

Tecnologías de acceso remoto a aplicaciones corporativas y Teletrabajo

José Pastor Mondéjar, 25 de Abril de 2.008

Índice :

- ✓ *Introducción*
- ✓ *Visión de la tecnología actual*
- ✓ *Beneficios / Riesgos*
- ✓ *Tipos de accesos (Vpn IpSec, Citrix, Vpn-SSL,...)*
- ✓ *Casos Prácticos*
- ✓ *Ruegos y preguntas*

*Según IDC → En 2 años, habrán **878 millones de trabajadores móviles** en todo el mundo, conectados con su empresa a través de PDA, equipos portátiles y teléfonos móviles. En resumen, una 1/4 parte de población laboral de todo el mundo.*

Hay que gestionar una rápida transición a un estilo de trabajo que admite personas de todo tipo a las que además de proporcionarles un equipamiento, hay que prestar una asistencia técnica adecuada.

El papel de un ingeniero en una empresa no tecnológica debe ser adaptar la tecnología a las necesidades de negocio de la empresa.

Trabajo móvil: *Existen varias definiciones que varían de acuerdo a la **cantidad de tiempo** que un empleado móvil dedica al trabajo fuera de la oficina y en función de las **ubicaciones** donde se realiza.*

Los empleados móviles son aquellos que trabajan al menos 10 horas por semana fuera de su hogar y de la oficina, por ejemplo, en viajes de negocios, en desplazamiento de viajes o en instalaciones de los clientes y usan conexiones informáticas en línea para realizar su trabajo.

El número de empleados móviles crece con mayor rapidez que los empleados que trabajan desde casa.

Las organizaciones con trabajadores móviles deben invertir en la creación y mantenimiento de unas óptimas relaciones de trabajo.

El aumento puede explicarse básicamente:

- Las tendencias tecnológicas y **culturales** se dirigen a la creciente adopción del trabajo móvil.
- *Las empresas (y las personas) desean **comunicarse** cuando se desplazan.*
- *La movilidad incrementa la **productividad** y la competencia.*
- *Dispositivos móviles, **tecnologías** y servicios de banda ancha bien desarrollados.*
- *La tecnología móvil refuerza la comunicación personal.*
- *La información y el contenido **digital** predomina cada vez más.*

Teletrabajo: *Utilización de las redes de telecomunicación para trabajar desde un lugar fuera de la empresa usando sus sistemas informáticos.*

Aplicaciones corporativas que han sido diseñadas para trabajar en un entorno “**controlado**”, de repente necesitan estar disponibles desde cualquier sitio y a cualquier hora → O se rediseña la aplicación (con el coste asociado) o se utiliza dispositivos que proporcionen la seguridad necesaria

Servicios como el correo, la intranet, la telefonía móvil o el VPN, son **críticos** para la función diaria, y una caída o una pérdida de rendimiento son muy mal acogidos por los usuarios e impactan directamente en la productividad empresarial.

Cada día más, las compañías cuentan con empleados itinerantes y delegaciones remotas que necesitan tener acceso a su información y aplicaciones corporativas desde cualquier lugar y dispositivo. A esto hay que sumarle que la mayoría de las empresas utilizan plataformas heterogéneas (windows, Unix...) lo que dificulta el despliegue de las aplicaciones y la información para todos los usuarios.

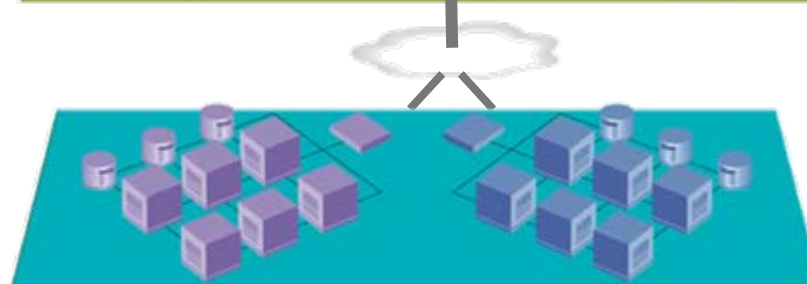
Movilidad del personal



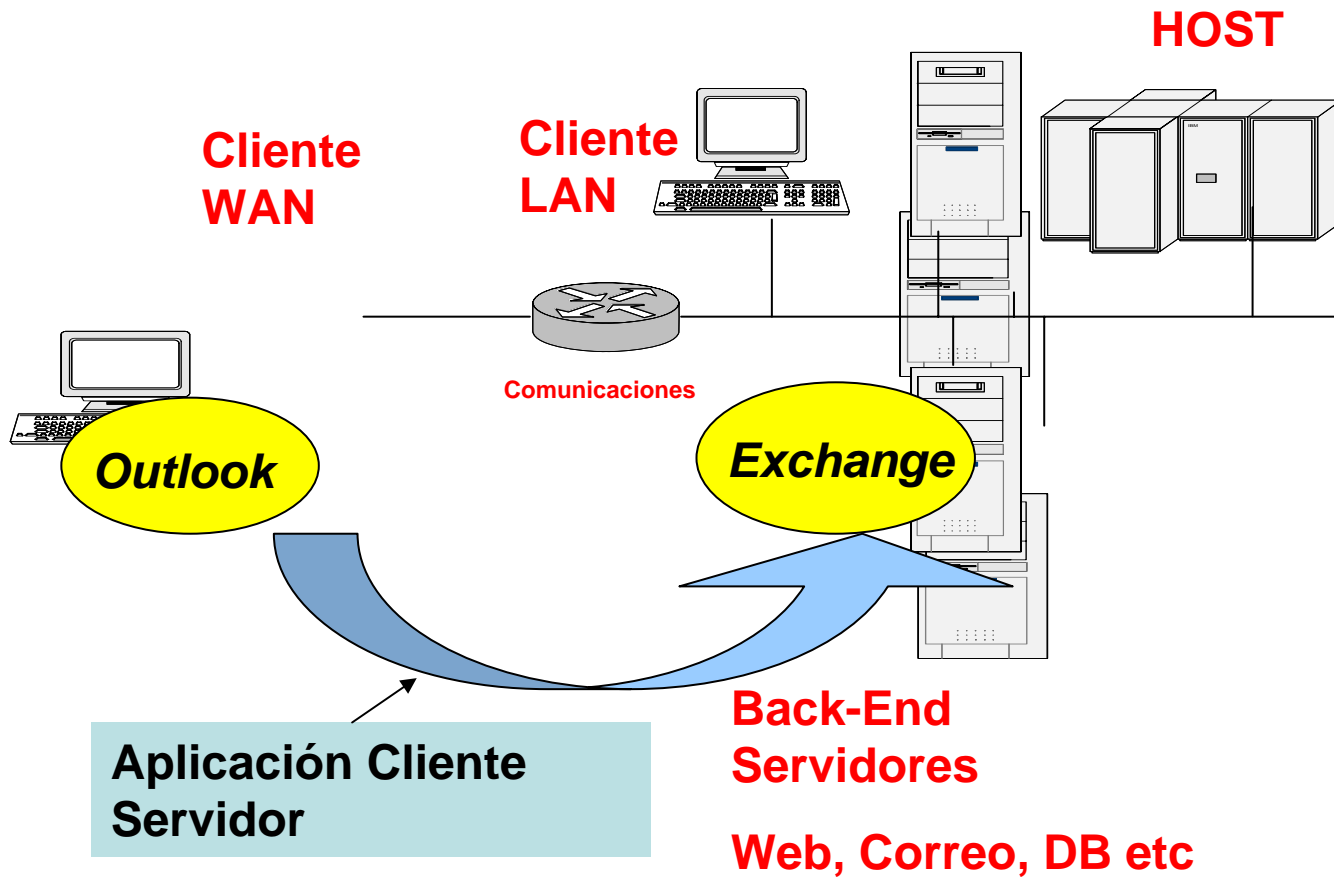
Conectividad de oficinas remotas



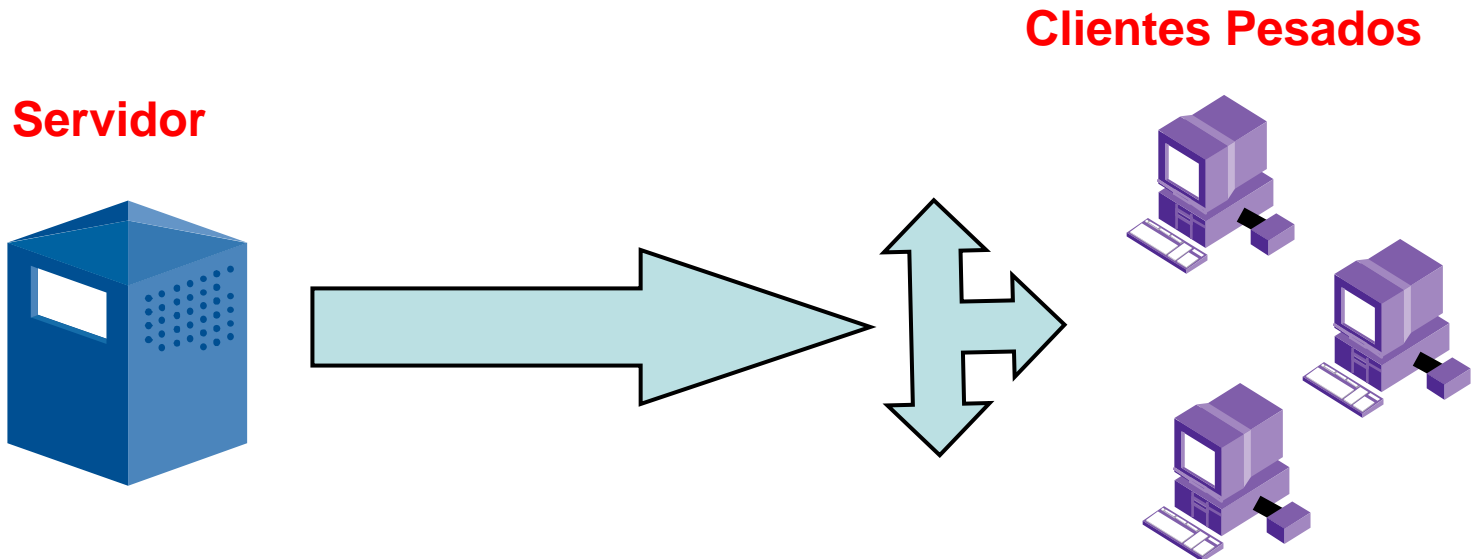
Despliegue de Aplicaciones



Entorno típico cliente/servidor en una organización



Problemática de este tipo de entornos:



- Ancho de Banda: Tráfico denso, creciente y variable
- Instalación de aplicaciones en los puestos clientes
- Mantenimiento / Gestión.

- Beneficios del Teletrabajo / Acceso Remoto:
 - Aumento de la Productividad.
 - Oportunidades de Negocio.
 - Ahorro de Costes (reducción costes fijos).
 - Flexibilidad laboral.
 - Ahorro de tiempo.
 - Aumento de Motivación
 - Retención de personal
 - Conciliación vida familiar y profesional.

- Para que un servicio tenga éxito en el día a día es necesario identificar, analizar y gestionar los Riegos y valorarlos frente a los beneficios:
 - **Seguridad:** Los recursos corporativos se publican en el exterior con información sensible.
 - **Viabilidad** técnica de la solución.
 - **Administración:** Controlar / Auditar accesos.
 - No implicación de los departamentos de negocio.
 - **Facilidad de uso:** Rechazo de los usuarios

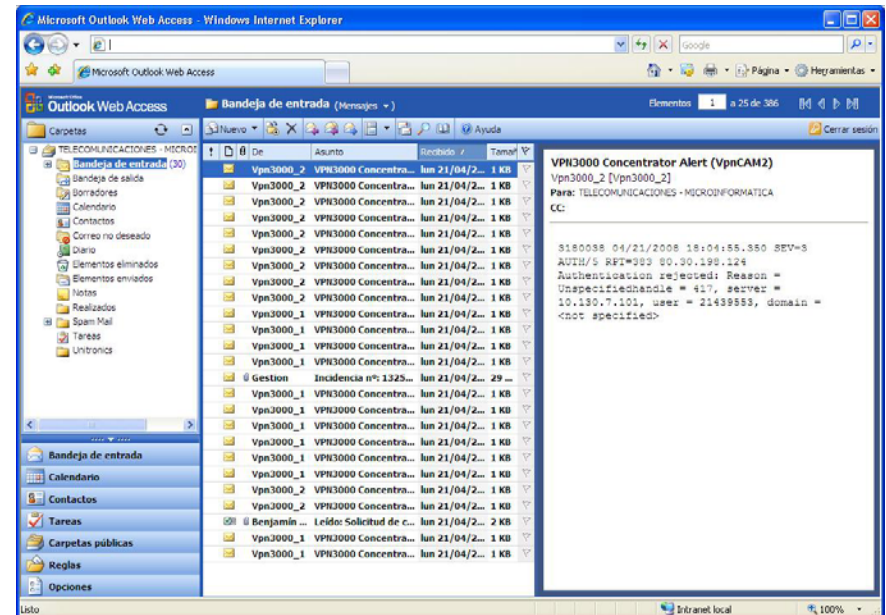
CARACTERÍSTICAS DEL ACCESO REMOTO

- Distintos Perfiles de usuarios:

Se realiza un “PERFILADO” centrado en el usuario: Se categoriza a los usuarios de la empresa, se especifican sus necesidades y entonces se construye un conjunto de soluciones para cada categoría.

- Empresas externas de aplicaciones
- Personal de Sistemas.
- Directivos.
- Desarrolladores
- Usuarios con bajos conocimientos de informática.
- etc...

- Distinto tipo de información:
 - Aplicaciones Web:
 - Correo Web
 - Intranet
 - Listín Corporativo
 - HelpDesk
 - Aplicaciones de Proveedores.
 - Etc..
 - Aplicaciones de “escritorio”:
 - Contabilidad
 - Facturación.
 - Terminal Financiero
 - Acceso a BBDD
 - Aplic. Departamentales.
 - ...



- Necesidades del acceso:
 - Disponibilidad 24x7
 - Desde distintos dispositivos (móviles, navegadores web, servidores, ...)
 - Facilidad de uso.
 - Encriptación de las comunicaciones.
 - Ancho de Banda eficiente.
 - Movilidad.
 - Etc ..

- *Métodos de autenticación:*

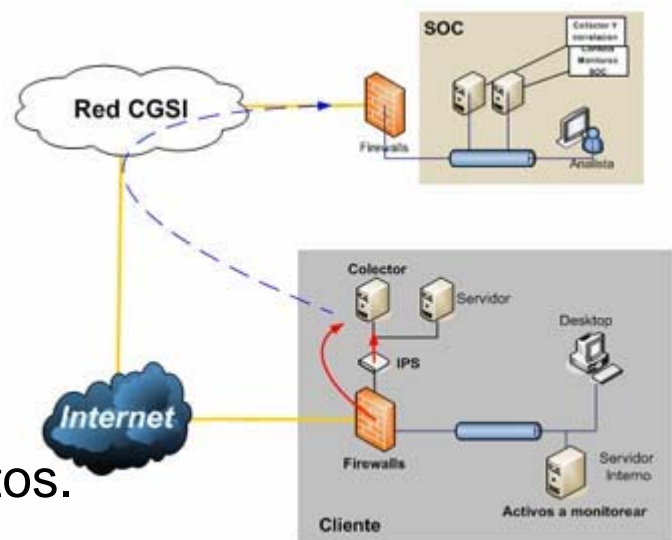
- *Usuario /Contraseña, Passphrase (lo que se)*
- *Token, Token móvil, SoftToken, ... (lo que tengo)*
- *Certificados usuario (lo que tengo)*
- *Tarjeta de claves (lo que tengo)*
- *Biometría. (lo que soy)*
- *Autenticación multifactor.*



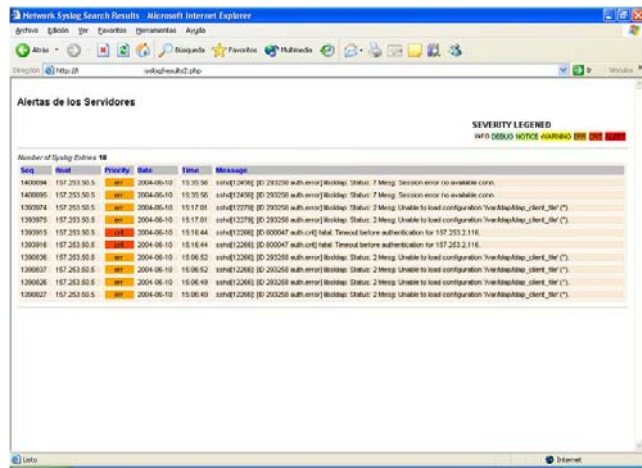
- **Factores a tener en cuenta:**

- *Ha de ser fiable con una probabilidad muy elevada (Tasa de fallos baja,).*
- *Económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto).*
- *Soportar con éxito cierto tipo de ataques.*
- *Ser **aceptable para los usuarios**, que serán al fin y al cabo quienes lo utilicen.*

- Sistema de auditoria:
 - Almacenamiento de Logs.
 - Trazabilidad.
 - Posibilidad de Análisis Forense.
 - Alertas en tiempo real.
 - Consolidación y correlación de eventos.



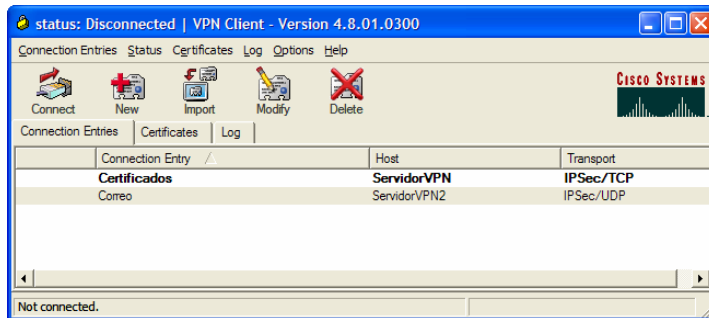
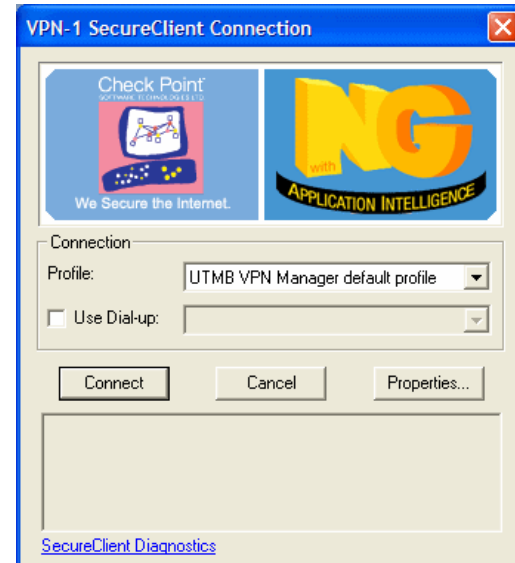
- Administración:
 - ¿Quién lo administra?
 - ¿Cómo se dan de alta, baja?



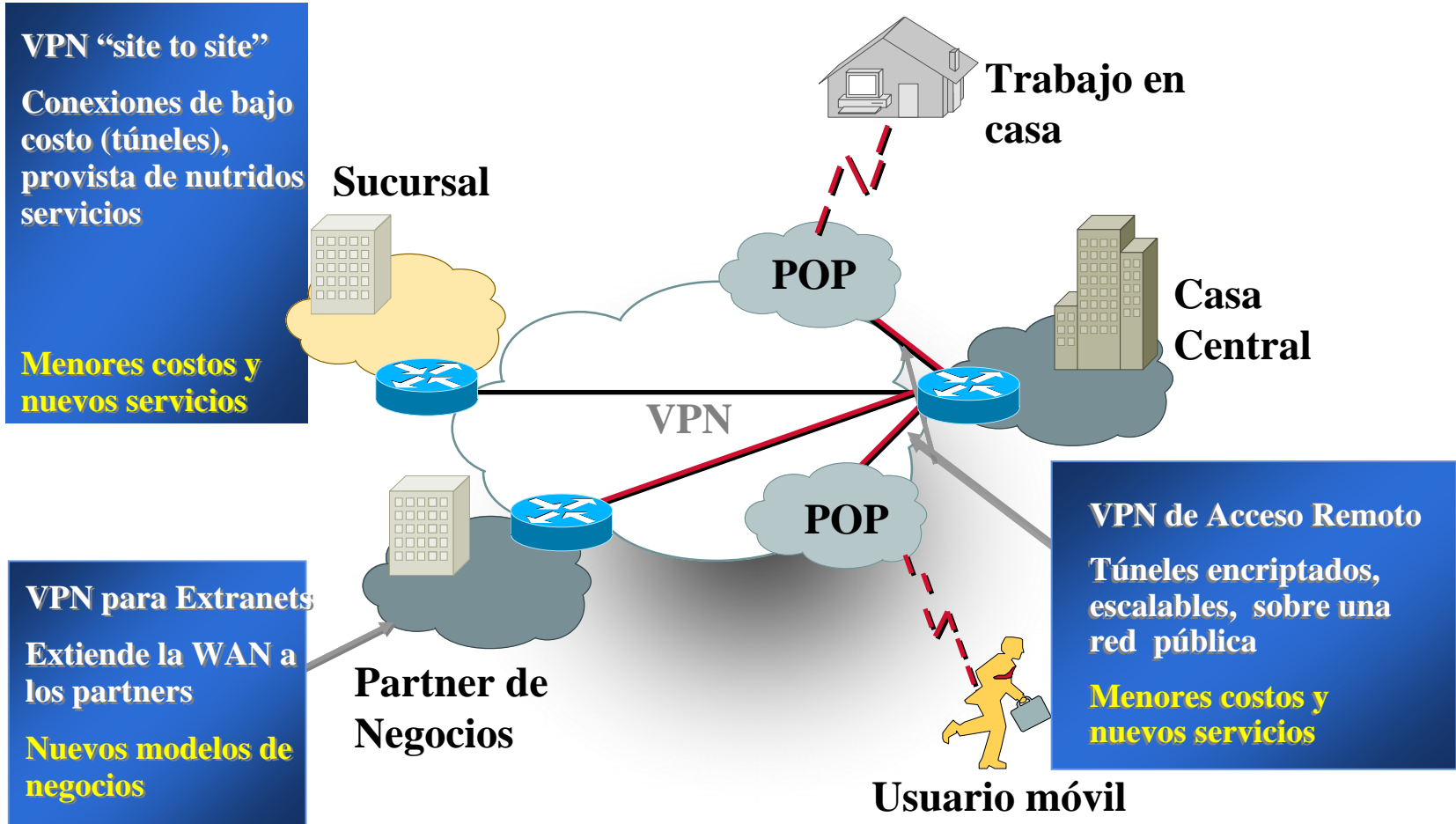
- Seguridad:
 - Establecer controles fuertes en los canales de acceso (control IP, certificados, etc ...)
 - Antivirus usuario / Servidor.
 - Comprobar procesos en ejecución.
 - Parches de Seguridad
 - Securizar el puesto de trabajo remoto.
 - Securizar las comunicaciones.

- Alternativas de mercado:
 - Acceso remoto por VPN (IpSec)
 - Acceso por VPN-SSL
 - Citrix / Terminal Server (seguridad, rendimiento)
 - Tecnologías Móviles:
 - GPRS /UMTS / HSPA
 - BlackBerry

Acceso remoto por VPN (IpSEc)



Esquema de VPNs

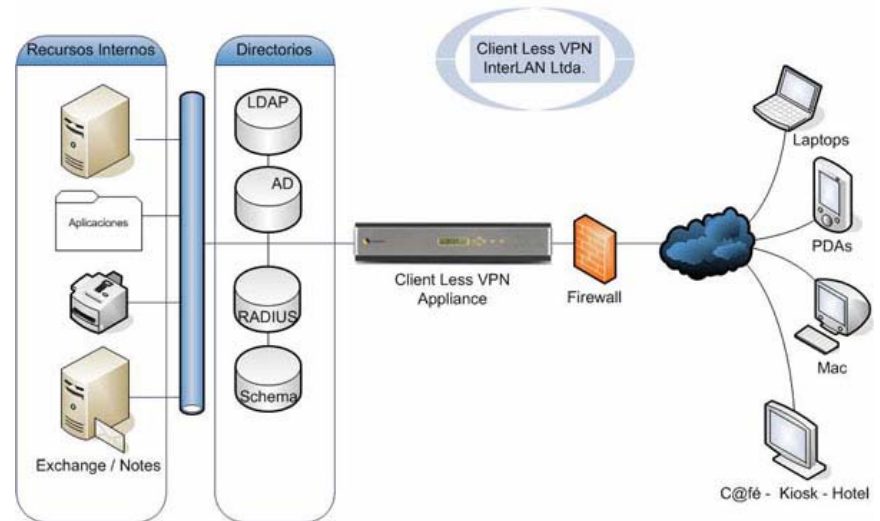
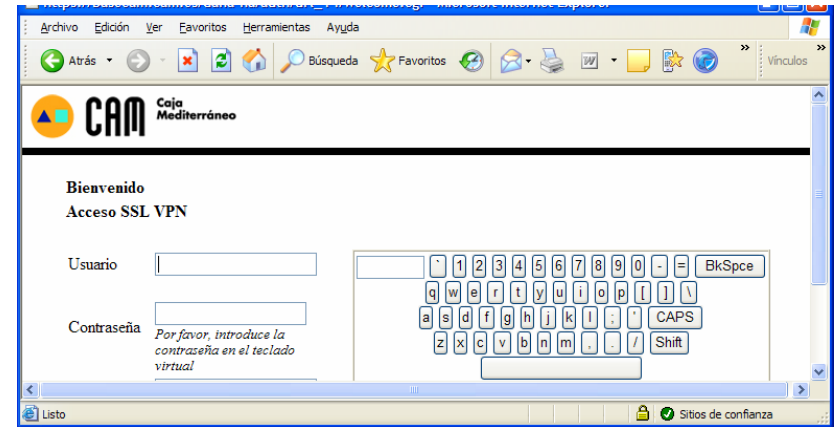
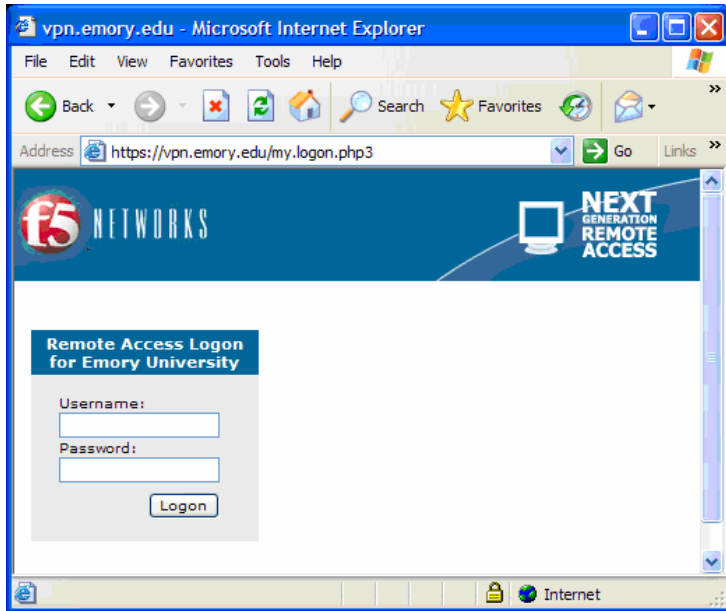


VPN "site to site"
Conexiones de bajo costo (túneles), provista de nutridos servicios
Menores costos y nuevos servicios

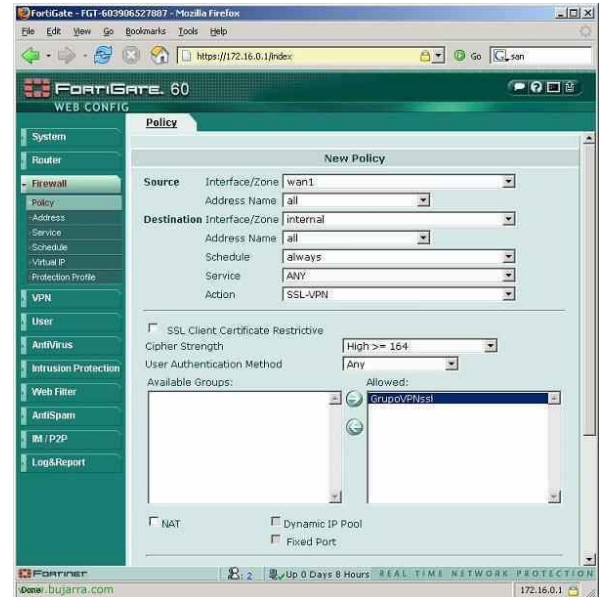
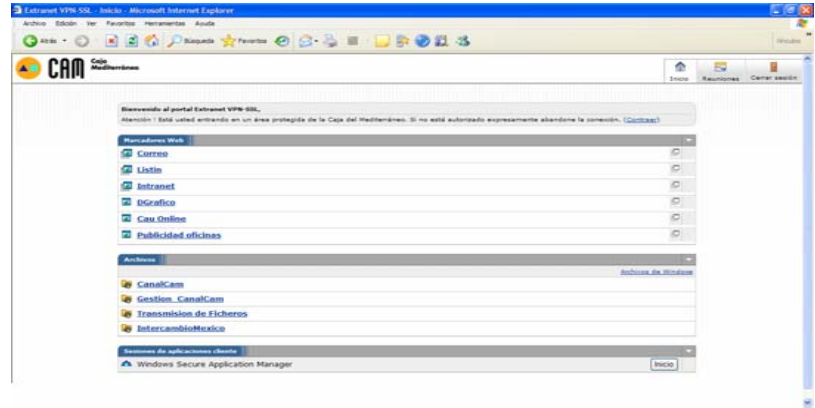
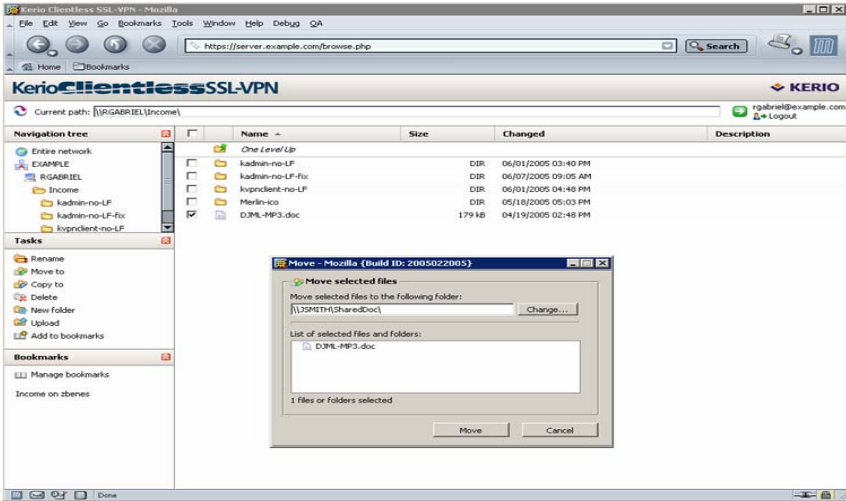
VPN para Extranets
Extiende la WAN a los partners
Nuevos modelos de negocios

VPN de Acceso Remoto
Túneles encriptados, escalables, sobre una red pública
Menores costos y nuevos servicios

- Acceso por VPN-SSL

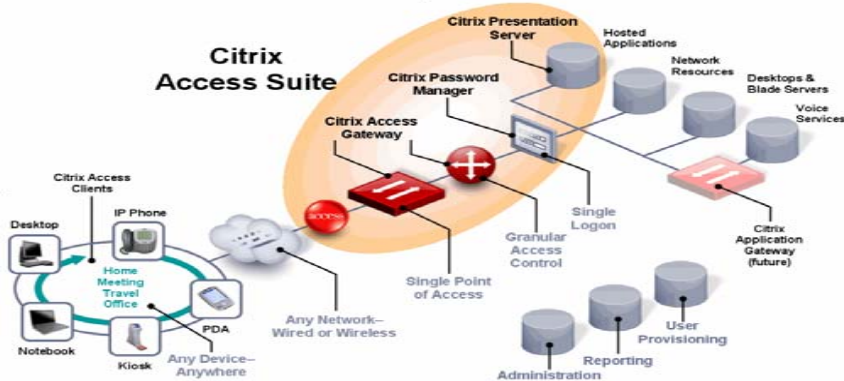


Tecnologías de acceso remoto a aplicaciones corporativas y Teletrabajo



Tecnologías de acceso remoto a aplicaciones corporativas y Teletrabajo

CITRIX®



Aplica

Program Neighborhood CITRIX

Windows

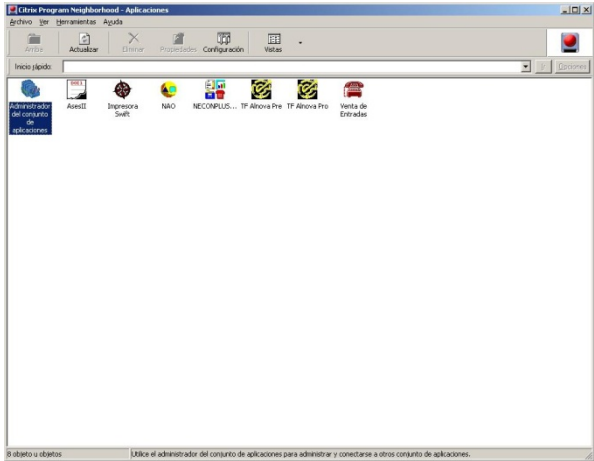
Nombre de usuario:

Contraseña:

Dominio:

Guardar contraseña

Aceptar Cancelar



Client File Security

CITRIX

A server application is trying to access your local client files.

What access should be allowed?

- No Access
- Read Access
- Full Access

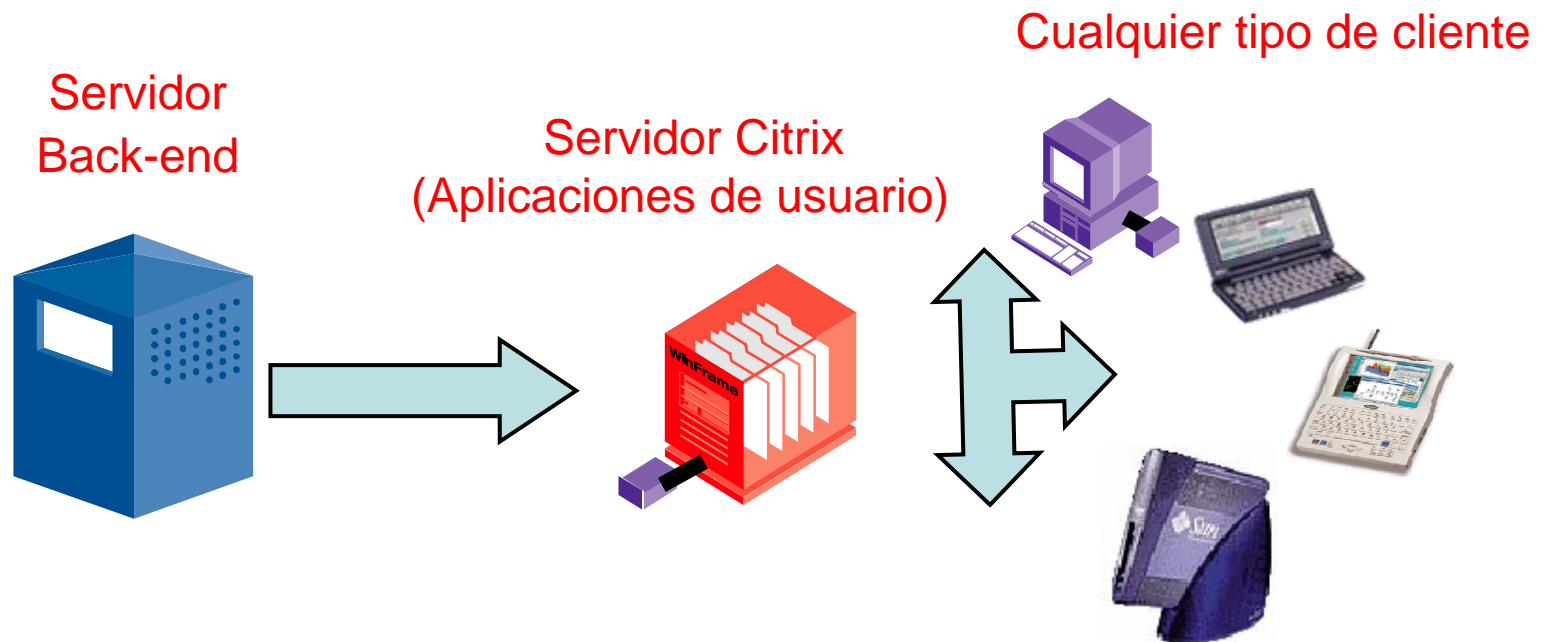
Do you want to be asked again?

- Always ask me
- Never ask me again for this site
- Never ask me again

OK Cancel



¿Cómo funciona con Citrix?

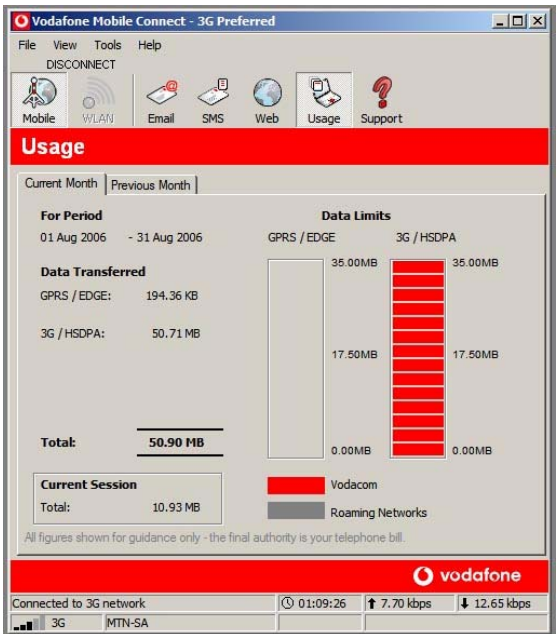


- Tráfico denso entre Servidores (dentro del CPD)
- Tráfico ligero entre Servidor Citrix y Clientes
- Instalación de aplicaciones centralizada

Beneficios generales (Citrix)

- Gestiona las aplicaciones empresariales desde una ubicación central y ofrece acceso “on demand” a ellas desde cualquier lugar.
- Las aplicaciones se distribuyen mucho más rápidamente con Presentation Server que instalándolas en los equipos de sobremesa.
- Los usuarios disfrutan de un rendimiento muy superior de las aplicaciones a través de la red, sobre todo los que trabajan a distancia a través de redes lentas.
- Todas las funciones de las aplicaciones están disponibles con plena seguridad a través de redes sin cables, y se accede a ellas mediante navegadores web estándar.

- Tecnologías Móviles:
GPRS /UMTS /BlackBerry





Activación de empresa

Correo electrónico: @cam.es

Contraseña:

Dirección de servidor de activación:

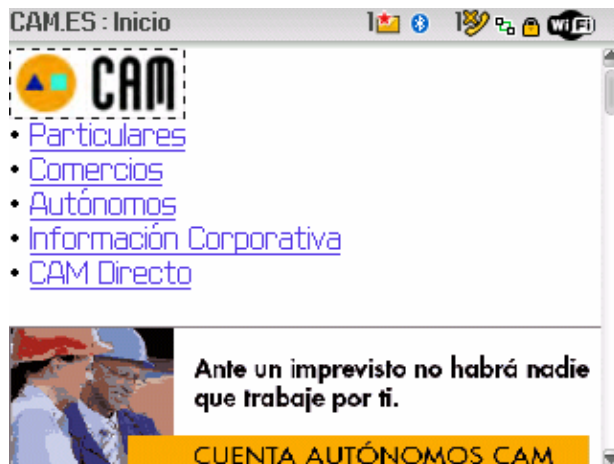
PIN: 00001507

Estado: activado para 21 Abr 2008

11:22 MAR, 22 ABR WiFi GPRS Y...
EMPRESA - Trabajo

Mar, 22 Abr, 2008

- 11:15 Anna Sant RE: licencias equi...
- 11:09 SYSMAN - T... RE: Logran salta...
- 11:04 SYSMAN - T... Me extraña que...
- 10:26 LOPEZ TRIGU... RE: Logran salta...
- 10:24 AGUILERA SA... RE: Logran salta...
- 10:23 PROSOL - OR... RV: Logran salta...
- 10:20 SOLANO GAR... RV: Resultados d...
- 09:39 CAPARROS A... RE: Yo, como sie...



Activation

Welcome to Mobile Desktop, please enter your code to activate the software. For a free trial or to buy, use the menu or visit www.rovemobile.com.

Device ID: 00001507

Version: 2.11

Activation Code: |

Activate Request Trial Buy

Opciones - Avanzadas

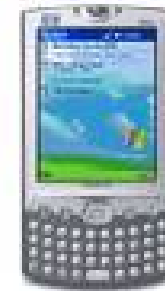
Activación de empresa

- Aplicaciones
- Difusión celular
- Explorador
- GPS
- Inserción del explorador
- Libro de servicios
- Servicios predeterminados
- Tabla de enrutamiento de host
- Tarjeta SIM

- **Securización:**
 - Identificar vulnerabilidades en cada área.
 - Poner en marcha medidas para cerrar vulnerabilidades.
 - Auditar la ejecución de las medidas.
 - Periódicamente, Reevaluar los factores de vulnerabilidad y riesgos (particularmente cuando hay cambios en el acceso).
 - Test de intrusión / Vulnerabilidades

Movilidad

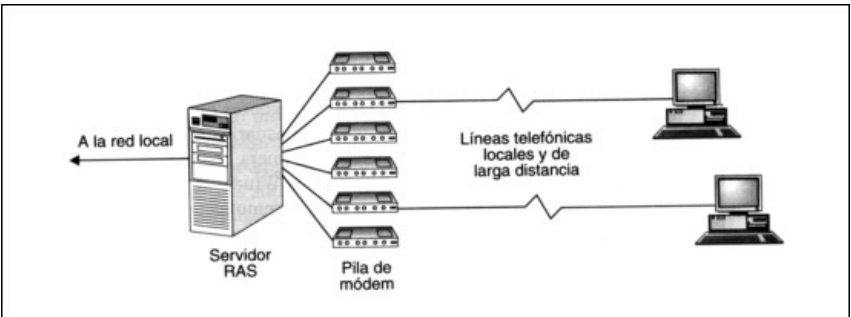
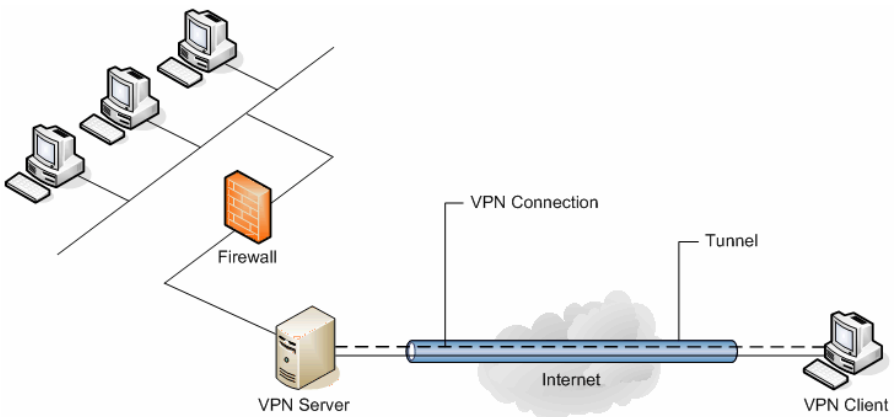
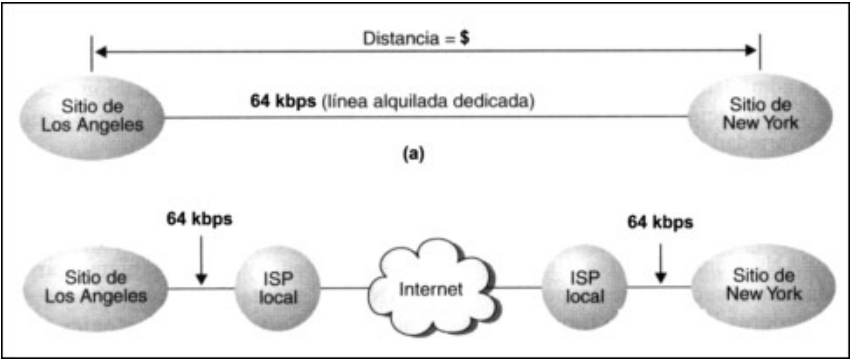
- **Telefonía Corporativa móvil dual IP / GSM-3G**
 - Mensajería Instantánea y servicios de presencia y localización
 - Voz, Videoconferencia y Colaboración
 - Email y Aplicaciones de ofimática
 - Acceso y compartición de ficheros
 - Acceso a Internet/Intranet
 - Aplicaciones de negocio: CRM, ERP, Riesgos, Morosidad



Ventajas de acceso remoto VPN

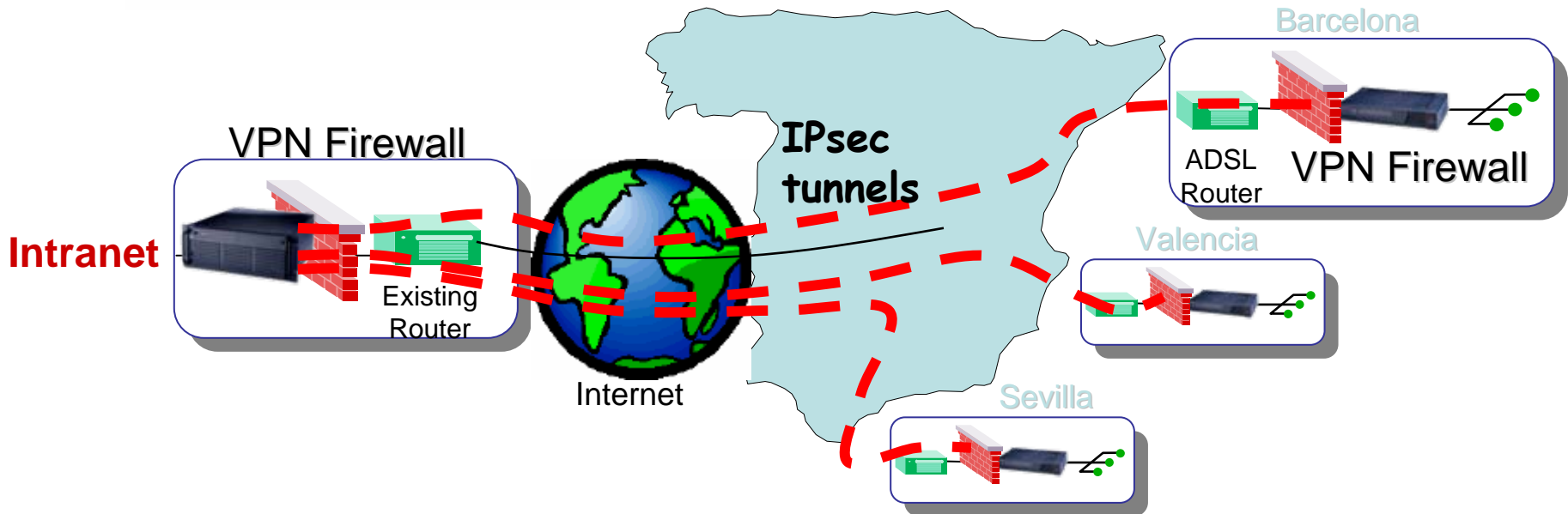
- Coste
- Escalabilidad
- Compatibilidad
- Administración centralizada
- Optimización del Ancho de Banda.
- Facilidad de uso

Acceso VPN



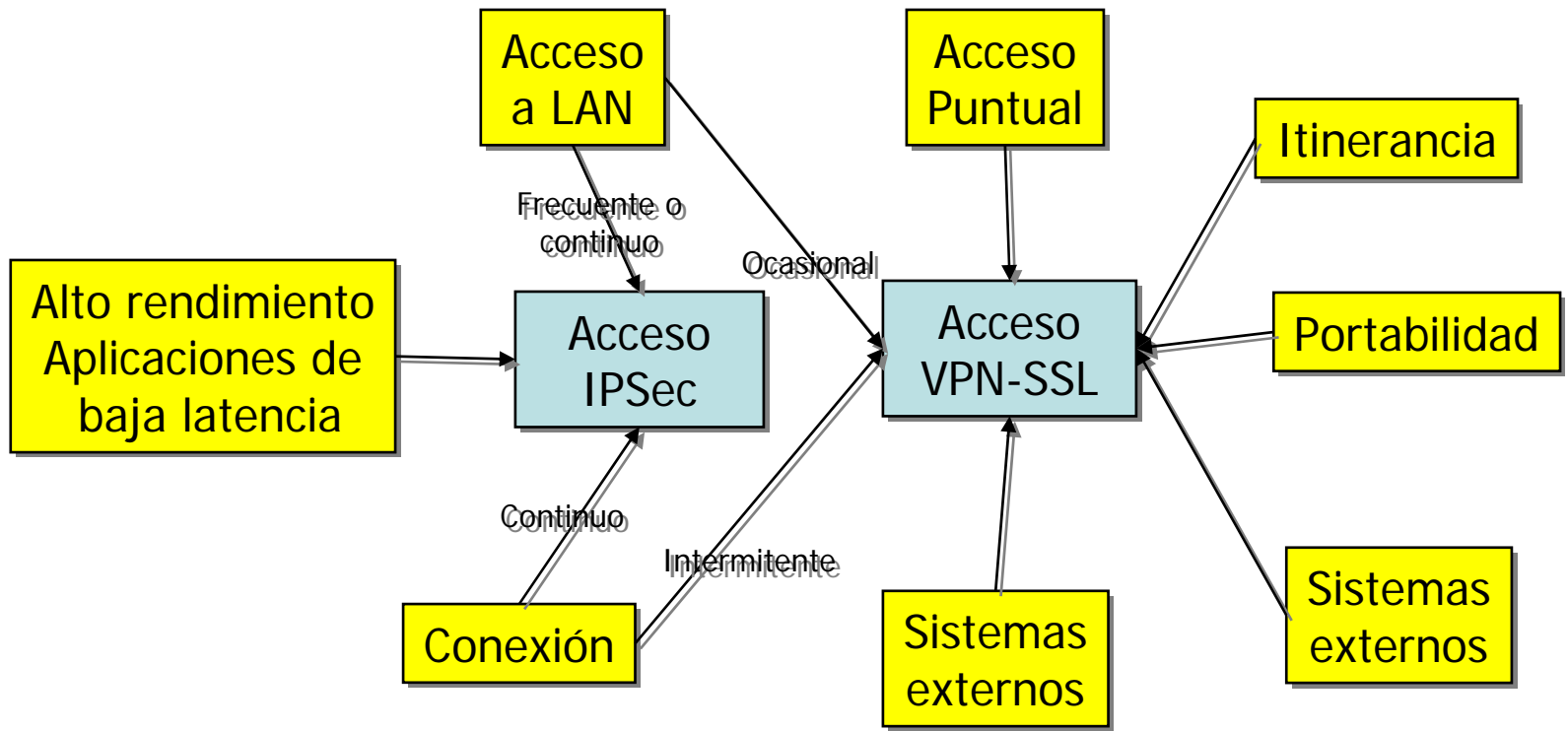
- Túnel LanToLan
 - Interconexión de redes.
 - Coste frente a líneas dedicadas.
 - Oficinas remotas.
- Cliente VPN
 - Acceso a recursos internos.
 - Acceso no dedicado.





- Las delegaciones se interconectan al resto de la Intranet a través de túneles IPsec sobre acceso ADSL
 - **Sustitución de las antiguas y caras líneas dedicadas!!**
- Los firewalls de las delegaciones sólo admiten tráfico proveniente de la intranet (con túneles Ipsec), nunca del resto de Internet
 - A pesar de tener conectividad directa a Internet mediante el ISP local

Selección del tipo de acceso: VPN IpSec vs VPN-SSL



Ventajas IpSec frente a VPN-SSL

- El cliente provee la seguridad y encriptación más elevada.
- Conexión transparente
- Acceso a aplicaciones con sus interfaces nativas.
- Indicada para acceso continuo.
- Se utiliza con el tráfico IP unicast.
- Acceso a la red del cliente.

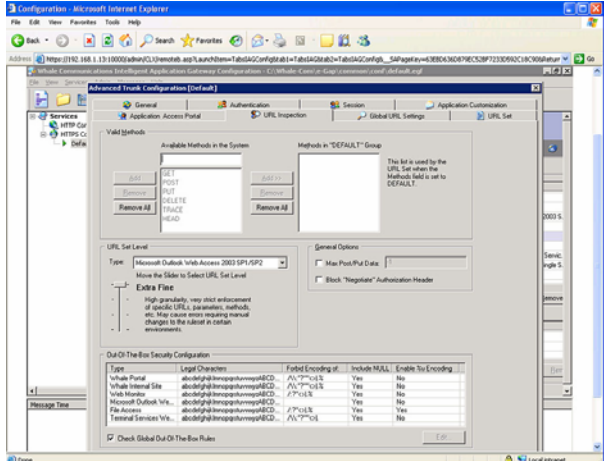
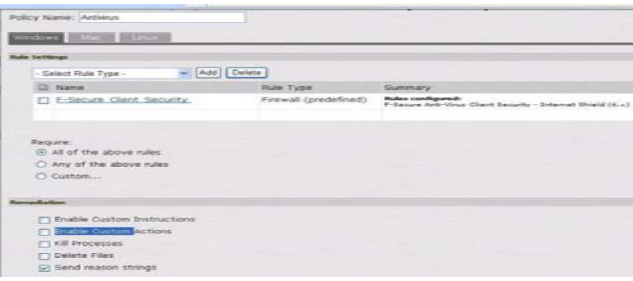
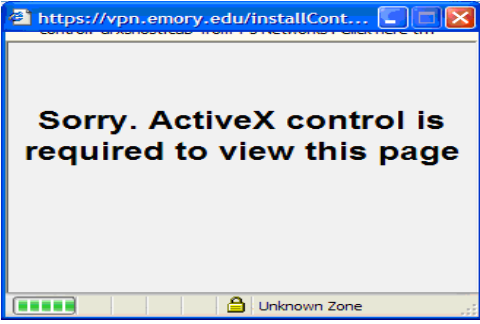
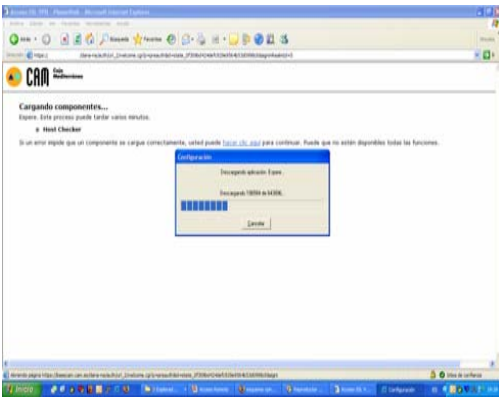
Ventajas VPN-SSL frente a IpSec

- Los privilegios de acceso se dan en función quien accede y desde dónde accede.
- No necesita instalación y mantenimiento en el equipo cliente.
- No necesita configuración por parte del cliente.
- Disponible en cualquier lugar con acceso a Internet (hoteles, empresas, PDAs,...)
- Seguridad y autenticación del cliente vía applets de Java y ActiveX
- Mayor fiabilidad en la conexión (no se desconecta la sesión por cortes intermitentes)
- Control granular de acceso (URL, fichero, servidor ...)
- Protege tráfico de aplicación (reescritura de código http)

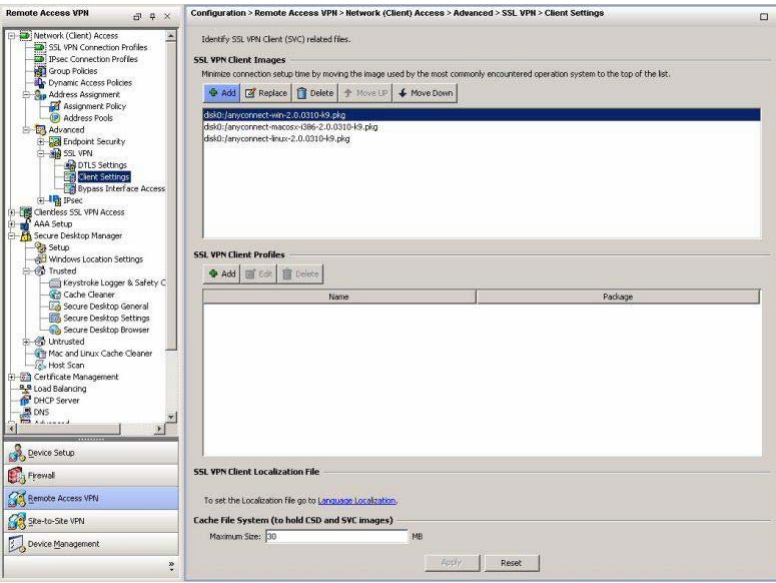
Otras Características de la solución de acceso remoto.

- Host Checker:
 - Comprobación del software instalado.
 - Antivirus.
 - Firewall Personal.
 - Malware
 - Permitir únicamente determinados ejecutables.
- Secure Meeting: Reuniones de soporte, presentaciones, integración con Outlook
- Permitir escritorio virtual para ejecutar únicamente las aplicaciones permitidas.
- Ayuda integrada en el equipo.
- Forzar la contraseña a x dígitos.
- Personalización de página inicio
- Reescritura de código http.
- Autenticación integrada con Directorio Corporativo, correo OWA, SharePoint, etc...

• Securización del puesto de trabajo



Each trunk definition in IAG 2007 has a specific set of properties that define the overall behavior of the trunk. Admins can be very specific when it comes to securing Web-based traffic by managing individual transactions in the traffic stream based on user rights and endpoint compliance.



Muchas gracias