Yazıyı PDF Yapan : Seyhan Tekelioğlu
seyhan@hotmail.com – http://www.seyhan.biz

VPN

VPN (Virtual Private Network)
Ağ teknolojilerindeki düzenli gelişmelere rağmen, kurumların hedefi daha hızlı ve daha verimli haberleşme olanaklarını kullanabilmektir. Personel ve yöneticiler dünyanın neresinde olurlarsa olsunlar, yerel ağlarına sanki ofislerindeymiş gibi erişebilmek isterler.
1980 ortalarında ve 1990 başlarında hedeflerine ulaşabilmeleri için uygulanan teknoloji telefon hatlarını kullanarak uzak erişim servisleriydi. Şirketler, yöneticilerinin taşınabilir bilgisayarlarına veri sıkıştırabilme yeteneğine sahip hızlı modemler yerleştirip, ofisteki sunuculara bağlanabilmelerini sağlayabilirler. Çalışanların ve yöneticilerin yapması gereken sadece bulundukları ortamda RJ-11 telefon konnektörünü modemlerine takmak ve uzak erişim sunucularına şifreleri yetkisinde bağlanabilmektir.
1990 sonlarında kurumlar, uzak erişimin şirketlerine sağladığı avantajları daha çok anlamaya başladılar ve bazı büyük şirketler, ülke içinde ücretsiz aranabilecek telefon numaraları ile çalışanlarına bu hizmeti sunabildiler. Uluslar arası ticaret yapan kurumlarda ise, milletlerarası telefon ödemeleri söz konusu olduğu için uzak erişim servisleri şirketlere ciddi bir maliyet getirmektedir.
Internet üzerinden paylaşılmış veri ağlarına erişebilmek, o bölgedeki yerel internet servis sağlayıcının aranması söz konusu olduğundan uzak bağlantılarda ödenen ücretler büyük ölçüde düşecektir. Hatta Asia Online, Amrica Online veya IBM gibi internet servis sağlayıcıları, tüm dünyaya yayıldıkları için, aynı kullanıcı adı ve şifre ile dünyanın çoğu yerinden yerel POP numaraları aranarak internete erişilebilir.
Sanal ve özel ağlar (VPN), yerel internet servis sağlayıcı ve kurumsal yerel ağlar arasında güvenli bir tünel üzerinden veri iletimi gerçekleştirerek çalışır. Shiva gibi bir çok ağ donanımı üretici internet gibi, paylaşılmış veri ağları üzerinden tünelleme ve şifreleme yapabilme yeteneğine sahip donanımları piyasaya sunmaktadır. Kurumsal ağlarını daha önceden bir takım güvenleri nedeni ile internete bağlamayan şirketleri yeni VPN teknolojileri ile güvenli bağlantılar sağlayabilecekler.
VPN Ekonomisi
Uzak erişimin maliyeti göz önüne alınırken, aramanın nereden kaynaklandığı çok önemlidir. Örneğin, kullanıcıların kendileri aile aynı şehirde bulunan uzak erişim sunucularını arayarak ağa erişmeleri için en ideal çözüm direk telefon hatlarını

kullanmak olabilir. Söz konusu işlem şehirlerarası veya milletlerarası aramayı gerektiriyorsa, VPN'in sağlayacağı maliyet hesapları çok daha düşük olacaktır.
Sanal ve özel ağ kavramı, bazı frame relay servisi sağlayan telefon şirketleri tarafından pazarlama amaçlı yanlış olarak belirtilmektedir. Bu şebekelerde kullanıcıların verileri özel paket anahtarlama devreleri ile birbirinden ayrılır ve ortada sanal olarak oluşturulan bir kavram yoktur, fakat veri güven altına alınır. Ücretlendirme ise kiralık hatlar gibi kapalı sistemlerle rekabet edecek derecede yüksektir.
İlk uzak erişim teknolojileri, her bir paketi şifreleme esasına dayanıyordu. Bu teknoloji, VPN teknolojisinin özelliklerinden sadece biridir. LAN ve WAN yönlendiricileri arasına özel şifreleme ve veri sıkıştırma donanımları yerleştirilerek, verinin paylaştırılmış ağa çıkması sağlanıyordu. Bu ürünlerin çoğu tescilli olmayan IP adresleri ile iletişimi engelliyerek çalışıyordu.
VPN ağlar, herkesin ulaşabileceği paylaştırılmış ağlarda, yetkilendirilmiş ve şifrelenmiş tünellerden oluşur. Tüneller ağ erişim noktaları (Shiva LanRover Access Switch® gibi) ile verinin iletileceği ağda kullanılacak tünel sonlandırıcı donanımlardan oluşur.
Ağ erişim noktasının görevi, kullanıcılardan gelen paketleri kapsüle ederek verinin güvenli bir şekilde iletilmesini sağlamaktır. Günümüzdeki uygulamalar, bu işlem için PPTP (Point-toPoint Tunneling Protocol) ve L2F (Layer Two Forwarding) protokollerini kullanır. PPTP, internet servis sağlayıcı tarafından akış kontrolü gibi görevlerle kullanılırken, L2F protokolünün kullanımı daha kolaydır ve yönetilebilir ağlara daha uygundur. Bu iki protokolün en iyi yönleri ele alınarak L2TP (Layer Two Tunneling Protocol) adı verilen bir protokol ortaya çıkmıştır. Bu protokolün çoğu üretici tarafından desteklenmesi bekleniyor. L2TF protokolü, özelleştirilmiş protokoller ile kullanıldığında internet üzerinden güvenli tüneller kurmamızı sağlayacaktır.
VPN Güvenliği Çözümleri
Günümüzdeki VPN çözümleri iki noktaya odaklanmaktadır; şifre doğrulama ve veri güvenliği. Kullanıcıların yetkilendirilmesi işlemi en iyi verinin kaynaklandığı yerel ağda gerçekleştirilebilir. Bu sayede kullanıcı veri tabanının servis sağlayıcıya taşınmasına gerek kalmaz. En temel şifre doğrulama protokolleri PAP (Password Athentication Protocol), CHAP (Challenge Handshake Athentication Protocol) ve SPAP (Shiva Password Authentication Protocol) protokolleridir. Daha güvenli şifre doğrulama çözümleri ise, zamanla senkronize edilmiş anahtarları ve dijital sertifika gibi gelişmiş teknolojileridir.
Veri güvenliği, arama yöntemi ile uzaktaki ağa bağlanan kullanıcıların verilerinin, bütünlük bozulmadan uzak ağa iletilebilmesini sağlamalıdır. IPSec protokolü, güçü bir şifreleme sağlarken, veri bütünlüğünü de garanti eder. IPSec protokolü ile farklı şifreleme metodları kullanılabilir; bunlardan en popüleri DES, (Digital Encryption Satandart) Dijital Şifreleme Standardıdır.

Farklı VPN Konfigürasyonları

En genel konfigürasyon, ağ erişim sunucusu ve yerel ağda bulunan tünel sonlandırıcı bir donanımdan oluşur. Kullanıcı gözü ile baktığımızda görünen, ISS yerel telefon numaralarının aranması, internet servis sağlayıcı tarafından şifremizin doğrulanması ve servis sağlayıcı tarafından güvenli bir tünel oluşturularak kurumsal yerel ağımıza erişebilmemizdir. IPX ve IP paketleri, PPTP veya L2TF protokolleri ile kapsüle edilir, verinin gideceği ağın adresi belirtilerek yeni bir IP paketi yaratılır. Kullanıcı, internet servis sağlayıcıyı aradığında, kendisine tescilli bir IP adresi verilerek yerel ağına bu adres ile ulaşması sağlanır. Kapsüle edilmiş paketler daha sonra uçtan uca IPSec veya eşdeğer bir protokol ile şifrelenebilir.

Veri, VPN tünelinde paketlenip, şifrelenip, diğer uçta paketten çıkartılıp ve şifresinin çözülmesi işlemlerinden VPN kullanıcısı haberdar olmaz. Görünen klasik bir internet'e bağlantı şeklidir. Kullanıcın bu tip ağ teknolojilerini bilmeye gereksinimi olmaması ve konfigürasyon sorunu yaşamaması, bu tip uygulamaları kolaylaştırır. Yukardaki örnekte, şifreleme ve paketlerinin internet servis sağlayıcı yerel POP istasyonu tarafından gerçekleştiğine değinilmişti. VPN teknolojisi, network erişim sunucu veya istemcilere entegre edilebilir. Bunun için istemcilere VPN arama yazılımı kurulabilir. Bu yöntemde ise internet servis sağlayıcı bağımsız bir uygulama görüyoruz. Kullanıcı dilediği internet servis sağlayıcı üzerinden güvenli bir tünel oluşturabilir. Farklı bir uygulama ise, bu yazılımın kullanıcıların PC'lerine yüklenmeden de yaratılabilir. Bu durumda VPN teknolojisinin, internet servis sağlayıcı ağ erişim sunucusu tarafından desteklenmesini gerektirir.

Kullanıcıların, internet servis sağlayıcı bağımlı veya bağımsız çözümlerde ISS'ten yeterli sayıda ve meşgul olmayan telefon numaraları sağlamasını istemeleri gerekir. İstemcilerde VPN yazılımı kullanılmayacaksa, ISS ağ erişim sunucunun VPN destekleyip desteklemediği sorulmalıdır.

İnternet servis sağlayıcı bağımsız modelde, yetkilendirme işlemi VPN destekleyen yazılım ile gerçekleştirilir. İnternet servis sağlayıcı sadece kullanıcı ile kendi uzak erişim sunucusu arasındaki asenkron hattı sağlar. Tünel ise kullanıcı ile erişeceği ağ üzerinden bulunan tünel sonlardırıcı donanım arasında kurulur.

Uzak erişim çözümleri yaratırken bilgi işlem müdürleri, performans, güvenlik, ağ yönetimi, erişim kontrolü, esneklik ve maliyet gibi faktörleri göz önüne almalıdır. Ayrıca internet servis sağlayıcı bağımlı çözümlerde, kullanıcıların VPN desteği verebilen internet servis sağlayıcılar ile sözleşme imzalaması gerekmektedir. Internet servis sağlayıcı bağımsız modelde ise, internet servis sağlayıcı paketlerin iletimine sadece bir vesile olduğu için, tünelleme işlemi bilgi işlem bölümü tarafından daha esnek bir şekilde yapılabilir.

Bilgi işlem yöneticileri, hangi model üzerinde seçim yapmaları gerektiğini aşağıdaki faktörlere göre karar vermelidir.

Performans

Ağ performansını etkileyen en önemli etkenler paket kaybı ve ortaya çıkabilecek gecikmelerdir. Sadece text tabanlı ve grafiklerin iletildiği bir çözümde, paket kaybı, ve gecikme çok fazla sorun çıkarmayacaktır ve kullanıcının işlemi yerine getirmek için bekleme süresini arttıracaktır. Fakat çoklu-ortam ve video konferans gibi zaman kritik uygulamalarda, verinin gecikmeye uğramadan iletilmesi gerekir.

Günümüzde internet servis sağlayıcılar, 10 abone için sadece 1 adet modem donanımı yatırımı yapmaktadır. Kurumsal uzak erişim çözümlerine bu oranın 5-1, hatta her bir kullanıcı için bir modem atanması gerekebilir.

Internet servis sağlayıcı bağımsız modelde, tünel sonlandırıcı donanımların, şifreleme ve sıkıştırma işlemleri için ayrı işlemciler. Bu tür çözümlerde ana işlemci tünelleme ve yönlendirme işlemlerini yerine getirirken, veri sıkıştırma ve şifreleme işlemleri performansın düşmesine yol açmaz.

Güvenlik

VPN güvenliği iki noktada incelenmelidir; şifre doğrulama ve veri güvenliği. Bazı servis sağlayıcılar iki adet kullanıcı yetkilendirme işlemi gerçekleştirmektedir. Bunlardan bir tanesi, ISP yerel POP'unda, bir diğeri ise kurumun yerel ağında gerçekleşir. Kullancılar için için, çok sayıda kullanıcı adı ve şifre hatırlamak zor olabilir. Veri güvenliği aynı zamanda, uzak kullanıcı tarafından gönderilen verinin, kurumsal ağa değişikliğe uğramadan iletilmesini, yani verinin bütünlüğünü içerir.

Ağ Yönetimi ve Erişim Kontrolü

Ağ yönetim yazılımları, bilgi işlem yöneticilerine tek bir merkezden, ağları üzerinde bulunan farklı donanımlarını gözlemlemelerini ve gerektiğinde bunların konfigürasyonlarını, kullanıcıların isteğine uygun olarak değiştirebilmelerini sağlar. Internet servis sağlayıcı bağımlı modelde, bilgi işlem yöneticileri VPN donanımlarını yönetme şansına sahip değillerdir ve konfigürasyon değişikliği gerektiğinde hizmet aldıkları servis sağlayıcıya başvurmaları gerekir.

Servis sağlayıcı bağımsız modelde ise bilgi işlem yöneticisi, farklı ağ yönetim araçları ve uygulamaları kullanarak, konfigürasyonlarına anında müdahale etme şansı vardır.

Ücretlendirme

Her iki VPN yönteminde de, kurumun bir servis sağlayıcı ile internete bağlanması gerekmektedir. Ücretlendirme, servis sağlayıcı firmanın kullanmakta olduğu VPN donanımı, ve bunların bakım ücretlerine göre artabilir. Servis sağlayıcı bağımsız model ise daha ekonomik görünmektedir.

Maliyet

VPN çözümleri, şehirlerarası ve milletlerarası telefon bağlantılarına son verdireceğinden, VPN'e yapılacak olan yatırım kısa sürede kendini amorte edecektir. Toplam sahip olma maliyetiniz düşer.

Esneklik ve optimizasyon

Uçtan uca bağlantılar : Kullanıcıların taşınabilir veya ev PC'leri ile kurumsal yerel ağ arasında iletişimin sağlıklı bir şekilde kurulabilmesi için, VPN yazılım ve donanımlarının birlikte çalışabilmeleri için uyarlanmaları gerekir.
Mevcut ağ yapısı ile entegrasyon : Bazı servis sağlayıcılar ile bağlantıda, mevcut ağ yapısı üzerinde bir değişiklik gerektirmezken, bazıları ise router'larında yazılım güncellemeleri veya tamemen yeni WAN arabirimine geçiş yapılmasını gerektirir. Ağ yönetimi ve gözlemlemesi için özel yazılımlar kurulabilir.
Esneklik : Kurumların ağları, işlerinin değişmesi, yeni yatırımlar, farklı sektörlere atılmaları gibi nedenlerle, ihtiyaçları cevap verebilmek amacıyla zamanla değişir. İş gereksinimleri değişikliğe uğradıkça mevcut uzak erişim çözümlerimiz buna ayak uydurabilmelidir. Servis sağlayıcıları çözümden çok ürün önerebilir ve bu ürünlerin gelişmemize ayak uydurabilmeleri ve esnek olmalarına dikkat etmeliyiz.
Ölçeklenebilirlik ve terfiler : Servis sağlayıcılar, kullanıcılarına sorunsuz ve ölçeklenebilir hizmet verebilmeliler. Örneğin bugünkü donanımı 1000 kişinin aynı anda bağlanabilmesini destekleyen bir servis sağlayıcı, mevcut donanımına eklentilerle daha fazla kullanıcıya destek verebilmelidir.
Internet Servis Sağlayıcı bağımsız modelin sağladığı avantajlar
VPN'i servis sağlayıcı bağımsız model ile kullanmanın dört önemli avantajı vardır.
Güvenlik : Internet servis sağlayıcı modelde, şifreleme ve sıkıştırma işlemleri ISS tarafından yapıldığı için tüm önemli verimizi, ISS'in yönetimine bırakmamız, verilerimizi tehdit edebilir.
Ağ Donanımı Optimizasyonu : Bilgi işlem yöneticileri, VPN donanımlarını kendi ağlarında kullanabilecekleri için, gerekli konfigürasyon değişikleri anında ve istenildiği gibi yapılabilir.
Daha az bağımlılık : Internet servis sağlayıcı bağımsız modelde, kullanıcılar, kolayca ISS'lerini değiştirebilirler veya farklı ISS'ler ile yedek bağlantılar gerçekleştirebilir.
Sonuç
Sanal ve özel ağlar teknolojisini kullanarak, dünyanın neresinde olursak olalım, internet üzerinden, yerel ağımıza oldukça ekonomik bir şekilde bağlantı kurabiliriz. Herkesin girebildiği internet gibi paylaşılmış bir ağda yaşayacağımız problemler güvenlik çözümleridir. Güvenlik sorunları internet üzerinden şifreleme teknikleri kullanılarak güvenli yollar oluşturularak çözülebilir. Bu konuda ki ağ donanım üreticileri VPN adı verilen çözümlerini piyasaya sunuyorlar. Intel tarafından geçtiğimiz aylarda satın alınan Shiva firması VPN konusunda öncü firmalardan biri ve bu birleşmeden sonra daha yüksek bir sermaye ile VPN ürünlerine yatırım yapılıyor.