ZyXEL

Application Guide

ZyXEL ZyWALL SSL 10

français

Options d'application

Chère cliente, cher client

Nous vous remercions d'avoir choisi un produit ZyXEL.
Ce guide vous présente les quatre options d'application principales du ZyWALL SSL 10. Pour chaque application, nous avons décrit l'implémentation de base.

En tenant compte de quelques points importants, vous gagnerez du temps lors de l'installation initiale de l'appareil.
Des exemples de configuration seront publiés au fur et à mesure dans la Kowledgebase sur **www.studerus.ch/f/knowledgebase**.

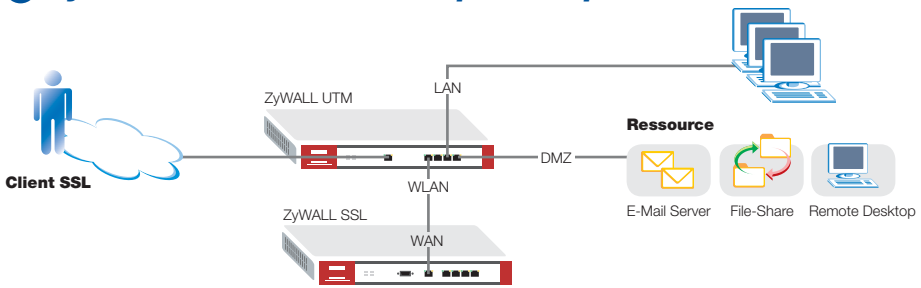
Options d'application ZyWALL SSL 10

- **A** ***ZyWALL SSL 10 dans zone pare-feu particulière***
- **B** ***ZyWALL SSL 10 dans DMZ du pare-feu/routeur ADSL***
- **C** ***ZyWALL SSL 10 dans LAN du pare-feu/routeur ADSL/LAN***
- **D** ***ZyWALL SSL 10 raccordé directement à l'Internet***
  (modem câble/ routeur ADSL en mode pont)

IMPORTANT pour toutes les options :

- Pour pouvoir utiliser les connexions SSL-VPN client, le ZyWALL SSL 10 doit être enregistré.
- Pour pouvoir utiliser toutes les fonctions, la résolution de noms est nécessaire, via DynDNS ou adresse IP fixe avec DNS.
- Pour l'installation, les ordinateurs client SSL ont besoin des droits de Java Runtime Environment.
- Le sous-réseau LAN-IP du ZyWALL SSL 10 doit toujours être différent de la zone LAN, DMZ et WLAN des pare-feu/routeurs ADSL.
- Le client SSL doit pouvoir accéder à l'interface WAN du ZyWALL SSL 10 via le port 443.
- Pour la gestion via l'interface WAN, le client SSL doit pouvoir accéder au ZyWALL SSL 10 via le port 8443.

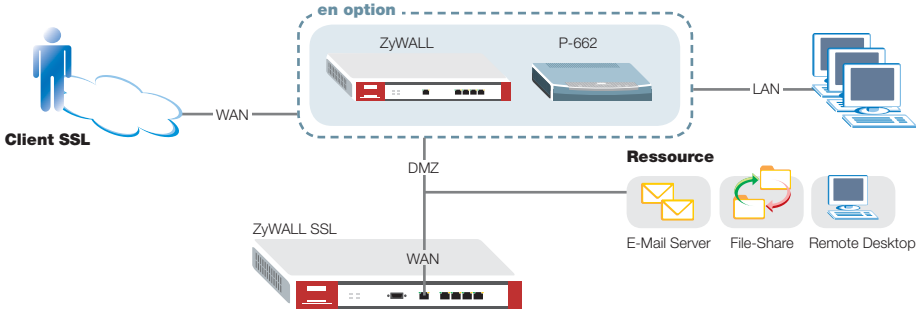
A ZyWALL SSL 10 dans la zone pare-feu particulière



Application : Le ZyWALL SSL 10 est installé dans une zone pare-feu particulière (exemple : la zone WLAN non utilisée du ZyWALL). Ce n'est alors que l'interface WAN du ZyWALL SSL 10 qui est connectée.

Avantage : Sécurité optimale pour DMZ et LAN grâce à la terminaison de la connexion dans la zone particulière. Si un ZyWALL SSL 10 est exploité avec un ZyWALL UTM et décrypté dans une zone particulière, la prévention d'intrusion et le contrôle antivirus sont appliqués pour les connexions SSL.

B ZyWALL SSL 10 dans DMZ du pare-feu/routeur ADSL

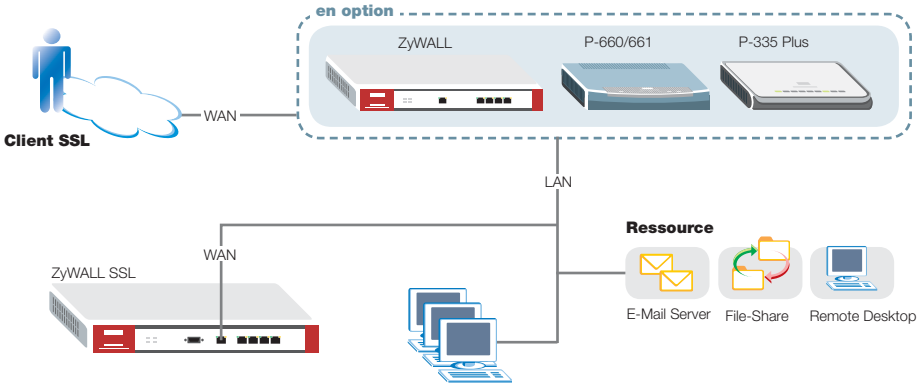


Application : Le ZyWALL SSL 10 est placé en zone DMZ du pare-feu/routeur ADSL (exemple : ZyWALL ou P-662). Ce n'est alors que l'interface WAN du ZyWALL SSL 10 qui est connectée.

Avantage : Sécurité pour le LAN grâce à la terminaison de la connexion dans la DMZ.

Options d'application

C ZyWALL SSL 10 dans LAN du pare-feu/routeur ADSL/LAN

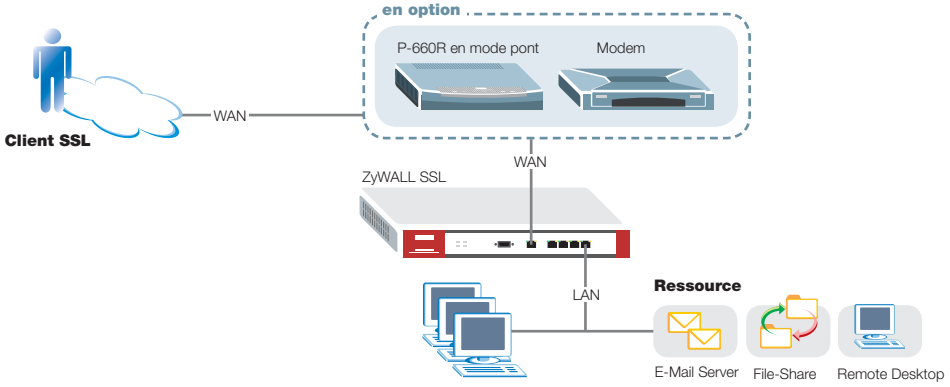


Application : Le ZyWALL SSL 10 est placé dans le LAN du pare-feu/routeur ADSL/LAN (exemple : ZyWALL ou P-660H/P-661H). Ce n'est alors que l'interface WAN du ZyWALL SSL 10 qui est connectée.

Avantage : Installation facile avec un routeur Internet existant sans zone DMZ particulière.

D ZyWALL SSL 10 raccordé directement à l'Internet

(modem câble/routeur ADSL en mode pont)



Application : Le ZyWALL SSL 10 est connecté directement à l'Internet via un routeur en mode bridge ou un modem câble. L'interface WAN du ZyWALL SSL 10 est raccordée au routeur en mode bridge ou au modem câble, l'interface LAN est connectée aux serveurs. La fonction NAT et pare-feu du ZyWALL SSL 10 doit être activée.

Avantage : Installation facile avec un routeur Internet existant équipé d'une seule interface LAN ou un modem câble.

Informations supplémentaires : www.studerus.ch/f/knowledgebase

Hotline Support : lundi à vendredi 8h30 – 12h00 /13h30 – 19h00
Utilisez-vous votre produit dans le domaine privé pour un seul PC ou un petit réseau ?
Appelez le : **0900 900 641**
Utilisez-vous votre produit dans un réseau d'entreprise ?
Appelez le : **0900 900 646**

Remarques générales indépendantes de l'option d'application

1. Authentification

Le ZyWALL SSL 10 supporte les trois procédés d'authentification suivants :

- Utilisateurs locaux / groupe : idéal pour petites entreprises sans Active-Directory et infrastructure serveur.
- AD/LDAP : pour PME. Intégration avec l'infrastructure serveur. L'avantage est que l'administration des utilisateurs et les mots de passe ne sont pas sauvegardés sur le ZyWALL SSL 10. La Security Policy est administrée sur le serveur.
- RADIUS avec solution ZyXEL OTP Token (One Time Password) : authentification à deux niveaux, haut niveau de sécurité, l'installation n'est conseillée qu'avec Windows 2000, 2003 Server en langue anglaise.

2. Contrôle sécurité End Point

L'accès n'est autorisé qu'après vérification de certains critères :

- Système d'exploitation, Service Pack, Auto Update, logiciel antivirus, navigateur, version du navigateur, processus actif, fichier disponible etc.
- La sécurité End Point peut être personnalisée pour chaque groupe d'utilisateurs.
- Inconvénient : peu de flexibilité pour l'accès via un lieu public (café Internet, hôtel etc.)

3. Accès aux applications

Le client peut accéder aux applications (autorisation selon l'utilisateur ou groupe d'utilisateurs).

En général, il faut faire la différence entre une application Web et une application.

- Application Web : prend en charge http et https pour applications et OWA (Outlook Web Access), serveur Web, serveur mail. L'accès a lieu directement via le portail Web du ZyWALL SSL 10.
- Application : par ex. Remote Desktop, VNC, Citrix, FTP etc. Une installation logicielle est nécessaire. L'accès au serveur a lieu via une adresse IP virtuelle (par ex. 127.0.0.2).
- Une définition Custom Port est possible pour des applications qui ne sont pas prédéfinies.

4. Partage de fichiers

Accès à la gestion des fichiers d'un serveur ou NAS (par ex. avec ZyXEL NSA-2400).

- Actions possibles dans le portail Web du ZyWALL SSL 10 : ouvrir, copier, renommer et effacer le fichier.
- La Policy du fichier est définie sur le serveur fichier, NAS.
- Il est conseillé d'utiliser l'option ZyWALL DMZ/WLAN avec l'UTM pour le contrôle IDP/antivirus.

5. NetExtender

Comme les IPSec-VPNs traditionnels : un adaptateur réseau virtuel est ajouté à l'ordinateur client afin de construire un tunnel entre les deux points finaux.

- « Inconvénient » : l'ordinateur client a accès à tout le réseau. C'est donc une option conseillée pour le ZyWALL DMZ/WLAN avec vérification des règles pare-feu.
- Le client SSL est sur le même réseau que le serveur.
- Droits d'administrateur sur l'ordinateur client sont nécessaires pour établir la connexion virtuelle.
- Les paramètres de sécurité de Windows Vista empêchent la fonction NetExtender.