(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 609 861**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/26 (2006.01)
H04L 12/859 (2013.01)
G06F 21/55 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.08.2012 PCT/CN2012/080571**

(87) Fecha y número de publicación internacional: **04.07.2013 WO13097476**

(96) Fecha de presentación y número de la solicitud europea: **24.08.2012 E 12862305 (5)**

(97) Fecha y número de publicación de la concesión europea: **12.10.2016 EP 2760162**

(54) Título: **Método y dispositivo para configurar y optimizar una regla de detección**

(30) Prioridad:

31.12.2011 CN 201110459531

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.04.2017

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian Longgang District, Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

JIANG, WU y
WANG, TAO

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y dispositivo para configurar y optimizar una regla de detección.

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo de la configuración de reglas de detección y en particular, a un método y un dispositivo para optimizar y configurar una regla de detección.

ANTECEDENTES DE LA INVENCIÓN

Con la amplia aplicación de ordenadores y la dispersión creciente de redes, las amenazas desde el interior y el exterior de las redes son cada vez mayores. Con el fin de proteger la seguridad de un sistema, necesita realizarse una detección de amenazas en una red. La detección de contenidos de protocolos es una clase de detección de amenazas.

Tomando a modo de ejemplo un dispositivo del Sistema de Prevención de Intrusión (IPS), la detección del contenido de protocolo existente se realiza principalmente utilizando un método de coincidencia de modos, es decir, la correspondencia de diferentes protocolos, siendo configuradas diferentes reglas de detección. Una función de personalizar una regla se proporciona en un dispositivo IPS, y se realiza una detección añadiendo, habilitando o cerrando algunas reglas de detección por un usuario por sí mismo. Sin embargo, existen miles de tipos de protocolos existentes, y existen decenas de miles de categorías de protocolos específicas de los tipos de protocolo. Se exige una amplia experiencia para configurar, con exactitud, una regla de detección y necesita dedicar mucho tiempo a tal respecto. Actualmente, la mayor parte de los usuarios realiza una detección en una manera de habilitación directa de todas las reglas de detección de protocolos. En la detección de amenaza de IPS, la mayor parte funcional de la detección de amenazas de IPS se consume en una parte de detección de contenidos de protocolos; por lo tanto, en una manera existente de habilitación directa de todas las reglas de detección de protocolos, se detecta también una amenaza de protocolo que no ocurre en una red, dando lugar a un consumo de numerosos recursos innecesario por IPS y disminuyendo la eficiencia y el rendimiento de la detección de IPS.

El documento US 2008/005795 A1 da a conocer un método y un sistema para optimizar un primer conjunto de reglas ejecutadas por un *firewall (cortafuegos)* sobre el tráfico de red. Las características del tráfico de red se examinan y dichas características se utilizan para generar un segundo conjunto de reglas. El primer conjunto de reglas puede tener un orden distinto que el segundo conjunto de reglas. El optimizador basado en las reglas está constituido por dos componentes – el Creador de Conjuntos Disjuntos (DSC) y el Fusionador de Conjuntos Disjuntos (DSM). El DSC detecta y elimina las dependencias del conjunto de reglas actual y luego, crea una nuevas definiciones de reglas (esto es, nuevas reglas) con el fin de hacer disyunto el conjunto de reglas completo. El DSM fusiona las reglas del conjunto disyunto obtenido por el DSC. El proceso de fusión selecciona una regla y la clasifica para la fusión de la regla con otras reglas. La fusión tiene lugar entre reglas con el mismo campo de acción, para preservar la integridad semántica. La fusión entre dos reglas, con respecto a un campo diferente específico, tiene lugar cuando los otros valores del campo correspondiente son los mismos para el espacio de campos.

El documento US 2009/271857 A1 da a conocer un método y aparato que permite una clasificación aproximada de los paquetes utilizando el método de clasificación de paquetes exacto y un método de clasificación de paquetes inexacto. El gestor de reglas transforma un conjunto de reglas especificado en un nuevo conjunto de reglas que es equivalente desde el punto de vista semántico. Para establecer un conjunto de reglas eficiente, el gestor de reglas muestrea continuamente el tráfico entrante y calcula las estadísticas específicas de este tráfico de muestra para conocer sus características actuales. El gestor de reglas calcula todos los flujos muestreados distintos y sus frecuencias. Sobre la base de esta información muestreada, el gestor de reglas crea y mantiene un pequeño conjunto de nuevas reglas que cubren todos los paquetes muestreados.

El documento US 7966659 B1 da a conocer técnicas para el análisis a nivel del sistema del tráfico de protocolo industrial para determinar una localización óptima de un dispositivo de seguridad y/o para crear, de forma dinámica y automática, reglas para dispositivos de seguridad. El sistema incluye un módulo colector que recoge información del tráfico desde al menos una fuente distribuida durante un modo de aprendizaje. El sistema incluye también un módulo creador de reglas que puede analizar la información de tráfico recogida en un contexto del sistema. Una regla de seguridad puede crearse utilizando el contexto del sistema y la regla de seguridad puede aplicarse automáticamente a un dispositivo de seguridad.

SUMARIO DE LA INVENCIÓN

La presente invención da a conocer un método y un dispositivo para optimizar y configurar una regla de detección, con el fin de identificar, mediante el conocimiento del tráfico en una red activa, una información relacionada con el protocolo utilizada en la red activa, y para generar un conjunto de reglas compacto en función de la información relacionada con el protocolo, con lo que se habilita la realización de la detección del protocolo posterior solamente para una amenaza sobre el protocolo que pueda tener lugar en la red activa; por lo tanto, se reduce el contenido que

necesita detectarse posteriormente, se mejora la eficiencia de la detección y se evita, al mismo tiempo, un consumo de rendimiento innecesario.

La presente invención da a conocer un método para optimizar y configurar una regla de detección, que incluye:

recibir un tráfico de red;

extraer un paquete desde el tráfico de red, e identificar, en función de una característica del paquete, información relacionada con el protocolo utilizada en la red, incluyendo la información relacionada con el protocolo un elemento de una combinación de varios elementos de información siguiente: un nombre de protocolo, un nombre de protocolo de aplicación, un número de puerto, un nombre de software de servidor y una versión de software de servidor;

salvaguardar la información relacionada con el protocolo y la correspondencia entre elementos de información en la información relacionada con el protocolo hacia una primera tabla de asociación de aprendizaje;

obtener una regla de vulnerabilidad, que se establece en correspondencia con la información relacionada con el protocolo en una base de reglas de vulnerabilidad, en conformidad con la información relacionada con el protocolo identificada; y

integrar la regla de vulnerabilidad obtenida para generar un primer conjunto de reglas compacto cuando se identifican múltiples conjuntos de información de protocolo, en donde el primer conjunto de reglas compacto consiste en una regla de vulnerabilidad que se establece en correspondencia con la información relacionada con el protocolo identificada en la base de reglas de vulnerabilidad;

antes de extraer un paquete desde el tráfico de red, el método comprende, además:

establecer un margen de aprendizaje, en donde el margen de aprendizaje comprende un segmento de red o una dirección IP que se determina por anticipado; y

en consecuencia, la extracción de un paquete desde el tráfico de red, comprende:

extraer, desde el tráfico de red, un paquete con una dirección transportada dentro del margen de aprendizaje.

De modo opcional, el método incluye, además:

realizar una detección de amenaza sobre el protocolo en función del primer conjunto.

De modo opcional, el método incluye, además:

enviar el primer conjunto y la primera tabla de asociación de aprendizaje a un usuario; y

proporcionar, por el usuario, el primer conjunto a un dispositivo cuando se confirma el primer conjunto de reglas compacto.

De modo opcional, el método comprende, además:

salvaguardar la información relacionada con el protocolo cambiada hacia una segunda tabla de asociación de aprendizaje cuando el usuario cambia la información relacionada con el protocolo en la primera tabla de asociación de aprendizaje; y

seleccionar una regla de vulnerabilidad desde la base de reglas de vulnerabilidad en función con la segunda tabla de asociación de aprendizaje, con el fin de generar un segundo conjunto de reglas compacto.

La presente invención da a conocer un método para optimizar y configurar una regla de detección, que incluye:

recibir un tráfico de red;

extraer un paquete desde el tráfico de red, e identificar, en función de una característica del paquete, información relacionada con el protocolo utilizada en la red, incluyendo la información relacionada con el protocolo un elemento o una combinación de varios elementos de la información siguiente: un nombre de protocolo, un nombre de protocolo de aplicación, un número de puerto, un nombre de software de servidor y una versión de software de servidor;

salvaguardar la información relacionada con el protocolo y la correspondencia entre los elementos de información en la información relacionada con el protocolo hacia una primera tabla de asociación de aprendizaje;

obtener una regla de vulnerabilidad, que se establece en correspondencia con la información relacionada con el

protocolo en una base de reglas de vulnerabilidad, en función con la información relacionada con el protocolo identificada; y

integrar la regla de vulnerabilidad obtenida para generar un primer conjunto de reglas compacto cuando se identifican múltiples conjuntos de información de protocolo, en donde el primer conjunto consiste en una regla de vulnerabilidad que se establece en correspondencia con la información relacionada con el protocolo identificada en la base de reglas de vulnerabilidad;

antes de extraer un paquete desde el tráfico de red, el método comprende, además:

establecer un margen de valores de tráfico válidos, en donde el margen de valores válidos es un porcentaje del tráfico de tipo preestablecido en el tráfico total; y

en consecuencia, la extracción del paquete desde el tráfico de red, comprende:

extraer un paquete en el tráfico de al menos un protocolo de aplicación desde el tráfico de red, en donde un porcentaje del tráfico de cada protocolo de aplicación en el al menos un protocolo de aplicación en el tráfico de red está dentro del margen de valores válidos.

La presente invención da a conocer, además, un dispositivo para optimizar y configurar una regla de detección, que incluye:

una unidad de recepción de tráfico, configurada para recibir un tráfico de red;

una unidad de extracción, configurada para extraer un paquete desde el tráfico de red;

una unidad de identificación de información, configurada para identificar, en función de una característica del paquete, información relacionada con el protocolo utilizada en la red, incluyendo la información relacionada con el protocolo un elemento o una combinación de varios elementos de la información siguiente: un nombre de protocolo, un nombre de protocolo de aplicación, un número de puerto, un nombre de software de servidor y una versión de software de servidor;

una primera unidad de salvaguarda, configurada para salvaguardar la información relacionada con el protocolo y la correspondencia entre los elementos de la información en la información relacionada con el protocolo hacia una primera tabla de asociación de aprendizaje; y

una primera unidad del conjunto de reglas compacto, configurada para obtener una regla de vulnerabilidad, que se establece en correspondencia con la información relacionada con el protocolo en una base de reglas de vulnerabilidad, en función de la información relacionada con el protocolo identificada; e integrar la regla obtenida para generar un primer conjunto cuando se identifican múltiples conjuntos de información de protocolo, en donde el primer conjunto de reglas compacto consiste en una regla de vulnerabilidad que se establece en correspondencia con la información relacionada con el protocolo identificada en la base de reglas de vulnerabilidad.

De modo opcional, el dispositivo incluye, además:

una unidad de detección, configurada para realizar una detección de amenaza de protocolo en conformidad con el primer conjunto de reglas compacto.

De modo opcional, el dispositivo incluye, además:

una unidad de envío, configurada para enviar el primer conjunto de reglas compacto y la primera tabla de asociación de aprendizaje a un usuario; y

una unidad de recepción, configurada para: cuando el usuario confirma el primer conjunto de reglas compacto, recibir el primer conjunto de reglas compacto proporcionado por el usuario.

De modo opcional, el dispositivo incluye, además:

una segunda unidad de salvaguarda, configurada para salvaguardar la información relacionada con el protocolo cambiada hacia una segunda tabla de asociación de aprendizaje cuando el usuario cambia la información relacionada con el protocolo en la primera tabla de asociación de aprendizaje, en donde

la unidad del conjunto de reglas compacto está configurado, además, para seleccionar una regla de vulnerabilidad desde la base de reglas de vulnerabilidad en función de la segunda tabla de asociación de aprendizaje, con el fin de generar un segundo conjunto de reglas compacto, y para generar un segundo conjunto de reglas compacto.

La presente invención da a conocer, además, un dispositivo para optimizar y configurar una regla de detección, que incluye:

una unidad de recepción del tráfico, configurada para recibir un tráfico de red;

una unidad de extracción, configurada para extraer un paquete desde el tráfico de red;

una unidad de identificación de información, configurada para identificar, en función de una característica del paquete, información relacionada con el protocolo utilizada en la red, incluyendo la información relacionada con el protocolo un elemento o una combinación de varios elementos de la información siguiente: un nombre de protocolo, un nombre de protocolo de aplicación, un número de puerto, un nombre de software de servidor y una versión de software de servidor;

una primera unidad de salvaguarda, configurada para salvaguardar la información relacionada con el protocolo y la correspondencia entre los elementos de información en la información relacionada con el protocolo hacia una primera tabla de asociación de aprendizaje; y

una primera unidad del conjunto de reglas compacto, configurada para obtener una regla de vulnerabilidad, que se establece en correspondencia con la información relacionada con el protocolo en una base de reglas de vulnerabilidad, en función de la información relacionada con el protocolo identificada, y para integrar la regla obtenida para generar un primer conjunto de reglas compacto cuando se identifican múltiples conjuntos de información de protocolos, en donde el primer conjunto de reglas compacto consiste en una regla de vulnerabilidad que se establece en correspondencia con la información relacionada con el protocolo identificada en la base de reglas de vulnerabilidad;

una primera unidad de establecimiento, configurada para establecer un margen de aprendizaje, en donde el margen de aprendizaje comprende un segmento de red o una dirección IP que se determina por anticipado;

en donde

la unidad de extracción está configurada, además, para extraer, desde el tráfico de red, un paquete con una dirección incluida dentro del margen de aprendizaje.

En comparación con la técnica anterior, la presente invención tiene las ventajas siguientes:

En conformidad con el método dado a conocer en la presente invención, el tráfico en una red activa se conoce e identifica para obtener información del protocolo que se utiliza en la red activa y se clasifica una regla de detección a partir de una base de reglas de vulnerabilidad en función de la información de protocolo, con el fin de generar un conjunto de reglas compacto correspondiente a un protocolo utilizado en la red activa. Solamente el protocolo utilizado en la red activa necesita detectarse cuando se realiza una detección utilizando el conjunto de reglas compacto. Por lo tanto, se resuelve un problema de que todos los protocolos necesitan detectarse durante la detección porque un usuario selecciona todas las reglas de detección en la técnica anterior, lo que mejora la eficiencia de detección y al mismo tiempo, evita un consumo innecesario de rendimiento.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para describir las soluciones técnicas en las formas de realización de la presente invención o en la técnica anterior, con mayor claridad, a continuación se introducen, de forma concisa, los dibujos adjuntos requeridos para describir las formas de realización. Evidentemente, los dibujos adjuntos en la descripción siguiente ilustran solamente algunas formas de realización de la presente invención y un experto en esta técnica puede deducir otros dibujos a partir de esos dibujos adjuntos sin necesidad de esfuerzos creativos.

La Figura 1 es un diagrama de flujo de la forma de realización 1 de un método en conformidad con la presente invención;

La Figura 2 es un diagrama esquemático de una primera tabla de asociación de aprendizaje antes del aprendizaje del tráfico en conformidad con una forma de realización de la presente invención;

La Figura 3 es un diagrama esquemático de una primera tabla de asociación de aprendizaje después del aprendizaje del tráfico en conformidad con una forma de realización de la presente invención; y

La Figura 4 es un diagrama estructural de un dispositivo en conformidad con la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN

A continuación se describe, de forma clara y completa, las soluciones técnicas en las formas de realización de la

presente invención haciendo referencia a los dibujos adjuntos en las formas de realización de la presente invención. Evidentemente, las formas de realización descritas son simplemente una parte y no la totalidad de las formas de realización de la presente invención. Todas las demás formas de realización obtenidas por un experto en esta técnica sobre la base de las formas de realización de la presente invención deberán caer dentro del alcance de protección de la presente invención.

Haciendo referencia a la Figura 1, la forma de realización 1 de la presente invención da a conocer un método para optimizar y configurar una regla de detección, en donde el método incluye:

S11: Recibir tráfico de red.

Tomando a modo de ejemplo un dispositivo IPS, se utiliza una manera de coincidencia de modos para la detección de protocolo del dispositivo IPS. Es decir, para diferentes protocolos, existen diferentes reglas de detección. Es conocido que existen diferentes vulnerabilidades en diferentes protocolos y una amenaza de un protocolo procede un ataque a estas vulnerabilidades. Por lo tanto, cuando se detecta un protocolo, solamente se refiere a su correspondiente. Es decir, para diferentes protocolos, existen diferentes reglas de detección. Es conocido que existen diferentes vulnerabilidades en diferentes protocolos y una amenaza de protocolo procede de un ataque a estas vulnerabilidades. Por lo tanto, cuando se detecta un protocolo, solamente necesita hacerse coincidir una regla de detección de vulnerabilidad correspondiente. Por lo tanto, con el fin de una coincidencia correcta de una regla de detección de vulnerabilidad, necesita conocerse primero un tipo de protocolo utilizado en un red activa.

Más concretamente, el tráfico en una red real puede conocerse en una etapa anterior cuando el dispositivo IPS accede a la red.

S12: Extraer un paquete desde el tráfico de red, e identificar, en función de una característica del paquete, información relacionada con el protocolo utiliza en la red.

La información relacionada con el protocolo incluye concretamente un elemento o una combinación de varios elementos de información tales como un nombre de protocolo, un nombre de protocolo de aplicación, es decir, un tipo de aplicación, un número de puerto, un nombre de software de servidor y una versión de software de servidor.

Con el fin de realizar una transferencia correcta de un paquete, la información relacionada con el protocolo mediante el que se transfiere el paquete se establecerá en el propio paquete. Por lo tanto, un paquete puede extraerse desde el tráfico obtenido en proceso de aprendizaje y se realiza una identificación de característica sobre el paquete para obtener la información relacionada con el protocolo. Más concretamente, un nombre de protocolo y un tipo de aplicación pueden identificarse en función de una característica del paquete. Un análisis a fondo se realiza, además, sobre el tipo de aplicación para obtener información de un número de puerto, un nombre de software de servidor y una versión del software de servidor. La información del protocolo está relacionada con la información de memorización de una base de reglas de vulnerabilidad que se menciona a continuación. Su relación específica se describe en un contexto posterior.

S13: Salvaguardar la información relacionada con el protocolo y la correspondencia entre la información relacionada con el protocolo hacia una primera tabla de asociación de aprendizaje.

La información correspondiente a un mismo elemento de tráfico está memorizada, de forma asociativa, cuando se memoriza la información obtenida. A modo de ejemplo, un elemento del tráfico se identifica y se obtiene que un protocolo del elemento de tráfico es TCP, un protocolo de aplicación del elemento de tráfico es HTTP, un puerto del elemento de tráfico es 80, un nombre de software del servidor del elemento de tráfico es Apache HTTPD y una versión de software de servidor es 2.2.3. Por lo tanto, no solamente necesita memorizarse la información anterior en la primera tabla de asociación de aprendizaje, sino también necesita memorizarse la correspondencia entre la información anterior.

En general, un usuario transmite datos solamente un determinado alcance de red. Por lo tanto, no se utiliza un protocolo más allá del alcance de la red, y un tipo de protocolo utilizado más allá del alcance de la red no necesita detectarse. Por lo tanto, en la forma de realización 2 de la presente invención, un margen de aprendizaje puede establecerse previamente para conocer el tráfico especificado. En este caso, solamente un paquete de tráfico en el margen de aprendizaje necesita extraerse para su identificación y a continuación, la información relacionada con el protocolo obtenido se memoriza en la primera tabla de asociación de aprendizaje. Más concretamente, un segmento de red o una dirección IP que ha de aprenderse puede establecerse a este respecto. Durante una puesta en práctica fichero, una manera de establecer múltiples opciones para el usuario para seleccionar puede utilizarse y también puede emplearse una manera de entrada por el propio usuario. Cuando el usuario no selecciona una opción o no realiza una entrada, el tráfico en la red completa puede establecerse para aprendizaje.

S14: Hacer coincidir un elemento de regla correspondiente desde una base de reglas de vulnerabilidad en función de la información relacionada con el protocolo con el fin de generar un primer conjunto de reglas compacto.

La base de reglas de vulnerabilidad es una herramienta de evaluación de la seguridad del sistema y memoriza una regla de vulnerabilidad correspondiente a cada protocolo. A modo de ejemplo, una base de reglas de vulnerabilidad memoriza lo siguiente:

[Servicio de correo] SendMail 7.0: 300 reglas de vulnerabilidad;

[Servicio de correo] SendMail 8.0: 200 reglas de vulnerabilidad;

[Servicio de correo] Exchange Server 2007: 500 reglas de vulnerabilidad;

[Servicio de correo] Exchange Server 2010: 300 reglas de vulnerabilidad;

[Servicio FTP] ProFTP 1.2.0: 1000 reglas de vulnerabilidad; y

[Servicio FTP] ProFTP 1.3.0: 500 reglas de vulnerabilidad.

Puede deducirse de la descripción anterior, que la base de reglas de vulnerabilidad, una regla de vulnerabilidad, es decir, una regla de detección, se establece en correspondencia con la información de protocolo tal como un protocolo de aplicación, un nombre de software de servidor de aplicación y una versión de software de servidor de aplicación. Por lo tanto, una regla de vulnerabilidad correspondiente puede obtenerse en conformidad con la información de protocolo identificada. A modo de ejemplo, la información de protocolo identificada es que el protocolo de aplicación es FTP, el nombre de software del servidor de aplicación es ProFTP y la versión es 1.2.0, de modo que existen 1000 reglas de detección correspondientes.

Cuando se identifican múltiples conjuntos de información de protocolo, se obtienen reglas de detección correspondientes a partir de la base de reglas de vulnerabilidad para integración, con el fin de formar el primer conjunto de reglas compacto.

En algunas situaciones operativas, el usuario solamente tiene previsto proteger y detectar el tráfico en un determinado margen de valores, a modo de ejemplo, tráfico grande, sin cuidarse de otro tráfico. Por lo tanto, en la forma de realización 3 de la presente invención el método incluye, además:

establecer un margen de valores de tráfico válidos. A modo de ejemplo, el margen se establece a 5 % - 80 %. A veces, cuando el tráfico que el usuario tiene previsto proteger está en varios márgenes discontinuos, se pueden establecer múltiples márgenes, a modo de ejemplo, 5 % - 30 % y 45 % - 90 %.

En una aplicación específica, el usuario no cuida del pequeño tráfico. Por lo tanto, un margen de detección puede establecerse en una manera de establecimiento de un umbral. A modo de ejemplo, se establece un 5 %, de modo que el tráfico inferior al 5 % es un margen del que el usuario no tiene que cuidarse y no se espera protección alguna. Por lo tanto, el usuario puede solamente extraer un paquete del tráfico dentro del margen de valores de tráfico válidos a partir del tráfico de red y realizar la identificación para obtener la información de protocolo correspondiente y luego, salvaguardar la información del protocolo.

En la presente invención, a veces, la identificación del tráfico se realiza antes de recoger datos estadísticos sobre un valor de tráfico, es decir, la información de protocolo correspondiente se obtiene identificando la característica del paquete antes de que pueda conocerse una magnitud del tráfico. En este caso, toda la información de protocolo correspondiente identificada necesita memorizarse primero en la primera tabla de asociación de aprendizaje, y la magnitud del tráfico, sobre el que se recogen estadísticas posteriormente, es también objeto de la memorización diente en la primera tabla de asociación de aprendizaje.

A continuación, el tráfico con una magnitud más allá del margen de valores válidos establecido y la información del protocolo correspondiente al tráfico más allá del margen de valores válidos establecido se suprimen de la primera tabla de asociación de aprendizaje en función con el margen de valores del tráfico válidos establecido, con el fin de generar una nueva tabla de asociación de aprendizaje. Además, un elemento de regla se clasifica desde la base de reglas de vulnerabilidad en conformidad la nueva tabla de asociación de aprendizaje, con el fin de generar un conjunto de reglas compacto.

El objetivo esencial de la forma de realización 2 y de la forma de realización 3 de la presente invención es establecer un margen de direcciones de red y un margen de magnitud para el tráfico. Dos maneras de establecimiento pueden realizarse respectivamente y pueden efectuarse también al mismo tiempo.

El conjunto de reglas compacto generado puede aplicarse directamente a un dispositivo. El usuario puede ver un registro de optimización y configuración específicas por intermedio de la información de registro. Con el fin de garantizar la exactitud, en la forma de realización 4 de la presente invención, el conjunto de reglas compacto puede enviarse primero al usuario y confirmarse finalmente por el usuario. Un proceso específico se describe como sigue:

El primer conjunto de reglas compacto y la primera tabla de asociación de aprendizaje se envían al usuario.

Más concretamente, el usuario puede conocer, observando la información en la primera tabla de asociación de aprendizaje, si un resultado del aprendizaje del dispositivo es compatible con un entorno de red real. Con el fin de obtener un resultado más exacto, la información del valor de tráfico obtenida puede memorizarse en la primera tabla de asociación de aprendizaje al mismo tiempo en una etapa de aprendizaje del dispositivo.

Conviene señalar que, en una situación en la que el margen de aprendizaje y el margen de valores de tráfico válidos se establecen, el usuario solamente comprueba la información en los márgenes establecidos cuando observa la información.

El usuario proporciona el primer conjunto de reglas compacto al dispositivo cuando confirma el primer conjunto de reglas compacto.

Cuando el resultado del aprendizaje, es decir, la información en la primera tabla de asociación de aprendizaje, es compatible con el entorno de red real, el usuario envía la información de confirmación y proporciona el primer conjunto de reglas compacto al dispositivo.

Cuando se considera, mediante observación, que la información en la tabla de asociación de aprendizaje no es compatible con el entorno de red real, el usuario puede efectuar un cambio cuando se requiera y el dispositivo memoriza la información relacionada con el protocolo cambiada en una segunda tabla de asociación de aprendizaje y genera un segundo conjunto de reglas compacto en conformidad con la segunda tabla de asociación de aprendizaje.

En la forma de realización de la presente invención, haciendo referencia a la Figura 1, el método incluye, además:

S15: Realizar una detección de amenaza de protocolo en conformidad con el primer conjunto de reglas compacto.

Un objetivo último de la configuración del conjunto de reglas compacto es proporcionar una regla para un dispositivo IPS para realizar una detección de protocolo. Por lo tanto, la detección del protocolo se realiza en conformidad con un conjunto de reglas compacto después de que el conjunto de reglas compacto se genere en el dispositivo IPS.

En la forma de realización 5 de la presente invención, en donde un margen de aprendizaje establecido es un segmento de red DMZ, una dirección IP es IP1-IP2 y un umbral de tráfico válido es 5 %, se toma, a modo de ejemplo, para describir el proceso de la presente invención en detalle.

En primer lugar, DMZ, IP1-IP2, y el 5 % se introducen por el usuario en los espacios en blanco correspondientes a un segmento de red, una dirección IP y un umbral de tráfico válido.

Después de que se complete el establecimiento operativo, el dispositivo IPS genera la primera tabla de asociación de aprendizaje para hacer una preparación para un trabajo posterior. Según se ilustra en la Figura 2, la primera tabla de asociación de aprendizaje generada incluye dos partes: establecimiento de aprendizaje y contenido del aprendizaje. La parte de establecimiento del aprendizaje está dividida en dos columnas: un objetivo de aprendizaje y un umbral de tráfico válido. La parte de contenido del aprendizaje se divide en un total de 6 columnas de contenido: un protocolo, un protocolo de aplicación, tráfico, un puerto, software de servidor y una versión de aplicación. La columna del tráfico representa un valor del tráfico, cuyo valor inicial es 0 %.

Después de recibir el tráfico de la red activa, el dispositivo IPS selecciona primero el tráfico e ignora el tráfico más allá de los márgenes de DMZ y de IP1-IP2. A continuación, se extrae un paquete desde el tráfico y se realiza la identificación de la característica en el paquete para obtener información de un protocolo y de un protocolo de aplicación. Se realiza un análisis a fondo sobre el protocolo de aplicación, y se identifica una información, tal como un nombre de software de servidor, una versión y un puerto que se utilizan en el protocolo de aplicación. La información anterior se memoriza en correspondencia en la primera tabla de asociación de aprendizaje. Se recogen datos estadísticos sobre la información del valor del tráfico y la información del valor de tráfico se memoriza, en correspondencia, en la primera tabla de asociación de aprendizaje. En este caso, en la primera tabla de asociación de aprendizaje ilustrada en la Figura 3, la información correspondiente obtenida se memoriza en una columna correspondiente.

El tráfico inferior al 5 % y otra información correspondiente al tráfico se suprimen desde la primera tabla de asociación de aprendizaje. Es decir, en la Figura 3, se suprime un tráfico que es del 0.1 % y la información del protocolo correspondiente.

La base de reglas de vulnerabilidad dada a conocer en la presente invención es como sigue:

[Servicio Web] Apache 1.0: 5000 reglas de vulnerabilidad;

[Servicio Web] Apache 2.0: 3000 reglas de vulnerabilidad;

[Servicio Web] Apache HTTPD 2.2.3: 1000 reglas de vulnerabilidad;

[Servicio Web] Apache Tomcat 5.0: 500 reglas de vulnerabilidad;

[Servicio Web] Apache Tomcat 6.0.1: 500 reglas de vulnerabilidad;

[Servicio Web] IIS 1.0: 3000 reglas de vulnerabilidad;

[Servicio Web] IIS 2.0: 2000 reglas de vulnerabilidad;

[Servicio FTP] ProFTP 1.2.0: 1000 reglas de vulnerabilidad;

[Servicio FTP] ProFTP 1.3.0: 500 reglas de vulnerabilidad;

[Servicio de correo] SendMail 7.0: 300 reglas de vulnerabilidad;

[Servicio de correo] SendMail 8.0: 200 reglas de vulnerabilidad;

[Servicio de correo] Exchange Server 2007: 500 reglas de vulnerabilidad;

[Servicio de correo] Exchange Server 2010: 300 reglas de vulnerabilidad;

[Servicio base datos] MySQL 4.0: 1000 reglas de vulnerabilidad;

[Servicio base datos] MySQL 4.1: 500 reglas de vulnerabilidad;

[Servicio base datos] MySQL 5.0: 500 reglas de vulnerabilidad;

[Servicio base datos] MySQL5.1: 300 reglas de vulnerabilidad;

[Servicio base datos] SQLServer 2000: 300 reglas de vulnerabilidad;

[Servicio base datos] SQLServer 2005: 200 reglas de vulnerabilidad; y

[Servicio base datos] SQLServer 2008: 250 reglas de vulnerabilidad.

Un protocolo de aplicación HTTP corresponde a un servicio de la web, un protocolo de aplicación de FTP corresponde a un servicio FTP, un protocolo de aplicación NFS corresponde a un servicio NFS y los protocolos de aplicación SMTP y POP3 corresponden a un servicio de correo.

A continuación, se extrae un conjunto de reglas correspondientes:

En relación con un servicio de web:

las reglas siguientes se extraen desde la base de reglas de vulnerabilidad en conformidad con los resultados del aprendizaje Apache HTTPD 2.2.3 y Apache Tomcat 6.0.1:

[Servicio Web] Apache HTTPD 2.2.3: 1000 reglas de vulnerabilidad; y

[Servicio Web] Apache Tomcat 6.0.1: 500 reglas de vulnerabilidad.

En relación con un servicio FTP:

las siguientes reglas se extraen desde la base de reglas de vulnerabilidad en conformidad con un resultado del aprendizaje ProFTP 1.3.0:

[Servicio FTP] ProFTP 1.3.0: 500 reglas de vulnerabilidad.

En relación con un Servicio de correo:

en la etapa de aprendizaje, se encuentra que existe un tráfico de protocolo de correo; sin embargo, no se identifica un software específicamente utilizado; por lo tanto, todas las reglas de vulnerabilidad del correo se extraen desde la base de reglas de vulnerabilidad:

[Servicio de correo] SendMail 7.0: 300 reglas de vulnerabilidad;

[Servicio de correo] SendMail 8.0: 200 reglas de vulnerabilidad;

[Servicio de correo] Exchange Server 2007: 500 reglas de vulnerabilidad; y

[Servicio de correo] Exchange Server 2010: 300 reglas de vulnerabilidad.

En relación con un servicio de base de datos:

ningún tráfico del servicio de base de datos se encuentra en la etapa de aprendizaje; por lo tanto, se considera que el servicio no existe en la red real y no se extrae una regla correspondiente al servicio de base de datos.

Las reglas extraídas anteriores se resumen en el conjunto de reglas siguiente:

[Servicio Web] Apache HTTPD 2.2.3: 1000 reglas de vulnerabilidad;

[Servicio Web] Apache Tomcat 6.0.1: 500 reglas de vulnerabilidad;

[Servicio FTP] ProFTP 1.3.0: 500 reglas de vulnerabilidad;

[Servicio de correo] SendMail 7.0: 300 reglas de vulnerabilidad;

[Servicio de correo] SendMail 8.0: 200 reglas de vulnerabilidad;

[Servicio de correo] Exchange Server 2007: 500 reglas de vulnerabilidad; y

[Servicio de correo] Exchange Server 2010: 300 reglas de vulnerabilidad.

Por último, el resultado del aprendizaje y el conjunto de reglas compacto se impulsan hacia el usuario juntos para su configuración, y después de la confirmación se proporcionan al dispositivo IPS para la detección del protocolo.

En resumen, en conformidad con el método dado a conocer en la presente invención, el tráfico en una red activa se aprende e identifica para obtener información relacionada con el protocolo utilizada en la red activa; y una regla de detección se selecciona de entre una base de reglas de vulnerabilidad en función de la información del protocolo, de modo que el conjunto de reglas compacto generado corresponda a un protocolo utilizado en la red activa. Solamente el protocolo utilizado en la red activa necesita detectarse cuando se realiza una detección utilizando el conjunto de reglas compacto. Por lo tanto, se resuelve un problema de que todos los protocolos necesiten detectarse durante la detección puesto que un usuario selecciona todas las reglas de detección en la técnica anterior, lo que mejora la eficiencia de la detección y al mismo tiempo, evita un consumo innecesario de recursos de rendimiento. Además, un protocolo utilizado en una red se cambia con frecuencia y al usuario le resulta difícil percibirlo; por lo tanto, utilizando el método dado a conocer en la presente invención, un conjunto de reglas compacto configurado puede corresponder a un tipo de protocolo actualmente utilizado en tiempo real.

Haciendo referencia a la Figura 4, la forma de realización 6 de la presente invención da a conocer, además, un dispositivo para optimizar y configurar una regla de detección, en donde el dispositivo incluye las unidades siguientes:

una unidad de recepción de tráfico 11 que está configurada para recibir tráfico de red.

Una unidad de extracción 12 que está configurada para extraer un paquete desde el tráfico de red.

En general, un usuario transmite datos solamente en un determinado alcance de la red. Por lo tanto, un protocolo más allá del alcance de la red no se utiliza, y un tipo de protocolo utilizado más allá del alcance de la red no necesita detectarse. Por lo tanto, en la forma de realización de la presente invención, el dispositivo incluye además: una primera unidad de establecimiento, que está configurada para establecer un margen de aprendizaje. La unidad de extracción está configurada para extraer un paquete desde el tráfico dentro del margen de aprendizaje. Más concretamente, un segmento de red o una dirección IP que ha de ser objeto de aprendizaje puede establecerse a este respecto. Durante una puesta en práctica específica, puede utilizarse una manera de establecer múltiples opciones para la selección del usuario y una manera de introducción por el propio usuario puede utilizarse también. Cuando el usuario no selecciona una opción o no realiza ninguna entrada, el tráfico en la red completa puede establecerse para aprendizaje.

Una unidad de identificación de información 13 está configurada para identificar, en función con una característica del paquete, información relacionada con el protocolo utilizada en la red, en donde la información relacionada incluye un nombre de protocolo, un tipo de aplicación, un número de puerto, un nombre de software de servidor y una

versión de software del servidor.

Una primera unidad de salvaguarda 14 está configurada para salvaguardar información relacionada con el protocolo y la correspondencia entre la información relacionada con el protocolo hacia una primera tabla de asociación de aprendizaje.

Una primera unidad del conjunto de reglas compacto 15 está configurada para establecer una coincidencia de un elemento de regla correspondiente desde una base de reglas de vulnerabilidad en función de la información relacionada con el protocolo, con el fin de generar un primer conjunto de reglas compacto.

En algunas situaciones, el usuario solamente espera proteger y detectar tráfico en un determinado margen de valores, a modo de ejemplo, tráfico intenso, sin tener en cuenta ningún otro tráfico. Por lo tanto, en otra forma de realización de la presente invención, el dispositivo incluye, además, una segunda unidad de establecimiento, configurada para establecer un margen de valores de tráfico válidos.

La unidad de extracción está configurada, además, para extraer un paquete del tráfico dentro del margen de valores de tráfico válidos desde el tráfico de red.

En la presente invención, a veces, se realiza una identificación del tráfico antes de que se efectúe una recogida de datos estadísticos sobre un valor de tráfico, es decir, la información de protocolo correspondiente se obtiene identificando la característica del paquete antes de que pueda conocerse una magnitud del tráfico. En este caso, toda la información de protocolo correspondiente identificada necesita memorizarse primero en la primera tabla de asociación de aprendizaje, y la magnitud del tráfico, sobre el que se recogen datos estadísticos posteriormente, es también memorizada, en correspondencia, en la primera tabla de asociación de aprendizaje.

A continuación, el tráfico más allá del margen de valores válidos establecidos y la información del protocolo correspondiente se suprimen desde la primera tabla de asociación de aprendizaje en función del margen de valores de tráfico válidos establecido, con el fin de generar una nueva tabla de asociación de aprendizaje. Además, un elemento de regla se selecciona desde la base de reglas de vulnerabilidad en conformidad con la nueva tabla de asociación de aprendizaje, con el fin de generar un conjunto de reglas compacto.

El conjunto de reglas compacto generado puede aplicarse directamente al dispositivo. El usuario puede ver un registro de optimización y de configuración específico por intermedio de la información del registro. Con el fin de garantizar la exactitud, en una forma de realización específica de la presente invención, el dispositivo incluye, además, las unidades siguientes:

Una unidad de envío está configurada para enviar el primer conjunto de reglas compacto y la primera tabla de asociación de aprendizaje al usuario.

Más concretamente, el usuario puede conocer, viendo la información en la primera tabla de asociación de aprendizaje, si un resultado del aprendizaje del dispositivo es compatible con un entorno de red real. Con el fin de obtener un resultado más exacto, la información del valor de tráfico obtenida puede memorizarse en la primera tabla de asociación de aprendizaje al mismo tiempo en una etapa de aprendizaje del dispositivo.

Conviene señalar que, en una situación en la que el margen de aprendizaje y el margen de valores de tráfico válidos se establecen, el usuario solamente comprueba la información en los márgenes establecidos cuando observa la información correspondiente.

Una unidad de recepción está configurada para: cuando el usuario confirma el primer conjunto de reglas compacto, recibir el primer conjunto de reglas compacto proporcionado por el usuario.

Cuando el resultado del aprendizaje, es decir, la información en la primera tabla de asociación de aprendizaje, es compatible con el entorno de red real, el dispositivo incluye, además: el envío, por el usuario, de información de confirmación y la entrega del primer conjunto de reglas compacto al dispositivo.

Cuando el usuario considera, mediante su visión que la información contenida en la tabla de asociación de aprendizaje no es compatible con el entorno de red real, el dispositivo incluye, además, una segunda unidad de salvaguarda, que está configurada para salvaguardar la información relacionada con el protocolo modificada para una segunda tabla de asociación de aprendizaje cuando el usuario cambia la información relacionada con el protocolo.

La unidad del conjunto de reglas compacto está configurada, además, para seleccionar un elemento de regla desde la base de reglas de vulnerabilidad en conformidad con la segunda tabla de asociación de aprendizaje, con el fin de generar un segundo conjunto de reglas compacto.

Un objetivo último de configurar el conjunto de reglas compacto es proporcionar una regla para que un dispositivo

IPS realice una detección de protocolo. Por lo tanto, en la forma de realización de la presente invención, haciendo referencia a la Figura 4, el dispositivo incluye, además:

una unidad de detección 16, configurada para realizar una detección de amenaza en un protocolo en conformidad con el primer conjunto de reglas compacto.

Un experto en esta técnica puede entender que la totalidad o una parte de las etapas de las formas de realización del método anteriores pueden ponerse en práctica mediante un programa informático que proporcione instrucciones a un hardware pertinente. Los programas anteriores pueden memorizarse en un soporte de memorización legible por ordenador. Cuando se ejecuta el programa, se realizan las etapas de las formas de realización del método. El soporte de memorización anterior incluye varios soportes capaces de memorizar un código de programa, tal como una memoria ROM, una memoria RAM, un disco magnético o un disco óptico.

Lo que antecede describe el método y el dispositivo para optimizar y configurar una regla de detección dada a conocer en la presente invención en detalle. El principio y las maneras de puesta en práctica de la presente invención se describen aquí mediante formas de realización específicas. En las formas de realización anteriores, la descripción de cada forma de realización tiene su énfasis respectivo. Para una parte que no se describe en detalle en una determinada forma de realización, puede hacerse referencia a la descripción relacionada en otra forma de realización. La descripción sobre las formas de realización de la presente invención está prevista simplemente para facilitar el entendimiento del método y las ideas básicas de la presente invención. Al mismo tiempo, un experto en esta técnica puede realizar variaciones y modificaciones a la presente invención en términos de las puestas en práctica específicas y los alcances de aplicación en conformidad con las ideas inventivas de la presente invención. En resumen, el contenido de la especificación no debe entenderse como una limitación para la presente invención.

REIVINDICACIONES

1. Un método realizado por una entidad de red para optimizar y configurar una regla de detección, que comprende:

recibir (S11) un tráfico de red;

extraer (S12) un paquete desde el tráfico de red, e identificar, en conformidad con una característica del paquete, información relacionada con el protocolo utilizada en la red, incluyendo la información relacionada con el protocolo un elemento de o una combinación de varios elementos de la información siguiente: un nombre de protocolo, un nombre de protocolo de aplicación, un número de puerto, un nombre de software de servidor y una versión de software de servidor;

salvaguardar (S13) la información relacionada con el protocolo y una correspondencia entre elementos de información en la información relacionada con el protocolo hacia una primera tabla de asociación de aprendizaje;

obtener (S14) una regla de vulnerabilidad, que se establece en correspondencia con la información relacionada con el protocolo en una base de regla de vulnerabilidad, en función con la información relacionada con el protocolo identificada; y

integrar la regla de vulnerabilidad obtenida para generar un primer conjunto de reglas compacto cuando se identifican múltiples conjuntos de información de protocolo, en donde el primer conjunto de reglas compacto comprende en una regla de vulnerabilidad que se establece en correspondencia con la información de protocolo relacionada identificada en la base de reglas de vulnerabilidad;

antes de extraer un paquete procedente del tráfico de red, el método comprende, además:

establecer un margen de aprendizaje, en donde el margen de aprendizaje comprende un segmento de red o una dirección IP que se determina por anticipado; y

en consecuencia, la extracción de un paquete desde el tráfico de red comprende:

extraer, desde el tráfico de red, un paquete con una dirección contenida dentro del margen de aprendizaje.

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

realizar (S15) una detección de amenaza de protocolo en conformidad con el primer conjunto de reglas compacto.

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

enviar el primer conjunto de reglas compacto y la primera tabla de asociación de aprendizaje a un usuario; y

recibir el primer conjunto de reglas compacto proporcionado por el usuario cuando el usuario confirma el primer conjunto de reglas compacto.

4. El método según la reivindicación 3, que comprende, además:

salvaguardar una información relacionada con el protocolo modificada hacia una segunda tabla de asociación de aprendizaje cuando el usuario cambia la información relacionada con el protocolo en la primera tabla de asociación de aprendizaje; y

seleccionar una regla de vulnerabilidad a partir de la base de reglas de vulnerabilidad en función de la segunda tabla de asociación de aprendizaje, con el fin de generar un segundo conjunto de reglas compacto.

5. El método según la reivindicación 1, que comprende, además:

establecer un margen de valores de tráfico válidos, en donde el margen de valores válidos es un porcentaje de tráfico de tipo preestablecido dentro del tráfico total; y

después de salvaguardar la información relacionada con el protocolo y la correspondencia entre elementos de la información en la información relacionada con el protocolo hacia una primera tabla de asociación de aprendizaje, el método comprende, además:

suprimir, desde la primera tabla de asociación de aprendizaje, la información relacionada con el protocolo correspondiente al tráfico más allá del margen de valores de tráfico válidos.

6. Un método realizado por una entidad de red para optimizar y configurar una regla de detección, que comprende:

recibir (S11) un tráfico de red;

extraer (S12) un paquete desde el tráfico de red, e identificar, en conformidad con una característica del paquete, información relacionada con el protocolo utilizada en la red, incluyendo la información relacionada con el protocolo un elemento o una combinación de varios elementos de la información siguiente: un nombre de protocolo, un nombre de protocolo de aplicación, un número de puerto, un nombre de software de servidor y una versión de software de servidor;

salvaguardar (S13) la información relacionada con el protocolo y la correspondencia entre elementos de información en la información relacionada con el protocolo hacia una primera tabla de asociación de aprendizaje;

obtener (S14) una regla de vulnerabilidad, que se establece en correspondencia con la información relacionada con el protocolo en una base de reglas de vulnerabilidad, en conformidad con la información relacionada con el protocolo identificada; y

integrar la regla de vulnerabilidad obtenida para generar un primer conjunto de reglas compacto cuando se identifican múltiples conjuntos de información de protocolo, en donde el primer conjunto de reglas compacto consiste en una regla de vulnerabilidad que se establece en correspondencia con la información relacionada con el protocolo identificada en la base de reglas de vulnerabilidad;

antes de extraer un paquete desde el tráfico de red, el método comprende, además:

establecer un margen de valores de tráfico válidos, en donde el margen de valores válidos es un porcentaje del tráfico de tipo preestablecido en el tráfico total; y

en consecuencia, la extracción de un paquete desde el tráfico de red comprende:

extraer un paquete en el tráfico de al menos un protocolo de aplicación a partir del tráfico de red, en donde un porcentaje del tráfico de cada protocolo de aplicación en el al menos un protocolo de aplicación en el tráfico de red está dentro del margen de valores válidos.

7. El método según la reivindicación 6, que comprende, además:

realizar (S15) una detección de amenaza de protocolo en función del primer conjunto de reglas compacto.

8. El método según la reivindicación 6, que comprende, además:

enviar el primer conjunto de reglas compacto y la primera tabla de asociación de aprendizaje a un usuario; y

recibir el primer conjunto de reglas compacto proporcionado por el usuario cuando el usuario confirma el primer conjunto de reglas compacto.

9. El método según la reivindicación 8, que comprende, además:

salvaguardar la información relacionada con el protocolo modificada hacia una segunda tabla de asociación de aprendizaje cuando el usuario cambia la información relacionada con el protocolo en la primera tabla de asociación de aprendizaje; y

seleccionar una regla de vulnerabilidad desde la base de reglas de vulnerabilidad en función de la segunda tabla de asociación de aprendizaje, con el fin de generar un segundo conjunto de reglas compacto.

10. Un dispositivo para optimizar y configurar una regla de detección, que comprende:

una unidad de recepción de tráfico (11), configurada para recibir un tráfico de red;

una unidad de extracción (12), configurada para extraer un paquete desde el tráfico de red;

una unidad de identificación de información, configurada para identificar, en función de una característica del paquete, información relacionada con el protocolo utilizada en la red, incluyendo la información relacionada con el protocolo un elemento de una combinación de varios elementos de la información siguiente: un nombre de protocolo, un nombre de protocolo de aplicación, un número de puerto, un nombre de software de servidor y una versión de software de servidor;

una primera unidad de salvaguarda (14), configurada para salvaguardar la información relacionada con el protocolo y la correspondencia entre elementos de información en la información relacionada con el protocolo hacia una primera tabla de asociación de aprendizaje; y

una primera unidad del primer conjunto de reglas compacto (15), configurada para obtener una regla de vulnerabilidad, que se establece en correspondencia con información relacionada con el protocolo en una base de reglas de vulnerabilidad, en función de la información relacionada con el protocolo identificada y para integrar la regla obtenida para generar un primer conjunto de reglas compacto cuando se identifican múltiples conjuntos de información del protocolo, en donde el primer conjunto de reglas compacto consiste en una regla de vulnerabilidad que se establece en correspondencia con la información relacionada con el protocolo identificada en la base de reglas de vulnerabilidad;

una primera unidad de establecimiento, configurada para establecer un margen de aprendizaje, en donde el margen de aprendizaje comprende un segmento de red o una dirección IP que se determina por anticipado;

en donde

la unidad de extracción está configurada, además, para extraer, desde el tráfico de red, un paquete con una dirección contenida dentro del margen de aprendizaje.

11. El dispositivo según la reivindicación 10, que comprende, además:

una unidad de detección, configurada para realizar una detección de amenaza sobre un protocolo en conformidad con el primer conjunto de reglas compacto.

12. El dispositivo según la reivindicación 10, que comprende, además:

una unidad de envío, configurada para enviar el primer conjunto de reglas compacto y la primera tabla de asociación de aprendizaje a un usuario; y

una unidad de recepción, configurada para: cuando el usuario confirma el primer conjunto de reglas compacto, recibir el primer conjunto de reglas compacto proporcionado por el usuario.

13. El dispositivo según la reivindicación 12, que comprende, además:

una segunda unidad de salvaguarda, configurada para salvaguardar una información relacionada con el protocolo modificada hacia una segunda tabla de asociación de aprendizaje cuando el usuario cambia la información relacionada con el protocolo en la primera tabla de asociación de aprendizaje, en donde

la unidad del conjunto de reglas compacto está configurada, además, para seleccionar una regla de vulnerabilidad desde la base de reglas de vulnerabilidad en función de la segunda tabla de asociación de aprendizaje, con el fin de generar un segundo conjunto de reglas compacto.

14. El dispositivo según la reivindicación 12, que comprende, además:

una segunda unidad de establecimiento, configurada para establecer un margen de valores de tráfico válidos, en donde el margen de valores válido es un porcentaje de un tráfico de tipo preestablecido en el tráfico total; en donde

la primera unidad de salvaguarda está configurada, además, para suprimir, desde la primera tabla de asociación de aprendizaje, una información relacionada con el protocolo en correspondencia con el tráfico más allá del margen de valores de tráfico válidos.

15. Un dispositivo para optimizar y configurar una regla de detección, que comprende:

una unidad de recepción de tráfico (11), configurada para recibir un tráfico de red;

una unidad de extracción (12), configurada para extraer un paquete desde el tráfico de red;

una unidad de identificación de información, configurada para identificar, en función de una característica del paquete, información relacionada con el protocolo utilizada en la red, incluyendo la información relacionada con el protocolo un elemento o una combinación de varios elementos de información siguiente: un nombre de protocolo, un nombre de protocolo de aplicación, un número de puerto, un nombre de software de servidor y una versión del software de servidor;

una primera unidad de salvaguarda (14), configurada para salvaguardar la información relacionada con el protocolo y la correspondencia entre elementos de información en la información relacionada con el protocolo hacia una

primera tabla de asociación de aprendizaje; y

una primera unidad del conjunto de reglas compacto (15), configurada para obtener una regla de vulnerabilidad que se establece en correspondencia con una información relacionada con el protocolo en una base de reglas de vulnerabilidad, en función de la información relacionada con el protocolo identificada; y para integrar la regla obtenida para generar un primer conjunto de reglas compacto cuando se identifican múltiples conjuntos de información de protocolo, en donde el primer conjunto de reglas compacto consiste en una regla de vulnerabilidad que se establece en correspondencia con la información relacionada con el protocolo identificada en la base de reglas de vulnerabilidad;

una segunda unidad de establecimiento, configurada para establecer un margen de valores de tráfico válidos, en donde el margen de valores válidos es un porcentaje del tráfico de tipo preestablecido en el tráfico total;

en donde

la unidad de extracción está configurada, además, para extraer un paquete en el tráfico de al menos un protocolo de aplicación desde el tráfico de red, en donde un porcentaje del tráfico de cada protocolo de aplicación en el al menos un protocolo de aplicación en el tráfico de red está dentro del margen de valores válidos.

16. El dispositivo según la reivindicación 15, que comprende, además:

una unidad de detección, configurada para realizar una detección de amenaza sobre un protocolo en conformidad con el primer conjunto de reglas compacto.

17. El dispositivo según la reivindicación 15, que comprende, además:

una unidad de envío configurada para enviar el primer conjunto de reglas compacto y la primera tabla de asociación de aprendizaje a un usuario; y

una unidad de recepción, configurada para: cuando el usuario confirma el primer conjunto de reglas compacto, recibir el primer conjunto de reglas compacto proporcionado por el usuario.

18. El dispositivo según la reivindicación 17, que comprende, además:

una segunda unidad de salvaguarda, configurada para salvaguardar una información relacionada con el protocolo modificada hacia una segunda tabla de asociación de aprendizaje cuando el usuario cambia la información relacionada con el protocolo en la primera tabla de asociación de aprendizaje, en donde

la unidad del conjunto de reglas compacto está configurada, además, para seleccionar una regla de vulnerabilidad desde la base de reglas de vulnerabilidad en función de la segunda tabla de asociación de aprendizaje, con el fin de generar un segundo conjunto de reglas compacto.

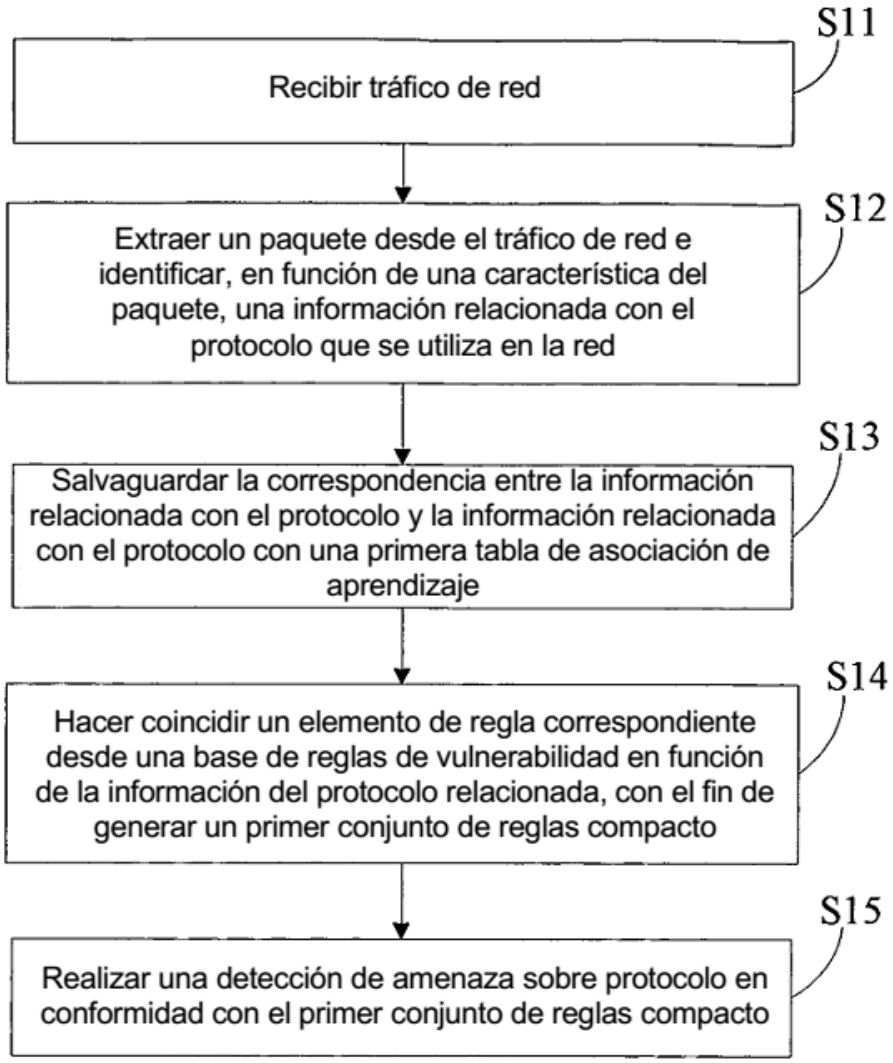
S11
Recibir tráfico de red
S12
Extraer un paquete desde el tráfico de red e identificar, en función de una característica del paquete, una información relacionada con el protocolo que se utiliza en la red
S13
Salvaguardar la correspondencia entre la información relacionada con el protocolo y la información relacionada con el protocolo con una primera tabla de asociación de aprendizaje
S14
Hacer coincidir un elemento de regla correspondiente desde una base de reglas de vulnerabilidad en función de la información del protocolo relacionada, con el fin de generar un primer conjunto de reglas compacto
S15
Realizar una detección de amenaza sobre protocolo en conformidad con el primer conjunto de reglas compacto

FIG. 1

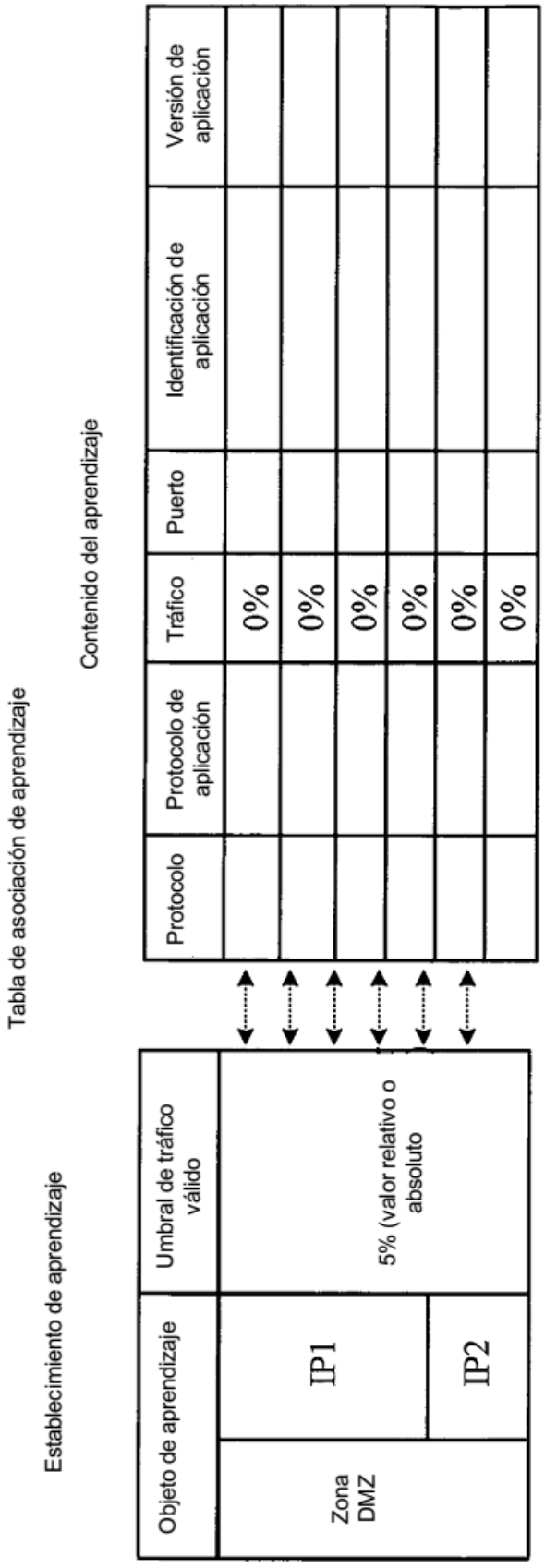
Establecimiento de aprendizaje
Objeto de aprendizaje
Umbral de tráfico válido
Zona DMZ
IP1
IP2
5% (valor relativo o absoluto
Tabla de asociación de aprendizaje
Contenido del aprendizaje
Protocolo
Protocolo de aplicación
Tráfico
Puerto
Identificación de aplicación
Versión de aplicación
0%
0%
0%
0%
0%
0%

FIG. 2

Tabla de asociación de aprendizaje

Objeto de aprendizaje		Umbral de tráfico válido	Protocolo	Protocolo de aplicación	Tráfico	Puerto	Identificación de aplicación	Versión de aplicación
Zona DMZ	IP1	5% (valor relativo o absoluto	TCP	HTTP	50%	80	Apache HTTPD	2.2.3
			TCP	HTTP	10%	8080	Apache Tomcat	6.0.1
			TCP	FTP	5%	21	ProFTP	1.3.0
			UDP	NFS	0.1%	2049	NFSD	V4
	IP2		TCP	SMTP	15%	25	Sendmail	8.12.5
			TCP	POP3	20%	110	Sendmail	8.12.5

FIG. 3

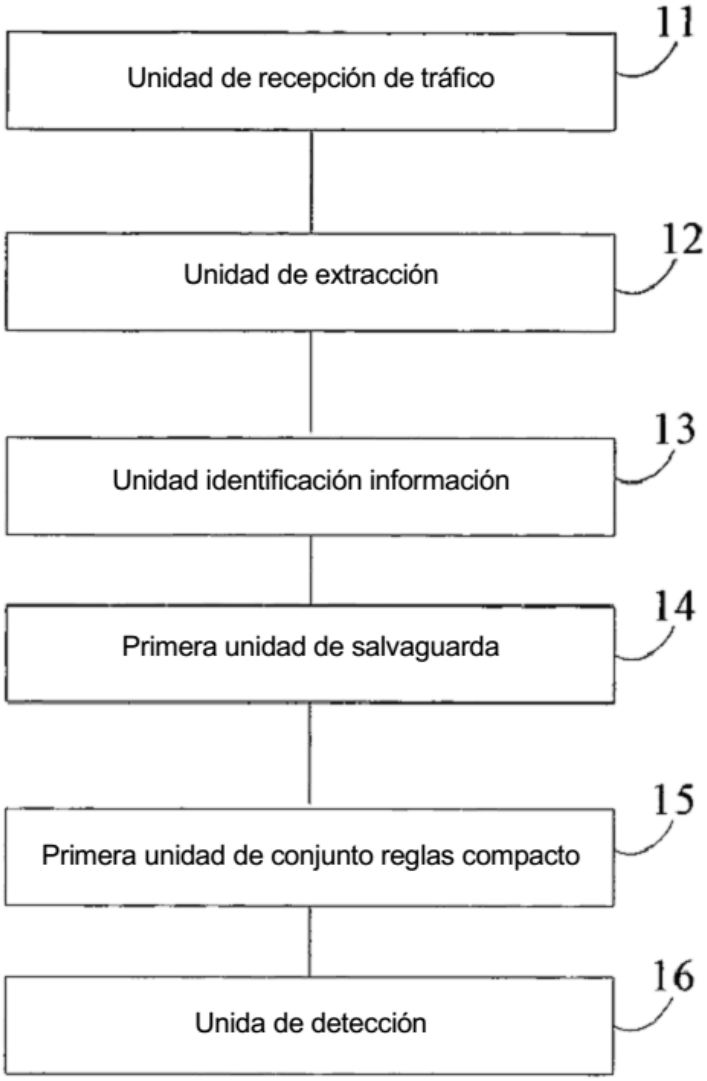
11
Unidad de recepción de tráfico
12
Unidad de extracción
13
Unidad identificación información
14
Primera unidad de salvaguarda
15
Primera unidad de conjunto reglas compacto
16
Unida de detección

FIG. 4