ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/ssl-dpi-kavramlari-esliginde-internet-trafigi-izleme-ve-karsi-guvenlik-onlemleri/

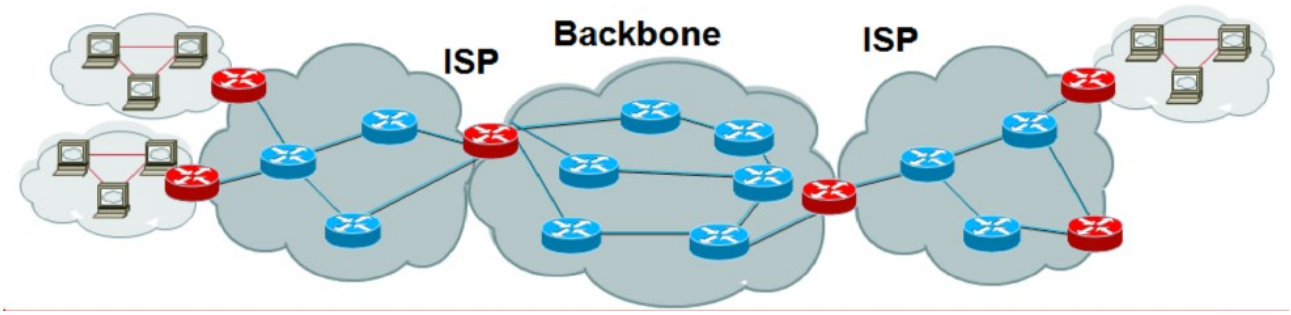
resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/SSL,%20DPI%20Kavramlar%C4%B1%20E%C5%9Fli%C4%9Finde%20%C4%B0nternet%20Trafi%C4%9Fi%20%C4%B0zleme%20ve%20Kar%C5%9F%C4%B1%20G%C3%BCvenlik%20%C3%96nlemleri.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

İnternet temeli 1970'li yıllarda atılmış askeri bir protokol olan TCP/IP üzerinde çalışır.



(Page 6)

2)

İnternet ortamında iletişimde gizlilik temelde iki şekilde gerçekleştirilir:

- İletişim protokollerini şifreli hale getirerek gizliliği sağlama
- İletişim protokollerinden bağımsız olarak özel araçlarla içeriği şifreleme (Her iki taraf da aynı algoritmayı kullanmalı)

İkisi de aynı hesaba geliyor, fakat ilk yöntem daha sık kullanılmaktadır. İlk yöntem merkezi güvenlik ve kontrol sağladığı için daha kolay, ikinci yöntem biraz daha uğraştırıcıdır.

Benim NOT: Sonuçta iletişim protokolü şifreli olursa kullanıcının ekstra bir şey yapmasına gerek olmaz. Güvenlik otomatize bir şekilde sağlanır. Fakat ikinci yöntemde ekstradan tool indirilmesi gerektiği için biraz daha uğraştırıcıdır.

(Page 7)

3)

Şifreli trafik sniff'lense bile anlamlı bir bilgi elde edilemez.

(Page 9)

4)

HTTPS = HTTP + SSL ya da
HTTPS = HTTP + TSL

(Page 22)

5)

SSL (Secure Socket Layer) protokolü sunucu ve istemci arasındaki trafiği şifreleyerek güvenli haberleşmeyi sağlayan bir protokoldür.

SSL merkezi bir güvenlik modeline sahiptir. Bizlerin kime güveneceği bu merkezi otoriteler tarafından kontrol edilip onaylanır. İstenildiği takdirde otorite seçme işlemini kullanıcı yapabilir.

SSL'in temel güvenlik unsuru sertifika otoritesi olarak adlandırılan aracı kurumlar ve bu kurumların bünyesindeki gizli anahtarlarıdır. SSL'i noter otoritesi ve onun mührü olarak düşünebiliriz.

SSL güvenliğinde sertifika otoritesi tüm gücü elinde bulundurur. Sertifika otoritesinde yaşanacak bir güvenlik problemi doğrudan kullanıcıyı da etkiler.

Güvenilir sertifika makamlarının listesi tarayıcı ve işletim sistemlerinde bulunmaktadır ve bu listeler güncellenerek bu makamlar tarafından imzalanmış sertifkaların geçerlilikleri sağlanır.

(Page 26)