

# HTTPS terminálása Server Name Indication TLS kiterjesztés használatával *Zorp Gateway*-en

2022. július 28.

Célunk a *Zorp Gateway* konfigurálása HTTPS Secure Sockets Layer (SSL) terminálására úgy, hogy Server Name Indication (SNI) Transport Layer Security (TLS) kiterjesztést is használunk.



# Tartalom

1. A probléma bemutatása .....	3
2. A megoldás bemutatása .....	4
3. Technikai megvalósítás .....	5
4. Konklúzió .....	8



## 1. A probléma bemutatása

Ha nem megoldható, hogy a HTTPS-en érkező kéréseket webszerverünk SSL terminálja, lehetőségünk van Zorp Gateway ezen kapcsolatok SSL terminálására. Ilyen esetben egyre gyakrabban van szükség az SNI TLS kiterjesztés használatára. SNI alkalmazása esetén egyazon IP cím és port használata esetén is lehetőségünk van különböző tanúsítványt felmutatni a kliens által elérni kívánt host név alapján.

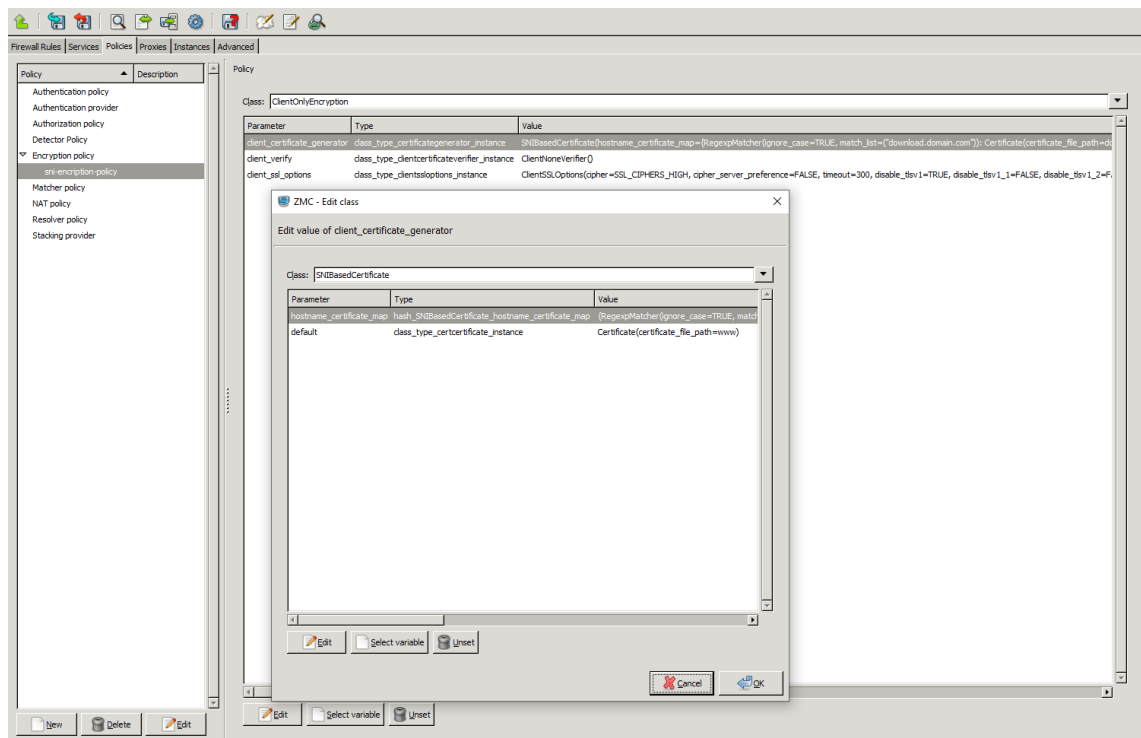


## 2. A megoldás bemutatása

*Zorp Gateway* Encryption policyban SNI alapú tanúsítvány (SNI-based certificate) generátor használatával SSL terminálni tudjuk a HTTPS-en érkező kéréseket.

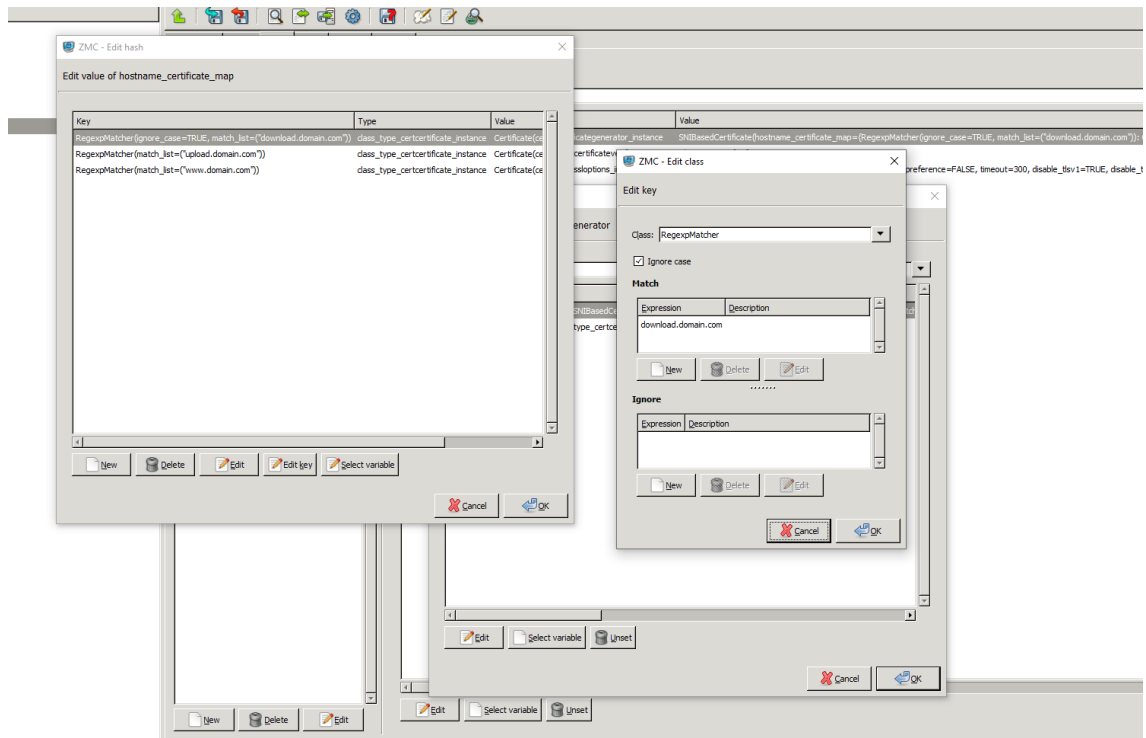
### 3. Technikai megvalósítás

1. Hozza létre vagy importálja a megfelelő tanúsítványokat a *Zorp Management Console (ZMC)* Public Key Infrastructure (PKI)-ban.
2. Hozzon létre egy Encryption policyt.
3. Konfigurálja a *client\_certificate\_generator* paramétert az SNI alapú tanúsítvány (SNI-based certificate) használatával.



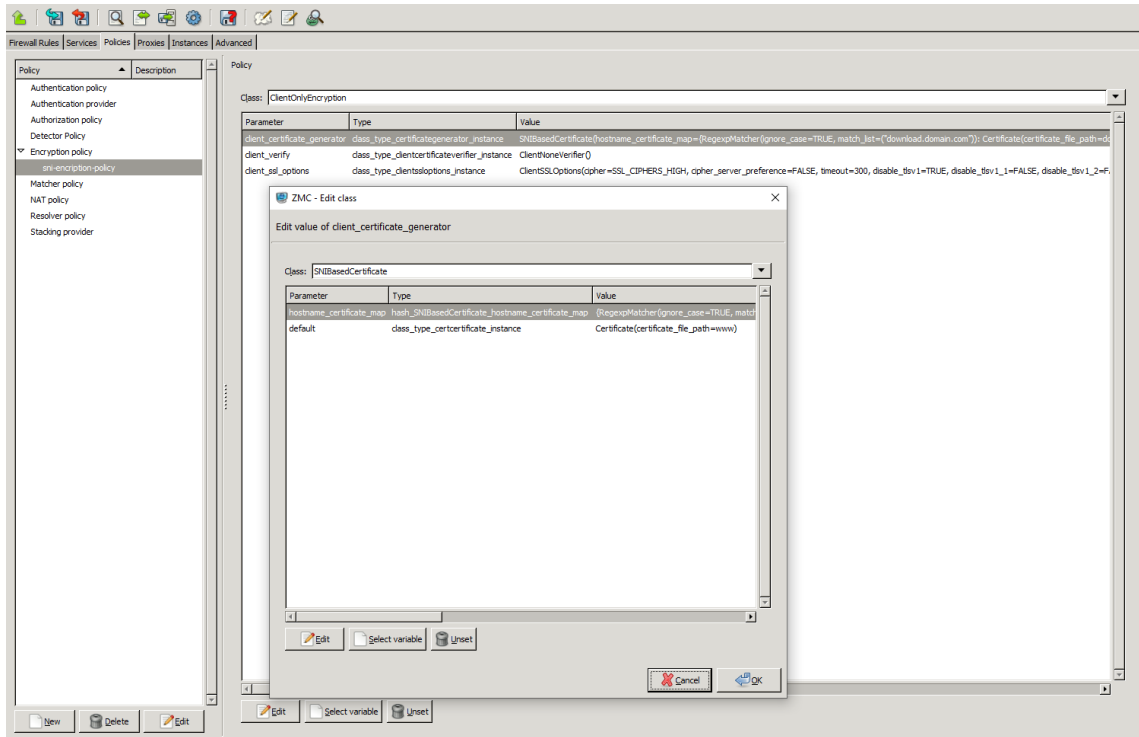
1. ábra - Client Certificate Generator szerkesztése

4. Állítsa be a domain tanúsítvány párokat a *RegexMatcher* segítségével.



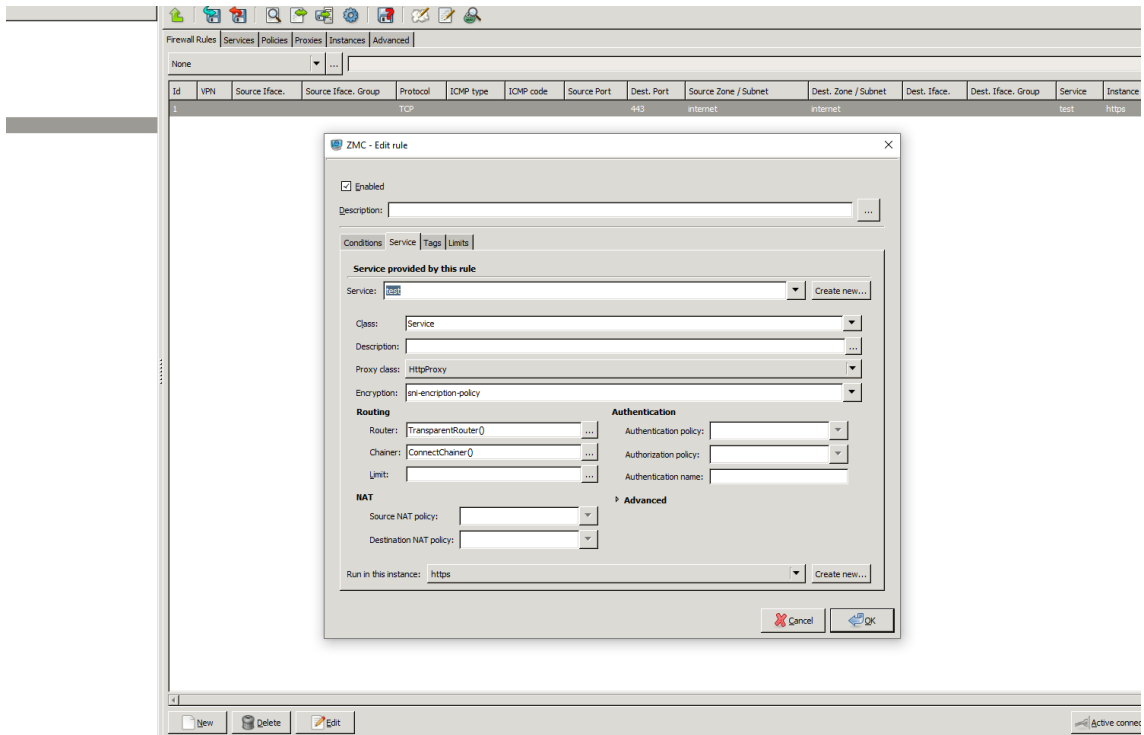
2. ábra - Domain tanúsítvány párok

5. Állítsa be a default tanúsítványt.



3. ábra - Default tanúsítvány beállítása

6. Használja fel a létrehozott Encryption policyt egy tűzfal szabályban.



4. ábra - Encryption policy használata



## 4. Konklúzió

A fenti leírás segítségével, a *Zorp Management Console (ZMC)* felületen tudunk SNI TLS kiterjesztés használatával HTTPS SSL terminálást beállítani a *Zorp Gateway* tűzfalunkon.

A funkcióról bővebb leírás a [\*How to configure HTTPS proxying\*](#) dokumentációban angol nyelven található.