UNIVERSIDAD PONTIFICIA
ICAI ICADE
COMILLAS
MADRID

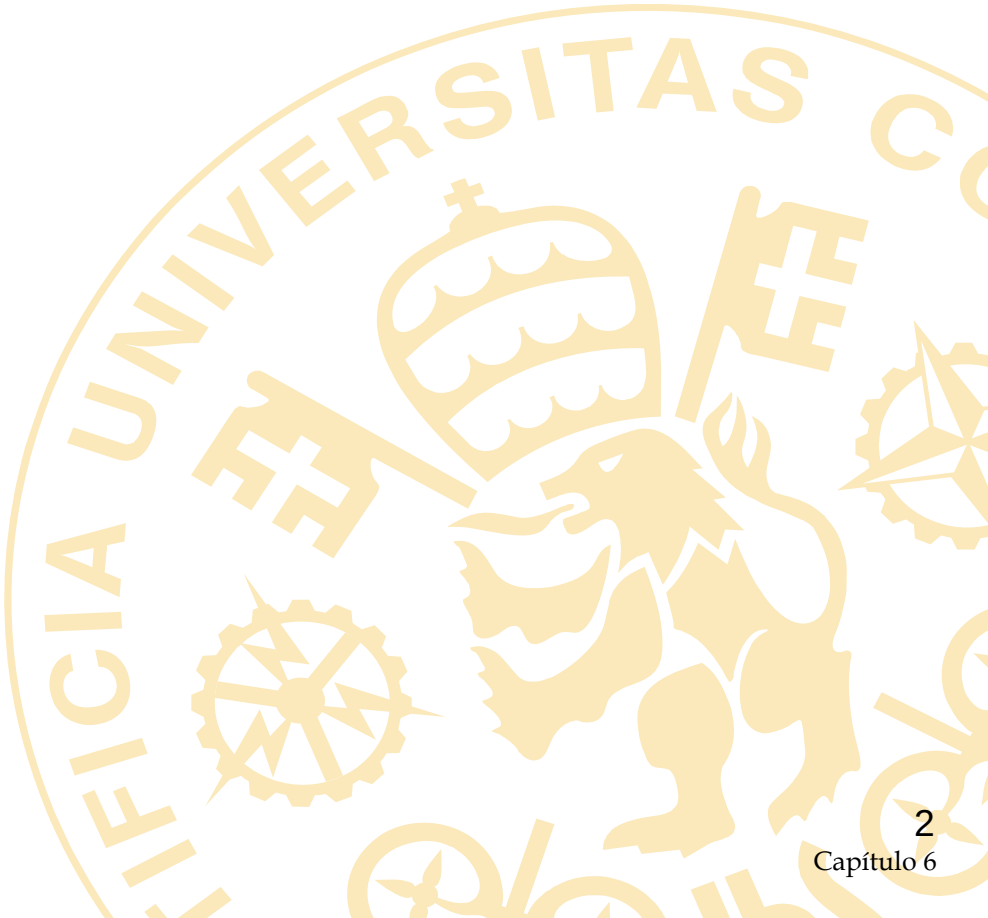
Seguridad Informática:

Capítulo 10: Seguridad Perimetral

Titulación: Ingeniero en Informática
Curso 5º - Cuatrimestral (2005-2006)

Javier Jarauta Sánchez
Rafael Palacios Hielscher
Jose María Sierra

Presentación



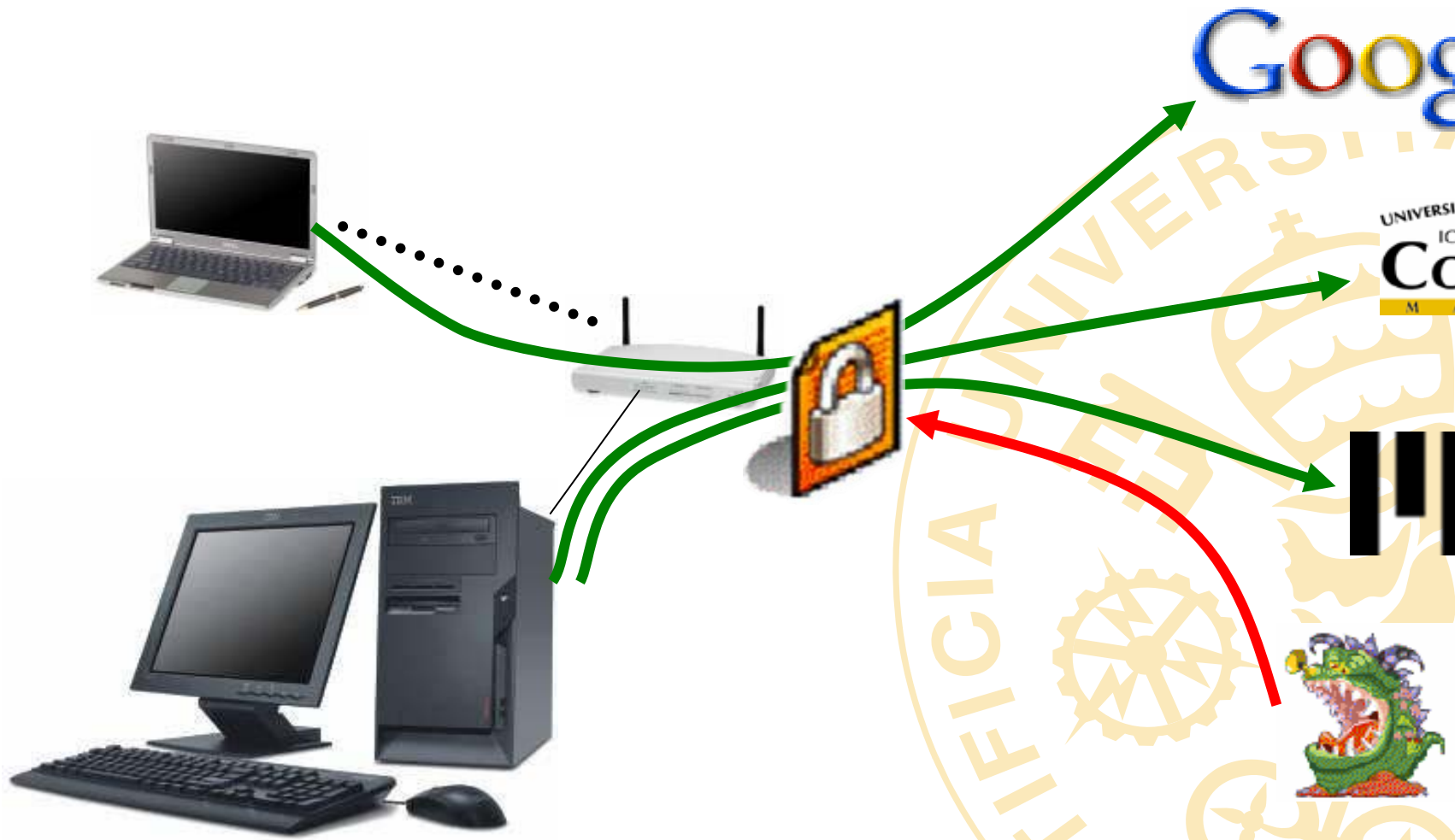
Capítulo 10: Seguridad Perimetral

- Cortafuegos (Firewall) y Proxy
- Redes Privadas Virtuales (VPN)
- IDS, IPS

Cortafuegos y Proxy

Funcionamiento general del Firewall

- Bloqueo de conexiones externas



Definiciones y conceptos básicos

- Cortafuegos o Firewall:
  - Sistema que implanta una política de control de accesos entre dos redes (p.e. Internet-LAN)
- Mecanismos que utiliza:
  - Bloquea o Permite él tráfico entre redes
  - Hay que tener muy claro lo que se quiere permitir o denegar
- ¿Por qué necesito un Firewall?
  - Permitir acceso a Internet de usuarios internos
  - Permitir acceso desde Internet a usuarios autorizados
  - Prohibir acceso desde Internet a los no autorizados

Contra qué protege un Cortafuegos

- Contra accesos no autenticados del exterior.
- Contra tráfico no autorizado del exterior
- Permitiendo salida desde el interior
- Proporciona un único punto para implantar una política de seguridad y auditoría.
- Ha de protegerse a si mismo

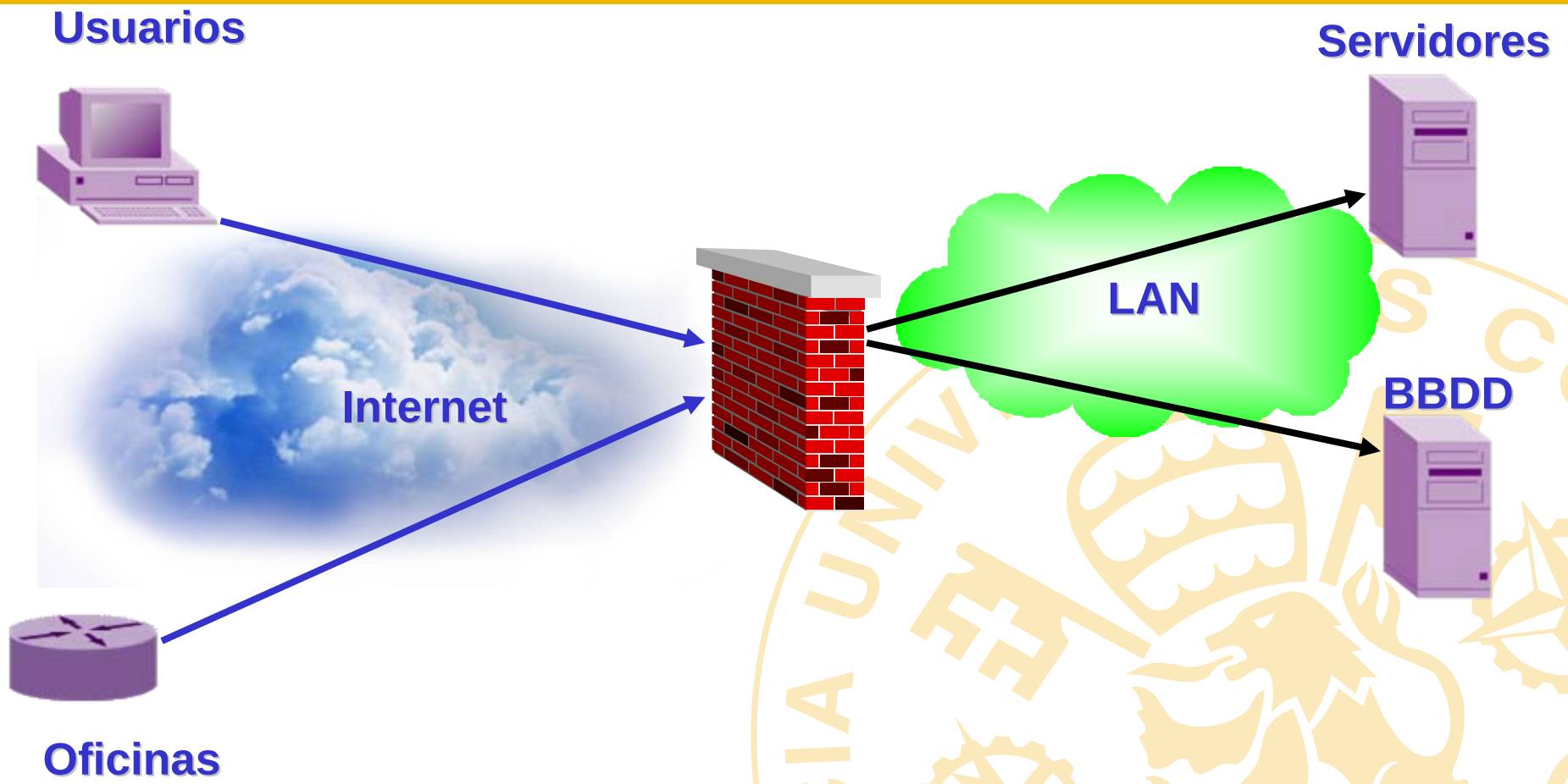
¡PUERTA BLINDADA!

Contra qué NO protege un Cortafuegos

- Contra accesos externos que no van por el cortafuegos (modems,...).
- Contra ataques desde el interior
- Contra virus, troyanos, túneles
- Contra salida de info por otro medio (disketes, etc.)
- Debe ser parte de una política global

¡NO VALE UNA PUERTA BLINDADA EN UNA CASA DE MADERA!

Arquitectura general - Cortafuegos corporativo



Tipos de cortafuegos

- Clasificación por tecnología:
  - Filtros de paquetes
  - Proxy de aplicación
  - Inspección de estados (statefull inspection)
  - Hibridos
- Clasificación por ubicación:
  - Cortafuegos personales (para PC)
  - Cortafuegos para pequeñas oficinas (SOHO)
  - Equipos hardware específicos (Appliances)
  - Cortafuegos corporativos

Tipos de Cortafuegos (1)

- Filtros de Paquetes (nivel de red):
  - Trabajan a nivel de red (IP)
  - Filtran paquetes IP según sus cabeceras y basados en los siguientes criterios:
    - Direcciones IP origen y destino
    - Puertos TCP/UDP origen y destino
  - Un router es un cortafuegos básico a nivel de red
  - Pueden utilizar filtros estáticos o dinámicos
  - PROS:
    - Independencia de las aplicaciones
    - Son muy rápidos y escalables
  - CONS:
    - Menor nivel de seguridad
    - No examinan el tráfico ni entienden el contexto

Tipos de Cortafuegos (2)

- Gateways de aplicación (nivel aplicación):
  - No permiten tráfico entre las dos redes, si no es mediante un proxy a nivel de aplicación.
  - Existe una conexión entre el exterior y el cortafuegos y otra entre el cortafuegos y el interior
  - Servidores proxy
  - PROS:
    - Alto nivel de seguridad
    - Examinan información a nivel de aplicación
    - Toman decisiones basadas en datos de cada aplicación
  - CONS:
    - Menor rendimiento y escalabilidad
    - Rompe el modelo cliente/servidor (requiere dos conexiones)
    - Requiere implantar un proxy por cada aplicación

Tipos de Cortafuegos (3)

- Inspección de estados (varios niveles)
  - Realizan filtros en base a las cabeceras, el paquete se intercepta a nivel de red, pero extrae información de los datos para analizar en función de la aplicación.
  - Mantiene una tabla dinámica de estados con información para las decisiones de seguridad
  - No rompe el modelo cliente/servidor
  - PROS:
    - Alta seguridad, velocidad y escalabilidad
    - Inspecciona los datos a nivel aplicación
  - CONS:
    - No se rompe la conexión totalmente

Tipos de Cortafuegos (4)

- Cortafuegos híbridos
  - La mayoría de los productos comerciales actuales
  - Incorporan mezcla de varias tecnologías
  - Pueden definirse reglas de filtros para tráfico que requiere alta velocidad, y proxy para alta seguridad
  - Adaptativos (proxy durante el establecimiento y filtro de paquetes durante la transferencia de datos)

Tipos de cortafuegos por ubicación

- Cortafuegos personales (PC):
  - Novedad en el mercado. Protegen el PC controlando el stack IP e inspeccionando las aplicaciones más comunes
  - Permiten filtros de entrada y salida.
  - Utilizables en PC en LAN, Modem, ADSL...
- Cortafuegos para pequeñas oficinas:
  - Small Office Home Office (SOHO)
  - Protegen a varios usuarios en pequeñas oficinas (típicamente entre 2 y 50)
  - Suelen ser pequeños equipos instalados antes del router, o incluso integrados
  - Muy utilizable para el acceso con ADSL

Tipos de cortafuegos por ubicación

- Equipos hardware (Appliances):
  - Utilizados en oficinas medias y sucursales
  - Fáciles de configurar, con funcionalidades básicas y gestionados centralizadamente
  - Utilizan sistemas operativos propios del hardware en el que están implantados
- Cortafuegos corporativos:
  - El punto central de accesos a Internet de una empresa.
  - Punto central donde se implanta la política de seguridad de la empresa
  - Puede conectar múltiples redes
  - Software que se instala en grandes servidores con configuraciones tolerantes a fallos

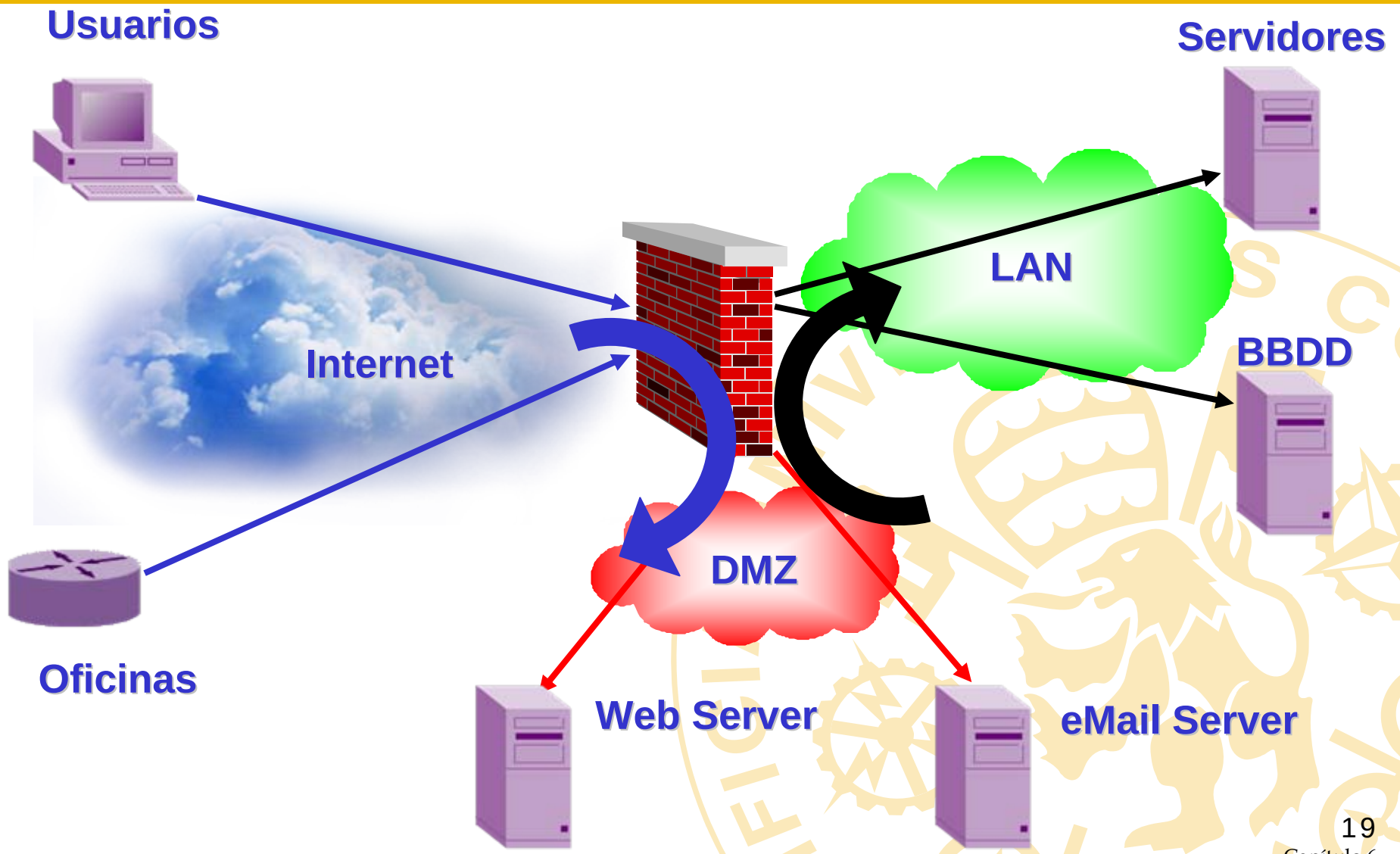
Arquitecturas de cortafuegos

- Arquitectura hardware:
  - Servidores estándar Windows o Unix con S.O. Seguros o reforzados
  - Hardware específico
- Arquitectura de red, Múltiples interfaces:
    - Interface Externo: Internet
    - Interface Interno: LAN, Intranet
    - Zona Desmilitarizada (DMZ): Servidores públicos
- Alta disponibilidad:
  - Arquitecturas tolerantes a fallos al ser un punto crítico de acceso

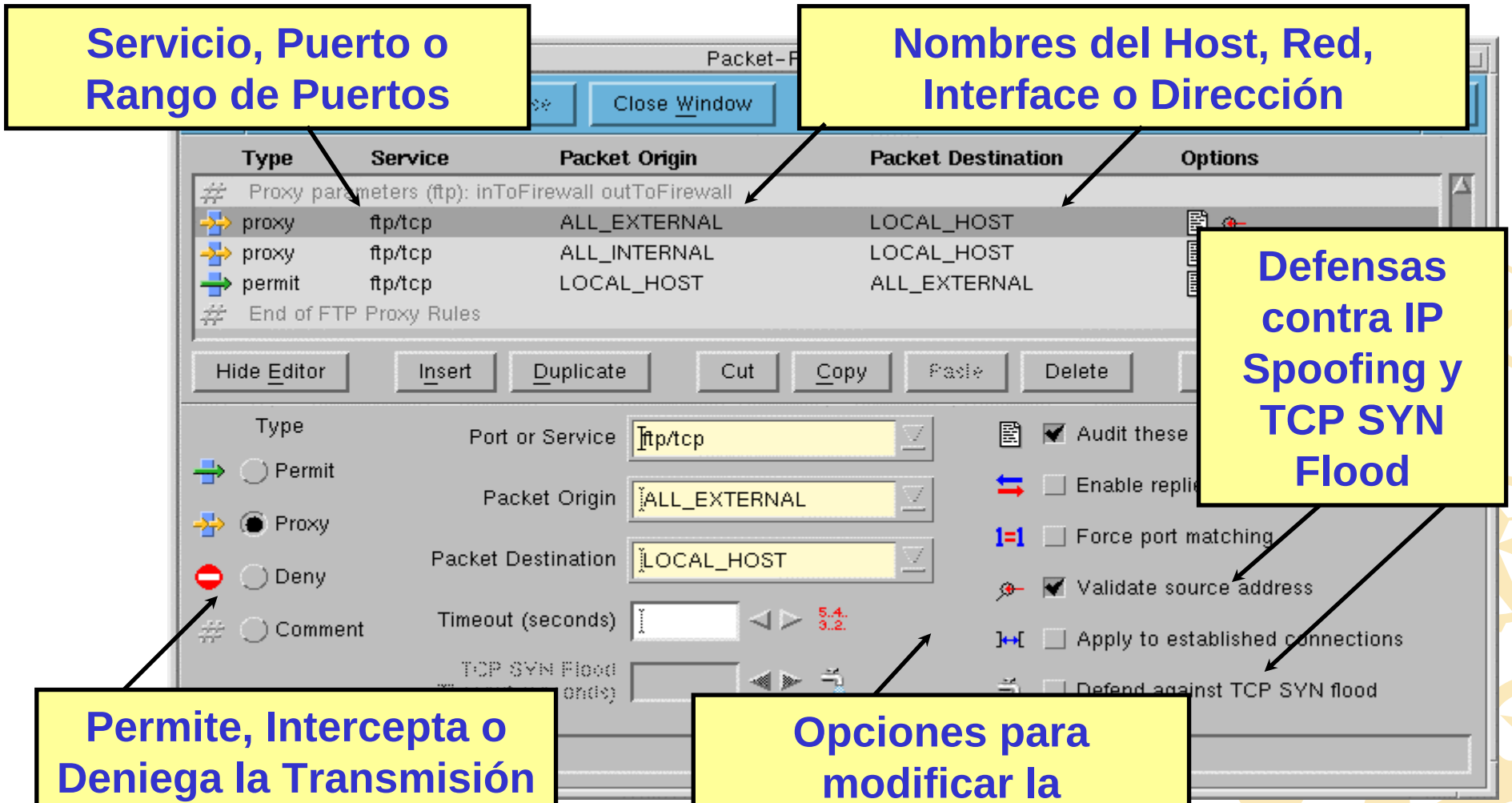
Concepto de zona desmilitarizada-DMZ

- Zona desmilitarizada DMZ:
  - Subred intermedia entre Internet y la Intranet
  - Se instalan los servidores de acceso público como Web, eMail, FTP
  - Los accesos a la Intranet pasan previamente por la DMZ, dando paso a la LAN solo lo imprescindible
  - Se instalan sistemas de filtrado y detección antivirus previo al envío a la Intranet
  - Se pueden establecer zonas de cuarentena
  - Los servidores de la DMZ se robustecen

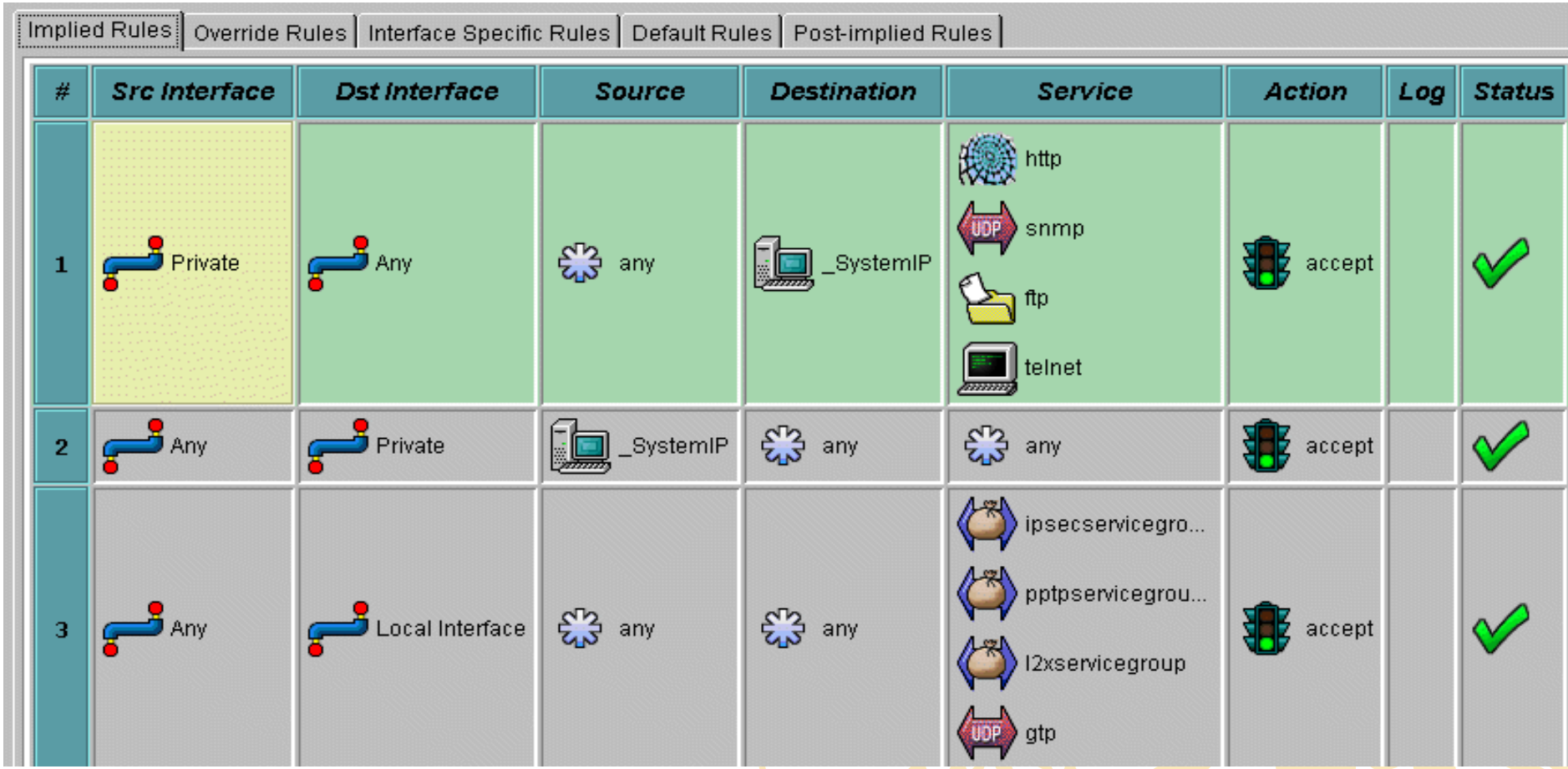
Arquitectura general - Cortafuegos corporativo



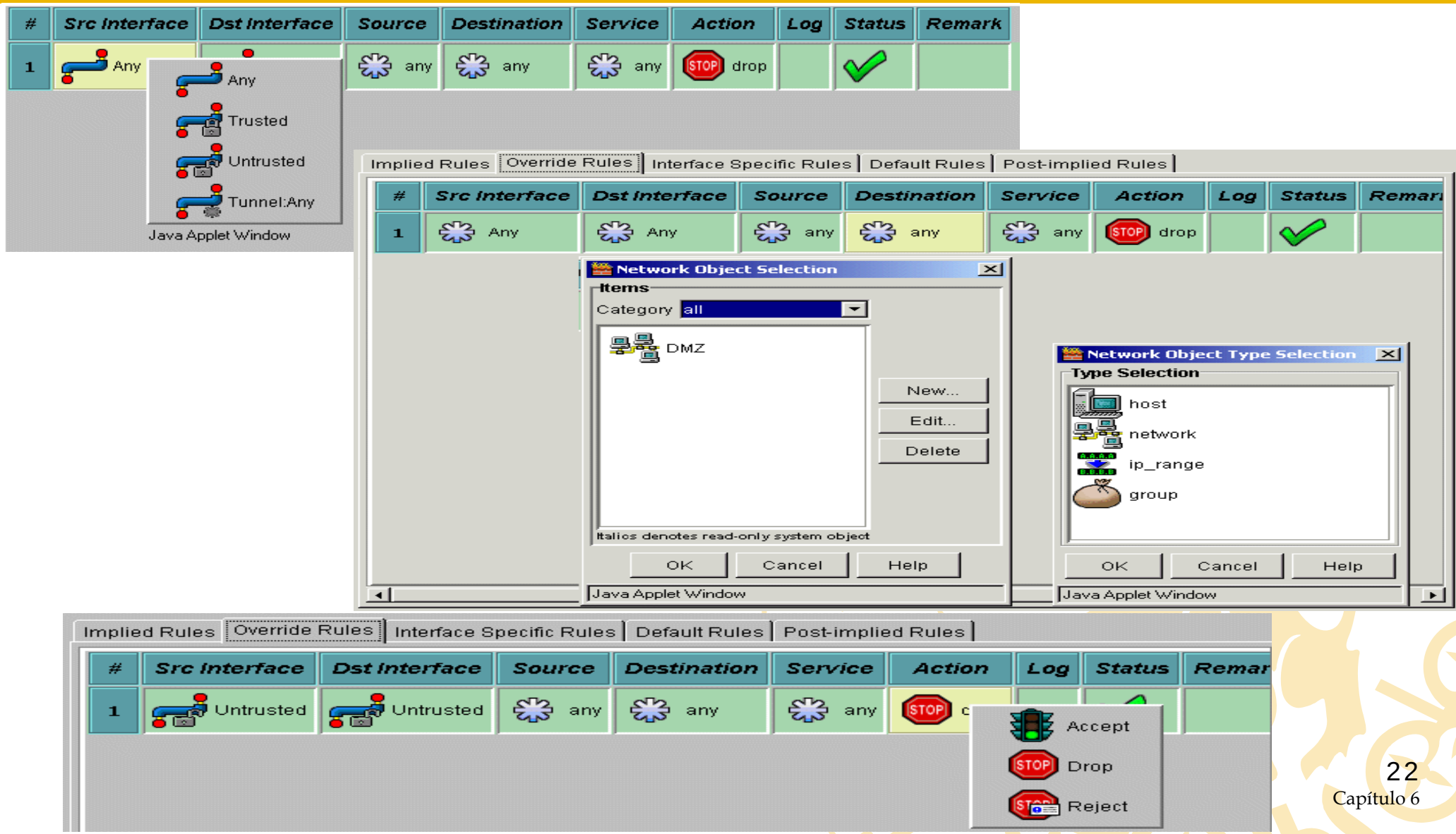
Ejemplo pantalla de configuración



Ejemplo pantalla de configuración



Ejemplo pantalla de configuración



Integración con otras tecnologías

- Autenticación de usuarios externos
  - Mediante usuario/password, mediante certificados digitales, tarjetas, acceso al directorio
- Sistemas antivirus:
  - Sistemas adjuntos en la DMZ
- Filtro de contenidos:
  - Filtrado de URL y navegación hacia el exterior
  - Filtro para control de la información que sale
- Sistemas de detección de intrusión (IDS)
  - Detectan y previenen ataques
- Redes privadas virtuales
  - Túneles cifrados para acceso remoto desde el exterior para teletrabajo

Posibilidades de bloqueo de un Fw

FTP, HTTP, SMTP: Viruses

STOP

File Transfers, Web, E-Mail, News, etc.Aceptables

ActiveX, Java, JavaScript, VBScript

STOP

Inappropriate Sites

STOP

Fallos comunes al implantar un firewall

- Implantar un Fw sin política de seguridad
- Añadir reglas y servicios sin distinguir entre “necesidades” y “deseos”
- Concentrarse en el Fw ignorando otras medidas de seguridad
- Ignorar las alarmas y logs que da el Fw
- Anular las alarmas de bajo nivel y repetitivas
- Permitir a demasiado personal acceder e incluso administrar parámetros del Fw
- Permitir el uso de modems independientes

Clases de ataques

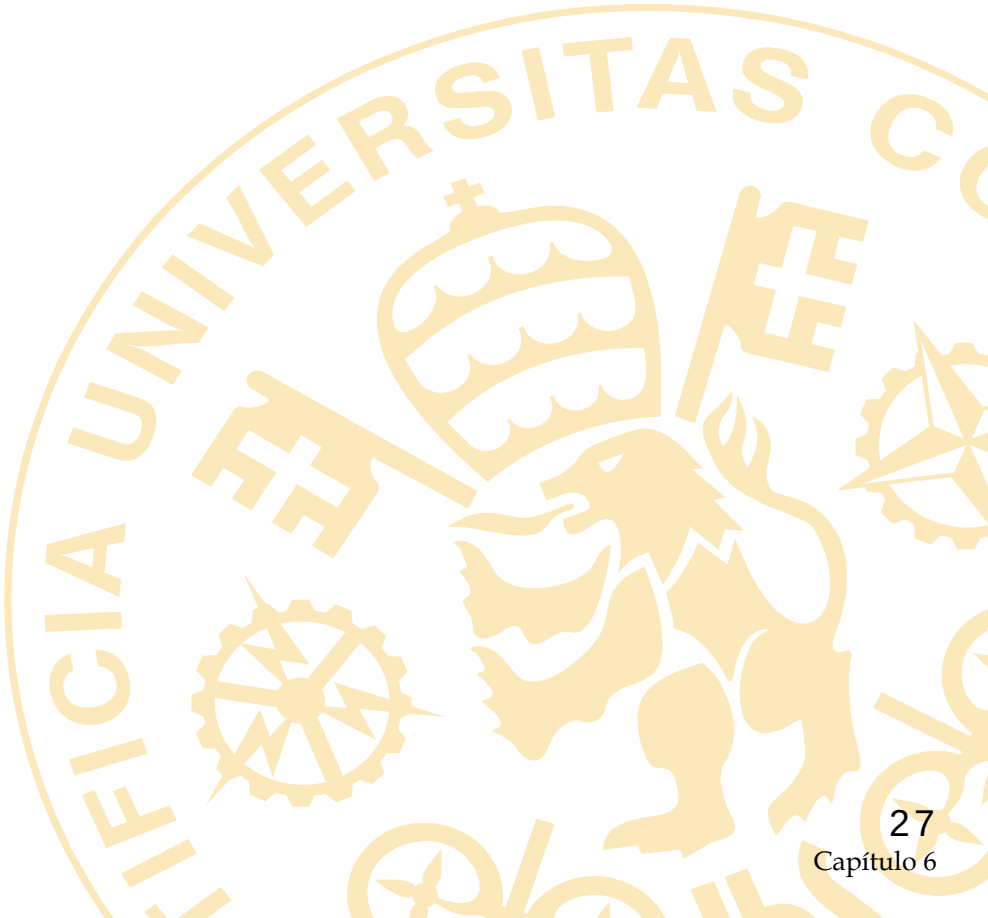
- Averiguación y robo de passwords
  - No es dificil hacerse Administrador o Root
- Aprovechar bugs y puertas traseras:
  - De los SO, software de base o aplicaciones propias
- Fallos en los mecanismos de autenticación:
  - Por la utilización de mecanismos débiles
- Fallos en los protocolos de comunicaciones
- Obtención de información transmitida o almacenada en claro
- Denegación de servicio (DoS)
- Ingeniería social

Fabricantes existentes en el mercado

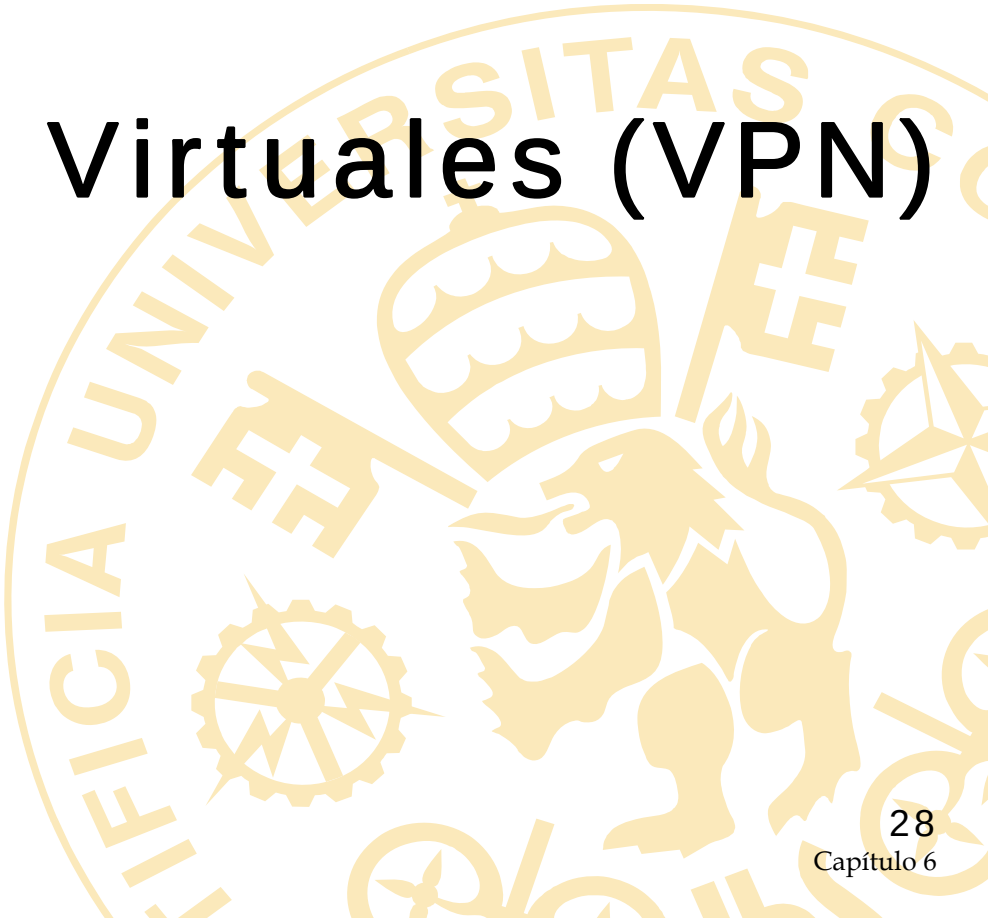
www.icsalabs.net

Productos firewall certificados por ICSA

- Checkpoint Firewall-1
- StoneGate
- Cisco PIX
- CyberGuard
- NetScreen
- Gaunlet



Redes Privadas Virtuales (VPN)



Redes Privadas Virtuales : VPN-IPSec

- Redes Privadas Virtuales VPN-IPSec
- Introducción
- Definiciones y conceptos básicos
- Para que sirve
- El estándar IPSec
- Aplicaciones reales

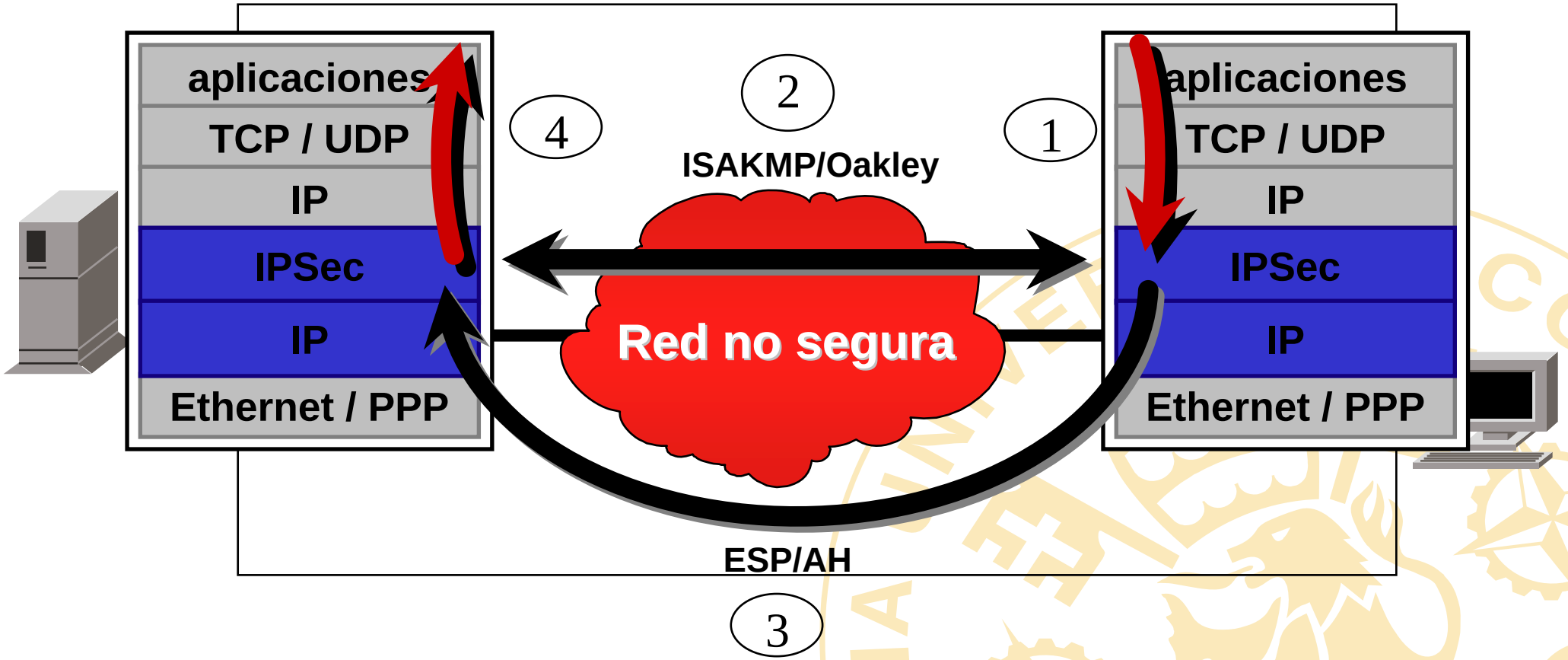
Para que sirve una VPN

- Las Redes Privadas Virtuales proporcionan confidencialidad en redes IP reduciendo costes de comunicaciones
- Tipos de VPN según tecnología:
  - VPN – IPSec
  - VPN – SSL
  - MPLS
- Ventajas de las VPN:
  - Utilizan estándares de seguridad fuerte IPSec, SSL
  - Interoperabilidad entre fabricantes
  - Vale para cualquier aplicación y cualquier modo de acceso; RTB, RDSI, LAN,
  - Integración con otras tecnologías como PKI, IDS
  - Accesos remotos seguros desde cualquier punto como si estuviera en la oficina
  - Reducción drástica de costes en comunicaciones

Ejemplos reales de uso

- Accesos remotos
  - Para explotación remota de sistemas
  - Acceso a información corporativa desde Internet
- Comunicaciones seguras entre oficinas
  - Utilización de redes públicas IP para comunicaciones seguras internas
- Teletrabajo
  - Sistemas de teletrabajo seguro con RDSI, ADSL, Cable-modem, etc

IPSec en la realidad



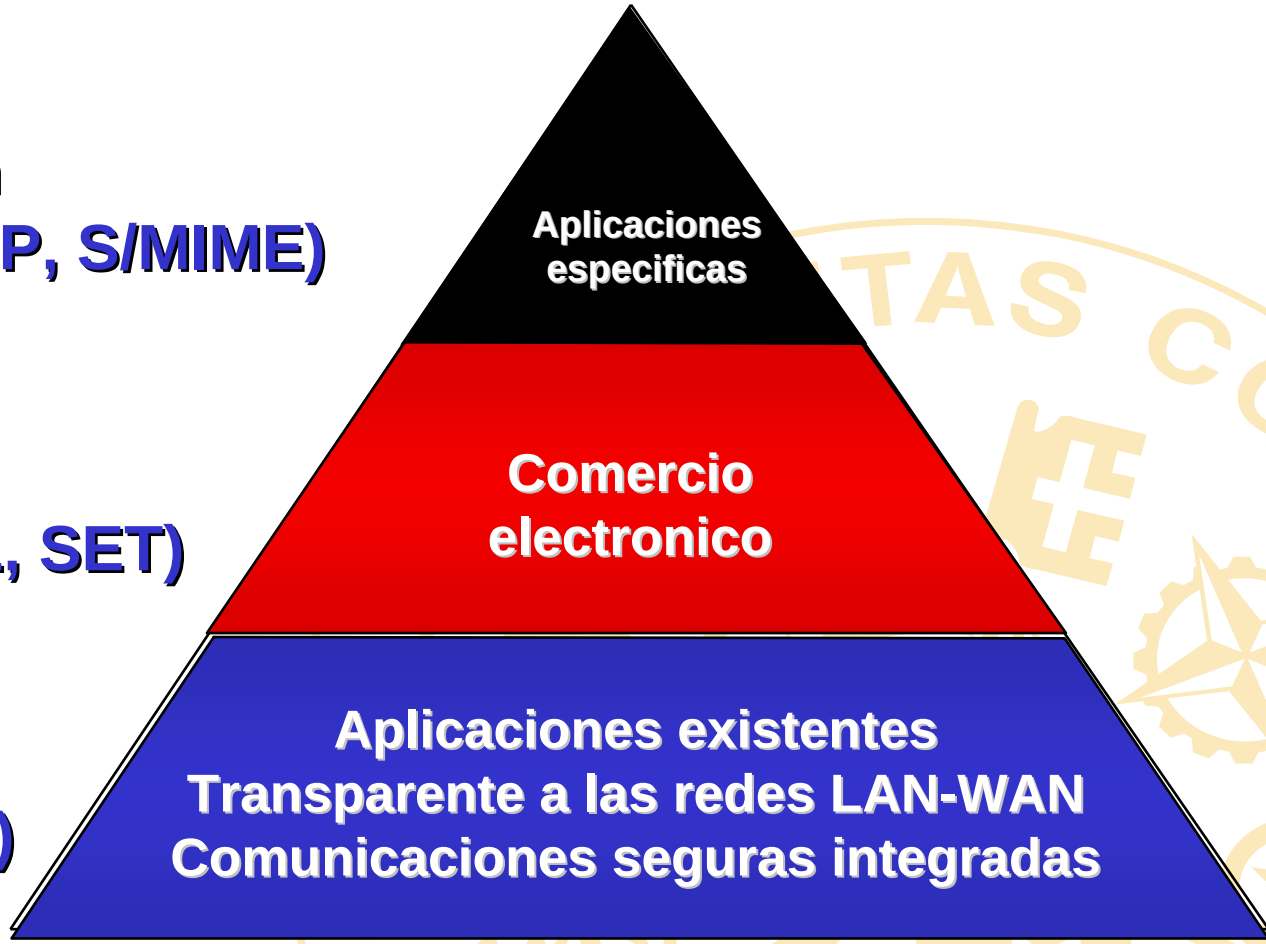
Autenticación y cifrado de datos extremo a extremo

Tecnologías de cifrado y niveles

Nivel de Aplicación
(ficheros/email: PGP, S/MIME)

Nivel de Sesión
(Web browser: SSL, SET)

Nivel de red
(VPN seguras: IPSec)



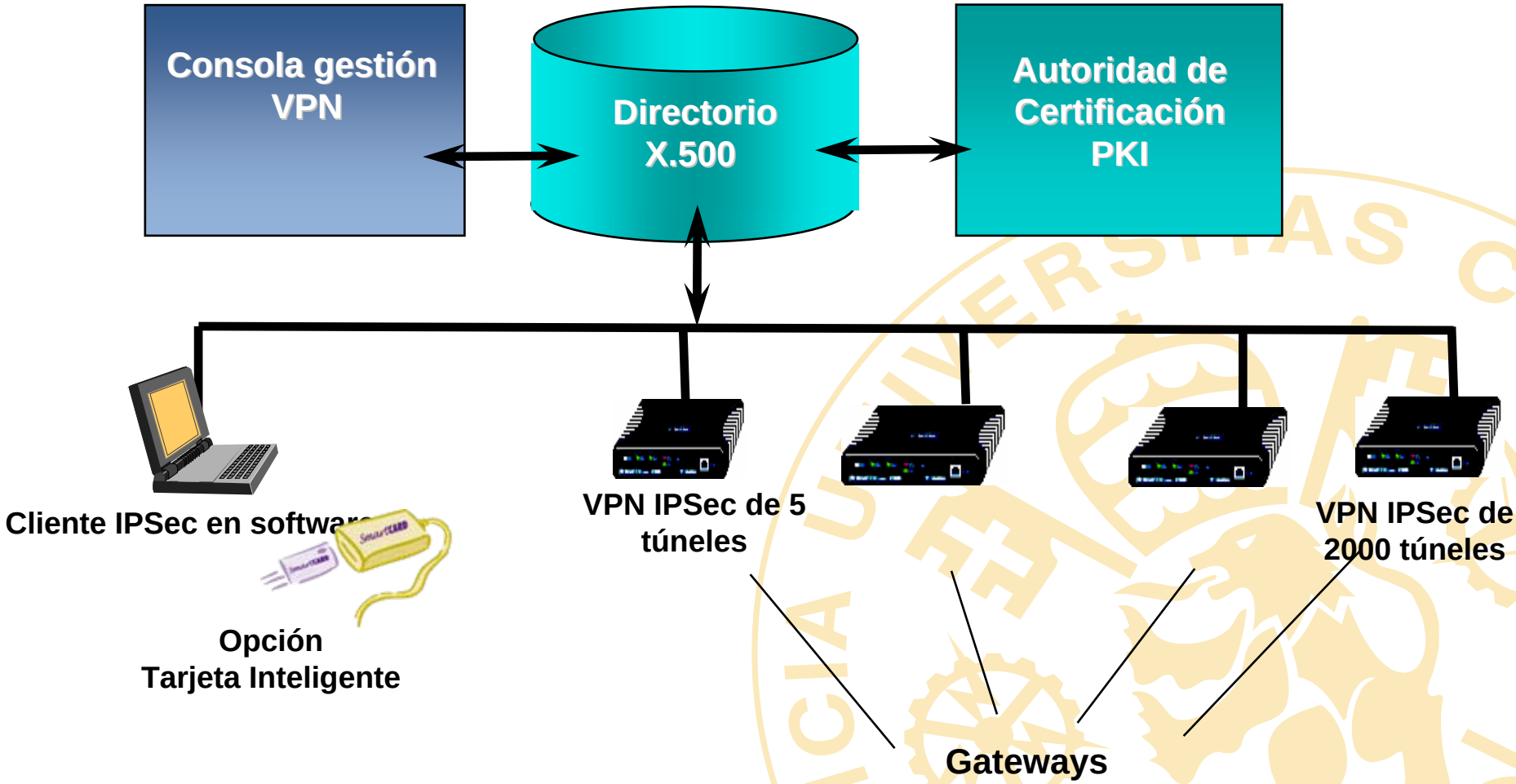
Estructura IPSec: ESP/AH

- Encapsulation Security Payload (ESP)
  - Confidencialidad:
    - DES, 3-DES, RC5, CAST, BLOWFISH, IDEA
- Autenticación de la Cabecera (AH)
  - Integridad y Autenticación de datos
    - HMAC, MD5, SHA1

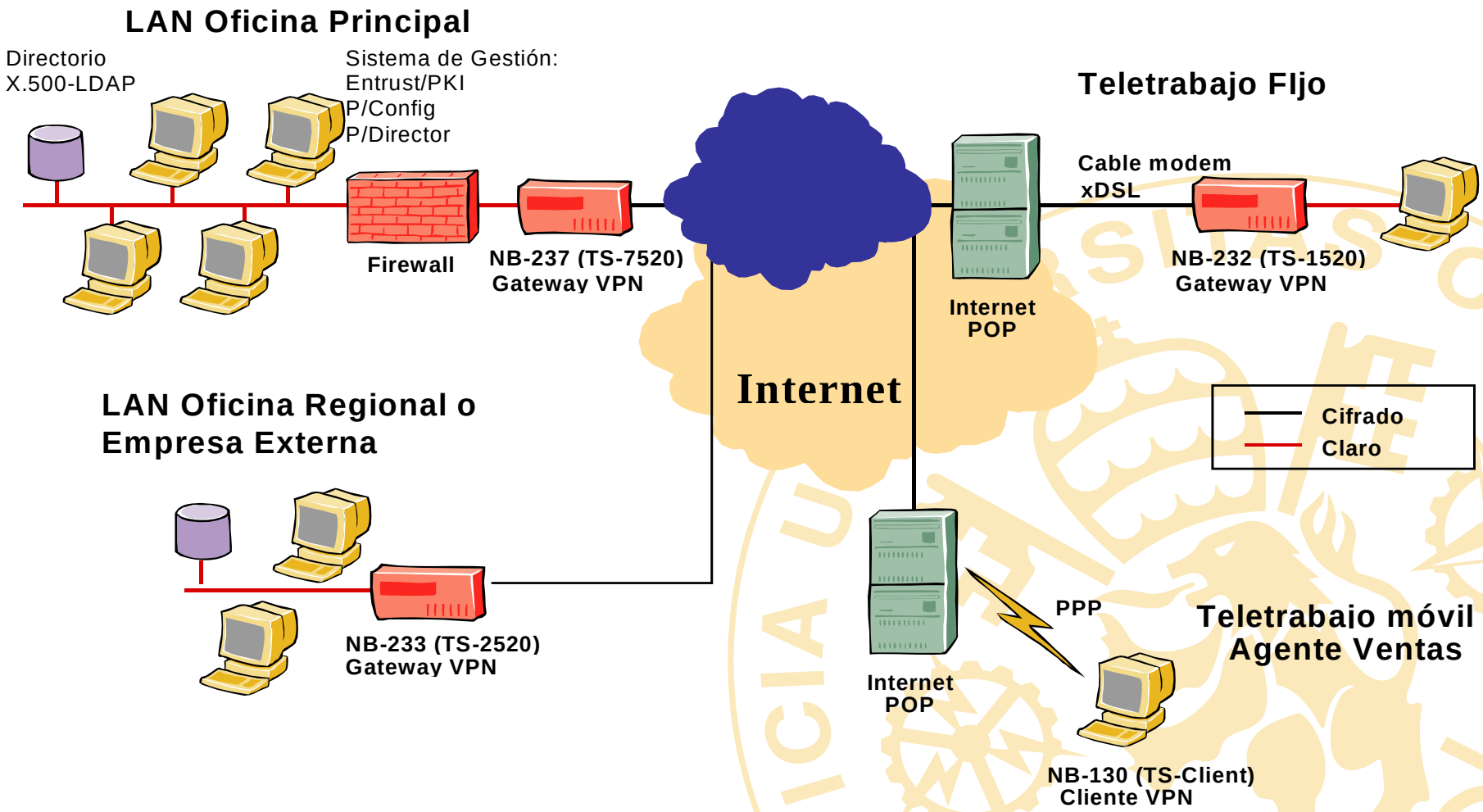
Estructura IPSec: IKE (ISAKMP/Oakley)

- Establece un contexto de seguridad entre dos partes
- Tres tareas primarias para la interoperabilidad:
  - Negociar la política de seguridad
  - Intercambio Diffie-Hellman de claves
  - Autenticar el intercambio Diffie-Hellman

Arquitectura de productos VPN



Arquitectura general de una VPN



Fabricantes VPN IPSec

- Nortel (Modelos Contivity)
- Nokia
- Cisco
- Netscreen
- Checkpoint

Siempre consultar www.icsalabs.net para certificacion

Sistemas de detección de intrusiones: IDS, IPS

Sistema Detección Intrusiones

- Sistema de detección y prevención de Intrusiones (IDS-IPS)
- Introducción
- Definiciones y conceptos básicos
- Para que sirven los IDS/IPS
- Arquitecturas de implantación
- Aplicaciones reales

Para que sirve un sistema IDS

- Protección y detección en tiempo real de ataques: DoS, Caballos de Troya, Escaner de puertos, etc.
- Existen productos software y dispositivos hardware (appliance)
- Tecnología basada en análisis de protocolo (sniffer) o en patern-matching
- Detecta ataques externos e internos
- Se integra con otras tecnologías: Firewall

Diferencias entre IDS e IPS

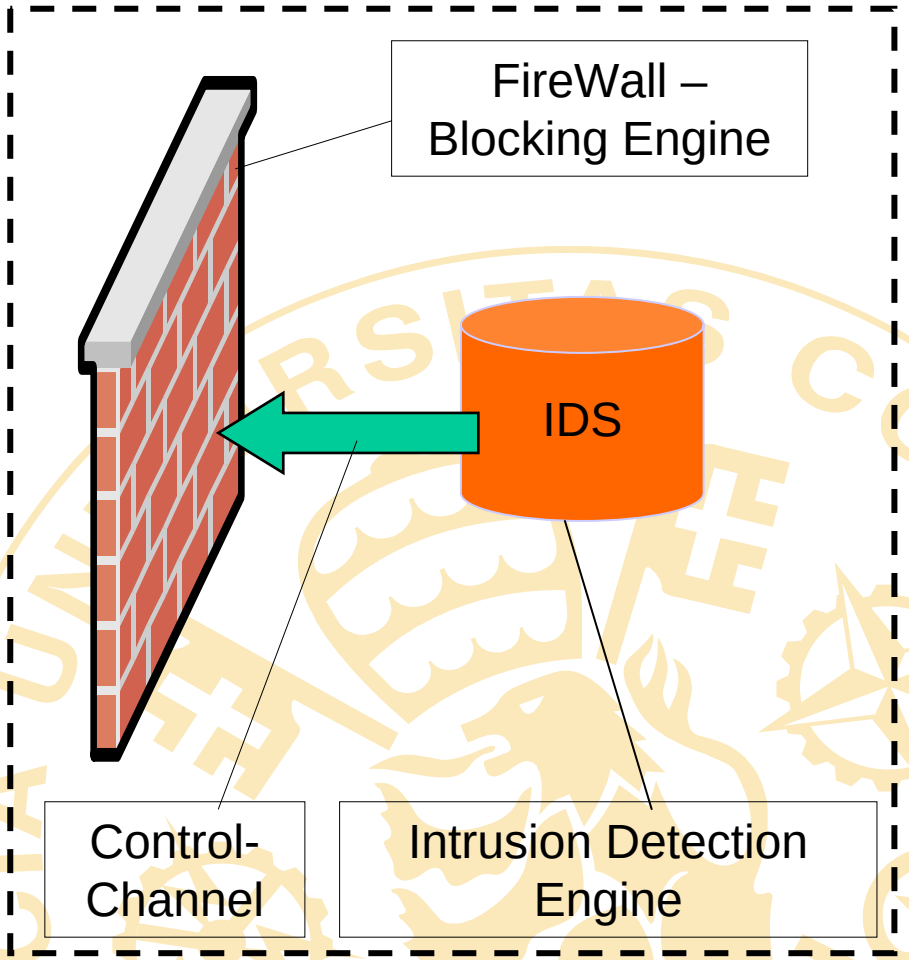
- IDS: Sistema de Detección de Intrusiones
  - Solo detecta intrusiones, da alarmas pero no actúa
  - Se conecta como una sonda en la red o en un equipo, sin interferir el tráfico
  - Utiliza solamente un interface Ethernet, no corta la red
- IPS: Sistema de Prevención de Intrusiones
  - Ademas de detectar, previene contra intrusiones actuando de forma proactiva
  - Se conecta en medio de la red, cortando la conexión
  - Utiliza dos interfaces Ethernet
  - Puede actuar conjuntamente con el Cortafuegos

Tipos de sistemas IDS / IPS

- Sondas de red (Network IDS)
  - Existen sistemas software o equipos appliance
  - Se conectan en una subred y analizan todo el tráfico que pasa
- Software para servidores (Host IDS)
  - Software que se instala en los servidores y detecta intrusiones al equipo
- Software para puesto de trabajo (Personal IDS)
  - Software que se instala en el PC y detecta intrusiones al equipo
  - Se combina con el software antivirus y firewall del PC

Sistema IDS / IPS

- **Detecta**
  - Detecta Intrusiones en tiempo real en el objetivo del ataque
- **Protege**
  - Bloquea en tiempo real el lugar que está siendo atacado
- **Identifica**
  - Identifica automáticamente el lugar de donde viene el ataque



Detección externa e interna