Règles pour Firewall 1 (Internet <-> DMZ)

1. **Accès entrant vers Reverse Proxy**
    - **Description** : Autoriser uniquement le trafic entrant de l'Internet vers le Reverse Proxy sur les ports 80 (HTTP) et 443 (HTTPS) pour les services web publics.
    - **Détails** : Source = Internet ; Destination = 192.168.20.13 ; Ports = 80, 443.
2. **Blocage du reste du trafic entrant vers DMZ**
    - **Description** : Bloquer tout autre trafic entrant depuis Internet vers la DMZ pour protéger les autres services et conteneurs.
    - **Détails** : Source = Internet ; Destination = DMZ ; Ports = Tous sauf 80, 443.
3. **Limitation des accès sortants du Reverse Proxy**
    - **Description** : Restreindre les connexions sortantes du Reverse Proxy aux seuls ports nécessaires (e.g., pour effectuer des vérifications DNS si nécessaire).
    - **Détails** : Source = 192.168.20.13 ; Destination = Internet ; Ports = uniquement requis pour services spécifiques (DNS, etc.).

Règles pour Firewall 2 (DMZ <-> LAN)

1. **Accès LAN vers Proxy**
    - **Description** : Permettre aux utilisateurs du réseau LAN d'accéder au Proxy dans la DMZ pour le trafic HTTP/HTTPS (ports 80 et 443).
    - **Détails** : Source = LAN ; Destination = 192.168.20.12 (Proxy) ; Ports = 80, 443.
2. **Proxy vers Internet**
    - **Description** : Autoriser le Proxy de la DMZ à se connecter à Internet uniquement pour le trafic sortant nécessaire (HTTP/HTTPS) et à travers le Firewall 1.
    - **Détails** : Source = 192.168.20.12 ; Destination = Internet ; Ports = 80, 443.
3. **Blocage direct LAN vers Internet**
    - **Description** : Empêcher le réseau LAN d'accéder directement à Internet (le trafic doit passer par le Proxy pour contrôle).
    - **Détails** : Source = LAN ; Destination = Internet ; Ports = Tous ; Action = Bloquer.
4. **Reverse Proxy vers Serveur Web**
    - **Description** : Autoriser le Reverse Proxy de la DMZ à rediriger les requêtes vers le Serveur Web, situé également dans la DMZ.
    - **Détails** : Source = 192.168.20.13 ; Destination = 192.168.20.14 (Serveur Web) ; Ports = 80, 443.
5. **Reverse Proxy vers Serveur Applicatif**
    - **Description** : Permettre au Reverse Proxy d'accéder au Serveur Applicatif pour rediriger des requêtes spécifiques depuis la DMZ.
    - **Détails** : Source = 192.168.20.13 ; Destination = 192.168.10.11 (Serveur Applicatif) ; Ports = 80, 443 ou autres ports applicatifs.

6. **Blocage supplémentaire vers Reverse Proxy**
    - **Description** : Bloquer tout autre trafic interne qui tenterait d'atteindre le Reverse Proxy pour sécuriser davantage le service web.
    - **Détails** : Source = LAN ou DMZ ; Destination = 192.168.20.13 ; Ports = Tous sauf 80, 443 ; Action = Bloquer.

Règles pour le Proxy

Le Proxy est destiné à gérer les requêtes sortantes du LAN vers Internet, en contrôlant l'accès pour améliorer la sécurité et le filtrage de contenu. Voici les règles spécifiques à mettre en place dans le **Firewall 2** (entre le LAN, la DMZ, et le sous-réseau SERVERS).

1. **Accès sortant HTTP/HTTPS vers Internet**
    - Permettre au Proxy d'accéder à Internet pour les connexions HTTP et HTTPS nécessaires aux utilisateurs du LAN.
2. **Limiter l'accès sortant du Proxy à Internet**
    - Autoriser uniquement les ports nécessaires pour le trafic sortant du Proxy vers Internet.
3. **Bloquer tout autre trafic du LAN directement vers Internet en passant par le Firewall 1**
    - Empêcher les utilisateurs du LAN de contourner le Proxy pour accéder directement à Internet.

Règles pour le Reverse Proxy

Le Reverse Proxy dans la DMZ est chargé de recevoir les requêtes externes HTTP/HTTPS et de les diriger vers le serveur Web ou le serveur applicatif. Ces règles doivent être configurées principalement sur le **Firewall 1** pour le trafic entrant depuis Internet, mais aussi sur le **Firewall 2** pour le trafic interne dans le réseau.

1. **Accès entrant HTTP/HTTPS depuis Internet**
    - Autoriser uniquement le trafic entrant sur les ports 80 et 443 vers le Reverse Proxy depuis l'Internet.
2. **Redirection interne vers Serveur Web**
    - Permettre au Reverse Proxy de rediriger les requêtes entrantes vers le Serveur Web.
3. **Redirection interne vers Serveur Applicatif**
    - Permettre au Reverse Proxy de rediriger certaines requêtes vers le Serveur Applicatif, selon la configuration des services.
4. **Blocage des autres connexions entrantes**
    - Bloquer tout autre trafic entrant vers le Reverse Proxy, sauf pour les services web autorisés.