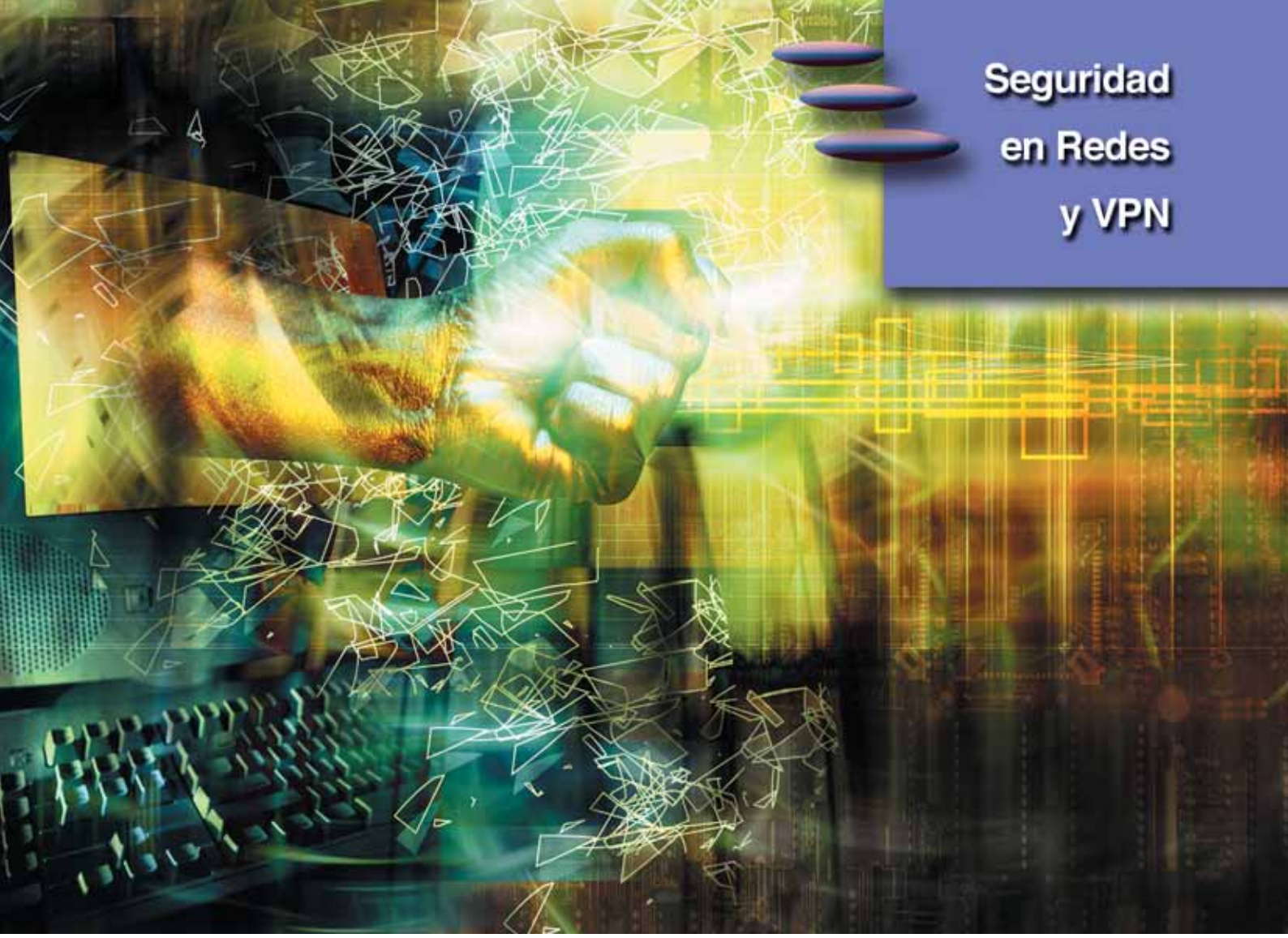


Seguridad en Redes y VPN

Seguridad en redes y Redes privadas virtuales (VPN)

MDtel ve un futuro en el que todo el mundo estará conectado a internet. Las empresas estarán conectadas, a través de la red, a sus clientes y proveedores. El mercado estará en la red.

Esta oportunidad de negocio, a su vez, está ocasionando también problemas para las organizaciones, ya que hay gente que se introduce en nuestras redes e intentan coger información de nuestra empresa. Por ello, ahora más que nunca necesitamos**, interconectar todas nuestras oficinas de forma sencilla y fiable y hacer seguras nuestras redes.**

MDtel contribuye a realizar el dimensionamiento adecuado de sus redes privadas virtuales, asegurándole un ahorro considerable en sus comunicaciones, con una alternativa segura, fiable y flexible.

Las redes privadas virtuales le permiten utilizar la red internet para su tráfico interno a través de túneles privados virtuales, consiguiendo un considerable ahorro frente a la utilización de líneas privadas, con las mismas garantías de seguridad.

Ventajas de una Red Privada Virtual

- **Ahorro de costes**. mucho más económico que el coste de circuitos dedicados privados. Entre un 20 % y un 40 % de ahorro.
- **Sin inversiones** en infraestructura.
- **Seguridad**, flexibilidad e integridad en la transmisión de datos.
- **Acceso remoto seguro** desde cualquier punto geográfico. Movilidad de los empleados.

MDtel TELECOMUNICACIONES

Soluciones para sus redes

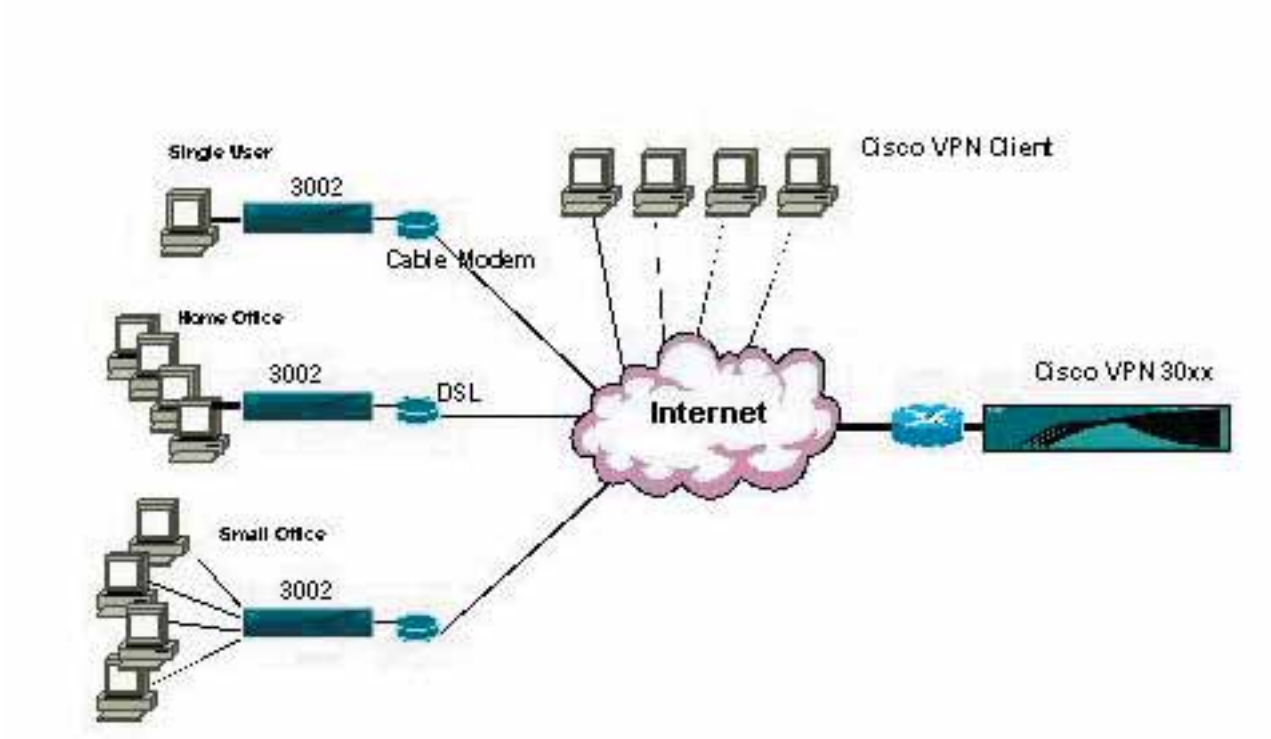
Para garantizar la interconexión y la seguridad en sus redes se utilizan, entre muchos otros los siguientes equipos:

Servidores de acceso remoto. Permiten al acceso a los recursos de datos de la compañía, conformando una red privada a nivel físico; el usuario se conecta vía RTC o RDSI a un dispositivo ubicado en las dependencias de la compañía, estableciendo un enlace físico temporal con la misma.

Servidores de túneles VPN. Aprovechando la conectividad a Internet existente en las compañías y sus dependencias, se puede utilizar esta para constituir enlaces virtualmente privados, de manera que se pueda usar un medio público y económico de transmisión de datos como es Internet. Las dependencias de una compañía y los usuarios remotos quedarán unidos entre sí gracias a la utilización de estos dispositivos.

Firewalls. La presencia pública de las compañías en Internet supone la adopción de mecanismos de seguridad que eviten que usuarios malintencionados accedan a recursos no públicos, o ejecuten ataques sobre las máquinas publicadas en Internet. Los firewalls constituyen una primera barrera en el perímetro de la red, orientada a evitar estos accesos malintencionados a recursos de la compañía.

Sistemas de detección de intrusos. Utilizados junto con los firewalls, complementan la funcionalidad de los mismos detectando ataques más complejos que evitan las reglas establecidas por los firewalls; se basan en un analizador de redes con un software específico de análisis de aplicación, unido a unas firmas de ataque actualizadas constantemente.



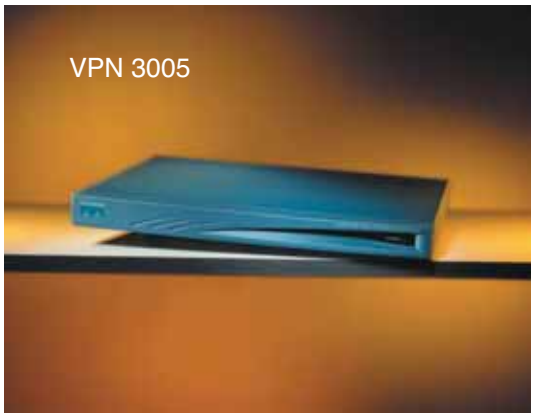
Soluciones de Cisco Systems

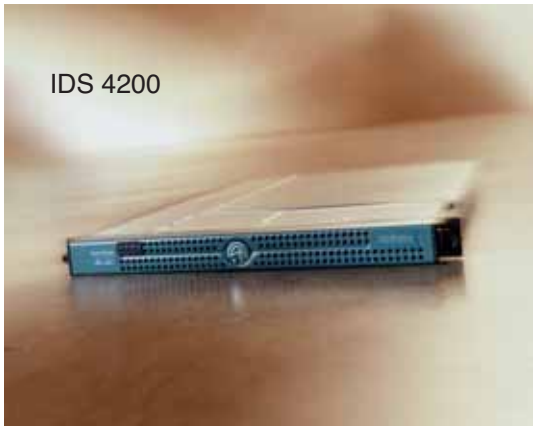
• **Servidores de acceso remoto y gateways Universales**. Familias 2500, AS5300, AS5400 y AS5800, permiten el acceso remoto de usuarios a los recursos centrales de la compañía. Familias de conjuntos de configuración fija y modular, permiten conexión RTB, RDSI básico y RDSI primario.

• **Servidores de túneles VPN**. Cisco Systems permite implementar túneles para despliegue de redes privadas virtuales sobre tres posibles plataformas: Routers Cisco con software para encriptación, Firewalls PIX con las debidas licencias o bien se puede disponer de concentradores de túneles de la familia VPN 3000, que ofrecen mayor densidad de túneles simultáneamente conectados, y mayores funcionalidades tanto en entornos de conexiones remotas de usuarios móviles como de conexiones entre dependencias fijas.

• **Firewalls**. Las funcionalidades de firewall dentro del fabricante Cisco Systems pueden desplegarse bien con routers convencionales con licencia para firewall, o bien con cajas especificadas, desarrolladas en la familia PIX; la conjunción de elementos de ambas familias (routers o PIX) permiten desplegar una arquitectura de seguridad perimetral de altas prestaciones en entornos desde el usuario móvil hasta los recursos centrales de una gran compañía u operador.

• **Sistemas de detección de intrusos**. Complementando las soluciones de Firewalls y Servidores de túneles VPN, Cisco Systems dispone de sistemas de detección de intrusos, familia IDS 4200, capaces de analizar el tráfico en busca de patrones de ataque hasta en conexiones Gigabit Ethernet.





¿Por qué MDtel?

MDtel, no solamente realiza la ingeniería para sus Redes Privadas Virtuales y ofrece los equipos para hacer más fiables sus redes, sino que llega más allá y ha desarrollado un **plan integral de seguridad**, que cubre las siguientes fases:

- Consultoría y análisis de sus redes, estudiando y analizando sus puntos débiles.
- Elaboración de un plan de acción y estudios de los equipos a instalar en sus instalaciones.
- Instalación y puesta en marcha de la electrónica.
- Formación de todas las personas implicadas en el plan de seguridad de la empresa.
- Mantenimiento de todos los equipos y redes.
- Supervisión y análisis continuo de sus redes.

Para llevar a cabo las políticas de seguridad en su compañía, MDtel cuenta con un equipo humano especialmente cualificado, con las certificaciones de los principales fabricantes del mercado, Cisco, 3Com….

Somos un equipo joven y dinámico, con una media de 32 años, y con más del 80 % de la plantilla con más de 10 años de experiencia en el sector.

Soluciones Globales

MDtel Telecomunicaciones
C/Manuel Tovar, 24 Dcha. • 28034 MADRID
Tel.: 91 334 61 00 • Fax: 91 358 52 30
e-mail: clientes@mdtelsa.com • www.mdtelsa.com

MDtel TELECOMUNICACIONES