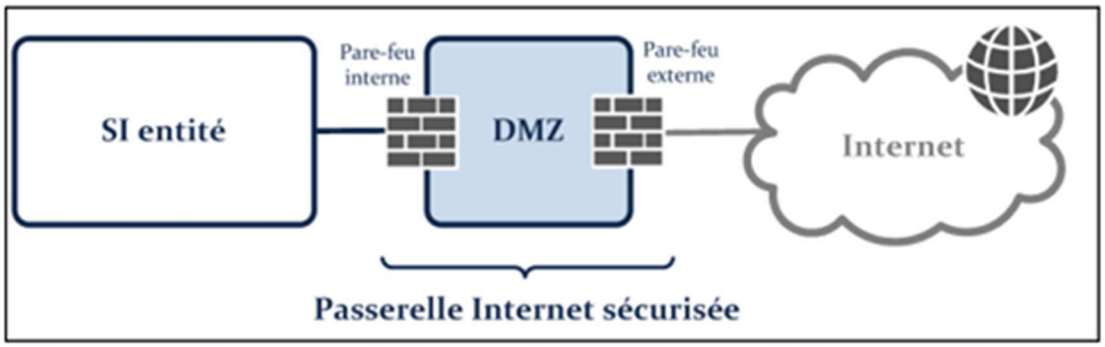
LA ZONE DEMILITARISEE (DMZ)

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise.

On parle alors de « zone démilitarisée » (notée DMZ pour DeMilitarized Zone) afin de désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.

La DMZ est considérée comme une zone neutre et perdable. En effet, sa sensibilité n'est pas nulle (des données du SI peuvent y transiter).

Mais une attaque de la DMZ ne doit pas remettre en cause de manière irréversible et durable le bon fonctionnement du SI.



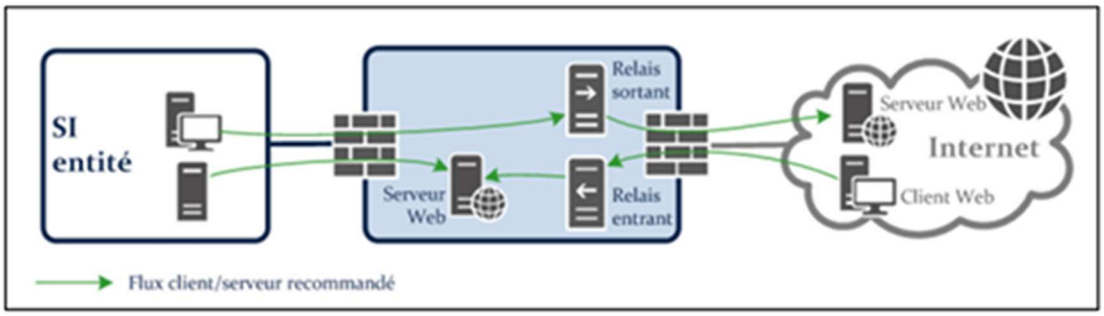
Comment fonctionne une DMZ ?

Les entreprises disposant d'un site Web public que les clients utilisent doivent rendre leur serveur Web accessible à Internet. Pour protéger le réseau local de l'entreprise, le serveur Web est installé sur un ordinateur distinct des ressources internes.

Un réseau DMZ sert de tampon entre Internet et le réseau privé d'une entreprise. La DMZ est isolée par une passerelle de sécurité, comme un pare-feu qui filtre le trafic entre la DMZ et un réseau LAN. Le serveur DMZ par défaut est protégé par une autre passerelle de sécurité qui filtre le trafic provenant de réseaux externes.

Elle est idéalement située entre deux pares-feux, et la configuration du pare-feu de la DMZ garantit que les paquets réseau entrants sont contrôlés par un pare-feu, ou d'autres outils de sécurité, avant qu'ils ne soient transmis aux serveurs hébergés dans la DMZ.

Si un assaillant parvient à infiltrer le pare-feu externe et à compromettre un système dans la DMZ, il doit également franchir un pare-feu interne avant d'accéder aux données sensibles de l'entreprise.


SI
entité
Relais
sortant
Serveur
Web
Relais
entrant
Serveur Web
Internet
Client Web
Flux client/serveur recommandé