

Desarrollo de supuestos prácticos de resolución de incidencias donde se ponga de manifiesto

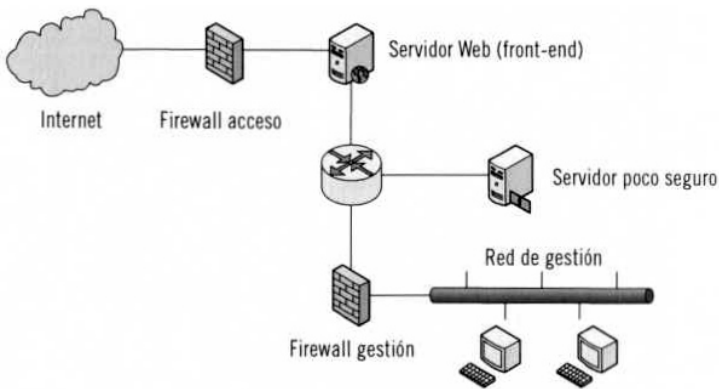
Se dispone de una gran cantidad de herramientas, tanto software como hardware para la gestión y la resolución de incidencias, que también sirven para la administración de las redes en general. Con estas herramientas, se trata de resolver el problema. En este epígrafe, se va a trabajar con un supuesto concreto de una posible incidencia, para poder intentar hacer un uso más concreto y práctico.

Supuesto práctico

Hay una red de que da servicio a un sistema de compras por Internet. En este sistema, hay un servidor central donde están los productos dentro de su espacio correspondiente y en una base de datos de las tres tiendas que están asociadas a través de esta página. Hay otro servidor que está conectado a este, pero no tiene acceso directo al público y es el que tiene el pago por Internet. Y todo esto a través de un cortafuegos y los correspondientes routers que dan acceso a Internet.

También hay una red interna de la oficina y de teletrabajo para el personal que trabaja en esta empresa. En la siguiente imagen, se muestra la estructura de la red.

Esquema de red de la tienda online



El dueño de una de las tiendas llama, un lunes laborable a las 11 a.m., explicando que han llamado clientes diciendo que pueden acceder a la tienda, pero que, a la hora de hacer el pedido y pagarlo, les da un error de que no se puede acceder al pago on-line.

Interpretación de la documentación técnica de los equipos implicados

Para poder trabajar con la incidencia, se debe hacer una interpretación de los sistemas que están implicados en el proceso. Lo primero que se debe conocer y saber son los tipos de sistemas (servidores, routers, etc.), pero, para lo que se trata en este tema, saber conocer las redes y, por supuesto, saber leer los mapas de red.

Con respecto a los sistemas, se debe estudiar la documentación que proporciona el fabricante para cada sistema en concreto y, por supuesto, tener buenos conocimientos en redes para poder interpretarla.

Esta documentación suele venir en inglés, ya que es el lenguaje común que se usa a nivel mundial para casi todos los oficios y particularmente en la profesión de administración de sistemas informáticos y de redes.

Por tanto, se deberá conocer y tener acceso a la documentación que proporciona el fabricante de cada sistema implicado en la red.

Pero, concretando en la red, lo primero que se debe de interpretar es el mapa de este ejemplo concreto.

En la imagen anterior, se pueden observar los servidores, los routers y los cables de red. Esto es un mapa conceptual de la red que es de mucha utilidad para empezar a poder examinar las posibles causas.

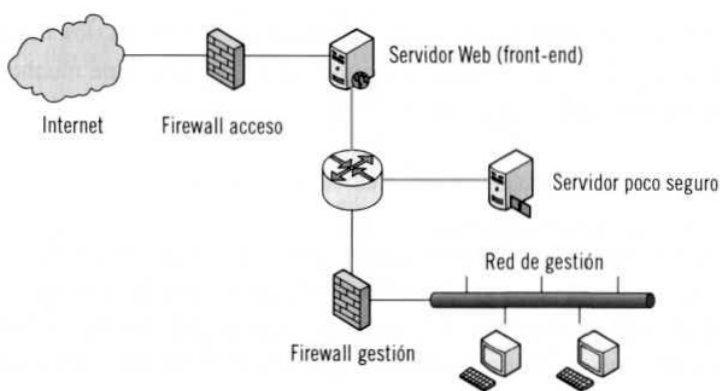
Interpretación de la documentación técnica del proyecto

Para empezar, se debe tener una visión global de la red y de los sistemas implicados en esta. Se tendrá también toda la documentación con la que se trabaja en el proyecto, como es la base de datos de incidencias, de problemas, el SLA, etc. Suele haber programas de gestión de contenidos, muy útiles para hacer más eficiente y menos costoso este trabajo.

Una vez recibida la incidencia, se debe revisar tanto la documentación que llega como la SLA, para ver qué requisitos mínimos se deben cumplir y, por supuesto, estudiar el mapa de red para poder dilucidar las posibles causas.

Como en la especificación de la incidencia en concreto explica que sí se tiene acceso a la tienda y a ver los productos, pero que lo que no se puede es realizar el pago, se puede delimitar la posible zona en la que se encuentra el problema, de la siguiente manera:

Red del ejemplo, destacando la zona en la que se detecta el problema



Una vez delimitada esta zona, las posibles causas son también muchas menos:

- Problema con el cableado entre el servidor al público de la tienda.
- Problema en los routers intermedios.
- Problema de una mala configuración de la red.
- Problema en el software de la configuración de la conexión en los servidores o problema en los servidores.

Por lo tanto, se deberían realizar pruebas para conocer cuál es el problema. Elección de las herramientas de diagnóstico en función del problema

Para conocer la causa real y definitiva del problema, se debe de hacer uso de las herramientas que se han descrito, tanto software como hardware.

Cuando hay un problema de falta de servicio total, siempre se puede hacer uso de una herramienta software en un principio, para que de esta manera se pueda descartar un problema de configuración o de protocolo. Así que, dependiendo del sistema que se esté utilizando o de que se pueda usar un programa de software libre o comprado, se usará:

- Para sistemas Windows: Microsoft Network Monitor o Wireshark.
- Para sistemas Linux o cualquiera de sus versiones o sistemas operativos basados en Unix o Linux: Tcpdump, Wireshark o Nagios.
- Para sistemas operativos Solaris: Snoopo Wireshark.
- Para sistemas operativos Mac OS: Wireshark.

Estas herramientas se pueden utilizar desde un PC remoto si se puede tener acceso remoto a los servidores o, si no se puede, se debe ir físicamente al lugar donde están los servidores y pinchar con un portátil que tenga instaladas estas herramientas en el switch o router que permita que el portátil en cuestión esté dentro de la red.

Sobre estas herramientas, se va a realizar una ejemplificación posteriormente.

Si se llega a la conclusión de que no es nada de software ni de protocolo de redes, se deben realizar pruebas físicas. Para esto, se haría uso de las herramientas hardware descritas. Dependerá un poco del tipo de herramientas que se tengan, porque no todas las empresas se pueden permitir tener todas las herramientas.

En el caso del ejemplo, se podría hacer uso de:

- El comprobador de cables. Se estudiaría el cable que va desde el servidor público de acceso a los clientes a la tienda on-line hasta el servidor de pago.
- En el caso de que se disponga de un certificador de cable, este podría hacer el papel de cualquier otro instrumento.

Se decanta por usar un comprobador de cables y se realiza la prueba con este, conectando cada terminal a un extremo del cable.

Al encender el comprobador de cableado, empiezan a encenderse las luces que identifican cada par de cables con su correspondiente en el extremo opuesto. Pero ocurre que una de las luces del receptor no se enciende. De aquí se deduce completamente que el problema está en el cable físico y se debe de arreglar este cable.

La estimación de la magnitud del problema para definir la actuación

Una vez que se conoce la causa, se tiene que realizar la solución.

Para poder realizar todas las pruebas y para planificar la solución que resolvería el problema en cuestión, se tiene que tener en cuenta, esencialmente, el acuerdo de SLA. De esta manera, se trabajará según ese acuerdo. Para esto, normalmente las empresas de mantenimiento y administración de sistemas y redes suelen ofrecer distintos servicios y tiempos, dependiendo de la criticidad de los sistemas que se quieran administrar y del coste que se desee asumir por parte del cliente. Así, es lógico encontrarse una serie de servicios, como por ejemplo:

- Servicio en horario laboral por la mañana: el menos costoso. Suele ser para clientes cuya red no es realmente crítica o para los que hacen uso de ella solo cuando están en su puesto de trabajo y no realizan otro servicio fuera de ese horario.
- Servicio de horario laboral extendido: un poco más caro que el anterior. Suele ser para empresas que necesitan también servicio por la tarde e incluso los sábados, por ejemplo en horario comercial.
- Servicio 24 x 7: el más costoso. Significa que hay un técnico de guardia todo el tiempo, incluso festivos. Es para sistemas críticos o que basan todo su trabajo en su sistema en red.

Aparte del servicio al que se llegue en el acuerdo, hay otro tipo de acuerdos en el SLA, como cuánto es el tiempo mínimo de actuación o cuánto tiempo como máximo puede estar la falta o la merma de servicio.

Todos estos acuerdos recogidos en el SLA son los que especificarán el tiempo de actuación, tanto para encontrar el error como para

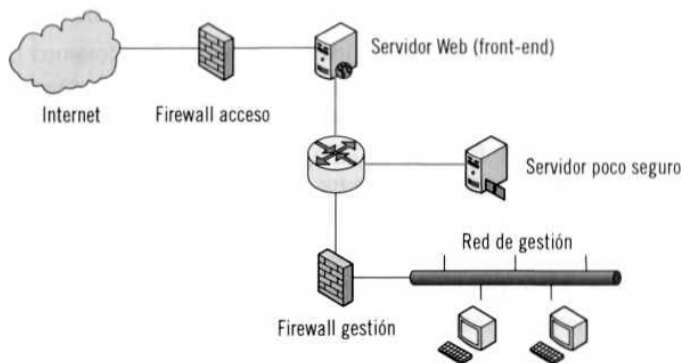
solucionarlo, ya que, por ejemplo, si no está contratado el servicio 24 x 7 y se deja de tener servicio a las 4 a.m., no habrá ningún técnico de guardia, por lo que se empezaría a estudiar la incidencia a la hora de entrada en el trabajo, a las 8 o a las 9 a.m., según se tenga concretado en el acuerdo.

Ejemplo:

En el ejemplo, se ha llegado a un acuerdo temporal laboral extendido, de manera que se otorga servicio los laborables de 8 a.m. a 20 p. m. y sábados de 9 a. m. a 15 p. m. Como el cliente ha llamado dentro de este horario, los técnicos se disponen a realizar el arreglo del cableado.

Aplicación práctica

En la red del ejemplo, que se puede observar en la siguiente imagen, se ha delimitado físicamente el error de manera que se sabe que es en el cable señalado de rojo. Para poder saber las causas del problema, ¿qué herramientas tanto software como hardware utilizaría?



SOLUCIÓN

Como herramientas de software, se pueden utilizar:

- Para sistemas Windows: Microsoft NetWare Monitor o Wireshark.
- Para sistemas Linux o cualquiera de sus versiones o sistemas operativos basados en Unix o Linux, se usaría Tcpdump, Wireshark o Nagios.
- Para sistemas operativos Solaris, se usaría Snoop o Wireshark.
- Para sistemas operativos Mac OS, se usaría Wireshark.

Estas herramientas se pueden utilizar desde un PC remoto si se puede tener acceso remoto a los servidores o, si no se puede, se debe ir físicamente al lugar donde están los servidores y pinchar con un portátil que tenga instaladas estas herramientas en el switch o router que permita que el portátil en cuestión esté dentro de la red.

En cuanto a herramientas hardware, se pueden usar:

- El comprobador de cables. Se estudiaría el cable que va desde el servidor público de acceso a los clientes a la tienda on-line hasta el servidor de pago.
- En el caso de que se disponga de un certificador de cable, podría realizar también la función de comprobador de cableado.