GÜVENİLİR SANAL ÖZEL INTRANET

Sinan ÛZCAN*

* SİMKO A.Ş.
Elektronik Müh.

Internet standardlarının açık yapısı iş ve hükümet kesimi kullanıcıları için bir açmaz yaratmaktadır. Bu açık yapı bir yandan farklı sistemler arasında iletişim imkanı yaratırken diğer taraftan emniyet ve veri bütünlüğü problemlerinin oluşmasında bir potansiyel yaratmaktadır. Bu nedenle başta iş ve hükümet kesimi olmak üzere yaptıkları iş gereği gizlilik ve kesintisiz iletişim ihtiyacı duyan kesimler kendi kuruluşları dahilinde intranet'ler kurup işletmeye başlamışlardır. Intranet altyapı olarak internet teknolojisini kullanan ancak belli bir kuruluş dışında dış dünyaya bağlantısı olmayan kapalı bir şebekedir. Intranetler vasıtasıyla bir şirketin dağınık veri tabanlarına farklı noktalardan, farklı yazılım ve donanım platformları üzerinden erişim ve dahili emniyetli elektronik posta gibi uygulamalar yapılabilir. Örneğin bir şirket yöneticisi basit bir standart browser kullanarak şirketinin personel kayıtlarını, stok durumlarını vs. takip edebilir. Intranetlerdeki emniyet ihtiyacı yakın zamana kadar bu şebekelerin pahalı kiralık devreler üzerine kurulmasını zorunlu kılmıştır. Ancak internetin baş döndürücü bir hızla gelişmesi ve erişim maliyetlerinin düşüklüğü iş ve hükümet çevrelerinin özel data şebekelerini kiralık hatlardan internete taşımalarına ya da sanal özel intranetler (Virtual Private Intranet) kurmalarına neden olmaktadır.

Sanal özel şebeke kavramı aslında yeni bir kavram değildir. Pek çok telekomünikasyon işletmesi, pazarın ilgi ve baskısından dolayı, sanal özel telefon şebekeleri ve Frame Relay teknolojisine dayalı sanal data şebekeleri kurmuşlardır. Sanal özel intranet kurmak bir kapalı kullanıcı grubu için data şebekesine emniyetli WWW sunucu ve emniyetli uygulamalar ekleyerek genel internet erişimi ve omurga şebekesinin genişletilmesi demektir.

Güvenli sanal özel intranetlerin (Secure Virtual Private Intranet) kurulması için PPTP protokolü (Point to Point Tunelling Protocol) geliştirilmiştir. PPTP protokolünü kullanarak uzaktaki bir kullanıcı lokal bir internet servis sağlayıcı üzerinden ve sadece internet şebekesini kullanarak şirketinin özel network'üne girebilir ve kendi masasındaymışçasına işlemlerini emniyetle yapabilir. Sanal özel şebeke (Virtual Private Network-VPN) teknolojisi kullanıcıların internet üzerinden emniyetli ve şifrelenmiş iletişim kurmalarına yönelik ekonomik ve kolay bir çözümdür. Burada güvenli sanal özel intranet bir uygulama ve PPTP bu uygulamanın yapılabileceği bir protoküldür. Bunu bir başka internet/intranet uygulamasına benzetecek olursak SMTP bir e-mail uygulaması yapabilmek için gerekli protokollerden biridir.

PPTP forumunu oluşturan şirketler IETF (Internet Engineering Task Force)'in Haziran 1996 toplantısında PPTP'yi IETF'in PPP geliştirme çalışma grubuna taslak standart olarak sunmuşlardır. Çalışma grubu PPTP ve Cisco tarafından geliştirilen L2F (Layer 2 Forvvarding) yaklaşımını birleştiren bu öneriyi

benimsemiştir. PPTP teknik spesifikasyonu güncellenmiş olup şu anda IETF Internet taslağı olarak mevcuttur. Örnek kaynak kodlarda WWW erişimine açılarak üreticilerin çeşitli işletim ve donanım platformlarında PPTP çözümleri üretmelerine yardımcı olunmaktadır. Endüstri kuruluşları da bu gelişmeyi önceden bir takım özel tünel protokolleri olmasına rağmen bir standardın eksikliğinin duyulması nedeniyle olumlu karşılamaktadırlar. Bu standarda doğru gidiş erişim sistemleri sağlayıcıları ve firevvall üreticilerine müşterilerine yeni Katma Değer Servisler sunmaları için bir fırsat yaratmaktadır.

Bir sanal özel şebeke (VPN) önceden sadece özel şebekeler ile sağlanabilen emniyet ve diğer özellikleri internet ya da başka bir kamu şebekesi üzerinden kurulan bir tünelden geçirerek sunan bir şebekedir. Örnek olarak evindeki ya da yoldaki bir mobil kullanıcının kamu şebekesini kullanarak şirketinin sunucusuna bağlanabilmesini sağlar. Sanal özel şebeke bir kuruluşun bölge büroları ya da diğer şirketler ile emniyetli bir PPTP bağlantısı üzerinden haberleşmesini sağlar. Kullanıcı açısından bakıldığında tünelle geçilen şebekenin fiziksel özellikleri bir önem taşımaz çünkü data sanki tahsis edilmiş özel bir devreden gönderiliyormuşçasına taşınır.

Daha teknik bir bakışla PPTP ile tünelleme İP, IPX ya da NetBEUI paketlerinin internette taşınmak üzere İP paketlerinin içine yerleştirilmesi ile gerçekleştirilir. Çünkü WAN olarak TCP/IP şebekesi en yaygın olarak kullanılmaktadır. Vanş noktasında dış İP paketleri açılır ve orijinal (İP, IPX ya da NetBEUI) paketleri tekrar elde edilir. Buradan çıkan bir sonuç da PPTP'nin yalnızca İP şebekelerinden gelen paketleri değil IPX ve NetBEUI gibi diğer protokollerden gelen paketleri de İP üzerinden taşıyabilmesidir. PPTP DES algoritmasını destekler ve RSA RC-4 ile şifrelenmiş veriyi tünelde taşır. Bu yazıda bilgisayar şifrelemesi ve bilgisayar güvenliği konularına detaylı olarak girilmesi amaçlanmamıştır.

PPTP istemci (client) makinada kurulu olması halinde uçtan uca emniyetli bir tünel kurulabilirken, bunun mümkün olmadığı durumlarda (istemcideki yazılımın sadece PPP protokolünü desteklemesi durumunda) lokal ISP'ye kadar PPP ile erişip daha sonra şirket şebekesine PPTP bağlantısı kurulması da mümkündür.

Güvenilir sanal özel intranet uygulamaları Türkiye gibi kısıtlı kaynaklarını en verimli şekilde kullanmak zorunda olan ülkeler için özellikle büyük önem taşımaktadır. Internet için ayrı ve intranet için de ayn bir fiziksel şebeke alt yapısının kurulması çoğunlukla kaynakların israfına neden olmaktadır. PPTP protokolü ile aynı data devresinin hem internet hem de güvenli intranet için paylaşımlı kullanılması sayesinde pahalı bir kaynak olan transmisyon ortamının tam olarak değerlendirilmesi mümkün olmaktadır.

Kaynakça:

* http://www. cisco. com/warp/public/728/General/updn-wp.htm
* http://www.microsoft com/ntserver/info/pptpfaq.htm
* PC Magazine December 171996, sayfa I26Networking Sofbvare.
* http://www. ascend. com/techdocs/pptpfaq.html http://dsl.intemic.net/std 51 txt