Règles pare-feu

Voici une présentation des protocoles autorisés sur notre réseau LAN ainsi qu’une brève présentation de leur protocoles :

HTTPS :

Il s'agit d'une version sécurisée du protocole HTTP. HTTPS utilise le chiffrement SSL/TLS pour garantir la confidentialité et l'intégrité des données échangées entre un client (comme un navigateur web) et un serveur. Cela permet de sécuriser les transactions en ligne, telles que les transactions bancaires ou les formulaires de connexion.

* Action: Pass
* Interface: LAN
* Address Family: IPv4
* Protocol: TCP
* Source: LAN net
* Destination: Any
* Destination Port Range: HTTPS (443)

HTTP :

Il s'agit du protocole utilisé pour la communication entre un client (comme un navigateur web) et un serveur sur Internet. Il permet le transfert de données, généralement au format HTML, pour afficher des pages web. Cependant, contrairement à HTTPS, HTTP ne garantit pas la sécurité des données lors de la transmission.

* Action: Pass
* Interface: LAN
* Address Family: IPv4
* Protocol: TCP
* Source: LAN net
* Destination: Any
* Destination Port Range: HTTP (80)

SMTP :

Il s'agit du protocole utilisé pour l'envoi de courriers électroniques. SMTP permet à un client d'envoyer un e-mail à un serveur de messagerie, qui se charge ensuite de le transférer au destinataire final. Il fonctionne sur le principe du "store-and-forward" (stocker et transférer).

* Action: Pass
* Interface: LAN
* Address Family: IPv4
* Protocol: TCP
* Source: LAN net
* Destination: WAN net
* Destination Port Range: SMTP (25)

NFS :

Il s'agit d'un protocole de partage de fichiers utilisé pour accéder à des fichiers distants sur un réseau. NFS permet à un ordinateur client d'accéder à des fichiers et répertoires partagés sur un serveur distant comme s'ils étaient locaux.

* Action: Pass
* Interface: LAN
* Address Family: IPv4
* Protocol: TCP
* Source: LAN net
* Destination: LAN net
* Destination Port Range: NFS (2049)

SMB :

Il s'agit d'un protocole de partage de fichiers et d'imprimantes largement utilisé dans les environnements Windows. Il permet à un ordinateur client d'accéder aux ressources partagées sur un serveur, telles que des fichiers, des imprimantes ou des ports série.

* Action: Pass
* Interface: LAN
* Address Family: IPv4
* Protocol: TCP
* Source: LAN net
* Destination: LAN net
* Destination Port Range: SMB (445)

DNS :

Il s'agit d'un protocole utilisé pour traduire les noms de domaine (comme www.example.com) en adresses IP compréhensibles par les ordinateurs. DNS joue un rôle essentiel dans la résolution des noms de domaine et permet de naviguer sur Internet en utilisant des noms plus conviviaux que les adresses IP numériques.

* Action: Pass
* Interface: LAN
* Address Family: IPv4
* Protocol: TCP/UDP
* Source: LAN net
* Destination: Any
* Destination Port Range: DNS (53)

LDAP :

Il s'agit d'un protocole utilisé pour accéder et interroger des annuaires d'informations, tels que des bases de données de contacts ou des répertoires d'utilisateurs. LDAP fournit un moyen standardisé d'interagir avec ces annuaires et est souvent utilisé pour l'authentification et l'autorisation dans les systèmes d'identification.

* Action: Pass
* Interface: LAN
* Address Family: IPv4
* Protocol: TCP/UDP
* Source: LAN net
* Destination: SRVAD
* Destination Port Range: LDAP (389)

KERBEROS :

Il s'agit d'un protocole d'authentification réseau sécurisé. Kerberos permet à des utilisateurs et à des services de prouver leur identité mutuelle de manière sécurisée sur un réseau non sécurisé. Il est couramment utilisé dans les environnements

* Action: Pass
* Interface: LAN
* Address Family: IPv4
* Protocol: TCP/UDP
* Source: LAN net
* Destination: SRVAD
* Destination Port Range: KERBEROS (88)

RDP :

Il s'agit d'un protocole qui permet à un utilisateur de se connecter et de contrôler un ordinateur distant à travers un réseau. RDP permet d'accéder à distance à un bureau complet, avec une interface graphique, et est couramment utilisé pour l'administration à distance ou le travail à distance.

* Action: Pass
* Interface: LAN
* Address Family: IPv4
* Protocol: TCP
* Source: SRVAD-04
* Destination: SRVAD-03, SRVAD-05
* Destination Port Range: RDP (3389)

ICMP :

Il s'agit d'un protocole utilisé pour la gestion et le contrôle du réseau. ICMP est principalement utilisé pour envoyer des messages de contrôle et de diagnostic, tels que les messages d'erreur ou les demandes d'écho (ping), entre les périphériques réseau.

* Action: Pass
* Interface: LAN
* Address Family: IPv4
* Protocol: ICMP (any)
* Source: LAN net
* Destination: any

SSH :

Il s'agit d'un protocole de communication sécurisé utilisé pour l'accès distant aux systèmes informatiques. SSH permet une connexion sécurisée et chiffrée entre un client et un serveur, ce qui permet d'exécuter des commandes à distance, transférer des fichiers ou accéder à des services réseau de manière sécurisée.

* Action: Pass
* Interface: LAN
* Address Family: IPv4
* Protocol: TCP
* Source: SRVAD
* Destination: BDD net, DMZ net
* Destination Port Range: SSH (22)

Voici une présentation des protocoles autorisés sur le réseau WAN ainsi qu’une brève présentation de leur protocoles :

POP3 :

POP3 est un protocole de courrier électronique largement utilisé pour récupérer les e-mails à partir d'un serveur distant vers un client de messagerie. Lorsque vous configurez un compte de messagerie POP3, les e-mails sont généralement téléchargés du serveur vers votre appareil et supprimés du serveur, à moins que vous ne choisissiez de les conserver sur le serveur. Cela signifie que vous pouvez accéder à vos e-mails hors ligne, mais les modifications effectuées sur un appareil ne sont pas synchronisées avec les autres appareils.

* Action: Pass
* Interface: WAN
* Address Family: IPv4
* Protocol: TCP
* Source: LAN net
* Destination: any
* Destination Port Range: POP3 (110)

SMTP :

* Action: Pass
* Interface: WAN
* Address Family: IPv4
* Protocol: TCP
* Source: LAN net
* Destination: any
* Destination Port Range: SMTP (25)

IMAP :

IMAP est un autre protocole de courrier électronique qui permet aux utilisateurs d'accéder à leurs e-mails sur un serveur distant. Contrairement à POP3, IMAP permet une meilleure synchronisation entre le client de messagerie et le serveur. Lorsque vous configurez un compte IMAP, les e-mails restent sur le serveur, et vous pouvez les consulter et les gérer depuis différents appareils. Les actions effectuées sur un appareil (comme la suppression d'un e-mail) sont reflétées sur tous les appareils connectés.

* Action: Pass
* Interface: WAN
* Address Family: IPv4
* Protocol: TCP
* Source: LAN net
* Destination: any
* Destination Port Range: IMAP (143)

ICMP :

* Action: Pass
* Interface: WAN
* Address Family: IPv4
* Protocol: ICMP
* Source: any
* Destination: any

HTTP/HTTPS :

* Action: Pass
* Interface: WAN
* Address Family: IPv4
* Protocol: TCP
* Source: LAN net
* Destination: any
* Destination Port Range: HTTP/HTTPS (80/443)

DNS :

* Action: Pass
* Interface: WAN
* Address Family: IPv4
* Protocol: TCP/UDP
* Source: LAN net
* Destination: any
* Destination Port Range: DNS (53)

Voici une présentation des protocoles autorisés sur le réseau DMZ :

DNS :

* Action: Pass
* Interface: DMZ
* Address Family: IPv4
* Protocol: TCP/UDP
* Source: LAN net
* Destination: any
* Destination Port Range: DNS (53)

ICMP :

* Action: Pass
* Interface: DMZ
* Address Family: IPv4
* Protocol: ICMP
* Source: any
* Destination: any

Voici une présentation des protocoles autorisés sur le réseau BDD :

DNS :

* Action: Pass
* Interface: DMZ
* Address Family: IPv4
* Protocol: TCP/UDP
* Source: LAN net
* Destination: any
* Destination Port Range: DNS (53)

ICMP :

* Action: Pass
* Interface: DMZ
* Address Family: IPv4
* Protocol: ICMP
* Source: any
* Destination: any