SSH Tunneling

SSH tünelleme bir protokole ait şifrelenmemiş trafiğin ssh protokolü ile şifrelenerek iletilebileceği bir kanal oluşturmaya verilen addır. Örneğin bir ftp client'ın ftp server ile olan trafiği şifreli halde değilken ftp trafiğini ssh tünele sokarak şifreleyebiliriz.

SSH tünelleme trafiği şifrelediği için firewall'ları bypass etmede de kullanılabilmektedir. Dolayısıyla bu yazıda ssh tünel ile firewall engellemelerini atlatma teknikleri gösterilecektir. Üç çeşit ssh tünelleme mevcuttur.

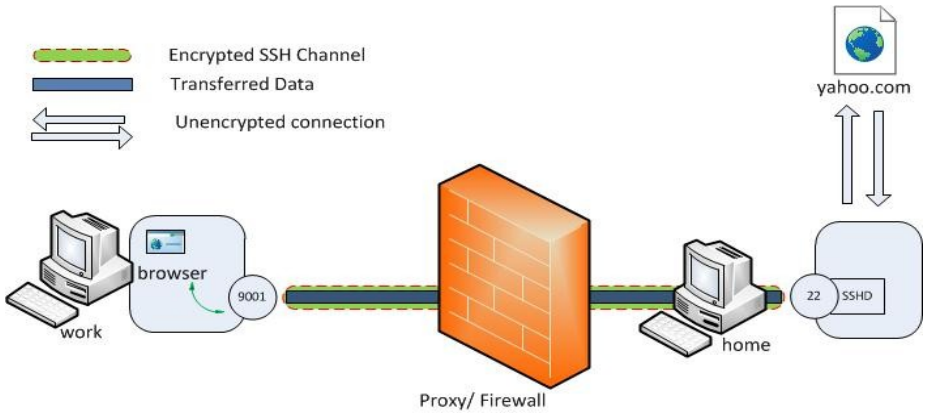
Yerel port yönlendirme (Local port forwarding)
Dinamik port yönlendirme (Dynamic port forwarding)
Uzak port yönlendirme (Remote port forwarding | Reverse Tunnelling)

a. Yerel Port Yönlendirme

Örneğin diyelim ki iş yerimizdeki ağda yer alan firewall yahoo.com sitesine erişim izni vermiyor. Bu durumda ssh tünelleme ile trafiğimizi şifreleyip iş yerimizdeki bilgisayardan evimizdeki bilgisayara oradan da yahoo.com sunucusuna bağlanabiliriz. Aşağıda bunun bir örneği verilmiştir:

```
> ssh -L 9001:yahoo.com:80 home-user@home-ip
```

Yukardaki komut iş yerimizdeki bilgisayarda girildiğinde iş yerimizdeki bilgisayar ile evimizdeki bilgisayar arasında bir ssh tünel açar. -L local anlamına gelir. Bu komut ile iş yerimizdeki bilgisayarın 9001nci portundan evimizdeki bilgisayarın 22nci portuna, oradan da ev bilgisayarımızın 80nci portundan yahoo.com sunucusuna bağlanabiliriz.



İş yerimizdeki bilgisayarda yukarıdaki komut ile ssh tünnellemeyi açtıktan sonra yapmamız gereken tek şey tarayıcıya aşağıdaki linki girmek olacaktır.

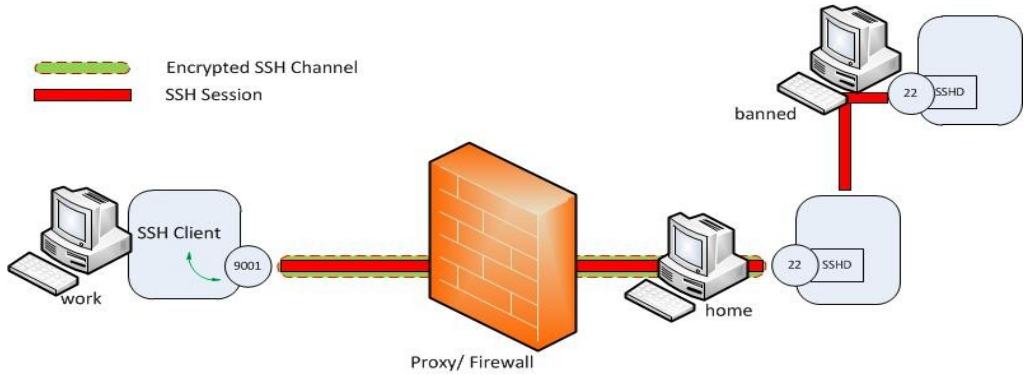
http://localhost:9001

Böylece tarayıcı bizi yahoo.com'a götürecektir ve firewall engeli aşılmış olacaktır. Bu ssh tünelleme çeşidinin syntax'ı şu şekildedir:

> ssh -L <local-port-to-listen>:<remote-host-ip>:<remote-port> <ssh-server-ip>

Bir başka örnek vermek gerekirse ssh tünelleme ile uzak sisteme ssh bağlantısı kurmak isteseydik yapacağımız işlem şu olurdu:

> ssh -L 9001:banned:22 home-user@home-ip // SSH Tünel açılır



> ssh -p 9001 localhost // Hedef sistemle ssh bağlantısı başlatılır.

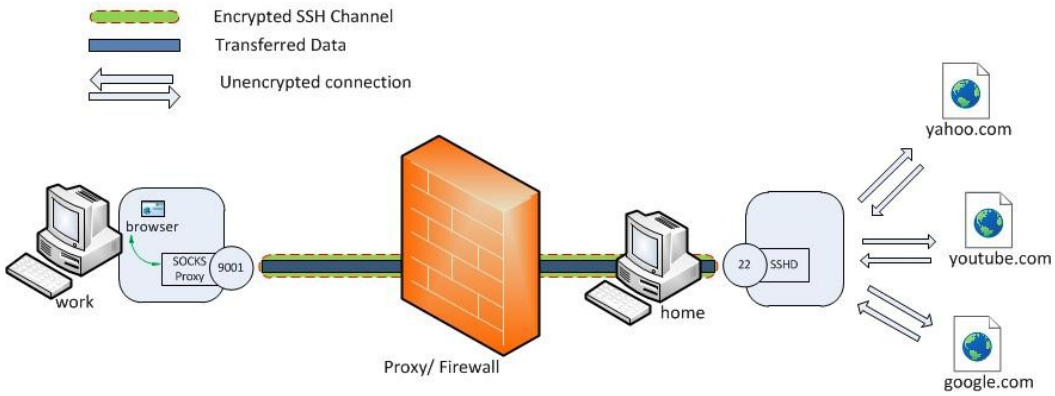
İlk komut ile iş yerindeki sistemimizden evimizdeki sistemimize ssh tünnel açılır. İkinci komut ile de kendi sistemimizin 9001nci portuna ssh bağlantısı kurmuş oluruz. Böylece 9001nci porta gelen veri ssh tünel ile ssh server'ın 22nci portuna, oradan da hedef sistemin 22nci portuna gidecektir ve ssh bağlantısı kurulmuş olacaktır.

b. Dinamik Port Yönlendirme

Yerel port yönlendirme bir yerel porttan spesifik bir uzak sisteme bağlanmamızı sağlamıştı. Dinamik port yönlendirme ise bir yerel porttan ssh tünel ile tüm uzak sistemlere bağlanabilmemizi sağlar.

> ssh -D 9001 home-user@home-ip

Yukarıdaki komut iş yerinde çalıştığırıldığında 9001nci porttan çıkan her trafik evimizdeki bilgisayara ve oradan da gitmesi gereken hedefe gidecektir.



SSH tünellemeyi yukarıdaki komut ile açtıktan sonra tarayıcımızın proxy ayarlarını

localhost 9001

yaparak tarayıcımızdaki her trafiği 9001nci porta yönlendirebiliriz. Böylece trafik ssh tünel aracılığıyla hedeflere gidebilecektir ve firewall'ın engellediği tüm sitelere girilebilecektir.

c. Ters Port Yönlendirme

Diyelim ki iş yerimizdeki bir sunucuya evimizden erişmek istiyoruz. Ancak iş yerimizdek sunucu dışarıya açık değil. Bu durumda evdeki bilgisayarımızdan iş yerimizdeki sunucuya erişebilmek için iş yerimizde yer alan bilgisayarımızdan evimize ters bir ssh tünel açabiliriz. Böylece evimizdeki bilgisayardan iş yerimizdeki bilgisayara ters tünel ile gidebilir, oradan da iş yerimizdeki sunucuya erişebiliriz.

```
> ssh -R 9001:intra-site.com:80 home-user@home-ip
```

Yukarıdaki komut iş yerimizdeki bilgisayarda çalıştırıldığında evdeki bilgisayarımıza ters bir ssh tünel açmış oluruz. Böylece evdeki bilgisayarımızın 9001nci portundan iş yerimizdeki bilgisayarın 22nci portuna, oradan da 80nci porttan iş yerimizdeki sunucuya erişebiliriz.

Sonuç

Ssh tünelleme aşağıdaki amaçlar doğrultusunda kullanılır:

- Güvensiz bir İnternet bağlantısı kullandığımız konumlarda bağlantı güvenliğimizi arttırmak için
- Ağ filtrelerine takılmamak (ağ filtrelerini aşmak) için
- Sistemlere uzaktan erişim için bir zıplama noktası oluşturmak için (VPN alternatifi)
- NAT arkasından gerçek dünyaya soket açmak (NAT arkasından dışarıya servis vermek)

Kaynaklar

https://chamibuddhika.files.wordpress.com/2012/03/localportforwarding.jpg

http://ozcan.com/blog/ssh-tunel-ile-baglanti-guvenligi-ssh-tunnel/