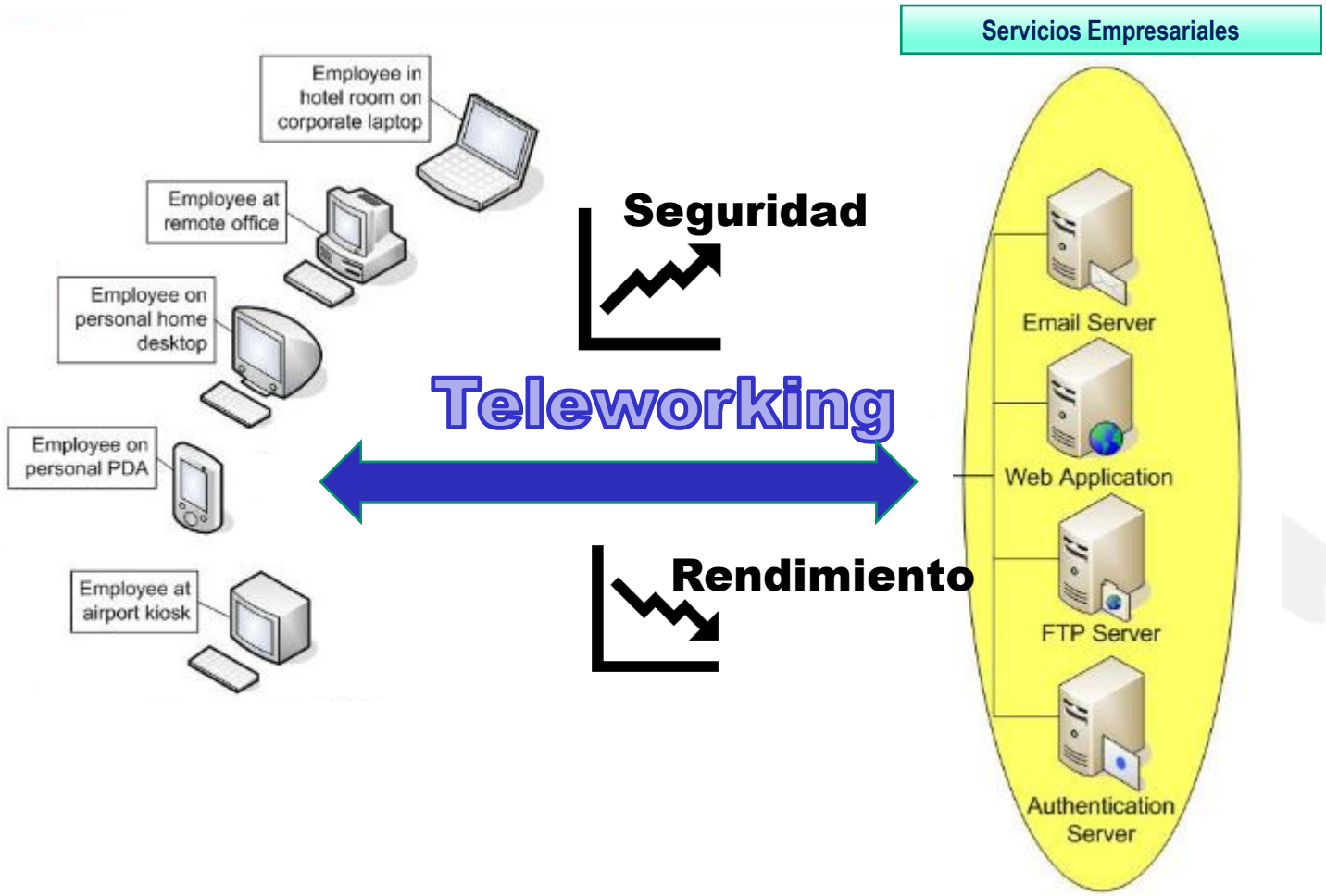
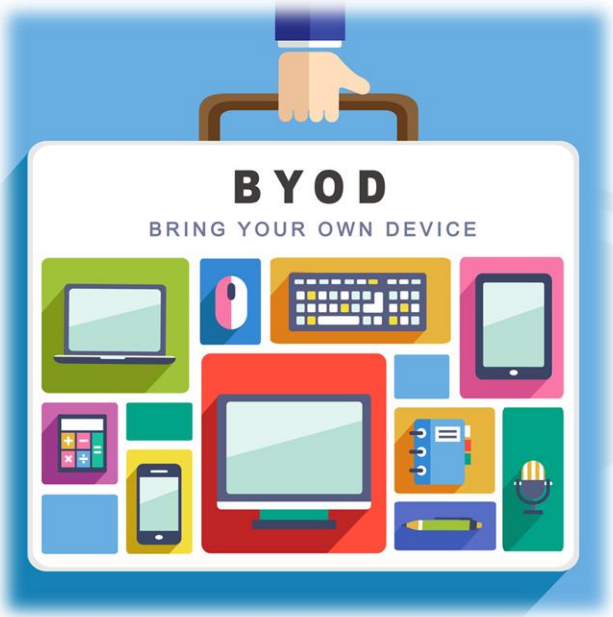
PAI-2. BYODSEC-BRING YOUR OWN DEVICE SEGURO USANDO ROAD WARRIOR VPN SSL PARA UNA UNIVERSIDAD PÚBLICA

Ángel Jesús Varela Vaca
Grupo de Investigación **IDEA Research Group**
Universidad de Sevilla

Acceso Remoto – Road Warrior

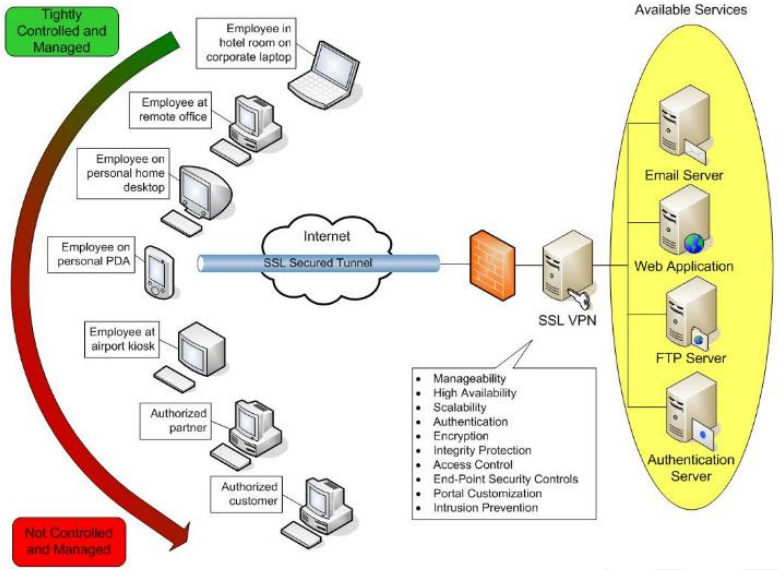


Bring your Own Device (BYOD)

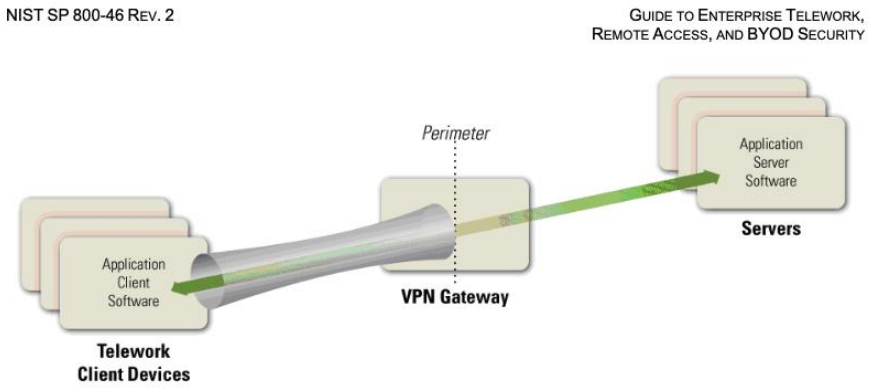


"… deberá ser confidenciales, íntegras y además autenticadas"

VPN (Virtual Private Networks)



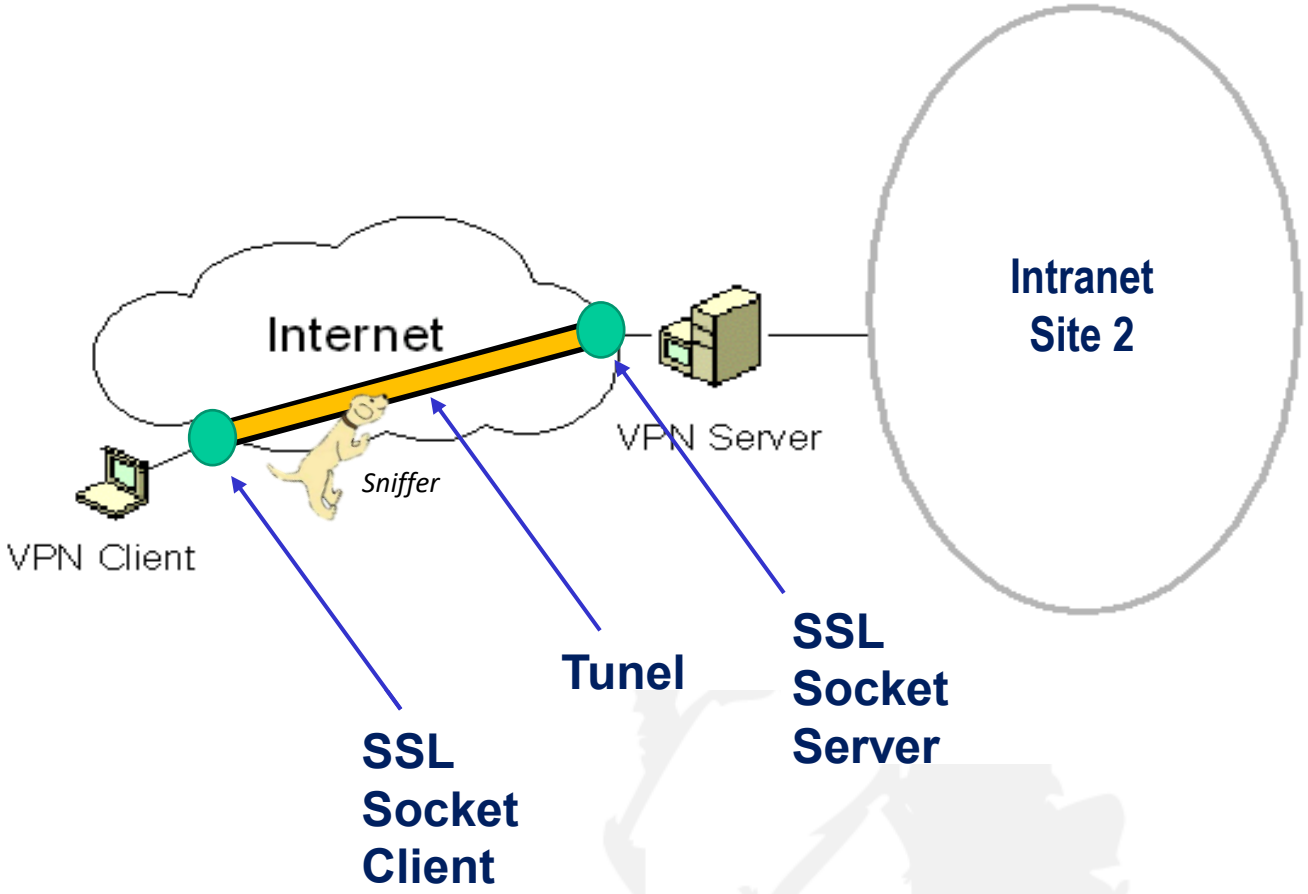
GUIDE TO SSL VPNs del NIST (2008)
https://doi.org/10.6028/NIST.SP.800-113



Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. NIST Special Publication 800-46 Revision 2 (2016)
https://doi.org/10.6028/NIST.SP.800-46r2

- **Host-to-Host (Point-to-Point VPN)**
  - Permite la comunicación segura entre dos puntos con conexión entre ellas y pueden estar dentro de una red local o en Internet.
- **Host-to-Gateway (Road Warrior)**
  - Muy usada. Permite a un conjunto de máquinas ya sean de la red local o Internet se conecten dentro de la VPN
  - Un servidor controla las conexiones que se realizan mediante certificados digitales.
- **Gateway-to-Gateway (Net-to-Net)**
  - Para conectar varias redes LAN en diferentes lugares físicos, podremos acceder de forma segura a cualquier recurso de la red que se encuentre en el otro extremo de la VPN

Canal seguro – VPN SSL



Objetivos

1. Desarrollar/seleccionar cómo llevar a la práctica de forma lo más eficiente posible los ***canales de comunicación segura*** para la transmisión *de credenciales (usuario, contraseñas) y mensajes usando* el ***protocolo SSL/TLS*** asegurando autenticidad, confidencialidad e integridad.

2. Tener en cuenta que el ***número de empleados*** *concurrentes* que usarán la aplicación son aproximadamente **300, realizar las pruebas de capacidad para demostrar que el sistema soporta este número de empleados.**

3. Utilizar alguna herramienta de ***análisis de tráfico*** que permita comprobar la confidencialidad e integridad de los canales de comunicaciones seguros.

4. Establecer ***Cipher Suites robustos que usen en la versión TLS 1.3*** evitando vulnerabilidades.

5. ***Realizar pruebas que demuestren la confidencialidad de la VPN SSL y si hay pérdida de rendimiento al usar la VPN SSL frente a no usarla.***

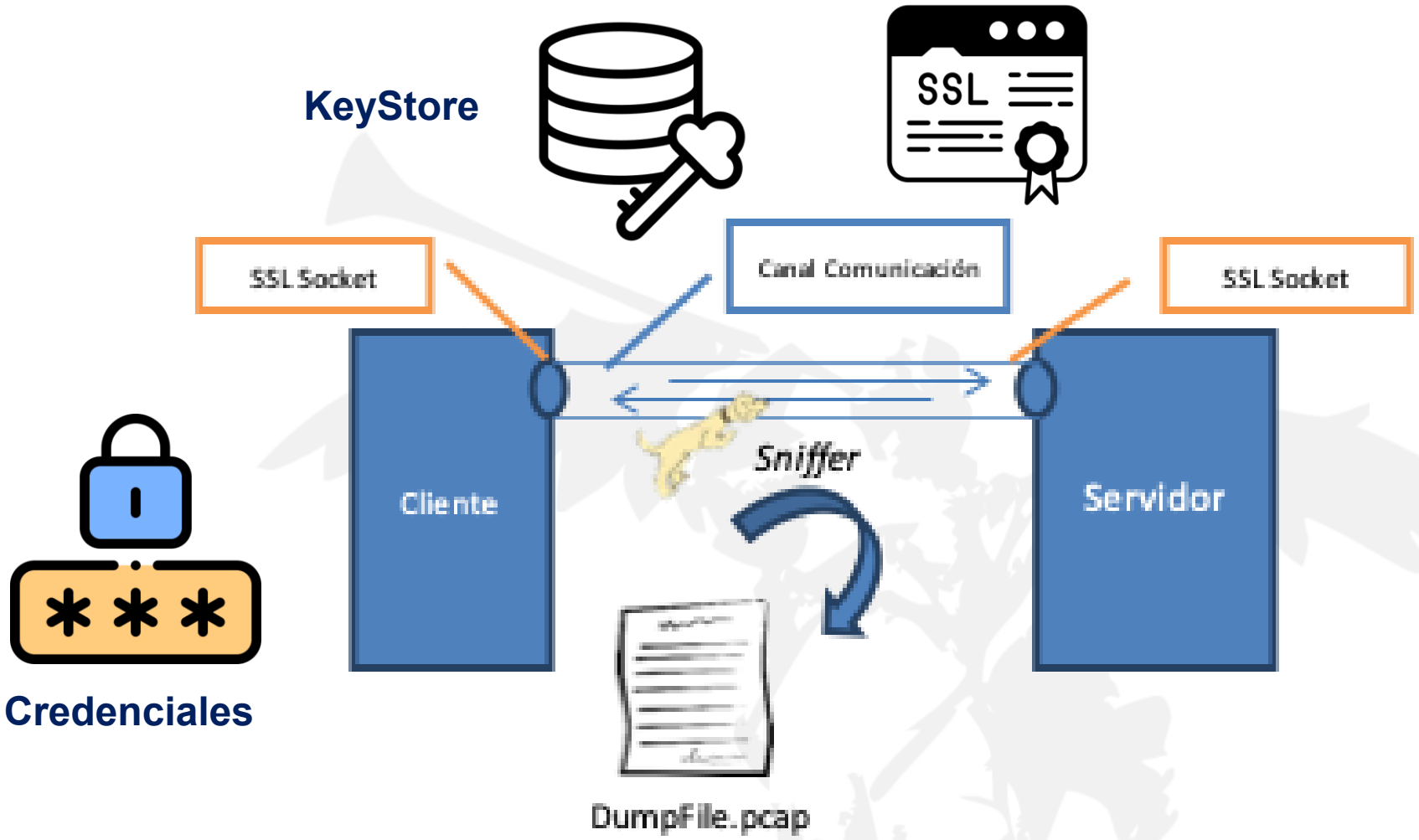
Requisitos funcionales:

1. **Registro de usuarios**
2. **Inicio de sesión**
3. **Verificar credenciales**
4. **Cerrar sesión**
5. **Gestión de usuarios preexistentes**
6. **Mensajes**
7. **Persistencia de datos**
8. **Interfaz de comunicación**

Requisitos información:

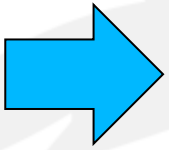
1. **Datos de usuarios**
2. **Registro inicial**
3. **Registro de mensajes**
4. **Mensajes**
5. **Mensajes del sistema**

Recomendaciones



¿Cómo y qué entrego en el PAI?

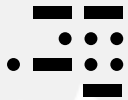
Especificación



Entregable

Informe

Test/Logs



Código/Configuración

Deadline: 21 de octubre

Penalizaciones: 10%

Muchas gracias por vuestra colaboración