Mise en place d'une DMZ

Contexte

L'entreprise Nexa Services vient de mettre en place un pare-feu pfSense entre son réseau interne et Internet.

L'ensemble des communications est actuellement autorisé, ce qui représente un risque de sécurité.

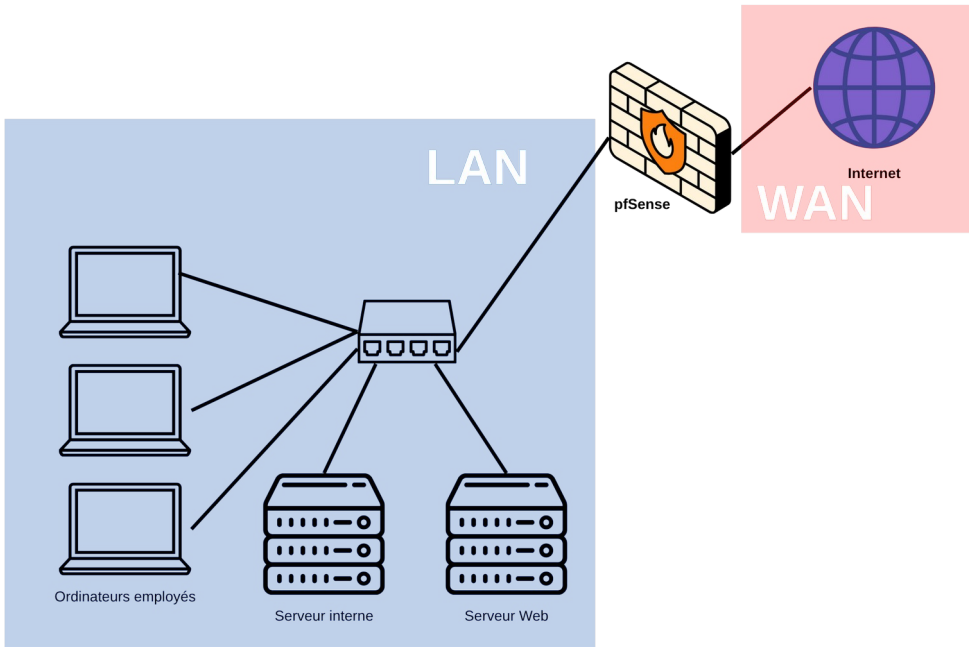
Votre mission consiste à mettre en œuvre une politique de filtrage conforme aux besoins de l'entreprise.

L'audit de sécurité réalisé par le RSSI met cependant en évidence un problème majeur : le serveur Web est hébergé directement sur le réseau interne de l'entreprise.

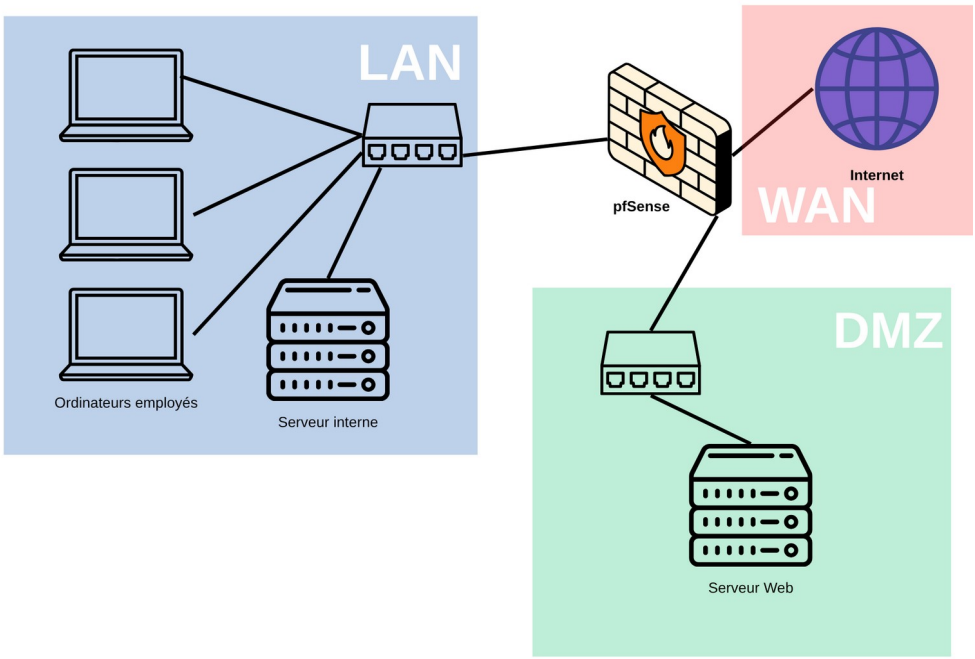
En cas de compromission du serveur, un attaquant pourrait accéder au réseau des utilisateurs et aux serveurs internes.

Le responsable de la sécurité demande donc la mise en place d'une DMZ afin d'isoler les services exposés.

Architecture actuelle



Architecture future



Firewall	Client	Serveur interne	Serveur Web
pfSense	Windows 11	Ubuntu 26.04	Ubuntu 26.04
WAN : 172.28.X.X LAN : 192.168.Y.254/24 DMZ : 10.10.Y.254/24	192.168.Y.10/24 (DHCP) GW : 192.168.Y.254	192.168.Y.200/24 GW : 192.168.Y.254	10.10.Y.10/24 GW : 10.10.Y.254
admin / admin123	client / Mdp!1234	srv-user / mdp123	srv-user / mdp123

Quel est l'objectif d'une DMZ dans cette situation ?

Partie 1 - Mise en place du NAT

Ouvrez Firewall > NAT > Outbound.

Quel mode est utilisé ?

Afin de permettre aux postes du réseau LAN d'accéder à Internet, il vous est demandé de mettre en place une règle de traduction d'adresses (Outbound NAT).

Testez votre configuration en ouvrant un navigateur web sur un client.

Vérifiez dans Diagnostics > States et recherchez la connexion correspondant au poste Windows.

Quelle est l'adresse IP source du poste avant la traduction ?

Quelle est l'adresse IP utilisée sur l'interface WAN après la traduction ?

Pourquoi plusieurs machines peuvent-elles partager cette même adresse WAN ?

Toutes les machines utilisent la même adresse WAN. Comment le pare-feu fait-il pour distinguer leurs connexions ?

Partie 2 - Mise en place du NAT pour le serveur web

L'entreprise souhaite rendre son site Web accessible depuis Internet.

Pour gagner du temps, un administrateur propose de publier directement le serveur Web situé sur le réseau interne.

Votre responsable vous demande de mettre en œuvre cette solution afin d'en analyser les avantages et les limites.

Le serveur Web est actuellement situé sur le réseau LAN. Créez une règle de redirection NAT permettant de publier le serveur Web sur le port externe 8080.

Sur le poste Windows connecté au réseau BTS, modifier le fichier :
`C:\Windows\System32\drivers\etc\hosts`

Ajouter la ligne suivante : `172.28.X.Y www.nexa.fr`
où X.Y sont la fin de l'adresse Wan du pfSense.

Vérifiez le bon fonctionnement : `http://www.nexa.fr:8080`

Le serveur Web est-il accessible depuis Internet ?

Est-il situé sur le LAN ?

Les postes utilisateurs sont-ils sur le même réseau ?

Quelles seraient les conséquences si ce serveur était compromis ?

Partie 3 - Création de la DMZ

Vous allez créer un nouveau réseau nommé : DMZ.

Configurez l'interface avec les informations que vous trouverez au dessus.

Le serveur Web doit désormais être connecté au réseau DMZ. Modifier son interface réseau, son adresse IP et sa passerelle.

Vérifiez que le serveur répond au ping depuis pfSense et que le serveur répond en HTTP depuis le LAN.

Partie 4 - Création des règles

Nous allons restreindre les communications en fonction de leur destination et de leur source.

On garde la politique de sécurité : on interdit tout et on autorise certains services.

Vous allez établir la liste des services à autoriser en fonction de la source et de la destination.

Source	Destination	HTTP	HTTPS	SSH	DNS	ICMP
LAN	WAN					
LAN	DMZ					
DMZ	LAN					
DMZ	WAN					
WAN	LAN					
WAN	DMZ					

Pour chaque règle, identifiez l'interface pfSense sur laquelle elle doit être créée.

Vérifiez que les règles mises en place fonctionnent.

Communication	Test réalisé
LAN → WAN *HTTP*	
LAN → WAN *HTTPS*	
LAN → DMZ *HTTP*	

LAN → DMZ *HTTPS*	
LAN → DMZ *SSH*	
DMZ → WAN *HTTP*	
DMZ → WAN *HTTPS*	
DMZ → WAN *DNS*	
DMZ → LAN	
WAN → LAN	
WAN → DMZ	

Partie 5 - Analyse des logs

Essayez de vous connecter en SSH au serveur à partir d'un poste client du LAN.

Puis ouvrez Status > Logs > Firewall, recherchez la ligne correspondante à l'action précédente.

Quelle règle bloque cette communication ?

Quelle est l'adresse IP source ?

Quelle est l'adresse IP destination ?

Quel protocole est utilisé ?

Cette communication est-elle bloquée par une règle explicite ou par la politique par défaut ?

Partie 6 - Analyse de l'architecture

Nous avons changé l'architecture réseau de l'entreprise, quels sont les avantages et les inconvénients de chacune des architectures ?

Architecture	Avantages	Inconvénients
Serveur Web sur le LAN		
Serveur Web en DMZ		

Partie 7 - Publication d'un serveur Web situé en DMZ

Vous avez créé une DMZ afin d'isoler les services accessibles depuis Internet.

Le serveur Web de l'entreprise a été déplacé dans cette nouvelle zone afin de limiter les risques en cas de compromission.

Cependant, les utilisateurs extérieurs ne peuvent plus accéder au site Internet.

Le responsable informatique vous demande de rendre ce serveur accessible depuis Internet tout en conservant l'architecture sécurisée mise en place.

Depuis le poste Windows situé sur le réseau BTS, ouvrez : http://www.nexa.local:8080

Le site est-il accessible ?

Pourquoi ?

Le serveur Web a changé d'adresse IP.

Modifier la règle NAT afin qu'elle pointe vers la nouvelle adresse située dans la DMZ.

Vérifiez que les changements fonctionnent.

Pourquoi le déplacement du serveur dans la DMZ n'a-t-il pas nécessité de modifier les postes clients du LAN ?