


# Seguridad IP para Microsoft Windows 2000 Server

## Documento estratégico

**Resumen**

El sistema operativo de Microsoft® Windows® 2000 Server incluye una implementación del protocolo de Seguridad IP de Internet Engineering Task Force. La Seguridad IP de Windows proporciona a los administradores de red una línea clave de defensa para proteger sus redes. La Seguridad IP de Windows existe abajo del nivel de transporte, por lo que los servicios de seguridad son heredados transparentemente por las aplicaciones. La actualización a Windows 2000 Server proporciona protecciones de integridad, autenticación y confidencialidad, sin tener que actualizar las aplicaciones, ni capacitar a los usuarios.

*Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA*

*0399*

## TABLA DE CONTENIDOS


**INTRODUCCION ..... 1**

**BENEFICIOS DE LA SEGURIDAD IP ..... 3**

Construir sobre la Seguridad IP 3

Soporte completo de estándares de la industria 3

- Técnica Diffie-Hellman (DH) 4
- Código de control de autenticación de mensajes (HMAC) 4
- HMAC-MD5 4
- HMAC-SHA 4
- DES-CBC 4

Estándares y referencias con soporte 4

Protocolos de seguridad flexibles 5

Asociación de seguridad de Internet y protocolo de administración clave **¡Error! Marcador no definido.**

- Oakley 5
- Encabezado de autenticación IP 5
- Protocolo de seguridad de encapsulamiento IP 5

Ahorros de costos 5

- Actualizaciones de Software 6
- Capacitación 6
- Administración clave criptografica 6

**INSTALAR LA SEGURIDAD IP DE WINDOWS ..... 7**

Evaluar la información 7

Crear escenarios 7

Determinar los niveles de seguridad requeridos 7

Construir políticas de seguridad con el administrador de seguridad 7

Políticas de seguridad flexible 8

Políticas de negociación flexibles 8

Filtros 8

Crear una política de seguridad 8

Diagrama de una instalación básica 10

- Notas de compatibilidad 11

**RESUMEN ..... 12**

**PARA MAYOR INFORMACION ..... 13**

## INTRODUCCION

El sistema operativo de Microsoft® Windows® 2000 Server simplifica la instalación y administración de la seguridad de red con la Seguridad IP de Windows®, una implementación solida del protocolo de Seguridad IP (IPSec).

La necesidad de una seguridad de red basada en el protocolo de Internet (IP), ya es grande y continúa en aumento. En el mundo empresarial de hoy día interconectado masivamente a Internet, intranets, sucursales y acceso remoto, información sensible cruza las redes constantemente. El reto para los administradores de red y otros profesionales de informática es asegurar que este tráfico esté:

- A salvo de modificaciones de datos mientras está enrutado.
- A salvo de interceptación, visualización o copia.
- A salvo de ser accesado por partes no autenticadas.

Estos aspectos se conocen como integridad, confidencialidad y autenticación de datos. Además, la protección contra reproducción evita la aceptación de un paquete reenviado.

Diseñado por Internet Engineering Task Force (IETF) para el protocolo de Internet, IPSec da soporte a la autenticación, integridad de datos y codificación a nivel de red. IPSec se integra a la seguridad inherente del sistema operativo de Windows 2000 Server a fin de proporcionar la plataforma ideal para salvaguardar las comunicaciones de intranet e Internet.

La Seguridad IP de Microsoft Windows utiliza algoritmos de codificación estándar de la industria y un enfoque de administración de seguridad completo para proporcionar seguridad a todas las comunicaciones TCP/IP en ambos extremos del *firewall* de una organización. El resultado es una estrategia de seguridad de extremo a extremo de Windows 2000 Server que se defiende contra ataques externos e internos.

Dado que la Seguridad IP de Windows se instala abajo del nivel de transporte, los administradores de red (y los proveedores de software) se ahorran el problema y gastos de tratar de instalar y coordinar la seguridad de una aplicación a la vez. Al instalar Windows 2000 Server, los administradores de red proporcionan un fuerte nivel de protección para toda la red, y las aplicaciones heredan automáticamente las salvaguardas de la seguridad de Windows 2000 Server. El soporte de codificación de la Seguridad IP de Windows se extiende también a las Redes privadas virtuales (VPNs).

Los administradores de red se benefician de la integración de IPSec con Windows 2000 Server por varias razones, incluyendo:

- **Estándar abierto de la industria**—IPSec proporciona una alternativa de estándar abierto de la industria en cuanto a tecnologías de codificación IP de propietario. Los administradores de red se benefician de la interoperabilidad resultante.
- **Transparencia—**IPSec existe abajo del nivel de transporte, lo que hace que sea transparente para las aplicaciones y usuarios, es decir, no hay necesidad

de cambiar las aplicaciones de red en el escritorio de un usuario cuando se implementa IPSec en el *firewall* o en el enrutador.

- **Autenticación—**Los servicios de autenticación firmes evitan la interceptación de datos a través de identidades falsas.
- **Confidencialidad—**Los servicios de confidencialidad evitan el acceso no autorizado a datos sensibles a medida que pasan entre las partes en comunicación.
- **Integridad de datos—**Los encabezados de autenticación IP y las variaciones del código de control de autenticación de mensajes de verificación aseguran la integridad de los datos durante la comunicación.
- **Repetición dinámica de claves—**La repetición dinámica de claves durante la comunicación contínua ayuda a proteger contra ataques.
- **Enlaces seguros de extremo a extremo—**La Seguridad IP de Windows proporciona enlaces seguros de extremo a extremo para usuarios de redes privadas, dentro del mismo dominio o a través de cualquier dominio confiable en la empresa.
- **Administración centralizada—**Los administradores de red utilizan políticas y filtros de seguridad para proporcionar niveles de seguridad adecuados con base en el usuario, el grupo de trabajo u otros criterios. La administración centralizada reduce los costos administrativos indirectos.
- **Flexibilidad—**La flexibilidad de la Seguridad IP de Windows permite políticas que pueden aplicarse en toda la empresa o en una sola estación de trabajo.

Estas son todas buenas noticias para los administradores de red y otros profesionales de informática responsables de proteger la seguridad de la información. El aumento significativo de intranets y la creciente integración de redes corporativas con Internet han provocado una mayor necesidad de seguridad. A pesar de que la inquietud clásica de seguridad es proteger los datos contra extraños, la Seguridad IP de Windows también proporciona protección contra ataques de la fuente más probable: el acceso no autorizado de personal interno.

Ya sea que se establezcan perfiles de seguridad para grupos de trabajo clave o para toda la red, el soporte de codificación de la Seguridad IP de Windows puede brindar a los administradores de red la tranquilidad que surge de proteger las comunicaciones de una empresa.

## BENEFICIOS DE LA SEGURIDAD IP

La mayoría de las estrategias de seguridad de red se han enfocado en evitar ataques externos a la red de la organización. Los *firewall*s, enrutadores seguros y autenticación de señales de acceso de marcación son ejemplos de los intentos administrativos por eliminar amenazas externas. Sin embargo, reforzar el perímetro de una red no sirve para protegerla contra ataques originados desde adentro.

De hecho, una organización puede perder una gran cantidad de información sensible por ataques internos emprendidos por empleados miembros del personal de soporte o concesionarios. Además, los *firewall*s no ofrecen protección contra tales amenazas internas.

Uno de los grandes beneficios de la integración de Windows 2000 Server con la Seguridad IP es la capacidad de protección contra ataques internos y externos. De nuevo, esto se realiza en forma transparente, y no implica esfuerzos ni costos adicionales para los usuarios individuales.

### Desarrollar con base en la Seguridad IP

La Seguridad IP, según define Internet Engineering Task Force (IETF), utiliza un encabezado de autenticación (AH) y una carga de pago de seguridad encapsulada (ESP). El encabezado de autenticación proporciona comunicación de datos con autenticación e integridad de fuente. La carga de pago de seguridad encapsulada proporciona confidencialidad, además de la autenticación e integridad. Con la Seguridad IP, solo el emisor y el receptor conocen la clave de seguridad. Si la autenticación de datos es válida, el receptor sabe que la comunicación viene del emisor y que no cambió durante el tránsito.

La Seguridad IP de Windows se desarrolla con base en el modelo IETF al combinar la criptografía de claves públicas y secretas, y al proporcionar administración automática de claves para maximizar la seguridad y obtener un rendimiento efectivo total de alta velocidad. Esto brinda una combinación de autenticación, integridad, no reproducción, y (opcionalmente) confidencialidad para lograr comunicaciones seguras. Ya que la Seguridad IP de Windows está abajo del nivel de red, es transparente para los usuarios y las aplicaciones existentes; las organizaciones obtienen automáticamente altos niveles de seguridad de red.

Las funciones de Seguridad IP de Windows incluyen:

- Soporte completo de los estándares de la industria (IETF)
- Protocolos flexibles de seguridad
- Fácil implementación y administración
- Políticas flexibles de seguridad
- Políticas flexibles de negociación
- Ahorro en costos

### Soporte completo de estándares de la industria

Windows 2000 aprovecha totalmente los poderosos algoritmos criptográficos

estándar de la industria y las técnicas de autenticación. Estos incluyen:

- La técnica Diffie-Hellman para acordar una clave compartida.
- El código de autenticación de mensajes de verificación (HMAC) y sus variantes, para proporcionar integridad y no reproducción.
- Estándar de codificación de datos—encadenamiento de bloques de cifras para confidencialidad.

#### Técnica Diffie-Hellman (DH)

La técnica Diffie-Hellman (nombrada así por sus inventores Whitfield Diffie y Martin Hellman) es un algoritmo de criptografía de claves públicas que permite que dos entidades se comuniquen para acordar una clave compartida. Diffie-Hellman se inicia con dos entidades que intercambian información pública. Cada entidad combina después la información pública de la otra junto con su propia información secreta para generar un valor secreto compartido.

#### Código de autenticación de mensajes de verificación (HMAC)

HMAC es un algoritmo de claves secretas que proporciona integridad y autenticación. La autenticación que utiliza la verificación con claves produce una firma digital para el paquete, que puede ser verificado por el receptor. Si el mensaje cambia durante el tránsito, entonces el valor de verificación es diferente y el paquete IP es rechazado.

#### HMAC-MD5

La función 95 de compendio de mensajes (MD5) es una función de verificación que produce un valor de 128 bits.

#### HMAC-SHA

El Algoritmo de verificación segura (SHA) es una función de verificación que produce un valor de 160 bits. A pesar de que es un poco más lento que HMAC-MD5, el HMAC-SHA es más seguro.

#### DES-CBC

Estándar de codificación de datos (DES)— El encadenamiento de bloques de cifras (CBC) es un algoritmo de claves secretas utilizado para confidencialidad. Un número aleatorio se genera y utiliza con la clave secreta para codificar los datos.

## Estándares soportados y referencias

Windows 2000 da soporte completo y emplea protocolos publicados por Internet Engineering Task Force. La implementación cumple con los últimos borradores IETF propuestos en el grupo de trabajo IPSec, incluyendo documentos completos de arquitectura y documentos pertenecientes a formatos y transformaciones de encabezados, además de los borradores ISAKMP/Oakley.

La Seguridad IP de Windows 2000 implementa el Protocolo de asociación de seguridad de Internet y administración de claves (ISAKMP), utilizando el protocolo de determinación de claves Oakley, que permite la repetición dinámica de claves.

## Protocolos flexibles de seguridad

Los protocolos de seguridad desarrollan varios servicios para garantizar las comunicaciones de red. Windows 2000 utiliza los siguientes protocolos de seguridad:

- Protocolo de asociación de seguridad de Internet y administración de claves
- Determinación de claves Oakley
- Encabezado de autenticación IP
- Protocolo de seguridad de encapsulamiento IP

## Protocolo de asociación de seguridad de Internet y administración de claves

Antes de que los paquetes IP puedan ser transmitidos de una computadora a otra, es necesario establecer una asociación de seguridad (SA). Una SA es un conjunto de parámetros que define servicios y mecanismos como las claves, necesarios para proteger las comunicaciones de un protocolo de seguridad. Debe existir una SA entre las dos partes en comunicación que utilizan la Seguridad IP. El Protocolo de asociación de seguridad de Internet y administración de claves (ISAKMP) define la estructura común para dar soporte al establecimiento de asociaciones de seguridad. ISAKMP no está vinculado a ningún algoritmo, método de generación de claves o protocolo de seguridad específicos.

### Oakley

Oakley es un protocolo de determinación de claves que utiliza el algoritmo de intercambio de claves Diffie-Hellman. Oakley da soporte a la Confidencialidad perfecta de retransmisión (PFS) que asegura que si una sola clave se compromete, solo permite el acceso a los datos protegidos por esa clave. Nunca reutiliza la clave que protege las comunicaciones para calcular claves adicionales y nunca usa el material original de generación de claves para calcular otra clave.

### Encabezado de autenticación IP

El Encabezado de autenticación IP (AH) proporciona integridad, autenticación y no reproducción. La confidencialidad no es una propiedad de AH. AH utiliza un algoritmo para calcular la verificación de mensajes en clave (un HMAC) para cada paquete IP.

### Protocolo de seguridad de encapsulamiento IP

Además de los servicios AH mencionados anteriormente, el Protocolo de seguridad de encapsulamiento IP (ESP) proporciona confidencialidad, utilizando el algoritmo DES-CBC.

## Ahorro en costos

Históricamente, las organizaciones han tenido que enfrentarse al dilema de encontrar un equilibrio difícil entre el deseo de proteger sus comunicaciones de datos y los altos costos de establecer y mantener dicha protección. La seguridad

puede imponer costos que exceden los costos de hardware de la red. Estos costos se pueden dividir en las siguientes categorías:

- Actualizaciones de Software
- Capacitación
- Administración de claves

### Actualizaciones de Software

Dado que la Seguridad IP de Windows se instala en el nivel de transporte, es transparente para las aplicaciones de software existentes. Con la Seguridad IP de Windows se proporciona seguridad para la red, las aplicaciones heredan esta seguridad y no es necesario modificar las aplicaciones. La seguridad a nivel de red proporciona enormes ahorros al eliminar la necesidad de actualizar las aplicaciones.

### Capacitación

Ya que la Seguridad IP de Windows 2000 es transparente para los usuarios, no se requiere capacitación para los mismos y este gasto es eliminado.

### Administración de claves criptográficas

Para proporcionar seguridad, es necesario cambiar las claves criptográficas regularmente. Cuando un administrador del sistema tiene que hacer esto manualmente, la administración de claves consume demasiado tiempo. Ya sea que las claves no se cambien con la frecuencia que una organización desearía o se cambien sólo en algunas computadoras importantes, la Seguridad IP de Windows maneja automáticamente la administración de claves. Los costos de cambiar manualmente las claves se eliminan y es posible establecer y mantener una protección máxima en toda la empresa.

## INSTALAR LA SEGURIDAD IP DE WINDOWS

Microsoft 2000 Server se ha diseñado para proporcionar muy altos niveles de seguridad de datos, aunados a la facilidad de implementación y administración. El resultado es la seguridad de la información en la empresa con bajos costos totales de propiedad. Windows 2000 Server proporciona gran flexibilidad con políticas de seguridad, de usuario y de dominio. El administrador de red puede aplicar políticas a toda la empresa o para un solo usuario o estación de trabajo. Las políticas de seguridad se pueden implementar transparentemente, sin necesidad de intervención posterior del administrador de red y sin capacitar otra vez a los usuarios.

A fin de establecer seguridad, un administrador de red debe llevar a cabo un proceso de cuatro pasos:

- Evaluar la información enviada a través de la red e Internet.
- Crear escenarios de comunicación.
- Determinar los modelos de seguridad requeridos por cada escenario.
- Desarrollar políticas de seguridad utilizando el Administrador de seguridad Windows.

### Evaluar la información

Toda la información enviada a través de redes o Internet está sujeta a interceptación, examen o modificación. Un administrador de sistemas puede determinar qué clase de información es más valiosa y cuáles escenarios de comunicación son los más vulnerables.

### Crear escenarios

Las organizaciones tienen ciertos patrones para sus flujos de información. Un administrador de sistemas puede determinar estos patrones predecibles. Por ejemplo, las oficinas remotas de ventas pueden enviar datos de ventas proyectados, órdenes de compra y otra información financiera a su oficina matriz. Cada uno de estos escenarios de comunicación puede tener diferentes políticas de Seguridad IP. Asimismo, un administrador de sistemas puede decidir, por ejemplo, que todas las comunicaciones con el departamento de recursos humanos deban ser seguras.

### Determinar los niveles de seguridad requeridos

Los niveles de seguridad requeridos cambian, dependiendo de la sensibilidad de la información y de la relativa vulnerabilidad del de transmisión. El Administrador de seguridad Windows 2000 permite a un administrador de red establecer rápida y fácilmente los niveles de seguridad apropiados.

### Desarrollar políticas de seguridad con el Administrador de seguridad

El Administrador de seguridad de Windows 2000 Server permite al administrador de red establecer algoritmos de seguridad y asignarlos a grupos de computadoras

o a computadoras únicas. Las políticas se desarrollan y asignan utilizando operaciones rápidas de señalar y hacer clic.

## Políticas flexibles de seguridad

Cada configuración de los atributos de la Seguridad IP de Windows se denomina una política de seguridad. Las políticas de seguridad se desarrollan a partir de políticas de negociación asociadas y filtros IP. Una política de Seguridad IP puede asignarse a la política de dominio predeterminada, a la política local predeterminada o a una política personalizada que usted elabore. Las computadoras en el dominio toman automáticamente las propiedades de las políticas de dominio predeterminadas y locales predeterminadas, incluyendo la política de Seguridad IP asignada a dicha política de dominio.

## Políticas flexibles de negociación

Las políticas de negociación determinan los servicios de seguridad que usted desea incluir para cada tipo de escenario de comunicación que labora para la empresa. Un administrador de red puede elegir entre los servicios que incluyen confidencialidad o aquellos que no lo hacen. El administrador puede establecer métodos múltiples de seguridad para cada política de negociación. Si el primer método no es aceptable para la negociación de seguridad, el servicio ISAKMP/Oakley continua consultando la lista en orden descendente hasta que encuentra uno que puede ser utilizado para establecer la asociación.

## Filtros

La filtración permite a Windows 2000 Server aplicar diferentes políticas de seguridad a distintas computadoras. Los filtros IP determinan las acciones a tomar, basados en el destino y el protocolo de los paquetes IP individuales.

## Crear una política de seguridad

Un ejemplo de creación de una política de seguridad se puede encontrar en una organización que tiene un departamento legal centralizado. Los administradores de red pueden decidir que las comunicaciones dentro del departamento deben ser seguras pero no confidenciales. Sin embargo, el administrador puede decidir que las comunicaciones entre el departamento legal y otros departamentos dentro de la organización deben ser tanto seguras como confidenciales. La Seguridad IP de Windows permite establecer filtros para aplicar las políticas de seguridad apropiadas a las comunicaciones iniciadas dentro del departamento legal. Si el destino de la comunicación es externo al departamento, la Seguridad IP de Windows aplica una política de seguridad que proporciona seguridad y confidencialidad. Si el paquete simplemente se traslada a otro destino dentro del departamento legal, se aplica la seguridad sin confidencialidad.

A fin de implementar el plan de seguridad para el departamento legal, el administrador debe emprender los siguientes pasos:

1. Crear una política de seguridad llamada Legal y asignarla a la política de dominio predeterminada. A medida que cada computadora en la compañía se registra dentro del dominio, el agente de políticas de la computadora puede seleccionar en el servicio de directorio la política de seguridad del departamento legal. La política de seguridad del departamento legal debe tener las siguientes políticas de negociación y filtros IP asociadas con ella:
2. Crear dos políticas de negociación y asociarlas con la política de seguridad del departamento legal:

   La primera política de negociación, Legal NP 1, se establece para un servicio que proporciona confidencialidad cuando los usuarios en el departamento legal se comunican con usuarios de otros departamentos ("los datos transferidos son confidenciales, auténticos y no modificables": protocolo de seguridad ESP).

   La segunda política de negociación, Legal NP 2, se establece para un servicio que proporciona únicamente autenticación y protección contra modificación cuando los usuarios del departamento legal se comunican entre sí ("Los datos transferidos son auténticos y no modificables": protocolo de seguridad AH).

3. Crear dos filtros IP y asociar cada uno de ellos con una política de negociación:
   Los usuarios en el departamento legal están en la red 157.55.0.0 con una máscara de subred 255.255.0.0. Los usuarios de otros departamentos están en la red 147.20.0.0 con una máscara de subred de 255.255.0.0. El primer filtro IP, Legal 1, es para usuarios en el departamento legal que se comunican con usuarios de otros departamentos. Este está asociado con la política de negociación Legal NP1. El administrador establece las propiedades del filtro con los siguientes valores:

   La dirección IP especificada para la fuente (emisor de datos) es 157.55.0.0. Esta dirección coincide con cualquier dirección IP dentro de la red del departamento legal, ya que en realidad es una dirección de subred IP.

   La dirección IP especificada para el destino (receptor de datos) es 147.20.0.0.

   Ya que el plan de seguridad de la compañía estipuló proteger todos los datos enviados a través del protocolo IP, el tipo de protocolo es Cualquiera.

   Los usuarios del departamento legal que se comuniquen con otros dentro del mismo departamento utilizan el segundo filtro IP, Filtro 2 Legal IP. Este se asocia con la política de negociación Legal NP 2, y las propiedades del filtro se establecen con los siguientes valores:

   - La dirección IP especificada para la fuente (emisor de datos) es 157.55.0.0.
   - La dirección IP especificada para el destino (receptor de datos) es 157.55.0.0.
   - El tipo de protocolo se establece en Cualquiera.

Cuando un usuario dentro del departamento legal envía información a cualquier otro usuario, las direcciones fuente y destino de los paquetes IP se revisan con base en los filtros IP de la política de seguridad legal. Si las direcciones coinciden con uno de los filtros, la política de negociación asociada determina el nivel de Seguridad IP para la comunicación.

Por ejemplo, si un usuario en el departamento legal con una dirección IP 157.55.2.1 envía datos a un usuario en 147.20.4.5, coincidiría con el filtro IP Legal 2. Esto significaría que la comunicación se envía en el nivel de seguridad especificado por la política de negociación Legal NP1, que proporciona autenticación y protección contra modificaciones (no modificable) y confidencialidad durante la comunicación.

## Diagramas de una instalación básica

En el siguiente ejemplo, un usuario en el *Host* A manda datos a un usuario en el *Host* B. La Seguridad IP de Windows se ha implementado para ambas computadoras.

Al nivel de usuario, el proceso de seguridad de los paquete IP es transparente. El usuario 1 lanza una aplicación que utiliza al protocolo TCP/IP, como el FTP, y envía los datos al usuario 2.

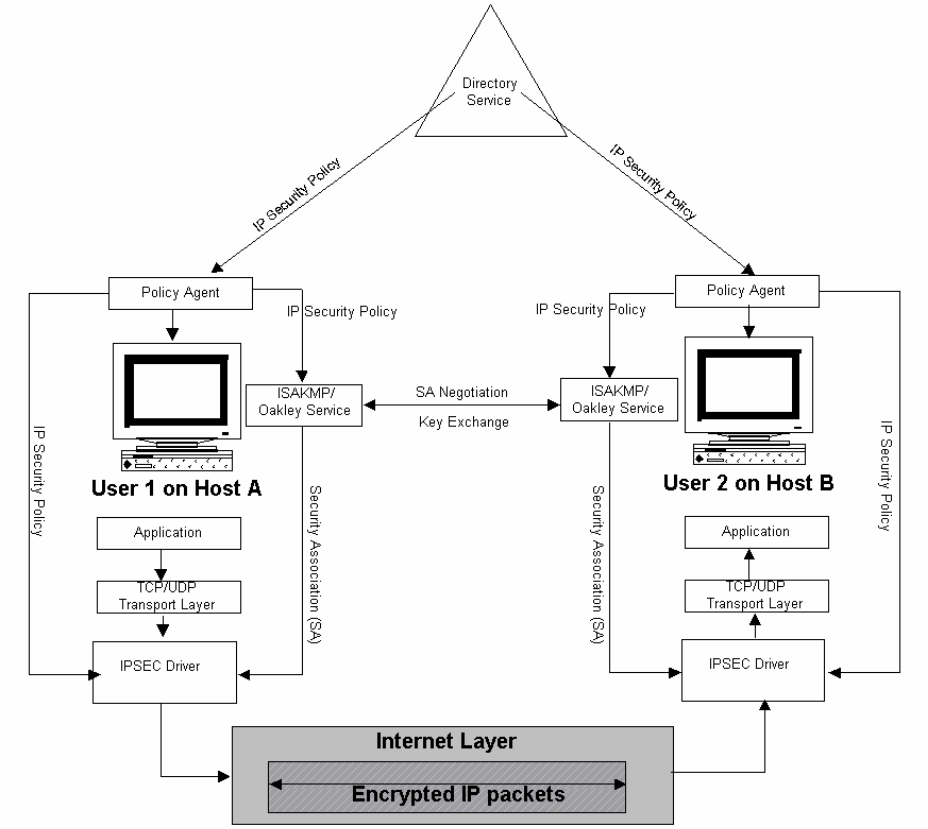


*Figura 2. Ejemplo de una instalación de Seguridad IP de Windows.*

Las políticas de seguridad que el administrador asignó al *Host* A y *Host* B determinan el nivel de seguridad de la comunicación. Estas son seleccionadas por el agente de políticas y se pasan al servicio ISAKMP/Oakley y al controlador IPSEC. El servicio ISAKMP/Oakley de cada computadora utiliza las políticas de negociación asociadas con la política de seguridad asignada para establecer la clave y un método común de negociación (una asociación de seguridad). Los resultados de la negociación de políticas ISAKMP entre las dos computadoras se pasan al controlador IPSEC, que utiliza la clave para codificar los datos. Finalmente, el controlador IPSEC envía los datos codificados al *Host* B. El controlador IPSEC en el *Host* B decodifica los datos y los pasa a la aplicación receptora.

### Notas de compatibilidad

A fin de asegurar una compatibilidad total de comunicaciones con Windows 9x y versiones anteriores de Windows NT, una computadora que ejecuta Windows 2000 configurada para Seguridad IP envía los datos sin codificación a una computadora que no ejecuta Windows 2000.

Cualquier enrutador o *switch* que esté en la ruta de los *hosts* en comunicación, ya sean dos usuarios o un usuario y un servidor de archivos, simplemente debe enviar los paquetes IP codificados directamente hacia su destino. Si existe un *firewall* u otra *gateway* de seguridad entre los *hosts* en comunicación, es necesario habilitar envíos IP o filtros especiales que permitan la retransmisión de los paquetes de Seguridad IP para que alcancen su destino correctamente.

## RESUMEN

La Seguridad IP de Windows integrada en Windows 2000 Server proporciona a los administradores de red una línea muy importante de seguridad. Ya que la Seguridad IP de Windows se instala abajo del nivel de transporte, la instalación de seguridad se simplifica enormemente. La actualización a Windows 2000 Server proporciona protecciones de integridad, autenticación y confidencialidad sin tener que actualizar las aplicaciones ni capacitar a los usuarios.

La Seguridad IP de Windows es una implementación del Protocolo de seguridad IP de Internet Engineering Task Force, lo cual asegura una máxima interoperabilidad con soluciones IPSec instaladas en otras redes.

La flexibilidad y la administración centralizada hacen que la Seguridad IP de Windows sea fácil de administrar, y los administradores de red puedan crear políticas de seguridad y filtros personalizados, basados en usuarios, grupos de trabajo u otros criterios.

La seguridad de extremo a extremo asegura que los datos enviados a través de cualquier red: LAN, WAN o Internet mantengan su integridad y confidencialidad durante el recorrido; también asegura que los datos solo sean accedidos por los usuarios autenticados.

En un momento en que la seguridad de red es cada vez más importante, Windows 2000 Server facilita que los administradores de red puedan proporcionar un poderoso nivel de protección a los recursos de información de su organización.

## PARA MAYORES INFORMES

Para la información más reciente sobre Windows 2000 Server, consulte el sitio Web en http://www.microsoft.com/ntserver o el Foro Windows NT Server en la Red Microsoft (GO WORD: MSNTS).

Para los borradores IPSec IETF más recientes consulte:

www.ietf.org/html.charters/ipsec-charter.html