

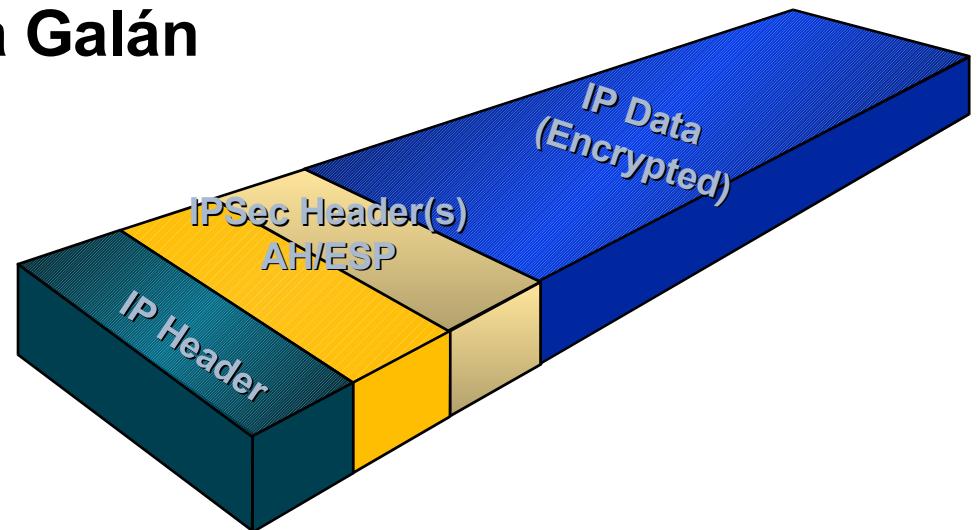


FIST Conference February 2004 @



# Introduction to Corporate Security in Communications

© Rafael Neila Galán





# **Introduction to Corporate Security in Communications**

**FIST Conference February 2004**

**© Rafael Neila Galán**

**Madrid, 21 February 2004**





# Indice

**La Seguridad como Política Global**

**Riesgos y Amenazas**

**Mecanismos y Servicios**

**Seguridad en Frame Relay**

**Seguridad en RDSI**

**Seguridad en IP**

**Resumen de Funcionalidades**



# Entorno Legal

Desde el 25 de Junio de 1999 el Ministerio de Justicia a través de la publicación del **Real Decreto 994/1999**, de 11 de Junio en el BOE, aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, el cual tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.



# Seguridad como Política Global

## Fuentes de Ataque:

**50-60% Errores debido a inexperiencia, mal uso,...**

**15-20% Empleados disgustados, accidentes de mantenimiento.**

**10-15% Desastres naturales**

**3-5% Causas externas: Hackers**



# Seguridad como Política Global

## Medidas de Seguridad:

Tipos	Prot Física	Medidas Técnicas	Organización
Preventivas	PF	PT	PO
Detectivas	DF	DT	DO
Correctivas	CF	CT	CO

PF: Guardias de Entrada, Respaldo Datos

DF: Monitores, detectores,...

CF: Respaldo de fuente de poder

PT: Firewalls, criptografía, ...

DT: Control de Acceso lógico, autenticación

CT: Antivirus,...

PO: Cursos actualización, organización de claves,...

DO: Auditorías,...

CO: Respaldos automáticos, plan de incidencias (sanciones),...



# Riesgos y Amenazas

**Compromiso**

**Modificación**

**Suplantación**

**Repudio**

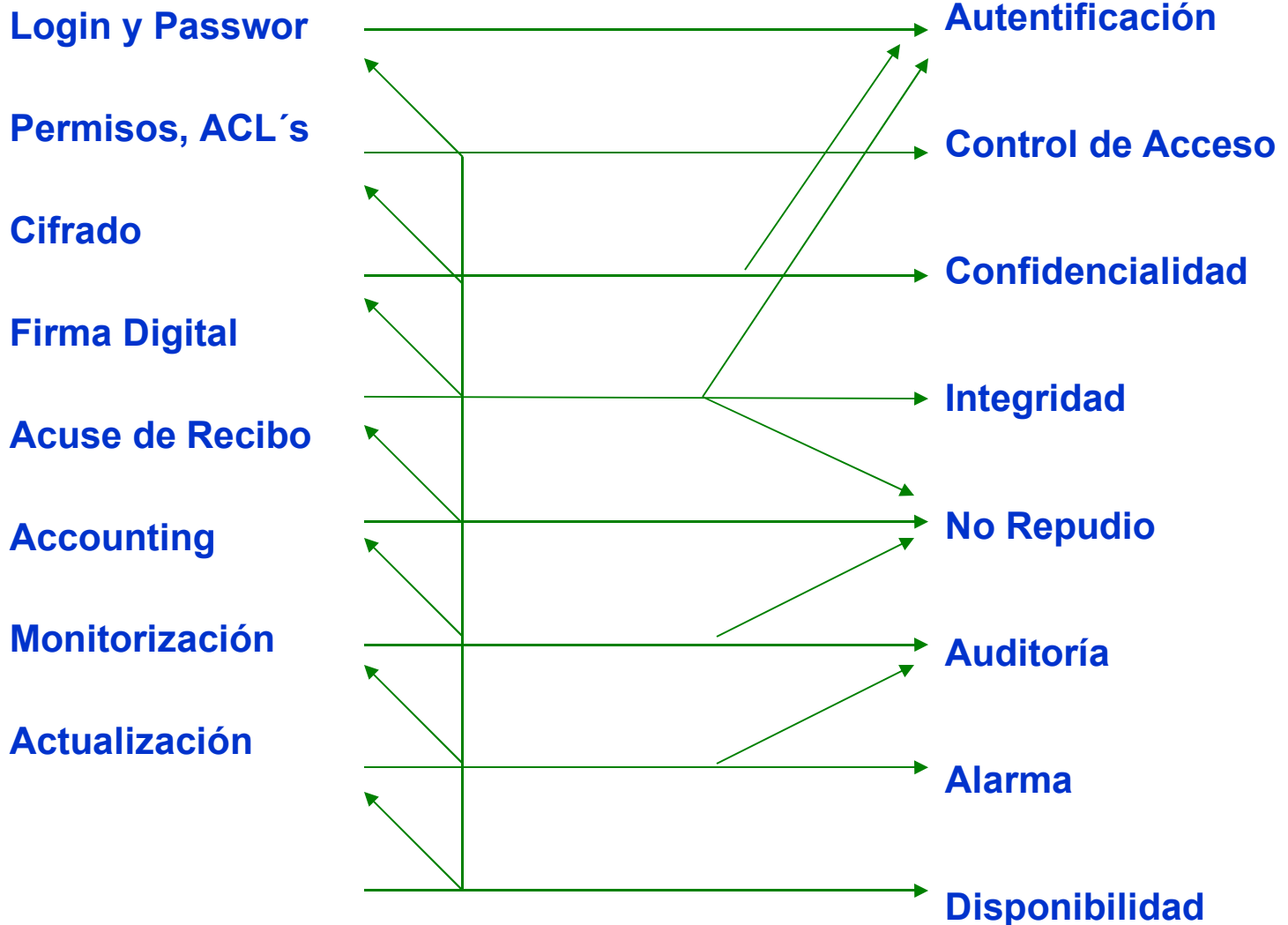
**Reenvío**

**Denegación de Servicio**

*✓ Todo está Relacionado*



# Mecanismos y Servicios





## **Seguridad en Nivel 2**



# Seguridad en Nivel 2. Frame Relay.

## Circuitos Virtuales Permanentes:

El administrador constituye las conexiones en tiempo de definición, no siendo posible el establecimiento de ningún canal CVP mientras no se satisfagan todas las condiciones de configuración.

## Link Integrity Verification (LIV):

El procedimiento requiere en el lado de usuario el intercambio de números de secuencia periódicamente en un intervalo de polling definido (T391), para que cada lado pueda determinar si la conexión adyacente está operativa.



# Seguridad en Nivel 2. RDSI

**Calling Line Identification (CLI).** Se examina el número llamante en cada llamada RDSI, comparándose con una lista de llamantes autorizados.

**Autenticación CHAP.** Sólo permite el establecimiento de la llamada tras una negociación de nombre de dispositivo y password. En este intercambio de información, el password viaja encriptado.

## Desde el router concentrador RDSI:

Se filtrarán todos los paquetes TCP dirigidos al *router* con puerto destino 23 (*well-known port* de Telnet)

Se filtrarán todos los paquetes TCP dirigidos al *router* con puertos origen por encima del puerto 1024 (rango de *well-known ports* de TCP).

Protocolo SNMP no estará activo en el router remoto con acceso RDSI



## **Seguridad en Nivel 3**



# Seguridad en Nivel 3. Objetivos

- **Seguridad de GCU (Grupo Cerrado de Usuarios).**

No accesibilidad a una red privada de cliente desde otra red privada de cliente.

- **Seguridad de red.**

Impedir el acceso a los routers de cliente desde cualquier punto distinto del Centro de Gestión.



# Seguridad en Nivel 3. Herramientas

**Filtros y Listas de Acceso**

**Firewalls**

**NAT**

**Túneles: GRE**

**Cifrado:**

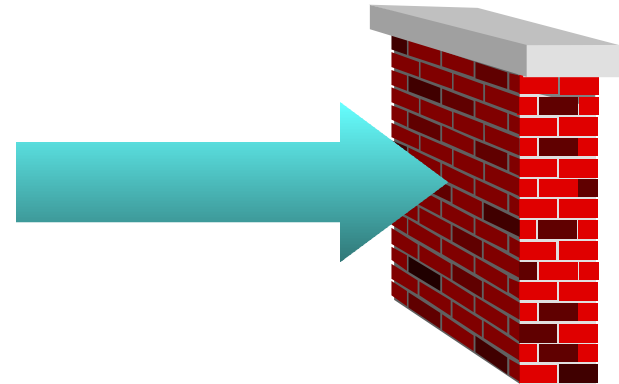
**Propietarios: CET (Cisco), Teldat**

**Estándar: IPSec**

**Claves:**

*Preconfiguradas*

*Mediante Autoridad de Certificación*





# Filtros y Listas de Acceso

**Se pueden establecer políticas en los equipos de acceso de nivel 3 con objetivo de:**

**Evitar la toma de control de los mismos a través de interfaces físicos o virtuales.**

**Evitar el acceso desde ciertas redes a otras redes de la propia corporación.**

**Se puede filtrar por dirección IP, puerto,...**



# Network Address Translation

**Utilización de direcciones de rango reservado para redes privadas, según RFC 1918.**

**Traducción de direcciones privadas a direcciones públicas en los puntos de acceso a redes públicas.**

**Traducción estática, dinámica, por dirección y/o por puerto.**



# Túneles

**Encapsular tráfico diferente a IP (IPX, SNA,...) a través de redes públicas IP.**

**Diferentes tipos de protocolos de tunelización (cifrando el campo de datos, sin cifrarlo).**

**Desventaja: Aumenta tamaño de paquete, incluso obligando a fragmentación del mismo, reduciendo eficiencia del acceso.**



# Criterios de Diseño

- ✓ **Colocación FW**
- ✓ **Colocación de Servidores de Túneles IPSec**
- ✓ **Colocación Radius**
- ✓ **Sondas**



# Colocación FW

**El FW es el elemento que debe proteger, o hacer de barrera, entre los elementos de la corporación y “el mundo exterior”.**

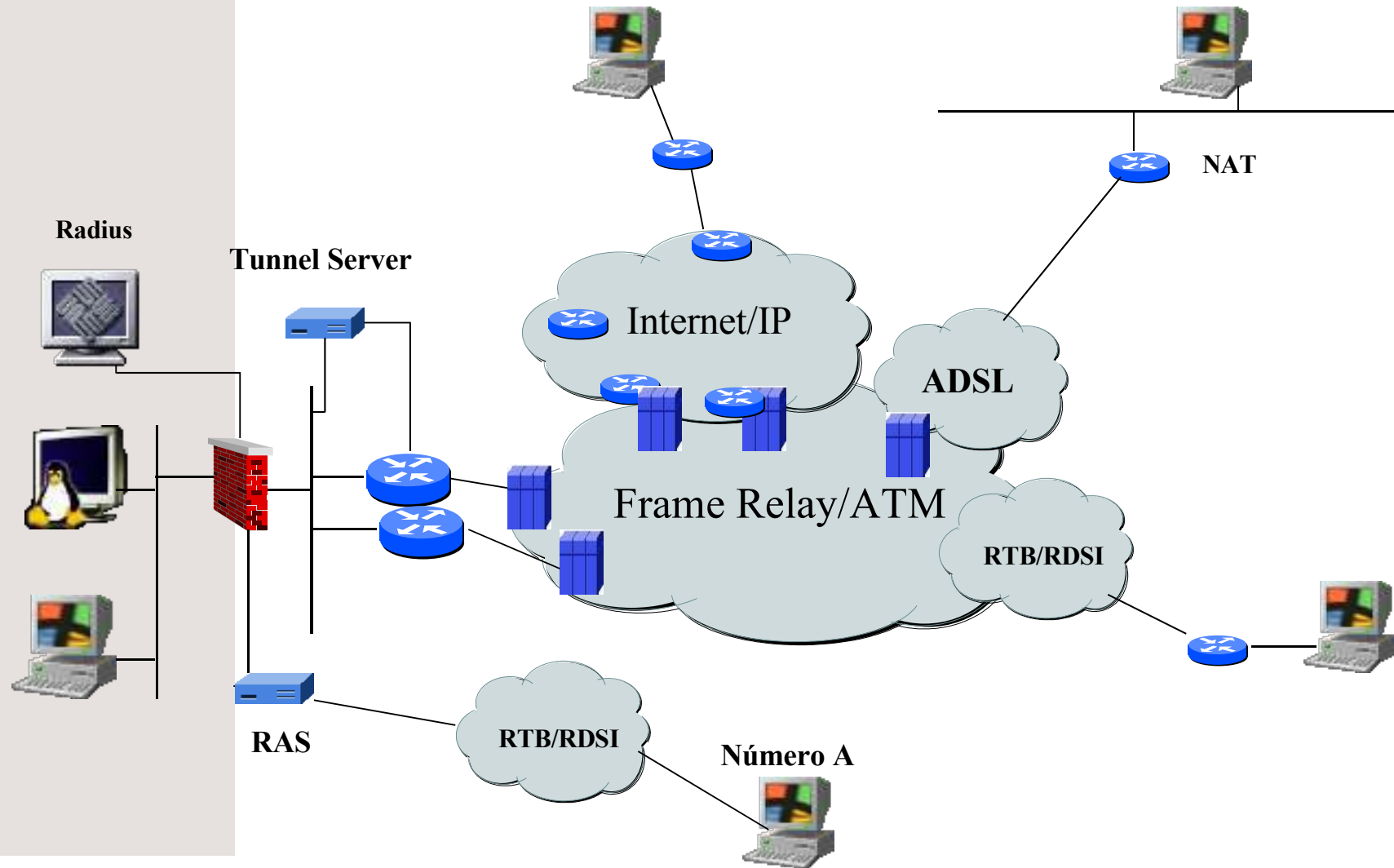
**¿Que elementos quiero hacer visibles a todos?**

**¿A qué elementos quiero que accedan mis partners?**

**¿Qué elementos son internos a mi corporación? ¿son críticos?**



# El FW, mi bastión.





# Colocación Tunnel Server (IPSec)

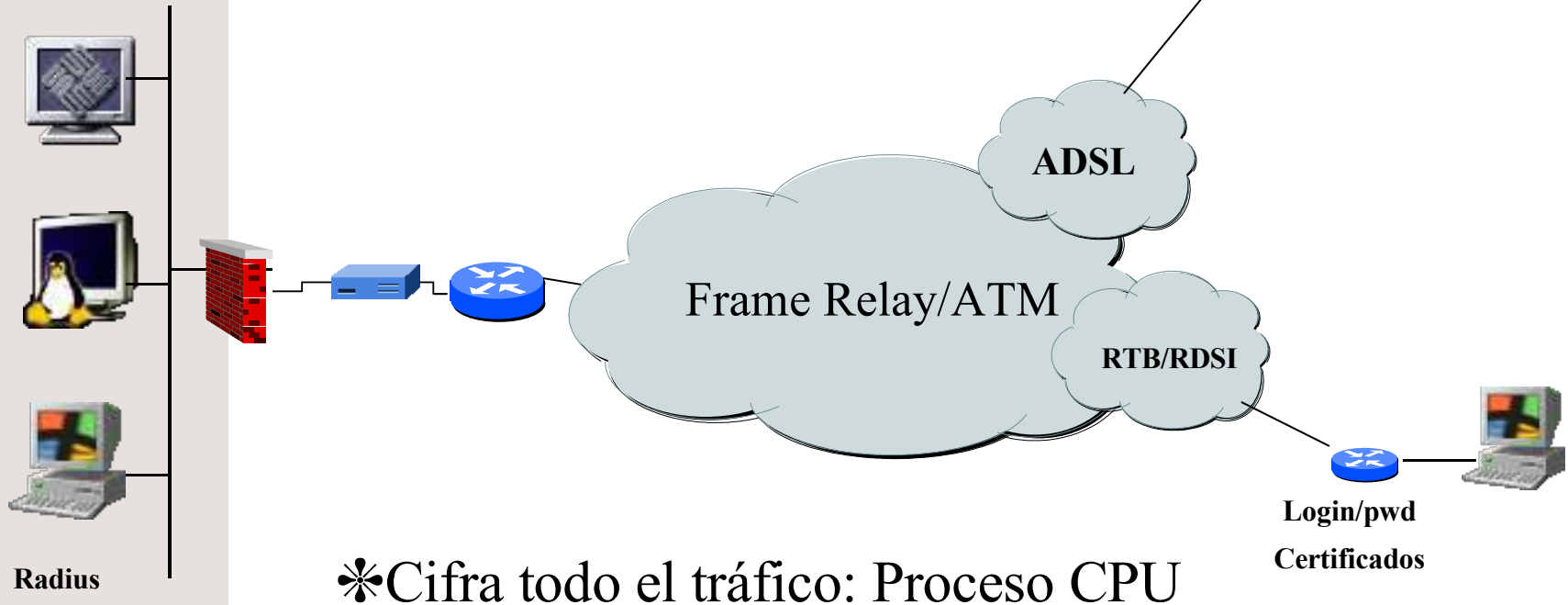
**ST entre router acceso y FW**

**ST en paralelo a DMZ**

**ST detrás del FW**

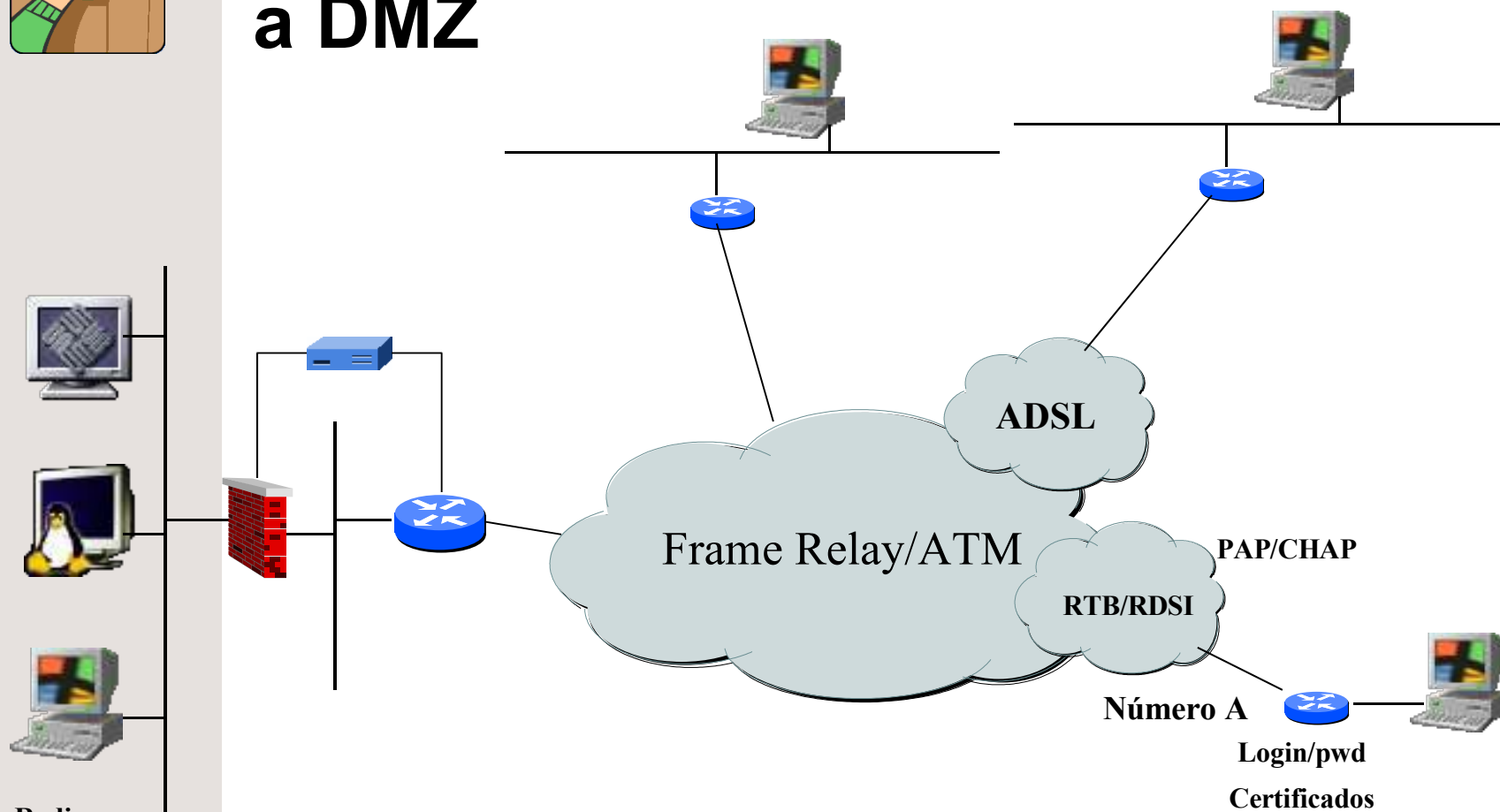


# IPSec: ST entre router acceso y FW





# IPSec: ST en paralelo a DMZ

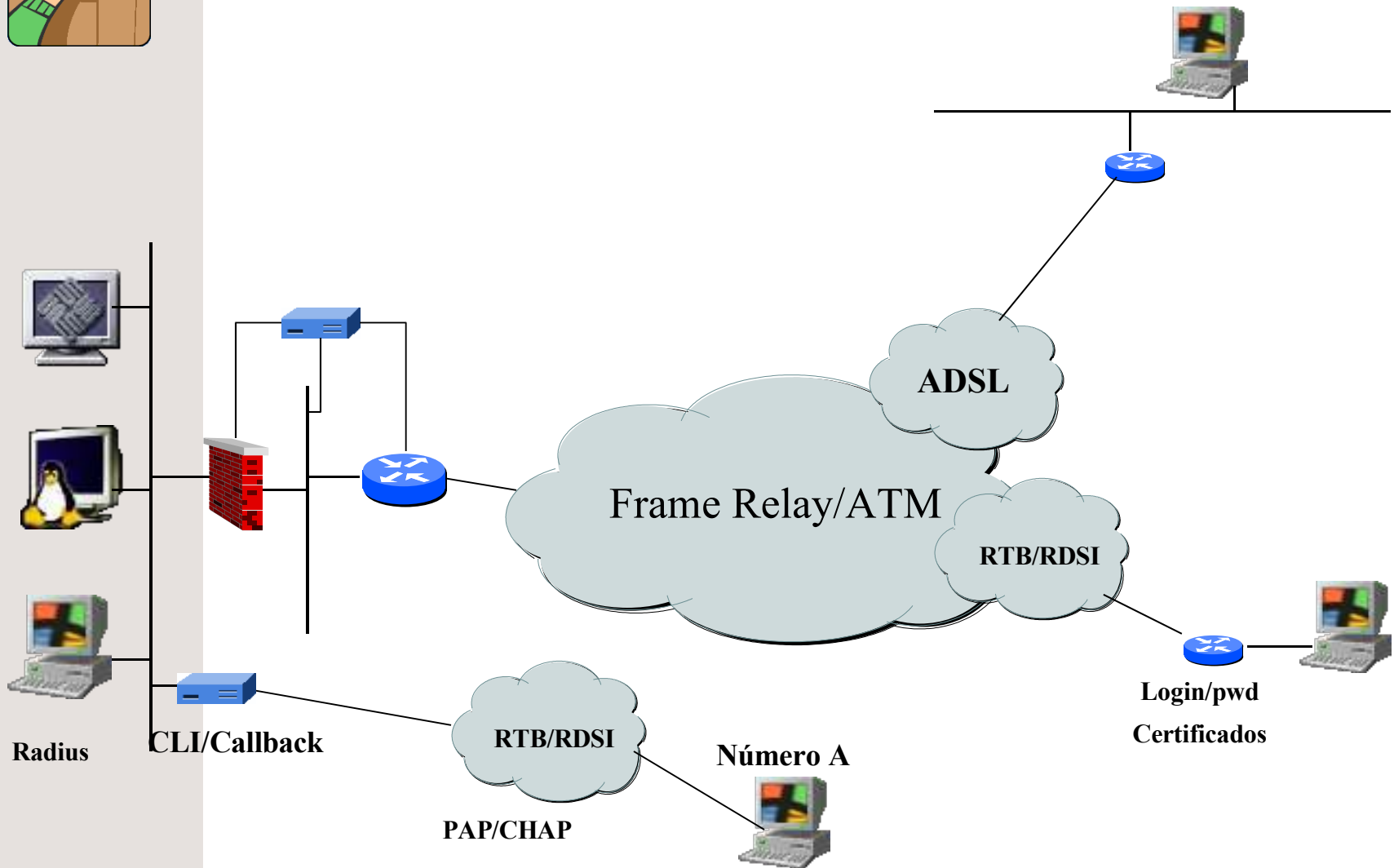


✓ ST paralela a la DMZ

\* Permite separar tráfico a cifrar corporativo y tráfico no corporativo



# IPSec: ST detrás del FW



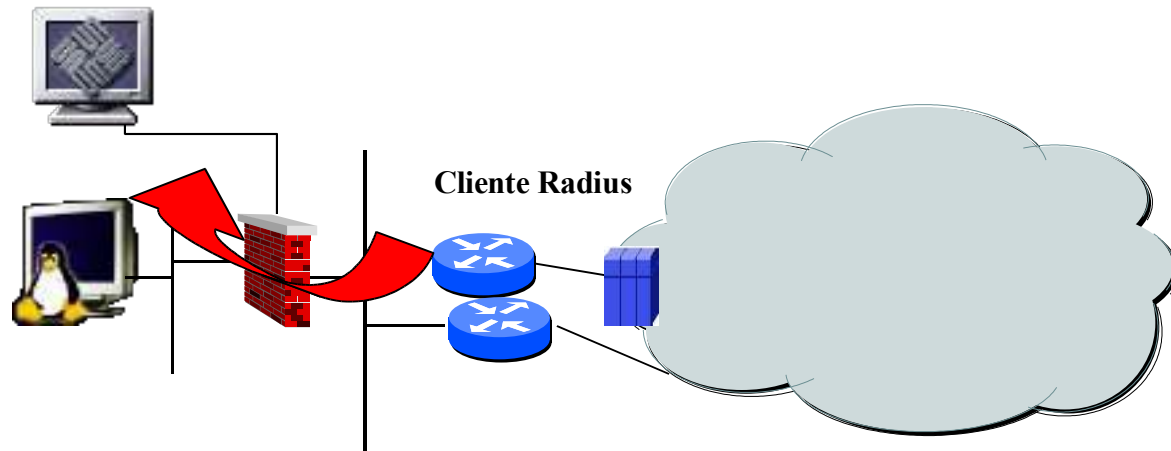


# Colocación del Radius

**El Radius Server tiene información importante de mi red: Se puede saber mi topología.**

**Protegerlo en segmento independiente, accesible sólo desde el cliente radius**

Radius Server





# Sondas

**Elementos de rastreo de patrones de tráfico, situados en los diferentes segmentos de la red a proteger.**

**Sirven para detectar, seguir y auditar accesos a los diferentes segmentos LAN.**



# Resumen de Funcionalidades

## Nivel 2:

**Autenticación.**

**Control de Acceso**

**Auditoría**

**Alarma**

**Disponibilidad**

## Nivel 3, añade:

**Confidencialidad:** Sólo leído por personas autorizadas.

**Integridad:** La información no es alterada en su trayecto

**No repudio:** No se puede negar autoría de un mensaje enviado.



**Gracias por Su Atención**