SSH Tünelleme ile İçerik Filtreleyicileri Atlatmak

İşimiz, mesleğimiz gereği çeşitli ortamlarda bulunup internete erişmek, bazı programları (Google Talk, MSN vs)kullanmak istiyoruz fakat bazen bulunduğumuz ortamın şartları bu tip isteklerimize izin vermeyebiliyor . Bazen de herkese açık kablosuz bir ağ ortamında bulunduğumuz için güvenilir tüneller kullanma ihtiyacı hissediyoruz.

Bu tip durumlarda genelde ağ yöneticisine durumu izah ederek bağlantı izni talep edilir. Ağ yöneticisine ulaşılamayacak durumlarda ya da ağ yöneticisini rahatsız etmeden işinizi kendiniz halletmek istediğinizde aşağıda anlatılanları uygulayarak çoğu içerik filtreleme (En popüleri Websense olmak uzere)sistemini atlatabilirsiniz. (Kablosuz ağ ortamlarında trafiğinizin izlenmemesi için de kullanılabilir)

Benzer şekilde ağ guvenliği yöneticileri kendi ağlarında bu tip gizli tünellerin çalıştırılmasını istemeyebilir. Burada anlatılan yöntemlerin sisteminizde çalışmaması için yazının son bölümündeki "Nasıl Engellerim" başlıklı kısmı inceleyebilirsiniz.

Icerik filtreleme sistemlerini atlatmak icin kullanacağımız yöntem SSH Tünelleme(SSH'in SOCKS proxy ozelligini kullanacagiz).

Kısaca bilgilerimizi tazeleyelim:

- SSH servisi öntanımlı olarak 22/TCP portunda çalışır ve istenirse değiştirilebilir.
- Proxy'ler CONNECT metodu ile http olmayan çeşitli bağlantılara izin verirler. Mesela HTTPS. Bunun için genelde Proxy yapılandırmalarında 443 TCP portu dışarıya doğru açıktır.
- SSH protokolü Proxy'lerin CONNECT yöntemini kullanarak ssh sunuculara bağlanabilirler.

Bu yazıda kullanacağımız yöntem de 443. porttan çalışan SSH sunucusu bulup kendi sistemimiz ile bu sunucu arasında tunnel kurarak web trafiğimizi bu tünelden geçirmek. Arada gidip gelen veri şifreli olduğu için içerik filtreleme yazılımları bize engel çıkarmayacaktır.

SSH sunucu Seçimi

Roothsell.be 443. portta(yaklasik 10 farkli porttan daha ssh hizmet sunuyor) çalışan ve SSH port Forwarding'e açık bir SSH servisi sunuyor. Siteden(rootshell.be) kayit olarak kendinize bir ssh hesabi açabilirsiniz. Ya da benzeri servis veren sistemlerden kendinize bir hesap oluşturabilirsiniz.

SSH ile Proxy Tünelleme (Dynamic port forwarding)

OpenSSH Dynamic Port forwarding desteği ile bir nevi socks proxy vazigesi görür. Socks RFC-1928 ile tanımlanmış basit ama güçlü bir TCP protokoldür. Socks 5 ile UDP desteği de eklenmiştir.

Örnek;

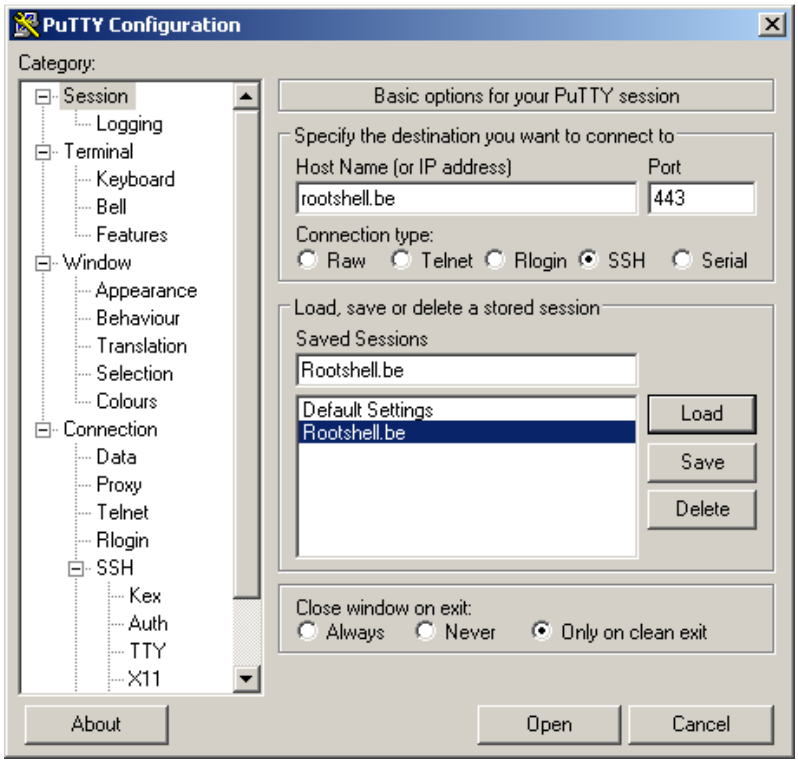
Linux sistemlerde aşağıdaki komutu ile Dynamic Port forwardingi calistirmis olursunuz.

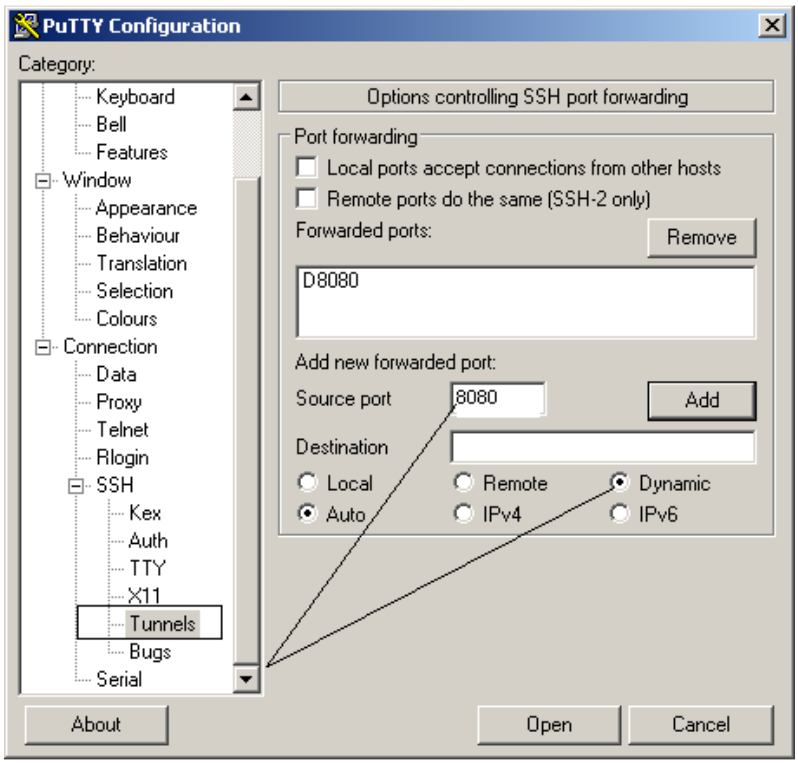
$ssh -D 8080 rootshell.be -p 443

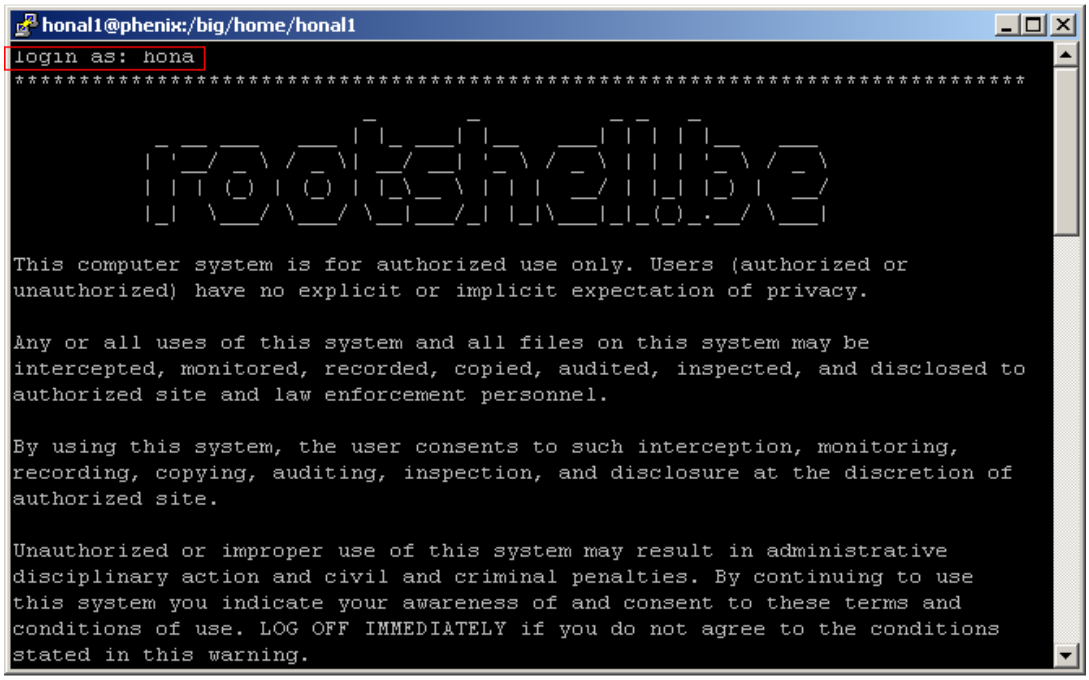
Bundan sonra kullandığım browserin proxy ayarlarından 8080 olacak şekilde yapılandırırsam herhangi bir kısıtlama olmaksızın rootshell.be makinesi aracılığı ile özgürce gezebilirim.

Putty ile SSH Tüneli Kurulumu

NOT: Putty yerine plink(aynı siteden edinilebilir) indirip kullanabilirsiniz ya da Linux komut satirindan aynı işlemleri tekrarlayabilirsiniz.


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
rootshell.be
443
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Rootshell.be
Default Settings
Rootshell.be
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel


PuTTY Configuration
Category:
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Tunnels
Bugs
Serial
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH-2 only)
Forwarded ports:
Remove
D8080
Add new forwarded port:
Source port
8080
Add
Destination
Local
Remote
Dynamic
Auto
IPv4
IPv6
About
Open
Cancel



SSH sunucuya bağlanma ve Tüneli aktif hale getirme

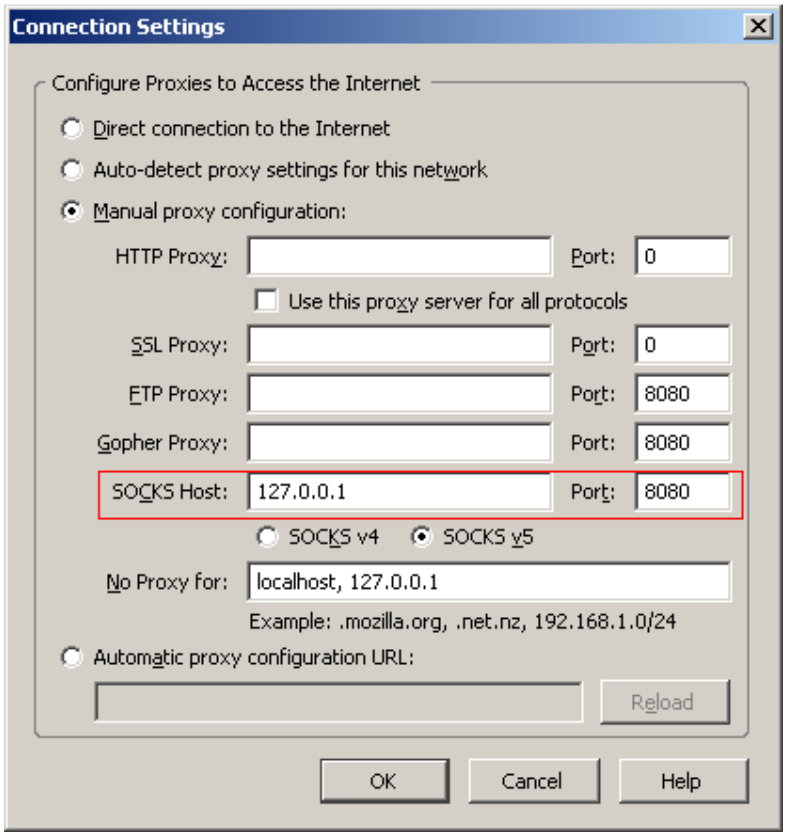
Tünelimizin açıldığını kontrol etmek için komut satırından aşağıdaki komutu verip çıktısını inceleyelim. Herhangi bir çıktı almıyorsanız biryerlerde yanlış/eksik yapmışsınız demektir, önceki adımları tekrar kontrol edin.

C:\Console2>netstat -an|find "8080"

TCP 127.0.0.1:8080 0.0.0.0:0 LISTENING

Browser Yapılandırması

Kullandığınız Browser'ın(buradaki örnek Firefox içindir) socks proxy kısmına 127.0.0.1 8080 tanımlarını girerek Browseri kapatıp tekrar açın

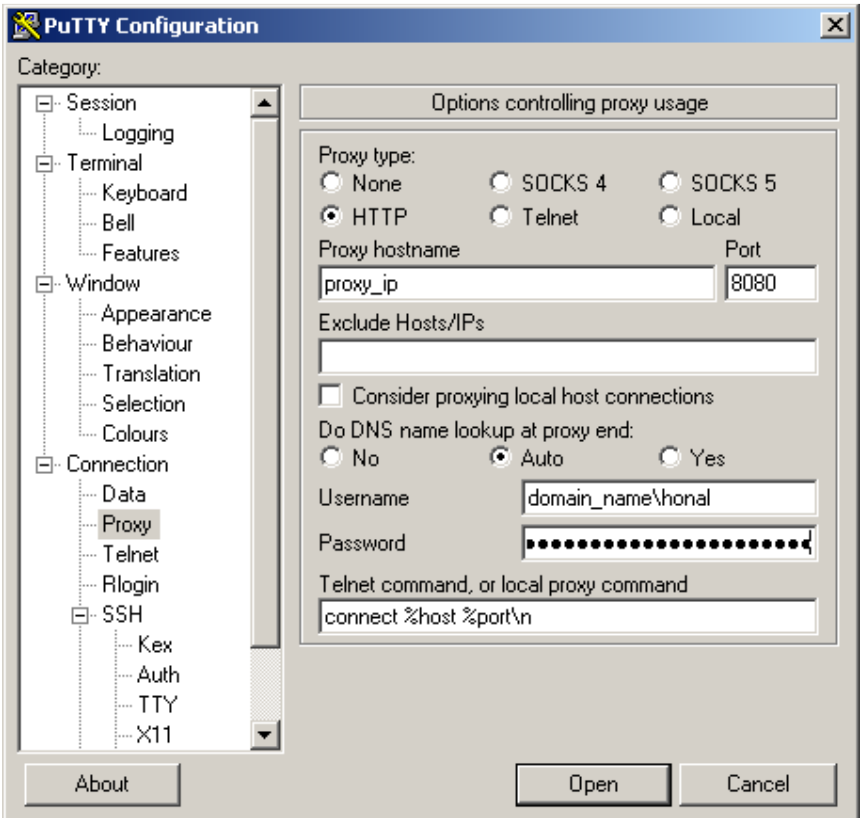


Firefox Proxy Ayarları

Sonrasında http://www.whatismyip.com adresinden IP adresinizi kontrol edip gerçekten Proxy üzerinden çıkıp çıkmadığınızı control edebilirsiniz.

Proxy Kullanılan Ortamlarda Gerekli Ayarlar

Internete Proxy üzerinden çıkıyorsanız (muhtemelen) ve Proxyden sadece 80 ve 443 portları açıksa – ek olarak proxy kullanici_adi/parola istiyor- bu durumda Putty/ssh istemcisi programınızda Proxy ayarlarınızı girmeniz gerekebilir. Linux'da bunun için Netcat kullanabilirsiniz.



Resim –V) SSH Proxy ayarı

NTLM Auth Kullanılan Ağlarda

Proxy amacli olarak Microsoft ISA Server ve NTLM Authentication kullanilan ortamlarda cogu internet uygulamasi calismaz. Bunun sebebi NTLM'in Microsoft'a ozgun bir protokol olmasi ve klasik authentication mekanizmalarindan fazlasiyla karisik olmasi sebebi ile yazilimcilarin bu destegi vermek icin ugraşmamasıdır.

İşte bu sebeptendir ki NTLM Auth kullanılan ağlarda çoğu program sağlıklı çalışmaz. Bunun için araya köprü vazifesi görecek ek uygulama gerekir.

Bizim_Uygulama----Köprü(NTLM_destekliyor)-----NTLM Auth isteyen Proxy

Mesela Websense ya da benzeri bir icerik filtreleme programini atlatmak icin Ultrasurf kullanmaniz gerekirse ya da rapidshare'den toplu dosya indirmek icin Flashget benzeri programlari kullanmak isterseniz hep bu ntlm auth problemi ile karşılaşılır.

Bu tip ntlm auth. gerektiren durumlarda Python ile yazilmis NTLMAPS yazılımı ya da Cntlm yazılımı kullanılabilir.

Nasıl Engelleyebilirim?

Ağınızda bu tip erişimleri engellemek için genel geçer bir çözüm yok*. Bu yazıdaki yöntemi engellemek isterseniz roothsell.be'e ait IP aralığını toptan yasaklarsanız ya da içerik filtreleme yazılımınızdan bu adreslere(rootshell.be vs) giden istekleri kapatabilirsiniz. Doğal olarak bu engelleme yöntemi sadece rootshell.be için olacaktır. Buna benzer birçok free SSH servisi sunan IP vardır.

*Piyasada SSL içeriği inceleyip içerik filtreleme yapan bazı ürünlerin varlığı bilinmekte fakat hem kullanım (gizliliği ihlal etmesi yönünden) hem de performans getireceği iş yükü sorunları yüzünden pek tercih edilmemektedir.

Huzeyfe ÖNAL

huzeyfe@lifeoverip.net