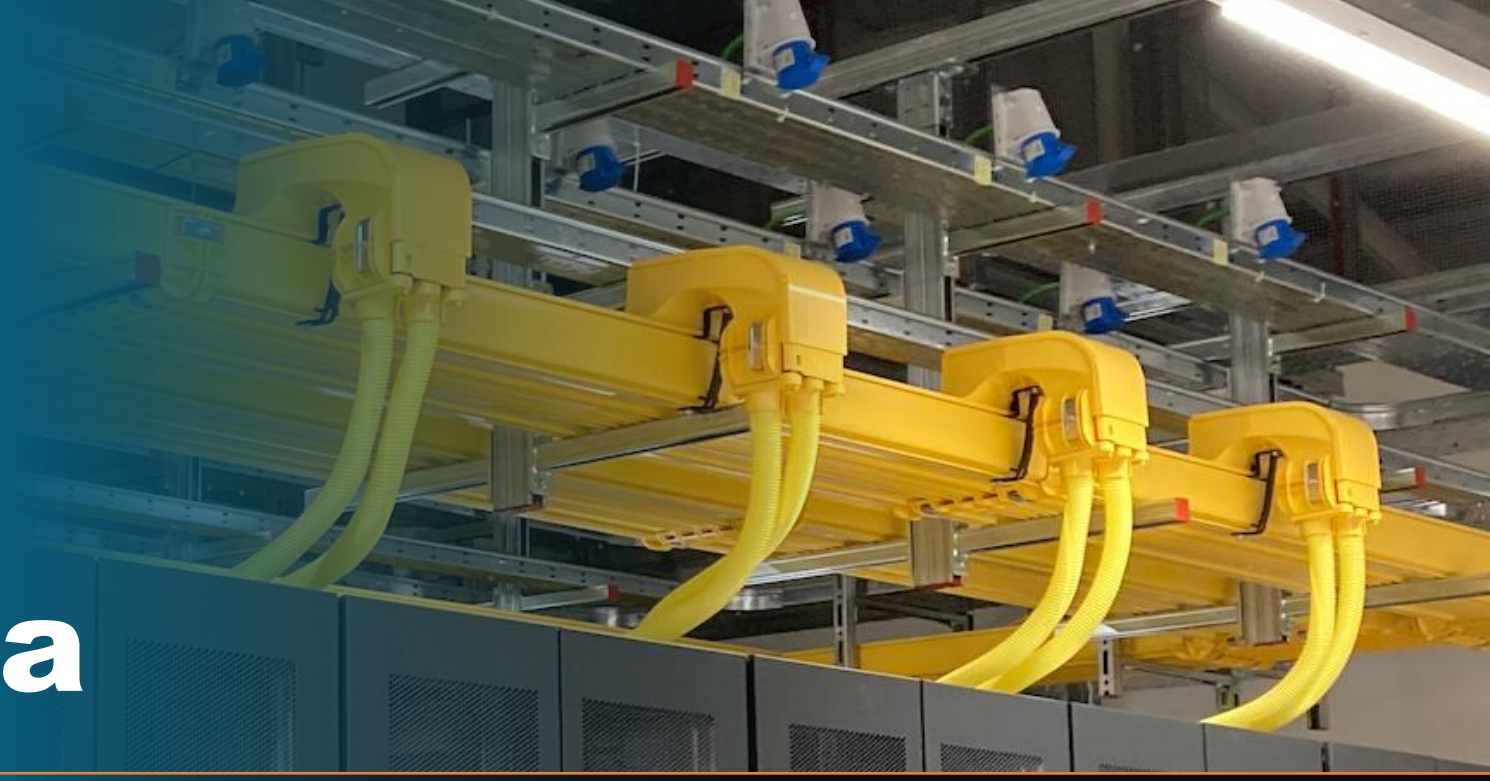


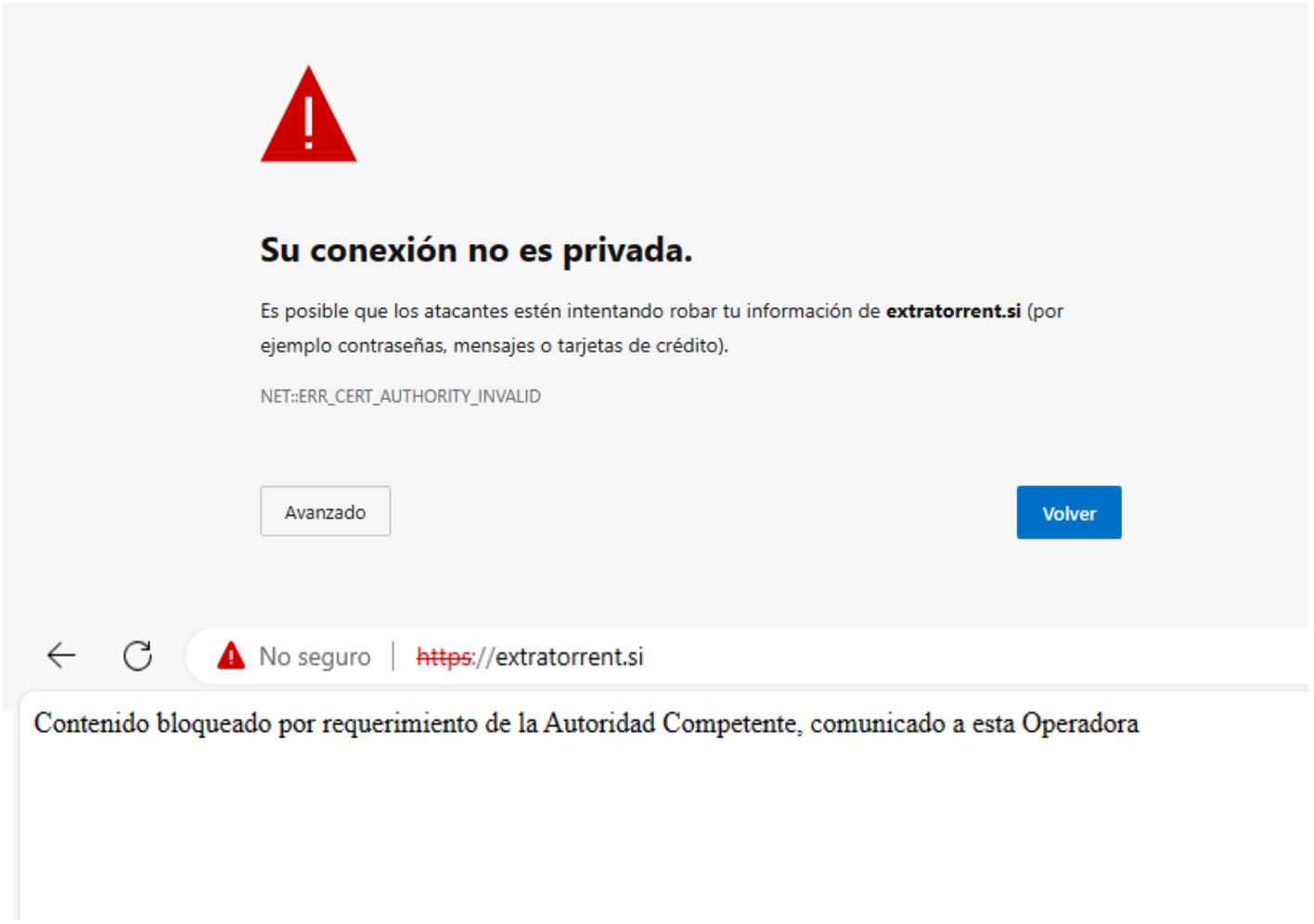
Tecnocrática

Centro de datos - SNI y TLS

TECNOCRÁTICA

¿Internet es un mundo feliz?

Suplantación del certificado



¿Por qué?

Demanda

Juzgado de lo Mercantil n[redacted] de Madrid.

Autos: [redacted]

Demandante: TELEFÓNICA AUDIOVISUAL DIGITAL, S.L.U.

Demandado: VODAFONE ESPAÑA, S.A.U., VODAFONE ONO, S.A.U., ORANGE ESPAGNE, S.A.U., MASMOVIL IBERCOM, S.A., EUSKALTEL, S.A., R CABLE Y TELECABLE TELECOMUNICACIONES, S.A.U., LYCAMOBILE, S.L., TELEFÓNICA DE ESPAÑA, S.A.U., TELEFÓNICA MÓVILES ESPAÑA, S.A.U.

SENTENCIA Nº.

En Madrid, a [redacted]

Vistos por mí, [redacted] los autos del Juicio Ordinario, procedo a dictar la siguiente resolución.

ANTECEDENTES DE HECHO.

PRIMERO.- Por la representación procesal de TELEFÓNICA AUDIOVISUAL DIGITAL, S.L.U. se interpuso demanda de Juicio Ordinario contra VODAFONE ESPAÑA, S.A.U., VODAFONE ONO, S.A.U., ORANGE ESPAGNE, S.A.U., MASMOVIL IBERCOM, S.A., EUSKALTEL, S.A., R CABLE Y TELECABLE TELECOMUNICACIONES, S.A.U., LYCAMOBILE, S.L., TELEFÓNICA DE ESPAÑA, S.A.U., TELEFÓNICA MÓVILES ESPAÑA, S.A.U. en fecha [redacted]

SEGUNDO.- Por decreto se admitió a trámite la demanda, dándose traslado de la misma a la parte demandada para su contestación. En el mismo escrito de contestación a la demanda, la parte demandada se allanó a las pretensiones de la demandante.

Fallo de la sentencia

Vistos los preceptos citados y demas de general y pertinente aplicacion,

FALLO.

Estimo totalmente la demanda interpuesta por la representación procesal de TELEFÓNICA AUDIOVISUAL DIGITAL, S.L.U. contra VODAFONE ESPAÑA, S.A.U., VODAFONE ONO, S.A.U., ORANGE ESPAGNE, S.A.U., MASMOVIL IBERCOM, S.A., EUSKALTEL, S.A., R CABLE Y TELECABLE TELECOMUNICACIONES, S.A.U., LYCAMOBILE, S.L., TELEFÓNICA DE ESPAÑA, S.A.U., TELEFÓNICA MÓVILES ESPAÑA, S.A.U., por lo que condeno a las demandadas a la siguiente medida de cesación de la actividad ilícita detectada, como medida de protección de los derechos de propiedad intelectual, afines o conexos, en Internet:

Fase 1: Acordar el bloqueo, por los Operadores de acceso a Internet, del acceso a las webs piratas identificadas a continuación en la presente resolución y en el punto sexto de los antecedentes de hecho de la demanda (listado adjunto con la Demanda en fichero txt), en toda su identificación como recurso web (URLs, Dominios, Direcciones IP), y bajo acceso en protocolos HTTP y HTTPs, en el plazo máximo de setenta y dos (72) horas desde la notificación de la Sentencia del presente proceso.

ID Nombre comercial URLs/Dominios ID IP

[redacted]

Bloqueos solicitados en la resolución

- URL
- Dominio
- Dirección IP
- Protocolo HTTP
- Protocolo HTTPS

HTTPS - HyperText Transfer Protocol Secure

- El envío de datos mediante HTTPS está protegido mediante TLS (Transport Layer Security) proporcionando:
  - Cifrado
  - Integridad de datos
  - Autenticación
- Necesitamos un certificado

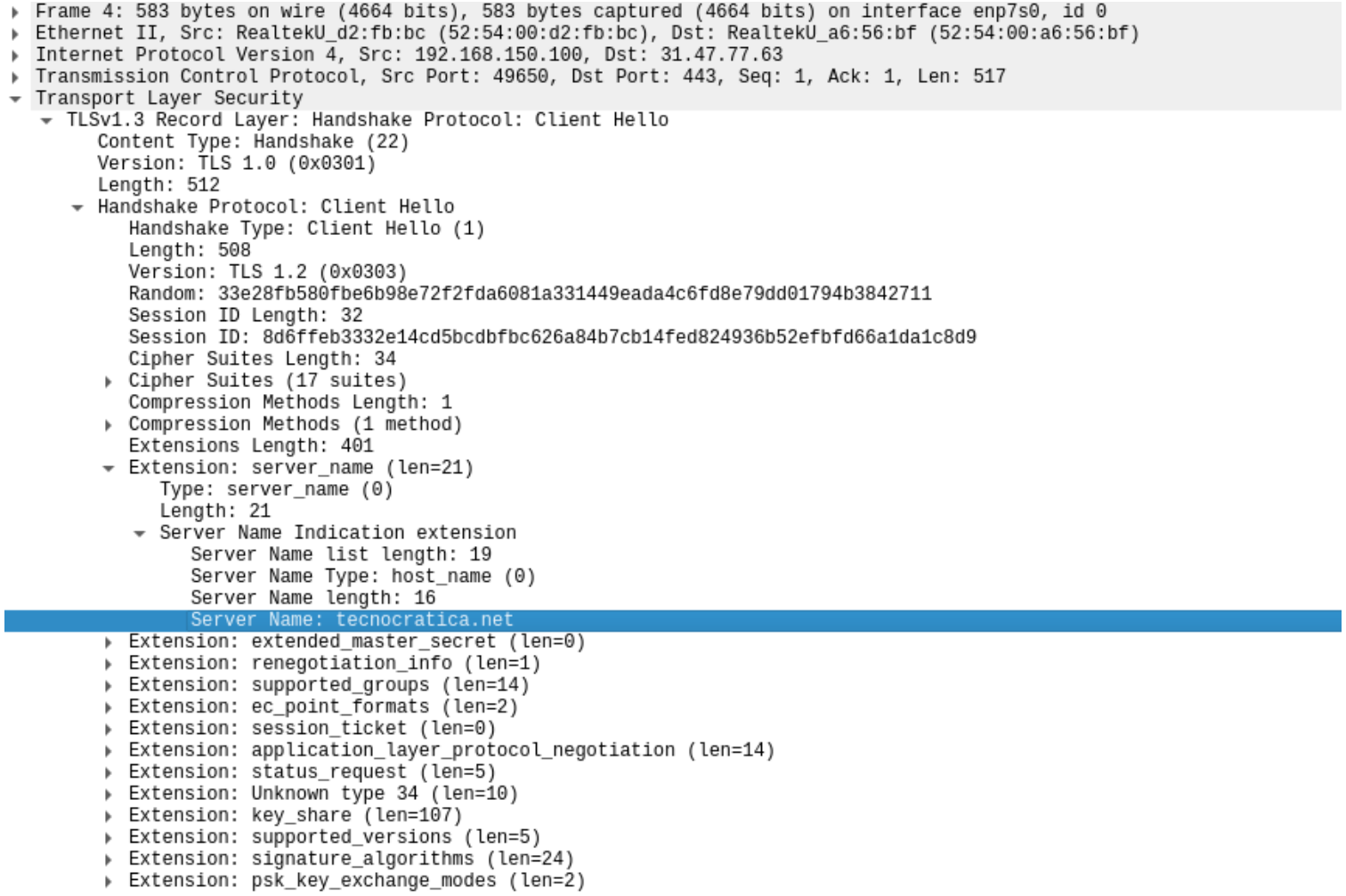
Certificado

- Los certificados tenían la limitación que se no permitían el disponer de varias webs en el mismo servidor, para eso se inventó la extensión de TLS: **SNI (Server Name Indicator)**.
- Gracias a SNI a día de hoy podemos tener certificados para todas las webs sin necesitar usar una IP por web.

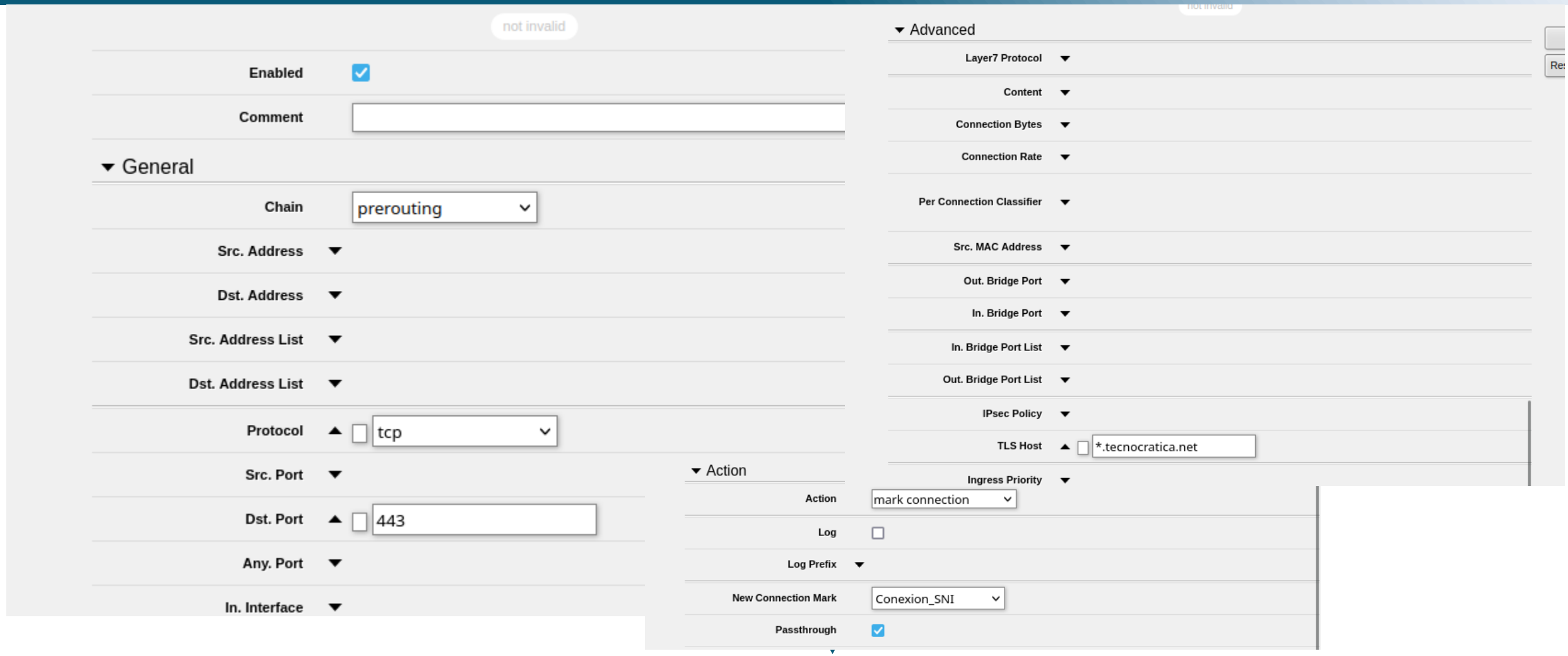
Problema de SNI

- Al usar HTTPS el handshake de TLS se realiza antes de la encriptación de HTTPS, así que podemos conocer la web que se va a visitar con HTTPS.
- Conclusión, es posible ver el nombre de la web y por tanto filtrarla.

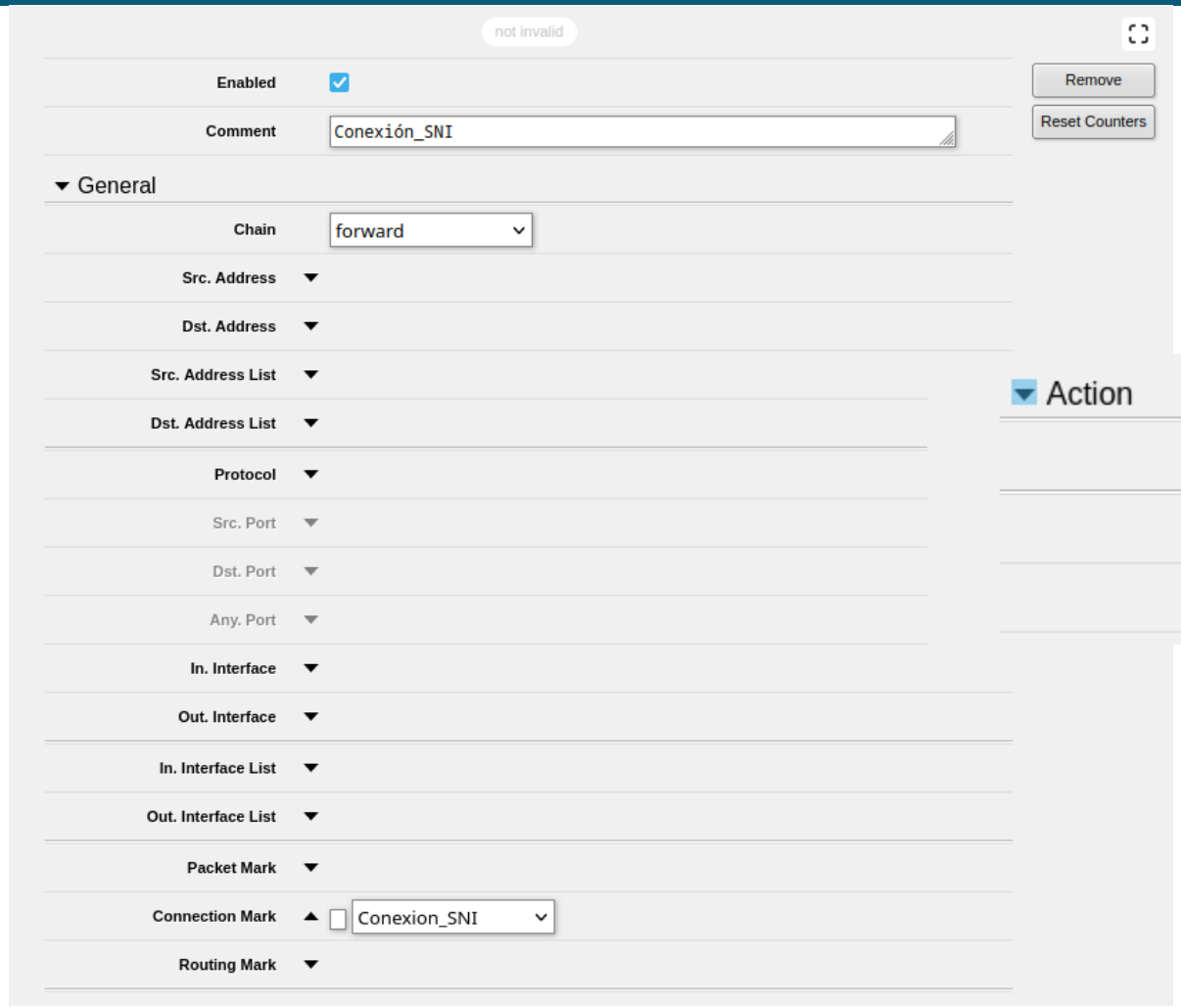
Ver el server name de SNI

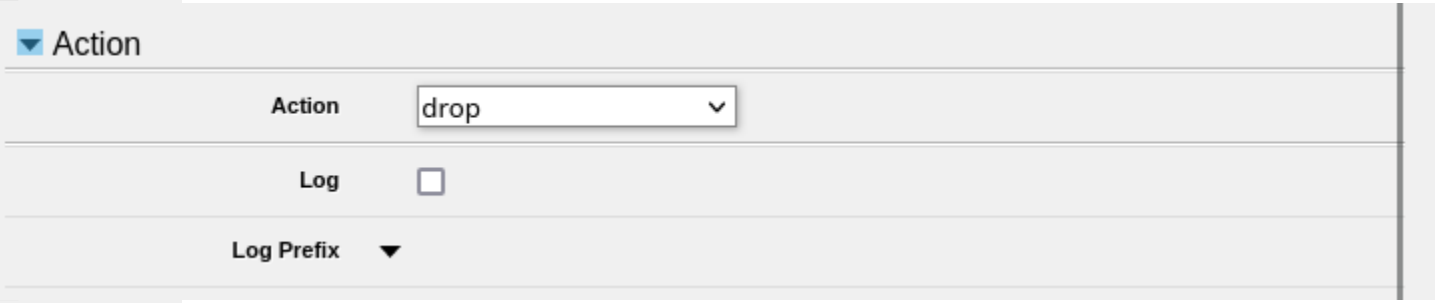


Marcado en Mikrotik



Descarte de tráfico en Mikrotik





Otras opciones

- ESNI (Encrypted SNI)
  - Tiene que soportarlo ambos extremos y no todos los servidores lo soportan.
  - Sólo soporta el problema del SNI, no vale para ALPN.
- ECH (Encrypted ClientHello)
  - Preferible, de hecho Firefox lo puso en la versión 85 para reemplazar el soporte de ESNI.

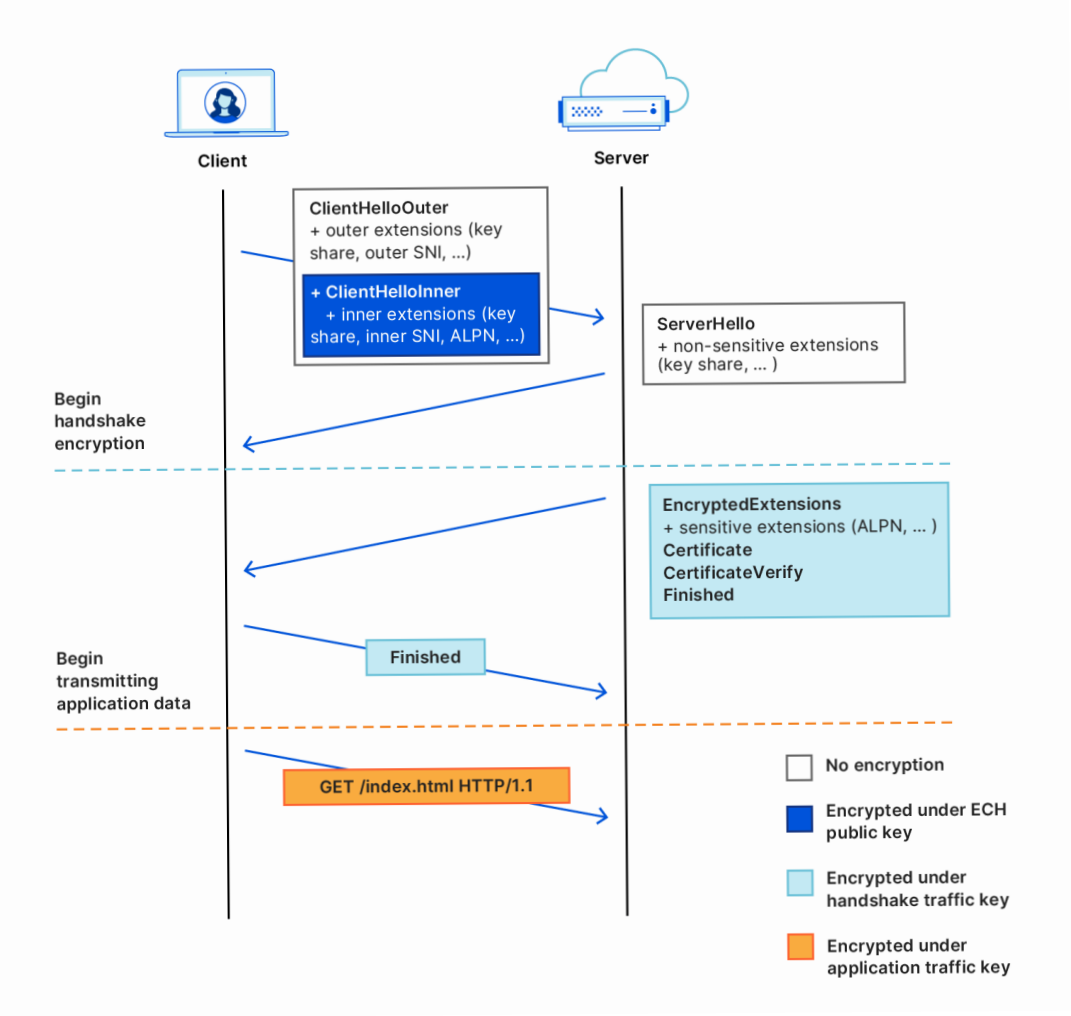
ECH (Encrypted ClientHello)

- El ECH hace que el handshake del TLS se mantenga secreto, y esto solucionaría el problema del SNI, pero no se queda en solucionar el problema del SNI, sino que soluciona todos los problemas generados por la negociación en plano del handshake del TLS.
- La extensión de TLS ALPN que decide qué protocolo superior se usará una vez realizado el handshake de TLS también se solucionaría con el ECH pues ya no se podrá ver en los paquetes al ir encriptada.

Cómo funciona TLS 1.3 sin ECH

- En un primer momento el cliente envía el ClientHello con la clave compartida. En ese mismo mensaje además viaja el SNI y el ALPN entre otros. Todo esto sin cifrar porque no ha habido aún intercambio de claves.
- El servidor contesta con el ServerHello que tiene la clave compartida del servidor. Este mensaje también va sin encriptar.
- A partir de aquí el cliente ya conoce su llave y la del servidor, con lo que ya se puede encriptar porque ya hemos tenido el intercambio de llaves
- El primer mensaje encriptado va desde el servidor al cliente y es el EncryptedExtensions donde se envían los parámetros sensibles del servidor como por ejemplo el ALPN del servidor y por supuesto el certificado.

Handshake de TLS 1.3 con ECH



Muchas gracias

C/ Salvatierra 4, 28034, Madrid, Spain
(+34) 910 059 045
comercial@tecnocratica.net

https://tecnocratica.net

https://twitter.com/TecnocraticaCPD

https://www.youtube.com/@TecnocraticaNet

https://www.linkedin.com/company/tecnocratica