**Auditoría/Informe del proyecto del equipo Gryffindor CIT31-01**

# ÍNDICE

[ÍNDICE 2](#_Toc105171966)

[ÍNDICE DE FIGURAS 3](#_Toc105171967)

[ENUNCIADO 4](#_Toc105171968)

[RED PROPUESTA 5](#_Toc105171969)

[AUDITORIA 7](#_Toc105171970)

[1. Enumeración de redes, componentes, topologías y protocolos 7](#_Toc105171971)

[2. Identificación de los sistemas operativos instalados 7](#_Toc105171972)

[3. Análisis de servicios y aplicaciones 8](#_Toc105171973)

[4. Detección, comprobación y evaluación de vulnerabilidades 8](#_Toc105171974)

[5. Medidas específicas de corrección 9](#_Toc105171975)

[6. Recomendaciones sobre implantación de medidas preventivas. 9](#_Toc105171976)

[REFERENCIAS 11](#_Toc105171977)

# ÍNDICE DE FIGURAS

[Figura 1: Modelo esquemático de la red propuesta (Sánchez, 2022). 6](#_Toc105171962)

# ENUNCIADO

Usted trabaja para la una empresa de SmartBuildings. Ante la emergencia de Coronavirus se le pide desplegar un sistema de SmartCities para comunicar en tiempo real a los miembros del sistema sanitario. Para ello despliega en dos edificios sistemas basados en gateways Linux (puede escoger la distribución más apropiada). Dichos sistemas permiten enviar información mediante una interfaz web a una base de datos alojada en uno de los edificios. A dicha base de datos y servicio web solo se puede acceder desde la intranet del edificio. Además, en el servidor, debe alojar una plataforma web para que todo el público pueda enviar consultas y otra información para permitir servicios de telemedicina.

Debe planificar un sistema seguro que permita a los gateway enviar los datos al servidor, que además debe estar accesible a los habitantes del edificio y cualquier usuario doméstico (todos ellos usuarios de Windows). Dichos usuarios se conectan desde Intranet donde se dispone de una LAN WiFi que mantiene conectados los equipos mencionados y, además, dispositivos móviles.

Adicionalmente, el profesor dijo que tratásemos de hacer nuestro proyecto de mensajería sin alterar la infraestructura original.

# RED PROPUESTA

(LO DE ACÁ ABAJO ACTUALIZA)

Inicialmente nos centramos por un diseño como el mencionado en el enunciado, tanto por simplicidad como por petición del enunciado, en el que se comunica el exterior con el interior mediante una VPN para evitar tener que alterar la infraestructura original de la empresa, incluyendo firewalls.

Inicialmente tratamos de usar la VPN de Windows que tiene pre-instalada, pero por comodidad decidimos emplear el software profesional para SSL VPN Fortinet. Según las instrucciones de instalación (JCCM, 2022), hemos decidido que nuestra VPN se llama VPN SmartCity, el Gateway Remoto es 100.200.0.1, la Clave Pre-compartida es “laPatata87Pocha” y el resto queda por defecto. Estos parámetros los utilizamos para el Firewall de su edificio también.

El usuario VPN es ssr y la contraseña (para probar) es laPatata87Pocha.

El edificio remoto tiene red 192.168.57.0/24, el edificio de la empresa 192.168.56.0/24 y la internet la simulamos con la 100.200.0.0/24, inicialmente tratamos de hacer una conexión entre dos ordenadores físicos virtualizando los edificios y con un módem físico entre medias, pero no funcionó así que pasamos a virtualizarlo todo en una máquina y quitarnos el router de en medio.

Hemos supuesto que en la infraestructura original los gateways son del tipo pfSense y utilizan un único firewall por edificio de política restrictiva, para mayor seguridad (menos funcionalidades supone menos potenciales vulnerabilidades), permitiendo la entrada por el puerto 443 y 80 (también está el 3306 para el mySQL pero para acceso local); y sin suponer mayor profundidad en la red, para permitir virtualizar varias máquinas.

Cada edificio en la versión final se simula en un edificio diferente.

La BBDD es SQL mediante xampp.

El material de nuestra red puede encontrarse en el github:

https://github.com/tardisfromtornspace/ProyectoGryffindorCIT31-01.git

(PUEDE QUE ESTO OTRO SEA UTIL PARA LA RED https://openwrt.org/)

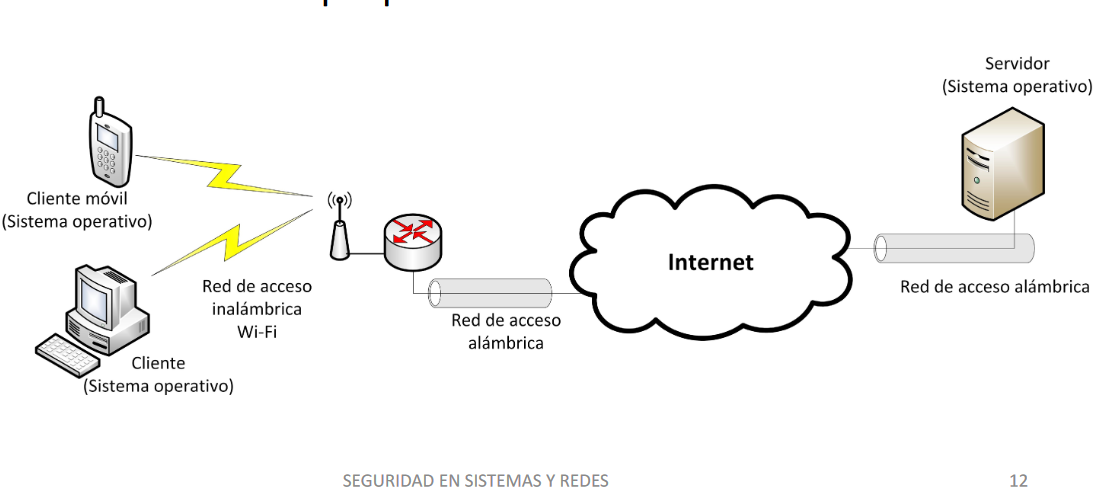


Figura 1: Modelo esquemático de la red propuesta (Sánchez, 2022).

# AUDITORIA

Hemos decidido emplear una auditoría de caja blanca por falta de tiempo y para mayor eficiencia, con un conocimiento total de la red.

<<<Los ataques se hacen desde 3 sitios, edificio de la empresa, edifico remoto y desde la internet, con una Kali Linux>>>

ER – Firewall --->Móvil que simula la red <--- Firewall – EE

Kali (Alex S) Kali(Javier, adaptador puente) Kali (Víctor)

## Enumeración de redes, componentes, topologías y protocolos

Hay 3 redes, mencionadas en el apartado red propuesta:

LANA – La red del edificio de la empresa 192.168.56.0/24 Tiene configurada una VPN. Tiene una máquina servidor (192.168.56.10) y el router pfSense1 (192.168.56.1)

LANB – La red edificio remoto 192.168.57.0/24. Tiene una máquina clienteRemoto (192.168.57.2) y el router pfSense2 (192.168.57.1)

WAN – Simulación del internet 100.200.0.0/24. Tiene a los dos routers (pfSense1 con 100.200.0.1 y pfSense2 con 100.200.0.2).

Todos ellos emplean topología en estrella, menos la conexión de WAN, simulada con un P2P. Todos ellos emplean máscara /24 por simplicidad.

Routers:

pfSense1: es el que conecta LANA con WAN

pfSense2: es el que conecta LANB con WAN

-Ambos actúan con el mismo tipo de firewall: política permisiva desde LAN y restrictiva desde WAN.

Usamos protocolo TCP/IP para las conexiones.

## Identificación de los sistemas operativos instalados

1. **pfSense1 (#R1)** y **pfSense2 (#R2)**: ambos utilizan FreeBSD 64-bit 12.2-STABLE
2. **ClienteRemoto** **(#LANB1**): Windows XP 32-bit con parche Service Pack 3
3. **Servidor (#LANB2):** Windows 10 Education 64-bit, versión 1903, versión del SO 18362.592.

## Análisis de servicios y aplicaciones

|  |
| --- |
| • En “caja blanca”, las aplicaciones pueden identificarse de forma sencilla viendo la lista ofrecida por el S.O. pero los servicios se estudian con Nmap • Posibles servicios “ocultos”  **pfSense1 (#R1)** y **pfSense2 (#R2)**:   * (lista de servicios)   **ClienteRemoto** **(#LANB1**):   * (lista de servicios)   **Servidor (#LANB2):**   * (lista de servicios) |

## Detección, comprobación y evaluación de vulnerabilidades

|  |
| --- |
| Para cada servicio y/o aplicación en cada una de las máquinas • Si la máquina es un S.O. o un dispositivo móvil, hay que utilizar las herramientas vistas en cada una de las unidades • Para servicios WEB se puede usar la metodología OWASP como vimos • También análisis generales como de denegación de servicio • Con Apache Benchmarking  **pfSense1 (#R1)** y **pfSense2 (#R2)**:   * (lista de servicios acá y vulnerabilidades) * Además, hay una vulnerabilidad posible, y es no haber cambiado las contraseñas de acceso al router de las por defecto (admin, pfsense) Hay que corregirlo   **ClienteRemoto** **(#LANB1**):   * (lista de servicios acá y vulnerabilidades)   **Servidor (#LANB2):**   * (lista de servicios acá y vulnerabilidades) |

## Medidas específicas de corrección

|  |
| --- |
| • De las vulnerabilidades descubiertas en el apartado anterior, cuales se corrigen y por qué. • Y cuales no y por qué **• En la entrega que se haga YA deben estar corregidas** |

## Recomendaciones sobre implantación de medidas preventivas.

Dejar los sistemas cerrados bajo llave (contraseña electrónica y llave física) dentro que una habitación con sistema de refrigeración y medidas anti-incendios, y filtros de aire (más una cámara de presión positiva) para prevenir polvo e insectos dentro de la cámara, con una trampa de luz ultravioleta para eliminar cualquier posible insecto que se cuele. El servidor debería estar desplegado en el edificio de la empresa, para mayor seguridad. Y tener cámaras con reconocimiento facial y otros métodos de seguridad biométrica.

También deberíamos añadir redundancias como medida extra en caso de caída o fallo (p. ej. backup de la BBDD, múltiples switches, generadores de emergencia) pero no lo hemos implementado porque o bien no se podían simular en máquina virtual, o se podrían simular pero a riesgo de falta de memoria (p.ej: un ordenador teniendo que soportar la red básica más los backups).

El control de acceso debería ser distribuido, de tal forma que dar privilegios más altos a alguien requiera de la colaboración de todos los administradores, para complicar corrupción permitiendo accesos maliciosos al sistema.

Para mejorar seguridad comunicaciones móviles, usaríamos la mejor encriptación, WPA3, y no escribas las contraseñas, y no hablar de los clientes públicamente ni de nada relacionado con las seguridad (nada fuera del entorno laboral). También los dispositivos móviles deberían tener una doble verificación de sistema biométrico y contraseña, y no estar rooteados. De hecho para mayor seguridad los móviles corporativos deberían resetearse cada mes para asegurarse de que no están rooteados.

Además como protección extra frente a alguien logrando robar credenciales de la VPN y acceder, deberíamos añadir un segundo firewall detrás del primero para evitar que alguien empleara el servicio VPN para mandar paquetes a servicios previamente inaccesibles; pero no lo hemos resuelto porque nos han pedido no alterar la infraestructura.

(Esta imagen de abajo es por referencia, no incluirla en la memoria final)Tabla

Descripción generada automáticamente)

# REFERENCIAS

JCCM. (2 de 6 de 2022). *Junta de Comunidades de Castilla-La Mancha*. Obtenido de JCCM: https://sum.jccm.es/node/33

Sánchez, B. B. (1 de 5 de 2022). *moodle.* Obtenido de Enunciado y propuesta Segundo Parcial: https://moodle.upm.es/titulaciones/oficiales/pluginfile.php/9386654/mod\_resource/content/3/Enunciado%20y%20propuesta%20Segundo%20parcial.pdf