Stunnel

Położenie: (nie dotyczy)

Informacje ogólne

- Program typu klient-serwer, służy do tunelowania protokołu TCP (także *pop3, smtp, http, imap, nntp, ppp, ldap, cifs*) za pomocą SSL. Wyjątkiem jest protokół FTP (bo działa jednocześnie na kilku dynamicznie przydzielanych portach). Stunnel pozwala na proste zestawienie komunikacji serwerów nie posiadających funkcjonalności SSL poprzez bezpieczne kanały SSL.
- Do działania potrzebuje *OpenSSL*.
- Dystrybucja na licencji GPL.
- Posiada wersje na *Windows* i *Linux*.
- Program nie wymaga praw administratora.
- Strona domowa: *http://www.stunnel.org*.

Certyfikaty

Podczas instalacji serwera *Stunnel* tworzony jest samopodpisujący się certyfikat *.pem (można go również stworzyć przy pomocy *OpenSSL*). Klient sprawdza ten certyfikat i go akceptuje, gdy serwer potwierdzi autentyczność swojego certyfikatu za pomocą swojego klucza prywatnego. Zawartość certyfikatu *.pem powinna mieć następującą postać:

-----BEGIN RSA PRIVATE KEY-----
[zakodowany klucz]
-----END RSA PRIVATE KEY-----
[pusta linia]
-----BEGIN CERTIFICATE-----
[zakodowany certyfikat]
-----END CERTIFICATE-----
[pusta linia]

Można go stworzyć za pomocą poleceń:
 # openssl req -new -x509 -days 365 -nodes -config stunnel.cnf -out stunnel.pem -keyout stunnel.pem
gdzie:
-x509 – samopodpisujący
-nodes – bez umieszczania hasła w certyfikacie
-config stunnel.cnf – plik konfiguracyjny dla *OpenSSL*
-out stunnel.pem – plik, w którym umieszczamy certyfikat
-keyout stunnel.pem – w tym samym pliku umieszczamy także klucz
Common Name (FQDN) – nazwa hosta, na którym działa Stunnel
 # openssl gendh 2048 >> stunnel.pem *(dodajemy do certyfikatu parametry Diffie-Hellmana)*
 # openssl x509 -subject -dates -fingerprint -in stunnel.pem *(wyświetla informacje o utworzonym certyfikacie)*

Przykładowa konfiguracja

Poniżej przykład konfiguracji klienta w *stunnel.conf*:

cert = cert.pem
; key = klucz.key (klucz do otwarcia certyfikatu podanego powyżej; powinien mieć prawa 600 dla właściciela)
client = yes (jeśli „no” lub brak tego wpisu, to pracuje w trybie serwera)
chroot = /usr/local/var/run/stunnel/ (procesy programu są „uwięzione” w tej lokalizacji; użytkownik na prawach którego uruchomiony jest Stunnel, musi mieć prawo zapisu do tego folderu)

[mysqls]
accept = 3308 (akceptuje połączenia wysyłane na port 3308; na serwerze będzie wpis „con-

nect=3308”)
connect = jakasDomena.pl:13308 (adres serwera Stunnel i jego port; w pliku konfiguracyjnym serwera będzie „accept=13308”)

[LDAP]
accept = 389
connect = jakasDomena.pl:1389

[apache]
accept = 1080
connect = jakasDomena.pl:1080

Ostatnia aktualizacja: 22 listopada 2016.