

Application Guide

ZyXEL ZyWALL SSL 10



© 2007 Copyright by Studerus Telecom AG, 8603 Schwerzenbach

Vers. 1.0/0704

Änderungen und Irrtümer vorbehalten.
Sous réserve de modifications et d'erreurs.

Einsatzszenarien ZyWALL SSL 10 (Seite 2)
Options d'application ZyWALL SSL 10 (page 5)

Einsatzszenarien

Liebe Kundin, lieber Kunde

Vielen Dank, dass Sie sich für ein ZyXEL-Produkt entschieden haben.

Diese Kurzübersicht zeigt Ihnen vier Haupt-Einsatz-Varianten für die ZyWALL SSL 10 auf. Für jedes Szenario ist die grundlegende Implementierung beschrieben.

Das Beachten ein paar wichtiger Punkte erspart Ihnen Zeit bei der ersten Inbetriebnahme.

Detaillierte Konfigurationsbeispiele werden fortlaufend publiziert in der Knowledgebase auf www.studerus.ch/knowledgebase.

ZyWALL SSL 10 Einsatzszenarien

A ZyWALL SSL 10 in eigener Firewall-Zone

B ZyWALL SSL 10 in DMZ von Firewall/ADSL-Router

C ZyWALL SSL 10 im LAN von Firewall/ADSL-/LAN-Router

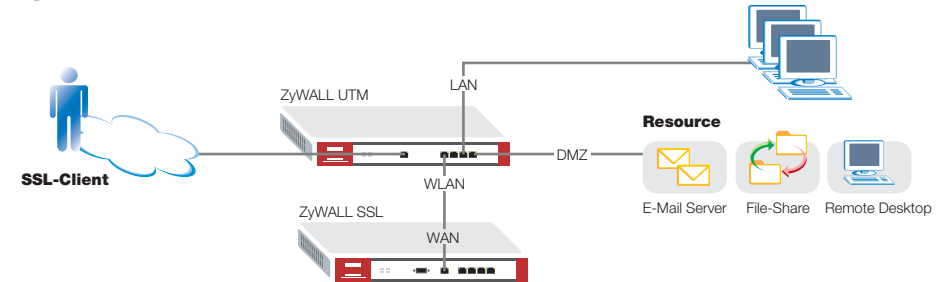
D ZyWALL SSL 10 direkt am Internet (Cable-Modem/bridged ADSL-Router)

WICHTIG für alle Varianten:

- Um Client SSL-VPN-Verbindungen zu nutzen, muss die ZyWALL SSL 10 registriert werden.
- Für die volle Funktionalität wird Namensauflösung benötigt, via DynDNS oder fixer IP-Adresse mit DNS.
- SSL Client-Rechner müssen die Rechte für die Installation von Java Runtime Environment haben.
- Das LAN-IP-Subnetz der ZyWALL SSL 10 muss sich in jedem Fall von der LAN-, DMZ- und WLAN-Zone der verwendeten Firewall/ADSL-Router unterscheiden.
- Das WAN-Interface der ZyWALL SSL 10 muss vom SSL-Client via Port 443 erreichbar sein.
- Für das Management über das WAN-Interface muss die ZyWALL SSL 10 vom SSL-Client via Port 8443 erreichbar sein.



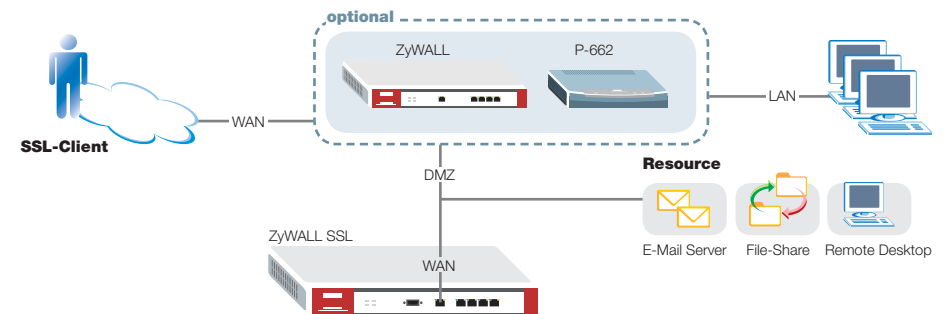
A ZyWALL SSL 10 in eigener Firewall-Zone



Einsatz: Die ZyWALL SSL 10 wird in einer eigenen Firewall-Zone platziert (Beispiel: die ungenutzte WLAN-Zone der ZyWALL). Nur das WAN-Interface der ZyWALL SSL 10 wird verbunden.

Vorteil: Optimale Sicherheit für DMZ und LAN durch Terminierung der Verbindung in einer eigenen Zone. Intrusion-Prevention und Anti-Virus-Überprüfung greifen bei SSL-Verbindungen in der Kombi-Lösung einer ZyWALL UTM, wenn SSL in einer separaten Zone entschlüsselt wird.

B ZyWALL SSL 10 in DMZ von Firewall/ADSL-Router

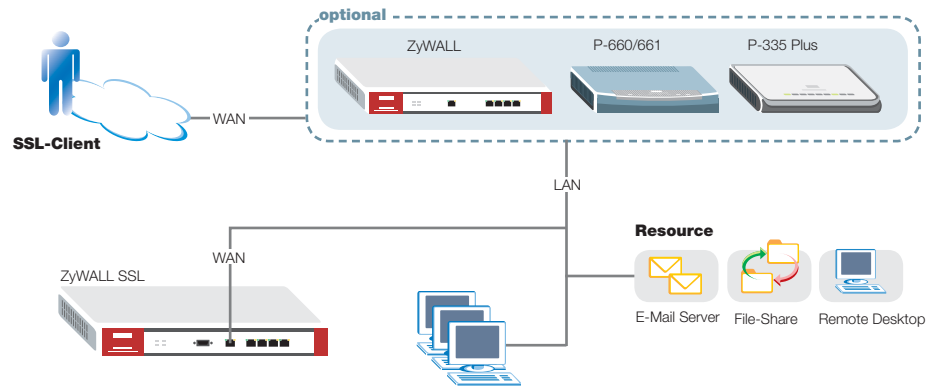


Einsatz: Die ZyWALL SSL 10 wird in der DMZ der Firewall/ADSL-Router platziert (Beispiel: ZyWALL oder P-662). Nur das WAN-Interface der SSL 10 wird verbunden.

Vorteil: Sicherheit für das LAN durch Terminierung der Verbindung in der DMZ.

Einsatzszenarien

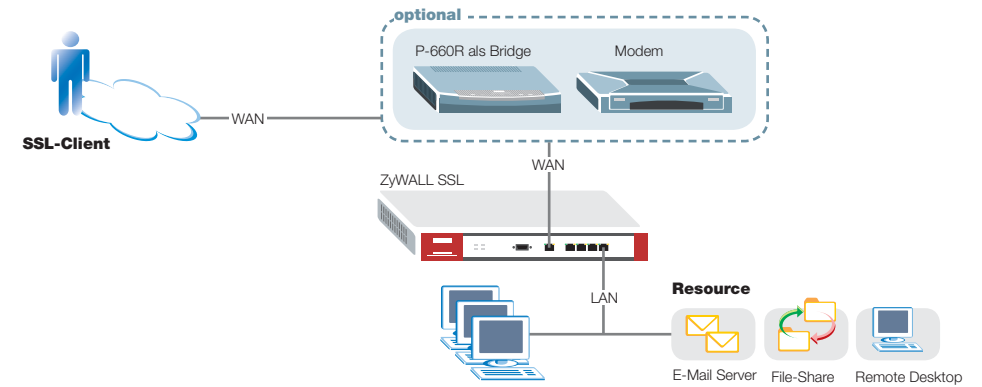
© ZyWALL SSL 10 im LAN von Firewall/ADSL-/LAN-Router



Einsatz: Die ZyWALL SSL 10 wird im LAN von Firewall/ADSL-/LAN-Router platziert (Beispiel: ZyWALL oder P-660H/P-661H). Nur das WAN-Interface der SSL 10 wird verbunden.

Vorteil: Einfache Installation bei bestehendem Internet-Router ohne separate DMZ-Zone.

© ZyWALL SSL 10 direkt am Internet (Cable-Modem/bridged ADSL-Router)



Einsatz: Die ZyWALL SSL 10 wird direkt über einen bridged Router oder ein Cable-Modem mit dem Internet verbunden. Das WAN-Interface der ZyWALL SSL 10 wird am bridged Router oder am Cable-Modem angeschlossen, das LAN-Interface wird mit den Servern verbunden. Die NAT- und Firewall-Funktion der ZyWALL SSL 10 muss aktiviert werden.

Vorteil: Einfache Installation bei bestehendem Internet-Router mit nur einem LAN-Interface oder einem Cable-Modem.



Weitere Informationen: www.studerus.ch/knowledgebase

Support Hotline: Mo – Fr 8.30 – 12.00 / 13.30 – 19.00 h

Nutzen Sie Ihr Produkt privat an einem einzelnen PC oder kleinen Netzwerk?

Wählen Sie: **0900 900 640**

Setzen Sie Ihr Produkt in einem Firmennetzwerk ein?

Wählen Sie: **0900 900 645**

Generelle Punkte unabhängig des Einsatzszenarios

1. Authentifizierung

Die ZyWALL SSL 10 unterstützt drei Authentifizierungs-Verfahren:

- Local Users / Group: ideal für kleine Firma ohne Active-Directory und Server-Infrastruktur.
- AD/LDAP: für KMU. Integration mit Server-Infrastruktur, Vorteil ist, dass keine User-Verwaltung und keine Passwörter auf der ZyWALL SSL 10 gespeichert werden. Die Security-Policy wird auf dem Server administriert.
- RADIUS mit ZyXEL OTP-Token (One-Time-Password) Lösung: Zwei-Stufen-Authentifizierung, hohes Sicherheits-Level, Installation nur auf Windows 2000, 2003 Server mit englischer Sprache empfohlen.

2. End-Point-Security-Kontrolle

Der Zugang wird nur nach Prüfung von bestimmten Kriterien gewährleistet.

- Betriebssystem, Service-Pack, Auto-Update, Antiviren-Software, Browser, Browser-Version, Prozess aktiv, Datei vorhanden usw.
- End-Point-Security kann für jede User-Group personalisiert werden
- Nachteil: wenig Flexibilität für Zugang über einen öffentlichen Ort (Internet Café, Hotel, usw.)

3. Application-Zugriff

Möglicher Client-Zugriff auf Applikationen (spezifisch auf Benutzer/Benutzergruppe zugelassen)

Grundsätzlich ist zu unterscheiden zwischen Web-Applikation und Applikation

- Web-Applikation: unterstützt sind http und https für Applikationen sowie OWA (Outlook Web Access), Web-Server, Mail-Server. Direkter Zugriff erfolgt mit einem Klick im Webportal der ZyWALL SSL 10.
- Applikation: wie Remote Desktop, VNC, Citrix, FTP, usw. Hier ist eine entsprechende Software-Installation notwendig. Der Server-Zugriff erfolgt über eine virtuelle IP-Adresse (z. B. 127.0.0.2).
- Eine Custom-Port-Definition ist für nicht vordefinierte Applikationen möglich.

4. File-Sharing

Zugriff auf die Datei-Verwaltung eines Servers oder NAS (z. B. mit dem ZyXEL NSA-2400).

- Mögliche Aktionen im Webportal der ZyWALL SSL 10: Datei öffnen, kopieren, umbenennen und löschen.
- Die Datei Policy ist auf dem File-Server, NAS definiert.
- Empfehlenswert ist das Szenario ZyWALL DMZ/WLAN inklusive UTM für IDP-/Viren-Prüfung.

5. NetExtender

Wie traditionelle IPSec-VPNs: Dem Client-PC wird ein virtueller Netzwerk-Adapter hinzugefügt, um einen Tunnel zwischen den zwei Endpunkten aufzubauen.

- «Nachteil»: Der Client-Rechner kann das gesamte Netzwerk sehen, darum empfehlenswertes Szenario für ZyWALL DMZ/WLAN mit Firewall-Regel-Prüfung.
- SSL-Client ist auf gleichem Netz wie der Server.
- Administratoren-Recht auf Client-Rechner notwendig, um die virtuelle DFÜ-Verbindung zu starten.
- Bei Windows Vista verhindern die Sicherheitseinstellungen die NetExtender-Funktion.

Application Guide

ZyXEL ZyWALL SSL 10



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 Knowledgebase 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

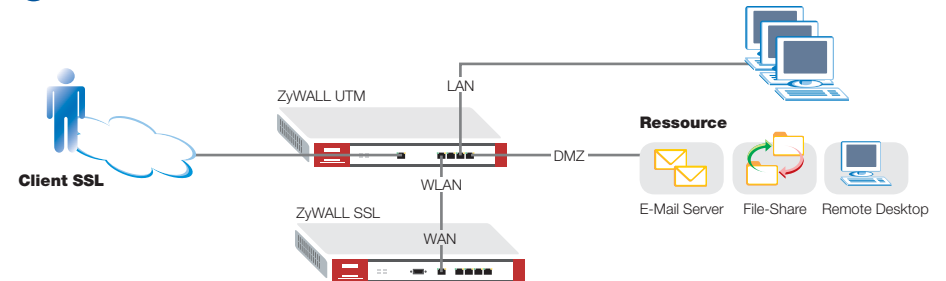
(modem câble/ routeur ADSL en mode pont)

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.



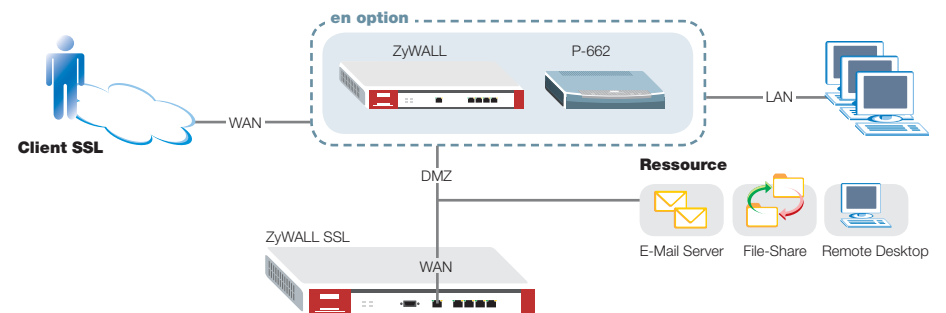
A ZyWALL SSL 10 dans la zone pare-feu particulière



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

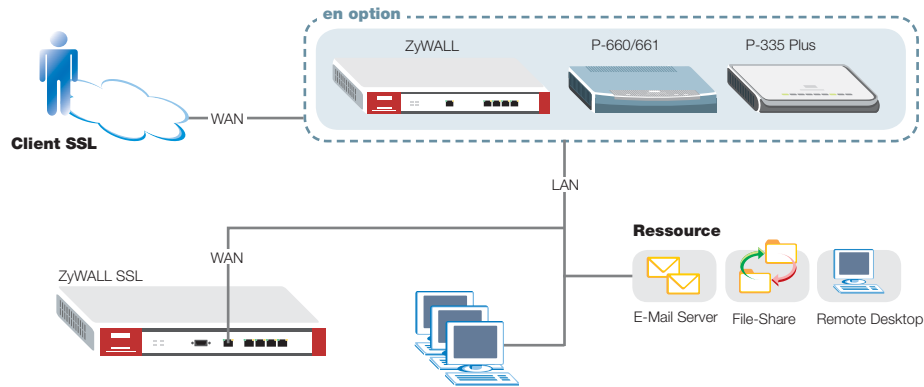


Application : Le ZyWALL SSL 10 est placé en zone DMZ du pare-feu/routeur ADSL (exemple : ZyWALL ou P-662). Ce n'est alors que l'interface WAN du ZyWALL SSL 10 qui est connectée.

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

Options d'application

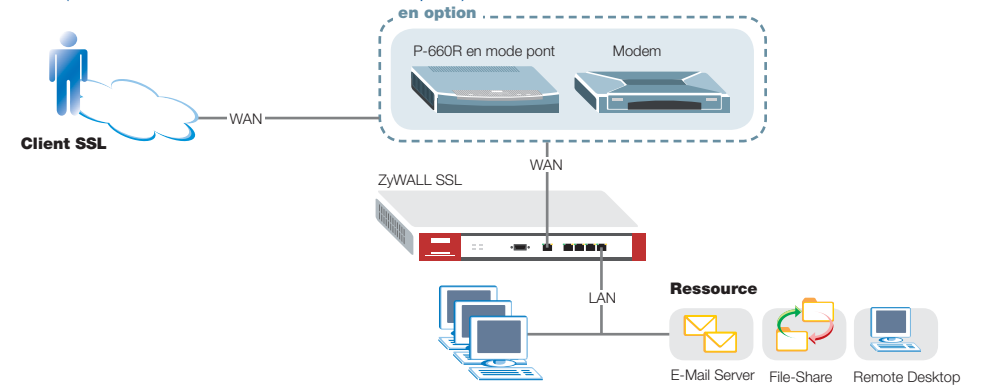
C ZyWALL SSL 10 dans LAN du pare-feu/routeur ADSL/LAN



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.