sayTEC

sayTRUST Secure Access

Güvenli Veri iletişimi, uygulama seviyesinde iletişim ve güvenli çalışma ortamı

SÜRÜM 1.0
2019/06

VPN yerine VPSC – Geleceğin iletişim çözümü:

- Network to Network yerine uygulama seviyesinde iletişim
- Sekiz aşamalı güvenlik sistemi; güvenlik tünele girmeden ve iletişim öncesi başlar
- Güvenli ve kopyalanamayan sertifika
- Bütünüyle güvenlik içine alınmış bir çalışma ortamı

sayTEC olarak, bizim için güvenlik vazgeçilmez bir zorunluluktur. Aynı zamanda güvenlik işlevsel ve kullanıcı için kolay olmalı. Bu ilkeden hareketle sayTRUST Secure Access için özel bir arayüz tasarlanmıştır. sayTRUST Secure Access'i geliştirirken müşteriler-den gelen talepler doğrultusunda hareket edilmiştir. Bu çabanın sonunda, yüksek güvenlik düzeyi ile kullanım kolaylığını birleştiren bir ürün ortaya çıkmıştır.

Güvenlik özellikleri konusunda bilinen genel standartlara (SSL, TLS, 20148-Bit'li X.509 sertifikası, Diffie-Hellman Perfect Forward Secrecy kullanıcı sertifikası) ek olarak özel sunucu yetkisi eklenmiştir. Bu yetkinin tünel içinde ayrıca uygulama seviyesinde bağlantı (geleneksel Layer 2 veya Layer 3 VPN yerine geçen) kurmak-tadır. Bu yöntemle zararlı olabilecek etkenler daha tünelin başında tespit edilerek bertaraf edilmektedir. Kendi CA'sına (Certificate Authority) sahip olduğu için, sayTRUST sertifikasyonlarını yabancı bir yerden temin etmek yerine kendi oluşturmaktadır. sayTRUST tüm iletişim, Kullanıcı bilgisayarının belleğinden (RAM) kurmaktadır.

Böylece bağlantı sonlandırıldığında, kullanılan bilgisayar ve iletişim hattında, kurulan bağlantı ile ilgili hiçbir bağlantı veya veri izi kalmamaktadır. Sıklıkla gündemde olan "Man in the Middle Attacke" saldırılarının böylece sisteme sızması imkânsızdır. Şifrelenmiş iletişim esnasında sanal bir ağ kartına ve koruyucu ağ ortamında herhangi bir IP adresine ihtiyaç yoktur. Bu durumda ağ ve ağ bilgileri dışardan görülememektedir. Aynı şekilde Kullanıcı (Client) bilgisayarında da bağlantı gözükmemektedir. Cihaz ağ bağlantısı hakkında bilgi sahibi olmadığından ağ bilgisine de ulaşamamaktadır.

Kullanıcı için en avantajlı durum ise, yanında taşıyacağı sayTRUST Secure Access mobil USB Stick ile istediği yerden, istediği cihaz üzerinden güvenle ağdaki kendi çalışma ortamına ulaşabilmesidir.

Bilgisayar içindeki ağ yönetimi, şahsın kullanım yetkisini merkezi olarak belirlediği için, ilgili kişi sadece kendisine özel hazırlanan uygulamalar ve çalışma ortamına ulaşabilir. Kullanıcı bir kere kayıtlı giriş yaptıktan sonra, tekrar tekrar şifre girmeye gerek kalmadan, otomatik olarak yetkisi olduğu tüm dosyalara ulaşabilir. Single-Sign-On şifre yöneticisi hem kullanıcının

çalışma ortamına ulaşmasını kolaylaştırır, hem de en üst seviyede güvenli bir iletişim ortamı sağlar. Kullanıcı şifrelenmiş veri bankası üzerinden farklı uygulamalara ve/veya platformlara, ilgili şifre ile kayıt yaptırabilir. Herhangi bir uygulamaya giriş yapılmaya çalışıldığında arka plandaki Single-Sign-On modülü güvenli bir kimlik doğrulaması için devreye girer. Tabiki uygulamaların her biri farklı şifrelerle koruma altında kalmaya devam eder.

Mobil uygulamaların hedef grupları, örneğin dışardan şirket ağına erişim sağlamak isteyen veya zorunda olan yöneticiler, teknisyen, danışmanlar, çalışanlardır. Bunlar dışarıdan erişim yetkilendirmeleri sayesinde güvenli ve izole ağ içinde çalışmalarını kolayca gerçekleştirip, birbirlerini hiç-bir şekilde görmemektedirler. sayTRUST okullarda bu sistemi; öğrenci, öğretmen ve idari işleri ayrıştırarak gerçekleştirmektedir. Aynı sistem Devlet Daireleri, Hastanelerde, hasta dosyalarına tıbben yetkili ve idari personelin ulaşması ile sağlanmaktadır. Yine aynı sisteme göre sanayi işletmelerinde, üretim ağındaki kadroların verilere erişimi güvenli bir şekilde birbirinden ayrıştırılmaktadır.