TEMA

Tema 8. Seguridad Perimetral

Administración de sistemas informáticos en Red

Seguridad y alta disponibilidad

Autor/a: Joaquín Erencia

Linkia FP

Tema 8: Seguridad Perimetral

¿Qué aprenderás?

- Qué partes componen el perímetro de defensa de una red
- Cómo un atacante puede entrar en nuestra red desde el exterior
- Qué es una VPN

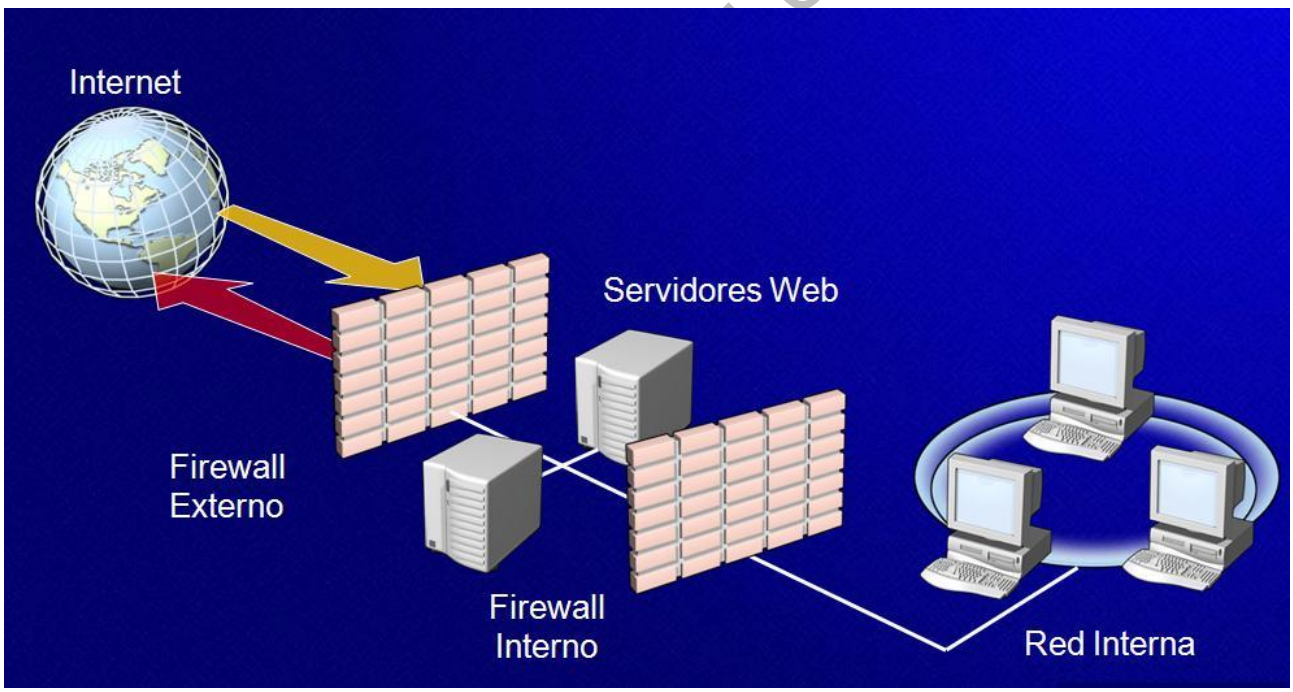
¿Sabías que…?

- McAfee ha apostado en sus soluciones de seguridad por VPN

7.1. INTRODUCCIÓN

En este tema vamos a seguir con algunas de las necesidades que han ido apareciendo dentro de los sistemas informáticos. Ya hemos hablado de cuando nuestros usuarios entraban dentro de nuestra red y se conectaban a la red inalámbrica. En este caso vamos a tratar la siguiente situación. Un departamento comercial ha comprado portátiles a todos sus miembros y estos, moviéndose continuamente por todo el territorio quieren conectarse a unos servicios o datos que se encuentran en el interior de nuestro sistema informático. Y claro, si ellos pueden, ¿cómo evitaremos que usuarios no deseados puedan acceder?

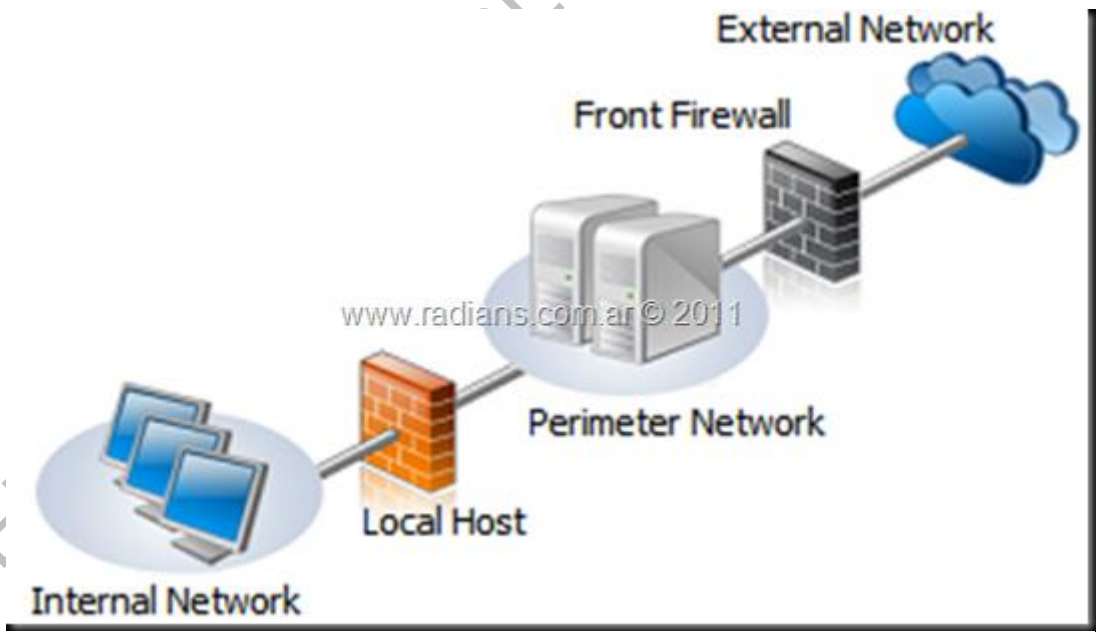
Para dar respuesta a esto vamos a estudiar la **Seguridad Perimetral**. Esta seguridad es un conjunto de técnicas de defensa de la red, que se basan en establecer elementos de seguridad en la parte externa de la red, la que está en contacto con Internet, gestionando el tránsito de usuarios externos al interior de la red e internos al exterior.



7.2. ELEMENTOS DE LA SEGURIDAD PERIMETRAL

Los elementos más importantes que componen esta seguridad perimetral son:

- **Router frontera**: Es el router ubicado entre la red interna y la red externa (Internet). Es la primera línea de defensa de red y de filtrado inicial y final. La configuración de Routers ya se imparte en otro módulo del ciclo, por lo que no la vamos a tratar.
- Cortafuegos (**Firewall**). ES un programa o hardware que controla los puertos y conexiones, limitando el paso y el flujo de datos según la dirección IP que realice la petición. Por ejemplo, en caso de encontrarse con una petición de IP desconocida, el Firewall la bloqueará en el momento. Este elemento es tan importante que le vamos a dedicar un tema solo para él.
- **VPN** (Virtual Private Network). Las VPN permiten la extensión segura de una red local. Además, el cifra todo el flujo de datos que pasa a través de él, lo que asegura que los datos no serán comprometidos y están protegidos.
- **IDS** (Intrusion Detection Systems). Un IDS es un software cuya función es la de controlar los accesos a la red informática para proteger los equipos de posibles ataque y abusos
- Pasarelas antivirus y antispam. Ya hemos hablado de estos sistemas en otros temas.
- **Honeypots**: Es un sistema configurado con vulnerabilidades que se usa para recoger ataques y estudiar nuevas técnicas de protección.



7.3. ESTRUCTURAS DE RED EMPRESARIAL

Para poder realizar una política de seguridad de una red, tenemos que empezar por el diseño de esta. Diseñar una red no es un servidor, un router, los switches y proporcionar direcciones IP a los host. Es mucho más que eso. Es pensar en cómo es red será más eficiente, sus finalidades, sus necesidades y SU SEGURIDAD.

A continuación, espero aclararte este tema.

Una red sin seguridad perimetral se caracteriza por:

- No está segmentada (subnetting)
- Los servicios internos (DNS, DHCP, BBDD) están accesibles
- No hay elementos de filtrado de entrada ni de salida
- No se verifica el malware
- Un cliente remoto puede acceder directamente a los servicios de la red

Una red con seguridad perimetral se caracteriza por:

- Instalación de cortafuegos que incluye
  - Una Zona Desmilitarizada
  - Una Red Interna
- Instalación de antispam y antivirus
- Instalación de IDS en las interfaces del cortafuegos
- Segmentación de los servicios públicos
- Servicios internos dentro de una red interna (BBDD)
- Los clientes remotos solo acceden por VPN

Ahora vamos a analizar algunos de estos componentes.

7.3.1. ZONA DESMILITARIZADA (DMZ)

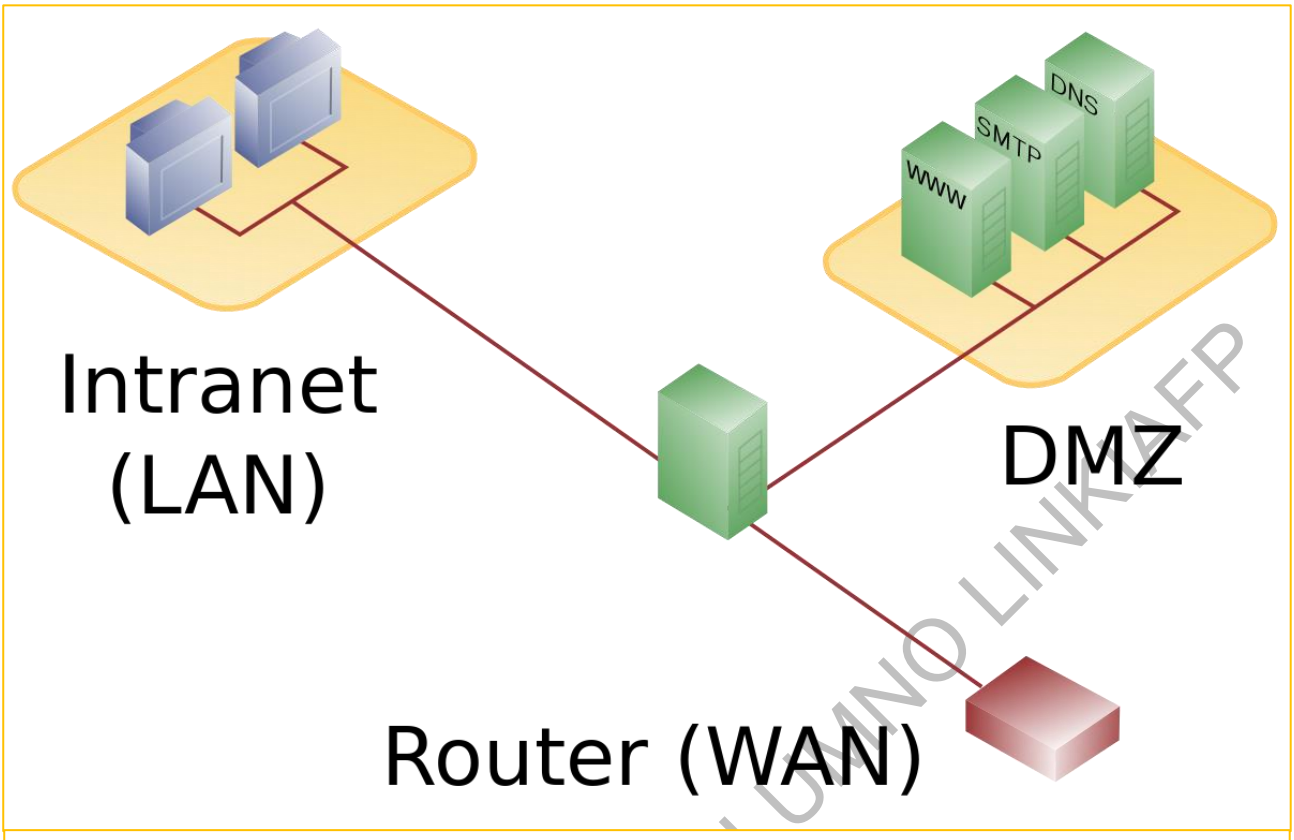
Una **DMZ** es una parte de la red local ubicada entre la red interna y la red externa (Internet).

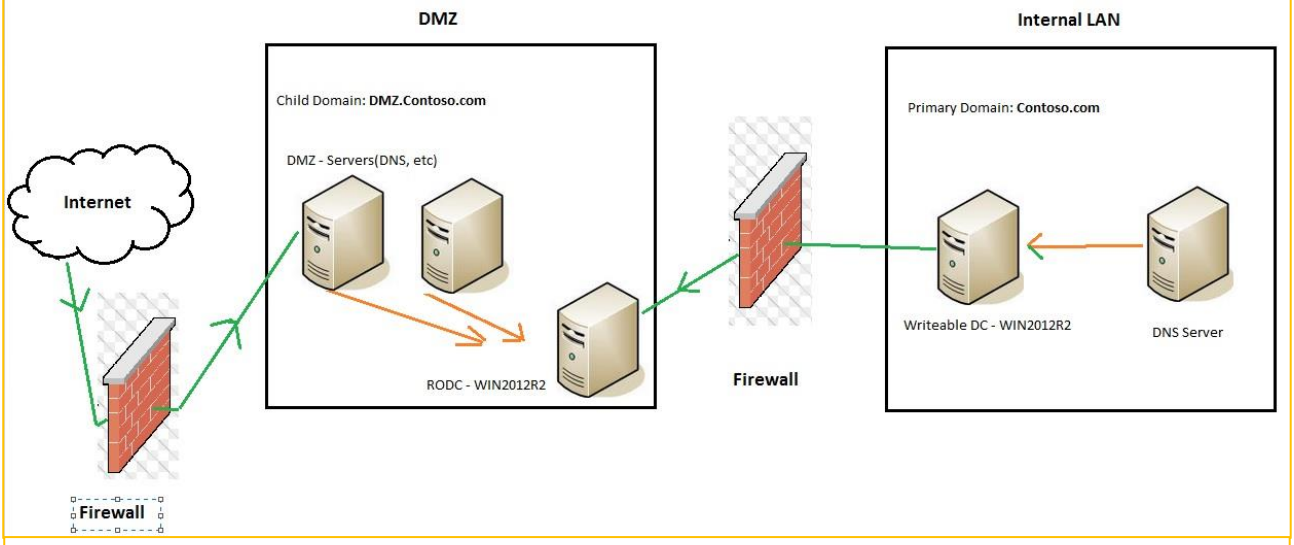
Se utiliza para albergar los servicios públicos: correo electrónico, DNS, Web, FTP,etc.

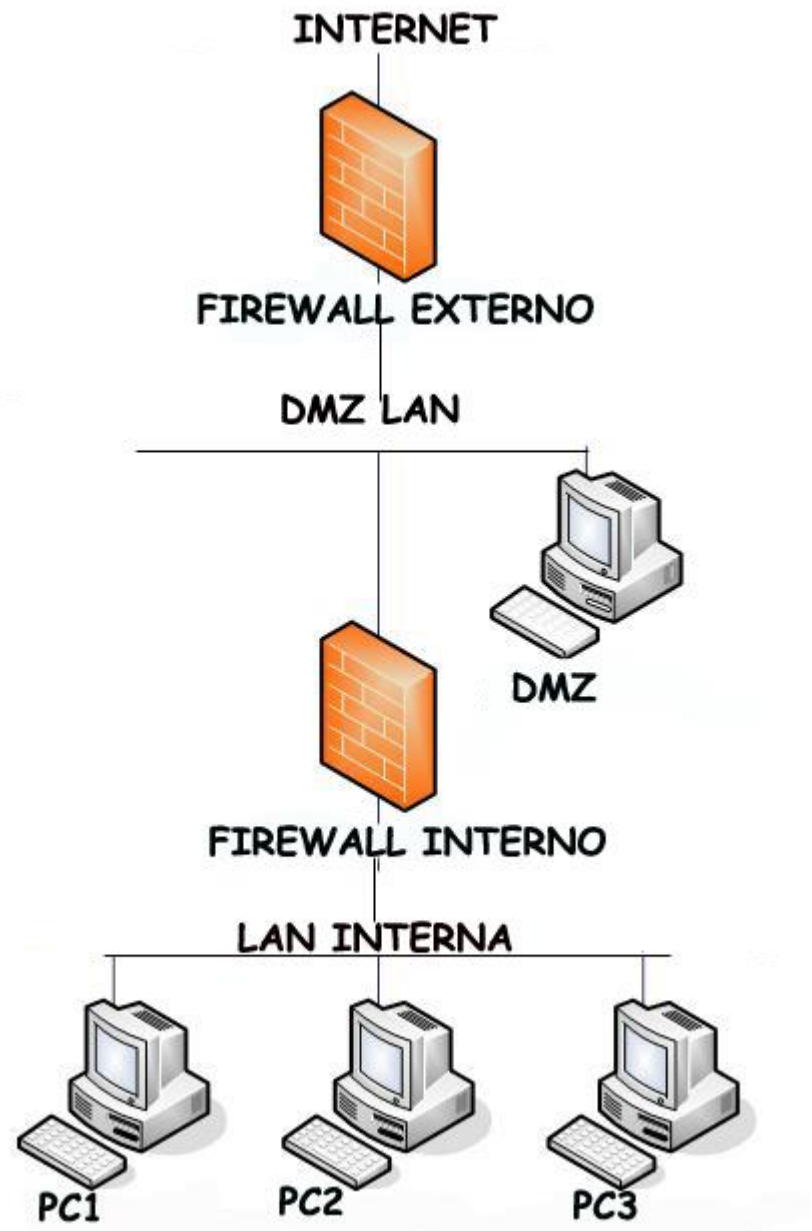
La disposición mínima exige la existencia de un cortafuegos (Internal Firewall) que hace de barrera entre esta red externa y la red interna. Este transito se realiza de la siguiente manera:

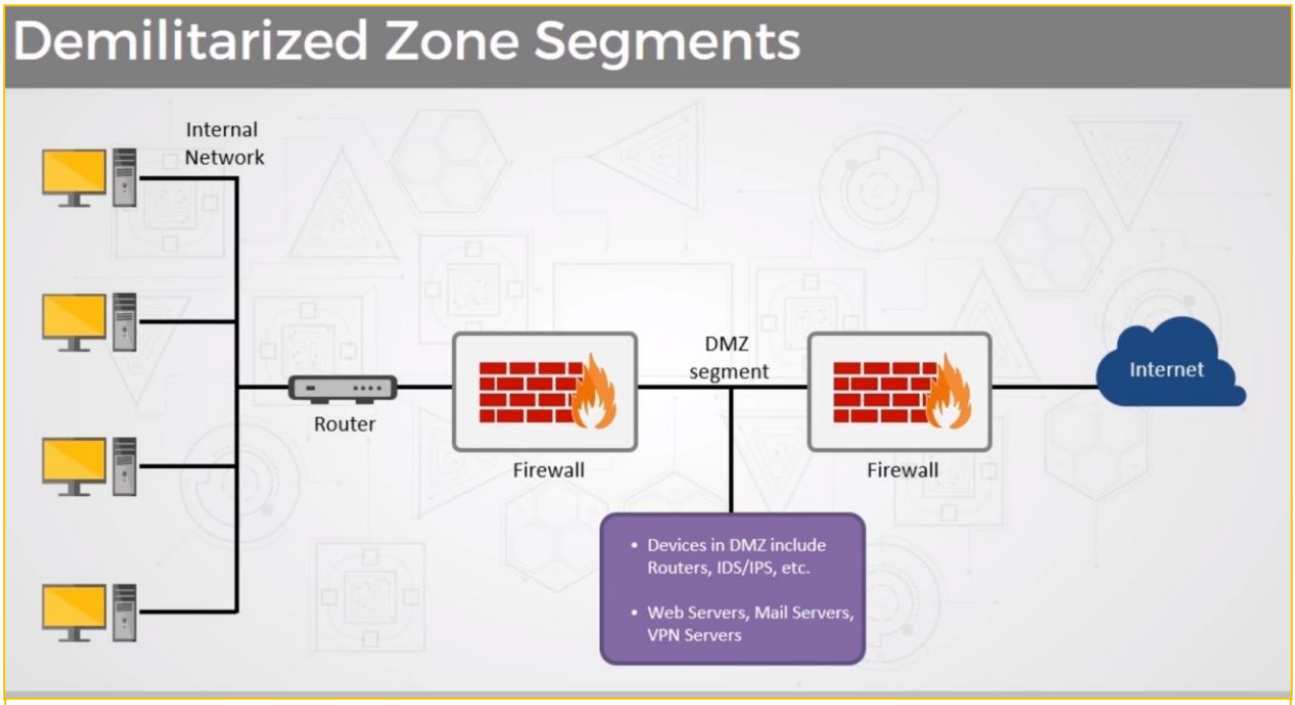
- Desde el exterior no se puede acceder a la red interna.
- Desde la red interna se puede acceder a los servicios que se hayan en la DMZ y al exterior.

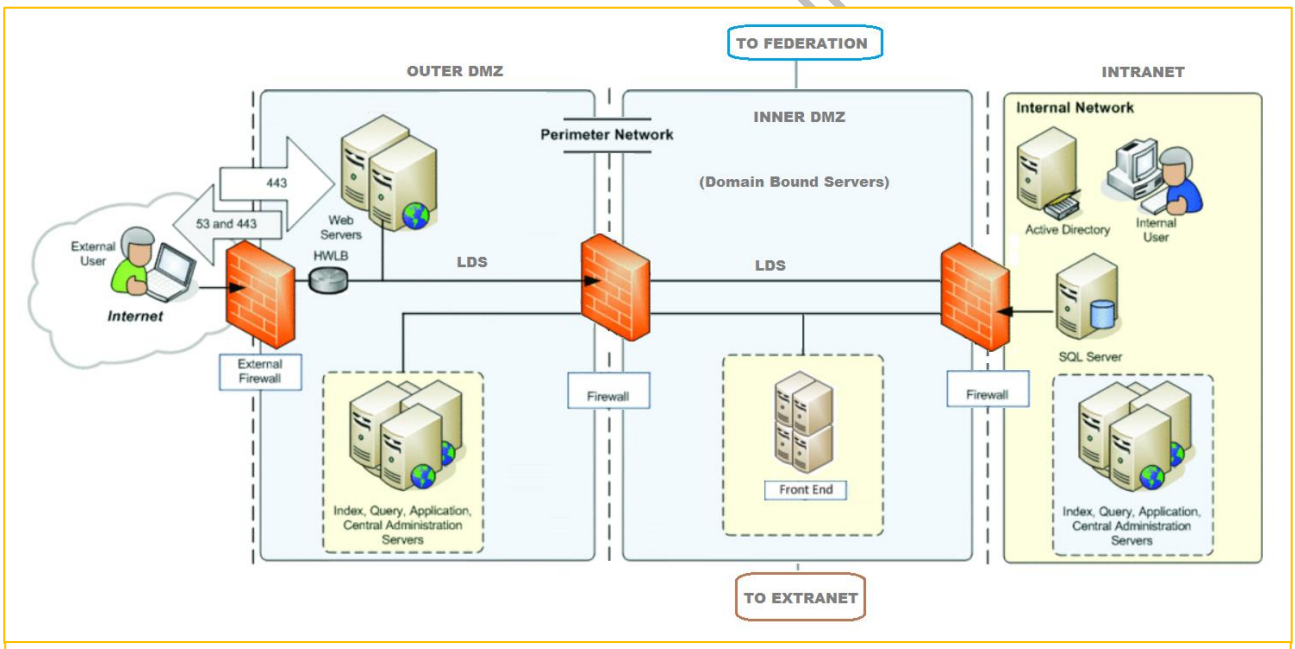
La disposición óptima ubica un segundo firewall (External Firewall) entre la DMZ e Internet para proteger esta.

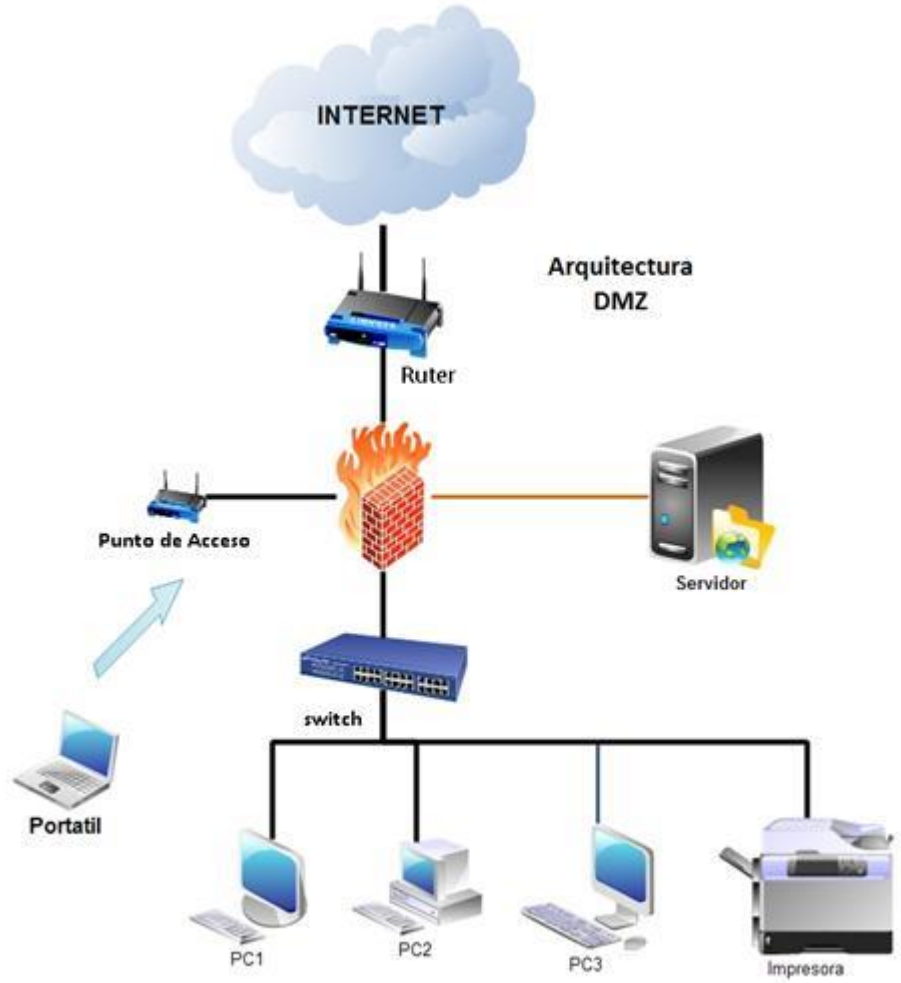












7.3.2. SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

Definimos **Intrusión** como la secuencia de acciones realizadas por un usuario no autorizado (Intruso) con el objetivo de acceder a un sistema informático.

¿Y el atacante qué hace para entrar en el sistema?

La intrusión en un sistema se lleva a cabo de la siguiente manera:

- **Vigilancia**: El atacante trata de descubrir servicios vulnerables y errores de configuración
- **Explotación de servicio**: El atacante se hará con privilegios de administrador gracias a las vulnerabilidades
- **Ocultación de huellas**: El atacante elimina entradas en ficheros de registros, desinstalación de aplicaciones o actualización de los sistemas para que no se pueda volver a entrar

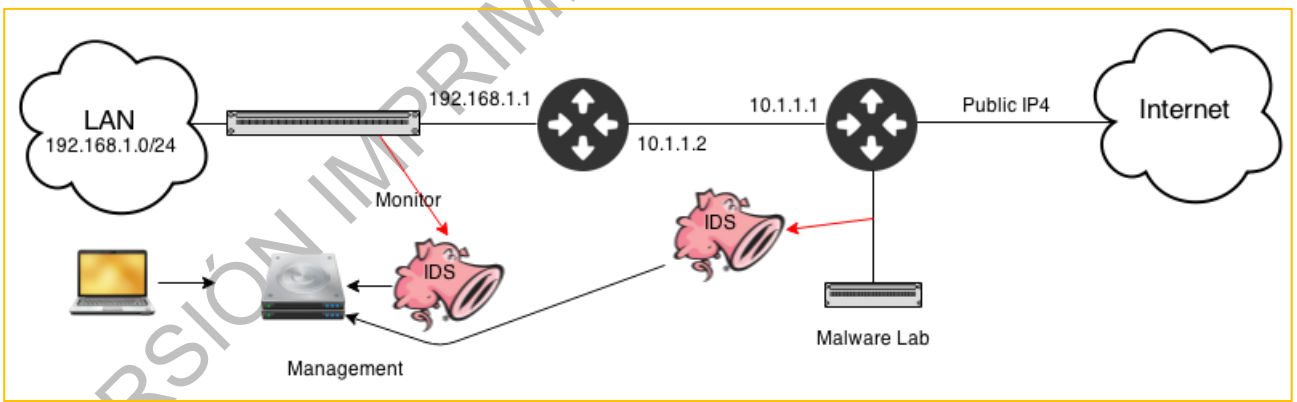
- **Extracción de la información**: El atacante revisa la información obtenida de la base de datos del sistema

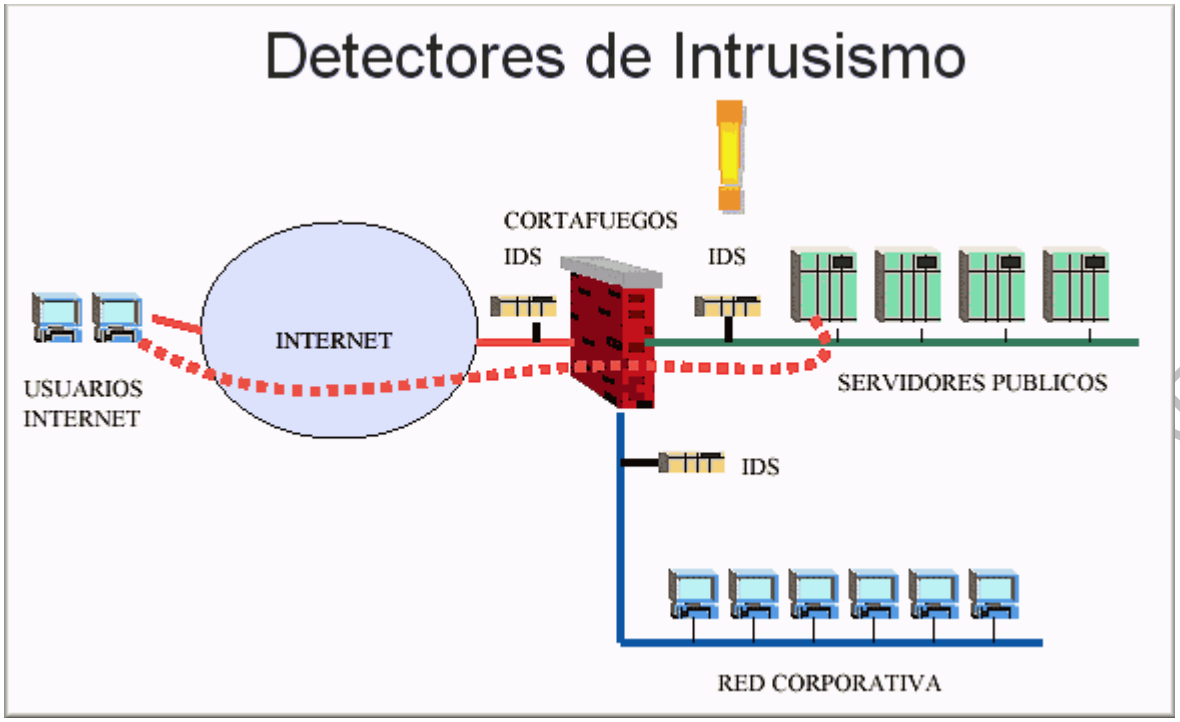
¿Y cómo lo hará?

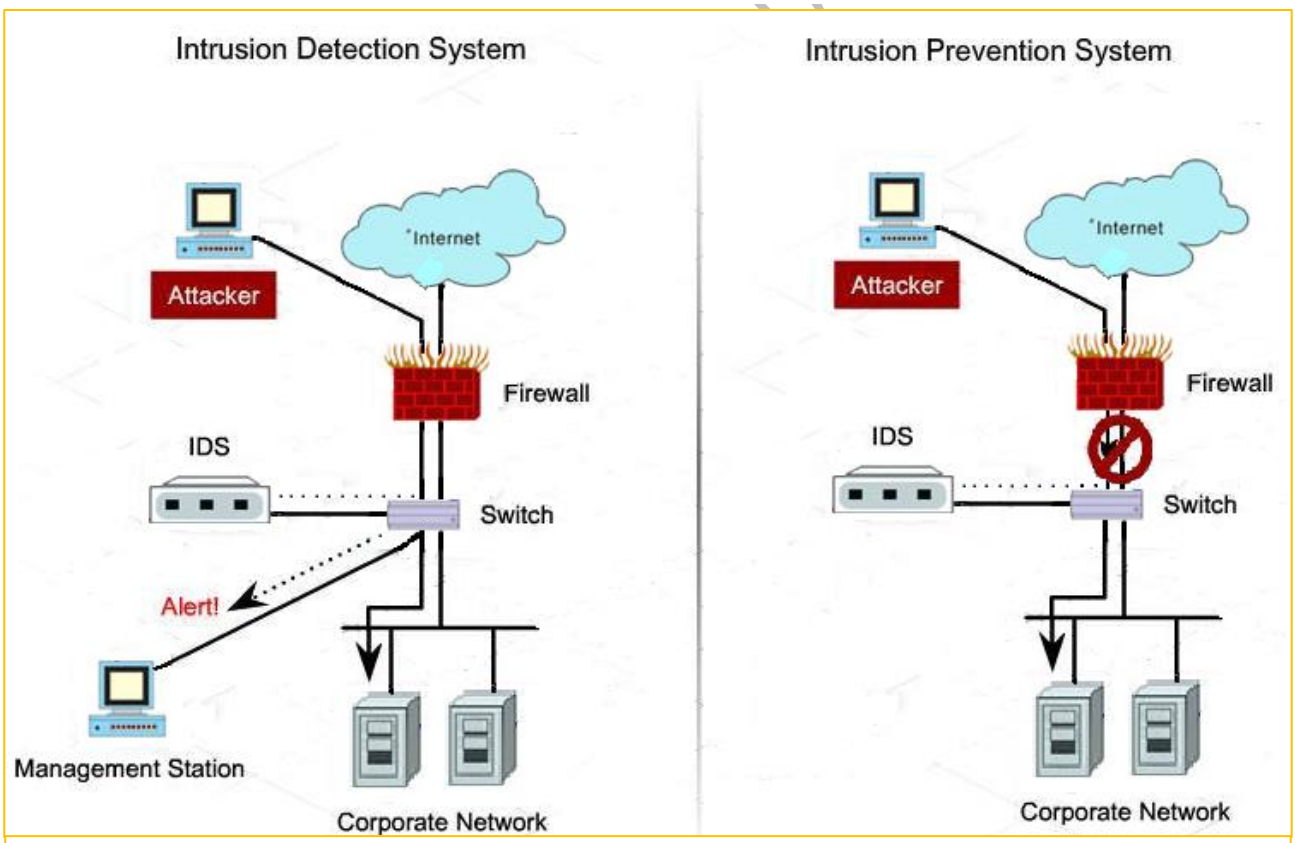
Hay multitud de técnicas, pero para que lo entendáis vamos a poner un ejemplo de una empresa que tiene un cortafuegos instalado.

Supongamos una web de una empresa www.miempresa.com y queremos introducirnos en su sistema:

1. Averiguaremos dónde se encuentra alojado el servidor web de la empresa. Para ello realizamos una serie de consultas al servidor DNS.
2. Realizaremos una exploración de puertos en cada una de las direcciones IP que hemos encontrado en el paso anterior. La idea es detectar servicios que se estén ejecutando.
3. Si el Administrador ha instalado un cortafuegos y lo tiene configurado mínimamente, solo veremos dos máquinas de la red: el Servidor DNS y el Servidor Web.
4. Vamos a por el Servidor Web. Tenemos que descubrir de qué tipo es (Apache o IIS) y la versión.
5. También nos interesa conocer el Sistema Operativo y el Hardware del servidor.
6. Con toda esta información podemos buscar los Exploit que utilizaremos para realizar el ataque de intrusión
7. Una vez ya hemos entrado, nos dedicaremos a borrar nuestro rastro. Después instalaremos una **Rootkit**. Una Rootkit es un conjunto de herramientas que nos dejarán Puertas Abiertas en el sistema atacado y así poder entrar cuando queramos y hacer lo que nos apetezca.







Un IDS es un programa o dispositivo con las siguientes funciones:

- Identificación de posibles ataques
- Registro de eventos
- Bloqueo del ataque
- Reporte al Administrador y personal de seguridad

Tenemos dos tipos de IDS principalmente:

- **Host-IDS**: Se instala en el equipo y monitoriza los cambios en el sistema operativo y las aplicaciones. Se ejecuta en segundo plano dentro de una máquina
- **Network-IDS:** Su función es monitorizar el tráfico de la red. Se instalan en cualquiera de los hosts o en elementos que reciban todo el tráfico de la red (enrutadores) y desde estos, monitorizar varias máquinas.

¿Cómo funcionan estos dispositivos?

Funcionan como los antivirus: por firmas y por patrones de comportamiento.

El sistema IDS más conocido es el **SNORT**.

7.3.3. HONEYPOTS

Como hemos comentado antes, son sistemas de pruebas ante malware. Hay que decir que deben estar especialmente controlados y desconectado de cualquier red.

Tenemos dos tipos principalmente:

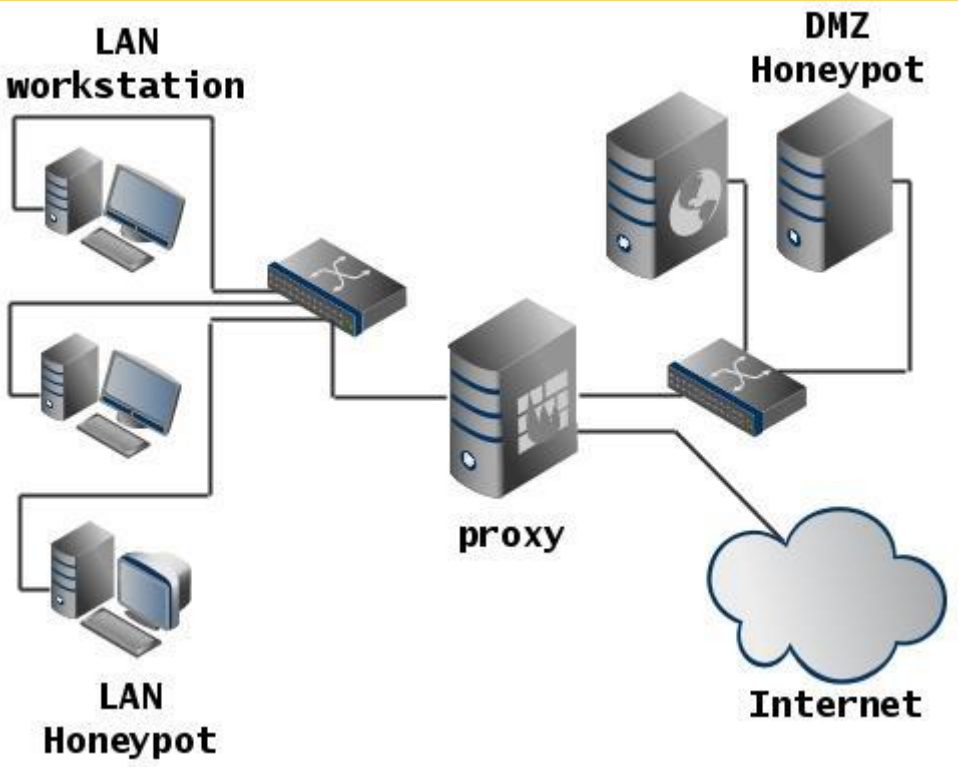
- De baja interacción: Es una aplicación que simula una vulnerabilidad en el sistema operativo
- De alta interacción: Es un sistema operativo con vulnerabilidad

Estos entornos de pruebas los podemos utilizar para probar configuraciones que queremos aplicar y comprobar su seguridad. Para ello podemos utilizar los Escáneres de Vulnerabilidades.

Un **escáner de vulnerabilidades** es un conjunto de aplicaciones que permite realizar pruebas o test de ataques para determinar si la red o el equipo tiene deficiencias de seguridad que pueden ser explotadas por un posible atacante.

Aplicaciones para realizar estas pruebas tenemos:

- COPS
- TIGER
- Nessus



7.3.4. REDES VIRTUALES PRIVADAS (VPN)

Estos sistemas de conexión desde el exterior de la red (Internet) resuelven el problema que planteamos al principio: poder acceder desde cualquier punto a servicios internos.

El problema principal de este necesidad del usuario es que cuando nos conectamos desde el exterior de la red, utilizamos Internet, que es una infraestructura pública, y, por lo tanto, poco segura.

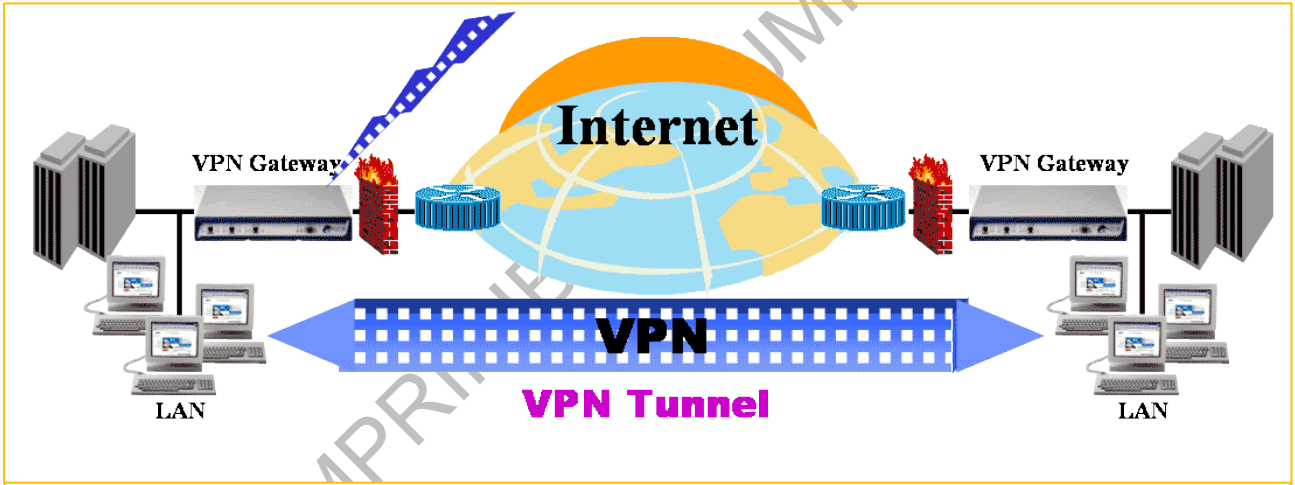
Por eso necesitábamos un sistema que generase una pasarela o túnel o vía que conectase punto a punto, nuestro ordenadores personal que está en casa con la oficina central, pero atravesando Internet. Esto es la VPN.

La VPN se caracteriza por contener:

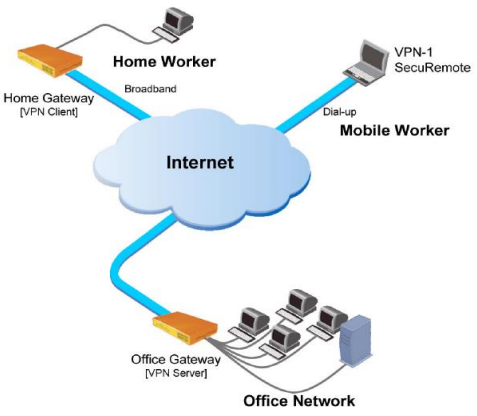
- Autentificación y autorización: Hay gestión de usuarios, roles y permisos.
- Integridad: Mediante el uso de algoritmos Hash
- Confidencialidad: La información viaja cifrada con DES, 3DES, AES, etc.
- No repudio: Los datos se transmiten firmados digitalmente

Tipos de VPN que nos podemos encontrar:

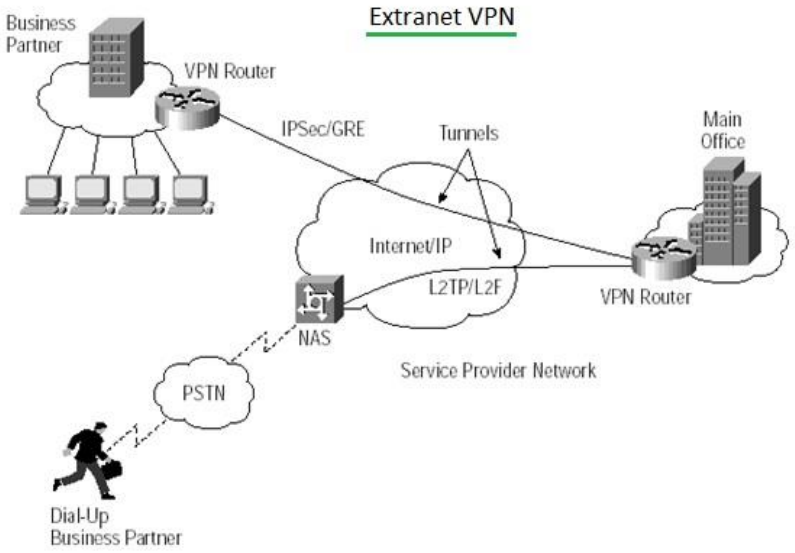
- **VPN entre redes locales**: Una empresa dispone de intranets en diferentes sedes, geográficamente separadas, que se encuentran restringidas a sus empleados. Un responsable quiere acceder a la intranet de otra sede por lo que implantamos una VPN que las conecte y genere una única intranet. Para esta situación se genera una Pasarela VPN (**Tunnel VPN**) en cada intranet. Esta pasarela se conecta a Internet y su misión es cifrar y descifrar los paquetes de la comunicación. Sale mucho más barato que una línea dedicada



- **VPN de acceso remoto**. Un empleado quiere acceder desde el PC de su casa a la intranet de la empresa. El empleado tiene en su ordenador instalado un cliente VPN que se comunica con la pasarela VPN de la intranet a la que quiere conectarse.



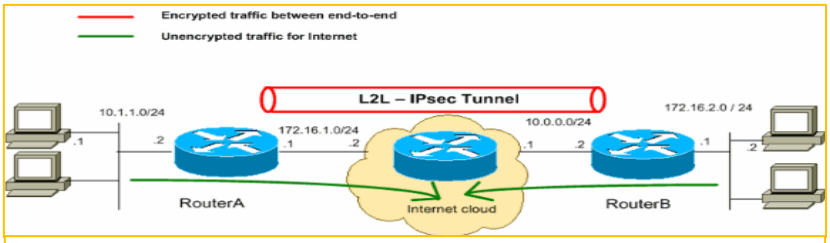
- **VPN extranet**. Una empresa está interesada en que proveedores puedan acceder de manera segura a su intranet. A esta red nueva que genera la VPN se denomina extranet. La gestión se realiza como las anteriores, como pasarelas VPN o un cliente VPN, el tema es que el control de acceso debe ser más restrictivo



¿Cómo se genera la seguridad en el VPN?

La seguridad dentro de una VPN se genera con los protocolos que se utilizan dentro de cada túnel. Entre los protocolos existentes los más usados son:

- Ipsec. Es el más utilizado en todas las opciones.
- PPTP (Point-to-Point Tunneling Protocol). Se utiliza a nivel de cliente VPN.
- L2F (Layer Two Forwarding). Se utiliza a nivel de cliente VPN y se suele combinar con un servidor RADIUS
- L2TP (Layer Two Tunneling Protocol). Combina las funcionalidades de PPTP y L2F
- SSH (Secure Shell).



7.3.5. LA GESTIÓN UNIFICADA DE AMENAZAS (UTM)

Para no tener que calentarnos la cabeza comprado e implantando todos los elementos de los que hemos hablado, existen en el mercado equipos que integran en un único dispositivo un conjunto de soluciones de seguridad perimetral, los UTM.

Estos dispositivos incorporan:

- Cortafuegos
- IDS
- Pasarelas antivirus y antispam
- VPN

7.4. LOS PROTOCOLOS DE SEGURIDAD

Hemos hablado de técnicas de comunicación, pero se merecen un apartado propio una serie de protocolos que nos brindan que estas comunicaciones serán seguras.

Para saber entender mejor lo que vamos a tratar analicemos el Modelo OSI. Si lo recordamos tenemos dos capas, la capa 3, la de Red, y la capa 4, la de Transporte.

La capa 3, o de Red, tiene la función de proporcionar el enrutamiento de mensajes y determina si el destino de estos es la capa 4 o la capa 2. En esta capa se generan lo que denominamos paquetes. El dispositivo que trabaja en esta capa es el Router y tiene como función decidir el reenvió de cada paquete que llega a su interfaz (Gateway). El protocolo con el que trabajamos en esta capa es el IP.

La capa 4, o de Transporte, es la responsable de la regulación del flujo de información desde el origen hasta el destino, en forma confiable y precisa. En esta capa se trabaja con Segmentos. En esta capa trabajamos con los protocolos TCP y UDP.

7.4.1. IPSec

El IPSEC es un conjunto de protocolos, que trabaja en la capa 3, que permite autentificar, autentificar y cifrar un flujo de datos. Para el cifrado utiliza cifrado simétrico y asimétrico.

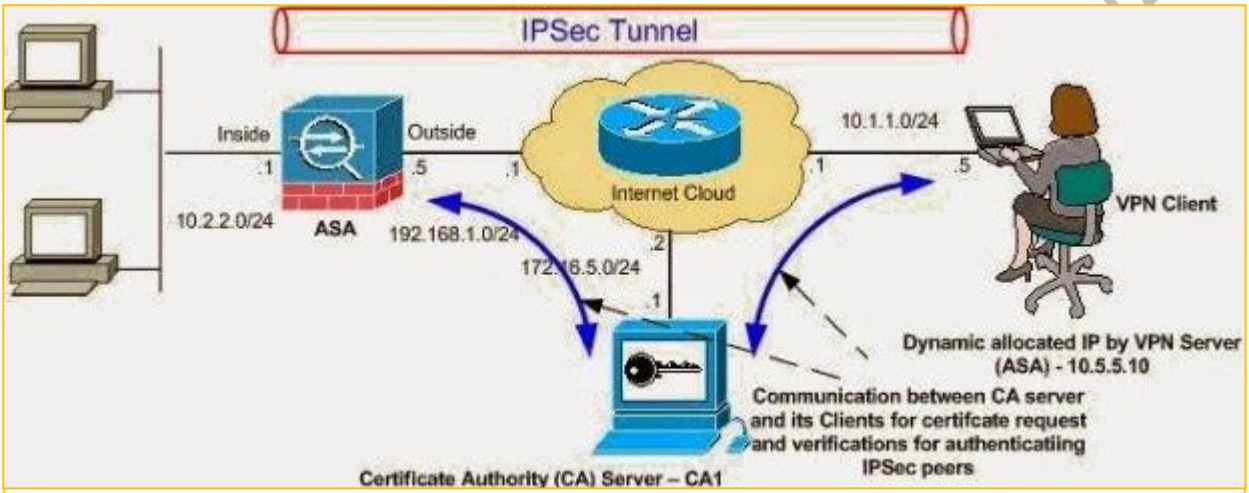
El IPSec añade servicios de seguridad al protocolo IP y a los superiores (TCP, UDP, ICMP).

Se compone de dos protocolos:

- AH (Authentication Header)
- ESP (Encapsulating Security Payload)

Estos protocolos son los que proporcionan autenticación y confidencialidad del paquete IP.

Para poder implementar una arquitectura IPSec necesitamos que el origen, el destino y los puntos intermedios (cortafuegos y routers) lo soporten. Por esto puede ser necesario cambiar los routers de la red.

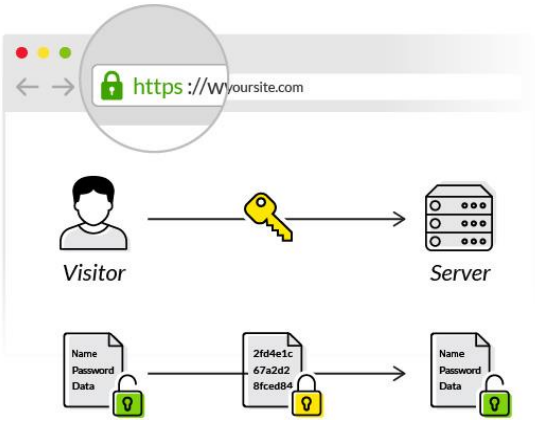


7.4.2. SSL/TLS

El protocolo **SSL (Secure Sockets Layer**) tiene como finalidad proteger las conexiones entre clientes y servidores web con el protocolo HTTP.

El SSL permite al cliente asegurarse de que se ha conectado al servidor auténtico y poder enviarle datos confidenciales con la confianza que nadie podrá verlos.

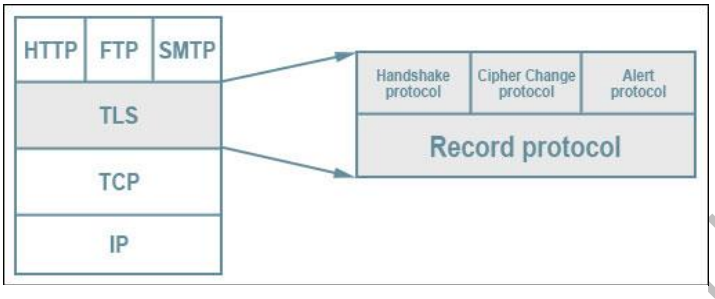
El **TLS (Transport Layer Security)** es una versión actualizada de SSL. Si os dais cuenta, os estará pasando en los navegadores que cuando visitáis alguna web os aparece un mensaje de que no puede visualizarla porque no tiene el TLS habilitado.



Los dos protocolos trabajan con certificados digitales para cumplir su función. Es responsabilidad de las empresas actualizarlos de SSL a TLS.

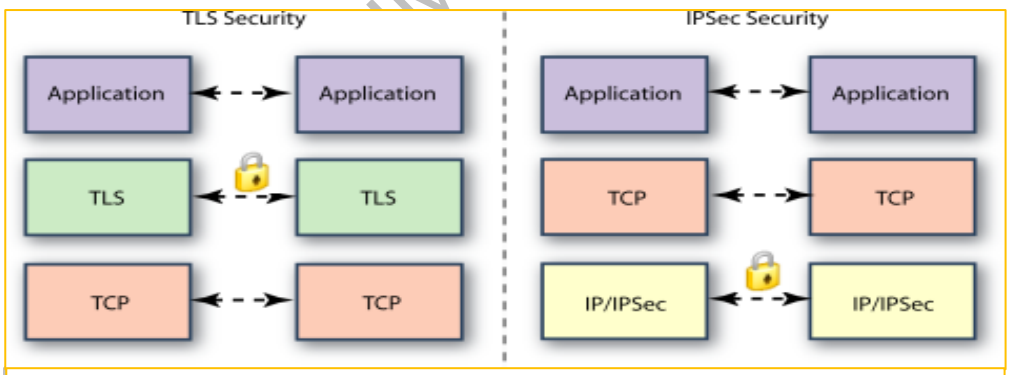
¿Cómo funcionan estos protocolos?

1. El cliente y el servidor entran en un proceso de negociación (handshake) en el cual se intercambian información
2. Una vez acaba la negociación, el servidor envía su certificado digital.
3. Usando clave preestablecida, se codifica y descodifica todo lo que se transmite hasta que cerremos la conexión



Cuando se diseñó el SSL se implementó a nivel de capa 4, transporte, lo que permite que otras aplicaciones lo puedan utilizar. Actualmente, hay numerosas aplicaciones que lo utilizan:

- TELNET/SSH
- FTP
- SMTP
- POP3 y IMAP



-

7.4.3. SSH

El protocolo **SSH (Secure Shell)** permite a los usuarios controlar y modificar sus servidores remotos a través de internet. Utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto suceden de manera encriptada. Permite, además, autenticar al usuario remoto.

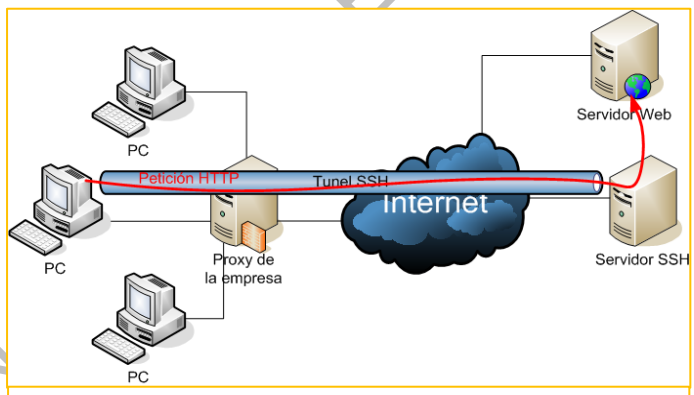
¿Como funciona SSH?

Este protocolo trabaja a nivel de aplicación, con el modelo cliente-servidor para poder realizar la autenticación de dos sistemas remotos y el cifrado de los datos que pasa entre ellos.

SSH opera en el puerto TCP 22 de forma predeterminada.

El servidor escucha en el puerto 22 para las conexiones entrantes.

El cliente inicia la conexión SSH indicando el protocolo TCP con el servidor, asegurando una conexión segura mediante clave con el servidor. Después presenta sus credenciales de usuario.



Actualmente hay multitud de cliente SSH, pero el que más me gusta es el **PuTTY**.

Para el software de Servidor, se utiliza actualmente el **OpenSSH**.

7.4.4. La lista CAN

Cuando un hacker planea realizar un ataque, debe plantearse una serie de pasos a seguir antes de realizar cualquier ofensiva. Existen muchas formas de entrar en determinados lugares con acceso restringido, cuyo objetivo puede ser la conquista de una máquina remota o simplemente la escalada de privilegios de un usuario en un ordenador local.

Para realizar un ataque siempre tenemos que investigar primero la víctima como, por ejemplo, sus direcciones IP, qué servicios se encuentran iniciados y en qué puerto están trabajando, qué aplicaciones utilizan. El conocimiento de esta información es vital para continuar con el siguiente paso.

Muchos programas y sistemas informáticos en la actualidad a veces por la rapidez en el diseño y escaso tiempo de prueba poseen una serie de errores de programación conocidos como **bugs**, que pueden ser aprovechados por un hacker malicioso para realizar un ataque. Estos errores constituyen verdaderas vulnerabilidades que ponen en peligro la seguridad de los datos de la víctima frente al exterior. Los problemas que plantea esta cuestión hacen que las compañías de software tengan que sacar una serie de actualizaciones para sus programas que permiten arreglar los agujeros de seguridad detectados lo antes posible.

La víctima es vulnerable a un ataque del exterior en el transcurso de tiempo desde que se descubre el error hasta que se saca una solución o parche para el UG. Durante este tiempo un intruso malintencionado podrá realizar ataques que exploten esta vulnerabilidad peligrando así la seguridad de la víctima. Igualmente, importante es que exista algún tipo de base de datos que contenga información que descubra el error, como se provoca y si existe o no alguna actualización que lo corrija.

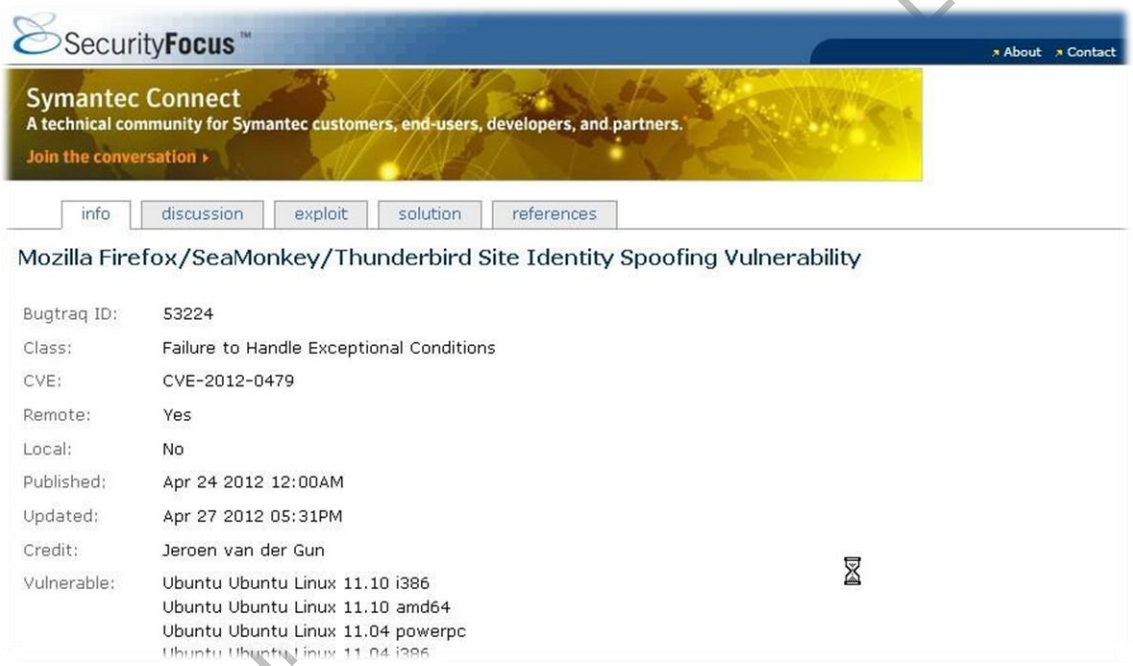
En la actualidad y debido a la gran cantidad de bugs que se han encontrado en los sistemas operativos y aplicaciones existen unas bases de datos que contienen información sobre vulnerabilidades, quien las descubre, qué clase de vulnerabilidades, cómo se pueden explotar, qué resultados provocan, qué sistemas y versiones afectados, y su solución, si los hubiere. Existen varias clasificaciones que describen y ordenan las diferentes vulnerabilidades que han descubierto; una de las más importantes es la base de datos **Bugtraq**, lo actualiza muy frecuentemente y es vital para encontrar mucha información acerca de los errores detectados de un software. También están las llamadas listas o diccionarios de vulnerabilidades **CVE-CAN** (conmuevo vulnerabilidad and Exposures) las cuales están formadas por un nombre que identifica la vulnerabilidad, por una descripción del problema y por una lista de referencias que amplía la información sobre el error encontrado.

CVE y CAN forman dos listas diferentes que se diferencian en la consideración o no de error como vulnerabilidad. el diccionario CVE está compuesto por aquellos errores que han sido estudiados y aceptados como vulnerabilidades y aquellos que todavía no han sido aprobados como tales se encuentran englobados en la lista **CAN**.

Los dos listados de información se clasifican de la misma manera: se hace referencia a ellos con el prefijo CVE o CAN seguido de una cifra de cuatro dígitos que distinguen al año, un guion y otra cifra que indica el número de error de aquel año: un ejemplo de este formato se CVE-2007 a 1003. Si

existe un error que en un principio se encuentra en la lista CAN como CAN-2007-1010 y tiempo más tarde se considera este error como una vulnerabilidad, la información identificaría igual sólo cambiando el prefijo CAN por sus siglas CVE, es decir, quedaría como CVE-2007-1010.

Si se quiere tener un sistema seguro y libre de vulnerabilidades es muy recomendable estar al día de las alertas de seguridad que aparecen en CVE_CAN. Una página muy recomendable para visitar se **http://www.securityfocus.com** donde se pueden encontrar la base de datos Bugtraq actualizada con las últimas vulnerabilidades, clasificada por tres criterios según sea el vendedor del software con problemas, su nombre y la versión con el error. Esta base de datos es muy recomendable ya que nos da mucha información sobre el error, donde encontrar un Exploit que se aproveche de la vulnerabilidad, como solucionar el bug y por último varias referencias de ayuda tanto a las listas CVE-CAN como artículos relacionados con el tema.



Recursos y enlaces

Conexión VPN. Windows 10 y Linux

Objetivo: En esta práctica vamos a realizar una conexión a un servicio VPN que previamente hemos contratado (server.vpn.com) desde un Windows 10 y un Ubuntu.

- https://youtu.be/2RzMmKpg5hY
- https://youtu.be/NAuOHOFo7_I

Conexión FTP Segura. FileZilla Server

Objetivo: En esta práctica vamos a instalar y configurar el servidor gratuito FileZilla Server para realizar conexiones seguras.

- https://youtu.be/KcakbX829w4

Conexión a Servidor SSH. OpenSSH y Putty

Objetivo: Instalar un servidor SSH en entorno Linux y conectarnos al mismo mediante el programa Putty desde un entorno Windows. Cómo sabéis el sistema operativo es indistinto.

- https://youtu.be/DipJpF4rCGo

- Listado VPN https://www.pcworld.es/mejores-productos/internet/mejores-vpn-gratis-3673126/

- Nessus https://www.tenable.com/products/nessus

- SNORT https://www.snort.org/

- Anti-Rootkit https://es.malwarebytes.com/antirootkit/

- Putty https://putty.org/

- OpenSSH https://www.openssh.com/

Test de autoevaluación

Indica cuál de los siguientes protocolos actúa en la capa de aplicación del modelo OSI:

a) IPSec
b) SSH
c) UDP
d) TCP

En una red empresarial, el primer elemento de seguridad es:

a) El Router Frotera
b) IDS
c) Antivirus
d) VPN

El protocolo SSH trabaja normalmente con el puerto:

a) 80
b) 8080
c) 22
d) 443

El conjunto de herramientas que permite al atacante poder ingresar al sistema una vez atacado es:

a) Spam
b) IDS
c) Virus
d) Rootkit

SOLUCIONARIOS

Test de autoevaluación tema 8

Indica cuál de los siguientes protocolos actúa en la capa de aplicación del modelo OSI:

a) IPSec
b) SSH
c) UDP
d) TCP

En una red empresarial, el primer elemento de seguridad es:

a) El Router Frotera
b) IDS
c) Antivirus
d) VPN

El protocolo SSH trabaja normalmente con el puerto:

a) 80
b) 8080
c) 22
d) 443

El conjunto de herramientas que permite al atacante poder ingresar al sistema una vez atacado es:

a) Spam
b) IDS
c) Virus
d) **Rootkit**