**FIREWALL**

**Next generation firewall**

Es parte de la tecnología de firewall de tercera generación, que combina un firewall tradicional

**Zona desmilitarizada (DMZ)**

DMZ o zona desmilitarizada (a veces denominada red perimetral o subred filtrada) es una subred física o lógica que contiene y expone los servicios externos de una organización a una red no confiable, generalmente más grande, como internet.

El propósito de una DMZ es agregar una capa adicional de seguridad a la red de área local (LAN) de una organización: un nodo de red externos puede acceder solo a lo que esta expuesto en la DMZ, mientras que el resto de la red de la organización esta protegida por firewall.

**Mejores prácticas diseño política firewall**

**No confíes en nadie**: siempre es recomendable habilitar todos los servicios y denegar el resto del tráfico. Analice los usos del usuario y, según el informe, asignarles esos servicios. Debe implementar el principio de menor privilegio para denegar todo acceso para realizar el trabajo sin problemas.

**Denegar el acceso físico al firewall:** siempre es una buena práctica mantener controlado cualquier tipo de acceso físico al firewall o negarlo por completo.

**Permitir solo los protocolos necesarios:** siempre es bueno tener una lista preparada de los protocolos que se deben ´permitir y los que se deben bloquear.

**Usar registros y alertas:** debe tener una etsrategia de resigro que proyecte el nivel y el tipo de registro, y debe asegurarse de monitorear todos esos registros de forma regular.

**Segmento de zona de seguridad:** los cortafuegos se utilizan para proteger el sistema interno…

**No usar el cortafuegos como servidor:** los cortafuegos nunca deben usarse en el diseño de incorporación de servidor.

**Establezca limites de conexión:** imponer límites de conexión en los firewalls del dispositivo de seguridad

**Combine la tecnología de firewall:** el filtrado de paquetes no debe hacerse solo para la línea de defensa. Se puede incorporar con lagunas inspecciones, como protocolo, estado o aplicación.

**Use firewalls como parte de una solución de seguridad integral:** los firewalls deben usarse en yuxtaposición con otros dispositivos para crear una solución de seguridad completa. Deben integrarse con otras tecnologías.

**Mantenga la instalación:** el software y los parches deben mantenerse actualizados. Actualice las configuraciones del firewall a media que cambien los requisitos de la aplicación.