	●	*16/06/2024 16:10:00*
par	●	Hugo SANCHEZ
diffusé le	●	*10/06/2024 17:00:00*
à	●	Julien LALLEMAND
Péremption, archivage et restriction de diffusion	●	

Nature de la restriction : confidentiel, diffusion restreinte, diffusion interne, restriction annulée

Table des mises à jour du document

version	date	objet de la mise à jour
01	06/06/2024	Version initiale
02	11/06/2024	Version intermédiaire
03	16/06/2024	Version finale

Table des matières

1 Document d'exploitation (pfsense)

1.1 Supervision

1.1.1 Supervision système

Les points de supervision système pour le pfSense Firewall incluent :

- **Processus** : Vérification que les services critiques (pfSense, DHCP, DNS, VPN) sont en cours d'exécution.
- **Espace disque** : Surveillance de l'espace disque disponible pour éviter les saturations.
- **Utilisation CPU et RAM** : Surveillance des ressources système pour détecter toute surcharge.
- **État des interfaces réseau** : Surveillance de l'état des interfaces WAN, LAN, et DMZ.

1.1.2 Supervision applicative

- **État de la page d'accueil** : Vérification que l'interface web de pfSense est accessible.
- **Journalisation** : Vérification régulière des journaux d'événements pour détecter toute anomalie ou activité suspecte.

1.2 Sauvegardes

1.2.1 Stratégie appliquée

- Minimum une **Sauvegarde totale** : Une sauvegarde complète de la configuration pfSense est effectuée une fois par semaine.

1.2.2 Sauvegardes journalières

Pour réaliser la sauvegarde journalière :

1. Accéder à l'interface web de pfSense.
2. Aller dans Diagnostics > Backup & Restore.
3. Sélectionner Backup et configurer la sauvegarde différentielle.
4. Enregistrer la sauvegarde sur un emplacement sécurisé (ex : serveur FTP, stockage cloud).

1.2.3 Sauvegardes hebdomadaires

Pour réaliser la sauvegarde hebdomadaire :

1. Accéder à l'interface web de pfSense.
2. Aller dans Diagnostics > Backup & Restore.
3. Sélectionner Backup et configurer une sauvegarde complète.
4. Enregistrer la sauvegarde sur un emplacement sécurisé (ex : serveur FTP, stockage cloud).

1.3 Restauration

1.3.1 Restauration du système

1. Démarrer le serveur/VM pfSense à partir du support d'installation.
2. Suivre l'assistant de récupération pour restaurer la configuration depuis une sauvegarde complète.
3. Vérifier que toutes les interfaces et services sont opérationnels.

1.3.2 Restauration des applicatifs

1. Accéder à l'interface web de pfSense.
2. Aller dans Diagnostics > Backup & Restore.
3. Sélectionner Restore et choisir la sauvegarde applicative à restaurer.
4. Appliquer la restauration et redémarrer les services nécessaires.

1.3.3 Restauration des données

1. Accéder à l'interface web de pfSense.
2. Aller dans Diagnostics > Backup & Restore.
3. Sélectionner Restore et choisir la sauvegarde de données à restaurer.
4. Appliquer la restauration et vérifier l'intégrité des données.

1.4 Procédure d’arrêt

1.4.1 Ordonnancement et séquencement

1. Informer tous les utilisateurs concernés de l'arrêt planifié.
2. Arrêter d'abord les services non critiques.
3. Arrêter les services critiques (VPN, DHCP, DNS).
4. Enfin, arrêter l'interface WAN pour couper l'accès externe.

1.4.2 Arrêt global et validation

1. Accéder à l'interface web de pfSense.
2. Aller dans Diagnostics > Reboot/Shutdown.
3. Sélectionner Shutdown et confirmer l'arrêt.
4. Valider l'arrêt complet de tous les services et interfaces.

1.4.3 Arrêt spécifique d’une application ou d'un service spécifique

1. Accéder à l'interface web de pfSense.
2. Aller dans Status > Services.
3. Sélectionner le service à arrêter (ex : DHCP, DNS, VPN).
4. Cliquer sur Stop et confirmer l'arrêt du service spécifique.

1.5 Procédure de démarrage

1.5.1 Ordonnancement et dépendance

1. **Démarrer les interfaces réseau** : Allumer le routeur et vérifier que les interfaces WAN, LAN et DMZ sont opérationnelles.
2. **Démarrer les services critiques** : Démarrer les services VPN, DHCP et DNS pour assurer la connectivité et la résolution des noms de domaine.
3. **Démarrer les services non critiques** : Allumer les autres services ou applications en fonction des besoins.

1.5.2 Relance du serveur et des applications

1. Allumer le serveur physique ou la VM hébergeant pfSense.
2. Accéder à l'interface web de pfSense pour vérifier l'état des interfaces et services.
3. Redémarrer manuellement les services si nécessaire via l'interface de gestion.

1.5.3 Relance d'une application ou d'un service spécifique

1. Accéder à l'interface web de pfSense.
2. Aller dans Status > Services.
3. Sélectionner le service spécifique à démarrer (ex : DHCP, DNS, VPN).
4. Cliquer sur Start et confirmer le démarrage du service.

1.6 Tests de bon fonctionnement

1.6.1 Contrôle quotidien des applications

1. **Vérification des services** : Accéder à l'interface web de pfSense et vérifier que tous les services critiques (DHCP, DNS, VPN) sont opérationnels.
2. **Examen des journaux** : Analyser les logs pour détecter toute anomalie ou activité inhabituelle.
3. **Tests de connectivité** : Effectuer des tests de connexion pour s'assurer que les utilisateurs peuvent accéder aux ressources internes et externes.

1.6.2 Plan de reboot régulier des serveurs ou composants

1. **Planifier les redémarrages** : Établir un calendrier de redémarrage régulier, par exemple une fois par mois, pendant une période de faible activité.
2. **Effectuer les redémarrages planifiés** : Redémarrer le serveur physique ou la VM hébergeant pfSense en suivant le calendrier établi.
3. **Vérification post-redémarrage** : Contrôler que tous les services redémarrent correctement et que l'infrastructure fonctionne comme prévu.

1.7 Pilotage des environnements

1.7.1 Logs

1. **Emplacement des logs** : Les journaux de pfSense sont stockés dans /var/log/ sur le système.
2. **Informations à analyser** : Examiner les journaux des services (DHCP, DNS, VPN) pour les erreurs et les activités suspectes.

1.7.2 Seuils et purges

1. **Niveaux de seuils** : Configurer des alertes pour les seuils critiques, comme l'utilisation de la CPU, la RAM et l'espace disque.
2. **Purges** : Mettre en place des scripts pour purger régulièrement les anciens logs et libérer de l'espace disque.

1.7.3 Traitements et batchs

1. **Scripts automatisés** : Utiliser des scripts pour automatiser les tâches courantes comme les sauvegardes, les mises à jour et la maintenance.
2. **Planification** : Configurer des tâches planifiées (cron jobs) pour exécuter ces scripts à des intervalles réguliers.

1.7.4 Gestion des droits applicatifs

1. **Profils utilisateurs** : Créer des profils d'utilisateurs dans l'interface web de pfSense.
2. **Droits associés** : Assigner des permissions spécifiques aux utilisateurs en fonction de leur rôle, par exemple, administrateur, utilisateur réseau, etc.

1.8 Maintenance et support

1.8.1 Plage de maintenance

Les maintenances sont effectuées chaque premier samedi du mois, de 2h à 6h du matin, pour minimiser l'impact sur les utilisateurs.

1.8.2 Mises à jour

- **Emplacement** : Les mises à jour sont disponibles sur le site officiel de pfSense.
- **Politique** : Les mises à jour critiques sont appliquées immédiatement, les mises à jour de sécurité mensuellement, et les mises à jour fonctionnelles trimestriellement

1.8.3 Contrats

- **Support Technique** : Contrat avec Netgate pour le support pfSense.
- **Détails** : Support 24/7 par email et téléphone, avec une réponse garantie en 4 heures pour les incidents critiques.

1.8.4 Licences

- **Type** : pfSense est une solution open-source, mais le support est sous licence Netgate.
- **Emplacement** : Les licences et les clés de support sont stockées sur un serveur interne sécurisé.
- **Implémentation** : Installer les licences via l'interface web de pfSense, sous System > User Manager > Authentication Servers.

1.9 Niveaux de support

1.9.1 Niveau 1

1.9.1.1 PLAGE HORAIRE

Support de niveau 1 disponible de 8h à 18h du lundi au vendredi.

1.9.1.2 ACTEURS

Le support de niveau 1 est assuré par l'équipe IT interne. Contact par téléphone ou par email à it-support@example.com.

1.9.1.3 ACTIONS REALISEES

- Résolution des problèmes de connectivité de base.
- Réinitialisation des mots de passe.
- Escalade des incidents complexes vers le niveau 2.

1.9.2 Niveau 2

1.9.2.1 PLAGE HORAIRE

Support de niveau 2 disponible de 8h à 22h du lundi au vendredi.

1.9.2.2 ACTEURS

Le support de niveau 2 est assuré par les administrateurs réseau seniors. Contact via un ticket d'incident sur le portail interne.

1.9.2.3 ACTIONS REALISEES

- Gestion des configurations avancées de pfSense.
- Résolution des problèmes liés aux services DHCP et DNS.
- Escalade vers le niveau 3 pour les problèmes critiques et complexes.

1.9.3 Niveau 3

1.9.3.1 PLAGE HORAIRE

Support de niveau 3 disponible 24/7 pour les incidents critiques.

1.9.3.2 ACTEURS

Le support de niveau 3 est assuré par les experts de Netgate. Contact via le portail support de Netgate.

1.9.3.3 ACTIONS REALISEES

- Diagnostic et résolution des incidents critiques.
- Support pour les mises à jour et les migrations complexes.
- Retour d'informations et solutions vers les niveaux 1 et 2 pour la documentation des procédures et l'amélioration des processus.

1.10 Niveaux de service

1.10.1 Description des niveaux de service

1.10.2 Niveau de service retenu

Cocher la case correspondante

Standard	
Critique	
Très critique	

1.11 Sécurité

1.11.1 Conformité RGPD

- **Politique de confidentialité** : Décrire les mesures prises pour garantir la confidentialité des données des utilisateurs.
- **Consentement des utilisateurs** : Expliquer comment le consentement des utilisateurs est obtenu et enregistré.
- **Accès aux données** : Préciser les contrôles d'accès mis en place pour garantir que seules les personnes autorisées peuvent accéder aux données personnelles.
- **Droits des utilisateurs** : Détailler le processus permettant aux utilisateurs d'exercer leurs droits (accès, rectification, suppression des données).
- **Sécurité des données** : Expliquer les mesures de sécurité techniques et organisationnelles mises en œuvre pour protéger les données personnelles.

1.11.2 Conformité NIS

- **Évaluation des risques** : Décrire l'évaluation des risques effectuée pour garantir la conformité avec la directive NIS.

- **Plan de réponse aux incidents** : Expliquer le plan de réponse aux incidents, incluant la détection, la gestion et la notification des incidents de sécurité.
- **Sécurité des réseaux et des systèmes** : Détails des mesures de sécurité mises en place pour protéger les réseaux et systèmes utilisés par le service.
- **Rapports de conformité** : Présenter les rapports de conformité et les audits réalisés pour garantir le respect de la directive NIS.

1.11.3 Tests d'intrusion

- **Type de tests réalisés** : Décrire les types de tests d'intrusion effectués (tests internes, externes, tests de pénétration).
- **Résultats des tests** : Présenter les résultats des tests d'intrusion, y compris les vulnérabilités identifiées et les mesures correctives prises.
- **Fréquence des tests** : Indiquer la fréquence à laquelle les tests d'intrusion sont réalisés pour garantir une sécurité continue.

1.11.4 Homologation ISO27001

- **Politique de sécurité de l'information** : Décrire la politique de sécurité de l'information mise en place pour l'homologation ISO 27001.
- **Procédures et contrôles** : Présenter les procédures et contrôles spécifiques implémentés pour répondre aux exigences de l'ISO 27001.
- **Audit et certification** : Expliquer le processus d'audit et de certification, y compris les audits internes et externes effectués pour maintenir l'homologation.
- **Amélioration continue** : Détailler les mesures prises pour l'amélioration continue du système de management de la sécurité de l'information.

1.12 Performances

1.12.1 Connexions concurrentes

- **Nombre de connexions supportées** : Préciser le nombre maximum de connexions concurrentes que le service peut supporter.
- **Tests de performance** : Décrire les tests de performance effectués pour déterminer la capacité de connexions concurrentes.

1.12.2 Temps de réponse attendus

- **Temps de réponse cible** : Préciser les temps de réponse attendus pour les principales fonctionnalités du service.
- **Mesures de performance** : Expliquer comment les temps de réponse sont mesurés et surveillés.

1.12.3 Test de charge

- **Scénarios de test** : Décrire les scénarios de test de charge utilisés pour évaluer la performance du service (nombre de connexions, volume de données, etc.).
- **Résultats des tests** : Présenter les résultats obtenus lors des tests de charge, y compris les éventuelles actions correctives entreprises pour améliorer la performance.

1.13 Support de formation

- **Supports de formation disponibles** : Lister les supports de formation disponibles pour différents profils d'utilisateurs (administrateurs, utilisateurs finaux, etc.).
- **Accès aux supports** : Expliquer comment les utilisateurs peuvent accéder aux supports de formation.
- **Mises à jour des supports** : Décrire le processus de mise à jour et de maintenance des supports de formation pour garantir leur pertinence et leur actualité.