OpenVPN Neden Tercih Edilmelidir?

- OPENVPN Neden Tercih Edilmelidir?

OPENVPN Neden Tercih Edilmelidir?

Aşağıda OpenVPN'in neden tercih edilmesi gerektiği listenlenmiştir.

· OpenVPN'in başlıca güçlü yanları: Bilinen sistemlerin çoğunda çalışabilmesi, yüzlerce veya binlerce istemciye ölçeklenebilmesi, nispeten kolay kurulumu ve dinamik IP adresleri ile NAT desteğini içermesidir.

· OpenVPN, özelleştirmeleri kolaylaştırmak amacıyla siteye özgü özelleştirmeleri destekleyen genişletilebilir bir VPN çerçevesi sunar. Örneğin, özelleştirilmiş bir kurulum paketini istemcilere dağıtma özelliği veya X509 sertifikası tabanlı kimlik doğrulama ile birleştirilebilen OpenVPN'in eklenti modül arabirimi (örneğin, openvpn-auth-pam modülü OpenVPN'in istemcileri herhangi bir PAM kimlik doğrulama yöntemi kullanarak kimlik doğrulamak için kullanılmasını sağlar) sunar.

· OpenVPN, bir OpenVPN hizmetini uzaktan kontrol etmek veya merkezi olarak yönetmek için kullanılabilecek bir yönetim arabirimi sunar. Yönetim arabirimi ayrıca OpenVPN için bir GUI veya web tabanlı bir ön yüz uygulaması geliştirmek için kullanılabilir.

· Windows'ta OpenVPN, Windows Crypto API'yi destekleyen sertifikaları ve özel anahtarları okuyabilir.

· OpenVPN, hem pasif hem de aktif saldırılara karşı koruma sağlamak üzere tasarlanmış endüstri standardı bir güvenlik modeli kullanır. OpenVPN'in güvenlik modeli, oturum kimlik doğrulaması için SSL/TLS ve güvenli tünelleme için IPSec ESP protokolünü kullanır. OpenVPN, oturum kimlik doğrulaması için X509 PKI (genel anahtar altyapısı), anahtar değişimi için TLS protokolü, tünel verilerini şifrelemek için OpenSSL'e bağımsız şifreleme sağlayan EVP arabirimini ve kimlik doğrulamak için HMAC-SHA1 algoritmasını destekler.

· OpenVPN, taşınabilirlik için tasarlanmıştır. Bu yazının yazıldığı sırada, OpenVPN Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X ve Windows (2000/XP ve sonraki sürümler) üzerinde çalışır. OpenVPN, bir çekirdek modülü veya IP katmanına karmaşık bir değişiklik olmadan bir kullanıcı alanı hizmeti olarak yazıldığı için taşıma çabaları dramatik olarak basitleştirilir.

· OpenVPN kullanımı kolaydır. Genel olarak, bir tünel, bir komutla oluşturulabilir ve yapılandırılabilir (ve herhangi bir yapılandırma dosyasına gerek olmadan). OpenVPN'in belgeleri, kullanım kolaylığını gösteren örnekler içerir.

· OpenVPN, güvensiz ağlarda güçlü bir şekilde çalışacak şekilde tasarlanmış ve test edilmiştir. OpenVPN'nin önemli bir tasarım hedefi, IP katmanının hem normal işlemler hem de hata

iyileştirmesi açısından yanıt verdiği gibi yanıt vermesi gerektiğidir. Bu, IP katmanı 5 dakika boyunca devre dışı kalırsa, devre trafiği hemen yeniden başlayacak anlamına gelir.

· OpenVPN, güçlü bir modüler tasarıma sahiptir. Tüm şifrelemeler OpenSSL kütüphanesi tarafından işlenir ve tüm IP tünelleme işlevselliği TUN/TAP sanal ağ sürücüsü ile sağlanır. Bu modülerliğin faydaları, örneğin OpenVPN'in yeni bir OpenSSL kütüphanesi sürümüyle dinamik olarak bağlandığı ve hemen yeni sürümde sunulan herhangi bir yeni işlevselliğe erişimi olduğu şekilde görülebilir. OpenVPN en son OpenSSL (0.9.7) sürümü ile derlendiğinde, otomatik olarak AES-256 (256 bit anahtarlı Advanced Encryption Standard) gibi şifreleme, şifre çözme ve kimlik doğrulama performansını optimize etmek için özel amaçlı donanım hızlandırıcıları kullanmayı mümkün kılan OpenSSL'in şifre bağımsız EVP arabirimini kullanma özelliğine sahiptir. Aynı şekilde, OpenVPN'in kullanıcı alanı tasarımı, TUN/TAP sanal ağ sürücüsü içeren herhangi bir işletim sistemine kolayca taşınmasına olanak tanır.

· OpenVPN, VPN tünelinin güvenlik parametrelerini kontrol etmek için birçok seçenek sunsa da sunucunun kendisini koruma seçenekleri sunar, örneğin OpenVPN daemon'ın erişim hakkına sınırlama getiren --chroot, başlatmadan sonra daemon ayrıcalıklarını düşürmek için --user ve --group ve anahtar malzemesini kullanır.