Clase de Seguridad

Capa de (?)

DC - FCEyN - UBA

8 de Noviembre de 2017

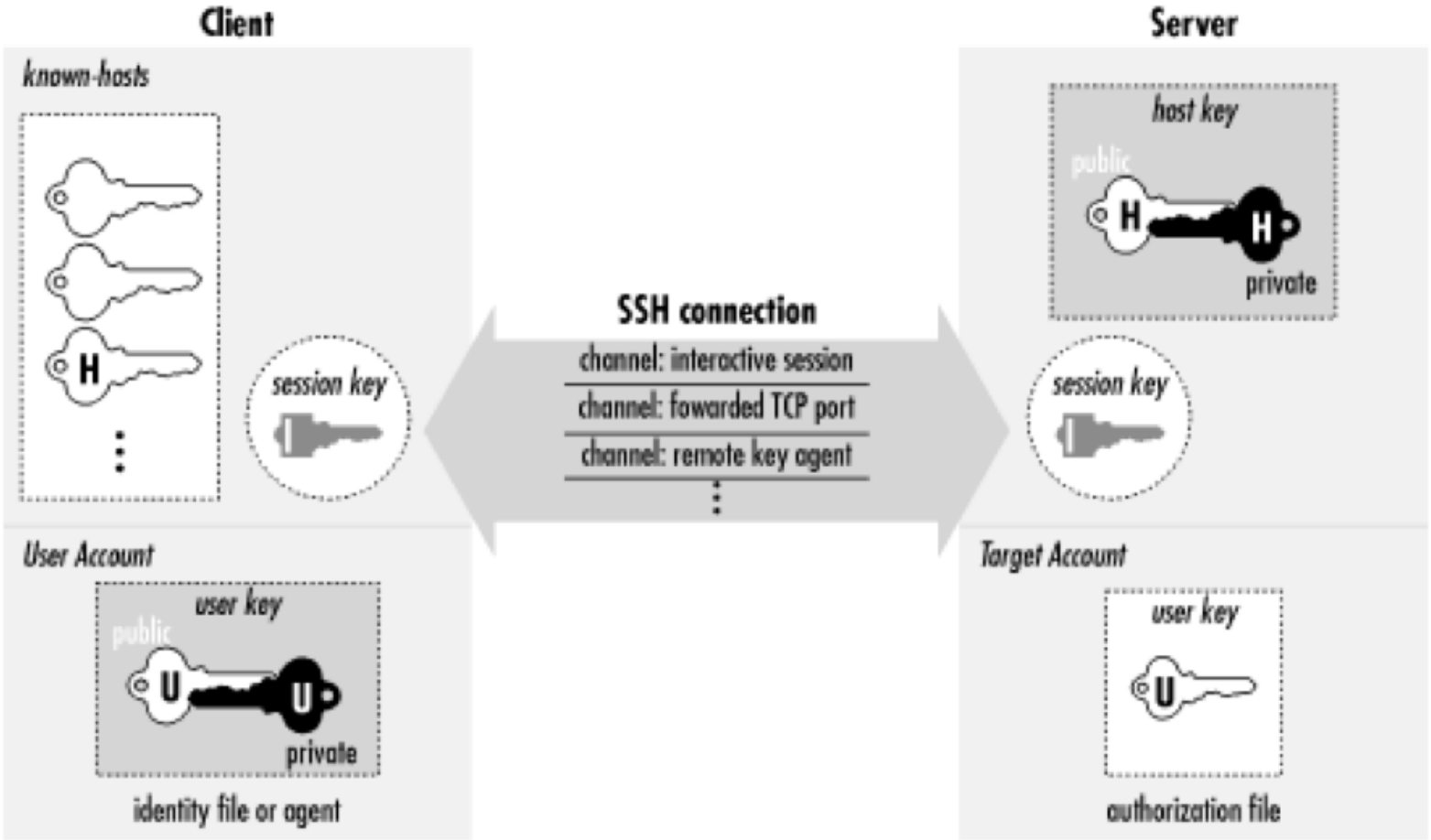
SSH

Es un protocolo para acceder a máquinas remotas de manera segura

- Alternativa segura a Telnet y FTP.
- Provee autenticación, confidencialidad e integridad.
- Permite hacer cosas más avanzadas como redirigir la salida de aplicaciones a través de canales seguros (port forwarding).
- Ese es un caso particular de túneles seguros.

Las fases SSH son similares a las fases TLS.

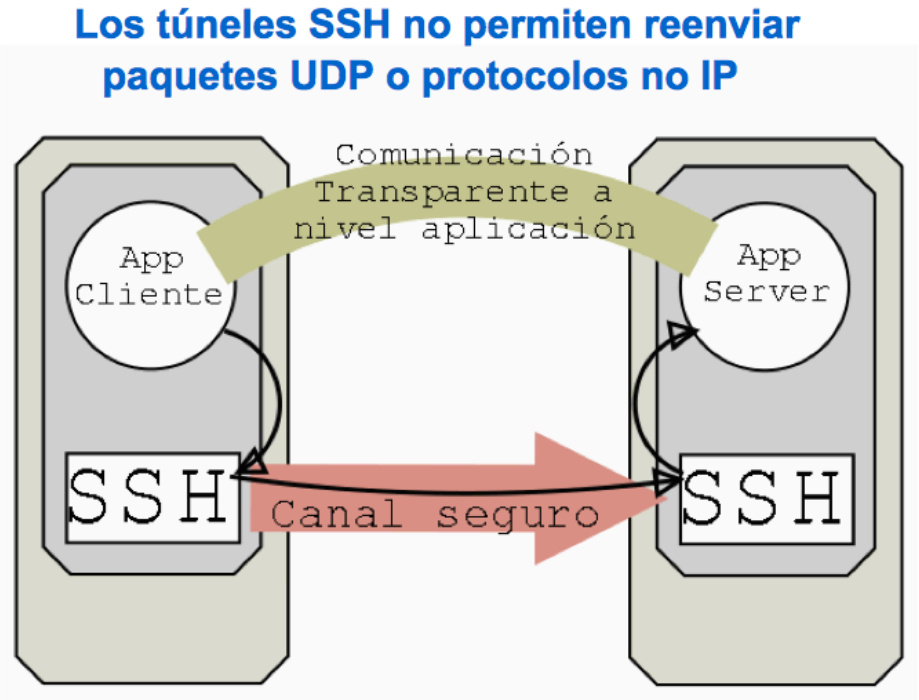
Handshake SSH a alto nivel



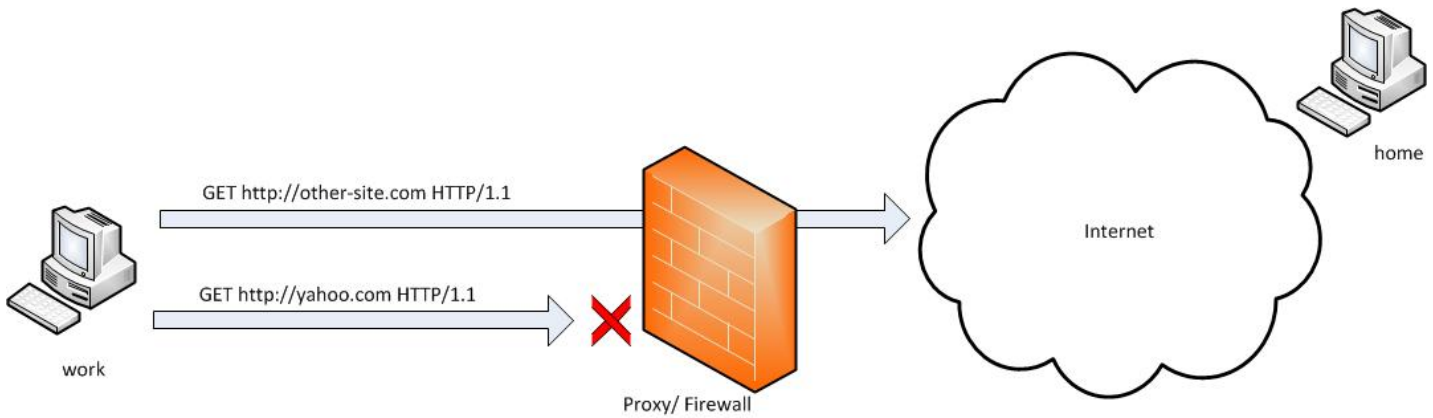
Túnel SSH

Sirven para:

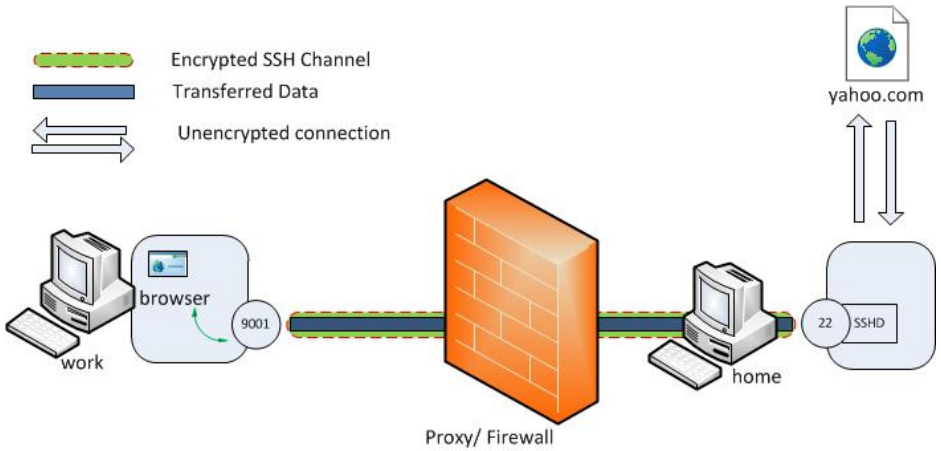
- proteger claves de protocolos inseguros (FTP, Telnet, IMAP).
- Atravesar Firewalls (si permiten ssh).
- Acceder a servicios internos de una LAN con ip privadas.



SSH local port forwarding escenario



SSH local port forwarding solución

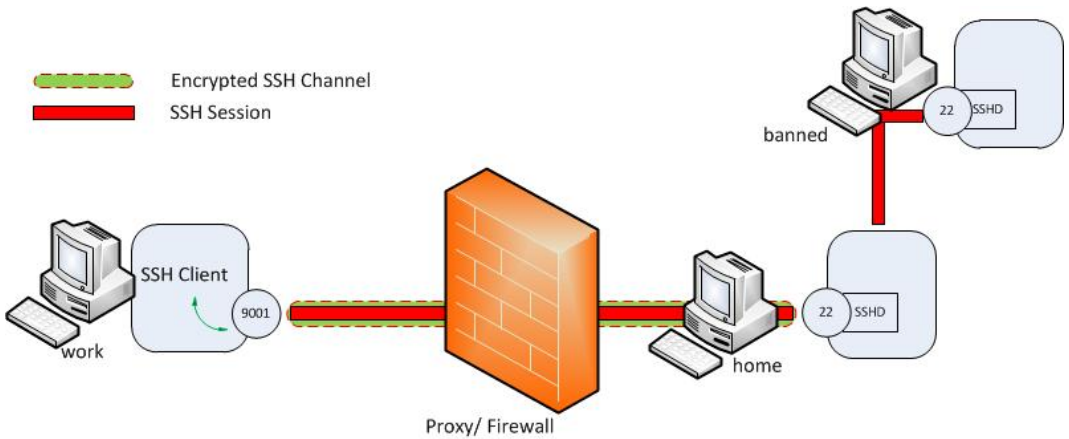


- ssh -L 9001:yahoo.com:80 home
- ssh -L <local-port-to-listen>:<remote−host>:<remote−port> <gateway>
- Conexión a yahoo.com entrando desde la máquina work a http://localhost:9001

SSH VNC session

- También se puede conectar a un puerto de la máquina home en lugar de conectarse directamente a una URL.
- *ssh* -L 5900 : *localhost* : 5900 home
- En el puerto 5900 de la máquina home debería haber un cliente de VNC escuchando.
- Este caso permite transferir todo tipo de datos y no solo datos web.

SSH Hop


Encrypted SSH Channel
SSH Session
banned
22
SSHD
SSH Client
9001
work
Proxy/ Firewall
22
SSHD
home

Ejercicio de parcial - Criptografía

La empresa Security First expone una API usando el protocolo HTTP. Dicha API tiene un método *getPrice* que devuelve el precio de frutas usando la siguiente url:
`http://api.securityfirst.com/?method=getPrice&fruit=Pera`.

- Es necesario agregar un método nuevo a la API que haga lo mismo que el getPrice pero que provea el servicio sólo a usuarios **autenticados** y brinde **integridad** del lado del servidor sobre los pedidos de los usuarios. Suponiendo que un usuario de la API, se autentica con el servidor HTTP a través de una conexión segura generando el siguiente secreto compartido relacionado a sí mismo: (usuario='tincho', secreto='recontrasecretodelrecontraespionaje'). Muestre una posible url que permita procesar el pedido y explique qué es lo que tiene que hacer el servidor para garantizar la integridad del mismo.
  Nota: Es requisito para lo anterior no usar encripción y no manejar sesiones.

¿Repasando...?

¿Dudas?,

¿Preguntas?