

Mapa conceptual / Interactividad

|  |
| --- |
| Seguridad Perimetral |
| Firewall | Es software o hardware que comprueba la información procedente de Internet o de una red y le permite el paso o la bloquea, de acuerdo a la configuración del firewall. Un firewall puede ayudar a impedir que hackers o software malintencionado (como gusanos) obtengan acceso al equipo a través de una red o de Internet. Un firewall también puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos. |
| IDS/IPS  | La sigla IDS se refiere a Sistemas de Detección de Intrusos (*Intrusion Detection Systems*). Son sistemas que por medio del monitoreo del tráfico de una red son capaces de detectar actividades hostiles y reportar acerca de los ataques. Pueden ser dispositivos como aplicaciones. La sigla IPS se refiere a Sistemas de Prevención de Intrusos (Intrusion Prevention Systems). Los IPS son considerados una extensión de los IDS ya que se encargan del monitoreo del tráfico y de las acciones correctivas a tomar al momento de la detección. La principal diferencia es que los IPS tienen la posibilidad de tomar acciones para prevenir o bloquear las intrusiones detectadas (DROP de paquetes, reinicio de la conexión, bloqueo de tráfico de cierto origen, etc). |
| WAF  | *Web Application Firewall*. Son un tipo de *firewall* que se utilizan para controlar el acceso a una aplicación o servicio web. A diferencia de un *firewall* tradicional, un IPS o IDS, la ventaja de un WAF es que opera sobre la capa de aplicación (capa 7 del modelo OSI), por lo que es posible considerar algunos tipos de protecciones más allá de las tradicionales con los dispositivos mencionados. |
| UTM  | *Unified Threat Management*. La gestión unificada de amenazas o UTM, por sus siglas en inglés, se refiere a una sola solución de seguridad, y por lo general un único producto de seguridad, que ofrece varias funciones de seguridad en un solo punto en la red. Un producto UTM generalmente incluye funciones como antivirus, anti-spyware, anti-spam, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas. Algunas unidades también ofrecen servicios como enrutamiento remoto, traducción de direcciones de red (NAT, Network Address Translation) y compatibilidad para Redes Privadas Virtuales (VPN, *Virtual Private Networ*k). Lo llamativo de la solución se basa en la simplicidad, por lo que las organizaciones que puedan haber tenido proveedores o productos para cada tarea de seguridad por separado, ahora los pueden tener todos en una sola solución, con el apoyo de un único equipo o segmento de TI, y que se ejecuta en una sola consola. |
| VPN  | *Virtual Private Network*. Una Red Privada Virtual o VPN, por sus siglas en inglés, es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar una VPN para que sus empleados, en forma remota, desde sus casas o cualquier sitio donde se encuentren, puedan acceder a recursos corporativos que de otro modo, no podrían. Sin embargo, conectar la computadora de un empleado a los recursos corporativos es solo una función de una VPN. En conjunto con lo anterior, una implementación correcta de esta tecnología permite asegurar la confidencialidad e integridad de la información. Como puede suponerse, a través de una VPN pasa información privada y confidencial que en las manos equivocadas, podría resultar perjudicial para cualquier empresa. Esto se agrava aún más si el empleado en cuestión se conecta utilizando un Wi-Fi público sin protección. Afortunadamente, este problema puede ser mitigado cifrando los datos que se envían y reciben. |
| DMZ  | *Demilitarized* zone. Una zona desmilitarizada o DMZ, por sus siglas en inglés, es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red. La intención de DMZ es asegurar que los servidores de acceso público no puedan comunicarse con otros segmentos de la red interna, en el caso de que un servidor se encuentre comprometido. Un firewall es relevante particularmente en la implementación de DMZ, ya que es responsable de garantizar que las políticas adecuadas para proteger a las redes locales de DMZ se encuentren habilitadas, mientras que se mantiene la accesibilidad a la zona desmilitarizada (DMZ). Debido a la naturaleza no-trivial de la implementación de DMZ, no se recomienda utilizar un DMZ salvo que tenga una gran familiaridad con las redes. Una DMZ no suele ser un requisito, pero en general es recomendada por los administradores conscientes de seguridad de la red. |