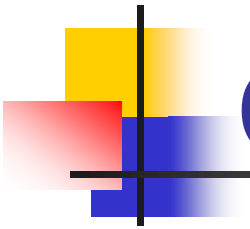
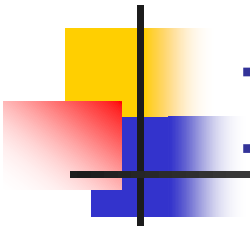
Bloque III
Seguridad en la Internet

Cortafuegos y redes privadas virtuales

Seguridad en Redes de Comunicaciones
María Dolores Cano Baños

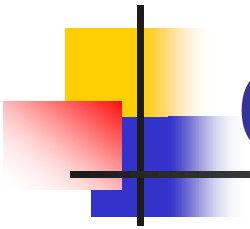


Contenidos



Introducción

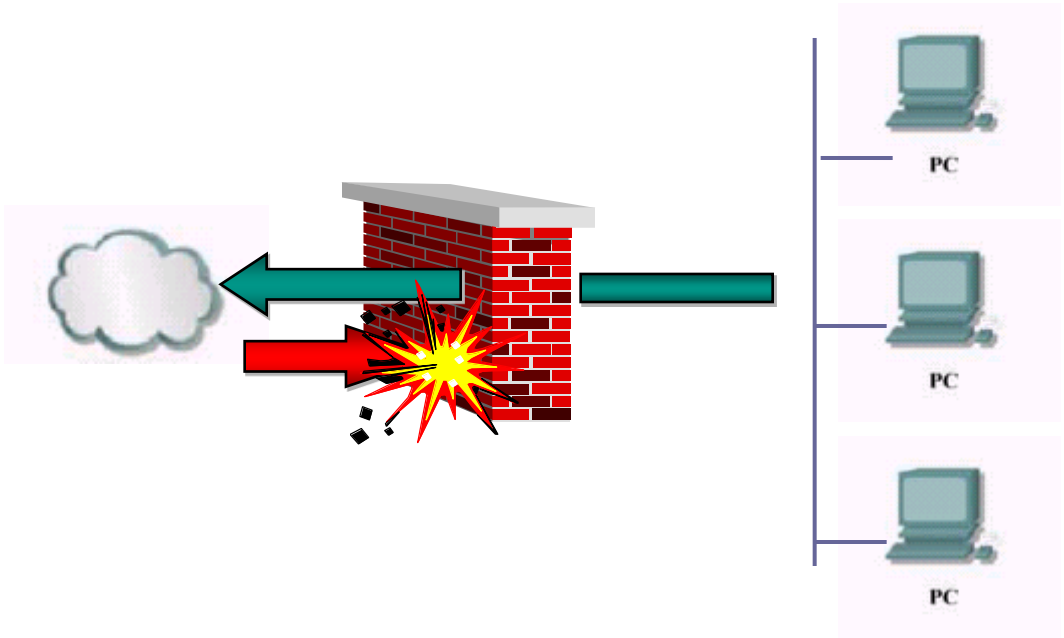
- Organizaciones descentralizadas
- Intranet
  - Red empresarial
  - Acceso limitado
  - Distribución y compartición de recursos
  - Reducción de costes
- Herramientas
  - Mecanismos AAA (Authentication, Authoritation, Accounting)
  - Cortafuegos
  - Redes Privadas Virtuales (VPN)

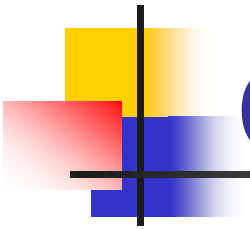


Contenidos

Cortafuegos

- Necesidad de mantener una conexión a Internet ⇨ amenaza
- **Cortafuegos:** sistema que protege a la red corporativa de la red pública





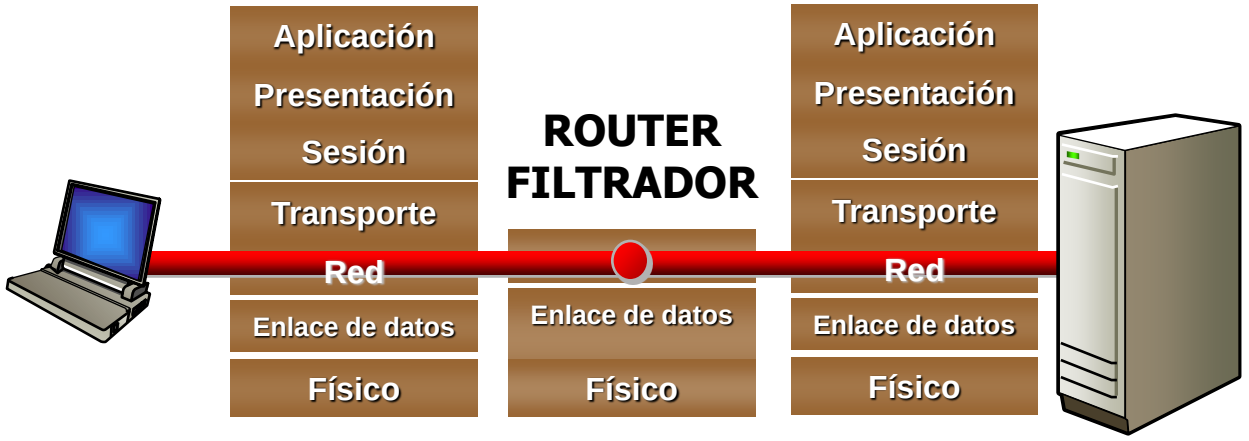
Cortafuegos

- Funciones del cortafuegos:
  - Restringir y controlar el acceso del tráfico (*inbound* y *outbound*) según indique la política de seguridad
    - Control de servicios
    - Control de dirección
    - Control de usuario
    - Control de comportamiento
  - Ocultación de información
  - Registro y alarmas
- Limitaciones del cortafuegos
  - Amenazas internas
  - Transferencia de programas
  - Fallos de nivel físico

Contenidos

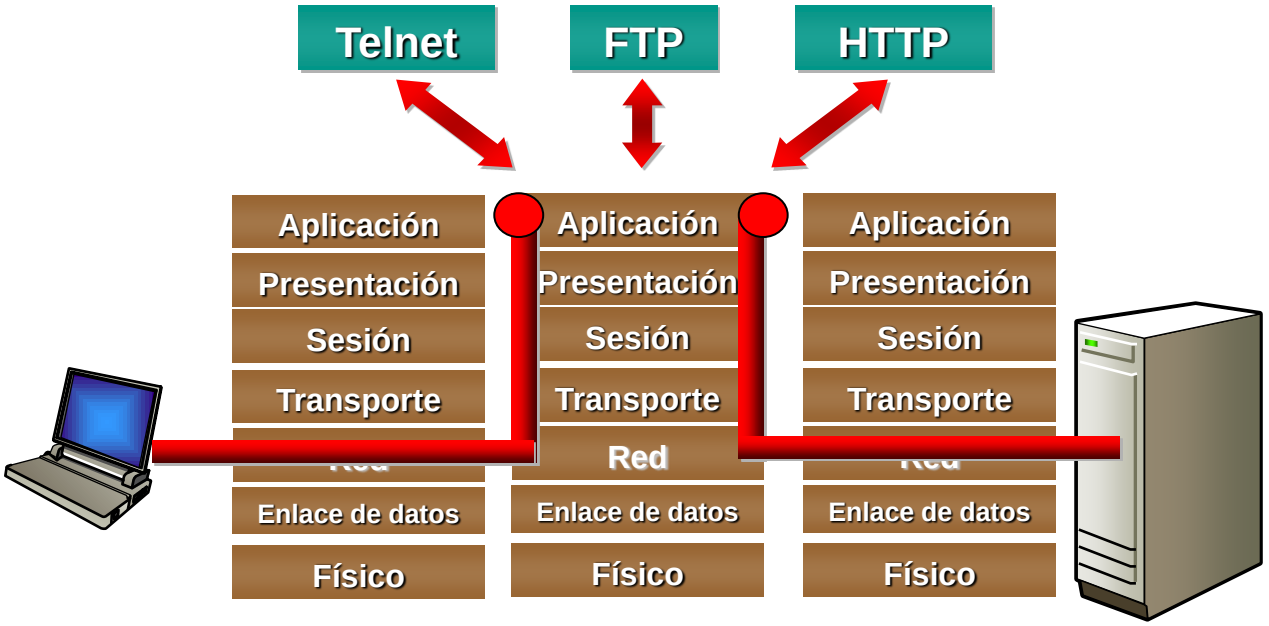
Cortafuegos

- **Routers filtradores**
  - Sencillos
  - Se permite o se deniega el paso de paquetes
  - Información de filtrado de cabecera IP
  - No mantienen información de estado
  - Transparente para el usuario final



Cortafuegos

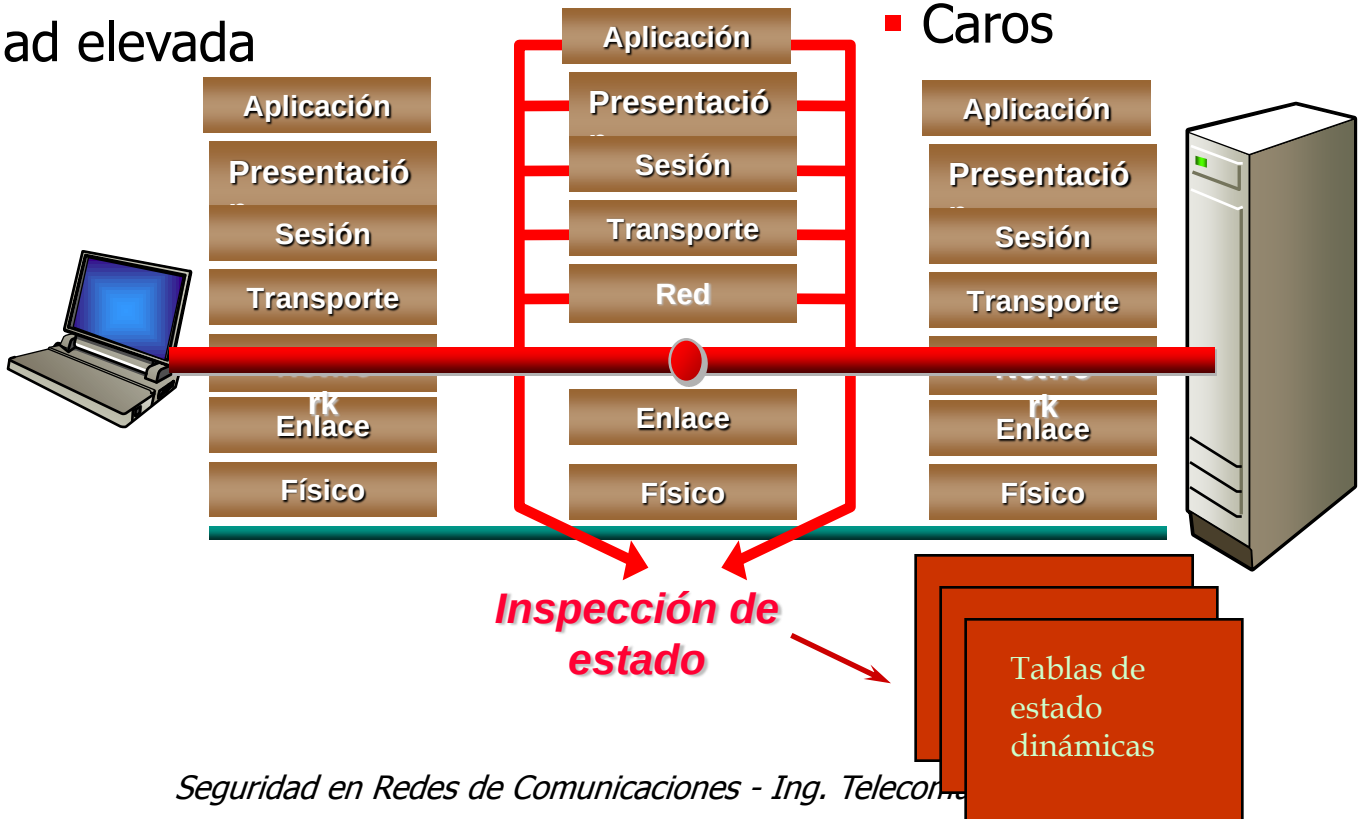
- **Pasarelas de Aplicación** (*Proxies* de aplicación)
  - Programas localizados entre el usuario final y la red pública
  - Intermediario entre los usuarios de la red corporativa e Internet
  - Topología "Host Bastión"
  - Seguridad elevada
  - No es transparente al usuario final

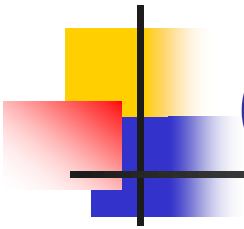


Cortafuegos

- **Cortafuegos de inspección de estado**

- Escalables y transparentes al usuario final
- Mantienen información de estado
- Seguridad elevada
- Funciones de registro y alarmas
- Caros





Contenidos

2.1 Introducción ✓

2.2 Cortafuegos

- 2.2.1 Definición ✓
- 2.2.2 Tipos de cortafuegos ✓
- 2.2.3 Implementación
- 2.2.4 Topologías

2.3 Redes Privadas Virtuales

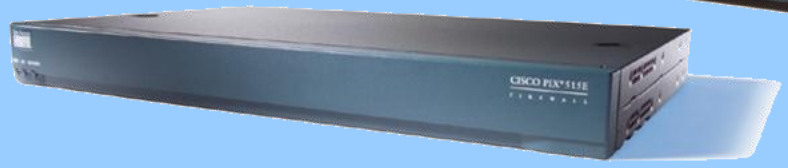
- 2.3.1 Evolución
- 2.3.2 Topologías
- 2.3.3 Tecnologías
- 2.3.4 Componentes

Cortafuegos

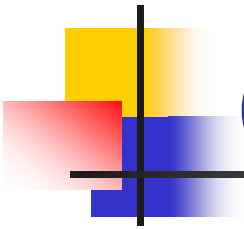
- Implementaciones:

Plataforma Estándar

Dispositivo Especial



Dispositivo Integrado



Contenidos

2.1 Introducción ✓

2.2 Cortafuegos

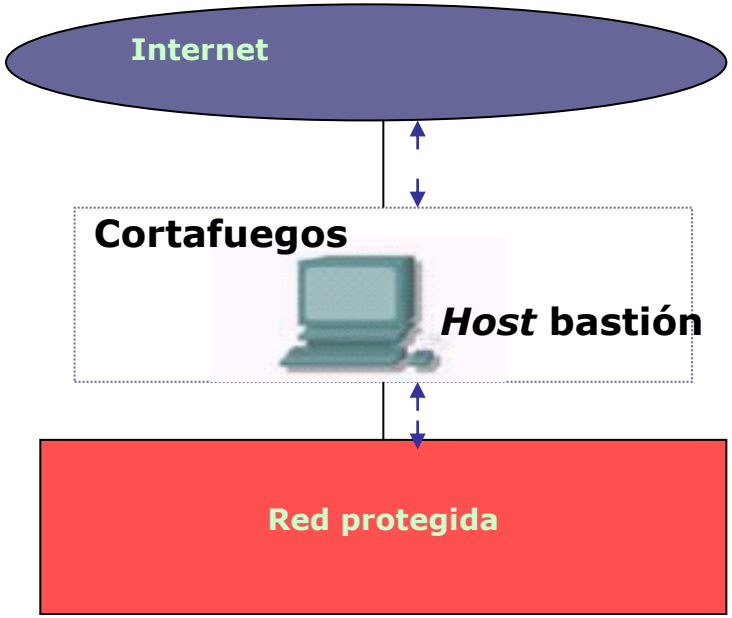
- 2.2.1 Definición ✓
- 2.2.2 Tipos de cortafuegos ✓
- 2.2.3 Implementación ✓
- 2.2.4 Topologías

2.3 Redes Privadas Virtuales

- 2.3.1 Evolución
- 2.3.2 Topologías
- 2.3.3 Tecnologías
- 2.3.4 Componentes

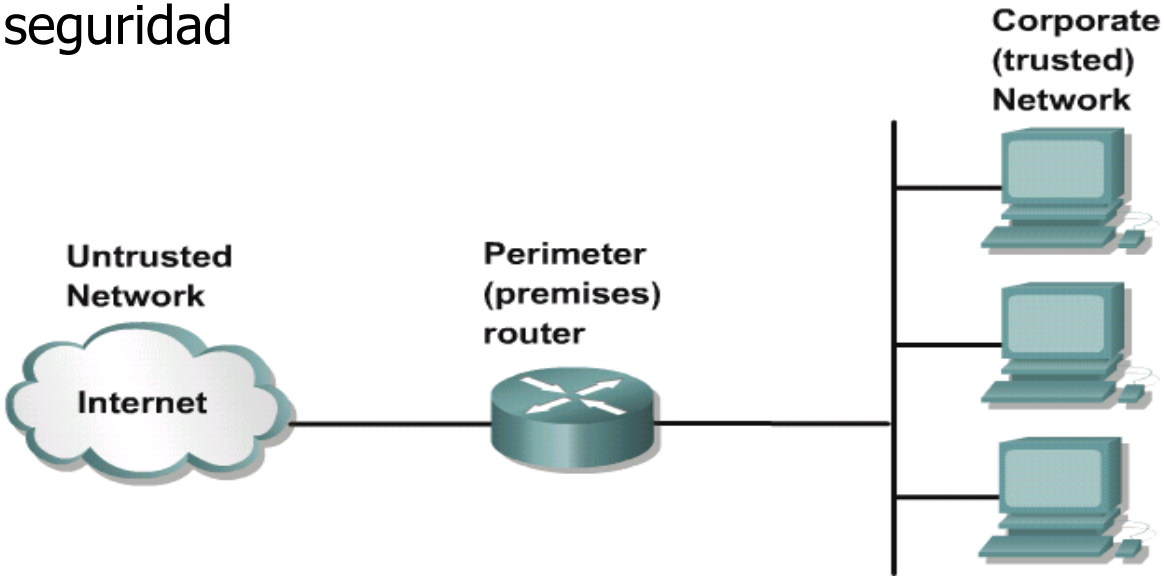
Cortafuegos

- **Host Bastión**
  - Punto crucial en la seguridad de la red
  - Software seguro
  - No hay cuentas de usuario
  - No existe relación de confianza
  - Unix o windows NT



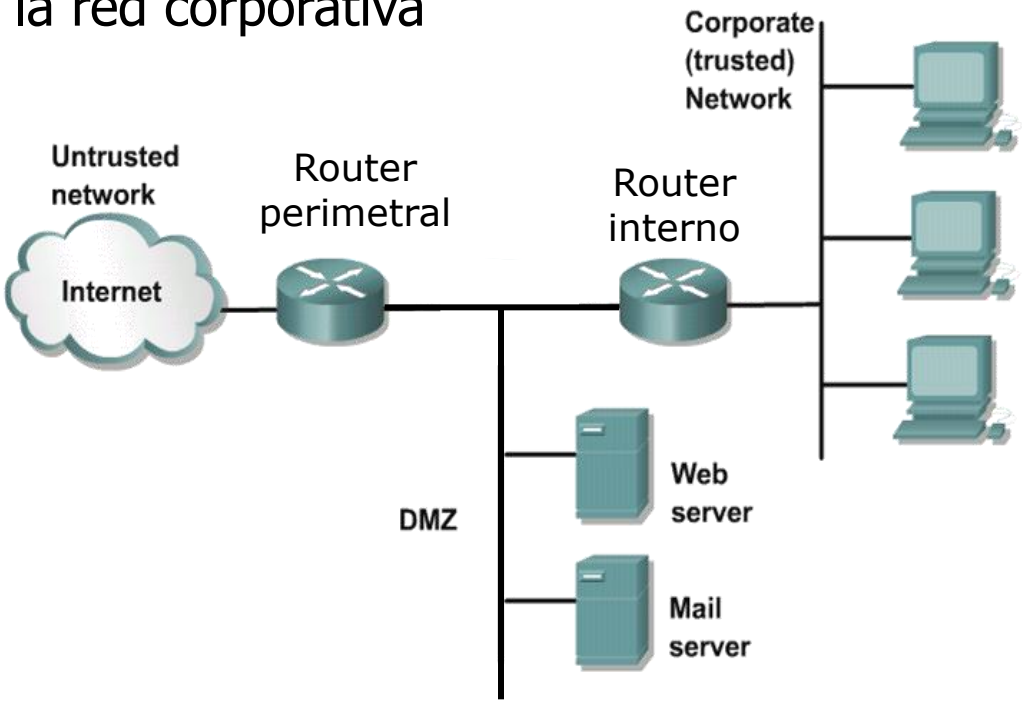
Cortafuegos

- **Router perimetral**
  - Red perimetral: zona de la red de la organización en la que se sitúan los servidores
  - Router filtrador de paquetes (S.O propietario): *autentica* usuarios de Internet y previene ataques
  - Equipos de la red incluyen sus propios mecanismos de seguridad



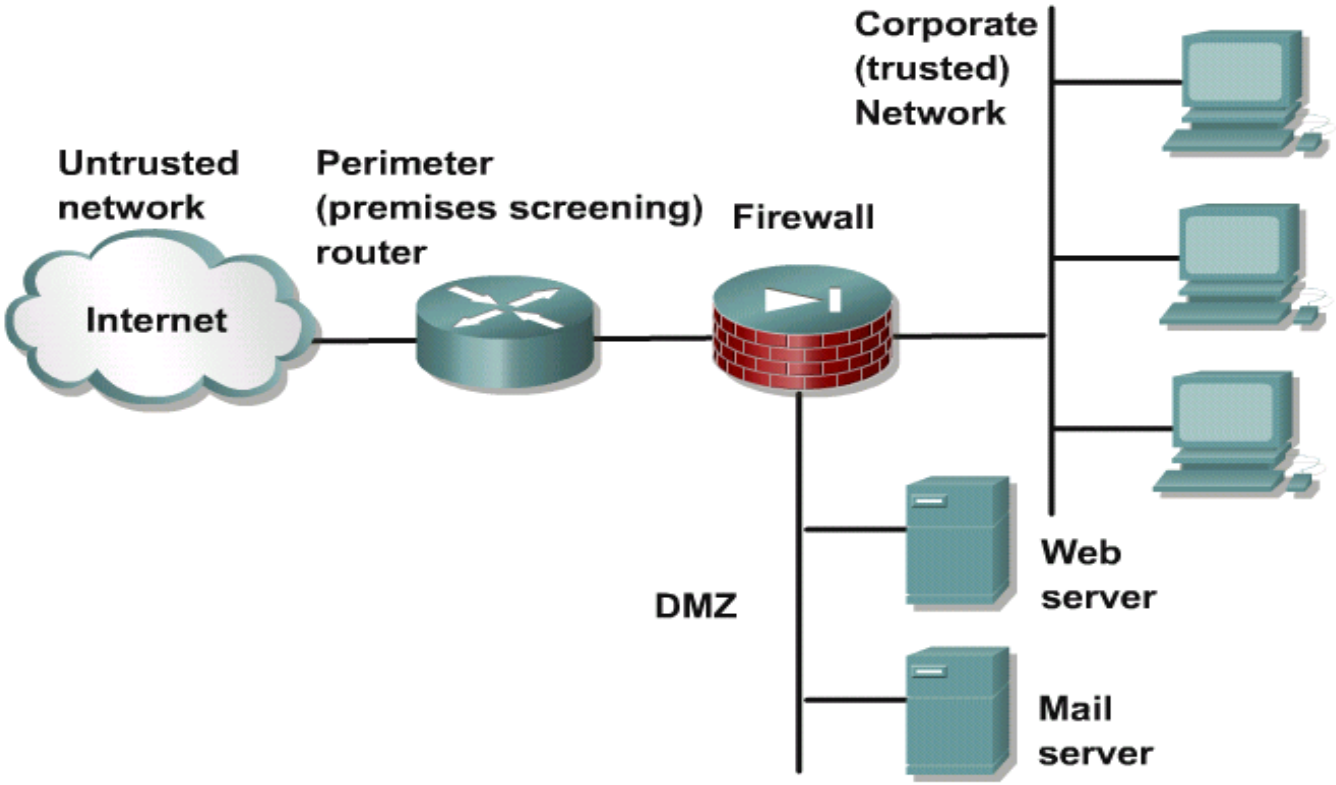
Cortafuegos

- **Router perimetral y DMZ**
  - DMZ ≡ Demilitarized Zone ≡ Red perimetral
  - Separar servidores del resto de la red corporativa
  - Router perimetral y router interno
  - Cada equipo de red perimetral es host bastión



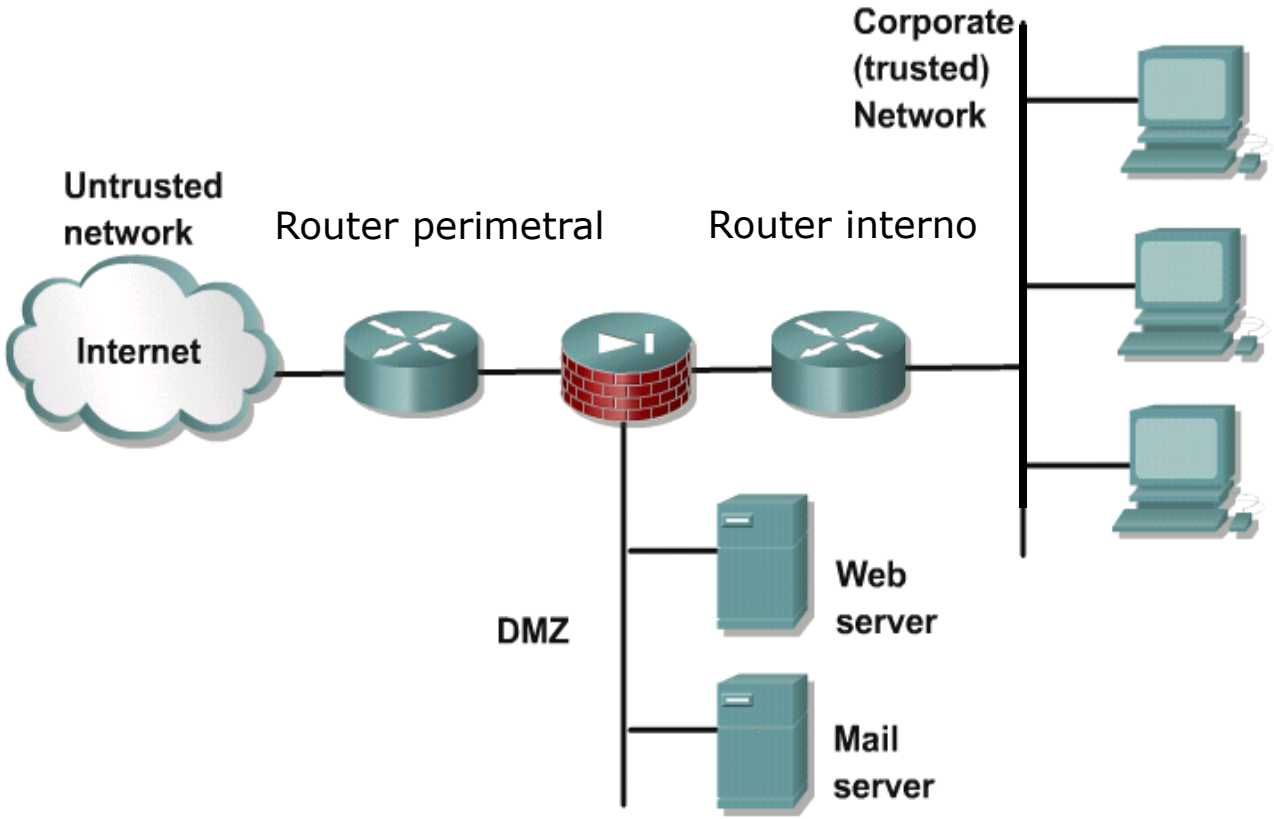
Cortafuegos

- **Router y cortafuegos combinado**



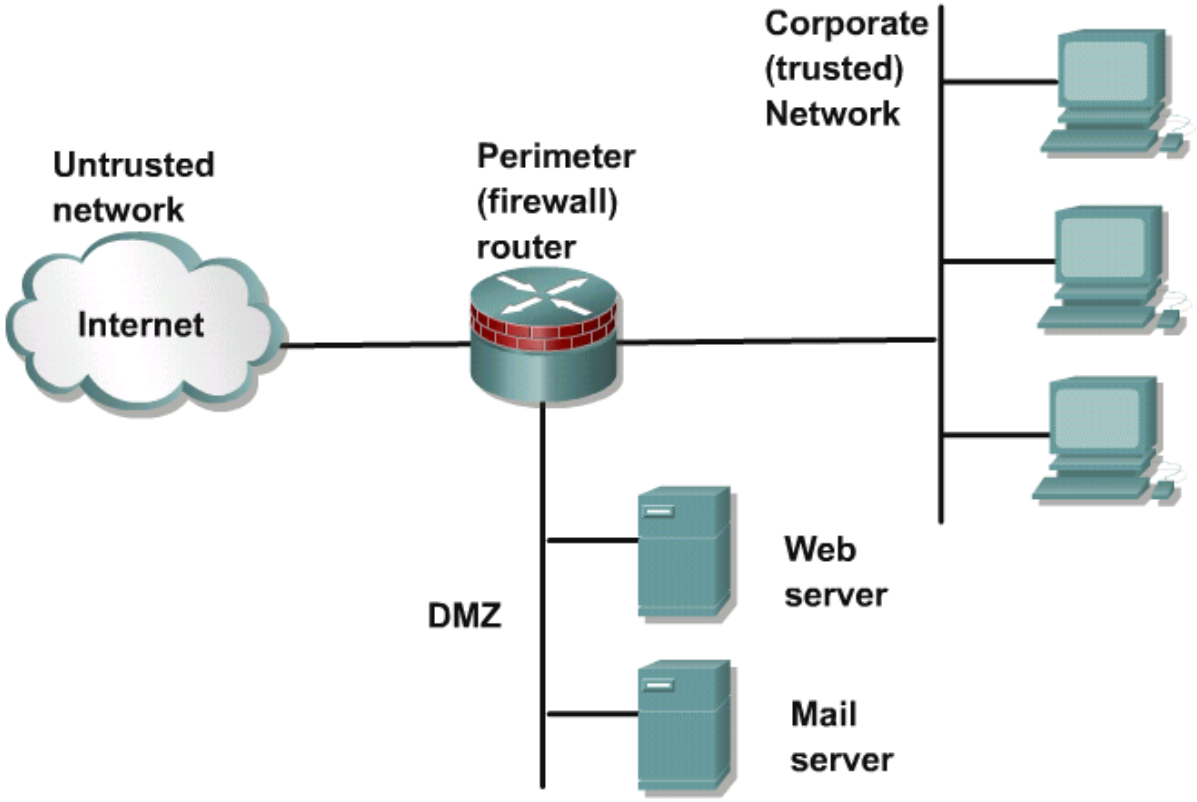
Cortafuegos

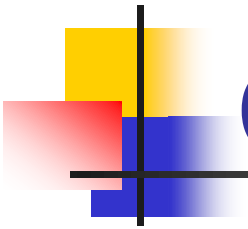
- **Router y cortafuegos combinado**



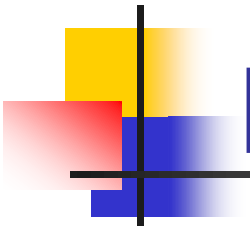
Cortafuegos

- **Red perimetral aislada**



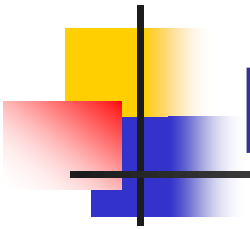


Contenidos



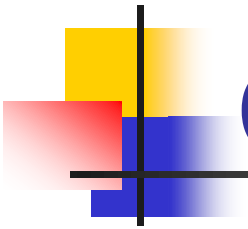
Redes Privadas Virtuales

- Unificar red privada de una compañía
- Garantizar comunicación fiable
  - ¿Cómo interconectar la infraestructura de telecomunicaciones de las sedes remotas?
- 1980 → Líneas dedicadas o alquiladas
- 1990 → Frame Relay, primeras "redes privadas virtuales"; RDSI
- 2000 → VPN basadas en Internet
  - Seguridad y prestaciones



Redes Privadas Virtuales

- Servicios de seguridad de una VPN
  - Autenticación del origen de datos
  - Control de acceso
  - Confidencialidad
  - Integridad de datos

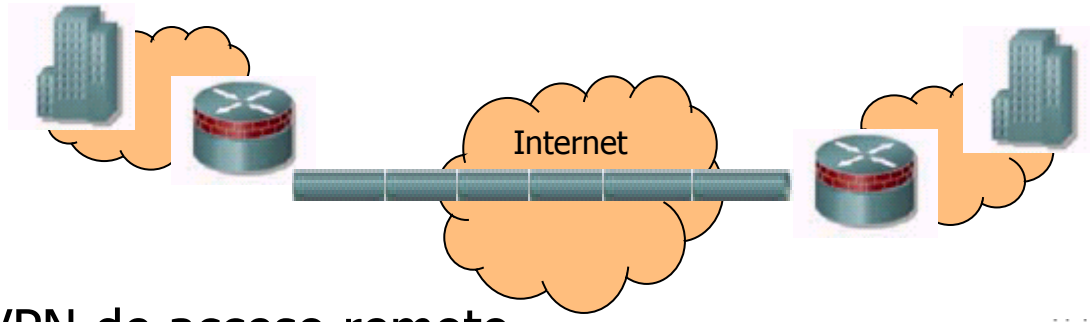


Contenidos

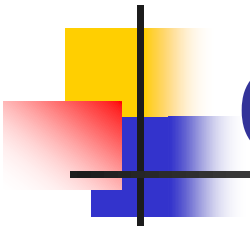
- 2.1 Introducción ✓
- 2.2 Cortafuegos ✓
  - 2.2.1 Definición ✓
  - 2.2.2 Tipos de cortafuegos ✓
  - 2.2.3 Implementación ✓
  - 2.2.4 Topologías ✓
- 2.3 Redes Privadas Virtuales
  - 2.3.1 Evolución ✓
  - 2.3.2 Topologías
  - 2.3.3 Tecnologías
  - 2.3.4 Componentes

Redes Privadas Virtuales

- Protocolos que crean túneles
  - Datos se encapsulan en paquetes IP
  - Infraestructura de Internet enmascarada para ambos extremos del túnel
- Extremos de un túnel: ordenador individual o red LAN con pasarela de seguridad
  - VPN LAN-a-LAN (LAN-to-LAN o site-to-site)

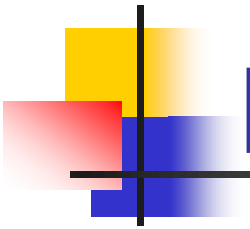


  - VPN de acceso remoto



Contenidos

- 2.1 Introducción ✓
- 2.2 Cortafuegos ✓
  - 2.2.1 Definición ✓
  - 2.2.2 Tipos de cortafuegos ✓
  - 2.2.3 Implementación ✓
  - 2.2.4 Topologías ✓
- 2.3 Redes Privadas Virtuales
  - 2.3.1 Evolución ✓
  - 2.3.2 Topologías ✓
  - 2.3.3 Tecnologías
  - 2.3.4 Componentes



Redes Privadas Virtuales

- Tecnologías VPN:
  - PPTP; L2F; L2TP; IPSec; MPLS
- **PPTP** (Point-to-Point Tunneling Protocol)
  - Propietario de Microsoft
  - Funciona con PPP
  - Encapsula paquetes PPP usando versión modificada del protocolo GRE (Generic Routing Encapsulation)
  - Mecanismos de autenticación CHAP y PAP
  - Ningún cifrado fuerte
  - Sólo una conexión por el túnel

Redes Privadas Virtuales

- **L2F** (Layer 2 Forwarding)
  - Propietario de Cisco
  - Puede funcionar con PPP
  - Mecanismos de autenticación CHAP, PAP o RADIUS
  - Más de una conexión por el túnel
- **L2TP** (Layer 2 Tunneling Protocol)
  - Desarrollado por el IETF
  - Utiliza PPP
  - Puede transportar paquetes de redes diferentes
  - Autenticación PAPA, CHAP o RADIUS
  - No incluye mecanismos de cifrado fuertes ni gestión de claves

Redes Privadas Virtuales

- **IPSec**
  - Decidir política de seguridad (IKE e IPSec)
    - IKE: distribución de claves, método de autenticación, direcciones IP y nombres, parámetros de la asociación de seguridad (algoritmo de cifrado, algoritmo de hash, etc.)
    - IPSec: protocolo AH y/o ESP, algoritmo de autenticación, algoritmo de cifrado, etc.
  - Crear túnel IPSec
    - 1ª fase: extremos del túnel se autentican y crean canal seguro
    - 2ª fase: negociación parámetros IPSec y establecimiento del túnel
  - Comunicación segura a través de VPN
  - Medida de seguridad fuertes

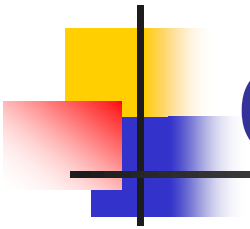
Redes Privadas Virtuales

- **MPLS**
  - Servicio VPLS (Virtual Private LAN Service)
  - Conectividad total
  - MPLS no incluye mecanismos de cifrado, autenticación o integridad de datos ⇨ combinar IPSec y MPLS

  "Virtual Private LAN Services: The evolution of Layer 2 VPNs", Technical White Paper, Alcatel

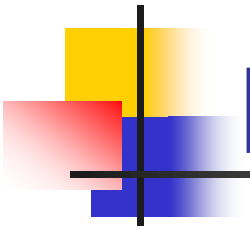
- **SSL**
  - No es necesario añadir cliente VPN en cada equipo
- **SSH**
  - En máquinas UNIX junto con PPP

  http://www.tldp.org/HOWTO/ppp-ssh



Contenidos

- 2.1 Introducción ✓
- 2.2 Cortafuegos ✓
  - 2.2.1 Definición ✓
  - 2.2.2 Tipos de cortafuegos ✓
  - 2.2.3 Implementación ✓
  - 2.2.4 Topologías ✓
- 2.3 Redes Privadas Virtuales
  - 2.3.1 Evolución ✓
  - 2.3.2 Topologías ✓
  - 2.3.3 Tecnologías ✓
  - 2.3.4 Componentes



Redes Privadas Virtuales

- Componentes de red VPN basada en Internet:
  - Internet
  - Pasarelas de seguridad
  - Servidores de políticas de seguridad
  - Autoridades de certificación