Configurer le pare-feu pour LAN et DMZ

Router Version	Centro Business 1.0 Centro Business 2.0 Centro Business 3.0
Doc. Version	3.0
Status	Final
update	01.2023

Instructions de configuration Centro Business

Swisscom (Suisse) SA
3050 Berne

swisscom

Contenu

Configurer le pare-feu pour LAN et DMZ

1.1 Besoins

Vous souhaitez restreindre le trafic du réseau Internet vers votre LAN / DMZ ou de votre LAN / DMZ vers le réseau Internet afin de protéger votre infrastructure et vos données.

1.2 Description

Le routeur Centro Business met à votre disposition deux pare-feux indépendants pour votre LAN et la DMZ. Vous avez le choix entre deux jeux de filtres prédéfinis pour chaque pare-feu, et vous pouvez créer vos propres filtres ou les désactiver. Vous pouvez créer des jeux de filtres séparés pour le trafic entrant (Inbound) et sortant (Outbound).

1.3 Conditions/restrictions

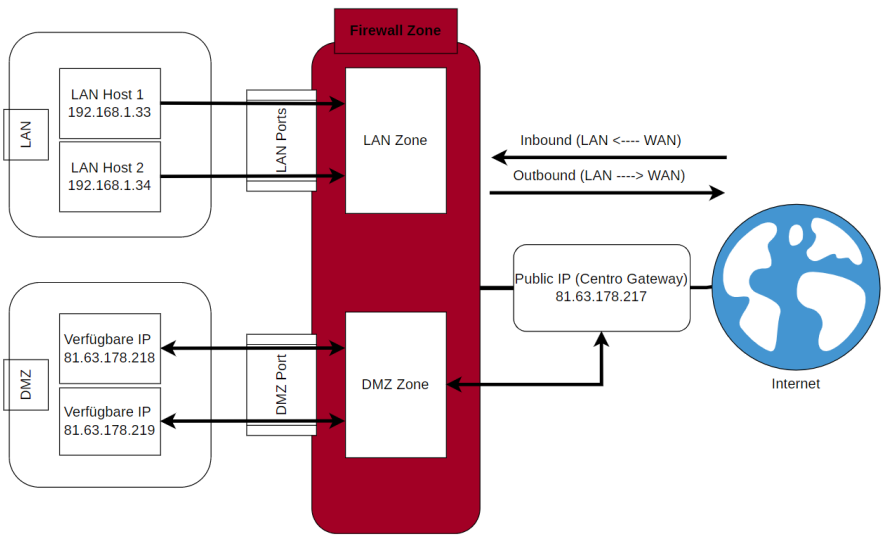
Conditions:

- Contrat Swisscom: Business Internet Services, My PME Office, Business Internet Light, Enterprise Connect XS ou Internet pour les particuliers
- Centro Business avec la version actuelle du firmware. Vous pouvez trouver le firmware sur la page d'aide officielle de Centro Business sous Mise à jour du firmware.
- L'accès est configuré sur le portail du routeur

Restrictions:

- Si le client n'a pas d'adresse IP fixe ou n'a pas activé de DMZ, seul le pare-feu pour le LAN est affiché.
- Le service BNS est activé sur le pack.

1.4 Illustration



1.5 Paramètres de base (filtres LAN et DMZ)

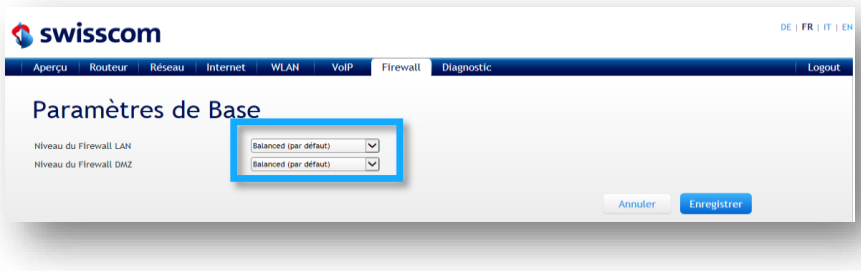
En fonction du raccordement ou de l'éventuelle utilisation d'adresses IP fixes, les paramètres du pare-feu sont affichés dans le menu **Firewall, Paramètres de base**. Si vous ne possédez pas d'adresse IP fixe publique ou si vous n'avez pas activé de DMZ, seul le pare-feu de votre réseau local (LAN) est affiché. Si la DMZ est activée, les pare-feux LAN et DMZ sont affichés.

Vous pouvez choisir un jeu de filtres parmi les suivants pour chaque pare-feu.

- **Balanced** (par défaut): Dans ce mode de fonctionnement, le pare-feu transfère toutes les données provenant du LAN ou de la DMZ vers Internet et provenant d'Internet vers le LAN, à l'exception d'un ensemble défini de protocoles.
- **Strict**: Le pare-feu bloque le trafic provenant d'Internet et à destination du LAN ou de la DMZ, à l'exception de celui reçu sur quelques ports utilisés pour la gestion du routeur. Seuls quelques ports sont bloqués pour le trafic envoyé du LAN ou de la DMZ du client vers Internet.
- **Custom**: Tout le trafic Internet provenant d'adresses IPv4 et IPv6 est bloqué et n'est pas transmis au LAN. Il n'y a aucun blocage pour le trafic envoyé du LAN du client vers Internet.
- **Off**: Le pare-feu est désactivé. Les connexions d'Internet vers le LAN ou la DMZ ou en sens inverse ne sont pas bloquées.

En général:
Dans tous les cas, il n'est pas recommandé de désactiver complètement le pare-feu du Centro Business car cela pourrait entraîner une surcharge des ressources système causée par des cyberattaques.

Les blocages activés pour chaque service ou port sont affichés dans les onglets «**Règles Firewall LAN**» et «**Règles Firewall DMZ**».



Q1 2023 NOUVEAU:

Le port HTTPS TCP:443 est rejeté (Drop) entrant (Inbound) pour le niveau de firewall "Balanced (par défaut)"

Rule setting for LAN and DMZ Firewall

Service	Destination Port	Inbound Rule	Outbound Rule	Balanced (Default)	Strict
Kerberos TCP	TCP:88	drop	reject	✓	✓
Kerberos UDP	UDP:88	drop	reject	✓	✓
Internet Printing Protocol	TCP:631	drop	reject	✓	✓
Simple Service Discovery Protocol TCP	TCP:2869	drop	reject	✓	✓
Simple Service Discovery Protocol UDP	UDP:1900	drop	reject	✓	✓
UPnP	UDP:3702	drop	reject	✓	✓
Sun RPC	TCP:111	drop	reject	✓	✓
Microsoft RPC	TCP:135	drop	reject	✓	✓
mDNS	UDP:5353	drop	reject	✓	✓
NetBIOS	TCP:139	drop	reject	✓	✓
Microsoft SMB	TCP:445	drop	reject	✓	✓
Remote Login	TCP:513	drop	reject	✓	✓
Remote Shell	TCP:514	drop	reject	✓	✓
Apple Filing Protocol	TCP:548	drop	reject	✓	✓
Link-Local Multicast Name Resolution	UDP:5355	drop	reject	✓	✓
Secure Shell (SSH)	TCP:22	drop	accept	✓	
Telnet	TCP:23	drop	accept	✓	
HTTP	TCP:80	drop	accept	✓	
HTTPS	TCP:443	drop	accept	✓	
Microsoft RDP	TCP:3389	drop	accept	✓	
VNC	TCP:5900	drop	accept	✓	
Default Policy	all packets	accept	accept	✓	
Default Policy	all packets	drop	accept		✓

Rule setting for DMZ Firewall only

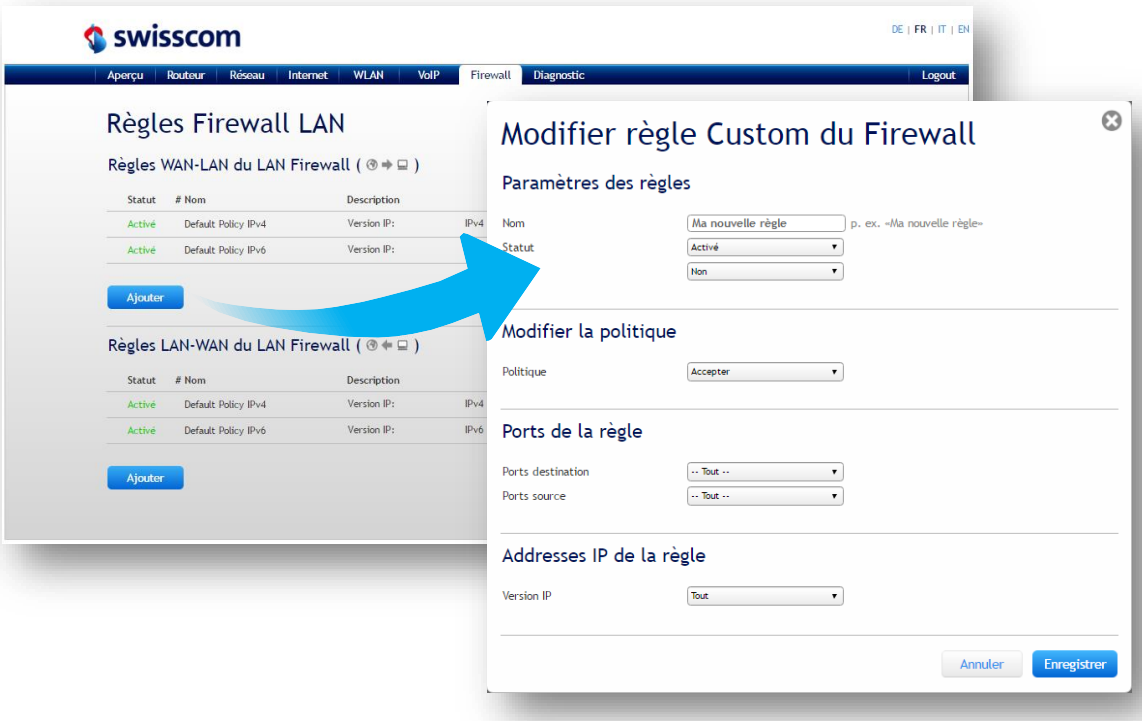
Block List "Balanced" Setting	Destination Port	Inbound Rule	Outbound Rule	Balanced (Default)	Strict
TO LAN	all packets	drop	drop	✓	✓

1.6 Créer ou modifier des règles de filtrage

Si «**Custom**» est défini dans les paramètres de base du pare-feu LAN ou DMZ, vous pouvez créer vos propres règles ou les modifier. Vous pouvez alors faire une distinction entre le trafic provenant d'Internet à destination du LAN ou de la DMZ et le trafic en sens inverse. Cliquez sur le bouton **Ajouter** Règles WAN-LAN ou Règles LAN-WAN dans **Règles Firewall LAN** ou **Règles Firewall DMZ** pour définir la règle souhaitée.

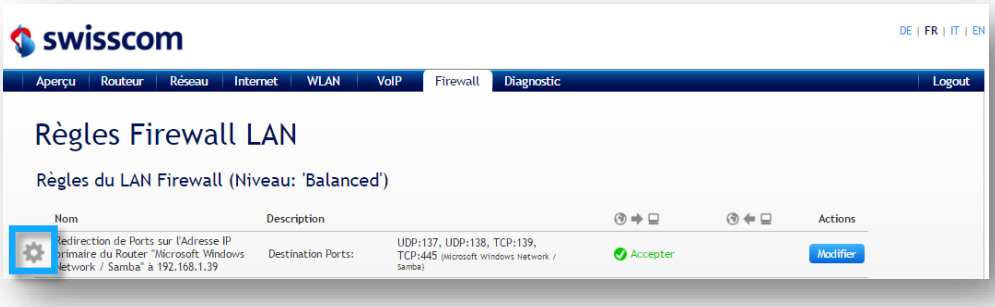
Toute règle de filtrage comporte les données suivantes.

- Nom (peut être défini individuellement)
- Statut (Activé/Désactivé)
- Log (Oui/Non)
- Politique (Accepter/Refuser)
- Ports destination (Port unique ou Port Range, ou Plusieurs ports ou Range)
- Ports source (Port unique ou Port Range, ou Plusieurs ports ou Range)
- Version IP (favori, IPv4 ou IPv6)
- Type critère destination (IPv6 ou IPv6) adresse favorite/adresse unique, Subnet, plage d'adresse
- Type critère source (IPv6 ou IPv6) adresse favorite/adresse unique, Subnet, plage d'adresse
- Indicateur exclusif (Exclusion)



1.7 Règles de filtrage définies automatiquement

Si un port est redirigé vers l'adresse IP du routeur ou une adresse IPv4 publique, une règle de filtrage automatique est configurée pour le pare-feu du LAN. Il est ensuite possible de la modifier, mais non de la supprimer. Les modifications suivantes sont possibles: version IP, adresse source et indicateur exclusif (exclusion). Les règles définies automatiquement sont indiquées de manière particulière.



1.8 Filtre de contenu

Certains mots clés peuvent être définis dans un filtre de contenu. Remarque: il n'est pas possible de filtrer les contenus échangés sur une connexion chiffrée.