(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 270 307**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **04291418 .4**
(86) Fecha de presentación : **07.06.2004**
(87) Número de publicación de la solicitud: **1605661**
(87) Fecha de publicación de la solicitud: **14.12.2005**

(54) Título: **Método y dispositivo para prevenir ataques a un servidor de llamadas.**

(45) Fecha de publicación de la mención BOPI:
01.04.2007

(45) Fecha de la publicación del folleto de la patente:
01.04.2007

(73) Titular/es: **ALCATEL**
54, rue La Boétie
75008 Paris, FR

(72) Inventor/es: **Oberle, Karsten;**
Tomsu, Marco;
Domschitz, Peter y
Otterbach, Jürgen

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Método y dispositivo para prevenir ataques a un servidor de llamadas.

La presente invención se refiere a un método para prevenir ataques a un servidor de red. El servidor está conectado a una red. Los datos se transmiten entre el servidor de red y la red a través de medios de restricción de acceso al servidor de red. El servidor de red comprende un dispositivo de detección de ataques para detectar e identificar ataques desde la red al servidor de red.

Además, la invención se refiere a un dispositivo de prevención de ataques para prevenir ataques a un servidor de red conectado a una red por medios de restricción de acceso al servidor de red desde la red. El dispositivo de prevención de ataques está adaptado para controlar los medios de restricción de acceso.

El método y el dispositivo de prevención de ataques se pueden utilizar, por ejemplo, para prevenir ataques a un servidor de llamadas en un entorno de servicios basados en llamadas. En ese caso, el servidor de red sería un denominado servidor de llamadas. El entorno de servicios basados en llamadas también se puede denominar entorno de servicios basados en sesiones. Un ejemplo de servicios basados en llamadas es el Protocolo de Voz en Internet (VoIP) o servicios multimedia. Los medios basados en llamadas o basados en sesiones que transmiten datos en la red son iniciados por una llamada.

Un servidor de llamadas está adaptado para controlar el establecimiento, mantenimiento y desmontaje de una conexión de transmisión de datos (es decir, un enlace de comunicaciones o trayecto de medios) que se va a establecer entre al menos un primer agente de usuario y al menos un segundo agente de usuario en la red. Los mensajes de señalización se utilizan para controlar el enlace de comunicaciones. Por supuesto, los entornos de red en los cuales se realiza la presente invención puede comprender más de un servidor de red, todos ellos conectados a la red. Un servidor de llamadas comprende medios para establecer llamadas en la red. Los agentes de usuarios pueden ser teléfonos de IP o cualquier tipo de ordenadores equipados con los equipos (hardware) apropiados de audio y video y de red, así como software de señalización apropiado. Los medios de restricción de acceso se denominan normalmente cortafuegos. Los cortafuegos pueden estar controlados individualmente con el fin de dejar que ciertos mensajes pasen a través de la red al servidor de llamadas, y filtrar, bloquear y/o limitar otros mensajes.

Los protocolos utilizados para señalizar las conexiones de voz sobre de IP (VoIP) son, por ejemplo, el Protocolo de Iniciación de Sesión (SIP), H.323.

Es conocido en el estado de la técnica instalar un dispositivo con reglas de filtrado de paquete estático y limitaciones de ancho de banda (por ejemplo, en una conexión de SIP 5060 por defecto de señalización) entre un servidor de llamadas de SIP (el denominado servidor proxy de SIP) y la red, con el fin de proteger el servidor proxy de SIP de sobrecargas. Sin embargo, un dispositivo de este tipo no puede detectar y eliminar mensajes de SIP maliciosos que ataquen al servidor proxy de SIP.

Además, las tecnologías de puerta de limite dinámico (por ejemplo, el cortafuegos Aravox de la antigua Aravox Technologies Inc., 4201 Lexington Avenue North, Suite 1105, Arden Hills, MN 55126, USA, que recientemente ha sido absorbida por Alcatel) son conocidos en la técnica, que ofrecen cortafuegos de 3 y 4 capas, ajustes basados en flujo y limitación de ancho de banda. Como concepto de cortafuegos dinámico, está controlado por una interfaz de estilo MIDCOM. Las reglas del cortafuegos se compilan y se insertan en los medios de restricción de acceso (lógica de cortafuegos). Normalmente, por el momento solamente se considera el trayecto de medios y no el trayecto de señales.

Para detectar ataques, el mismo servidor de llamadas puede tener la capacidad de clasificar internamente todos los mensajes recibidos y, a continuación, eliminar los mensajes maliciosos después de la inspección directa en la entrada. Aunque esto evita que el servidor de llamadas mantenga demasiados estados de llamadas no completadas en la memoria, no inhibe la situación de sobrecarga en la entrada del servidor de llamadas debido a que los mensajes tienen que alcanzar el servidor de llamadas, en donde cada mensaje se clasifica y se elimina en caso de que sea malicioso. Esto significa que, en la técnica, los mensajes ciertamente tienen que ser procesados pero eventualmente son eliminados, con la confianza de que no produzcan ningún daño al servidor de llamadas.

Puesto que el cortafuegos delante del propio servidor de llamadas no tiene percepción de aplicaciones, en particular no puede diferenciar entre mensajes correctos y ataques, todos los mensajes tienen que alcanzar el servidor de llamadas para la inspección. Esto significa que la relación de mensajes válidos a maliciosos en la entrada del servidor de llamadas no se modifica y la disponibilidad del servidor de llamadas para los llamadores válidos sigue siendo insatisfactoria. De esta manera, las reglas de filtrado de paquetes estáticos y limitaciones de ancho de banda solamente proporcionan una seguridad muy básica al servidor de llamadas, mientras no se comprueba completamente toda la información de aplicaciones (mensajes).

Los métodos conocidos para prevenir ataques en un servidor de llamadas en un entorno de VoIP tienen normalmente un dispositivo de detección de ataques que está asignado, o incluso incorporado, al servidor de llamadas. El dispositivo de detección de ataques comprende algoritmos y reglas para analizar el tráfico recibido por el servidor de llamadas y para detectar ataques potenciales. Por ejemplo, el servidor de llamadas puede observar la frecuencia de llamadas completadas (CCR). Si el CCR está por debajo de un cierto nivel, esto puede ser una señal de un rechazo de

ataque de servicio (DoS) o un ataque distribuido DOS (DDoS) al servidor de llamadas. En ese caso, el agente de usuario atacante envía numerosos mensajes de señal al servidor de llamadas requiriendo el establecimiento de enlaces de comunicación de VoIP a otros agentes de usuarios (por ejemplo, mensajes de "invitación" en SIP). El ataque puede ser dirigido desde un agente de usuario (ataque DoS) o desde numerosos agentes de usuarios distribuidos (ataque DDoS). Otra señal de un ataque al servidor de llamadas es un número exagerado de intentos de llamadas por segundo (CAPS). Por ejemplo, un número exagerado de 10.000 CAPS/segundo, en lugar de un número normal de aproximadamente 100 a 200 CAPS/segundo indica un ataque al servidor de llamadas.

En el estado de la técnica, los medios de restricción de acceso están controlados directamente por el servidor de llamadas. Esto significa que el servidor de llamadas tiene que manejar y procesar cada mensaje que entra, incluso si después o durante la acción del cortafuegos se considera que es un mensaje malicioso y es eliminado consecuentemente. El tratamiento y el manejo de cada mensaje provocan una carga de trabajo excesiva al servidor de llamadas.

Las solicitudes de patente DE 10152010 A1 y US 2003/0145225 A1 describen servidores de red que ejecutan en la práctica la detección de ataques y los mecanismos de protección.

El documento de REYNOLDS B.; GHOSAL D. "Telefonía de IP segura utilizando protección multicapa" PROCEEDINGS OF THE 10TH ANNUAL NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM, SAN DIEGO, CA. USA (Actas del Décimo Simposio Anual de Seguridad de Redes y Sistemas Distribuidos, San Diego, California, USA), 6 - 7 de febrero de 2003, INTERNET SOCIETY, RESTON, VA, USA ISBN: 1-891562-16-9, describe dispositivos sensores para proteger servidores telefónicos de IP y terminales contra los ataques por inundación. Los dispositivos sensores pueden detectar ataques analizando el transporte y el tráfico de capas de aplicación. Cuando se detecta un ataque, los sensores pueden activar medidas de protección dando órdenes al servidor telefónico de IP o al cortafuegos para que bloquee el ataque.

Es un objeto de la presente invención proporcionar un método para prevenir ataques en un servidor de llamadas en un entorno VoIP, asegurando el método, por un lado, un filtrado seguro y fiable de mensajes maliciosos destinados al servidor de llamadas, y reduciendo, por otro lado, la carga en el servidor de llamadas para manejar, procesar y filtrar los mensajes entrantes.

Este objeto se consigue por un método del tipo que se ha mencionado más arriba, que está caracterizado por las siguientes etapas:

- los parámetros característicos de los ataques identificados se incluyen en una lista negra,
- el contenido de la lista negra se transmite a un dispositivo de prevención de ataques para controlar los medios de restricción de acceso,
- el dispositivo de prevención de ataques inspecciona y analiza el tráfico dirigido desde la red al servidor de red y controla los medios de restricción de acceso de acuerdo con el contenido de la lista negra y de acuerdo con los parámetros característicos del tráfico analizado, y
- los medios de restricción de acceso restringen el acceso desde la red al servidor de red de acuerdo con las órdenes de control recibidas desde el dispositivo de prevención de ataques.

De acuerdo con la presente invención, se proporciona un método avanzado por una combinación rápida y de alta respuesta de un dispositivo de detección de ataques con un dispositivo de prevención de ataques que opera con una lista negra especial. El tipo y la realización del dispositivo de detección de ataques no es parte de la presente invención. En una realización posible, el dispositivo de detección de ataques ha de ser fácilmente programable, con el fin de reaccionar rápidamente a tipos y escenarios nuevos de ataque concretos. El dispositivo de detección de ataques puede estar dispuesto por separado del servidor de red. Alternativamente, puede estar incluido parcial o completamente en el servidor de red.

Es necesario derivar información distintiva de los mensajes conspicuos o maliciosos del tráfico, por ejemplo atributos y parámetros característicos de estos mensajes. La información distintiva se introduce en la lista negra y es utilizada por el dispositivo de prevención de ataques para distinguir mensajes maliciosos (que forman parte de un ataque) de los mensajes normales (que forman parte de un procedimiento de señalización o de un flujo de medios).

El dispositivo de prevención de ataques puede funcionar por medio de la inspección de paquetes de datos y de operaciones de adaptación de pautas, con el fin de conseguir el filtrado, bloqueo y/o limitación de los mensajes, cuya información distintiva se corresponda con la información distintiva contenida en la lista negra. Un método de adaptación de pautas, que es posiblemente el más eficiente, puede ser ejecutado fácilmente en la práctica como consultas de tabla de elección arbitraria. Aunque el dispositivo de prevención de ataques puede ejecutar operaciones de inspección y análisis, esto es, puede identificar el contenido de los mensajes inspeccionados, no entiende el contenido de los mensajes ni ejecuta cualquier proceso del contenido. El dispositivo de prevención de ataques puede explorar cualquier tipo de datos en un cierto contenido, con independencia del protocolo de la transmisión de datos y/o de un protocolo de señalización.

El contenido de la lista negra es un resultado importante de la presente invención. La lista negra contiene la información completa requerida por el dispositivo de prevención de ataques para manejar cada mensaje o cada paquete de datos respectivamente direccionados al servidor de red. El contenido de la lista negra es creado por el dispositivo de detección de ataques de acuerdo con ciertos parámetros de definición para definir los mensajes o los paquetes de datos.

El dispositivo de prevención de ataques tiene una inteligencia restringida. Su función se puede comparar al trabajo de un portero, que tiene que controlar el acceso a un área restringida (que corresponde al servidor de red). El portero mira a una persona (que se corresponde con los mensajes) que desea acceder al área restringida, y tiene que decidir, de acuerdo con ciertos algoritmos, reglas o listas, etc. (contenidas en la lista negra) si se permite o no la entrada a la persona. Dependiendo de la decisión del portero, el portero abre la puerta (que se corresponde con los medios de restricción de acceso) y deja pasar a la persona o mantiene la puerta cerrada y rechaza la entrada de la persona. El portero no adquiere conocimiento respecto a la razón por la que la persona quiere entrar en el área restringida o lo que la persona lleva con ella. El portero simplemente comprueba si se cumplen ciertas condiciones obvias (por ejemplo, si la persona lleva un arma, o si la persona lleva una tarjeta de identificación apropiada) y deja que la persona pase o rechaza la entrada de la persona consecuentemente.

El dispositivo de prevención de ataques bloquea o limita el tráfico destinado al servidor de red, sobre la base del contenido de la lista negra. La lista negra, por ejemplo, contiene pautas o atributos que describen tráfico malicioso o conspicuo. En un entorno de protocolo de voz en Internet (VoIP), los atributos o pautas posibles podrían ser, por ejemplo, en SIP: campos “a”, “desde”, campos de “vía”, direcciones de IP, accesos de TCP (Protocolo de Control de Transmisión)/UDP (Protocolo de Datos de Usuario), etc. y combinaciones de los mismos. Las pautas y atributos son creados por el dispositivo de detección de ataques, se introducen en la lista negra y se transfieren al dispositivo de prevención de ataques. Las pautas y atributos pueden introducirse en la lista negra en el dominio del dispositivo de detección de ataques y a continuación pueden ser transmitidos al dispositivo de prevención de ataques en la lista negra. En este caso, la lista negra es creada por el dispositivo de detección de ataques y transmitida en su totalidad al dispositivo de prevención de ataques.

Alternativamente, las pautas y atributos de los mensajes identificados que son conspicuos o maliciosos pueden ser transmitidos al dispositivo de prevención de ataques e introducidos en la lista negra en el dominio del dispositivo de prevención de ataques. Esto tiene la ventaja de que, cada vez que se actualiza la lista negra, solamente tienen que transmitirse al dispositivo de prevención de ataques los cambio de las pautas y atributos y no la lista negra completa.

De acuerdo con una realización preferente de la presente invención, se sugiere que el servidor de red sea un servidor de llamadas que forme parte de un entorno de servicios basados en llamadas. El entorno comprende la red, el servidor de llamadas conectado a la red y al menos un agente de usuario conectado a la red. El servidor de llamadas está adaptado para establecer una conexión de transmisión de datos entre el al menos un agente de usuario y al menos otro agente de usuario por medio de mensajes de señalización. Los mensajes de señalización se transmiten entre el servidor de llamadas y los agentes de usuarios a través de la red o a través de los medios de restricción de acceso. El dispositivo de prevención de ataques inspecciona y analiza los mensajes de señalización del tráfico dirigido desde la red al servidor de llamadas. Preferiblemente, el entorno de servicios basados en llamadas es un entorno de Protocolo de Voz en Internet (VoIP).

Se sugiere que las pautas y/o atributos que definen tráfico conspicuo o malicioso dirigido desde la red al servidor de red se introduzcan en la lista negra como parámetros característicos. Preferiblemente, las pautas y/o atributos que definen el tráfico dirigido al servidor de red se identifican como conspicuos o maliciosos por medio del dispositivo de detección de ataques. Con este propósito, los atributos y características de los mensajes de tráfico conspicuos y maliciosos tienen que ser derivados y definidos antes de que el método de acuerdo con la invención pueda ser ejecutado adecuadamente. Por ejemplo, en SIP, la combinación de atributos depende del escenario y de un conocimiento *a priori* del suministrador de SIP. Por ejemplo, si se inhibe la simulación de direcciones para sus clientes de acceso a la red, un filtrado puede forzar una influencia sobre la relación entre el campo de SIP “desde” y la dirección de fuente de IP, de manera que los ataques de DoS desde su propio dominio puedan ser bloqueados. Si un atacante de DDoS utiliza una pauta específica dentro de cualquier campo de encabezamiento de SIP, o una metainformación específica entre los campos de encabezamiento regulares, puede ser detectada y bloqueada a la velocidad de cable.

De acuerdo con una realización preferida de la presente invención, el contenido de la lista negra es actualizado constante y dinámicamente durante de la operación del servidor de red.

De acuerdo con otra realización preferida de la presente invención, se sugiere que el contenido de la lista negra sea transmitido al dispositivo de prevención de ataques por medio de un trayecto de realimentación. De acuerdo con esta realización, se proporciona un trayecto para la transmisión de datos entre el dispositivo de detección de ataques y el dispositivo de prevención de ataques. Preferiblemente, el trayecto permite transmisión de datos a la velocidad de cable.

De acuerdo con todavía otra realización preferida de la presente invención, los pasos de:

- detectar e identificar ataques desde la red al servidor de red,
- introducir los parámetros característicos de los ataques identificados en la lista negra,
- transmitir el contenido de la lista negra al dispositivo de prevención de ataques,
- analizar el tráfico dirigido desde la red al servidor de red y controlar los medios de restricción de acceso de acuerdo con el contenido de la lista negra y de acuerdo con los parámetros característicos del tráfico analizado, y
- restringir el acceso desde la red al servidor de red de acuerdo con las órdenes de control recibidas desde el dispositivo de prevención de ataque

se ejecutan a la velocidad de cable. El tratamiento a la velocidad de cable también se denomina tratamiento en tiempo real o tratamiento no bloqueante. El tratamiento a velocidad de cable en el dispositivo de detección de ataques y en los medios de prevención de ataques significa que la relación total de tratamiento se debe corresponder, al menos, al ancho de banda máximo deseado para transmitir mensajes en la red al servidor de red en cualquier condición de funcionamiento del entorno de VoIP. Preferiblemente, la velocidad de tratamiento es más alta que el ancho de banda máximo para transmitir mensajes en la red con el fin de asegurar el tratamiento a la velocidad de cable, incluso en el peor de los casos.

Se sugiere que el dispositivo de prevención de ataques efectúe una inspección y análisis del tráfico dirigido desde la red al servidor de red con el fin de determinar si los mensajes dirigidos al servidor de red se corresponden o comprenden pautas y/o atributos contenidos en la lista negra. En particular, el análisis del tráfico comprende comparar los parámetros característicos introducidos en la lista negra y definir el tráfico identificado como conspicuo o malicioso.

Preferiblemente, el dispositivo de prevención de ataques ejecuta un filtrado, bloqueo y/o limitación del tráfico inspeccionado cuyos parámetros característicos se correspondan con los parámetros característicos introducidos en la lista negra y que definen tráfico identificado como conspicuo o malicioso. Para efectuar el filtrado, bloqueo y/o limitación de los mensajes inspeccionados del tráfico, el dispositivo de prevención de ataques envía las señales de control apropiadas a los medios de restricción de acceso. Por supuesto, el dispositivo de prevención de ataques y los medios de restricción de acceso se pueden incorporar en un único dispositivo común, que puede ser denominado cortafuegos habilitado en sesión.

Es particularmente importante prevenir ataques al servidor de red con mensajes de señalización conspicuos o maliciosos. Por lo tanto, se sugiere que el dispositivo de prevención de ataques efectúe una inspección y análisis de los mensajes de señalización de tráfico dirigido desde la red al servidor de red. Preferiblemente, el dispositivo de prevención de ataques ejecuta una inspección y análisis de los mensajes de señalización de acuerdo con la norma de SIP (Protocolo de Iniciación de Sesión). Alternativamente, el dispositivo de prevención de ataques efectúa una inspección y análisis de los mensajes de señalización de acuerdo con la norma H.323.

Además, el objeto que se ha mencionado más arriba se consigue por el dispositivo de prevención de ataques del tipo que se ha mencionado más arriba, que comprende

- medios de entrada para recibir una lista negra que comprende parámetros característicos de los ataques desde la red al servidor de red, siendo detectados e identificados los ataques por un dispositivo de detección de ataques que forma parte del servidor de red,
- medios para ejecutar una inspección y un análisis del tráfico dirigido desde la red al servidor de red, y para determinar parámetros característicos del tráfico,
- medios para crear señales de control para los medios de restricción de acceso de acuerdo con el contenido de la lista negra y de acuerdo con los parámetros característicos del trafico analizado, y
- medios de salida para transmitir las señales de control a los medios de restricción de acceso.

De acuerdo con una realización de la invención, se sugiere que los medios para efectuar una inspección y un análisis del tráfico dirigido desde la red al servidor de red inspeccionen y analicen los mensajes de señalización de tráfico. En particular, se sugiere que el servidor de red sea un servidor de llamadas que forme parte del entorno de servicios basados en llamadas. El entorno comprende la red, el servidor de llamadas conectado a la red y al menos un agente de usuario conectado a la red. El servidor de llamadas está adaptado para establecer una conexión de transmisión de datos entre al menos un agente de usuario y al menos otro agente de usuario por medio de mensajes de señalización. Los mensajes de señalización se transmiten entre el servidor de llamadas y los agentes de usuarios a través de la red y a través de los medios de restricción de acceso. Los medios para efectuar una inspección y un análisis del tráfico inspeccionan y analizan los mensajes de señalización del tráfico dirigidos desde la red al servidor de red.

Preferiblemente, los medios para efectuar una inspección y análisis del tráfico dirigido desde la red al servidor de red inspeccionan y analizan mensajes de señalización de acuerdo con la norma de SIP (Protocolo de Iniciación de Sesión).

De acuerdo con todavía otra realización preferida de la invención, se sugiere que la lista negra contenga pautas y/o atributos que describen tráfico malicioso y/o conspicuo y que los medios para efectuar una inspección y un análisis del trafico dirigido desde la red al servidor de red efectúen una operación de adaptación de pautas y/o atributos con el fin de determinar si el tráfico inspeccionado y analizado comprende un ataque al servidor de red.

Características y ventajas adicionales de la presente invención se explican con mayor detalle más abajo, con referencia a los dibujos que se acompañan. La figura muestra:

la figura 1: una vista general de un entorno de Voz en de IP (VoIP) en el cual se puede ejecutar el método de acuerdo con la presente invención.

A continuación, a título de ejemplo y haciendo referencia a la figura 1, se describirá la presente invención con más detalle en un entorno de Protocolo de Voz sobre Internet (VoIP). En particular, comprende la señalización del Protocolo de Iniciación de Sesión (SIP). Sin embargo, la presente invención no está limitada a la señalización de SIP. Otros protocolos de señalización, por ejemplo el protocolo H.323, también se pueden usar. Además, la invención no está limitada a los entornos de VoIP. Por el contrario, la presente invención se puede utilizar en cualquier tipo de enlace de comunicaciones entre pares que se establezca o que ya haya sido establecido entre el servidor de red y cualquier parte de la red (por ejemplo, otros servidores o agentes de usuarios conectados a la red). Finalmente, la invención no está limitada a inspeccionar y analizar mensajes de señalización, sino que también se puede utilizar para inspeccionar y analizar mensajes de carga de pago (por ejemplo, información de medios).

En la figura 1 se muestra un entorno de VoIP, en el cual se puede ejecutar el método de acuerdo con la presente invención. El entorno de VoIP utiliza mensajes de señalización de SIP. En la figura 1, una red de Protocolo de Internet (IP) se designa con el número de referencia 1. Por supuesto, se puede utilizar también cualquier otro tipo de protocolo de red. Un número de agentes de usuarios UA1, UA2, UA3,... UAn-1, UAn, todos designados con el signo de referencia 2, están conectados a la red de IP 1. Además, un servidor de llamadas 3, es decir, el Servidor de Proxy (representación) de SIP, se conecta a la red de IP 1. Los medios de restricción de acceso 4, es decir, un cortafuegos, se disponen entre el Servidor de Proxy de SIP 3 y la red de IP 1. El cortafuegos 4 impide que ciertos mensajes de SIP alcancen el Servidor de Proxy de SIP 3 fuera de la red de IP 1. Por lo tanto, esa parte de la red de IP 1 dispuesta más allá del cortafuegos 4 puede considerarse como la parte segura o el lado seguro 1' de la red 1. El cortafuegos 4 no efectúa ningún análisis del tráfico dirigido al servidor de llamadas 3. Simplemente es una puerta sin inteligencia propia y controlada por una o más entidades distintas con el fin de abrirla o cerrarla y dejar pasar ciertos datos y rechazar otros datos.

El cortafuegos 4 está controlado por un dispositivo 5 de prevención de ataques, es decir, una puerta de SIP. La puerta de SIP 5 indica al cortafuegos 4 cuando debe abrir para dejar que ciertos mensajes de SIP pasen y cuando debe cerrar para impedir que ciertos mensajes de SIP se introduzcan en el lado seguro 1' de la red 1 y alcancen al Servidor de Proxy de SIP 3. La puerta de SIP 5 tiene una inteligencia restringida que le permite inspeccionar y analizar mensajes entrantes para determinar la presencia de ciertos parámetros característicos de los mensajes. La puerta de SIP 5 no entiende el contenido de los mensajes explorados ni tampoco trata el contenido con una amplitud tal que efectúe ciertas acciones como resultado del contenido. Esto permite a la puerta de SIP 5 trabajar independientemente del protocolo de señalización (por ejemplo, SIP) utilizado en el entorno.

La puerta de SIP 5 recibe una denominada lista negra 6 desde el servidor de Proxy de SIP 3 a través de un trayecto 7 de realimentación. La lista negra 6 comprende información sobre aquellos mensajes de SIP que deben ser bloqueados o al menos restringidos en número. La lista negra de SIP no contiene información individual de cada mensaje de SIP que debe ser bloqueado o restringido. Por el contrario, la lista negra 6 comprende parámetros característicos, por ejemplo ciertas pautas o atributos, que definen el tipo de mensajes de SIP que deben ser bloqueados o restringidos. La puerta de SIP inspecciona y analiza los mensajes de SIP dirigidos al Servidor de Proxy de SIP 3 con el fin de determinar si los mensajes de SIP inspeccionados y analizados comprenden un ataque al Servidor de Proxy de SIP 3, o no. La inspección y el análisis de los mensajes de SIP comprenden la comparación de los parámetros característicos de los mensajes de SIP inspeccionados con parámetros característicos respectivos contenidos en la lista negra 6 y que definen mensajes de SIP conspicuos o maliciosos. En particular, la inspección y análisis de los mensajes de SIP por la puerta de SIP 5 comprende operaciones de adaptación de pautas y/o atributos. El cortafuegos 4 y la puerta de SIP 5 conjuntamente constituyen un denominado cortafuegos habilitado por sesión.

El contenido de la lista negra 6 es creado en un dispositivo 8 de detección de ataques situado en o cerca del servidor de Proxy de SIP 3. Las reglas, pautas y/o atributos que definen mensajes de SIP conspicuos o maliciosos se introducen en la lista negra 6 y a continuación se transmiten a la puerta de SIP 5 por medio del trayecto de realimentación 7. Alternativamente, las reglas, pautas y/o atributos que definen los mensajes de SIP conspicuos o maliciosos se transmiten a la puerta de SIP 5 y allí se introducen en la lista negra 6. El dispositivo 8 de detección de ataques puede efectuar un algoritmo de detección de ataques estático para detectar mensajes de SIP atacantes de una manera conocida en la técnica. Es posible que el dispositivo 8 de detección de ataques efectúe nuevos algoritmos para detectar mensajes

de SIP atacantes tan rápida y fiablemente como sea posible, que no son conocidos en la técnica. Sin embargo, los algoritmos utilizados por el dispositivo 8 de detección de ataques no son el objeto de la presente invención.

Un resultado principal de la presente invención es el hecho que el dispositivo inteligente, esto es, el dispositivo 5 de prevención de ataques, ejecuta la detección real de los mensajes de SIP atacantes y crea las reglas, pautas y/o atributos para definir aquellos mensajes de SIP que constituyen un ataque al Servidor de Proxy de SIP 3. Las reglas, pautas y/o atributos de estos mensajes de SIP se introducen en la lista negra 6. Además, un dispositivo con inteligencia restringida, es decir, el dispositivo de prevención de ataques o la puerta de SIP 5, efectúa el control del cortafuegos 4 dependiendo del contenido de la lista negra 6. Esto tiene la ventaja de que los mensajes de SIP conspicuos o maliciosos son bloqueados o restringidos antes, y no después, de alcanzar el Servidor de SIP 3. Para inspeccionar y analizar los mensajes de SIP entrantes, la puerta de IP 5 solamente mira el contenido de los mensajes SIP, por ejemplo, en la información contenida en el encabezamiento o en la información de carga de pago, pero no tiene que entender el contenido. La puerta de SIP 5 tiene que efectuar simples operaciones de adaptación de pautas y/o atributos. La inteligencia reducida de la puerta de SIP 5 permite una velocidad de tratamiento muy alta de la puerta de SIP 5. Además, la inteligencia reducida de la puerta de SIP 5 hace muy difícil a los atacantes potenciales dirigir realmente un ataque sobre la puerta de SIP 5 para manipular el cortafuegos 4 y abrir el camino para ataques posteriores al Servidor de Proxy de SIP 3.

Para permitir una reacción rápida a un ataque detectado al Servidor de Proxy de SIP 3, preferiblemente los pasos de:

- detectar e identificar ataques desde la red de IP 1 al servidor de Proxy de SIP 3,
- introducir los parámetros característicos que definen los mensajes atacantes en la lista negra 6,
- transmitir el contenido de la lista negra 6 a través del trayecto 7 de realimentación a la puerta de SIP 5,
- explorar, inspeccionar y/o analizar el tráfico dirigido desde la red de IP 1 al Servidor de Proxy de SIP 3 y controlar el cortafuegos 4 de acuerdo con el contenido de la lista negra 6 y de acuerdo con los parámetros característicos del tráfico analizado, y
- restringir el acceso desde la red de IP 1 al Servidor de Proxy de SIP 3 de acuerdo con las órdenes de control recibidas desde la puerta de SIP 5

se efectúan a la velocidad de cable. El contenido de la lista negra 6 es actualizado constante y dinámicamente durante la operación del Servidor de Proxy de SIP 3. Sin embargo, como se ha mencionado más arriba, el contenido de la lista negra 6 se utiliza solamente para controlar el cortafuegos 4. La detección de mensajes maliciosos y sospechosos se efectúa independientemente de la lista negra 6 en el dispositivo 8 de detección de ataques del servidor de Proxy de SIP 3. Por lo tanto, la modificación del contenido de la lista negra 6 modifica el comportamiento del cortafuegos 4, pero no tiene influencia en la detección de mensajes maliciosos y sospechosos.

La idea de la presente invención es emitir el análisis de los paquetes de datos de bajo nivel desde el Servidor de Proxy de SIP 3 a la puerta de SIP 5. Haciéndolo así, los paquetes de datos conspicuos o maliciosos pueden ser detectados y eliminados por el cortafuegos 4 antes de alcanzar el Servidor de Proxy de SIP 3 y consumir recursos allí. Sin embargo, solamente el análisis de bajo nivel es emitido a la puerta de SIP 5 con el fin de asegurar el tratamiento rápido en el cortafuegos 4, 5 habilitado por sesión. Preferiblemente, el cortafuegos 4, 5 habilitado por sesión funciona a la velocidad de cable o en tiempo real.

REIVINDICACIONES

1. Método para prevenir ataques a un servidor (3) de red conectado a una red (1), en el que los datos se transmiten entre la red (1) y el servidor (3) de red a través de medios (4) de restricción de acceso al servidor (3) de red, en el que el servidor (3) de red comprende un dispositivo (8) de detección de ataques para detectar e identificar ataques desde la red (1) al servidor (3) de red, y en el que

- parámetros característicos de los ataques identificados se introducen en una lista negra (6),
- el contenido de la lista negra (6) se transmite a un dispositivo (5) de prevención de ataques para controlar a los medios (4) de restricción de acceso,
- el dispositivo (5) de prevención de ataques inspecciona y analiza el tráfico dirigido desde la red (1) al servidor (3) de red y controla los medios (4) de restricción de acceso de acuerdo con el contenido de la lista negra (6) y de acuerdo con los parámetros característicos del tráfico analizado, y
- los medios (4) de restricción de acceso restringen el acceso desde la red (1) al servidor (3) de red de acuerdo con las órdenes de control recibidas desde el dispositivo (5) de prevención de ataques.

2. Método de acuerdo con la reivindicación 1, que se **caracteriza** porque el servidor (3) de red es un servidor de llamadas que forma parte de un entorno de servicios basados en llamadas, comprendiendo el entorno la red (1), el servidor (3) de llamadas conectado a la red (1) y al menos un agente de usuario (2) conectado a la red (1), estando adaptado el servidor (3) de llamadas para establecer una conexión de transmisión de datos entre el al menos un agente (2) y al menos un otro agente de usuario (2) por medio de mensajes de señalización, en el que los mensajes de señalización se transmiten entre el servidor (3) de llamadas y los agentes de usuarios (2) a través de la red (1) y a través de los medios (4) de restricción de acceso, y en el que el dispositivo (5) de prevención de ataques inspecciona y analiza los mensajes de señalización del tráfico dirigido desde la red (1) al servidor (3) de llamadas.

3. Método de acuerdo con la reivindicación 2, que se **caracteriza** porque el método se utiliza para prevenir ataques a un servidor (3) de llamadas en un entorno de Protocolo de Voz en Internet (VoIP).

4. Método de acuerdo con cualquiera de las reivindicaciones precedentes,

que se **caracteriza** porque pautas y/o atributos que definen el tráfico conspicuo o malicioso dirigido desde la red (1) al servidor (3) de red se introducen en la lista negra (6) como parámetros característicos.

5. Método de acuerdo con cualquiera de las reivindicaciones precedentes,

que se **caracteriza** porque el contenido de la lista negra (6) se actualiza constante y dinámicamente durante la operación del servidor (3) de red.

6. Método de acuerdo con cualquiera de las reivindicaciones precedentes,

que se **caracteriza** porque los ataques son identificados y los parámetros característicos son introducidos en la lista negra (6) por el dispositivo (8) de detección de ataques.

7. Método de acuerdo con cualquiera de las reivindicaciones precedentes,

que se **caracteriza** porque el contenido de la lista negra (6) se transmite al dispositivo (5) de prevención de ataques por medio de un trayecto (7) de realimentación.

8. Método de acuerdo con cualquiera de las reivindicaciones precedentes,

que se **caracteriza** por los pasos de

- detectar e identificar ataques desde la red (1) al servidor (3) de red,
- introducir los parámetros característicos de los ataques identificados en la lista negra (6),
- transmitir el contenido de la lista negra (6) al dispositivo (5) de prevención de ataques,
- analizar el tráfico dirigido desde la red (1) al servidor (3) de red y controlar los medios (4) de restricción de acceso de acuerdo con el contenido de la lista negra (6) y de acuerdo con los parámetros característicos del tráfico analizado, y
- restringir el acceso desde la red (1) al servidor (3) de red de acuerdo con las órdenes de control recibidas desde el dispositivo (5) de prevención de ataques, se efectúan a la velocidad de cable.

9. Método de acuerdo con cualquiera de las reivindicaciones precedentes, que se **caracteriza** porque el análisis del tráfico dirigido desde la red (1) al servidor (3) de red comprende comparar los parámetros característicos del tráfico inspeccionado con los parámetros característicos introducidos en la lista negra (6) y definir el tráfico identificado como conspicuo o malicioso.

10. Método de acuerdo con la reivindicación 9, que se **caracteriza** porque el dispositivo (5) de prevención de ataques efectúa un filtrado, bloqueo y/o limitación del tráfico inspeccionado cuyos parámetros característicos se correspondan con los parámetros característicos introducidos en la lista negra (6), y define el tráfico identificado como conspicuo o malicioso.

11. Método de acuerdo con una de las reivindicaciones 2 a 10,

que se **caracteriza** porque el dispositivo (5) de prevención de ataques ejecuta una inspección y un análisis de los mensajes de señalización de acuerdo con una norma de SIP (Protocolo de Iniciación de Sesión).

12. Método de acuerdo con una de las reivindicaciones 2 a 10,

que se **caracteriza** porque el dispositivo (5) de prevención de ataques efectúa una inspección y un análisis de los mensajes de señalización de acuerdo con una norma H.323.

13. Dispositivo (5) de prevención de ataques para prevenir ataques a un servidor (3) de red conectado a una red (1) a través de medios (4) de restricción de acceso al servidor (3) de red desde la red (1), en el que el dispositivo (5) de prevención de ataques está adaptado para controlar los medios (4) de restricción de acceso, en el que el dispositivo (5) de prevención de ataques comprende

- medios para efectuar una inspección y un análisis del tráfico dirigido desde la red (1) al servidor (3) de red y para determinar parámetros característicos del tráfico,

- medios de salida para transmitir señales de control a los medios (4) de restricción de acceso,

que se **caracteriza** porque el dispositivo (5) de prevención de ataques comprende

- medios de entrada para recibir una lista negra (6) que comprende parámetros característicos de ataques de la red (1) sobre el servidor (3) de red, siendo detectados e identificados los ataques por el dispositivo (8) de detección de ataques que forma parte del servidor (3) de red,

- medios para crear las señales de control para los medios (4) de restricción de acceso de acuerdo con el contenido de la lista negra (6) y de acuerdo con los parámetros característicos del tráfico analizado.

14. Dispositivo (5) de prevención de ataques de acuerdo con la reivindicación 13,

que se **caracteriza** porque el servidor (3) de red es un servidor de llamadas que forma parte de un entorno de servicios basados en llamadas, comprendiendo el entorno la red (1), el servidor (3) de llamadas conectado a la red (1) y al menos un agente de usuario (2) conectado a la red (1), estando adaptado el servidor (3) de llamadas para establecer una conexión de transmisión de datos entre el al menos un agente de usuario (2) y al menos un otro agente de usuario (2) por medio de mensajes de señalización, en el que los mensajes de señalización se transmiten entre los agentes de usuarios (2) y el servidor (3) de llamadas en la red (1) y a través de los medios (4) de restricción de acceso, y en el que los medios para efectuar una inspección y un análisis del tráfico inspeccionan y analizan los mensajes de señalización del tráfico dirigido desde la red (1) al servidor (3) de llamadas.

15. Dispositivo (5) de prevención de ataques de acuerdo con la reivindicación 14, que se **caracteriza** porque los medios para efectuar una inspección y un análisis del trafico dirigido desde la red (1) al servidor (3) de llamadas inspeccionan y analizan mensajes de señalización de acuerdo con una norma de SIP (Protocolo de Iniciación de Sesión).

16. Dispositivo (5) de prevención de ataques de acuerdo con una de las reivindicaciones 13 a 15, que se **caracteriza** porque la lista negra (6) contiene pautas y/o atributos que describen tráfico malicioso y/o conspicuo y porque los medios para efectuar una inspección y un análisis del tráfico dirigido desde la red (1) al servidor (3) de red efectúan una operación de adaptación de pautas y/o atributos con el fin de determinar si el tráfico inspeccionado y analizado comprende un ataque al servidor (3) de red.

Fig. 1