

Reverse proxy beállítása Apache szerveren

Apache szerverrel megvalósított reverse proxy beállítása tanúsítványok használatával

1. Tartalomjegyzék

1.	Tartalomjegyzék.....	2
2.	Bevezető	3
3.	A Reverse proxy funkcionalitás lényege.....	3
4.	Előzetes követelmények – A háttérszerver beállítása tanúsítványok használatára	4
5.	Kiadott tanúsítvány telepítése.....	5
5.1.	Példa a konfigurációs állományra.....	6

2. Bevezető

E tájékoztató célja, hogy leegyszerűsítse egy Apache szerverrel megvalósított Reverse Proxy funkcionalitás beállítását.

Kérjük, olvassa el figyelmesen és kövesse a leírtakat.

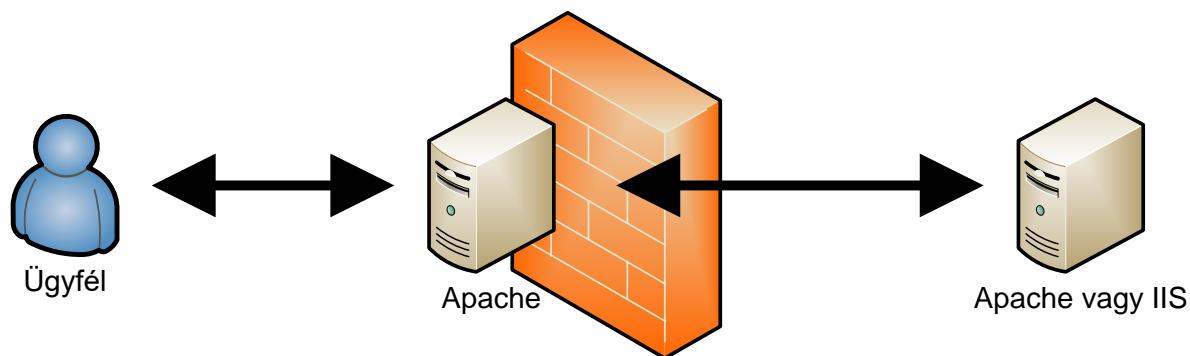
Amennyiben bármilyen kérdése van vagy problémája támad, Ügyfélszolgálatunk a(z) +36 1 437 6655 telefonszámon, az info@netlock.hu e-mail címen vagy személyesen a 1101 Budapest, Expo tér 5-7. szám alatt hétfőtől - csütörtökig 8:30 és 17 óra között pénteken 8:30 és 14 óra között készséggel áll rendelkezésére.

3. A Reverse proxy funkcionalitás lényege

Amennyiben egy olyan szerverrel rendelkezik, amely a szervezete/cége hálózatán belül szolgáltatást nyújt, előfordulhat, hogy egyes szolgáltatásokat kifelé is szeretne használni úgy, hogy közben nem akarja a szervert veszélynek kitenni.

Ilyen esetekben használhat Reverse Proxy funkcionalitást, melynek célja, hogy az Internetről elérhető szerver a tűzfalon csak meghatározott célokra jusson át a belső szerverre, és a belső szerver felé a Proxy szerver viselkedjen kliensként.

Ez biztonságnövelő megoldásként szolgálhat.



4. Előzetes követelmények – A háttérszerver beállítása tanúsítványok használatára

Ahhoz, hogy a Proxy a háttérszerverrel SSL kapcsolaton keresztül legyen képes kommunikálni, helyesen be kell állítani a tanúsítványok használatához.

Ehhez szerverspecifikus útmutatóinkat javasoljuk, melyek közül a megfelelőt a www.netlock.hu weboldal Terméktámogatás oldaláról tud letölteni.

Közvetlen link: <http://www.netlock.hu/html/termektamogatas.html#szerverek>

A háttérrendszer szempontjából a Reverse Proxy olyan, mintha egy hagyományos kliens lenne, így a háttérszerver beállítások az egyébként megszokott beállításokat követik.

5. Kiadott tanúsítvány telepítése

A tanúsítvány a kiadás után letölthetővé válik, amit másoljon fel szerverére, az Apache megfelelő könyvtárába, majd konfigurálja be a szerveret.

Az SHA256 –os kiadók és az onlinessl.netlock.hu oldalról igényelt tanúsítvány esetében szükséges beállítani az SSLProxyCACertificateFile opciót is.

Ehhez az alábbi címekről le kell töltenie a kiadói tanúsítványok egyikét:

Közjegyzői	(SHA256)	www.netlock.hu/index.cgi?ca=caca
Üzleti	(SHA256)	www.netlock.hu/index.cgi?ca=cbca
Expressz	(SHA256)	www.netlock.hu/index.cgi?ca=ccca
OnlineSSL	(SHA256)	www.netlock.hu/index.cgi?ca=olsslgca

5.1. Példa a konfigurációs állományra

```
#<VirtualHost *:443>

DocumentRoot /srv/www/vhosts/reverse
ServerName host1.akarmi.hu
ServerAdmin admin@akarmi.hu

SSLProxyEngine On
ProxyVia On

SSLEngine On

# saját tanusitvány es kulcs amely megtalalhato a hatterszerveren is

SSLCertificateFile /etc/apache2/ssl.crt/akarmi.crt
SSLCertificateKeyFile /etc/apache2/ssl.key/akarmi.key

# kiadoi tanusitványok beallitasa a fenti saját tanusitványhoz
# mert az Apache a mogotte levo szerver tanusitványait ellenorzi

#a kiadoi tanusitványnak a koztes kiadonak kell lennie

SSLProxyCACertificateFile /etc/apache2/cer/caca.cer
SSLProxyCACertificateFile /etc/apache2/cer/cbca.cer
SSLProxyCACertificateFile /etc/apache2/cer/ccca.cer

ProxyRequests off

ProxyPass / https://belsosite.akarmi.hu/

ProxyPassReverse / https://belsosite.akarmi.hu/

SetOutputFilter proxy-html
RequestHeader set Front-End-Https "On"
ProxyPreserveHost On

<Directory /srv/www/vhosts/reverse>
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

</VirtualHost>
```