Gestión de Redes Seguras Con Software Libre (SL)

La Red Segura

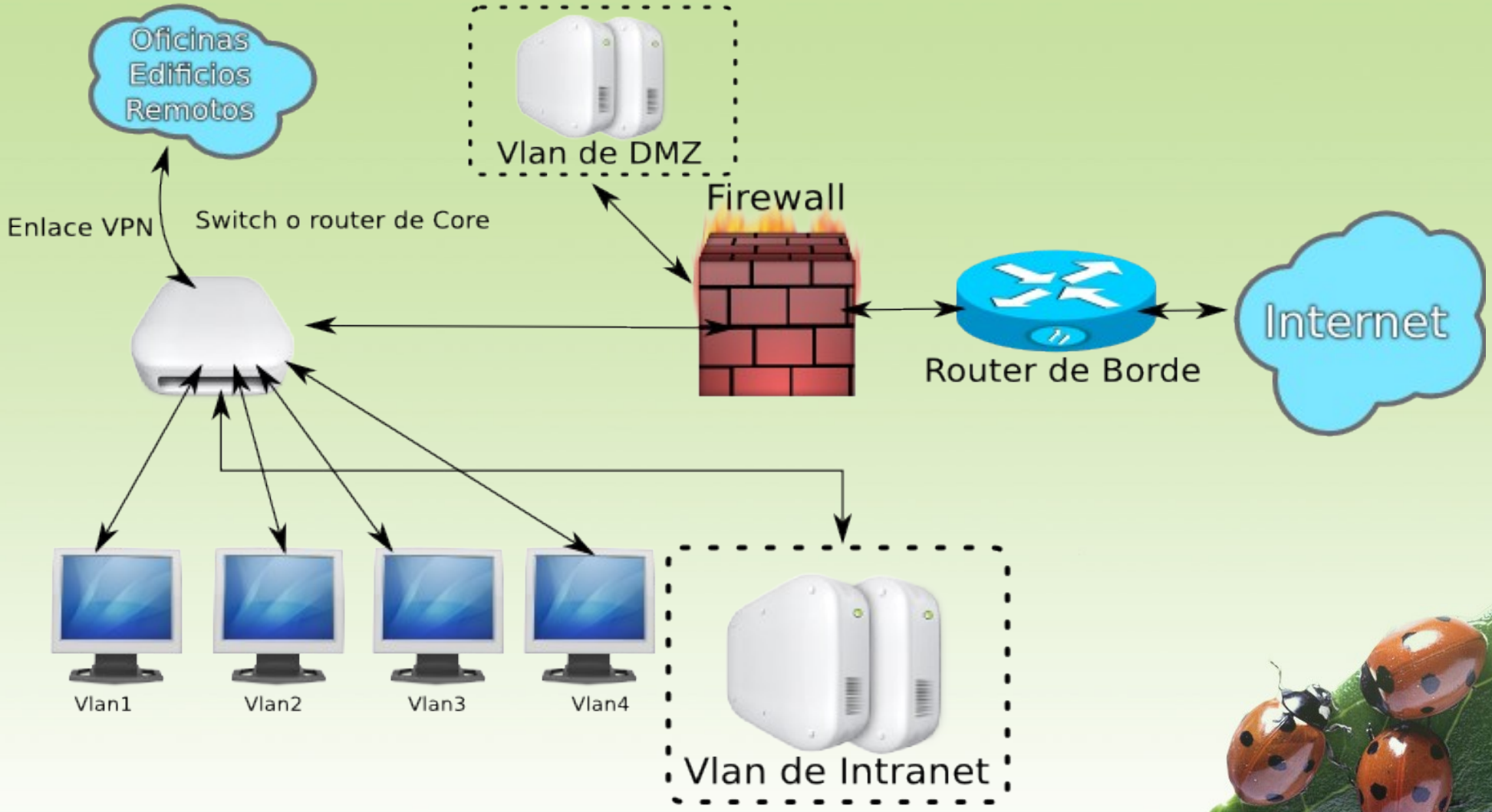
Debe ser capaz de proveer:

- Confidencialidad
  - Asegurar que la información está accesible solo a aquellos autorizados al acceso
- Integridad
  - Mantener la exactitud e integridad de la información y de los métodos de su procesamiento
- Disponibilidad
  - Asegurar que los usuarios autorizados tenga acceso a la información y a los recursos relacionados cuando se requiera

La Red Segura depende de:

- Importancia que da la directiva o gerencia.
- Inversión en equipos y capacitación.
- Políticas de seguridad definidas claramente.
- Buena documentación de todos los recursos.
- Nivel de conocimiento de sus administradores.
- Buena planificación.
- Buena administración y gestión de la misma.

Esquema de Red



Esquema Básico de una Red Mediana

Areas de una Red

Independientemente del tamaño y equipamiento una red tiene tres áreas en donde centrar la seguridad:

- Estaciones de trabajo.
  - Computadoras de escritorio, portátiles, PDA's, teléfonos celulares, usuarios.
- Transporte de datos.
  - Switch's, Routers, Cableado, enlaces.
- Servicios y Servidores.
  - Servicios de red que se proveen internos y externos.

Estaciones de Trabajo (WS)

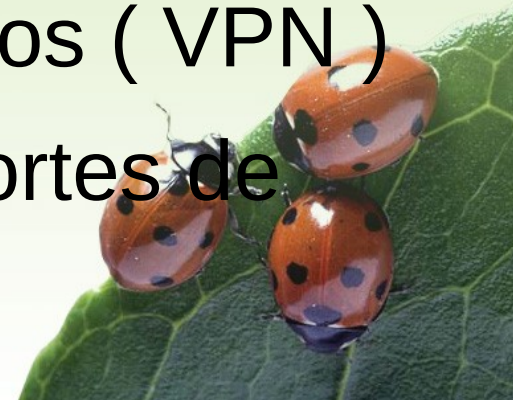
Para tener estaciones de trabajo (WorkStations) seguras la red debe ser capaz de proveer:

- Perfiles de usuario restringidos.
- Políticas de software que se puede instalar y usar bien definidas.
- Buena documentación a nivel de usuario.
- Control de los recursos de red a los cuales se puede acceder.
- Software de protección contra amenazas.

Transporte de datos

Para garantizar la seguridad, disponibilidad y la integridad de los datos que transitan por nuestra red, la red segura debe proveer:

- Segmentación de la red por Vlans.
- Firewalls de protección.
- Documentación adecuada de la red.
- Tener un sistema de cableado bien organizado.
- Cifrado de datos entre enlaces remotos (VPN)
- Software/hardware adecuado de reportes de tráfico, monitoreo, control de la red.



Servicios

Para el área de servicios la red segura debe ser capaz de proveer:

- Control de las licencias y versiones del software instalado.
- Firewall por software en cada servidor.
- Buena documentación de las fallas más comunes en los servicios instalados.
- Buen feedback entre usuarios y el área de servicios.

Ventajas de Usar SL

- Cero costos en licencias de uso.
- Estabilidad, mejor rendimiento e interoperatividad.
- Cero obligaciones con proveedores.
- Uso de estándares.
- Disponibilidad del código fuente.
- Abundante ayuda e información en linea.
- Tecnología lista para usar.

Dificultades para implementar SL

- Los costos del software ilegal es casi cero.
- La curva de aprendizaje es alta.
- Poca disponibilidad de soluciones integrales.
- El Software propietario se diseña para no ser interoperativo con SL.
- Resistencia al cambio.
- Falta de recurso humano calificado y falta de oferta en proveedores.

SL para una red

- Autenticación centralizada
  - protocolo ldap, por ejemplo: Openldap, Fedora Directory Server.
- Manejo de perfiles de usuario en desktop
  - sabayon y puppet para GNU/linux, samba y ldap (PDC) con politicas de gpo para Windows.
- Chat
  - openfire (jabber), ejabberd.

SL para una red (cont.)

- Correo
  - zimbra,postfix+spamassasin+ClamAV+openwebmail/horde/squirrelmail, roundcube.
- Navegación
  - Squid+DansGuardian+ClamAV
- Websites
  - apache/lighttpd/nginx/cherokee
- Enrutamiento y firewalls
  - iptables, netfilter, iproute, dhcpd

SL para una red (cont. 1)

- Bases de datos
  - PostgreSQL, MySQL.
- Monitoreo
  - opennms, zabbix, nagios, zenoss (snmp)
- Estadísticas
  - awstats, sarg, ntop.
- IDS (detección de intrusos)
  - snort, tripwire.

SL para una red (cont. 2)

- Auditoría de redes
  - nmap, nessus, tcpdump, backtrack (distribución).
- Logs centralizados
  - syslog-ng
- Backup
  - clonezilla, amanda, bacula.
- DNS
  - bind

SL para una red (cont. 3)

- Inventario de equipos de red
  - ocs-inventory, php-ip
- Documentación y educación
  - wiki, moodle, zimbra
- GUI para administración de servicios
  - webmin
- Antivirus para servidores GNU/Linux
  - ClamAV
- Certificados digitales y cifrado de datos
  - openssl, tinyCA, openCA, gnupg

Dimensionamiento de Servicios en una Red

- Red de 1 a 50 usuarios
  - Proxy y Filtro de Contenidos, Firewall, DHCP, VPN.
- Red de 50 usuarios hacia arriba

  Dependiendo de las necesidades operativas
  - Proxy y Filtro de Contenidos, Firewall, DHCP, VPN, correo, autenticación centralizada, DNS, PDC, Software de inventario y crecer en servicios según sus necesidades especificas.

Datos de Contacto

Edwind Richzendy Contreras Soto
Correo: Richzendy@gmail.com
Website: http://www.Richzendy.org