

Arquitecturas de seguridad en Red

Las redes de datos en las empresas han experimentado una drástica evolución desde los comienzos de su desarrollo (unos 20 años atrás), hasta la situación actual, en la que las mismas son parte clave del negocio de las industrias, teniendo por tanto un impacto directo en los resultados financieros de las mismas. De esta forma, las redes se han convertido en estructuras enormemente complejas, con múltiples medios de acceso para la conexión de sus usuarios. Esta característica se ha incrementado recientemente con la aparición de nuevas estrategias (e-bussiness, bussiness-to-bussiness, etc) que interrelacionan diferentes empresas entre sí, así como permiten a sus clientes la adquisición de productos a través de conexiones públicas (fundamentalmente Internet).

Todas estas consideraciones han provocado que las medidas de seguridad destinadas a proteger las redes deben seguir un nuevo modelo: frente a la estrategia usual (normalmente interposición de firewalls o sistemas de defensa perimetral), surge el concepto "holístico"; esto es, considerar la seguridad en las redes de forma global. Así, la arquitectura de una red debe diseñarse en función de los requisitos de seguridad necesarios.

En este artículo se realizará una breve descripción de las arquitecturas de seguridad, comentando las medidas implicadas en cada zona.

ZONAS DE SEGURIDAD

Como base de partida, vamos a considerar que una red típica se divide en las siguientes zonas:

• Francisco García

Director Técnico de
Enterasys Networks



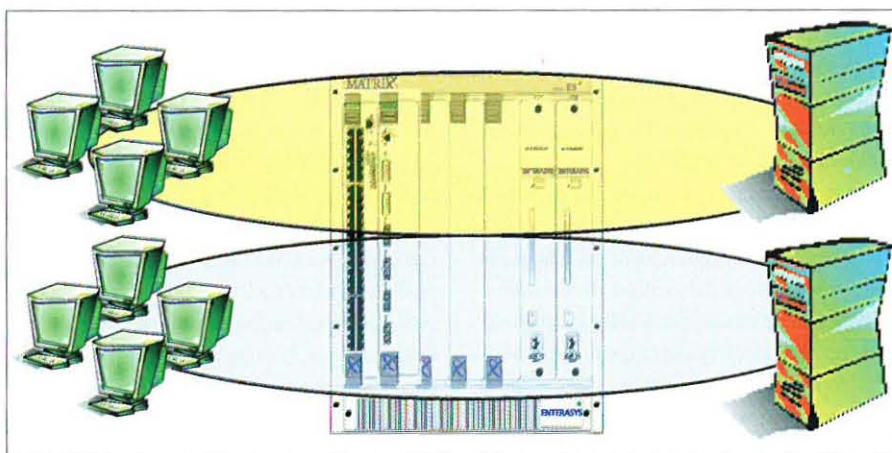
- Acceso: Definimos como zona de acceso aquella a la que se conectan los usuarios locales (típicamente podremos definir dos tipos de usuarios: fijos y los conectados a través de redes inalámbricas).
- Remota: La zona remota es aquella a la que se conectan las comunicaciones con los usuarios remotos (los cuales pueden ser usuarios u otras empresas).
- Núcleo: En esta zona es donde residen los recursos de la red (servidores, hosting,...)

Seguridad en el Acceso

En esta zona nos aseguraremos de que los usuarios únicamente acceden a los recursos a que tienen derecho, con la calidad de servicio asignada. Analizaremos aquí las posibilidades para dichas implementaciones:

– Asignación de usuarios a redes virtuales.

Las redes virtuales (VLAN), estandarizadas por el protocolo 802.1Q, consisten básicamente en el establecimiento de grupos de trabajo, de forma que los usuarios únicamente pueden acceder, de forma directa, a los recursos que se hallan en dicho grupo. Por tanto, una primera estrategia de seguridad es la de implementar redes virtuales en los equipos de acceso, de forma que garanticemos que los usuarios no podrán acceder a recursos fuera de su VLAN, tal y como plantea la siguiente figura:



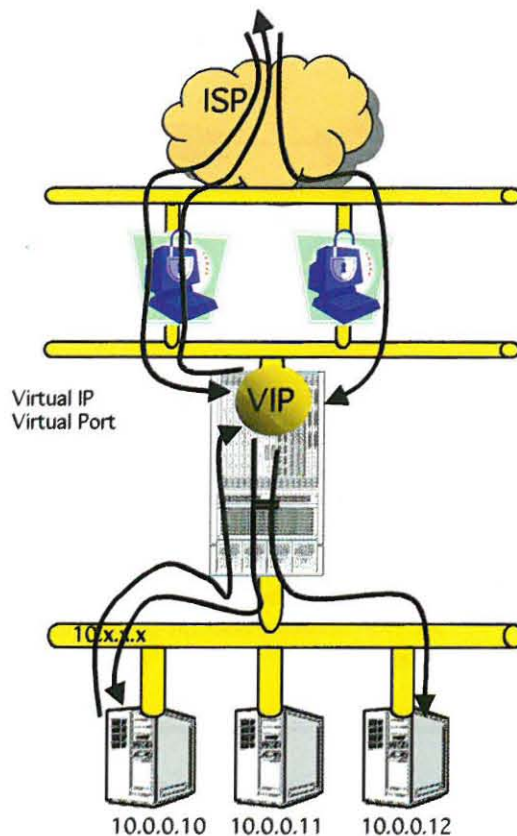
- **Conmutación de nivel 4.** La conmutación de nivel 4 permite que el dispositivo de acceso examine no solamente la información del subnivel MAC, sino también los campos de niveles 3 y 4. Dicho de otra forma: es posible establecer criterios de acceso y/o filtrado mediante la información contenida en estos campos. Así, podemos realizar un filtrado del tráfico o asignarlo a una VLAN de forma dinámica, en función de la aplicación (nivel 4) que esté siendo transportada por la trama. Por ejemplo, podemos permitir que un usuario se comuniquen con un recurso de la red (digamos un servidor de ficheros), pero evitar que dicho usuario haga un TELNET a dicho servidor.
- **Limitación de tráfico.** Una de las características más importantes de los controles de seguridad en el nivel de acceso debe ser la de limitar el tráfico permitido para cada usuario (asimismo en función de los niveles 2, 3 y 4). Además de faci-

- **Encriptación.** Para los casos de redes inalámbricas, además de todos los pasos anteriores, es conveniente que las comunicaciones entre usuarios y puntos de acceso estén encriptadas con el objeto de evitar escuchas en la red.

Seguridad en el Núcleo

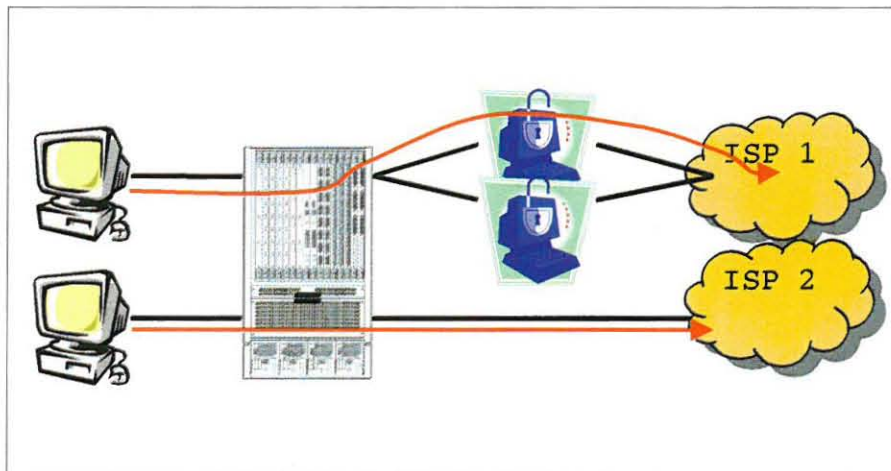
En el núcleo de la red es preciso implementar políticas específicas de seguridad, las cuales describimos a continuación:

- **Filtrado y limitación de tráfico.** De forma análoga a la comentada en el anterior apartado, estableciendo distinciones según los niveles 2, 3 y 4.
- **Políticas de tráfico IP.** Mediante esta capacidad es posible distribuir el tráfico IP según su naturaleza. Por tanto, podemos elegir que determinados usuarios vayan siempre por un determinado camino en la red, distribuyendo las rutas de comunicaciones. En la siguiente figura podemos ver un ejemplo:



Seguridad en los Usuarios Remotos

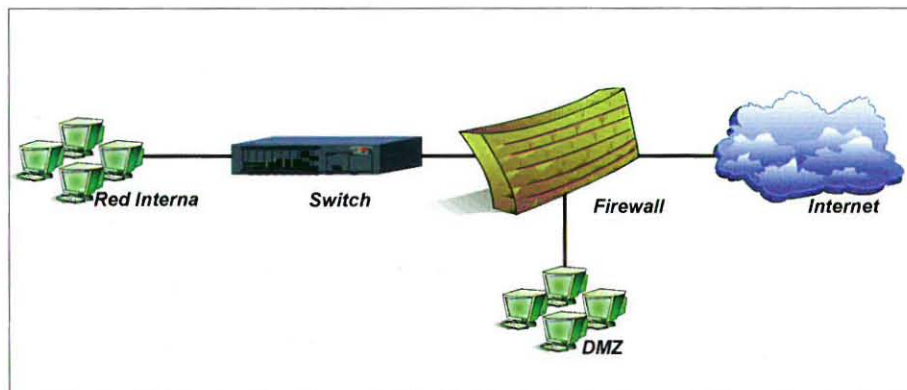
- **Utilización de VPNs.** Típicamente, la solución para la conectividad de los usuarios remotos van a ser las VPN (redes privadas virtuales). Dichas VPN utilizan infraestructura pública (normalmente Internet) para la transmisión de datos privados. La forma de operar consiste en la creación de túneles, (conexiones extremo a extremo), las cuales pueden ser encriptadas para asegurar la privacidad en las comunicaciones.
- **Firewalls.** Las empresas que proporcionan servicios a través de Internet, utilizan frecuentemente un cortafuegos (firewall) con el ánimo de filtrar el tráfico entrante a través de Internet. Es común la implementación de una zona llamada militarizada (DMZ), la cual contiene los servicios solicitados a través de Internet y que está separada de la red interna. En la siguiente figura podemos observar un esquema:



litar el cumplimiento de los Acuerdos de Nivel de Servicio, esta característica permite evitar intentos de envíos masivos de tráfico (característicos de ciertos ataques).

- **Autenticación de usuarios.** La reciente implementación del protocolo 802.1x permite la autenticación de usuarios (no de equipos) en los puertos de acceso, lo que permite el establecimiento de perfiles, asignación de políticas,...

- **Balanceo de direcciones.** El protocolo LSNAT permite el establecimiento de una dirección virtual, con la que se comunican los usuarios. De esta forma, es posible tener un grupo de servidores, los cuales atienden las peticiones de los usuarios, de forma que sus direcciones IP (y sus números de puerto) no son conocidos por aquéllos. Esta solución es muy útil en entornos de "hosting". A continuación vemos un ejemplo:



Sistemas de Detección de Intrusos

Además de lo comentado anteriormente, es necesario implementar un sistema de detección de intrusos (IDS). Dichos sistemas permiten monitorizar actividades sospechosas, detectan brechas de seguridad, etc. Normalmente constan de los siguientes elementos:

- **Servidor.** Actúa como el gestor de políticas, y es el repositorio de datos donde se almacenan y analizan los eventos.
- **Sensor.** Elemento detector de intrusos. Se conecta al segmento de red que deseamos analizar.

- **Cliente para equipos.** Similar al anterior, pero consiste únicamente en un software que se ejecuta en la máquina que deseamos proteger, monitorizando su actividad.

CONCLUSIONES

En este artículo hemos descrito la arquitectura necesaria para la implementación de redes seguras. La conclusión más importante que podemos extraer es que una red segura debe ser diseñada con este propósito, no siendo válido el simple añadido de protecciones perimetrales, sino que es preciso una visión de más largo alcance que tenga en cuenta usuarios, requisitos, ancho de banda disponible, acceso a recursos, etc.



EVOLUCIONANDO

