



# Centro de Orientación de Seguridad

Microsoft

## Administración de la Seguridad con ISA Server 2006

- **Administración**
  - Asistentes.
  - Gestión de certificados.
  - Propagación de directivas
  
- **Publicación de servidores:**
  - Asistente publicación OWA.
  - Asistente de publicación de SPPS.
  - Soporte para Exchange 2007.
  - Traducción de enlaces.
  - Cache de bits.
  - Balanceo de carga para publicación web.
  - Calidad de servicio mediante el filtro Web Diffserv
  
- **Autenticación:**
  - Autenticación LDAP.
  - Single Sign-On.
  - Autenticación basada en formularios para sitios web.
  - Control de sesión
  
- **Soporte Firewall:**
  - Asistentes de creación de reglas.
  - Resistencia a ataques por saturación.
  - Recuperación en caso de ataque.



### Características de seguridad

#### • Filtros IP

- Filtrado IP a nivel de paquetes.
- Inspección de parámetros en cabeceras.
- Bloqueos de fragmentos IP

#### • Reglas de acceso

ISA Server 2006 proporciona una serie de reglas con los que se puede controlar la información que circula por la red en función de:

- Protocolos.
- Usuarios.
- Tipos de contenido.
- Franjas de tiempo.
- Objetos de red.

#### • Publicación de servicios

- Se utilizan para publicar servidores.

#### • Asistentes de publicación:

- Clientes de Acceso Web de Exchange.
- Servidor de correo.
- Sitio de Share Point.
- Sitios Web.
- Otros servicios.

#### • Filtros de aplicación.

#### • Detección y alertas contra intrusos.

- ISA Server 2006 cuenta con medidas para prevenir contra ataques por desbordamiento.
- Admite la definición de límite ante ataques potenciales.
- Permite definir excepciones a la regla.

### Publicación servidores con ISA Server 2006 Asistentes

- ISA Server 2006 presenta diferentes asistentes en función del servicio a publicar.
- La publicación de Servicios WEB admite la funcionalidad de publicar servidores o servicios balanceados.
- Los sitios Web admiten las funcionalidades de Bridging HTTPS



### **Listener**

- Define la escucha para las peticiones al servidor publicado.
- Admite la utilización de múltiples certificados.
- Admite diferentes mecanismos de autenticación.

### **Autenticación.**

- Admite los siguientes mecanismos de autenticación:
  - Autenticación de formulario HTML.
  - Autenticación HTTP.
  - Autenticación SSL.
  - No autenticar.

### **Validación de credenciales**

- Los mecanismos de validación pueden ser:
  - Directorio Activo.
  - LDAP.
  - Radius.
  - Radius OTP.
  - RSA SecurID.

### **Firewall de aplicación**

- Inspeccionar el tráfico al nivel de aplicación.
- Permitir o denegar el paso de datos a determinados contenidos o aplicaciones.
- Proporcionan controles sobre determinados ataques.
- Sistema extensible sobre filtrados de conexiones.

### **Filtro HTTP**

- Las necesidades de la empresa permiten el tráfico a través del puerto 80.
- Por el puerto 80 no solo viaja tráfico HTTP puro, sino que puede disfrazar otras comunicaciones.
  - Malware
  - P2P
  - Servicios de mensajería
  - Determinados ataques contra Servicios Web pueden ser controlados a este nivel



### **Controles HTTP**

- Mediante el filtro HTTP pueden ser controlados estos aspectos de la comunicación:
  - Técnicas de Buffer Overflow.
  - Denegación de servicio.
  - Subida de datos en escenarios de publicación.
  - Control de métodos.
  - Control de cabeceras.

### **Filtro contenido HTTP**

- Controlan el tráfico de datos a través de firmas.
  - En transmisión de datos.
  - En recepción de datos.
  - Impedir tráfico a palabras claves.
  - Control de acceso a sitios web.
  - Detención de comunicaciones de aplicaciones por firma y cabecera.

### **Filtro Proxyweb**

- Se aplica de forma directa sobre HTTP.
- Permite la extensión del filtro HTTP y de autenticación sobre otros protocolos.
- Garantiza el control sobre comunicaciones en entornos propietarios.

### **Arquitectura de Caché**

- ISA Server proporciona un sistema de almacenamiento para los objetos más consultados por los usuarios.
- La caché puede ser configurada mediante reglas que van a determinar cómo y con qué frecuencia va a ser almacenada la información.
- Mejora las condiciones de acceso a Internet mediante:
  - Soporte múltiples unidades de caché.
  - Soporte Caché en Arrays.
  - Caché Pasiva.
  - Soporte Caché Activa.
  - Soporte de Jobs de Caché.
  - Soporte de Caché Negativa.
  - Perfiles de cache por reglas.



### **Reglas de Caché**

- Las reglas van a determinar qué tipo y como se van a almacenar los objetos en la caché.
- La caché puede almacenar objetos HTTP, SSL y FTP.
- Si una petición no cumple una regla de caché esta es remitida hacia Internet.
- Permiten personalización por conjuntos de origen y/o destino.
- Permiten múltiples caracterizaciones.
- Permite planificación de trabajos de caché.
- Permite cachear en función de:
  - Tipos de contenido.
  - Tamaños.
  - Tipos de protocolo.

### **Priorización de paquetes Diffserv**

- Mediante el filtro Diffserv pueden establecerse prioridades del envío de paquetes HTTP.
- La asignación de prioridades se asignan sobre los objetos Redes de ISA Server 2006.
- El establecimiento de prioridades se realiza sobre:
  - URL.
  - Dominios.
- La asignación de prioridades se establece mediante la definición de valores.

### **Soporte contra desbordamientos**

- ISA Server 2006 cuenta con medidas para prevenir contra ataques por desbordamiento.
- Admite la definición de límite ante ataques potenciales.
- Permite definir excepciones a la regla.

### **Monitorización**

- Monitorización de servicios de ISA Server.
  - Firewall.
  - Data Engine.
  - Isa Server Job Scheduler.
  - Remote Access.
- Monitorización de sesiones VPN.
- Monitorización de conectividad.
- Soporte de LOG por filtros de servidor.



- Integración con bases de datos.
  - MSDE.
  - SQL.
- Soporte de consultas sobre logs.
- Filtro de consultas.

### **Informes**

- ISA Server presenta el sistema de Reporting.
  - Informes sumariales.
  - Informes de utilización de aplicaciones.
  - Informes de utilización web.
  - Informes de seguridad.
  - Informes de tráfico y uso.
- Generación y publicación de informes planificada.