MATERIAL DIDACTICO

Firewalls y Proxis: Seguridad en Redes

y Telecomunicaciones, Seguridad en

Sistemas inalámbricos

16 al 20 de Abril de 2007

CC-04

Seguridad Administrada

Presentación
Diplomado de Seguridad UNAM

Parte I

Abril, 2007

mexis
Seguridad Administrada

Agenda

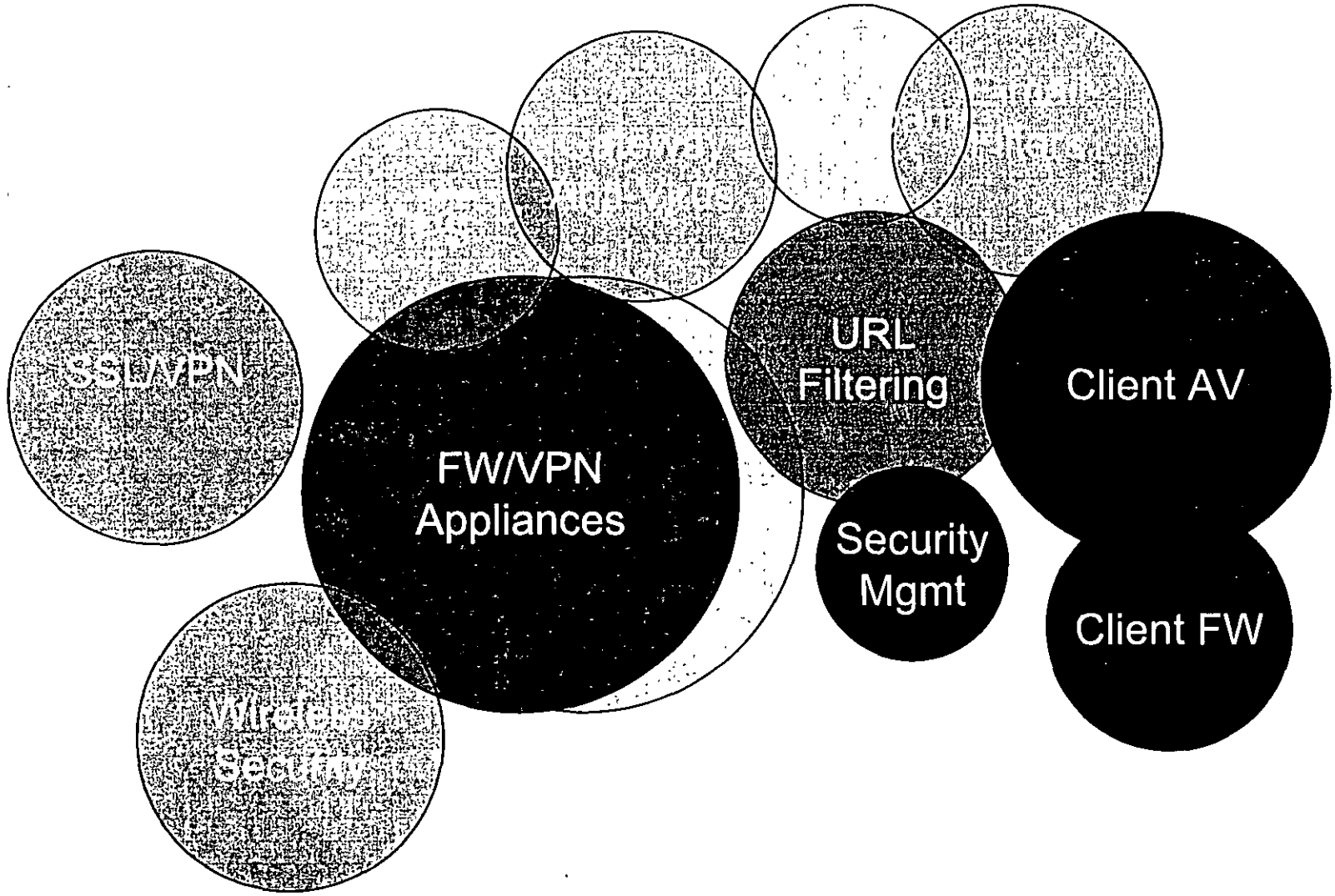
1. Mercado
2. Seguridad Tendencias
3. Seguridad Perimetral y WAN (VPN´s)
4. Servicios de Seguridad Administrada MEXIS (SOC)
5. Acuerdo de Nivel de Servicio

Seguridad Administrada

Mercado

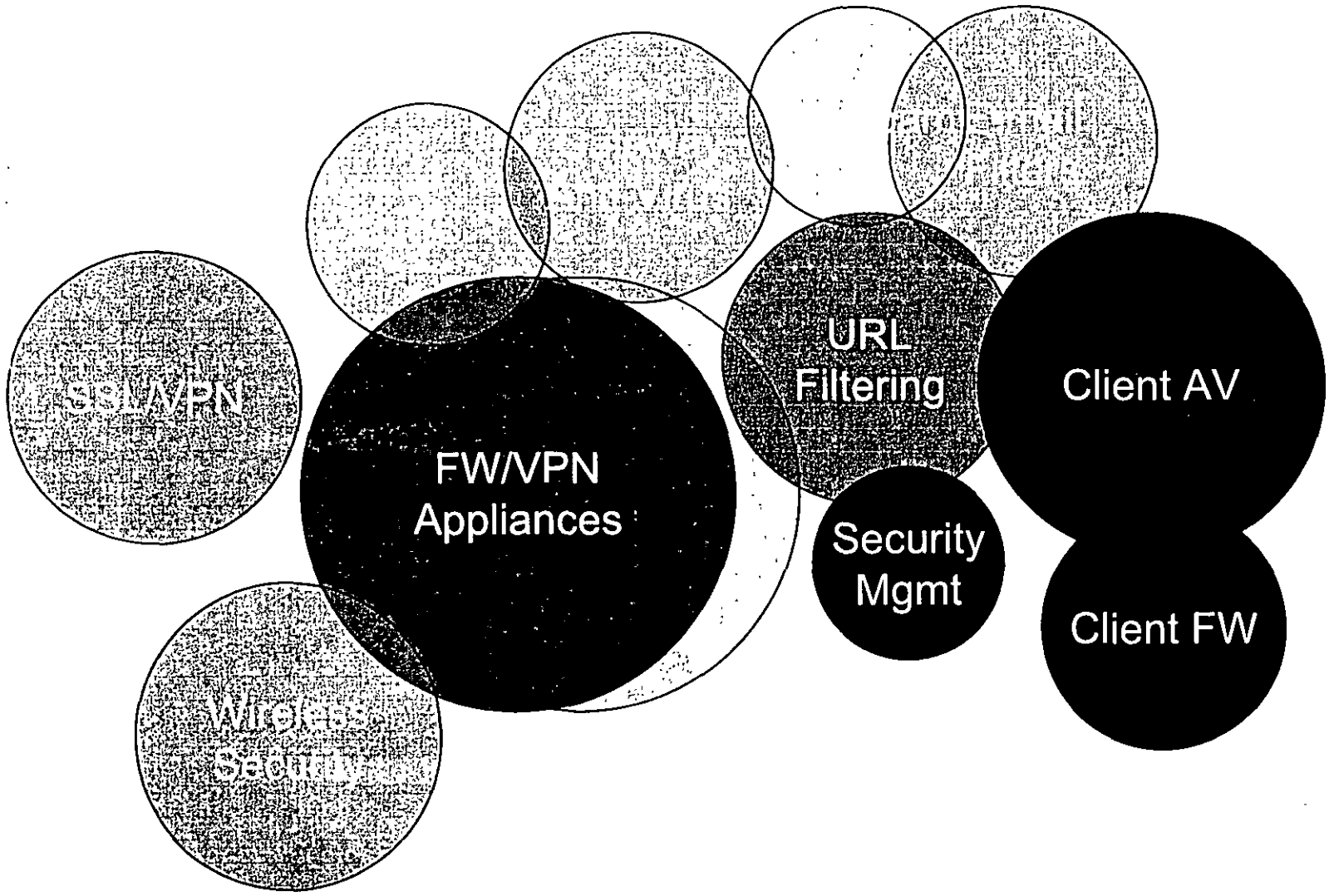
Seguridad Administrada

Antes



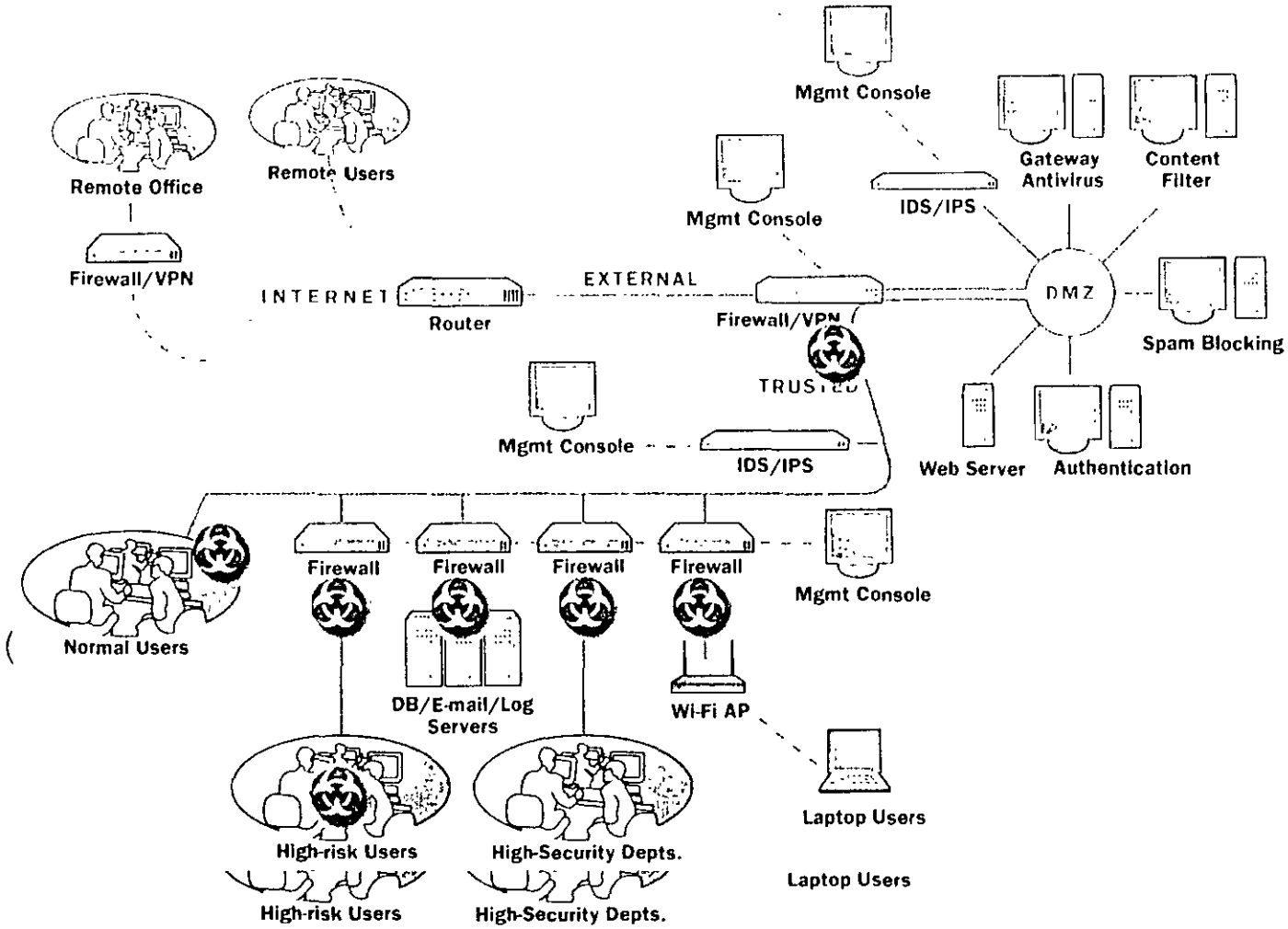
Seguridad Administrada

Evolución



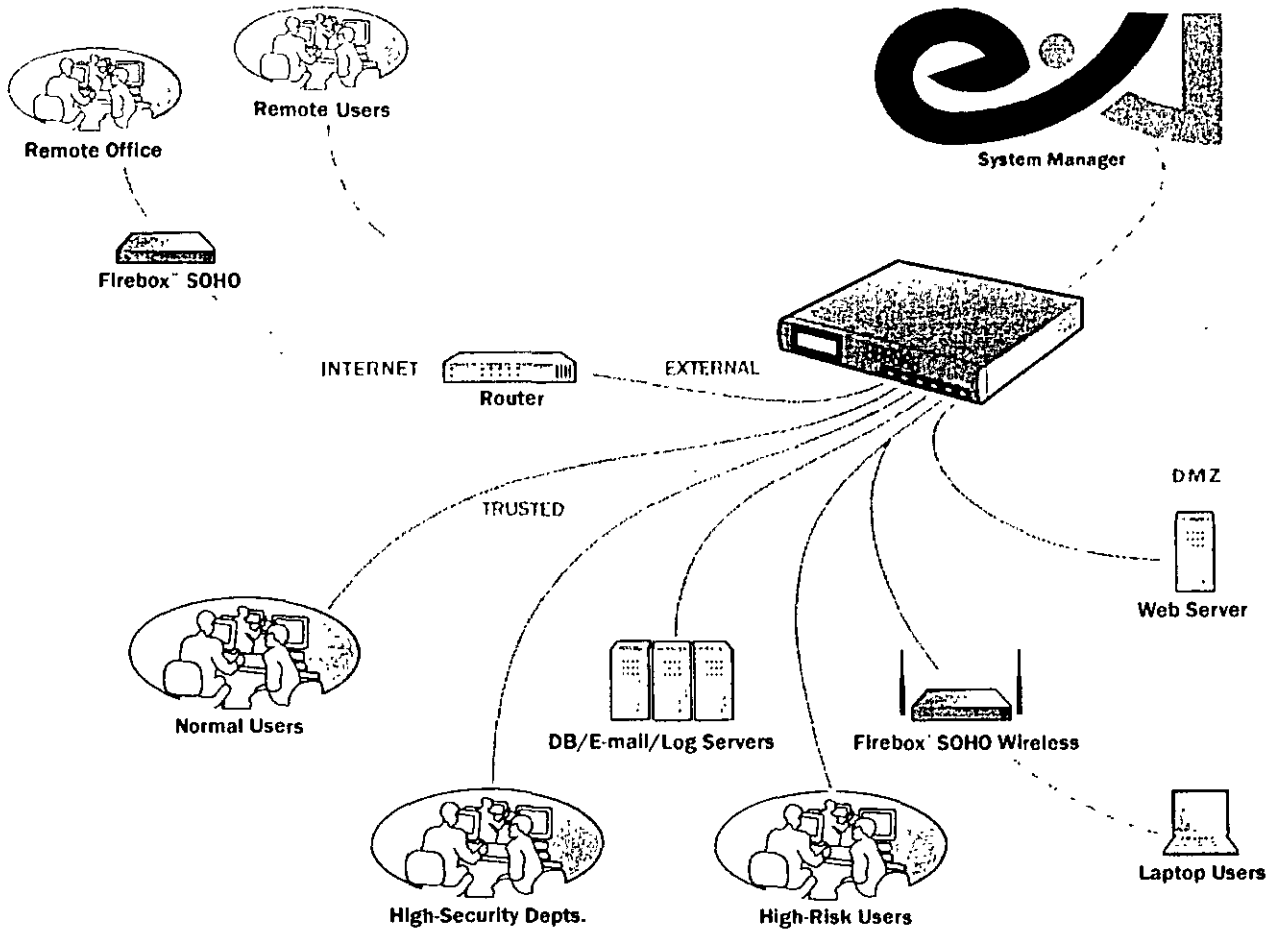
Seguridad Administrada

Arquitectura Tradicional de Red



Seguridad Administrada

Arquitectura con Seguridad Integral



Seguridad Tendencias

Seguridad Administrada

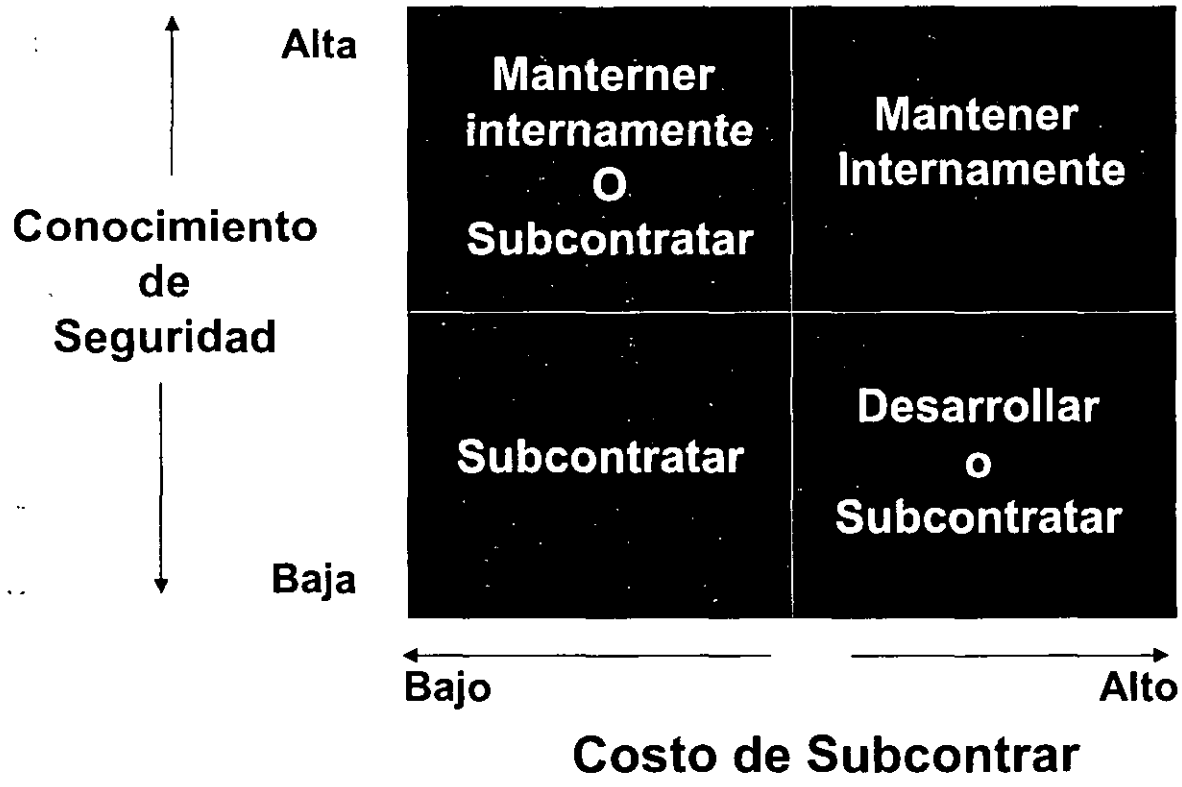
Hacerlo yo o un Tercero?

El usuario final tiene que preguntarse:

- ¿Estare realmente seguro al comprar e instalar los equipos Firewalls por mi mismo?
- ¿Puedo contar con los recursos económicos?
- ¿Puedo contar con los recursos humanos?
- ¿Puedo contar con los recursos de infraestructura?
- ¿Puedo contar con los recursos de tiempo para administrar la infraestructura?

Seguridad Administrada

¿Seguridad es mi núcleo de negocio?



Fuente: Gartner Group White Paper

Seguridad Administrada

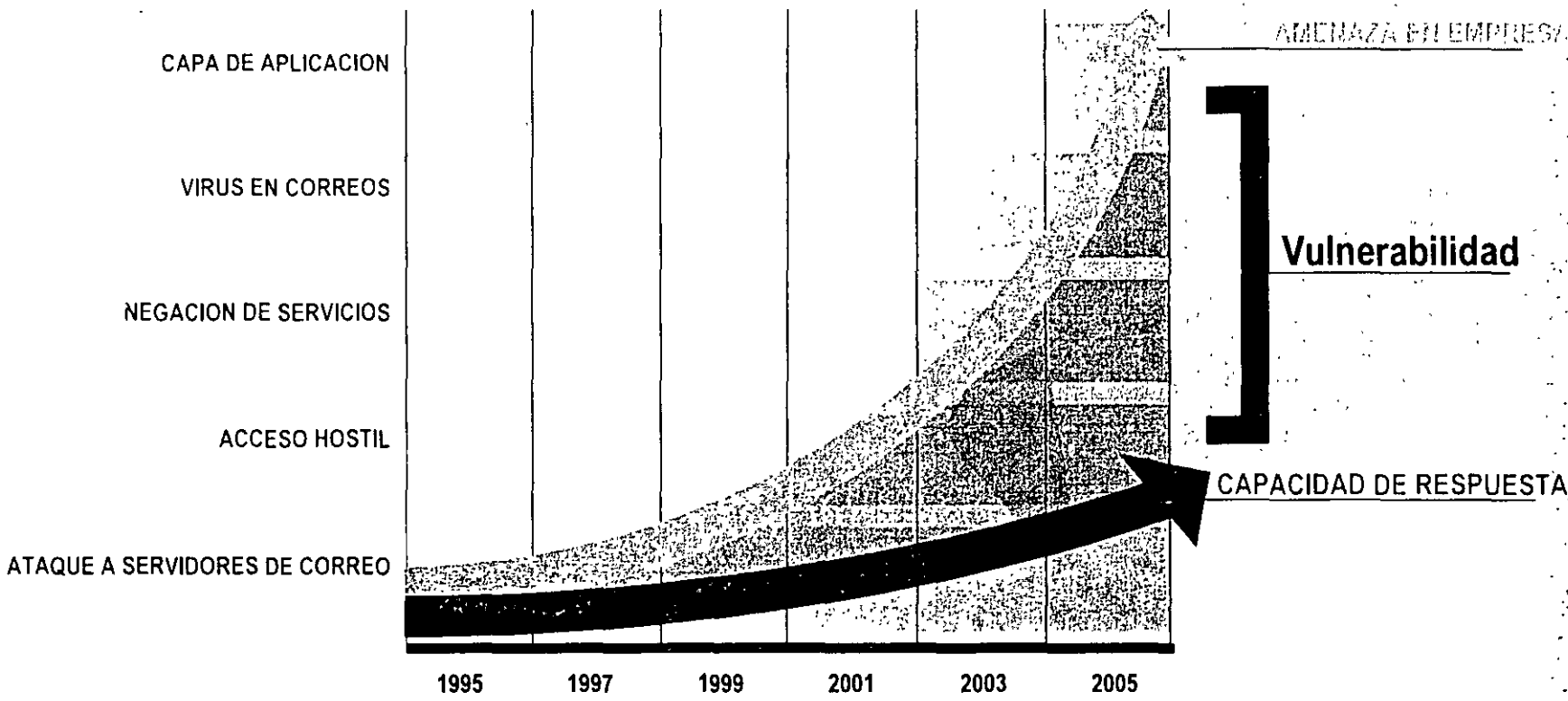
¿Qué es Seguridad Administrada (MSSP)?

- Proveer un servicio de monitoreo y administración de dispositivos y sistemas de seguridad
- Los servicios más comunes son:
  - Dimensionamiento de Seguridad
  - Administración de Firewall (IPS, Antivirus Gateway, Antispam Gateways, etc.)
  - Detección de Intrusos
  - VPN's
  - Escaneo de Vulnerabilidades
  - Administración de Antivirus
- Cuentan con Centros de Operación de Seguridad (SOC) de alta disponibilidad para proveer servicios "24x7xSiempre" para incrementar los tiempos de reacción ante las amenazas
- Determinan Acuerdos de Nivel de Servicio para definir tiempos de respuesta

Seguridad Administrada

THE THREAT

LA CRECIENTE BRECHA DE VULNERABILIDAD



Seguridad Administrada

Seguridad...

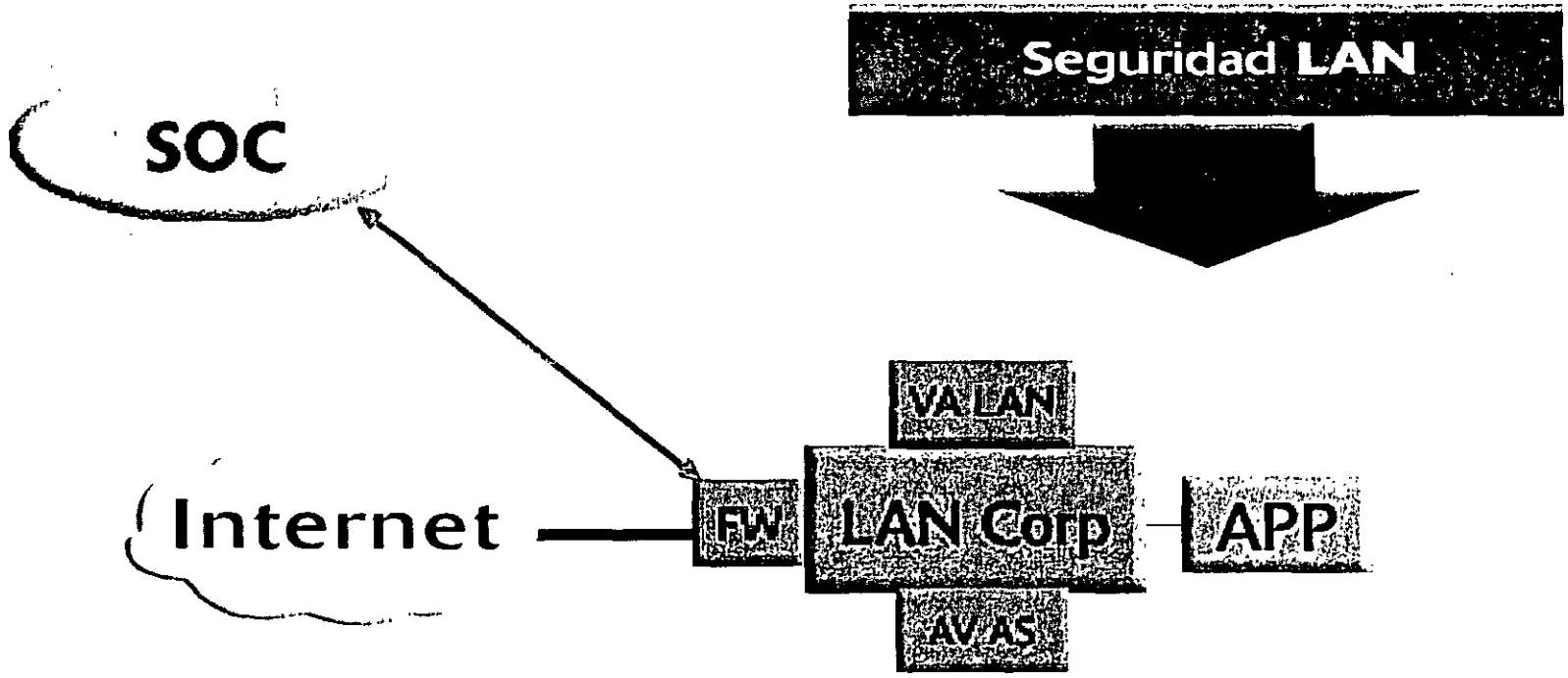
Continuidad de Negocio...

Seguridad Administrada

Seguridad Perimetral y WAN (VPN´s)

Seguridad Administrada

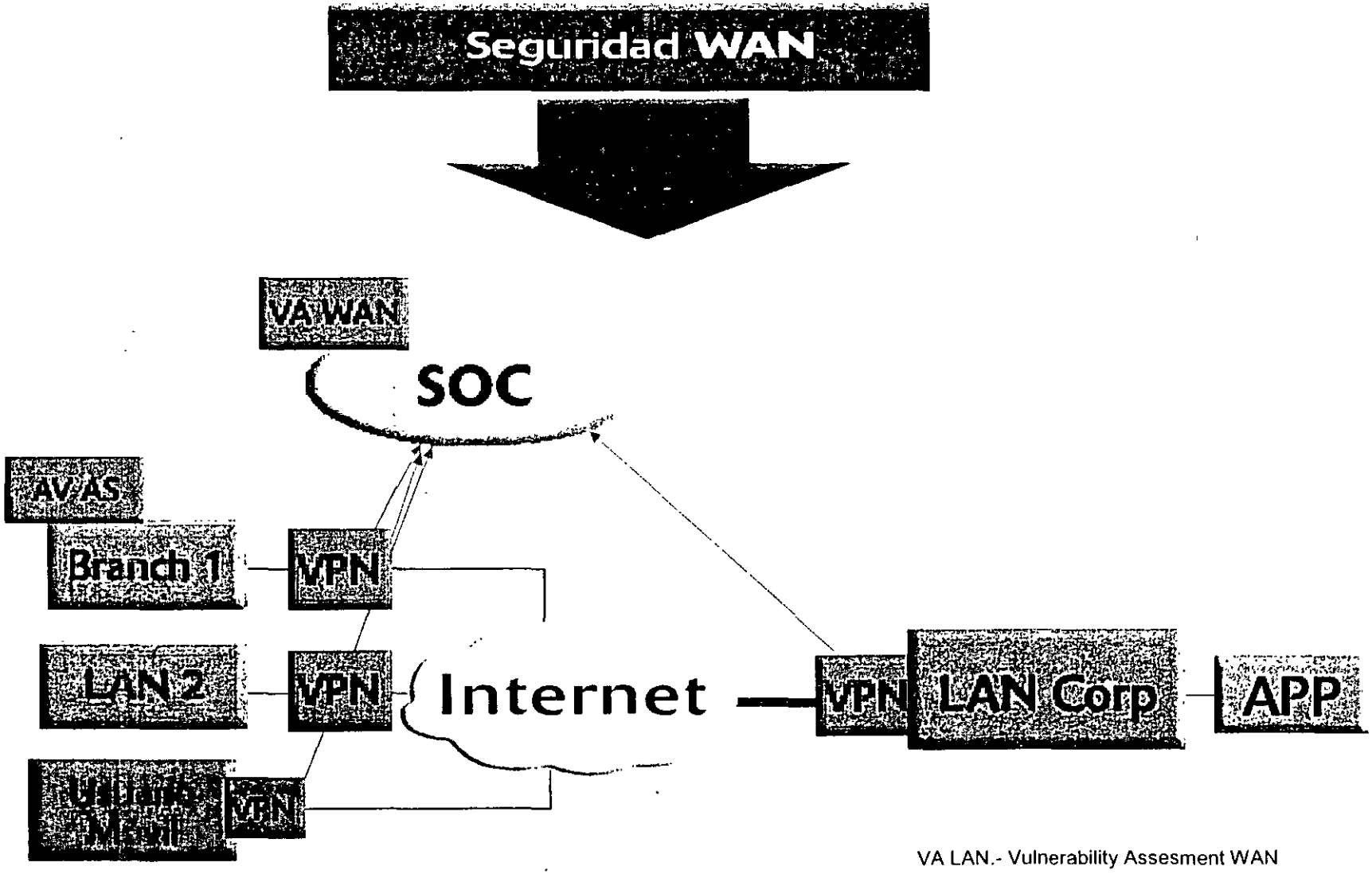
SEGURIDAD PERIMETRAL



VA LAN.- Vulnerability Assesment LAN
AV AS.- Antivirus Antispam

Seguridad Administrada

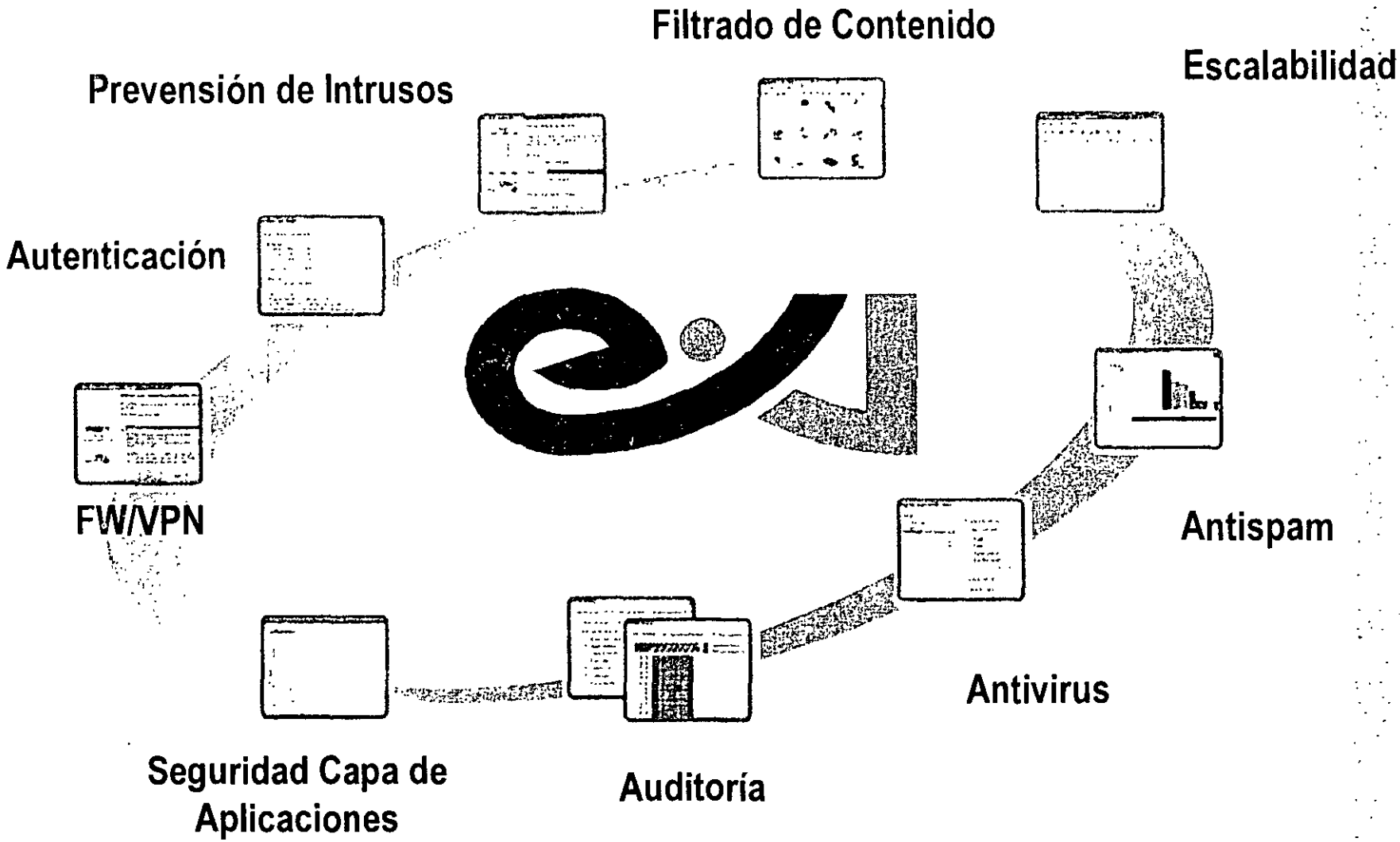
SEGURIDAD WAN



VA LAN.- Vulnerability Assesment WAN
AV AS.- Antivirus Antispam

Seguridad Administrada

Integracion Total



Seguridad Administrada

Servicios de Seguridad Administrada MEXIS (SOC)

Seguridad Administrada

Servicios de Seguridad

- **Actualización de patrones, versiones y up grades** se realizan determinadas modificaciones y actualizaciones periódicas, con el fin de obtener un mejor desempeño.

- **Altas, Bajas y cambios** se solicitan al centro de contacto con el cliente y los realizan técnicos capacitados a través del levantamiento de casos numerados para ser rastreados hasta su resolución y cierre.

Seguridad Administrada

Servicios de Seguridad

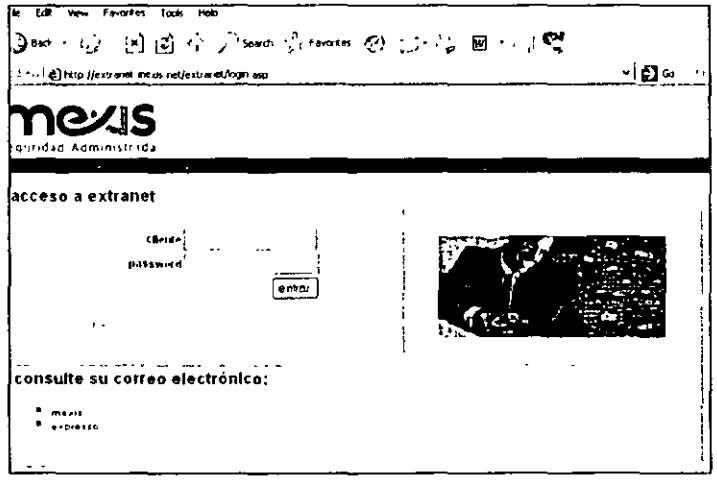
- **Administración de Vulnerabilidades** la red es examinada de manera preventiva para detectar puntos de exposición. Se identifican y eliminan los puntos débiles susceptibles de comprometer la confidencialidad, integridad o disponibilidad de la información.

Seguridad Administrada

Reportes

- **Monitoreo, Alertas y Reportes** son generados diariamente y los puede acceder en línea en tiempo real y desde cualquier lugar a través de la extranet.

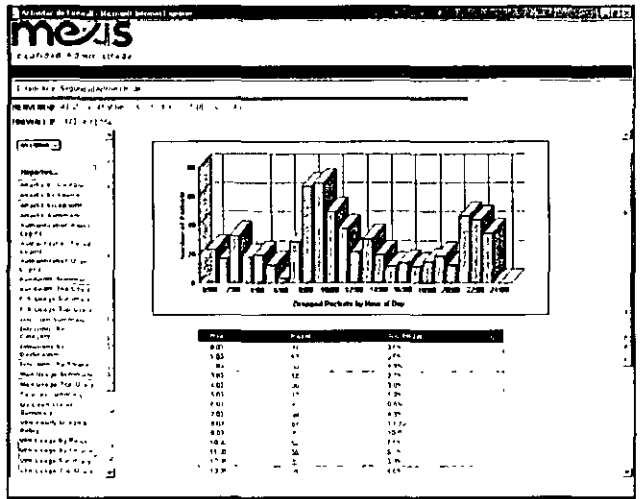
- Usted podrá visualizar las estadísticas, comportamientos, eventos y tendencias de las actividades que se realizaron en el firewall.



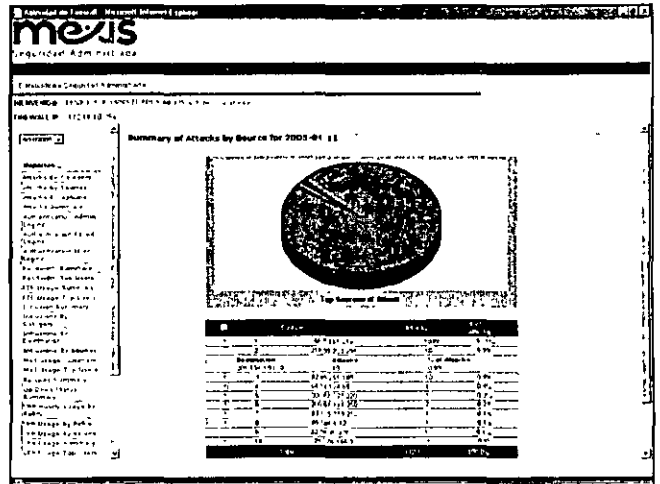
mexis
Seguridad Administrada

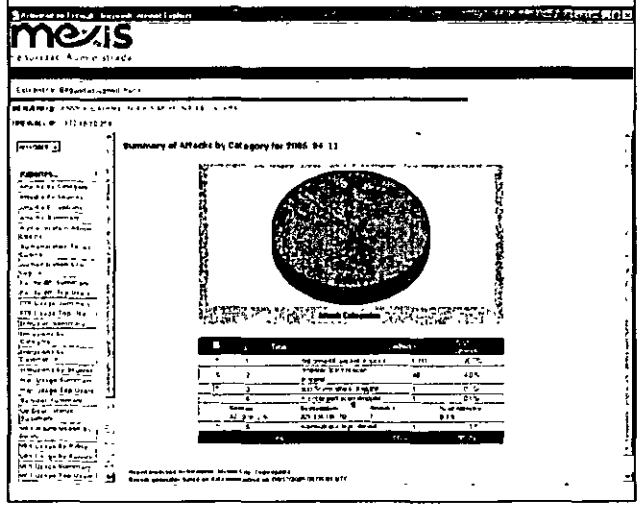
Reportes en Línea

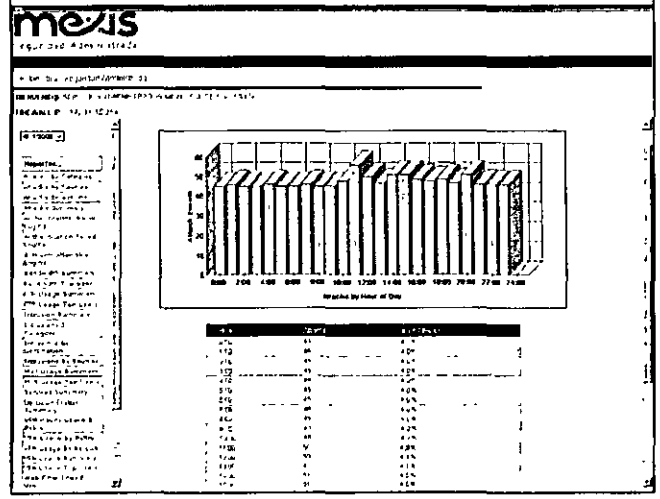
Ataques por Categoría



Ataques por Origen







Paquetes Descartados

Resumen de Ataques

Seguridad Administrada

Acuerdo de Nivel de Servicio

Seguridad Administrada

CARACTERISTICAS: ADMINISTRACIÓN

CONFIGURACIÓN BASICA

- Configuración de equipos
  - Configuración de políticas iniciales en base conocimiento de riesgos
  - Asesoría en la definición e implementación de políticas básicas iniciales de seguridad en la frontera perimetral y en el control de la salida a internet de los usuarios en la red local
  - Alta en consola de monitoreo y administración

Ventajas:

- Disminuye el riesgo de vulnerabilidad inmediata
- Incrementa el uso adecuado de las funcionalidades del equipo
- Permite realizar una implementación rápida y sencilla
- Monitoreo instantaneo al conectar a Internet

Seguridad Administrada

CARACTERISTICAS: ADMINISTRACIÓN

INSTALACIÓN EN SITIO O REMOTA

- En sitio o remota
  - Plan de instalación de equipos y configuración final en sitio
  - Creación remota de VPN's con políticas iniciales
  - Puesta a punto de políticas seguridad en la red

Ventajas:

- Disminuye el tiempo de implementación de nuevas tecnologías de seguridad
- No requiere recursos especializados en seguridad
- Disminuye la interrupción del servicio de Internet

Seguridad Administrada

CARACTERISTICAS: ADMINISTRACIÓN

ADMINISTRACIÓN (SLA Silver)

- Alta, Bajas o Cambios
  - Soporte telefónica para solicitud de administración 7x24x365
  - Evaluación de riesgos al momento del cambio
    - Apertura de puertos
    - Cambios de políticas de seguridad en servicios (http, smtp, ftp, etc.)
    - Alta y Baja de políticas
  - Alta o Baja remota de políticas en VPN's ilimitidas
  - Cambios de emergencia no programados (opcional por evento)

Ventajas:

- Disminuye el tiempo de evaluación de nuevas políticas
- Soporte télefonico 7x24x365 ilimitado
- Minimiza el riesgo de vulnerabilidad al realizar cambios en la red
- Creación de esquema de políticas grupales para VPN's

Seguridad Administrada

CARACTERISTICAS: ADMINISTRACIÓN

GARANTIAS Y ACTUALIZACIONES

- Cobertura
  - Reemplazo por falla de equipo en sitio
  - Alta de respaldo de políticas de seguridad de red y de VPN's

- Licenciamiento
  - Se incluyen las actualizaciones de versiones
  - Evaluación de seguridad por medio de nuestro equipo de expertos ante diferentes tipos de ataques como intento de hackeo y/o virus

Ventajas:

- Disminuye el tiempo de baja inesperada en el servicio
- No se requiere re-configuración total del equipo
- No existen costos inesperados de licenciamientos
- Evita la obsolecencia tecnológica de hardware y software
- No requiere inversiones de tiempo para re-instalación

Seguridad Administrada

CARACTERISTICAS: ADMINISTRACIÓN

SOPORTE y MONITOREO

- Soporte telefónico
  - A través de nuestro equipo de ingenieros certificados
  - Acceso Telefónico 7x24x365
  - Verificación y seguimiento de Trouble Tickets via web
- Monitoreo Remoto
  - Verificación de status de redes y VPN's
  - Laboratorio de evaluaciones de vulnerabilidad de red
  - Alertamiento sobre riesgos en tiempo real

Ventajas:

- Apoyo ilimitado para mejor desempeño del servicio
- Incrementa el nivel de respuesta a riesgos

mexis
Seguridad Administrada

CARACTERISTICAS: ADMINISTRACIÓN

INFORMACIÓN EN LINEA

- www.mexis.net
  - Extranet de Información sobre:
    - Estadisticas de Servicio de CPE's
    - Reporte de Filtrado de Paquetes
      - Por horario
      - Por Host
      - Por Servicio
      - Por Sesión
    - Reporte de Proxies
      - HTTP
      - SMTP
    - Detalle de servicios denegados

Ventajas:

- Conocimiento de los servicios más utilizados dentro de la red para toma de desiciones

Seguridad Administrada

CARACTERISTICAS: ADMINISTRACIÓN

RESPALDO (POLITICAS Y REGISTROS)

- Respaldo de políticas de seguridad
  - Mantenemos infraestructura que permite el respaldo de políticas de seguridad
  - Capacidad de respuesta en caso de re-inicialización de equipos restaurando políticas
  - Restauración de red de VPN Móviles y Oficina a Oficina

- Respaldo de Registros
  - Creación de respaldos en servidores resguardados
  - Restauración de respaldos para verificación de riesgos

Ventajas:

- No requiere de costos adicionales de infraestructura
- Se realizan de manera recurrente por ingenieros certificados

Seguridad Administrada

Valores Adicionales

1. Evita el riesgo
   - Selección de proveedor
   - De dimensionamiento
   - Tecnológico/ obsolescencia
2. Mayor y mejor garantía y servicio de los proveedores
3. Solución 100% garantizada
4. Escalabilidad
5. Always On
6. Minimiza vulnerabilidad de dependencia
   - Capacitación/pirateo
   - Sólo uno sabe como
   - Todas las llaves en una sola mano
7. Soporte Técnico 7x24x365
8. Suscripción a entidades world class de seguridad
9. Knowledge base
10. Una empresa especializada solo en seguridad

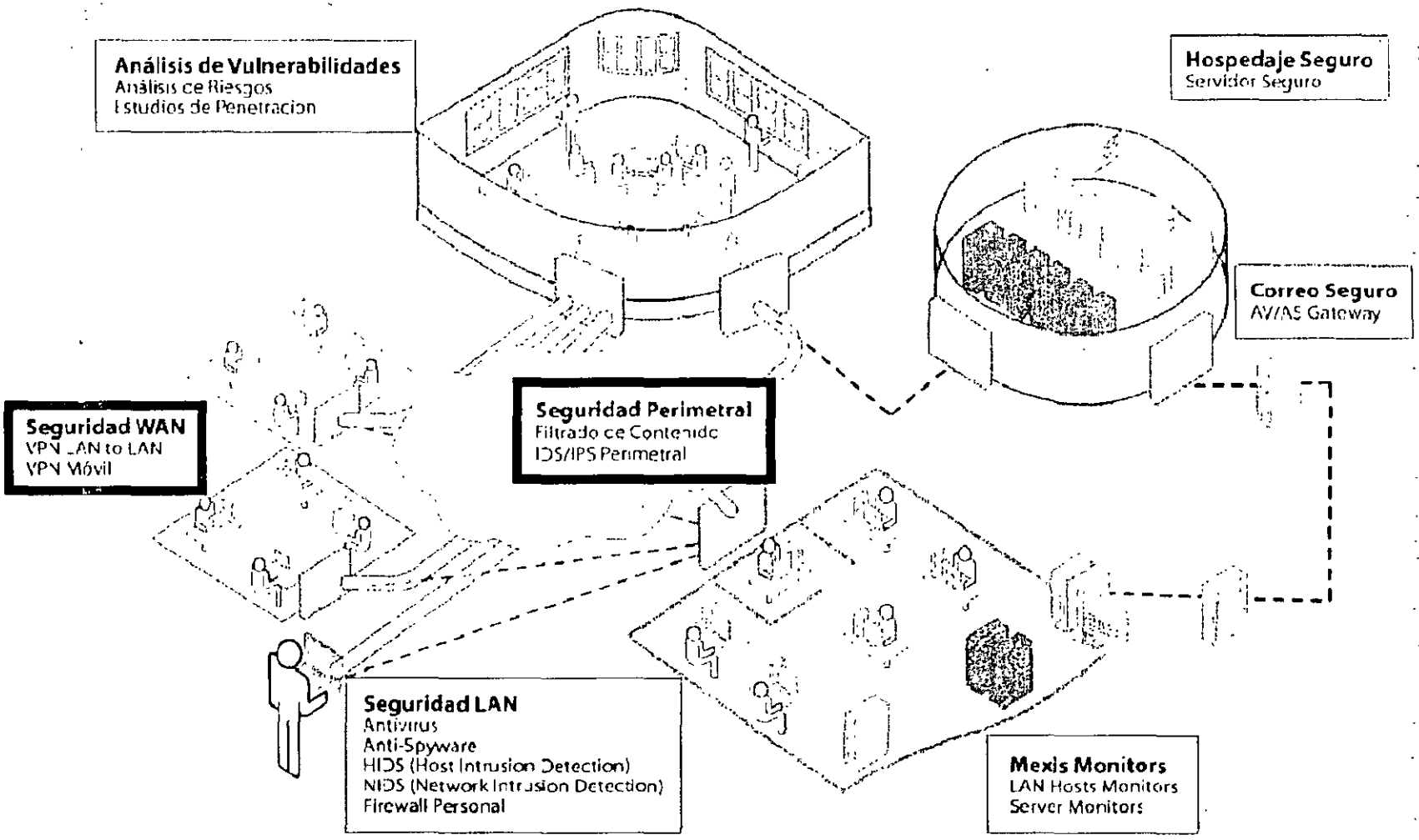
mexis
Seguridad Administrada

Diferenciadores MEXIS

- **Experiencia**
  - Pioneros desde hace más de 13 años.
- **Ahorro**
  - Menor Costo Total de Propiedad (TCO)
  - No existen costos ocultos.
- **Integración**
  - Arquitectura de soluciones de acuerdo con sus necesidades.
  - Servicio integral con múltiples plataformas tecnológicas.
- **Flexibilidad**
  - Escalabilidad, incremento o reducción de usuarios sin afectar.
  - Altas, bajas y cambios ilimitados.
- **Rapidez**
  - Velocidad de respuesta: prevenimos y corregimos.
  - Tiempo de implementación: se mide en días.
  - Acuerdo de Nivel de Servicio: tiempos de respuesta.

mexis
Seguridad Administrada

Familia - Servicios



Seguridad Administrada

Presentacion
Diplomado de Seguridad UNAM

Parte II Características Técnicas
Abril 2007

Seguridad Administrada

Agenda

- Caracteristicas Tecnicas de Dispositivos
  - Defensa de Ataques (Deep Packet Inspection)
  - IDS/IPS (detección y prevención de intrusos)
  - Filtrado de Contenido
  - Alta Disponibilidad
  - Segmentación de Red
  - Autentificación y Autorización de Servicios
  - Antivirus Gateway
  - AntiSpyware Gateway
  - AntiSpam Gateway
  - WAN Failover
  - WAN Load Balancing

Seguridad Administrada

Definición de Caracteristicas

- **Defensa de Ataques.** Por medio del firewall se bloquean ataques dirigidos a dispositivos o servidores, ya que se detectan y detienen antes de que estos logren causar daño. Dentro de este tipo de ataques se encuentran ataques de denegación de servicios (Ping de la muerte, TCP Sync, etc.) y paquetes anómalas o que no están bajo estándares.

- **IDS/IPS**: Previene e identifica una extensa selección de amenazas en la capa de aplicación rastreando paquetes para detectar gusanos, troyanos, vulnerabilidades de software como buffer overflows, peer-to-peer y aplicaciones de mensajería instantánea, backdoor exploits, y otros códigos maliciosos.

Seguridad Administrada

Definición de Caracteristicas

- **Defensa de Ataques.** Por medio del firewall se bloquean ataques dirigidos a dispositivos o servidores, ya que se detectan y detienen antes de que estos logren causar daño. Dentro de este tipo de ataques se encuentran ataques de denegación de servicios (Ping de la muerte, TCP Sync, etc.) y paquetes anómalas o que no están bajo estándares.

- **IDS/IPS**: Previene e identifica una extensa selección de amenazas en la capa de aplicación rastreando paquetes para detectar gusanos, troyanos, vulnerabilidades de software como buffer overflows, peer-to-peer y aplicaciones de mensajería instantánea, backdoor exploits, y otros códigos maliciosos.

Seguridad Administrada

Definición de Caracteristicas

- **Filtrado de Contenidos** programas configurados en el firewall que examinan los encabezados de los archivos de paquetes entrantes y los envía o rechaza basándose en las reglas preestablecidas para ese filtro.

- **Alta Disponibilidad** permite la instalación de dos ó más firewalls en una red con una configuración especial, teniendose dos posibles opciones:
  - Activo/Pasivo. Donde un dispositivo permanece activo y el segundo se mantiene siempre listo para activarse en caso de que el primero falle.
  - Activo/Activo. Los dos dispositivos se encuentran activos y balanceando la carga y el trafico entre ellos. En caso de que uno falle, la carga total es manejada por el que permanece activo.

Seguridad Administrada

Definición de Caracteristicas

- **Segmentación de Red** (mayor protección de servicios críticos) Al separar ciertas partes de tráfico de la red basado en Zonas, se mejora el rendimiento, seguridad y fiabilidad.

- **Autentificación y autorización de servicios** método usado para rastrear el nombre de un usuario a una dirección IP de una estación de trabajo, lo que permite rastrear conexiones basadas en usuarios en lugar de la dirección IP.

Seguridad Administrada

Gateway Antivirus y AntiSpyware

- Protección directa a través del análisis de las conexiones que cruzan por el Firewall comparando los archivos descargados y enviados por e-mail, contra una extensa base de datos de firmas, códigos o patrones maliciosos para detectar y detenerlos oportunamente.

- La base de datos de las firmas es constantemente actualizada para ofrecer la mayor protección posible contra una amenaza que siempre cambia. Las firmas nuevas son creadas y agregadas a la base por diversas fuentes de organismos internacionales

Seguridad Administrada

Gateway Antivirus

- El servicio de Gateway Antivirus revisa las conexiones que cruzan el firewall que se encuentra instalado entre la red LAN e Internet, a través del motor de inspección de paquetes de alto rendimiento del equipo.

- Las conexiones que revisa el Gateway antivirus del tráfico de entrada son los correspondientes a los puertos o servicios: HTTP, FTP, POP3, SMTP e IMAP y de las conexiones del trafico de salida exclusivamente será el SMTP.

Seguridad Administrada

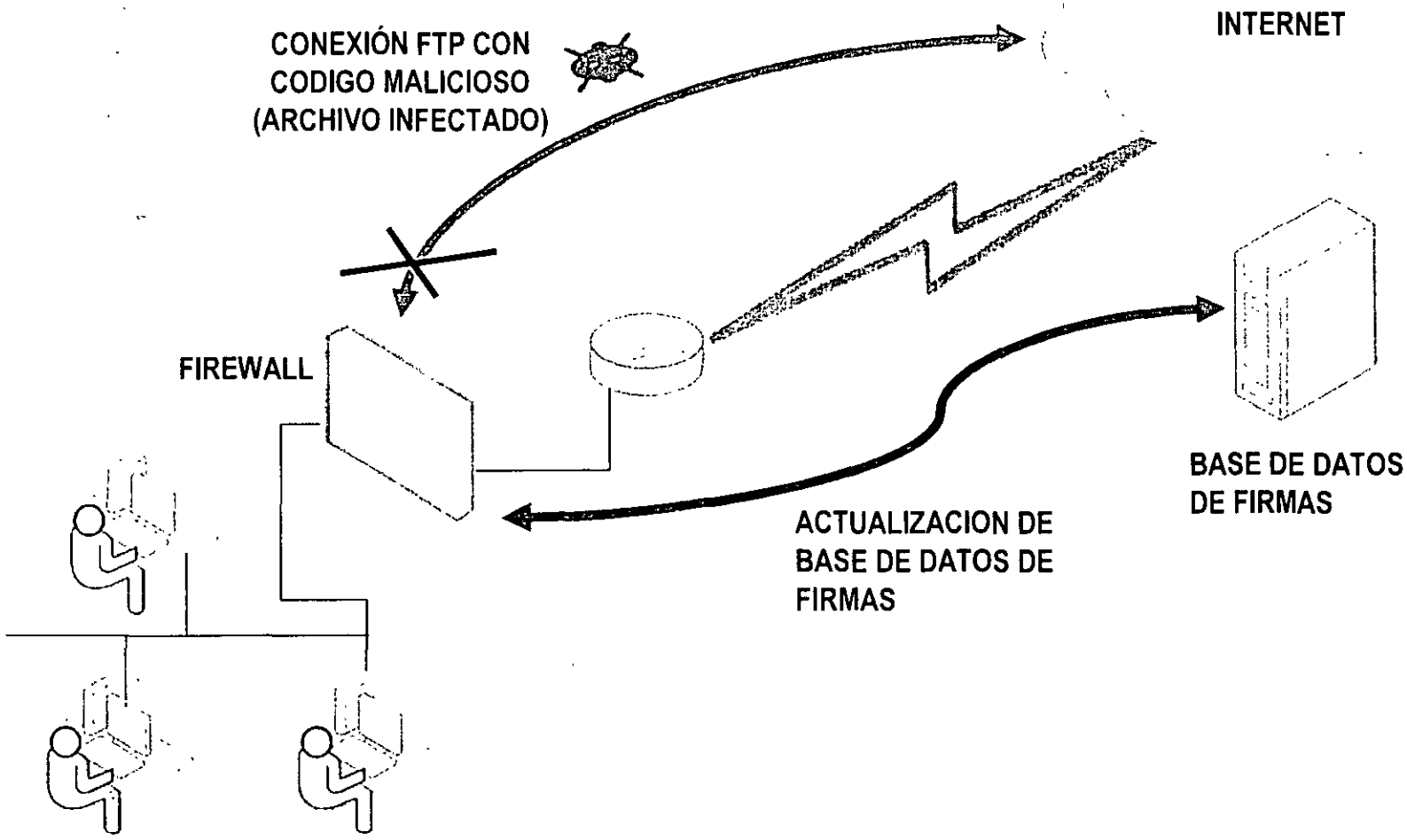
Gateway AntiSpyware

- El modulo o servicio previene spyware malicioso, bloqueando el programa de instalación en la entrada e interrumpiendo la comunicación de programas spyware que transmiten datos confidenciales.

- Las conexiones que revisa el AntiSpyware del tráfico de entrada son los correspondientes a los puertos o servicios: HTTP, FTP, POP3, SMTP.

Seguridad Administrada

Gateway Antivirus AntiSpyware



Seguridad Administrada

Gateway AntiSpam

- Esta característica previene bloquear correo no deseado cuando el usuario cuenta con un servidor de correo dentro de sus oficinas, existen diferentes técnicas a aplicar entre las que se encuentran:

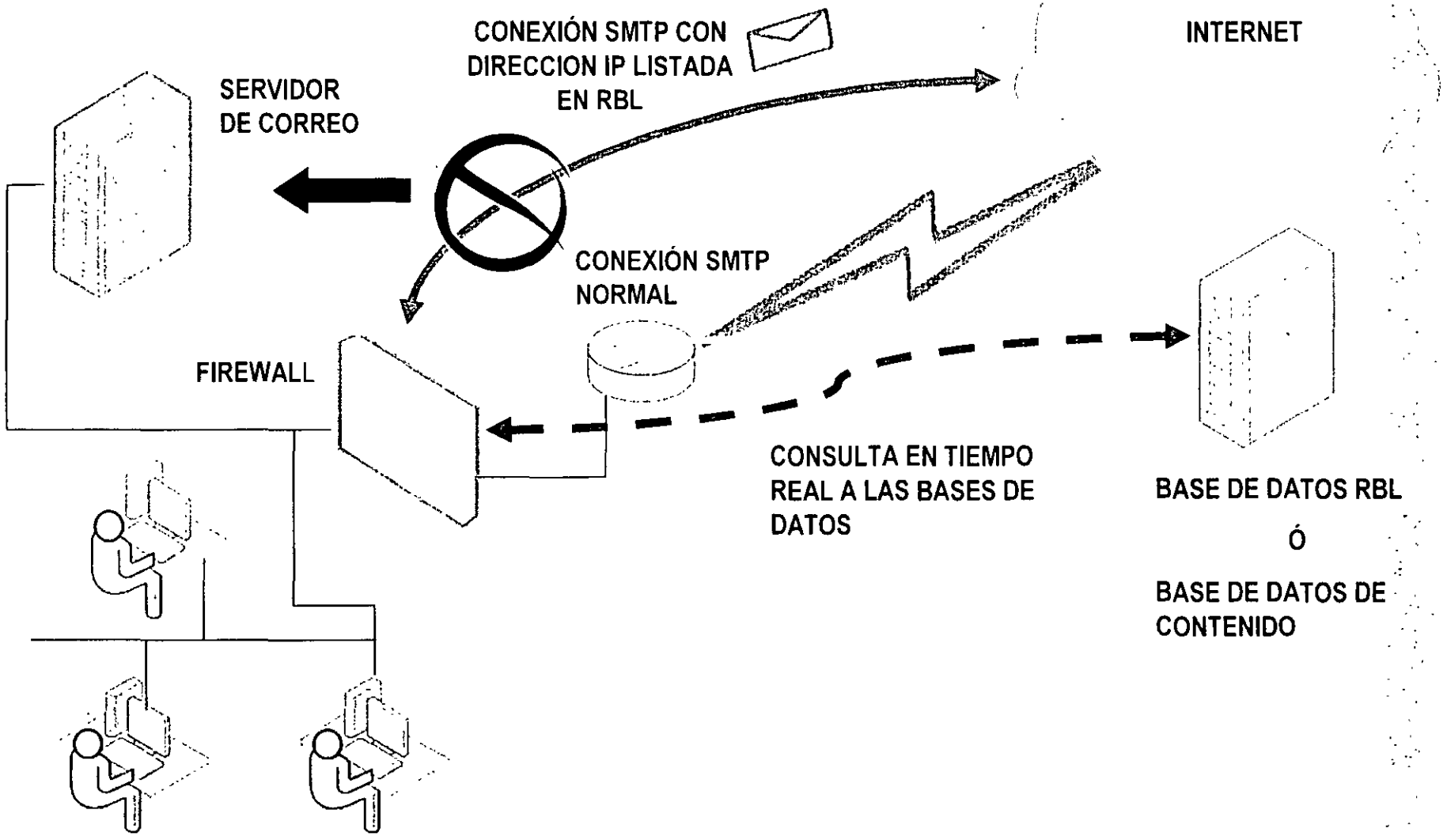
  - Técnica de filtrado de correo no deseado por medio de Listas Negras Publicas ó Real-Time Black list Spam Filtering (RBL). Estas listas contienen las IP´s de los servidores SMTP que realizan SPAM o que tienen abierto el relay de SMTP

    Se usa al DNS para consultar las bases de RBL y denegar las conexiones de SMTP de entrada hacia el servidor de correo electrónico cuando provenga de una dirección IP que se encuentre en las listas.

  - Técnica de filtrado de correo no deseado basado en contenido y firmas

Seguridad Administrada

Solución AntiSpam



Seguridad Administrada

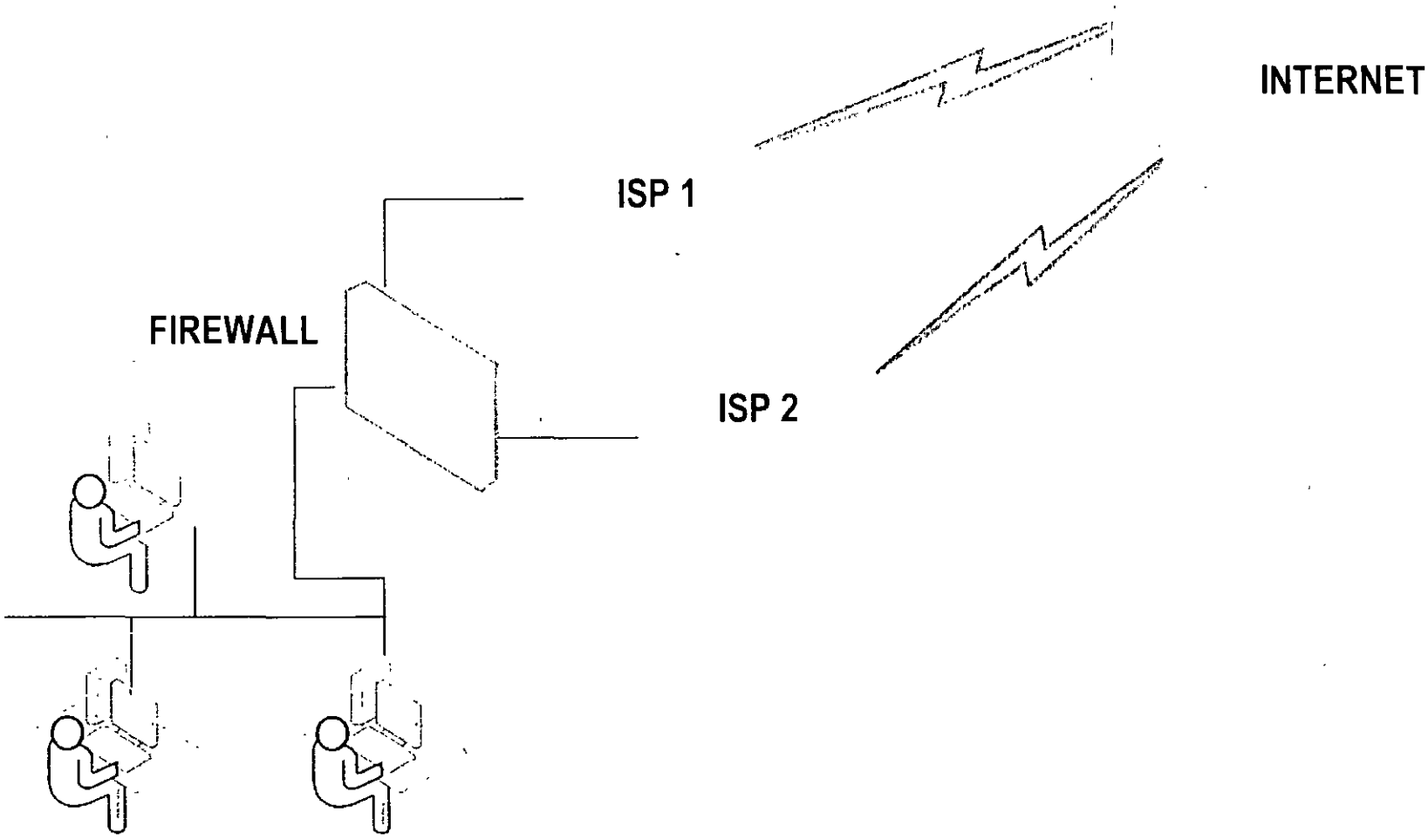
WAN Failover

- Se brinda un esquema de redundancia en el tráfico de salida o de acceso a Internet, que incluye enlaces de diferentes proveedores (ISP´s), capacidades y tecnologías (ADSL, Enlace dedicado, Cable-Modems, Satelital, etc.)

- Un esquema de redundancia en su sitio central para la operación e interconexión de VPN´s Site to Site o Usario Móvil a Site Central.

Seguridad Administrada

WAN Failover



Seguridad Administrada

WAN Load Balancing ó Dual ISP

- Al tener dos diferentes salidas o accesos a Internet se conectan cada una a un puerto Ethernet diferente del Firewall.

- En base a las necesidades y a la infraestructura instalada se puede definir una de las 4 opciones para poder manejar el tráfico de salida a Internet:
  - Redundancia Basica Activo-Pasivo
  - Roun Robin
  - Spilover
  - Basada en porcentaje

Seguridad Administrada

Redundancia Básica Activo/Pasivo

- El tráfico de salida será enviado al ISP2 o WAN2 secundario exclusivamente cuando el ISP1 ó WAN1 primario a sido marcado como inactivo por detectarse alguna falla en la salida de ISP1.

- Cuando se restablezca el acceso a Internet por el ISP1, automáticamente regresará el trafico al WAN1

- Se recomienda cuando los dos accesos a Internet tienen diferente ancho de banda (uno mucho mayor que otro) o el acceso primario (WAN1) con un enlace dedicado y el acceso de respaldo (WAN2) es por ADSL.

Seguridad Administrada

Balanceo por Round Robin

- Es un simple método de balanceo de cargas no muy granular ni con mucho control, pero que le permitirá utilizar la capacidad de ambos enlaces.

- El firewall decidirá en base a la IP destino por cual interfaz ó proveedor enviar el tráfico y aceptar el retorno. En caso de no ser posible lo anterior enviara un paquete por un enlace y un paquete por el otro (Fifty - Fifty)

Seguridad Administrada

Balanceo Spillover ó por desbordamiento

- El usuario puede especificar cuando el firewall puede comenzar a enviar tráfico a través de la interfaz WAN2 o ISP2

- Este método se recomienda cuando se desee que el trafico de salida no sea enviado a través del WAN2 secundario a menos que se sobrecargue el WAN1 primario.

- Si el tráfico de salida por la interfaz WAN1 primaria excede la definición en Kbps que se hizo por un periodo mayor a 20 segundos, entonces el firewall comenzará a desbordar trafico por la interfaz WAN2 secundaria

Seguridad Administrada

Balanceo Basado en Porcentaje

- El usuario puede definir el porcentaje de tráfico enviado a través de la interfaz WAN1 primaria y la interfaz WAN2 secundaria.
- Le permite activamente utilizar ambos accesos a Internet y con un mayor control.
- Se recomienda cuando el cliente tiene accesos a Internet de similar ancho de banda y de la misma tecnología.