tecnimap 2002
www.tecnimap.com
VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
Ponencias

Proyecto del diseño de los Sistemas de Seguridad Avanzada de la Subsecretaría del Ministerio de Hacienda.

Rafael Luis Santos García

Consejero Técnico en la Subsecretaría del Ministerio de Hacienda.

1. INTRODUCCIÓN.

La incorporación, prevista por el Ministerio de Hacienda, de nuevas tecnologías asociadas con la evolución de las comunicaciones, la agilización de los procesos administrativos y el acercamiento de la Administración al ciudadano, implican un mayor nivel de exposición de los sistemas de información a diversos riesgos derivados de la apertura de las redes de comunicaciones utilizadas y la multiplicación de los accesos.

Este hecho, unido a las necesidades que ello conlleva en materia de integridad, confidencialidad y disponibilidad de la información, indican que tal evolución no sería posible si no se aseguran al mismo tiempo unos estándares elevados en materia de seguridad de los sistemas de información que participan en el proceso.

Con el objetivo de mejorar la seguridad de los sistemas de información y las redes de comunicación del Ministerio de Hacienda, y anticiparse a las vulnerabilidades que podrían surgir como resultado de esta anunciada apertura, la

Subsecretaría del Ministerio de Hacienda ha decidido acometer el "Diseño, Implantación y Operación del los Sistemas de Seguridad Avanzada del Ministerio de Hacienda".

2. ARQUITECTURA TÉCNICA.

El objetivo fundamental del diseño de arquitectura del sistema que se ha tenido en cuenta es conseguir un sistema que en su conjunto sea de alta disponibilidad (tolerante a fallos) y escalable (que pueda crecer en el futuro), de tal forma que la atención y servicio a los ciudadanos se vea garantizada y pueda incrementarse según la demanda.

Las distintas funciones a cubrir por el sistema, se pueden sintetizar en las siguientes:

2.1 Sistema para Gestión de Ancho de banda.

Este sistema será el encargado de gestionar el ancho de banda de las líneas de comunicaciones que posee el Ministerio con Internet, aumentando así el rendimiento de las mismas y eliminando problemas tales como cuellos de botella; diversificando los servicios ofrecidos por el Ministerio a los distintos usuarios.

Se recomienda situar el sistema de gestión de ancho de banda y tráfico (Calidad de servicio) entre el router de conexión a Internet y la primera línea de cortafuegos (segmento WAN).

2.2 Cortafuegos.

La arquitectura propuesta se describe en la ilustración 1 y está compuesta por dos líneas de Cortafuegos soportadas en productos de distintos fabricantes. De esta manera se consigue un mayor nivel de seguridad ya que el intruso tendría que atacar y superar las defensas de dos productos distintos y al mismo tiempo separar y segmentar los servicios de acuerdo al público objetivo al que están destinados (ciudadanos en general, empresas o funcionarios de las distintas Administraciones).

El sistema de cortafuegos formará una arquitectura de dos niveles proporcionando mayor estabilidad, seguridad y rendimiento al servicio:

- Nivel 1.- Cortafuegos Perimetrales, encargados de filtrar todas las conexiones provenientes tanto de Internet como de otros organismos.

  Actualmente el Ministerio tiene una línea Internet de 3.84 Mb. de ancho de banda. Si se decidiera adquirir otra línea adicional, aunque sea de otro proveedor, la solución de Cortafuegos Perimetrales adoptada permitiría realizar una gestión de las líneas Internet, proporcionando mecanismos de alta disponibilidad con balanceo de carga entre líneas, sin necesidad de incorporar hardware adicional.

- Nivel 2.- Cortafuegos Internos, encargados de filtrar todas las conexiones provenientes de los Cortafuegos Perimetrales y de los usuarios de la red interna (LAN).

2.3 Antivirus.

El sistema de antivirus se conectará directamente al cluster de Cortafuegos Perimetrales. De este modo, todo el tráfico que pase por dichos cortafuegos, sensible de ser analizado, se reenviará al antivirus, el cual lo analizará en busca de patrones de virus conocidos. En el caso de que detecte algún virus, actuará sobre unas políticas definidas.

Es recomendable que los sistemas de antivirus y diferentes consolas de administración y tratamiento de históricos estén situados en su propio segmento de red (segmento gestión), exclusivo para ellos. Siguiendo las premisas del presente diseño, estos productos se deberían instalar en configuración de alta disponibilidad.

Al mismo tiempo se implanta un sistema antivirus residente en los puestos de trabajo, los servidores departamentales, los servidores Web y los servidores de correo, los cuales se gestionan mediante una única consola, ubicada en el segmento de gestión, desde la que se realizan las actualizaciones y descargas de firmas en los referidos equipos.

Este sistema antivirus tendrá una tecnología distinta del otro antivirus perimetral, para así obtener una protección mayor frente a posibles ataques.

2.4 Sondas de detección de intrusión.

El sistema de detección de intrusión será el encargado de analizar el tráfico, de determinados segmentos de la red, en busca de intentos de ataque a los sistemas que conforman la plataforma Internet / Intranet del Ministerio. En el caso de que detecte un intento de ataque, actuará mediante unas políticas definidas.

En todos y cada uno de los segmentos de red que se definan en el sistema, actuará al menos un sensor de red para detectar posibles intrusiones en el sistema. Este sistema analiza el tráfico de red en tiempo real. Además se incluyen las sondas necesarias para todos los servidores críticos del sistema.

Se dispondrá de tres sondas ubicadas en los segmentos de DMZ, Intranet y BBDD.

2.5 VPN.

Para el acceso de usuarios móviles (conectados a través de Internet), se establecerá un sistema de seguridad basado en VPN (en modo túnel + cifrado del canal), asegurando la privacidad de las comunicaciones extremo a extremo. Cada usuario móvil tendrá un cliente VPN y el servidor VPN será el cluster de Cortafuegos Internos.

La autenticación de usuarios se realizará contra un servidor AAA (propiedad del Ministerio).

2.6 Gestión de Históricos.

Para tener un control unificado de lo que acontece en cada uno de los clusters de cortafuegos (Cortafuegos Perimetrales y Cortafuegos Internos), se dotará a la plataforma de un servicio centralizado de históricos.

2.7 Otras consideraciones.

El proceso de apertura y servicio a los ciudadanos mediante procedimientos informáticos conlleva que en el futuro se tengan que utilizar transacciones SSL para garantizar la seguridad de determinados procesos. Puesto que este sistema criptográfico de clave pública es lento, ya que requiere mayores recursos de procesado, se hace necesario incorporar tarjetas aceleradoras a los servidores que proporcionen estos servicios.

Se realizarán, de acuerdo a un calendario prefijado, análisis para verificar las posibles vulnerabilidades del sistema y así tenerlo actualizado.

Todos los equipamientos enunciados se gestionan y administran mediante consolas y servidores ubicados en el segmento de gestión. Con respecto a las consolas de gestión y supervisión es necesario realizar las siguientes consideraciones:

1- No es recomendable la integración de las consolas de los productos de Cortafuegos en una única, debido principalmente a razones de seguridad, por lo que recomendamos que se use la propia consola de cada producto.

2- No obstante, será necesario integrar en la fase de implantación un sistema centralizado de gestión de red y sistemas con el sistema de gestión de los equipos y productos de seguridad. De esta manera se controla y verifica la disponibilidad de los servicios 24X7.

Hay que tener muy presente que toda esta tecnología no tendrá validez si no se realiza al mismo tiempo un programa de concienciación e información de usuarios y administradores.

En los usuarios externos, conviene utilizar un sistema de autenticación fuerte basado en Tokens de usuario con introducción de una contraseña diferente cada vez que se conecte.

La arquitectura del sistema diseñado está destinada a dar soporte a los servicios que el Ministerio de Hacienda preste en Internet a los ciudadanos, a los que preste en la Intranet de la Administración General del Estado y a los que se definan para sus propios funcionarios.

La Ilustración muestra, a nivel lógico, la arquitectura propuesta:

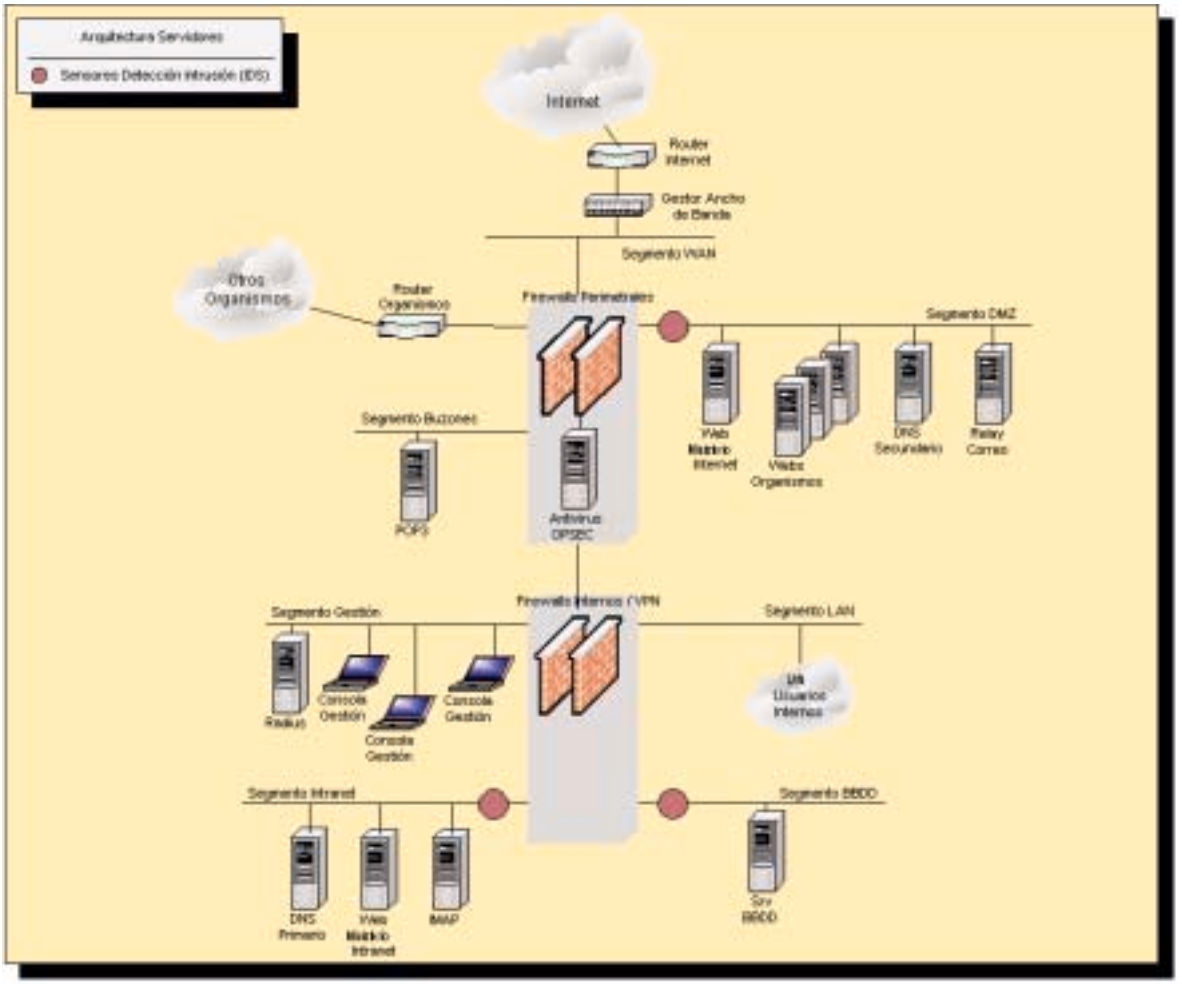

Ilustración Arquitectura propuesta

En ella se puede observar como grandes bloques la plataforma de seguridad y los distintos segmentos que conforman la red, descritos en detalle en los anteriores apartados.

3. DESCRIPCIÓN DE LA ARQUITECTURA.

3.1 SEGMENTOS.

Para dotar a la plataforma de un mayor rendimiento y seguridad se ha dividido la red en segmentos, según el tipo de servicios y el tráfico generado. En los siguientes apartados se da una breve descripción de los segmentos que albergan.

3.1.1 Segmento WAN.

Dedicado a la conexión del Ministerio con la red externa Internet.

En este segmento se albergarán los siguientes equipos:

- Router conexión Internet. Encargado de las comunicaciones con Internet.
- Gestor ancho de banda. Encargado de gestionar el ancho de banda de las líneas de comunicaciones con Internet.

3.1.2 Segmento DMZ.

Se utiliza para proporcionar los servicios del Ministerio a los ciudadanos y como interfase entre la red interna e Internet.

En este segmento se albergarán los siguientes equipos:

- Servidor Web Ministerio Internet. Encargado del servicio web corporativo del Ministerio de Hacienda (www.minhac.es).
- Servidores Web Otros Organismos. Encargado del servicio web corporativo de otros organismos.
- Servidor DNS Secundario. Encargado de resolver los nombres de las máquinas que conforman la plataforma Internet / Intranet del Ministerio Es una réplica (acceso en modo sólo lectura) del servidor DNS Primario, ubicado en el Segmento Intranet.

- Servidor Relay Correo. Encargado de realizar las siguientes funciones:
  - Relay de correo entrante y saliente de los usuarios del Ministerio.
  - Relay de correo entrante y saliente de los usuarios de Otros Organismos.
  - Servidor SMTP de los usuarios del Ministerio.
  - Servidor SMTP de los usuarios de Otros Organismos.

3.1.3 Segmento BUZONES.

Tiene como finalidad proporcionar los servicios de Correo Electrónico externo.

En este segmento se albergarán los siguientes equipos:

- Servidor POP3. Encargado de servir los mensajes de correo de los usuarios de Otros Organismos.

3.1.4 Segmento GESTIÓN.

Su utilidad consiste en independizar y asegurar la gestión y administración del equipamiento de seguridad.

En este segmento se albergarán los siguientes equipos:

- Servidor AAA. Encargado de realizar la autenticación de los usuarios que se conectan a través de la VPN.
- Consolas de Gestión. Encargadas de la administración de los dos clusters de cortafuegos (Cortafuegos Perimetrales y Cortafuegos internos), de la gestión centralizada de Históricos y del gestor de ancho de banda y de los dos antivirus.
- El servidor y la consola del Sistema de detección de intrusiones.
- En este segmento se incorporará también la consola gráfica y el servidor de gestión de red y sistemas.

3.1.5 Segmento LAN.

Sirve para agrupar a los usuarios internos del Ministerio.

En este segmento se albergarán los siguientes equipos:

- Equipos usuarios red Interna. PCs de los usuarios que conforman la red interna del Ministerio de Hacienda.

3.1.6 Segmento INTRANET.

Dedicado a dar servicios de Intranet a los funcionarios del Ministerio.

En este segmento se albergarán los siguientes equipos:

- Servidor Web Ministerio Intranet. Encargado del servicio web Intranet del Ministerio de Hacienda.
- Servidor IMAP. Encargado de recibir los mensajes de correo de los usuarios del Ministerio.
- Servidor DNS Primario. Encargado de resolver los nombres de las máquinas que conforman la plataforma Internet / Intranet del Ministerio. Es el Master (acceso en modo lectura / escritura). Tiene una réplica en el Segmento DMZ (DNS Secundario).

3.1.7 Segmento BBDD.

Utilizado para asegurar y aislar el repositorio general de datos del Ministerio.

En este segmento se albergarán los siguientes equipos:

- Servidor BBDD. Encargado de almacenar los datos de la distintas aplicaciones que posee el Ministerio.

4. ÁREAS TECNOLÓGICAS BENEFICIADAS.

La Subsecretaría tiene un interés especial en que estos proyectos de infraestructura sirvan como marco para asegu-

rar la Confidencialidad, Integridad y disponibilidad de las operaciones y además para que los demás Organismos del Ministerio de Hacienda puedan utilizarlos a la hora de proporcionar a los ciudadanos los servicios que de ellos requieren. Se trata de elaborar una referencia válida, homogénea para todos y, al mismo tiempo, adaptable a las distintas exigencias de seguridad que se presenten de acuerdo con las demandas externas.

Algunas de las áreas tecnológicas que se verán sin duda beneficiadas con la aplicación del proyecto son las siguientes:

4.1 INGENIERÍA DEL SOFTWARE Y SOLUCIONES DE BUSINESS INTELLIGENCE.

Sirve para preparar las aplicaciones nuevas que se realicen así como reutilizar las ya existentes.

- Metodología para la planificación, análisis, diseño, desarrollo, prueba y despliegue de aplicaciones y su mantenimiento.
- Middleware, integración de entornos heterogéneos y conectividad web-to-host para aplicaciones heredadas.
- Soluciones para el análisis y la explotación de datos de negocio de la empresa.

4.2 E-BUSINESS.

Al tener la información agrupada y segura, es posible relacionarla y coordinarla y al mismo tiempo particularizar para el ciudadano así como para la criticidad de las aplicaciones.

- Infraestructura de sistemas Multinet: servidores de aplicación, web, mensajería y directorio.
- Despliegue de aplicaciones de misión crítica en Internet.
- Soluciones de recuperación del conocimiento y la difusión personalizada de la información.
- Arquitectura de la Información y Gestión del Conocimiento.
- Posibles sistemas CRM (Customer Relationship Management).
- Soluciones de comercio electrónico y procesos de negocio en Internet.

4.3 SEGURIDAD CORPORATIVA E INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI).

Esta área es de máximo interés ya que la infraestructura desplegada permite la incorporación de tecnologías de seguridad que se verán implantadas en el futuro incrementando la seguridad de acceso de los ciudadanos.

- Análisis de la seguridad en sistemas informáticos conectados a redes.
- Redes privadas virtuales.
- Cortafuegos y sistemas de autenticación fuerte.
- Soluciones para la construcción de Infraestructuras de Clave Pública (PKI) y para asegurar los entornos de eBusiness.

4.4 CALIDAD DE SERVICIO.

Tiene como finalidad la excelencia en los servicios presentados a los diferentes usuarios del sistema.

- Soluciones de Alta Disponibilidad y Balanceo de Carga.
- Monitorización del Rendimiento y la Calidad de Servicio para redes, servidores y aplicaciones.
- Gestión y optimización de los recursos de ancho de banda.
- Aceleración de la entrega de contenidos en Internet.