(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 702 097**

(51) Int. CI.:

H04L 12/22 (2006.01)
G06Q 50/00 (2012.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.12.2010 PCT/US2010/060089**

(87) Fecha y número de publicación internacional: **16.06.2011 WO11072289**

(96) Fecha de presentación y número de la solicitud europea: **13.12.2010 E 10836803 (6)**

(97) Fecha y número de publicación de la concesión europea: **19.09.2018 EP 2510648**

(54) Título: **Sistema y servicio de cortafuegos basado en la nube**

(30) Prioridad:

12.12.2009 US 285958 P
10.12.2010 US 965188

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.02.2019

(73) Titular/es:

AKAMAI TECHNOLOGIES, INC. (100.0%)
8 Cambridge Center
Cambridge, MA 02142, US

(72) Inventor/es:

LAGHATE, PRASANNA;
DEVANNEAUX, THOMAS;
DILLEY, JOHN y
SUMMERS, JOHN

(74) Agente/Representante:

INGENIAS CREACIONES, SIGNOS E INVENCIONES, SLP

DESCRIPCIÓN

Sistema y servicio de cortafuegos basado en la nube

Campo de la invención

La presente invención se refiere en general a un sistema y servicio de cortafuegos basado en la nube, incluyendo en particular tales sistemas y servicios implementados en sistemas informáticos de borde y otros sistemas informáticos distribuidos.

Antecedentes de la invención

Sistemas informáticos distribuidos se conocen en la técnica. Un sistema informático distribuido de este tipo es una "red de distribución de contenidos" o "CDN" que se opera y gestiona por un proveedor de servicios. El proveedor de servicios habitualmente proporciona el servicio en nombre de terceras parte. Un "sistema distribuido" de este tipo habitualmente se refiere a una colección de ordenadores autónomos enlazados mediante una red o redes, junto con el software, sistemas, protocolos y técnicas diseñadas para facilitar diversos servicios, tal como distribución de contenido o el soporte de infraestructura de sitio externalizada. Típicamente, "distribución de contenido" significa el almacenamiento, almacenamiento en caché, o transmisión de contenido, medios de difusión en continuo y aplicaciones en nombre de proveedores de contenido, incluyendo tecnologías auxiliares usadas con los mismos que incluyen, sin limitación, tratamiento de peticiones de DNS, aprovisionamiento, supervisión y notificación de datos, focalización de contenido, personalización e inteligencia empresarial. Típicamente, la expresión "infraestructura de sitio externalizada" significa los sistemas distribuidos y tecnologías asociadas que habilitan que una entidad opere y/o gestiones una infraestructura de sitio web de una tercera parte, en su totalidad o en parte, en nombre de la tercera parte.

En un sistema conocido, tal como se muestra en la Figura 1, un sistema informático distribuido 100 se configura como una CDN y se supone que tiene un conjunto de máquinas 102 distribuidas alrededor de la Internet. Típicamente, la mayoría de las máquinas son servidores ubicados cerca del borde de la Internet, es decir, en o adyacentes a redes de acceso de usuario final. Un centro de control de operaciones de red (NOCC) 104 gestiona operaciones de las diversas máquinas en el sistema. Sitios de terceras parte, tal como el sitio web 106, descargan distribución de contenido (por ejemplo, HTML, objetos de página embebidos, medios de difusión en continuo, descargas de software y similares) al sistema informático distribuido 100 y, en particular, a servidores de contenido (también denominados como "servidores de borde") que se ejecutan en las máquinas 102. Típicamente, proveedores de contenido descargan su distribución de contenido solapando (por ejemplo, mediante un CNAME de DNS) dominios de proveedor de contenido dados o subdominios a dominios que se gestionan por servicio de nombres de dominio autorizado del proveedor de servicios, más detalles de lo cual se exponen en la Patente de Estados Unidos N.º 7.293.093 y 7.693.959. Usuarios finales que operan máquinas cliente 122 que desean que el contenido se dirija al sistema informático distribuido 100, y más particularmente a una de sus máquinas 102, para obtener ese contenido de forma más fiable y eficiente.

El sistema informático distribuido también puede incluir otra infraestructura, tal como un sistema de recopilación de datos distribuidos 108 que recoge el uso y otros datos desde los servidores de borde, agrega esos datos a través de una región o conjunto de regiones y pasa esos datos a otros sistemas finales 110, 112, 114 y 116 para facilitar supervisión, registro, alertas, facturación, gestión y otras funciones operacionales y administrativas. Agentes de red distribuida 118 supervisan la red así como las cargas de servidor y proporcionan datos de red, tráfico y carga a un mecanismo de tratamiento de consultas de DNS 115, que está autorizado para que dominios de contenido se gestionen por la CDN. Un mecanismo de transporte de datos distribuido 120 puede usarse para distribuir información de control (por ejemplo, metadatos para gestionar contenido, facilitar equilibrio de carga y similares) a los servidores de borde. Más acerca de la distribución de información de control en una CDN puede encontrarse en la Patente de Estados Unidos N.º 7.240.100.

Como se ilustra en la Figura 2, una máquina dada 200 comprende hardware básico (por ejemplo, un Intel Pentium u otro procesador) 202 que ejecuta un núcleo de sistema operativo (tal como Linux o variante) 204 que soporta una o más aplicaciones 206a-n. Para facilitar servicios de distribución de contenido, por ejemplo, máquinas dadas habitualmente ejecutan un conjunto de aplicaciones, tal como un intermediario de HTTP 207 (en ocasiones denominado como un proceso de "anfitrión global" o "fantasma"), un servidor de nombres 208, un proceso de supervisión local 210, un proceso de recopilación de datos distribuido 212 y similares. Para medios de difusión en continuo, la máquina habitualmente incluye uno o más servidores de medios, tal como un Servidor de Medios de Windows (WMS) o servidor Flash, según se requiera por los formatos de medios soportados.

Las máquinas cliente 122 incluyen ordenadores personales convencionales, portátiles, otros dispositivos de procesamiento de datos digitales. Máquinas cliente también incluyen clientes móviles, que pueden incluir una cualquiera diversidad de dispositivos móviles, a menudo denominados como teléfonos inteligentes o asistentes digitales personales (PDA). Un servidor de borde de CDN se configura para proporcionar una o más características de distribución de contenido extendidas, preferentemente en una base específica de dominio y específica de cliente, preferentemente usando archivos de configuración que se distribuyen a los servidores de borde usando un sistema de configuración. Un archivo de configuración dado preferentemente se basa en XML e incluye un conjunto de reglas de tratamiento de contenido y directivas que facilitan una o más características de tratamiento de contenido avanzadas. El archivo de configuración puede distribuirse al servidor de borde de CDN a través del mecanismo de transporte de datos. La Patente de Estados Unidos N.º 7.111.057, ilustra una infraestructura útil para la distribución y gestión de información de control de contenido de servidor de borde, tal como el que controla las peticiones de purga de archivos.

La CDN puede incluir un subsistema de almacenamiento (NetStorage), tal como se describe en la Patente de Estados Unidos N.º 7.472.178.

La CDN puede operar una jerarquía de caché de servidor (Cache-H) para proporcionar almacenamiento en caché intermedio de contenido de cliente; un sistema de jerarquía de caché de este tipo se describe en la Patente de Estados Unidos N.º 7.376.716.

Para distribución de difusión en continuo en directo, la CDN pueden incluir un subsistema de distribución, tal como se describe en la Patente de Estados Unidos N.º 7.296.082.

La CDN puede proporcionar distribución de contenido segura entre un navegador cliente, servidor de borde y servidor de origen de cliente de la manera descrita en la Publicación de Estados Unidos N.º 2004/0093419 y/o Patente de Estados Unidos N.º 7.363.361.

Distribución de contenido segura como se describe en este documento obliga a enlaces basados en SSL entre el cliente y el proceso de servidor de borde, por una parte, y entre el proceso de servidor de borde y un proceso de servidor de origen, por otra parte. Esto habilita que una página web protegida mediante SSL y/o componentes de la misma se distribuyan a través del servidor de borde.

El documento WO 02/054699, 11 de julio de 2002 (11-07-2002), divulga un proveedor de servicio de CDN (CDNSP) que despliega una o más regiones de CDN detrás de un cortafuegos corporativo de una empresa.

Sumario

En este documento se divulga un sistema y servicio de cortafuegos basado en la nube que protege sitios de origen de clientes de ataques, fuga de información confidencial y otras amenazas de seguridad. Un sistema y servicio de cortafuegos de este tipo puede implementarse en conjunto con una red de distribución de contenidos (CDN) que tiene una pluralidad de servidores de contenido distribuidos.

Por ejemplo, en una realización ilustrativa de la invención, se proporciona un método de distribución de contenido en una CDN operada por un proveedor de servicios de red de distribución de contenidos (CDNSP) en nombre de proveedores de contenido participantes. Los proveedores de contenido participantes identifican contenido a distribuir a través de la CDN. El método de distribución de contenido implica recibir primeros ajustes de cortafuegos desde un primer proveedor de contenido participante que especifica cómo tiene que operarse un cortafuegos con respecto a peticiones de contenido identificadas por ese primer proveedor de contenido participante para distribuir a través de la CDN. Otros ajustes, potencialmente diferentes, de cortafuegos se reciben desde un segundo proveedor de contenido participante que especifica cómo tiene que operarse un cortafuegos con respecto a peticiones de contenido identificadas por ese segundo proveedor de contenido participante para distribuir a través de la CDN. Los ajustes se envían a diversos servidores de contenido en la CDN en un archivo de configuración de metadatos u otra forma. En uno de esos servidores de contenido, se recibe una primera petición de contenido identificada por el proveedor de contenido participante para distribuir a través de la CDN. El servidor de contenido evalúa la primera petición usando un cortafuegos configurado con el uno o más primeros ajustes de cortafuegos. Se recibe una segunda petición de contenido identificado por el segundo proveedor de contenido participante para distribuir a través de la CDN. La segunda petición se evalúa usando un cortafuegos configurado con el uno o más segundos ajustes de cortafuegos.

En realizaciones relacionadas, en un método como se describe anteriormente, la evaluación de la primera petición usando un cortafuegos configurado con el uno o más primeros ajustes de cortafuegos implica probar la primera petición contra uno o más criterios. La evaluación de la segunda petición puede proceder de forma similar. Si se cumplen los criterios, puede tomarse una acción, tal como denegar la petición, generar una alerta, modificar la petición, detener el procesamiento de la petición y registrar la petición.

Los ajustes de cortafuegos pueden incluir direcciones IP para las que se toma una acción particular, por ejemplo,

puede bloquearse tráfico desde direcciones IP particulares o puede permitirse tráfico desde esas direcciones con todo el resto de tráfico bloqueado. Por lo tanto, el cortafuegos puede aplicar seguridad en la capa de aplicación (a peticiones de HTTP y otras), la capa de red y/o otras capas.

En otra realización ilustrativa de la invención, se proporciona un método de distribución de contenido en una CDN que implica recibir una primera configuración de cortafuegos y segunda configuración de cortafuegos (por ejemplo, cada una con uno o más ajustes de cortafuegos) desde un proveedor de contenido participante. El proveedor de contenido participante también especifica el uso de criterios que exponen si la primera configuración de cortafuegos tiene que usarse para evaluar una petición de contenido, y uso de criterios que exponen si la segunda configuración de cortafuegos tiene que usarse para evaluar una petición de contenido. Los criterios de uso pueden tener en cuenta tales características como un nombre de dominio en una petición, subdominio en una petición, URL de una petición, tipo de contenido solicitado, nombre de archivo de contenido solicitado, extensión de archivo de contenido solicitado.

Continuando con el ejemplo anterior, estos ajustes y criterios de uso se envían al servidores de contenido en la CDN. En uno de servidores de contenido se recibe una petición de contenido del proveedor de contenido participante. Basándose en la petición y los primeros criterios de configuración de uso de cortafuegos, el servidor de contenido determina si la primera configuración de cortafuegos tiene que usarse, y si es así, evalúa la petición usando un cortafuegos configurado con la primera configuración de cortafuegos. Basándose en la petición y los segundos criterios de configuración de uso de cortafuegos, el servidor de contenido determina si la segunda configuración de cortafuegos tiene que usarse, y si es así, evalúa la petición usando un cortafuegos configurado con la segunda configuración de cortafuegos. Prestaciones y características adicionales se exponen a lo largo de esta divulgación.

Breve descripción de los dibujos

La invención se entenderá más completamente a partir de la siguiente descripción detallada tomada en conjunto con los dibujos adjuntos, en los que:

la Figura 1 es un diagrama de bloques de una red de distribución de contenidos en la que la presente invención puede implementarse;

la Figura 2 es un diagrama de bloques simplificado de un servidor de contenido en una CDN;

la Figura 3 es un diagrama de un sistema de cortafuegos basado en la nube distribuido de acuerdo con una realización de la invención;

la Figura 4 es un diagrama de flujo que ilustra la configuración de un cortafuegos de acuerdo con una realización de la invención;

la Figura 5 es un ejemplo de una interfaz de usuario para seleccionar ajustes de capa de aplicación para configurar un cortafuegos;

la Figura 6 es un ejemplo de una interfaz de usuario para seleccionar ajustes de capa de red para configurar un cortafuegos;

la Figura 7 es un ejemplo de una interfaz de usuario para designar criterios de coincidencia para identificar esas propiedades digitales y/o archivos a los que se aplicará una configuración de cortafuegos particular;

la Figura 8 es un ejemplo de código que configura un cortafuegos;

la Figura 9 es un diagrama de flujo que ilustra operación de un cortafuegos configurado de acuerdo con una realización de la invención; y

la Figura 10 es un diagrama de bloques simplificado de un sistema informático con el que puede implementarse la presente invención.

Descripción detallada

La siguiente descripción detallada expone realizaciones para proporcionar un entendimiento general de los principios de la estructura, función y uso de los métodos y sistemas divulgados en este documento. Los métodos y sistemas descritos en este documento e ilustrados en los dibujos adjuntos son ejemplos no limitantes; el alcance de la presente invención se define solamente mediante las reivindicaciones. Las características descritas o ilustradas en conexión con una realización ilustrativa pueden combinarse con las características de otras realizaciones. Tales modificaciones y variaciones se conciben para incluirse dentro del alcance de la presente invención.

Los métodos y sistemas divulgados en este documento puede implementarse en un sistema informático distribuido,

por ejemplo, una red de distribución de contenidos ("CDN") como se ilustra en las Figuras 1-2, y se describirá con respecto a una CDN de este tipo. Sin embargo, no se limitan a tales implementaciones. La infraestructura de red distribuida y compartida descrita en este documento puede usarse, entre otras cosas, para suministrar contenido desde una pluralidad de sitios web.

La Figura 3 ilustra un sistema y servicio de cortafuegos basado en la nube distribuido 300 de acuerdo con una realización de la invención. Los servidores de contenido 302 se distribuyen alrededor de la Internet como parte de una CDN, como se ha analizado anteriormente en conexión con las Figuras 1-2. En este sistema 300, cada servidor de contenido 302 incluye y/o se acopla a un cortafuegos 302a. Los cortafuegos 302a inspeccionan y filtran tráfico, y se configuran para bloquear o pasar tráfico basándose en criterios de seguridad especificados. Los cortafuegos 302a pueden operar en la capa de aplicación, capa de red o en otras capas de interconexión informáticas. Los cortafuegos 302a puede implementarse en hardware, software o una combinación de los mismos.

Las máquinas cliente 322 que desean contenido desde el servidor de origen 306 se dirigen a uno de los servidores de contenido 302. Las peticiones (por ejemplo, una petición de HTTP o HTTPS) se examinan en el borde de red por los cortafuegos 302a, que se configuran para examinar el tráfico para ataques, fuga de información u otras clases de riesgos de seguridad. Las peticiones que pasan los cortafuegos 302a se procesan de forma normal, sirviéndose el contenido solicitado desde la caché del servidor de contenido 302 o recuperándose por el servidor de contenido 302 desde el servidor de origen 306 para distribuir a la máquina cliente 322 o se trata de otra manera. Las peticiones que se identifican como ataques u otras amenazas de seguridad (tal como las de la máquina de atacante 324) desencadenan que el cortafuegos 302 tome una cierta acción, por ejemplo, bloquear la petición, registrar la misma para alerta o de otra manera. Por lo tanto, se identifican y bloquean amenazas o de otra manera se abordan por el sistema 300 más cercano a la fuente y antes de alcanzar el servidor de origen 306, descargando esa carga del servidor de origen 306. En el caso en el que los servidores 302 se ubican en los "bordes" de red, los cortafuegos 302a abordan esas amenazas en el borde de red. Se ha de observar que el servidor de origen 306 puede emplear su propio sistema de cortafuegos centralizado y protección/detección de intrusión u otro sistema de seguridad, además del sistema de cortafuegos desplegado en el servidores de contenido 302.

Aunque el proveedor de CDN puede configurar los cortafuegos 302a (por ejemplo, con un ajuste por defecto o de otra manera), el sistema 300 permite que el proveedor de contenido asociado con el servidor de origen 306, como un cliente de la CDN, configure los ajustes de cortafuegos que aplicará a peticiones de contenido de ese proveedor de contenido.

Porque el módulo de cortafuegos se implementa en múltiples procesos fantasma a lo largo de toda la CDN, la solución ilustrada en la Figura 3 es un "cortafuegos distribuido" que proporciona un anillo defensivo exterior y altamente escalable para la protección de aplicaciones web. La solución es altamente configurable a través de las técnicas de configuración de metadatos descritas en este documento. El módulo, a través de la implementación de controles de Capa de Red y de Aplicación, ayuda a evitar amenazas y técnicas de explotación, tal como inyección de SQL, Secuencias de Comandos en Sitios Cruzados (XSS) y otros ataques de HTTP.

Implementando la materia objeto descrita en este documento en una red distribuida tal como una CDN, un proveedor de servicios de CDN proporciona un servicio gestionado de cortafuegos. El servicio proporciona un sistema de defensa de borde escalable para bloquear, entre otras cosas, ataques a aplicaciones web en la nube. El servicio de cortafuegos proporciona a clientes de CDN con un enfoque único para defender fácil y económicamente sus aplicaciones web. Sin hardware que gestionar o mantener, los clientes de CDN gestionan su propia regla de seguridad establecida a través del portal (extranet) de cliente del proveedor de servicio de CDN. Adicionalmente, el servicio de cortafuegos ayuda a habilitar el cumplimiento con la Norma de Seguridad de Datos para el Sector de las Tarjeta de Pago. La infraestructura se comparte a través de múltiples clientes de CDN, pero cada cliente puede proporcionar y gestionar su propio cortafuegos para protegerse contra ataques.

Con la anterior visión de conjunto, la materia objeto de este documento se describirán ahora en más detalle.

1.0 Cortafuegos basado en la nube

Cortafuegos basado en la nube (CF) es un módulo de seguridad para clientes de red de distribución de contenidos. El módulo de CF aplica una evaluación basada en reglas de peticiones para buscar comportamientos sospechosos, tal como violaciones de protocolo, violaciones de política de HTTP, violaciones de límite de peticiones, robots, puertas traseras de troyanos, ataques genéricos (tal como secuencias de comandos en sitios cruzados, diversos ataques de inyección y así sucesivamente), fuga de contenido de salida (anuncios de servidor) y varias otras categorías.

El cumplimiento con normas de seguridad de datos para el sector de las tarjeta de pago (PCI-DSS) requiere que se use un cortafuegos de aplicación por compañías que procesan transacciones de pago con tarjeta para supervisar y proteger la infraestructura de origen de los muchos ataques de interfaz web existentes que existen en la actualidad. El módulo de CF puede usarse en conjunto con un módulo de PCI para ayudar a clientes a cumplir con estos requisitos de cumplimiento con PCI. La solución de CF protege un servidor de origen de peticiones que se

encaminan a través de los servidores de CDN; también puede utilizarse un medio adicional de proteger el origen. Una solución de este tipo se describe en la Patente de Estados Unidos N.º 7.260.639.

Preferentemente, el cortafuegos en la nube se basa en un conjunto de reglas principales (por ejemplo, un conjunto de reglas disponible de Breach Security Labs, por ejemplo, ModSecurity v1.6). ModSecurity aplica un conjunto amplio de criterios de coincidencia a peticiones de HTTP para identificar comportamientos que pueden clasificarse como ataques, fuga de información u otras clases de amenazas de seguridad. El Conjunto de Reglas Principal define reglas de seguridad así como parámetros de configuración para el servidor web Apache. En un nivel alto, una regla de seguridad es una expresión asociada con datos. La expresión normalmente es la combinación de un operador, variables y traducciones, que producen una booleana. Una expresión también puede ser una lógica OR o AND entre otras expresiones, o la negación de otras expresiones. Los datos para cada regla consisten en un identificador (o "id"), una etiqueta, un mensaje, una bandera que indica si la petición debería denegarse, un nivel de severidad, etc.

Como se ha indicado anteriormente, preferentemente el cortafuegos aprovecha un conjunto de reglas, tal como Conjunto de Reglas Principal de ModSecurity de código abierto soportado por Breach Security, que define tipos de ataques comunes y dañinos y técnicas de explotación, tal como inyección de SQL, Secuencias de Comandos en Sitios Cruzados (XSS) y otros 10 ataques principales de Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP). Pueden utilizarse otros conjuntos de reglas.

Estas reglas principales (o un subconjunto de las mismas) se convierten en una solución funcional de metadatos, con metadatos de control distribuyéndose y aplicándose a los servidores de CDN de la manera descrita en la Patente de Estados Unidos N.º 7.240.100. En particular, preferentemente los metadatos se provisionan a través de un portal de extranet orientado al cliente (por ejemplo, a través de una interfaz de usuario basada en web) y proporcionan a los servidores de contenido dentro de un archivo de configuración de metadatos. Porque el archivo de configuración puede necesitar cambiar frecuentemente (ocuparse de escenarios de ataques), preferentemente la configuración de metadatos relacionados con CF se distribuye a procesos de servidor de contenido de CDN usando un canal de comunicación especializado y rápido. Véase la Patente de Estados Unidos N.º 7.149.807 para una infraestructura de comunicación útil que puede usarse para este propósito. En algunas realizaciones, el despliegue de los archivos de configuración a lo largo de todo el sistema distribuido puede lograrse dentro de un corto periodo de tiempo, habilitando ventajosamente respuesta en tiempo real a ataques.

El archivo de configuración de metadatos de CF debería estar listo para búsqueda cuando el cortafuegos se activa en un servidor de contenido particular. Como se describirá a continuación en conexión con la Figura 8, se proporcionan varias etiquetas y características en la estructura de metadatos de modo que el proceso de servidor de contenido de CDN (fantasma) puede soportar el procesamiento de conjunto de reglas.

2.0 Visión de conjunto de configuración

La Figura 4 ilustra el proceso de configuración. En la etapa 400, se crea o selecciona una instancia de cortafuegos (para cortafuegos anteriormente configurados). En la etapa 402, se configuran los ajustes de capa de aplicación. La funcionalidad de filtrado del cortafuegos se controla estableciendo criterios que definen ataques u otras clases de amenazas de seguridad, usando la cual el cortafuegos examinará tráfico. (En realizaciones alternativas, pueden implementarse criterios para definir tráfico seguro o "confiable", por ejemplo, tráfico desde una fuente particular o con una firma particular. Por conveniencia de descripción, la expresión "criterios de seguridad" se usa en lo sucesivo para referirse a, colectivamente, las clases anteriores de criterios.) Criterios de seguridad pueden elegirse seleccionando/habilitando reglas predefinidas de conjuntos de reglas o, como alternativa, autorizando directamente expresiones booleanas u otra lógica explícitamente. La Figura 5 ilustra una interfaz de usuario para seleccionar reglas predefinidas que aplicarán a una instancia de cortafuegos identificada como "Prueba-Prueba." La interfaz de usuario también permite selección de acciones que el cortafuegos tiene que tomar tras la detección de tráfico que cumple con los criterios de seguridad.

En la etapa 404, se configuran ajustes para la capa de red. Tales ajustes pueden incluir una designación de direcciones IP a bloquear (lista negra) u otros criterios de seguridad. Ajustes también puede incluir, por ejemplo, una designación de una lista blanca que consta de direcciones IP de anfitriones/redes para garantizar acceso sin inspección adicional u otras reglas basándose en la información recibida en la petición de contenido. La Figura 6 ilustra una interfaz de usuario para configurar los ajustes de capa de red introduciendo direcciones IP individualmente o en notación de CIDR (encaminamiento entre dominios sin clase).

Una configuración particular del cortafuegos puede usarse para evaluar algunas peticiones de contenido, pero no otras. En la etapa 406, se define el uso de la configuración. Esto puede lograrse designando criterios que indican que la configuración se aplicará, denominados como Objetivos de Coincidencia. Por ejemplo, los ajustes mostrados en la Figura 5 y 6 pueden aplicarse únicamente a peticiones de contenido desde dominios o subdominios seleccionados o pueden aplicarse únicamente a peticiones para ciertas clases de contenido (por ejemplo, aquellos con extensiones de archivo especificadas o con otras características). La Figura 7 ilustra una interfaz de usuario para especificar tales criterios.

El proceso de configuración del cortafuegos también puede incluir definir reglas para la capa de transporte (por ejemplo, el cortafuegos puede configurarse para tratar tráfico usando TCP de forma diferente que tráfico usando UDP u otros protocolos) u otras capas de interconexión. Aunque habitualmente se aplicará una configuración de cortafuegos de forma uniforme a través de servidores de contenido para un cliente dado, en realizaciones alternativas los cortafuegos que operan en diferentes servidores de contenido pueden configurarse de forma diferente para el cliente dado.

En la etapa 408, la configuración del cortafuegos se despliega a servidores de contenido en la CDN (por ejemplo, desplegando un archivo de configuración de metadatos en un canal de comunicación, como se describe anteriormente).

2.1 Archivos de configuración

En una realización preferida, el módulo de CF implica dos archivos de configuración: (1) un archivo de configuración de reglas de CF que gestiona las reglas de aplicación y red, así como Configuración de Notificación en Tiempo Real (denominado en este documento como un "archivo de configuración de metadatos de CF" o "archivo de configuración de reglas de CF"). (2) Archivo de configuración de localizador de recursos alternativos (ARL) estándar que gestiona los ajustes del sitio (denominado en este documento como un "archivo de configuración maestro"). Realizaciones alternativas pueden no usar archivos de configuración duales o usar archivos de configuración en absoluto.

2.2 Archivo de configuración de reglas de CF

Preferentemente, un cliente de CDN que se contrata para CF tiene únicamente un archivo de configuración de CF. A través del uso de Instancias de Cortafuegos y Objetivos de Coincidencia, pueden aplicarse políticas de CF separadas a diferentes propiedades digitales y URL con este único archivo. Esto sí proporciona alguna flexibilidad adicional que puede permitir que diferentes políticas de cortafuegos se apliquen a diferentes URL en la misma propiedad digital y permite que la misma política de cortafuegos se aplique a otras propiedades, también. La configuración de reglas de CF preferentemente contiene varios componentes:

Instancias de Cortafuegos - los ajustes a aplicar al objetivo de coincidencia.
Configuración de Controles de Capa de Aplicación
Configuración de Controles de Capa de Red
Configuración de Notificación en Tiempo Real (RTR)

Objetivos de Coincidencia - los criterios usados para determinar si la instancia de cortafuegos necesita aplicarse.

Objetivos de Coincidencia
Instancia de cortafuegos a aplicar
Aplicar Controles de Capa de Aplicación
Aplicar Controles de Capa de Red

2.3 Instancias de cortafuegos

Una instancia de cortafuegos representa el agrupamiento de controles habilitados que tienen que aplicarse a una petición cuando la instancia específica se suscita basándose en los criterios de Objetivo de Coincidencia. En una implementación, un Objetivo de Coincidencia puede suscitar únicamente una instancia de cortafuegos. Los Objetivos de Coincidencia pueden procesarse de tal forma que la coincidencia inferior gana y se usa la instancia de cortafuegos apropiada. Los Objetivos de Coincidencia también pueden procesarse de acuerdo con una jerarquía, de tal forma que un Objetivo de Coincidencia (y configuración de cortafuegos asociada) que aplica a dominio se supera por un Objetivo de Coincidencia que aplica a un subdominio, que se supera por un Objetivo de Coincidencia que aplica a un tipo de contenido particular y así sucesivamente.

Controles de Capa de Aplicación definen los criterios de seguridad a comprobar con cada petición y la acción a tomar si se identifica el ataque. Posibles acciones son Alertar (no denegar la petición, únicamente generar una alerta y continuar el procesamiento de la solicitud de HTTP) y Denegar (denegar la petición, resultando en una respuesta HTTP 403, generación de una alerta y detención del procesamiento de la solicitud de HTTP). Controles de Capa de Aplicación se agrupan en agrupaciones de nivel superiores para una clasificación de ataques, por ejemplo, basándose en ModSecurity o otros conjuntos de reglas. Dentro de cada clasificación, preferentemente existen varias reglas de detección específicas.

Clientes pueden aplicar únicamente las reglas específicas que eligen para seleccionar y configurar cada regla para o bien alertar, denegar o bien tomar otra acción.

Controles de Capa de Red definen las restricciones de IP, por ejemplo, que tienen que aplicarse al sitio. Peticiones desde direcciones IP particulares pueden bloquearse y/o permitirse, o puede aplicarse una lista negra/lista blanca

estricta. Múltiples direcciones IP pueden especificarse usando notación de CIDR.

Notificación en Tiempo Real define la URL, a través de una propiedad digital servida por CDN, a la que el proceso de servidor de borde (fantasma) PUBLICARÁ datos basándose en la regla o reglas que se desencadenaron. La CDN puede incluir un servicio de distribución de registro (LDS) basado en correo electrónico de servidor que notifica datos al cliente de CDN. El LDS de CDN pueden incluir opciones para añadir campos para W3C y formatos combinados. Para proporcionar más información en tiempo real al cliente de CDN, se usa Notificación en Tiempo Real para enviar datos específicos de CF a clientes rápidamente. Como los datos se envían como una PUBLICACIÓN, el cliente puede crear la aplicación de procesamiento de PUBLICACIÓN para reaccionar de cualquier forma apropiada a sus necesidades, tal como la generación inmediata de alertas o alertar únicamente su se generan X alertas en Y minutos.

Es útil apreciar la distinción entre activación/desactivación de una instancia de cortafuegos y habilitación/deshabilitación de procesamiento de reglas dentro de esa instancia. Activación/desactivación debería producirse infrecuentemente - únicamente cuando una instancia de cortafuegos se crea o borra por primera vez. Activación/desactivación controla el proceso de incluir/eliminar la referencia al fichero de datos de CF, por ejemplo, dentro de un archivo de configuración de metadatos mayor (que puede incluir otra información de control para el proceso fantasma de servidor de contenido). Preferentemente, implica la modificación/despliegue del archivo fantasma de metadatos (que incluye tal otra información de control).

Por otra parte, la habilitación/deshabilitación de procesamiento de reglas dentro de un instancia de cortafuegos activada se controla mediante la etiqueta de metadatos de estado contenida en el archivo de configuración. La modificación/despliegue de un archivo de configuración se concibe para ser un proceso más rápido que la modificación/despliegue del archivo de metadatos fantasma, preferentemente usando un canal de comunicación (desde el portal a los servidores de contenido) que se especializa para este propósito. De esta manera, la habilitación/deshabilitación de procesamiento de reglas puede producirse más frecuentemente (si se necesita que lo sea). La deshabilitación provoca que las reglas se ignoren hasta que se reactiven (las reglas aún estarán activadas el servidor de contenido pero no se ejecutarán hasta que se rehabiliten). La distribución rápida de configuración de cortafuegos por lo tanto preferentemente usa un canal de metadatos especializado para transportar archivo de configuración por cliente que referencia las reglas de Conjunto de Reglas Principal seleccionadas y reglas de bloqueo de IP para todas las instancias de cortafuegos de cliente.

2.4 Objetivos de Coincidencia

Un Objetivo de Coincidencia representa criterios específicos que indican que las reglas de cortafuegos deberían aplicarse. Si una URL coincide con un Objetivo de Coincidencia, se aplicará la instancia de cortafuegos especificada y los Controles de Capa de Aplicación y/o los Controles de Capa de Red, como se seleccionan para el Objetivo de Coincidencia.

Objetivos de Coincidencia requieren una propiedad digital de cliente de CDN (por ejemplo, un dominio de cliente, subdominio o similar) y al menos otro criterio de coincidencia de URI estándar: trayectoria, fichero por defecto y extensiones de archivo. Una vez que se evalúan todos los criterios de coincidencia, el proceso de servidor de contenido (fantasma) que ejecuta CF sabrá si tiene que aplicarse una instancia de cortafuegos y los controles dentro de esa instancia que tienen que aplicarse.

2.5 Archivo de configuración maestro

El archivo de configuración maestro de metadatos para la propiedad digital tiene el módulo de CF habilitado a través de una opción de características opcionales antes de que se use el archivo de configuración de reglas de CF, independientemente de los Objetivos de Coincidencia.

La configuración de reglas de CF se "inserta" en el archivo de configuración maestro dinámicamente usando una etiqueta, tal como la etiqueta <akamai:insert>. Cuando se habilita la característica opcional de CF, la etiqueta <akamai:insert> se inserta en el comienzo de los metadatos de sitio de cliente (véase, la Patente de Estados Unidos N.º 7.240.100) con las etiquetas apropiadas para identificar el archivo de configuración de reglas de CF. Como un requisito de seguridad cuando se habilita el módulo de CF, se habilita autenticación fantasma a fantasma (G2G).

2.6 Estructura de metadatos

La Figura 8 ilustra metadatos que codifican dos reglas ilustrativas que activan un cortafuegos cuando se cumplen ciertos criterios. Varias etiquetas y características se incluyen en la estructura de metadatos de modo que un proceso de servidor de contenido de CDN (por ejemplo, fantasma) puede soportar el procesamiento de conjunto de reglas.

En el ejemplo en la Figura 8, ambas acciones están dentro de <match:regex>, pero podría usarse realmente cualquier coincidencia o combinación de coincidencias. La etiqueta <akamai:fw-rules> se usa para agrupar juntas las

reglas de cortafuegos.

La siguiente terminología puede usarse:

Nombre	Definición
Metadatos de cortafuegos	Cualquier bloque de metadatos incluido dentro de <akamai : firewall-config>
Regla de cortafuegos	Combinación de una de más coincidencias y una acción. Reglas deben pertenecer a metadatos de cortafuegos.
Acción de cortafuegos	Metadatos que definen qué se hace cuando se desencadena la regla.

2.6.1 Controles de metadatos

La característica de CF se controla con las siguientes etiquetas de control de metadatos. En esta realización, se establecen en el comienzo del archivo de metadatos, antes de que se encuentre cualquier metadato de cortafuegos.

Etiqueta	Tipo	Por defecto	Descripción
security:firewall.off	bandera	desactivada	Esta es un conmutador de línea base para deshabilitar globalmente la característica de cortafuegos en la nube a través de todos clientes en caso de que se detecte un error de programación crítico.
security: firewall.activate	bandera	desactivada	Habilitar/deshabilitar la característica de cortafuegos en la nube. Si se deshabilita, se ignoran los metadatos de cortafuegos.
security: firewall.id	cadena	N/D	ID de aplicación. Esta se usa únicamente para notificación.
security: firewall.debug. activate	bandera	desactivada	Activar/desactivar depuración. Véase el párrafo acerca de depuración.
security: firewall.debug.max-limit	Entero	10	Número máximo de líneas por segundo en cache.log
security:	bandera	desactivada	Esto es útil para depuración.
firewall.debug.respect-xff			

2.6.2 Acciones

Acciones se definen con <security:firewall.action>, que es un nodo que se puede listar. El nodo <security:firewall.action> puede contener cualquiera de estas etiquetas:

Etiqueta	Tipo	Por defecto	Descripción
id	cadena	N/A	Identificador para la regla. Este es un parámetro obligatorio. Si la bandera de denegación está activada, la AK_FIREWALL_DENY_RULEID variable incorporada contiene este identificador.
reject	bandera	desactivada	Si el valor está desactivado, fantasma produce un aviso pero el flujo de control de la petición no se modifica. Si el valor está activado, fantasma detiene la evaluación de otras reglas y la petición de cliente se deniega.
msg	cadena	Cadena vacía	Mensaje de error para la acción. Se visualiza en registros.
tag	cadena	Cadena vacía	Etiqueta usada para categorizar la regla. Se visualiza en registros.
data	cadena	Cadena vacía	Datos de usuario asociados con la acción. Se visualizan en registros. Esta etiqueta es opcional. Se usa habitualmente para mostrar qué parte de la entrada coincidió con una expresión regular.
http-status	entero	403	Usada cuando denegación está "activa" para decidir qué página de error devolver al cliente. Necesita estar en el intervalo de 400-599.

Metadatos de cortafuegos se ejecutan si el cortafuegos en la nube se activa. Si una acción tiene la bandera de denegación activada, el flujo de control se reanuda después de los metadatos de cortafuegos. Una vez que se aplican metadatos para la etapa, el servidor de borde fantasma devolverá una página de error al usuario con el código de estado de error de la acción.

3.0 Procesamiento de petición de cortafuegos

La Figura 9 ilustra el procesamiento de una petición mediante un cortafuegos, que en muchas implementaciones se está ejecutando en o en conjunto con un servidor de contenido. En la etapa 900, se recibe una petición. Cuando una petición se hace a un servidor de contenido de CDN (o más particularmente, a un proceso fantasma que se ejecuta en ese servidor), la propiedad digital se evalúa para determinar el archivo de configuración apropiado a usar con la petición. (Véase, la Patente de Estados Unidos N.º 7.240.100.)

En la etapa 902, el archivo de configuración maestro para esa propiedad digital se recupera y evalúa. La configuración de reglas de CF (por ejemplo, metadatos en formato XML o de otra manera) se inserta en el archivo de configuración maestro de metadatos usando la etiqueta <akamai:insert>. (En otras realizaciones, el archivo de configuración de reglas de CF puede evaluarse de forma separada o puede usarse otro medio de comunicar la configuración de cortafuegos deseada.)

En la etapa 904, los Objetivos de Coincidencia de CF especificados en la configuración se evalúan para determinar si tiene que recurrirse a una instancia de cortafuegos. Por ejemplo, la petición puede probarse contra los criterios de Objetivo de Coincidencia mostrados en la Figura 7, anterior, para determinar si es para contenido desde un dominio coincidente, subdominio, tiene extensión de archivo coincidente y así sucesivamente. Si ninguno de los criterios se cumple, significando que el cliente configuró el cortafuegos para no activarse para peticiones de tal contenido, a continuación no necesita recurrirse al cortafuegos y CF finaliza. El proceso fantasma evalúa el resto del archivo de configuración maestro y la petición continúa procesándose por consiguiente. En respuesta a la petición, por ejemplo, el servidor de contenido puede servir contenido desde su caché o recuperar tal contenido desde el servidor de origen para distribuir al solicitante.

Si la petición coincide con un Objetivo de Coincidencia, a continuación en las etapas 910-914 se recurre a la instancia de cortafuegos para evaluar la petición contra los criterios de seguridad. Si la petición no cumple con ninguno de los criterios de seguridad, entonces la petición limpia el cortafuegos y continúa procesándose como normal, y de acuerdo con otras instrucciones en el archivo de configuración maestro. (Etapa 916.) Este procesamiento puede resultar en un servidor de contenido en la CDN que sirve el contenido solicitado desde su caché, o recupera el mismo desde un servidor de origen para distribuir al solicitante.

Si una condición de regla habilitada desencadena una condición de seguridad, entonces el cortafuegos toma una acción. La acción a tomar se especifica en el archivo de configuración de reglas. (Véase, la Figura 5.) Por ejemplo, en el modo "Únicamente Alerta", la alerta se anota/registra con la regla que desencadenó la alerta y las reglas de CF continúan procesándose contra la petición. (Etapas, 918, 920.) En el modo "Denegación", la alerta se anota/registra y se detiene el procesamiento de las reglas de CF y el archivo de configuración. (Etapas 918, 922.) Si se detectase cualquier acción de "alerta" o "denegación", se activará Notificación en Tiempo Real si se configura. Registros/notificaciones de ataques detectados, acciones tomadas y otra información relacionada con el módulo de cortafuegos se comunica al usuario a través del portal (extranet).

4.0 Implementación

Los clientes, servidores y otros dispositivos descritos en este documento puede implementarse en sistemas informáticos convencionales, según se modifican mediante los contenidos de este documento, con las características funcionales descritas anteriormente realizadas en software, hardware o una combinación de los mismos.

Software puede incluir uno o varios programas discretos. Cualquier función dada puede comprender parte de cualquier módulo dado, proceso, hilos de ejecución u otra construcción de programación tal. Generalizando, cada función descrita anteriormente puede implementarse como código informático, en concreto, como un conjunto de instrucciones informáticas, para realizar la funcionalidad descrita a través de ejecución de ese código usando medios convencionales, por ejemplo, un procesador, un ordenador, una máquina, un sistema, dispositivo de procesamiento de datos digital u otro aparato.

La Figura 10 es un diagrama de bloques que ilustra hardware en un sistema informático 1000 en el que tal software puede ejecutarse para implementar realizaciones de la invención. El sistema informático 1000 puede incorporarse en un dispositivo cliente, servidor, ordenador personal, estación de trabajo, ordenador de tableta, dispositivo inalámbrico, dispositivo móvil, dispositivo de red, encaminador, concentrador, pasarela u otro dispositivo.

El sistema informático 1000 incluye un procesador 1004 acoplado al bus 1001. En algunos sistemas, pueden emplearse múltiples procesadores y/o núcleos de procesadores. El sistema informático 1000 incluye adicionalmente una memoria principal 1010, tal como una memoria de acceso aleatorio (RAM) u otros dispositivo de almacenamiento, acoplada al bus 1001 para almacenar información e instrucciones a ejecutar mediante el procesador 1004. Una memoria de solo lectura (ROM) 1008 se acopla al bus 1001 para almacenar información e instrucciones para el procesador 1004. Un dispositivo de almacenamiento no volátil 1006, tal como un disco magnético, memoria de estado sólido (por ejemplo, memoria flash) o disco óptico, se proporciona y acopla al bus 1001 para almacenar información e instrucciones. Otros circuitos integrados específicos de la aplicación (ASIC), campo de matrices de puertas programables (FPGA) o circuitería pueden incluirse en el sistema informático 1000 para realizar funciones descritas en este documento.

Una interfaz periférica 1012 acopla comunicativamente el sistema informático 1000 a un visualizador de usuario 1014 que visualiza la salida de software que se ejecuta en el sistema informático, y un dispositivo de entrada 1015 (por ejemplo, un teclado, ratón, panel táctil, pantalla táctil) que comunica entrada de usuario e instrucciones al sistema informático 1000. La interfaz periférica 1012 pueden incluir circuitería de interfaz, lógica de control y/o de

desplazamiento de nivel para buses locales tal como RS-485, Bus Serial Universal (USB), IEEE 1394 u otros enlaces de comunicación.

El sistema informático 1000 se acopla a una interfaz de comunicación 1016 que proporciona un enlace (por ejemplo, en una capa física, capa de enlace de datos o de otra manera) entre el bus de sistema 1001 y un enlace de comunicación externo. La interfaz de comunicación 1016 proporciona un enlace de red 1018. La interfaz de comunicación 1016 puede presentar una Ethernet u otra tarjeta de interfaz de red (NIC), una interfaz inalámbrica, módem, una interfaz óptica u otra clase de interfaz de entrada/salida.

El enlace de red 1018 proporciona comunicación de datos a través de una o más redes a otros servicios. Tales dispositivos incluyen otros sistemas informáticos que son parte de una red de área local (LAN) 1026. Adicionalmente, el enlace de red 1018 proporciona un enlace, a través de un proveedor de servicio de internet (ISP) 1020, a la Internet 1022. A su vez, la Internet 1022 puede proporcionar un enlace a otros sistemas informáticos tal como un servidor remoto 1030 y/o un cliente remoto 1031. El enlace de red 1018 y tales redes pueden transmitir datos usando enfoques de transmisión de conmutación de paquetes, conmutación de circuitos u otros.

En la operación, el sistema informático 1000 puede implementar la funcionalidad descrita en este documento como resultado del procesador ejecutando código. Tal código habitualmente se lee de o proporciona mediante un medio legible por ordenador no transitorio, tal como la memoria 1010, ROM 1008 o dispositivo de almacenamiento 1006. Otras formas de medio legible por ordenador no transitorio incluyen discos, cintas, medios magnéticos, CD-ROM, medios ópticos, RAM, PROM, EPROM y EEPROM. También puede emplearse cualquier otro medio legible por ordenador no transitorio. También puede leerse código de ejecución del enlace de red 1018 (por ejemplo, a continuación de almacenamiento temporal en una memoria intermedia de interfaz, memoria local u otra circuitería).

REIVINDICACIONES

1. Un método de distribución de contenido en una red de distribución de contenidos, CDN, operada por un proveedor de servicios de red de distribución de contenidos, CDNSP, en nombre de una pluralidad de proveedores de contenido participantes, en el que la pluralidad de proveedores de contenido participantes identifican contenido a distribuir a través de la CDN, comprendiendo el método:

recibir uno o más primeros ajustes de cortafuegos desde un primer proveedor de contenido participante que especifica cómo tiene que operarse un cortafuegos con respecto a peticiones de contenido identificadas por el primer proveedor de contenido participante para distribuir a través de la CDN;
recibir uno o más segundos ajustes de cortafuegos desde un segundo proveedor de contenido participante que especifica cómo tiene que operarse un cortafuegos con respecto a peticiones de contenido identificadas por el segundo proveedor de contenido participante para distribuir a través de la CDN;
comunicar el uno o más primeros ajustes de cortafuegos y el uno o más segundos ajustes de cortafuegos con una pluralidad de servidores de contenido en la CDN;
en uno de la pluralidad de servidores de contenido en la CDN, recibir una primera petición de contenido identificada por el proveedor de contenido participante para distribuir a través de la CDN y evaluar la primera petición usando un cortafuegos configurado con el uno o más primeros ajustes de cortafuegos;
en uno de la pluralidad de servidores de contenido en la CDN, recibir una segunda petición de contenido identificada por el segundo proveedor de contenido participante para distribuir a través de la CDN y evaluar la segunda petición usando un cortafuegos configurado con el uno o más segundos ajustes de cortafuegos.

2. Una red de distribución de contenidos, CDN, operada por un proveedor de servicios de red de distribución de contenidos, CDNSP, en nombre de una pluralidad de proveedores de contenido participantes, en el que la pluralidad de proveedores de contenido participantes identifican contenido a distribuir a través de la CDN, comprendiendo la CDN una pluralidad de servidores de contenido que tienen un procesador y una memoria que almacena instrucciones que, cuando se ejecutan por el procesador, provocan que la pluralidad de servidores de contenido ejecuten las siguientes etapas:
recepción de uno o más primeros ajustes de cortafuegos que especifican cómo tiene que operarse un cortafuegos con respecto a peticiones de contenido identificadas por un primer proveedor de contenido participante para distribuir a través de la CDN;
recepción de uno o más segundos ajustes de cortafuegos que especifican cómo tiene que operarse un cortafuegos con respecto a peticiones de contenido identificadas por un segundo proveedor de contenido participante para distribuir a través de la CDN;
en uno de la pluralidad de servidores de contenido en la CDN, recepción de una primera petición de contenido identificada por el proveedor de contenido participante para distribuir a través de la CDN y evaluación de la primera petición usando un cortafuegos configurado con el uno o más primeros ajustes de cortafuegos;
en uno de la pluralidad de servidores de contenido en la CDN, recepción de una segunda petición de contenido identificada por el segundo proveedor de contenido participante para distribuir a través de la CDN y evaluación de la segunda petición usando un cortafuegos configurado con el uno o más segundos ajustes de cortafuegos.

3. El método de la reivindicación 1 o una CDN de acuerdo con la reivindicación 2, en el que una configuración de cortafuegos especificada por el uno o más primeros ajustes de cortafuegos es diferente de una configuración de cortafuegos especificada por el uno o más segundos ajustes de cortafuegos.

4. El método de la reivindicación 1 o una CDN de acuerdo con la reivindicación 2, en el que evaluar la primera petición usando un cortafuegos configurado con el uno o más primeros ajustes de cortafuegos comprende:

probar la primera petición contra uno o más criterios, y si se cumple el uno o más criterios, tomar una acción con respecto a la primera petición.

5. El método de la reivindicación 4, en el que la acción tomada es una acción protectora.

6. El método de la reivindicación 4, en el que evaluar la segunda petición usando un cortafuegos configurado con el uno o más segundos ajustes de cortafuegos comprende: probar la segunda petición contra uno o más criterios, y si se cumple el uno o más criterios, tomar una acción con respecto a la segunda petición.

7. El método de la reivindicación 1 o una CDN de acuerdo con la reivindicación 2, en el que cualquiera del uno o más primeros ajustes de cortafuegos y el uno o más segundos ajustes de cortafuegos especifican al menos uno de: (i) uno o más criterios contra los que probar una petición de contenido y (ii) una acción a tomar con respecto a una petición de contenido que cumple con uno o más criterios.

8. El método de la reivindicación 1 o una CDN de acuerdo con la reivindicación 2, en el que cualquiera del uno o más primeros ajustes de cortafuegos y el uno o más segundos ajustes de cortafuegos especifican uno o más criterios contra los que probar una petición de contenido, definiendo el uno o más criterios reglas que buscan identificar amenazas de seguridad.

9. El método de la reivindicación 1 o una CDN de acuerdo con la reivindicación 2, en el que cualquiera del uno o más primeros ajustes de cortafuegos y el uno o más segundos ajustes de cortafuegos especifican una acción a tomar con respecto a una petición si esa petición cumple con uno o más criterios, la acción seleccionada del grupo de acciones que son: denegar la petición, generar una alerta, modificar la petición, detener el procesamiento de la petición y registrar la petición.

10. El método de la reivindicación 1 o una CDN de acuerdo con la reivindicación 2, en el que cualquiera del uno o más primeros ajustes de cortafuegos y los segundos ajustes de cortafuegos especifican una o más direcciones IP, tráfico desde el cual se somete a una acción dada.

11. El método de la reivindicación 10, en el que cualquiera del uno o más primeros ajustes de cortafuegos y los segundos ajustes de cortafuegos especifican una o más direcciones IP desde las que se bloquea tráfico.

12. El método de la reivindicación 1 o una CDN de acuerdo con la reivindicación 2, en el que al menos uno de la primera petición y la segunda petición es una petición de capa de aplicación.

13. El método de la reivindicación 12, en el que al menos uno de la primera petición y la segunda petición es una solicitud de HTTP.

14. El método de la reivindicación 1 o una CDN de acuerdo con la reivindicación 2, en el que el uno o más los primeros ajustes de cortafuegos y el uno o más segundos ajustes de cortafuegos se comunican a la pluralidad de servidores de contenido en un archivo de configuración de metadatos.

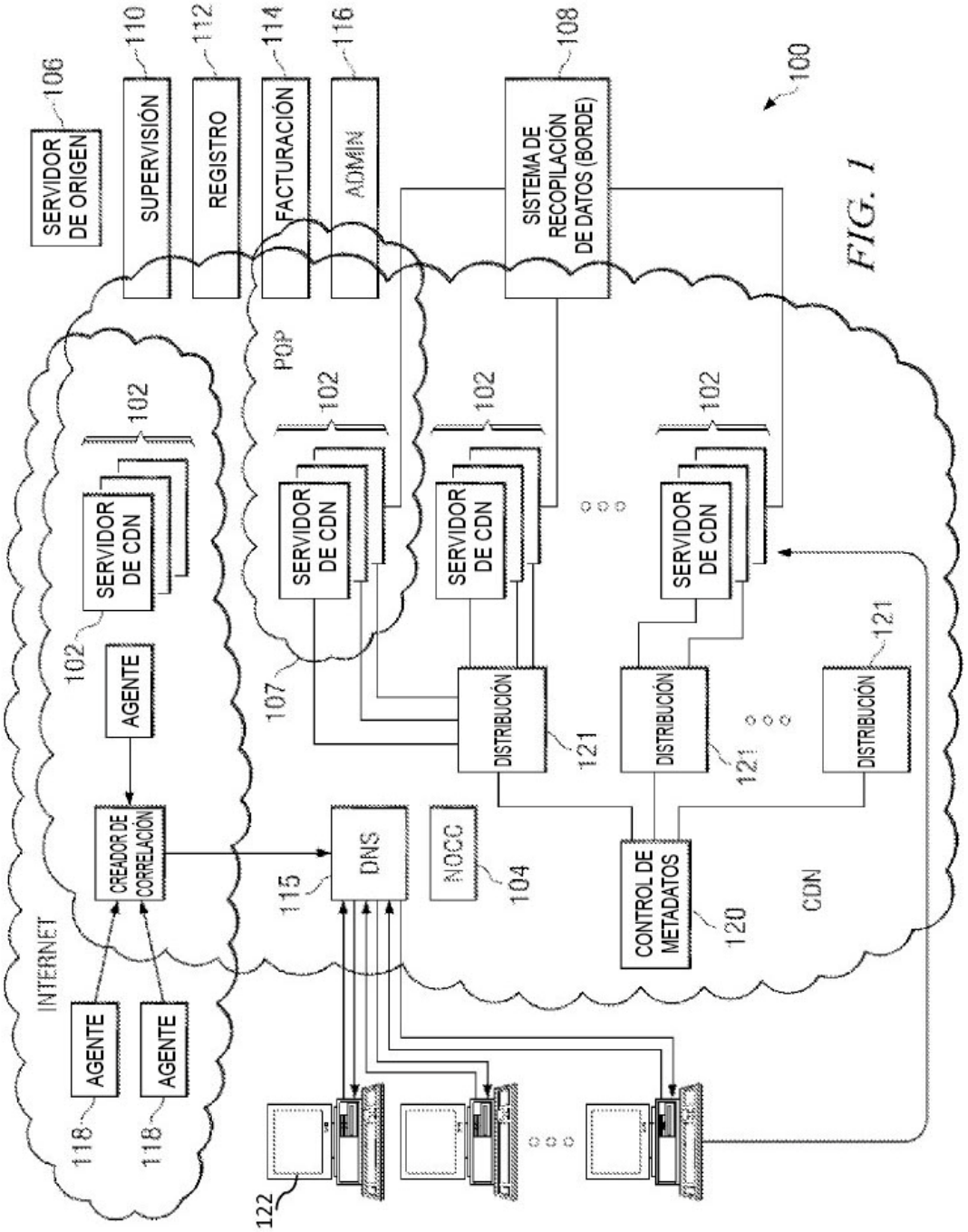

SERVIDOR DE ORIGEN
106
SUPERVISIÓN
110
REGISTRO
112
FACTURACIÓN
114
ADMIN
116
SISTEMA DE RECOPILACIÓN DE DATOS (BORDE)
108
100
POP
102
SERVIDOR DE CDN
AGENTE
CREADOR DE CORRELACIÓN
DISTRIBUCIÓN
121
DNS
115
NOCC
104
CONTROL DE METADATOS
120
CDN
INTERNET
118
122
107

FIG. 1

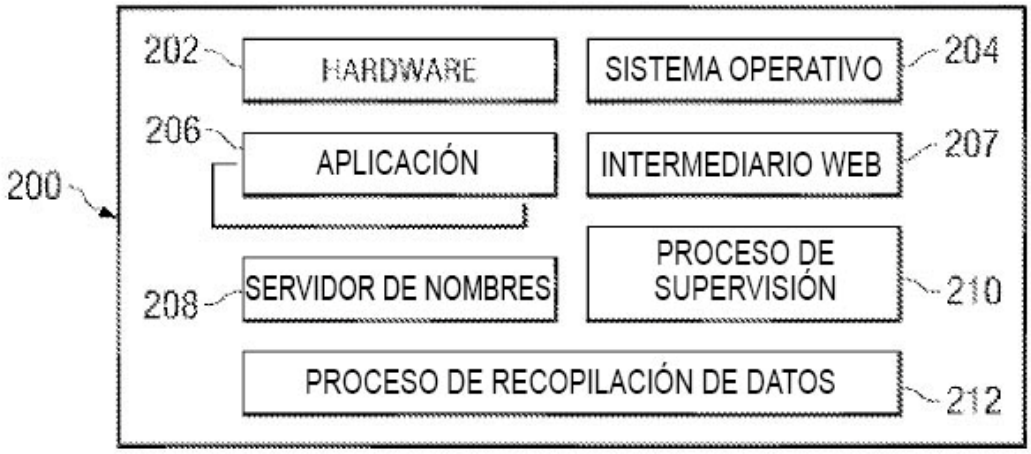

200
202
HARDWARE
204
SISTEMA OPERATIVO
206
APLICACIÓN
207
INTERMEDIARIO WEB
208
SERVIDOR DE NOMBRES
PROCESO DE SUPERVISIÓN
210
PROCESO DE RECOPILACIÓN DE DATOS
212

FIG. 2

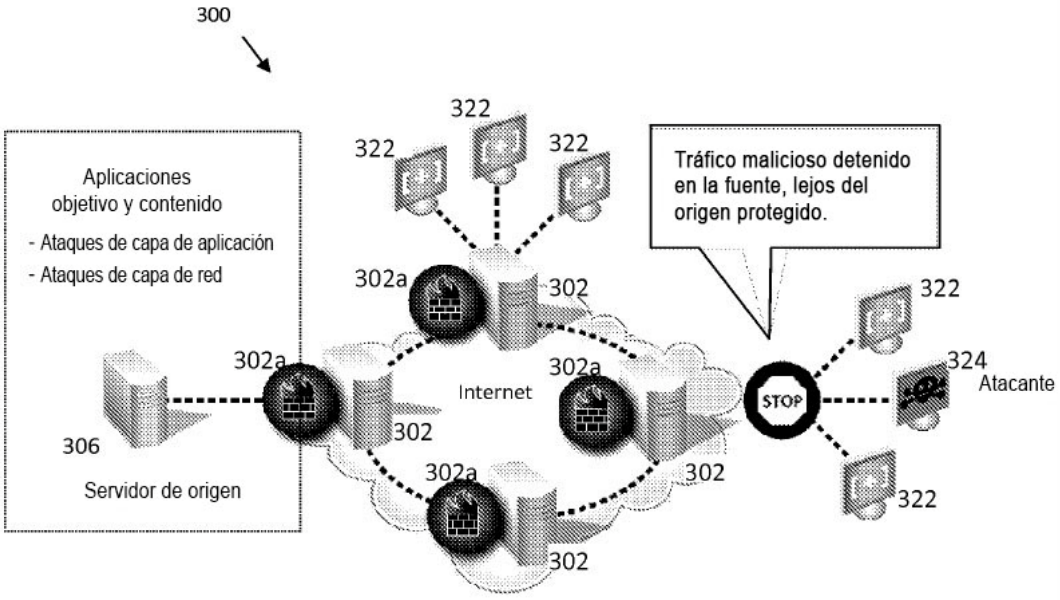

300
Aplicaciones
objetivo y contenido
- Ataques de capa de aplicación
- Ataques de capa de red
306
Servidor de origen
322
322
322
302a
302
302a
302
Internet
302a
302
302a
302
Tráfico malicioso detenido
en la fuente, lejos del
origen protegido.
STOP
322
324
Atacante
322

Fig. 3

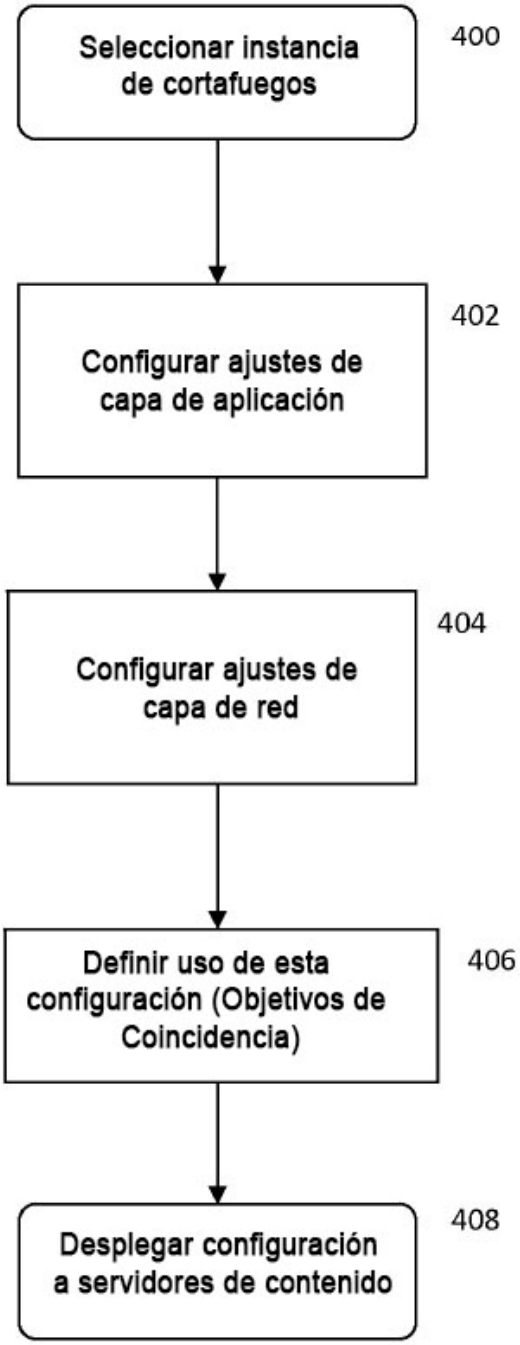

Seleccionar instancia de cortafuegos
400
Configurar ajustes de capa de aplicación
402
Configurar ajustes de capa de red
404
Definir uso de esta configuración (Objetivos de Coincidencia)
406
Desplegar configuración a servidores de contenido
408

Fig. 4

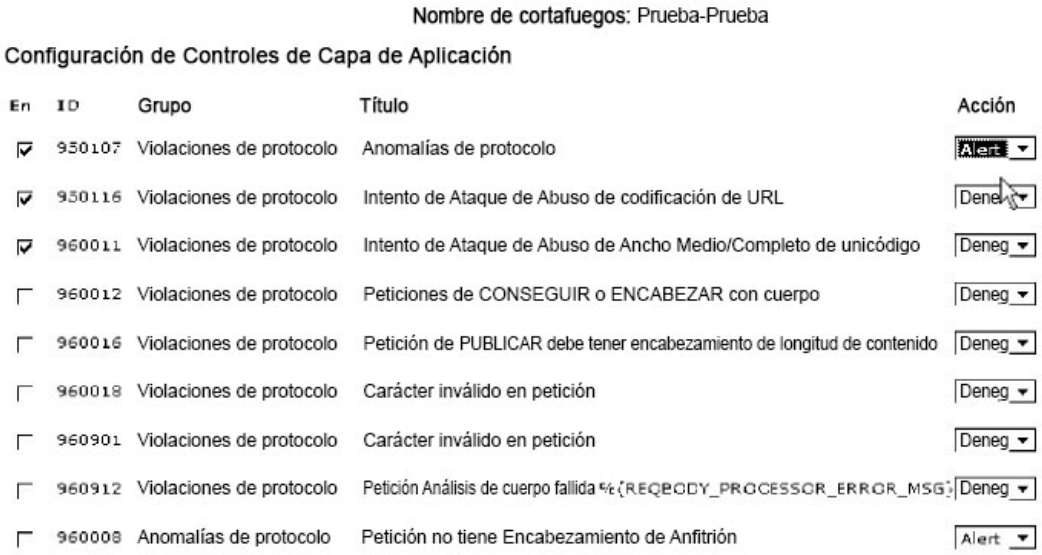

Nombre de cortafuegos: Prueba-Prueba
Configuración de Controles de Capa de Aplicación
En ID Grupo Título Acción
950107 Violaciones de protocolo Anomalías de protocolo Alert
950116 Violaciones de protocolo Intento de Ataque de Abuso de codificación de URL Deneg
960011 Violaciones de protocolo Intento de Ataque de Abuso de Ancho Medio/Completo de unicódigo Deneg
960012 Violaciones de protocolo Peticiones de CONSEGUIR o ENCABEZAR con cuerpo Deneg
960016 Violaciones de protocolo Petición de PUBLICAR debe tener encabezamiento de longitud de contenido Deneg
960018 Violaciones de protocolo Carácter inválido en petición Deneg
960901 Violaciones de protocolo Carácter inválido en petición Deneg
960912 Violaciones de protocolo Petición Análisis de cuerpo fallida %{REQBODY_PROCESSOR_ERROR_MSG} Deneg
960008 Anomalías de protocolo Petición no tiene Encabezamiento de Anfitrión Alert

Fig. 5

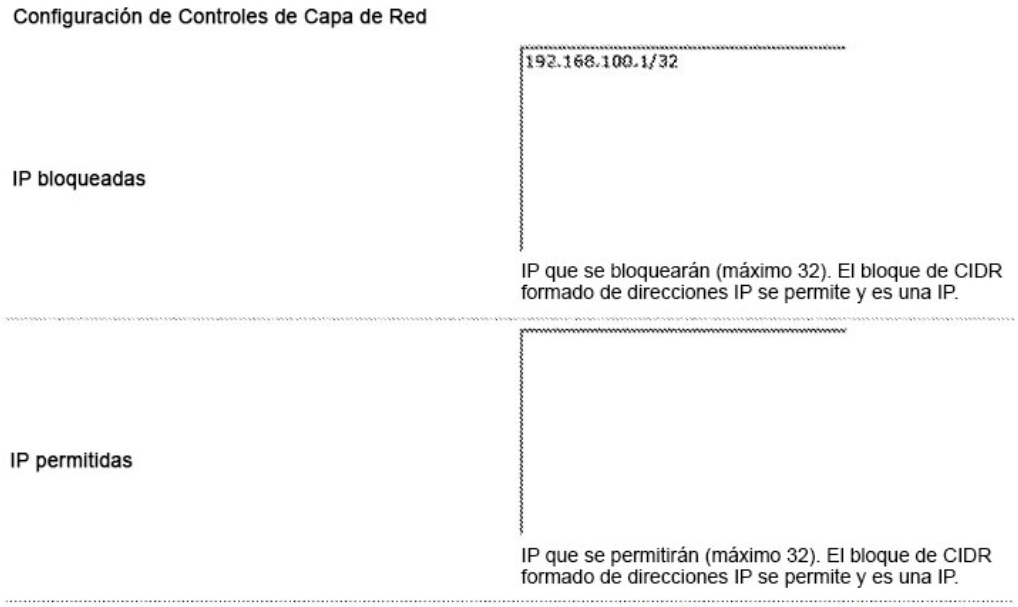

Configuración de Controles de Capa de Red
192.168.100.1/32
IP bloqueadas
IP que se bloquearán (máximo 32). El bloque de CIDR formado de direcciones IP se permite y es una IP.
IP permitidas
IP que se permitirán (máximo 32). El bloque de CIDR formado de direcciones IP se permite y es una IP.

Fig. 6

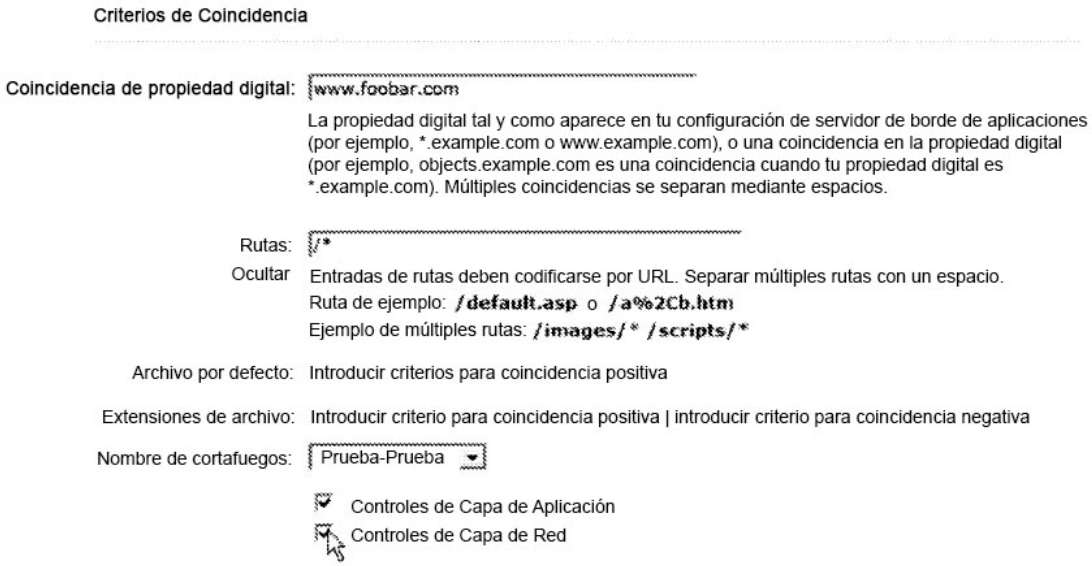
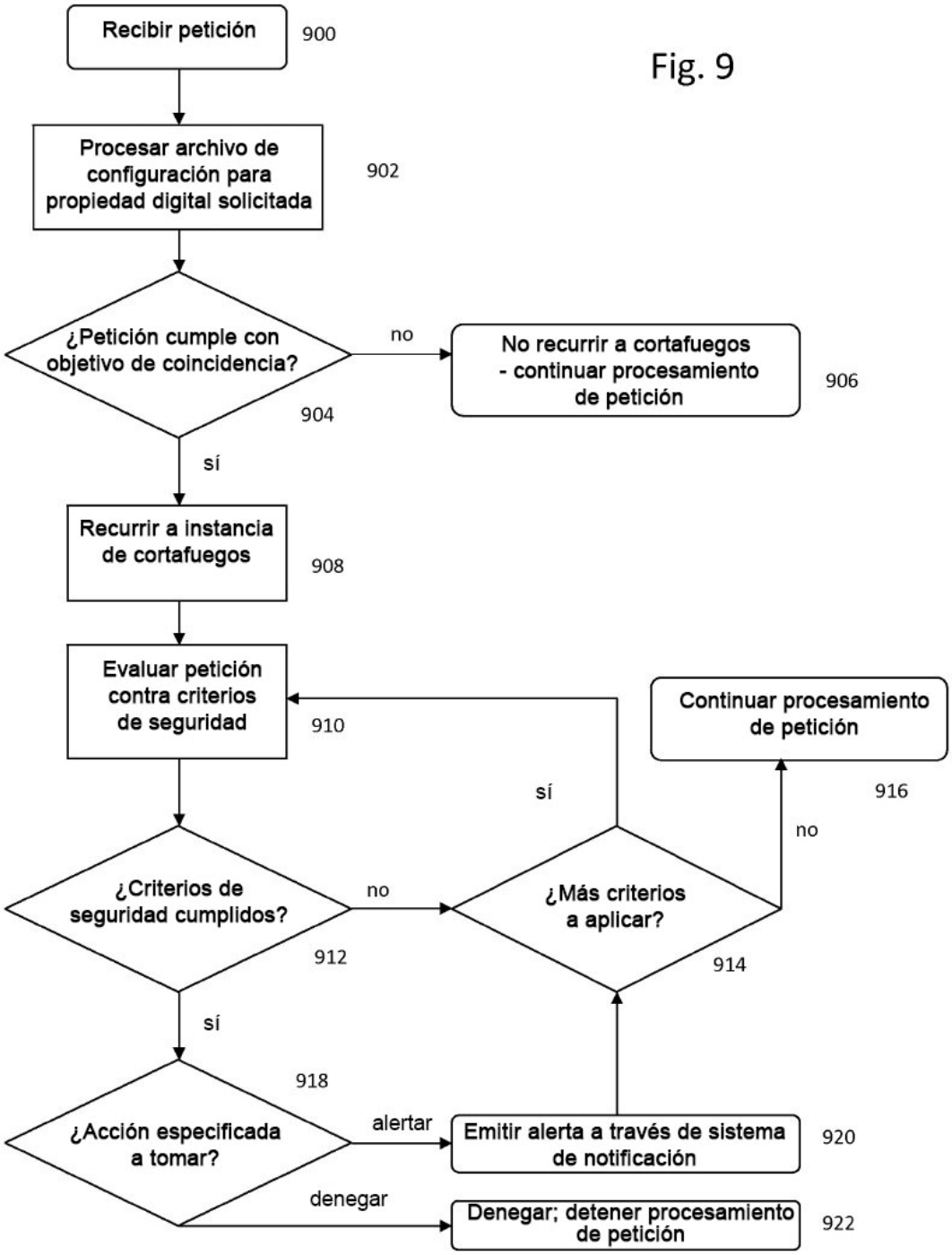

Criterios de Coincidencia
Coincidencia de propiedad digital:
www.foobar.com
La propiedad digital tal y como aparece en tu configuración de servidor de borde de aplicaciones (por ejemplo, *.example.com o www.example.com), o una coincidencia en la propiedad digital (por ejemplo, objects.example.com es una coincidencia cuando tu propiedad digital es *.example.com). Múltiples coincidencias se separan mediante espacios.
Rutas:
/*
Ocultar
Entradas de rutas deben codificarse por URL. Separar múltiples rutas con un espacio.
Ruta de ejemplo: /default.asp o /a%2Cb.htm
Ejemplo de múltiples rutas: /images/* /scripts/*
Archivo por defecto:
Introducir criterios para coincidencia positiva
Extensiones de archivo:
Introducir criterio para coincidencia positiva | introducir criterio para coincidencia negativa
Nombre de cortafuegos:
Prueba-Prueba
Controles de Capa de Aplicación
Controles de Capa de Red

Fig. 7

```
1.  <security:firewall.activate>on<security:firewall.activate>
2.
3.  <akamai:firewall-config>
4.
5.          <!-- Regla 1: denegar peticiones con “root.exe” en la url -->
6.          <match:regex string=”%(AK_URL)” regex=”root\.exe”>
7.                  <security:firewall.action>
8.                          <reject>on</reject>
9.                          <id>1</id>
10.                         <msg>Fishy url</msg>
11.                 <security:firewall.action>
12.         </match:regex>
13.
14.         <!-- Regla 2: denegar peticiones con “crawler” en agente de usuario-->
15.         <match:regex select=”REQUEST_HEADER:User-Agent” regex=”crawler”>
16.                 <security:firewall.action>
17.                         < reject >on</reject>
18.                         <id>2</id>
19.                         <msg>Fishy user-agent</msg>
20.                 <security:firewall.action>
21.         </match:regex>
22.
23. </akamai:firewall-config>
```

Fig. 8

Fig. 9


Recibir petición
900
Procesar archivo de configuración para propiedad digital solicitada
902
¿Petición cumple con objetivo de coincidencia?
904
no
No recurrir a cortafuegos - continuar procesamiento de petición
906
sí
Recurrir a instancia de cortafuegos
908
Evaluar petición contra criterios de seguridad
910
¿Criterios de seguridad cumplidos?
912
no
¿Más criterios a aplicar?
914
sí
no
Continuar procesamiento de petición
916
sí
¿Acción especificada a tomar?
918
alertar
Emitir alerta a través de sistema de notificación
920
denegar
Denegar; detener procesamiento de petición
922

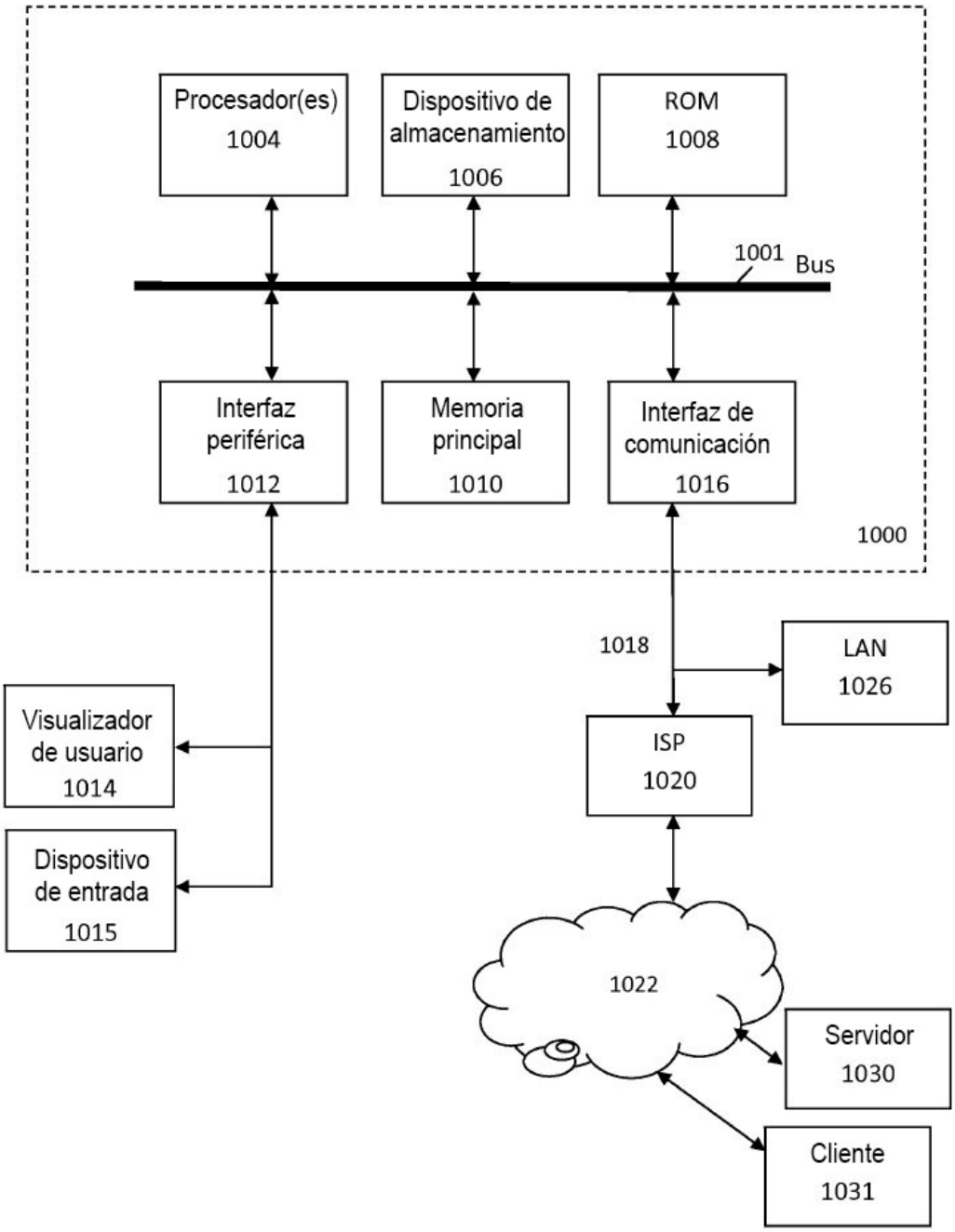

Procesador(es)
1004
Dispositivo de almacenamiento
1006
ROM
1008
1001
Bus
Interfaz periférica
1012
Memoria principal
1010
Interfaz de comunicación
1016
1000
1018
LAN
1026
Visualizador de usuario
1014
ISP
1020
Dispositivo de entrada
1015
1022
Servidor
1030
Cliente
1031

Fig. 10