UD6 – CONNEXIÓ I GESTIÓ DE RECURSOS EN XARXA-I

1º DAW - CFGS

Prof. Manuel Enguidanos
menguidanos@fpmislata.com

6.1. SEGURETAT EN XARXES INFORMÀTIQUES

6.1. Seguridad en las redes informáticas

Entenem per seguretat informàtica el ***conjunt d'accions, ferramentes i dispositius l'objectiu dels quals és dotar a un sistema informàtic d'integritat, confidencialitat i disponibilitat***. Hem de ser conscients que les pèrdues d'informació no poden vindre només d'atacs externs sinó que poden produir-se per errors nostres o per accidents o avaries en els equips.

L'element clau d'un sistema d'informació són les dades i hi ha dos principals amenaces externes al programari i a les dades:

- **Codi maliciós (malware)**
- **Enginyeria social**


Su tarjeta linea abierta ha sido desactivada

atenciones@m.caixa.com <atenciones@m.caixa.com>

05:36 pm

Para: migueltecnologia@hotmail.com

Estimado/a cliente: migueltecnologia@hotmail.com

Le informamos que su "Tarjeta Linea Abierta" ha sido desactivada.

IP de conexión: 185.48.101.210
Hora de operación: 2018-11-14 15:32:00

A Partir de la fecha anterior, no puede realizar ninguna operación desde su linea abierta hasta que configurar CaixaBank Sign. Si usted no realizó la operación, ingrese el enlace para configurar CaixaBank Sign : https://m5-caixa.es/caixa_sign/autorizar_/
Le enviamos este mensaje para ayudarle a garantizar la seguridad de los servicios de que dispone en Caixa Bank.

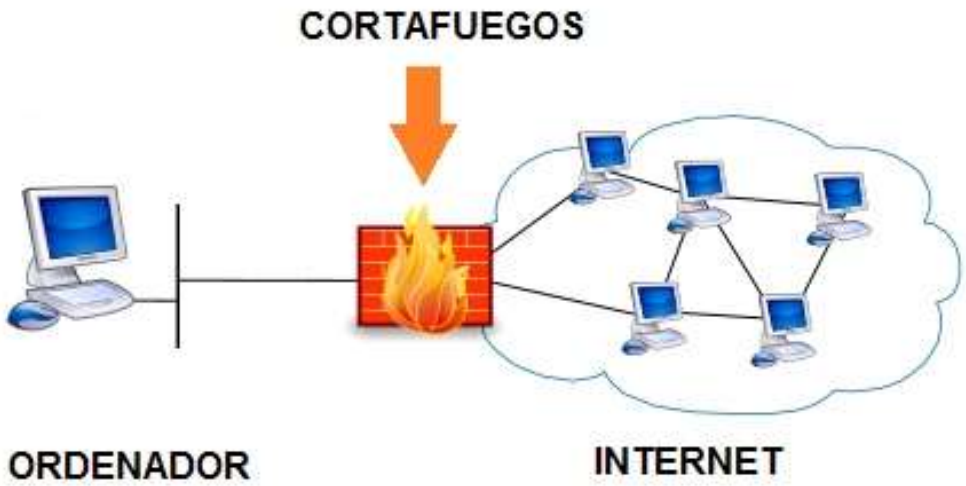
Atentamente,
Atención al Cliente de Caixa Bank.

6.1. Seguridad en las redes informáticas

6.1.1. Control de acceso

6.1. Seguridad en las redes informáticas

6.1.2. Cortafuegos (*firewall*)



6.1. Seguridad en las redes informáticas

6.1.2. Cortafuegos (*firewall*)

Cortafuegos *hardware*

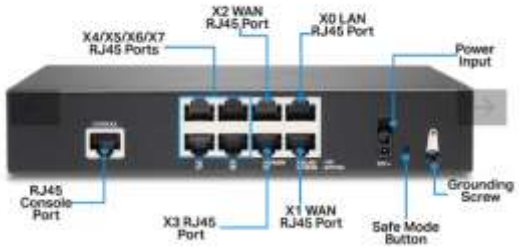
Sonicwall Tz270 Cortafuegos (hardware) 2000 Mbit/s

443,00 €

Sin impuestos
366.12 €

TZ270 Front Panel

TZ270 Rear Panel

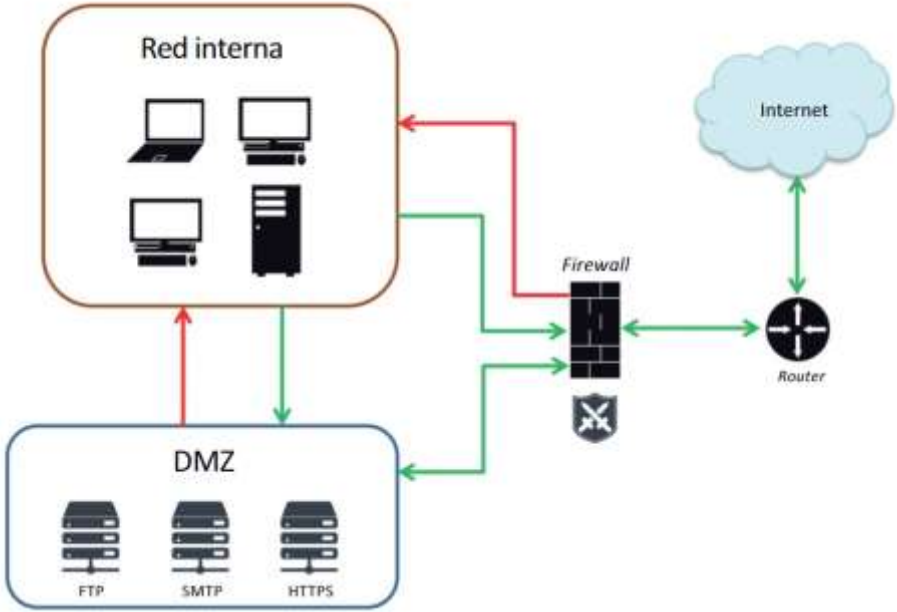


6.1. Seguridad en las redes informáticas

6.1.2. Cortafuegos (*firewall*)

Cortafuegos *hardware*

DMZ o zona desmilitarizada



6.1. Seguridad en las redes informáticas

6.1.2. Cortafuegos (*firewall*)

Cortafuegos *software*

Los sistemas operativos Linux y Windows traen incorporadas varias aplicaciones de cortafuegos por software, como **`ufw`**, **`iptables`**, **`nftables`** en Linux, y en Windows se puede utilizar Firewall de Windows Defender. Además, siempre es posible utilizar algún software de terceros para tal fin, como TinyWall, Netdefender, ZoneAlarm, Comodo Firewall o un *firewall* incluido como parte de un paquete antivirus como Norton Firewall, AVS Firewall u otros.

6.1. Seguridad en las redes informáticas

6.1.2. Cortafuegos (*firewall*)

Cortafuegos en Linux

Se puede gestionar el cortafuegos en Linux con el comando `ufw` (***u**ncomplicated **f**ire**w**all*, cortafuegos sin complicaciones). Esta herramienta es una forma sencilla de utilizar las **iptables** y su sucesor, **nftables**, que son el *software* que hace de *firewall* en Linux.

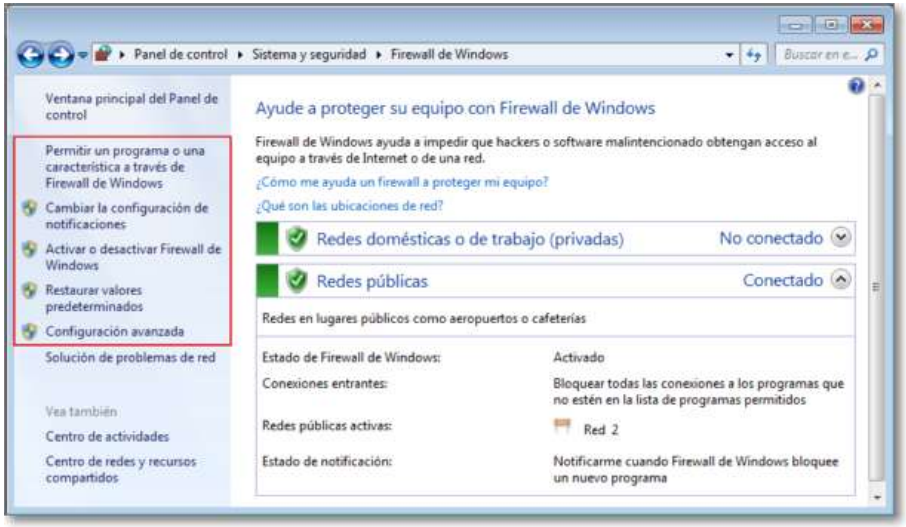
```
ufw
```

Este comando tiene las siguientes sintaxis dependiendo de la función que se vaya a realizar con él y las opciones que se utilicen. Recarga y habilita en el arranque/descarga y deshabilita del arranque/recarga.

6.1. Seguridad en las redes informáticas

6.1.2. Cortafuegos (*firewall*)

Cortafuegos en Windows



6.1. Seguridad en las redes informáticas

6.1.2. Cortafuegos (*firewall*)

Cortafuegos en Windows

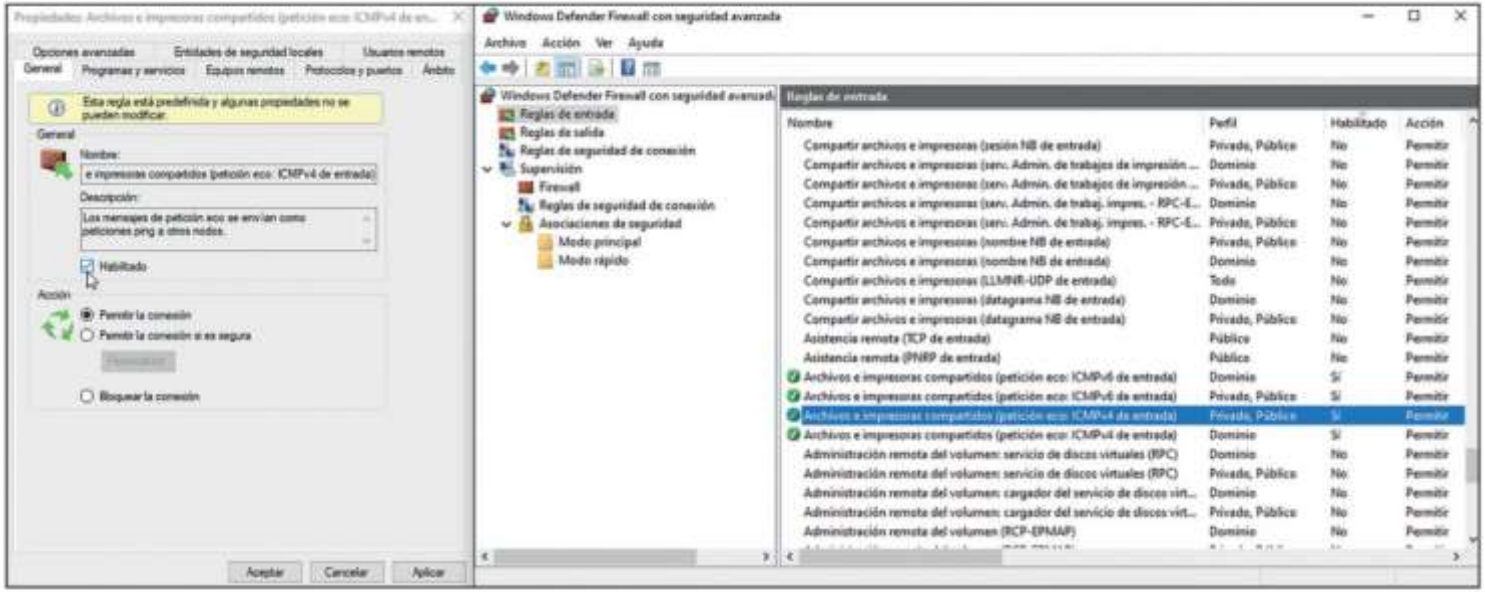


Figura 6.7. *Firewall de Windows Defender con seguridad avanzada. Regla de entrada de petición eco: ICMPv4 de entrada (si se habilita y se bloquea no podrán hacer* ping *al equipo).*

6.1. Seguridad en las redes informáticas

6.1.2. Cortafuegos (*firewall*)

Cortafuegos en Windows

Comandos

También es posible configurar el *firewall* en Windows a través de la interfaz de comandos, por ejemplo:

`Get-NetFireWallProfile`	Muestra en PowerShell el estado de los perfiles del *firewall*.
`netsh advfirewall`	Configura el *firewall* desde comandos.
`netsh advfirewall show allprofiles state`	Muestra el estado del *firewall* de todos los perfiles (`allprofiles`) o del perfil actual (`currentprofile`).

6.1. Seguridad en las redes informáticas

6.1.3. Sistemas de detección de intrusión

Existen una serie de herramientas que monitorizan y detectan las intrusiones, como los sistemas IDS, IPS y SIEM. Los tres son sistemas para proteger las comunicaciones y detectar intrusiones, pero funcionan de forma diferente entre sí:

- **IDS** (***I**ntrusion **D**etection **S**ystem,* sistema de detección de intrusiones): sistema que detecta accesos no autorizados a equipos o redes. Es un sistema pasivo ya que se dedica a detectar la intrusión y, en caso de detectarla, emite una alarma.
- **IPS** (***I**ntrusion **P**revention **S**ystem,* sistema de prevención de intrusiones): protege al sistema de la intrusión. Es un sistema activo ya que se encarga de monitorizar las entradas y las salidas en busca de ataques cibernéticos y de *malware.* Si detecta una amenaza actúa para detenerla.
- **SIEM** (***S**ecurity **I**nformation and **E**vent **M**anagement,* información de seguridad y gestión de eventos): sistema que analiza los eventos de seguridad en una red. Se complementa con los anteriores y centraliza la información, descartando falsos positivos.

Activitats Resoltes

Actividad resuelta 6.1

Comprueba si en Linux está instalado el cortafuegos `ufw`. Si no es así, instálalo. Actívalo y examina las aplicaciones disponibles que tienes para aplicar. Cambia la política predeterminada a permitir. Muestra el estado del cortafuegos de forma detallada.

Solución

```
dpkg -s ufw
sudo apt update
sudo apt install ufw
sudo ufw status
sudo ufw enable
sudo ufw app list
sudo ufw default allow
sudo ufw status verbose
```

Activitats Resoltes

Actividad resuelta 6.2

Comprueba en Windows el estado del cortafuegos. Actívalo si no lo está. Comprueba las reglas que tiene habilitadas, las que no y las que estén habilitadas para la conexión activa.

Solución

Para consultar el estado del firewall en Windows, puedes ir a **Panel de control → Firewall de Windows Defender.** En la red donde aparezca **Conectado,** puede ser una red privada o una pública, comprueba si en **Estado de Firewall de Windows Defender** aparece la palabra **Activado.**

También puedes obtener la información si vas a PowerShell o al Símbolo del sistema y escribes:

```
netsh advfirewall show allprofiles state
```

En este caso también te muestra la información del perfil de dominio (cuando estás en una red con un controlador de dominio), privado (red privada detrás de un *firewall* o un router) y público (red pública como la que se suele encontrar en los lugares públicos).

Si aparece **Desactivado**, ve a activar o desactivar el Firewall de Windows Defender y marca las opciones **Activar Firewall de Windows Defender**, tanto en **Configuración de red privada** como en **Configuración de red pública.**

Para ver las reglas que tiene activadas, ve a **Configuración avanzada.** Allí podrás ver las reglas de entrada y las de salida. De cada regla puedes ver si está habilitada o deshabilitada, dependiendo de si tiene icono de permitida o no delante del nombre. Si no aparece el icono es que no está habilitada. En el perfil verás si la regla se aplica para el perfil público, privado o de dominio. En **Habilitado** puedes ver si está habilitada o no lo está. También puedes ver el protocolo, si se va a permitir esa regla, se va a bloquear o solo se va a permitir cuando la conexión sea segura (Figura 6.8). Otra información que puedes ver es el número de puerto, el protocolo, los programas, etcétera.

Figura 6.8. Firewall de Windows Defender con seguridad avanzada. Reglas de entrada si están habilitadas y permitidas, habilitadas y no permitidas, o no habilitadas.

Si vas a **Supervisión → Firewall** puedes monitorizar las reglas de entrada y de salida que estén habilitadas en la conexión activa.

6.1. Seguridad en las redes informáticas

6.1.4. Herramientas de cifrado y seguridad

Existen varias herramientas que permiten encriptar archivos y carpetas, así como la información que viaja por la red. Utilizan algoritmos de cifrado.

- **OpenSSL:** es un paquete que ofrece herramientas de seguridad para TLS y SSL. También ofrece utilidades de criptografía que se pueden utilizar por otras aplicaciones.
- **LIbreSSL:** es una bifurcación o *fork* del proyecto anterior. Ofrece varias utilidades, como **libcrypto, libssl** o **libtls,** que son bibliotecas de criptografías y utilidades para TLS.

```
openssl req
```

Utilidad para generar certificados. Puede crear certificados autofirmados para usarlos como raíz CA. En principio los certificados los genera en formato PKCS#10.

6.1. Seguridad en las redes informáticas

6.1.4. Herramientas de cifrado y seguridad

OpenSSH

Paquete que ayuda a la seguridad ofreciendo la herramienta SSH y otras aplicaciones para cifrar las comunicaciones en una red. Es una herramienta que funciona en muchos sistemas operativos. Además de `ssh`, que se verá a continuación, ofrece **ssh-keygen**, que permite generar claves.

OpenSSH cifra las conexiones evitando posibles escuchas y otros ciberataques, y ofrece además la **capacidad de tunneling para encapsular un protocolo de red sobre otro** y aumentar así la privacidad de los datos y redes creadas con este mecanismo.

6.1. Seguridad en las redes informáticas

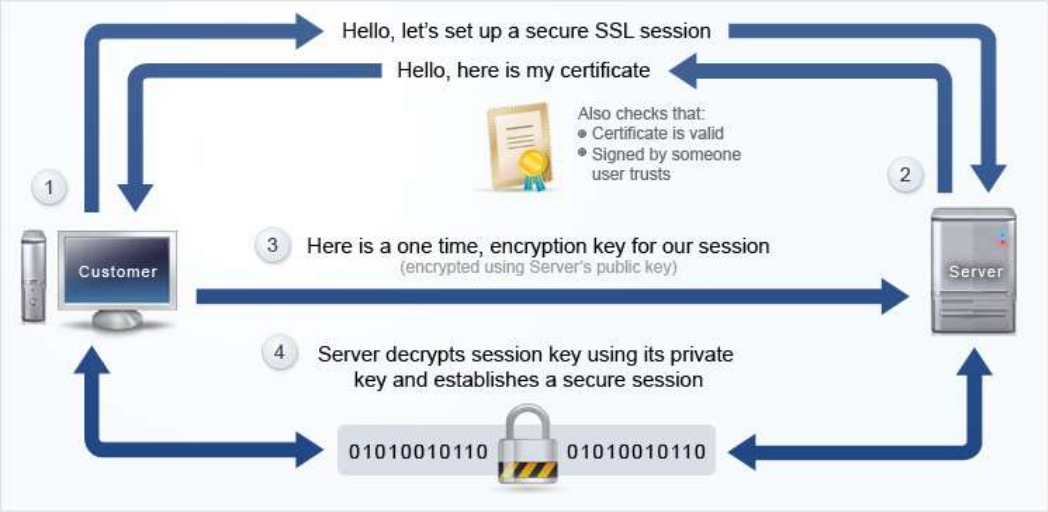
6.1.4. Herramientas de cifrado y seguridad

Certificados

Un certificat digital li permet validar el seu domini i el seu servidor de manera segura, a l'efecte d'evitar que un altre servidor prenga el seu lloc començant a respondre pel seu domini.

Addicionalment, una vegada que el seu navegador i el servidor web han establit una connexió segura, les dades que s'intercanvien estan xifrats, evitant que qualsevol els puga veure mentres naveguen pels canals d'Internet.

El següent gràfic és una mostra dels passos que amb els quals el servidor i el seu navegador es reconeixen amb Certificats Digitals i després comencen un diàleg xifrat:



6.1. Seguridad en las redes informáticas

6.1.4. Herramientas de cifrado y seguridad

Certificados

Los certificados generan un par de claves: una pública y una privada. La clave privada la mantiene el servidor, mientras que la pública se envía al equipo cliente y así se asegura la identidad del servidor.

Las extensiones o formatos de los certificados más utilizados son: .CSR, .KEY, .DER, .CRT, .CERT, .CER, .PEM, etc., y es posible convertir un tipo de certificado en otro.

Al navegar por un sitio web se puede ver si la conexión es segura. Si se pincha a la izquierda de la barra de direcciones, sobre el candado, en **La conexión es segura**, se ofrece más información sobre la conexión. Al pinchar sobre **El certificado es válido** se muestra información sobre el certificado (Figura 6.9).

Figura 6.9. *Información sobre el certificado que asegura la identidad del sitio remoto.*

6.1. Seguridad en las redes informáticas

6.1.4. Herramientas de cifrado y seguridad

Comprobación de certificados instalados en Windows

Los certificados instalados en un sistema operativo Windows pueden ser certificados de equipos y certificados de usuario:

- Ejecutar `certmgr.msc` para ver los certificados del usuario actual.
- Ejecutar `certlm.msc` para ver los certificados del equipo local.

Comprobación de certificados instalados en Linux

En Linux los certificados se encuentran en el directorio **/etc/ssl/certs**. Aquí están junto con el fichero **ca-certificates.crt**.

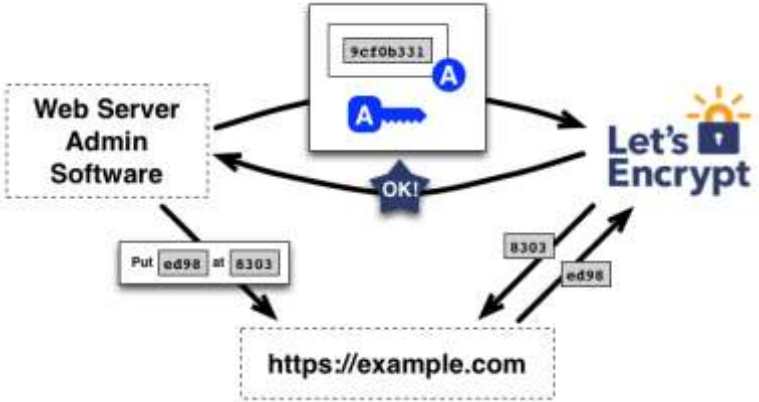
Una aplicación que se desee configurar para usar un certificado de una autoridad certificadora (CA) debe añadir su certificado al archivo **ca-certificates.crt**.

6.1. Seguridad en las redes informáticas

6.1.4. Herramientas de cifrado y seguridad

Let's Encrypt

Herramienta con la que se puede conseguir un certificado digital de forma gratuita y válido para usarlo en la web con el protocolo HTTPS. Es una autoridad de certificación. Hay que solicitar el certificado y después confirmar el dominio. Se puede obtener la información desde su sitio web: https://letsencrypt.org/



Activitats Resoltes

Actividad resuelta 6.3

Comprueba en Windows y en Linux los certificados que tengas instalados en tus equipos.

Solución

En Linux ve a la ruta **/etc/ssl/certs**. Allí puedes ver todos los certificados que tienes instalados en el equipo.

En Windows, con el botón derecho del ratón sobre **Inicio,** selecciona **Ejecutar** y escribe:

```
certlm.msc
```

Después pulsa **Aceptar.** Cuando te pregunte si quieres permitir que el programa realice cambios en el equipo, responde que sí. En **Entidades de certificación,** en **Certificados,** puedes ver los certificados que se han ido instalando en el equipo con información de para quién se emitió, el emisor, la fecha de expiración y el propósito para el que se emitió, entre otra información.

6.1. Seguridad en las redes informáticas

6.1.5. Configuración del *router*

Para acceder al *router* y poder configurarlo será necesario tener su dirección IP y un nombre de usuario y una contraseña. En el Apartado 5.3.4 y en la Actividad resuelta 5.10 se vio cómo se puede acceder al *router* en una red.

Si es una LAN pequeña será también el que ofrezca salida a internet a través de un módem integrado y puede tener incorporado el *firewall* y un servidor DHCP. Por defecto tiene la dirección IP 192.168.1.1 o 192.168.0.1, pero se puede configurar para que sea otra. Para conocer la dirección IP del *router* normalmente hay que consultar la dirección IP del *gateway* o puerta de enlace de la red.

Una puerta de enlace o *gateway* permite a los equipos de una red tener salida al exterior, con lo cual también suele tener una dirección privada y otra pública y traduce las direcciones de dentro de la red a través del sistema NAT a direcciones públicas.

`traceroute` o con `tracert`

`netstat`

Activitats Resoltes

Actividad resuelta 6.4

Consulta la dirección IP de tu *router* y comprueba si puedes entrar. Comprueba desde el Símbolo del sistema con el comando `tracert` la ruta que siguen los paquetes que salen por la IP de la puerta de enlace. Comprueba con `netstat` las conexiones abiertas y los puertos de escucha.

Solución

Se puede obtener de varias formas. En un equipo Windows abre el Símbolo del sistema y escribe **Ipconfig**. En la conexión que tengas activa, mira el valor de puerta de enlace predeterminada. Para poder acceder, en un navegador web escribe la dirección IP anterior. Te deberá pedir un nombre de usuario y una c
pendiendo de sus características, podrás c
Los menús y dónde está cada opción varía

Para comprobar la puerta de enlace, escrit

```
ipconfig
```

En la información que te muestra, mira cu
determinada. A continuación escribe:

```
tracert google.es
```

Y verás que la primera línea te muestra qu

En el sistema operativo Linux, para ver la
cribir:

```
ip route
```

La dirección IP de la puerta de enlace o gat

```
default via <dir_ip_enlace>
```

(En ambos casos puedes cambiar el destino **google.es** por cualquier otro para ver la ruta de los paquetes hacia él).

Para utilizar el comando `netstat`, en Windows puedes escribirlo en una terminal. En el sistema operativo Linux, si no está instalado, puedes instalarlo mediante el paquete:

```
sudo apt install net-tools
```

Después, para ver las conexiones abiertas y los puertos de escucha, puedes escribir:

```
netstat -an
```

Si la información es demasiado larga, puedes paginarla escribiendo:

```
netstat -an | more
```

Con este comando puedes ver si hay una conexión con tu equipo de la que no eres consciente. Para conocer las conexiones abiertas y en ejecución utilizarás el comando anterior. Te indica los protocolos (TCP o UDP), la IP local, la IP remota, los números de puertos y el estado de la conexión.

Si la utilidad **traceroute** no está instalada, puedes instalarla escribiendo:

```
sudo apt install traceroute
```

A continuación, para ver la ruta que siguen los paquetes que salen por la IP de la puerta de enlace, escribe:

```
traceroute google.es
```

Realitzar Pràctica 1

UD6 – CONNEXIÓ I GESTIÓ DE RECURSOS EN XARXA-I

1º DAW - CFGS

Prof. Manuel Enguidanos
menguidanos@fpmislata.com