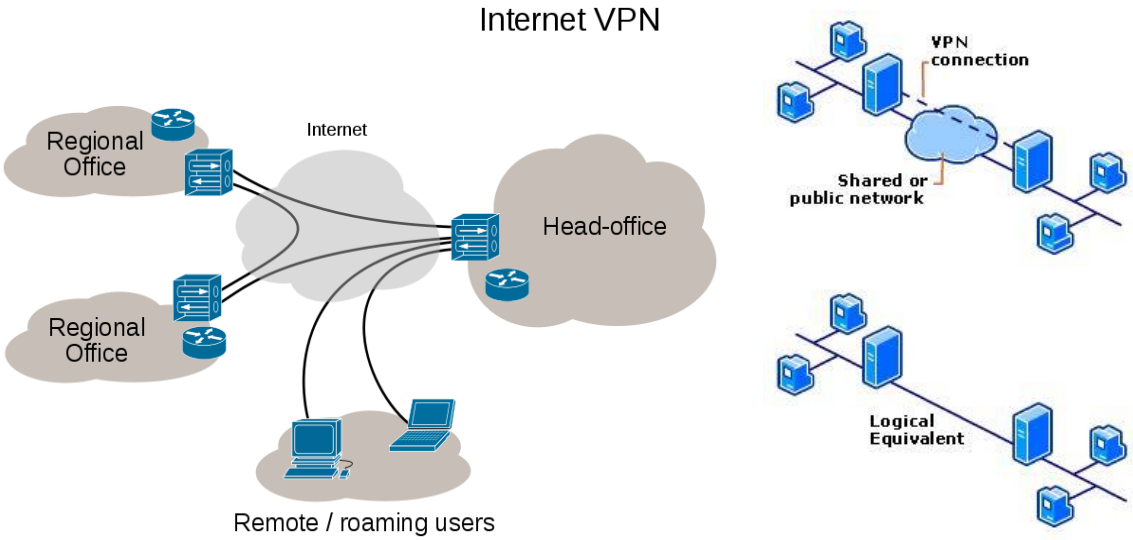
TOR BROWSER, İNTERNETTE ANONİMLİK VE SANAL ÖZEL NETWORKLER (VPN)

Betül Biteker, BTYÖN Danışmanlık

Bugünlerde, Türkiye'de internet erişimine getirilen kısıtlamalarla birlikte merak konusu haline gelen VPN ve TOR gibi, bu tip kısıtlamaları aşmayı sağlayan teknolojilerin çalışma mantıklarına, detaylara çok takılmadan, kısaca değinelim istedik.

Açılımı, Virtual Private Network olan VPN, sanal özel ağ demektir. VPN sayesinde yereldeki bir ağa fiziksel olarak erişiminiz yoksa bile uzaktaki ağlara erişim sağlayabilirsiniz. Seyahat halindeyken işyerinizdeki ya da evinizdeki ağa bağlanmak isterseniz bunu VPN sayesinde yapabilirsiniz. VPN'in bir diğer kullanım amacı da internette güvenli bir şekilde gezinmektir.



Şekil-1-VPN şemaları

VPN dediğimiz bu sanal özel ağların, İnternet gibi bir özel ağ (private network) üzerinden veya ortak bir kamu ağı (public network) üzerinden noktadan - noktaya bağlantıları vardır . VPN istemcisi , VPN sunucusu üzerindeki sanal bir bağlantı noktasına sanal bir arama yapmak için , tünel protokolleri adı verilen özel TCP / IP tabanlı protokolleri kullanır .

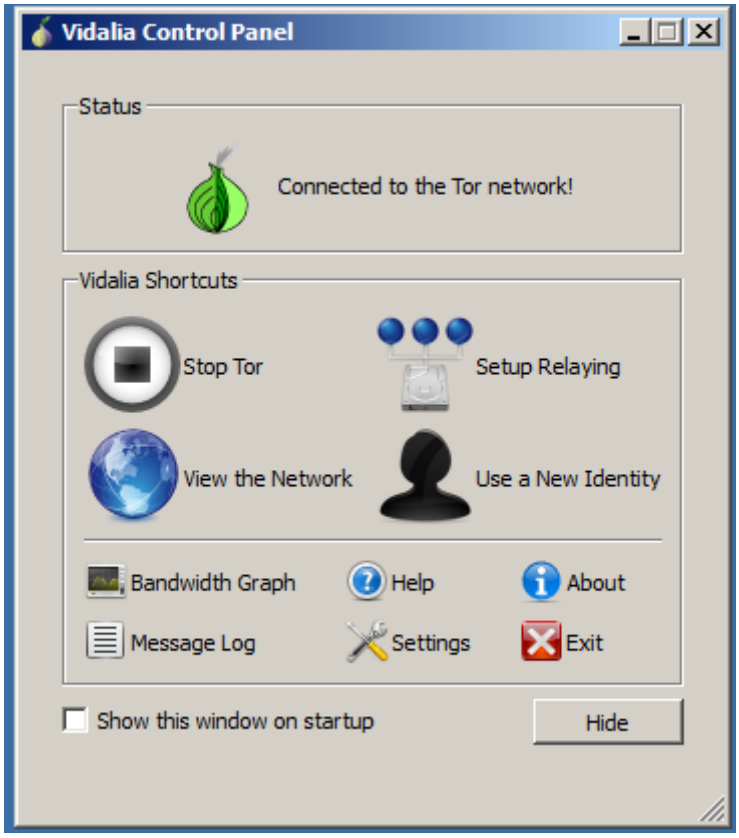
Tipik bir VPN dağıtımında, istemci, İnternet üzerinden uzaktan erişim sunucusuyla sanal, noktadan noktaya bir bağlantı başlatır. Uzaktan erişim sunucusu, gelen isteği yanıtlar ve istemcinin kimlik bilgisini doğrular ve böylece VPN istemcisi ile VPN hizmeti aldığımız firmanın özel ağı arasında veri aktarımı başlamış olur. Noktadan noktaya bir bağlantıyı taklit etmek için veriler, bir başlık (header) ile sarılır ve şifrelenir(encapsulation). Bu başlık (header),verilerin ortak ağ ya da paylaşım alanlarındaki hedef noktalara erişebilmesi için gerekli yönlendirme(routing) bilgisini sağlar.Bu özel bağlantıyı oluştururken gönderilen veriler gizlilik için şifrelenir. Paylaşılan veya ortak ağda olan bu paketler şifreleme anahtarı olmadan çözülemez.

Özetleyecek olursak, özel verilerin saklandığı ve şifrelendiği bağlantılar, VPN bağlantısı olarak bilinir. VPN hizmeti alınan firmanın alt yapısı kullanılarak internete çıkılır. Bilgisayarınız önce VPN ile, hizmet aldığınız firmanın ağına bir eleman olarak eklenir. Doğrudan o ağ üzerinden, erişmek istediği yere güvenli şekilde ulaşır.

TOR

The Onion Router ya da kısaca TOR adı ile bilinen teknoloji, bilgisayarınıza kurup internette anonim şekilde gezinebilmenizi sağlayan bir programdır diyebiliriz. 2002'de birincil amacı ABD'de hükümet konuşmalarını gizlemek olarak geliştirilmiştir ancak bugün tüm dünyaya yayılmıştır ve ücretsiz olarak indirilip kurulabilmektedir.

TOR, internette bir sisteme erişmek istendiği zaman, dağıtık bir ağ üzerinde bu isteği rastgele bilgisayarlar üzerinden iletir. Yani hedef sistem ile kullanıcı arasında doğrudan iletişim kurulmadan anonimlik sağlanır. İnternet bağlantınızı izleyen birinin hangi siteleri ziyaret ettiğinizi görmesini ve ziyaret ettiğiniz internet sitelerinin, fiziksel lokasyonunuzu öğrenmesini engeller. TOR, bu korumayı iletişiminizi dünyanın dort bir yanındaki gönüllü insanlar tarafından calıştırılan TOR node'ları uzerinden dolaştırmak vasıtasıyla yapar. TOR browser'ı bilgisayarınıza kurduğunuzda Şekil-2 deki gibi bir ekran gelmektedir. Burada setup relaying kısmından gönüllü TOR exit node(çıkış düğümü) olunabilmektedir.



Şekil 2- Tor Kontrol Paneli

Ancak bu durumda her isteyenin kendi sistemini TOR çıkış düğümü (exit node) olarak TOR ağına dahil etmesi mümkün olduğu için potansiyel olarak çok ciddi güvenlik ve gizlilik sorunları mevcuttur. TOR çıkış düğümü üzerinde bir saldırıya uğramamak için yapılması gereken şey, protokol seviyesinde

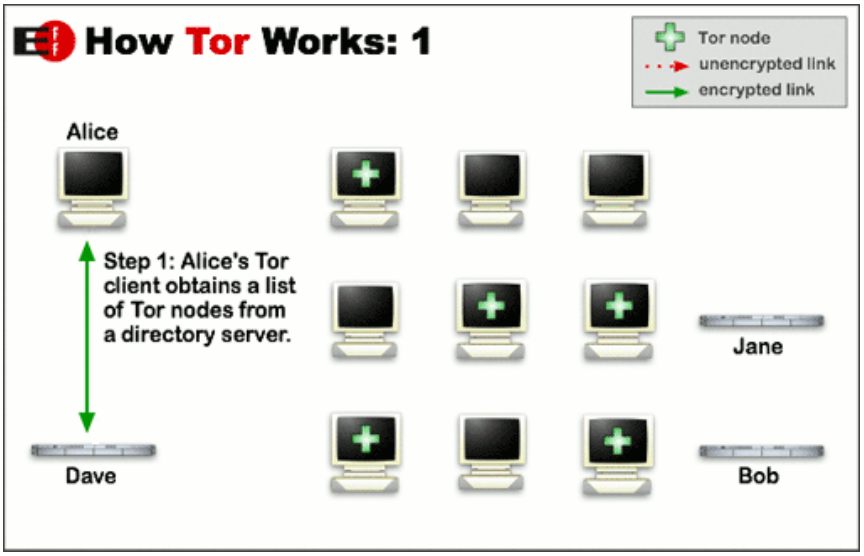
mümkün olduğunca şifreleme kullanmaktır. Bu yüzden TOR üzerinden yönlendirmesini yaptırdığınız web trafiği için HTTPS kullanılması güvenliğiniz açısından önemlidir.

TOR'un Çalışma Mantığı Nedir? Diğer Proxy'lerden Farkı Nedir?

Tipik bir proxy server, internet üzerinde bir yere bir sunucu kurar ve trafiğinizi bu proxy üzerinden geçirmenize olanak sağlar. Bu basit bir mimaridir.Tüm kullanıcılar aynı server üzerinden giriş-çıkış yapar. Servis sağlayıcı, proxy kullanımı için ücret alarak ya da server üzerinden reklam yoluyla maliyetlerini finanse edebilir.

TOR, sizi hedefe göndermeden önce trafiğinizi en az üç farklı sunucu üzerinden geçirir. Her farklı yayın için farklı şifreleme katmanları olduğundan TOR, sizin paket içinde hangi bilgiyi gönderdiğinizi dahi bilmez ve bu bilgiyi değiştiremez. Şekiller üzerinden çalışma mantığını aşağıdaki gibi özetleyebiliriz.

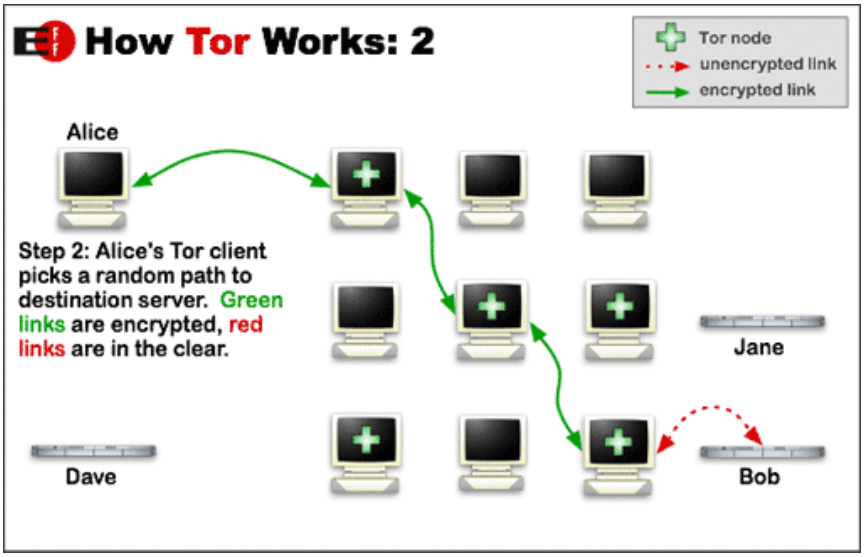
Şekil-3'te Alice isimli kullanıcı, Dave isimli kullanıcıdan mevcut TOR çıkış düğümlerinin listesini alıyor.



Şekil 3-Tor Çalışma Prensibi-1

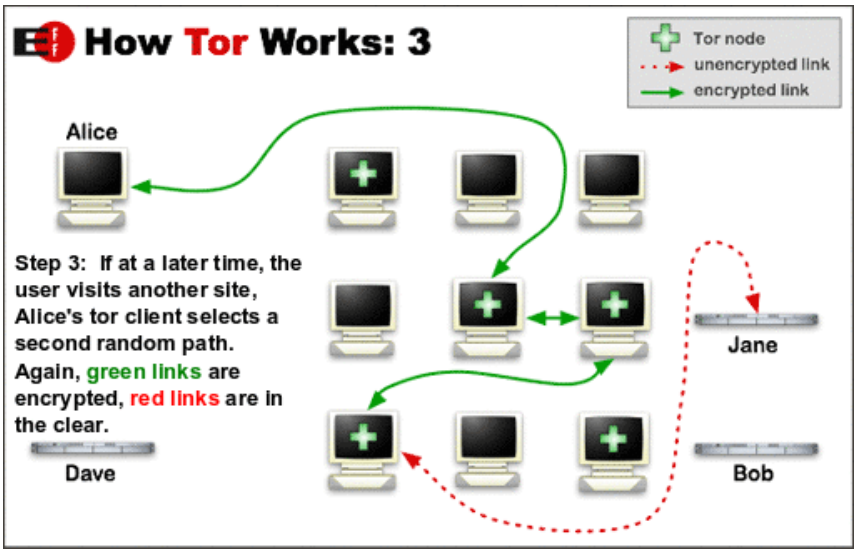
Şekil-4'te ise Alice isimli kullanıcı, Bob isimli kullanıcıya ulaşmaya çalışıyor. Yeşil "+" işareti ile gösterilmiş TOR çıkış düğümlerinden geçerek hedef noktası olan Bob'a ulaşıyor.Bu şekilde yeşil oklardan anlaşılabileceği üzere tüm TOR düğümleri arasındaki iletişim şifrelidir.

Ancak kırmızı oklar ile gösterildiği üzere hedef noktası olan Bob ile TOR çıkış düğümü arasındaki trafik, TOR ağı içerisinde gerçekleşmediğinden, TOR tarafından şifrelenememektir. Dolayısıyla Alice ile Bob'un arasında iletişim protokolleri seviyesinde bir şifreleme mevcut değil ise, TOR çıkış düğümü ile Bob arasındaki iletişim, şifresiz şekilde olacak ve TOR çıkış düğümü tarafından trafiğin dinlenmesi mümkün olacaktır. Bu da daha önce belirttiğimiz gibi, gönüllü TOR node olmanın güvenlik zafiyeti yarattığı konusuna açıklık getirebilir.



Şekil-4- Tor Çalışma Prensibi-3

Şekil 5'te ise Alice isimli kullanıcı, bu kez Jane isimli kullanıcıya ulaşmak istiyor. Burada da tekrar rastgele TOR düğümleri seçilerek trafik iletiliyor ve TOR ağı içerisine dahil olan tüm düğüm noktaları arasındaki trafik şifreli, Alice ile Jane arasında ise HTTPS üzerinden bağlantı sağlanmadıysa Jane ile TOR çıkış düğümü arasındaki iletişim gene kırmızı oklarda görüleceği üzere şifresiz olacak ve güvenlik zafiyetine sebep olacaktır.



Şekil-5 Tor Çalışma Prensibi-4

Kaynaklar

1. https://www.torproject.org/about/overview.html.en
2. http://technet.microsoft.com/en-us/library/cc731954(v=ws.10).aspx
3. http://en.wikipedia.org/wiki/Virtual_private_network