

## FreeBSDistemcileri arasında Ipsec tünelleme

Birtürüpgüvenlikçe şidiolanIpsec,ippaketseviyesinekadarolanInternettrafiğini şifrelemeyöntemidir.BudaSMTPgibigüvenli şidüşükolanprotokollerigüvenlihaline getirebilmesansını bize veriyor.Ipv6açısındanne kadarIpv4tarafındagibigözüksede IpsecIpv6ileçokrahatbir şekildeçalı şabiliyor.Makalede İngilizceterimlerinekarşılık olarakkullandığımızkelimeleriaçıklayıcıolmasıbakımındanbelirteceğimizebaşlayalım:

```
access point = erişim noktası
transport mode = taşıma modu
tunnel mode = tünel modu
tunneling = tünelleme
key lifetimes = anahtar süreleri
pre-shared key = ön paylaşım anahtarı
host = istemci
```

Ipsec`inikiönemlibölümüAuthenticationHeader(AH)veEncapsulatingSecurity Protocol(ESP)`dir.AHgönderilenbilginingerçekten bilgiolduğunuvegönderenkişinin gerçekteğönderenolduğunuispatetmekiçinkullanılıyor.ESPisegönderilen paketleri şifreleyerekpaketinyolaldığısureiçindekotugözlerdenuzakdurmasınıgaranti yapıyor.

HemESP`hemdeAHtünelveyetaşıma(Transport)sekindekullanılabiliniyor.taşıma moduikisinnoktaarasındagüvenliksağlarken,tünelmoduiseVPNturugüvenlik sağlıyor.Taşımamodundapaketlerdeyazılıbulunanbaşlıkveaynakadresiişimzalanıp şifreleniyor.Dahasonravarışnoktasınağönderilen paketleralındıktan sonra onaylanıyor, şifreleri açılıp normal paket haline getiriliyor. taşımamodu en çok olarak istemci arasındaki kullanılıyor.Yalnız kaynak IP`si önemli olduğundan NAT kullanılabilmeyen ağlarda maalesef kullanılamıyor.

Tünel modunda AH veya ESP (Bazen her ikisi de) tüm paketi şifreleyerek veya imzalayarak yeni bir pakete haline getiriyorlar ve bu paket karşı tarafta aynı şekilde tekrar onaylanıyor ve şifresi açılıyor. şifresi açılıp onaylanan paket bundan sonra normal bir paket olarak işlem görüp son hedefine gönderiliyor.Anlaşılabilirceğigibi tünel modu ki router veya istemci ile router arasındaki kullanılmak için mükemmel bir yöntem sunuyor.Orijinal paket kendibütünü olduğu içinde şifrelenip imzalandığı için tünel modunda ESP NAT kullanılabilmeyen ağlar üzerinde kullanılabiliyor.

Tünel modu ESP`sinin üzerindeki güvenliği keşif edilmiş bölümlerini güvenli hale getirmek için harika bir yöntem.Örneğin su anda bu yazıyı yevim de bulunan kablo su taşıyıcıları için ilsalonumda yazıyorum.Laptopum ve internet aracısındaki trafik ilk olarak FreeBSD

kullandığı meri şifre noktam tarafından şifrelenip tünelleniyor. Böylece laptop`um ve erişim noktam (Accesspoint) arasındaki bilgileri yakalay an her hangibirki şifre bilgileri anlayamıyor.

## Ipsec kurulumu

### IKE

İlk olarak her iki istemciyi IKE yani Internet Key Exchange kullanmaları için ayarlamamız gerekiyor. IKE Ipsec`in fazlasıyla da olan şifre anahtarlarını istemciler arasında güvenli şekilde geçirmesine olanak tanıyor. FreeBSD`de IKE FreeBSD4.0 ve üstü versiyonlarında standart olarak gelen racoon`d eamon`u tarafından idare ediliyor. Uyumluluk konusunda emin olmak için her iki istemci üzerinde aynı versiyonu işletim sistemi kullanılabiliyor.

Racoon`u /usr/ports/security/racoon dosyası içinden yükleyebiliyoruz. Bunun için tek yapmamız gereken

```
kullanici$: su
password:
root$: cd /usr/ports/security/racoon
root$: make & install & clean
```

Racoon programının konfigürasyon dosyası standart yüklemelerle /usr/local/etc/racoon/racoon.conf olarak belirleniyor ve yanına bir depke.txt dosyası ile geliyor. .conf dosyası üzerinde çok fazla oynamamız gerek olmamasına rağmen life time xxx <min|sec|hour|> bölümünde bulunan anahtar süreleri (Key lifetimes) ile oynamak isteyebilirsin iz. Kısacası söylemek gerekirse daha kısa anahtar süreleri`ları sizeda güvenli bir ortam sağlayacaktır. Bunun yanına daha uzun anahtar süreleri çok fazla işlemci gücünü yiyebilir ve yakurulu olan ba ğlantıları engelleyebilir.

Burada bizim için önemli dosya pkc.txt dosyası. Burada önemli olan budosyanın chmod 600 ve süper kullanıcıya ait olması gerekmektedir. Eğer bunlar sağlanmazsa racoon programı budosyayı okumayı reddedecektir. Bu dosya racoon`un ilk ba ğlantıyı kurması için gerekli olan daha önceden paylaşılmış anahtarları içermekte.

Örnek zamanı. Mason (10.0.0.2), tünel sunucusu ve gl uon (10.0.0.77) arasında tünel kurmayı deneyelim. Hepsinde kullanılacak olan ön-pa ylaşım anahtarı Macplusbsdcool.Mason`da bulunan pkc.txt dosyası:

```
10.0.0.77 macplusbsdcool
```

şeklinde görürüzükürken, Gluon`da:

```
10.0.0.2 macplusbsdcool
```

Şeklinde olmalı. Şimdi her iki istemci de daemon'ları başlatalım:

```
/usr/local/sbin/racoon -f \
/usr/local/etc/racoon/racoon.conf -l /var/log/racoon.log
```

## Kurallar

Şu anda her iki istemci de anahtarları değiştirilmemiş haldedir ve bu yapıları gerektirmediğini bilmiyorlar. Bunun için son olarak her iki istemci üzerinde, istemcilerin IPsec kurallarının ne zaman ve nasıl uygulanması gerektiğini belirtecek IPsec kurallarını belirlememiz gerekecek. Bunun için `setkey` komutunu kullanacağız. Bu açacağımız tünelle devamlı açık kalmasını isteyeceğimizi tüm kuralları bir dosyaya koyup `setkey`'in bu dosyadan okumasını isteyeceğiz:

```
pico /etc/rc.conf
setkey -f /etc/ipsec.rules
```

Tünelleme için istemci paketlerinin masanın üzerinden güvenli hale getirilip oradan hedefe ulaştırılmasını istiyoruz. Bunun için `gluon` üzerindeki `onfigürasyon` dosyası:

```
spdadd 10.0.0.77 0.0.0.0/0 any -P out ipsec
esp/tunnel/10.0.0.77-10.0.0.2/require;
spdadd 0.0.0.0/0 10.0.0.77 any -P in ipsec
esp/tunnel/10.0.0.2-10.0.0.77/require;
```

Şeklinde olurken `Masondaise`:

```
spdadd 0.0.0.0/0 10.0.0.77 any -P out ipsec
esp/tunnel/10.0.0.2-10.0.0.77/require;
spdadd 10.0.0.77 0.0.0.0/0 any -P in ipsec
esp/tunnel/10.0.0.77-10.0.0.2/require;
```

Olmalı. Satırları sınırımı yeterince açık; `spdadd` yeni bir IPsec kuralı eklemek istediğinizi, `any` kuralının bütün protokolleri içine gerektirdiğini, `out` ve `in` paketin hareket ettiği yönü belirtiyor. Son olarak `esp/.../require` kernelin IPsec tünelle modunda kullanması gerektiğini ve bunun yazılı olan birinci ipden ikinci ip'ye yapmasını belirtiyor.

Busenaryonun IPv6 daçalı şması için gerektirdiği şey IPv4 yerine IPv6 adreslerinin kullanılmasını olacaktır. Her iki makinede `setkey` komutunu kullanarak kuralları etkinleştirin.

## Sıra Testte

Testiçinyapmamızgerekençokbasit. Şubizimeskiveherderdedevadostumuzu kullanacağız.

```
ping 10.0.0.1
```

BağlantınızınIpsec`ikullanıpkullanmadı ğınıanlamakiçinise tcpdump`iistemci üzerindekiullanıpyakaladı ğımızpaketlerebirgözatalım:

```
tcpdump -a -vv -i tun0
```

```
13:58:39.045831 gluon > mason: ESP(spi=0x099e806d,seq=0x723)
13:58:39.046566 mason > gluon: ESP(spi=0x0d8d15b6,seq=0x6b2)
13:58:39.187444 gluon > mason: ESP(spi=0x099e806d,seq=0x724) (frag
64877:1480@0+)
```

Bu şekildebirçıkırtalıyorsanızher şeyyolundademektir.

EğerESPdı şıherhangibirtrafikgörüyorsanızisebir şeyleryanlı şgidiyordemektir.Bu durumda İstemciüzerindevarisadresinin 0.0.0.0/0oldu ğundaneminolun.E ğerhiçbir ESPtrafi ğigöremiyorsanıziseikimakinüzündebelirledi ğimizkurallarıkontrolledip doğruluğundanvepke.txtdosyalarında yazılananahtarların aynioldu ğundanemin olun.Eğeryinebirproblembulamıyorsanızsonçareolarak /var/log/racoon.log dosyasınabirgözatin.

Biröneridaha.E ğermakinelerdenbirinibootettiysenizveba ğlantısorunubundansonra başlamışiseikiistemciüzünde kianahtarları setkey -Fkomutuiletemizleyin.Tekrar başlatmaışlemimuhtemelenanahtarlarında ğişikliğeu ğramasınayolaçmı ştır.

## Sonuç

Şuandaçalı şanbirIpsectünelinizolmasıvebilgilerinizekims eninmüdahale edemeyeceğibirortamınkeyfinigönülrahatlı ğıyla şayabilirsiniz

ÖzgürÖzdemircili

<http://www.enderunix.org>

<http://news.enderunix.org>

<http://haber.enderunix.org>

Sorularınızıçin: [dionypheles@gmx.net](mailto:dionypheles@gmx.net)

## **Kaynaklar**

*MikeDeGraw-Bertsch* `in“IpsectunellingbetweenFreeBSDhosts”adlıya zısından çevrilmiştir.

Yazar`insayfasına <http://www.onlamp.com/pub/au/188>,orijinalmetneise <http://www.onlamp.com/pub/a/bsd/2001/12/10/ipsec.html> adresindenula şabilirsiniz.