Bilindik engelleme yöntemlerinin dışında olan, kurumsal web filitreleri nasıl aşılır ?

Not : Yazdıklarım tamamen öğretim amaçlıdır. Yaşanacak her türlü sıkıntının sorumlusu uygulayan kişidir. Sorumluluk kabul etmediğimi belirtirim.

ANALİZ

Kurumsal engelleme yapan yazılımlar farklı olarak ne yapar ?

- Proxy kullanamazsınız çünkü standart http headerleri denetlendiği için proxy isteği anında anlaşılır ve bloklanır. Headerleri inceleyince çok net fark görülüyor zaten.

- ssh tünelleme mükemmel çözüm fakat, istemci ve sunucu şifreli iletişime geçmeden önceki tanışma faslını temsil eden mesajlar plain text olduğundan tanınır ve bloklanır.

- SSL sertifikası kurumunuza aitse işiniz çok daha zor . Zira artık güvenli mesajlaşma protokülünüz kurumunuzun inisiyatifindedir. tüm içerikleriniz filitrelenebilir, kara listedeki kelimeler vb istekler engellenir.

Bunları tespit etmem 2-3 günümü aldı. Engeli aşmak için kafamdaki senaryo belliydi fakat ihtiyacım olan python bilgisine sahip olmadığımdan işim dahada zorlaşmıştı.

SENARYO

Yapmam gereken bir proxy scripti bulup, kurum dışında bir makinede çalıştırıp bu bilgisayarı vekil olarak kullanmaktı. Tabi bilindik yöntemlerden farklı olmalıydı

Http headerlerini localde kendime göre biçimlendirip bunu sunucuya gönderdikten sonra tekrar düzenli halde kullanmam gerekiyordu. Onlarca deneme ve haftalarca araştırmalarım sonunda nihayet bir çözüm buldum. Hem en iyisi diye bilirim. Başka çözümde var tahminim fa onu denemedim. hele bunu tüketelim :)

İhtiyaçlar

1. Kurum dışında bir PC. Mümkünse yurt dışından bir VDS . Bu yoksa evinizdeki bilgisayarda olur
   (Evdeki PC için modemden 80. portu PC nize yönlendirmelisiniz)

2. Modifiye ettiğim bu python scripti
   Aşağıdaki *örnek kodlarda* ***simpleproxy_cln_ham.py*** *veya* ***simpleproxy_haw.py*** *olarak kullandım. Sizin indirdiğiniz dosya adı* ***proxy.py****. Siz bunu yazın.*

3. Windows istemciler için putty yazılımı

4. Sabır ve sabır…

KISA ANLATIM

1. Sunucu tarafındaki 80 nolu portu boşa çıkartın . varsa kullanan programı kapatın.(mesala apache gibi)

```
root: /home/okul $ service apache2 stop
 * Stopping web server apache2
 *
root: /home/okul $
```

2. Sunucu da SSH configini düzenleyin. (RSA keyi istemeden sadece parolalı giriş için bir düzenleme)

```
root: /home/okul $ nano /etc/ssh/sshd_config
```

```
root: /home/okul $ service ssh restart
ssh stop/waiting
ssh start/running, process 2122
root: /home/okul $
```

3. proxy.py scriptini sunucu tarafında çalıştırın.

```
okul: ~ $ sudo su
root: /home/okul $ python simpleproxy_haw.py 10.0.66.136:80 localhost:22
```

10.0.66.136.80 olan ip sunucun yerel ip si. Bazı sunucularda WAN ip sini yazınca oluyor.

4. Local istemci pc de scripti çalıştırın (sonra konsolu kapatmayın açık kalsın)
   a. linux makinede python script çalıştırmak için
   simpleproxy_cln_ham.py scriptin adı. Sizin indirdiğiniz dosya adı ***proxy.py***. Siz bunu yazın

```
root@debian:/home/[redacted]/Masaüstü/proxy02# python simpleproxy_cln_ham.py localhost:22 u[redacted]:80
```

   b. Win makinelerde python script çalıştırmak için
   Win makinelerde python3x i kurun
   komut satırını açın.
   python.exe dizinine gidin.
   bu dizinde iken
   c:\..... . .>python.exe ***proxy.py localhost:22 server_adresi:80***

   import fcntl hatası alırsanız proxy.py de ilgili satırı silin. Kaydedip tekrar deneyin.

   Win de python çalıştırmak için Bu linkteki belgeyi inceleyin. Windows bölümüne bakın lütfen

5. Local pc de yeni bir konsolda tünel açalım .
   (Benim sunucumdaki kullanıcı adım okul Değiştirmeyi unutmayın)

a. **Linux makinelerde**

```
root@debian:/home/[redacted]/Masaüstü/proxy02# ssh -D 8080 okul@localhost
okul@localhost's password:
```

b. **win makinelerde**
Win makineler için putty kullanımı aşağıdaki geniş anlatımda mevcut

6. Firefox için proxy ayarı
Aşağıda geniş anlatımda mevcut

DETAYLI ANLATIM

1. Sunucu olarak kullancağımız bilgisayarda 80 nolu port boşta olmalı.

apache vb varsa kaldırın yada port unu değiştirin. Fakat 80 kesinlikle bizim olmalı onu biz kullanacağız. Kurumunuzun internetinde port yasaklama yoksa istediğinizi kullanabilirsiniz.

```
root: /home/okul $ service apache2 stop
 * Stopping web server apache2
 *
root: /home/okul $
```

2. SSH için ön hazırlık.

- ssh güvenlik olarak RSA kullanır ve key oluşturmak gerekir. Fakat sunucunuzdaki ssh configinde bir satırı değiştirerek sadece password ile giriş yapmak daha pratik.

```
root: /home/okul $ nano /etc/ssh/sshd_config
```

her hangi bir editörle sshd_conf dosyasını açıp ilgili satırı değiştirin. Ben nano kullandım.

PasswordAuthentication no
yerine
PasswordAuthentication **yes**

Olarak değiştirin dosyayı kaydedip kapatın

- Sonra ssh servisini restart edin.

```
root: /home/okul $ service ssh restart
ssh stop/waiting
ssh start/running, process 2122
root: /home/okul $
```

3. proxy.py scriptini sunucuda çalıştırmak için linux makinelerde root olduktan sonra aşağıdaki komutu verin.

#python proxy.py 10.0.66.136:80 localhost:22

(80 . porta gelen isteği 22 nolu porta yönlendiriyoruz. tabi bu istek filitreleme sistemi anlamasın diye encrypt ettim , karşıya ulaşınca decrypt ediliyorum)

sizin yapmanız gereken **10.0.66.136** bu IP yi değiştirmek. Burası önemli vds kullanıyorsanız yerel ağ IP sini (deneme yapmak lazım) yada gerçek IP yi yazmalısınız *(! 127 x x x değil)*. Ev deki PC nizi kullanacaksanız sanırım aynı şey geçerli, ev PC mi server olarak henüz denemedim.
Not :linux makinelerde yerel ağ ip sini ***ifconfig*** komutuyla alabilirsiniz.

```
okul: ~ $ sudo su
root: /home/okul $ python simpleproxy_haw.py 10.0.66.136:80 localhost:22
```

ilk satırda root oldum
ikinci satırda scripti çalıştıracak komutu yazdım ve entere bastım.
scriptin bulunduğu dizinde olduğunuzdan emin olun.

4. İstemci bilgisayarda (ofisinizdeki pc)

Linux makinelerde
Gene aynı scripti çalıştırın. fakat bu sefer argümanlar farklı

#python proxy.py localhost:22 server_adresi:80
(localdeki 22 nolu porta gelen istekleri uzak sunucudaki 80 nolu porta gönderiyoruz tabiki şifreli olarak maksat filitreden kaçmak :))

Bu komut satırında ***server_adresi*** sizin VDS nizin yada evdeki PC nizin adresi / IP si olacak.

```
root@debian:/home/[redacted]/Masaüstü/proxy02# python simpleproxy_cln_ham.py localhost:22 u[redacted]:80
```

Win makinelerde
python3x i kurun

komut satırını açın.
python.exe dizinine gidin.
bu dizinde iken
c:\..... . .>python.exe ***proxy.py localhost:22 server_adresi:80***

import fcntl hatası alırsanız proxy.py de ilgili satırı silin. Kaydedip tekrar deneyin.

5. Buraya kadar sorunsuz geldiniz umarım. Artık offisimizdeki PC de ssh ile tünel açama safhasına geldik.

Amacımız yerel pc mizdeki 8080 nolu porta gelen istekleri. Gene yerel pc de çalışan python scribine yönlendirmek. scriptimiz gelen istekleri şifreleyip sunucuya 80 . portan yönlendirecek. datalar şifreli olduğu için filitreden geçebilecek.

Sunucuya gelen şifreli datalar decrypt edilip sunucunun 22 nolu portunu dinleyen ssh a iletilecek. Cevapta aynı yolu izleyerek bize şifreli olarak gelecek.

LİNUX MAKİNELERDE SSH TÜNEL AÇALIM

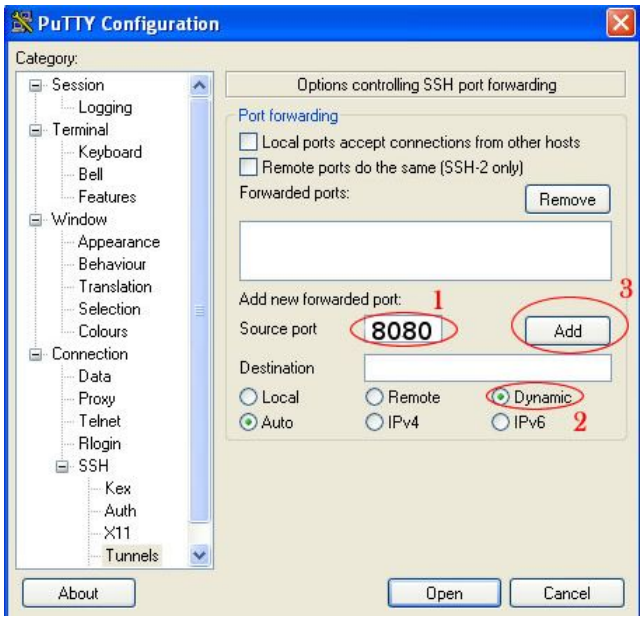
Benim uzak sunucudaki kullanıcı adım **okul** siz kendi kullanıcı adınızı yazmalısınız

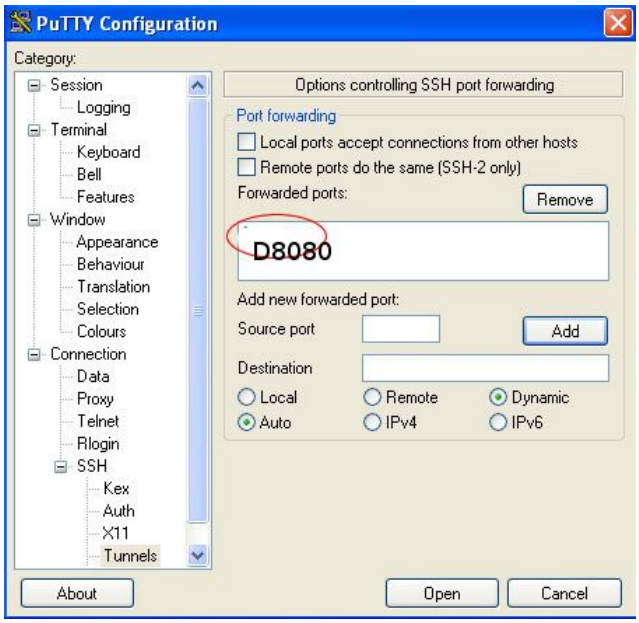
```
root@debian:/home/[redacted]/Masaüstü/proxy02# ssh -D 8080 okul@localhost
okul@localhost's password:
```

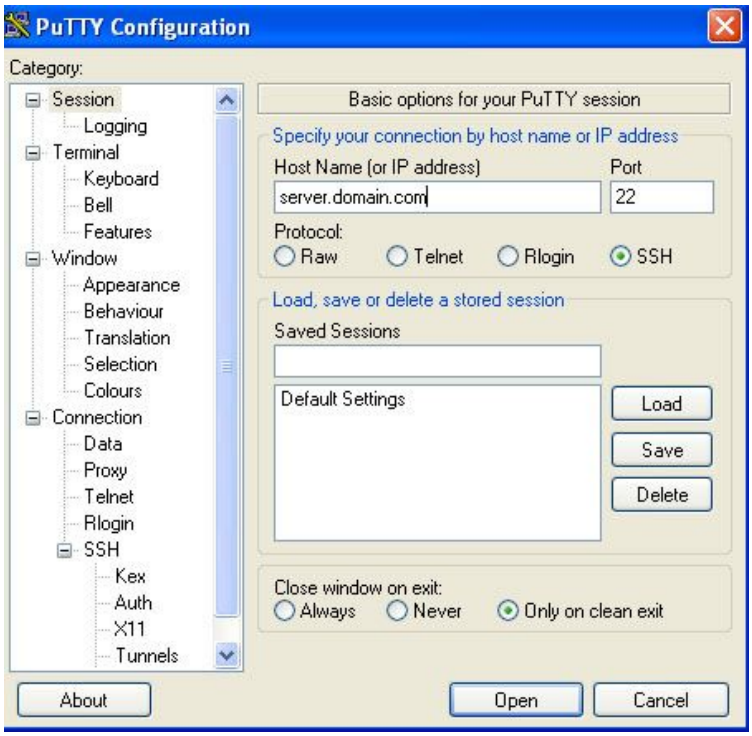
İlk satırdaki kodu girdikten sonra entere basın uzaktaki sunucu sizden parola isteyecektir. kullanıcı parolasını girdikten sonra ssh oturumu açılacaktır muhtemelen aşağıdaki görüntüyü elde edeceksiniz.

```
 * Documentation:  https://help.ubuntu.com/

  System information as of Tue Jun  7 10:28:13 UTC 2016

  System load:  0.0               Processes:           112
  Usage of /:   57.8% of 2.82GB   Users logged in:     1
  Memory usage: 21%               IP address for eth0: 10.0.66.136
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

250 packages can be updated.
155 updates are security updates.


*** /dev/xvda1 should be checked for errors ***

Last login: Tue Jun  7 10:28:13 2016 from localhost
okul: ~ $
```

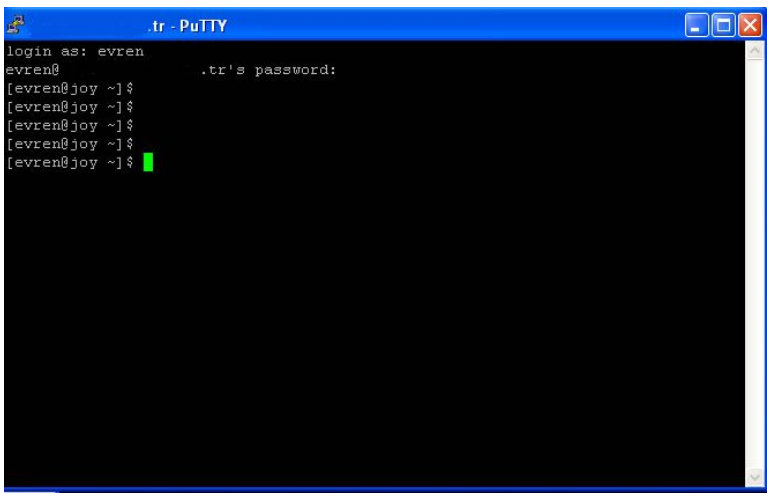
WİNDOWS MAKİNELERDE PUTTY İLE SSH TÜNEL AÇMA







Dikkat Host Name kutusuna **localhost** yazmalısınız

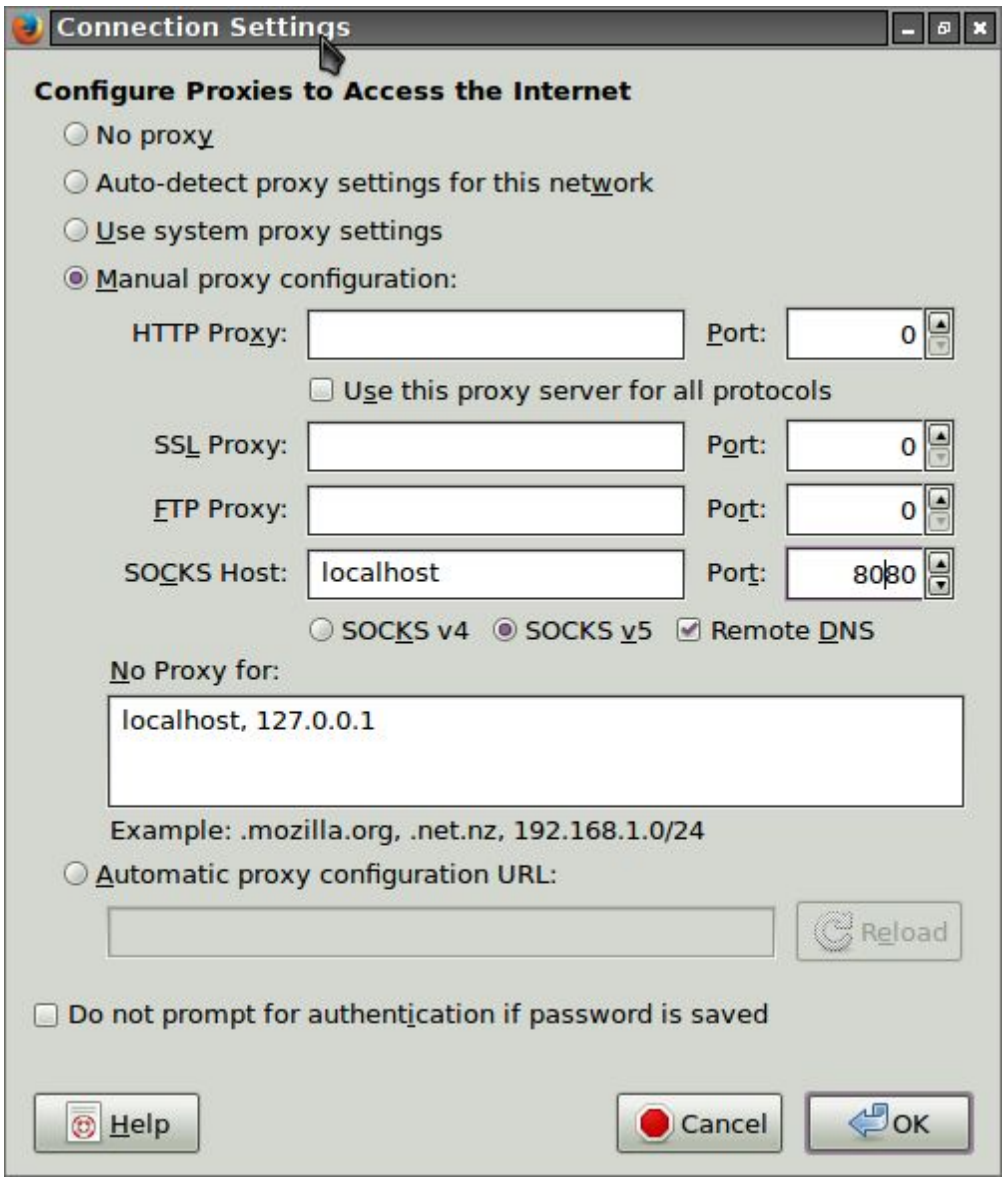


Kaynak : http://shukko.com/tunel/index.html

putty ile ilgili daha geniş bilgiyi araştırın

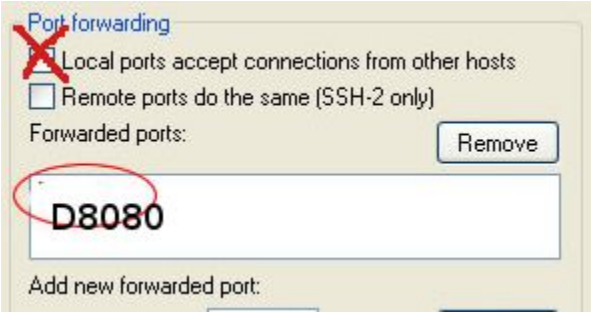
Artık uzak makinede ssh oturumu açtınız . Tünelimiz hazır.

Firefox u açıp SOCKS ayarını aşağıdaki gibi yapın. Artık sisteminiz hazır. Güle güle kullanın.



Not 1 : Kurumunuzdaki bir pc tünel oluşturduysa diğerleride bunun üzerinden internete çıkabilir. Yapmaları gereken firefox ta SOCK kısmına localhost yerine tünel sahibi PC nin IP sini yazmak.
Linux makinenizi paylaşmak için ssh tünel açma komutuna bir parametre eklemelisiniz
ssh -g -D 8080 kullanici_adi@llocalhost

win makinelerde paylaşım için
Tabi putty den yönlendirme izni almak lazım. Local port acc… i işaretleyin.



Not 2 : Kaliteli bir VDS alınabilir. ve onlarca kişi ortak kullanabilir.

Bu yolu evimde denedim hız normal bağlantıdan hiç farklı değil . Fakat kurumsal internet filitre yazılımı ve donanımı hızı çok düşürüyor. Bedava sirke baldan tatlıdır hesabı çaresiz kullanıyorum.

Not 3 : **Adress already using**.. benzeri hata alıyorsanız. 80 ve 22 nolu portlar başka yazılımlar tarafından kullnılıyor demektir. onları kapatın.
linux makinelerde root iken
service apache2 stop
service ssh stop

DÜŞÜNCE SU GİBİDİR, KOLAY YOLU SEÇER.
DOĞRU OLDUĞUNDAN EMİN OLUN