

ALOHA LOAD BALANCER

MISE EN ŒUVRE DU SSL BACKEND

« APPNOTES » #0022 — MISE EN ŒUVRE DU SSL BACKEND

Cette note applicative a pour vocation de vous aider à implémenter la gestion du SSL sur le backend (chiffrement des données avant connexion vers le serveur HTTPS) au sein de la solution ALOHA Load Balancer.

CONTRAINTE

Les serveurs Web attendent exclusivement des connexions SSL chiffrées.

OBJECTIF

Permettre que les requêtes non sécurisées (HTTP) arrivent à destination des serveurs Web de manière transparente pour les utilisateurs.

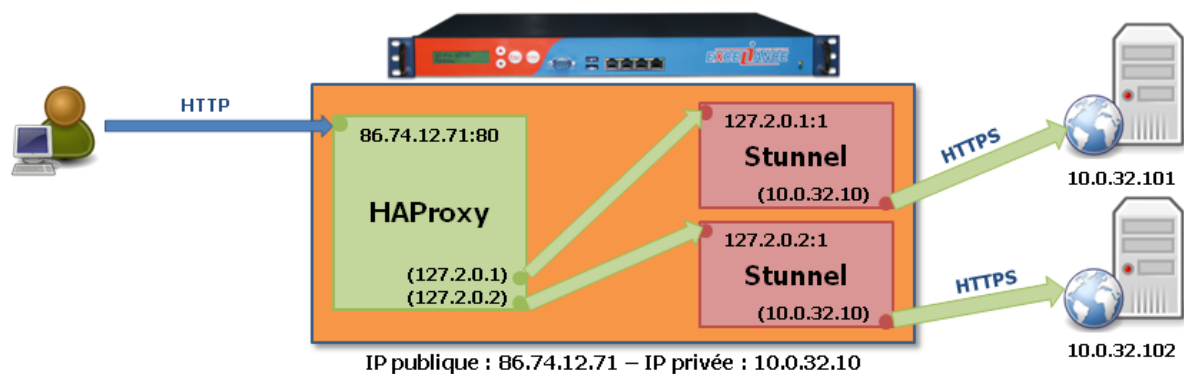
COMPLEXITE



VERSIONS CONCERNEES

V 3.x et ultérieures

SCHEMA CIBLE



EXTRAIT DE LA CONFIGURATION SSL

```
; Service-level configuration for backend
; receive haproxy traffic on 127.2.0.x
[ssl_backend_1]
client = yes
accept = 127.2.0.1:1
connect = 10.0.32.101:443

[ssl_backend_2]
client = yes
accept = 127.2.0.2:1
connect = 10.0.32.102:443
```

La configuration de Stunnel est accessible directement dans l'onglet SSL.

Lors d'une implémentation du SSL en mode frontend, seuls quelques paramètres sont à renseigner :

- le mode de fonctionnement : client ou non SSL (dans le cas présent, le module Stunnel devra être configuré en mode client. L'option «client = yes» devra être choisie),
- l'adresse et le port d'écoute des requêtes en provenance d'HAProxy,
- l'adresse et le port de redirection des requêtes à destination du serveur Web.

EXTRAIT DE LA CONFIGURATION LB NIVEAU7

```
##### The first public address as seen by the clients
frontend frt
  bind 86.74.12.71:80          # address:port to listen to
  mode http
  log global                  # use global log parameters
  option httplog              # Enable HTTP logging
  maxconn 4000                # max conn per instance
  timeout client 25s          # maximum client idle time (ms)
  default_backend bck         # send everything to this backend by default

##### This backend manages the servers and the load balancing algorithm
backend bck
  balance roundrobin          # roundrobin | source | uri | leastconn
  mode http
  log global                  # use global log parameters
  option httplog              # Enable HTTP logging
  cookie SERVERID insert indirect nocache # provide persistence with cookie
  option httpchk HEAD /       # how to check those servers
  option forwardfor except 127.0.0.1/8 # add X-Forwarded-For except local
  fullconn 4000               # dynamic limiting below
  timeout server 25s          # max server's response time (ms)
  server srv1 127.2.0.1:1 cookie s1 weight 10 maxconn 100 check inter 1000 fall 3
  server srv2 127.2.0.2:1 cookie s2 weight 10 maxconn 100 check inter 1000 fall 3
```

Après modification de la configuration de Stunnel et l'implémentation du(des) certificat(s), il ne reste plus qu'à modifier celle du niveau 7 qui est accessible directement dans l'onglet LB niveau7.

Il convient de modifier les adresses des serveurs de destination qui devront être identiques aux adresses IP des instances de Stunnel définies au niveau des paramètres «connect» dans la configuration du SSL.

DEMARRAGE DU SERVICE STUNNEL

IMPORTANT

En cas de première configuration du SSL, un message d'avertissement indique que le service «Stunnel» n'est pas démarré. Dans l'onglet Service, éditez la configuration du service Stunnel en cliquant sur le bouton «stunnel options».

```
service stunnel
##### The SSL tunnel Daemon
# config <dir>      : daemon configuration file
config /etc/stunnel/stunnel.conf
# no autostart # commenter le no devant autostart
```

Il ne reste plus qu'à démarrer le service en cliquant sur le bouton «démarrer».

