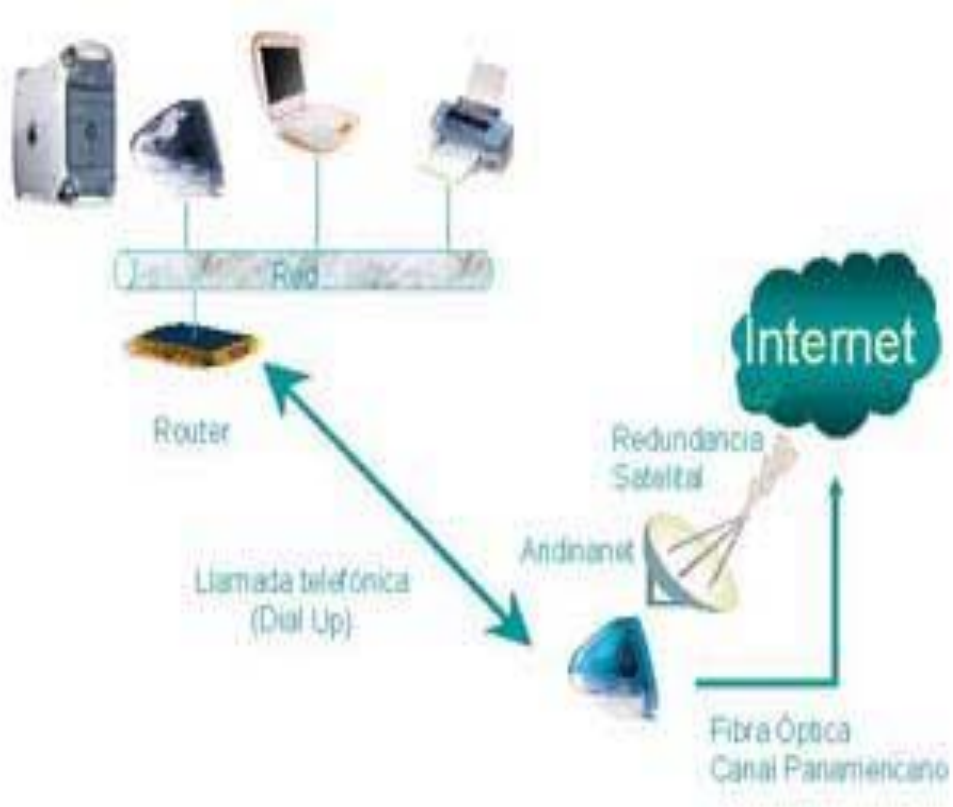
ESTUDIO DE SEGURIDAD EN LOS ENLACES DE BANDA ANCHA, APLICADA A LAS REDES PRIVADAS VIRTUALES

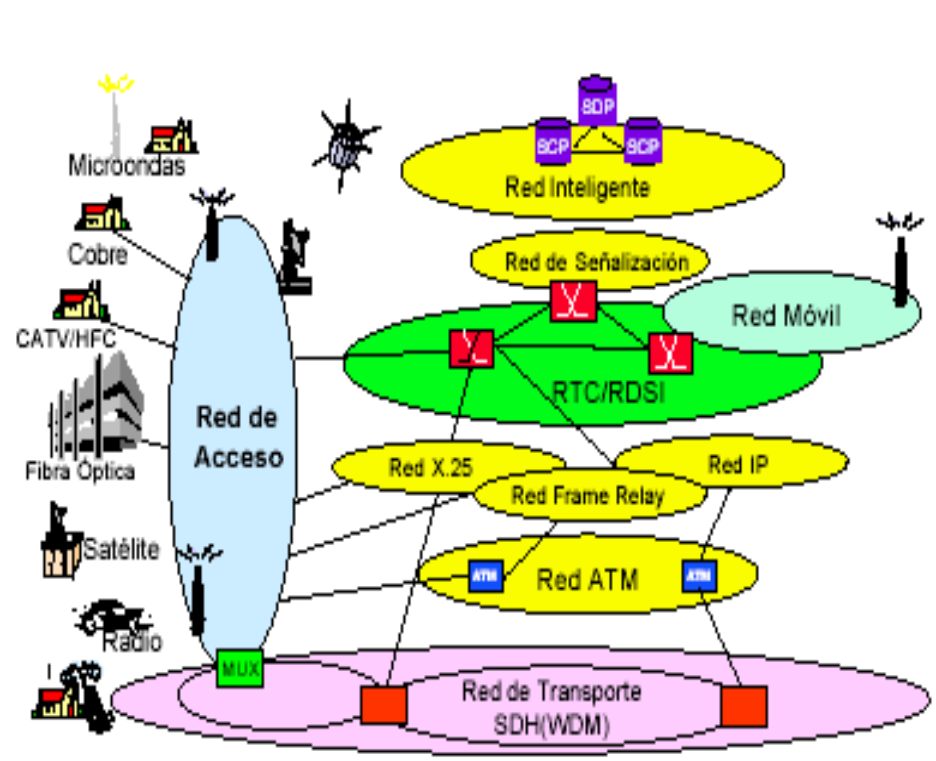
- TRANSMISIÓN EN BANDA ANCHA
- EQUIPOS Y PROCEDIMIENTOS UTILIZADOS EN LA SEGURIDAD DE REDES DE BANDA ANCHA
- FIREWALLS
- REDES PRIVADAS VIRTUALES (VPN)
- INVESTIGACION Y ESTUDIO DE UNA RED

TRANSMISIÓN EN BANDA ANCHA



- Las necesidades han incrementado las demandas de acceso de banda ancha.
- Facilita el flujo de multimedia, voz, datos imágenes con calidad.
- La banda ancha ofrece velocidades iguales o superiores a 2 Mbit/s

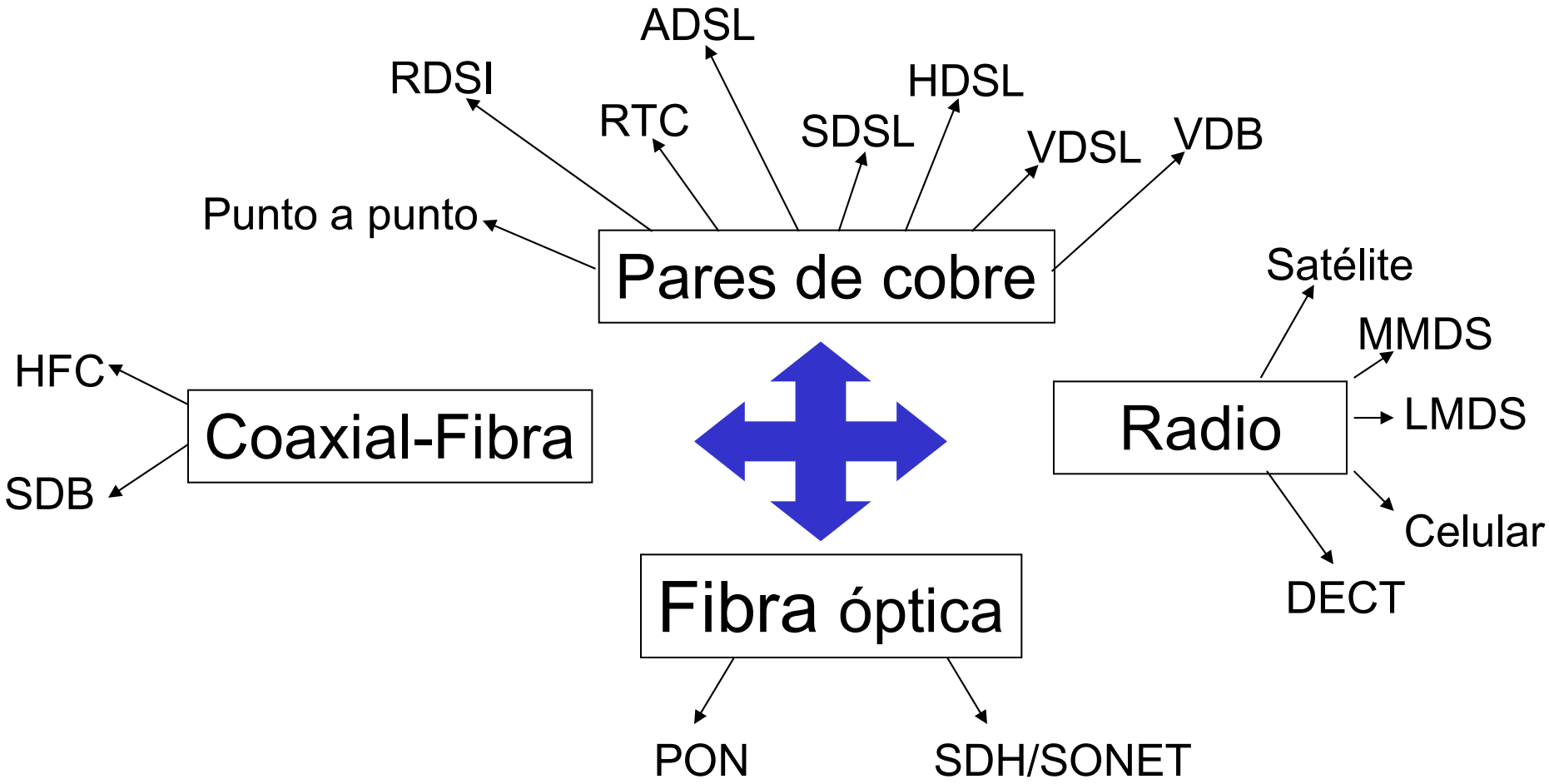
TRANSMISIÓN EN BANDA ANCHA



- La RDSI de Banda Ancha (ATM)
- Banda Estrecha vs. Banda Ancha
- Conexión de Banda Ancha
- Acceso y Redes de Banda Ancha

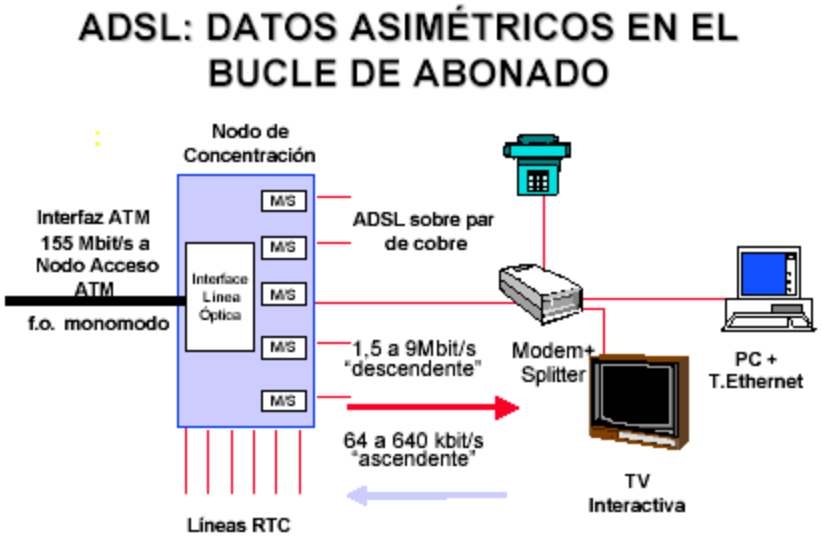
Clasificación de las Redes de Acceso

ALTERNATIVAS PARA ACCESO A INTERNET



TRANSMISIÓN EN BANDA ANCHA

Clasificación de las Redes de Acceso

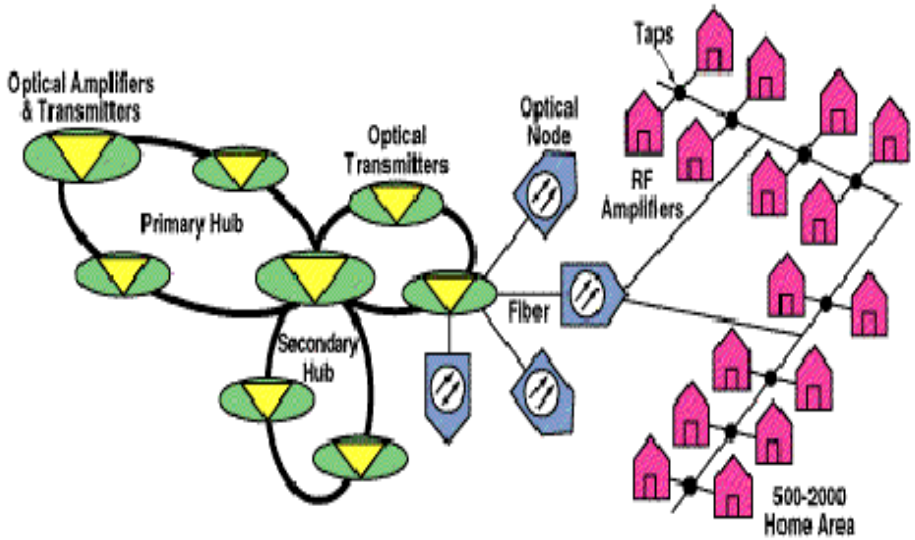


Acceso por pares de cobre

- a. Empleo de la RTC haciendo uso de módems (36.600 bit/s la real es 1 o 2 Kbit/s)
- b. Utilización de la RDSI: 64 Kbit/s. Se puede tener conexión al Internet y hablar por teléfono.
- c. Uso del bucle de abonado con tecnologías xDLS:

TRANSMISIÓN EN BANDA ANCHA

Clasificación de las Redes de Acceso

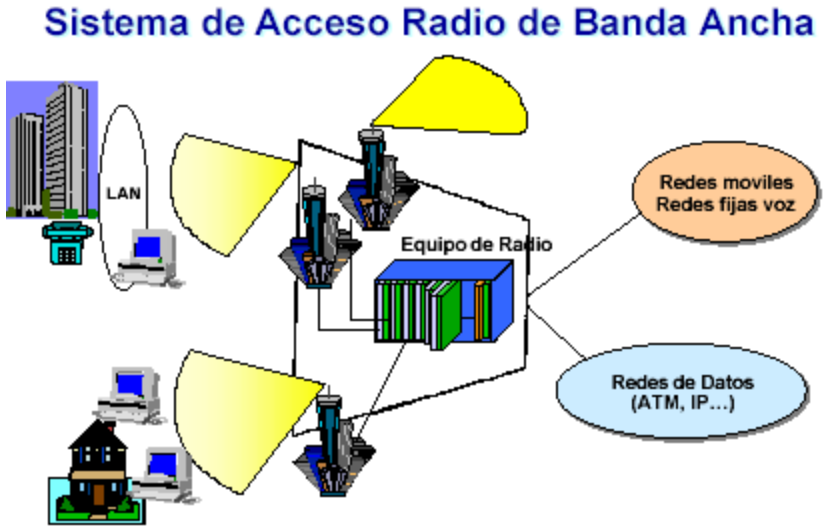


Acceso por fibra coaxial

- Unidireccional HFC. 30Mbit/s, utilizado para CATV. Mediante un módem se puede tx datos
- Bidireccional HFC. Se puede tener acceso a internet, difusión de canales de video y del telefónico.
- SDB (Swithed Digital Broadband) descendente = 50 Mbit/s y ascendente = 1.5 Mbit/s.

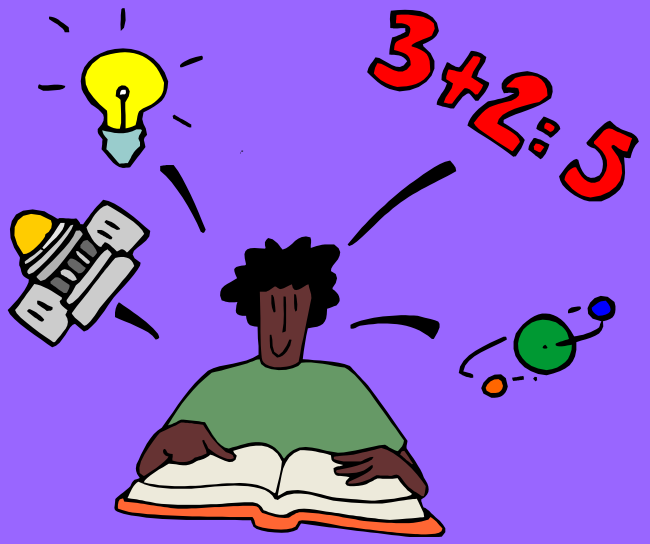
TRANSMISIÓN EN BANDA ANCHA

Clasificación de las Redes de Acceso



Acceso por radio

- Celular. Módem PCMCIA colocado en un PC portatil, 9.6 Kbit/s
- Difusión Terrestre. Microondas: MMDS (10 Mbit/s a 50 Km) y LDMS(menor distancia, máximo 5 Km.)
- Difusión por satélite. Sist. VSAT, 1Mbit/s



EQUIPOS Y PROCEDIMIENTOS UTILIZADOS EN LA SEGURIDAD DE REDES DE BANDA ANCHA

- La llegada de nuevas tecnologías, (RDSI, XDSL,etc. Han hecho que la seguridad sea un tema de preocupación.
- La gran desventaja de la conexión por banda ancha es la dirección IP fija.
- Un hacker tomará en cuenta los los sistemas con debilidades en la seguridad

Herramientas de Seguridad

Firewalls

- Es posible realizar ataques a través de los servicios habilitados.
- Requieren constante análisis de los logs
- Requieren trabajo especializado

IDS

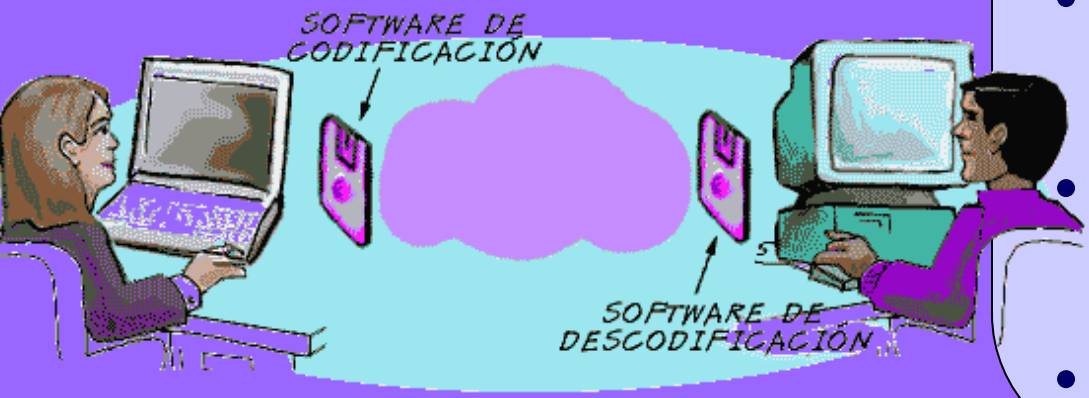
- Necesita constante análisis de logs
- Gran cantidad de falsos positivos
- Requiere trabajo especializado analizar los logs y mantener el ambiente

Configuración Segura

- Los errores de configuración son comunes
- Es difícil crear estandares de configuración y garantizar su aplicación
- Los estandares se olvidan durante el manteniemiento.

EQUIPOS Y PROCEDIMIENTOS UTILIZADOS EN LA SEGURIDAD DE REDES DE BANDA ANCHA.

Construir un plan de seguridad.

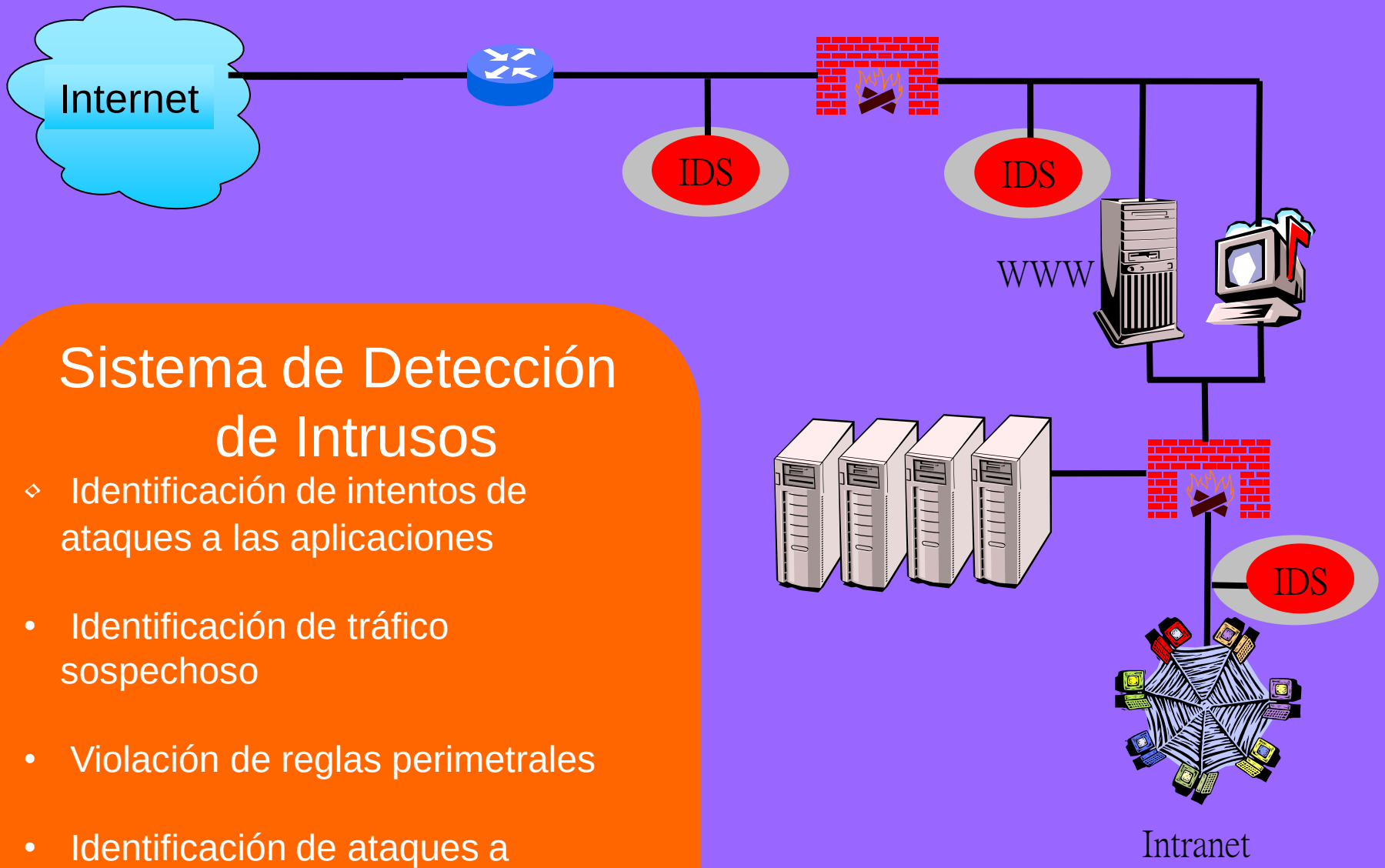


- Adaptar los métodos conocidos a las nuevas necesidades.
- Controlar el acceso de archivos.
- Establecer prioridades.
- Hacer una auditoria del sistema.
- Uso efectivo de la enciptación.
- Mantener sencillo el sistema

EQUIPOS Y PROCEDIMIENTOS UTILIZADOS EN LA SEGURIDAD DE REDES DE BANDA ANCHA.

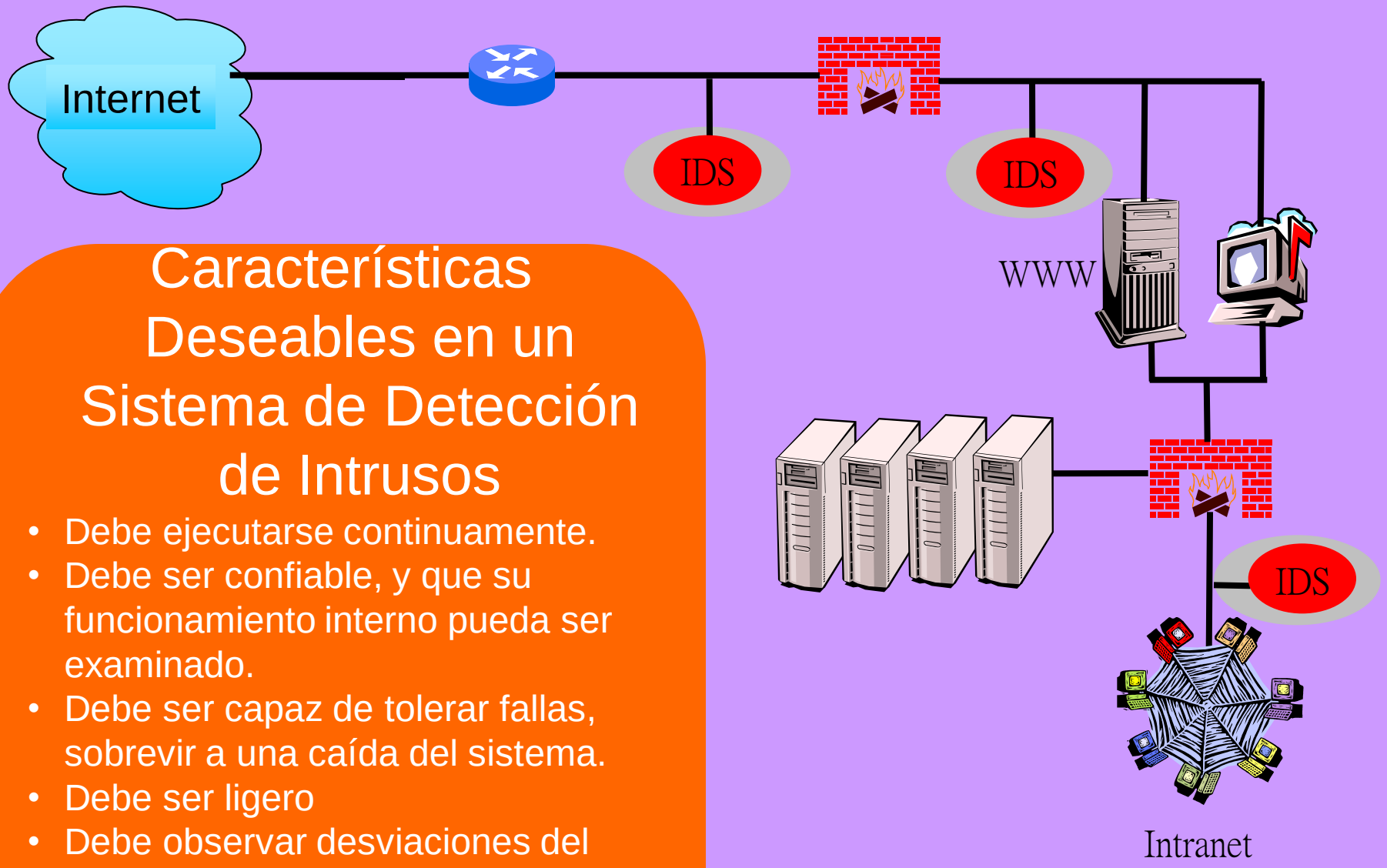
Funciones de seguridad importantes en las vpns.

- Identificación y autenticación.
- Control de acceso.
- Responsabilidad
- Rastros de auditoria
- Reutilización de los objetos.
- Presición
- Confiable
- Intercambio de datos a traves de canales de comunicación seguros



Sistema de Detección de Intrusos

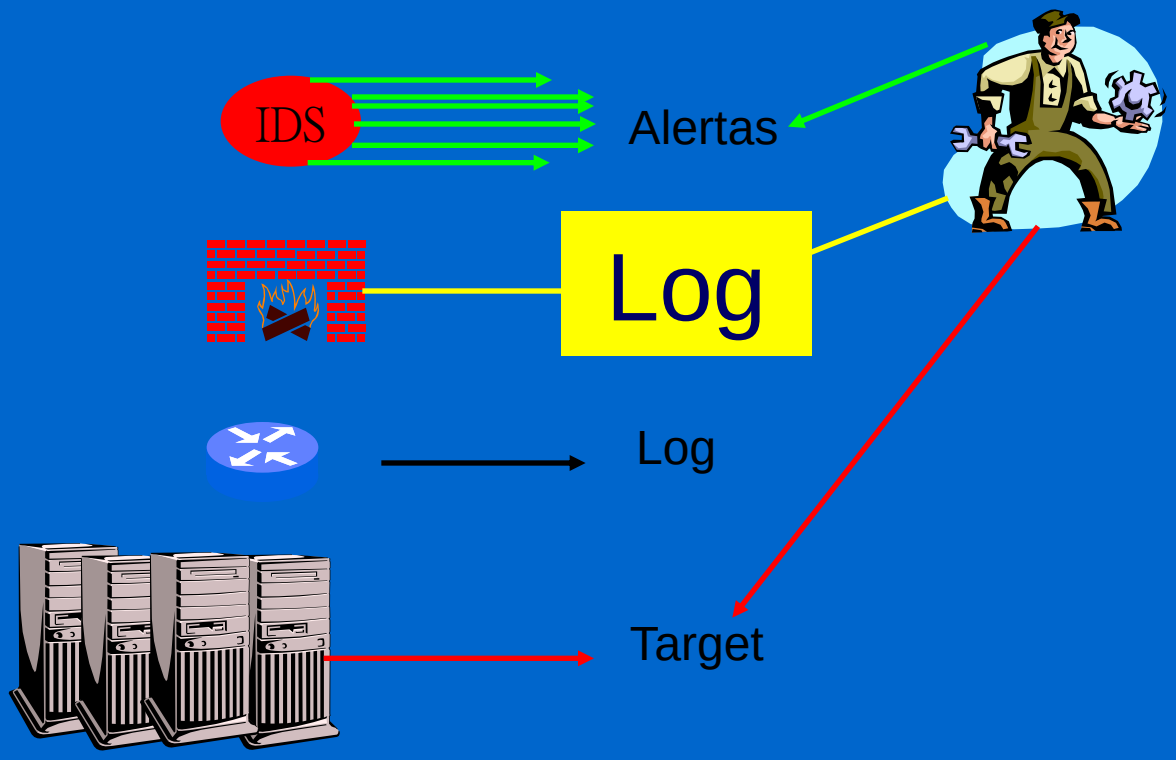
- Identificación de intentos de ataques a las aplicaciones
- Identificación de tráfico sospechoso
- Violación de reglas perimetrales
- Identificación de ataques a sistemas básicos



Características Deseables en un Sistema de Detección de Intrusos

- Debe ejecutarse continuamente.
- Debe ser confiable, y que su funcionamiento interno pueda ser examinado.
- Debe ser capaz de tolerar fallas, sobrevir a una caída del sistema.
- Debe ser ligero
- Debe observar desviaciones del comportamiento estándar.
- Debe adaptarse al comportamiento cambiante del sistema.

Detección tradicional de un incidente



Recepción de la alerta
Análisis
Filtrado de información relevante

Verificación de firmas de ataques adicionales

Muchas veces ignorado

Verificación del ataque e intento de resolución

Existen gran cantidad de falsos positivos

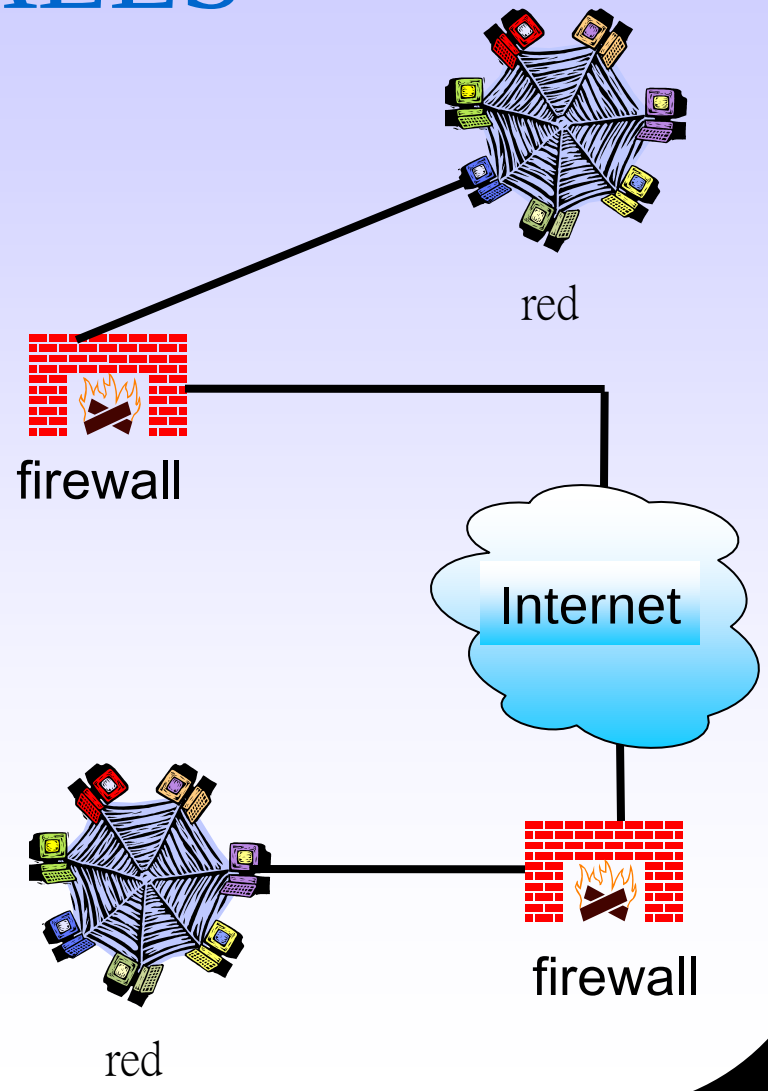
Los logs se vuelven extensos y complejos, haciendo que su análisis sea más lento

En ambientes complejos el análisis se hace mas difícil

Acciones Reactivas
Altos costos
Baja productividad

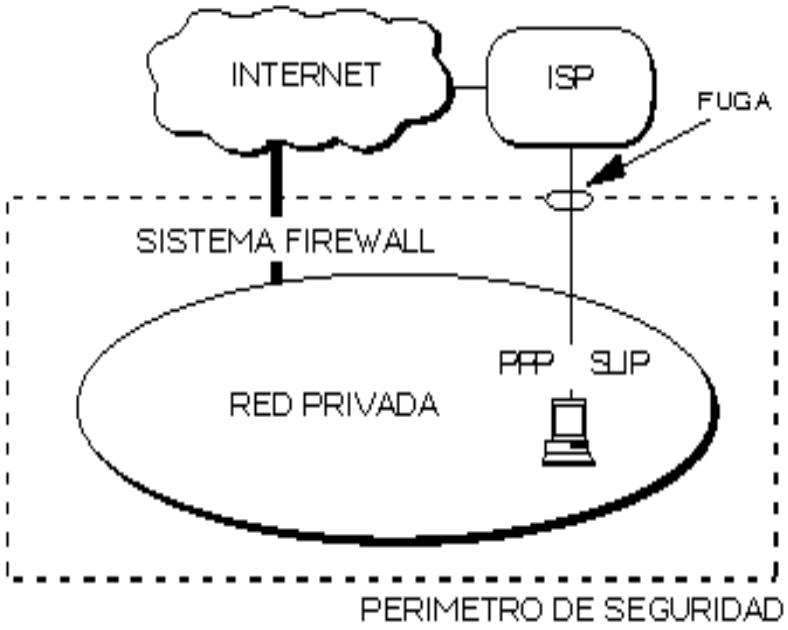
FIREWALLS

- La seguridad ha sido el principal tema en cuanto una empresa desea conectar su red privada al Internet.
- En cuanto la red privada esté dentro del Internet, expone sus datos a los hackers.

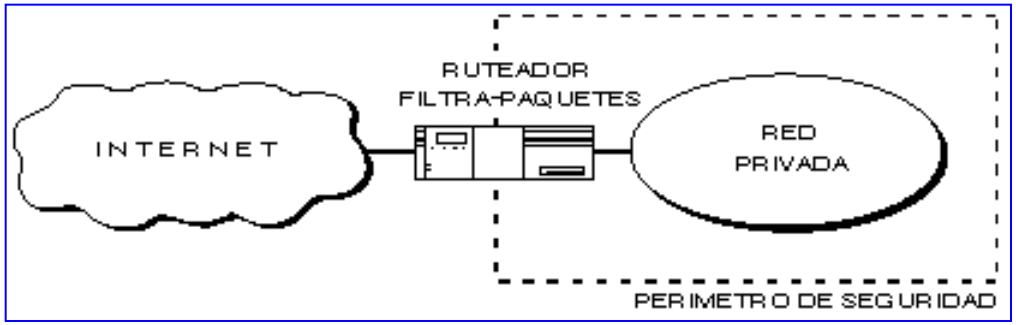


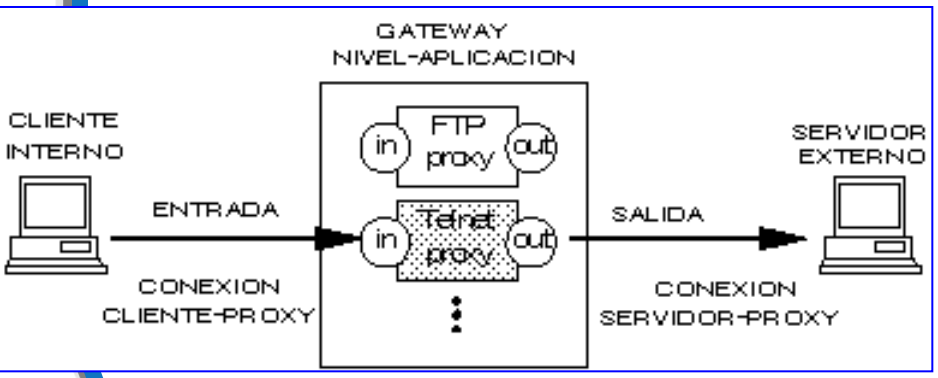
Firewalls y seguridad en Internet

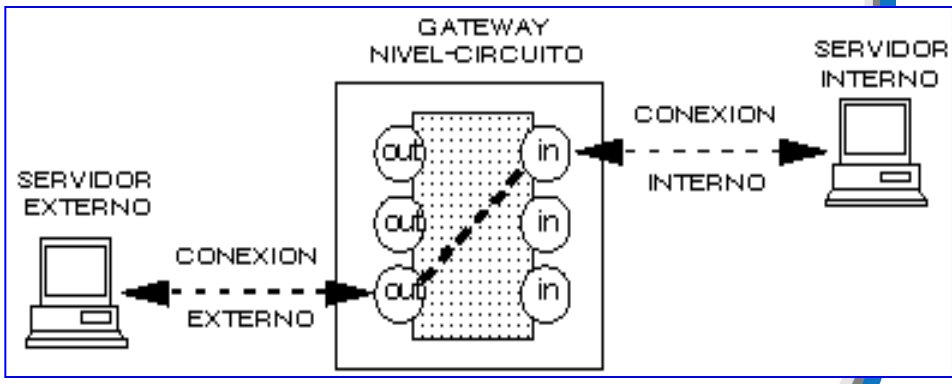
- Beneficios de un firewall en Internet.
- Limitaciones de un Firewall
- Polítcas del firewall
- Políticas internas de Seguridad.
- Costo del firewall



Componentes del sist. Firewall

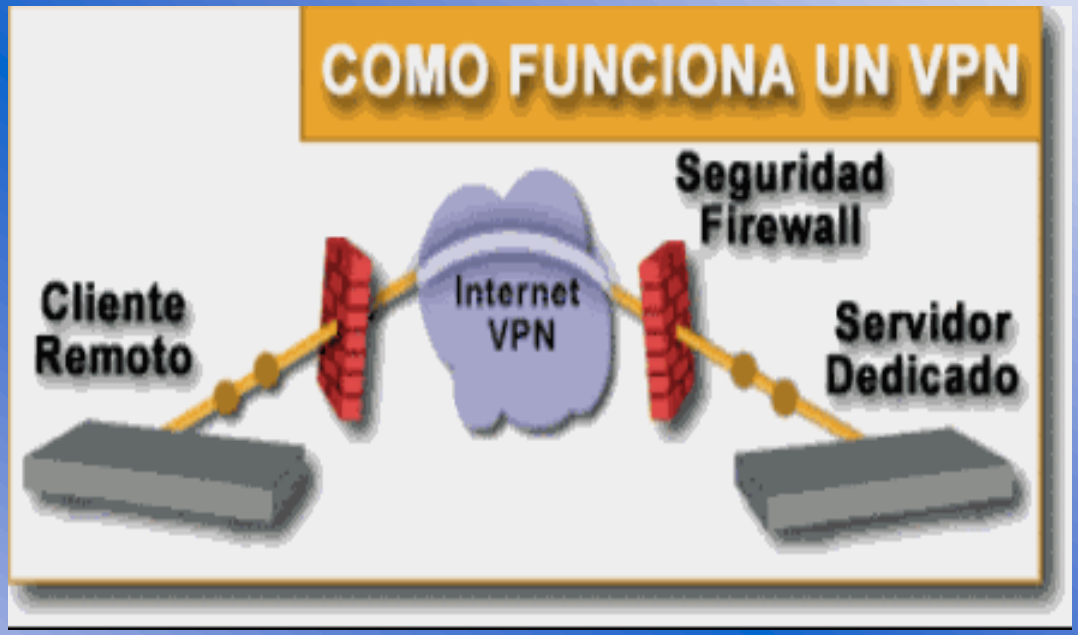




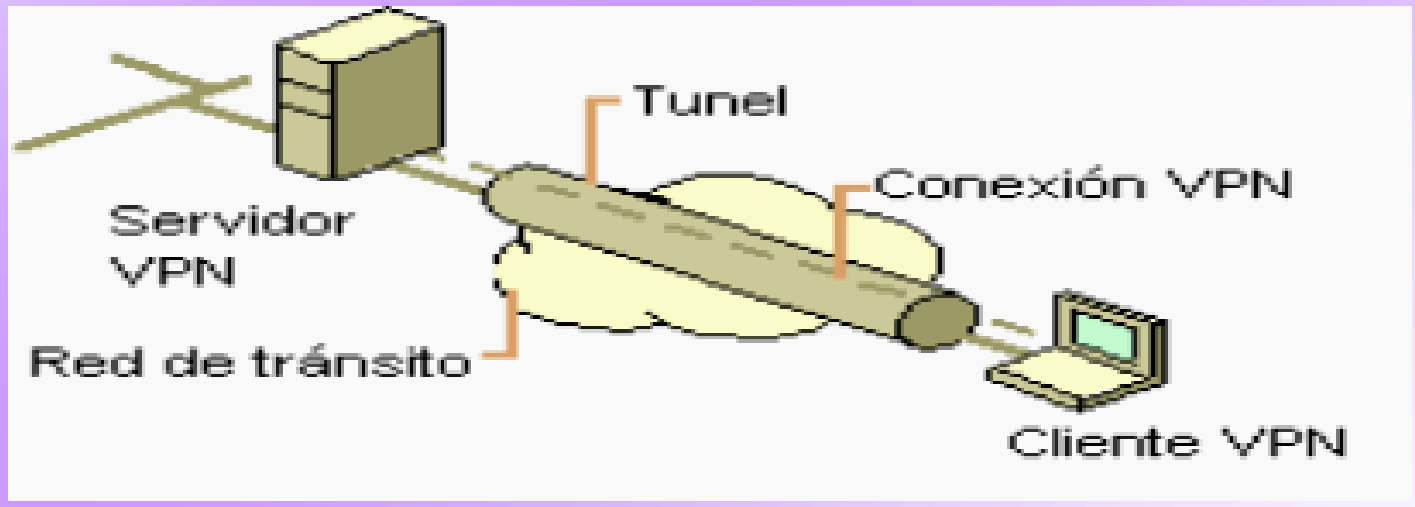


REDES PRIVADAS VIRTUALES

- Las redes se han convertido en un factor vital para cualquier empresa.
- Constituyen una gran ventaja, especialmente cuanto se tienen oficinas remotas y se transmite información confidencial.



- Internet, Intranet y Extranet
- Por qué una VPN?: módem; Línea Privada o Vpn.
- Principio de las Vpns
- Tecnología de túnel

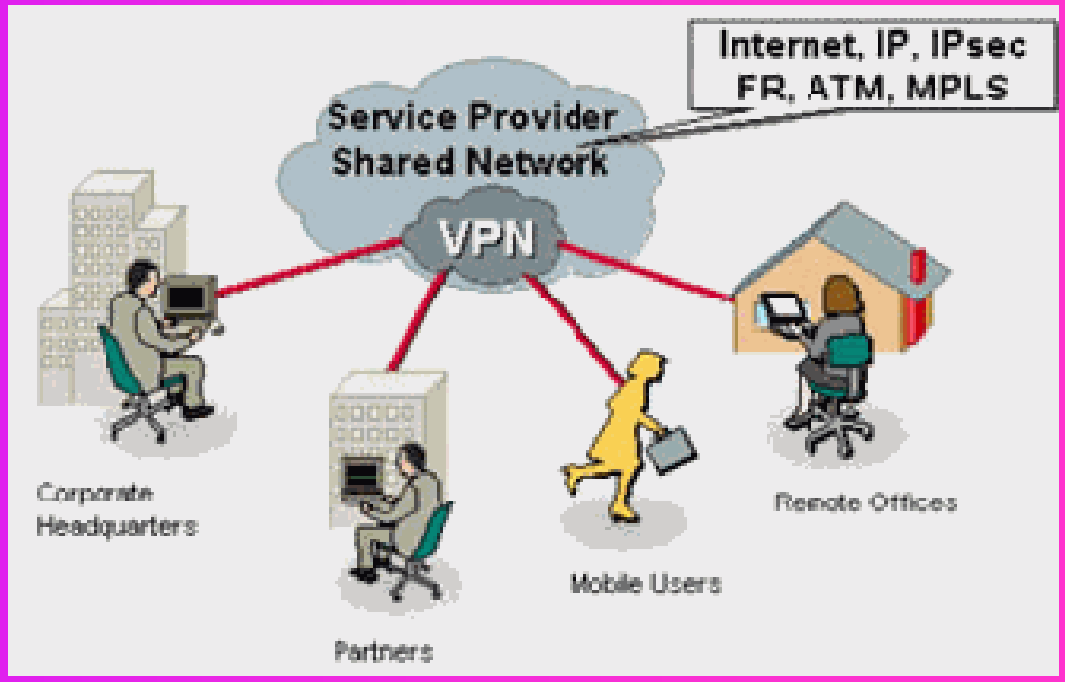


Requerimientos básicos de una VPN.

- Identificación del usuario
- Administración de direcciones
- Codificación de datos
- Administración de claves
- Soporte a protocolos múltiples

Herramientas de una VPN

- VPN gateway
- Software
- Firewall
- Router



Por qué la tecnología Web es tan atractiva

- Acceso inmediato a la información
- Libertad de elección
- Seguridad
- Facilidad de uso
- Costo de instalación moderado
- Costo de impresión y procesamiento más bajos
- Flujo de trabajo más simplificado
- Costos de capacitación más bajos
- Mejor dinámica de grupo

Aplicaciones de una VPN

- Procesamiento de pedidos
- Proyectos conjuntos
- Comunicación sin distorsión
- Servicio y soporte al cliente
- Correo electrónico
- Acceso total

HACKERS

- ✓ Las incursiones de los piratas informáticos ocacionan grandes pérdidas.
- ✓ Hay diferencia entre hackers y crackers?
- ✓ Cuál es el significado de los términos: hacker, phreaker y pirata?

Métodos y herramientas de ataque.

- Eavesdropping y Packet Sniffing: interceptación pasiva (sin modificación), colocan sniffer para capturar passwords, etc.
- Snooping y Downloading: el mismo que el anterior pero además de interceptar el tráfico realiza downloading de información.
- Trampering o Data Diddling: modificación desautorizada de datos, con motivo de fraude.
- Spoofing: usada para actuar en nombre de otros usuarios, como el envío de falsos mails

Métodos y herramientas de ataque.

- Jamming o Flooding: Desactiva o saturan los recursos del sistema. Consumir el espacio disco.
- Caballos de Troya: introducir un programa con una rutina no autorizada y cuando se lo ejecuta acctua en forma diferente (formatear el disco)
- Bombas Lógicas: introducir un programa con una rutina que en una fecha determinada provocará el cuelgue del sistema.
- Ingenieria Social: Convencer a la gente de que haga lo que en realidad no debería (llamar al usuario haciendose pasar por el administrador)

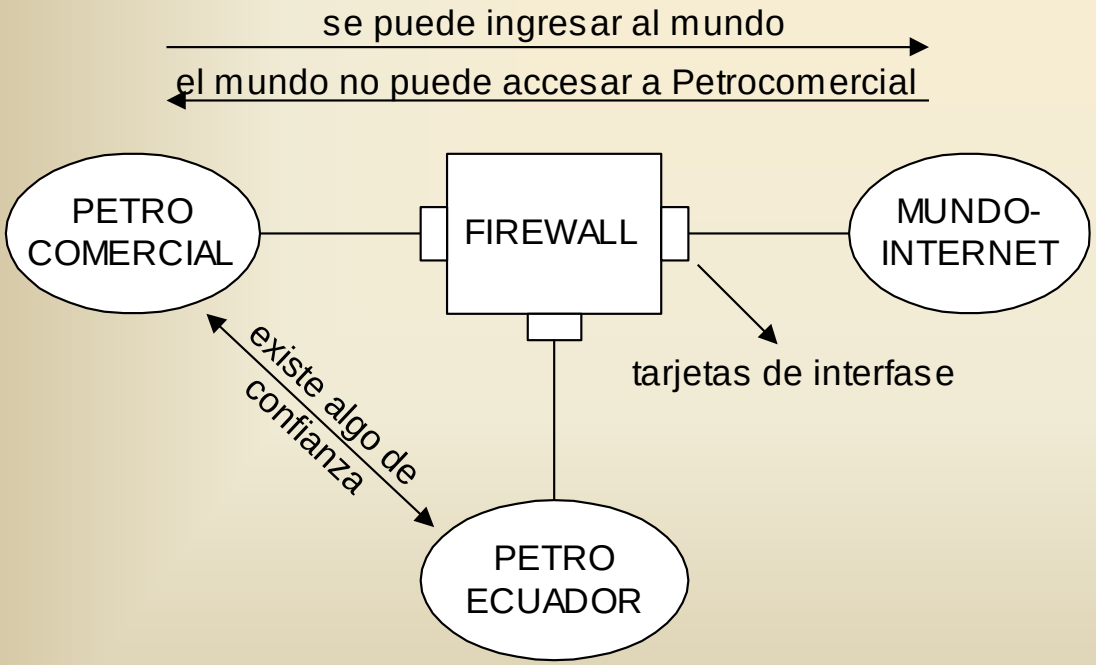
Métodos y herramientas de ataque.

- Difusión de Virus: difiere del trampering porque puede ser ingresado por dispositivos externos (disquets) o a travez de la red.(mails)
- Explotación de Errores de Diseño, Implementación u Operación: muchos sist. estan expuestos a agujeros que son usados para obtener privilegios, acceder a archivos o realizar sabotaje
- Obtención de passwords, códigos o claves: usualmente llamado cracking, se realiza con la ayuda de programas especiales y diccionarios
- Ping mortal: un paquete ping ilicitamente enorme TCP/IP permite máximo 64Kbit/s

INVESTIGACION Y ESTUDIO DE UNA RED

- Red privada virtual de banda ancha
- Condiciones actuales
- Tecnología empleada: dispositivos y métodos
- Seguridad actual: física, lógica
- Necesidades
- Problemas de la falta de seguridad

INVESTIGACION Y ESTUDIO DE UNA RED



- Alternativas
- Ventajas
- Desventajas
- Inversión de un sistema de protección y seguridad
- Beneficio
- Justificación de la inversión

CONCLUSIONES Y RECOMENDACIONES

- Recomendaciones sobre la seguridad
- Aspectos básicos
- Mejoras específicas
- Análisis costo/inversión
- Costo del hardware
- Costo del software
- Recomendaciones