

Exploiter un serveur mail et web ou une passerelle de sécurité (Security Gateway) dans la DMZ

ID document	Exploiter un serveur mail et web ou une passerelle de sécurité (Security Gateway) dans la DMZ
Version	2.0
Statut	Version finale
Date d'édition	04.2017

Contenu

1.1 Besoins	3
1.2 Description	3
1.3 Conditions/Restrictions	3
1.4 Illustration	4
1.5 Activer la DMZ	4
1.6 Vérification	4

Exploiter un serveur mail et web ou une passerelle de sécurité (Security Gateway) dans la DMZ

1.1 Besoins

Vous souhaitez gérer le trafic de données Internet-réseau par le biais d'une passerelle de sécurité (Security Gateway, SG) ou d'un pare-feu.

Vous souhaitez créer un réseau privé virtuel (VPN) par le biais de votre passerelle de sécurité (SG).

Vous souhaitez exploiter un serveur mail ou web dans une zone démilitarisée (DMZ) sur votre routeur Centro Business.

1.2 Description

Sur le routeur Centro Business, au moyen du paramètre DMZ publique, vous pouvez router les adresses IP publiques fixes vers un appareil, par exemple un serveur ou une passerelle de sécurité (SG). Cet appareil doit être branché sur le port LAN 1 du routeur Centro Business. Vous pouvez bien entendu brancher plusieurs appareils au moyen d'un switch supplémentaire.

Si la DMZ publique est activée, vous pouvez exploiter un réseau (LAN) sur les ports LAN 2 à 4 et par le réseau sans fil (WLAN). La configuration du LAN est la même que la configuration par défaut. Le LAN est disponible pour tous les services Swisscom et accès Internet.

L'accès de la DMZ au réseau (LAN) est bloqué. L'accès du LAN à la DMZ s'effectue au moyen des adresses IP publiques. L'accès au portail du routeur s'effectue par

le biais du réseau ou de la télégestion. L'accès de la DMZ au portail du réseau n'est pas possible.

1.3 Conditions/restrictions

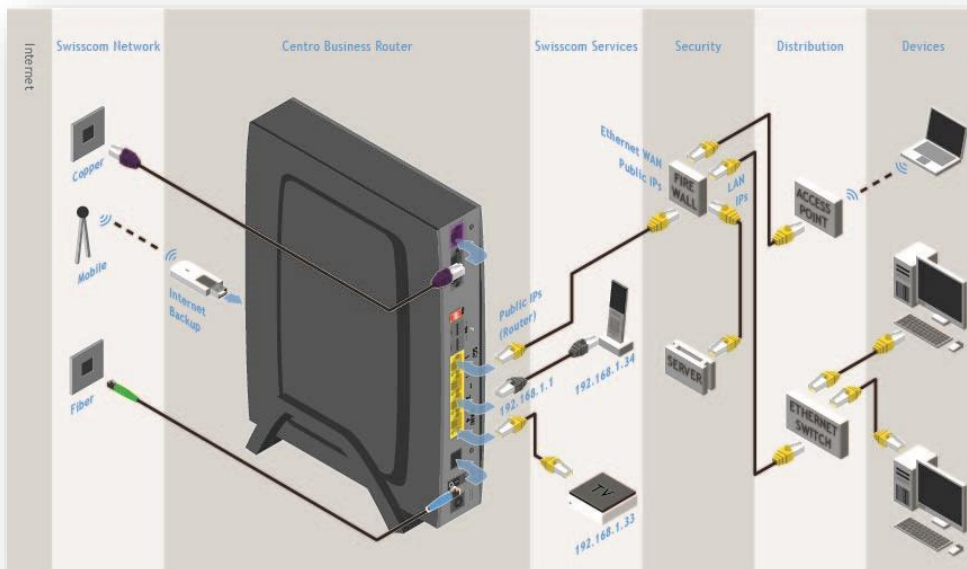
Conditions:

- Contrat Swisscom: Business Internet Services, My PME Office, Enterprise Connex XS, Business Internet Light
- Centro Business 2.0 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
- Plusieurs adresses IP fixes (au moins 4 IP)

Restrictions:

- Si la DMZ publique est activée, les paramètres **IP-Passthrough**, **PPPoE Passthrough** et **IP Pool public en tant que pool DHCP** ne peuvent pas être exploités.

1.4 Illustration*

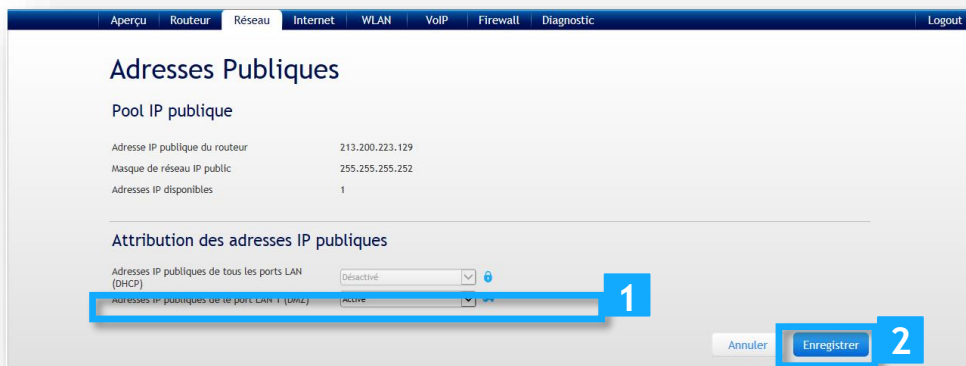


Instructions de
configuration Centro
Business

Swisscom (Suisse) SA
3050 Berne

1.5 Activer la DMZ

Sous **Réseau**, **Adresses publiques**, sélectionnez «Activé» pour le champ **Adresses IP publiques du port LAN 1 (DMZ)**. Sauvegardez la saisie en cliquant sur **Enregistrer**.



1.6 Vérification

Si le message «Les paramètres ont été enregistrés» apparaît, la DMZ publique est activée. Les adresses IP publiques fixes peuvent désormais être exploitées sur le port LAN 1 du routeur Centro Business.

* Illustration identique pour Centro Business 1.0 et Centro Business 2.0.