/***\
* **Gökhan ALKAN**
* gokhan [at] enderunix [dot] org
* EnderUNIX Yazılım Gelistirme Takımı
* http://www.enderunix.org
*
* Sürüm : 1.0
* Tarih : 06.08.2006
* Makalenin en yeni versiyonuna http://www.enderunix.org/docs/stunnel.pdf
* adresinden elde edilebilir.
***/

1 STUNNEL NEDİR?

İstemci ile sunucu arasında ssl tetikleyici uygulaması olarak çalışır. Unix ve Windows ortamlarında çalışabilir. POP, IMAP, LDAP gibi doğasında şifreleme özellikleri bulunmayan protokoller için aracı vazifesi görür.

2 STUNNEL KURULUMU

2.1 Kaynak Koddan Kurulum

Öncelikle stunnel temin edilmelidir. http://www.stunnel.org/download/source.html adresinden temin edilebilir.

```
$ cd /home/galkan
$ fetch http://www.stunnel.org/download/stunnel/src/stunnel-4.15.tar.gz
$ tar -zxvf stunnel-4.15.tar.gz
$ cd stunnel-4.15
$ ./configure –prefix=/usr/local/stunnel
$ make
$ su root
#  make install clean
```

…
…
Country Name (2 letter code) [PL]:TR
State or Province Name (full name) [Some-State]:Kocaeli
Locality Name (eg, city) []:İzmit
Organization Name (eg, company) [Stunnel Developers Ltd]:EndersSYS
Organizational Unit Name (eg, section) []:EnderUNIX
Common Name (FQDN of your server) [localhost]:www.endersys.com

…
…
#

Sertifika için gerekli bilgiler girildikten sonra yapılandırma dosyasındaki ayarlamalar yapılmalıdır. Burada önemli olan Common Name (FQDN of your server) bölümüdür. *–prefix* değeri ile */usr/local/stunnel* dizini verildiği için stunnel /usr/local/stunnel dizini altına kurulmuştur.

```
# cd /usr/local/stunnel/
# ls –al
drwxr-xr-x  3 root  wheel  512 Jul 10 17:09 etc
drwxr-xr-x  2 root  wheel  512 Jul 10 17:09 lib
drwxr-xr-x  3 root  wheel  512 Jul 10 17:09 man
drwxr-xr-x  2 root  wheel  512 Jul 10 17:09 sbin
drwxr-xr-x  3 root  wheel  512 Jul 10 17:09 share
drwxr-xr-x  3 root  wheel  512 Jul 10 17:09 var
#
```

2.2 FreeBSD Port Ağacından Kurulum

Stunnel FreeBSD port ağacında /usr/ports/security/stunnel dizi altında bulunur. Kurulum için

```
# cd /usr/ports/security/stunnel
# make
```

Ekrana gelen curses tabanlı menüden istenilen özellikler seçilebilir.

```
[ ] FORK      use the fork(3) threading model
[X] PTHREAD   use the pthread(3) threading model (default)
[ ] UCONTEXT  use the ucontext(3) threading model
[ ] IPV6      enable IPv6 support
```

```
# make install
```

Stunnnel kurulumu tamamlandıktan sonra yeni bir sertifika oluşturmak için aynı dizin içerisinde *make cert* komutu verilir.

```
# make cert
```

…
…
Country Name (2 letter code) [PL]:TR
State or Province Name (full name) [Some-State]:Kocaeli
Locality Name (eg, city) []:İzmit
Organization Name (eg, company) [Stunnel Developers Ltd]:KOU
Organizational Unit Name (eg, section) []:KOU - Bilgi İşlem Daire Başkanlığı
Common Name (FQDN of your server) [localhost]:KOU - Bilgi İşlem Daire Başkanlığı
…
…

Stunnel'in her açılışta etkin olabilmesi */etc/rc.conf* dosyasında aşağıdaki şekilde belirtilmesi gerekmektedir.

```
# edit /etc/rc.conf
stunnel_enable="YES"
```

Bunun yanında yapılandırma dosyası için *stunnel_config="/path/stunnel.conf"* ve *stunnel.pid* dosyası içinde *stunnel_pidfile="/path/stunnel.pid"* ile belirtilebilir. Yapılandırma dosyası için ön tanımlı değer *"/usr/local/etc/stunnel/stunnel.conf*" stunnel.pid dosyası için ön tanımlı değer ise *"/usr/local/var/stunnel/stunnel.pid"* dır.

3 STUNNEL YAPILANDIRMASI

Kurulum ile beraber örnek bir yapılandırma dosyası gelmektedir. Yapılandırma için bu dosya kullanılabilir.

```
# cd /usr/local/etc/stunnel
# cp stunnel.conf-sample stunnel.conf
# vi stunnel.conf
```

cert = /usr/local/etc/stunnel/mail.pem
cert ile kullanılacak olan sertifikanın tam yeri belirtiliyor

setuid = stunnel
stunnel'in hangi kullanıcı ile çalışacağı belirtiliyor.

setgid = stunnel
stunnel'in hangi grup ile çalışacağı belirtiliyor. FreeBSD port ağacından kurulum yapıldığında stunnel adı ile grup ve kullanıcı oluşturulmaktadır. Kaynak koddan kurulumda ise nobody kullanıcısı ve nogroup grubu ile gelmektedir. İsteğe kullanıcı ve grup oluşturularak bu değerler değiştirilebilir.

[pop3s]
accept = 995
connect = 110

Bu şekilde bir tanımla ile pop3s servisi için 995 numaralı portun kullanılacağı belirtiliyor. Yine aynı şekilde https servisi içinde örnek yapılandırma

[https]
accept = 443
connect = 80

şeklinde olmalıdır. Örneğin mysqls servisini çalıştırabilmek için aşağıdaki gibi bir tanım yapılabilir.

[mysqls]
accept = 3309
connect = 3306

Chroot değeri için verilen dizin izinleri ile beraber oluşturulmalıdır.

```
# mkdir /var/tmp/stunnel
# chown stunnel:stunnel /var/tmp/stunnel
# chmod 700 /var/tmp/stunnel
```

Kurulum ile beraber sertifika gelmektedir(stunnel.pem). İstenirse oluşturulabilir.

```
# openssl req -new -x509 -days 3650 -nodes -out stunnel.pem -keyout
stunnel.pem
```

Çalışma dizininde *stunnel.pem* oluşmaktadır. Bu sertifikayı *stunnel.conf* dosyasında belirtilen dizin altına konulmalıdır.

4 STUNNEL ÇALIŞTIRILMASI VE HATA TAKİBİ

FreeBSD Port ağacından kurulduğunda hazır betiklerde sisteme kurulmaktadır.Stunneli çalıştırmak için

```
# /usr/local/etc/rc.d stunnel.sh start
```

Stunnel'i durdurmak için

```
# /usr/local/etc/rc.d/stunnel.sh stop
```

ile durdurulabilir.

Yada kaynak koddan kurulum gerçekleşti ise stunnel ikilisi çalıştırılır.

```
/usr/local/stunnel/sbin/stunnel
```

ps komutu ile çalışması kontrol edilebilir.

```
# ps –auwx | grep 'stunnel'
stunnel 82988 0.0 0.1 3684 2896 ?? Is 5:02PM 0:00.05 /usr/local/sbin/stunnel
/usr/local/etc/stunnel/stunnel.conf
#
```

servisler port numaralarından da çalışıp çalışmadığı kontrol edilebilir. Örneğin mysqls servisi için

```
# netstat –na | grep '3309'
tcp4       0      0  *.3309                 *.*                    LISTEN
#
```

Stunnnel log'larını stunnel.conf dosyasında belirtilen output değerindeki dosyaya basar.

```
# edit /usr/local/etc/stunnel.conf
```

debug = 7
output = /var/log/stunnel.log
#

debug 0 ve 7 dahil 8 farklı değer alabilir. "7" değeri ile stunnel çalışması hakkında en fazla bilgi alınabilir. Ön tanımlı değeri "5"'tir.

Output değeri ilede stunnel loglarının yazılacağı dosya belirtilmektedir. Stunnel logları izlenebilir.

 # tail –f /var/log/stunnel.log
…
…
2006.07.10 23:22:28 LOG7[12750:134723072]: Connection from 127.0.0.1:59445 permitted by libwrap
2006.07.10 23:22:28 LOG5[12750:134723072]: mysqls connected from 127.0.0.1:59445
2006.07.10 23:22:28 LOG7[12750:134723072]: SSL state (accept): before/accept initialization
2006.07.10 23:22:28 LOG7[12750:134635520]: Cleaning up the signal pipe
2006.07.10 23:22:28 LOG6[12750:134635520]: Child process 12772 finished with code 0
2006.07.10 23:22:31 LOG3[12750:134723072]: SSL_accept: 140760FC: error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol
…
…

5 ÇIKABİLECEK SORUNLAR VE ÇÖZÜM YOLLARI

wrong permissions on /usr/local/etc/stunnel/stunnel.pem

Sertifika izinlerinde problem var demektir gerekli izinler verilerek sorun çözülebilir. İzinler aşağıdaki gibi değiştirilmelidir.

```
# chown root:wheel stunnel.pem
# chmod 600 stunnel.pem
```

FreeBSD Port ağacından kurulum yapıldı ancak /usr/local/etc/rc.d/stunnel.sh ile stunnel durdurulduğunda stunnel not running? (check /var/run/stunnel.pid) gibi bir mesaj alınıyor ve stunnel çalışıyor görünüyorsa eğer

Stunnel örnek yapılandırma dosyasında *chroot* değeri *"/var/tmp/stunnel"* dizinidir *ve* stunnel uygulaması için stunnel.pid'si *pid = /stunnel.pid* değeri ile bu dizin altında oluşturulmaktadır. Betik ise pid dosyasını /var/run/stunnel.pid olarak aramaktadır. /usr/local/etc/rc.d/stunnel.sh dosyasında stunnel.pid dosyasının yeri çözülerek sorun giderilebilir. stunnel_pidfile="/var/run/${name}.pid" olan satır

```
# vi /usr/local/etc/rc.d/stunnel.sh
stunnel_pidfile="/var/tmp/stunnel/${name}.pid"
#
```

olarak değiştirilerek sorun çözülebilir. Yada yapılandırma dosyasında belirtilen dizinlere göre ayarlanabilir.