Per-Analysis Network Routing ve Basit Global Routing

Cuckoo `2.0-rc1`'den itibaren per-analysis network routing özelliği bulunmaktadır. Başka bir deyişle, bir VM'niz varsa ve analiz edilecek üç örnek varsa, ilk analiz için internet erişimini engellemek, ikinci analizi bir VPN üzerinden yönlendirmek ve üçüncü analizi Tor ağı üzerinden çekmek mümkündür.

Ancak, daha gelişmiş analiz başına yönlendirme dışında, daha önce lüks yönlendirme henüz mevcut olmadığında popüler olan bir varsayılan rota da mümkündür.

Örneklerimizde, varsayılan makina seçeneğimiz olduğu için `VirtualBox`'a odaklanacağız.

Daha karmaşık ve özellik açısından zengin per-analysis network routing'e girmeden önce, bir kez ayarlandığında değiştirilmeyen global `iptables` kurallarına dayanan daha eski bir yaklaşımı ilk ele alacağız.

Aşağıdaki kurulumda, VirtualBox VM'imize atanan arayüzün `vboxnet0` olduğunu, VM'nin IP adresinin `192.168.56.101` olduğunu (bir `/24` alt ağda), internete bağlı çıkış arayüzünün `eth0` olduğunu varsayıyoruz. Bu kurulumla, aşağıdaki `iptables` kuralları, VM'lerin Cuckoo ana makinesine (bu kurulumda `192.168.56.1`) ve internete tam erişim sağlamasına izin verecektir, bu da internete bağlanan herhangi bir uygulamadan beklediğiniz gibi.

```
$ sudo iptables -t nat -A POSTROUTING -o eth0 -s 192.168.56.0/24 -j
MASQUERADE

# Default drop.
$ sudo iptables -P FORWARD DROP

# Existing connections.
$ sudo iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

# Accept connections from vboxnet to the whole internet.
$ sudo iptables -A FORWARD -s 192.168.56.0/24 -j ACCEPT
```

```
# Internal traffic.
$ sudo iptables -A FORWARD -s 192.168.56.0/24 -d 192.168.56.0/24 -j ACCEPT

# Log stuff that reaches this point (could be noisy).
$ sudo iptables -A FORWARD -j LOG
```

Bu kurallar ayarlandığında neredeyse başlamaya hazırız. Ancak, bu kurallar, çekirdekte IP yönlendirmesi açıkça etkinleştirilmediği sürece herhangi bir paket yönlendirmesi yapmaz. Bunu yapmak için, geçici bir yöntem ve kapatma veya yeniden başlatma kadar süren geçici bir yöntem bulunmaktadır. Basitçe söylemek gerekirse, genellikle bu iki komutu çalıştırmanız gerekecektir:

```
$ echo 1 | sudo tee -a /proc/sys/net/ipv4/ip_forward
$ sudo sysctl -w net.ipv4.ip_forward=1
```

Iptables kuralları, yeniden başlatmalar arasında kalıcı değildir, bu nedenle onları korumak istiyorsanız bir komut dosyası kullanmalısınız veya sadece `iptables-persistent` kurmalısınız.

Daha yeni Linux dağıtımları, udev'in arayüz adlandırma düzenini benimsemiştir. Bu, `eth0`'ın artık ana arayüz olmayabileceği anlamına gelir. Olası arayüz adları, `ensXX`, `enp0sXX` ve `emXX`'i içerir, burada `XX` kısmı bir numarayı tanımlar. Bu, yukarıdaki NAT ifadesi için özellikle önemli bir nottur.

Revision #1
Created 25 December 2023 09:10:34 by Ertan Sözer
Updated 25 December 2023 09:12:25 by Ertan Sözer