A dark blue vertical bar on the left side of the page. A blue arrow points to the right from the bar, containing the date.

07/04/2024

Mise en place d'une solution PfSense

Lycée Aristide Berges

Several thin, curved, light blue lines that sweep upwards from the bottom left corner of the page.

Mathis Heulot

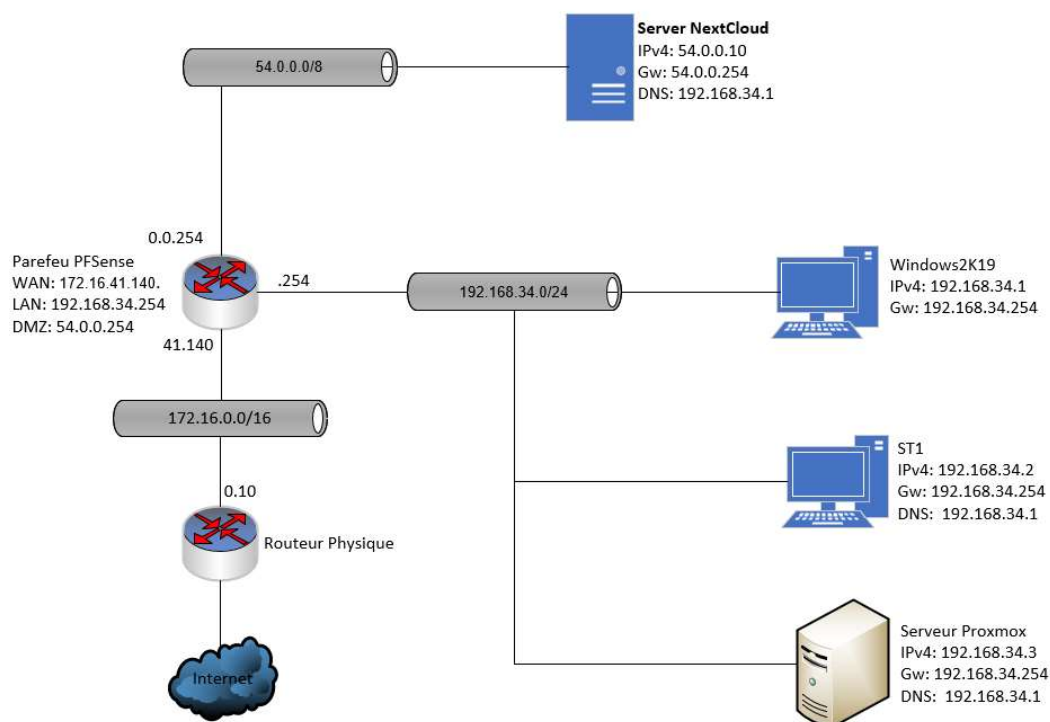
Table des matières

1) Introduction.....	2
2) Schéma Réseau.....	2
3) Principe d'un Pfsense	3
4) Mise en Œuvre de la solution.....	3
5) Conclusion	4

1) Introduction

Dans le cadre d'une évolution de l'infrastructure réseau de la mairie, une activité cruciale a été initiée pour renforcer la sécurité et la performance du réseau. Cette mission consistait à remplacer l'ancien pare-feu IPCop par une solution PfSense plus moderne et à mettre à jour le contrôleur de domaine existant. L'objectif était d'implémenter un environnement réseau plus intuitif et sécurisé, capable de répondre aux besoins actuels et futurs de l'organisation.

2) Schéma Réseau



Le schéma ci-dessus illustre la structure actuelle du réseau, où l'on distingue 3 parties différentes, Un en 54.0.0.0/8 avec un serveurs web NextCloud, et ensuite le réseau 192.168.34.0/24 avec une machine client et 2 serveurs, le 2k19 et un proxmox.

Et pour finir la Parefeu qui sépare le réseau et protège l'infrastructure.

3) Principe d'un Pfsense

La solution déployée est une combinaison d'un contrôleur de domaine Windows Server 2019 et d'une solution de routage-filtrage PfSense. PfSense, étant un pare-feu open-source et un routeur basé sur FreeBSD, a été choisi pour sa facilité de gestion et de mise en place grâce à son interface graphique pratique lisible.

Il s'agit d'un système flexible et configurable qui offre des fonctions avancées telles que le VPN, le contrôle de trafic, et la possibilité de définir des règles de filtrage précises pour le LAN, le WAN, et la DMZ.

4) Mise en Œuvre de la solution

La mise en place de PfSense a comporté la configuration de trois interfaces réseau avec des adresses IPv4 fixes, définissant clairement les segments LAN, WAN et DMZ. Des règles de filtrage ont été établies pour garantir une connectivité sélective et sécurisée. Le contrôleur de domaine Windows Server 2019 a été configuré pour être gérable via le protocole RDP, avec des règles spécifiques permettant la gestion à distance sécurisée.

Règles (Faire glisser pour changer l'ordre)											
<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
Autorisation											
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP/UDP	172.16.42.14	*	192.168.34.1	3389 (MS RDP)	*	aucun	Règle RDP	
Accès SSH depuis salle 42											
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	172.16.42.14	*	192.168.34.254	22 (SSH)	*	aucun	Règle 4: Gérable en ssh depuis poste salle 42	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP/UDP	172.16.42.14	*	54.0.0.10	22 (SSH)	*	aucun	Règle 4: Gérable en ssh depuis poste salle 42	
Gestion Web depuis salle 42 par poste 14 sur Nextcloud et Pfsense											
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP/UDP	172.16.42.14	*	192.168.34.254	4000	*	aucun	Règle HTTP	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP/UDP	172.16.42.14	*	54.0.0.10	80 - 443	*	aucun	Règle HTTP	
Règle pour ping la carte WAN, LAN, DMZ depuis salle 42											
<input type="checkbox"/>	✓	0/0 B	IPv4 ICMP any	172.16.42.14	*	192.168.34.1	*	*	aucun	Règle 1	
<input type="checkbox"/>	✓	0/0 B	IPv4 ICMP any	172.16.42.14	*	192.168.34.2	*	*	aucun	Règle 1	
<input type="checkbox"/>	✓	0/0 B	IPv4 ICMP any	172.16.42.14	*	LAN address	*	*	aucun	Règle 1	
<input type="checkbox"/>	✓	0/0 B	IPv4 ICMP any	172.16.42.14	*	WAN address	*	*	aucun	Règle 1	
Fermé											
<input type="checkbox"/>	✗	0/100 KiB	IPv4+6	*	*	*	*	*	aucun	Bloque Tout	

5) Conclusion

Le déploiement de la solution PfSense, conjointement avec la mise à jour du contrôleur de domaine vers Windows Server 2019, a constitué une étape majeure dans l'amélioration de l'infrastructure réseau de la mairie. Cette modernisation offre désormais une gestion de réseau plus intuitive et sécurisée, tout en posant les bases pour une évolutivité future. Avec la documentation complète, comprenant les configurations de base et les exemples de règles de filtrage, l'organisation est bien équipée pour maintenir et élargir sa plateforme réseau de manière efficace.