(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 439 765**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.07.2009 E 09780451 (2)**

(97) Fecha y número de publicación de la concesión europea: **18.09.2013 EP 2452476**

(54) Título: **Método para seleccionar una política IPsec**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.01.2014

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

KRUPP, DANIEL y
SZABÓ, GERGELY

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método para seleccionar una política IPsec

Campo técnico

La invención se refiere a una Base de Datos de Políticas de Seguridad en una red de comunicación, y en particular a consultar y rellenar una Base de Datos de Políticas de Seguridad.

Antecedentes

La arquitectura de seguridad para el Protocolo de Internet (IPsec) se describe en la RFC 4301: “Security Architecture for the Internet Protocol”. La RFC 4301 describe una estructura para protección de tráfico IP que está basada en requerimientos definidos por una Base de Datos de Políticas de Seguridad (SPD). Una SPD está almacenada y mantenida en un nodo, y se establece y mantiene por un usuario o administrador de sistemas, o por una aplicación que opera dentro de las restricciones establecidas o bien por un usuario o bien por un administrador de sistemas de la anterior.

Una política de seguridad (SP) contenida en la SPD es una regla que dice a un nodo que recibe un paquete IP cómo procesar ese paquete. Una SP puede definir qué tipo de paquetes se deberían procesar usando IPsec, cómo se debería aplicar la IPsec, etc.

Cuando un nodo envía o recibe un paquete IP, se debe consultar a la SPD si el tráfico se envía en una interfaz habilitada IPsec, con independencia de ya sea IPsec o no IPsec. Los equipos de telecomunicación que implementan la estructura IPsec necesitan almacenar ocasionalmente un alta cantidad de políticas, de esta manera el tamaño de la SPD puede ser grande. La operación de emparejamiento de política para cada paquete IP se debe realizar tan rápidamente como sea posible a fin de mantener la capacidad de red del nodo.

La RFC 4301 no define la estructura de una SPD o cómo debería hacer de interfaz con otras funciones. No obstante, la RFC 4301 especifica que la SPD debe almacenar las SP como una lista ordenada de entradas. Un ejemplo de una estructura SPD existente implementada en núcleos FreeBSD 7.0 o Linux 2.6.x se describe en USAGI IPv6 IPsec Development para Linux. Mitsuru Kanda, Kazunori Miyazawa, Hiroshi Esaki http://hiroshi1.hongo.wide.ad.jp/hiroshi/papers/SAINT2004_kanda-ipsec.pdf. Este documento describe un esquema de ordenación y almacenamiento de políticas en el que el coste algorítmico de búsqueda de políticas aumenta linealmente con el número de las SP almacenadas en el caso de que no se pueda encontrar ninguna SP relevante. Cuando una nueva SP se suministra en la SPD, se suministra en secuencia; en otras palabras, el orden de las políticas en la SPD se determina por la secuencia en la que fueron introducidas. El tiempo de búsqueda de SP por lo tanto depende de cuándo fue suministrada la SP en la SPD. A fin de mejorar el tiempo de búsqueda de la SP, se puede emplear un almacenamiento en caché para asegurar que una política que aplica a un paquete se puede almacenar en caché y posteriormente recuperar desde la caché y aplicar a paquetes posteriores que requieren la misma política.

La publicación WO 2005/010777-A1 también se debería mencionar como una técnica anterior relevante, dado que describe un método de consulta de una base de datos de Políticas de Seguridad IPsec. No obstante la publicación mencionada no dice nada acerca de determinar un valor de la más alta prioridad de Política de Seguridad y no distingue expresamente entre los eventos de cuándo se debería aplicar, o no, una acción de Política de Seguridad a un paquete IP.

Compendio

Los inventores han reconocido que la velocidad de búsqueda de una Política de Seguridad (SP) almacenada en una Base de Datos de Políticas de Seguridad (SPD) puede ser lenta, y han ideado métodos de consulta y relleno de una SPD que proporcionan una búsqueda de SP más rápida que los métodos conocidos.

Según un primer aspecto de la invención, hay proporcionado un método de consulta de una SPD IPsec que comprende una pluralidad de grupos de SP a los que se han asignado un valor de prioridad. Los siguientes pasos se llevan a cabo:

a) un nodo de red recibe un paquete IP;

b) se determina un valor de la más alta prioridad de SP;

c) la base de datos de Protocolos de Seguridad IPSec se consulta para un conjunto de SP que tiene el valor de prioridad de SP determinado;

d) se hace una determinación en cuanto a si una acción de SP del conjunto de SP se debería aplicar al paquete IP;

e) en el caso de que se debiera aplicar una acción de SP al paquete IP, la SP se devuelve y aplica al paquete IP.

No obstante, si no se debiera aplicar ninguna acción de SP del conjunto de SP al paquete IP, entonces se determina un valor de prioridad de SP inferior y se repiten los pasos c) a e). Adicionalmente, si no hay un conjunto de SP que tengan un grupo de prioridad inferior, se hace una determinación de que no se puede encontrar ninguna SP para aplicar al paquete IP.

Como opción, se usa una información de la cabecera del paquete IP para determinar si se debería aplicar una SP al paquete IP. Como una opción adicional, el método además comprende calcular un valor de troceo usando información de la cabecera del paquete IP, comparando el valor de troceo calculado para el paquete IP con los valores de troceo asociados con una lista vinculada de SP. En el caso de que los valores de troceo se emparejen, se hace una determinación de si se debería aplicar una acción de SP contenida en la lista vinculada de SP al paquete IP, y en el caso de que los valores de troceo no se emparejen, se hace una determinación de que no se debería aplicar ninguna acción de SP a partir de la lista vinculada de SP al paquete IP. Como opción adicional, el método usa información seleccionada de cualquiera de un prefijo fuente, un puerto fuente, un prefijo de destino, un puerto de destino y un Protocolo de Capa Superior.

Hay también proporcionado un método de rellenado de una base de datos de SP IPsec. Un nodo de red recibe una SP a ser insertada en la base de datos de SP y calcula un valor de prioridad para asignar a la política. Se sitúa un grupo de políticas almacenadas en la base de datos que tienen el mismo valor de prioridad que el valor calculado, y la SP se almacena en ese grupo de políticas en la SPD.

En una realización opcional, en el caso de que un grupo que tiene el mismo valor de prioridad no esté disponible en la base de datos de SP, entonces se crea un nuevo grupo en la SPD que tiene el valor de prioridad.

Como opción, el método además comprende calcular un valor de troceo para la SP usando información contenida en los campos de Selector de SP y asociando el valor de troceo con la SP en la SPD. Como opción adicional, se selecciona la información a partir de cualquiera de un prefijo fuente, un puerto fuente, un prefijo de destino, un puerto de destino y un Protocolo de Capa Superior.

Según un segundo aspecto de la invención, hay proporcionado un nodo para usar en una red de comunicación. El nodo está dotado con una SPD IPsec que almacena una pluralidad de SP dispuestas en grupos de políticas cada grupo de políticas al que se ha asignado un valor de prioridad. También se proporciona una función de consulta para consultar la SPD para encontrar un emparejamiento para un paquete IP buscando grupos de SP en orden descendente de valor de prioridad hasta que se encuentra un emparejamiento o se determine que no se debería aplicar ninguna SP al paquete IP.

Como opción, el nodo además comprende un receptor para recibir un paquete IP, una función IPsec para aplicar una acción para la SP emparejada al paquete IP, y un transmisor para enviar el paquete IP a un nodo de red adicional.

Como opción adicional, la función de consulta se dispone para calcular un valor de troceo usando información contenida en la cabecera del paquete IP, y la función de consulta se dispone además para comparar el valor de troceo calculado con un valor de troceo asociado con un grupo de SP para determinar si se debería aplicar una SP al paquete IP.

También hay proporcionado un nodo para rellenar una SPD IPsec que almacena una pluralidad de SP dispuestas en grupos de políticas. El nodo está dotado con un receptor para recibir una SP a ser insertada en la SPD y un procesador dispuesto para calcular un valor de prioridad a asignar a la SP y almacenar la SP con un grupo de políticas que tiene el valor de prioridad en la SPD.

El procesador está dispuesto opcionalmente para crear un nuevo grupo en la SPD en el caso de que un grupo que tiene el mismo valor de prioridad no esté ya disponible en la base de datos de SP.

El procesador está dispuesto opcionalmente además para calcular un valor de troceo para la SP usando información contenida en un campo de Selector de SP, y asociar el valor de troceo con la SP en la SPD.

Según un tercer aspecto de la invención, hay proporcionado un programa de ordenador, que comprende un código legible por ordenador que, cuando se ejecuta en un nodo de red programable, hace a la red programable realizar un método como se describió anteriormente en el primer aspecto de la invención.

Según un cuarto aspecto de la invención, hay proporcionado un medio de registro que almacena el código legible por ordenador descrito anteriormente en el tercer aspecto de la invención.

Según un quinto aspecto de la invención, hay proporcionado un medio portador que transporta el código legible por ordenador descrito anteriormente en el tercer aspecto de la invención.

Según un sexto aspecto de la invención, hay proporcionado un nodo de red que tiene instalado en el mismo el programa descrito anteriormente en el tercer aspecto de la invención.

Breve descripción de los dibujos

Algunas realizaciones preferidas de la invención se describirán ahora a modo de ejemplo solamente y con referencia a los dibujos anexos, en los que:

La Figura 1 ilustra esquemáticamente en un diagrama de bloques una Base de Datos de Políticas de Seguridad y estructura según una realización de la invención;

La Figura 2 es un diagrama de flujo que muestra una operación de inserción cuando se suministra una nueva Política de Seguridad en una Base de Datos de Políticas de Seguridad según una realización de la invención;

La Figura 3 ilustra esquemáticamente en un diagrama de bloques una correlación de bit de función de prioridad ejemplo según una realización de la invención;

La Figura 4 es un diagrama de flujo que muestra una operación de búsqueda en una Base de Datos de Políticas de Seguridad según una realización de la invención;

La Figura 5 es un diagrama de flujo que muestra una operación de búsqueda de emparejamientos en una Base de Datos de Políticas de Seguridad según una realización de la invención;

La Figura 6 ilustra esquemáticamente en un diagrama de bloques un nodo para realizar una operación de búsqueda de políticas; y

La Figura 7 ilustra esquemáticamente en un diagrama de bloques un nodo para rellenar una base de datos de Políticas de Seguridad.

Descripción detallada

Con referencia a la Figura 1, se ilustra una Base de Datos de Políticas de Seguridad (SPD) 1. Una pluralidad de Políticas de Seguridad (marcadas SP en la Figura 1) se suministran en la base de datos 1. A diferencia de las SPD de la técnica anterior, las SP se agrupan juntas en grupos de SP (2, 4, 6) que tienen el mismo valor de prioridad. Un valor de prioridad es un valor asignado a cada SP cuando se suministra en la base de datos.

Como se ve a partir de la Figura 1, varias SP puede ser otorgadas todas con el mismo valor de prioridad, y así se agruparían todas juntas en un grupo de políticas único (2, 4, 6). Los grupos de políticas en la lista ordenada requerida por la RFC 4301 están ordenados por el valor de prioridad de las políticas contenidas.

Cuando se recibe un paquete IP en un nodo de red (por ejemplo, en una Función de Control de Sesión de Llamada en una red IMS), el nodo debe comprobar para ver, en su caso, qué SP aplican al paquete IP. Hace esto consultando la SPD. Los grupos de SP se comprueban a su vez para las SP emparejadas al paquete IP. El grupo con la más alta prioridad se comprueba primero, y si no se encuentra ninguna SP emparejada entonces se comprueba el grupo con la siguiente prioridad más alta, y así sucesivamente, hasta que una SP se devuelve y aplica al paquete IP, o se devuelve un mensaje informando al nodo que ninguna SP se emparejan al paquete. En el caso de que ninguna SP se empareje al paquete, no se aplicará IPsec al paquete.

Cada SP almacenada en la SPD comprende un selector y una o más acciones, y se puede indicar: SP: (SELECTOR, ACTION [, ACTION….])

Se demanda un selector para determinar si se debería aplicar la SP a un paquete IP. Si un paquete IP se empareja al selector de una SP entonces necesitan ser ejecutadas las acciones definidas por esa SP dada. El selector se define como sigue:

SELECTOR: (SOURCE_ADDRESS, SOURCE_PREFIX, DESTINATION_ADDRESS, DESTINATION_PREFIX, SOURCE_PORT, DESTINATION_PORT, UPPER_LAYER_PROTOCOL)

Una dirección fuente y una dirección de destino son cada una un número de 32 bit (en el caso de IPv4) o de 128 bit (en el caso de IPv6), y se pueden indicar:

SOURCE_ADDRESS: <32 bit integer> | <128 bit integer>

DESTINATION_ADDRESS: <32 bit integer> | <128 bit integer>

Los números de prefijo fuente y destino representan el número de los bits valiosos en una dirección fuente o de destino de selector respectivamente. Los bits valiosos se cuentan siempre desde los bits más significativos a los bits menos significativos en las direcciones fuente o de destino. Los prefijos fuente y de destino se indican como sigue:

SOURCE_PREFIX: <0-32> | <0-128>

DESTINATION_PREFIX: <0-32> | <0-128>

El protocolo de capa superior es un número que se almacena en el campo de Protocolo de un datagrama de IPv4 o en el campo de Siguiente Cabecera de un datagrama de IPv6. En caso de una descripción de selector el protocolo de capa superior se puede fijar al valor ANY, como sigue:

UPPER_LAYER_PROTOCOL: <8 bit integer> ANY

Los puertos fuente y de destino son números de puertos usados por el protocolo de capa superior. En caso de una descripción de selector los puertos fuente y de destino se pueden fijar al valor ANY como sigue:

SOURCE_PORT: <16 bit integer> | ANY

DESTINATION_PORT: <16 bit integer> | ANY

Las acciones asignadas a una SP dada se ejecutan en el caso de que un paquete IP se empareje al selector de la SP. Las acciones pueden variar desde descartar el paquete de emparejamiento a requerir procesamiento IPsec. Las acciones descritas en la presente memoria se proporcionan a modo de ejemplo solamente.

Cuando se suministra una nueva SP en la SPD, se realiza una operación de inserción. La operación de inserción no es frecuente; y así no necesita ser optimizada en términos de tiempo de ejecución. La operación de inserción se describe como:

insert(SPD, SP)

La Figura 2 ilustra los pasos de insertar una SP, con la siguiente numeración que corresponde a la numeración de la Figura 2

S1. Se recibe una nueva SP, por ejemplo en una CSCF en una red IMS.

S2. Una función de prioridad calcula un valor de prioridad de la SP a ser insertada:

p = priority(SP.SELECTOR).

Un valor de prioridad puede ser, por ejemplo, un número entero para un SELECTOR: priority(SELECTOR) -> integer dado.

El valor de prioridad de una SP no es necesariamente único dentro de una SPD, ya que se puede otorgar a muchas SP el mismo valor de prioridad.

Cuando se inserta una política en la SPD 1, se calcula un valor de prioridad en base a los campos de SELECTOR y se inserta en un Grupo de Políticas que corresponde al valor de prioridad dado. El Grupo de Políticas se etiqueta por los campos de SELECTOR de la política, que fueron usados para calcular la prioridad del Grupo de Políticas. Por lo tanto cada grupo de políticas está etiquetado mediante: los valores SOURCE_PREFIX, DESTINATION_PREFIX, los campos de comodín SOURCE_PORT, comodín DESTINATION_PORT y comodín UPPER_LAYER_PROTOCOL.

Una implementación ejemplar de la función de prioridad es para que la función de prioridad correlacione los valores de SOURCE_PREFIX, DESTINATION_PREFIX, SOURCE_PORT, DESTINATION_PORT y UPPER_LAYER_PROTOCOL a una correlación de bits. Una correlación posible se muestra en la Figura 3, en la que los valores SOURCE_PREFIX 8 y DESTINATION_PREFIX 10 se almacenan en los bits 0-6 y 8-15. El 7º bit se fija a 0 a menos que el SOURCE_PORT 9 sea ANY. El 16º bit se fija a 0 a menos que el DESTINATION_PORT 11 sea ANY. El 17º bit también se fija a 0 a menos que el UPPER_LAYER_PROTOCOL 12 sea ANY. Por supuesto, se pueden fijar otras correlaciones de bits por los operadores de red dependiendo de los requerimientos de la SP.

S3. Se realiza una búsqueda para el grupo de políticas con el mismo valor de prioridad en la cadena de grupo de políticas. Para acelerar el proceso de búsqueda se puede usar una tabla de troceo auxiliar, como se describe más adelante.

S4. Si se encuentra un grupo de políticas con el mismo valor de prioridad, entonces la operación continúa en el paso S6. Si no entonces la operación continúa en el paso S5.

S5. Ya que se encontró un grupo de políticas que tiene un valor de prioridad p, se crea un nuevo grupo de políticas.

S6. Se calcula un valor de troceo usando una función de troceo del grupo de políticas. La entrada para la función de troceo se compone de los bits seleccionados del campo de SELECTOR de SP. Los bits seleccionados son:

a. los bits especificados en los campos de dirección fuente y de destino que no se enmascaran

b. el SOURCE_PORT a menos que esté fijado a ANY

c. el DESTINATION_PORT a menos que esté fijado a ANY

d. el UPPER_LAYER_PROTOCOL a menos que esté fijado a ANY

La SP se inserta al frente de la lista vinculada designada por el valor de troceo calculado.

Señalar que, este ejemplo describe una estructura de lista vinculada, pero puede ser cualquier estructura ordenada dinámica.

En algunas circunstancias (por ejemplo mantenimiento de la base de datos), se requiere una operación de búsqueda para asegurar que la base de datos contiene información actualizada y relevante. Una operación de búsqueda se usa para recuperar una SP con un SELECTOR particular de la SPD 1, y se puede describir como:

lookup(SPD, SELECTOR) -> SP | NO_SP_FOUND

La Figura 4 muestra los pasos de una operación de búsqueda, con la siguiente numeración que corresponde a aquélla de la Figura.

S7. En el inicio de la operación de búsqueda, se calcula el valor de prioridad del SELECTOR a ser buscado:

p = priority(SELECTOR)

S8. Se consulta el grupo de políticas que tiene el mismo valor de prioridad. Para acelerar el proceso de búsqueda se puede usar una tabla de troceo auxiliar.

S9. Si se encuentra el grupo de políticas, entonces la operación continúa en el paso S11, y si no se encuentra el grupo de políticas que tiene el valor de prioridad entonces la operación continúa en el paso S10.

S10. El grupo de políticas no se encuentra, y este resultado se devuelve a un nodo que solicita la búsqueda de política.

S11. Se encuentra el grupo de políticas que tiene el mismo valor de prioridad que el selector, y así se realiza una búsqueda de las SP en el grupo de políticas. Se calcula un valor de troceo usando una función de troceo de grupo de políticas, de la misma forma que se describió anteriormente en el paso S6. Se realiza una búsqueda de la lista vinculada usando el valor de troceo calculado para la SP con el campo de SELECTOR especificado.

S12. Si se encuentra la SP, la operación continúa en el paso S14, de otro modo la operación continúa en el paso S13.

S13. No se encuentra la SP, y este resultado se devuelve a un nodo solicitante de la búsqueda de política.

S14. La SP se devuelve al nodo solicitante de la búsqueda de política.

Para mantenimiento de la base de datos, puede ser deseable eliminar una SP desactualizada o incorrecta de la SPD 1. En este caso, se realiza una operación de borrado, la cual se describe como:

delete(SPD, SELECTOR)

La operación de borrado se puede realizar mediante una operación de búsqueda seguida por una operación de eliminación del elemento de la lista vinculada que contiene la SP especificada. Como la operación de borrado se realiza con poca frecuencia, no necesita ser optimizada en términos de tiempo de ejecución.

La operación más común es una operación de búsqueda de emparejamiento. Cuando un paquete IP va a ser enviado, el nodo debe determinar si se debería aplicar o no una SP al paquete, y si es así entonces qué SP se debería aplicar al paquete. La operación de búsqueda de emparejamiento devuelve la SP con el valor de la más alta prioridad que tiene selectores que emparejan el paquete IP dado. En el caso de que más de una SP se empareje al paquete IP, entonces solamente se devuelve la SP con el valor de la más alta prioridad. Como la operación de búsqueda de emparejamiento es una operación frecuente, debe estar altamente optimizada.

La operación de emparejamiento se describe como:

matchlookup(SPD, IP) -> SP | NO_SP_FOUND

donde

matched(IP, SP.selector) == verdadero

y no hay SP_i en la SPD donde

matched(IP, SP_i.selector) AND priority(SP_i.SELECTOR) > priority(SP)

Una operación de búsqueda de emparejamiento se ilustra en la Figura 5, con la siguiente numeración que

corresponde a la numeración de la Figura 5:

S15. Un nodo tal como una CSCF recibe un paquete IP y debe tomar una decisión acerca de aplicar una Política de Seguridad al paquete.

S16. Se consulta la SPD 1. El primer grupo de políticas buscado es el grupo que tiene el valor de la más alta prioridad.

S17. Tomar los bits valiosos de la cabecera del paquete IP lo cual se determina por la Etiqueta de SELECTOR del Grupo de Políticas. Se calcula un valor de troceo usando una función de troceo. La entrada para la función de troceo está compuesta de los bits valiosos de los campos de cabecera IP. Los bits valiosos son:

a. los bits especificados en el campo de dirección fuente que no están enmascarados por la mask (IP.SOURCE_ADDRESS, PGROUP.SOURCE_MASK)

b. los bits especificados en el campo de dirección de destino que no están enmascarados por la mask (IP.DESTINATION_ADDRESS, PGROUP.DESTINATION_MASK)

c. el IP.SOURCE_PORT a menos que el PGROUP.SOURCE_PORT esté fijado a ANY

d. el IP.DESTINATION_PORT a menos que el PGROUP.DESTINATION_PORT esté fijado a ANY

e. el IP.UPPER_LAYER_PROTOCOL a menos que el PGROUP.UPPER_LAYER_PROTOCOL esté fijado a ANY

El valor de troceo calculado se compara frente a los valores de troceo almacenados para una lista vinculada de las SP en el grupo de políticas que tienen el valor de prioridad que usa una función 'emparejada'. Emparejada es una operación Booleana que comprueba si un datagrama IP empareja un selector dado. Esta operación se llama para todos los paquetes IP entrantes y salientes para determinar qué política, en su caso, aplica al paquete IP.

matched(IP, SELECTOR) -> verdadero | falso

Esta operación se puede describir con el siguiente pseudo código:

(mask (IP.SOURCE_ADDRESS, SELECTOR.SOURCE_PREFIX) == SELECTOR.SOURCE_ADRESS)

Y

(mask (IP.DESTINATION_ADDRESS, SELECTOR.DESTINATION_PREFIX) == SELECTOR.DESTINATION_ADRESS)

Y

(IP.SOURCE_PORT == SELECTOR.SOURCE_PORT || SELECTOR.SOURCE_PORT == ANY)

Y

(IP.DESTINATION_PORT == SELECTOR.DESTINATION_PORT || SELECTOR.DESTINATION _PORT == ANY)

Y

(IP.UPPER_LAYER_PROTOCOL == SELECTOR.UPPER_LAYER_PROTOCOL || SELECTOR.UPPER_LAYER_PROTOCOL == ANY)

S18. Si el valor de troceo calculado empareja un valor de troceo de SP almacenado en la SPD 1, entonces la operación continúa en el paso S22, de otro modo la operación continúa en el paso S19.

S19. Ya que no fue encontrado ningún emparejamiento de SP en el grupo de políticas previo, se hace una determinación para determinar si existe un grupo de políticas adicional que tenga un valor de prioridad inferior. Si es así, entonces la operación continúa en el paso S21, y si no entonces la operación continúa en el paso S20.

S20. En este punto en la operación, se han consultado todos los grupos de políticas y no se ha encontrado ninguna SP que aplique al paquete IP, así se devuelve un resultado de no encontrada ninguna SP. El paquete IP entonces se procesa sin usar ninguna SP.

S21. Se selecciona el grupo de políticas con el siguiente valor de la más baja prioridad, y la operación se repite desde el paso S17.

S22. Se hace una determinación para encontrar una SP en la lista vinculada de SP que empareja el paquete IP. Si se encuentra una SP, entonces el proceso continúa en el paso S23, de otro modo el proceso regresa al paso S19.

S23. Se ha encontrado una SP en el grupo con la más alta prioridad y se devuelve esta SP. La SP entonces se

aplica al paquete IP.

En términos del coste algorítmico de las operaciones descritas anteriormente, la operación de inserción, la operación de búsqueda y la operación de borrado cada una requiere dos búsquedas de tabla de troceo de políticas almacenadas en la SPD. Una operación de búsqueda de emparejamiento requiere que se haga un intento para emparejar el paquete IP con una SP almacenada en el grupo de políticas con la más alta prioridad y este proceso continúa hasta que se encuentra la primera SP de emparejamiento. Si hay P grupos de políticas, entonces en el escenario del peor caso, se deben realizar P búsquedas de troceo. Será evidente que el número máximo de grupos de políticas es independiente del número de SP almacenadas en la SPD. Él solamente depende de la longitud de los campos de selector usados para el cálculo de la prioridad. De esta manera el coste de búsqueda de emparejamiento es O(1) con el número de políticas almacenadas en la SPD.

Volviendo ahora a la Figura 6, se ilustra un nodo 13 tal como una CSCF para realizar una operación de búsqueda de políticas. Se proporciona un receptor 14 para recibir un paquete IP. Una función de consulta 15, típicamente implementada como un procesador, se proporciona para consultar la SPD 1 y obtener de la SPD una SP de emparejamiento devuelta. Señalar que en este ejemplo, la SPD se sitúa en el nodo, pero en muchas implementaciones la SPD se situará remotamente del nodo. Una función IPsec 16 se proporciona para aplicar una acción para la SP de emparejamiento devuelta al paquete IP. También se proporciona un transmisor 17 para enviar el paquete IP a un nodo de red adicional. La SPD 1 ilustrada en la Figura 6 está estructurada y opera de la misma forma que la SPD ilustrada en la Figura 1.

Volviendo ahora a la Figura 7, se ilustra un nodo 18 para rellenar una base de datos de Políticas de Seguridad SPD 1. El nodo 18 está dotado con un receptor 19 para recibir una SP a ser insertada en la SPD 1, y un procesador 20 dispuesto para calcular un valor de prioridad para asignar a la SP y almacenar la SP con un grupo de políticas que tiene el valor de prioridad en la SPD 1. La invención introduce una ordenación de políticas basada en selector. La RFC 4301 no especifica un método de ordenación pero requiere a la SPD 1 estar ordenada. Una función de prioridad bien elegida facilita la coordinación de múltiples usuarios de la SPD, ya que esta solución es menos propensa a una anulación no deseada de políticas. Otra ventaja es la eficiente operación de búsqueda de emparejamiento, que es la operación más común en la SPD. Las políticas se devuelven sobre la base de un valor de prioridad asignado, en lugar de sobre la base de cuándo fueron suministradas en la SPD 1.

La invención se describe a modo de ejemplo con referencia a una CSCF en una red IMS, pero se apreciará que puede aplicarse igualmente a cualquier tipo de red que use Políticas de Seguridad IPsec.

Las siguientes abreviaturas se han usado en esta especificación:

IP Protocolo de Internet

SP Política de Seguridad

SPD Base de Datos de Políticas de Seguridad

TCP Protocolo de Control de Transmisión

UDP Protocolo de Datagrama de Usuario

REIVINDICACIONES

1. Un método de consulta de una base de datos de Políticas de Seguridad IPSec (1) que comprende una pluralidad de grupos de Políticas de Seguridad, cada grupo de Políticas de Seguridad que tiene un valor de prioridad, el método que comprende:

a) en un nodo de red, recibir un paquete IP (S15);

b) determinar un valor de la más alta prioridad de Política de Seguridad;

c) consultar la base de datos de Protocolos de Seguridad IPSec para un conjunto de Políticas de Seguridad que tiene el valor de prioridad de Política de Seguridad (S16);

d) determinar si una acción de Política de Seguridad del conjunto de Políticas de Seguridad se debería aplicar al paquete IP (S17, S18);

e) en el caso de que una acción de Política de Seguridad se debiera aplicar al paquete IP, aplicar la acción de Política de Seguridad al paquete IP (S22, S23), y en el caso de que no se debiera aplicar ninguna acción de Política de Seguridad del conjunto de Políticas de Seguridad al paquete IP, determinar un valor de prioridad de Política de Seguridad inferior y repetir los pasos c) a e) (S21) y, en el caso que no haya ningún valor de prioridad de Política de Seguridad inferior, determinar que no se puede encontrar ninguna Política de Seguridad (S20).

2. El método según la reivindicación 1, que además comprende usar información de la cabecera del paquete IP para determinar si se debería aplicar una Política de Seguridad al paquete IP (S17, S18).

3. El método según la reivindicación 1 o 2, que además comprende:

calcular un valor de troceo que usa información de la cabecera del paquete IP (S17),

comparar el valor de troceo calculado para el paquete IP con los valores de troceo asociados con una lista vinculada de Políticas de Seguridad (S17);

en el caso de que los valores de troceo se emparejen, determinar si se debería aplicar una acción de Política de Seguridad contenida en la lista vinculada de Políticas de Seguridad al paquete IP (S22, S23), y en el caso de que los valores de troceo no se emparejen, determinar que no se debería aplicar ninguna acción de Política de Seguridad de la lista vinculada de Políticas de Seguridad al paquete IP (S20).

4. El método según la reivindicación 2 o 3, que comprende usar información seleccionada de cualquiera de un prefijo fuente, un puerto fuente, un prefijo de destino, un puerto de destino y un Protocolo de Capa Superior.

5. Un nodo (13) para uso en una red de comunicación, el nodo que comprende

una base de datos de Políticas de Seguridad (1) que almacena una pluralidad de Políticas de Seguridad dispuestas en grupos de políticas, cada grupo de políticas que tiene un valor de prioridad;

una función de consulta (15) para consultar la base de datos de Políticas de Seguridad para encontrar un emparejamiento para un paquete IP buscando grupos de Políticas de Seguridad en orden descendente de valor de prioridad hasta que se encuentra un emparejamiento

y el nodo (13) que está adaptado además para realizar el método como se define en la reivindicación 1.

6. El nodo según la reivindicación 5, que comprende

un receptor (14) para recibir un paquete IP;

una función IPsec (16) para aplicar una acción para la Política de Seguridad que empareja el paquete IP; y

un transmisor (17) para enviar el paquete IP a un nodo de red adicional.

7. El nodo según la reivindicación 5 o 6, en donde la función de consulta (15) está dispuesta para calcular un valor de troceo usando información contenida en la cabecera del paquete IP, y la función de consulta (15) está dispuesta además para comparar el valor de troceo calculado con un valor de troceo asociado con una lista vinculada de grupo de Políticas de Seguridad para determinar si se debería aplicar una Política de Seguridad al paquete IP.

8. Un programa de ordenador, que comprende un código legible por ordenador el cual, cuando se ejecuta en un nodo de red programable, hace a la red programable realizar un método según cualquiera de las reivindicaciones 1 a 4.

9. Un medio de registro que almacena un código legible por ordenador según la reivindicación 8.

10. El programa de la reivindicación 8, transportado en un medio portador.

11. Un nodo de red que ha instalado en el mismo el programa de la reivindicación 8.

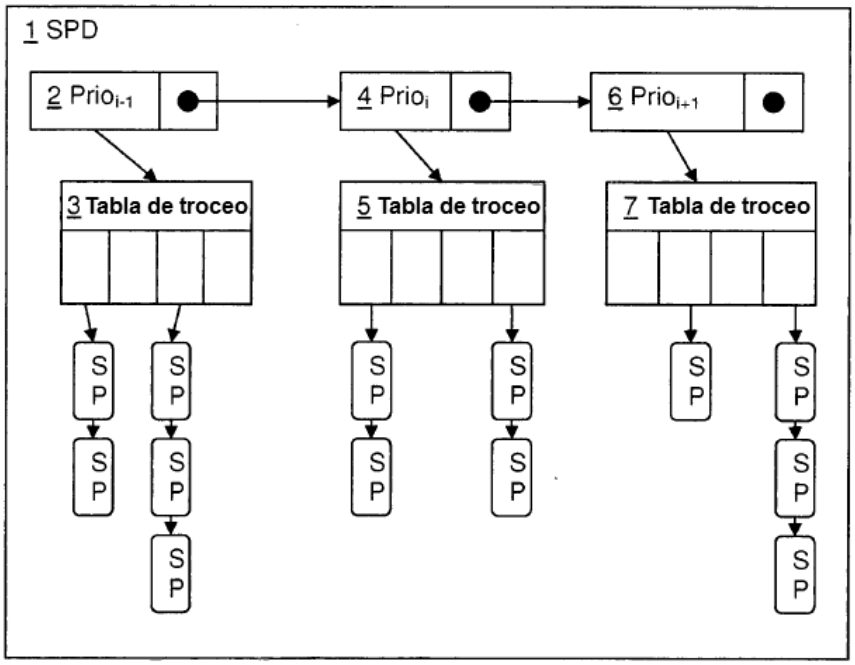
1 SPD
2 Prio$_{i-1}$
4 Prio$_i$
6 Prio$_{i+1}$
3 Tabla de troceo
5 Tabla de troceo
7 Tabla de troceo
SP

Figura 1

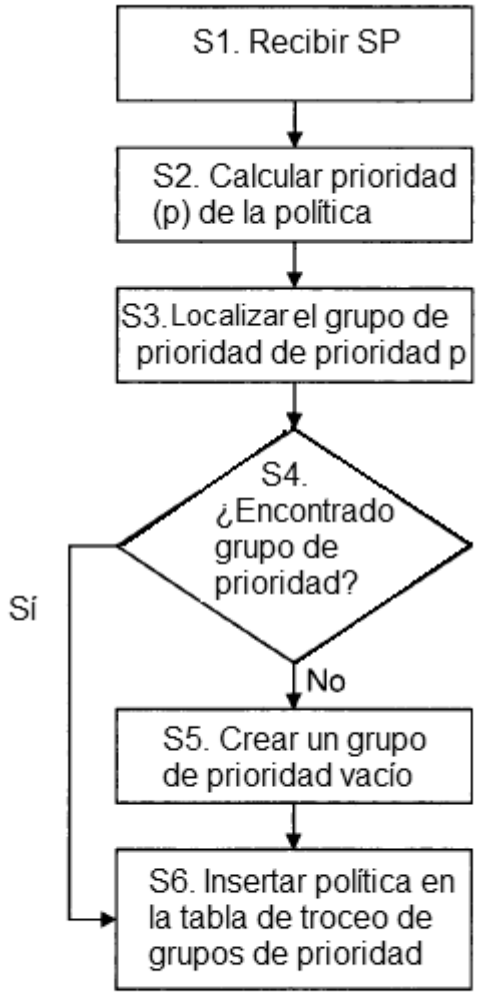

Figura 2

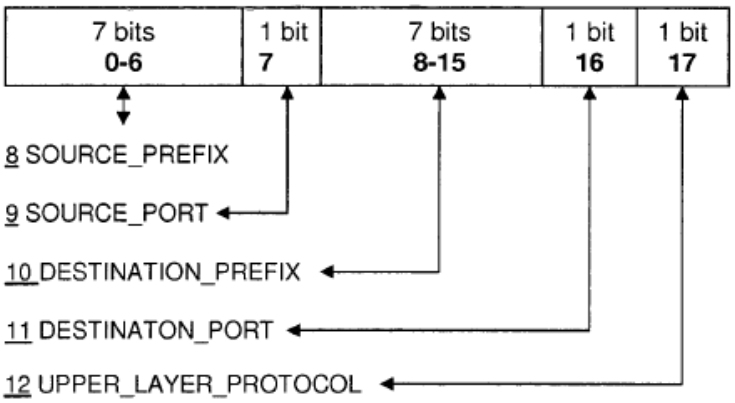

Figura 3

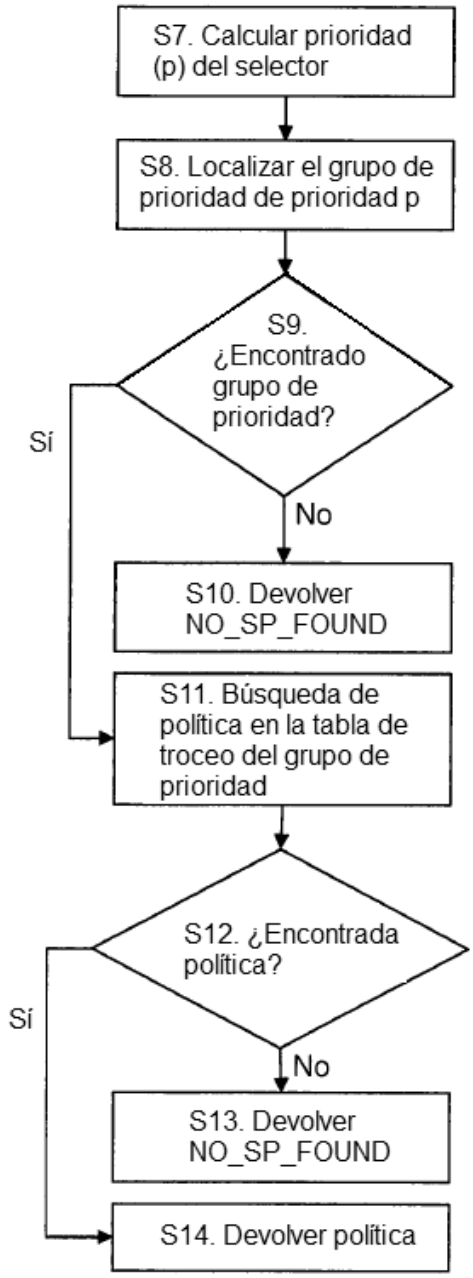
S7. Calcular prioridad (p) del selector
S8. Localizar el grupo de prioridad de prioridad p
S9. ¿Encontrado grupo de prioridad?
Sí
No
S10. Devolver NO_SP_FOUND
S11. Búsqueda de política en la tabla de troceo del grupo de prioridad
S12. ¿Encontrada política?
Sí
No
S13. Devolver NO_SP_FOUND
S14. Devolver política

Figura 4

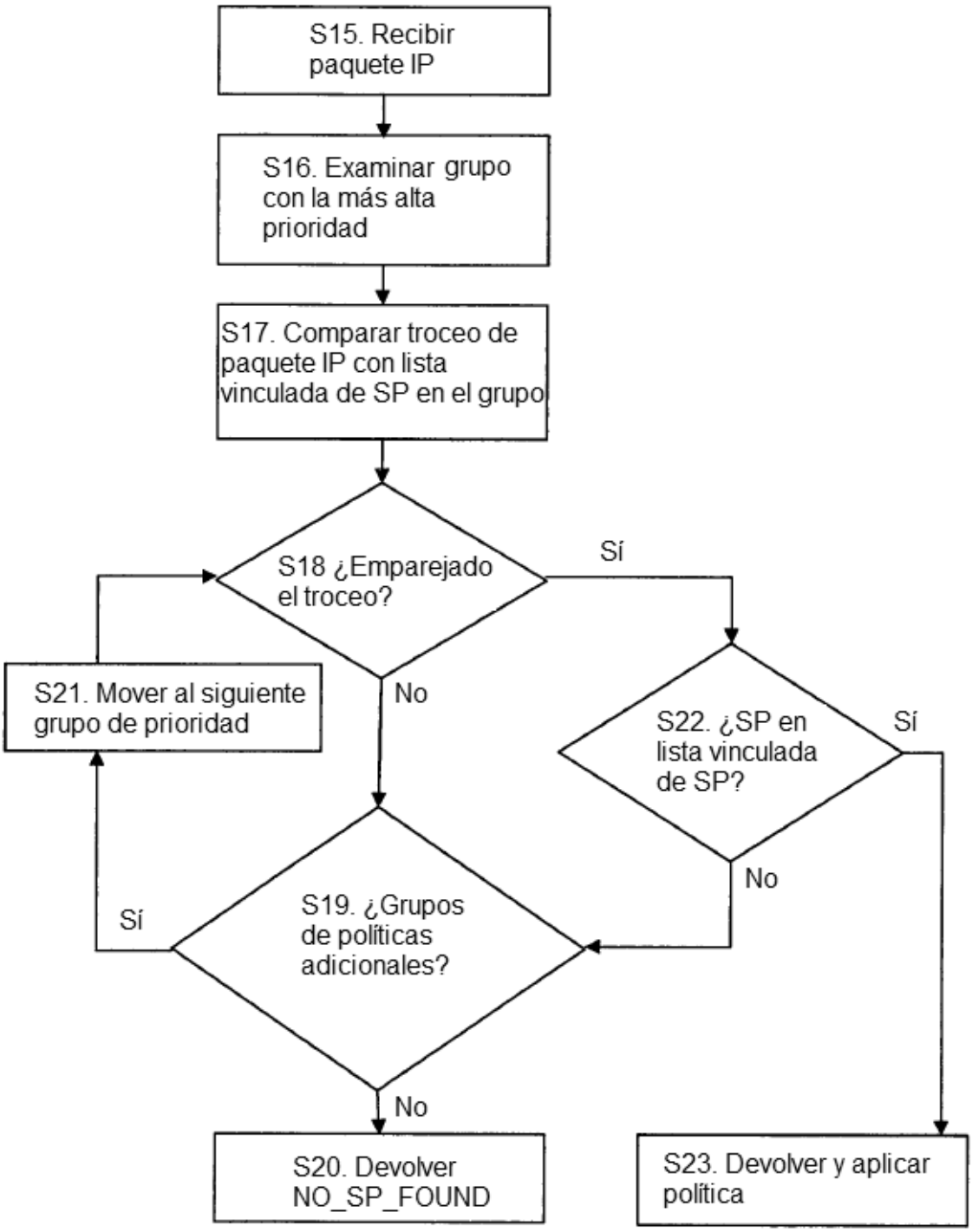
S15. Recibir paquete IP
S16. Examinar grupo con la más alta prioridad
S17. Comparar troceo de paquete IP con lista vinculada de SP en el grupo
S18 ¿Emparejado el troceo?
Sí
No
S21. Mover al siguiente grupo de prioridad
S22. ¿SP en lista vinculada de SP?
Sí
No
S19. ¿Grupos de políticas adicionales?
Sí
No
S20. Devolver NO_SP_FOUND
S23. Devolver y aplicar política

Figura 5

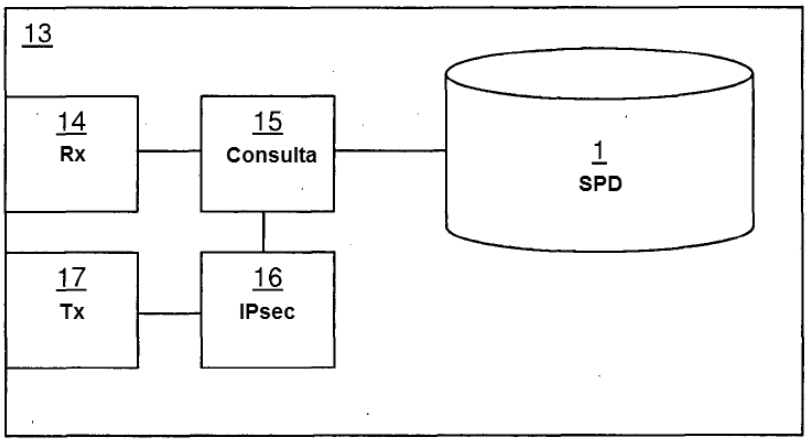

Figura 6

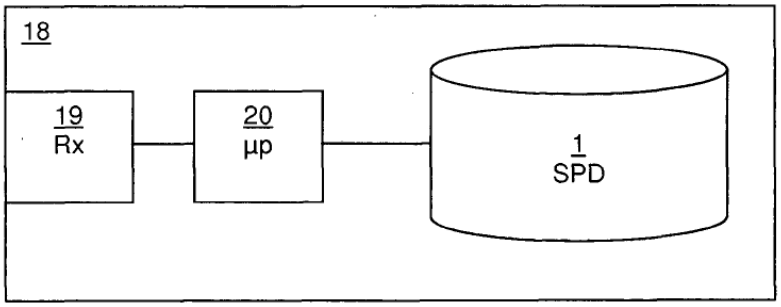

Figura 7