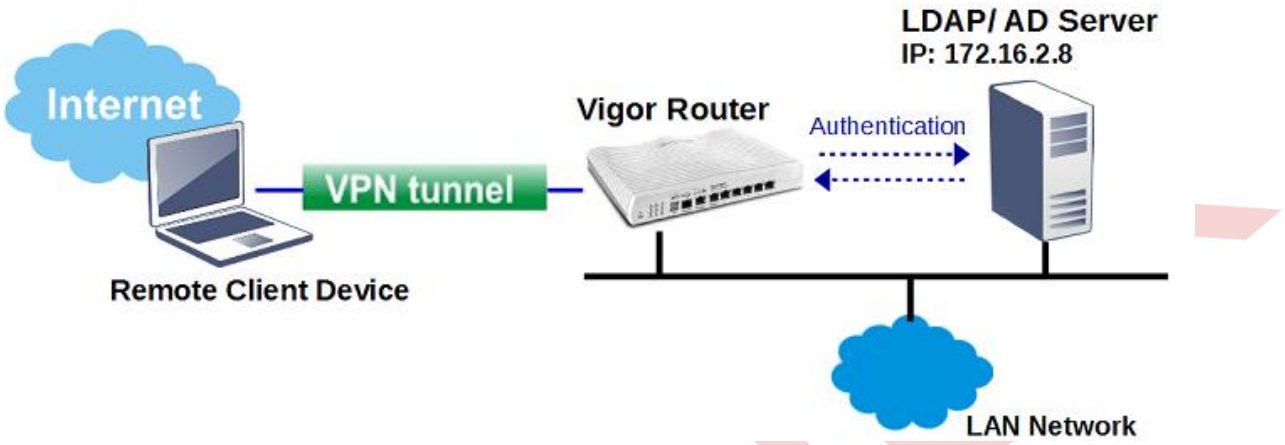
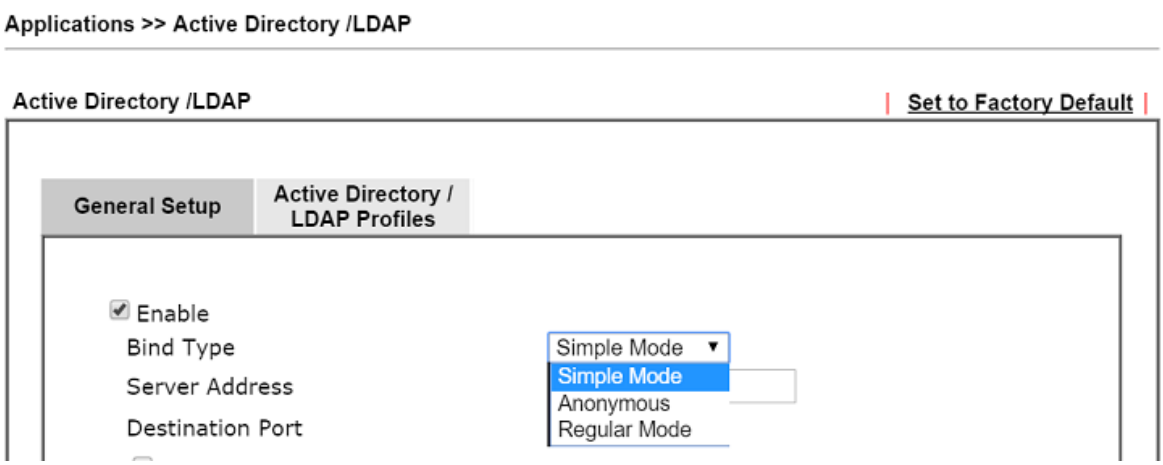
AD/LDAP SERVER İLE UZAKTAN ÇEVİRMELİ VPN İSTEMCİLERİNİ DOĞRULAMA

Vigor Router, PPTP veSSL Remote Dial-in VPN bağlantılarının yerel veri tabanı veya RADIUS, LDAP / AD ve TACACS + dahil olmak üzere harici kimlik doğrulamam sunucuları tarafından doğrulanmasını destekler. Bu makalede, VPN kimlik doğrulaması için harici bir LDAP / AD sunusu kullanma yapılandırması açıklanmaktadır.

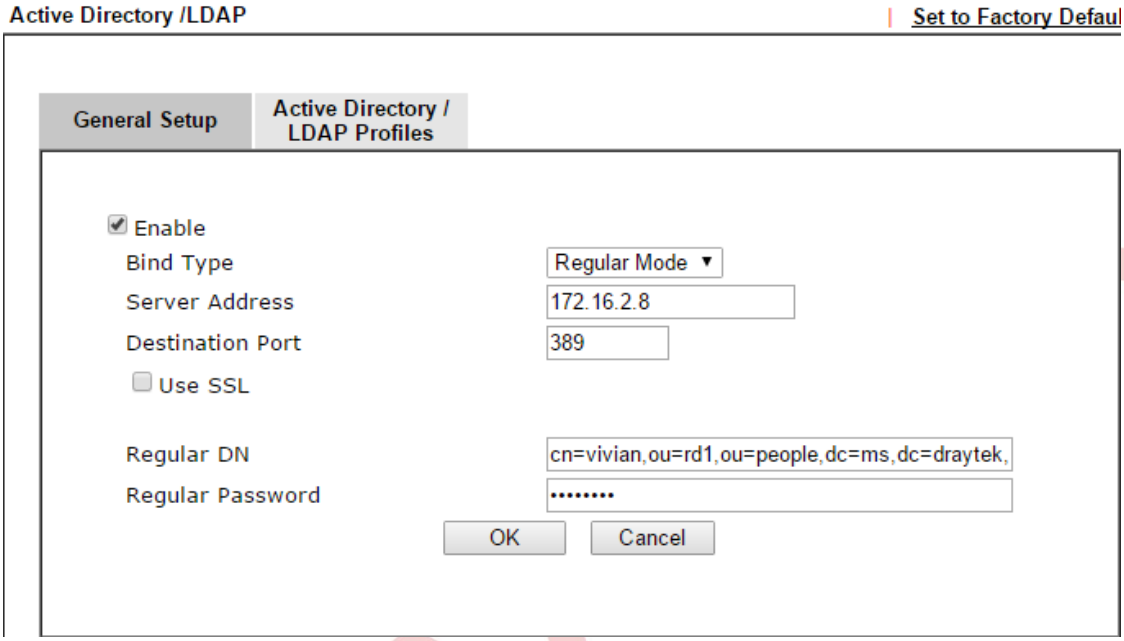


1. **Applications >> Active Directory /LDAP** 'a gidin. **Enable** 'yi tıklayın ve **Bind Type** seçin. Üç tip Bind tip vardır.
   I. **Simple Mode** – genellikle kullanıcıların tümü AD / LDAP sunucusunda aynı klasörde ve seviyede olduğunda seçilir. Routera yalnızca kimlik doğrulaması yapar ancak arama yapmaz.
   II. **Anonymos Mode** – önce anonim modda arama yapar daha sonra kimlik doğrulması yapar. Nadiren kullanılır. Aslında Windows AD sunucusu varsayılan olarak Anonymos hesabın kimliğini doğrulamayı reddediyor.
   III. **Regular Mode** – Genellikle kullanıcılar farklı alt klasörlerdeyken kullanılır. Çoğunlukla Anonymos Modu ile aynıdır, ancak sunucu ilk önce Regular DN ve Regular Password doğrulaması ile arama yetkiniz olup olmadığını kontrol eder. Bu modda routera bu Regular DN ve Regular Password ile Bind isteğini LDAP / AD sunucusuna gönderir. Kimlik doğrulamasını geçtikten sonra routera arama yapar. Daha sonra LDAP sunucusu tam kullanıcının DN'sini farklı alt klasörlerde bulur.

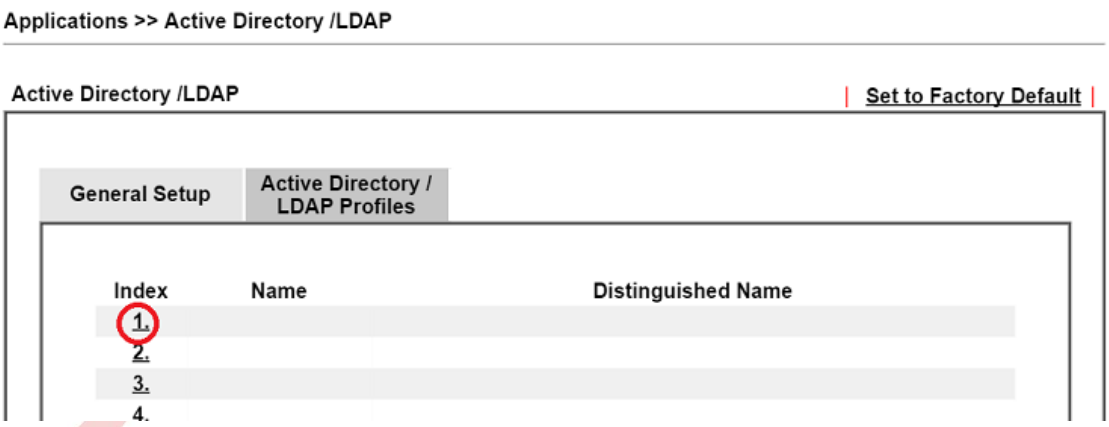
Bu örnekte Regular Modu kullanacağız. DrayTek LDAP sunucusunun OU çalışanları altında OU Çalışanları ve OU RD1, RD2, RD3 olduğunu ve OU RD1, RD2, RD3 altındaki kullanıcıların VPN erişimine izin verildiğini varsayalım.



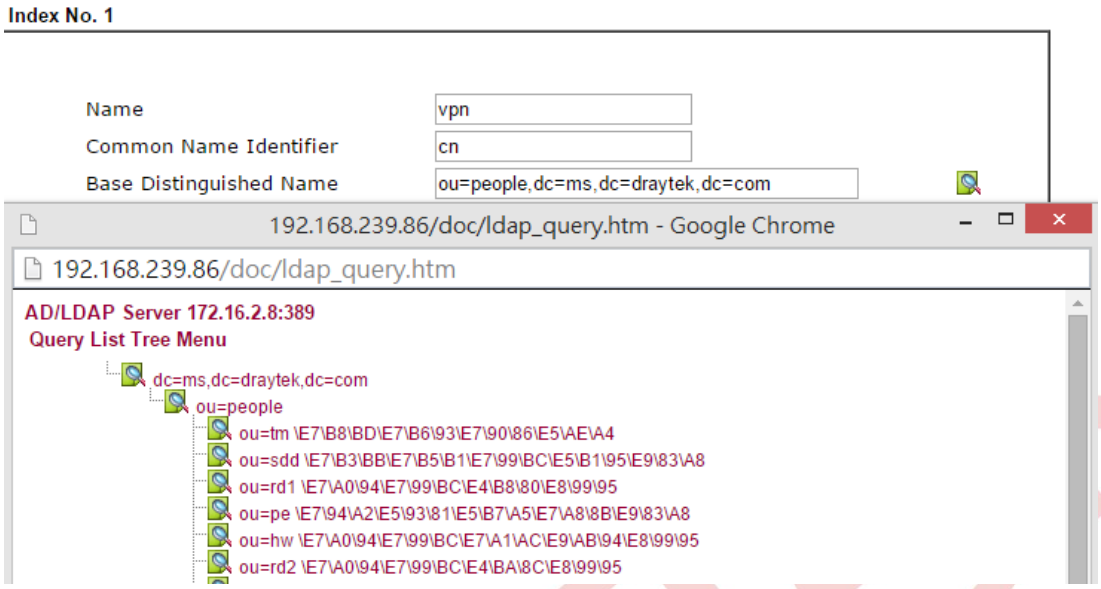
2. LDAP / AD sunucusunun IP adresini **Server Address**'inde girin. **Regular DN ve Regular Password** girin. **OK**'a tıkladıktan sonra Vigor sistemin yeniden başlatılmasını isteyecektir.
   Not: Sahip olduğunuz LDAP sunucusu Windows AD sunucusuysa, her zaman **cn**= Regular DN ile başlatılmasını sağlayın.



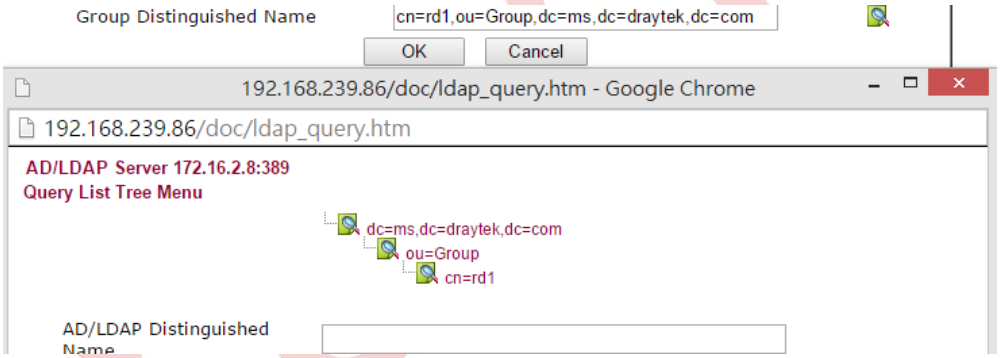
3. LDAP sunucusu profilleri oluşturun. **Active Directory / LDAP** sekmesinde profilini düzenlemek için bir index numarasına tıklayın.



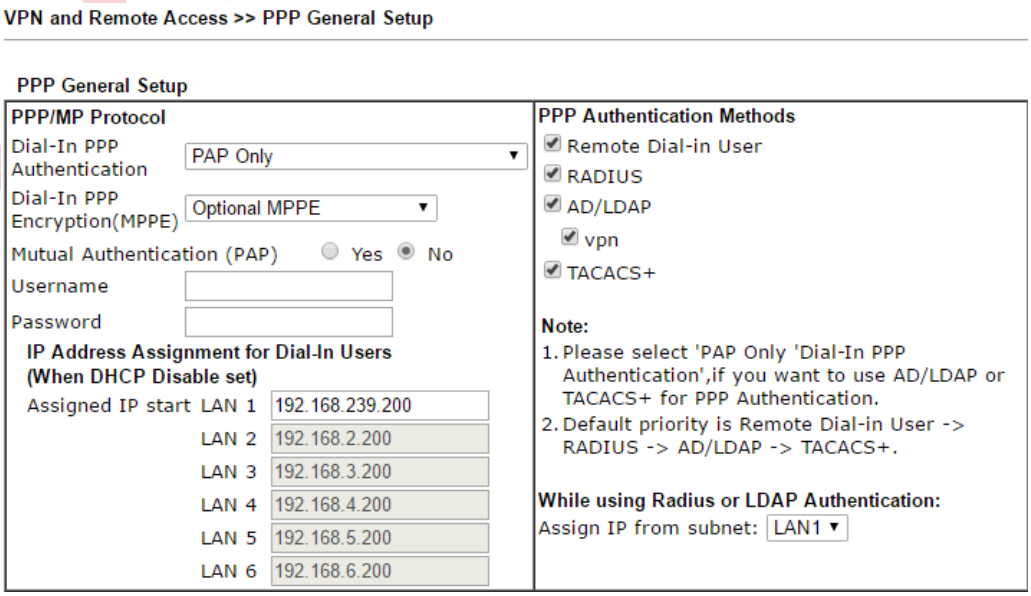
4. Profil için bir **Name** girin. Server routerın kullandığı Regular DN / Password 'ü doğruladıktan sonra **Base Distinguished Name** 'ini hızlı bir şekilde girmek için Arama simgesini kullanabilirsiniz. Bu örneke OU RD1, RD2 ve RD3 altındaki kullanıcıların VPN'e erişmesine izin vermek istiyoruz. Bu nedenle Base Distinguished Name için OU RD1, RD2 ve RD3 içeren OU kişilerini seçiyoruz. Ardından **OK**'a tıklayın.



1. (Isteğe bağlı) Ek filtreleme için DN grubu. Hem Base DN hem de Group DN belirtilmişse, yalnızca her iki yoldaki kullanıcılar da kimlik doğrulamasını geçebilir.



2. Routerı harici sunucu ile Host-LAN VPN'e doğrulamak için yapılandırın. **VPN and Remote Access >> PPP General Setup**'a gidin. PPP Authentication Methods'ta AD / LDAP'ı ve önceki adımlarda oluşturulan profili etkinleştirin.



Yukarıdaki yapılandırma ile uzak VPN istemcileri LDAP sunucusundaki kullanıcı hesaplarıyla VPN kurabilecektir.

Not:

1. 4 PPP Kimlik Doğrulama Yöntemi vardır: Uzaktan Çevirmeli Kullanıcı (yerel veri tabanı), RADIUS, AD / LDAP, TACACS +. Hepsi etkinleştirildiğinde, yönlendirici önce yerel veri tabanını kontrol edecek, eğer uyuşmuyorsa, kimlik doğrulama bilgilerini RADIUS sunucusuna iletecektir. Ardından, RADIUS sunucusunda kimlik doğrulaması da başarısız olursa, LDAP / AD sunucusu.
2. Kimlik doğrulama için LDAP sunucusunu kullanırken, LDAP kimlik doğrulamasının bir sınırlaması olarak, Akıllı VPN İstemcisi ile yapılan aramada PAP'ı seçmeliyiz; bu, şifreleme olmadan kurulan PPTP VPN'e neden olacaktır; bu nedenle, daha yüksek güvenlik için RADIUS kimlik doğrulaması kullanmanız önerilir.

Sorun giderme

Kimlik doğrulama için Windows AD sunucusunu kullanırken, ldp.exe dosyasını çalıştırarak "vpn-user" hesabını test edebiliriz. Windows AD sunucusunun Domain Controller'ına bağlanmak için AD sunucusunda bir Simple Bind gerçekleştirin. AD sunucusundaki Simple Bind çalışıyor ancak VPN hala AD kimlik doğrulamasını geçemiyorsa, lütfen bize teknik@netfast.com.tr adresinden ulaşın ve aşağıdaki bilgileri sağlayın.

- LDAP / AD sunucusundaki wireshark paketleri
- AD / LDAP sunucusundaki Kullanıcı hesabının ekran görüntüleri
- Routerdaki LDAP / AD yapılandırmalarının ekran görüntüleri
- Routerın uzaktan yönetim bilgisi
- LDAP / AD sunucusundaki test için bir hesap / şifre