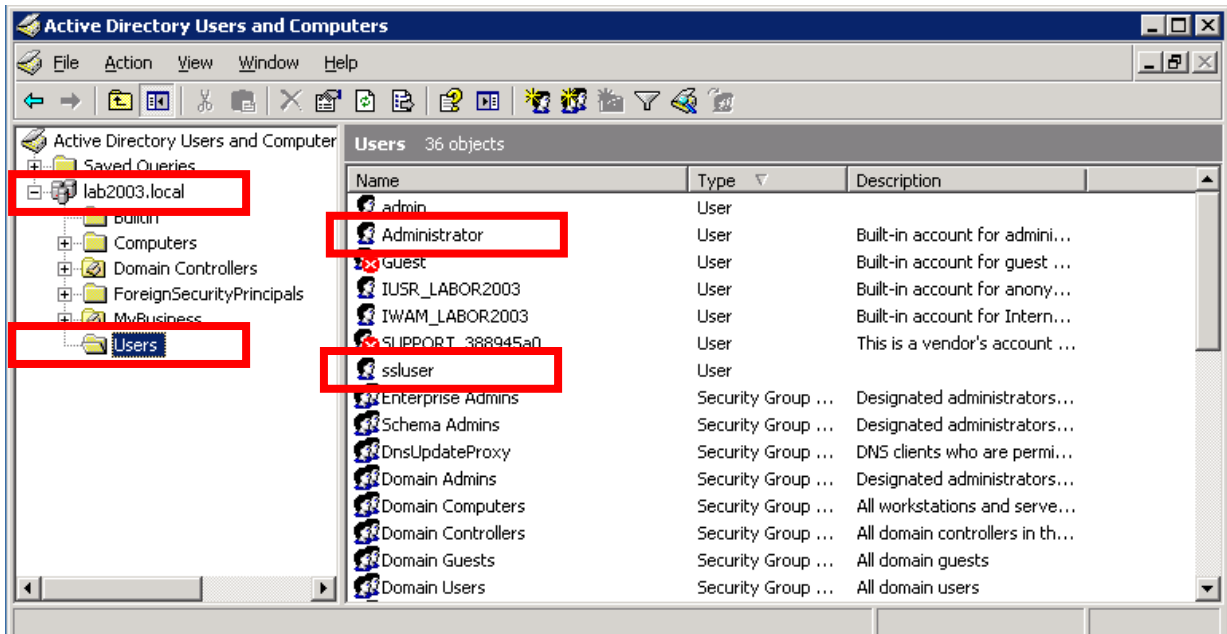


SSL-VPN-Zugang mit Benutzeridentifikation über Active Directory

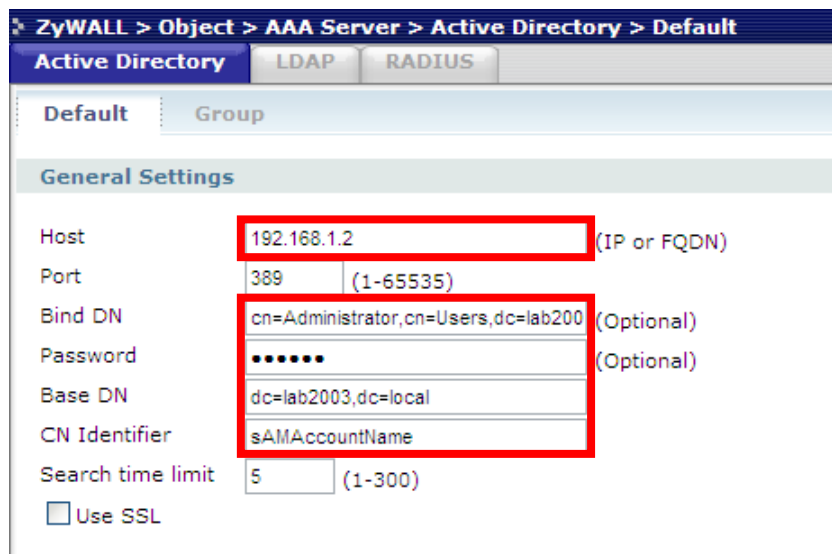
Der SSL-VPN-Zugang lässt sich benutzerabhängig regeln. Zur Benutzer-Identifikation kann Active Directory (AD) von Windows 2003 eingesetzt werden.

Das Konfigurations-Beispiel nutzt folgende Active Directory-Struktur:



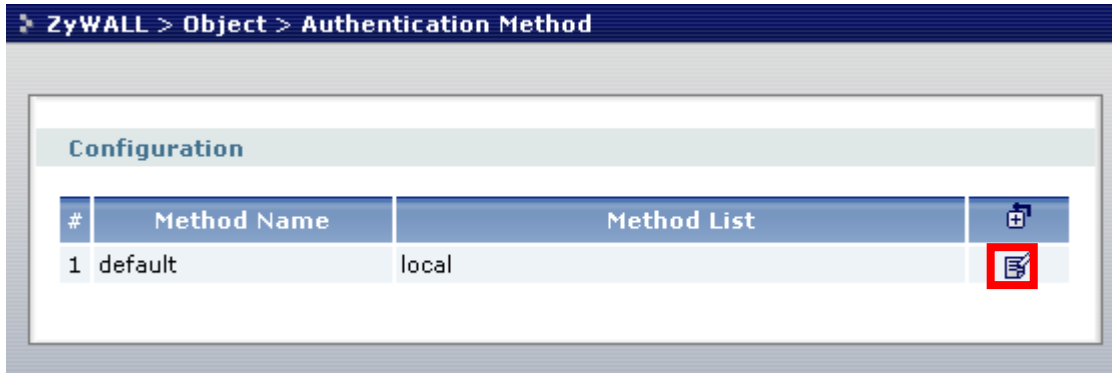
Die AD-Anbindung wird über das Menü *Object > AAA Server* konfiguriert.

Host entspricht der IP-Adresse des AD-Servers. Unter *Bind DN* muss ein Benutzer mit Administrationsrechten auf dem AD-Server verwendet werden. Der Pfad in unserem Beispiel lautet *CN=administrator, CN=Users, DC=lab2003, DC=local*. Das Passwort ist dasjenige des verwendeten Benutzers. Unter *Base DN* wird der Pfad angegeben, auf dem die ZyWALL mit der Suche nach den Benutzern beginnen soll.

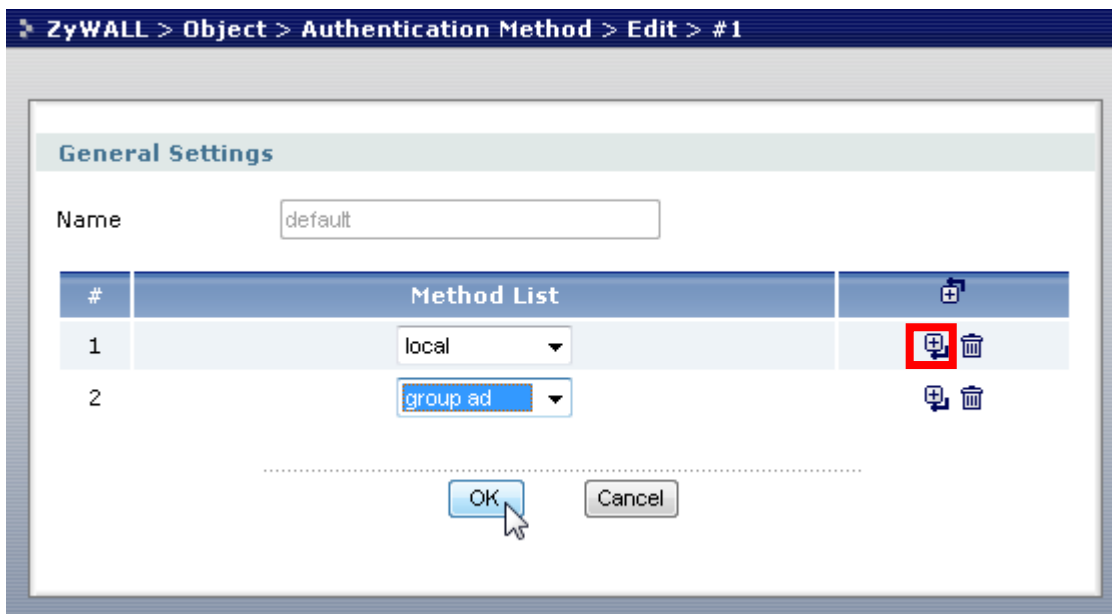


Unter *Object > Authentication Method* ist per Default nur *local* (die lokale Datenbank) aufgeführt. Damit die ZyWALL Authentifizierungs-Versuche von Benutzern die nicht lokal definiert sind an den AD-Server weiterleitet, muss auch die AD-Gruppe *'group ad'* hinzugefügt werden.

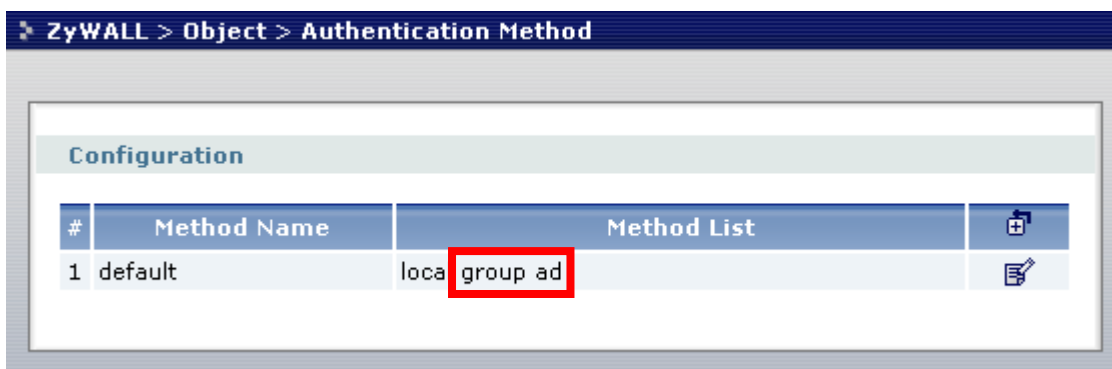
Editieren Sie dazu die Standard-Gruppe *default*:



Fügen Sie über [+]
eine neue Zeile hinzu und wählen Sie *group ad*.



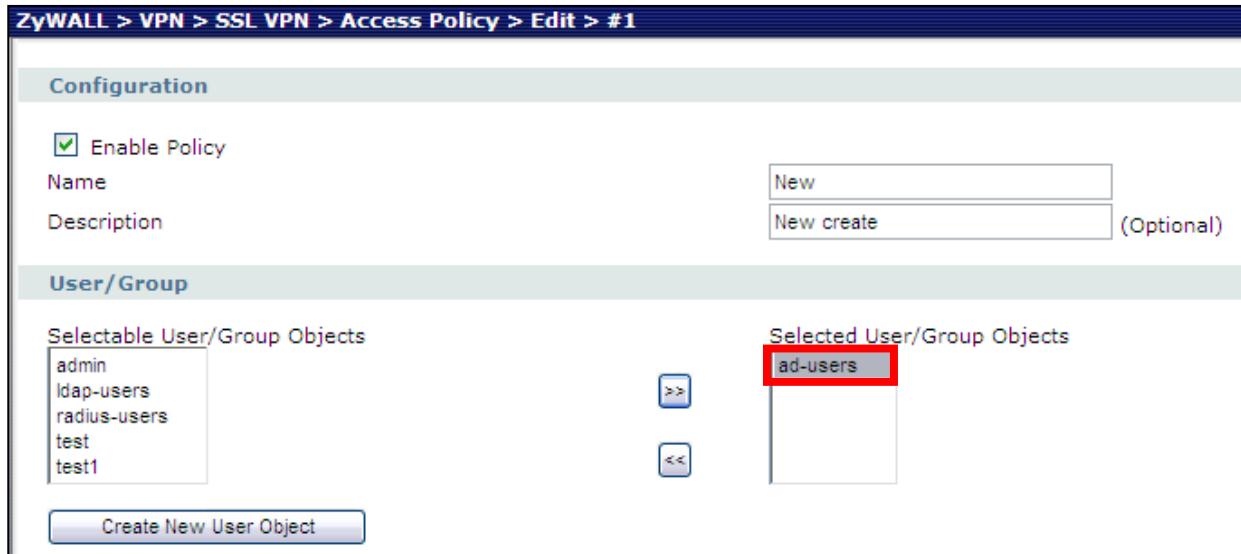
Nach dem Speichern führt die Übersicht auch die Gruppe *group ad* auf:



SSL VPN Regel erstellen:



Die Gruppe *ad-users* zu den ausgewählten Benutzern hinzufügen:



Der SSL-VPN-Login kann nun mit den Benutzerinformationen eines AD-Benutzers erfolgen:

